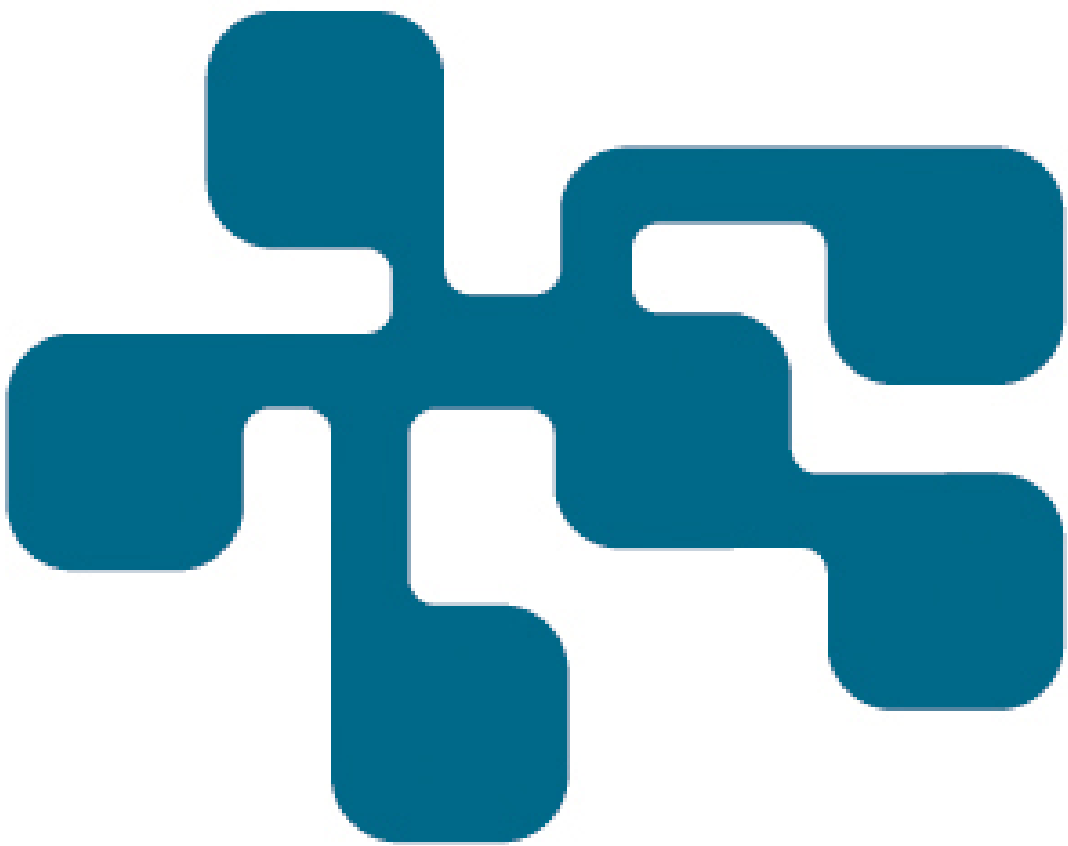
NCS3 - Översikt över arbetet med cyberfysiska system på kommunal nivå

FREDRIK MALMBERG ANDERSSON,
ANN-SOFIE STENÉRUS DOVER

FOI
MSB



FOI-R--4370--SE
MSB 2016-1196
ISSN 1650-1942

December 2016

Fredrik Malmberg Andersson, Ann-Sofie Stenérus Dover

NCS3 – Översikt över arbetet med cyberfysiska system på kommunal nivå

FOI-R--4370--SE
MSB 2016-1196

Titel	NCS3 Studie – Översikt över arbetet med cyberfysiska system på kommunal nivå
Rapportnr/Report no	FOI-R--4370--SE
Månad/Month	December
Utgivningsår/Year	2016
Antal sidor/Pages	29
ISSN	1650-1942
Kund/Customer	Myndigheten för samhällsskydd och beredskap
Forskningsområde	5. Krisberedskap och samhällssäkerhet
Projektnr/Project no	E13538
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Denna studie genomfördes i syfte att få fram en bild över vilken hjälp kommuner ser som relevant i sitt arbete med att hantera cyberfysiska system inom kommunens verksamhet (inkluderande begrepp för digitala system som styr fysiska processer såsom industriella informations- och styrsystem, SCADA, styr- och reglersystem, och dylikt).

Ett antal tjänstemän (chefer inom IT och informationssäkerhet, säkerhetssamordnare med flera) i kommuner intervjuades kring hur kommunerna arbetar i dag med de cyberfysiska systemen, och var inom det cyberfysiska området de ser behov av hjälp och stöd. Resultatet visar på en varierande grad av överblick och kontroll inom området.

Överlag noteras hjälp i form av guider, checklistor, mallar och konkreta exempel som värdefullt. Ett förslagsområde rör sig kring stöd för att kunna kartlägga de cyberfysiska systemen inom kommunen så att man känner att man gör detta på ”rätt” sätt. Ett annat område handlar om stöd i upphandlingen av system. Vad gäller upphandling verkar det variera hur man upplever situationen. En del ser inga problem med detta medan en del noterar att det kräver stor juridisk och teknisk kompetens, och efterlyser konkret stöd inom detta område. Ytterligare ett område där konkret stöd ses som relevant är inom hur man strukturerar upp sin cyberfysiska miljö på bästa sätt. Även stöd i att få högre ledning att ägna mer fokus åt området nämns. (En heltäckande lista över stödinsatser som nämndes som relevanta/intressanta återfinns i bilaga B).

I rapporten finns en lista över identifierade typer av cyberfysiska system. Denna lista kan förslagsvis användas vid en inventering i den egna kommunen. Dessutom listas ett antal diskussionspunkter som kan användas som stöd för att komma igång med tankearbete, kartläggning och strukturarbete med de cyberfysiska systemen.

Nyckelord:

cyberfysiska system, scada, industriella informations- och styrsystem, digital undercentral

Summary

The purpose of this study was get an overview of what assistance Swedish municipalities would consider relevant in their work towards proper management of the cyber physical systems within their domain. The term “Cyber physical systems” is here used as an including term for digital systems that controls physical processes. Examples of these systems are industrial information- and control systems, SCADA et cetera.

