ASPEKTER PÅ ANTAGONISTISKA HOT MOT SCADA-SYSTEM I SAMHÄLLSVIKTIGA VERKSAMHETER

Erik Johansson[1], Henrik Christiansson[2], Richard Andersson[3], Gunnar Björkman[1] och Arne Vidström[3].

Sammanfattning

Samhällsviktiga verksamheter blir allt mer beroende av infrastrukturen för styrning, reglering och övervakning av fysiska processer. Den grundläggande infrastrukturen består till stora delar av datorbaserade system, vilka brukar benämnas SCADA-system (Supervisory Control And Data Aquisition). Dessa SCADA-system utgör det centrala nervcentret inom den allt viktigare samhällskritiska infrastrukturen, genom att de samlar in och förmedlar vital information från kritiska processer. SCADA-systemen utgör idag ofta en förutsättning för att kunna upptäcka problem och vidta åtgärder för att vidmakthålla en pålitlig drift av de fysiska processerna.

Denna rapport ger inledningsvis en övergripande bild av hur SCADA-systemen i vår kritiska infrastruktur har utvecklats samt visar hur sårbarheter (svagheter som kan komma att utnyttjas av en angripare) i dessa system har uppstått. Detta görs bland annat genom en historisk beskrivning av SCADA-systemens utveckling ur ett informationssäkerhetsperspektiv. Därutöver beskrivs kända cyberattacker mot SCADA-system samt hur utvecklingstendenserna ser ut ur framförallt ett tekniskt utvecklingsperspektiv. Dessutom presenteras en övergripande analys av den existerande informationen om SCADA-säkerhet som studien till vissa delar grundar sig på, samt en enkel kvalitativ värdering av denna information. Studien avslutas med att lista de viktiga SCADA-säkerhetsområden där författarna anser att staten behöver engagera sig. Dessa områden kan förenklat sammanfattas med begreppen kartläggning, fallbeskrivningar, kvalitetsgranskning, testanläggningar, utbildning, samverkan samt riktlinjer.

Rapporten har en övergripande karaktär och den lämnar inte tekniska rekommendationer om hur exempelvis nätverksarkitekturer eller säkerhetspolicys skall utformas. Avsikten med rapporten är att ge läsaren en första inblick i behoven av informationssäkerhet hos SCADA-system. Den skall också inventera och beskriva de aktiviteter som genomförs internationellt och vad som initialt behöver genomföras för att minska samhällets sårbarhet för avsiktliga antagonistiska hot mot dessa system. Den tänkta läsekretsen är framförallt säkerhetspersonal på olika nivåer vars ansvar på något sätt berör SCADA-system. Det går utmärkt att läsa utvalda kapitel allt efter vilka behov man har.

Nyckelord

SCADA (Supervisory, Control and Data Acquisition), informationssäkerhet, infrastruktur, sårbarhet, DCS (Distributed Control Systems), PCS (Process Control Systems), RTU (Remote Terminal Unit).

---

[1] Kungliga Tekniska högskolan (KTH)
[2] Totalförsvaret forskningsinstitut (FOI) och Krisberedskapsmyndigheten (KBM)
[3] Totalförsvaret forskningsinstitut (FOI)

INNEHÅLLSFÖRTECKNING

FIGURFÖRTECKNING

FÖRORD

Denna rapport är resultatet av en övergripande studie som genomförts i nära samarbete mellan Kungliga Tekniska högskolan, Totalförsvarets forskningsinstitut samt Krisberedskapsmyndigheten.

Framtagandet av denna rapport har finansierats av Krisberedskapsmyndigheten. Författarna vill tacka ett flertal personer för värdefulla synpunkter på olika utkast av denna rapport, bland andra: Tore Carrick (Preem AB), Hans Hol och Göran Eriksson (Svenska Kraftnät), Johan Schubert (Know IT Technowledge AB), Åke Holmgren (FOI) samt Alf Lundström (Vattenfall AB).

ÖVERGRIPANDE SUMMERING

Under den senaste trettioårsperioden har användandet av informationsteknik vid styrning, reglering och övervakning av processer i den tekniska infrastrukturen ökat på ett remarkabelt sätt. I denna rapport benämns dessa system SCADA-system.

SCADA-system förekommer i en rad olika processer och industrier, bland annat inom följande samhällskritiska verksamheter:

- produktion och distribution av energi, el, vatten och drivmedel
- produktion inom petrokemisk industri
- drift av spårbunden trafik.

Orsakerna till den ökade användningen av SCADA-system är framförallt funktionella, såsom att bättre utnyttja såväl tekniska som personella resurser, men även för att öka förmågan att hantera tekniska fel i processen. Det är dessutom allt svårare att få tillstånd att bygga ut den primära processen, till exempel att bygga nya kraftverk, högspänningsledningar eller rörledningar för gas. Detta gör att de befintliga anläggningarna måste utnyttjas allt hårdare och därmed även allt närmare sina stabilitetsgränser. För att under dessa omständigheter säkerställa leveranser i samhällets kritiska verksamheter införs därför mer och mer avancerade och datoriserade styrsystem vilka bättre än tidigare kan övervaka, varna och automatiskt styra processerna. Allt finare modeller över processerna, och allt mer avancerade applikationer i styrsystemen, blir därmed nödvändiga. Här kan man jämföra med utveckling inom flygindustrin där flygplan i princip blivit omöjliga att manövrera utan datorer, till exempel JAS 39 Gripen. På samma sätt bedöms utvecklingen, med ökade krav på funktionell prestanda, leda till att SCADA-systemen blir en alltmer integrerad del av själva processen, och att det knappt är möjligt att styra, övervaka och vidmakthålla dessa samhällskritiska processer utan SCADA-system.

Parallellt med att SCADA-systemens betydelse för viktiga processer växer, har avreglering av olika typer av marknader gjort att informationen som lagras i SCADA-system och dess historiska databaser blivit en strategisk tillgång för hela verksamheter och bolag. Detta har bidragit till att SCADA-systemen börjat öppnas och integrerats med andra system via de traditionellt administrativa kontorsnätverken.

Vid detta öppnande och integrerande av avancerade kritiska SCADA-system med andra system inom bolagen via kontorsnätverk har allvarlig sårbarhet skapats, kopplad till nya typer av hot. Ett exempel är antagonistiska hot, även kallad cyberterrorism, det vill säga att någon medvetet utnyttjar möjligheten att styra, reglera och övervaka processer i syfte att störa eller förstöra den kritiska infrastrukturen. Några exempel på cyberattacker mot SCADA-system är följande:

- Mars 2000. En missnöjd tidigare konsult tar över kontrollsystemet för ett vattenreningssystem i Australien. Konsekvensen av attacken blir att tusentals kubikmeter obehandlat vatten översvämmar området.
- December 2000. En grupp hackare angriper ett datornätverk i en elkraftanläggning i USA genom att utnyttja svagheter i ett använt protokoll. Sedan används de övertagna nätverksresurserna för att spela datorspel. Detta utnyttjande av dator- och nätverksresurser hindrar påtagligt möjligheten för anläggningen att bedriva affärer med sin elektricitet (electricity trading).
- Januari 2003. Driftsäkerhetsövervakningssystemet vid kärnkraftverket Davis-Besse i USA, som vid tillfället är avställt för revision, infekteras med SLAMMER-masken. Systemet är ur funktion i nära fem timmar. Orsaken är dels en felaktigt uppsatt förbindelse in i kärnkraftverkets datornät, dels en dator utan virusskydd eftersom den betraktas som fristående och därmed inte i behov av skydd. Det finns redundanta, analoga reservsystem som är opåverkade av masken men operatörerna vid verket får en avsevärt ökad arbetsbelastning.
- Augusti 2003. En amerikansk tågoperatörs datornätverk för signalering infekteras av en mask vilket leder till att alla operatörens tåg står stilla i en halv dag.
- Maj 2004. SASSER-masken infekterar ett signal- och kontrollsystem hos den australiensiska lokaltågsoperatören Railcorp. Följdeffekten blir att 300 000 pendlare till och från Sydney saknar transportmedel under en dag.

Det är viktigt att notera att alla dessa antagonistiskt relaterade incidenter härrör från icke kvalificerade antagonister.

För att förstå problematiken kring säkerhetsaspekter hos SCADA-system i den kritiska infrastrukturen krävs en förståelse för hur dessa verksamheter och system har utvecklats historiskt. I denna rapport belyses därför SCADA-systemens utveckling över tre perioder där skillnader i teknik åskådliggörs:

1. system för ren datainsamling och fjärrstyrning (från 1930-talet till 1980-talet)
2. system med processmodeller för avancerade applikationer (till 1990-talets mitt)
3. öppna, integrerade system med koppling till omvärlden (dagens system).

Denna uppdelning är en grov förenkling ur ett rent SCADA-perspektiv men relativt funktionell sett ur ett informationssäkerhetsperspektiv.

I den tidiga första fasen var SCADA-systemen relativt enkla, sårbarheterna få och säkerheten förhållandevis hög i relation till den rådande hotbilden (vilken då framförallt ansågs vara fysisk påverkan vid anläggningar).

I den andra fasen blev SCADA-systemen allt mer komplexa samtidigt som mer och mer av utrustningen köptes från tredjepartsleverantörer. Sårbarheterna i dessa system ökade medan hotbilden föreföll relativt låg. Driftcentralerna flyttades ut från skyddade bergrum till normala kontorsbyggnader.

I den tredje evolutionsfasen som består av öppna, integrerade system med kopplingar till omvärlden har inte bara sårbarheterna ökat betydligt. Även den generella hotbilden i samhället, samt medvetenheten om dessa hot, har ökat väsentligt under senare år.

Sammanfattningsvis har det inte varit säkerhet (med ett antagonistperspektiv) som varit drivkraften för utvecklingen av SCADA-system. Det har snarare varit behovet av utökad funktion samt en allmän prispress som har dominerat utvecklingen. Samverkan mellan ständigt mer lättåtkomliga attackmetoder samt den större skada dessa kan orsaka utgör därför ett växande säkerhetsgap. Detta gap (med fler identifierade sårbarheter och potentiellt fler antal hot) måste försöka överbryggas. Det är idag osäkert om hur stora konsekvenser ett misslyckande i det avseendet kan komma att få.

Rapportens rekommendationer för svenska statens fortsatta engagemang inom SCADA-säkerhetsområdet handlar ytterst om att etablera ett bra säkerhetsskydd för SCADA-system eftersom dessa utgör en central del av samhällets kritiska infrastruktur. Skyddet bör svara mot den hotbild som man antar råder mot svenska SCADA-system och den kritiska infrastrukturen. Detta säkerhetsskydd består av allt från grundläggande kompetens om IT-säkerhet till möjliga specifika tekniska åtgärder som till exempel appliceringen av specialframtagna brandväggar för PLC:er. Om det anses att hotbilden mot svenska SCADA-system inte innehåller risken att en antagonist till exempel kartlägger och sedan utnyttjar specifika SCADA-protokoll för att uppnå sina syften, så behöver man inte lägga tid och resurser för att etablera skydd mot denna typ av antagonist. Valet av dimensionerande hotbild är således avgörande för vilka verksamheter som inom SCADA-säkerhetsområdet staten skall satsa resurser på.

Vår slutsats är dock att staten skall ha ett långsiktigt engagemang i SCADA-säkerhetsområdet. Detta engagemang bör bestå i att dels finansiera insatser som syftar till att upprätthålla nationell säkerhet, dels att ha en samordnande roll för att effektivitet skall uppnås. För detta krävs kompetens att bedöma aktuell hotbild samt att analysera de potentiella konsekvenserna som attacker kan innebära för samhället.

I listan med rekommendationer som presenteras i rapporten finns det aktiviteter som hanterar flera typer av hot. De områden som bör prioriteras har tagits fram med utgångspunkt från de slutsatser som författarna har dragit från arbetet med studien. Önskvärda aktiviteter för staten bör enligt vår mening ske inom områdena kartläggning, fallbeskrivningar, kvalitetsgranskning, testanläggningar, utbildning, samverkan samt riktlinjer. Den övergripande strategin är att kartläggning, fallbeskrivningar, kvalitetsgranskning, samverkan och utbildning främst skall hantera det stora behovet av att medvetandegöra samhällsviktiga verksamheter om de nya typer

av hot mot SCADA-system som kan identifieras. Områdena testanläggningar och riktlinjer svarar mot behovet av att ta fram ny kunskap. Erfarenheter från USA visar att området testanläggningar är centralt även för de övriga områdena som beskrivits ovan.

1 STYRNING OCH KONTROLL AV SAMHÄLLSVIKTIG INFRASTRUKTUR

Samhällsviktiga verksamheter blir allt mer beroende av en infrastruktur som till stora delar består av datorbaserade system för styrning, reglering och övervakning av fysiska processer. I detta avsnitt ges en kort introduktion till de system som döljer sig bakom den engelska beteckningen Supervisory Control And Data Aquisition (SCADA). Dessa SCADA-system[4] utgör den centrala nerven för all kritisk infrastruktur genom att de förmedlar vital information som möjliggör en säker verksamhet.

1.1 Introduktion

Användningen av SCADA-system är väl utbredd i världen. Uppskattningsvis fanns cirka tre miljoner SCADA-system i drift i världen 2006 (DMEA, 2006). Storlek och kostnad när det gäller SCADA-system varierar med vilken typ av fysisk process som hanteras. Exempelvis kan vattenreningsanläggningar för en mindre stad kosta en till två miljoner kronor, medan en mer omfattande anläggning för exempelvis eldistribution kan kosta 100–200 miljoner. Många av dessa SCADA-system styrs från kontroll- eller driftcentraler. Bara inom EU finns det uppskattningsvis 100 000 kontrollcentraler för olika tekniska verksamheter (Ober, 2006).

För att förstå hela problematiken kring hot och risker med SCADA-system i samhällskritiska verksamheter krävs en helhetsbild. Därför kommer denna rapport att inledningsvis belysa behoven och utvecklingen av SCADA-system utifrån ett historiskt perspektiv. Denna beskrivning avser att ge en bakgrundsförståelse för de speciella förhållanden som, tillsammans med samhällets utveckling, har bidragit till att sårbarheter förenade med SCADA-system har blivit viktiga att studera idag. De aspekter som i huvudsak beskrivs i denna rapport är följande:

- motiven till varför samhället inför och använder SCADA-system
- generella sårbarheter och egenskaper som utvecklingen av SCADA-systemen har medfört

[4] Dessa system benämns på olika sätt i olika sektorer och beroende på vad systemen används till. Här kommer Supervisory Control And Data Aquisition (SCADA) att användas som ett övergripande begrepp för systemen. Andra förekommande beteckningar är Distributed Control Systems (DCS) och Process Control Systems (PCS).

- information om cyberattacker mot SCADA-system[5]
- litteratur och forskning kring SCADA-system
- värdering av artiklar och litteratur ur ett informationssäkerhetsperspektiv
- behovet av värdering och analys av incidenter relaterade till SCADA-system.

Ett annat problem med dagens alltmer komplexa SCADA-system är bristande kvalitet i programvaran vilket bland annat kan resultera i bristande tillgänglighet. Ett exempel på detta är den stora störningen 2003 i nordöstra USA. Den hade som en utlösande orsak en icke fungerande larmhantering i ett SCADA-system. Sådana former av kvalitetsbrister behandlas dock inte i denna rapport vilken istället fokuserar på antagonistiska hot.

1.2 Läsanvisning

Denna rapport ger inledningsvis en övergripande bild av hur SCADA-systemen i vår kritiska infrastruktur används och har utvecklats, och hur sårbarheter (svagheter som kan utnyttjas av en angripare) har uppstått i dessa (kapitel 1 och 2). Därefter ges en beskrivning av SCADA-systemens utveckling ur ett informationssäkerhetsperspektiv. Sedan beskrivs det som är känt om inträffade cyberattacker mot SCADA-system samt hur utvecklingstendenserna ser ut ur framförallt ett tekniskt utvecklingsperspektiv (kapitel 3). Därefter presenteras en övergripande analys av den existerande information om SCADA-säkerhet som studien till vissa delar grundar sig på, samt en enkel kvalitativ värdering av denna information (kapitel 4). Avslutningsvis dras slutsatser för vilka områden som staten bör engagera sig i inom SCADA-säkerhetsområdet (kapitel 5). Dessa områden kan grovt beskrivas av begreppen kartläggning, fallbeskrivningar, kvalitetsgranskning, testanläggningar, utbildning, samverkan samt riktlinjer.

Nedan följer ett par kortfattade exempel på hur rapporten kan användas av olika läsare beroende på vilken utgångspunkt man har. För den som inte känner till SCADA-system är kapitel 1 och 2 en bra introduktion. Kan man lite om SCADA-system och mest är intresserad av hoten mot dessa system går det relativt bra att bara läsa kapitel 3. För den som vill fördjupa sig inom området är kapitel 4 en bra grund för att navigera inom produktionen av information om SCADA-säkerhetsområdet. För den som är beslutsfattare inom stat eller infrastruktur är kapitel 2 och 5 troligtvis det vikigaste att läsa.

[5] I denna rapport kommer begrepp som cyberattacker, cybersårbarheter och cybersäkerhet att användas eftersom de är mer eller mindre vedertagna begrepp bland de viktigaste aktörerna inom SCADA-säkerhetsområdet se till exempel rapporter från Idaho National Laboratory samt Department of Energy (DoE, 2006).

