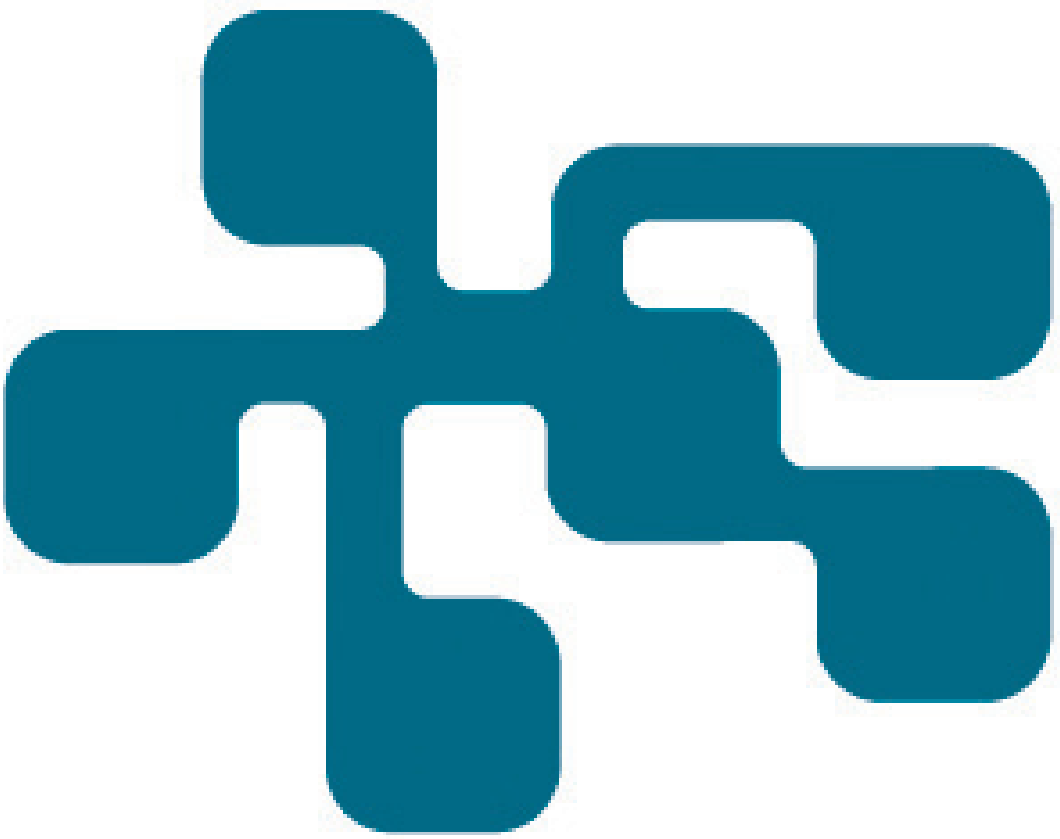
NCS3 - Funktioner och IT inom kommunal fastighetsautomation

Tre fallstudier

HANNES HOLM, KARIN MOSSBERG SONNEK



FOI-R--4308--SE
MSB 2015-2528
ISSN 1650-1942 Augusti 2016

Hannes Holm, Karin Mossberg Sonnek

NCS3 - Funktioner och IT inom kommunal fastighetsautomation

Tre fallstudier

FOI-R--4308--SE

MSB 2015-2528

Titel	Funktioner och IT inom kommunal fastighetsautomation
Title	Functions and IT within municipal building automation
Rapportnr/Report no	FOI-R--4308--SE
Månad/Month	Augusti
Utgivningsår/Year	2016
Antal sidor/Pages	49
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	5. Krisberedskap och samhällssäkerhet
FoT-område	
Projektnr/Project no	E13518
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Fastighetsautomation inbegriper styrning och övervakning av fastighetsnära funktioner. Idag finns olika system för fastighetsautomation implementerade i så gott som alla större byggnader och Sveriges kommuner spelar en central roll för hantering av fastigheter. Kommuner äger fastigheter och ansvarar i hög grad för upphandling, installation och drift av fastighetssystemen i dessa. Det finns dock en mycket begränsad allmän insikt i hur fastighetsautomationen fungerar i den kommunala kontexten.

Denna studie innefattar fallstudier i tre kommuner av olika storlek som har valt skilda lösningar för hur de styr och övervakar sina fastighetssystem. I rapporten redovisas hur de olika kommunerna har valt att organisera sig, vilken IT-utrustning de nyttjar och vilken fysisk och logisk nätverksarkitektur de använder. Det finns både likheter och skillnader mellan kommunerna, men det är svårt att utifrån dessa dra några generella slutsatser om hur det ser ut i Sveriges kommuner.

Resultatet inkluderar ett utkast till en referensmodell som beskriver den fysiska och logiska topologin för hur kommunala fastighetsautomationssystem är konstruerade. Referensmodellen är tänkt att användas som ett verktyg i dialogen mellan MSB och kommuner rörande diskussioner av IT-säkerhet i de industriella styr- och övervakningssystem som ingår i fastighetsautomationen.

Nyckelord: Fastighetsautomation, NCS3, IT-säkerhet, referensmodell, topologi, nätverksarkitektur

Summary

Real estate typically contain various systems that enable monitoring and controlling different building functions within them (e.g., heating). Sweden's municipalities play a central role in the management of real estates. Municipalities owns buildings and are to a large extent responsible for the procurement, installation and operation of the building automation systems. However, the understanding of how building automation is implemented in the municipal context is limited.

This report describes case studies of three municipalities of different sizes that have chosen different approaches for how to monitor and control their building automation systems. It is described how the municipalities have chosen to organize themselves and what IT equipment, as well as physical and logical network architecture, they use. There are both similarities and differences between the municipalities. However, the limited sample size makes it difficult to make any general conclusions regarding building automation systems used within Swedish municipalities.

The results include a draft of a reference model that describes the physical and logical topology of how municipal building automation systems are designed. The reference model is intended to be used as a tool in the dialogue between MSB and municipalities regarding discussions of IT security in industrial monitoring and control systems that are part of building automation systems.

Keywords: Building automation, NCS3, IT security, reference model, topology, network architecture

Innehållsförteckning

Ordlista

AD	Active Directory
COTS	Commercial Off The Shelf
DDOS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSec	Domain Name System Security Extensions
DUC	Datoriserad UnderCentral
FTP	File Transfer Protocol
HMI	Human Machine Interface
IP	Internet Protocol
LON	Local Operating Network
MPLS	Multiprotocol Label Switching
NCS3	Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet
OPC	Open Platform Communications
OSPF	Open Shortest Path First
PLC	Programmable Logic Controllers
PM3	På Maintenance Management Model
PXE	Preboot Execution Environment
RDP	Remote Desktop Protocol
SCADA	Supervisory Control And Data Acquisition
SRÖ	Styrning, Reglering och Övervakning
SQL	Structured Query Language
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

1 Inledning

1.1 Bakgrund

1.1.1 Studier inom NCS3

NCS3[1] är ett kompetenscentrum som drivs i samarbete mellan Totalförsvarets forskningsinstitut (FOI) och Myndigheten för samhällsskydd och beredskap (MSB). Syftet med NCS3 är att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsaspekter inom industriella informations- och styrsystem. Inom ramen för centrumet bedrivs utbildning, övningar, forskning och studieverksamhet.

En av de studier som genomfördes under 2015 var en förstudie inom fastighetsautomation [1]. Studien resulterade i en översiktlig beskrivning av de system som förekommer för styrning av fastigheter, vilka tjänster som är vanligast förekommande och vilka aktörer som finns inom området. Studien belyste också hur olika berörda system samverkar, i vilken mån de är uppkopplade mot internet samt gav en överblick över hur olika begrepp används inom sektorn.

Under 2016 genomförs en studie vars mål är att skapa en teoretisk referensmiljö (en generisk beskrivning) av industriella informations- och styrsystem för utpekade tillämpningar [2]. Syftet med miljön är att den ska kunna användas som utgångspunkt för att konkretisera viktiga säkerhetsfrågor utan att äventyra informationssäkerhet och förtroende vilket kan vara fallet då man diskuterar specifika system. Miljön ska användas som referensram vid kunskapsspridning och informationsdelning kring hot, sårbarheter och säkerhetsaspekter.

1.1.2 Behov av stöd i kommunerna

Sveriges kommuner äger fastigheter, såväl hyreslägenheter som tekniska anläggningar (exempelvis VA- och fjärrvärmeverk), och har ansvar för de IT-system som styr och övervakar funktioner i fastigheterna. Fastighetsautomationen är uppbyggd olika i olika kommuner och kunskapen kring säkerheten i systemen varierar. MSB har uppfattat att många kommuner har ett behov av stöd i frågor kring hur man upphandlar system och hur man skyddar dem mot oönskade intrång.

[1] Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet, www.foi.se/ncs3 (hämtad 2016-05-25).

1.2 Syfte och mål

Syftet med studien som redovisas i den här rapporten har varit att bygga vidare på tidigare studier för att ta fram ett diskussionsunderlag inom området fastighetsautomation och IT-säkerhet som kan användas i kommunikationen mellan MSB och kommunerna.

Målet har varit att skapa en generell referensmodell för området fastighets-automation på kommunal nivå som kan fungera som en gemensam referensram vid kunskapsspridning och informationsdelning kring t.ex. hot, sårbarheter och säkerhetsaspekter. I första hand är referensmodellen tänkt att beskriva den tekniska arkitekturen (t.ex. nätverk, datorer och protokoll) och i andra hand den organisatoriska uppbyggnaden i kommunerna. Målgruppen för beskrivningarna är kommunala aktörer på förvaltningsnivå.

1.3 Avgränsningar

Studien har haft en begränsad omfattning och bygger på intervjuer i tre kommuner. Resultatet kan därför ses som en första hypotes till en teoretisk referensmodell som kan förfinas efter hand. Målsättningen har varit att aktörerna ska känna igen sig i modellen men att den inte behöver vara generisk på så sätt att den gäller för alla kommunala verksamheter i alla kommuner.

Referensmodellen ska på sikt kunna implementeras i FOI:s träningsanläggning CRATE[2], men detta har inte varit studiens primära syfte.

De vi intervjuat har haft ansvar för drift och/eller IT-stöd. De har primärt sett fastighetsautomationssystem som ”system” eller komponenter som ska driftas eller kopplas upp i ett nätverk, funktionen som systemen ska bidra med (t.ex. värme eller ventilation) har inte varit det primära för deras del. Därför har funktionsperspektivet inte blivit så tydligt i studien.

Vi har riktat in oss på att beskriva modellen, inte på att diskutera problem, brister och svagheter.

[2] CRATE = Cyber Range And Training Environment, www.foi.se/crate (hämtad 2016-08-22).

2 Metod

För att undersöka hur fastighetsautomation är uppbyggd inom kommunal verksamhet genomförde vi fallstudier i tre kommuner som sinsemellan har olika lösningar för styrning och övervakning av sina fastighetssystem. Kommunerna valdes ut bland dem som MSB har haft kontakt med i samband med kurser och konferenser och där vi hittade respondenter som var villiga att ställa upp på intervjuer.

Verksamheterna i kommunerna representerar just tre fall och ger inte en representativ bild av hur det ser ut i Sveriges 290 kommuner. Detta har heller inte varit studiens syfte. Den sammantagna bilden av hur fastighetsautomationen fungerar i de tre studerade kommunerna fyller däremot syftet att användas som en utgångspunkt för diskussioner kring säkerhet i industriella informations- och styrsystem i den kommunala kontexten.

Inom varje kommun gjorde vi intervjuer med en eller två personer. Valet av intervju som metod motiverades av att vi ville få detaljerad information om varje kommun, något som är svårt att få genom exempelvis enkäter. Frågebatteriet som användes under intervjuerna (se bilaga 1) bygger på teoretiska ramverk såsom [3]–[16], och har förädlats utifrån praktiska erfarenheter från olika studier inom NCS3, såsom [17], [18], och framför allt de studier som projektet baseras på (se avsnitt 1.1).

Intervjuerna var semi-strukturerade i den bemärkelsen att frågebatteriet låg som grund för intervjuerna utan att för den skull följas slaviskt. Frågebatteriet begränsades eller förlängdes under intervjuerna beroende på respondenternas kunskap och intressen samt vilka tekniska och administrativa komponenter de fokuserade på.[3] Frågebatteriet kan delvis ses som en processmodell som beskrev ett antal intressanta frågeområden och som länkade översiktliga frågor till mer detaljerade frågor.

