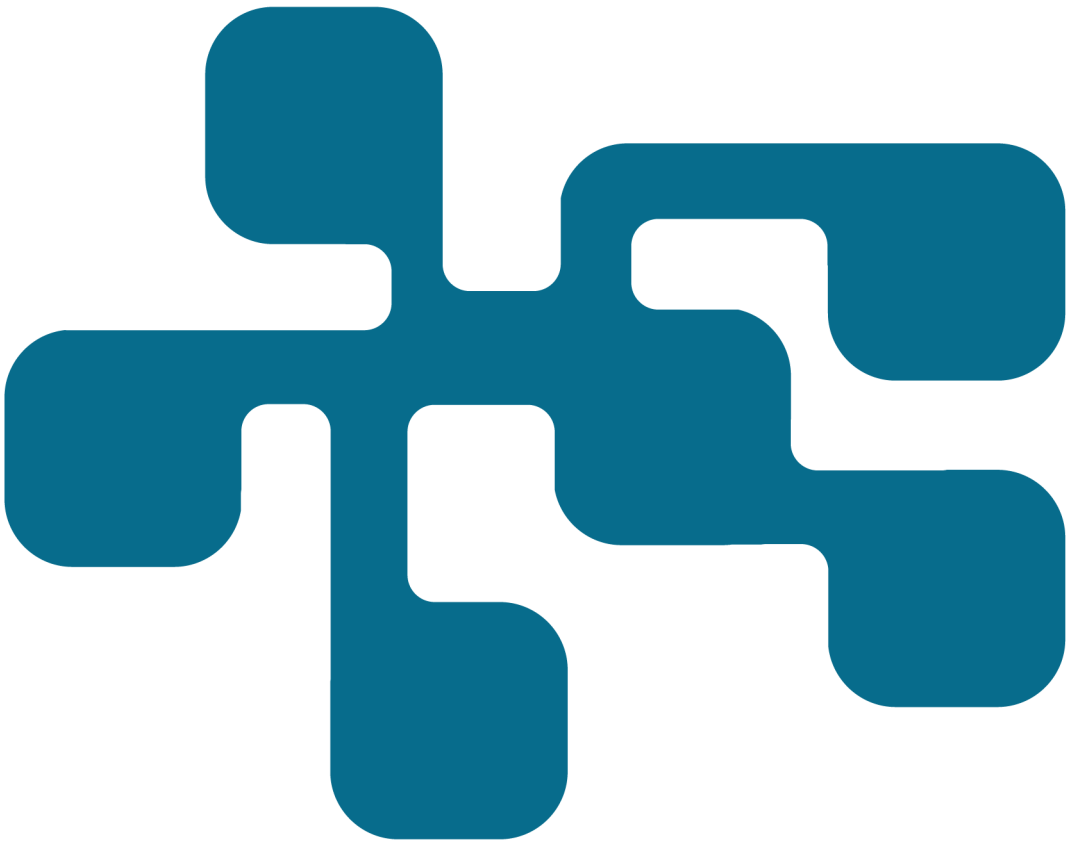
NCS3 Förstudie – Bortom sakernas internet

Vidar Hedtjärn Swaling, Fredrik Malmberg Andersson FOI



FOI-R--4643--SE
MSB 2016-3606 November 2018
ISSN 1650-1942

Vidar Hedtjärn Swaling,
Fredrik Malmberg Andersson

NCS3 Förstudie – Bortom sakernas internet

Titel	NCS3 Förstudie – Bortom sakernas internet
Title	NCS3 Pilot study – Beyond the Internet of things
Rapportnr	4643
Månad	November
Utgivningsår	2018
Antal sidor	39
ISSN	1650-1942
Kund	MSB
Forskningsområde	5. Krisberedskap och samhällssäkerhet
FoT-område	Ej FoT
Projektnr	E13572
Godkänd av	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Internet of Things (IoT), eller *sakernas internet*, är ett begrepp som används för att beskriva att allt fler föremål utrustas med möjligheten att anslutas till internet och andra nätverk. Myndigheten för samhällsskydd och beredskap (MSB) har efterfrågat en framtidsstudie om IoT med särskilt fokus på industriella informations- och styrsystem (ICS).

I studien identifieras påverkansfaktorer som grund för att skapa explorativa (utforskande) framtidsscenarier för IoT-utvecklingen. En ambition är att kunna se *bortom sakernas internet*, med frågor som: Går det att se en utveckling där IoT inte kommer att dominera på det sätt som ofta förespeglas? Går det att se en utveckling där pendeln stannar av eller till och med slår tillbaka? Vilka är de faktorer som styr utvecklingen av IoT?

Arbetet har resulterat i en bruttolista med påverkansfaktorer inom områdena politik, ekonomi, socialt liv, teknik, juridik och miljö. Under arbetet har också två väsentligt olika framtidsbilder utkristalliserats. Dels en ”silo-framtid” där kommunikationen mellan olika enheter är strikt avtalsreglerad och framförallt sker inom en organisation. Dels en ”mesh-framtid” där i princip alla enheter kan kommunicera fritt med varandra. Silo-framtiden kan ses som representativ för den industriella utvecklingen medan mesh-framtiden snarast representerar vardagens IoT på individnivå.

En viktig slutsats när det gäller IoT på ICS-området är att riskerna kan komma att öka, men att introduktionen av smarta produkter kommer att konfronteras av de än så länge starkare incitamenten att bevara affärsmässig integritet, undvika oförutsedda kostnader och att skydda tredje part.

Nyckelord: Internet of Things, framtid, scenarier, påverkansfaktorer, ICS.

Summary

The Internet of Things (IoT) is a concept used to describe how ever more objects are being equipped with the ability to be connected to the Internet and other networks. The Swedish Civil Contingencies Agency, MSB, has requested a futures study of IoT, with a specific focus on industrial information and control systems (ICS).

The study identifies influence factors as a basis for creating scenarios on the future development of IoT. The ambition is to be able to see *beyond the Internet of Things*, through such questions as: Is it possible to discern a path of development where IoT will fail to be as dominant as has been so often predicted? Is it possible to see a pathway where the pendulum stops, and even swings back? What are the factors that govern the development of IoT?

The work has resulted in a gross list of influence factors within the areas of politics and policy, economics, social life, technology, law, and environment. As the study proceeded, two essentially different pictures of the future became prominent. One is a "silo future", where the communication between various units is strictly procedural and primarily occurs within an organisation. The other is a "mesh future", where in principle any unit may communicate freely with any other. The former can be seen as representative of the industrial development path, whereas the latter more resembles today's IoT at the individual level.

An important conclusion regarding IoT in the area of ICS is that the risks associated with it may increase, while the incentives for introducing smart products will have to keep thrashing it out against the – so far – even stronger incentives to maintain commercial integrity, avoid unforeseen costs, and protect third parties.

Keywords: Internet of Things, future, scenarios, influence factors, ICS.

Författarnas förord

Under 2016 hölls en serie möten mellan MSB och FOI i syfte att diskutera framtidsutvecklingen inom Internet of Things. Tidigt togs ett beslut att göra en skriftlig sammanställning av bakgrundsmaterial såväl som diskussionstrådar som underlag till fortsatta studier. När underlaget väl var på plats framstod emellertid innehållet som så pass självständigt och viktigt att det nu, på uppdrag av MSB, ges ut i form av denna FOI-rapport. Trots att utgivningsåret är 2018 innebär den relativt långa tillblivelseprocessen att framställningen bygger på händelser och källor från 2016 eller tidigare.

Innehållsförteckning

1 Inledning

Internet of Things (IoT), eller *sakernas internet*, är ett begrepp som används för att beskriva att allt fler föremål, både för privat och industriellt bruk, utrustas med möjligheten att anslutas till internet och andra nätverk. Myndigheten för samhällsskydd och beredskap (MSB) har efterfrågat en framtidsstudie om utvecklingen av IoT med särskilt fokus på industriella informations- och styrsystem (ICS).

Exempel på frågor som MSB vill ha belysta är: Går det att se en utveckling där IoT inte kommer att dominera på det sätt som ofta förespeglas? Går det att se en utveckling där pendeln stannar av eller till och med slår tillbaka? Vilka är de faktorer som styr utvecklingen av IoT? Är det samma faktorer nu som i framtiden?

I denna studie tas en grund fram för fortsatt analys av IoT som företeelse inom i första hand ICS-området. Utgångspunkten är IoT i vid bemärkelse och de skillnader i tekniker och trender som finns mellan olika samhällsdomäner, i första hand individen, samhället och industrin.

Studien har utförts av Totalförsvarets forskningsinstitut (FOI) inom ramen för NCS3[1].

1.1 Syfte och mål

Studiens övergripande syfte är att vara ett stöd för fortsatt analys av IoT inom ICS-området, men även inom IT. Utgångspunkten är därför IoT i vid bemärkelse. I förlängningen ska studien bidra till att stärka det strategiska arbetet inom NCS3 genom att anta ett längre tidsperspektiv än vad som normalt görs, samt öka förutsättningarna att fånga upp trender som ligger utanför den gängse diskursen om framtiden för IoT.

Målet är att identifiera påverkansfaktorer som grund för att skapa explorativa (utforskande) scenarier med avseende på utvecklingen inom IoT i allmänhet och inom ICS-området i synnerhet. En ambition är att kunna se *bortom sakernas internet*, det vill säga bortom vad som avses med IoT i uttryck som ”IoT är redan här”, ”Framtiden stavas IoT”, etc. Med andra ord – *genom att undersöka begreppets gränser vill vi skapa en tydligare bild av vad som är möjligt och vad som påverkar möjligheterna.*

[1] NCS3: Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet. NCS3 är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsaspekter inom industriella informations- och styrsystem. Centrumet är ett samarbete mellan FOI och MSB.