A number of municipality managers within IT-, information security and security coordination was interviewed regarding the current status of their work with the cyber physical systems. The results indicate notably varying degrees of structure and process maturity.

There seems to be a general desire for help and assistance through means such as guides, check lists, templates and concrete hands-on examples. One specifically noted area is help with mapping of the municipality’s cyber physical systems and infrastructure so that actors could get a verification that they are conducting this activity in a correct manner. Another noted area where help would be relevant is about tendering processes. Some municipalities sees the tendering process as a cost and a barrier that requires great judicial and technical skills, while others consider it to be of no bother at all. Other noted areas where help would be appreciated regards how to structure the cyber physical environment according to some sort of best practice, and how to get upper management to increase focus on cyber issues. The complete list of help noted as relevant can be found in appendix B.

Key terms:

cyber physical systems, scada, industrial information- and control systems, duc

Innehållsförteckning

1 Inledning

1.1 Bakgrund

Sverige är indelat i 290 kommuner med stor spännvidd vad avser bland annat invånarantal, geografisk yta och organisation. De har mycket olika förutsättningar att arbeta med frågor som handlar om säkerhet i industriella informations- och styrsystem, samtidigt som många av dessa system är viktiga för kommunala verksamheter som vatten och avlopp, eldistribution, värme, fastighetsautomation. En enkätundersökning om kommunernas informationssäkerhetsarbete som Myndigheten för samhällsskydd och beredskap (MSB) genomförde under våren 2015 visade på mycket stora skillnader mellan olika kommuner i hur man såg på säkerhetsansvaret för egna IT-system, och för IT-system vars drift låg inom kommunalt ägda bolag.[1]

Denna studie genomförs på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB) inom ramen för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3).[2]

1.2 Syfte och mål

Syftet med studien är att ge en bild av hur arbetet med cyberfysiska system (se kapitel 1.4 för resonemang kring begreppet) bedrivs inom kommunerna idag för att ge underlag till MSB för att utforma ett ”hjälp-till-självhjälpskit”.

I målet ingår att undersöka vilken form av stöd, och på vilket format, kommunerna ser att MSB skulle kunna bidra med i arbetet med hanteringen av cyberfysiska system. (Som tidigare nämnts, ett generöst begrepp som inkluderar bland annat industriella informations- och styrsystem)

1.3 Genomförande

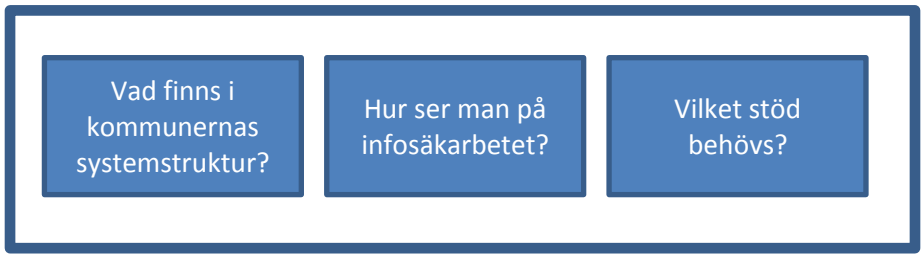
Inom ramen för studien genomfördes sex intervjuer med representanter för sju kommuner (där två av kommunerna delar IT/Säk-verksamhet av resursskäl), Kommunernas personal har varit positivt inställda till att bidra med information

[1] MSB-publikation. ”En bild av kommunernas informationssäkerhetsarbete 2015”. Publ.nr MSB943

[2] NCS3 är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsaspekter inom industriella informations- och styrsystem. Centrumet är ett samarbete mellan FOI och MSB och ingår i MSB:s program för ökad säkerhet i industriella informations- och styrsystem

men är samtidigt överlag tydligt belastade av mycket arbete. Kommunerna var alla utom en (som var större) i storleksordningen 5.000–50.000 invånare. De personer som intervjuades i kommunerna hade titlar som IT-chef, Driftsansvarig, Informationssäkerhetschef, Säkerhetssamordnare, Säkerhetschef, IT-avdelningschef, IT-arkitekt och IT-strateg.

Intervjuerna strukturerades utifrån tre områden i syfte att dels få ut den information som eftersöktes och dels få fram ett underlag som kunde indikera nulägesnivån för kommunerna avseende arbetet inom det cyberfysiska området. Intervjuerna strukturerades enligt följande block med diskussionspunkter.



1.3.1 Resonemang kring tillvägagångssätt

Projektet diskuterade initialt med en kommunal IT/säk-relaterad chef angående vilka som kan vara lämpliga att intervjua för att få en övergripande bild av kommuners arbete och situation inom området cyberfysiska system. Det visade sig att för den övergripande kommunbilden ansågs det lämpligt att intervjua folk med rollbeskrivningar som t.ex. kommunens IT-chef, IT-/säkerhetschef och liknande. Intervjuade personer med dessa roller har kunnat ge en bild av hur man från kommunens sida ser på, och arbetar med området, vilken riktning kommunen har och vilka behov kommunen har. Under vissa av intervjuerna har de varit understödda av personal från den operativa IT-verksamheten.

Mellan kommunerna varierar det avseende vilka cyberfysiska system som driftmässigt ligger var, och vilken överblick och kontroll man därmed har över strukturerna och systemen. En del system ligger i kommunala bolag och en del i kommunregi, dvs. de kommunala förvaltningarna ansvarar för drift och underhåll.

För att få en lite bredare bild har projektets ambition varit att få till stånd intervjuer med representanter för kommuner av varierande storlek. I denna ambition har utfallet berott på kommunrepresentanternas möjligheter att avsätta tid för intervjuer.

En aspekt som är tydlig inom området är att många frågor kan vara känsliga ur ett säkerhetsperspektiv. Projektet har inte upplevt några hinder utifrån detta men det

är ändå värt att vara medveten om att det kan finnas information som pga. känslighet inte har förmedlats.