Baserat på vår erfarenhet blir många respondenter mindre öppna när de delger känslig information (såsom säkerhetsrelevanta egenskaper) när samtalet spelas in. Av den anledningen nyttjades inte inspelningsutrustning. För att säkerställa datakvaliteten tilläts istället alla respondenter att kommentera de renskrivna intervjuanteckningarna samt utkastet till denna rapport. I varje fallstudie

[3] T.ex. kan en teknisk miljö innefatta en heterogen flora av system, eller så kan miljön vara tämligen homogen, såsom en nätverksinstallation av Windows 7 som delas av alla datoranvändare. I det förstnämnda exemplet är det av vikt att förstå hur den heterogena miljön uppstått för att på så sätt skapa logik ur ”bruset”; i det andra scenariot är det av vikt att förstå hur homogeniteten realiseras, och svara på frågor såsom ”*Hur får en dator kontakt med servern som skickar operativsystem över nätverket*?” och ”*Krävs det något lösenord för att installera operativsystemet?*”.

förädlades intervjudokumentationen i flera steg genom maildiskussioner mellan forskare och respondenter.

Totalt intervjuades fem respondenter inom tre kommuner. Med tanke på att det kan vara känsligt att ge en helhetsbild över hur den fysiska IT-arkitekturen är uppbyggd i en kommun har vi valt att inte redovisa vilka kommuner som ingått i studien utan presenterar dem som kommun A, B och C. En översikt av dessa finns i Tabell 1.

Tabell 1. Respondenter

Kommun	Kategori[4]	Respondent	Roll i kommunen
A	3. Större städer	R1	Chef för den enhet som ansvarar för test och integration av kommunens fysiska IT-arkitektur.
		R2	Arbetar på drift- och service-förvaltningen, ansvarig för alla tekniska installationer bland annat i skolor och boenden.
B	1. Storstäder	R3	Arbetar med IT-utrustningen som möjliggör nätverksaccess inom kommunens stadsnät.
		R4	Arbetar i en förvaltning som ansvarar för fastighetsautomation.
C	3. Större städer	R5	Arbetar på IT-avdelningen och till del med säkerhetsfrågor i ett nationellt informationsnätverk.

Baserat på teorin kring IT-arkitekturer för SCADA-system[5] (se kapitel 4) och resultaten från intervjuerna (se bilaga 2) presenteras i kapitel 5 en hypotetisk referensmodell för området fastighetsautomation inom kommunal verksamhet som ska kunna fungera som en gemensam referensram vid kunskapsspridning och informationsdelning kring t.ex. hot, sårbarheter och säkerhetsaspekter.

[4] Enligt SKL:s kommungruppsindelning som har en tiogradig skala där 1 står för storstäder och 10 för kommuner i glesbefolkad region, http://skl.se/tjanster/kommunerlandsting/faktakommunerochlandsting/kommungruppsindelning.
[5] SCADA = Supervisory Control And Data Acquisition.

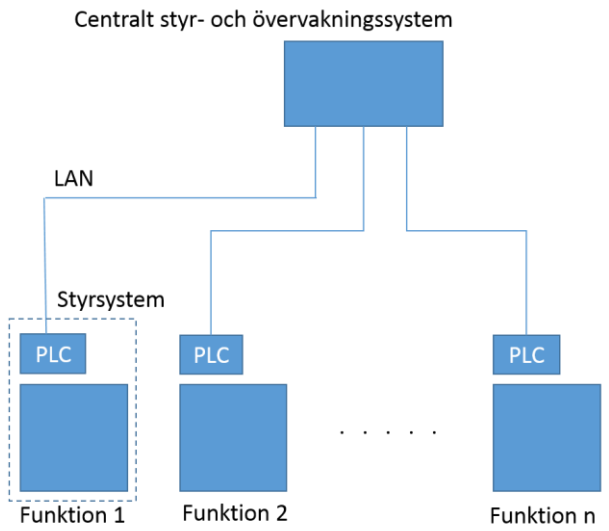
3 Fastighetsautomation

Fastighetsautomation innefattar styrning och övervakning av fastighetsnära funktioner som värme, ventilation, belysning, hissar och passersystem. Fastighetsautomationen har utvecklats snabbt de senaste åren i strävan efter att effektivisera energianvändningen. Traditionellt har informations- och styrsystem inom en fastighet varit isolerade från omvärlden, men i och med den tekniska utvecklingen kopplas de i allt större utsträckning upp mot internet. Detta gör det möjligt att styra och övervaka systemen från ett centralt styr- och övervakningssystem och även att uppdatera systemen på distans. Sammantaget medför det ekonomiska vinster men också ökade säkerhetsrisker.

Under 2015 initierade MSB en studie som syftade till att ge en övergripande bild av hur fastighetsautomation ser ut idag i byggnader som rymmer samhällsviktig verksamhet [1]. Studien innefattade litteraturstudier och intervjuer med yrkesutövare med ansvar för utveckling, installation eller drift av fastighetsautomationssystem, med ansvar inom IT och informationssäkerhet och som nyttjare av systemen (hyresgäst). Respondenterna valdes ut så att de representerade fastighetsbestånd som finns spridda över Sverige så att det skulle finnas incitament för att centralisera styrningen och övervakningen. Intervjuerna gav en bild av vilka begrepp som används inom området, 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 eventuella sårbarheter.

Sammantaget visade studien att fastighetsautomation är en komplex sektor som rymmer många aktörer som behöver interagera med varandra. Medvetenheten inom branschen om säkerhetsriskerna varierar.

Systemen inom fastighetsstyrning kan struktureras på olika nivåer. Figur 1 visar hur detta kan se ut samt olika sätt på vilka nivåerna kan benämnas. Delsystemen och komponenterna har ofta olika livslängd, olika leverantörer och olika tekniska lösningar vilket är en utmaning för dem som ska hantera systemen.

<table>
<tr><th>Locum</th><th>Specialfastigheter</th><th>Rapport från SBUF[6]</th><th>MSB:s vägledning[7]</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 1. Schematisk bild, översikt av olika beteckningar för att beskriva systemnivåer inom styr- och övervakningssystem (FOI-R--4206--SE).

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

4 Teoretisk referensmiljö

Under 2015 initierade MSB en studie som syftade till att ge en teoretisk generell referensmiljö för verksamheter som nyttjar industriella informations- och styrsystem [2]. Denna teoretiska referensmiljö presenterar inte någon generell arkitektur, utan snarare kategorier som kan nyttjas vid datainsamling rörande industriella informations- och styrsystem.

Referensmiljön delar upp en organisation i fem nivåer (Figur 2). Nivåerna beskriver vilken verksamhet som respektive nivå ansvarar för, vilka tekniska system som används samt vilka tekniska och kommunikationsmässiga krav som ställs av den aktuella nivån (se nedan). En central aktivitet för referensmiljön är att modellera de olika informationsflöden som finns mellan dessa fem nivåer.

Nivå 4 Verksamhetsledning
Nivå 3 Produktionsledning
Nivå 2 Produktionskontroll
Nivå 1 Direktkontroll
Nivå 0 Fältnivå

Figur 2. Referensmiljöns lager.

Fältnivån handlar om den fysiska process som informations- och styrsystemet kontrollerar och övervakar. I större system såsom en fabrik motsvarar processen de steg som är automatiserade från inkomna råvaror eller komponenter, till den sammansatta och leveransklara produkten. För distributionssystem fokuserar processnivån på distributionskedjan från producent till konsument, antingen hela kedjan eller en delmängd av den.

Direktkontroll handlar om de signaler som tas upp från sensorer och skickas som styrinstruktioner till ett enskilt ställdon. Uppgifter från sensorer skickas även vidare till en central kontroll- eller övervakning, likväl kan instruktioner komma från en kontrollstation.

Produktionskontroll handlar om mänsklig styrning av operatörer för en avgränsad del av en fabriksproduktion. Syftet med denna kontroll är att bevara styrning och stabilitet över den fysiska processen.

Produktionsledning handlar om att koordinera och administrera personal, utrustning och material i syfte att optimera produktionen.

Verksamhetsledning handlar om att indirekt styra över den verksamhet som påverkar eller påverkas av produktionssystemen via ledningsbeslut.

Denna studie nyttjade den teoretiska referensmiljön för skapande av frågebatteriet (se metoddiskussionen i kapitel 2).

5 En preliminär referensmodell

Referensmodellen för fastighetsautomation inom kommunal verksamhet som tagits fram inom denna studie kan ses som preliminär då den baseras på mager empiri. Läsaren bör ta detta i beaktande. Detta kapitel behandlar först (avsnitt 5.1) de likheter och skillnader mellan de tre fallstuderade kommunerna. Mer detaljerade beskrivningar av resultatet redovisas i bilaga 2. Avsnitt 5.2 behandlar likheter och skillnader mellan den teoretiska referensmodell detta arbete grundades på (kapitel 4) och de tre fallstudierna. Slutligen beskrivs den preliminära referensmodellen i avsnitt 5.3.

5.1 Likheter och skillnader mellan kommuner

Det är svårt att jämföra kommuner som är av signifikant skilda storlekar och därmed har olika förutsättningar vad gäller exempelvis tillgängliga resurser för att arbeta med IT-system. Med detta sagt redogör detta avsnitt för de likheter och skillnader som observerats för de tre studerade kommunerna. Denna analys presenteras med samma struktur som den som beskrivs i bilaga 2. Det bör poängteras att kommun A och C storleksmässigt är mer representativa för kommuner i Sverige än kommun B; resultaten från dessa kommuner kanske därmed också är mer representativa. Flertalet av Sveriges kommuner är dock mindre än de kommuner vi har studerat och hur pass väl resultaten stämmer för dem kan vi inte uttala oss om.

5.1.1 Organisation

Alla tre kommuner vi studerat äger egna fastigheter. Dessa inkluderar hyreslägenheter, skolor, boenden, affärs- och föreningslokaler samt idrottsanläggningar. Alla tre kommuner ansvarar helt eller delvis för fastighetsautomationen i fastigheterna. Detta görs i två kommuner av kommunala fastighetsbolag. I den tredje kommunen ligger delar av ansvaret på en förvaltning och resten sköts av privata fastighetsbolag med vilka kommunerna samarbetar. I en av kommunerna ansvarar VA-verket själv för sina fastighetsautomationssystem.

Gemensamt för alla kommuner är att ansvaret för kommunens nätverk för styrning, reglering och övervakning (SRÖ-nätverk) och för att ansluta komponenter (system) till nätverket ligger på en kommunal förvaltning. I några kommuner ansvarar förvaltningarna även för upphandling, inköp, installation och drift samt tillhandahåller en servermiljö, medan dessa ansvarsområden i andra kommuner har lagts på fastighetsbolagen eller på funktionsentreprenörer.

5.1.2 Fastighetsautomation

5.1.2.1 Begreppet fastighetsautomation

Det råder ingen enig bild bland dem vi intervjuat om vilka funktioner som hör till fastighetsautomation, troligen eftersom de själva inte beskriver sina verksamheter med det begreppet. Att värme, kyla, ventilation och belysning ingår är alla överens om. Därutöver finns en rad andra funktioner som också styrs och övervakas via det kommunala nätet för styrning, reglering och övervakning (SRÖ) och som ur ett IT-perspektiv inte skiljer sig från de traditionella funktionerna inom fastighetsautomation. Dessa är brand- och inbrottslarm, passage- och låssystem, reglering av processer i vatten- och reningsverk (t.ex. att reglera pH-värdet i en vattenbassäng), reservkraft till stålverk, badvattenrenare, elladdstolpar, solcellspaneler, informationsskärmar, kameraövervakning och bensinpumpar.

Fysiskt sett ser installationerna lika ut i kommunerna. De olika funktionerna i fastigheterna (värme, ventilation, etc.) styrs från en eller flera datorer med objektspecifika program som sitter i låsta apparatskåp inuti låsta rum. Dessa datorer kallas för Programmable Logic Controllers (PLC) eller datoriserade undercentraler (DUC). Varje apparatskåp har en eller flera intilliggande nätverksportar som är uppkopplade mot olika portar i en switch av något slag som finns i fastigheten för att kunna kommunicera med omvärlden.

5.1.2.2 Central och lokal styrning

I alla tre kommunerna har utvecklingen gått mot att många funktioner inom fastighetsautomationen kan styras och övervakas centralt av ett SCADA-system. Framför allt är det möjligheten till energieffektivisering som har drivit på utvecklingen. Systemen är dock inte beroende av den centrala styrningen. Skulle den gå ner så fungerar fastighetsautomationssystemen autonomt och kan styras lokalt av drift- och fastighetstekniker.

5.1.2.3 Strategier, kravställning och standarder

I kommun B har man aktivt valt att satsa på ett enda centralt SCADA-system för att underlätta installation och drift av olika fastighetsautomationssystem (som i den följande texten även kallas SRÖ-system eftersom de är inkopplade på SRÖ-nätet). Innan man gick över till ett centralt styr- och övervakningssystem så hade man flera olika SCADA-system. Övergången var inte smärtfri eftersom de stora styrföretagen (som levererade och driftade systemen) ville behålla sina egna system.