1.3 En incident och ett scenario relaterade till angrepp på SCADA-system

På eftermiddagen den 10 juni 1999 gick en rörledning sönder för företaget Olympic Pipe Line Company vid dess anläggning i Bellingham, Washington (NSTB, 2002). Detta ledde till att 900 000 liter bensin läckte ut i en närbelägen flod. Senare antändes bensinen och den påföljande branden ödelade cirka 2,4 km av floden och dess närmaste omgivning vilket återges i figur 1. Två tioåriga pojkar och en artonårig man omkom vid branden. Ytterligare åtta personer skadades. Ett bostadshus samt stadens vattenreningssystem skadades också allvarligt. Den uppskattade kostnaden för de materiella skador som olyckan åstadkom är för närvarande uppe i 315 miljoner kronor.

Figur 1. Fotografi av den utbrända floden efter olyckan i Bellingham.

Orsakerna till olyckan var framförallt två (NSTB, 2002). Den främsta orsaken var den rörskada som uppkom redan 1994 vid en större renovering av anläggningen och den oförmåga som företaget sedan visade genom att inte identifiera den under de fem år som gick fram till olyckan. Den andra och kanske mer intressanta orsaken för denna rapport var de modifieringar företaget genomförde i SCADA-systemets databas vid tiden för olyckan, vilka ledde till att man vid olyckstillfället inte hade möjlighet att övervaka och styra den fysiska processen.

Denna tragiska olycka visar framförallt på de effekter som kan uppstå vid samverkande problem mellan de fysiska processerna, och de system som övervakar de fysiska processerna. Denna samverkan är signifikant och allvarlig eftersom den försvårar den analys som krävs när antagonistiska hot mot SCADA-system skall beaktas. En angripare som på ett genomtänkt sätt angriper fysiska processer och SCADA-system kan förorsaka mycket stor skada. Denna skada kan dessutom vara svår att komma till rätta med eftersom dyrbar utrustning i de fysiska anläggningarna ofta är svåra att snabbt byta ut. Tänkbara angripare kan vara främmande stater, terrorister, aktivister, hackare, insider och ”script kiddies” (NISCC, 2004) (se avsnitt 3.1). Det finns dock mycket få dokumenterade attacker mot SCADA-system vilket framgår av kapitel 3 i denna rapport vilket är ett problem när man skall motivera säkerhetsskyddsarbetet för SCADA-system.

Att även exempelvis databaser över historiska värden för processen (så kallad SCADA-historik) kan vara ett mål vid attacker mot SCADA-system, framgår vid den demonstration som det amerikanska nationella säkerhetslaboratoriet Idaho National Laboratory (INL) utför vid en av sina kurser rörande SCADA-säkerhet. Den demonstrator som används (figur 2) kan anses vara en rimlig representation av ett SCADA-system med avseende på såväl komponenter och arkitektur som IT-säkerhetslösningar. I det tillhörande kursmaterialet[6] finns övergripande beskrivningar av hur man går till väga vid attackdemonstrationen. Ett av delmålen som man pekar ut för attacken är just databasen för SCADA-historik. Angriparen når dit genom att utnyttja svagheter i dels kontorsnätverket, dels kopplingen till SCADA-nätverket från kontorsnätverket (figur 2). När väl access till arbetsstationen i SCADA-nätverket (Engineering Workstation) har uppnåtts har angriparen i princip tillgång till alla resurser i SCADA-nätverket.

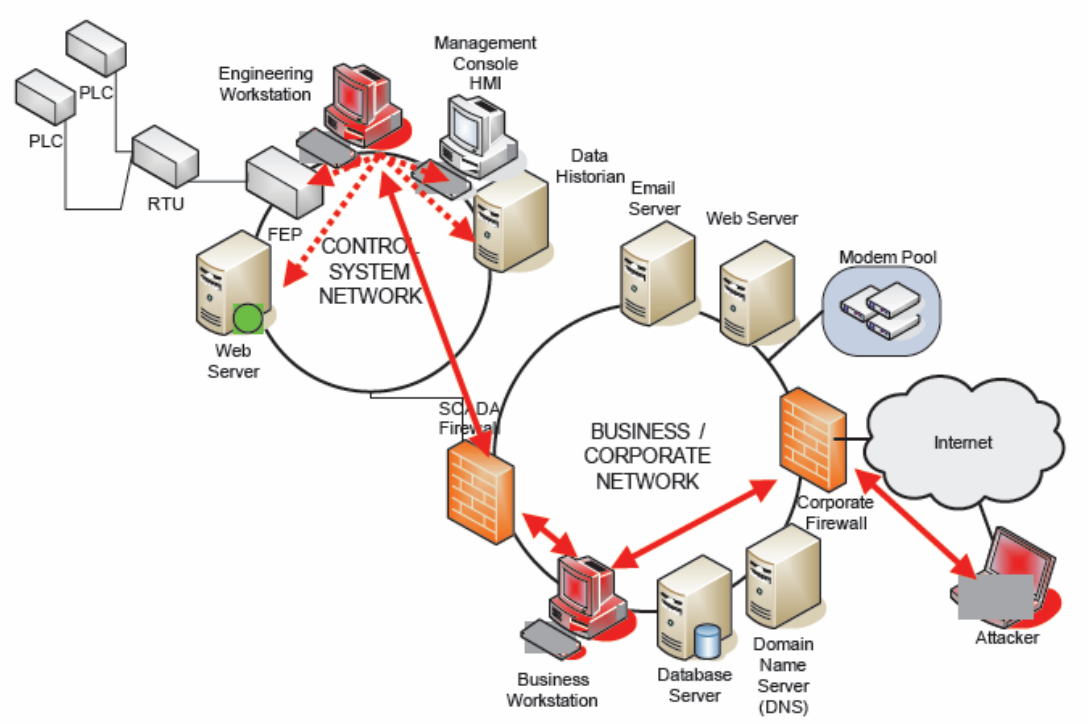
Motivet för att ta fram denna demonstrator har varit att visa vilka möjligheter som finns för att angripa SCADA-system, eftersom det finns mycket få rapporterade attacker mot denna typ av system. Det dilemma som skapas för säkerhetsarbetet

[6] Idaho National Laboratory, *Introduction SCADA Security for Managers and Operators* www.inl.gov/nationalsecurity/d/inl_ss1_4h_nerc_training.pdf

identifieras av det internationella projektet *SCADA (*Control Systems Security Project[7]) där det angavs att

> ***SCADA-systems are so critical that whether the threat has been demonstrated (fact) or conceptualized (fiction), the reality is […] these systems have to be protected.***

Detta ställningstagande är viktigt att reflektera över för varje användare av SCADA-system. Det är också viktigt att fundera över hur kritiska organisationens SCADA-system är för verksamheten, men också vilka konsekvenser ett angrepp mot dessa system skulle få för samhället på sikt.



Figur 2. Beskrivning av attackväg som används vid INL-demonstrationen. Lägg märke till att en av de markerade delmålen är databasen för SCADA-historik som finns bredvid HMI-konsolen.

[7] SANS Webcast 18 May 2006, *The SCADA (Control System Security Project): Common Security Requirement Language for Procurements & Maintenance Contracts*, Will Pelgrin, New York State, Michael Assante, Idaho National Laboratory, Rita Wells, Idaho National Laboratory.

1.4 Vilka samhällskritiska verksamheter använder SCADA-system?

Under den senaste trettioårsperioden har användandet av informationsteknik vid styrning, reglering och övervakning av processer i den tekniska infrastrukturen ökat på ett remarkabelt sätt. I denna rapport benämns dessa system som SCADA-system. SCADA-system förekommer i en rad olika processer och industrier, bland annat inom följande samhällskritiska verksamheter:

- produktion och distribution av energi, el, vatten och drivmedel
- produktion inom petrokemisk industri
- drift av spårbunden trafik.

Skälen till den ökade användningen av dessa system är framförallt funktionella, såsom att bättre kunna utnyttja såväl tekniska som personella resurser, men även för att öka systemens förmåga att hantera tekniska fel.

Det går att göra stora vinster ur flera perspektiv på ett effektivare resursutnyttjande och en ökad effektivitet, vilket i sin tur leder till en ökad teknisk komplexitet i systemen. Allt finare modeller över processerna, och allt mer avancerade applikationer i styrsystemen blir därmed nödvändiga. För att under dessa omständigheter säkerställa leveranser i samhällets känsliga verksamheter införs därför mer och mer avancerade och datoriserade styrsystem. Dessa kan övervaka, varna och automatiskt styra processerna bättre än tidigare. Här kan man jämföra med utveckling inom flygindustrin där flygplan i princip blir omöjliga att manövrera utan datorer, till exempel JAS 39 Gripen. På samma sätt bedöms utvecklingen med ökade krav på prestanda leda till allt mer avancerad funktionalitet även inom områden som nyttjar SCADA-system.

Vid integrering av avancerade SCADA-system uppkommer emellertid även sårbarheter som är kopplade till nya typer av hot. Dessa kan vara antagonistiska hot det vill säga att någon medvetet utnyttjar möjligheten att styra, reglera och övervaka processer.

En av de viktigaste anledningarna till den ökade sårbarheten hos SCADA-systemen är kvalitetsbrister ur ett säkerhetsperspektiv i hård- och mjukvara. SCADA-systemen har utvecklats under årtionden. Idag är de så pass avancerade (innehåller mycket komplex programvara) att de i praktiken är omöjliga att fullständigt testa för att hitta alla eventuella kvalitetsbrister. Ett exempel på effekter av sådana kvalitetsbrister är den stora blackouten i USA 2003. Den hade som en utlösande faktor felaktigheter i programvaran för det existerande SCADA-systemet (US-C PSOTF, 2004).

Det finns idag ett flertal aktörer i världen som, inom ramen för sin verksamhet, studerar risker och sårbarheter vid användandet av SCADA-system. Dessa olika grupper har olika utgångspunkter och inriktningar för sina verksamheter beroende på var de befinner sig organisatoriskt. Kvaliteten på de arbeten som genomförs synes också skifta. Mer om detta återfinns i kapitel 4 i denna rapport.

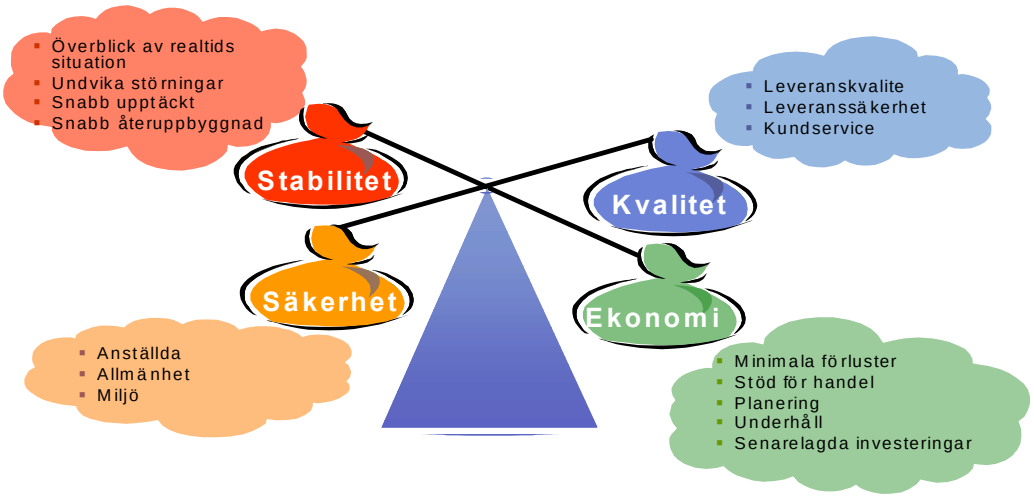
1.5 Vad är SCADA-system och varför behöver samhället dessa system?

För att övervaka och styra fysiska processer i realtid behövs information direkt från den övervakade processen. De processer vi diskuterar i denna rapport är ofta stora och innehåller ansenliga mängder information som skall insamlas i realtid (det vill säga med minsta möjliga tidsfördröjning). De skall dessutom presenteras på ett rationellt och överskådligt sätt för de personer (operatörer) som är ansvariga för driften. Processerna kan innehålla hundratusentals mätpunkter (ofta spridda över geografiskt stora områden) som kontinuerligt skall samlas in och övervakas. Vidare kan tiotusentals olika objekt ute i processen behöva manövreras (fjärrstyras). Eftersom de kritiska processerna ofta är känsliga för olika former av störningar, är det av yttersta vikt att den information som presenteras för operatören (och de avancerade applikationerna) är korrekt och verkligen visar processens nuvarande och verkliga tillstånd.

I denna komplexa informationsvärld är processoperatörerna ansvariga för många olika aspekter av driften. De fyra viktigaste övergripande kraven på driften av processen handlar om (utan prioritetsordning):

1. processens stabilitet
2. ett ekonomiskt och optimalt utnyttjande av processens resurser
3. säkerheten för de människor som arbetar i processen eller omgivningen
4. kvaliteten av den vara som processen skall leverera.

Dessa krav är ofta motstridiga och operatörerna måste därför väga dem mot varandra i realtid (se Figur 3).



Figur 3. Avvägning mellan olika operationella aspekter.

Utöver denna ständiga driftavvägning kommer som en effekt av bland annat avregleringar ett allt hårdare utnyttjande av tillgängliga resurser, det vill säga processens resurser används allt närmare deras fysiska begränsningar. För att klara ovanstående krav krävs det intelligenta, pålitliga och ständigt tillgängliga datoriserade verktyg och hjälpmedel.

Det är i denna värld som SCADA-systemen kommer in. De samlar in information från den primära (fysiska) processen och presenterar denna information för process-operatörerna. På grund av den mycket stora mängden information som processen levererar måste SCADA-systemen snabbt kunna göra ett intelligent urval av den för tillfället viktigaste informationen, och göra operatörerna uppmärksamma på precis denna information.

Operatörerna behöver kunna använda SCADA-systemet för att styra processen, till exempel för att öppna en brytare i elnätet eller stänga en ventil i en gasledning. Denna styrmöjlighet måste i princip alltid vara tillgänglig. Styrningen kan antingen ske direkt via manuell inmatning, automatiskt av SCADA-systemet eller genom att operatören initierar automatiska sekvenser.

SCADA-systemen används även för att ändra driftläggningen i den övervakade processen, till exempel vid utbyte av felaktiga enheter, och för planerat underhåll. Vid dessa tillfällen finns i allmänhet personal som arbetar direkt i processen och dessa människors säkerhet måste garanteras. Därför är en viktig del av SCADA-systemets uppgifter att planera dessa ändringar av driftläggningen, testa om ändringarna kan komma att äventyra processens stabilitet samt att utföra driftomläggningar i nära samarbete med fältpersonal. Det är också angeläget att markera för andra operatörer att en viss del av processen är under förändring så att inga återkopplingar sker av misstag.

SCADA-systemet måste också säkerställa så långt som det är möjligt att operatörerna inte gör misstag. Ett exempel på en sådan operatörskontroll är att dela in den över-vakade processen i områden, och låta bestämda operatörer endast ha tillåtelse att utföra fastställda åtgärder inom bestämda områden i processen, så kallad behörighetskontroll.

Avancerade SCADA-system skall också kunna föreslå åtgärder som operatörerna skall utföra för att uppnå en optimal driftläggning. De skall till exempel minimera över-förningsförluster, varna för kritiska tillstånd och föreslå bästa möjliga åtgärder att styra bort processen från kritiska driftsområden.

SCADA-systemet skall även dokumentera allt vad som skett i och med processen. Alla spontana händelser (som att en brytare löser ut på grund av en signal från ett skyddsrelä) måste sparas på medier som möjliggör långtidslagring. Grafer skall kunna ritas över historiska förlopp. Alla åtgärder som operatörerna utför måste sparas, tidsättas och märkas med operatörens identitet. Olika typer av rapporter skall kunna framställas både för eget internt bruk och som följd av krav från myndigheter.

SCADA-systemen är sammanfattningsvis en nödvändig komponent för att effektivisera driften, säkerställa att inga person- eller sakskador inträffar, garantera stabiliteten samt dokumentera och rapportera händelseförlopp i en del av samhällets allra viktigaste infrastrukturprocesser.

1.6 Olika typer av SCADA-system

Det finns i princip två typer av SCADA-system sett från en konstruktionssynpunkt. Det ena, och det man vanligen avser med SCADA-system, är system som övervakar och styr geografiskt vitt spridda processer. Exempel på processer som övervakas med denna typ av system är elnät, gasnät, telekommunikationsnät, fjärrvärmenät och försörjning av dricksvatten. Dessa SCADA-system kännetecknas av långa geografiska avstånd, långsam kommunikation och centrala driftcentraler. Den andra typen av SCADA-system är till för övervakning och styrning av lokalt begränsade processer, till exempel inom en enstaka kraftstation, en petrokemisk industri, ett stålverk etc. Dessa SCADA-system kännetecknas av relativt snabb processkommunikation, korta avstånd och distribuerad funktionalitet. Denna typ av system brukar kallas processkontroll-system. Dessa två typer av SCADA-system bygger traditionellt på två olika systemlösningar baserade på de skilda förutsättningar som gäller, speciellt på skillnaden i kommunikationshastighet.

SCADA-system för de geografiskt spridda processerna använder vanligtvis en realtidsdatabas som avbildar processen i en centralt belägen driftcentral. Applikationer och presentationsverktyg arbetar mot denna databas. Däremot har lokala SCADA-system, på grund av de snabba kommunikationslösningarna som används (t.ex. fiber), möjlighet att hämta och skicka data direkt från och till givare och PLC:er (Programmable Logic Controllers). Därmed har systemen inte samma behov av en centraliserad lösning.