Intervjuerna har varit semistrukturerade och i regel genomförts över telefon. Ett underlag med frågor skickades ut till intervjuobjekten i förväg. (Se bilaga A.)

1.4 Disposition

Kapitel 1 ger syfte och bakgrund till studien. I kapitel 2 diskuteras hur de intervjuade kommunerna arbetar med cyberfysiska system i nuläget, och var de befinner sig mognadsmässigt. I detta kapitel presenteras även en lista över olika typer av cyberfysiska system som kan falla inom ramen för det kommunala. I kapitel 3 återges hur kommunerna ligger till avseende säkerhetsarbetet kopplat till de cyberfysiska systemen. Kapitel 4 går vidare med att lista ett antal specifika förslag på hjälp som kommunerna ser skulle vara relevant. Slutligen nedtecknas en kort slutsats tillsammans med förslag på hur man kan ta resultaten vidare.

1.5 Begrepp och avgränsningar

I intervjuerna har termen *cyberfysiska system* använts som ett paraplybegrepp för alla former av digitala/IT- system som i slutändan styr någon form av fysisk process. Detta förhållningssätt har anammats för att inte begränsa respondenterna till en terminologi eller ett förhållningssätt som visserligen må vara stringent och ”korrekt”, men som kanske inte nödvändigtvis återspeglar deras verklighet, och kanske heller inte låter dem uttrycka de behov de ser inom sina verksamheter. Inom ramen för detta mer inkluderande begrepp har intervjupersoner omväxlande använt termer som t.ex. SCADA (Supervisory Control and Data Acquisition), styrsystem, ICS (Industrial Control Systems), SRÖ (Styr, Regler och Övervakning), Duc:ar (datoriserade undercentraler) och till och med i vissa fall diskuterat möjligheter med ”internet of things” i samband med vård av äldre i hemmet. I denna rapport används termerna omväxlande för att återspegla den terminologi som användes vid diskussionerna. Begreppet ”cyberfysiska system” är inte något begrepp som framträtt som det allena rådande hos kommunerna.

Övrigt arbete med informationssäkerhet, som inte rör cyberfysiska system (till exempel integritetsproblem i administrativa system) inkluderas inte i studien.

1.6 Målgrupp

Målgruppen för studien är sedan tidigare i ämnet insatta personer med intresse för ett kommunperspektiv på hur man jobbar med bland annat säkerhet i cyberfysiska system och vilket typ av stöd kommunerna ser skulle vara relevant och givande.

2 Cyberfysiska system i kommuner

Vilka system räknar kommunerna som ”cyberfysiska”? Hur ser det ut rent allmänt i kommunerna inom området? Har de väl kartlagda strukturer eller återstår detta att få till? Hur jobbar man med säkerhetsaspekter, säkerhetsklassning och dylikt? Nedan sammanfattas de diskussioner som förts under intervjuerna. De som intervjuats har målat upp ungefär samma bild med avseende på områdets mognad i kommunerna just nu. De ger ungefär samma bild av att området kan utvecklas mer för att hamna på samma mognadsnivå som mer traditionella områden som t.ex. IT-säkerhet avseende hur bra överblick man har, och hur väl strukturerat och säkerhetsmedvetet området/systemen är både i praktik och teori.

Beroende på var man drar gränsen för vad som ingår i ”cyberfysiska system” kan listan göras mer eller mindre omfattande för vilka system som kan påträffas i en kommun. Nedan följer en sammanställning av de system som de intervjuade kommunrepresentanterna själva anser falla in under begreppet cyberfysiska system. Systemen är sorterade utifrån de kommunala ansvarsområden inom vilka systemen används. Rubrikerna/indelningen för de kommunala ansvarsområdena har tagits fram genom att sammanfoga de kommunala ansvarsområden som tre olika kommuner (Örebro, Botkyrka och Ängelholm) beskriver på sina hemsidor. Dessa kommuner har inte varit med i undersökningen annat än att områdesindelningarna i nedanstående lista inspirerats av hur desamma presenterats på deras hemsidor.

Skola och barnomsorg

- Fastighetsautomation (system för värme/kyla, ventilation, hissar, belysning)
- System för (kamera)övervakning och larm, inkl. trygghetslarm
- System i storkök
- Datanätet (routrar, switchar, trådlösa noder mm.)

Social omsorg, vård av äldre och funktionshindrade

- Fastighetsautomation (system för värme/kyla, ventilation, hissar, belysning)
- System för (kamera)övervakning och larm, inkl. trygghetslarm
- System i storkök
- Medicinska system

- Datanätet (routrar, switchar, trådlösa noder mm.)

Underhåll av kommunala gator och parker

- System för belysning (trafikbelysning mm.)
- Datanätet (routrar, switchar, trådlösa noder mm.)

Lokal och regional trafik

- System för dörrar/bommar/företräde i lokaltrafik
- Datanätet (routrar, switchar, trådlösa noder mm.)

Fritid, idrott, kultur, ungdom

- Fastighetsautomation (system för värme/kyla, ventilation, hissar, belysning)
- System för reglering av klorhalt i simbassänger
- Datanätet (routrar, switchar, trådlösa noder mm.)

Kommunhusrelaterade aktiviteter (Socialtjänst, Försörjningsstöd, Miljö- och hälsofrågor, Plan- och byggfrågor, Bostadsfrågor, Civilförsvar, Bibliotek)

- Fastighetsautomation (system för värme/kyla, ventilation, hissar, belysning)
- System för (kamera)övervakning och larm, inkl. trygghetslarm
- Skalskyddssystem av olika slag, in- och utpassering
- Datanätet (routrar, switchar, trådlösa noder mm.)

Produktion och distribution av vatten och avlopp (biogas, el, fjärrvärme*)

- System för styrning, reglering och övervakning av processer
- Fastighetsautomation (system för värme/kyla, ventilation, hissar, belysning)
- System för (kamera)övervakning och larm, inkl. trygghetslarm
- Skalskyddssystem av olika slag, in- och utpassering
- Datanätet (routrar, switchar, trådlösa noder mm.)

