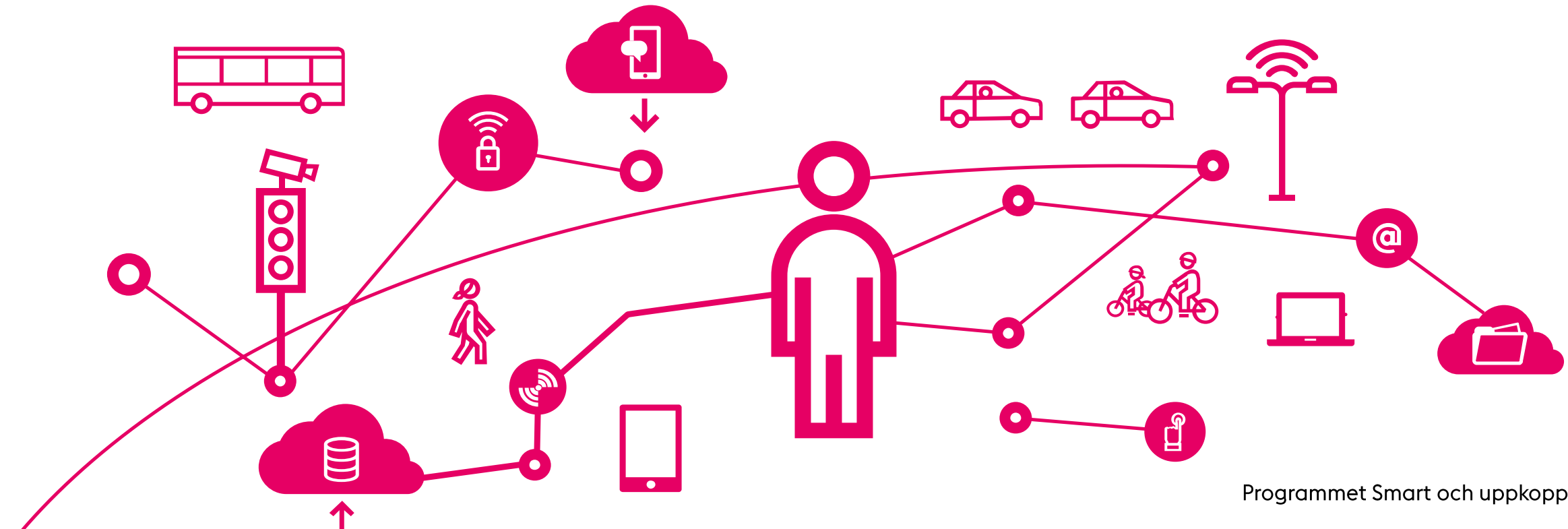


Projekt IoT Stockholm

Målarkitektur för IoT och dataplattformar

- Samla in, bearbeta och dela data
- [Version 1.0 2020-12-18]



Innehållsförteckning

1. Syfte, innehåll och omfattning	3
2. IoT-arkitektur	7
– Vägval	8
– Edge/ytterkant	14
– IoT-plattform	20
– Dataströmmar	31
3. Förhållande till övrigt IT-landskap	34

Dokumentets syfte, innehåll och omfattning

Syfte, innehåll och omfattning

- 1 Presentationen är en sammanfattning av Målarkitekturen, vilken beskrivs mer i detalj i huvudversion med samma namn i .docx,, .pdf. *Dokument finns hos SLK it- och digitalisering, projektet IoT Stockholm*
- 2 Presentationen syftar till att förklara hur IoT kan användas och implementeras. Målarkitekturen beskrivs på hög nivå och hur den delas upp konceptuellt i Edge, Plattform och Verksamhet
- 3 Beskriva enhetshantering i syfte att sätta ramarna för vilka förmågor enhetshanteringen behöver för att kunna skala upp IoT-lösningar i hela staden
- 4 Beskriva översiktliga metoder för hur tillgängliggörande och användning av insamlad IoT-data och insikter kan ske med tillsammans med befintliga plattformar i staden
- 5 Beskriva var Målarkitekturen för IoT och datahantering befinner sig i förhållande till arkitekturen för den smarta och uppkopplade staden
- 6 Belysa IoT-säkerhetsfrågor som behöver hanteras i samband med användning av IoT

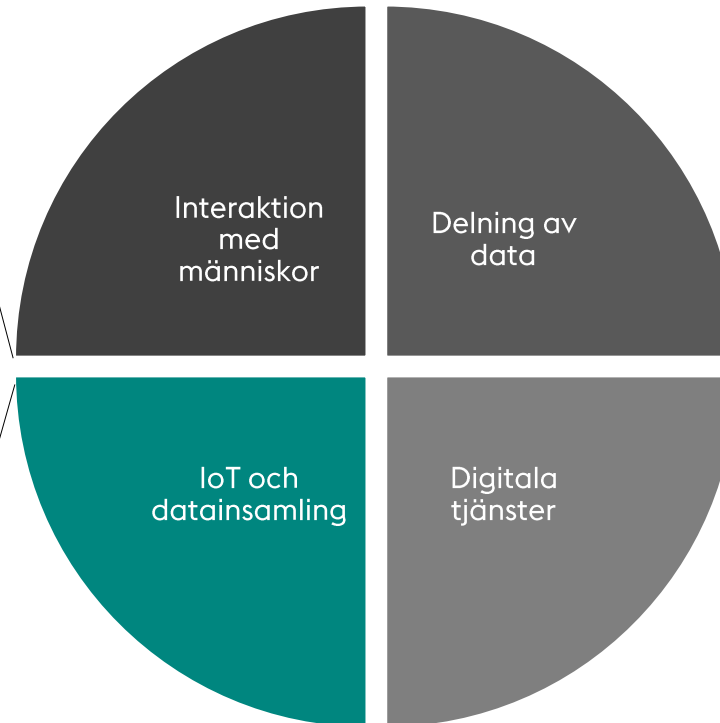
Arkitektur för den smarta staden Stockholm

En smart och uppkopplad stad kräver att verksamheterna har ett väl fungerande it-stöd för att de ska kunna utföra sina uppdrag kopplat till verksamhetssystem, analys- och processtöd

En smart stad har flera arkitekturella delar som bygger på befintlig verksamhets-it

Digitala platser för **interaktion mellan människor och den smarta staden**. Det kan vara appar, portaler, högtalare, enheter eller likande digitala platser för att människor ska få tillgång till stadens digitala tillgångar, tjänster och information

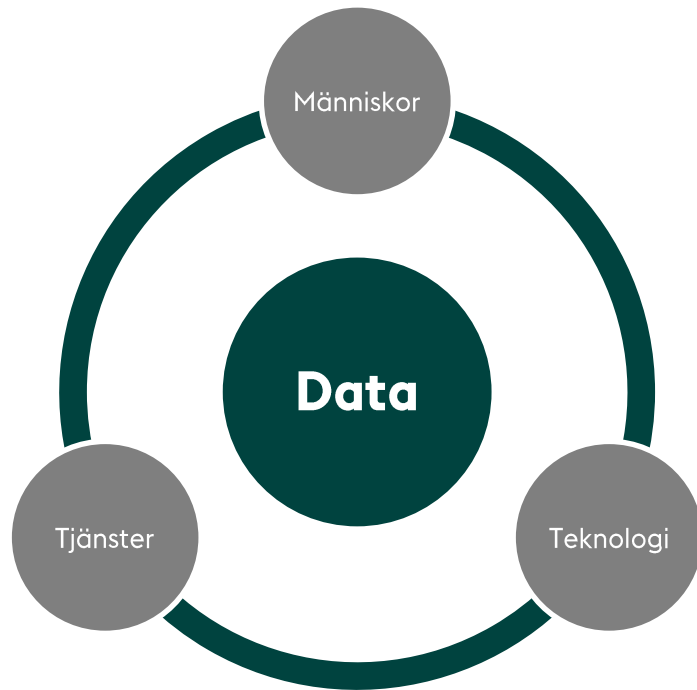
Arkitektur för IoT och datainsamling med förmågor att samla in, hantera data från IoT-enheter och tillgängliggöra data till verksamheten



Delning av data från staden både internt mellan verksamheter och externt utanför stadens verksamheter

Tjänsteorienterad arkitektur för att möjliggöra via **digitala tjänster**, som API:er, hantera förfrågningar från medborgare, näringsliv, internt mellan förvaltningar i staden och andra samhällsfunktioner att få en tjänst utförd