I kommun A har man, genom att ställa krav vid upphandlingen av system, begränsat sig till två centrala styr- och övervakningssystem från två olika styrföretag.

Kommun C har ingen uttalad strategi för vilka system man ska satsa på nu och i framtiden. Där finns i dagsläget fler än sex olika centrala styr- och övervakningssystem vilket skapar merjobb både för IT-avdelningen och för driftteknikerna. Avsaknaden av standarder har också lett till att det finns en flora av system i kommunen som använder olika protokoll och att det finns ett visst överlapp i de styr- och övervakningssystem som används. De kommunala fastighetsbolagen i kommunen upplever det svårt att förändra situationen eftersom de enbart kan ställa krav på funktionerna som systemen ska leverera vid upphandlingar och inte krav på systemens utformning.

5.1.2.4 Åldrande system

Systemen för fastighetsautomation har olika åldrar. Gemensamt för alla kommuner är att det finns äldre system (komponenter) som kan vara uppåt 20-25 år gamla. De sitter ofta i byggnader som kommunerna av olika anledningar inte vill investera i.

5.1.2.5 Säkerhet

Intervjuerna hade inte som syfte att ta upp säkerhetsfrågor, men respondenterna tog själva upp ämnet vid några tillfällen. Att det finns säkerhetsluckor inom fastighetsautomation är alla överens om, men hur mycket resurser man ska lägga ner för att täppa till dessa kan diskuteras. De bör stå i proportion till vilken skada som kan uppstå om systemen går ner eller manipuleras menar en av respondenterna. Respondenterna anser att även om konsekvenserna av att ett värmesystem eller en ventilationsanläggning slutar fungera kan bli märkbara i enskilda fastigheter, så är det knappast samhällsviktiga verksamheter som slås ut.

5.1.3 Arkitektur

Som kan ses i Figur 5-Figur 10 i bilaga 2 så är de övergripande fysiska arkitekturerna i kommunerna relativt lika, medan de logiska arkitekturerna delvis skiljer sig åt. Avsnitt 5.1.3.1 - 5.1.3.6 beskriver dessa likheter och skillnader.

5.1.3.1 Nätverk

Det finns både likheter och skillnader gällande nätverkskonfigurationerna i kommunerna:

- Kommun B använder Multiprotocol Label Switching (MPLS) för routing/switching, medan kommun A och C använder Open Shortest Path First (OSPF)[8].

[8] Teknologier som bestämmer vilka vägar nätverkspaket skickas inom stora/komplexa datornätverk.

- Kommun B hanterar sin egen routerinfrastruktur, medan kommun A och C anlitar en extern aktör för detta arbete.
- Alla tre kommunerna har ett antal centrala brandväggar som reglerar den huvudsakliga trafiken i deras nätverk.
- Alla tre kommunerna har system för fjärraccess: kommun A och B nyttjar primärt Citrix för fjärraccess[9], där kommun A dessutom använder Microsoft Direct Access. Kommun B har genomfört ett mer omfattande arbete med att knyta upp Citrix mot olika system (såsom sitt SCADA-system), men har fortfarande kvar en del maskiner som tillåter fjärr-inloggning via RDP (Remote Desktop Protocol)[10]. Kommun C använder Virtual Private Network (VPN)[11] och ett verktyg kallat Mobility Guard, vilket erbjuder fjärraccess av webbapplikationer.
- Alla tre kommunerna använder Virtual Local Area Network (VLAN)[12] som huvudsaklig separationsmekanism, men av olika omfattning: kommun A har huvudsakligen ett platt nätverk; kommun B har arbetat mycket med denna separation, särskilt för SRÖ-system; kommun C har fem olika VLAN för SRÖ-komponenter, ett VLAN för varje fysisk fiberring i kommunen.
- Alla tre kommunerna har centrala och huvudsakligen virtualiserade serverfarmer som exekverar majoriteten av kommunens IT-system. Detta inkluderar t.ex. Dynamic Host Configuration Protocol (DHCP)-servrar[13], mailservrar, Domain Name System (DNS)-servrar[14], intranäts-applikationer och faktureringssystem.
- Nätverkskonfigurationen för fastighetsautomationssystemen i kommun A och kommun C är lite lika en tidigare version av fastighets-automationssystemet i kommun B, där varje styrsystemsentreprenör hade stort inflytande. Dock är det oklart om styrsystem från olika entreprenörer tidigare delade samma VLAN i kommun B, vilket görs idag inom kommun A (och i viss omfattning för kommun C). Den lösning som kommun A arbetar mot liknar ytligt den som idag finns på kommun B (ett centralt ”servicecenter” för fastighetsautomation).

[9] Fjärraccess är ett samlingsnamn för teknologier som möjliggör fjärran användning av datorresurser. T.ex. att kunna logga in på sin kontorsdator från hemmet genom en applikation i hemdatorn.
[10] En typ av fjärraccess där användaren får tillgång till datorresursens faktiska grafiska gränssnitt.
[11] VPN möjliggör för datorer som sitter på olika publika datornätverk att prata med varandra som om de sitter på samma lokala privata nätverk.
[12] VLAN möjliggör logisk separation av nätverkstrafik, och kan därmed ses som en billigare men mindre säker ersättning för fysiskt separerade kablar.
[13] DHCP möjliggör automatisk tilldelning av IP-adresser.
[14] DNS är ett protokoll för att koppla IP-adresser (t.ex. 127.0.0.1) till domännamn (t.ex. localhost).

Kommun A planerar att separera produkter från olika entreprenörer på olika VLAN, men dock nödvändigtvis inte fastighetssystem inom olika fastigheter på olika VLAN (vilket är fallet hos kommun B). Det är oklart hur denna framtid ser ut för kommun C.

5.1.3.2 Mjukvara

Mjukvarumässigt finns det fler likheter än skillnader mellan kommunerna:

- Klientsidan baseras i alla tre kommuner på Windows 7, vilket fjärrinstalleras via lösenordskyddad Preboot Execution Environment (PXE)[15].
- Kommunerna nyttjar Microsofts anti-virussystem.
- Kommunerna nyttjar VMware vSphere för virtualisering[16] och har liknande typer av operativsystem och tjänster (primärt Microsoft).
- Patchning av klienter sker via en intern Microsoft-baserad patchserver[17]. Patchning av servrar sker manuellt vid behov. Det skiljer sig dock gällande fastighetsautomationssystemen, där entreprenörer har mer ansvar för patchning i kommun A och C än i kommun B.
- Patchning sker överlag mer frekvent än för SCADA-system som NCS3 observerat i andra verksamheter, såsom spårbunden trafik [18]. Orsaken till detta är att åtkomsten av SCADA-systemen för fastighetsautomation inom kommunal verksamhet är mindre reglerad. Detta då den anses vara mindre kritisk för samhällets säkerhet och funktion.
- Användares möjlighet att installera mjukvara är låst via Active Directory (AD)-policies.
- SCADA-system, DUC:ar och PLC:er skiljer sig mellan kommunerna då kommun B kommit längre med att ersätta den tidigare dominanta heterogena fastighetsautomationsmiljön, där det nyttjades flera olika SCADA-system, med Citect. Kommun A har nyligen börjat ett liknande arbete men har lång väg kvar att vandra. Kommun B och C skiljer sig på så sätt att kommun B endast köper in PLC:er, och kommun C endast köper in DUC:ar.

[15] PXE möjliggör installation av operativsystem och applikationer över nätverkskommunikation och är därmed ett enkelt sätt att förbereda nya datorer åt användare. En dator med PXE aktiverat skickar under boot en DHCP-fråga efter tillgängliga PXE-servrar. Om det finns någon sådan hämtar datorn relevant installationsmedia från PXE-servern.

[16] Virtualisering innebär här att flera datorer exekveras av en och samma hårdvara genom en särskild applikation (i kommunernas fall är detta en mjukvara skapad av VMware).

[17] En server som kontinuerligt uppdateras med Microsofts mjukvaruuppdateringar. Dessa uppdateringar skickas sedan över till andra datorer i nätverket där de automatiskt installeras.

5.1.3.3 Hantering av behörigheter

Alla tre kommuner använder sig av Microsoft AD-lösning, vilken underhålls av ett fåtal dedikerade medarbetare. Kommun B har dock genomfört ett mer omfattande arbete med att knyta denna AD-lösning mot olika system, såsom sitt SCADA-system. De allra flesta användarna inom kommunerna är inte lokala administratörer över sina egna datorer.

5.1.3.4 Teknisk monitorering och övervakning

Det loggas en del teknisk data inom alla tre kommuner, särskilt sådant som passerar brandväggar. Endast kommun C menar att de gör ett dedikerat arbete för att gå igenom det resulterande datamaterialet.

5.1.3.5 IT-säkerhetsrelevant träning och utbildning

Det genomförs ingen särskild IT-säkerhetsrelevant träning eller utbildning inom någon av kommunerna.

5.1.3.6 Säkerhetstester

Det genomförs inga kontinuerliga IT-säkerhetsrelevanta tester inom kommunerna. Det har dock tidigare genomförts ett penetrationstest på nätverksnivå inom kommun B och ett par sådana inom kommun A.

5.2 Likheter och skillnader mellan teori och verklighet

Alla fem nivåer som beskrivs i den teoretiska referensmiljön [2] (se Figur 2) finns tydligt representerade i de tre kommunerna. En jämförelse mot de mer konkreta generiska arkitekturerna för olika industriella informations- och styrsystem som presenteras i NIST 800-82 [15] visar att de tre kommunerna fysiskt sett är relativt lika ett tågövervakningssystem (se Figur 2-6, sida 24 i [15]). Trafik går via Internet Protocol (IP) över fiberringar till olika tågsektioner, där varje tågsektion kan liknas vid en fastighet i en kommun. Den övergripande skillnaden mot de övriga arkitekturskisserna i NIST 800-82 är att modem inte är särskilt förekommande i kommunerna. Mer detaljerade likheter/skillnader går inte att identifiera eftersom abstraktionsnivån för referensarkitekturerna i NIST 800-82 är för hög.

När det gäller goda råd i guider såsom [8], [15], [19] så har alla tre kommunerna arbetat på något sätt med de allra flesta punkter. Exempelvis nyttjar de i mer eller mindre omfattning logisk separation av nätverksresurser, minsta möjliga åtkomst, samt olika typer av mjukvaruskydd. Som beskrivs i avsnitt 5.1 skiljer det dock en del hur mycket resurser kommunerna har tilldelat säkerhetsfunktioner, särskilt gällande SRÖ-systemen.

5.3 Beskrivning av modellen

Referensmodellen består av två olika topologier - en fysisk topologi (Figur 3) och en logisk topologi (Figur 4). Den fysiska topologin beskriver hur fastighetsautomationssystemet rent fysiskt är konstruerat. Exempelvis hur de fiberringar som möjliggör nätverkskommunikation är placerade, eller var olika tekniska komponenter sitter i fastigheter. Den logiska topologin beskriver hur fastighetsautomationssystemet realiseras rent logiskt. Exempelvis vilka nätverksprotokoll och mjukvaror som används.

Referensmodellen fokuserar ej på olika systemfunktioner, såsom värme, kyla och ventilation. Anledningen till detta är att dessa praktiskt sett installeras, underhålls och övervakas på snarlika sätt IT-mässigt.