1.2 Målgrupp

Studien vänder sig i första hand till personer som arbetar med ICS- och IoT-relaterade frågor samt personer med anknytning till MSB:s program för ökad säkerhet inom ICS, inklusive NCS3. Studien bör också kunna vara intressant för personer med ett allmänt intresse av kris- och riskhantering och samhällets beroende av tekniska system.

1.3 Upplägg

I kapitel 2 presenteras vald metod och arbetsgång. I kapitel 3 presenteras exempel på hur IoT används och definieras i olika sammanhang. I kapitel 4 identifieras påverkansfaktorer, det vill säga faktorer som kan antas har inflytande på utvecklingen av IoT. Faktorerna analyseras även med avseende på ömsesidiga beroenden och drivkrafter. I kapitel 5 sammanfattas bilden i några framtidsbilder som har utkristalliserats under arbetets gång. I kapitel 6 förs en avslutande diskussion samt föreslås ett antal frågor att ta med i det fortsatta arbetet.

2 Metod

2.1 Om metodvalet

När det gäller framtidsstudier finns huvudsakligen tre möjliga ansatser:

- Explorativa studier/scenarier
- Normativa studier/scenarier
- Prediktiva studier/scenarier

Explorativa studier/scenarier syftar till att identifiera och variera påverkansfaktorer (till exempel tekniska, socioekonomiska eller politiska) för att framställa möjliga scenarier. Syftet är inte att peka ut en sannolik framtid utan att ”vidga tänkandet” och skapa förutsättningar för att strukturera osäkerheter i olika diskurser och beslutsproblem.[2] I normativa scenarier är utgångspunkten istället bestämda, oftast önskade, framtider eller sluttillstånd. Utifrån dessa går man sedan baklänges till nutid för att analysera vad som måste hända för att sluttillstånden ska nås (så kallad back-casting). Prediktiva scenarier syftar, enkelt uttryckt, till att förutsäga framtiden.

Bedömningen är att en explorativ ansats är vad som lämpar sig bäst för föreliggande studie. Vad gäller normativa scenarier är det svårt att se vilka meningsfulla målkriterier som skulle kunna sättas upp utan att det först görs någon form av explorativ studie. Syftet är heller inte prediktivt, det vill säga avsikten är inte att förutsäga framtiden, utan att diskutera ett spektrum av möjligheter.

2.2 Arbetsgång

Studien omfattar en områdeskartläggning via skriftliga källor och intervjuer med branschaktörer i syfte att (1) definiera och beskriva sakernas internet, (2) identifiera tidigare gjorda arbeten, (3) utveckla en brutto-uppsättning påverkansfaktorer, och (4) identifiera viktiga frågor för det fortsatta arbetet.

En fortsättning på detta arbete föreslås ta de identifierade påverkansfaktorerna och frågeställningarna som utgångspunkt för att utarbeta mer detaljerade framtidsscenarier. I viss mån kommer även påverkansfaktorerna att behöva

[2] Jonsson (2017). Explorativa scenarier ska enligt Jonsson vara relevanta och trovärdiga, dock behöver de inte vara sannolika vilket betonar deras betydelse som diskussionsunderlag. De ska dessutom ”spänna upp utfallsrummet” så att intressanta möjligheter inte systematiskt utesluts.

förankras och utvecklas vidare, beroende på vilka frågeställningar som anses viktigast att gå vidare med, och när.

3 Bakgrund – IoT i teori och praktik

Det interaktiva eller kommunicerande kylskåpet är ett så vanligt förekommande exempel på vad IoT är att det för många kanske rentav blivit själva sinnebilden av IoT, eller *sakernas internet* som blivit en vanlig svensk benämning. Andra tillämpningar som ofta lyfts fram handlar om självkörande bilar och hjälpmedel inom vården. Eftersom det troligen inte finns någon bortre gräns för hur och i vilka sammanhang IoT kan tillämpas, samtidigt som utvecklingen går mycket snabbt, är det förmodligen viktigare att belysa vad som gör något till en ”IoT-sak” än att ge många exempel på sådana saker.

I en presentation av Östen Frånberg från Luleå Tekniska Universitet konstateras att det bara är att lägga till prefixet ”smart” så blir en vanlig sak en IoT-sak. Om en *manuell* termostat kan slås av och på, och en *digital* termostat kan programmeras att göra detsamma, så kan en *smart* termostat sköta detta själv baserat på interaktion med andra apparater.[3] Denna analogi gör det möjligt att föreställa sig många olika tillämpningar av IoT, och även bedöma deras eventuella potential.

3.1.1 Olika definitioner av IoT

Internet myllrar av olika mer eller mindre genomarbetade försök att definiera och beskriva IoT. På webbplatsen *Postscapes*[4] görs ett försök att sammanställa olika definitioner för att visa på den stora bredden (och kanske förvirringen) och för att identifiera gemensamma nämnare. Det konstateras att begreppet IoT förekommer i allt från marknadsföringsmaterial till vetenskapliga artiklar. I djungeln av relaterade begrepp hittar vi *physical internet, ubiquitous computing, ambient intelligence, machine to machine (M2M), industrial internet, web of things, connected environments, smart cities, spimes, everyware, pervasive internet, connected world, wireless sensor networks, situated computing, future internet and physical computing*.

På webbplatsen *Den digitala resan*[5] konstateras att IoT är ett samlingsbegrepp för den utveckling som innebär att maskiner, fordon, gods, hushållsapparater, kläder och andra saker samt varelser (inklusive människor), förses med små inbyggda sensorer och datorer som kan kommunicera med sin omgivning och som därmed kan skapa situationsanpassade beteenden, miljöer, varor och tjänster.

[3] Frånberg 2014.
[4] Postscapes 2018.
[5] Den digitala resan 2015.

Något liknande anförs på Wikipedia[6], där sakernas internet beskrivs som ”alla föremål [- - -] som har inbyggda elektroniska delar (sensorer, processorer, etc.), internetuppkoppling (fysiskt eller trådlös), en unik och identifierbar adress och som utbyter data.”

En tredje, något mer koncentrerad, beskrivning hittar vi hos Tritech, ett av flera företag som specialiserat sig på att utveckla ”tjänster för det uppkopplade samhället”.[7] Tritech beskriver IoT som ”ett världsomspännande nätverk av uppkopplade objekt som är unikt adresserbara och baseras på standardiserade kommunikationsprotokoll.”[8]

I en FOI-studie från 2016 gör Kamrani m.fl. ett försök att hitta en mer allmängiltig och entydig definition.[9] Enligt Kamrani m.fl. är det en utmaning att begreppet spänner över forskningsområden inom såväl teknik som humaniora och samhällskunskap. Utgångspunkten är dock enkel – IoT syftar på fysiska enheter och apparater (eng. devices) som är kopplade till internet.[10] Kamrani m.fl. påpekar att även om IoT-enheter ofta är små anordningar som innesluter en trådlös transmissionskanal gäller detta inte allt som kallas IoT. Mer karaktäristiskt är att systemen åtminstone till viss del är *inbyggda* (eng. embedded) *och styr något i sin omgivning*. Den definition som enligt Kamrani m.fl. bäst inkluderar även denna aspekt kommer från U.S. Department of Homeland Security. IoT beskrivs där som ”*the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the internet) via interoperable protocols, often built into embedded systems.”*[11] Det vill säga, ungefär, **fysiskt mätande, avläsande eller påverkande system och enheter som via interoperabla protokoll, ofta implementerade i inbyggd elektronik, sammankopplas med informationsnätverk**.

3.2 Vad är det som händer, och varför händer det nu?

År 2014 nådde IoT fas två på den så kallade Gartner-kurvan, och 2018 ligger den fortfarande kvar där.[12, 13] Gartner-kurvan delar upp en innovations utveckling i fem faser. Först kommer ett tekniskt genombrott som skapar stort intresse. I den andra fasen kommer de första företagen ut med produkter på marknaden och

[6] Wikipedia 2018a.
[7] Tritec 2018.
[8] Ibid.
[9] Kamrani m.fl. 2016, s. 7.
[10] Ibid.
[11] Department of Homeland Security, 2016.
[12] Ny Teknik 2014.
[13] Gartner 2018.

förväntningarna på den nya tekniken är mycket höga. I fas tre övergår förväntningarna i besvikelse över att tekniken inte tycks hålla vad den lovar. I fas fyra har tekniken mognat och fler företag förstår hur den kan användas och i fas fem har den slutligen nått sitt breda genombrott.

Enligt Gartner är alltså IoT ännu bara i stadie två på en femgradig skala, det vill säga tekniken är i någon mening omogen. Enligt somliga finns inte IoT ännu. Claus Popp Larsen, chef för affärs- och innovationsavdelningen Urban Life på Swedish ICT, hävdar i en intervju i tidningen *Ny teknik* att det finns embryon till IoT, och han kan tänka sig att kalla vissa försök för *Intranet* of Things, men inget företag har en öppen IoT-plattform som släpper in många andra kommersiella aktörer till fri konkurrens.[14] Vi kan till exempel inte använda samma rörelsedetektor för att styra belysningen när någon går in i rummet som för att larma vid inbrott, eller för att larma om en äldre person inte rört på sig på ett tag. Tekniskt sett går det, men det finns inget företag med en lösning som öppnar upp för *andras tjänster*. Bristen på öppenhet beror enligt Larsen på affärsmodellen som företagen väljer: ”Innan det finns en "tjänstemäklare" med en fungerande affärsmodell, som öppnar upp för många tjänsteleverantörer, kommer inte sakernas internet att slå igenom.” Claus Popp Larsen jämför med företag i delningsekonomin, exempelvis Uber och Airbnb, som inte har egna konsumenttjänster men som har en öppen plattform som de låter bilförare och rumsuthyrare använda sig av. På sikt tror Larsen att det blir helt nya företag som går in och tar den rollen, företag som inte själva har någon IoT-tjänst, och därmed inte konkurrerar med sina kunder.