Övrig kommunal verksamhet:

Hamnbolag

- Skalskyddssystem av olika slag, in- och utpassering

Ingen av kommunerna har någon centralt fastställd lista över vilka cyberfysiska system som finns och de säkerhetsaspekter som är relevanta. De dokument som finns avhandlar inte specifikt säkerhet i informations- och styrsystem/cyberfysiska system, utan är mer traditionellt IT-säkerhetsinriktade. Behovet av att kartlägga och ta fram helhetsbilden, med beroenden och kopplingar, är identifierat hos de intervjuade. Överlag framträder bilden av att området cyberfysiska system ännu inte fått det fokus och de resurser som de andra mer etablerade områdena som t.ex. traditionell IT har. Detta kan delvis förklaras av att kunskaperna på alla håll ännu inte nått full mognad.

De mer traditionella IT-systemen är i högre grad analyserade ur ett säkerhetsperspektiv ute hos kommunerna. Vid diskussioner kring de cyberfysiska systemen framkom att IT-avdelningarna blir mer och mer inblandade i hanteringen i och med en ökande grad av digitalisering och uppkoppling, speciellt vid utbyte av gamla komponenter. Arbetet med att säkerhetsklassificera system är ingalunda komplett, utan påbörjas och pågår.

Utifrån studiens resultat ges att en del verksamhet med inslag av cyberfysiska system i varierande grad bedrivs i kommunala bolag. Exempel på sådan verksamhet som oftast verkar ligga i kommunala bolag är vatten och avlopp, energi samt fiber/internet. Hos en del av kommunerna ligger även hanteringen av bostäder och fastigheter i kommunala bolag.

För den verksamhet som ligger ute på kommunala bolag har kommunens centrala IT-funktion generellt mindre insyn i strukturer, teknik och säkerhet etc. gällande de cyberfysiska systemen. Där ligger utförandeansvaret, och säkerhetsansvaret, på de enskilda bolagen. Dock ses, som nämnts tidigare, en trend att den centrala IT-funktionen blir mer och mer inblandad i övriga verksamheters IT/cyberfysiska-aspekter i och med att ”allt” inom kommuner blir mer och mer ihopkopplat för varje ny uppgradering som sker i verksamheter. Kommunen får sakta mer komplett bild över system, accesser och strukturer överlag.

Exempel på en lite ovanligare lösning är en kommun som lagt ut vissa verksamheter på kommunala bolag men som fortfarande driftar själva systemen. På så vis har de fortfarande kontroll och överblick över IT-miljön på ett tillfredsställande sätt. Denna kommun har dessutom ett nyframtaget analysverktyg som ska användas för att analysera och hålla koll på systemen i kommunen.

Något som också framkommit är synen på möjligheter med en ökad grad av ”cyberfysifiering”/digitalisering i kommunernas verksamheter. Som exempel nämns ”internet of things” och möjligheterna att med hjälp av olika typer av sensorer effektivisera och underlätta t.ex. hemvård av äldre. I en kommun håller de t.ex. på att sätta upp ett nät som är förberett för att kunna kopplas in och användas som ”välfärdsnät” för att underlätta ett flexibelt stöd till de äldre. Dock

noterar de att det finns en del säkerhetsaspekter som blir högst aktuella vid denna utveckling.

I och med utveckling som ovan noterades kan IT-funktionen få ett större ansvar och uppdrag inom den cyberfysiska arenan, och säkerhetsfrågor i samband med området cyberfysiska system/styrsystem kan få ett större fokus från ledningen. Huruvida IT-avdelningarna ute i landet har kapacitet att ta sig an en ökad arbetsbörda i form av hantering även av cyberfysiska system går ej att utröna ur de svar som framkommit i denna studie. Det som säkert kan sägas är att ett antal av de som intervjuats uttryckt att de ser behovet av ökat fokus men inte fått fullt genomslag i ledningen för frågorna avseende fokus och resurser.

I samband med intervjuerna fick kommunrepresentanterna frågan om de såg några utmaningar, brister eller behov kopplat till privata bolag inom kommunens gränser med cyberfysiska system. Svaren var antingen att kommunerna inte såg att det fanns några relevanta privata bolag ur det perspektivet, eller att kommunerna inte visste hur bolagen i så fall arbetade med sina cyberfysiska system. Privata bolag, och deras hantering av cyberfysiska system, verkar inte vara någon prioriterad fråga ur kommunens perspektiv. I ett teoretiskt fall då privata bolag bedriver verksamhet som kan anses kritisk för kommunens möjlighet att erbjuda invånarna den service de förväntar sig, skulle det kunna tänkas vara av yttersta vikt att man verkligen kontrollerat att säkerhetsarbetet har det fokus som behövs för att i möjligaste mån säkra driften.

3 Säkerhetsarbete i kommunerna

Säkerhetsmognaden och arbetet med cyberfysiska system varierar mellan systemen i den enskilde kommunen så väl som mellan kommunerna. En kommun menade att det varierar så pass mellan olika verksamheter att det inte går att ge något enhetligt svar på frågor kring roller och ansvar, behörigheter, sekretessavtal, riktlinjer för lösenord och beställningar etc. De cyberfysiska systemen, med sina mekaniska och elektroniska komponenter, kan också vara lite äldre än de ”rena” IT-systemen och därmed inte erbjuda samma möjligheter till inbyggd kontroll av behörigheter, loggning osv. Där har man löst det genom att lägga dessa system i egna nät med skal byggt runt om. När de äldre lösningarna byts ut och uppdateras blir de ofta mer digitaliserade och uppkopplade vilket innebär mer inblandning av IT-funktionerna och mer möjligheter till att bygga in IT-säkerhet från grunden. Uppdateringar och moderniseringar kommer även mer och mer med önskemål om mobila lösningar vilket ger ett nytt fokus på säkerhetstänk.

Överlag verkar det inte vara vanligt att kommunerna anser sig ha processer på plats för att kartlägga sina cyberfysiska system. Snarare är det så att det tillhör undantagen att man har kommit så långt så att man har kartlagt dem. Förutom kartläggning av systemen beskriver kommunerna också andra områden inom vilka de uppmärksammat att arbete behövs, som segmentering av system, modernisering av gamla system, säkerhetsklassning[3] och avtalsreglering med konsulter. I en del kommuner sker pågående arbete inom dessa områden, i andra fall känner kommunerna till problemen men hänvisar till att det är något som man får ta ställning till framöver.