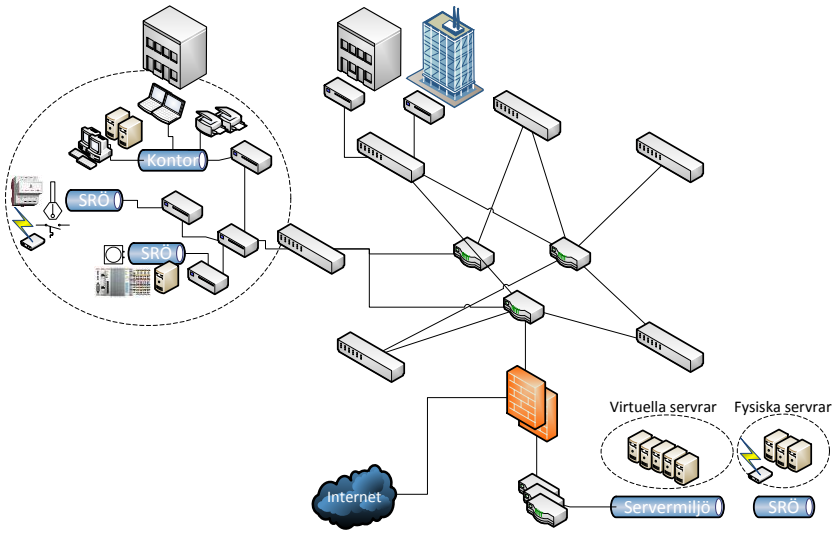
Fastighetsautomationssystemet (SRÖ-systemet) realiseras av ett flertal komponenter tillsammans: Sensorer i fastigheter som skickar signaler till inbyggda system som sitter i särskilda låsta utrymmen i fastigheter. Dessa inbyggda system pratar över ethernet och IP via VLAN-separerade nätverk till servrar. Anställda konfigurerar och övervakar systemet via IT-resurser på diverse olika fysiskt och logiskt skilda platser. Exempelvis ute i fastigheten, via fjärraccess, eller via en operatörsdator som sitter på samma VLAN som servrarna. Ofta sitter många olika typer av SRÖ-komponenter på samma VLAN, där de kan prata med varandra relativt obehindrat. Exempelvis en arbetsstation, en switch och några PLC:er eller DUC:ar. Andra IT-resurser i fastigheter, såsom en datorsal i en skola, sitter på andra VLAN men är anslutna till kommunens nätverk och IT-resurser på liknande sätt.

Rent fysiskt är allt ihopkopplat via ett par fiberringar, routrar, switchar och brandväggar som möjliggör fysisk redundans. En fastighet som är av särskild vikt kan koppla upp sig mot flera komponenter och ringar för att minimera potentiella driftstopp. Serverhallar är ofta fysiskt redundanta. Den redundanta serverhallen innefattar dock typiskt enbart en delmängd av alla system, såsom centrala routrar. Den redundanta funktionen testas dessutom relativt sällan. Tjänster i serverhallar (t.ex. DHCP, DNS och SRÖ) är ofta separerade på olika VLAN. Oftast används flera SRÖ-system då produkter från olika leverantörer stöds av olika styr- och övervakningssystem. Äldre SRÖ-system körs oftast i virtuella maskiner. Modernare SRÖ-system och ”vanliga” IT-resurser såsom DHCP-servrar och Windows AD (Active Directory) körs i virtuella maskiner (vanligen VMWare VSphere).

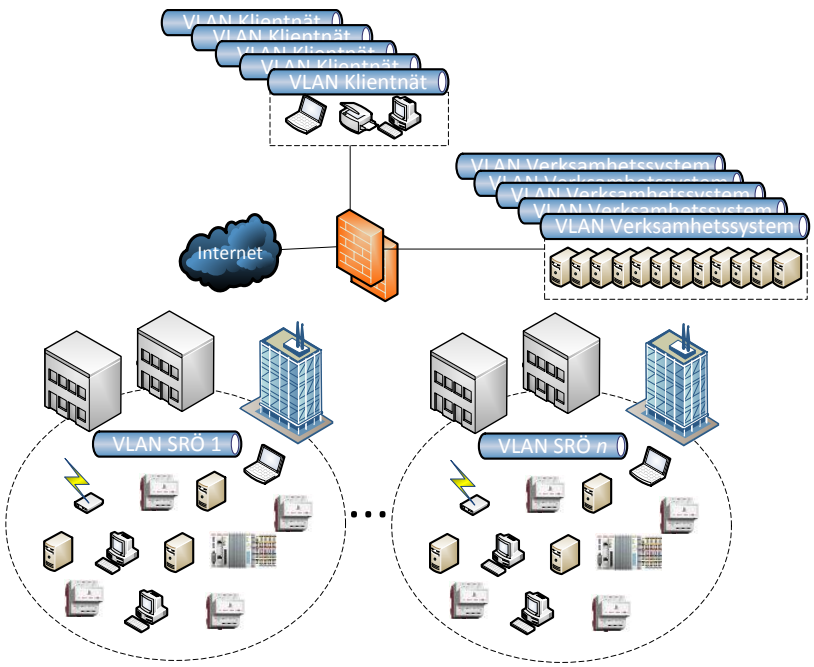
Klientdatorer, såsom en kontorsdator, kommunicerar typiskt genom samma fysiska komponenter och kablar som servrar, men på andra VLAN. De allra flesta arbetsdatorer fjärrinstalleras över nätverk via lösenordskyddad PXE-boot.

Den vanligast tillämpade typen av inbyggt system för fastighetsautomation är en DUC. PLC:er blir dock allt vanligare då de har modernare funktionalitet.

Det är möjligt att fjärrstyra de allra flesta IT-resurser om användaren har rätt behörighet. Fjärrstyrning sker via en mängd olika metoder, från enstaka RDP-lösningar till omfattande Citrix-system. Allokering av behörigheter sker i Windows AD. Detta är en halvt automatiserad process då användare till stor del automatiskt kan skapas via exportering av uppgifter från personalhanterings-system. På grund av att många manuella ändringar behöver göras på exporterade poster krävs det ändå flera heltidstjänster att hantera behörigheter.



Figur 3. Gemensam fysisk nätverksarkitektur.



Figur 4. Gemensam logisk nätverksarkitektur.

6 Förslag på framtida arbete

Denna studie har analyserat tre kommuner gällande deras industriella informations- och styrsystem inom fastighetsautomation. Syftet var att identifiera en generell arkitektur som kan ligga till grund för liknande studier i framtiden.

Det är svårt att dra några generella slutsatser från tre kommuner, och den teori som idag finns är på en högre abstraktionsnivå än denna studie ämnade analysera. Det finns dock tydliga likheter och skillnader mellan kommunerna (se avsnitt 5.1). Alla tre studerade kommuner bedöms vara långt fram i arbetet med sina IT-arkitekturer och väl medvetna om sina styrkor och svagheter. De skiljer sig dock delvis, särskilt gällande arbetet med just fastighetsautomationssystemen. Här har kommun B kommit längst med arbetet att implementera traditionella IT-styrningsmekanismer såsom standardisering av komponenter och logisk separation av resurser, även om mycket jobb kvarstår. Det bedöms sannolikt att även andra kommuner kommer vandra mot en sådan lösning.

För att erhålla ett bra statistiskt underlag krävs det att många fler kommuner involveras. Möjligen skulle en enkät kunna tillämpas för att identifiera översiktliga likheter och skillnader för de mest relevanta frågeställningarna. En sådan frågeställning skulle kunna vara vilka leverantörer som är typiska inom området.

Referenser

[1] K. M. Sonnek and F. Lindgren, “Industriella informations- och styrsystem inom fastighetsautomation - en förstudie (FOI-R--4206--SE),” 2016.

[2] Lars Westerdahl, D. Eidenskog, P. Andersson, and E. Westring, “Teoretisk referensmiljö.”

[3] D. Mellado, E. Fernández-Medina, and M. Piattini, “A common criteria based security requirements engineering process for the development of secure information systems,” *Comput. Stand. interfaces*, vol. 29, no. 2, pp. 244–253, 2007.

[4] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, “Introduction to the OCTAVE Approach,” *Pittsburgh, PA, Carnegie Mellon Univ.*, 2003.

[5] A. Calder, *Information security based on ISO 27001/ISO 17799: a management guide*. Van Haren Publishing, 2006.

[6] M. S. Lund, B. Solhaug, and K. Stolen, *Model-driven risk analysis: the CORAS approach*. Springer Verlag, 2011.

[7] M. Mertz, “NERC CIP compliance: We’ve identified our critical assets, now what?,” in *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, 2008, pp. 1–2.

[8] CPNI, “Good Practice Guide -- Process Control and SCADA Security.” Center for the Protection of National Infrastructure (CPNI), 2008.

[9] ISA, “Security for Industrial Automation and Control Systems Part 1 : Terminology, Concepts, and Models,” 2007.

[10] R. Melton, T. Fletcher, and M. Donaldson, “System Protection Profile - Industrial Control Systems,” 2004.

[11] GAO, “Cybersecurity for Critical Infrastructure Protection.” United States General Accounting Office (GAO), 2004.

[12] G. Finco and others, “Cyber Security Procurement Language for Control Systems,” *Idaho Natl. Labs*, no. August, 2007.

[13] P. Herzog, “Open--source security testing methodology manual,” *Inst. Secur. Open Methodol.*, 2003.

[14] DOE, “21 Steps to Improve Cyber Security of SCADA networks.” Office of Energy Assurance, U.S. Department of Energy, 2002.

[15] N. S. P. NIST, “800-82,” *Guid. to Ind. Control Syst. Secur. Final Public Draft. Natl. Inst. Stand. Technol.*, 2008.

[16] H. Holm, K. Shahzad, M. Buschle, and M. Ekstedt, “P CySeMoL: Predictive,

Probabilistic Cyber Security Modeling Language," *Dependable Secur. Comput. IEEE Trans.*, vol. 12, no. 6, pp. 626–639, 2015.

[17] H. Holm and E. Westring, "NCS3: Informations- och styrsystem inom hälso- och sjukvård – En kartläggning av produkter och incidenter (FOI-R--4088--SE)," 2015.

[18] K. M. Sonnek, H. Holm, J. Lindgren, F. Lindgren, and E. Westring, "NCS3 - informations- och styrsystem inom spårbunden trafik. En kartläggning (FOI-R--4029--SE)," 2015.

[19] MSB, "Vägledning till ökad säkerhet i industriella informations och styrsystem," 2014.

Bilaga 1. Intervjuguide

Intervjupersonen

- Beskriv din roll/befattning i organisationen och vilka uppgifter som hör till rollen.
- Beskriv i korthet hur din verksamhet (administrativ alternativt teknisk) fungerar i din kommun.

Fastigheter

- Vilka fastigheter ingår i den specifika kommunala verksamheten?
- Vilka system för fastighetsautomation används och vad de har för funktion?
  - Hur gamla är de?
  - Finns det redundans?
- Hur övervakas och styrs systemen (centralt/lokalt)?
  - I vilken utsträckning sker övervakning och styrning centralt för flera fastigheter?
  - Vad sker manuellt/automatiskt?
- Vilka aktörer finns inom och utanför kommunen?
  - Vem äger fastigheterna och systemen?
  - Vem beställer systemen?
  - Har ni riktlinjer för hur ni kravställer dem?
  - Vem levererar systemen?
  - Vem förvaltar systemen?
- Vilka organisatoriska enheter i kommunen har ansvar för att automationen ska fungera?
- Har ni riktlinjer och krav att förhålla er till?
- Har ni samarbeten och informationsutbyten med andra kommuner?
  - Inom olika nätverk?
- Vilka konsekvenser skulle det få om systemen för fastighetsautomation slutar att fungera?
- Finns det något du vill tillägga vad gäller fastighetsautomationen?

Arkitektur

När det gäller arkitekturfrågor ämnar de inte ge en komplett beskrivning respondentens arkitektur. Frågorna nedan fungerar mer som stöd för att visa på vilken typ av information som eftersöks. För en delmängd av arkitekturen kommer det behövas mer detaljerade frågor; för en stor del av arkitekturen kommer endast övergripande information inhämtas. Exempelvis är det inte relevant att kartlägga alla mjukvaror i en stor kontorsmiljö, utan värdefullare att försöka identifiera gemensamma nämnare och nyckelegenskaper. Såsom att alla kontorsdatorer bygger på samma grund-installation, eller att en viss kontorsdator har en koppling till ett automationssystem.

- *Mjukvara och dess konfigurationer*
    - Vilka typer av operativsystem (t.ex. Windows 7 eller CentOS) används?
    - Vilken typ av hårdvara nyttjas?
    - Används TPM/kryptering av diskar?
    - Vilka typer av applikationer används?
    - Hur ofta sker egenutveckling av mjukvara?
    - Hur ofta sker egen förädling av mjukvara?
    - Hur uppdateras mjukvara? Exempelvis, används någon intern patchserver eller direktkoppel mot Microsoft/Adobe/etc?

- *Administration av IT-resurser*
    - Vilka behörighetssystem används (t.ex. Active Directory-strukturer och specifika rättighetssystem för webbapplikationer)?
    - Hur många användare har administratörsprivilegier?
    - Vilken typ av administration omfattar installation, drift och nyttjande av tekniska resurser?
    - Hur går en typisk installation av ett nytt system (bestående av olika tekniska resurser) till?
    - Vilka är ansvariga för olika administrativa processer rörande IT-resurser (t.ex. ändringshantering och behörighetshantering)?
    - Används några typer av ärendehanteringssystem av tekniska resurser?
    - Hur används bärbara medier, såsom USB-diskar och DVD-skivor?
    - Hur många tar med sig kontorsdatorer till externa platser, eller icke-kontorsdatorer till kontoret (och kopplar upp dessa mot nätverk)?

