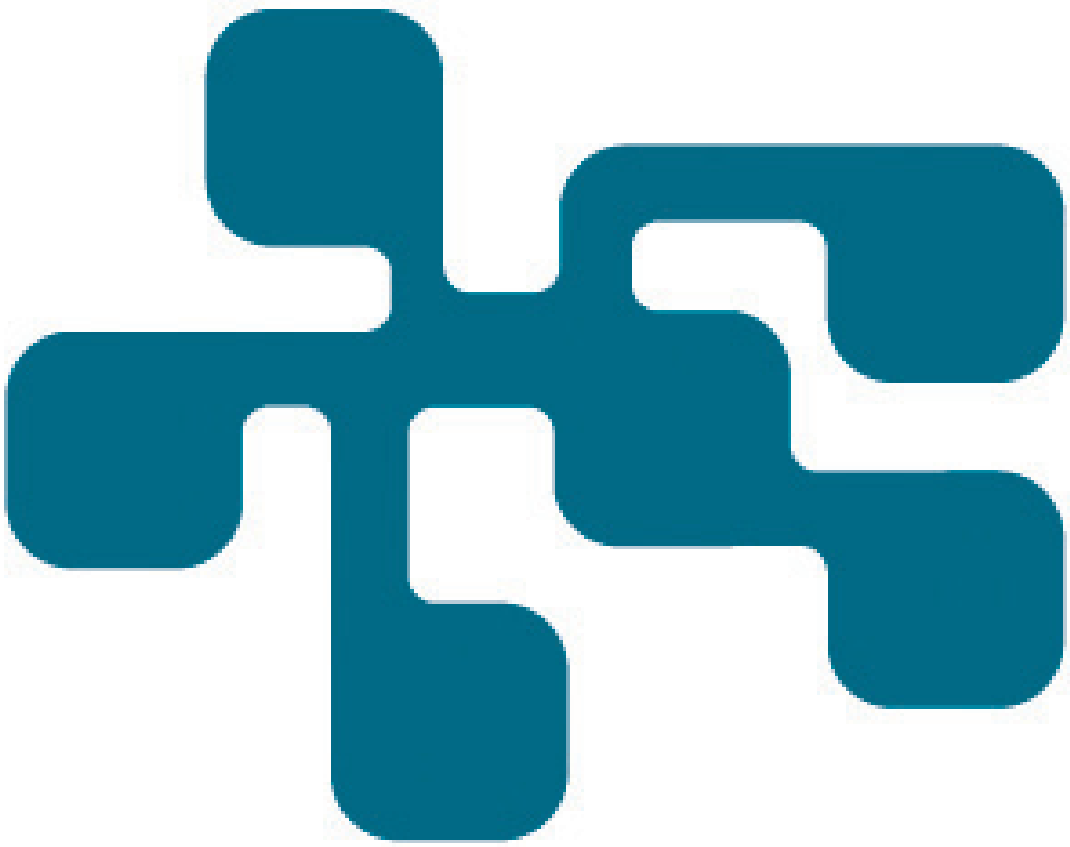
NCS3 - Industriella informations- och styrsystem inom fastighetsautomation

En förstudie

KARIN MOSSBERG SONNEK, FREDRIK LINDGREN

FOI
MSB



FOI-R--4206--SE
MSB 2015-953
ISSN 1650-1942

December 2015

Karin Mossberg Sonnek, Fredrik Lindgren

NCS3 – Industriella informations- och styrsystem inom fastighetsautomation

En förstudie

Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet

FOI-R--4206--SE

MSB 2015-953

Titel	Industriella informations- och styrsystem inom fastighetsautomation – en förstudie
Title	Industrial Control Systems in Building Automation - a pilot study
Rapportnr/Report no	FOI-R--4206--SE
Månad/Month	December
Utgivningsår/Year	2015
Antal sidor/Pages	42 p
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	
Projektnr/Project no	E 13471
Godkänd av/Approved by	Maria Lignell Jakobsson
Ansvarig avdelning	Försvarsanalys

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Fastighetsautomation är ett samlingsbegrepp för styrning och övervakning av fastighetsnära funktioner som värme, ventilation, belysning, hissar och passersystem. Fastighetsautomationen har utvecklats snabbt de senaste åren i strävan efter en ökad energieffektivisering. Det finns dessutom ekonomiska vinster med att kunna styra och övervaka flera fastigheter från en och samma plats. Utöver centrala styr- och övervakningssystem så innehåller fastighetsautomation en mängd olika informations- och styrsystem som styr enskilda funktioner. Dessa har traditionellt varit isolerade från omvärlden, men i och med den tekniska utvecklingen så kopplas fler och fler system upp mot internet vilket har ökat säkerhetsriskerna.

Samhällsviktig verksamhet är beroende av att fastighetsautomationen fungerar. Ett exempel är operationer på ett sjukhus som är beroende av att temperatur och ventilation fungerar tillfredsställande. För att få en övergripande bild av hur fastighetsautomation fungerar i Sverige så har MSB låtit genomföra en förstudie som har tittat på vilka aktörer som finns inom området, vilka tjänster som levereras och vilka system som stödjer tjänsterna. Studien har genomförts dels som en litteraturstudie, dels med hjälp av intervjuer av fastighetsägare och förvaltare, hyresgäster och ansvariga inom IT och informationssäkerhet.

Studien visar att fastighetsautomation är en komplex sektor som rymmer många aktörer som behöver interagera med varandra. Det samlade systemet för fastighetsstyrning består av delsystem och komponenter med olika livslängd, olika leverantörer och olika tekniska lösningar. Medvetenheten inom branschen om säkerhetsriskerna hos styrsystemen varierar. I de intervjuer som gjorts inom studien har vi tagit del av flera exempel på arbete med strategier, riktlinjer och krav för hur fastighetsautomationssystem ska kravställas, upphandlas och förvaltas. Rapporten kan användas till att identifiera områden inom vilka medvetandehöjande åtgärder kan genomföras.

Nyckelord: Fastighetsautomation, industriella informations- och styrsystem, samhällsviktig verksamhet, intervjustudie

Summary

Building automation is a generic term for control and monitoring of functions in buildings; such as heating, ventilation, lighting, elevators and access control system. Building automation has developed rapidly in recent years in the aim of increasing the energy efficiency. There are also economic benefits in being able to control and monitor multiple buildings from a single location. In addition to central control and monitoring system, building automation also includes a variety of information and control systems that control individual functions. These have traditionally been isolated from the outside world. With recent technology development it has become more common that these systems are linked to the Internet leading to increased safety risks.

Many critical societal functions are dependent on building automation functions. For instance are some activities in a hospital, such as operations, critically dependent of the regulation of temperature and ventilation. To get a comprehensive picture of how building automation are used in Sweden today, MSB initiated at study to identify which actors are involved, which services are delivered and what systems support these services. The study has been made partly as a literature study and partly by interviews of property owners and managers, tenants and responsible persons within IT and information security.

The study shows that building automation is a complex sector that includes many actors who need to interact with each other. The overall system for building automation consists of subsystems and components with different life times, different suppliers and different technologies. The awareness of the security risks within the area varies. In the interviews we got several examples of ongoing work of policies, guidelines and requirements describing how building automation systems should be purchased and managed. The report can be used to identify areas in which awareness raising activities could be implemented.

Keywords: Building automation, industrial control systems, critical society functions, interview study

Innehåll

1 Inledning

Med fastighetsautomation avses vanligen styrning och reglering av olika fastighetsanknutna funktioner såsom värme, ventilation och belysning. Även andra funktioner som hissar, rulltrappor, inpassering och larm kan ingå i området. ”Smarta fastigheter” förutsätter förutom styr- och reglersystem även att man utnyttjar sensorer och kommunikationsteknik. Inom detta område samman-strålar många begrepp och tekniker: cyberfysiska system, sakernas internet och industriella informations- och styrsystem.

1.1 Syfte

Syftet med studien som redovisas i detta memo har varit att ge en övergripande bild av hur fastighetsautomation ser ut i Sverige idag och specifikt i byggnader som rymmer samhällsviktig verksamhet. Fokus har legat på att beskriva vilka tjänster och funktioner som finns, vilka system som stödjer dessa tjänster och funktioner samt vilka aktörer som finns inom området. Mer perifert har studien även syftat till att beskriva vilka begrepp som används inom området och hur dessa förhåller sig till begrepp som MSB använder inom området industriella informations- och styrsystem, samt ansvarsförhållanden och beroenden.

1.2 Metod

Inledningsvis gjordes en litteraturstudie för att beskriva situationen inom fastighetsautomation i Sverige idag med avseende på vilka begrepp som finns och hur de används, vilken typ av system som finns och hur de är kopplade till varandra, vilka aktörer som finns på marknaden och vilka säkerhetsaspekter som finns samt förslag på lösningar för att komma till rätta med dessa. Litteratur-studien gjordes genom sökningar på internet, kontakt med kollegor inom FOI och ämnesansvariga på MSB.

Därefter genomfördes intervjuer med ett antal personer i företag och organisationer som äger fastigheter, som hyr fastigheter och som levererar och förvaltar fastighetsautomationssystem. De personer som intervjuades hade antingen ansvar för utvecklingen, installation eller drift av fastighetsautomationssystem eller också var de ansvariga inom IT, inklusive informationssäkerhet. Respondenterna redovisas i bilaga 1 och intervjuguiden i bilaga 2.

Respondenterna valdes ut enligt kriterierna:

- Verksamheten som bedrivs ska vara samhällsviktig eller direkt påverka samhällsviktig verksamhet.
- Aktörens fastighetsbestånd bör vara utspritt i olika delar av landet eller i olika delar av en region. (Så att det finns incitament att centralisera övervakning och styrning.)

De intervjuer som gjordes kan betraktas som fallstudier, det vill säga att de beskriver verksamheten vid de företag och organisationer där intervjupersonerna arbetar. Dessa beskrivningar är ett antal nedslag inom området och kan inte generaliseras till att beskriva det allmänna läget i Sverige, men förhoppningsvis kan de ge uppslag om intressanta frågor att studera vidare.

1.3 Avgränsningar

Fokus i studien har legat på fastighetsautomation (exempelvis ventilation, värme, kyla, luftkonditionering, belysning, solskydd, hissar, rulltrappor och entrélösningar) och inte på säkerhetssystem (exempelvis passersystem, kameraövervakning, brandlarm och inbrottslarm). Vissa frågor om säkerhetssystem och vilka beroenden det finns mellan dem och system för fastighetsautomation har dock ställts under intervjuerna.

Studien har inte omfattat ”smarta hem” i betydelsen utnyttjande av modern teknik inom databearbetning, kommunikation och sensorer i privatbostäder. Studien har inte heller syftat till att beskriva konsekvenserna av om systemen skulle upphöra att fungera eller om de manipuleras.

2 Bakgrund

I detta avsnitt redovisas resultatet av den inledande litteraturstudien vilket också var den förförståelse vi som intervjuare hade innan vi genomförde intervjuerna och som låg till grund för intervjuguiden (bilaga 2). En del av det som redovisas i det här kapitlet kom även upp under intervjuerna, och det är därför visst överlapp i innehållet i kapitel 2 och 3. Vi har dock valt att vara tydliga med vilka uppgifter vi har kunnat hitta i litteraturen och vad vi har fått reda på genom intervjuerna eftersom vi tycker att det säger något om området.