Tillgång till data är en grundförutsättning i en smart och uppkopplad stad



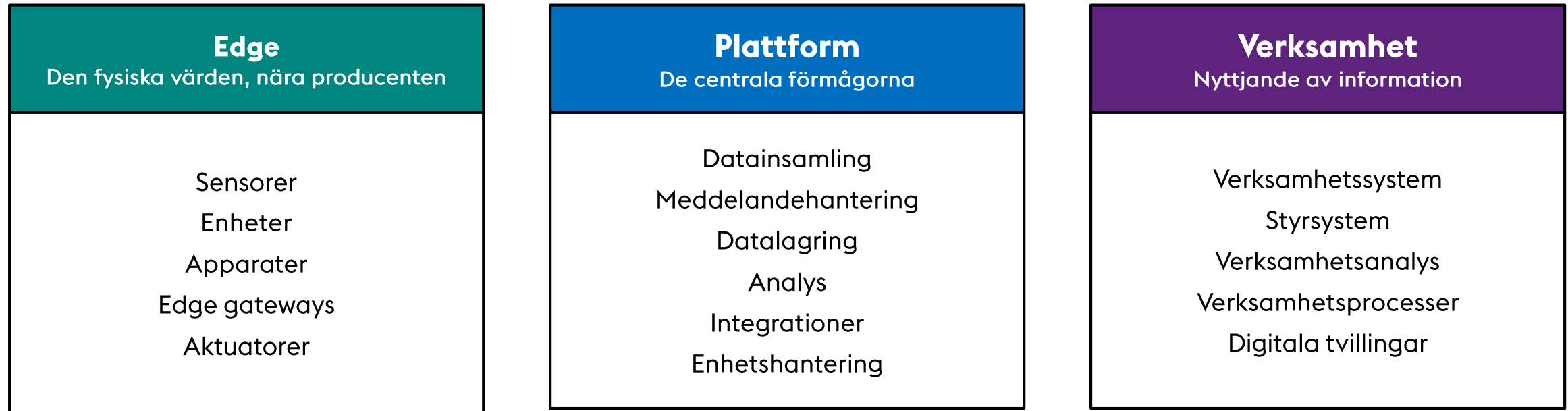
- Interaktionen med människor kan ske utan tillgång till data men utan insikter och information finns inget att berätta eller erbjuda
- Om tjänster ska kunna tillgängliggöras digitalt måste informationen, det vill säga data, också vara digital
- Teknologin kan skapa värde och möjlighet för att driva och utveckla befintliga förmågor i verksamheten
- Med hjälp av data kan beslutsfattare och tjänstemän fatta beslut baserade på information istället för uppskattningar och modeller

IoT-arkitektur

- Edge/Ytterkant
- IoT-plattform
- Verksamhetssystem
- Vägval

Uppdelning av IoT arkitekturen på hög nivå

IoT arkitekturen utgår från tre huvudsakliga delar – Edge, Plattform och Verksamhet. I den smarta staden samverkar dessa delar med varandra

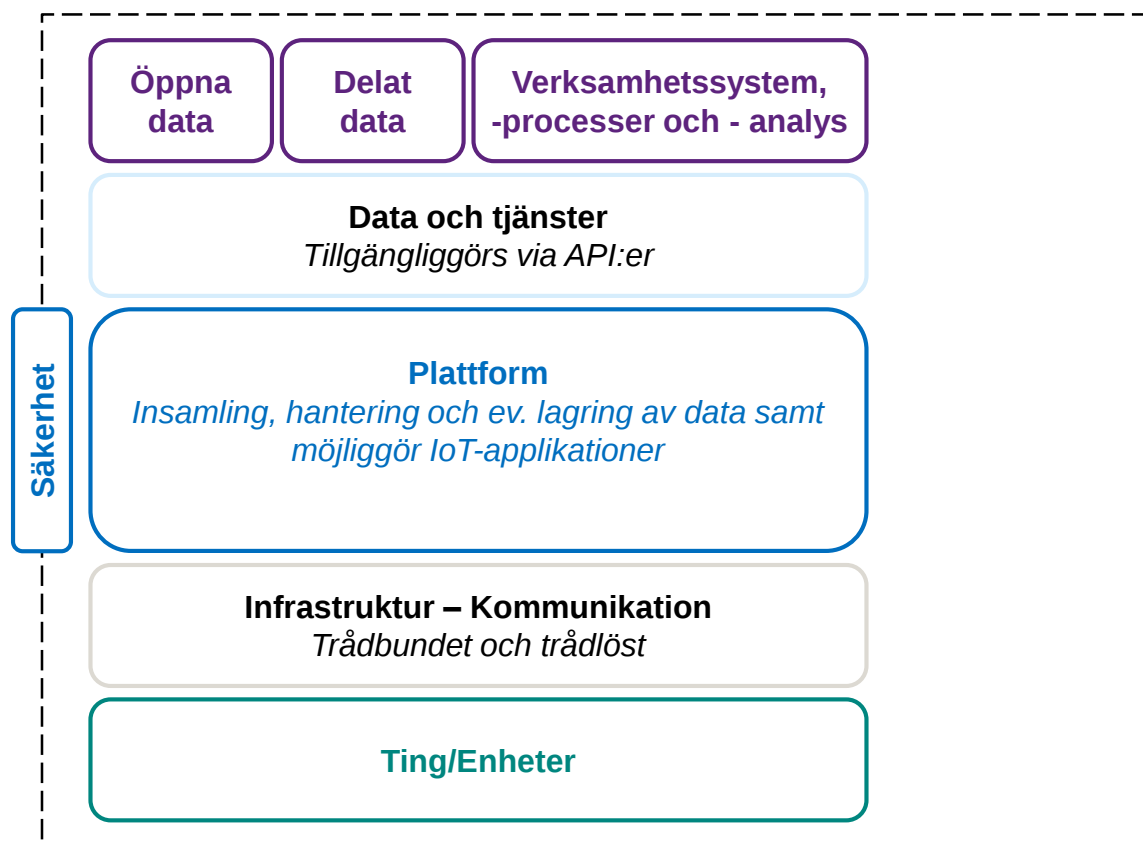


Färgkodning IoT arkitektur

● Edge ● Gemensamma förmågor ● Verksamhetssystem

Arkitektur för insamling av data

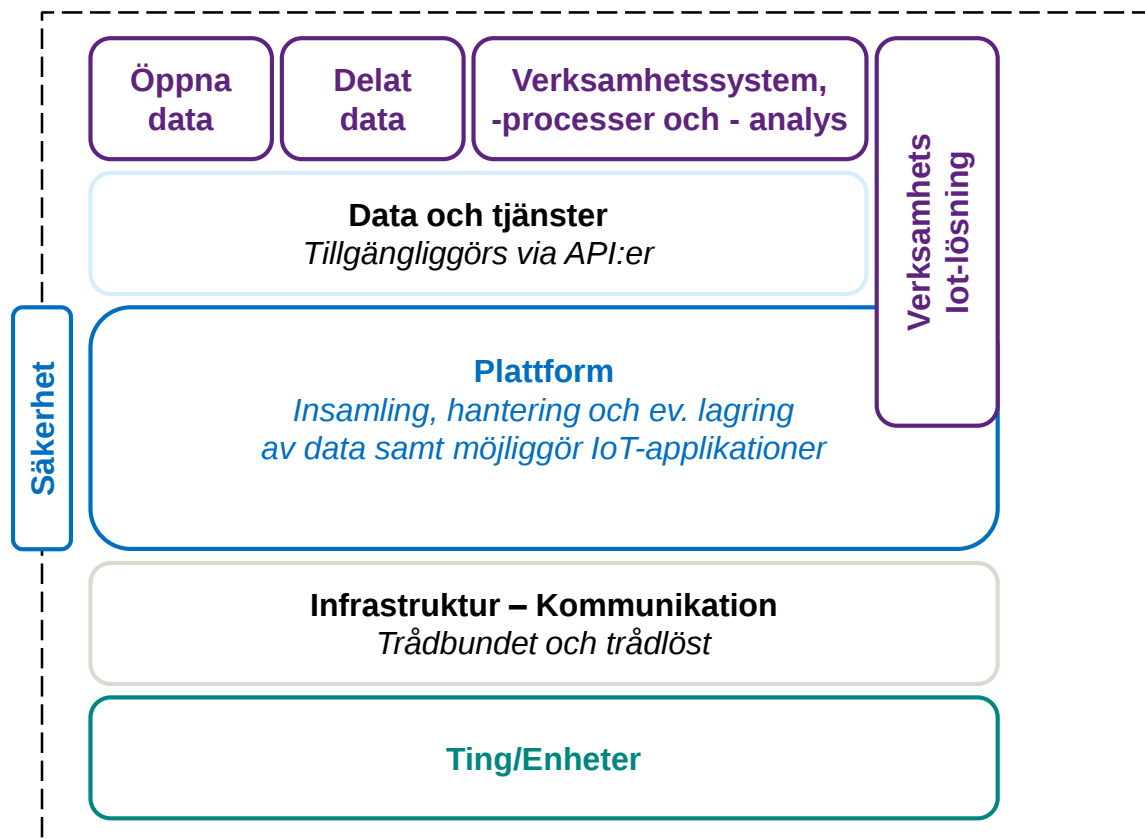
Insamling av data från Edge direkt till verksamhetsanvändning