- *Nätverkskonfigurationer*
  - Hur är nätverk konfigurerade? T.ex., hur är IP-trafik segmenterad av brandväggar?
  - Vilka större ”publika” nätverk (såsom Internet) är system uppkopplade mot?
  - Hur underhålls brandväggsregelverk? Exempelvis, hur går det till vid installation av en ny server-klient-lösning?
  - Hur tillämpas separation av nätverk? Logiskt (VLAN) eller fysiskt?
  - Vilka nätverksprotokoll, såsom DHCP, DNS, BGP, FTP, SMB och RDP, används (och var används dessa)?
  - Vilka andra typer av logiska hopkopplingar av fysiskt separerad mjukvara/hårdvara, såsom modemuppkopplingar, används?
  - Hur interagerar automationssystemet med sin omgivning? T.ex., hur ser uppkopplingar mot kontorssystemet eller Internet ut?

- *Tester under utveckling och i drift*
  - Hur ofta görs tekniska och administrativa granskningar av olika systemkomponenter, eller systemet som helhet?

- *Sensorer och loggning*
  - Vilka typer av sensorer används för att undersöka vad som finns, samt att ”allt står rätt till” (exempelvis portscanning, sårbarhetsskannrar, närverksdetektorer och anti-virus)?
  - Vilka typer av tekniska händelser loggas?
  - Hur sker uppföljningen av loggar?

- *Träning och utbildning*
  - Vilken typ av träning och utbildning genomgår utvecklare, driftansvariga och slutanvändare av systemen?
  - Hur och var används konsulter?
  - Vilka policies och rutiner finns för utvecklare, driftansvariga och slutanvändare av system?

- *Fysisk access*
  - Hur är olika komponenter placerade rent fysiskt?

- *Framtiden*
  - Hur ser framtiden/planen ut för ovan frågeställningar?

Avslutning

- Finns det något som du tycker att vi skulle fråga om, som inte togs upp under intervjun?
- Finns det något skriftligt material du vill dela med dig av, med bakgrund i intervjuns innehåll
- Känner du att det är något du vill tillägga?
- Med bakgrund i de frågor vi ställt och det du berättat, finns det någon mer person du tycker att vi borde prata med?
- Hur går vi vidare nu, vi återkommer runt [datum]
- Tack

Bilaga 2. Resultat

Denna bilaga beskriver resultatet från de intervjuer som genomfördes under studien. Beskrivningarna bygger enbart på vad respondenterna har förmedlat, vi har inte kontrollerat innehållet mot andra källor.

B2.1 Kommun A

B2.1.1 Respondenter

Materialet för kommun A kommer från två intervjuer: en intervju på cirka två timmar med respondent R1, samt en intervju på cirka 40 minuter med respondent R2. R1 är chef för den enhet som ansvarar för test och integration av kommunens IT-arkitektur. R2 arbetar på drift- och serviceförvaltningen och är där ansvarig för alla tekniska installationer att handla upp entreprenörer och att sköta driften av de tekniska systemen, bland annat i skolor och boenden.

B2.1.2 Organisation

Organisatoriskt finns det två huvudsakliga enheter inom kommunen som har hand om installation, tester och underhåll av IT: test och integration samt drift. Test och integration är ansvariga för klientsidan, såsom standardimagen för klientdatorer. Driftenheten är ansvarig för backbone-delar, såsom servermiljön och nätverk, inklusive verksamhetssystem och fastighetsautomationssystem.

Arbetets omfattning för driftenheten har ökat sedan R1 tillträdde. Exempelvis har antalet verksamhetssystem som driftenheten har ansvar för ökat från 40 till 80 sedan 2005, men antalet drifttekniker består. R1 uppskattade att 60-80 % av driftenhetens tid ägnades åt verksamhetssystemen.

Kommunen äger egna fastigheter, bland annat för skolor (för-, grund- och gymnasieskolor) och för några enstaka boenden. Dessa förvaltas av drift- och serviceavdelningen. Därutöver finns det två kommunala fastighetsbolag som ansvarar för andra byggnader i kommunen. Kommunens vattenverk ansvarar för sig självt.

B2.1.3 Fastighetsautomation

Från R1:s perspektiv involverar de fastighetsautomationssystem som övervakas och styrs inom kommunen exempelvis brandlarm, passage- och låssystem, vattenverk, reningsverk, ventilation och värme. Vissa funktioner som typiskt kan tänkas ligga inom industriautomation (t.ex. att reglera pH-värdet i en vattenbassäng) ligger även inom ramen för dessa system. Det var dock oklart för

R1 exakt vilka typer av funktioner som fanns samt i vilken omfattning dessa kunde styras snarare än enbart övervakas. För R1 är det ungefär samma underhåll oavsett funktion.

Inom drift- och serviceförvaltningens ansvarsområde (R2:s perspektiv) ryms värme, kyla, ventilation, belysning och övervakning av inkommande tappkall- och tappvarmvatten till fastigheterna (mätning av läckage och läckagelarm). Larm och brandlarm kan också anses ingå inom begreppet fastighetsautomation men ligger inte inom förvaltningens ansvarsområde.

Systemen för de allra flesta funktioner, temperaturer, pumpstatus, etc. (cirka 95 % av alla SRÖ-komponenter[18]) kan övervakas från två olika styr- och övervakningssystem: ett från Siemens (cirka 20 % av komponenterna) och ett från Schneider Electric (cirka 80 % av komponenterna). De fåtal resterande funktionerna har egna lösningar från andra entreprenörer. Dessa komponenter är typiskt äldre; de äldsta driftsattes under 90-talet. Dessa sitter i byggnader som kommunen av olika anledningar inte vill investera i.

Kommunen har en standard som systemen måste följa. Denna ställs som krav vid upphandlingar. Krav inom standarden är t.ex. att all utrustning skall vara programmerbar och att det skall finnas tillgång till programmeringsverktyg. Siemens och Schneider Electric var de enda som klarade av att uppfylla dessa krav.

Vissa delar av belysningen i fastigheterna kan fjärrstyras. Om den centrala styrningen och övervakningen skulle gå ner så kan den skötas lokalt i varje skola.

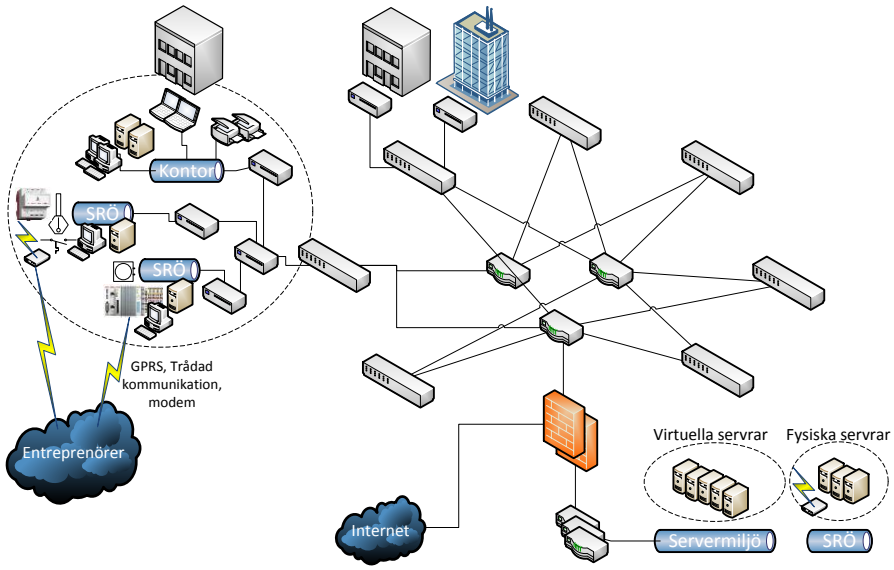
I de fall kommunen bygger nya fastigheter från grunden så är det bygg-avdelningen som har hand om det. Alla nybyggda fastigheter läggs ut på totalentreprenad.

En utmaning är att det kommer många nya produkter inom fastighetsautomation. Det gäller att hitta rätt lösning till rätt fastighet.

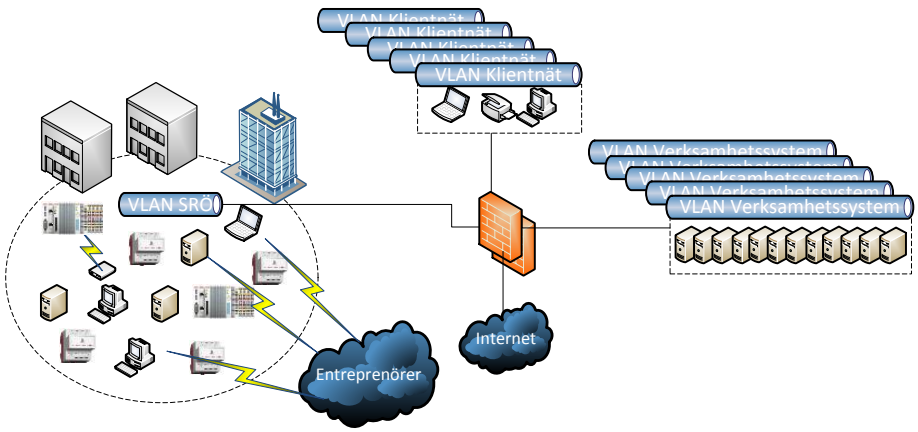
B2.1.4 Arkitektur

En översikt av kommunens fysiska IT-arkitektur visas i Figur 5 och den logiska i Figur 6. De resterande avsnitten i detta kapitel beskriver komponenterna i dessa figurer.

[18] SRÖ = Styrning, reglering och övervakning.



Figur 5. Fysisk nätverksarkitektur kommun A.



Figur 6. Logisk nätverksarkitektur för kommun A.

B2.1.4.1 Nätverk

Den fysiska nätverksarkitekturen, såsom kablage och switchar, installeras och driftas av ett externt företag. Routerinfrastrukturen inom kommunen bygger på Open Shortest Path First (OSPF). Kommunen äskar efter konfigurations-ändringar såsom att ändra vilken port som skall tillhandahålla ett särskilt VLAN. VLAN är för övrigt den huvudsakliga nätverkssegmenteringsmekanismen som används.

Kommunens nätverkstopologi består av tre huvudsakliga komponenter: en serverpark, en administration/klient-del, och en del för styrning, reglering och övervakning (SRÖ). Var och en av dessa delar är segmenterade i olika VLAN. De är alla sammankopplade via två brandväggar (en aktiv och en passiv) av märket Checkpoint. Dessa brandväggar agerar också paketfilter på payload-nivå. Filter erhålls dels genom Checkpoint själva, och dels genom anpassning/egen-utveckling. All trafik mellan de olika segmenterade VLAN:en är tänkt att gå via dessa brandväggar. Serverparkerna lever med statiska IP-addresser, även om de också har interna DNS-servrar. Klientparkerna använder DHCP.

Serverparken är fysiskt redundant via en spegling på en geografisk skild plats. Det gjordes nyligen ett test för att verifiera att denna spegling fungerar. Den hanterar den mjukvara som krävs för att kommunens alla datoranvändare skall kunna interagera med kommunens system. Detta inkluderar exempelvis resurser för hantering av behörigheter (Active Directory, AD), nätverksinstallation av operativsystem (Preboot Execution Environment, PXE), hantering av fjärraccess (via Citrix och Microsoft Direct Access), mailservar och koppling mellan IP-nummer och domännamn vid webbsurfning (Domain Name System, DNS). Den innefattar också olika verksamhetsspecifika system såsom felanmälan, intranäts-applikationer och ekonomisystem. Kommunikationen inom och till/från serverparken går via kabelöverförd IP-trafik. Resurserna är placerade på olika VLAN efter typ av funktion. T.ex. är system som skall vara nåbara från Internet (t.ex. mailservrar och webbservrar) placerade på ett eget VLAN.

Klientnätet är alla resurser som kommunens personal och invånare interagerar med dagligen, såsom personaldatorer och skrivare. Datorer på klientnätet får NAT-adresser kopplade till två olika klass C-nät via två centrala DHCP-servrar.

Vissa klientdatorer och användare har access till serverparken; de allra flesta har det dock inte. Ute i klientnätet finns otaliga switchar och liknande för att tillhandahålla nätverk till kommunens spridda geografiska platser. Kommunikationen inom och till/från klientnätet går dels via kabelöverförd IP och dels via trådlösa accesspunkter (separerade i olika VLAN).