Samtidigt som IoT i flera avseenden är ett nytt fenomen, delvis ännu icke-existerande, så påpekar många att det inte är teknologin i sig som är ny utan förutsättningarna att tillämpa den som förändrats; snabbare nätverk, bättre sensorer och billigare hårdvara. Befintliga teknologier finns som gör att vi kan bygga IoT-system på globalt accepterade standarder, så som HTML, RFID, streckkoder och biometri. Begreppet ”Maskin till maskin”, eller M2M, som etablerades för omkring 50 år sedan[15], anges ofta som en förutsättning för, och integrerad del av, IoT. Tritech uttrycker det som att Internet of Things är det lager man bygger värdeskapande tjänster på, medan M2M är den teknik som gör det möjligt att ansluta till den infrastruktur som redan finns på plats.[16]

Utvecklingen mot allt fler uppkopplade enheter manifesteras inom mobiltelefonin med smartare plattformar, inom trådlös kommunikation med utvecklingen inom 5G, och inom datakommunikation med IPv6 (Internet Protocol version 6) som tillåter varje enskild sak att ha en unik IP-adress.

[14] Ny Teknik 2015.
[15] Wikipedia 2018b.
[16] Tritec 2018.

Enligt International Data Corporation (IDC) är prognosen att antalet IoT-anslutningar inom EU mer än tredubblas mellan 2013 och 2020, från 1,8 miljarder till närmare 6 miljarder. IDC menar vidare att utvecklingen främst sker inom konsumentelektronik och sensorer (bland annat inom industriproduktion och sjukvård), att Sverige är det EU-land som förväntas stå för den största procentuella tillväxten inom IoT, samt att politiken och juridiken hittills inte har utvecklats i samma takt som tekniken.[17]

3.3 IoT inom olika områden

En fråga är om IoT-utvecklingen, med dess utmaningar och möjligheter, ser likadan ut överallt eller om det finns skillnader mellan olika domäner, sektorer, verksamheter etc.

Nedan är ett försök att ge en inledande bild av IoT inom domänerna individ, samhälle och industri.[18] En ambition är att detta ska tillåta oss att ställa frågor av typen; Är det individuella eller samhälleliga behov som driver utvecklingen eller är det industrin som skapar behoven åt oss? Är det en domänöverskridande utveckling som handlar om universella drivkrafter?

3.3.1 Individ

Mycket av IoT-diskussionen handlar om privatkonsumtion och saker som i första hand är smarta ur ett individperspektiv. På individnivå kan ett upplevt effektiviserings- och rationaliseringsbehov vara viktigt, liksom den sociala aspekten; vi konsumerar inte bara produkter och tjänster för att vinna ekonomiska fördelar, utan också för att få status eller för att vi har vissa personliga preferenser. En ”pryl” kan stärka vår känsla av social tillhörighet. Inom individ-domänen är det svårt att i förväg få en bild av hur en teknik faktiskt kommer att användas och till vad. E-postens och sms:ets stora genomslag nämns ofta som exempel på oförutsägbarheten inom denna domän. Vi kommer med säkerhet att få ökade möjligheter att utbyta information med omgivningen, och att styra saker omkring oss utifrån vilka vi är och vad vi vill, men exakt hur, vilka saker, och i vilket syfte är ytterst svårt att sia om.

3.3.2 Samhälle

Diskussionen om IoT handlar också om att effektivisera samhället och hitta lösningar som är billiga och som förbättrar livskvaliteten för många. På

[17] Europeiska kommissionen 2014.

[18] Detta är en grov och högst preliminär uppdelning av världen, och givetvis bara en av många möjliga uppdelningar.

samhällsnivå är effektiviseringsbehovet, säkerhetsaspekterna och långsiktig planering avseende till exempel klimatförändringar och en åldrande befolkning viktiga drivkrafter för innovation. Alltmer forsknings- och utvecklingsmedel styrs mot innovationer på systemnivå för att lösa samhällets utmaningar. Även näringslivet har ett stort mandat i detta avseende.

3.3.3 Industri

Inom industrin finns ett naturligt incitament att effektivisera för att maximera kapacitet och vinst. Det finns således en stark trend mot digitalisering av industrin. Begreppet Industri 4.0, som lanserades i Tyskland 2011, gör gällande att vi nu är inne i den fjärde industriella revolutionen efter ångmaskinen, elektriciteten och elektroniken.

Digitaliseringen avser både affärs- och produktdimensionen med målet att nå självorganiserande fabriker som gör kundanpassade produkter i små serier till konkurrenskraftiga priser. Produktionslinjerna är, enkelt uttryckt, uppbyggda av twittrande maskiner, som är uppkopplade och kommunicerar med varandra genom ett ständigt flöde av tweets.[19]

Dock föreligger en hel del utmaningar som eventuellt är speciella för just industri-domänen. PIMM är ett projekt som syftar till att implementera 5G i en av Bolidens gruvor för att ge styr- och övervakningsutrustningen snabb tillgång till olika molntjänster.[20] De förväntade resultaten av projektet är både förbättrad säkerhet och produktivitet genom bland annat färre människor under jord, övervakning av utrustning samt förebyggande underhåll genom fjärrdiagnos.

Men projektet syftar också till att utveckla en kravställning för industriell 5G vad gäller både miljökrav, tekniska krav, fördröjning och bandbredd samt att studera olika affärsmodeller och roller för de iblandade.

I samtal med företrädare för projektledningen framkom flera aspekter på vad som påverkar betingelserna för industriell IoT.[21]

Trådlösheten: Inom industrin är det viktigt att säkra driften, att skydda känslig information samt att se till att säkerhetsföreskrifter efterlevs. Det trådlösa upplevs allmänt som obeprövat och riskabelt. Trådbunden övervakning är relativt lätt att flytta över till trådlöst, men ”styrning chansar man inte med i onödan”. Detta gör till viss del den industriella sfären mer svårpåverkad än andra. Samtidigt som det rimligen är här mycket av *tekniken* utvecklas, så är dess

[19] Tysk-svenska handelskammaren (2018). Enligt tysk-svenska handelskammaren satsar Tyskland mer än 400 miljoner euro på IoT i sin tillverkningsverksamhet.

[20] Projektet är ett samarbete mellan Volvo, ABB, TeliaSonera, Ericsson, Wolfit, Luleå Universitet och Boliden.

[21] Punkterna är diskuterande och helt och hållet avhängiga författarnas tolkning av samtalet.

användning begränsad och hårt styrd av krav på avkastning, varumärkeskontroll, och trovärdighet inför kunder och leverantörer.

Algoritmerna: Om den första puckeln att komma över handlar om tillit till det trådlösa i sig, så är tilliten till algoritmerna nästa. Om man vill förverkliga idén om det trådlösa automatiserade produktionsflödet så måste man känna tillit till de algoritmer som ska styra produktionen. I vissa sammanhang, till exempel där personalsäkerhet är en stor fråga, är det ett långt steg att ta; den fullt ut automatiserade gruvan är troligtvis långt bort.

En fråga är vilken funktion industrin har för innovation och tekniskspridning jämfört med till exempel kollektiva nyttigheter och produkter för privatkonsumtion? Kan man se att utvecklingen följer något mönster? Generellt kan sägas att stora företag jobbar mer strukturerat med innovation, även om små företag ibland kan uppfattas som mer innovativa. Den gemensamma nämnaren inom industri är just de ekonomiska faktorerna. Om någonting till synes är lönsamt försöker man göra det, annars inte. Även tekniskspridning drivs av egenintresse inom industrin.

4 Påverkansfaktorer

I detta kapitel utvecklar och presenterar vi påverkansfaktorer, det vill säga faktorer som vi tror kan påverka utvecklingen av IoT. Vi för också en diskussion om faktorernas inbördes förhållanden (begreppsliga överlapp, kausala beroenden, mm.).

Tanken är att påverkansfaktorerna ska kunna användas för att ta fram explorativa scenarier. En möjlighet är till exempel att använda dem i en så kallad morfologisk analys, där kombinationer av attribut/egenskaper hos de olika påverkansfaktorerna används som byggstenar.[22]

4.1 Utveckling och presentation av påverkansfaktorerna

En uppsättning påverkansfaktorer konstrueras lämpligen med en kombination av två angreppssätt, dels utgående från generella kriterier (*top-down*), dels utgående från exempel (*bottom-up*).

En generell struktur att utgå ifrån finner vi i den så kallade PESTLE-modellen som används av organisationer för strategisk analys och planering i syfte att hitta faktorer i den omgivande makromiljön som påverkar verksamheten.[23] Modellen består av dimensionerna politik (P), ekonomi (E), sociala faktorer (S), teknik (T), juridik (eng. legislation (L)) och miljö (eng. environment (E)). Att modellen är så generell gör den lämplig i en förstudie som denna. Om ytterligare iterationer behövs kan en annan mer specialiserad eller komplex modell användas, beroende på vilka frågor som är intressanta, eller om det finns aspekter som inte kan belysas utifrån PESTLE-modellen.