Angrepp på de mer lokalt begränsade SCADA-systemen får i teorin inte lika stora konsekvenser som ett noggrant och väl utfört angrepp på ett mer distribuerat SCADA-system. Det beror på att dessa lokalt begränsade system oftast är inneslutna inom mycket begränsade och avspärrade områden, vilka dessutom ofta är övervakade. De har också historiskt sett färre kopplingar till yttre datanät, och har ett mindre informationsutbyte med andra system. Dessa system är från en nationell synpunkt vanligen mindre känsliga eftersom en störning normalt inte får nationella följder även om de kan medföra synnerligen allvarliga ekonomiska konsekvenser för processägarna. Undantagen är vissa större anläggningar, såsom exempelvis ett kärnkraftverk eller ett oljeraffinaderi.

När det gäller nationell säkerhet ur ett SCADA-perspektiv är en säker drift och distribution av till exempel el, energi, vatten och spårbunden trafik av största vikt. Av

detta skäl kommer denna rapport i fortsättningen att fokusera på SCADA-system för geografiskt spridda processer och de följdverkningar som störningar i dessa system kan få för samhället i stort. En del av de slutsatser och rekommendationer som rapporten beskriver är dock lika applicerbara för de lokala SCADA-systemen.

2 UPPBYGGNADEN AV SCADA-SYSTEM UR ETT HISTORISKT PERSPEKTIV

För att förstå hela problematiken kring säkerhetsaspekter rörande SCADA-system krävs en förståelse för hur dessa verksamheter och system har utvecklats. Därför kommer rapporten i detta avsnitt att utifrån ett historiskt perspektiv belysa den evolution som SCADA-system genomgått under det senaste decenniet.

2.1 SCADA-evolutionens tre faser

Detta kapitel belyser förenklat SCADA-systemens utveckling i tre steg med exempel hämtade från elkraftsindustrin. Elkraftindustrin har varit tongivande för SCADA-systemens utveckling och andra områden har i princip övertagit denna industris system-lösningar (möjligen med undantag för övervakningssystem för telekommunikations-processen).

Beskrivningen har koncentrerats på hur, varför och under vilka tekniska förutsättningar som SCADA-systemen utvecklats, och vilket fokus som denna utveckling har haft i olika faser. Detta för att öka förståelsen för varför SCADA-systemen av idag ser ut som de gör och varför vissa aspekter, till exempel skydd med avseende på IT-säkerhet, är så begränsade. Mer detaljerad information om dessa systems tekniska uppbyggnad i dagsläget (2006) står i Appendix A, SCADA-systemens uppbyggnad och konstruktion.

Detta avsnitt belyser SCADA-systemens historiska utveckling under tre tidsperioder:

1. system för ren datainsamling och fjärrstyrning (1930–1980-tal)
2. system med processmodeller för avancerade applikationer (1980–1995)
3. öppna, integrerade system med koppling till omvärlden (1995–idag)

Denna uppdelning är en grov förenkling ur ett SCADA-perspektiv men relativt funktionellt ur ett säkerhetsperspektiv.

2.2 System för ren datainsamling och fjärrstyrning

Redan mycket tidigt under 1930-talet användes analog teknik för att samla in mätvärden i realtid från mätpunkter ute i den geografiskt spridda processen. Dessa mätvärden skickades till en centralt placerad driftcentral som även fjärrstyrde objekt i processen. På elkraftssidan samlade man in data om effekter (aktiva och reaktiva) från kraftgeneratorer och från kraftlinjer inom det högspända överföringsnätet. Även data om läget hos viktiga brytare och frånskiljare samlades in. Möjligheten att fjärrstyra brytare och att skicka börvärden (önskade värden) till generator infördes också tidigt.

Den främsta anledningen till att införa denna typ av fjärrövervakning och fjärrstyrning var för att spara personal ute på fältet samt för att få en bättre överblick över det totala tillståndet i nätet.

Under 1960- och 1970-talen började man använda digitala datorer såväl i driftscentralerna som ute i processerna för insamlingen av mätvärden (spänning, aktiv och reaktiv effekt, status för brytare med mera). I själva kraftstationerna placerades mikrodatorer, så kallade Remote Terminal Units (RTU), och i driftcentralen användes minidatorer för att få ett övervakningssystem med kapacitet att samla in mycket större mängder data än tidigare. De nya systemen gav också möjlighet att presentera den insamlade informationen för operatörerna på ett mer överskådligt och intelligent sätt än tidigare då det endast fanns bildskärmar med begränsade grafiska möjligheter. En principskiss för de nya systemens uppbyggnad visas i Figur 4 även om användandet av lokala nätverk (LAN, Local Access Network) tillkom först under slutet av perioden.

En viktig parameter för hur konstruktionen av SCADA-system utvecklades under denna period var den begränsade tillgängligheten av kommunikation till transformatorerna och kraftstationerna i processen. Man hade endast tillgång till en kommunikationshastighet på 200 eller 600 bitar per sekund (baud) och i vissa fall så lågt som 50 baud. För att få tillräcklig snabbhet och säkerhet för att kunna upprätthålla den fysiska processen måste man tillgripa två konstruktionsprinciper som även återspeglas i dagens SCADA-system.

1. Den begränsade bandbredden för kommunikationen och kravet på datatillgänglighet ledde till att skräddarsydda kommunikationsprotokoll utvecklades. Det gällde att utnyttja varenda bit som skickades, samtidigt som det måste säkerställas att störningar i kommunikationen inte påverkade säkerheten i processen. Det fick inte förkomma att fel brytare manövrerades eftersom detta kunde leda till mycket allvarliga person- och sakskador. Kommunikationsmiljön runt elkraftsprocessen kan vara störd på grund av höga elektriska och magnetiska fält. Därför infördes flera paritetsbitar för att kunna upptäcka kommunikationsfel och även kunna korrigera sådana fel.

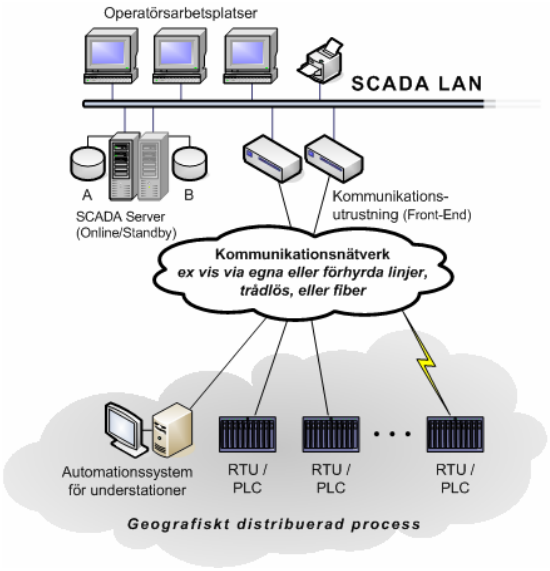
   Ingen diskussion om IT-säkerhet runt dessa protokoll förekom. Tack vare att varje leverantör av konkurrensskäl utvecklade sina egna, unika protokoll och på grund av att teknologin inte medgav andra lösningar blev protokollen ändå skyddade och mycket svåra att förstå (security by obscurity). En annan effekt av denna utveckling var att kunderna blev bundna till den ursprungliga leverantören.

2. Den långsamma kommunikationen gjorde det omöjligt att begära in information från givarna i själva processen när operatörna själva ville ha tillgång till tillståndet i processen. Istället insamlades data, i en från operatörerna oberoende process, till driftcentralen. Processens tillstånd avbildades så exakt

som möjligt i en realtidsdatabas. När operatörerna begärde fram processbilder på sina arbetsstationer för att visa processens tillstånd hämtades den dynamiska informationen direkt från realtidsdatabasen. På detta sätt kunde mycket snabba svarstider åstadkommas.

Funktionen för dessa tidiga system var enkel. Det gällde att samla in stora mängder mätdata, lagra dessa i driftcentralens SCADA-servrar, presentera processen tillstånd samt uppmärksamma operatörerna på förändringar via operatörsarbetsplatserna (Figur 4). Tidigare system presenterade oförädlade mätvärden från processen vilket krävde kunniga och pålitliga operatörer. Under senare år har mycket gjorts för att presentera den viktigaste informationen på ett så enkelt sätt som möjligt för operatörerna. Rapportering och dokumentation var andra viktiga uppgifter för systemen att hantera.

Utmaningen för leverantörerna hos dessa tidiga system låg i att behandla mycket stora mängder data med bibehållen hög prestanda samt att behärska de tidiga datorsystemens höga komplexitet. Utgångspunkten var också att endast utvald personal hade tillgång till SCADA-systemen rent fysiskt. Dessutom var det inga andra än operatörerna som kunde göra något med informationen. Därför var behovet och medvetenheten om IT-säkerhetsproblem med SCADA-systemen vid denna tidpunkt mycket låg, för att inte säga obefintlig, och därför ägnades dessa frågor ingen uppmärksamhet.



Figur 4. En schematisk struktur för ett grundläggande SCADA-system.

2.3 System med processmodeller för avancerade funktioner

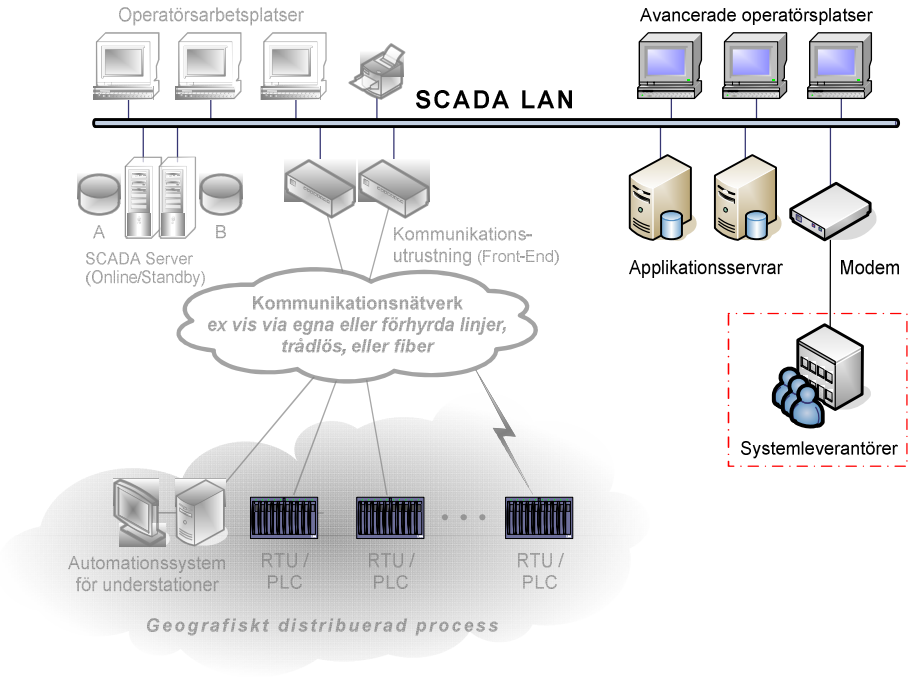
Under 1980- och 1990-talen ersattes gradvis de speciella minidatorer som tidigare använts, till exempel av typ VAX/VMS. Istället infördes mer kommersiella datorer med större användningsområde av typ Unix eller mot persondatorer ihopkopplade i ett snabbt och lokalt nätverk (Dy-Liacco 1994). Denna nya generation datorer innebar mycket mer datorkraft som kunde användas för kontrollen av processerna. En av de första förändringarna som gjordes tack vare denna datorkraft var att ersätta de tidigare semigrafiska arbetsstationerna med fullgrafiska. Semigrafiska bildskärmar har mycket begränsade grafiska möjligheter. Därmed ökade möjligheterna till betydligt mer avancerad presentationer.

En annan och kanske viktigare möjlighet med de kraftfullare datorerna var att tillämpa applikationer baserade på processmodeller. Dessa kunde med god noggrannhet *förutsäga* hur systemen skulle bete sig. Från att tidigare ha varit rena insamlings- och fjärrstyrningssystem av många enskilda mätpunkter, kunde man nu via processmodeller beräkna, förutsäga och optimera processens beteende. Användningen av processmodeller tog sin början inom elkraftsindustrin. Där hade man tillgång till relativt sett enkla men ändå fullständiga matematiska modeller. Exempel på sådana modeller är Ohms och Kirchhoffs lagar som kunde programmeras i högnivåspråk och lösas med en sådan noggrannhet att resultatet delvis kunde användas vid processtyrningen. Genom att använda SCADA-data tillsammans med en processmodell samt genom att utnyttja matematiska beräkningar kunde operatörerna övervaka och förstå processen på ett helt nytt sätt. Det blev nu möjligt att bland annat övervaka ställen i processen där inga mätningar fanns tillgängliga (State Estimator), beräkna framtida lastflöden efter planerade omkopplingar i nätet (Dispatcher Load Flow), testa potentiella felfall i nätet innan de inträffade (Contingency Analyses), minimera nätförlusterna (Optimal Power Flow), etc. SCADA-systemen kunde tolka förändringar och förädla information från processen där man tidigare varit hänvisade till erfarna operatörer.

System med applikationer började nu kallas SCADA/EMS, där EMS står för Energy Management Systems. Konfigurationer utökades med datorer för applikations-beräkningar och arbetsstationer för applikationsanvändare. SCADA-system fick ett typiskt utseende enligt Figur 5.

Det är viktigt att förstå att medan arkitekturen för SCADA-system enligt avsnitt 2.2, i princip är oberoende av den övervakade processen, är SCADA-system med avancerade applikationer och processmodeller unika för respektive process. De applikationer som nämnts ovan är elkraftsapplikationer men motsvarande funktioner finns för gas-, vatten-, och fjärrvärmesystem. Detta är förklaringen till att samma grundläggande SCADA-system från samma leverantör ofta finns i många processer men med olika uppsättningar applikationer.

Ett resultat av att använda de avancerade applikationerna var att det blev möjligt att utnyttja processerna betydligt närmare sina fysiska begränsningar, det vill säga närmare instabilitet. De tidiga och rena SCADA-systemen var framförallt ett sätt att spara personalkostnader via fjärrstyrning, medan de nya systemen blev en nödvändig förutsättning för driften, kanske framförallt vid återuppbyggnad efter störningar.



Figur 5. SCADA-system med avancerade funktioner.

Under denna period började kommunikationssystem med större bandbredd finnas tillgänglig. Detta ledde till att fler mätpunkter kunde användas och därmed behövdes fler komponenter. Vid denna utbyggnad var det lämpligt att göra systemen mer oberoende av leverantörer vilket medförde att en större opinion för en standardisering tog form. Det gällde framförallt RTU-kommunikationen där användarna ville undvika att vara beroende av en enskild leverantör i samband med utbyggnad. IEC (International Electrotechnical Commission) skapade nu standarder som kom att antas av alla större leverantörer av SCADA-system och RTU-tillverkare.

Ingen uppmärksamhet ägnades vid denna tidpunkt åt IT-säkerheten i dessa protokoll. Protokollen var mycket robusta mot olika typer av telekommunikationsstörningar men de var inte krypterade. Protokollen var byteorienterade och innehållet kunde enkelt

avlyssnas ifall man kom åt kommunikationsmediet. Protokollbeskrivningar var fritt tillgängliga för vem som helst att hämta.

Under denna period började SCADA/EMS systemen öppna upp sig mot omvärlden som framgår av Figur 5. Från att tidigare av skyddskäl ha haft systemen inlåsta i bergrum, flyttades datorutrustningen till allmänna datorrum. Det började bli möjligt att ringa upp SCADA-systemen via telefonmodem, framförallt för att ge leverantörerna möjlighet till fjärrfelsökning i den levererade programvaran. Via modemet fick då leverantören tillgång till hela programsystemet, och kunde införa vilka förändringar som helst. Denna typ av uppkopplingar avhandlades oftast på telefon varefter användarna tillfälligt kopplade in modemet och möjliggjorde access.

Några spektakulära och stora strömavbrott under 2003 (nordvästra USA och Kanada, Sverige och Italien) visar på SCADA-systemens betydelse då de var en av orsakerna till att störningen uppstod. Trots SCADA- och EMS-systemens allt större betydelse låg inte heller under denna period fokus på SCADA-systemens IT-säkerhetsaspekter.

Eftersom livstiden på SCADA/EMS-system är tio till femton år är många av dessa system från 1990-talet fortfarande i drift runt om i världen.

2.4 Öppna, integrerade system med koppling till omvärlden

I slutet av 1990-talet skedde en avreglering som resulterade i att tidigare vertikalt integrerade elbolag splittrades. Detta betyder att generering, transmission och ibland även distribution separerades. Elbolagen hamnade i en konkurrenssituation där tillgång till data, inklusive mätdata från processen, blev en strategisk tillgång. Eftersom SCADA/EMS-systemen är ägare till processdata blev det nödvändigt att öppna upp SCADA-systemen mot omvärlden på ett långt mer avancerat sätt än tidigare.

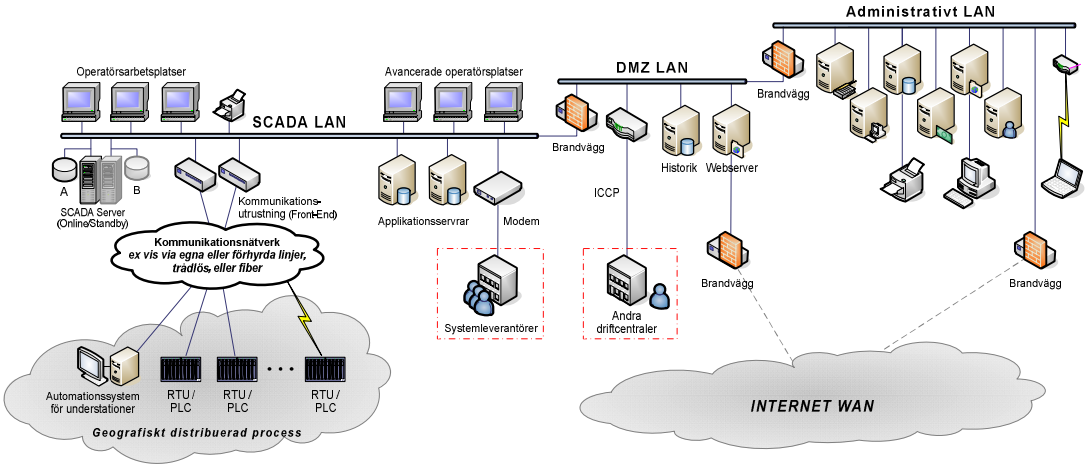
Det blev också nödvändigt att skapa avancerade arkivfunktioner inom SCADA/EMS världen för att kunna lagra råa och upparbetade processdata under långa tider. Databaser baserade på kommersiella relationsdatabaser av typ Oracle började användas och dessa gjordes tillgängliga för kontors- och planeringsanvändare.