2.1 Vad som ingår i begreppet fastighetsautomation

Begreppet fastighetsautomation handlar om att *styra*, *reglera* och *övervaka* (se tabell 1) olika tekniska installationer och system i fastigheter för bland annat värme, ventilation, kyla, luftkonditionering, belysning och solskydd. Som ett samlingsbegrepp för funktionerna värme, ventilation och luftkonditionering används ofta, även i svenska sammanhang, den engelska förkortningen HVAC (Heat, Ventilation and Air Conditioning). Även andra system kan ingå i området, t.ex. hissar, rulltrappor, brandlarm och (tillträdes-)larm. System för inpassering och andra funktioner som handlar om tillträde till en fastighet räknas däremot inte alltid in i begreppet fastighetsautomation utan betecknas som säkerhets-system. [1]

Tabell 1. Exempel på styrning, reglering och övervakning

Styrning	att slå av och på en fläkt eller pump
Reglering	funktionsspecifik justering, t.ex. temperaturreglering
Övervakning	av temperatur, koldioxidhalt, närvaro, etcetera

De tekniska installationerna i en fastighet kan delas in i två kategorier, *klimatstyrande* respektive *betjänande* installationer.[2] De klimatstyrande installationerna svarar för inomhusklimatet och hit hör system för värme, kyla, ventilation och solskydd. De betjänande installationerna är knutna till verksamheten i fastigheten och hit hör system för tappvatten och avlopp, elnät, telenät, datanät, hissar, rulltrappor och passagesystem.

[1] Enno Abel och Arne Elmroth, *Byggnaden som system*, Forskningsrådet Formas, 2006.
[2] Ibid.

Tidigare användes ofta separata system för de olika funktionerna som styr/reglerar/övervakar, men digitaliseringen har inneburit att olika funktioner har integrerats i samma utrustning/system. ”Smarta fastigheter” förutsätter förutom styr- och reglersystem även att man utnyttjar sensorer, kommunikationsteknik och annan utrustning, se tabell 2.

Drivkraften för de senaste årens utveckling mot mer integrerade system för styrning av fastigheter har framför allt varit energieffektivisering.[3]

Tabell 2. Kategorier av utrustning för fastighetsautomation, hård- och mjukvara[4]

Kategori	Exempel
Styrsystem	för en eller flera funktioner
Operatörsverktyg	operatörspaneler, HMI, handdatorer, appar mm
Programvara	styrning, service/UH, mätning, energi, analys, energioptimering
Datanät	kommunikationsutrustning, fjärråtkomst, kommunikationsprotokoll
Trådlöst	kommunikationsutrustning, fjärråtkomst
Motorstyrning	elmotorer, motorstyrning, frekvensomriktare
Mätinstrument	temperatur, el/energi, flöde, vatten, gas, tryck, luftfuktighet mm

Fastighetsautomation delas i vissa sammanhang in i följande kategorier[5]:

- Bostäder
- Kontor och affärscentrum
- Produktionsfastigheter
- Specialfastigheter (sjukhus, museer, fängelser, m.fl.)

Ju längre ner i listan, desto mer komplexa blir installationerna och desto större blir kraven på driftsäkerhet.

[3] Ny Teknik, ”Automatik ska minska energinota”, 2012-03-06, (http://www.nyteknik.se/nyheter/automation/fastighetsautomation/article3408579.ece, hämtad 2015-02-25).
[4] Ur tidningen Automation, nr 10, 2012.
[5] Presentation av Magnus Edbolm vid Automation Summit, 2013, http://www.automationsummit.se/filer/presentationer2013/Magnus_Edblom.pdf.

Parallellt med *fastighetsautomation* används begrepp som *byggnadsautomation* och *fastighetsstyrning*.[6] Inom branschen är också *styr- och övervakningssystem* vanligt förekommande. Även begreppet *fastighetssystem* förekommer men används även som beteckning på system för rent administrativa uppgifter, t.ex. hantering av hyresavier. På engelska används bl.a. begreppet Building Automation Systems (BAS) och Building Management Systems (BMS) respektive iBMS (intelligent BMS).[7]

2.2 Uppbyggnad av system för fastighets-automation

Ett system för fastighetsautomation kan schematiskt delas in i tre nivåer (se figur 1)[8]:

- Informationsnivå
- Automationsnivå
- Fältnivå

På den översta nivån, *informationsnivån*, kan man övervaka och styra de tekniska installationer som ingår i den eller de fastigheter som ingår i systemet, exempelvis för att optimera energianvändningen. Här ingår bland annat programvara för att analysera och bearbeta den information som samlas in och operatörspaneler för att visualisera informationen (mätdata, driftdata, larm) och för att manuellt interagera med systemet.

På nästa nivå, *automationsnivån*, sker övervakning och reglering av elektrisk och mekanisk utrustning i fastigheten. På den här nivån är driften till stor del autonom (utgående från i förväg definierade börvärden för t.ex. temperatur eller koldioxidhalt), vilket innebär att systemen löper vidare utan avbrott vid eventuella fel på informationsnivån, då dock utan eventuella systemövergripande optimeringsfunktioner. Hårdvaran på denna nivå finns normalt i apparatskåp placerade i teknikutrymmen och kan oftast manövreras lokalt.

[6] Antal träffar vid Googlesökning: fastighetsautomation – 98 400 st, byggnadsautomation – 20 800 st, fastighetsstyrning – 2470 st, styr- och övervakningssystem – 37 000 st, fastighetssystem – 68 300 träffar (www.google.se, sökning utförd 2015-02-25)

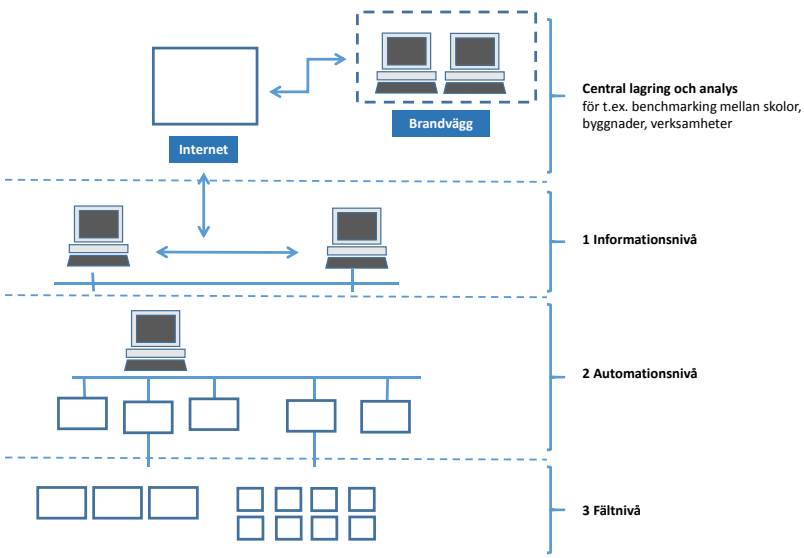
[7] Se bland annat David Fisk (2012) Cyber security, building automation, and the intelligent building, Intelligent Buildings International, 4:3, 169-181, http://dx.doi.org/10.1080/17508975.2012.695277).

[8] Texten i detta avsnitt är, om inte annat anges, baserat på beskrivningar i följande rapport: Göran Gustafsson, *SBUF 12471 Slutrapport Projekt Styr och Övervakning*, via http://www.sbuf.se/Projekt/?q=12471 (hämtad 2015-02-25). SBUF står för Svenska Byggbranschens Utvecklingsfond som finansierat projektet.

Fältnivån slutligen omfattar utrustning för detektion (t.ex. av rök och gas), mätning (t.ex. av temperatur) och manövrering via ställdon (av t.ex. fläktar och värmeelement). På denna nivå kan styrning av vissa funktioner ske på rums- eller zonnivå via vred, knappar eller paneler i de berörda lokalerna.

Det som inom området industriella informations- och styrsystem generellt benämns PLC (Programmable Logic Controller) kallas i fastighetssektorn ibland DUC (datoriserad undercentral). DUC:en har operativsystem, kör program och kommunicerar via nätverk, trådbundna eller trådlösa WiFi-nät. Relaterat till DUC är även begreppet DHC (datoriserad huvudcentral) till vilken det kopplas ett operatörsgränssnitt för övervakning.

Det finns en bred variation i datormiljöer, i kommunikationens utformning, i programvaror, i rapporteringsfunktioner samt i larmrutiner och styrmöjligheter, men det pågår en ökad standardisering för t.ex. kommunikation (kommunikationsprotokoll). Den pågående övergången till existerande standarder inom nätverks- och webbteknik för överföring av signaler och information kan innebära säkerhetsproblem. Detta genom att fastighetssystem i högre grad än tidigare ges funktioner för fjärråtkomst och i viss utsträckning också är exponerade mot internet.



Figur 1. Ritad utifrån figuren på s.11 i ”SBUF 12471 Slutrapport Projekt Styr och Övervakning” av Göran Gustafsson.

Såväl inom som mellan de olika nivåerna ingår även utrustning för överföring av information i form av mätdata och styrsignaler. Det finns kommunikations-protokoll speciellt utvecklade för fastighetsautomation, bl.a BACnet, LonWorks och KNX. Data kan överföras via så kallade bussar, olika former av trådbundna nätverk eller trådlöst.

2.3 Aktörer på marknaden för fastighetsautomation i Sverige

I den informationssökning vi har gjort, bland öppet publicerade källor, har vi inte hittat någon samlad analys av marknaden för fastighetsautomation i Sverige. Vi har därför idag inte något underlag för att peka ut dominerande aktörer på olika delar av marknaden i termer av omsättning och marknadsandelar. Vi har heller inte stött på några uppskattningar av hur stor den totala marknaden för fastighets-automation är i termer av årlig försäljning.

Det underlag som vi har gått igenom har däremot innehållit uppgifter om företag som är aktiva på marknaden och deras erbjudanden i termer av produkter och system. Underlaget om företag som i första hand erbjuder tjänster inom området är än så länge begränsat.

En marknadsöversikt publicerad i tidningen Automation beskriver produkt-erbjudanden från 36 olika företag som är verksamma i Sverige.[9] Översikten delar in marknaden för fastighetsautomation utifrån olika produktkategorier (hård- och mjukvara) och redovisar verksamma företag inom olika kategorier:

- Styrsystem (för en eller flera funktioner)
- Operatörsverktyg (operatörspaneler, HMI, handdatorer, appar mm)
- Programvara (styrning, service/UH, mätning, energi, analys, energioptimering)
- Datanät (kommunikationsutrustning, fjärråtkomst, kommunikationsprotokoll)
- Trådlöst (kommunikationsutrustning, fjärråtkomst)
- Motorstyrning (elmotorer, motorstyrning, frekvensomriktare)
- Mätinstrument (temperatur, el/energi, flöde, vatten, gas, tryck, luftfuktighet mm)

Här finns såväl stora aktörer (ABB, Honeywell, IBM, Siemens) som mindre och nischade företag (Elektro Relä, Piigab, CA Mätsystem) representerade. Värt att notera är att de riktigt stora aktörerna i flera fall har etablerat särskilda

[9] ”Marknadsöversikt: Fastighetsautomation”, Automation, nr 10, 2012.

divisioner/dotterbolag inriktade mot fastighetsautomation (Honeywell Building Solutions, Siemens Building Technologies.)