- För Edge är arkitekturen och tekniska krav på enheterna gemensamma
- Befintlig kommunikationsinfrastruktur används för kommunikationen mellan Edge och plattform
- Vid insamling av data ska de gemensamma förmågorna i Plattformen användas
- Data som uppstår i plattformen tillgängliggörs som API:er med hjälp av Integrationsplattformen
- Data som tillgängliggörs används i befintliga verksamhetsprocesser genom integration i verksamhetssystem eller för analys
- Tillgängliggjorda API:er kan delas som öppet eller delat data

Arkitektur för IoT-lösning

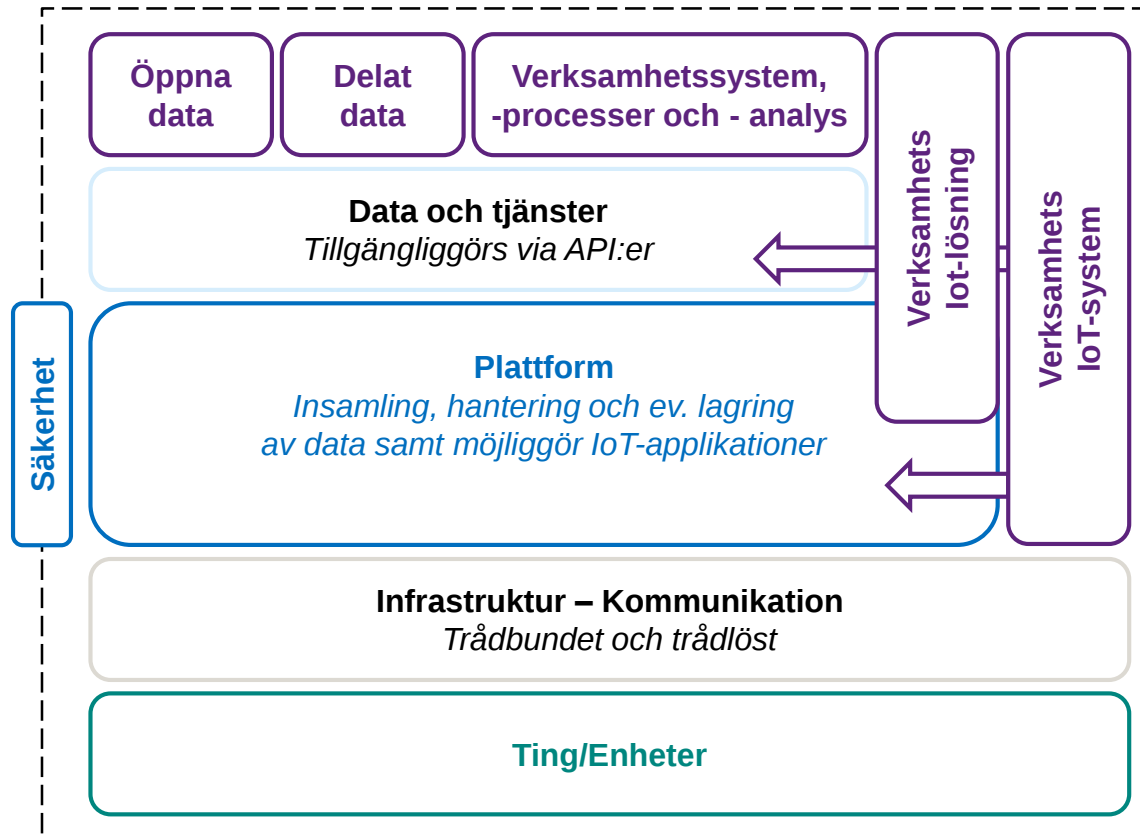
Använda plattformsförmågor till hantering av data



- Vid skapande av unika lösningar för att hantera data, t.ex. transformera eller filtrera innan det kan tillgängliggöras till verksamheten används plattformens förmågor
- Vi behov av lösning som återkopplar till enheterna i Edge baserat på data från Edge eller andra källor används plattformens förmågor
- Lösningen kan antingen upphandlas som ett system baserad på den gemensamma plattformens teknologi alternativt utvecklas med plattformens förmågor och teknologier

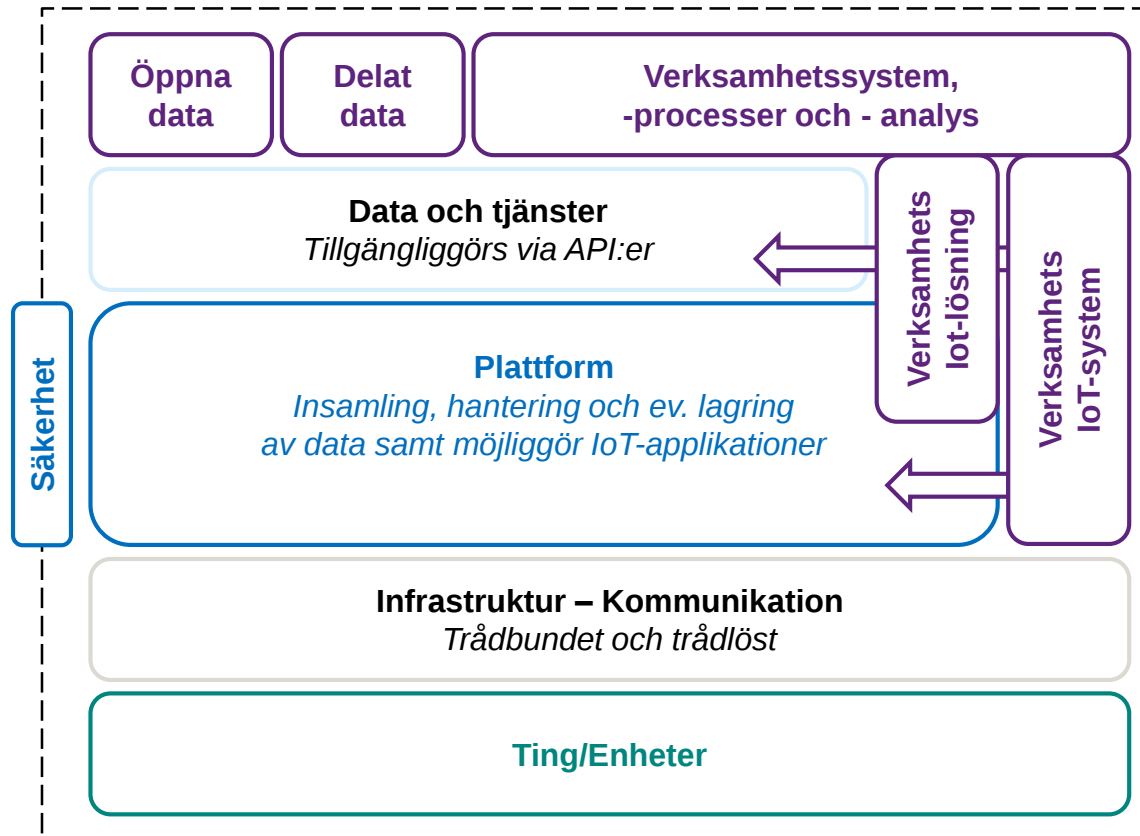
Arkitektur för IoT-system

Specifika verksamhetsbehov



- Det finns verksamheter och verksamhetsbehov som behöver samma förmågor som plattformen erbjuder men ändå inte ska/kan implementeras i plattformen
- Det är framförallt system som är specialiserade på att styra/interagera med enheter som utför specialiserade verksamhetsuppgifter, exempel på detta kan vara att styra vägbommar, hantera vattenpumpar
- System av mycket känslig art som direkt kan påverka "liv och död" bör hanteras för sig
- För att kunna hantera denna typ av system behöver ändå *arkitekturen för IoT och datainsamling* följas för att systemet kan utnyttja gemensamma förmågor vid behov