SRÖ-nätet innefattar de komponenter som behövs för att styra och övervaka kommunens alla olika fastighetsautomationssystem. Styrning och övervakning görs dels av fastighetsavdelningen, dels av två kommunala bolag, och dels av vattenverket. SRÖ-nätet beställdes av fastighetssidan från en privat aktör i slutet

av 90-talet. Då var man inte så säkerhetsmedveten. SRÖ-komponenter sitter i apparatskåp bakom låsta utrymmen. Varje komponent kopplas in i kommunens fibernätverk via en industriswitch som sitter i respektive fastighet. Kommunens IT-enhet hjälper till att patcha ut rätt VLAN till portar i switchen. Enligt R1 är dock SRÖ-nätet av en relativt platt struktur spridet över ett fåtal VLAN (det finns inga direkta restriktioner för hur olika komponenter på nätet får prata med varandra). Det är också så att alla dess olika leverantörer, utvecklare och nyttjare mer eller mindre har enkel och direkt access till det. Exempelvis kan en nyttjare inom kommunens vattenverk från sitt kontor kommunicera både mot servernätet (t.ex. för felanmälan), SRÖ-nätet (t.ex. för att övervaka en sensor) samt de flesta andra komponenter i SRÖ-nätet. Eller helt enkelt koppla upp sig på plats mot en komponent. Det finns planer för att partitionera upp SRÖ-nätet i olika VLAN efter funktion och involverade entiteter. Kommunikationen till/från SRÖ-nätet går via en blandning av de metoder som SRÖ-nätets intressenter funnit värdefulla. Detta inkluderar primärt olika IP-kopplingar (varav vissa inte går via IT-enhetens centrala brandväggar). Modem används ytterst sällan.

B2.1.4.2 Mjukvara

Tidigare fanns det en del egenutvecklade applikationer inom kommunen. Nu är dock i princip allt Commercial Off The Shelf (COTS)-lösningar. Bärbara medier såsom USB och CD/DVD-skivor är i regel tillåtna (t.ex. inte avstängda genom någon domänpolicy i AD:t eller fysiskt demonterade från några enheter).

Serverparken består av 10 bladservrar som kör VMWare Vsphere, vilket relativt nyligen (för ett par år tillbaka) införskaffades (VMWare har dock använts i cirka tio år). Dessa servrar kör cirka 180 virtuella maskiner, från Windows Server 2003 till Windows Server 2012. Serverna tillhandahåller en blandning av standardtjänster för IT-administration såsom AD, DNS[19], mail, fjärraccess (via Citrix Netscaler), databaser och fildelning, samt mer specifika lösningar såsom intranätsapplikationer och ekonomisystem (dessa system benämns som verksamhetssystem i kommunen). Mjukvaruuppdateringar installeras manuellt på servrar.

Klientdatorer installeras till en Windows 7-image via PXE-boot. PXE-boot innebär att ett färdigkonfigurerat operativsystem, komplett med alla standard-applikationer som behövs (t.ex. Microsoft Office) installeras via nätverket (tillhandahållet från servermiljön). R1 tror att ett lösenord används i denna process; vilken dator som helst kan därmed inte installera denna standardimage. Det är dock oklart hur denna process faktiskt hanteras (t.ex. vilket/vilka lösenord som används). Defaultkontona för dessa datorer har inte rätt att installera

[19] Det finns både interna och externa DNS-servrar. Dessa har för närvarande ej stöd för DNSSec (Domain Name System Security Extensions), men det finns planer på att byta ut dem.

mjukvara eller liknande. Detta sätts som en policy i behörighets-hanteringssystemet i serverparken (AD:t). Det finns dock tankar på att byta denna lösning mot Microsoft Applocker. Likt de flesta andra verksamheter så har kommunalanställda möjlighet att ta med sina arbetsdatorer (bärbara datorer) till externa platser, där de utsätts för externa nätverk och system (såsom de anställdas hemmanätverk). Microsoft Security Essentials, det anti-virussystem som tillhandahålls gratis av Microsoft, är installerat i alla klienter. Mjukvaru-uppdateringar installeras automatiskt på klienter via en intern Microsoft-patchserver.

SRÖ-nätet består av en blandning av virtuella och fysiska servrar som kör olika versioner av Windows Server (huvudsakligen 2008 – 2012). Enligt R2 används fysiska servrar för äldre SRÖ-komponenter där det inte gjorts nyinvesteringar. Det innefattar också diverse olika inbyggda system för övervakning och reglering. Det är oklart för R1 exakt vilka typer av inbyggda system (t.ex. DUC:ar, PLC:er och liknande) som finns. Enligt R2 är det dock enbart DUC:ar som nyttjas. Anledningen till detta är helt enkelt att det alltid har varit så, och att det därmed skulle krävas en kostnad för att byta till något annat. För att interagera med dessa system finns även olika Human Machine Interface (HMI)-datorer i SRÖ-nätet. Dessa är i princip vanliga arbetsstationer som kör Windows-installationer eller liknande. Många intressenter tar även med sina egna datorer till SRÖ-nätet. Det är väldigt olika hur ofta olika leverantörer uppdaterar sina system. Microsoftservrar uppdateras dock varje månad.

B2.1.4.3 Hantering av behörigheter

Kommunen har 5000 anställda, varav cirka 100 är administratörer över sina egna maskiner. Dessa 5000 användare omfattar cirka 1000 olika användargrupper i AD:t. Dessa användare och grupper har alla olika access till olika resurser, såsom access till olika filer och mappar i en fildelningsserver i verksamhetsnätet (kallad ”E:/”). Det krävs ett gediget arbete för att underhålla denna lösning. Två personer har ansvar för att hantera behörigheter i AD:t.

Endast ett fåtal nyckelpersoner har rättigheter för att administrera resurser i serverparken. I SRÖ-nätet är många komponenter inte domänanslutna till kommunens AD; rättigheterna finns istället lokalt på olika komponenter och mjukvaror.

B2.1.4.4 Teknisk monitorering och övervakning

Det som passerar brandväggar loggas. Det är dock oklart för R1 vad exakt som loggas och hur saker följs upp. Tidigare fanns det en person som jobbade specifikt med säkerhet, men den personen är inte kvar.

B2.1.4.5 IT-säkerhetsrelevant träning och utbildning

Det finns ingen särskild IT-säkerhetsträning för personal inom kommunen, oavsett roll.

B2.1.4.6 Säkerhetstester

Det har genomförts ett antal tester av kommunens IT-säkerhet av privata företag. Exempelvis har det utförts penetrationstester. Kommunen fick bra betyg i dessa tester.

B2.2 Kommun B

B2.2.1 Respondenter

Intervjun på kommun B genomfördes under cirka två timmar med två respondenter (R3 och R4).

Respondent R3 arbetar med backbone-delen av kommunens stadsnät, d.v.s., IT-utrustningen som möjliggör nätverksaccess inom kommunen. Detta inkluderar exempelvis routing, switching, brandväggar och installation samt drift av diverse hårdvara och mjukvara som stödjer detta. Respondenten har haft en central roll i detta arbete ända sedan ”IP-fieringen” började i kommunen.

Respondent R4 arbetar som projektledare på kommunens fastighetsavdelning med en inriktning mot fastighetsautomation. Respondenten har haft denna roll i cirka fem år och har sedan tidigare en bakgrund inom IT.

B2.2.2 Organisation

Fastighetsförvaltningens primära ansvar är att upprätta och bibehålla erfordrad funktion för de fastigheter som kommunen äger.[20] Detta arbete görs tillsammans med två privata bolag, vilka hanterar cirka hälften av alla fastigheter (kommunen hanterar den andra hälften).

Kommunen börjar för närvarande se resultaten från en stor satsning på SCADA-system som påbörjades under 2011. Tidigare hade kommunen flera olika SCADA-lösningar (Siemens Desigo, TAC Vista, Johnson M5, Johnson MSEA, Honeywell INUvision och Honeywell EBI), där de olika tillverkarna och konsulterna för olika inbyggda system och SCADA hade stort ansvar för installation och drift. Denna lösning lämnades till förmån för ett centralt

[20] På kommunens hemsida kan man läsa att förvaltningens viktigaste mål är att minska användningen av energi och ersätta med förnybar energi samt använda energin effektivare.

SCADA-system av märket Citect som installerats och driftas av kommunen. Övergången var (och är) inte helt smärtfri eftersom de stora styrföretagen gärna ville behålla sin monopolsituation.

Organisatoriskt saknar kommunen en systemförvaltare för de övergripande systemen; den tänkta systemförvaltaren blev tidigt långtidssjukskriven så projektledaren sköter systemet på deltid tillsammans med konsult.

Kommunen anlitar s.k. funktionsentreprenörer vars uppgift är att upprätthålla systemfunktioner i fastigheter. De är användare av SCADA-systemen, varifrån de har möjlighet att styra och övervaka fastigheterna. Inköp och upphandling står ett av fastighetsbolagen för. Det är ett krav att funktionsentreprenörerna ska kunna nå sina system via internet. De har access både till Citect och till de äldre SCADA-system som ännu inte fasats ut. Dock är accessen till Citect mer restriktiv än till de äldre systemen.

Det finns även en utvecklingsmiljö i vilken de entreprenörer som installerar och konfigurerar styrsystemen (t.ex. kopplar upp PLC:er i en fastighet eller integrerar processbilder i Citect) kan testa sina lösningar.

B2.2.3 Fastighetsautomation

Till de funktioner som räknas in i begreppet fastighetsautomation i kommunen ingår kyla, värme, sol, el, fjärrvärme, ventilation, belysningsstyrning, reservkraft, mätare av olika slag, och hissar (hisslarm). Andra system, såsom badvattenrening, finns också integrerade i Citect. Dessa ses dock som processverksamhet snarare än fastighetsautomation. Passage och inbrottslarm är ej integrerade.

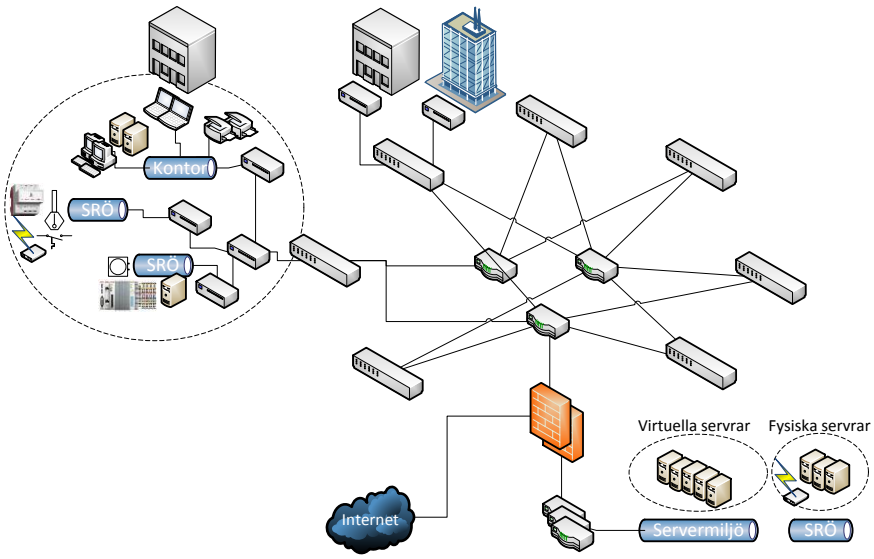
Respondenterna tror över lag inte att konsekvenserna blir särskilt stora om fastighetsautomationssystemen inte skulle fungera. ”Ingen kommer dö om fläkten stannar.” Om värmen å andra sidan slutar att fungera i kommunens nya konferensanläggning, där värmesystemet även nyttjas av ett externt hotell, eller i badhuset, så kan problemen bli större. Slutar pumparna som pumpar upp grundvatten fungera så kan det i värsta fall bli översvämning.

Hur mycket resurser man lägger ner på säkerheten i systemen måste stå i proportion till vilken skada som kan inträffa om systemen går ner/manipuleras. Det är en större risk med insiders än med hackare utifrån.

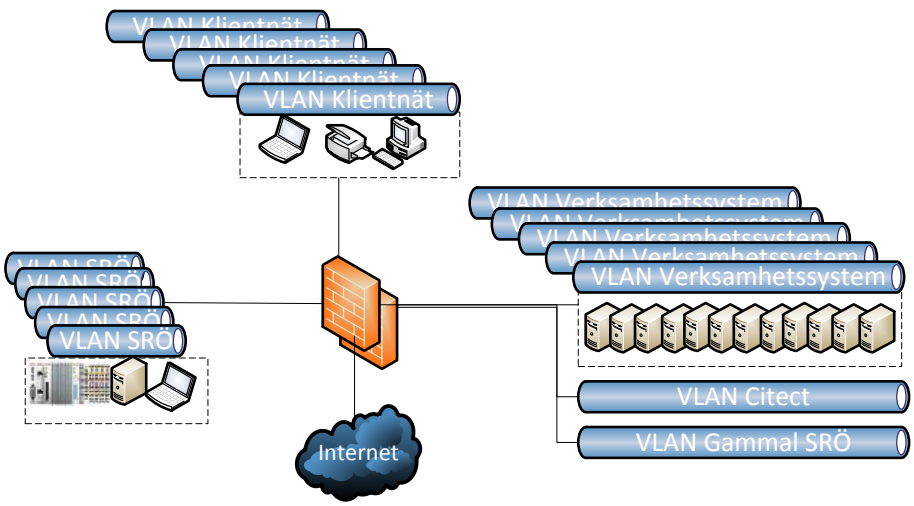
Skulle den centrala styrningen av systemen sluta fungera kan de styras på plats av drift- och fastighetstekniker. Alla funktioner kan fungera autonomt.