Schneider Electric och Imtech (f.d. NEA) är exempel på medelstora/stora aktörer på marknaden med en tydlig inriktning mot fastighetsautomation och som i likhet med ”bjässarna” också har erbjudanden i de flesta av produktkategorierna ovan.

Tidningen Automations lista[10] är dock långt ifrån heltäckande, här saknas t.ex. Kabona vars system Webbdatorcentral uppmärksammades i samband med DN:s granskning av informationssäkerhet under hösten 2014[11] (och då är Kabona sett till omsättning och anställda större än många av de andra företagen på listan.)

Genom att listan fokuserar på produkter bedömer vi att den saknar många av de aktörer som mer renodlat har valt rollen som återförsäljare, tekniska konsulter eller systemintegratörer. Under byggprocessen uppfattar vi att det är vanligt att anlita särskilda konsulter som upprättar de handlingar för styrsystem som behövs inför och vid själva bygget. Därefter anlitas ofta underentreprenörer för att leverera och installera systemen under byggnationen (det kan vara olika eller samma entreprenör).

Det finns få uppgifter om hur eftermarknaden ser ut i termer av drift och underhåll av systemen. Rimligen erbjuder leverantörerna support, service och uppdateringar till de system som de själva sålt och installerat. I vilken utsträckning fastighetsägare/-förvaltare erbjuds löpande drift och hantering av systemen som en del i ett helhetserbjudande från systemleverantörerna har vi inte lyckats klarlägga.

Däremot finns det i fastighetsbranschen aktörer som är speciellt inriktade mot fastighetsförvaltning och -drift i dess helhet. Eftersom systemen för styrning av fastigheternas olika funktioner är centrala för den tekniska driften av fastigheter bör rimligen det dagliga handhavandet av systemen ingå i dessa aktörers verksamhet. Begreppet teknisk fastighetsförvaltning används ibland för att skilja det från ekonomiadministrativa eller andra tjänster knutna till en fastighet. Exempel på företag inom området är Coor Service Management och Veolia (tidigare Dalkia).

Energimyndigheten initierade 2001 en beställargrupp för lokaler (BELOK) med syfte att sprida kunskap om energieffektivisering av fastigheter. Inom ramen för BELOK drivs för närvarande ett projekt om framtidens styr- och övervakning av

[10] ”Marknadsöversikt: Fastighetsautomation”, Automation, nr 10, 2012.
[11] Dagens Nyheter, ” IT-expert: Bristerna ett hot mot rikets säkerhet”, 2014-11-03 (http://www.dn.se/nyheter/sverige/it-expert-bristerna-ett-hot-mot-rikets-sakerhet/, hämtad 2015-02-24).

fastigheter. Ett mål för arbetet är att revidera befintliga kravspecifikationer för styr- och övervakningssystem som BELOK tidigare tagit fram.[12]

I BELOK ingår Sveriges största fastighetsägare med inriktning på kommersiella lokaler: AMF Fastigheter, Akademiska Hus, Castellum, Diligentia, Fabege, Fastighetskontoret Stockholms stad, Fortifikationsverket, Hufvudstaden, Jernhusen, Locum, Lokalförvaltningen (Göteborgs stad), Malmö Stad, Serviceförvaltningen, Midroc Property Development, Skolfastigheter i Stockholm AB, Specialfastigheter, Statens fastighetsverk, Swedavia, Vasakronan och Västfastigheter.[13]

Planeringen för hur fastighetsautomation ska utnyttjas bör komma in i flera skeden av byggprocessen; på idé- och programskedet, i projekteringsskedet, i upphandlingsskedet, byggskedet och slutligen i förvaltningsskedet. Det kan därför vara intressant att även följa ett byggföretag. Det finns flera myndigheter som ställer funktionskrav som måste beaktas (främst Boverkets Byggregler, BBR och Arbetsmiljöverkets föreskrifter AFS) och därutöver verksamhets- och byggnadsspecifika krav.

2.4 Säkerhetsaspekter inom fastighetsautomation

Övergången till existerande standarder inom nätverks- och webbteknik för överföring av signaler och information kan innebära säkerhetsproblem. Detta genom att fastighetssystem i högre grad än tidigare ges funktioner för fjärråtkomst och i viss utsträckning också är exponerade mot internet.

Fjärråtkomst har flera fördelar, det finns ingen geografisk begränsning för informationen och driftpersonalen kan komma åt, avläsa och analysera informationen såväl på plats som på distans. Fjärråtkomst innebär även att underhåll, uppgradering och felsökning av programvara som används kan skötas på distans, oavsett om det är med egen personal eller extern personal från t.ex. systemleverantören.

Frågan om säkerhet inom området fastighetsautomation har uppmärksammats på senare tid, bl.a. genom en artikelserie om sårbarheter i det digitala samhället i

[12] BELOK, Kravspecifikation för styr- och övervakningssystem, augusti 2006 (http://belok.se/download/kravspecifikationer/styr.pdf, hämtad 2015-02-25).
[13] Se http://belok.se, informationen hämtad 2015-02-25.

Dagens Nyheter.[14] I rapporteringen gavs flera exempel på fastigheter vars styrsystem fanns exponerade på internet, bl.a. polisstationer, järnvägsstationer och flygplatsbyggnader.[15]

MSB redovisade i januari 2015 exempel på inträffade IT-incidenter i Sverige och då bland annat ett fall där Västra Götalandsregionen drabbades av skadlig kod. Angreppet med skadlig kod ledde bland annat till störningar i fastighetsstyrning, inpasseringssystem och utrustning för medicinsk teknik. En infekterad server som hanterar larm från hissar, gas och fläktsystem vid Uddevalla sjukhus var tvungen att tas ur drift och uppgifterna fick hanteras manuellt av extrainkallad personal.[16]

Sveriges Kommuner och Landsting har, just med hänvisning till uppmärksamheten i media, publicerat en checklista för att undersöka om det finns några säkerhetsbrister i digitala styrsystem i kommunala eller landstingsdrivna fastigheter.[17]

I februari 2015 arrangerade Energi- och Miljötekniska föreningen (EMTF)[18] ett seminarium om framtida IT-säkerhet och fastighetsautomation. På programmet stod frågor om hur fastighetsägare ska kunna utnyttja enkla och robusta system för driften av fastigheter och samtidigt kunna upprätthålla företags- och samhällsviktiga säkerhetsfunktioner.[19] Vid ett senare arrangemang i EMTF:s regi återkom frågan om säkerhet på programmet.[20]

[14] Dagens Nyheter, ” IT-expert: Bristerna ett hot mot rikets säkerhet”, 2014-11-03 (http://www.dn.se/nyheter/sverige/it-expert-bristerna-ett-hot-mot-rikets-sakerhet/, hämtad 2015-02-24).

[15] Dagens Nyheter, ”Polisen efter larmet: ”Vi slet ut kabeln till internet”, 2014-11-03, (http://www.dn.se/nyheter/polisen-efter-larmet-vi-slet-ut-kabeln-till-internet/, hämtad 2015-02-24).

[16] MSB, *It- och informationssäkerhet i Sverige – erfarenheter och reflektioner från några större it-incidenter under 2012-2014*, MSB721, jan 2015.

[17] Sveriges Kommuner och Landsting, ”Digitala styrsystem och informationssäkerhet”, 2015-01-22 (http://skl.se/naringslivarbetedigitalisering/digitalisering/nyhetsarkivdigitalisering/arkivdigitaliseri ng/digitalastyrsystemochinformationssakerhet.4170.html, hämtad 2015-02-24. Enligt uppgift på SKL:s nyhetssida publicerades en första version av informationen 2014-11-03).

[18] EMTF är en personförening inom byggsektorn med inriktning på energieffektivisering och innemiljö med ca 7500 medlemmar (2015).

[19] EMTF, ”Göteborg: Seminarium om framtida IT-säkerhet och fastighetsautomation”, 2015-02-24 (http://www.emtf.se/event-registration/?ee=340, hämtad 2015-02-24).

[20] En programpunkt vid arrangemanget i april löd ”Så hindrar du DN:s reporter från att ringa i kyrkklockorna”. (http://www.emtf.se/event-registration/?ee=345, hämtad 2015-02-25).

3 Sammanställning av svaren från intervjuerna

Det här avsnittet innehåller en sammanställning av de intervjuer vi gjorde under maj och juni 2015 med företrädare inom området fastighetsautomation. Innehållet i avsnittet bygger på vad som sades under intervjuerna[21] och är strukturerat efter områden som togs upp av oss (via intervjuguiden) och sådant som lyftes fram av respondenterna. I och med att ambitionen är att redovisa vad som sades under intervjuerna överlappar områdena delvis varandra och delvis innehållet i kapitel 2, ”Bakgrund”.

Eftersom materialet baseras på intervjuer med personer från företag som har myndigheter och landsting med samhällsviktig verksamhet som främsta kunder är det inte säkert att underlaget går att generalisera till fastighetsautomation i stort.

3.1 Aktörer och roller

Respondenterna representerade några av de aktörer som finns på fastighetsmarknaden: ägare och förvaltare av fastigheter, mer renodlade förvaltare och verksamhetsutövare (både som hyresgäst och nyttjare av egna fastigheter).

Vi frågade de som äger och/eller förvaltar fastigheter om vilka aktörer som är involverade i driften. En fastighetsägare svarade att de sköter driften av de egna fastigheterna med egen personal men att det annars är vanligt att företag specialiserade på drift av fastigheter anlitas för detta. Vi fick ett exempel på att en hyresgäst upphandlat särskild hjälp med den tekniska driften för delar av en fastighet som hade extra höga krav på att fungera störningsfritt.

Det är vanligt att en aktör bygger ett system och att någon annan sköter driften, men det finns också stora aktörer som både bygger och ”driftar”. I relationen mellan hyresvärd och hyresgäst är förvaltning och drift i första hand hyresvärdens ansvar, gränsdragningar uttrycks i hyresavtal och kan variera beroende på typ av fastighet och verksamhet.

3.2 Begrepp och definitioner

Alla personer som intervjuades var bekanta med benämningarna SCADA-system och industriella informations- och styrsystem. Inom fastighetsbranschen talas

[21] På några ställen i texten redovisas uppgifter som inte kommer från intervjupersonerna, källorna till dessa uppgifter redovisas då i fotnoter.

det dock oftare ”fastighetsautomation” eller ”byggnadsautomation”[22]. Även benämningarna ”styrsystem” och ”styr- och övervakningssystem” togs upp. Det som i MSB vägledning kallas för ”process-IT”[23] kallades av våra respondenter för ”fastighets-IT” eller ”fastighetsnära IT”. En respondent definierar fastighetsnära IT som ”utrustning som råkar vara IT-utrustning som skulle följa med huset om man sålde det”.

Ett annat begrepp som dök upp är Facility Management (FM) som avser tillhandahållandet av tjänster till en fastighet. ”Hard FM”-tjänster inkluderar alla fastighetsanknutna tjänster, såsom energioptimering, hissar och säkerhetslösningar. Även gräsklippning, snöröjning och sophantering gavs som exempel på tjänster som hörde dit. ”Soft FM”-tjänster handlar om service såsom städning, mat och tvätt.

En av respondenterna önskar att begreppen var mer standardiserade inom sektorn så att det skulle vara lättare att förstå varandra och påpekade också att det är viktigt att man inom den egna organisationen har definitioner av olika begrepp.