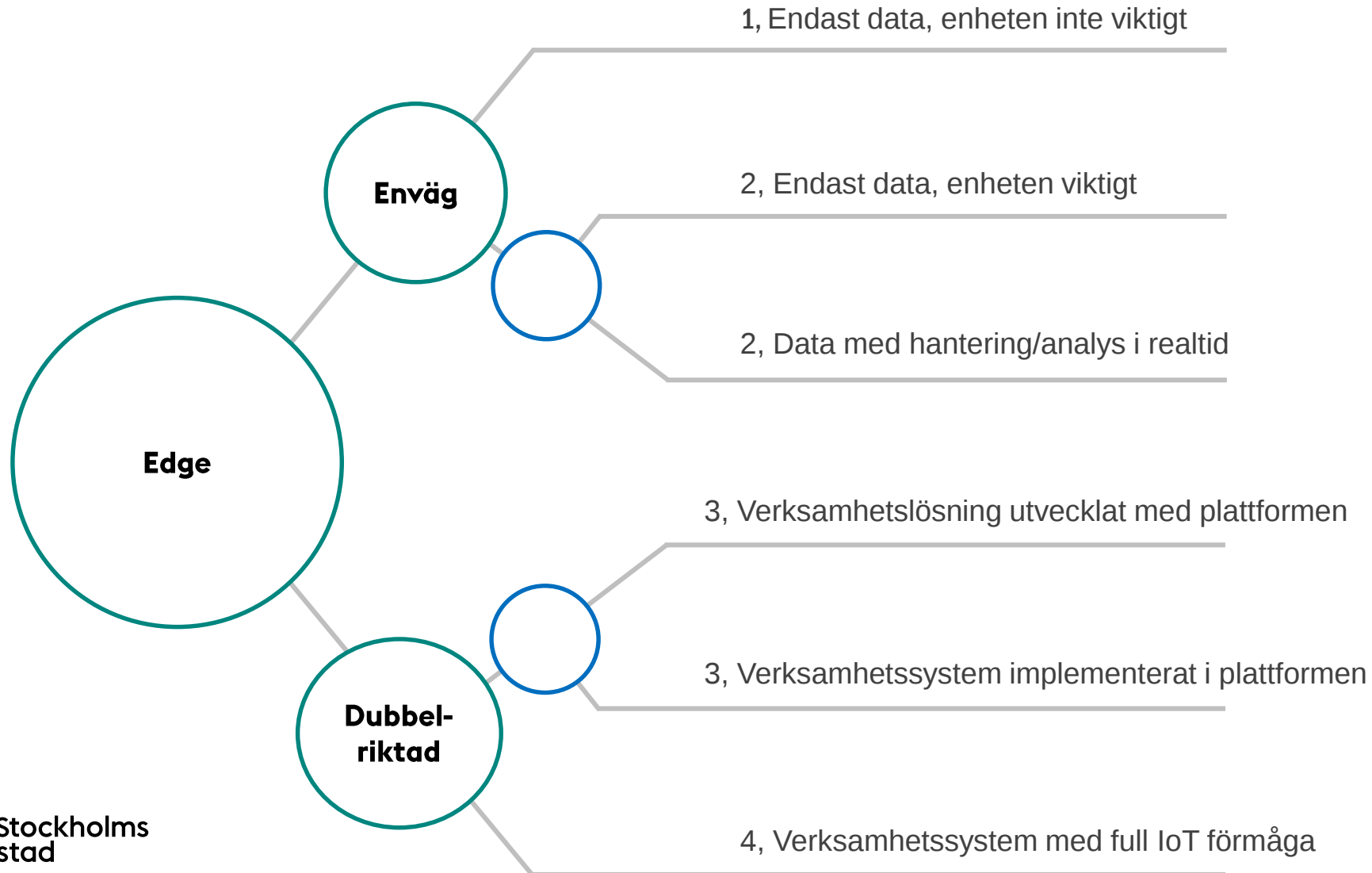
Arkitektur för IoT integrerad som en del smarta staden



- När IoT-lösningarna och IoT-systemen är en naturlig och integrerad del av verksamhetssystem och verksamhetsprocesser finns ingen skillnad mellan IoT eller andra informationskällor eller informationshantering

Vilket mönster ska man välja?

Det är viktigt att först bestämma till vad och vart i verksamheten informationen ska användas!



Beskrivning av Edge/Ytterkant

Funktioner i Edge

I ytterkant (Edge) finns ting (IoT-enheter) som kan producera och dela data med resten av arkitekturen. En IoT-enhet kan delas upp utifrån tre huvudfunktioner enligt nedan

Sensor/Aktuator

Den del som interagerar med den riktiga analoga världen.

- **Sensor:** Mäter eller känner av omgivningen och/eller enhetens status (temperatur, passage, radioaktivitet etc.).
- **Aktuator:** Agera eller återkoppla på omgivningen. T.ex. tryckknappar och dimmer.

Hantering och kontroll

Insamling och **hantering** av det avlästa analoga värdet till digitalt data.

Beroende på hur intelligent enheten är kan den agera direkt på data från sensorn för att t.ex. styra en aktuator i enheten genom att:

- Öka fläkthastigheten vid överstigen temperatur
- Slå på en lampas strömbrytare vid mörker
- Alternativt "bara" skicka data vidare till kommunikation

Enheten kan även ha komplex hantering (Edge computing) som t.ex. AI-funktioner för bildigenkänning, röstförståelse eller aggregering av data.

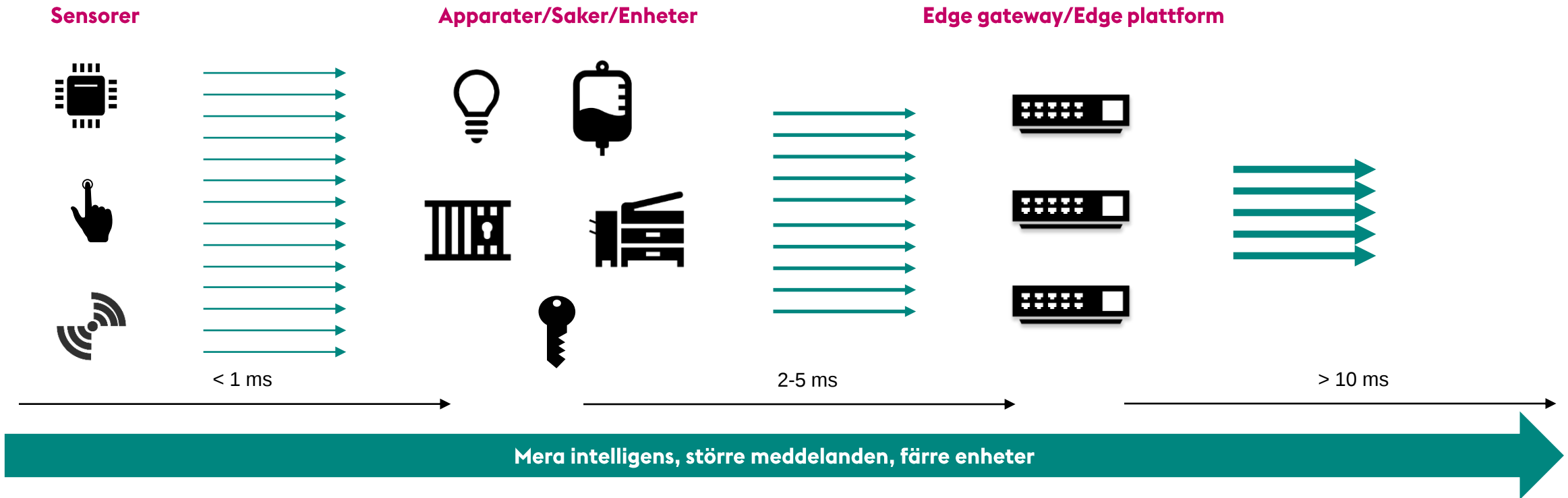
Kommunikation

Enheten kan **kommunicera** med omgivningen (plattformar, andra Edge plattformar eller andra enheter) med hjälp av en kommunikationsfunktion. Detta sker på olika sätt med olika protokoll och infrastruktur.