För att inte äventyra realtidsdriften i driftcentralen (systemen var ju fortfarande lika kritiska för övervakning och styrning av stabiliteten hos processen) skapades speciella zoner på de lokala nätverken. Dessa zoner, så kallade Demilitarized Zones (DMZ), avskilde de rena kontorsnätverken från processnätverken. De olika nätverkstyperna isolerades med brandväggar (Figur 6).

Flera andra typer av system kopplades nu ihop med SCADA-systemen via DMZ, mer eller mindre hårt kopplade till SCADA-informationen. Exempel på sådana system är arbetsorderssystem (Work Order Management*)*, geografiska informationssystem (GIS),

underhållssystem (Asset Management), kundinformationssystem (CIS) samt allmänna företagsinformationssystem (exempelvis SAP).

Den snabba utvecklingen inom IT-området ledde till nya möjligheter att öppna upp SCADA-systemen mot Internet och intranätanvändare. Det blev – genom att känna till namnet på en webbserver eller en IP-adress och ett lösenord – möjligt att logga in och få tillgång till information från ett SCADA-system i drift.



Figur 6. Öppna, integrerade SCADA-system.

Olika driftcentraler började under denna period kopplas ihop via egna nätverk i olika typer av hierarkier. Till exempel kunde flera regionala driftcentraler kopplas via ett nätverk till en gemensam nationell driftcentral. Man använde nya öppna standardprotokoll för driftcentral kommunikation (Inter Center Communication Protocol, det vill säga ICCP eller TASE.2). Med dessa protokoll kan man samla in mätdata från underliggande driftcentraler samt även sända styrorder till processen. Dessa protokoll är normalt inte krypterade och det är en speciell utmaning ur IT-säkerhetssynpunkt att använda dem för att koppla samman SCADA-system från olika leverantörer.

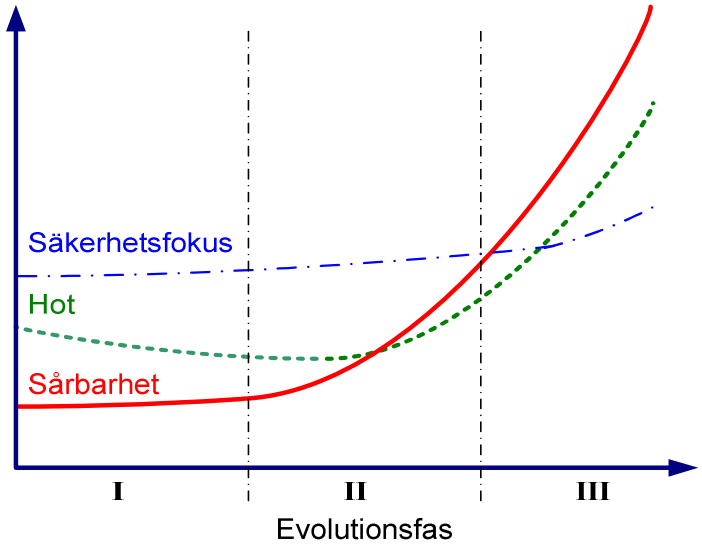
I och med att systemen öppnades upp mot allt fler användare började medvetenheten om IT-säkerhetsfrågor att höjas allt mer. Det första steget från användarna var att kräva uppdaterade virusskydd på samtliga datorer. På senare år, framförallt i USA, har det börjat ställas allt strängare krav på IT-säkerhet. Kraven åberopar standarder som

exempelvis NERC[8] CIP[9] och ISO/IEC 17799. Test och verifiering av SCADA-system har börjat genomföras av oberoende institut, till exempel Idaho National Laboratory.

2.5 Summering av informationssäkerheten i SCADA-system

Eftersom SCADA-systemen utgör en allt väsentligare del av själva infrastrukturen ökar även behovet av skydd för den information som SCADA-system hanterar. Förhållandevis lite utveckling har lagts på att skydda den känsliga informationen som finns lagrad i SCADA-systemen. Även skydd mot intrång i SCADA-system och illvilliga försök att skada systemen, eller skydd mot angripare som via SCADA-systemen försöker manipulera den underliggande kritiska processen, har helt eller delvis saknats.

Figur 7 avser att grovt åskådliggöra hur författarna till denna rapport uppfattar hur *cybersäkerhetsaspekterna* i dagens SCADA-system **inte** har utvecklats i takt med sårbarheter och hot under de tre beskrivna evolutionsfaserna.



Figur 7. Cybersäkerhet, sårbarhet respektive hot i relation till SCADA-evolutionsfaserna.

[8] North America Electrical Reliability Council
[9] Critical Infrastructure Protection

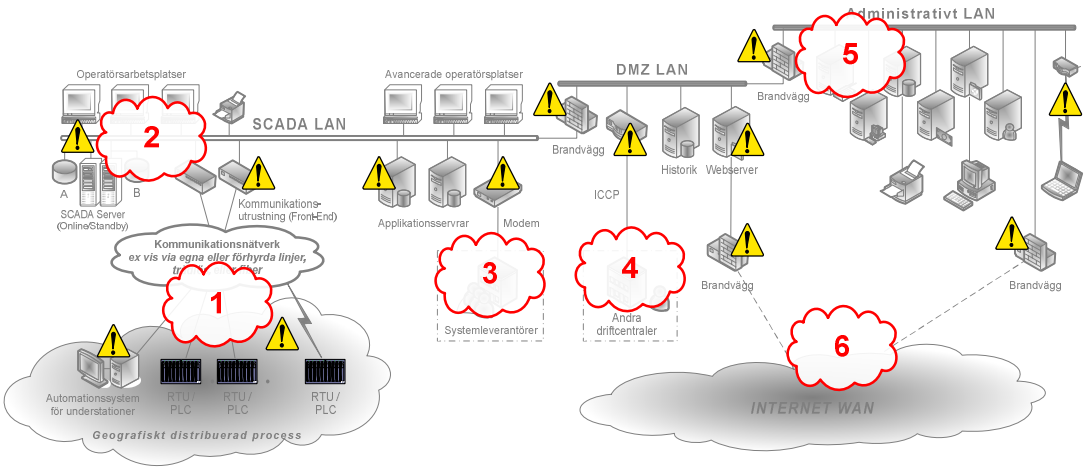
I den tidiga första evolutionsfasen var SCADA-systemen relativt enkla, sårbarheten låg och säkerheten förhållandevis hög i relation till den rådande hotbilden (vilken då framförallt var fysisk påverkan vid anläggningar).

I den andra evolutionsfasen blev SCADA-systemen allt mer komplexa samtidigt som mer och mer av utrustningen köptes in från tredjepartsleverantörer. Sårbarheterna i dessa system ökade medan hotbilden förblev relativt låg. Driftcentralerna flyttades ut från skyddade bergrum till normala kontorsbyggnader.

I den tredje evolutionsfasen med öppna, integrerade system kopplade till omvärlden, ökade sårbarheterna betydligt. Den generella hotbilden i samhället och medvetenheten om dessa hot har dessutom ökat väsentligt under senare år. Detta har skapat en farlig klyfta som illustreras i Figur 7

Följande avsnitt ger en kortfattad summering av de viktigaste IT-säkerhetsaspekterna som måste hanteras i samband med dagens SCADA-system. Diskussionen sker med utgångspunkt från sex olika systemkomponenter (Figur 8):

1. processdatainsamlingen
2. driftcentralsystemet
3. fjärrdiagnostik
4. driftcentralkommunikation
5. kontorsnät
6. Internet och intranät.



Figur 8. IT-säkerhetsaspekter i moderna SCADA-system.

Generellt sett kan sägas att det som är mest SCADA-specifika problem finns naturligt i komponenterna 1–3 (se även Figur 8) eftersom det är här unik SCADA-hård- och

mjukvara finns. Till exempel leder säkerhetssvagheter i operativsystem (dvs som ej har kontinuerligt uppdaterats när svagheter identifierats) hos de underliggande systemen samt säkerhetssvaga implementeringar av unika SCADA-protokoll till att det total SCADA-systemet i komponenterna 1-3 har många och vissa fall kritiska sårbarheter. Ett exempel på en relativt unik SCADA-sårbarhet är att de SCADA-protokoll som används ofta av administrativa skäl enbart utnyttjar en begränsad mängd portar för sin kommunikation (i praktiken används oftast bara en TCP/IP-port) vilket gör systemet känsligare för så kallad denial-of-service-attacker (DoS) mot dessa specifika portar.

Dessutom kan det vara svårt att införa traditionella IT-säkerhetsmekanismer bland komponenterna 1–3 helt enkelt på grund av de designbegränsningar som de hårda realtidskraven ställer på dessa. Realtidskraven försvårar även möjligheten att säkerhetsuppdatera de olika delarna i systemkomponenterna 1–3. Nedan ges exemplifieringar av IT-säkerhetsaspekter i de olika systemkomponenterna.

1. Processdatainsamlingen

Ägare och användare av SCADA-systemen antar ofta att deras SCADA-kommunikationsnät är väl skyddade, bland annat eftersom kommunikationer med processutrustningen (såsom med PLC:er och RTU:er) ofta använder sig av en unika protokoll för branschen (baserat på exempelvis RS-232, RS-485 med Modbus, DNP eller IEC 870) som få känner till. Det antas dessutom att datakommunikationen dessutom sker över egna telefonlinjer, bärvåg på kraftlinjerna, radiosystem eller fiber vilket ofta ökar känslan av säkerhet. Denna känsla är delvis falsk eftersom även dessa kommunikationslinjer enkelt kan avlyssnas samtidigt som tillgängligheten till kommunikationsmediet ofta är större för otillbörlig personal än vad som vanligen uppfattas. Branschspecifika SCADA-protokoll har sällan något inbyggt säkerhetsskydd. Detta håller på att förändras men det tar tid att dels hitta IT-säkerhetslösningar som passar dessa protokoll, dels införa dessa lösningar på alla ställen där de behövs. De protokoll som nu används är öppna standarder där protokollbeskrivningar kan laddas ned från Internet och sedan analyseras för att identifiera sårbarheter[10].

2. Driftcentralsystemet

Program- och hårdvara i driftcentralen är verksamhetskritiskt och måste fungera dygnet runt årets alla dagar. Detta för att möjliggöra fullständig övervakning av processens status, och på så sätt kunna initiera stabiliserande åtgärder om och när störningar inträffar. Dessa applikationer är oftast mycket speciella och framtagna av SCADA-

[10]Filmen *MODBUS Hacking, Security Video 2.0*, framtagen av British Columbia Institute of Technology. Där hackas protokollet MODBUS som används av en PLC

leverantören tillsammans med slutanvändaren. Dock är systemen i driftcentralen driftsatta på kommersiella plattformar av typ Windows eller Unix och skulle kunna utsättas för exempelvis följande typer av attacker:

- använda denial-of-service-attacker (DoS) för att krascha en SCADA-server vilket leder till nedsläckning av system
- logga tangenttryckningar för att få tag på användarnamn och lösenord
- logga företagskänsliga driftdata
- ändra datapunkter eller vilseleda operatören till att tro att processen är utan kontroll och behöver stängas av.

Andra typer av hot mot själva driftcentralen kan vara rent fysiska attacker. Något som kanske är troligare, är attacker från en missnöjd medarbetare (eller en antagonist med tillräckliga resurser och uthållighet som tar anställning) hos en användare eller en leverantör och som planterar in illvillig kod (exempelvis en trojan) i systemen innan de levereras i syfte att sabotera, idka utpressning eller liknande. En sådan kod skulle kunna fjärrstyra processen utan manuella ingrepp eller helt enkelt krascha systemet och göra det omöjligt att återstarta.

I princip samma typ av hot som ovan men kanske långt allvarligare är att källkoden för SCADA-systemet traditionellt har medföljt leveransen. Detta har sitt ursprung i att slutanvändarna har krävt att kunna modifiera källkoden själva, till exempel genom att göra egna felrättningar eller för att programmera funktionella tillägg. Detta har medfört att källkoden för de stora SCADA-systemen har spridits runt hela världen, inklusive till länder som står nära terroristorganisationer. Eftersom leverantörerna naturligtvis vill sprida sina utvecklingskostnader över så många kunder som möjligt byggs SCADA-system med maximal grad av återanvändning av programvarukomponenter. Därmed kommer även källkoden att spridas över ett stort antal levererade system. Det har medfört att det möjligt att studera källkoden från ett projekt och för att senare kunna attackera hundratals system från samma leverantör.

3. Fjärrdiagnostik

Som nämnts ovan började man under den andra evolutionsperioden införa möjligheter för de ursprungliga leverantörerna att genomföra felsökningar av systemen på distans och även införa felrättningar eller andra uppdateringar. Detta skedde oftast med hjälp av uppringda linjer där inkoppling av modem eller liknande utfördes av SCADA-ägarna efter överenskommelse på telefon. På detta sätt fick systemanvändaren kontroll över när dessa aktiviteter förekom. Eftersom leverantören vid dessa tillfällen måste kunna uppdatera programvaran finns ingen egentlig begränsning eller kontroll av vilken kod

som uppdaterades. Det vore alltså fullt möjligt att utan problem vid dessa tillfällen, illvilligt eller av misstag, förstöra systemet eller införa trojaner i det.

4. Driftcentralkommunikation

Via kommunikation med andra driftcentraler med standardiserade och publika protokoll (till exempel ICCP[11]) öppnas möjligheten att införa felaktig process-information till driftcentralen, eller till och med fjärrstyra processen. Det betyder att en viss driftcentral, kanske den svagaste länken, har möjlighet att skicka meddelanden till andra driftcentraler om falska processändringar eller med begäran om att styra process-objekt. Överenskommelser om vilka data som skall utbytas, och därmed vilka delar i processen som kan övervakas och styras, sätts dock upp i ömsesidiga överens-kommelser så att data som inte är definierat för utbyte är dolt för andra driftcentraler. Detta har införts av prestandaskäl men har även en säkerhetshöjande effekt.

5. Kontorsnät

Många personer i verksamheterna som inte arbetar direkt med SCADA-systemen tror ofta att dessa system sitter separerade från kontorsnätverken och att de därför är säkra från externa cyberhot. Detta antagande är tyvärr alltför ofta helt felaktigt.

Dagens SCADA-system är oftast ihopkopplade med andra nätverk, vilket gör att de lider av samma problem som drabbar alla andra företagsnätverk. Visserligen används brandväggar men dessa i sig utgör inte ett säkert skydd. För att göra informationen i SCADA-systemen tillgängliga för kontorsanvändare måste portar i brandväggen öppnas, vilka kan möjliggöra för otillåtna användare att nå SCADA-informationen. SCADA-informationen är visserligen skyddad med ett lösenord, men detta skydd kan kompromet teras.

Många SCADA-system öppnar dessutom upp för mer avancerad användning från kontorsnät med möjligheter att direkt uppdatera SCADA-information eller möjligheter att starta tjänster i SCADA-plattformen, exempelvis att sända styrorder till processen.

Det är uppenbart att ett av de enklaste sätten att nå och påverka dagens SCADA-system och dess kritiska information är via kontorsnäten hos de bolag som äger och styr de samhällskritiska processerna.

6. Internet och intranät

[11] Inter Control Center Communications Protocol

Den dominerande trenden i samhället i dag är användandet av Internet i alla delar av olika organisationers verksamhet. Också SCADA-systemen har idag gränssnitt mot Internet eller lösningar med bolagsunika intranät. Enligt författarnas vetskap har hittills inte lösningar använts där det är möjligt att styra processen med direkta kommandon via Internet, utan Internet- och intranätlösningar används uteslutande för presentation. Dock är tekniska lösningar för att enkelt införa denna form av styrning tillgängliga.

Till slut bör helt kort två andra viktiga säkerhetsfaktorer nämnas i samband med dagens SCADA-system vilka dock är av intresse för alla typer av IT-system. Dagens SCADA-system är i hög grad beroende av stöd från flera, till huvudorganisationens externa, organisationer såsom system- och tjänsteleverantörer. Detta innebär att SCADA-system är i allt högre grad även beroende av det säkerhetsarbete som dessa externa organisationer bedriver.

Ytterligare en viktig säkerhetsfaktor hos SCADA-system är de kulturella skillnader beträffande säkerhetsarbetet som ofta råder i de organisationsdelar som arbetar med SCADA-systemen. Traditionellt sett är organisationsdelarna som ligger nära SCADA-systemen ovana att tänka i IT-säkerhetstermer samtidigt som IT-säkerhetspersonal är ovana att tänka i mer processnära SCADA-termer.

Sammanfattningsvis kan man säga att säkerhet (med ett antagonistperspektiv) hittills inte varit den huvudsakliga drivkraften för utveckling inom SCADA-systemområdet. Istället har det har varit behovet av olika typer av funktionalitet som dominerat utvecklingen. Samverkan mellan de ständigt mer lättåtkomliga attackmetoderna och den större skada dessa kan orsaka utgör ett allt mer växande säkerhetsproblem. Denna lucka är svår att överbrygga och det är idag ytterst osäkert om hur stora konsekvenser ett framtida bakslag kan komma att få.