3.3 Fastighetsautomation

En respondent beskriver fastighetsautomation som att det finns ett antal system som alla löser en funktion och som har möjlighet att dela information med varandra. Systemen designas med hänsyn till säkerhet, energieffektivitet och andra kriterier som driftssäkerhet och stabilitet.

3.3.1 Uppkoppling mot internet

Från början var styrsystemen inom fastighetsautomation isolerade från omvärlden. I och med den tekniska utvecklingen har dock fler och fler leverantörer börjat koppla upp sina system mot webben. Det ger fördelar eftersom det går att logga in från vilken plats som helst för att styra eller för att plocka ut information från systemen. Men det innebär också en säkerhetsrisk att vara uppkopplad mot internet. Från de intervjuade får vi bilden att många aktörer inom branschen inte har funderat över säkerhetsaspekterna, även om man talar mer om dem nu än för några år sedan.

3.3.2 Systemens livslängd

Systemen för fastighetsautomation är normalt väldigt långlivade och byts inte ut så ofta. Respondenterna anger att livslängden hos systemen är mellan 10 och 30 år, vilket är långt i jämförelse med många andra system och framför allt jämfört

[22] En fastighet kan bestå av flera byggnader – men det är i princip ingen skillnad på begreppen.
[23] MSB718, Vägledning till ökad säkerhet i industriella informations- och styrsystem.

med administrativa IT-system. Det finns exempel på byggnader som har system från 60-talet som fortfarande används. Fastighetsägarna har sällan incitament för att byta ut systemen inom den ekonomiska livslängden, men ibland måste systemen bytas ut eftersom det inte längre går att få tag på reservdelar.

Gammal utrustning saknar ofta möjlighet att kommunicera med omkringliggande system. Hissbranschen är ett exempel där man tidigare ofta ställt en dator i ett hissmaskinrum (motsvarande) varifrån man har kunnat plocka ut information vid behov. En respondent påpekar att när sådana system byts ut görs det ofta mot modernare system med exempelvis PLC:er som kan kommunicera med andra system.

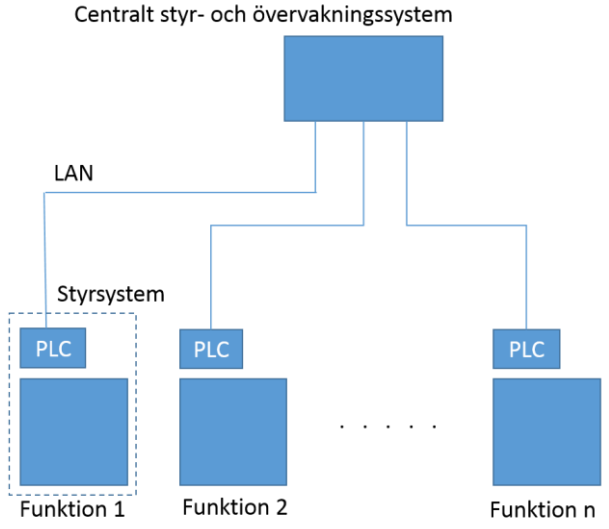
Servrar och datorer har kortare livslängd, typiskt fem år, och byts ut enligt plan. Nätverk däremot har en förväntad livslängd uppemot 50 år. En speciell utmaning som lyfts under intervjuerna är att då man bygger samman system, datorer och nätverk så måste man planera för att kunna ta hand om dem hela deras livstid. Tar man över befintliga system måste man alltid ta hänsyn till arvet och planera för att ta hand om och byta ut delar allt eftersom.

3.3.3 Korta kontra långa avtal

Fastighetsförvaltning som outsourcas till en extern part har ofta korta avtalstider. En aktör som levererar fastighetsförvaltning åt andra får ofta ettåriga eller treåriga avtal och då är det inte möjligt att investera i verktyg och utrustning som är specifikt anpassade till en fastighet utan man får använda generella ärendesystem och generella verktyg. Med längre avtal går det att anpassa verktygen för fastigheten eftersom avskrivningstiden för dem är betydligt längre än tre år. Det kan exempelvis vara IT-system för att mäta, följa upp och hantera logistik och ärenden som ger en effektivare fastighetsförvaltning.

3.4 Schematisk indelning av nivåer

I en fastighet finns det många olika funktioner som ska övervakas och styras. Exempel på sådana funktioner är värme, ventilation, kyla, belysning, pumpsystem, hissar, passagesystem och brandlarm. Hit hör också funktioner som avbrottsfri kraft (UPS) och rörpost. De personer vi talade med gav en gemensam bild av hur dessa system är strukturerade i olika nivåer och hur de kan styras och övervakas centralt (se figur 2), men de benämner de olika nivåer på olika sätt.

<table>
<tr><th>Locum</th><th>Specialfastigheter</th><th>Rapport från SBUF[24]</th><th>MSB:s vägledning[25]</th></tr>
<tr><td></td><td></td><td>Central lagring och analys</td><td rowspan="2">Centrala bemannade system</td></tr>
<tr><td rowspan="4"> 
</td><td>Visualiseringsnivå/ accessnivå</td><td>Informationsnivå</td></tr>
<tr><td>Kommunikationsnivå</td><td></td><td>Dataöverföring via nätverk</td></tr>
<tr><td>Digitala kontrollsystem</td><td>Automationsnivå</td><td rowspan="2">Lokala obemannade system</td></tr>
<tr><td>Komponentnivå</td><td>Fältnivå</td></tr>
</table>

Figur 2. Schematisk bild och översikt av olika beteckningar för att beskriva skilda systemnivåer inom styr- och övervakningssystem.

[24] Göran Gustafsson, *SBUF 12471 Slutrapport Projekt Styr och Övervakning*.
[25] MSB718, Vägledning till ökad säkerhet i industriella informations- och styrsystem.

3.4.1 Central styrning och övervakning

Det centrala styr- och övervakningssystemet kan, förutom att styra och övervaka underliggande system, även vidarebefordra information till användare om exempelvis larm, drift och energi. Gemensamt för systemen i de organisationer vi har studerat är att de vid behov kan styras lokalt men att de i regel styrs och övervakas centralt från ett styr- och övervakningssystem. Skulle den centrala nivån eller kommunikationen till den centrala nivån falla bort så fortsätter de lokala systemen ändå att fungera enligt de inställningar som är gjorda.

Bland de styr- och övervakningssystem som finns på marknaden och används inom fastighetssektorn nämndes iFIX från General Electric och Citect från Schneider Electric. Det senare används t.ex. inom Stockholms Läns Landsting (SLL). Andra landsting har valt andra system, vilket försvårar utbytet av erfarenheter.

3.4.2 Styrsystem

Varje funktion styrs av en egen dator (eller flera datorer) med objektspecifika program. Datorn kallas PLC (eng. Programmable Logic Controller) eller DUC (Datoriserad Undercentral). Ofta sitter datorn i ett apparatskåp med en operatörspanel från vilken man kan avläsa information och styra funktionen, även om detta vanligtvis sköts på central nivå.

Systemen för fastighetsstyrning räknas som en del av fastigheten och stannar kvar i fastigheten om denna överlåts. Det innebär att om man byter fastighetsförvaltare så bör systemen vara utformade så att den nya enkelt kunna ta över drift och handhavande av systemen.

Styrsystemen för de olika funktionerna kan befinna sig i olika delar av livscykeln och det finns normalt livscykelplaner för de olika funktionerna i och med att komponenter har olika livslängder. Vartefter tekniken utvecklas kan man skifta ut en teknik mot en annan, och detta kan då göras i en funktion oberoende av övriga funktioner.

Vanligtvis är det olika leverantörer för styrsystemen inom respektive funktion där var och en är specialiserad mot vissa områden. Det är då viktigt att beställaren kan beskriva för leverantören enligt vilken standard som systemen ska kommunicera med det övergripande styr- och övervakningssystemet. En av de större standarderna heter BACnet, och den används exempelvis på Nya Karolinska Solna men det finns även andra standarder som används inom fastighetsautomation (t.ex. KNX).

3.4.3 Kommunikation

Kommunikationen mellan styrsystemen för de olika funktionerna och det centrala styr- och övervakningssystemet sker via nätverk (LAN). Hos dem vi intervjuade användes trådbundna nät. Vi fick exempel på såväl helt fysiskt separerade nät (ett dedikerat fastighets-LAN) som logiskt separerade nät som delas med administrativa funktioner (”kontors-IT”). En respondent pekade på att skillnaden mellan fysisk och logisk separering inte alltid är uppenbar för dem som kopplar in sin utrustning på eller utnyttjar näten.

De flesta systemen är inte beroende av kommunikation med andra system, men det finns undantag. Exempelvis kan två ventilationssystem som vardera ansvarar för tilluft och frånluft behöva kommunicera med varandra. Detta kan då ske mellan berörda PLC:er via en dedikerad kommunikationsbuss som är åtskild från det övriga nätet.

Flera aktörer ser möjligheter att utnyttja det faktum att tekniken gör det möjligt att låta systemen kommunicera med varandra, antingen via separata bussystem eller via det centrala styr- och övervakningssystemet. En sådan möjlighet som utreds just nu är en s.k. grön våg på sjukhus. Det innebär att om en patient behöver föras snabbt till en operationssal, exempelvis på grund av hjärtstopp, så ska man kunna trycka på en ”panikknapp” som gör att belysningen dras upp, hissen går till rätt plan och stannar där, dörrar öppnas, ventilationen startas och så vidare.

Motsvarande lösningar finns redan idag i kommersiella fastigheter där belysning och ventilation exempelvis initieras av att man kör ner bilen i parkeringsgaraget och drar sitt kort där. Skillnaden är att kravet på säkerhet skiljer mellan kontors-fastigheter och den offentliga sjukhusmiljön, och diskussionen om fördelar och nackdelar med en grön våg på sjukhus pågår därför. För att hålla möjligheten öppen ställer en del förvaltare krav på att nya system, exempelvis hissar, ska kunna kommunicera med ett centralt styr- och övervakningssystem även om de traditionellt är fristående system.

3.5 Installation och uppdateringar av mjukvara

På Locum kallas de som levererar och installerar styrsystemen för styr-entrepenörer. Dessa upphandlas via LOU (lagen om offentlig upphandling). De som arbetar med styr- och övervakningssystemet (Citect) kallas för system-integratörer och de har upphandlats via ett ramavtal. Styrentreprenörerna har inte tillgång till det centrala styr- och övervakningssystemet och tillåts inte att installera någonting där. Systemintegratörerna tillåts på motsvarande sätt inte att koppla in sig på LAN:et och installera något i systemen.

För att systemen på de olika nivåerna ändå ska fungera tillsammans kräver Locum att styrentreprenörer och systemintegratörer samarbetar och samordnar sina system.

3.5.1 Testmiljö

Några av fastighetsförvaltarna har utvecklingsmiljöer i vilka man kan utveckla större projekt innan de lyfts in i den skarpa miljön. Där går det också att testa patchar och nya funktioner. Testmiljön efterliknar datamiljön och delvis den fysiska miljön, dvs. den inkluderar PLC:er men inte själva styrsystemen. Hissar finns exempelvis inte med, men genom att emulera signaler går det att indikera om hissen är uppe eller nere och om hissdörren är öppen eller stängd. Det är kostsamt att ha en testmiljö och alla fastighetsförvaltare anser sig inte ha råd med det.