De flesta av de intervjuade kommunerna har uppmärksammat säkerhetsaspekterna avseende styrsystem men det finns inte något tryck från centralt håll att samordna arbetet med detta. Det beskrivs överlag som att de kommunala bolagen ”kör sin grej” och förvaltningarna sin. Samarbetet däremellan är inte strukturerat i någon större utsträckning avseende IT/säk-frågorna. En respondent väcker funderingen att en kartläggning av allt kanske skulle ge uppmärksamhet åt frågan om samarbete inom området mellan kommunal förvaltning och kommunala bolag. En annan respondent hade funderingar på hur de från kommunens sida kunde se till att bolagens säkerhetsarbete åtminstone lever upp till en miniminivå.

Relaterat till avsaknaden av samordning från centralt håll inom kommunerna uttryckte en respondent att det ofta saknas någon inom kommunen som har ett uttalat ansvar för frågor rörande säkerhet i cyberfysiska system, till skillnad mot IT-säkerhetsområdet. Det gör också att det generellt finns en informationssäkerhetspolicy, men att den sällan inkluderar något om cyberfysiska

[3] Två av kommunerna nämner att de använder ett system kallat Klassa för klassningen av system.

system. Inte heller bland andra säkerhetsrelaterade dokument och analyser inkluderas särskilt mycket, om något, kring cyberfysiska system. Ekonomiska skäl lyfts i det här sammanhanget fram som en av anledningarna till avsaknaden av någon roll med uttalat ansvar för frågor om cyberfysiska system. När resurserna är otillräckliga, vilket är fallet för många små kommuner, lyftes bland respondenterna istället möjligheten att samverka med grannkommuner för att exempelvis anställa en gemensam expertkompetens. Resursfrågan kommer också igen i det som en respondent uttryckte, att man från IT-avdelningens sida gärna skulle vilja ha mer kontakt med de kommunala bolagen i säkerhetsfrågor, men att det samtidigt skulle innebära att arbetsbelastningen blir för hög.

Notervärt i detta spår är att den kommun i studien som har all IT-drift centraliserad till den kommunala IT/säk-funktionen anser sig tillhöra den skara kommuner som har väldigt bra överblick över systemen och kopplingar etc. Det är förstås mycket lättare att ta ett helhetsgrepp om struktur och säkerhet om man har helhetsgreppet redan i driftfrågan. Detta bör ses som en stor fördel ur ett helhets- och säkerhetsperspektiv.

4 Kunskapsnivå och behov av stöd

Går det då att dra några generella slutsatser/finns någon röd tråd i kommunernas behov och nuvarande situation? Respondenterna, IT-chefer och säkchefer och liknande, har alla uttryckt att de ser frågan och är medveten om den. Samma sak sägs gälla för de kommunala bolagen. Trots att kommuncentrala IT-funktioner inte har full överblick över, och insyn i, hur de kommunala bolagen bedriver sina verksamheter, och hur dessa verksamheter är strukturerade och uppsäkrade, så tänker man sig att bolagen ”har koll”. Cyberfysiska system som ligger inom direkt kommunal kontroll har kommunens IT-funktioner större möjligheter att ha överblick över, både hur det ser ut i dag och vilka utmaningar man med fördel skulle behandla. Det kan dock variera i vilken grad man har kartlagt de olika delarna. En del kommuner anser sig ha en bra överblick över de olika cyberfysiska systemen, både i helhet och vad gäller komponenter, i sin regi, medan andra anser sig ha mindre koll på detta.

Det uttrycktes utmaningar i att få stöd och mandat att ta helhetsgreppet för att strukturera upp och implementera säkerhet för helheten avseende de cyberfysiska systemen. Det cyberfysiska området må i skrivande stund vara hett på många fronter men vad kommunledningar anbelangar har frågan inte ännu fått full fokus. I de kommuner där man kommit längre i kartläggning av sin cybermiljö har man upplevt tydligt stöd från kommunledning i utförande och mandat.

I en sammanfattande mening kan det uttryckas så här: Allmänt vill kommunerna främst ha stöd i *hur* man ska göra. Det är relativt lätt att se *vad* som behövs göras för att få styrsel på arbetet med de cyberfysiska systemen, men att förstå *hur* är inte alls lika lätt.

Trots kommunernas tydligt varierande strukturer och förutsättningar lyser ett antal teman igenom avseende vilken hjälp man skulle se som relevant och värdefull.

En initial övergripande tanke som fler uppmärksammat är att MSB skulle kunna kartlägga fler kommuners arbete inom området och leta reda på de som kommit längre. Dessa skulle kunna få agera som bra exempel som man kan referera till vid frågor kring hur på bästa sätt förbättrar sig och löser utmaningarna inom området. En annan källa till hjälp som nämnts på övergripande nivå är t.ex. Försvarsmaktens lista på certifierade produkter[4]. Denna lista hjälper till i valet av säkra produkter.

Nedan listas ett antal specifika förslag som angetts och som bör kunna ge stor effekt. (För en fullständig lista med de förslag som kom upp under intervjuerna se bilaga B):

[4] Se FMV-CSEC: http://www.fmv.se/Verksamhet/CSEC---Sveriges-Certifieringsorgan-for-IT-Sakerhet/

4.1.1 Kartläggning av system

Kommuner som upplever att de har mindre väl kartlagda cyberfysiska miljöer nämner hjälp med hur man får till detta som önskvärt. Flertalet efterlyser något i stil med checklistor, steg-för-steg-guider eller liknande, där de skulle kunna få hjälp i hur man kommer igång och hur man genomför kartläggningar

- En möjlighet för MSB här är att ta tillvara på de erfarenheter och lösningar som de kommuner som ligger lite längre fram anammat. En analys över hur de gjort tillsammans med tillgänglig litteratur kring ”best practise” på området skulle kunna mynna ut i ett relevant stöd till de kommuner som vill ha hjälp. Exempelvis en guide som med konkreta exempel som går igenom hur man gör. Detta skulle kunna täcka in kartläggningar, hjälp med checklistor och goda exempel.
- Som utgångspunkt i arbetet med att kartlägga sina system och strukturer kan man som kommun med fördel börja med att fundera på de frågor som listas i ”BOX 1” och ”BOX 2” i bilaga A. Genom att arbeta igenom dessa frågor med stöd av sammanställningen i kapitel 2, som ett första steg genereras svar och ytterligare frågor som kan agera stöd i arbetet och agera språngbräda.