Rent generellt handlar åtgärdsinsatserna för att höja säkerheten SCADA-system om att härda systemen (precis som vanliga IT-system) såväl cybermässigt som fysiskt. Men med den skillnaden att man har mycket högre krav på säkerhet i SCADA-miljön, som dessutom är en mycket mer komplex och okänd miljö (än vanliga IT-system). Det finns inte heller många explicita råd på en teknisk nivå som det finns för administrativa IT-system. Det har flera orsaker. Bland annat beror det på att det är svårt att uttala sig generellt om SCADA-system eftersom dessa system ser så olika ut hos olika användare. Det finns emellertid utkast till riktlinjer för vad man skall begära att leverantörer av SCADA-system skall göra med avseende på exempelvis härdning av system[12].

[12] http://www.cscic.state.ny.us/msisac/scada/documents/1-aug-06-scada-procurement-draft-1.4.pdf

3 CYBERATTACKER MOT SCADA-SYSTEM

I detta kapitel beskrivs den öppet tillgängliga *historik* som finns om cyberattacker mot SCADA-system samt den verksamhet som pågår för att identifiera den kunskap och de trender som är viktiga för att förstå cyberhotet mot SCADA-system i ett framtidsperspektiv.

3.1 Hotaktörer

I denna rapport avses med attacker (cyberattacker) en verksamhet där angriparen med en hjälp av en illasinnad kod eller med obehörig access till ett system slår mot eller utnyttjar de informationstekniska resurser i SCADA-systemen som har beskrivits i tidigare kapitel. Det betyder att de hotaktörer som är relevanta vid attacker mot administrativa IT-system teoretiskt sett även är relevanta vid attacker mot SCADA-system. Dessa generiska hot mot SCADA-system utgörs av (NISCC, 2004):

- Främmande stater. De kan ha avsikter av fientlig eller underrättelsekaraktär.
- Terrorister. Dessa kan ha som avsikt att lägga cyberattacker till sin arsenal.
- Aktivister. Dessa kan ha som avsikt att genomföra publicitetsskapande attacker.
- Hackare (crackers) och virusskapare. Motiveras framförallt av utmaning och en fascination över högteknologi.
- Insider. Det vanligaste kända motivet för insiderverksamhet är hämnd. I denna grupp kan såväl anställda som tidigare anställda ingå.
- ”Script kiddies”. Dessa är oftast fientligt inställda mot allt på Internet eller spänningssökande i allmänhet.

Exempel på attacker mot SCADA-system där dessa hotaktörer förekommer beskrivs kortfattat nedan (Naedele et al., 2005a):

- Mars 2000: En missnöjd tidigare konsult tar kontroll över kontrollsystemet för ett vattenreningssystem i Australien. Konsekvensen av attacken blir att tusentals kubikmeter obehandlat vatten översvämmar området.
- December 2000: En grupp hackare angriper ett datornätverk i en kraftanläggning (power utility) i USA genom att utnyttja svagheter i ett använt protokoll. Sedan användes det övertagna nätverksresurserna för att spela datorspel. Detta utnyttjande av dator- och nätverksresurser hindrar påtagligt

möjligheten för anläggningen att bedriva affärer med sin elkraft (electricity trading).

- Januari 2003: Driftsäkerhetsövervakningssystemet vid kärnkraftverket Davis-Besse i USA, som vid tillfället är avställt, infekteras med Slammermasken. Systemet är ur funktion i nära fem timmar. Orsaken är dels en fel uppsatt förbindelse in i kärnkraftverkets datornät, dels en dator utan virusskydd som betraktas som fristående och därmed inte i behov av skydd. Det finns redundanta, analoga reservsystem som är opåverkade av masken men operatörerna vid verket får en avsevärt ökad arbetsbelastning.
- Augusti 2003: En amerikansk tågoperatörs datornätverk för signalering infekteras av en mask vilket leder till att alla operatörens tåg står stilla i en halv dag.
- Maj 2004: SASSER-masken infekterar ett signal- och kontrollsystem hos den australiensiska lokaltågsoperatören Railcorp. 300 000 pendlare till och från Sydney saknar transportmedel under en dag.

Attackerna vid de ovan nämnda incidenterna genomfördes av olika hotaktörer. Dessa angripare var i fallet med

- avloppssystemet – en insider
- kraftanläggningen – en grupp hackare
- kärnkraftsverkets och de två tågoperatörernas system – infektioner av maskar som troligen konstruerats av vanliga virusskapare; maskarna var inte speciellt avsedda för att slå mot dessa system.

Det är viktigt att notera att alla dessa antagonistiskt relaterade incidenter härrör från vad man skulle betrakta som icke-kvalificerade antagonister.

När det gäller de andra typerna av hotaktörer – främmande stater och terrorister – finns det färre exempel. När det gäller hotaktören terrorister finns det inga kända fall av angrepp på SCADA-system (US-CERT CSSC, oktober 2005). När det kommer till främmande stater som attackerar SCADA-system i någon annan nation finns det ett enda känt exempel. Det härrör från 1982 och handlar om hur den amerikanska underrättelsetjänsten CIA placerade en trojan i koden till ett kanadensiskt tillverkat SCADA-system som sedan sovjetiska underrättelsetjänsten KGB ”stal” från SCADA-leverantören för att brukas i Sovjetunionen. Attacken beskrivs i ett amerikanskt myndighetsdokument (DoE, 2006):

> *While the following cannot be fully confirmed, it has been reported that during the Cold War the CIA inserted malicious code into control system software leaked to the Soviet Union. The software, which controlled pumps, turbines, and valves on a Soviet gas pipeline, was programmed to malfunction after a set interval. The malfunction caused the control system to*

> *reset pump speeds and valve settings to produce pressures beyond the failure ratings of pipeline joints and welds, eventually causing an enormous explosion.*

Denna incident har till vissa delar verifierats av en före detta underrättelseofficer i KGB (Cherkashin, 2005).

När det gäller en bedömning av olika angripares avsikter med att angripa SCADA-system är det rimligt att anta att det allvarligaste och mest troliga motivet att förbereda och genomföra sabotage mot den verksamhet som SCADA-systemet stödjer. Andra tänkbara motiv, men möjligen mindre sannolika, är att attackera system i utpressningssyfte. Anledningen till att detta är mindre sannolikt är helt enkelt att det finns andra system att angripa som ger avsevärt större finansiell vinst med avsevärt mindre insats. Bedömningar av olika angripares förmåga att angripa SCADA-system ligger utanför denna rapport och det är dessutom utomordentligt svårt att bedöma med mer än att man bedriver såväl egen testverksamhet som underrättelsesinhämtning.

Generellt sett kan det sägas att det finns mycket lite öppen information om inträffade incidenter i SCADA-system. En studie av öppen information rörande attacker mot SCADA-system anger att det är färre än 200 stycken under de senaste 35 åren (Rodriguez et al, 2006), (US-CERT CSSC, oktober 2005). Det finns för övrigt ingen tillgänglig öppen information om någon inträffad SCADA-säkerhetsincident i Sverige. I de öppna incidentdatabaser som finns är det svårt att söka på SCADA-incidenter eftersom de saknas sökbara begrepp i dessa databaser som relaterar specifikt till SCADA. De databaser som specifikt hanterar SCADA-incidenter är alla skyddade på något sätt och inte allmänt tillgängliga. Några orsaker till att det finns så lite öppen information om inträffade attacker mot SCADA-system kan var att det saknas etablerad standard för incidentrapportering eller organisation som tar emot incidentinformationen och att informationen som berörs ofta är mycket känslig. Det kan till exempel röra information som definitionsmässigt betraktas gälla rikets säkerhet.

3.2 Analys av inträffade SCADA-säkerhetsincidenter

I oktober 2005 publicerades en studie av det amerikanska nationella säkerhets-laboratoriet Idaho National Laboratory, som bland annat hanterar US-CERT Control Systems Security Center, med titeln Cyber Incidents Involving Control Systems (US-CERT CSSC, oktober 2005). Syftet var bland annat att

- etablera goda exempel för att motivera organisationer att satsa på SCADA-säkerhet (”business cases” för SCADA-säkerhet)
- utveckla metoder för rapportering och analys av SCADA-säkerhetsincidenter.

Studien resulterade i att 120 incidenter valdes ut efter analys av en rad olika källor[13] som bedömdes kunna innehålla information om attacker mot SCADA-system. De utvalda incidenterna ansågs viktiga ur perspektivet att de gav underlag om cyberterroristhotet mot SCADA-system. Detta hot anses som prioriterat av amerikanska myndigheter. De 120 incidenterna hämtades från fem av de tolv studerade databaserna och ingen av dessa fem databaser är tillgängliga för allmänheten. Det skall dock understrykas att alla incidenterna inte orsakades av en angripare med ont uppsåt utan att vissa av dem berodde på rena handhavandefel av SCADA-systemen. De utvalda incidenterna analyserades ur perspektiven typ av incident, varifrån incidenten initierades, typ av angripare samt angriparens motiv och presenterades översiktligt i rapporten. Nedan presenteras nämnda studies resultat kortfattat i fyra diagram. Det bör understrykas att de kategoriseringar som används för presentationen av resultaten inte är exklusiva vilket leder till att tolkningen av resultaten är behäftade med osäkerheter.

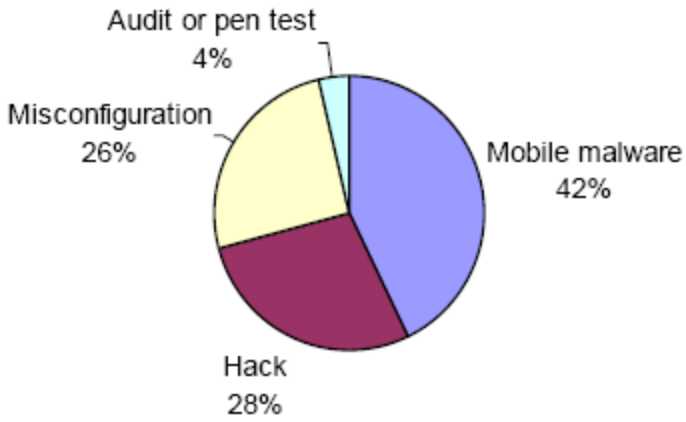
3.2.1 *Typ av incident*

I studien ansågs det relevant att dela upp de analyserade incidenterna i kategorierna gransknings- eller penetrationstester (audit or pen test), användarfel (misconfiguration), riktade attacker (hack) och mobil illasinnad kod (mobile malware). Med typen användarfel avses här att en legitim användare av systemet och utan ont uppsåt har hanterat systemet på ett sådant sätt att incidenten har uppstått. Med mobil illasinnad kod avses maskar och virus.

[13] Källorna var

- Industrial Security Incident Database (ISID; British Columbia Institute of Technology [BCIT] proprietary)*
- Energy Incident Database (proprietary)*
- National Memorial Institute for the Prevention of Terrorism (MIPT)
- Process Control Cyber Security Forum
- National Counterintelligence Center
- Embedded systems failures
- Supervisory Control and Data Acquisition (SCADA) discussion list
- SysAdmin, Audit, Network (SANS) Institute
- 2003 CSI/FBI Computer Crime and Security Survey
- Kema Inc.:s Informal Process Control System Cyber Impact Database*
- Lawrence Livermore National Laboratory (LLNL)*
- Idaho National Laboratory (INL) Cyber Incident Database.*

De med * markerade var de som bidrog med underlag till de 120 utvalda SCADA-säkerhetsincidenterna

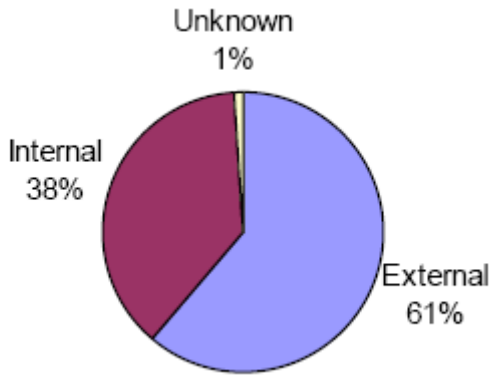


Figur 9. Typer av attacker mot SCADA-system (US-CERT CSSC, okt 2005).

Det är intressant att konstatera att riktade attacker utgör en så pass stor del som 28 procent. När det gäller typen maskar och virus, en incidenttyp som dominerar med 42 procent, är det okänt om, men högst osannolikt att, dessa maskar och virus var speciellt avsedda för de SCADA-systemen som drabbades.

3.2.2 *Incidenternas ursprung*

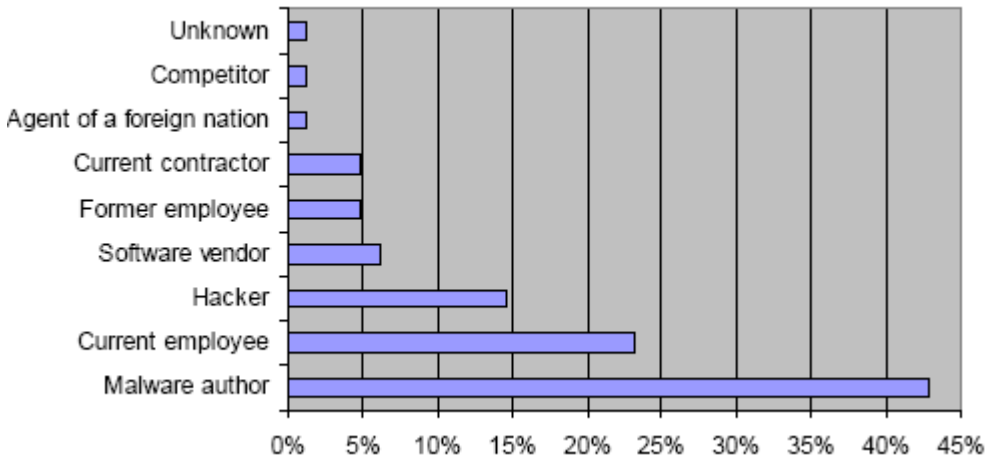
I studien ansågs det relevant att dela upp vari incidenterna initierades i kategorierna Internt (internal), externt (external), och okänt (unknown). Fördelningen var nästan 2/3 externt initierade incidenter och 1/3 internt initierade incidenter.



Figur 10. Varifrån SCADA-systemincidenterna initierades (US-CERT CSSC, okt 2005).

3.2.3 *Typ av angripare*

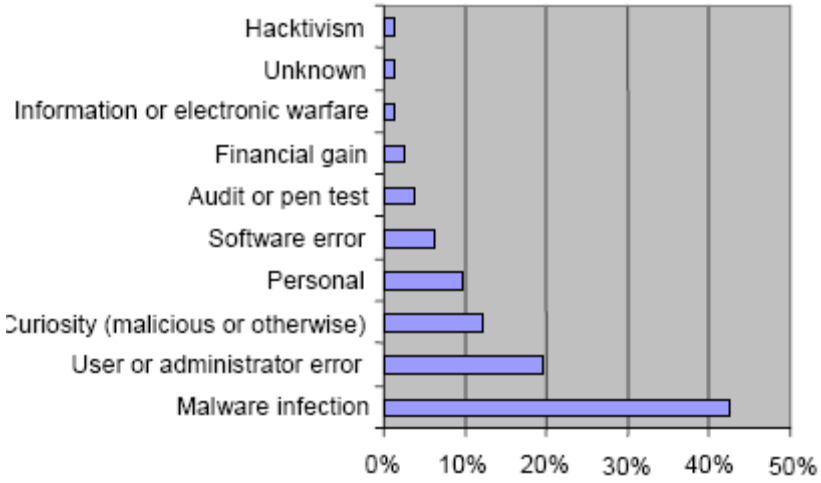
I studien delades typen av angripare in i följande kategorier; konstruktörer av illasinnad kod (malware authors), anställda (current employees), hackare, mjukvaruleverantörer (software vendors), tidigare anställda (former employees), konsulter (current contractors), underrättelsepersonal från främmande makt (agents from foreign nations) och okända (unknown). Konstruktörer av illasinnad kod dominerar med 43 procent och därefter kommer anställda med 23 procent.



Figur 11. Typ av angripare av SCADA-system (US-CERT CSSC, okt 2005).

3.2.4 *Angriparens motiv*

I studien ansågs det relevant att dela upp angriparens motiv i följande kategorier; spridning av illasinnad kod (malware infection), användarfel utan ont uppsåt (a result of user or administrator error), nyfikenhet (curiosity), personliga motiv (personal), mjukvarufel (software error*),* fel i samband med säkerhetsarbete (audit or pen test), ekonomisk vinst (financial gain) informations- eller telekrigföring (information or electronic warfare), okänt (unknown) och hacktivism (hacktivism). Spridning av illasinnad kod dominerar med 43 procent och därefter kommer användarfel utan ont uppsåt 20 procent.



Figur 12. Angriparens motiv för att ”angripa” SCADA-system (US-CERT CSSC, okt 2005).

3.2.5 *Tolkning av analysen av de utvalda SCADA-incidenterna*

De två övergripande slutsatserna av analysen av incidenterna är att

- det är anmärkningsvärt få incidenter inrapporterade
- majoriteten av dem härrör från ickeriktade attacker från ickekvalificerade angripare.

Tolkningen av dessa slutsatser kan vara att många SCADA-system ännu inte är tillräckligt externt uppkopplade för att till exempel ickeriktade attacker (virus och maskar) skall kunna slå mot dessa system. När dock externa kopplingar finns mot SCADA-system är dessa känsliga för normala ickeriktade attacker. Dessutom verkar attraktionskraften för att slå mot system inte vara särskilt stor ännu eftersom det är mycket få riktade attacker. Därutöver är det en total avsaknad av incidentinformation som berör kvalificerade angripare.