Testmiljön kan också användas för att samordna test. Exempelvis ska automatiska truckar, ATG[26], kunna skicka en signal till hissystemet att öppna dörren och brandsystemet ska kunna skicka signaler till hissar och truckar. De funktionerna levereras av olika leverantörer och kan testas i testmiljön.

Enligt dem vi intervjuat är många leverantörer på fastighetssidan ovana vid testmiljöer. I vanliga fall är leverantören färdig när den genomfört installationen, men efter att den testats i testmiljön ska förändringen lyftas in i produktionsmiljön vilket blir ytterligare ett moment. Dessutom ska förändringen dokumenteras och det ska finnas en driftinstruktion och en handhavarinstruktion både för drift och installation. En av fastighetsförvaltarna har dessutom krav på leveranstestprogram och funktionstest som måste genomföras innan något får installeras i produktionsmiljön.

Ett problem som lyfts i samband med testmiljöer är att det krävs SCADA-licenser även för att köra applikationer i testmiljön och dessa är ofta dyra (”i miljonklassen”). För att få använda licenser även i testmiljön måste det finnas en överenskommelse om det i avtalet mellan leverantören och användaren. Det brukar lösa sig, säger en respondent, eftersom det ju egentligen är leverantören som använder testmiljön, inte vi.

3.5.2 Uppdateringar

Styr-, övervaknings- och fastighetssystemen hanteras inte som vanliga IT-system enligt en av respondenterna. De patchas inte varje vecka eftersom uppfattningen är att det inte finns några potentiella hot utifrån. Leverantören gör istället patchningar och förändringar när det finns funktionella brister i deras system.

[26] ATG = Automated Guided Vehicle

Olika förvaltare hanterar uppdateringar av systemen olika. En fastighetsägare låter leverantörerna komma till fastigheten och göra sina uppgraderingar där. De USB-minnen som leverantörerna har med sig scannas först för att se att de är rena och sedan får leverantören genomföra ändringarna under överinseende. Händer det något då så vet fastighetsförvaltaren vem som har gjort det. Andra förvaltare tillåter att deras leverantörer gör uppgraderingar via fjärråtkomst.

3.6 Fjärrdrift respektive drift på plats

Även om det blir allt vanligare att sköta funktioner från ett centralt styr- och övervakningssystem, och då särskilt byggnadens klimat i syfte att minimera energiförbrukningen, så tillämpas det inte överallt. En respondent hanterar sina fastigheter olika utifrån vilken typ av verksamhet som bedrivs i fastigheten. Det är inte alla fastigheter som är anslutna till ett centralt styr- och övervakningssystem, några fastigheter styrs manuellt och några har lokala isolerade system. Dessa är olika och går att hantera, men de är dyrare i drift. Det finns fastigheter till vilka kunden inte vill ha någon uppkoppling till yttervärlden överhuvudtaget. Då kan man ta en kopia av sin miljö och lägger lokalt.

I Nya Karolinska Solna har Coor valt bort fjärrdriften. Sjukhuset är så pass stort att det kan finnas folk på plats som sköter systemen. Allt är designat för att vara autonomt och redundant. SLL har också till del fjärrdrift men det går inte att styra alla sjukhus från samma plats. Det är dock möjligt att utvecklingen går mot en central driftcentral, men det finns inte idag.

3.7 Bygga nytt/överta befintliga fastigheter

Det är skillnad på att bygga nytt och att överta en befintlig anläggning. I befintliga fastigheter är man bunden till de investeringar som finns och till befintlig byggnadsstrukturer. Det kanske inte finns tillräckligt stora tekniska utrymmen, redundanta kabelvägar och rörkanalisation som är redundant för att kunna implementera de lösningar man vill. Man får ta den säkerhetsnivå som finns. Dessutom är man beroende av att fastighetsägaren eller förvaltaren lämnar över all dokumentation och information. En respondent säger att om de övertar en byggnad gör de ett ekonomiskt övervägande av vad det kostar att bygga om det befintliga jämfört med att investera i nya system. I sådana beräkningar tar de hänsyn till livslängden hos systemen och nätet.

Bygger man däremot nytt går det att påverka utformningen av byggnaden. Coor, som är driftleverantör till Nya Karolinska Solna, framhåller sin unika möjlighet att få vara med från start parallellt med att Skanska bygger. Där har man delat in huset i två delar och byggt separata kulvertar som inte möts någonstans. Det skulle ha varit svårt att åstadkomma i en befintlig miljö. Det genomsyrar även godsmottagning, truckar och rörpost som också går två vägar och har redundans.

Dessutom får Coor möjlighet att vara med och besiktiga och godkänna installationerna och hinner lära känna anläggningen innan den går i drift.

En annan respondent säger att de inte gör skillnad mellan nybyggnation och befintliga fastigheter. Det fysiska nätverket kan visserligen få en annan struktur då man bygger nytt, och det finns möjlighet att ställa krav på att system som tidigare inte har kommunicerat med omvärlden nu ska kunna göra det, men i övrigt är det samma riktlinjer som gäller.

Ytterligare en respondent framhåller att det finns stora möjligheter då man bygger nytt eftersom man kan designa systemet utifrån ett IT- och datakom-perspektiv, men att den möjligheten inte alltid utnyttjas inom fastighets-branschen. Istället hittar man ofta fiffiga lösningar för att koppla ihop system och skapa åtkomst datakommässigt och skaffar möjligheter för att ladda upp data för att kunna konfigurera systemen på distans. Det man borde göra, menar respon-denten, är att etablera patch-hanteringar och sektioneringar av nät så att man skyddar systemen från varandra. Utgår man från ett vitt papper så kan man börja bottom-up och ”bara öppna de hål man vill ha, inte tvärtom – att springa efter och stänga”. Man bör fråga sig vilka som ska få lov att komma åt systemen på distans och vad de kopplingarna för med sig.

3.8 Kulturskillnader mellan fastighetsnära och administrativ IT

Flera av dem vi har intervjuat vittnar om att det finns olika kulturer hos dem som arbetar med fastighetsnära IT respektive administrativ IT. De senare är vana att ha ett högt säkerhetstänkande och att använda anti-virus-program, uppdatera operativsystem, göra förändringshanteringar och säkerhetsgranska systemen. Anledningen till det, säger en av respondenterna, beror på finanssektorn och de hot som har funnits där. Fastighetsautomationssektorn har inte varit lika drabbad och dessutom har systemen tidigare ofta varit isolerade från omvärlden, så där finns inte samma säkerhetstänkande. Incidenterna det senaste året har dock bidragit till att öka medvetenheten.

Styrsystemen är heller inte designade för att uppdateras. Tillgängligheten kan bli lidande under en uppdatering och inom fastighetsautomationsvärlden har oftast driften satts före säkerheten enligt respondenterna. Att säkerheten kan påverka driften är inte alltid uppenbart. Det är inte heller säkert att systemen fungerar om de exempelvis uppdateras med det senaste virusskyddet eftersom de inte är konstruerade för sådana uppdateringar.

En av dem som har sin bakgrund i administrativ IT beskriver att det var en chock att första gången se hur stor klyftan mellan de båda sidorna är och hur olika ”tänket” är. Samma person säger att det går att förändra säkerhetstänkandet, men att det kräver stor envishet.

3.9 Säkerhetsaspekter

Vi ställde frågor om säkerhet, dels övergripande om säkerhetstänkande i anslutning till fastighetssystem, dels mer specifika om hur säkerhet implementeras i systemen. Flera av respondenterna tog upp att DN:s artikelserie fungerat som en väckarklocka för många i branschen och upplever att det blivit lättare att få gehör i frågor om IT-säkerhet såväl inom som utanför den egna organisationen.

I och med att medvetenheten höjts generellt om dessa frågor borde trycket på leverantörerna att arbeta mer aktivt med säkerhet ha ökat. Samtidigt nämndes att det nog kommer att inträffa ett antal försök till intrång och påverkan från individer som inspirerats av uppmärksamheten kring system för fastighetsautomation.

En incident som nämndes var dataintrånget mot ett bostadsbolag i Motala år 2010 där värmen stängdes av för bl.a. ett stort antal lägenheter och ett äldreboende. Samtidigt konstaterades att många incidenter nog inte blir kända utanför den organisation där de inträffar.

Kopplingen mellan säkerhet och relationen till sina leverantörer betonades av flera. Förutom formella åtgärder som säkerhetsklassning handlar det om att bygga upp ett förtroende och att leverantörerna bygger upp kunskap om kundernas verksamhet och rutiner. Att inom ett och samma område ha flera parallella leverantörer blir därmed krävande, samtidigt som dubbla leverantörer inom vissa områden minskar sårbarheten och därför kan vara önskvärt.

3.9.1 Skydd mot incidenter, tekniska och mänskliga fel

Behörighet och loggning

Våra respondenter redovisade flera exempel på ett systematiskt arbete med hantering av behörigheter. Genom inloggningen styrs vem som har tillgång till vilka delar av systemet och vilken information i systemet. Vi fick också exempel på att inloggningar hanteras separat för olika nivåer och delar i fastighetens samlade styr- och övervakningssystem.

En respondent beskrev det som en utmaning att utforma gemensamma behörighetsprinciper för den samlade IT-miljön med såväl administrativa system som styrsystem. Leverantörer kan ges tidsbegränsade behörigheter till vissa delar av systemen (begränsad åtkomst), med eller utan möjlighet till fjärråtkomst.

Grundläggande funktioner vid loggning av aktiviteter är t.ex. vem som är inne i systemet, vid vilken tidpunkt och från vilken plats inloggning sker. En respondent konstaterade att de som en del i säkerhetsarbetet skapat förutsättningar för

att logga sådan information, men att de valt att inte alltid ha dessa funktioner aktiverade.

I händelse av en incident finns det goda möjligheter att efteråt följa upp vad som skett genom loggfiler och annat. Användning av separata loggservrar nämndes. En respondent menade att loggverktygen även skulle kunna användas för att notera avvikelser under drift, men att det inte är givet vad som är viktigt att logga och vilken information man ska leta efter för att kunna upptäcka och förhindra någon typ av angrepp. Ovanliga kommandon? Aktivitet vid oväntade tidpunkter?

Att kunna spåra aktiveter inne i mjukvaran hos styrsystemen är beroende av hur själva systemen hanterar loggning. En respondent påpekade att loggning av aktiviteter i styrsystem inte är särskilt väl utvecklad jämfört med andra typer av mjukvara.

Redundans

Vi fick olika exempel på hur man utnyttjar redundans för att öka driftsäkerheten och stabiliteten i systemen. Det kan handla om att dubblera utrustning, ibland till och med ha tre olika installationer, för att ett bortfall i en del av systemet inte ska påverka driften.

Den tekniska utvecklingen mot en ökad virtualisering har minskat beroendet av specifik hårdvara under drift och det går enkelt att flytta över drift från en datorhall till en annan. Teknikutvecklingen har underlättat fastighetsautomationen på flera sätt, digitalisering av switchar och brandväggar minskar konsekvenserna av hårdvarufel, virtualisering och spegling av datalagring likaså. Det har blivit enklare att byta ut hårdvarukomponenter utan att driften påverkas.