Nedan presenteras påverkansfaktor utifrån PESTLE-modellens sex dimensioner. I några fall har dimensionerna brutits ned tematiskt för att framställningen ska bli lättare att följa. Varje dimension avslutas med ett antal frågor och osäkerheter som kan vara värda att ta med i en fortsatt analys.

[22] Morfologisk analys är en processinriktad metod att strukturera problem genom definition av problemvariabler och dessas respektive tillståndsrymder. Scenarier väljs sedan som kombinationer av tillstånd över de olika variablerna. Processen sker ofta i workshopform. Den morfologiska metoden är generellt tillämpbar på allt som kan karaktäriseras som komplexa problem och kan med fördel användas för just scenariokonstruktion. För en introduktion, se till exempel Ritchey 2006.

[23] Pestle Analysis 2018.

4.1.1 Politik

- **Kontroll**: I Sverige finns ingen central aktör som styr utvecklingen av IoT. En miljö med många aktörer på arenan kan vara kreativ, men den kan också innebära att utvecklingen går långsamt (olika standarder kan stötas mot varandra under en lång period innan någon ”tar lead”) och att den inte kommer över trösklar som kräver övergripande beslut. Överstatliga program som till exempel EU:s digitaliseringsplan[24], som hanterar förutsättningarna för regler, teknisk innovation, att äga data, nät osv., kan på lång sikt få stor betydelse. Kina och Ryssland med flera stater argumenterar för att IoT bör omfattas av nationell snarare än överstatlig kontroll, så kallad ”internetsuveränitet”. Detta innebär att man vill genomföra en begränsning av internetfriheten för att främja länders säkerhet och stabilitet.[25] Debatten om IoT tenderar att fokusera på möjligheterna med smarta lösningar eller säkerhetsriskerna. Men enligt Philip Howard, professor vid Oxford-universitetets Internetinstitut är IoT:s påverkan på politiken den absolut viktigaste faktorn.[26] För demokratier kommer IoT att påverka hur väljare påverkar det egna landets regering, men även hur regeringen påverkar och övervakar våra liv. För auktoritära styren har IoT specifika användningsområden, som vi redan idag kan skönja; framöver kommer information om medborgare och samhälle inte längre i huvudsak (eller kanske inte alls) baseras på opinionsundersökningar och samhällsvetenskaplig forskning, utan på kontinuerlig insamling av data om våra beteendemönster och andra aspekter av vår vardag. Detta innebär också stora möjligheter att påverka människor. Det viktiga, enligt Howard, är att beslutsfattare och medborgare är medvetna om konsekvenserna av IoT innan det blir en realitet. Det blir allt viktigare att nationella och internationella standarder som reglerar internet är transparenta och att privatpersoner är medvetna om var deras data hamnar i slutändan, men även att det finns möjligheter att påverka tillgången på privat data för politiska syften.
- **Internationell handel**: Handelshinder som fördyrar teknik har en dämpande effekt på utvecklingshastigheten. Om stater inte litar på varandra, och skapar egna system med mjuk- och hårdvaruprodukter, så uppstår kanske många olika svar på samma typer av konsumentbehov. Om de avgränsade marknaderna är små kanske utvecklingen blir ineffektiv och/eller resultaten suboptimala?
- **Offentlig förvaltning**: Något som ofta nämns är den offentliga sektorns ansvar för ”horisontalisering” och demokratisering av tekniken i termer av datadelning och transparens. I vilken grad kan samhället åtnjuta effekter av

[24] Europeiska kommissionen 2018.
[25] Dowel & Goldstein 2016.
[26] Howard 2015.

den nya utvecklingen (socialt, tekniskt, ekonomiskt) och i vilken mån kan offentlig förvaltning stimulera den? Blir den offentliga förvaltningen katalysator eller bromskloss?

4.1.1.1 Frågor/osäkerheter

- Hur framgångsrika blir de stora digitaliseringsprogrammen (till exempel EU:s)?
- Vem kommer ta ansvar för näten?
- Kommer samhällskritisk verksamhet att prioriteras?

4.1.2 Ekonomi

- **Affärsmodeller**: När aktörer vill skydda sig genom att stänga inne data från sina produkter och tjänster uppstår inte den dynamik som kan vara nödvändig för etablerande av en ny teknik. Om inte aktörerna vill dela data fritt och förlita sig på att deras tjänster står på egna ben affärsmässigt, så kanske det behövs ”datamäklare” som ser till att rätt data kommuniceras till rätt aktör vid varje givet tillfälle.[27]
- **Tillverkningskostnader**: Det behöver vara relativt billigt att producera alla dessa kommunicerande komponenter. Även batterier behöver, förutom att ha hög kapacitet, vara billiga att tillverka.
- **Tillväxt**: Konsumenternas köpkraft påverkar utvecklingshastigheten, särskilt eftersom det handlar om nätverksteknologi där kommunikation och smarta algoritmer står i fokus. Ju fler som använder tekniken desto fler kommer att vilja hoppa på tåget. Ju mer global marknaden är desto större är den potentiella effekten. En viktig fråga är om användarna har råd och är intresserade av den nya funktionaliteten, och därmed skapar ”pull”.
- **Arbetsrollen**: Automatisering av fysiskt arbete och beslutsfattande tenderar att göra den traditionella arbetaren överflödig.

4.1.2.1 Frågor/osäkerheter

- Vem äger data och hur delas den? Vem kommer att vilja äga produkterna? Vem kommer att tjäna pengar på data?
- Hur billigt kan det bli att tillverka batterier och sensorer?

[27] Se till exempel Ny Teknik 2015.

- Kan man överbrygga stuprören med bra affärskontrakt? Hur påverkas möjligheten att skapa affärsöverenskommelser och allianser, och hur känsligt är IoT-området för aktörers misslyckanden?
- Kommer användarna att finnas där?
- Kan facken bromsa utvecklingen?

4.1.3 Sociala faktorer

- **Tillit**: Tillitsaspekten kan röra teknikens eventuella påverkan på miljön och på människors hälsa och välbefinnande, att processer skyddas vederbörligen, liksom att data hanteras på korrekt sätt och att produkter och algoritmer gör vad de ska.
- **Kultur**: Den kulturella kontexten påverkar hur vi använder produkter och tjänster och är en viktig del i hur de definieras och utvecklas. När det gäller utvecklingen av IoT kommer synen på vad som är privat och rätten till ägande av information att kunna spela stor roll. Vilka aktörer kommer se sig som de rättmätiga ägarna av informationen som skapas? Vilken information kommer det att vara begränsad tillgång till och varför? Kommer staten att skaffa sig tillgång till all information för att garantera medborgarnas säkerhet? Vilka kommer då att vilja, respektive inte vilja, använda olika IoT-saker? Hur kommer det att påverka hur människor beter sig om alla faktiskt i praktiken är konstant övervakade?
- **Demografi**: En kontinuerligt ökande andel äldre som behöver vård kan sätta tryck på vissa samhällsfunktioner. Detta kan katalysera acceptansen för IoT.
- **Upplevd nytta** (behovstillfredsställelse, känsla av välbefinnande, etc.): Denna parameter samspelar med tilliten till IoT. Om den upplevda nyttan är stor så kan eventuellt något avkall göras på säkerheten. Å andra sidan gäller detta olika tjänster och produkter i olika utsträckning. För vissa är säkerheten sekundär och nyttan primär. För andra, kanske främst i den industriella sektorn, är förhållandet oftast det omvända.

4.1.3.1 Frågor/osäkerheter

- Vad händer med synen på personlig integritet? Kommer människan att anpassa sig till tekniken?
- Kommer IoT aktivt att väljas bort? Är ”IoT-fria” produkter nästa stora marknadsnisch?
- Hur utbredd/stark kommer ”IoT-kriminaliteten” att bli?

4.1.4 Teknik

- **Tillgänglighet**:
    - Takten i teknikutvecklingen påverkas av hur tillgänglig tekniken är. I detta fall behöver rätt typ av teknik vara billig. Alla ingående komponenter måste bli billiga med tanke på hur många IoT-enheter som ska spridas i samhället.[28]
    - Öppen källkod ses av vissa som en förutsättning för att skapa allianser för utveckling av den nya tekniken. Exempel på ett område där detta skulle kunna vara givande är kommunikationsalgoritmer och protokoll. Detta för att öka transparensen och tilliten till exempelvis säkerheten.
- **Infrastruktur**:
    - *Batterikapacitet*: Eftersom många av de ingående enheterna i ett IoT-system är trådlösa blir batterikapacitet och energieffektivitet viktiga parametrar. Utvecklingen av batteriteknik och kapacitet kommer specifikt att påverka delar av utvecklingen mot ett samhälle med ”uppkopplade prylar”. Ju mindre och kraftfullare man kan göra batterier desto fler möjligheter öppnar upp sig.[29, 30]
    - *Sensorer*: Billiga, stabila sensorer är en förutsättning för IoT. Sensorteknikens mognadsgrad, och de osäkerheter som eventuellt finns inom området har en tydlig koppling till utvecklingen.
    - *Kommunikationer*: Hastigheterna och räckvidden i det trådlösa IoT-samhällets kanaler kommer att påverka utvecklingen. Kanske görs kvantsprång tidigt i utvecklingen som gör att man relativt snart når en nivå där bandbredden är tillräcklig för de flesta applikationer? Kanske är behovet av ökad bandbredd något som aldrig avtar? Vad gäller kommunikationstekniken i sig ses 5G som den kanske viktigaste *möjliggöraren*. Tekniken är framtagen för mobil kommunikation i hög hastighet. En annan teknik som anses ha stor betydelse är Narrowband/LTE.[31] Denna teknik kännetecknas av låg energiåtgång, lång räckvidd och billig teknik. Potentiella hot mot utbredningen av smalband respektive 5G skulle kunna uppstå i form av oförutsedda tekniska tillkortakommanden.
- **Säkerhet**: Säkerhetsaspekterna, och vår förmåga att upprätthålla säkerhet i dess olika former kan påverka vad tekniken används till och kostnaderna för