Ytterligare analys av de studerade incidenterna indikerar följande slutsatser (US-CERT CSSC, oktober 2005):

- Trenden för antalet incidenter ökar. Även Byres et al., 2004 och ett flertal industriexperter inom området anser att antalet incidenter är tiofaldigt större än det som kan ses i de källor som studien presenterar.
- När det gäller konsekvenserna av incidenterna kan dessa vara av olika karaktär (Byres et al., 2004). De uppskattade ekonomiska förlusterna från incidenterna är för närvarande låga och överstiger sällan en miljon dollar dock med reservation

för att det sällan görs monetära uppskattningar för IT-incidenter i allmänhet och för SCADA-incidenter i synnerhet eftersom det är synnerligen svårt (Christiansson, 2004).

- Av det ovanstående kan man dra slutsatsen att risken för nationell infrastruktur för närvarande är reell men mycket låg (risk = konsekvens x sannolikhet) dock med reservation för det otillräckliga historiska underlaget.
- Diskrepansen mellan antal attacker mot administrativa IT-system och SCADA-system anses bero på att terrorister och illasinnade stater hittills inte har uppfattat SCADA-system som attraktiva mål. Detta kan ha flera orsaker:
    - Värdet av data i IT-världen är ofta lättbegripligt (bankkontonummer etc.) medan värdet av data i SCADA-världen är svårbegripligt om man inte förstår de fysiska processer som SCADA-systemen hanterar.
    - För att åstadkomma avsevärd skada på SCADA-system krävs det detaljerad teknisk kunskap om de fysiska processerna. Högriskprocesser skyddas fortfarande av redundanta ickeelektroniska skyddssystem (dessa är inte angripbara med illasinnad kod).
    - Det är fortfarande lättare att angripa kritisk infrastruktur med fysiska medel.

Det skall återigen poängteras att underlaget i studien inte är tillnärmelsevis tillräckligt för att kunna göra några statistisk grundade utsägelser om SCADA-säkerhetsincidenter. Det leder till den viktiga slutsatsen att det behövs mycket bättre incidentrapportering, såväl kvalitativt som kvantitativt.

3.3 Bedömningar av den framtida risken för SCADA-säkerhetsincidenter

Det finns dock en potential för att riskerna för SCADA-incidenter i framtiden är avsevärt högre och med allvarligare konsekvenser. (Rodriguez et al, 2006), (US-CERT CSSC, oktober 2005) Det har följande förklaringar:

- Det blir lättare för angriparen när attackverktygen mot SCADA-system blir bättre och enklare att använda samtidigt som tillgängligheten till SCADA-systemen och kunskapen om dem blir bättre. Antalet applikationer i SCADA-systemen kommer också att öka vilket innebär att attackytan ökar. Fysiska attacker blir kanske mer svårtillgängliga och därmed mindre attraktiva.
- Angriparen kan slå mot flera olika infrastrukturer på en gång eftersom samma typer av SCADA-system förekommer i olika infrastrukturer (Christiansson, 2004). Det kan krävas lång planering och hög kompetens för att slå mot flera

infrastrukturer samtidigt, men själva genomförandet behöver inte kräva speciellt mycket och effekterna kan potentiellt sett bli stora.

- Upptäcktsrisken för attackeraren är mycket liten. Att spåra attacker mot SCADA-system är ännu svårare än attacker mot vanliga IT-system, eftersom
    - SCADA-systemen ännu inte har någon funktion för spårning av IT-säkerhetsrelaterade händelser
    - SCADA-systemen används skarpt och inte kan tas ur drift och är de ur drift är det högsta prioritet att få dem i drift.
- Attackerna kan samordnas med fysiska attacker vilket kan skapa mycket stor utväxling för angreppet i sin helhet

De ovannämnda punkterna är hypoteser och bedömningar som till stora delar bottnar i de erfarenheter som några av de amerikanska nationella laboratorierna[14] har byggt upp under den senaste femårsperioden (Kenchington, 2006) i sitt arbete med SCADA-säkerhet. Detta arbete sker på ett flertal olika sätt men framförallt genom

- säkerhetsanalyser av SCADA-system och SCADA-systemkomponenter i laboratoriemiljö
- säkerhetsanalyser i skarpa miljöer hos användare av SCADA-system.

Arbetet sker i nära samverkan med leverantörer och användare av SCADA-system. Det fungerar mycket väl eftersom de nationella laboratorierna anses som neutrala och dessutom mycket kompetenta inom SCADA-säkerhetsområdet. Denna bedömning framfördes av flera företrädare för såväl leverantörer och användare av SCADA-system, som statliga organisationer vid konferensen SANS SCADA Security Summit 2006. Vid detta arbete uppnås flera mål, nämligen: djupare kunskap om alla typer av sårbarheter som SCADA-systemen har; vilka egenskaper i form av vilka underrättelser och kompetens inom olika sakområden som angriparen måste besitta för att kunna angripa SCADA-system på ett kostnadseffektivt sätt; vilka åtgärder som kan vidtas för att avhjälpa sårbarheterna samt identifiera vilka trender som finns inom SCADA-området såväl hos leverantör som hos användare (Wells, 2006a), (Parks et al., 2005), (Rolston, 2005), (Duggan et al., 2005), (Davidson et al., 2004).

När det gäller de egenskaper som de nationella laboratorierna studerar vid säkerhets-analyserna finns det ingen internationellt vedertagen och etablerad standard, utan man har vid de nationella laboratorierna etablerat en praxis för praktiska säkerhetstester av

[14]Energidepartementets Idaho National Laboratory (INL), Lawrence Livermore National Laboratory (LLNL), Pacific Northwest National Laboratory (PNNL) samt Sandia National Laboratory (SNL). Dessutom tillkommer National Institute of Standards and Technology (NIST) som ligger under näringslivsdepartementet.

SCADA-utrustning. Denna praxis innebär att man säkerhetsanalyserar SCADA-systemen och dess komponenter om hur de hanterar funktioner som (Wells, 2006b)

- klartextkommunikation
- användarkontohantering
- verifiering av användare (autentisering)
- om god programmeringspraxis har tillämpats (ur ett säkerhetsperspektiv)
- förekomst av ickeanvända tjänster
- nätverksadressering
- hur system integreras med varandra
- om det förekommer ”opatchade” systemkomponenter
- om det förekommer ”Web services”
- perimeterskydd.

Funktionerna ovan kan i någon mening sägas motsvara funktioner som kan angripas specifikt i attacker mot SCADA-system. När man sedan genomför säkerhetsanalyserna gör man bedömningar ur framförallt två perspektiv, dels hur enkelt den specifika funktionen kan angripas, dels hur allvarligt för systemets funktion som ett eventuellt angrepp skulle vara[15].

Förutom säkerhetsanalyser ägnar de nationella laboratorierna tid åt att analysera hotet mot SCADA-system. Detta görs framförallt genom att man bevakar olika typer av IT-säkerhetsforum, ur såväl ett SCADA-säkerhetsperspektiv som ett IT-säkerhets-perspektiv, som till exempel hackerkonferenser och IT-säkerhetsdiskussionsforum på Internet och genom att följa trenderna på dessa[16]. Sedan kan denna information

[15] Vid analyserna används följande skala
- Ease of Attack
  - Elevated skill level with adequate time and resources
  - Enhanced Skill Level
  - Moderate skill level with commonly available tools
- Severity/Impact
  - Little affect on normal operations but may provide insight to system (i.e. enumeration)
  - Moderate impact to system (i.e. slow response)
  - Could bring system down or compromise integrity

[16] Några av de konferenser som INL har bevakat och specifikt pekat ut presentationer som berört SCADA-säkerhet är
- Blackhat USA 2005 – Shmoo Group presentation on 802.11 wireless networking within a nuclear power plant
- Toorcon 2005 – SCADA Exposed
- Blackhat Federal 2006 – SCADA Security and Terrorism: We’re Not Crying Wolf!

användas för att exempelvis konstruera attackmetoder speciellt anpassade för SCADA-system (Assante et al., 2006), (Larsen, 2006). En trend som särskilt framfördes vid konferensen SANS SCADA Security Summit 2006 var att man i en framtid eventuellt skulle behöva skydda centrala SCADA-komponenter från illasinnad kommunikation från fältutrustningen som eventuellt kommer att vara lätta att kompromettera.

Sammanfattningsvis kan man säga att allt det arbete som de amerikanska nationella säkerhetslaboratorierna bedriver syftar till att ta fram kunskap om såväl enkla som avancerade angripare och sedan nyttja denna kunskap på bästa sätt för att hjälpa leverantörer och användare av SCADA-system.

4 KARTLÄGGNING OCH VÄRDERING AV INFORMATION RÖRANDE SCADA-SÄKERHET

Kapitel 2 beskriver hur cybersårbarheter i SCADA-system har byggts in under årens lopp av olika orsaker. Detta bottnar ofta i att man vid tillfället för förändringen, och med den då gällande kunskapen och miljön, inte har krävt högre säkerhet än vad som sedan har anammats. När sedan miljön och förutsättningarna förändras leder det naturligt till att behovet av SCADA-säkerhet förändras. Som man lätt förstår är det många olika typer av kompetenser som rör sig inom SCADA-säkerhetsområdet vilket gör det synnerligen svårt att bedöma riktigheten och relevans i den information som produceras. I detta kapitel analyseras och värderas tillgänglig information om SCADA-säkerhet. Detta ger information om vilka delområden inom SCADA-säkerhetsområdet som betraktas av andra parter som viktiga och vilka aktörer som är kunniga inom området. Detta är viktigt för att kunna prioritera det fortsatta arbetet samt skapa samarbete med strategiskt viktiga aktörer.

4.1 Olika utgångspunkter vid SCADA-säkerhetsstudier

Olika grupper inom SCADA-säkerhetsområdet har olika utgångspunkter och inriktningar för sina verksamheter beroende på var de organisatoriskt befinner sig. Kvaliteten på de arbeten som de genomför synes också skifta. De aktörer som kan utskiljas inom området är (Hildick-Smith, 2005):

- Användare av processkontroll- och SCADA-system. Dessa genomför risk- och sårbarhetsanalyser av sina SCADA-system. Svenska aktörer är till exempel Vattenfall, Eon, Fortum, Svenska kraftnät, Banverket, Stockholms lokaltrafik, Stockholm vatten och Preem.
- Leverantörer av processkontroll- och SCADA-system. Dessa arbetar med säkerheten i sina produkter på olika sätt. ABB, Cactus, Cisco, Netcontrol och Siemens är bara några exempel på leverantörer som levererar SCADA-system till svensk infrastruktur. Beträffande intresset för säkerhetsarbetet hos leverantörerna så styrs det idag i hög grad av beställaren och vad denne är beredd att betala.
- Konsulter inom processkontroll- och SCADA-systemområdet. Dessa erbjuder specifika expertkunskaper inom olika delar av området. Kema och PA Consulting Group är några av de konsultbolag som arbetar inom SCADA-säkerhetsområdet. De utför arbeten åt såväl amerikanska Department of Homeland Security (US DHS) som brittiska National Infrastructure Security Co-ordination Centre (UK NISCC).
- Forskare vid universitet och högskolor utför tillämpad forskning och tekniska studier. British Columbia Institute of Technology (BCIT) är det mest kända

akademiska forskningscentret när det gäller SCADA-säkerhet de samarbetar med såväl amerikanska nationella säkerhetslaboratorier som UK NISCC. I Sverige bedriver framförallt KTH:s avdelning för Industriella informations- och styrsystem (ICS) forskning om hur informationssäkerhetsarbetet skall hanteras på en högre ledningsnivå samt hur SCADA-säkerhet kan utvärderas.

- Nationella säkerhetsforskningslaboratorier utför avancerad forskning som berör nationell säkerhet. Exempel på denna typ av laboratorier är US Sandia National Laboratory och Idaho National Laboratory. I Sverige har framförallt Totalförsvarets forskningsinstitut (FOI) bedrivit denna typ av forskning och studieverksamhet om än i begränsad omfattning.
- Oberoende organisationer som tar fram standarder inom SCADA-säkerhetsområdet en sådan är till exempel Cigre (International Council on Large Electric Systems)
- Nationella myndigheter med speciella uppgifter relaterade till SCADA-säkerhet. Exempel på en sådan myndighet är UK NISCC.
- Leverantörer av IT-säkerhetsprodukter. Här kan till exempel nämnas stora amerikanska företag som Symantec samt mindre företag såsom kanadensiska Verano.

För att skapa en grund för olika typer av analyser, till exempel för att identifiera trender och viktiga aktörer inom SCADA-säkerhetsområdet, har en litteraturstudie genomförts. Den insamlade informationen har också värderats ur ett IT-säkerhetsperspektiv för att identifiera områden vilka är specifika för SCADA-säkerhet, som kan generera rekommendationer specifika för SCADA-området och som inte har någon direkt motsvarighet inom IT-säkerhetsområdet.

4.2 Litteraturstudie

Slutsatser i studien baseras till stor del på en insamling av relevanta dokument med inriktning mot SCADA-säkerhetsområdet. Studien har inte för avsikt att vara heltäckande utan är tänkt att demonstrera och visa ett axplock av de initiativ och arbeten som har gjorts inom SCADA-säkerhetsområdet. Eftersom SCADA-säkerhetsområdet är relativt nytt och informationen kan emanera från en rad olika typer av aktörer har dokumenten insamlats med utgångspunkt från den expertis som finns inom Sverige (till exempel FOI, Vattenfall, Eon, KTH, KBM). Det är också viktigt att poängtera att många dokument som samlats in, framförallt under senare tid och som tyvärr inte har analyserats inom ramen för studien, endast har erhållits genom direkt förfrågan till dem som producerat dokumenten. Dessa dokument finns alltså inte tillgängliga via Internet.

Statistik som redovisas, baserad på denna insamling av dokument, är inte statistiskt säkerställd på något sätt. Den bör ändå ge en överskådlig bild av det arbete som har genomförts inom SCADA-säkerhetsområdet.

Studien har dokumenterats i en databas där de värderade dokumenten sammanfattats. Det totala antalet dokument i studien är 136 stycken. Dokumenten är insamlade under perioden 2003-01-01–2006-02-02. Varje rad eller post i databasen sammanfattar ett dokument. De rubriker som ansågs relevanta att sammanfatta dokumenten är: titel, organisation, författare, årtal, beskrivning, typ, område, sektor, hot, sårbarhet, konsekvens, åtgärd, mottagare samt kvalitet. Efter att dokumentbearbetningen i databasen avslutades (2006-02-02) har det tillkommit dokument som även används i stor omfattning i denna studie men vilka tyvärr inte har ingått i analysen av insamlade dokument. Databasen kan rekvireras från KBM.

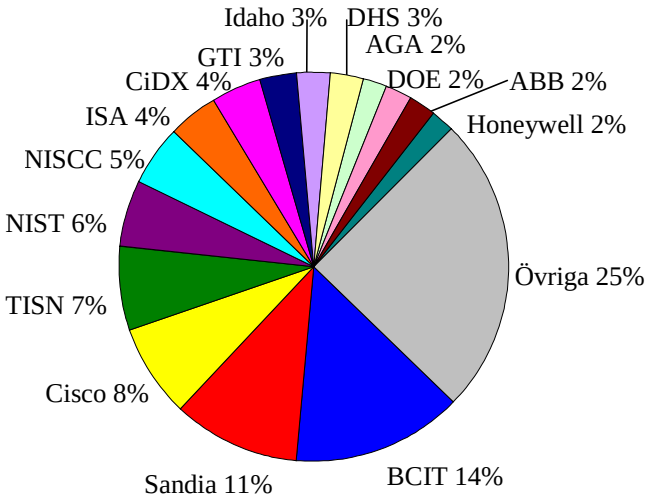
Organisation anger varifrån författarna kommer och inte den organisation som har beställt dokumentet. Beställarorganisationer står istället under mottagare. Författare är inte alltid namngivna i dokumentet, men om de är det anges de också. Årtal betecknar när dokumentet är utgivet (angivet så exakt som möjligt). Under beskrivning finns en kort sammanfattning om vad dokumentet handlar om. *Typ* kategoriserar övergripande vilken sorts dokument det rör sig om, med andra ord hur formellt det är och i viss mån dess syfte. Område kategoriserar med hjälp av övergripande nyckelord vad dokumentet handlar om. Sektor beskriver ifall dokumentet är inriktat mot någon specifik industridomän, till exempel elkraft och olja. Hot beskriver ifall dokumentet på något sätt har behandlat SCADA-hotbilden. Sårbarhet beskriver huruvida eventuella sårbarheter i SCADA-system beskrivs. Konsekvens visar på ifall dokumentet tar ställning till vad intrång i SCADA-system kan få för konsekvenser. Under rubriken åtgärd beskrivs vad dokumentet eventuellt förespråkar för lösning eller inriktningar för SCADA-säkerhetsarbetet. Mottagare betecknar som tidigare nämnts eventuella beställare, men även om en särskild målgrupp för dokumentet kan urskiljas. Slutligen värderas under rubriken kvalitet dokumentet och dess relevans för SCADA-säkerhet i stort.

Förutom sammandrag och värdering av SCADA-säkerhetsdokument, så omfattar databasen även sammanställningar och diagram samt en sammanfattning av identifierade aktörer inom SCADA-området. I de följande avsnitten presenteras resultatet med utgångspunkt från kategorier som angivits ovan.