Informationsflöde för insamling i Edge

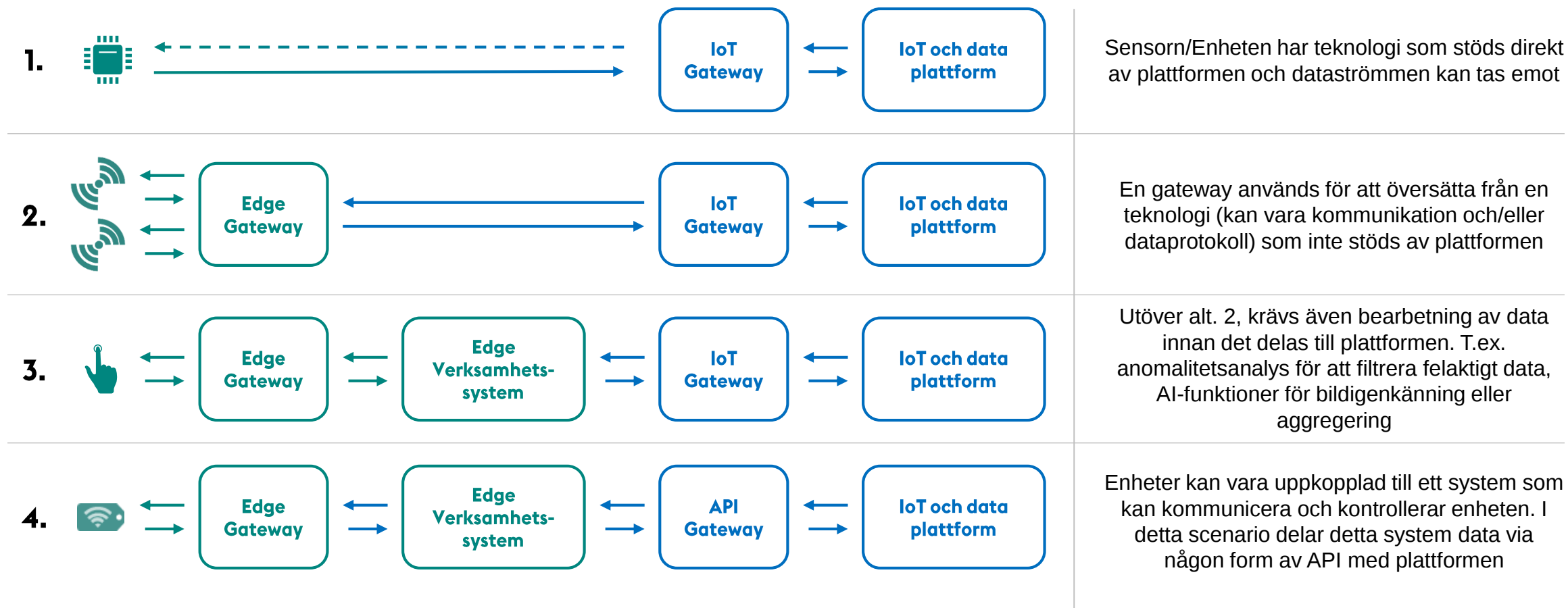
Det är mycket små signaler som skickas från sensorerna, oftast med hög frekvens. Detta sker antingen periodiskt eller meddelandestyrt dvs när något har förändrats i en sensors omgivning

- I sensorn omvandlas signaler till data och frekvensen hur ofta detta data skickas vidare kan följa hur ofta sensorn uppfattar eller konfigureras i enheten
- En Gateway kan användas om mer avancerad hantering av data i Edge krävs eller att plattformen (eller annan mottagare av data) inte stödjer det tekniska protokoll eller infrastruktur som enheterna använder. Gatewayen används för att samla ihop kommunikationen från dessa enheter till en gemensam punkt



Kommunikation med IoT-plattform och dataplattform

Förenklat kan kommunikationen mellan Edge och IoT- och dataplattformen ske på fyra sätt



Nödvändiga egenskaper i Edge IoT-gateway

Det är viktigt att bland annat ha möjligheten att kunna hantera data i Edge (Edge computing)

IoT-gateway ska minst ha egenskaper att

- Fungera som en mellanhand mellan enheten och andra enheter eller enheten och enterprise (IoT-plattform, verksamhets IoT-system)
- Vara uppkopplad både på nätverket som enheten använder och nätverket för enterprise
- Kunna "översätta" mellan olika kommunikationsprotokoll
- Kunna implementera ett säkert och stabilt sätt för enheterna att kommunicera
- Isolera enheten från enterpriset, dvs. åtkomst till en enhet betyder inte tillgång till enterprise

Datahantering i Edge

- Kunna autonomt styra i Edge utan uppkoppling, för att uppnå t.ex. robusthet och latency
- Tolkning av sensordata, t.ex. bildigenkänning, kvalitetskontroll, gränsvärden
- Aggregering; informationen har högre noggrannhet än vad som är intressant för analys utanför enheten
- Filtrering för att minska datamängden som ska skickas vidare arkitekturen

Varför är det viktigt?

- Enheter som behöver kunna fungera när uppkoppling saknas/avbryts
- Skicka allt data till gemensam plattform kan vara dyrt och ineffektivt användande av infrastrukturen
- Delar av datat filtreras bort för att det kan inte skickas till gemensam plattform av integritetsskäl eller säkerhetsskäl
- Lagra allt rådata kan vara ineffektivt, dyrt och inte hållbart
- Latency att kunna analysera och skicka tillbaka återkoppling för styrning till Edge kan bli för lång

Säkerhet i Edge

It-säkerhet i Edge är beroende på användningen och/eller behovet av enheterna och det data som de producerar. Nedan följer en kontrollista som motsvarar den **längsta** säkerhetsnivån som bör finnas i Edge

Kontrollista för lägsta säkerhetsnivå i Edge

1. Enheterna ska ha certifikatbaserad kommunikation (t.ex. PKI eller 802.x Certifikat) mot centrala plattformar och system

- För att kunna verifiera att enheten är tillförlitlig
- För att kunna ta tillbaka certifikat och förnya dessa vid behov

2. Kommunikationen till/från enheterna bör kunna vara krypterad

- För att data inte ska kunna manipuleras under transport

3. Identifieringen av enheten måste finnas i hårdvaran (tex via MAC ID eller enhets ID)

- För att enheter inte ska kunna simuleras som riktiga enheter.

4. Enheterna måste kunna uppdateras; firmware, operativsystem eller annan styrprogramvara separerat från varandra

- Uppdatering av programvara i enheterna nödvändigt speciellt för att det kan uppstå säkerhetsrisker i dem
- Uppdatering ska ske löpande på alla enheter
- Uppdateringarna ska kunna fungera på krypterad kommunikation

5. Om enheterna levereras med ett lösenord måste dessa kunna ändras

- Default lösenord ska alltid ändras innan utsättning
- Om det inte finns någon annan möjlighet än inloggning med lösenord måste det kunna ändras även utan fysisk tillgång till enheten

6. Motstånd mot fysisk påverkan av enheter

- Enheterna måste kunna stå emot fysisk påverkan för att säkert kunna leverera rätt kvalitet och data
- Avaktivera fysiska interface på enheten som inte används

7. Konfigurera enheterna så de bara kan koppla upp mot godkända trådlösa nätverk

Beskrivning av IoT-plattform

IoT-plattformens roll i målarkitekturen

En IoT-plattform tillhandahåller tekniska förmågor som skapar förutsättningar för att kunna lösa verksamhetsbehovet. Samtidigt förhåller den sig till och kan kommunicera med övriga gemensamma plattformar och verksamhetssystem



IoT-plattformens roll

IoT-plattformens roll i målarkitekturen är att utgöra en plats där den tekniska implementationen av förmågorna fungerar tillsammans, oberoende av vilket verksamhetsproblem som ska lösas.

Dessa förmågor kompletterar den befintliga arkitekturen i stadens gemensamma it-förmågor.

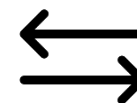


IoT-plattformens förmågor

Plattformen löser inte ensamt verksamhetsbehovet utan skapar förutsättningarna att göra det på ett effektivt, säkert och skalbart sätt.

Det krävs fortfarande en applikation eller system där verksamheten kan utnyttja dessa funktioner, information och insikter som skapas.

Denna applikation kan utvecklas i plattformen eller utnyttja ett antal av förmågorna som stöd i applikationen.