[28] Ibland i dessa sammanhang används uttrycket att ”strössla” med IoT-produkter.
[29] McKinsey Global Institute 2015.
[30] Mattern & Floerkemeier 2010.
[31] Se till exempel U-blox (2018).

produktion och användning. Framgång i skyddandet av data kommer att vara avgörande för tilltron till den nya tekniken i alla sektorer. ”Privacy by design” och andra principer (till exempel de som förordas av DHS[32]) måste få stort genomslag relativt snabbt. Konfidentialitet, riktighet, tillförlitlighet och spårbarhet blir ytterst viktiga på samhällsnivå och inom industrin där säkerhet kan handla om liv och död, eller företagets fortsatta existens. I industriella applikationer är tillförlitligheten så pass överordnad att den anses ha en tydlig påverkan på acceptansen av tekniken. Inom ramen för säkerhet återfinns även behovet av att kunna upprätthålla den personliga integriteten. Eftersom både IoT och IT i grunden handlar om kommunikation och information finns det enligt Kamrani m.fl. (2016) skäl att anta att många av de utmaningar beträffande säkerhet och integritet som är typiska inom IT också kommer att vara de mest framträdande inom IoT, och att det förhåller sig på samma sätt med strategier för bemötande av dessa utmaningar. Dock finns enligt Kamrani m.fl. ett antal skillnader som ställer krav på nya strategier. Skillnaderna kan sammanfattas med ökad heterogenitet, stora mängder ackumulerad persondata, enheter som ”kommer och går” samt ökad fysisk exponering.[33]

- **Standarder**: Något som krävs för fullt genomslag i kommunikationsflödena är att man lyckas få till någon eller några enhetliga standarder för hur alla saker ska kommunicera. Inom industrin är en av utmaningarna att få till standarder som leverantörerna använder sinsemellan.
- **Smarta algoritmer, molntjänster, big data analytics, etc.**: Poängen med att koppla upp saker är att de ska kunna agera utifrån analyser av den information som nätverket av saker sammantaget bidrar med. Detta gäller förutom stora mängder delad data även smarta algoritmer.

4.1.4.1 Frågor/osäkerheter

- Tekniska genombrott: Hur utvecklas batteritekniken? När sker genombrottet för IPv6 och hur viktig är tekniken för IoT? I vilken skala och hur snabbt kan 5G byggas ut och vilka alternativ finns? Kommer sensornäten att kunna utgöra en redundant struktur? Vad händer inom områden som big data, molntjänster, och smarta algoritmer? Hur snabbt går utvecklingen inom till exempel AI? Hur viktig är denna utveckling för olika tillämpningar?
- Tillförlitligheten hos system i industriella applikationer kommer att vara avgörande för hur snabbt trådlös kommunikation för styrning kommer att

[32] Department of Homeland Security 2016.
[33] I Swaling & Johansson (2018) diskuteras strategier kopplade till risker som dessa egenskaper kan föra med sig.

accepteras. Hur robusta och säkra kan systemen bli? Slår ”privacy by design” och andra viktiga säkerhetsprinciper igenom?

4.1.5 Juridik

De juridiska faktorerna speglar i mångt och mycket faktorerna på de andra områdena. Det handlar om juridiska aspekter av införandet av tekniska standarder och regelverk för till exempel upphandling, liksom affärsmodeller och andra slags överenskommelser. Den sociala acceptansen för, och tilliten till, ny teknik är beroende av möjligheterna att lagföra brott. Vad händer när en IoT-sak tar beslut som skadar eller inkräktar på annans liv eller egendom? Vad händer när ett antal ”prylar” gemensamt tar ett sådant beslut? Vad händer om beslutet är korrekt men bygger på felaktig data från en tredje aktör? Juridikens svårigheter att hänga med i teknikutvecklingen (se avsnitt 3.2) kan fortsatt tänkas påverka teknikutvecklingen, och fortsatt ge merkostnader för samhälle, industri och individ (jämför till exempel privatkopieringsavgiften).

4.1.5.1 Frågor/osäkerheter

- Vad händer med juridikens oförmåga att hänga med i teknikutvecklingen? Kommer juridiken att halka allt längre efter och därmed bromsa utvecklingen ännu mer än tidigare, eftersom tillit är en så viktig faktor?
- Vem ska ha ansvaret för händelser som orsakas av IoT-saker? Tillverkaren?
- Vad innebär GDPR för utvecklingen?

4.1.6 Miljö

Den gröna omställningen och behov av anpassning till ett förändrat klimat antas vara viktiga drivkrafter bakom utvecklingen av IoT, till exempel genom flera stora forskningssatsningar med inriktning mot framtidens smarta elnät. I det avseendet kan den reella utvecklingen på miljöområdet ha effekt på utvecklingen inom IoT.

4.1.6.1 Frågor/osäkerheter

Hur snabbt går omställningen och hur ser dessa beroende ut till utvecklingen inom IoT? Kan flaskhalsar uppstå på grund av att de olika spåren utvecklas i olika takt eller på olika villkor?

4.2 Faktorernas inbördes förhållanden

Ovan presenteras faktorerna utan någon strikt analys av hur de förhåller sig till varandra. Om påverkansfaktorer ska användas för att ta fram scenarier kan det emellertid vara viktigt att beakta om de till exempel förutsätter varandra logiskt eller kausalt, om det ena tillståndet alltid föregår det andra eller om någon faktor fungerar som drivkraft för flera andra faktorer. Vidare kan vissa faktorer ha karaktären av hot mot utvecklingen, medan andra snarare *är* utvecklingen. Andra faktorer kan handla om hur IoT tolkas och förstås. Nedan förs ett inledande resonemang som förhoppningsvis gör det lättare att tillämpa faktorerna i ett framtida arbete.

4.2.1 Drivkrafter

Är det innovationerna i sig, ekonomiska krafter eller de individuella och samhälleliga behoven som driver utvecklingen? Stenumgaard (2015) kopplar utvecklingen till fenomenet *vinstgap* vilket kan sammanfattas med att IoT är en frukt av att telekombranschen inte längre kan göra pengar på uppkopplade människor eftersom dessa är för få. Det behövs, menar Stenumgaard ett nytt koncept för kostnadseffektiv och skalbar mobil infrastruktur för den ökande mängden mobil data, om marknaden ska kunna fortsätta växa. Eftersom mängden mobilabonnemang som är möjlig att uppnå dessutom begränsas av antalet människor på jorden, så måste nya tillämpningar för mobil bredbandskommunikation utvecklas. Målet framöver är därför att utrusta de flesta elektroniska system med trådlös internetuppkoppling. Genom att göra detta inom i princip samtliga samhällssektorer skapas visionen om det fullt uppkopplade samhället, och till detta behövs enligt Stenumgaard 5G.[34]

Mer behovsorienterade argument brukar handla om möjligheter att förbättra servicen inom äldrevården, att hitta anpassningar för att minska miljöpåverkan (smarta elnät och hus) samt den alltjämt fortgående urbaniseringen. Här handlar det om behov av effektivisering för att få ner kostnader i hela värdekedjan, inklusive slitage på miljön, och samtidigt erhålla ökad välfärd.

Men vad är då en drivkraft? Det kan vara svårt att peka ut en specifik faktor som den huvudsakligen drivande, och ett sådant utpekande kanske inte heller ger varken en sann eller särskilt intressant bild av hur saker och ting förhåller sig. Somliga för fram teknikens naturliga utveckling och inneboende kraft[35], och i så måtto kanske IoT kan ses som den naturliga utlöparen av internet. Med en alltför ”teknikdeterministisk” syn kan man dock missa aspekter som exempelvis den

[34] Stenumgaard 2015.
[35] Se till exempel Blomqvist & Kaijser 1998.

roll som olika användargruppers tolkningar spelar för vilket paradigm som slutligen etableras.[36]

I någon mån är IoT en del av samhällets (och teknikens) utveckling i stort, och i så måtto torde utvecklingen kunna kopplas till ett antal övergripande, tvärsektoriella och globala, megatrender. Sådana återfinns exempelvis i Energimyndighetens *4 framtider – Energisystemet efter 2020*.[37] Bland trenderna hittar vi exempel på vad skulle kunna utgöra både tekniska och behovsmässiga incitament till utvecklingen inom IoT, och vissa som till och med skulle kunna sägas inbegripa eller *vara* utvecklingen av IoT. Därmed är det svårt att inte se IoT som något som faktiskt hänger ihop med hur samhället och kulturen utvecklas i stort.

4.2.2 Grundläggande förutsättningar

På samma sätt som med drivkrafterna är det svårt att säga vad som är de yttersta förutsättningarna för IoT. Efter att någorlunda förutsättningslöst ha gått igenom flera olika påverkansfaktorer kan vi dock sätta fingret på några utan vilka vi har *svårt att ens tänka IoT*. Det gäller till exempel den tekniska infrastrukturen, och människorna som använder den. Men vi har också sett att ett moget IoT troligen kommer att bygga på nya affärsmodeller, standarder och regelverk, och att säkerhetsaspekten och tredje mans förtroende för utvecklingen går som en röd tråd genom hela sammanhanget.