4.1.2 Upphandling

Upphandling har nämnts som något som försvårar arbetet snarare än underlättar. Det har även nämnts som något som inte alls egentligen utgör något hinder. Upphandlingsregler kan leda till att säkerhets- och kompabilitetsfrågor kommer på efterkälken, och man hamnar i strukturer som kan liknas vid mindre kompatibla lapptäcken. Inom ramen för detta ryms två aspekter, dels reglerna för offentlig upphandling i sig som krånglar till det, och dels behovet av kompetens vid upphandlingar. För att kunna upphandla korrekta funktioner behövs kompetenser inom både juridik och teknik, något som inte alltid är möjligt att få till i tillräcklig utsträckning.

- Inom ramen för upphandlingsproblematiken har nämnts att kommuner skulle vara behjälpliga av t.ex. checklistor, mallar för kravspecifikationer och liknande. Det behövs både kompetens i hur de specifika kraven ska ställas inom det cyberfysiska området, och mallar till hjälp för vilka krav som behöver täckas. Här bör man kunna ta åtminstone initial hjälp av befintliga upphandlingsstöd inom IT.
- Som princip behövs kompetens på beställarsidan både avseende tekniska aspekter och avseende juridiska aspekter.

4.1.3 Hur man gör på bästa sätt

Best practice! Något som lyser igenom diskussionerna med kommun-representanterna är att ingen egentligen har något facit för hur man idealt skulle strukturera upp cyberfysmiljön. Det är ju omöjligt att applicera en mall som ska passa varje kommun ut i detaljerna men kanske skulle det vara möjligt att producera något som kan ge principiellt stöd tillsammans med ett antal exempel som underlättar implementation ute hos kommuner med olika förutsättningar.

- I linje med detta uppmärksammade behov skulle man kunna ta fram bra exempel på hur kommunens infrastruktur kan/bör se ut för att fungera på ett bra sätt. Ett sätt där man tagit hänsyn till de risker som finns inom styrsystemsmiljöer. I detta skulle man med fördel kunna belysa var svagheter och utmaningar ofta finns. Är det möjligt att ge några utvalda kommuner tid och resurser att ta fram något sådant?
- I samband med en kartläggning av systemstrukturen skulle man kunna ha nytta av stöd i hur det bör se ut. Till exempel konkreta exempel på hur best practice implementeras/implementerats i praktiken i någon styrsystemsmiljö. Här bör man kunna ta hjälp av ”vanlig” systemarkitekturkunskap.
- I en del fall har kommunledning inte det fokus på cyberfys-relaterade frågor som IT-funktionerna skulle önska. IT-funktionerna har inte möjlighet att trycka upp frågorna på agendan på samma sätt som med mer generella IT-frågor.
    - I linje med ovanstående skulle MSB kunna ta fram och förmedla information om cyberfrågor och hur viktiga de är. MSB skulle kunna informera om att kartläggning och uppsäkring behövs för att höja medvetandenivån och därigenom verka för en ökad förståelse för frågorna. Lite i samma spår uttrycktes tankar om att MSB eller annan relevant part skulle kunna sätta upp regler inom området som tvingar kommuner att ha ansvariga inom området. (Osäkert vilken part som skulle ha mandat och vilja att reglera området på detta sätt, men tanken luftades i alla fall)

Värt är också att notera att två av de intervjuade kommunerna inte ansåg att de var i behov av något specifikt stöd från MSB rörande säkerhetsfrågor och cyberfysiska system. Detta får i sammanhanget anses positivt, eftersom det betyder att det finns kommuner som anser sig både ha kunskap, mandat och resurser att driva säkerhetsfrågor. En av dessa kommuner påtalade också att de flitigt nyttjade den information som MSB idag redan publicerar på webben om säkerhet i industriella informations- och styrsystem.

5 Slutsatser och förslag på fortsatt arbete

Utifrån denna undersökning tecknas en bild av att området cyberfysiska system inte är lika väletablerat som det traditionella IT-området hos kommunerna. Vissa kommuner upplever utmaningar i samband med att de tar sig an området, och vissa upplever att de har kommit längre i arbetet och ser det därmed som enklare och lättare. Den cyberfysiska domänen är speciell till sin karaktär i och med att den innehåller både digitala och fysiska (såväl som nya och gamla) komponenter, och detta ger både huvudbry och upplevda möjligheter.

Det finns en tydlig möjlighet att ta tillvara kunskaper från de kommuner som kommit längre i arbetet och med detta hjälpa de som inte kommit lika långt. De som upplever sig ha tagit sig förbi de initiala utmaningarna har uttryckt att de gärna är med och hjälper till. Denna inställning och källa till hjälp och utvecklingsassistans bör säkerligen kunna hittas i fler kommuner.

Ett genomgående tema avseende de upplevda behoven inom olika cyberfysiska delområden är att man ser det som värdefullt med hjälp i hur man konkret hanterar utmaningarna. Checklistor, mallar, guider och exempel nämns primärt som sådant som kan hjälpa de ansvariga i sin vardag med att ta sig framåt. Övriga former av hjälp tackar man inte nej till men ovan nämnda format ses som mest givande. Framtagning av relevanta konkreta stödprodukter ter sig därmed som givande framtida hjälpaktiviteter. Flertalet av de listade hjälpinsatserna i kapitel 4, och i bilagan, bör kunna operationaliseras som projekt, förslagsvis med stöd och inblanding av relevanta kommuner.

BILAGA A

Diskussionspunkter för projektet ”cyberfys i kommuner” (SCADA/ICS/Styrsystem osv.) i den form de användes.