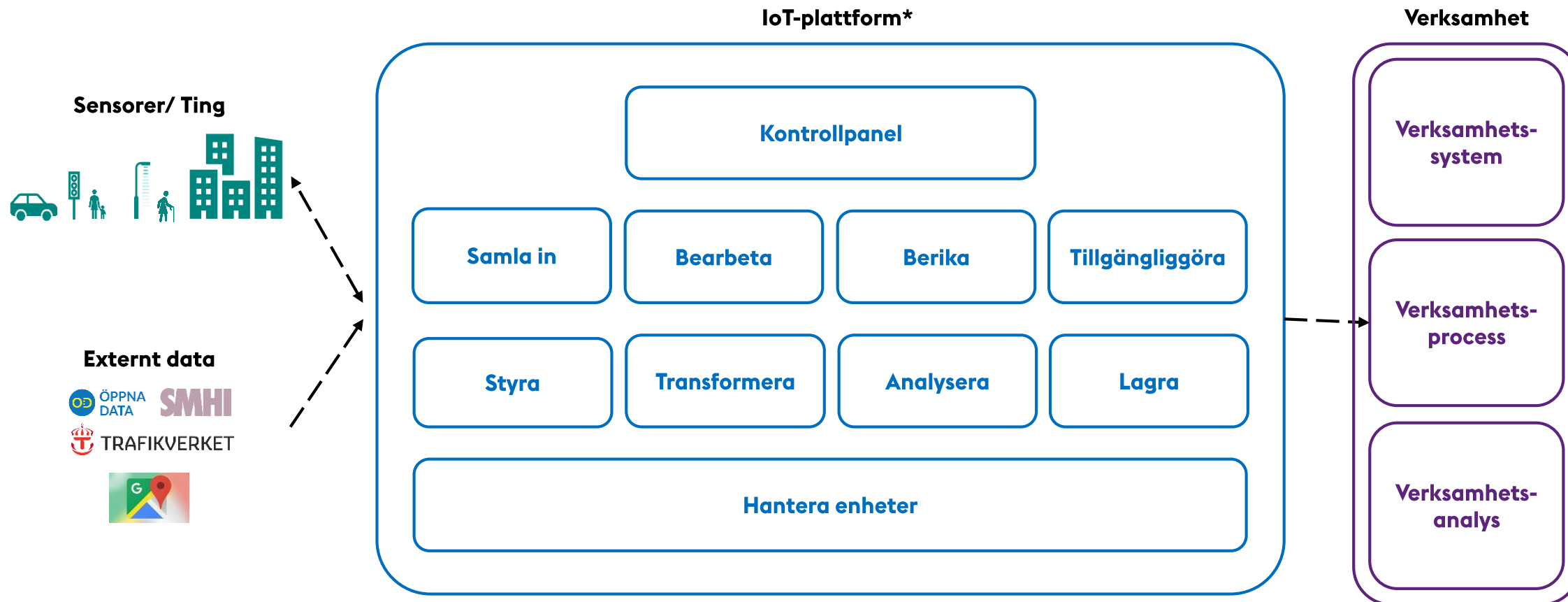


Samverkan med andra system och plattformar

Plattformen måste kunna samverka och integreras med stadens nuvarande verksamhetssystem och verksamhetsanalys för att kunna dra nytta av IoT i befintliga processer och beslut.

IoT-plattformens förmågor

Bilden beskriver de viktigaste funktionella förmågorna som bör finnas på en IoT-plattform. Säkerhet har exkluderats då det är en förmåga som spänner över samtliga av de övriga förmågorna och beskrivs därför separat



IoT-plattformens förmågor: Samla in och Styra



Samla in

Tar emot data och meddelanden från Edge eller andra datakällor i den takt som krävs. Det är mottagningspunkten av meddelanden från de källor som är uppkopplade mot plattformen och fördelar till plattformens övriga förmågor utan lagring.

Typiska egenskaper:

- Kommunikerar säkert med enheter med hjälp av t.ex. kryptering.
- Implementerar dataprotokoll, som saknas i integrationsplattformen till enheterna som t.ex. MQTT, AMQP, CoAP för att hantera dessa enhetligt och standardiserat.
- Hanterar kommunikation i båda riktningarna, dvs både ta emot meddelanden och skicka meddelanden för att kunna styra enheterna.
- Hantera stora mängder av enheter (datapunkter) och dataströmmar.
- Flexibilitet i att kunna utöka med nya dataprotokoll och anslutningssätt.



Styra

Kommunicerar med uppkopplade enheter genom att återanvända egenskaperna som beskrivs i förmågan "Samla in". Agerar mottagningspunkt av meddelanden från plattformens förmågor för kommunikation till de uppkopplade enheterna.

Typiska egenskaper:

- Hantera stora mängder av enheter och möjlighet att kunna skicka meddelande till enskilda eller grupper av enheter, dvs 'en-till-en' och 'en-till-många'.
- Möjlighet att kunna skicka styrkommandon och filer till enheterna.
- Kommunikerar säkert med identifierade enheter.
- Återanvänder dataprotokoll, som förmågan "Samla in".

IoT-plattformens förmågor: Bearbeta och Transformera



Bearbeta

Data behöver normaliseras, tvättas och kategoriseras. I fallet för IoT är det dataströmmar med data i rörelse som kommer i höga volymer och hastighet.

Typiska egenskaper:

- Validera kvalitet mot gränsvärden eller dataserier
- Ta bort brus
- Bestämma om värdet ska skickas vidare
- Skapa nya händelser
- Eventuellt aggregera händelser eller olika strömmar



Transformera

Transformera strömmande data i plattformen till förbestämda modeller för att möjliggöra och optimera användningen av detta data för övriga förmågor.

Att transformera insamlat data till en hanterbar struktur ökar värdet och möjligheten att använda data för plattformen.

- Exempel på transformering kan vara att kunna ta emot samma information från flera olika typer av enheter i olika format och transformera dessa till samma modell för att effektivare kunna utnyttja analysmodeller, utvecklingsverktyg, testning och lagring.
- Exempel på datamodeller är FIWARE, TALQ, OSCP eller andra av staden bestämda standardmodeller per verksamhetsdomän

IoT-plattformens förmågor: Berika och Analysera



Berika

Berika möjliggör att med hjälp av metadata och masterdata från andra källor eller enhetshanteringen kunna skapa en kontext till sensordatat.

För att effektivt kunna utnyttja analysförmågan i IoT-plattformen krävs någon form av berikning för att beskriva i vilket sammanhang data har uppstått.

Typiska berikande funktioner är:

- Addera data om enhetens placering, temperatur eller status.
- Geografiskt data som typ av omgivning (park, gata, sjö).
- Väderdata.
- Enhetskonfiguration (mätnoggrannhet, enhet, periodicitet).



Analysera

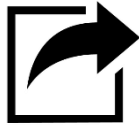
Analysförmågan ska komplettera de verksamhetsanalysförmågor som redan finns inom staden med möjligheten att effektivt kunna analysera data i rörelse - realtidsdata.

Typiska analysförmågorna i IoT-plattformen är att kunna svara på frågorna: *"Vad kommer sannolikt hända?"* och *"Vad bör vi göra?"*

För att kunna detta krävs:

- Förmågan att analysera sekvenser av strömmande data.
- Förmåga att kunna dra nytta av flera datakällor i realtid.
- Hantera allt data även som man i förväg inte visste värdet i data.
 - Allt data ska inte vara aggregerat.
 - Allt data kan innehålla information.
- Kunna förutspå vad som kommer hända med hjälp av dataströmmar, kan vara självlärande algoritmer som Machine Learning.

IoT-plattformens förmågor: Tillgängliggöra och Lagra



Tillgängliggöra

I IoT-plattformen skapas verksamhets API:er för de dataströmmar som ska tillgängliggöras till verksamhetssystem, verksamhetsprocesser och verksamhetsanalys.

Dataströmmarna tillgängliggörs via förmågan genom att skapa API:er från plattformen.

API:erna delas i staden via Integrationsplattformens API-gateway för att effektivare kunna användas och integreras i resten av it-landskapet.



Lagra

Lagring i IoT-plattformen är dels lagring av rådata, dvs den obearbetade dataströmmen från enheterna, samt lagring av hanterat data i köer. Data i kö betyder att data tillgängliggörs till konsumenter på ett sätt så att de ska hinna ta emot sitt data.

- Ta emot meddelande för lagring från vilken förmåga som helst i plattformen.
- Hantera lagring oberoende på informationsmodeller och struktur.
- Hantera åtkomst av lagrat data till övriga förmågor.

Lagringen kan ske på olika sätt beroende på hur data är strukturerat och senare ska användas. Exempel på tekniker är Kafka, NoSQL och Blob.

Andra teknologier som kan bli nödvändigt för att effektivt kunna exportera stora datamängder ut ur plattformen beroende på användningsfallet.

IoT-plattformens förmågor: Dashboard/Kontrollpanel



Dashboard/Kontrollpanel

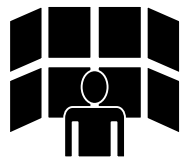
Att kunna visualisera dataflöden och lösningar i plattformen kan vara avgörande för förståelsen av komplexa lösningar och flöden.

Kontrollpanelförmågan i IoT-plattformen ska främst stödja förvaltare, utvecklare och analytiker att kunna förstå implementerade dataflöden för att kunna hantera dessa i form av vidareutveckling och/eller felsökning.

Typiska funktioner är att kunna använda standardiserade visualiseringsmetoder som grafer, staplar och diagram men även andra kraftfullare metoder som t.ex. visualisering på kartor.