Utan dessa saker menar vi att det är svårt att se hur IoT skulle kunna komma att bli något väsentligt nytt eller bra, eller alls matcha de mer vågade föreställningarna om vad IoT skulle kunna vara.

4.2.3 Hot och sårbarheter

Nästan all litteratur och alla intervjuer om IoT berör olika hotbilder. Ibland handlar det om hot mot IoT och huruvida IoT är sårbart för dessa. Ibland handlar det om hot som är förknippade med eller kan bli en del av IoT, som ett slags cancersvulster, och som samhället bör försöka undvika eller bygga bort på olika

[36] Både teknikdeterminismen och betydelsen av olika samhällsgruppers tolkningar av ny teknik har diskuterats flitigt inom området science and technology studies (STS), se till exempel Blomqvist & Kaijser (red.) 1998. Starka företrädare för det socialkonstruktivistiska perspektivet är till exempel Wiebe Bijker och John Law (se exempelvis Bijker m.fl. 1987).

[37] Energimyndigheten (2016). De megatrender som föreslås är att global uppvärmning fortsätter, att fattigdom minskar och utbildningsnivån ökar, att natur-, miljö- och hälsofrågor blir allt viktigare, att digitalisering utvecklar helt nya tjänster, att teknisk utveckling fortsätter i snabb takt, att globalisering länkar ihop länder på nya sätt, att fler människor behöver bostäder samt att konkurrensen om naturresurserna ökar.

sätt. I vissa fall handlar det om att IoT i sig är ett hot, mot samhället, demokratin, eller självaste internet.[38]

Bland hot förknippade med IoT nämns ofta saker som elektromagnetisk störning eller vilseledning med eventuella olyckor eller andra olägenheter som följd. Sådana händelser behöver inte vara överlagda utan kan också uppstå på grund av system- eller handhavandefel. Det talas också ofta om olika cyberhändelser i samband med IoT, exempelvis DDoS-attacker (DDoS = Distributed Denial of Service) eller stöld av data för sabotage eller utpressning (ransomware). [39]

Hotet mot samhället består såtillvida i att IoT antas utgöra ett slags hävstång för olika redan kända fenomen genom att konsekvenserna blir större (i vissa framställningar rentav oöverskådliga), samt att angreppen kommer att bli både fler och lättare att genomföra eftersom det finns fler enheter att angripa och eftersom dessa är trådlösa.[40] Förekomsten av sådana hot är något som själva tekniken för med sig; de är så att säga medaljens baksida.

En sak som vi tror är viktig är att även den teknik som idag betraktas som gammal och etablerad erbjuder många användningar som går emot dess syften utan att dessa för den skull exploateras.[41] Säkerligen kommer kriminella att hitta nya vägar i och med de möjligheter som erbjuds med uppkopplade ”prylar”, big data etc., men å andra sidan är detta sådant som alltid kommer med den tekniska utvecklingen. Det är till syvende och sist industrins och allmänhetens förtroende för tekniken som kommer att vara gränssättande.

4.2.4 Mål eller medel

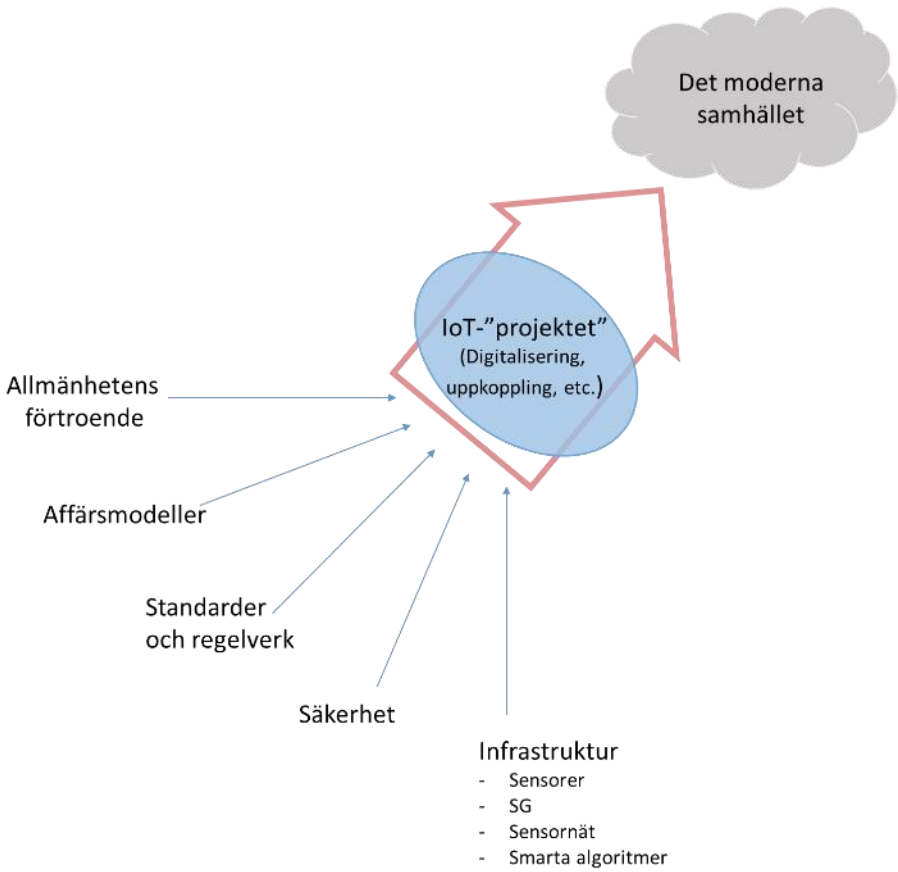
Att prata om hot och sårbarheter framstår inte som meningsfullt om det inte finns något som hotas, det vill säga ett skyddsvärde. Normalt används hot om något som hotar en resurs eller en aktivitet och som därmed hindrar ett mål från att uppnås.

IoT kan formuleras både som ett mål i sig eller som en aktivitet för att uppnå ett högre mål. Om IoT i sig är målet kanske *digitalisering*, *uppkoppling*, och annat kan sägas vara de aktiviteter som leder dit. Om IoT istället är det medel som

[38] Hyppönen 2017.
[39] För en sammanställning av olika hot och risker med IoT, se Swaling & Johansson 2018.
[40] Ibid.
[41] Vad beror det på? Kanske är det så att samhällets ”tolkning” av tekniken gör att den i bästa fall bidrar med att den blir internaliserad som något gott? Hur många tänker, varje gång de ser en hammare, att ”där ligger något man kan slå ihjäl någon med”? Hur många sådana ”negativa” användningar av teknik finns implicit runt omkring oss? Inte nödvändigtvis färre än de goda användningarna, varav många vilar oupptäckta, och kanske förblir oupptäckta för evig tid.

leder mot högre mål som i ”världens smartaste stad år 2040”, som Stockholms stad uttrycker sin vision, så kanske man kan tala om IoT som ett projekt.[42]

En modell för att strukturera mål-medel-hierarkier återfinns inom den så kallade programteorin, vars grundläggande syfte är att möjliggöra uppföljning av projekt. Programteorins kärnbegrepp är aktiviteter, resurser och resultat.[43] Figur 1 visar hur det kan se ut när begreppsstrukturen tillämpas på IoT. Hur det som hotar kommer in i bilden är något oklart. Ritar man upp det som vi har gjort så är hoten något som slår mot resurserna. Om man å andra sidan väljer att se resurserna själva som en del av IoT måste man kanske istället tolka hoten i termer av anomalier.

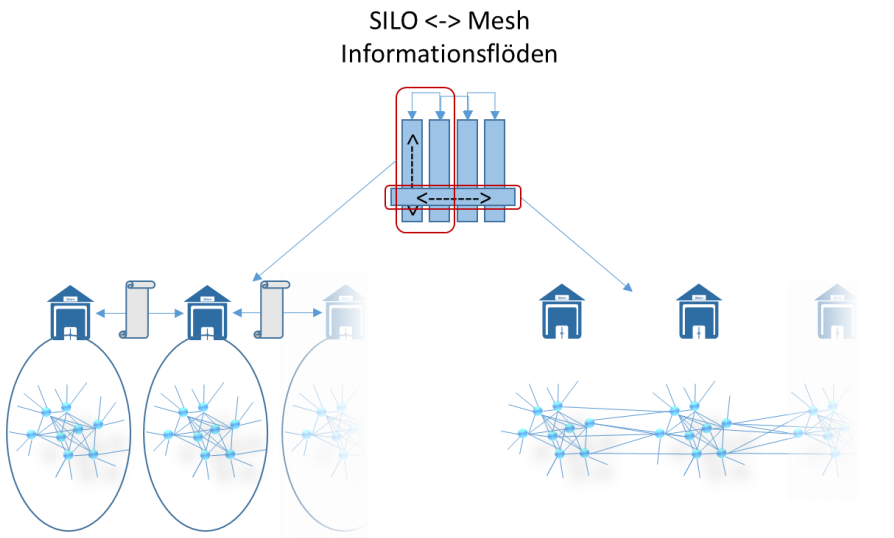


Figur 1: IoT som projekt betraktat, med resurser till vänster och resultatet uppe till höger.