4.2.1 *Organisationer*

Här presenteras de organisationer som har bidragit med flest dokument i studien. De visas i Figur 13 tillsammans med en uppgift om hur stor del av studien organisationens dokument utgör. Som synes har flest dokument från British Columbia Institute of Technology (BCIT) studerats. Andra organisationer som bidragit med relativt många

dokument är amerikanska nationella säkerhetslaboratoriet Sandia National Laboratory (Sandia), företaget Cisco, australienska Business-Government Partnership – the Trusted Information Sharing Network (TISN), amerikanska nationella forskningsinstitutet National Institute of Standards and Technology (NIST), brittiska National Infrastructure Security Coordination Centre (NISCC), amerikanska intresseorganisationen Instrumentation, Systems and Automation Society (ISA) och amerikanska intresseorganisationen Chemical Industry Data Exchange (CIDX). De övriga organisationerna är amerikanska Department of Homeland Security (DHS), amerikanska Department of Energy (DoE), företaget Asea Brown-Boveri (ABB), företaget Honeywell, intresseorganisationen American Gas Association (AGA), amerikanska nationella säkerhetslaboratoriet Idaho National Laboratory (INL, Idaho) samt det amerikanska forskningsinstitutet Gas Technology Institute (GTI). Det bör nämnas att exempelvis DHS och DoE finansierar mycket av det som till exempel utförs av SNL och INL.

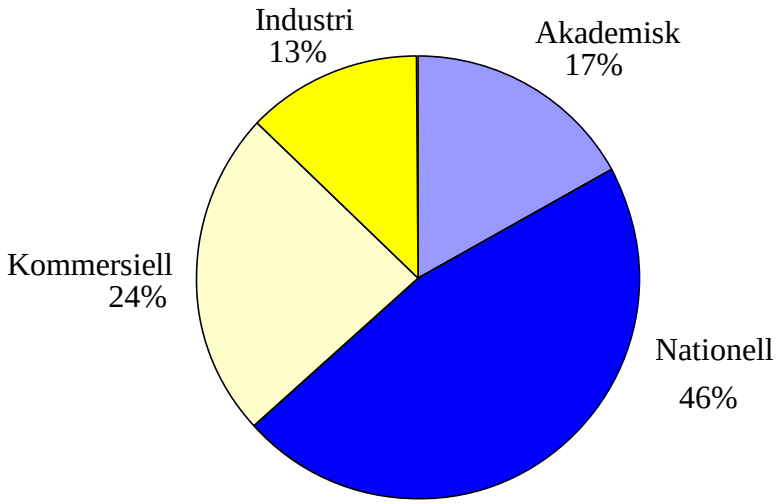


Figur 13. Organisationer som producerat dokument.

Det kan vara av större intresse att kategorisera dessa studerade dokument efter andra kriterier än organisationstillhörighet för att kunna dra slutsatser om *var* och *hur* utveckling inom SCADA-säkerhet bedrivs. Ett sett är att kategorisera efter vilken genre organisationen kan klassas som. En enkel klassificering vore att dela upp organisationer i nationella (för statligt finansierade verksamheter), kommersiella (för privata företag),

akademiska (för forskning som bedrivs av universitet) samt industriella (för gemensamma samarbetsansträngningar inom industrin).

När studerade dokument kategoriseras efter typ av organisation istället för specifika organisationer erhålls fördelningen i Figur 14. Som synes är det nationella verksamheter som har resulterat i flest dokument med hela 46 procent. Till dessa hör bland annat organisationerna Sandia, TISN, NIST och NISCC. Näst flest dokument, 24 procent, härrör från kommersiella organisationer som Cisco. Därefter kommer den akademiska sektorn på 17 procent, där BCIT är den största enskilde aktören. Sist hamnar industrisektorn på 13 procent och här utmärker sig bland annat TISN och CiDX.

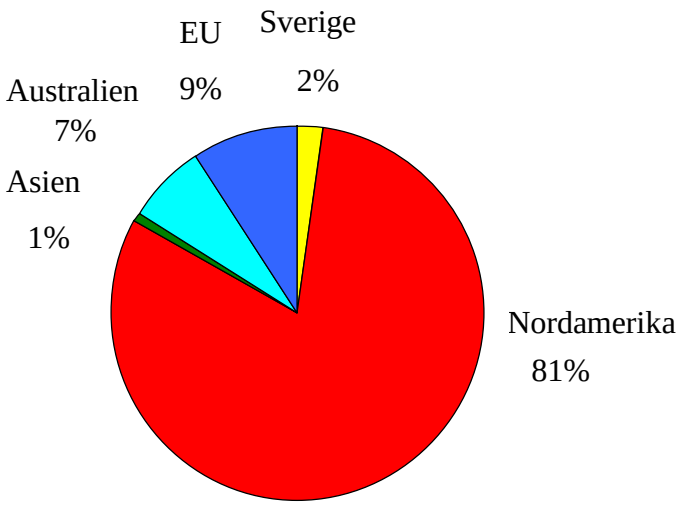


Figur 14. Typer av organisationer som producerat dokument.

Ytterligare ett sätt att kategorisera är att dela upp studerade dokument efter *var* de producerande organisationerna hör hemma någonstans. Detta åskådliggör var forskningen bedrivs. Sammanställningen i Figur 15 visar att den i särklass största delen av forskningen, hela 81 procent, bedrivs i USA och Kanada. Därefter kommer Europa med 11 procent och Australien med 7 procent. Som synes utgör forskning i Sverige endast två procent av de studerade dokumenten. De flesta dokument som härrör från NISCC är framtagna (för NISCC räkning) av organisationer i Nordamerika, som till exempel BCIT. Detta betyder att skevheten mot Nordamerika egentligen är ännu större än vad som avspeglas i figuren.

Till viss del beror dessa siffror på att det är lättare att få tag i och ta till sig dokument från en viss organisation eller på ett visst språk. Asien står säkerligen för betydligt mer än en procent av den sammanlagda forskningen inom området, särskilt med tanke på

att INL har bistått den japanska staten med hjälp för att bygga upp en SCADA-säkerhetstestanläggning[17]. Men av språkliga skäl är det inte lika lätt att studera deras resultat.

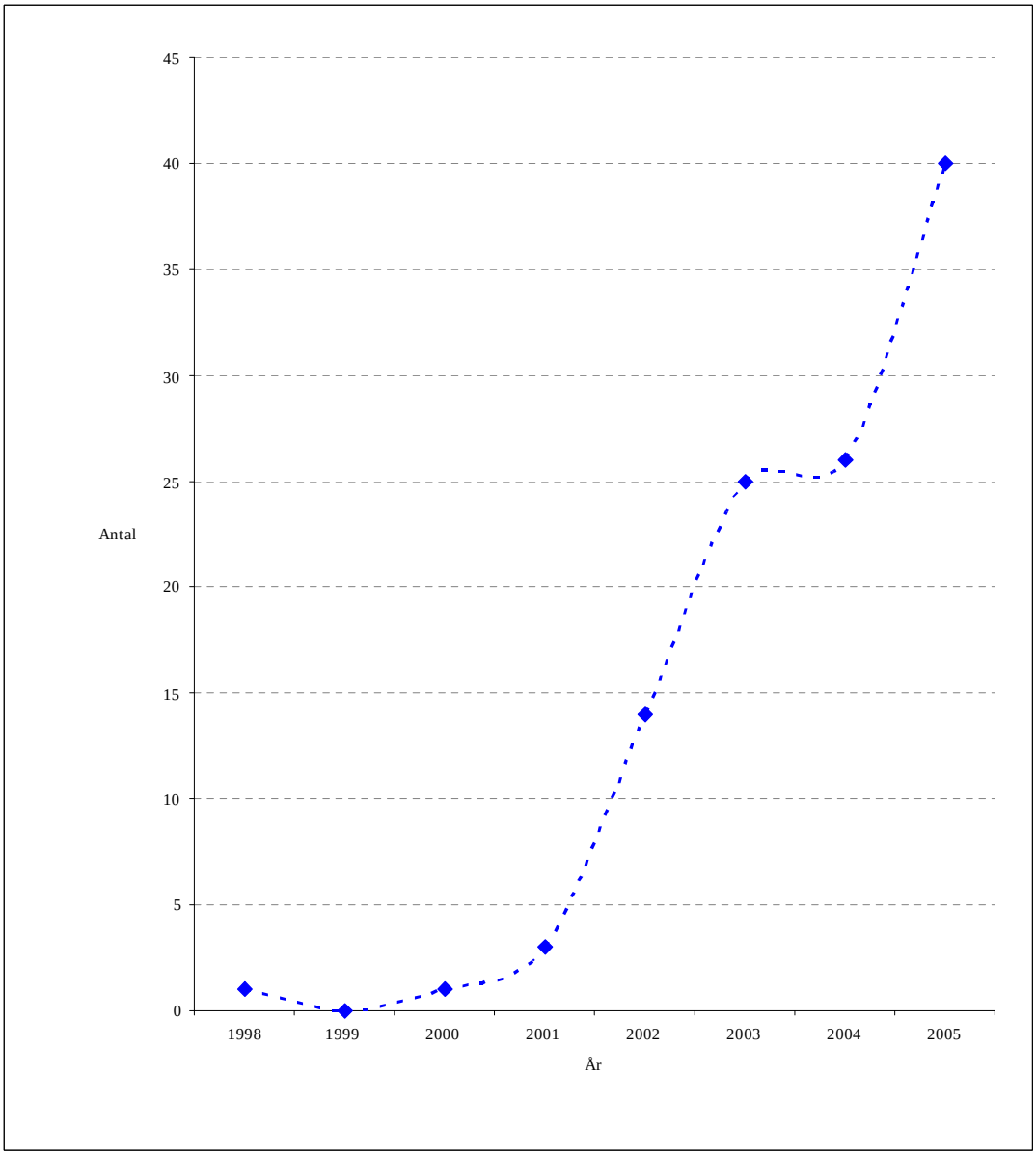


Figur 15. Geografiska områden som producerat dokument.

4.2.2 *Årtal*

De flesta dokument i studien har skrivits under eller efter 2001 vilket visas i Figur 16. En slutsats är att efter 11 september så ökade medvetandet om behovet att skydda kritisk infrastruktur och för hur sårbara vi är i det moderna samhället. Många statliga säkerhetsmyndigheter, framförallt i Nordamerika, har fått sig tilldelade mycket resurser för att säkra ländernas kritiska infrastruktur, vilket är en av förklaringarna till den ökande mängd dokument som producerats där. Dock är det absoluta antalet dokument litet vilket kan bero på att de mest intressanta dokumenten inte är öppna eller att det dröjer innan de publiceras öppet. När det till exempel gäller det amerikanska nationella säkerhetslaboratoriet, Idaho National Laboratory som hanterar den nationella SCADA-säkerhetstestanläggningen (NSTB), kan man efterfråga och ibland få ut dokument rörande SCADA-säkerhet. Dokumenten måste dock genomgå en relativt lång granskningsprocedur innan de lämnas ut. Man kan se en tydlig trend att det sedan december 2005 har släppts cirka 5–10 dokument från INL och SNL rörande SCADA-säkerhet, varav några ingår i studien men inte alla. Generellt sett håller dessa dokument hög kvalitet och har mycket intressant innehåll.

[17] Informell diskussion med Mike Assante, INL Critical Infrastructure Protection manager.

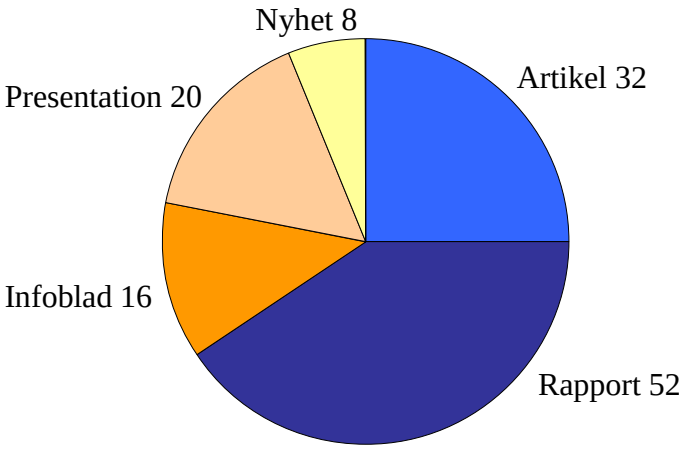


Figur 16. År som dokumenten producerats.

4.2.3 *Typ*

Studien är baserad på olika typer av dokument, innehållandes information av varierande kvalitet. Dokumenten har klassificerats efter vilken typ de tillhör. De är antingen mer omfattande dokument, oftast med hög kvalitet såsom artiklar eller rapporter, eller av en

mindre formell typ, som informationsblad, presentationer eller nyhetsartiklar. Dessa är ofta av lägre kvalitet (men inte alltid) och innehåller oftare påståenden utan några djupare förklaringar. Exempelvis är presentationer ibland gjorda för att väcka åhörares intresse, men den information som de innehåller är sällan kontrollerbar eller användbar på samma sätt som en studie är. En kategorisering av studerade dokument efter denna indelning visas i Figur 17. Det är flest rapporter och artiklar, sammanlagt 84 stycken. De övriga 44 dokumenten, med oftast sämre kvalitet, står för ungefär en tredjedel av samtliga dokument.



Figur 17. Typer av dokument som producerats.

4.2.4 *Område*

Här redovisas de nyckelområden som identifierats under studien. Nyckelord skapades för att på en övergripande nivå försöka klassificera vad dokumenten handlar om. Ett dokument kan innehålla ett till flera olika nyckelord. Antalet gånger som ett nyckelord påträffats under studien har räknats samman för att utgöra underlag för hur ofta ett visst ämnesområde dyker upp i dokumenten. En sammanställning på alla nyckelord samt deras frekvens i studien kan ses i Tabell 1. Nyckelorden har därefter kategoriserats efter vilket huvudområde de täcker in. En summering av antalet referenser från dokument till dessa huvudområden har också gjorts.

Tabell 1. Nyckelområden inom SCADA-säkerhetsområdet.

Nyckelord	Antal ref.	Summa	Nyckelord	Antal ref	Summa
Krav		**42**	Upplysande	1	
Behov	3		Samarbete	4	
Säkerhetsfunktioner	3		Terminologi	1	
Säkerhetskrav	11		**Teknisk säkerhet**		**72**
Standarder	13		Brandväggar	6	
ISO 17799	6		Testning	6	
Common Criteria	6		Testanläggning	5	
Teoretisk säkerhet		**57**	IDS	4	
Modellering	8		WLAN	5	
Säkerhetspolicy	13		Penetrationstest	3	
Säkerhetsvärdering	2		Sårbarhet	2	
Riskanalys	14		Nätverk	10	
Riskhantering	5		Protokoll	12	
Attackträd	3		Kryptografi	5	
Administration	2		Kritisk infrastruktur	7	
IT-säkerhet	7		Inbäddade system	2	
Tillämpning av IT säkerhet till SCADA-säkerhet	3		Realtidssystem	1	
Samarbete		**50**	VLAN	1	
Riktlinje	25		IP telefoni	2	

Sammanställningen av de fyra övergripande kategorierna blir således; teknisk säkerhet (72), teoretisk säkerhet (57), samarbete (50) och krav (42). Slår man samman nyckelorden ytterligare kan man säga att krav och samarbete är teoretiska aspekter, vilket får till följd att nyckelordet teoretisk säkerhet omfattar 149 referenser. Det skulle betyda att det är ungefär dubbelt så många dokument som snarare behandlar teoretiska aspekter än tekniska.

Det klart populäraste teoretiska ämnet är riktlinjer (25). Många av de dokument som studerats har som syfte att vägleda företag i säkerhetsföreskrifter med hjälp av riktlinjer. Därefter följer forum (14), riskanalys (14), standarder (13), säkerhetspolicy (13) och säkerhetskrav (11). Detta tyder på en medvetenhet om behovet av att träffas och diskutera SCADA-säkerhet i forum med representanter från olika områden. Det är

också mycket som kommer från IT-säkerhet, vilket andelen dokument som behandlar riskanalys tyder på. Dessvärre är sällan de studerade riskanalyserna på något sätt anpassade till SCADA-området. En riskanalys enligt IT-säkerhet bygger på att prioritera åtgärder genom att värdera hot och dess sannolikhet mot konsekvensen. Inom SCADA-området blir riskanalyser dessvärre än så länge intetsägande då de flesta organisationer vet väldigt lite om både hot och konsekvenser. Det verkar finnas en medvetenhet om nödvändigheten att skapa och hantera säkerhetspolicy och administrera SCADA-system. Däremot verkar det saknas ekonomiska medel för att hantera dessa. Standarder är förstås ett sätt för att hantera detta och de är också i högsta grad omskrivna.

För de tekniska ämnena är det teknisk utrustning som har analyserats mest i de studerade dokumenten. Protokoll (12), nätverk (10), brandväggar (6) och *WLAN* (5) är tydliga exempel på detta. Det är en naturlig följd av att denna utrustning är sårbar, och det är via dem som cyberattacker utifrån oftast sker. Antalet under kritisk infrastruktur är också märkbart (7), vilket är en konsekvens av att nationella myndigheter i USA har identifierat området kritisk infrastruktur som ett område som är av stor betydelse för nationell säkerhet. Det har gjorts en hel del studier om praktisk testning, vilket nyckelorden testning (6), testanläggningar (5) och penetrationstester (3) tyder på. Dock är detta område känsligt eftersom till exempel resultat från tester ger information om sårbarheter som högst troligt finns i skarpa SCADA-system vilka finns i samhällsviktig infrastruktur. Dessutom blir denna information känslig för leverantörerna av de testade SCADA-systemen eftersom dessa inte vill att deras system skall betraktas som dåliga.