IoT-plattformens förmågor: Enhetshantering (1/2)

Förmågan Enhetshantering kräver en mer detaljerad beskrivning än övriga av IoT-plattformens förmågor då flera delförmågor omfattas



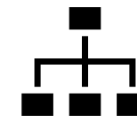
Huvuduppgifter

Förmågan Enhetshantering har två huvuduppgifter:

- Hålla rätt på samtliga enheter som är uppkopplade mot IoT-plattformen
- Övervaka och hantera underhållet av enheter i stadens kontroll

Till dessa huvuduppgifter hör möjlighet att:

- Hantera avvikelser om något inte fungerar korrekt och påverkar verksamheten
- Hantera den digitala kopian av enheten



Delförmågor

Autentisering

- En enhet måste identifieras och verifieras av enhetshanteraren innan data kan tas emot
- En säker identifiering är nödvändigt för att veta vem som anslutit enheten

Provisionering/auktorisering

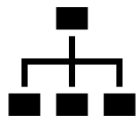
- Enhetens egenskaper registreras när enheten har autentiserats

Konfiguration och kontroll

- Enheter ska kunna automatiskt konfigureras vid uppstart
- Möjlighet att kunna komplettera enhetsinformation i efterhand, ev. information som enheten själv inte kan registrera
- Konfiguration kan vara t.ex. hur ofta data skickas, format, dataprotokoll, noggrannhet

IoT-plattformens förmågor: Enhetshantering (2/2)

Förmågan Enhetshantering kräver en mer detaljerad beskrivning än övriga av IoT-plattformens förmågor då flera delförmågor omfattas



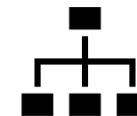
Fort. Delförmågor

Övervakning & monitorering / Dashboard

- Dashboard med filtreringsmöjligheter på t.ex. typer av enheter, placering
- Kontrollera enhetens och kommunikationens status
- Möjlighet att ladda ner loggar från Edge
- Möjlighet att stänga av en enhet

Mjukvaruuppdatering och hantering

- Enheternas mjukvaror måste kunna uppdateras centralt
- En enhets mjukvaror kan bestå av:
 - Firmware, Operativsystem, Kontrollprogramvaran, Säkerhetsprogramvara
- Uppdateringar måste kunna ske i bulk och regelbaserat (för att kunna göra A/B tester)



Fort. Delförmågor

Identifiering

- Enheten måste kunna ha en unik identifiering och kunna beskriva vad en utför

Rapportering

- Kunna skicka koordinater var enheten är placerad vid varje omstart/förflyttning
- Version av firmware, operativsystem och styrprogramvara.
- Kommunikationssätt, sensortyp och sensorkategori, modellbeteckning och tillverkare

Övervakning

- Status: Kunna skicka statusuppdateringar hur enheten fungerar och vilken status den har
- Batteri: Vid batteridrift kunna rapportera batterinivå
- Felrapportering: Automatiskt kunna rapportera fel

Säkerhet i IoT-lösningar

It-säkerhet som plattformen kan bidra med är listat nedan. Det finns flera komponenter i lösningarna som behöver ha sina respektive säkerhetsprinciper och plattformen och Edge ensamt står inte för helheten ur ett säkerhetsperspektiv

Säkerhetsegenskaper i plattformen

1. Varje implementerad

- För att kunna verifiera att enheten är tillförlitlig
- För att kunna ta tillbaka certifikat och förnya dessa vid behov

2. Kommunikationen till/från enheterna bör kunna vara krypterad

- För att data inte ska kunna manipuleras under transport

3. Identifieringen av enheten måste finnas i hårdvaran (tex via MAC ID eller enhets ID)

- För att enheter inte ska kunna simuleras som riktiga enheter.

4. Enheterna måste kunna uppdateras; firmware, operativsystem eller annan styrprogramvara separerat från varandra

- Uppdatering av programvara i enheterna nödvändigt speciellt för att det kan uppstå säkerhetsrisker i dem
- Uppdatering ska ske löpande på alla enheter
- Uppdateringarna ska kunna fungera på krypterad kommunikation

5. Om enheterna levereras med ett lösenord måste dessa kunna ändras

- Default lösenord ska alltid ändras innan utsättning
- Om det inte finns någon annan möjlighet än inloggning med lösenord måste det kunna ändras även utan fysisk tillgång till enheten

6. Motstånd mot fysisk påverkan av enheter

- Enheterna måste kunna stå emot fysisk påverkan för att säkert kunna leverera rätt kvalitet och data
- Avaktivera fysiska interface på enheten som inte används

7. Konfigurera enheterna så de bara kan koppla upp mot godkända trådlösa nätverk

Dataströmmar

Data- och informationsbehandling i IoT

Det finns några typiska skillnader i egenskaper för IoT-data och hantering av data i system eller som analysdata

Data

IoT-data uppstår genom att enheter producerar och skickar data istället för att data hämtas för analys

- IoT-data produceras av enheter och tjänster runt enheterna
- IoT handlar om att samla data och analysera den i realtid för att skapa händelser alternativt hitta mönster i data som kan vara intressant för verksamheten

Källan

För traditionell dataanalys produceras större delen av data genom någon mänsklig input
IoT-data skapas och produceras uteslutande av maskingenererad data som aggregeras, filtreras och analyseras.

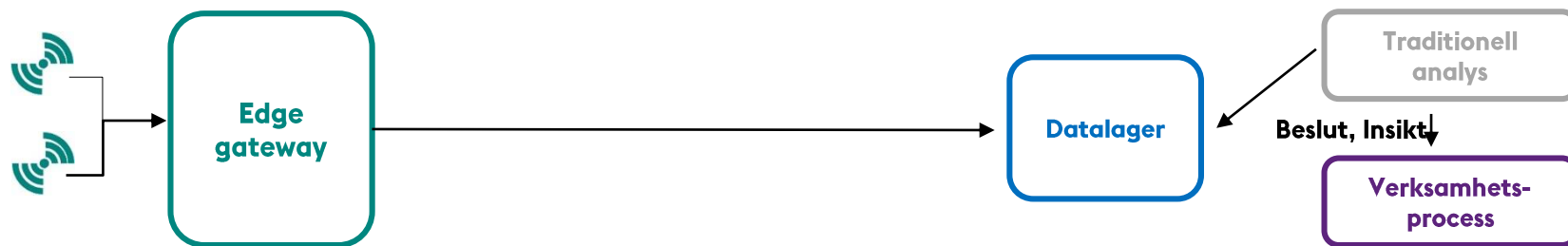
Tiden

I traditionell dataanalys och datasystem är det ok att data är i "vila" innan analysen utförs.

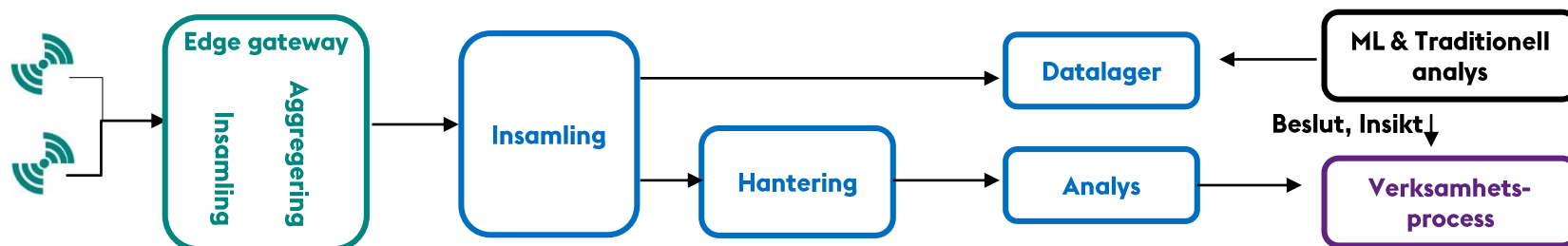
I IoT är tiden eller åldern på data av yttersta vikt. Åldern är en del av värdet i datat. Därför är realtidshantering av data ytterst viktigt för att kunna realisera nya användningsfall som t.ex. att optimera underhåll på utrustning, larm om trasig utrustning, styrning av trafiksignaler, öppnande av säkerhetsbommar etc.

Löst kopplade dataströmmar

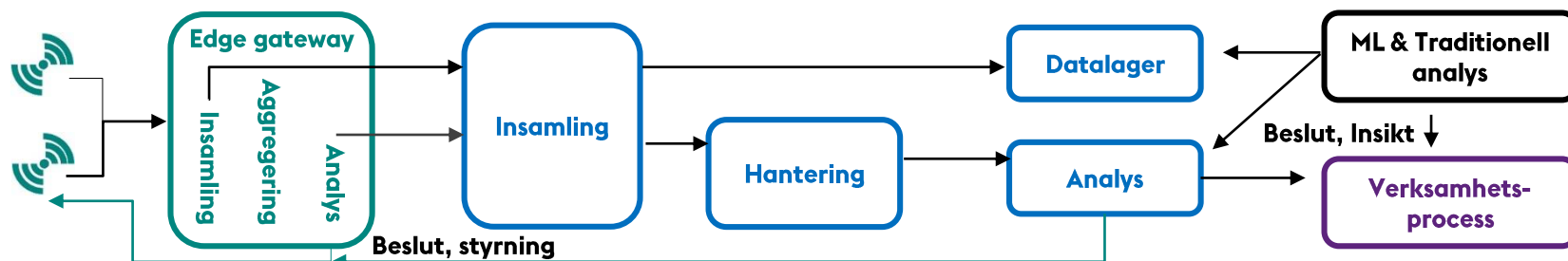
Dataströmmar till och genom plattformen måste vara löst kopplade för att data ska kunna nyttjas av plattformens förmågor. Insamling av data ska kunna vara händelsestyrd, vilket innebär att förändringar i data skapar meddelanden som övriga förmågor kan agera på