[42] Stockholms stad 2018.
[43] Donaldson 2007.

5 Framtidsbilder

Data- och informationsdelning kommer att vara en vital komponent i IoT-utvecklingen. Frågan är bara hur delningen kommer att gå till. I vår research har vi tyckt oss kunna identifiera två relativt tydliga, delvis mot varandra stående, framtidsbilder; ”mesh-framtiden” och ”silo-framtiden”, representerade av vertikalt respektive horisontellt orienterad informationshantering. Skillnaden mellan de två framtiderna illustreras i Figur 2 och beskrivs utförligare nedan.



Figur 2: Illustration av skillnaden mellan en vertikalt orienterad silo-struktur och en horisontellt orienterad mesh-struktur. Silo-strukturen innebär att kommunikationen mellan olika användare är strikt avtalsreglerad och framförallt sker mellan olika organisationers övre strukturnivåer. Kommunikation mellan enheter i de fysiska lagren sker därmed endast inom en och samma silo. Mesh-strukturen innebär att i princip vilken enhet som helst kan kommunicera fritt med vilken annan enhet som helst, oavsett organisationstillhörighet.

Mesh-framtiden: Ett mesh-nätverk är i korthet ett nätverk av noder där varje nod är kopplad till en eller flera andra noder. ”Full mesh” är ett nätverkstypologiskt begrepp som innebär att alla noder är kopplade till alla andra noder, vilket ger största grad av redundans. Mesh-framtiden är därmed konsistent med en framtid där *allt pratar med allt*. I detta horisontella informationsflöde är IoT-visionen mer total/allomfattande och utvecklas mer organiskt. Mesh-framtiden företräds typiskt av samhällsbyggare och digitaliseringsentreprenörer.

Silo-framtiden: I kontrast till mesh-framtiden ser andra aktörer framför sig en framtid där saker inte alls tillåts prata fritt med varandra. I denna framtid sker istället informationsutbyten i vertikala segment, silos, inom en aktörs

kontrollerade sfär, och mellan aktörer på hög organisatorisk nivå eller strikt reglerat genom avtal. Informationsutbytet mellan exempelvis bilar av olika märken sker då på central nivå mellan respektive företag. Företagen låter i sin tur bilarna kommunicera endast strikt specificerad information via olika protokoll med motiveringen att informationen i sig är helt avgörande för företagets överlevnad.

Silo-perspektivet företräds typiskt av industriaktörer, och tidshorisonten är typiskt kortare än hos mesh-förespråkare.

5.1.1 Vart är vi på väg?

Under projektet har det blivit tydligt att det råder skilda uppfattningar om vart utvecklingen är på väg. Att säga att IoT-utvecklingen handlar om saker som agerar självständigt utifrån ett omfattande informationsflöde är inget kontroversiellt. Dock varierar bilden av hur långt i utvecklingen vi kommer att ha hunnit vid en viss tidpunkt, och hur långt utvecklingen kommer att gå över huvud taget.

När det gäller samhällsrisker hävdar somliga att IoT visserligen ger upphov till nya möjligheter och kan bidra till ekonomisk tillväxt, men att det samtidigt finns stora utmaningar i form av sårbarheter för kritisk infrastruktur och risker med hantering av information om individer, till exempel var de befinner sig, och att det därför inte är lämpligt att utvecklingen av IoT överlämnas helt till den privata sfären eller till andra nationer. Enligt EU-kommissionen är den grundläggande utmaningen att garantera informationssäkerhet:[44] ”*Strengthening trust, security and end-to-end personal data protection and privacy by taking into account the needs of the digital and digitised industry in the field of IoT is a priority for the Europeiska kommissionen.*”[45] Även IERC är inne på samma linje: ”*IoT requires an inclusive governance framework which is as yet inexistent.*”[46]

Men även riskerna för själva ”IoT-projektet” lyfts fram. Till exempel framhåller IDC EMEA lägre ekonomisk tillväxt och begränsat politiskt stöd som de största riskerna för IoT-utvecklingen.[47]

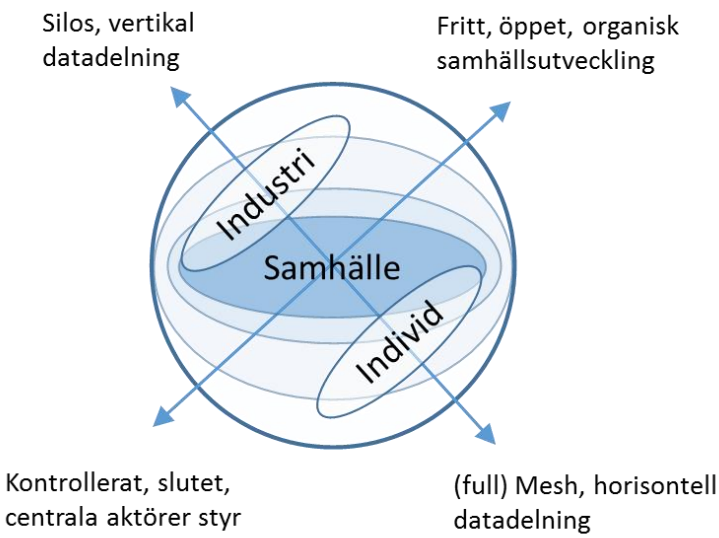
5.1.2 Dimensioner

Oavsett hur snabbt utvecklingen går, och vad den för med sig, tror vi oss ha identifierat två dimensioner som spänner upp IoT-tillvaron vid en given tidpunkt.

[44] Europeiska kommissionen 2009.
[45] Europeiska kommissionen 2016.
[46] Europeiska kommissionen 2015.
[47] Ibid., s. 27.

Den ena dimensionen handlar om data- och informationsdelning, vi kan kalla den ”silo-mesh”-dimensionen. Silo-framtiden representeras av den övre och vänstra kvadranten i Figur 3, medan mesh-framtiden representeras av den undre och högra kvadranten.

Den andra dimensionen handlar om hur öppet eller kontrollerat IoT blir över tid. Antingen följer utvecklingen en kurva motsvarande den för till exempel internet, som kan anses ha varit fritt och öppet till en början, för att (eventuellt) successivt bli mer och mer kontrollerat, eller så lägger myndigheter och andra aktörer på lager av kontroll tidigt i utvecklingen. Vi kan kalla dessa ”fritt/öppet-kontrollerat/slutet”-dimensionen. ”Fritt och öppet” representeras av den övre och högra kvadranten i Figur 3 medan ”Kontrollerat och slutet” representeras av den undre och vänstra kvadranten.



Figur 3: Övergripande dimensioner i utvecklingen av IoT.

Om vi betraktar IoT utifrån ovan beskriva dimensioner ser vi flera olika möjligheter beroende på var i samhället vi befinner oss.

I den framtid som motsvaras av den vänstra kvadranten upplever vi en hård styrning från dominerande aktörer avseende vilka informationsflöden som tillåts (silos och kontrakt) samtidigt som aktörerna utifrån säkerhetsargumentet styr utvecklingen baserat på hur de vill utvecklas (kontroll och säkerhet). Denna utveckling är (vilket vi också såg i avsnitt 3.3) fullt logisk för industriella tillämpningar, men man kan också tänka sig att industrin utvecklar sig på ett mer

organiskt och fritt sätt *med samma resultat*. Detta på grund av att aktörerna, stora som små, håller hårt på sin affärsmässiga integritet och helt enkelt inte vill dela information med varandra. Slutsatsen är att *industrinivån är konsistent med en silo-struktur* vilket illustreras med ”industri-bubblan” i Figur 3.

Motsatta betingelser antar vi råder på individnivå, det vill säga här tror vi att mesh-strukturen blir dominerande även i ett styrt och slutet samhälle eftersom informationen inte på samma sätt är kritisk och eftersom utvecklingen styrs av konsumenter på en konkurrensutsatt marknad där alternativen vanligen är många. Slutsatsen är att *individnivån är konsistent med en mesh-struktur* vilket illustreras med ”individ-bubblan” i Figur 3.

När det gäller samhället i stort och samhällsviktiga funktioner och system är det svårt att se hur en fri och öppen samhällsutveckling skulle vara konsistent med en utveckling där informationen låses in i silos och kontrolleras strikt av olika aktörer. Snarare går vi i det fallet mot något slags mesh-framtid även om det här finns breda marginaler och möjlighet för många olika strukturer att samexistera under lång tid framöver. Motsvarande gäller ett kontrollerat och slutet samhälle, det vill säga här är mesh-strukturen mer långsökt, om än inte utesluten.

Det ska påpekas att Figur 3 är mycket schematisk och bara översiktligt kan peka ut begreppskorrelationer, tendenser och vad som utifrån denna studie verkar mer sannolikt än annat.

5.1.3 Heterogenitet

Oavsett var i utfallsrummet vi kommer att befinna oss vid en given tidpunkt kommer vi troligtvis att fortsätta diskutera var vi är och var vi av olika anledningar borde vara. Figur 3 illustrerar att utvecklingen kan bli både kontrollerad och fri, vertikal och horisontell beroende på vilken domän som studeras.

Kanske är den ultimata lösningen en kombination av dessa strukturer med ett ordinarie samhällsnät och ett skuggnät som ger diversitet och därmed skapar robusthet? I en sådan framtid skulle en silo-struktur, exempelvis med 5G som bärande teknik, att stå för kommunikationen företag-företag och företag-användare och kanske främst i domäner där det ställs stränga krav på säkerhet, medan en mesh-struktur baserad på långvågig och billig svagströmsteknik, med låga säkerhetskrav (6Lowpan, LoRaWAN, ZigBee, etc.) står för kommunikationen mellan individer.