BOX 1: Vad finns i kommunen/systemstruktur?

- Vilka typer av cyberfysiska finns i kommunal verksamhet/regi
- Syfte: Få en bild av hur väl de cyberfysiska systemen är kartlagda.
    - Har man kommit så långt att man har kartlagt dom? Finns en samlad dokumentation över cyberfys/scada/SRÖ-nätet/näten?
    - Finns det aktuella flödesbeskrivningar
    - Är näten segmenterade
    - Hur är systemen och dess information säkerhetsklassade?
- Hur bra koll har kommunen på vilka behov som finns avseende att:
    - Säkra upp systemen (infosäk)
    - Säkra upp systemen (driftkompetens)
    - Säkra upp systemen (modernitet/åldrande etc)

(Svar på ovanstående punkter kanske kan komplettera de direkta svaren med en indikation på hur det ser ut)

BOX 2: Vad är kommunens syn på informationssäkerhetsarbetet?

- Syfte: Ge en bild av hur arbetet med cyberfysiska system bedrivs inom kommunerna idag (Upplevs utmaningar inom något av dessa listade områden?)
    - Finns processer för att kartlägga de cyberfysiska systemen?
        - Finns kontinuitetsplaner?
    - Finns uttalade roller/ansvar satta för att hantera arbetet med cyberfysiska system?
        - Är roller och ansvar klarlagda och beslutade
        - Behörighetsnivåer till ingående system
        - Vem har beställarrollen?
        - Används konsulter, finns dessa reglerade i avtal, sekretessavtal?
        - Hur är beställnings-/felanmälningsvägarna?
        - Finns riktlinjer för lösenordssättning på ingående produkter/enheter?
    - Ser kommunen några utmaningar/brister/behov kopplat till cyberfysiska system för någon/några av följande?

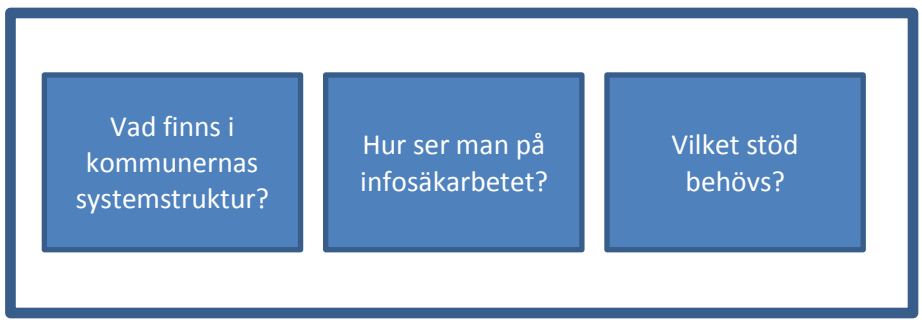
- för kommunens egna system
- för system vars drift ligger inom kommunalt ägda bolag
- för system i privat ägo
- eventuell övrig form

BOX 3: Vilket stöd behöver kommunen från MSB?

- Inom vilket område önskas stöd?
  - Kartläggning?
  - Uppsäkring?
  - Processer?
  - …
- Och på vilken form (av självhjälp)?
  - Checklistor?
  - Process-exempel?
  - Kompetensöverföringsforum?
  - Allmänna informationsbroschyrer?
  - …

ÖVRIGT:

Hur ser aktörerna på eventuella upphandlingstvång. Innebär det någon utmaning? Påverkar det systemstrukturen avseende t.ex. drift och säkerhet? Lapptäcke? Kompabilitet? Support? Har man tillräcklig kunskap om hur man kan göra upphandlingar där säkerhet ska vara en aspekt (dvs .skulle stöd vara intressant) och ser man problem med att publicera underlag i upphandlingsprocessen som i sig kanske avslöjar saker som är känsligt exempelvis?



BILAGA B

Lista över de förslag på relevant stöd som nämndes under intervjuerna med kommuner angående arbetet med cyberfysiska system. En kommun såg varken behov eller hade kommentarer och är därmed av utrymmesskäl utelämnade ur tabellen.

Kommun	1	2	3	4	5
Förslag					
Information till ledningar	MSB kan informera om att kartläggning & uppsäkring behövs, till kommunala bolag och kommunchefer, för att skapa förståelse.				Kommunen ser inget behov av stöd
Regelstyrning	Sätta upp regler om att det måste finnas någon säkerhetsansvarig för styrsystem, likt för IT-system. Regler för hur styrsystem ska hanteras. (Checklistor / hur man bör göra/				

	när-vad-hur)				
Regelstyrning	Ge politikerna förslag på lagar som ålägger kommuner att bedriva ett bra säkerhetsarbete inom området.				
Upphandlings-hjälp	Kravspecifikationer, ”tänk på detta när ni gör en upphandling”. Upphandlingshjälp.	Upphandling – kravspecifikationer för upphandling av styrsystem (med hänsyn till den stora bredden blir det väldigt brett i vilka kompetenser som behövs). Mallar för det hela, kravspec-mallar			

Goda exempel	Ta fram bra exempel på kommuner där det fungerar bra, ”vi löste problemet på det här sättet”. Som man kan referera till.		Plocka fram goda exempel, ”kommuner man kan ringa”. Beskriva hur dom jobbat, vanliga missar, ”gör/gör inte”. Konferenser där man redovisar goda exempel.	Denna kommun, med sin lösning, kan tänka sig agera som ett bra exempel på hur man kan lösa en del av arbetet med cyberfys-system	
Standardise-ring av produkter	Certifierade produkter från T.ex http://www.fmv.se/sv/Verksamhet/CSEC---Sveriges-Certifieringsorgan-for-IT-Sakerhet/Evaluering-och-certifiering/ Så blir det ännu lättare att välja säkrare produkter.				
Ekonomiskt stöd	MSB kan ge ekonomiskt stöd för att				

	få igång arbetet med att uppmärksamma säkerhetsfrågor kring styrsystem.				
Kartläggning		Kartläggningen skulle kunna göras väldigt mycket likadant för alla kommuner. Hjälp med detta vore bra. Behovet är identiskt bland kommunerna. Man skulle vlija ha listor med vilka system som bör räknas in. (dvs att MSB producerar dessa listor)		Nej, kartläggning av kommunens egna system finns redan idag	