Autonoma system

Flera respondenter betonade att systemen på de lägre nivåerna, nära de faktiska funktionerna (hissar, brandlarm etc.), byggs så att de fungerar även om kommunikationen med det överordnade styrsystemet skulle falla bort eller om det överordnade systemet slutar fungera. Om något händer går man över till autonom drift, dvs. styrningen sker lokalt ute i fastigheterna. Det lager som skickar data till styrsystemet kopplas bort. Ska några inställningar ändras får det göras via kontrollpaneler i apparatskåpen. Lokal styrning kräver därmed mer personal på plats. En respondent uttryckte viss oro för kunskapen om hur de olika funktionerna manövreras lokalt i ett läge när de i normala fall bara manövreras via styrsystemet.

Vi fick också exempel på att även i bestånd av fastigheter med möjligheter till central styrning så exkluderas vissa funktioner medvetet så att de inte går att styra på distans. Ett exempel som nämndes var belysning.

Åtkomlighet, sårbarhet för yttre faktorer

I takt med att medvetenheten ökat om sårbarheterna i systemen har insatser gjorts för att hantera hårdvara och åtkomst till denna på ett mer enhetligt sätt. En av respondenterna beskrev hur de arbetat med att inventera hårdvara i sina fastigheter och samlat den i bättre kontrollerade utrymmen, både för att öka driftsäkerheten (reservkraft, anpassad temperatur) och för att minska direkt åtkomst till styrsystemen.

I fråga om att förhindra eller försvåra obehörig åtkomst till systemen är den fysiska säkerheten den del som lättast går att påverka. Andra metoder är svårare att ha kontroll på, t.ex. via nätåtkomst eller USB-stickor.

3.9.2 Antagonistiska hot

Om en antagonist skulle skaffa sig åtkomst till en av de övre nivåerna och detta upptäcks så kan lägre nivåer i systemet isoleras och styras manuellt (se även avsnitt om autonoma system ovan).

Angrepp genom placering av skadlig kod från insidan i systemen togs upp som möjliga vägar för angrepp. Kontroll av leverantörer och underleverantörer som kan få tillträde till utrustningen togs upp som en skyddsåtgärd.

Efter installation och inför slutbesiktning av anläggningen ska styrentreprenören lämna över all programkod, programmeringsverktyg mm till beställaren. Alla ändringar därefter ska ingå i versionshanteringen. Eventuella ändringar som görs utan att dokumenteras (medvetet eller genom slarv) innebär risker vid den fortsatta förvaltningen av systemet. Ett konkret problem som togs upp i sammanhanget var att det inte går att låsa PLC:erna, det vill säga det finns inget sätt att skydda dem från att bli omprogrammerade. Detta har dock uppmärksammats av några utrustningsleverantörer i branschen.

Flera respondenter beskrev att förmågan hos styrsystem att motstå olika typer av angrepp och avvikelser från normal drift är sämre än andra typer av IT-system. De är inte konstruerade för att kopplas upp i stora nätverk och uppdateras inte med samma frekvens som andra system.

En respondent konstaterade att det rent fysiskt finns många punkter där det går att koppla upp sig mot nätverket och ansluta sig till deras system i och med att nätverken har en stor utbredning. I en offentlig byggnad där det rör sig många människor, inte bara anställda, kan det vara lättare att dölja sådana försök. En annan respondent beskrev hur konkreta åtgärder vidtagits genom skalskydd och receptioner, genom sektionering av fastigheterna med låsta dörrar, krav på synliga ID-kort och genom att förse besökare med passerkort till utvalda delar av fastigheten.

Uppkoppling mot internet

Exponering av styrsystem mot internet varierade mellan ingen alls och mycket begränsad hos de organisationer vi intervjuade. En respondent beskrev hur de aktivt inventerat alla relevanta IP-adresser i det egna nätet samt täppt igen glipor i systemet och kontrollerat vilken information som kan passera genom brandväggarna. En annan att molntjänster inte förekommer kopplade till fastighetssystemen, även om de utnyttjas i rent administrativa funktioner.

En respondent beskrev att det överordnade styrsystemet hämtar sina uppdateringar via nätet, men att alla ändringar av mjukvara i de respektive styrsystemen måste göras på plats, innanför brandväggarna. Skillnaden bedömde man vara acceptabel eftersom de olika funktionerna kan styras manuellt/lokalt i händelse av att det överordnade systemet går ner. Vissa leverantörer har klagat över att inte kunna genomföra ändringar och uppdatera på distans, men förståelsen för detta har ökat efter DN-artiklarna hösten 2014.

När det ändå finns behov av att tillåta en extern part att koppla upp sig mot något av delsystemen beskrev en respondent att de erbjöd behörighet och tunnlad trafik under en begränsad tid, t.ex. till en specifik IP-adress för att nå en enskild PLC. En annan respondent konstaterade att deras upphandlade systemintegratörer har vissa möjligheter att nå ”sina” installationer på distans.

Uppkoppling mot intranät, LAN

Graden av separation i de lokala näten mellan administrativ IT och fastighetsnära IT varierade hos de organisationer vi intervjuade, från att utgöra helt separata nät till att helt eller delvis samutnyttja samma nät. Även inom en organisation kunde detta variera beroende på vilken typ av verksamhet som bedrevs i en viss fastighet, i vissa fall är det helt enkelt uteslutet att göra några kopplingar mellan det administrativa nätet och fastighetsnätet. Det gavs också exempel på gränsfall, exempelvis informationsskärmar i entréer, som är en liten dator med anslutning till fastighetsnätet, men som inte skyddad på samma sätt som andra komponenter i systemet.

Vi fick några exempel på information som behöver överföras mellan de olika näten (ifall de är separerade.) Exempelvis data om energiförbrukning (värme, kyla, el) som samlas in i fastighetsnätet och därefter förs över till den administrativa sidan för att aggregeras och bearbetas, i det här fallet hos en extern aktör.

Trådlösa nätverk

Bland de intervjuade förekom det knappt några inslag av trådlös dataöverföring knuten till fastighetssystemen. Det enda exempel som nämndes handlade om kommunikationen mellan automatiska truckar och de berörda fastigheternas hissar.

Vad får säkerhet kosta? Riskanalyser

Flera resonerade om att behoven av säkerhet, och därmed den eftersträvade säkerhetsnivån, varierar beroende på vilken typ av verksamhet som bedrivs i en viss fastighet eller fastighetsbestånd. En kontors- eller bostadsfastighet måste kanske inte ha samma krav på avbrottsfri drift som ett sjukhus.

Vilka satsningar som görs på säkerhet måste också stå i relation till bedömda risker för allvarliga störningar eller angrepp. Analysen bör också omfatta en bedömning av vilka skador som kan uppstå vid en störning och vilka konsekvenser detta får. Dessutom finns det alltid hot som man inte har förberett sig för. Man måste ställa sig frågan: vad är värst, om personalsystemet blir hackat eller om operationssalen stängs av?

På motsvarande sätt behöver planerade förändringar av systemen för fastighetsautomation analyseras utifrån ett säkerhetsperspektiv. Bara för att det går att koppla ihop olika system är det kanske varken nödvändigt eller önskvärt. Om central styrning å andra sidan leder till väsentligt längre kostnader är man kanske beredd att acceptera lite större risker.

3.10 Kravställning/riktlinjer/strategier

3.10.1 Krav från kunder/hyresgäster på fastighetsägare/fastighetsförvaltare

Kunder (hyresgäster) ställer ofta krav på energieffektivitet, driftsäkerhet och kostnader. I hyresavtalen kan det ställas krav på funktioner men inte hur dessa ska lösas tekniskt. MSB, som är den enda representanten för hyresgäster i vår undersökning, har ännu inga riktlinjer för hur fastighetssystemen i deras byggnader ska vara utformade men kommer troligen att ta fram det till nästa förnyelse av hyreskontrakten.

En respondent kommenterade att det nog kommer att bli vanligare att ta upp frågor om system för fastighetsautomation i hyresavtal mot bakgrund av artikelserien i DN. Myndigheter ska lämna kopia på sina hyresavtal, inklusive gränsdragningslista, till ESV.[27] I den mån handlingarna inte omfattas av sekretess i någon form skulle dessa kunna vara en källa till att undersöka i hur stor utsträckning frågor om fastighetsautomation uppmärksammas i hyresavtal.

Medvetenheten om säkerhet hos dem som nyttjar lokalerna påverkar förstås vilka krav som ställs på styrsystemen, om alls några. Kunder som t.ex. kräver att

[27] Skyldigheten att redovisa hyresavtal till ESV regleras i förordningen (1993:528) om statliga myndigheters lokalförsörjning. En gränsdragningslista redovisar hur ansvaret för olika fastighetsanknutna frågor fördelas mellan hyresvärd och hyresgäst.

systemen ska vara helt fria från uppkoppling har rimligen gjort en värdering av olika risker knutna till system för fastighetsautomation. Som hyresgäst är det viktigt att kunna få tydlig information om säkerheten i berörda system från fastighetens förvaltare eller ägare, oavsett vilken nivå säkerheten ligger på.

På ett sjukhus är många försörjningsfaktorer viktiga, som vatten, el, gas, värme och kyla och det finns ofta hårda krav på dem. Vissa rum behöver exempelvis hålla ±0,5 °C och i andra rum kan kravet på det maximala antalet bakterier per volymenhet vara så lågt som fem bakterier/m^3. Ett annat krav på sjukhus är att om inte el och värme kan tillföras utifrån så ska det kunna tillverkas på plats.

3.10.2 Krav på leverantörer av styrsystem från byggherrar/fastighetsägare

Vi fick ta del av olika sätt för fastighetsförägare att ställa krav på dem som levererar och integrerar styrsystem i fastigheter. En fastighetsägare har utvecklat strategier för hur system, komponenter och kommunikation ska se ut på olika nivåer. Strategierna ska fungera för en värld inom LOU. Fastighetsautomations-världen är komplex eftersom det finns många intressenter. Det är en föränderlig bransch och är man för styrande och tydlig kan man hämma branschen och missa den utveckling som sker där. Är man för otydlig så riskerar man som beställare att inte veta vad man får, vilket i sin tur kan utgöra en säkerhetsrisk. Därför är det viktigt att hitta rätt avvägning och att forma styrande dokument för olika nivåer.

En respondent betonade att det som saknas är ett tydligt ramverk för hur IT-miljön ska se ut. För nätverksnivån finns det en branschstandard. För processer, applikationer och komponenter på styrsystemnivå finns det exempelvis standarder för hur programmeringsspråket ser ut men inte kring säkerhet, patchning och uppdatering. Där finns inget stöd idag som vi kan falla tillbaka på, säger en av respondenterna

Standarderna på kommunikationsnivån behöver inte vara styrande, men en av respondenterna betonade att de vill att nätverken ska se ut och dokumenteras på ett visst sätt. Framför allt vill de veta vad som är inkopplat. Längre ner på den nivå där de styrsystemen finns är det däremot noga med att specificera hur kopplingen till den högre centrala nivån ska se ut. En utmaning som lyftes var att om man som ensam aktör ställer specifika krav på t.ex. säkerhet så får man själv bära kostnaden, det vore önskvärt om fler aktörer gick samman och formulerade gemensamma krav.