6 Avslutande diskussion

Syftet med denna rapport var att ta fram ett antal påverkansfaktorer att använda vid konstruktion av explorativa scenarier för att i förlängningen kunna dra slutsatser om vad som skulle kunna hända med IoT långt in i framtiden. Dessa påverkansfaktorer har tagits fram med utgångspunkt i PESTLE-modellen.

I identifieringen av påverkansfaktorerna har två olika framtidsbilder utkristalliserats. För det första en ”silo-framtid” där kommunikationen mellan olika enheter är strikt avtalsreglerad och framförallt sker inom en organisation. För det andra en ”mesh-framtid” där alla enheter kommunicerar fritt med varandra.

För det fortsatta arbetet har vi därmed några olika valmöjligheter. Vi kan välja att göra som tanken var från början, nämligen att bygga scenarier helt och hållet utifrån påverkansfaktorerna. Men vi kan också utnyttja de redan identifierade framtidsbilderna och med hjälp av påverkansfaktorerna undersöka utfallsrummet mellan dem och omkring dem. Detta skulle ge ytterligare insikt i bildernas soliditet och hur de förhåller sig till varandra.

En viktig fråga är också huruvida vi betraktar IoT som mål eller medel. Under projektets genomförande har vi stött på argument för bägge synsätten. Om vi betraktar IoT som mål, och om vi vill belysa hot och risker gentemot detta mål, behöver vi reda ut saker som *vad* detta mål faktiskt är, och *vem* som har detta mål. De som betraktar IoT som medel resonerar kanske snarare i termer av att teknik ska effektivisera produktion, men att denna teknik kan vara IoT eller något helt annat.

Vem tjänar då på IoT-utvecklingen? När kunder förväntar sig flat rate-abonnemang ser det ut som att teleoperatörerna kommer att få kämpa för att upprätthålla marginalerna. De kommer att uppleva högre krav på trafik parallellt med förväntningar om fasta priser. Samma utsikt kan tänkas möta dem som tillverkar de olika hårdvarukomponenterna som behövs i infrastrukturen. Deras branscher är redan lågmarginalbranscher. Möjligheterna för de som utvecklar tjänster och teknik för lagring och analys, med nya affärsmodeller på plats, kan vi dock idag knappast föreställa oss.

Säkerhetsaspekterna ligger som ett raster över flera påverkansfaktorer och har en särskild status inom ICS-området. Dels måste driftsäkerheten säkerställas, dels måste det finnas ett förtroende för den nya tekniken innan trådlöst kan bli aktuellt. Enskilda individer kanske fortsätter att avtala bort sitt privatliv i utbyte mot en smart ”pryl”, men det vi har lärt oss om IoT på ICS-området är snarast att incitamenten att introducera smarta produkter än så länge är svaga. Förklaringen är att när det gäller styrning av samhällsviktiga processer kan den exklusiva och oavkortade tillgången till garanterat korrekt data vara skillnaden mellan normalläge och katastrof.

Referenser

Bijker, W. E., Hughes, T. P., Pinch, T. (red.) (1987). *The Social Construction of Techno-logical Systems – New Directions in the Sociology and History of Technology*, The MIT Press, Cambridge.

Blomkvist, P., Kaijser, A. (red.) (1998). *Den konstruerade världen – Tekniska system i historiskt perspektiv*, Brutus Östlings Bokförlag Symposium, Stockholm.

Den digitala resan (2015). *Vad är Internet of Things?* Tillgänglig på: http://dendigitalaresan.se/vad-ar-internet-of-things/ Besökt 2018-10-25.

Department of Homeland Security (2016). *Strategic principles for securing the Internet of Things (IoT).* Version 1.0 November 15, 2016.

Donaldson, S.I. (2007). *Program Theory-Driven Evaluation Science – Strategies and Applications*. Psychology Press, New York. ISBN 978-08-05-84670-6.

Energimyndigheten (2016). *4 framtider – Energisystemet efter 2020*. ET 2016:0 4, Bromma.

Europeiska kommissionen (2009). *Internet of Things — An action plan for Europe*. Tillgänglig på: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF. Besökt 2018-10-25.

Europeiska kommissionen (2014). *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination*, s. 26. ISBN 978-92-79-47760-7. Tillgänglig på: https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination. Besökt 2018-10-25.

Europeiska kommissionen (2016). *Staff Working Document: Advancing the Internet of Things in Europe*, s.27. Tillgänglig på: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-Internet-things-europe. Besökt 2018-10-25.

Europeiska kommissionen (2018). *Digitalising European Industry*. Tillgänglig på: https://ec.europa.eu/digital-single-market/en/digitising-european-industry. Besökt 2018-10-25.

Frånberg, Ö. (2014). *Grunden för loT är en referensarkitektur.* Presentation vid IoT-seminarium hos Ericsson i Kista 26 oktober 2014. Tillgänglig på: http://docplayer.se/8275629-Iot-utblick-26-oktober-ericsson-kista-osten-franberg-iot-direktor-lulea-tekniska-universitet-centrum-for-distansoverbryggande-teknik.html. Besökt 2018-02-13.

Gartner (2018). *5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018*. Tillgänglig på: https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/. Besökt 2018-10-25.

Howard, P. (2015). *Politico: The Internet of Things is poised to change democracy itself*, http://philhoward.org/politico-the-Internet-of-things-is-poised-to-change-democracy-itself/. Besökt 2018-10-25.

Hyppönen, M. (2017). "State of the net", s. 21, Presentation på bl.a. Internetdagarna 2016 (arrangör IIS), nedladdningsbar via https://www.slideshare.net/mikkohypponen/state-of-the-net-73341628. Besökt 2018-10-25.

Jonsson, D.K. (2017). *Att använda scenarier i planering för civilt försvar*, Totalförsvarets forskningsinstitut, FOI-R--4434--SE, ISSN 1650-1942, Stockholm.

Kamrani, F., Wedlin, M., Rodhe, I. (2016). *Internet of Things: Security and Privacy Issues.* Totalförsvarets forskningsinstitut, FOI-R--4362--SE, Linköping.

Mattern, F., Floerkemeier, C. (2010). From the Internet of Computers to the Internet of Things. Tillgänglig på: https://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf. Besökt 2018-10-25.

McDowell, R.M., Goldstein, G.M. (2016). *The Authoritarian Internet Power Grab*. Tillgänglig på: https://www.wsj.com/articles/the-authoritarian-internet-power-grab-1477436573?tesla=y. Besökt 2018-10-25.

McKinsey Global Institute (2015). *Unlocking the potential of the Internet of Things*. Tillgänglig på: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-Internet-of-things-the-value-of-digitizing-the-physical-world. Besökt 2018-10-25.

Ny Teknik (2014). *Prylarnas internettoppar hajpkurvan*. Tillgänglig på: http://www.nyteknik.se/digitalisering/prylarnas-internet-toppar-hajpkurvan-6398526. Besökt 2018-10-25.

Ny Teknik (2015). *Därför dröjer Internet of Things*. Tillgänglig på: http://www.nyteknik.se/digitalisering/darfor-drojer-internet-of-things-6344142. Besökt 2018-10-25.

Pestle Analysis (2018). *What is PESTLE Analysis? A Tool for Business Analysis*. Tillgänglig på: https://pestleanalysis.com/what-is-pestle-analysis/. Besökt 2018-10-25.

Postscapes (2018). *Internet of Things Infographic. What Is The "Internet of Things"?* Tillgänglig på: https://www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/ Besökt 2018-10-25.

Ritchey, T. (2006). ”Problem structuring using computer aided morphological analysis”, *Journal of Operational Research Society*, 57(7):792-801.

Stenumgaard, P. (2015). ”Det fullt uppkopplade samhället – vision som kräver strategiska vägval”, i Sandö, C., Rydqvist, J., Langlais, R., red., *Strategisk utblick 6*, s. 97–104, Totalförsvarets forskningsinstitut, FOI-R--4130--SE, ISSN 1650-1942, Stockholm.

Stockholms stad (2018). *Världens smartaste stad år 2040*. Tillgänglig på: http://www.stockholm.se/OmStockholm/Smart-och-uppkopplad-stad/Varldens-smartaste-stad-ar-2040/. Besökt 2018-10-25.

Swaling, V.H., Johansson, J. (2018). *IoT-relaterade risker och strategier*, Totalförsvarets forskningsinstitut, FOI-R--4591--SE, MSB 2017-1554, ISSN 1650-1942.

Tritec (2018). *Internet of Things.* Tillgänglig på: http://tritec.se/erbjudande/internet-of-things/. Besökt 2018-10-25.

Tysk-svenska handelskammaren (2015). *Industrie 4.0: Svensk industri satsar på framtidsteknik*. Tillgänglig på: http://www.handelskammer.se/nyheter/industrie-4-0-svensk-industri-satsar-pa-framtidsteknik. Besökt 2018-10-25.

U-blox (2018). Tillgänglig på: https://www.u-blox.com/en/narrowband-iot-nb-iot. Besökt 2018-10-25.

Wikipedia (2018a). *Sakernas internet.* Tillgänglig på: https://sv.wikipedia.org/wiki/Sakernas_internet. Besökt 2018-10-25.

Wikipedia (2018b). *Maskin-till-maskin-kommunikation*. Tillgänglig på https://sv.wikipedia.org/wiki/Maskin-till-maskin-kommunikation. Besökt 2018-10-25.

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se