B2.2.4 Arkitektur

En översikt av kommunens fysiska IT-arkitektur beskrivs i Figur 7 och en översikt av den logiska arkitekturen i Figur 8. De resterande avsnitten i detta kapitel beskriver komponenterna i dessa figurer.



Figur 7. Fysisk nätverksarkitektur för kommun B.



Figur 8. Logisk nätverksarkitektur för kommun B.

B2.2.4.1 Nätverk

Översiktligt består nätverksarkitekturen i kommunen av tre centrala routrar. På olika platser i kommunen finns det sedan högpresterande nätverksswitchar som vardera är uppkopplade mot två routrar. Dessa nätverksswitchar är konfigurerade för att hantera VLAN-taggad trafik. Olika verksamheter i kommunen är inkopplade i systemet genom egna switchar som i sin tur får den VLAN-trafik som trunkats[21] ut av de högpresterande nätverksswitcharna. Varje port i dessa switchar tilldelas sedan specifika VLAN. De resulterande IP-segmenten konfigureras att tillåtas genom kommunens centrala brandväggar så att de kan erhålla olika IT-tjänster i kommunen såsom e-post och DHCP. Multiprotocol Label Switching (MPLS) är tillämpat i routing-systemet.

De flesta fastigheter, såsom en skola eller en ishall, har flera switchar som allihop får samma VLAN-taggade trafik. Dessa switchar finns i låsta utrymmen i fastigheterna. Fastighetsautomationssystem, såsom en PLC som styr belysningen i en ishall eller värmen i en skola, sitter i så kallade apparatskåp. Invid varje apparatskåp finns ett dubbelt nätverksuttag där utrustningen får den ena porten och drifttekniker som behöver konfigurera utrustningen på plats den andra. Båda portar tillhandahåller samma VLAN. Detta VLAN är tillåtet att kommunicera med Citect-systemet (se senare i detta avsnitt) samt de IT-resurser som behövs för att systemet skall fungera. Då det oftast finns mer än en IP-enhet i varje skåp sätts oftast även en industriswitch i skåpet. Exempel på sådana IP-enheter är PLC:er, PiiGab Mbus-uppsamlingsenheter, och panel-PC:er.

En central servermiljö tillhandahåller de resurser som olika IP-segment i kommunen erfordrar. Dessa tjänster inkluderar exempelvis AD, DHCP, DNS, mailservar, PXE, olika verksamhetssystem, Citect-systemet och ett Citrix Netscaler-system. Denna servermiljö är till större delen virtualiserad (cirka 80 % av alla operativsystem) genom ett antal fysiska VMware vSphere-servrar som exekverar cirka 250 VMware-gästoperativsystem. Exempelvis är både Citrix och Citect virtualiserade. Det finns dock fortfarande ett antal fysiska servrar som är planerade att bytas ut. I synnerhet finns det en mindre datorhall hos fastighetsförvaltningen som innefattar den gamla driftmiljön för fastighetsautomation där Siemens Desigo, TAC Vista, Johnson M5, Johnson MSEA, Honeywell INUvision och Honeywell EBI fortfarande är i drift. Denna driftmiljö finns kvar eftersom många äldre DUC:ar kommunicerar via protokoll som inte är kompatibla med Citect. Exempelvis Local Operating Network (LON), vilket stöds av TAC Vista, men ej av Citect. En delmängd av trafiken till den gamla driftmiljön går via modem. Citect får in en del av informationen från den gamla driftmiljön via konnektorer mot de korresponderande SCADA-

[21] http://www.cisco.com/c/en/us/tech/lan-switching/virtual-lans-vlan-trunking-protocol-vlans-vtp/index.html (hämtad 2016-05-25).

systemen, exempelvis erhåller Citect informationen från DUC:ar uppkopplade mot TAC Vista via Open Platform Communications (OPC).

För att förenkla administrativa sysslor så finns det idag få/inga nätverksadministrativa IT-lösningar ute i fastigheter. Istället tillhandahålls sådana tjänster av den centrala servermiljön. Exempelvis, om en ny dator kopplas in i en skolas labbmiljö så kommer DHCP-servern i den centrala servermiljön att delge den en IP-adress i det designerade VLAN-segmentet. Verksamhetssystem är kontextspecifika applikationer såsom faktureringssystem och intranäts-applikationer. Citrix tillhandahåller fjärraccess till olika delar av kommunens IT-miljö. Autentiseringen i Citrix görs genom uppslag mot kommunens AD-system. Det finns dock undantag från denna lösning. Exempelvis så får användare av ett av de äldre styrsystemen access till detta genom remote desktop. En speglad version av denna servermiljö finns på en annan plats. Det görs periodvisa tester för att säkerställa att denna speglade miljö kan ta över om den primära av någon anledning inte fungerar. Vissa äldre system är dock inte med i dessa tester (t.ex. det gamla fastighetsautomationssystemet).

Citect-systemet finns på två VLAN i servermiljön. Detta system används av drifttekniker för att övervaka och styra över tillståndet för olika fastighetssystem. Det ena VLAN:et innefattar en Structured Query Language (SQL)-server och en klientserver; det andra innefattar en huvudserver, en Input/Output (I/O) server och en test- och utvecklingsserver. En användare som vill interagera med SCADA-systemet loggar in på klientservern via Citrix, varifrån det är möjligt att kommunicera med huvudservern. Huvudservern kommunicerar i sin tur med I/O-servern som pratar med olika fastighetsautomationssystem såsom datoriserade undercentraler (DUC) och Programmable Logic Controllers (PLC). Utöver kommunikationen med den gamla styrsystemsmiljön går kommunikationen mellan fastighetsautomationssystem och Citect-systemet primärt via trådad IP-trafik, men det förekommer trådlös IP-kommunikation via 3G-routers. I dessa fall sker kommunikationen via en centralt placerad VPN-gateway från Telenor. Ett antal olika styrsystemsprotokoll utnyttjas, dock främst OPC, Modbus TCP, BacNet och M-bus. Olika fabrikat har dessutom egna drivrutiner för dessa protokoll.

B2.2.4.2 Mjukvara

Den virtualiserade servermiljön består av ett antal fysiska serverar som kör VMware vSphere, vilket införskaffades för något år sedan. Denna miljö har en blandning av gästoperativsystem, framförallt i form av Windows Server 2008 och nyare, men även Red Hat, Ubuntu och Solaris. Vissa av dessa operativ-system tillhandahåller generella IT-lösningar som DHCP, DNS, AD och PXE; andra tillhandahåller mer specialiserade lösningar såsom Citect-systemet, Citrix Netscaler och ekonomisystem. Citect-komponenterna är installerade i en Windows Server 2008 R2-miljö. Datorhallen som hanterar kontakt med äldre

utrustning (DUC:ar) är inte virtualiserad och består av sex datorer med operativsystem från Windows XP och Windows Server 2003 till Windows Server 2008. Uppdatering av servrar görs vid behov manuellt genom inloggning mot varje server. Installation och drift av dessa system görs främst av IT-enheten på kommunen, men det förekommer tillfällen då externa konsulter nyttjas. Exempelvis installerade konsulter Citrix Netscaler-systemet.

Datorer i klientmiljön bygger på en standardimage av Windows 7 som levereras via PXE. PXE-lösningen är inställd på att kräva lösenord för att installera en ny image. Specifika detaljer kring PXE-processen var dock utanför respondenternas ansvarsområden. Mjukvaruinstallation är per default avstängt på dessa maskiner; detta sker via sannolikt via en policy i AD:t.

Det pågår ett arbete för att konsolidera vilka typer av inbyggda system som används för fastighetsautomation, såsom DUC:ar och PLC:er. Fördelningen mellan dessa är cirka 80 % DUC:ar och 20 % PLC:er, men denna fördelning förändras långsamt då alla nya enheter som köps in är PLC:er (vilka kan kopplas upp mot Citect). De vanligaste PLC-fabrikaten som används är Saia, Beckhoff och Mitsubishi. Arbetet med att byta ut gamla DUC:ar är omfattande - en studie av kommunen under 2012 visade att det behövde bytas ut cirka 900 av 1550 DUC:ar samt integrera cirka 4300 bilder[22] i Citect för att komma ifatt det eftersatta underhållet på fastighetsautomationen. Sedan 2012 har cirka 230 DUC:ar bytts ut och 1400 bilder integrerats i Citect.

B2.2.4.3 Hantering av behörigheter

Kommunen har cirka 24000 anställda, varav ungefär 15000 behöver rättigheter till kommunens IT-system. Av dessa har drygt 50 access till Citect. Sedan finns det ytterligare cirka 50 externa användare (t.ex. besiktningsmän och funktionsentreprenörer) som har behörigheter i Citect. Hantering av de korresponderande rättigheterna görs av ett par heltidsanställda i kommunen. Detaljerad information om denna process var utanför respondenternas vetskap, men det är självfallet ett omfattande arbete att hantera alla roller, grupper och behörigheter av olika slag som behövs för kommunens många anställda.

Behörighetssystemen för de allra flesta IT-system i kommunen är kopplade mot AD:t, vilket innebär att en inloggning mot AD:t även ger autentisering mot andra system. I fallet med Citect, som har ett eget behörighetssystem, skapas unika behörigheter för varje användare som skall ha access till det. När en användare sedan loggar in med sitt ”vanliga” användarnamn och lösenord mot AD:t sker ett

[22] Mjukvarumoduler till Citect som realiserar grafisk styrning och övervakning av en särskild typ av fastighetsautomationssystem.

uppslag mot motsvarande behörigheter i Citect. Därmed räcker det med att en användare minns sina logginuppgifter för Windows-domänen.

Anställda kan erhålla lokala administratörsrättigheter om de har behov och fyller i en särskild digital blankett. Det är dock sällan detta sker i praktiken.

B2.2.4.4 Teknisk monitorering och övervakning

Det som passerar brandväggar loggas. Det är dock oklart för respondenterna vad exakt som loggas och hur saker följs upp. Även förändringar i styrningen av systemen i Citect (t.ex. värden för värme och ventilation) loggas.

B2.2.4.5 IT-säkerhetsrelevant träning och utbildning

Det finns ingen särskild IT-säkerhetsträning för personal inom kommunen, oavsett roll.

B2.2.4.6 Säkerhetstester

Respondenterna kunde komma på ett penetrationstest som genomförts. Detta involverade en hotmodell i form av externa aktörer som skulle försöka hitta konfigurationsfel i de centrala brandväggarna. Dessa externa aktörer misslyckades med sitt intrångsförsök.

B2.2.5 Övriga reflektioner

Kommunen har en systemförvaltningsmodell (På Maintenance Management Model, PM3) som används av systemförvaltare. I fallet Citect har det dock ännu inte rekryterats/utsetts någon förvaltare. Det finns även ett glapp mellan de som har god IT-kunskap och de som har god OT-kunskap som skulle behöva bryggas.

Bortsett från IT-egenskaper bedömer respondenterna att det finns en stor besparingspotential med rätt konfigurerade fastighetsautomationssystem. Det gäller huvudsakligen tidsstyrning och av ventilationsaggregat som skulle kunna stängas av under lov. Detta skulle kunna hanteras på ett enkelt sätt genom Citect.

B2.3 Kommun C

B2.3.1 Respondent

En intervju om cirka en timme utfördes med respondent R5 i kommun C.

Respondent R5 arbetar på IT-avdelningen i kommun C. R5 har en bakgrund från den tekniska sidan. Till 20 % arbetar respondenten med säkerhetsfrågor i ett nationellt informationsnätverk.

B2.3.2 Organisation

I kommunen finns två kommunala fastighetsbolag som ansvarar för fastighetsautomationen. Ett av bolagen (FB1) har mest företag som hyresgäster medan det andra (FB2) har många privata hyresgäster. IT-avdelningen har inte så mycket med FB2 att göra utöver att kommunen hyr en del lokaler av dem. Dessutom tillkommer kommunens räddningstjänst, vilka nyttjar kommunens IT-system på ungefär samma sätt som FB1.