En respondent beskrev att de tagit fram en pärm med riktlinjer för hur systemen för respektive funktion ska utformas. Riktlinjerna är bland annat ett sätt att säkerställa att gränssnitten mot operatörerna och systemdokumentationen (t.ex. driftkort) blir enhetliga. I pärmen finns det också fastställt hur alla komponenter (ned till enskild temperaturgivare) ska ges beteckningar för att få unika ”adresser” i det samlade systemet. För att underlätta projektering av styrsystemen

finns också en lathund med exempel på produkter som klarar de övergripande kraven i riktlinjerna.[28]

En kommentar gjordes om att den som kravställer och låter installera ett system för fastighetsautomation ofta är en annan aktör än den som använder systemet. Detta ställer i sin tur krav på god dokumentation och att utbytet av information i olika faser under fastighetens livslängd fungerar väl. En respondent kommenterade att verksamheten i sig, t.ex. i vilken grad de utgör viktiga samhällsfunktioner, påverkar vilka krav som ställs på systemen, driften av dem och även hur väl dokumenterade de bör vara.

Ytterligare en respondent pekade på att det vid nyinstallation av system, i samband med att en fastighet byggs eller totalrenoveras, är viktigt att ställa krav i termer av principiell utformning, dokumentation med mera och inte bara i termer av funktionalitet. Det företag som bygger eller renoverar fastigheten anlitar ofta olika typer av konsultföretag inom bygg och teknik för att omsätta kraven till tekniska lösningar. Deras kunskap och medvetenhet i frågor om säkerhet i system för fastighetsautomation påverkar vilka lösningar som väljs.

3.11 Lagkrav och föreskrifter

Vi frågade vilka lag- och myndighetskrav som kan påverka inköp, utformning och underhåll av styrsystemen för fastighetsdrift. Ingen av respondenterna uppgav några specifika krav som rör just fastighetsautomation men påpekade att de som alla andra måste följa de krav som gäller för byggnader. Detta exemplifierades med Boverkets krav på hållbarhet vid nybyggnation och med myndighetskrav på energieffektivitet. Det senare medför att man måste kunna mäta energiförbrukningen vilket indirekt ställer krav på viss mätutrustning.

Därutöver finns exempelvis lagkrav kring hur man hanterar elkraft. Om någon arbetar med elen så ska den inte kunna påverkas någon annanstans ifrån. Övervakningskameror, som finns i vissa byggnader, kräver också myndighetsgodkännanden. Eftersom dessa i regel hör till fastighetsägaren så är det dennes ansvar att söka tillstånden. Utöver dessa krav nämndes lagen om offentlig upphandling, LOU, som påverkar hur specifikt en beställarorganisation kan uttrycka sig när den upphandlar leverantörer.

[28] Locum AB redovisar övergripande krav på funktionalitet, förvaltning och projektgenomförande av styr- och övervakningssystem i Stockholms läns i *Locum AB, Riktlinje Styr och övervakning, R.18, 2013-09*-12, (http://www.locum.se/MirroredFiles/Kvalitetssystemet/S-Stod/Teknikstod/R%2018%20Riktlinjer%20Styr%20och%20%C3%B6vervakning%20med%20projekteringsanvisningar.pdf , hämtad 2015-02-04).

3.12 Utveckling inom området, trender

Vi frågade alla vi intervjuade vilka trender de såg inom området och fick många svar:

- Fastighetsautomationen blir mer och mer anpassat till det övriga informationssamhället med krav på tillgänglighet och snabbhet. Det finns redan idag massor av appar som används inom fastighetsautomationsbranschen.
- Det blir vanligare att övervaka och styra olika funktioner och installationer, t.ex. pumpar och fläktar, på distans. Även leverantörerna vill komma åt den utrustning de har sålt via nätet för att erbjuda uppgraderingstjänster, övervakningstjänster och dylikt.
- En annan trend är att man vill lägga upp information i molnet.
- Det blir billigare och billigare med elektronikprodukter vilket öppnar möjligheten till att installera nya system och nya funktioner.
- Det kommer in mer s.k. konsumentutrustning i fastighetsnäten. Det kan vara switchar som är enkla och billiga och har en protokollstack som inte är den vassaste och mest genomtestade. Det kanske är känt hur man hackar stacken vilket gör det lätt att få maskinen att trilla på ändan.
- Leverantörer av fastighetsautomationssystem är idag inte vana vid virtualisering, men det kommer att förändras i och med att fastighetsägarna ställer krav.
- Det pågår en utveckling av standardisering på kommunikationssidan. BACnet är ett standardprotokoll för kommunikation som blir alltmer vanligt, men det finns också andra kommunikationsprotokoll.
- Vi ser att allt fler funktioner blir allt mer digitaliserade även om de traditionellt sett inte har varit det, exempelvis hissar, sopsugar och rörpost.
- Det pågår en omstrukturering i branschen där stora leverantörerna håller på att köpa upp mindre vilket kommer leda till färre leverantörer.
- Samhället ställs om till en annan form av energiförsörjning och blir beroende av system som kan skifta mellan olika energikällor som sol och vind.

3.13 Utmaningar

Det finns ett flertal utmaningar inom branschen. Flera av respondenterna påpekar att dessa finns både internt och i dialogen med leverantörer. Många som arbetar inom fastighetsautomation ser inte styrsystemen som traditionella IT-system med sårbarheter och hot – och driftteknikerna tänker inte alltid på att omvärlden förändras. Då gäller det att utbilda, och att utbilda kontinuerligt, dels för att nöta in kunskapen och dels därför att omvärlden fortsätter att förändras och utbildningen måste förändras med den.

Utöver de interna satsningarna är det viktigt med en pågående dialog med kunderna, de som utnyttjar fastigheterna. Det är en utmaning att få dem att förstå säkerhetsaspekterna och ställa krav på fastighetsägarna som kan vidareförmedla dessa till sina leverantörer. Dessutom behövs en förståelse för att säkerhet kostar.

Intervjusvaren är samstämmiga i att leverantörerna måste bli bättre på att säkerhetsuppdatera sina system och att detta i sig är en utmaning. Många lever i tron att deras system fortfarande är isolerade. De måste tänka på säkerhet i sina enheter, produkter och system och dessutom generellt. Leverantörerna saknar ofta ett säkerhetstänk, vilket enligt flera respondenter beror på att det inte finns någon kravställning från kunderna, och att leverantörerna inte säljer något som ingen kund har ställt krav på.

En respondent lyfter virtualisering som en av de kommande utmaningarna. Virtualiseringen innebär ett kulturskifte och många leverantörer har hittills varit tveksamma att certifiera sina system så att de kan ingå i en virtuell miljö.

En annan utmaning är att livscykelhantera systemen som ingår i fastighetsnätet och att kunna byta komponenter under full drift i hundra år framåt. Systemen får inte stanna någon gång och det måste exempelvis gå att byta standarder på kommunikationssnitt. IT-utvecklingen gör att kommunikationssätt och infrastrukturer kanske kommer att bytas med 25-30 års mellanrum. Däremellan kommer komponenter i nätverken, exempelvis switchar, att behöva bytas ut. Även om nya komponenter ofta är bakåtkompatibla så kan det bli problem om man kommer med mer bandbreddsintensiva lösningar. Då blir det en utmaning att kunna byta komponenter och samtidigt inte ge avkall på tillgängligheten.

En mer generell utmaning är att balansera mellan att vara konservativ och nytänkande samtidigt som systemen ska fungera i offentlig miljö.

Dessutom påpekades det att hela IT-branschen och nätverksbranschen måste mogna för att kunna ta tag i de här frågeställningarna.

3.14 Samverkan

På frågan om det finns en aktiv diskussion i branschen om IT-säkerhet och om det tas några gemensamma initiativ för att möta utmaningarna så får vi till svar att även om frågorna diskuteras inom den egna organisationen så är det osäkert om det finns någon generell insikt i branschen. Inte heller kan någon peka på initiativ som har tagits för att samordna olika aktörer.

En respondent hoppas att företagen i branschen kommer att samverka mer och påpekar att det behövs samverkansforum för de här frågorna. Det finns idag flera samverkansråd i byggbranschen för inköp och miljö och kanske kommer det ett motsvarande inom det här området också.

Mellan landstingen finns en viss form av samverkan i form av PTS (Program-Teknisk Standard). Det är valfritt för landstingen att vara med. Bland dem som arbetar med styrsystem är det få som är med eftersom man valt olika plattformar för sina styr- och övervakningssystem. Däremot sker informationsutbyten mellan landstingen och mot leverantörer, entreprenörer och andra fastighetsägare.

3.15 Önskad draghjälp från myndigheter

När vi frågar efter behovet av lagar och riktlinjer från myndigheter ger respondenterna förslag på kvalitetsstämpling av reservaggregat med avseende på driftsäkerhet och på lagar kring olika systems tillförlitlighet inom energisektorn, sådant som syftar på traditionell fastighetsautomation och inte i första hand på en ökad säkerhet.

När det gäller säkerhetsbiten tror en av respondenterna att det är information som är viktigast i början, inte lagstiftning. Det viktiga är att nå ut med att digitala eller industriella kontrollsystem är en IT-produkt och ska hanteras som sådana säkerhetsmässigt.

Ytterligare ett förslag som dök upp under intervjuerna var att fastställa en standard för kravställning på samma sätt som det finns för t.ex. inbrottsskydd och larminstallationer. Om fler och fler efterfrågar någon form av certifiering så borde det bli intressant att erbjuda en sådan. Respondenterna tycker dock att det i första hand ska vara större leverantörer och andra säkerhetsaktörer som driver ett sådant arbete, inte myndigheter.

3.16 Vilka aktörer som MSB bör sprida kunskap till

Flera av de intervjuade kände igen MSB:s vägledning för ökad säkerhet i SCADA-system. En respondent önskade sig ett avsnitt som vänder sig direkt till landstingen eftersom de hanterar frågorna olika idag.

På frågan om vilka övriga aktörer som MSB bör sprida information till nämndes branschen inom processautomation, fastighetsbranschen och konsulter inom byggnadssektorn. Dessutom ansåg de att de själva skulle han nytta av utbildning och information.

En respondent påpekade att det redan idag finns ett stort antal forum där säkerhetsaspekter diskuteras eller som skulle kunna utnyttjas för sådana diskussioner. Dessa är för byggbranschen och fastighetsägare, framförallt offentliga fastighetsägare som är mer långsiktiga i sitt ägande.

4 Slutsatser

4.1 Slutsatser baserat på intervjuerna

4.1.1 Allmänt

En hypotes om hur fastighetsautomation skiljer sig från andra sektorer är den stora mängden olika funktioner, alla med egna styrsystem (inte sällan från olika leverantörer), som kopplas samman i ett samlat system för fastighetsstyrning. Exempel på vanliga funktioner är värme, kyla, ventilation, luftkonditionering, solskydd, belysning, hissar/rulltrappor, belysning, lås och brandlarm. Även funktioner såsom avbrottsfri kraft, rörpost och lokal distribution av gaser/vätskor kan ingå.

En annan hypotes är att den långa livslängden hos fastigheter och hos de tillhörande styrsystemen (10-30 år) och nätverken (uppemot 50 år) innebär att det samlade systemet för fastighetsstyrning ofta består av delsystem och komponenter som byggts på efterhand. Bäst möjligheter att konstruera ett sammanhållet system ges vid nybyggnation eller en genomgripande fastighetsrenovering.

4.1.2 Säkerhet och sårbarheter

Fastighetsautomation är traditionellt inriktat på funktion snarare än säkerhet. Systemen var från början isolerade från omvärlden, men i och med att uppkoppling mot internet blir allt vanligare så ökar säkerhetsriskerna och det är inte alla leverantörer medvetna om. Det är dessutom svårare att lägga till säkerheten i efterhand än att bygga in den från början.