Best practice		Best practice för hur kommunens infrastruktur bör se ut för att fungera på bästa sätt, där man tagit hänsyn till de risker som finns inom styrsysteme n. Information om var svaga punkter ofta finns. Idealbild på strukturer och flöden. Best practice för infrastruktur en.	Vägledande mall (t.ex ABB har sådana). Cecklistor och processexemp el, bra.	Föreslå infrastrukturell design, tex segmenterat nät. Säkerhetsanalys motsvarande penetrationstester. Om MSB skulle kunna stötta i ovan så skulle det vara till hjälp för kommunen. Cyberfysiska system hamnar ofta i skymundan. Steg för steg guide för infrastrukturdesig n och behörighetshanter ing. Checklistor som beskriver vad man bör tänka på. Processer för kartläggning, uppsäkring, processer för att lägga till behörighet (eftersom det idag ofta sker muntligt, odokumenterat, gör att personal kan få tillgång till fastigheter som man inte bör ha behörighet till).	

Kvalitetscheck/ revision			Det skulle vara bra med hjälp med kvalitetssäkring av arbetet om typ 2-3 år när de är klara. Man skulle kunna ha som en extern genomgång som är någon typ av revisionslikknande grej från MSB.		
Omvärlds-bevaknings-funktion			Omvärldsbevakning. Vad finns. Vad kan moderna saker göra + säkerhetsaspekter.		
Broschyrer				Broschyrer kan nog vara tillgodo för många kommuner. Systemen kanske är halvviktiga idag, men på sikt så kommer de att vara alltmer viktiga. En informationsbroschyr skulle vara bra, inget komplicerat, men frågorna kring cyberfysiska system behövs uppmärksammas,	

				”tänk även på dessa system!!”	
Upphandling					
Kommentarer kring upphandlings-frågan	Vad gäller ventilations system mm så är IT aldrig involverade vid upphandlin g. För passersyste men är IT involverade, men mest kanske för att de själva har bearbetat och varit intresserade av att ta tag i säkerhetsfrå gorna kopplat till detta. Upphandlin gar är aldrig lätta. De upplevs som en krånglande aspekt som	Molnsystem – strategi att förbättra mallarna för upphandling. Det är så många som är inblandade i upphandling arna att man behöver styra från kommunens sida. Det är en kompetens som måste stärkas inom hela kommunen. Infosäkchef en har bra koll. Man håller på och tar fram mall för att beakta IT-säk i upphandling ar. Upphandlin	Det kan uppstå kompabilitets problem vid upphandlingar. Om låssmeden inte jobbar i det system som man använder i kommunen = problem. Det kan drabba IT-funktionalitet. Styrsystem som inte kan kommunicera bra med leverantörens komponenter. De har tidigare hamnat i lägen med olika komponenter som ej är helt kompatibla. Då får man mecka med	Upphandlingsfråg an kan fragmentera IT-miljön över tid (en fragmenterad IT-miljö kan handla om olika servermiljöer, inkompatibla system mm.) I kommunen finns en central upphandlingsenhe t (Upplevs som mkt bra grej!) vilket gör att IT-miljön för kommunen inte har blivit fragmenterad. Om man inte har en central upphandlingsenhe t så finns risk att IT-miljön fragmenteras.	Tips från de intervjuade: Kammarkol legiet har någon form av samlad ramavtalsm öjlighet som kommuner kan ansluta sig till. Denna möjlighet finns för en drös olika områden (IT, etc etc) och erbjuder bra möjligheter att styra sina upphandlin gar.

	skapar onödig kreativitet i kravspecar.	gsmallar och upphandling skompetens behövs stärkas upp. Speciellt inom IT/SÄK.	konverterings moduler. Kommunen har dock en bra upphandlare som är kompetens och gör ett bra jobb. Andra kommuner kan nog ha behov inom detta.		
Övrigt					
Övriga kommentarer	* ”Är intresserade av att vara fortsatt involverade i arbetet!” * ”internet of things kommer ge mkt nya möjligheter, men kräver moderniseringar i kommunen” ”En del IT/ICS sköts i bolag, en del via kommunens IT-funktion, ingen har översyn över hela kedjan”		Intervjun i sig har varit lärande och fått respondenten att tänka till och igenom sakerna.	* Sammantaget anser respondenterna att man har rätt bra koll på sina system. Genom att titta på frågorna som vi skickat har de själva fått upp ögonen för vissa frågor att kika närmare på. * Kommunen har en känsla av att deras svagheter och brister är utsatt för kartläggning av någon aktör. Därför är de skeptiska vid kontakter. * Respondenterna använder inte begreppet	Respondenterna i denna kommun kan gärna agera exempel på hur man kan lösa saker och ting. De har dessutom ett verktyg/system som de ska använda för att analysera alla system innan de sätts i drift. Detta system täcker aspekter så som roller,

	IT-avdelningen har allmänt blivit mer och mer involverade i frågor rörande (IT-)säkerhet. = bra.			cyberfysiska system, har aldrig hört det, utan använder begreppet Fastighetssystem och DUC. * De är gärna med i fortsatt arbete. * Övergripande så anser respondenterna att de har koll på en hel del saker vad gäller kommunens egna (cyberfysiska) system, nät och DUC'ar, men de menar samtidigt att det finns mycket mycket mer som skulle kunna göras. De har exempelvis svårt att avgöra standarden på säkerheten för cyberfysiska system eftersom mycket ligger på leverantörerna. För övriga IT-system har respondenterna själva möjlighet att avgöra vilken standard/säkerhets nivå som finns.	regler, säkerhet, etc. De noterade att, Visst skulle man kunna använda MSB's e-learning-portal, men de kommer använda en egen. Bl.a. för att de vill kunna trycka in fler typer av utbildningar i sin e-learning-portal framöver, och då är det enklare att själv kunna hantera den.

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