R5 har ansvar för installation och drift. Inköp sköts av fastighetsbolagen. IT-avdelningen ser till att alla SRÖ-komponenter har möjlighet att kommunicera med de resurser som de behöver kommunicera med (t.ex. för öppning av portar i brandväggar samt tilldelning av IP-adresser). Det är upp till FB1 och FB2 att hantera själva SRÖ-komponenterna.

Ett stort ansvar för IT-avdelningens är att ansluta enheter (en enhet = en fysisk plats) till kommunens nätverk. Det finns ungefär 200 sådana enheter som är anslutna.

B2.3.3 Fastighetsautomation

R5 ser från sin IT-roll ingen skillnad på systemen utifrån deras funktion (t.ex. värme eller ventilation). R5:s ”kunder” talar om vad det är för system som ska kopplas in (dessa registreras i en databas) och vilka kravnivåer som ska uppfyllas. Funktionsperspektivet syns inte.

Fastighetsbolagens ansvar inkluderar värme, fläktar och brandlarm medan hyresgästerna ansvarar för funktioner som passersystem, kameror och inbrottslarm. Om hyresgästen är kommunal så kan den använda sig av kommunens nät. Privata hyresgäster har egna nät.

R5 nämner ytterligare funktioner som finns men kanske inte bör räknas som fastighetsautomation: elladdstolpar, belysningsstyrning, solcellspaneler, informationsskärmar, kameraövervakning och bensinpumpar.

Kommunen har ingen strategi för vilken typ av system man vill ha i framtiden. FB1 och FB2 har påpekat svårigheten med att de inte kan ange krav på systemleverantörer vid stora upphandlingar, däremot kan de ställa krav på funktioner. Som det är idag anpassar FB1 och FB2 varje lösning mot varje enskild fastighet som skall byggas eller moderniseras. Detta gör att det finns en stor flora med olika typer av komponenter som pratar olika protokoll. Denna mångfald har konkret inneburit att kommunen behöver flera olika styr- och övervakningssystem körandes parallellt. Idag finns det fler än sex olika styr- och övervakningssystem för fläkt och ventilation i kommunen. Dessa inkluderar även övervakningsfunktioner för brandvarnare och till viss del värme. FB1 och FB2 delar inte system, även om de i vissa fall hade haft möjlighet att göra så. Det är sannolikt att de överlappar i sina SCADA-lösningar.

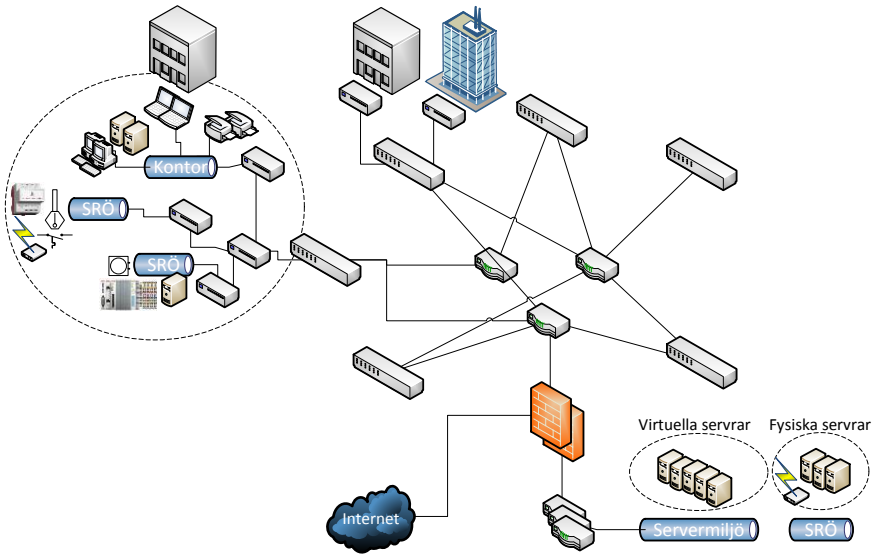
En stor skillnad mellan FB1 och FB2 är att FB1 till fullo nyttjar kommunens IT-system, t.ex. finns deras SCADA-system i kommunens servermiljö. FB2 utnyttjar endast kommunens grundläggande tjänster och har alla SCADA-servrar hos sig.

Att det finns så många olika typer av system ställer till svårigheter, både för IT-avdelningen som ska hantera (hosta) servrar och uppdatera (patcha) dem och för teknikerna som arbetar konkret med systemen och som måste lära sig skillnaden mellan dem. IT-avdelningen skulle önska att vissa system kunde fasas ut, men bolagen har inte samma inställning.

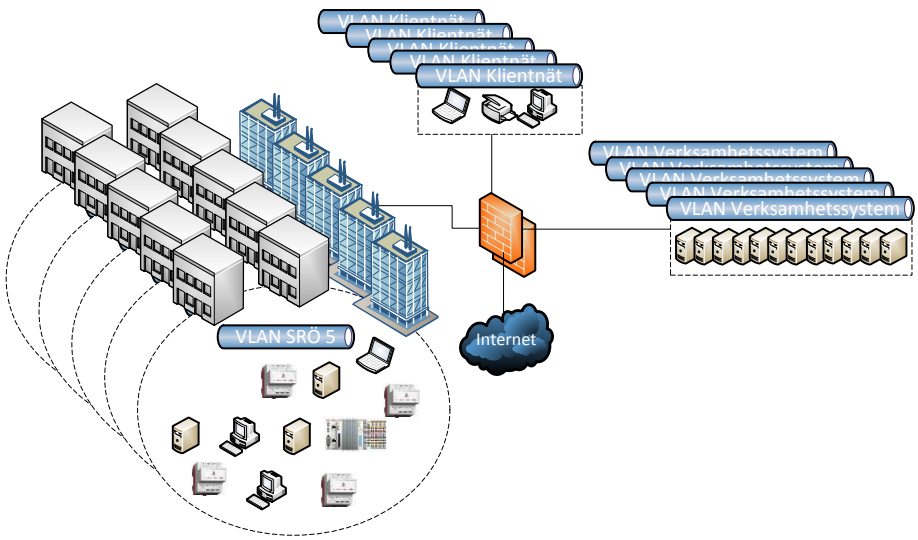
Fastighetsautomationssystemen uppdateras av entreprenörer, inte av IT-avdelningen. Systemen inom kommunen har mycket olika ålder. En del är hyfsat nya, andra väldig gamla. Respondenten beskriver utvecklingen av systemen som ”sen”.

B2.3.4 Arkitektur

En översikt av kommunens fysiska IT-arkitektur visas i Figur 9 och den logiska i Figur 10. De resterande avsnitten i detta kapitel beskriver komponenterna i dessa figurer.



Figur 9. Fysisk nätverksarkitektur för kommun C.



Figur 10. Logisk nätverksarkitektur för kommun C.

B2.3.4.1 Nätverk

Fysiskt bygger kommunens nätverkstopologi på fem ringar av fiber, som alla är sammankopplade till två par av CISCO-routrar och Fortigate-brandväggar (där ett par är aktivt och ett annat passivt/redundant). Dessa ringar dras till fastigheter som skall kopplas in i fibernätet. Fibernätet ägs och driftas av energibolaget som därigenom blir en viktig aktör. Nästan all kommunikation (cirka 99 %) går genom fiber, vilket gör energibolaget till en viktig aktör.

Logiskt sköts all routing via OSPF. Separation genomförs primärt via VLAN, där alla fastighetsautomationskomponenter på varje fiberring delar på ett VLAN. IP-adresser äskas från IT-avdelningens centrala servermiljö. För klientdatorer (t.ex. en datorsal i en skola) görs detta via centrala DHCP-servrar som tilldelar adresser på ett klass C-nät. För DUC:ar och liknande i fastighetsautomationssystemet görs detta via statiska IP-adresser. Brandväggarna konfigureras manuellt för att tillåta olika IP-slingor att prata mot olika delar av server-miljön. Två personer har ansvar för att underhålla dessa brandväggar, vilket kräver omfattande manuellt arbete.

Kommunen har två serverhallar som befinner sig på olika platser inom samma fastighet. Den ena serverhallen är byggd ”enligt konstens alla regler”, och inkluderar t.ex. en Uninterruptible Power Supply (UPS), dieselaggregat och reservkyla. Denna datorhall har det ena paret av kommunens core-routrar och brandväggar, samt kommunens olika verksamhetssystem. Den andra serverhallen innehåller kommunens andra par av core-routrar och brandväggar, samt diverse datalagring. Det genomförs ibland tester av denna redundans, men R5 tycker att det görs lite för sällan.

SRÖ-komponenter inom fastigheter sitter i apparatskåp som befinner sig inom låsta utrymmen. Dessa har antingen en eller två accessportar som går till en central switch i varje fastighet. Oftast är detta inte en industriswitch. Denna switch kopplar sedan upp fastigheten till kommunens IT-nätverk.

Fjärraccess är möjlig på två huvudsakliga sätt. Dels via en applikation kallad Mobility Guard, vilken möjliggör access av webb-baserade verksamhetssystem såsom intranätsapplikationer, e-post och filhanteringsapplikationer. Det är även möjligt via VPN. Ett fåtal kritiska användare har access till valfritt VLAN. Personal på FB1 har fjärraccess till sina egna servrar. Autentisering beror på system; det nyttjas både en-faktor och två-faktorautentisering.

R5 har ingen större koll på vilka protokoll som används av fastighets-automationssystemen, mer än att det finns ett stort antal olika och att det mesta är TCP/IP-baserat.

B2.3.4.2 Mjukvara

Kommunens primära serverhall är till huvudsak virtualiserad genom VMware vSphere, vilken exekverar cirka 200 virtuella maskiner. Dessa kör nästan bara Windows-baserade operativsystem från Windows Server 2008 och framåt. Traditionella IT-system såsom DHCP, e-post, PXE, File Transfer Protocol (FTP), mailservrar samt verksamhetssystem finns på dessa maskiner. Det finns även mellan 30 och 40 fysiska servrar i den primära datorhallen. Servrarna inom fastighetsautomationssystemen sitter huvudsakligen här. Windows är dominant även här (huvudsakligen Windows Server 2008 och framåt). Det finns överlag väldigt få Linux-baserade servrar. Den sekundära datorhallen har väldigt få servrar, utan mest redundans för nätverkskomponenter.

Klientdatorer installeras via PXE-boot. PXE-processen initieras dock inte per automatik när en ny komponent ansluts till nätverket, utan görs manuellt av IT-avdelningen vid behov (t.ex. vid förberedelse av en ny dator till en anställd). Nya datorer levereras med en Windows 7-baserad lösning.

Mjukvarupatchning av operativsystem görs via interna Microsoft-patchservrar inom kommunen. I server-miljön används en kombination av automatiskt och manuellt arbete med patchning. Eftersom det nästan bara handlar om Windows-datorer görs patchningen huvudsakligen när Microsoft släpper nya patchar (vid en så kallad ”Patch Tuesday ”). Mjukvarupatchning av fastighetsautomations-systemen för FB1 görs av FB1 samt de respektive entreprenörerna. Uppdatering av klientsidan görs automatiskt.

R5 är osäker på exakt vilka typer av SRÖ-komponenter som nyttjas, mer än att det finns väldigt många olika varianter. Det finns dock möjlighet att ta reda på sådan information då IT-avdelningen begär information om (samt registrerar) alla SRÖ-komponenter som är inkopplade i kommunens nätverk.

B2.3.4.3 Hantering av behörigheter

Kommunen har ett centralt AD-system som hanterar IT-behörigheterna för kommunens anställda.

Tillägg av nya behörigheter är en semi-automatisk process, där nya behörigheter läggs till baserat på information i kommuns personaldatabas.

Lokala administratörsprivilegier hanteras på lite olika sätt beroende på roll. På skolsidan finns det inga direkt restriktioner mot att skaffa sådana behörigheter, medan ingen på den IT-administrativa sidan bör ha lokala administratörs-behörigheter.

B2.3.4.4 Teknisk monitorering och övervakning

Det finns en person som har ansvar för att övervaka loggar som skapas av brandväggar. T.ex. uppmärksammas det här när kommunen utsätts för Distributed Denial of Service (DDOS)-attacker. Accessloggar för servrar undersöks även ibland.

B2.3.4.5 IT-säkerhetsrelevant träning och utbildning

En grundläggande utbildning kring IT-säkerhet ges i samband med kommunens introduktionsutbildning. Denna utbildning krävs för att få ett användarkonto.

B2.3.4.6 Säkerhetstester

Det har genomförts en övergripande IT-revision hos kommunen. Denna innefattade dock ej fastighetsautomationssystemet.

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