Förmågan hos styrsystem generellt att motstå olika typer av angrepp och avvikelser från normal drift är sämre än hos andra typer av IT-system. Det finns ”hål” i säkerheten som är kända av dem som arbetar med fastighetsautomation, exempelvis möjligheten att plantera in farlig kod med ett USB-minne (insiders) eller att koppla upp sig mot ett nätverk i en offentlig byggnad och ansluta sig till systemen där. Det finns också problem kring att det inte går att låsa PLC:er (programmeringsmässigt) i dagsläget. Dessutom ökar användningen av s.k. konsumentutrustning i fastighetsnäten, utrustning som är enklare och billigare och som inte är testad ordentligt och därför kan vara lätta att hacka.

Det är möjligt att det finns risker med att tillåta uppdateringar av det centrala styr- och övervakningssystemet på distans/via internet. Det skulle kunna vara en

kanal in till styrsystemen för enskilda funktioner. I händelse av en sådan incident finns det ofta möjlighet att följa förloppet genom loggfiler och annat, däremot är loggning av aktiviteter ”inuti” i styrsystemen svagt utvecklat.

4.1.3 Aktörer och roller

Byggherren, som kravställer systemen, är oftast inte samma aktör som förvaltar dem. Fastighetsförvaltare kan dessutom bytas ut med jämna mellanrum. Detta torde ställa högre krav på dokumentation och enhetlighet i styrsystemen jämfört med andra sektorer. (Vi saknar dock underlag som visar hur rörligheten bland fastighetsförvaltare ser ut.)

Konsulter inom bygg och teknik är en viktig grupp att bearbeta/höja medvetenheten hos om säkerhet inom fastighetsautomation. De omsätter byggherrens krav till tekniska lösningar, vid nybyggen och renoveringar, och påverkar därför i hög grad vilken nivå av och hur säkerhet realiseras i systemen. Det är också viktigt att byggherrar och förvaltare lär sig att ställa krav på konsulter och leverantörer och att verka för en samsyn i vilka krav som bör ställas på säkerhet i system för fastighetsautomation.

4.1.4 Skillnader i synsätt och andra utmaningar

Begrepp och beteckningar skiljer sig mellan olika aktörer. Mer enhetliga begrepp inom branschen skulle underlätta såväl dialog med leverantörer som erfarenhetsutbyte med andra aktörer.

Det finns olika syn på behovet av att separera nätverk för fastighetstjänster respektive ”vanlig” IT och vi har sett exempel på såväl logisk som fysisk separering. För dem som utnyttjar, och ibland även för dem som kopplar in utrustning mot nätverken, är denna skillnad inte alltid uppenbar. Det finns ett behov av att överbrygga kulturskillnader och skilda arbetssätt i fråga om säkerhet mellan traditionell IT och styrsystem.

Utvecklingen mot en större grad av virtualisering nämns som en utmaning. Virtualiseringen innebär ett minskat beroende av specifik hårdvara under drift och att det enkelt går att flytta över drift från en datahall till en annan. Men det innebär också ett kulturskifte och många leverantörer har hittills varit tveksamma att certifiera sina system så att de kan ingå i en virtuell miljö.

4.2 Förslag på fortsatta studier

Den studie som har genomförts och presenteras i rapporten är en förstudie som har syftat till att ge en övergripande bild av hur fastighetsautomation ser ut i Sverige idag. Förstudien kan användas till att sätta ramarna för en fördjupad studie inom samma område. En sådan studie skulle kunna ge en bredare bild av fastighetsautomation som täcker in fler typer av fastighetsägare och förvaltare, som fokuserar på en större bredd av samhällsviktiga verksamheter och där fler aktörer intervjuas, exempelvis leverantörer som saknas i den genomförda studien. En fördjupad studie skulle också kunna utformas för att ge en djupare förståelse av de tekniska nivåerna, exempelvis kring hur olika kommunikationslösningar ser ut. En sådan studie skulle ge ett underlag för att göra en jämförande studie om vad som skiljer fastighetsautomation från andra verksamheter som utnyttjar industriella informations- och styrsystem och även ge ett underlag för att identifiera och diskutera eventuella sårbarheter och åtgärder för att skydda sig mot dessa.

Under studiens gång identifierade vi även ett antal frågor som skulle vara intressanta att besvara. En sådan fråga är vad lagar och föreskrifter säger om ansvarsförhållanden mellan olika aktörer inom fastighetsautomation och i vilken utsträckning ansvarsförhållandena alls är reglerade. En annan fråga är att undersöka i vilken utsträckning frågor om fastighetsautomation uppmärksammas i hyresavtal. Det skulle också vara intressant att ta fram underlag som visar hur rörligheten bland fastighetsförvaltare ser ut.

Utöver ovanstående förslag, som bygger på att fördjupa den kunskap som redan tagits fram, så skulle en ny studie kunna fokusera på andra aspekter. Ett exempel på en sådan aspekt är vilka konsekvenser som skulle uppstå i samhället om fastighetsautomationen inom en samhällsviktig verksamhet får reducerad funktion. En annan möjlighet är att sätta fokus på de riskanalyser som görs idag då man installerar och förvaltar fastighetsautomationssystem. Det är av intresse att se hur analyserna utformas, vilka system som anses vara kritiska och vad som anses vara skyddsvärt. En ytterligare aspekt är att undersöka vilka utmaningar som finns i kommuner, och andra myndigheter som har ansvar för samhällsviktig verksamhet, i sin roll som kravställare av system som används vid fastighetsautomation.

Bilaga 1. Respondenter

Nedan listas de personer som intervjuades inom ramen för studien:

Specialfastigheter

Specialfastigheter äger och förvaltar fastigheter med höga krav på säkerhet. Bland hyresgästerna finns Kriminalvården, Rikspolisstyrelsen, Statens institutionsstyrelse, Försvarsmakten, Försvarets materielverk och FOI.

- Peter Kalin, ansvarig för utvecklingen av fastighetsautomation inom Specialfastigheter.
- Masse Antonsson, IT-chef och informationssäkerhetsansvarig.

MSB

MSB har lokaler i Revinge, Sandö (båda skolor), Kristinehamn (logistik/förråd), Stockholm och Karlstad (primärt kontor).

- Magnus Kjellman, ansvarig handläggare för lokalfrågor inom MSB.

Coor Service Management

Coor Service Management är leverantör av bland annat tjänster inom fastighetsautomation och har fått i uppdrag att utveckla och leverera fastighetstjänster till Nya Karolinska Solna fram till och med 2040.

- Roland Davidsson, IT-arkitekt, jobbar med IT, styrfrågor och säkerhet.

Locum AB

Locum AB ägs av Stockholms läns landsting (SLL) och har ett fastighetsbestånd på cirka två miljoner kvadratmeter i Stockholms län. Bland hyresgästerna dominerar sjukvården.

- Anders Gidrup, säkerhetschef.
- Mikael Rubensson, SCADA- och Citect-specialist. Ansvarig för installationer, riktlinjer och projekteringsanvisningar.
- Tomas Pettersson, ansvarig för driftmiljöer och systemdriftspecialist på fastighetsrelaterad IT.
- Johan Mårtensson, IT-chef.

Bilaga 2. Intervjuguide

Alla frågor var inte relevanta för alla respondenter utan ett urval gjordes från nedanstående bruttolista med avseende på respondentens roll och organisationstillhörighet.

Bakgrund

- Beskriv din roll/befattning i organisationen och vilka uppgifter som hör till rollen.
- Vilka fastigheter har du ansvar för?
    - Vem äger fastigheterna?
- Har du tidigare erfarenheter av fastighetsautomation?
- Hur ser ert fastighetsbestånd ut?
    - Omfattning?
    - Användning?
    - Geografisk spridning?
    - Ålder?
- Hur är förvaltning och drift av era fastigheter organiserad?
    - Vilka är de viktigaste aktörerna i detta?
    - Vem ansvarar för att specificera, kravställa och installera nya system?

System för styrning och övervakning/fastighetsautomation

- Vilka funktioner (tjänster) finns ”inbyggda” i era fastigheter?
    - Vilka av dem styrs lokalt och vilka styrs från en annan plats (centralt)?
- För varje funktion:
    - Vilka system i era fastigheter stödjer funktionerna?
    - I vilken utsträckning är de integrerade med system som stödjer andra funktioner?

    Om tillämpligt:
    - Var finns hårdvaran i systemen placerad?
    - Finns det någon redundans?
    - Är det några aktörer utöver er som är involverade i skötseln?
- I vilken utsträckning sker övervakning och styrning centralt för flera fastigheter?
    - Vilka funktioner övervakas och styrs centralt?

  - Vilka funktioner/system regleras automatiskt?
  - Om styrningen/regleringen inte fungerar, går det då att ”ta över den” manuellt?
  - ”Vilka system överrider varandra?”
- Är några av systemen kritiska för att fastighetsautomationen ska fungera?
  - Finns det några gränssättande faktorer?
- Har ni tagit fram några (skriftliga) riktlinjer för styr- och övervakningssystem i ert fastighetsbestånd?

Nya kontra befintliga fastigheter, med mera
- Är ni även med i byggprocessen av nya fastigheter?
- Vad är skillnaden mellan att installera systemen vid nybyggnation mot att bygga in dem i befintliga fastigheter?
- Hur mycket anpassar ni ”gamla system” för fastighetsautomation till ny teknik?
- Finns det några lag-, myndighets- eller verksamhetsspecifika krav ni måste följa?

Säkerhet
- Hur tänker ni kring säkerhet i systemen för fastighetsautomation?
- Hur ser kopplingen ut mellan systemen för fastighetsautomation och ”kontors-IT”/”vanliga IT:t”?
- Finns det ett specifikt nät för fastighetsautomation?
  - Används samma nät även för annan kommunikation och andra system?
  - Är något av systemen för fastighetsautomation kopplade till internet?
  - Har ni molntjänster?
- Utnyttjas trådlös kommunikation i styrningen av fastigheterna?
  - I så fall: inom vilka funktioner och med vilken teknik?
- Finns det några möjligheter att koppla upp sig mot systemet via fjärråtkomst?
  - Vilka interna och externa aktörer har i så fall denna möjlighet?
  - Finns det några särskilda rutiner att följa för den som behöver koppla upp sig?
- Hur fungerar mjukvaruuppdateringar?
- Roller inför och vid installation av system samt drift av system:
  - Vem gör vad?

- Hur ser ansvarsförhållandena ut?
- (Beroendekedjor?)

Övrigt

- Hur ser utvecklingen inom området fastighetsautomation ut?
  - Vilka trender och tendenser ser ni?
  - Vilka utmaningar leder denna utveckling till?
  - Vilken del av denna utveckling tror ni kommer att påverka er egen verksamhet mest?
- Begreppet fastighetsautomation
  - Använder ni det?
  - Vilka begrepp används inom er verksamhet?

Visa eventuellt bilderna som illustrerar innehållet i MSB:s rapport "Vägledning till ökad säkerhet i industriella informations- och styrsystem".

  - Känner ni igen er?
  - Går det att översätta terminologin så att ni känner er mer hemma med den?
- Vilka risker ser ni att det finns inom fastighetsautomation?
  - Hur kan man hantera dessa?
  - Vilka konsekvenser kan det bli om någon av automatiken fallerar eller manipuleras?

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