Traditionell insamling för analys i efterhand. Resultatet av analysen används som rapporter etc. för att förändra regelverk eller processer



Insamlingen sker dels för att stödja scenario (1) och för att kunna användas direkt in i verksamhetsprocesserna. Analysen kopplar tillbaka direkt på dataströmmarna

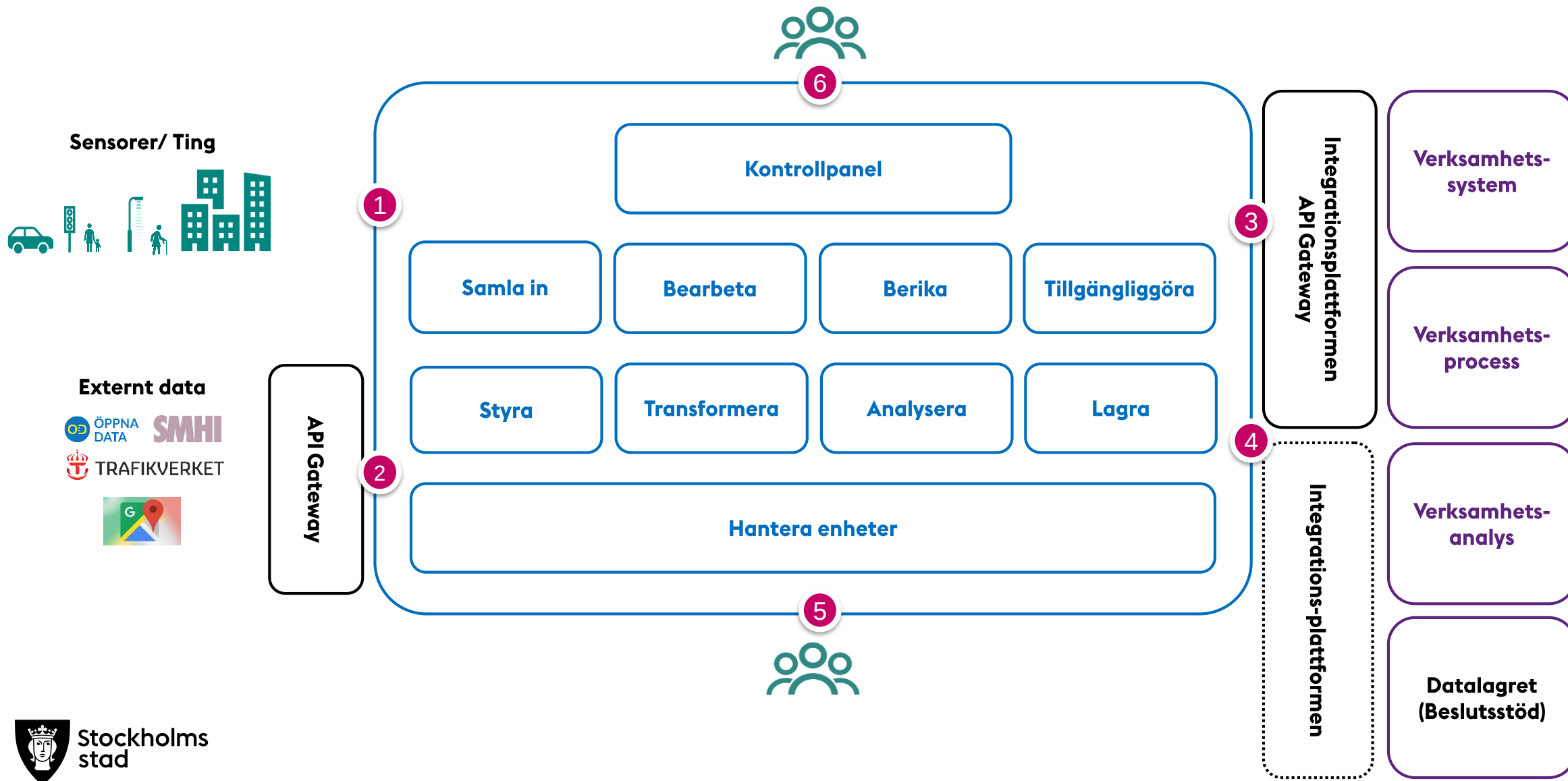


Återkopplingarna och analysen sker i flera delar av dataflödet, för att kunna ge effekter så tidigt som möjligt. Återkoppling och analys sker på flera delar i arkitekturen både i Edge, Plattform & Verksamhetssystemen. Samverkan för hur resultaten kan användas är viktigt

Förhållande mellan IoT-plattformen och övrigt it-landskap

IoT-plattformens förhållande till andra delar av it-landskapet

I det här avsnittet beskrivs IoT-plattformens koppling till andra delar av stadens it-landskapet i detalj



Förhållandet mellan IoT-plattformen och övrigt it-landskap (1/3)

1

Inhämta data från Edge

Inom IoT finns det specifika egenskaper för dataflöden som Integrationsplattformen inte har stöd för. Dessa nya dataflöden hanteras via en insamlingsförmåga i IoT-plattformen.

- En IoT Gateway i plattformen har bland annat stöd för standardprotokoll som är specifika för IoT som t.ex. MQTT och AMQP
- Den har också stöd för att ta emot strömmande data och slussa det vidare i plattformen
- Strömmande data kan delas ut till övriga förmågor i plattformen som lösningen behöver och transformeras till meddelanden som passar för verksamhetens användning i sina verksamhetssystem eller –processer
- Bearbetning som sker i plattformen kan återkopplas tillbaka till Edge. Integrationen sker då via IoT Gateway genom återanvändning av de protokoll för kommunikation med Edge

2

Inhämta data från externa datakällor

Om externa datakällor stödjer de protokoll och mekanismer som API-gateway stödjer tas detta data emot till IoT-plattformen via API-gateway.

Nya verksamhetsscenariorna som det idag kan saknas stöd för integrationsplattformen:

- Externa datakällor kräver tekniker som inte stöds av Integrationsplattformen t.ex. Kafka eller Pub/Sub bör dessa kompletteras i Integrationsplattformen över tid alternativt återanvända motsvarande mekanismer i IoT-plattformen
- Vid integration inom en verksamhet i staden kan integration direkt från datakällan till IoT-plattformen användas om det är lämpligt enligt arkitekturen för lösningen utifrån parametrarna effektivitet, förvaltningsbarhet och kostnad

Förhållandet mellan IoT-plattformen och övrigt it-landskap (2/3)

3

Tillgängliggöra data

IoT-plattformen skapar verksamhets API:er för de dataströmmar (data i rörelse) som ska tillgängliggöras.

API Gateway, en komponent i Integrationsplattformen, använder IoT-plattformen för att tillgängliggöra verksamhets API:er som skapats

- Samma princip gäller för IoT-plattformens som övrig integration med API:er från verksamhetssystem
- De API:er som skapas och tillgängliggörs via IoT-plattformen följer de standarder/metoder som erbjuds i Integrationsplattformen

Detta görs enligt Integrationsplattformens princip *"Vid extern kommunikation eller vid kommunikation mellan bolag ska stadens API-Gateway användas"*

4

Tillgängliggöra data

API Gateway kompletterar IoT-plattformens API:er med framförallt:

- Virtualisera och publicera API:er
- Övervaka användningen
- Hantera behörigheter till API:er
- Tilldela resurser och åtkomst

Sentinet, produkten för Stadens API Gateway, stödjer utöver ovanstående funktioner, följande tekniska format för API:er:

- REST och SOAP

Om data behöver tillgängliggöras i stora mängder t.ex. för annan analys / bearbetning eller lagring utanför IoT-plattformen kan API Gatewayen vara begränsad.

Alternativa teknologier för att tillgängliggöra data från IoT-plattformen kan vara:

- Kafka, Pub/Sub, Filöverföring och ETL (där framförallt Extrakt förmågan)

IoT Plattformen ska vara förberedd för att agera klient för ovanstående scenarion. Eventuellt behöver Integrationsplattformen kompletteras för att ansvara för Kafka och Pub/sub förfarande i framtiden.

Förhållandet mellan IoT-plattformen och övrigt it-landskap (3/3)

Vissa användargrupper har direkt tillgång till IoT-plattformen utan att använda API:er

5

Användare av IoT-plattformens enheter

Enhetshantering

- Användare med ansvar för de uppkopplade enheterna behöver ha tillgång till enhetsinformation och enhetsstatus (se avsnittet om enhetshantering). Detta sker genom tillgång till enhetshanteringens användargränssnitt i IoT-plattformen

6

Användare av IoT-plattformens data

Kontrollpanel

- Förvaltare och informationsägare av informationsflödena genom plattformen har behov av att visualisera dataflödet för att få en bättre förståelse vad som sker. Användbara situationer är bland annat vid felsökning och vidareutveckling i hanteringen av informationsströmmen genom förmågorna