4.3 Värdering av litteraturstudien ur ett IT-säkerhetsperspektiv

Den insamlad information har också värderats ur ett IT-säkerhetsperspektiv för att försöka identifiera det som är specifik SCADA-säkerhet, och som kan generera rekommendationer specifika för SCADA-området och inte har någon direkt motsvarighet inom IT-säkerhetsområdet.

4.3.1 *Urvalskriterier*

Efter studier av ett antal slumpvis utvalda dokument ansågs många av dem falla inom en eller flera av följande grovt beskrivna kategorier:

- Statistik som är tänkt att visa hur vanliga angrepp är, hur kostsamma de är osv. I många fall är korrektheten hos sådan statistik mycket tveksam eftersom den är speciellt preparerad för att till exempel öka olika företags försäljningssiffror.
- Verkliga fall hämtade från tidningsartiklar. Tyvärr är tillförlitligheten hos sådana artiklar generellt sett mycket låg. Dels är journalisterna sällan kunniga inom

området, dels överdrivs eller felbeskrivs händelserna i de flesta fall för att få ökat nyhetsvärde, dels handlar det ofta om uppgifter som förmedlats i flera led och troligtvis delvis förändrats i varje led.

- Texter som på ytan ser ut att handla om SCADA-säkerhet men egentligen bara beskriver redan välkända områden inom IT-säkerhet generellt.
- Texter som innehåller unik eller intressant information.

De dokument som efter en snabb genomläsning inte tycktes tillföra något sorterades bort i första urvalsomgången. Här finns självklart en risk att enstaka användbara dokument har fallit bort.

I nästa steg lästes de kvarvarande dokumenten noggrannare och dokument som inte uppfyllde följande krav sorterades bort. Dokumenten skulle

- innehålla fakta som är tillräckligt korrekt för att inte ge läsaren en falsk bild av området ur ett IT-säkerhetsperspektiv
- tillföra något utöver den kunskap som redan finns inom IT-säkerhetsområdet generellt
- ge ett seriöst och professionellt helhetsintryck.

Nedan ges mycket korta presentationer av de dokument som ansågs innehålla information eller aspekter av SCADA-säkerhet som är unik i relation till IT-säkerhetsområdet. Dokumenten är av mycket olika karaktär och berör allt från policyer till användandet av vissa protokoll och därför är presentationerna nedan av olika karaktär. Syftet är inte att ge en fullständig bild av vad som är viktigt i litteraturen utan snarare understryka att det behövs värdering av existerande information. Syftet är också att och ge vissa inriktningar om hur sådan värdering kan göras och vad de kan innehålla.

4.3.2 *21 Steps to improve Cyber Security of SCADA Networks (US Department of Energy)*

Tjugoen lättlästa och kortfattade steg till säkrare SCADAnätverk, (DoE, 2003b). Det mesta av innehållet är generellt och kan därför också tillämpas i helt andra sammanhang. Delar är dock inriktade extra mycket mot problematik som är speciell för SCADA och andra miljöer med liknande egenskaper. Dokumentet är läsvärt för alla tänkbara målgrupper, men kanske speciellt för IT-säkerhetsansvariga i organisationer som är för små för att ha flera personer som på heltid arbetar med IT-säkerhet. Innehållet är sakligt och har bra balans mellan teknik och riskstyrning.

4.3.3 *Cryptographic Protection of SCADA Communications (American Gas Association)*

I AGA (2004), listas ett antal faktum som gäller miljön i vilken SCADA-system opererar, och för varje sådant faktum ett antal konsekvenser i form av krav på kryptolösningar. Själva innehållet är intressant nog i sig, men dokumentet är också ett bra exempel på hur man bör analysera förutsättningarna innan man börjar designa säkerhetslösningar. Den här sortens dokumentation är av intresse i till exempel interna utvecklingsprojekt, vid beställningar från externa leverantörer och som en inparameter vid forskning inom området.

4.3.4 *SCADA Security and Terrorism: We're not crying wolf (Internet Security Systems, ISS)*

Maynor et al. (2006) är en presentation från konferensen Blackhat Federal 2006 av personer från Internet Security Systems (ISS) – en internationell konsultfirma inom informationssäkerhetsområdet. Av störst intresse är innehållet under rubriken "Real world examples" där ISS beskriver sina erfarenheter av penetrationstester av SCADA-system. En genomgående trend i exemplen är att personalen från respektive anläggning gör grova missbedömningar av den faktiska säkerhetsnivån i sina system. Det är troligt att dessa incidenter inte finns representerade i de databaser som nämns i avsnitt 3.2 utan är unika beskrivningar från denna konsult. Incidenterna är:

- Ett kärnkraftverk: I det första exemplet lyckas ISS ta sig in via en helt oskyddad trådlös accesspunkt som är kopplad direkt på det administrativa nätverket. Nästa steg är att bryta sig in i en dator som är ansluten både till det administrativa nätverket och till SCADA-nätet.
- Ett oljebolag: I det andra exemplet finns kopplingar mellan SCADA-nätet och det vanliga företagsnätet. Kopplingarna finns inte med på några nätskisser. Majoriteten av personalen tror därför att näten är fysiskt separerade. Samma företag har också haft en incident där en masksmittad bärbar dator anslutits till nätverket med ett produktionsbortfall på miljontals dollar som följd.
- Ett kraftbolag: I det tredje exemplet säger det undersökta företaget att det inte finns några anslutningar mellan Internet och SCADA-nätverket. ISS tar sig in via en Internetansluten webbserver, vidare genom en databasserver och en VPN-tunnel till SCADA-nätet.
- Elnätet för ett helt land (ej USA): Det fjärde exemplet är inte lika tydligt men resultatet är att intrång är möjligt utifrån Internet ända in till SCADA-nätverket.

4.3.5 *Finding the Holes in Your Control System Before the Hackers Do (British Columbia Institute of Technology)*

En presentation med en ovanlig kombination av bredd och djup i jämförelse med majoriteten av det som finns skrivet om SCADA-säkerhet (Byres, 2005). Av särskilt intresse är avsnitten som behandlar hur dålig stabilitet nätverkskoden i många inbyggda system har, och varför den testning som normalt görs inte räcker till för att upptäcka problemen. Ett par andra viktiga avsnitt handlar om risken att krascha utrustning vid säkerhetstestning i allmänhet, samt om nackdelar med att använda vanliga sårbarhetsskannrar vid testning.

En sida i presentationen presenterar en statistisk beräkning av antalet sårbarheter i en genomsnittlig SCADA-systemkomponent med special framtagen mjukvara (PLC/DCS/RTU/IED). En av uppgifterna som används är att kommersiell mjukvara har ungefär 0,6 defekter per tusen rader kod. Det är mycket tveksamt om en genomsnittlig SCADA-systemkomponent är så väl testad att antalet defekter är så lågt. I praktiken brukar mjukvara som används enbart för specialtillämpningar innehålla betydligt fler säkerhetsdefekter än mer generell mjukvara (där talet förmodligen är en god uppskattning för större leverantörer av mjukvara). Det vore inte orimligt, om än absolut inte vetenskapligt belagt, att i det här fallet anta minst tio defekter per tusen rader kod. Därmed skulle antalet säkerhetsbrister i ett SCADA-systemen, som har minst fem miljoner rader kod, kunna uppskattas till runt femtio tusen stycken. Självklart är den här sortens bedömningar mycket osäkra, men ändå viktiga att göra för att ge en uppfattning om resterande robusthet och risknivå som kvarstår även efter noggrann testning.

4.3.6 *Vulnerability Testing of Industrial Network Devices (Cisco Systems)*

Beskriver bland annat tester som Cisco gjort av robustheten i nätverksstacken i till exempel PLC:er. Det är samma bild som man får i Finding the Holes in Your Control System Before the Hackers Do. Ett intressant faktum som förs fram är att det finns brister SCADA-mjukvara av typer som rensades ut från vanliga operativsystem redan under mitten av 1990-talet (Franz, 2003).

4.3.7 *IT security and the plant floor (British Columbia Institute of Technology & University of Victoria)*

I Byres et al (2002) presenteras fyra anledningar till att traditionella IT-säkerhets-åtgärder är svåra att applicera oförändrade på SCADA-system:

1. ”Security” får inte gå före ”safety” i SCADA-sammanhang. Exempelvis får inte en operatör på ett kärnkraftverk bli utelåst från kontrollsystemet i 15 minuter

efter att ha i panik ha skrivit fel lösenord några gånger på grund av att en härdsmälta är på gång.

2. I traditionell IT sätts stor fokus på att servrar och andra centrala punkter är säkra. I SCADA är det allra viktigaste att ändpunkterna (till exempel PLC:er) är säkra.
3. Hård- och mjukvaruprestanda är viktigare i SCADA-sammanhang; många processer kräver realtidsprestanda och kontinuerlig övervakning.
4. Det används ofta ickestandardiserade programvarukomponenter som till exempel speciella operativsystem i SCADA-system vilket gör att standard-säkerhetsmjukvaror inte alltid går att använda.

4.3.8 *Network Security Infrastructure Testing (Sandia)*

I Parks et al. (2005) beskrivs tester av hur några vanliga kommunikationsprotokoll för SCADA fungerar ihop med paketfiltrerande brandväggar, Network Adress Translation (NAT), samt Virtual Private Network (VPN). Både när befintliga lösningar byggs om för ökad säkerhet och när nya lösningar designas så är den sortens information som artikeln innehåller mycket värdefull. En intressant slutsats i rapporten är att protokollet OPC[18] är problematiskt att hantera med brandväggar och NAT. Ytterligare en reflektion dessa gör är att eftersom OPC bygger på RPC/DCOM[19], som i sin tur har haft säkerhetsmässigt mycket dåliga implementationer, så verkar OPC vara en olycklig konstruktion ur flera avseenden för att användas i SCADA-system.

4.3.9 *Penetration Testing of Industrial Control Systems (Sandia)*

Här beskrivs hur riskabelt det kan vara att göra penetrationstester mot SCADA-system, (Duggan et al, 2005). Bland annat ges exempel där ett ping sweep fick en robotarm att aktiveras och svänga runt 180 grader, ett annat ping sweep låste ett styrsystem och orsakade skador för 50 000 dollar, samt ett fall där testning låste ett system och därmed stängde en gaspipeline i fyra timmar.

Generellt föreslås användande av passiva tekniker snarare än aktiva tekniker för identifikation av allt från datorer till tjänster och sårbarheter. Därmed minskar risken för allvarliga bieffekter av testningen.

Hela området bör studeras närmare eftersom det finns många fler relaterade problem och lösningar än vad som avhandlats här.

[18] OPC – Object Linking and Embedding (OLE) for Process Control Linking and Embedding (OLE) for Process Control.
[19] Remote Procedure Call/Distributed Common Object Model.

4.3.10 *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks (British Columbia Institute of Technology).*

Huvuddelen av den här rapporten är egentligen inte specifik för SCADA utan handlar om nätverksarkitektur och systemkonfiguration i största allmänhet (BCIT/NISCC, 2005). Innehållet är ibland ovanligt intressant och klarsynt, men verkar ibland konstigt och ogenomtänkt. Den största delen av innehållet håller dock bra klass.

Några stycken handlar om vilka protokoll som behöver passera mellan SCADA-nät och administrativa nät (alternativt Internet). Även om vissa protokoll är välkända för de flesta som är aktiva inom IT-säkerhet så behandlas SCADA-specifika aspekter av välkända protokoll. Dessutom behandlas SCADA-specifika protokoll.

På sidorna 22 och 23 finns en tabell med förslag till regler för konfiguration av brandväggar. Tabellen ser användbar ut som underlag vid konfigurationsvall men innehållet bör anpassas efter varje enskilt fall.

På sidorna 31 och 32 tas några framtida teknologier upp:

- Brandväggar som kan filtrera SCADA-protokoll. Enligt rapporten fanns inga kommersiella lösningar när den skrevs men däremot tillägg till Linux firewall.
- Distribuerade mikrobrandväggar. Brandväggar som kan placeras framför varje enhet i SCADA-nätet. Enligt rapporten planerades att en sådan produkt skulle finnas i slutet av 2004.
- Ökad användning av quality of service (QoS) som medel mot DoS-attacker.
- Envägskommunikationer genomförda med user datagram protocol (UDP). När rapporten skrevs visste inte författarna om några sådana produkter på marknaden.

4.4 Sammanfattning

Några korta sammanfattande reflektioner från kartläggningen och värderingen av SCADA-säkerhetsdokument är följande:

- Den mesta informationen kommer från ett fåtal aktörer i Nordamerika.
    - av dessa bör nämnas den satsning som bedrivs vid de nationella säkerhetslaboratorierna i USA och som finansieras av DHS
    - den europeiska noden inom området är brittiska NISCC som samarbetar nära med de amerikanska nationella säkerhetslaboratorierna och enligt vissa indikationer till stora delar får ta del av även det hemliga underlag som de nationella laboratorierna tar fram

  - det kan dock finnas anledning att ytterligare bevaka området, exempelvis har man i Japan fått hjälp av INL att bygga upp en SCADA-säkerhetstestanläggning[20].

- Efter 11 september ökade intresset för SCADA-säkerhet eftersom det fanns farhågor att hot skulle riktas mot bland annat kritisk teknisk infrastruktur. Materialet från tiden kring 2001 är av övergripande natur och syftade till övervägande del att höja medvetenheten om möjliga hot mot SCADA-system. Numera är det etablerat ett område som framförallt drivs av amerikanska säkerhetsmyndigheter.
- Författarna av denna rapport bedömer att den praktiska användbarheten på de under 2005–2006 publicerade dokumenten har ökat markant sedan tidigare år. Fram till 2004 har det mesta handlat om teori och det fanns lite gjort på en praktisk och teknisk nivå.
- Den ökande kvaliteten märks framförallt när det gäller riktlinjer för hur man säkrar SCADA-system ur olika perspektiv. Detta kan tolkas som att många anser att det är viktigt att hantera de problem som finns i dagens system eftersom de kommer att dominera verksamheterna lång tid framöver. Det är också bland denna typ av dokument som den största kvalitetsförbättringen kan skönjas. Riktlinjerna är av alla möjliga typer, allt från om hur man skriver SCADA-säkerhetspolicyer till hur man använder brandväggar eller genomför penetrationstester i SCADA-miljöer.
- Mycket av informationen kommer från aktörer som har tillgång till olika typer testanläggningar, och det verkar vara en förutsättning för att kunna ta fram ny och användbar kunskap inom SCADA-säkerhetsområdet.

[20] Enskild diskussion med representant från INL

5 DISKUSSION OCH SLUTSATSER

Den fortsatta diskussionen syftar till att ta fram *rekommendationer* för svenska statens fortsatta engagemang inom SCADA-säkerhetsområdet. Detta fortsatta arbete måste naturligtvis ske tillsammans med andra aktörer. Ytterst handlar det om att etablera ett bra säkerhetsskydd för SCADA-system som motsvarar den hotbild som man antar råder mot svenska SCADA-system. Detta säkerhetsskydd består av allt från grundläggande IT-säkerhet till möjliga specifika åtgärder som exempelvis appliceringen av specialframtagna brandväggar för PLC:er. Om det anses att hotbilden mot svenska SCADA-system inte innehåller möjligheten att en antagonist till exempel kartlägger och sedan utnyttjar specifika SCADA-protokoll för att uppnå sina syften, så behöver man inte lägga tid och resurser för att etablera skydd mot denna typ av antagonist. *Valet* av dimensionerande hotbild är således avgörande för vilka verksamheter som inom SCADA-säkerhetsområdet staten skall satsa resurser på.

Vår slutsats är att staten skall ha ett engagemang i SCADA-säkerhetsområdet. Detta engagemang bör bestå i att finansiera insatser som syftar till att upprätthålla nationell säkerhet samt ha en samordnande roll för att effektivitet skall uppnås. I listan med rekommendationer finns det aktiviteter som motsvarar alla typer av hot. De områden som bör prioriteras har tagits fram med utgångspunkt från de slutsatser som författarna har från arbetet med studien. Önskvärda aktiviteter för staten bör enligt oss ske inom områdena kartläggning, fallbeskrivningar, kvalitetsgranskning, testanläggningar, utbildning, samverkan samt riktlinjer. Den övergripande strategin är att kartläggning, fallbeskrivningar, kvalitetsgranskning, samverkan och utbildning främst skall hantera behovet av att medvetandegöra hotet mot SCADA-system. Områdena testanläggningar och riktlinjer svarar mot behovet av att ta fram ny kunskap. Det är viktigt att påpeka att området testanläggningar är helt centralt för de övriga områdena vilket erfarenheter från USA visar. Presentationen av de olika områdena sker under dessa rubriker och görs kortfattat.

5.1 Kartläggning

En mycket viktig uppgift är att kartlägga vilka SCADA-system som idag finns i det svenska samhället, och i vilka viktiga infrastrukturprocesser de används. För närvarande

finns ingen samlad bild av dessa system, hur många de är och var de finns. Det är inte säkert att alla SCADA-system är lika kritiska för att upprätthålla samhällsviktiga funktioner. Därför behöver en klassificering av existerande system göras avseende deras kriticitet för samhället. De identifierade SCADA-systemen kommer att vara av varierande ålder och därmed från olika generationer. Det betyder att hanteringen av IT-säkerhetsfrågor med all säkerhet kommer att vara mycket olika i de olika systemen och ytterligare en klassificering ur sårbarhetssynpunkt måste göras per system. Basen för denna klassificering bör vara den lista av riktlinjer för IT-säkerhet som beskrivs i en separat åtgärdspunkt under detta kapitel, se avsnitt 5.7. Baserat på kriticitet och sårbarhet arbetas en lista fram som föreslår åtgärder per system. Exempel på rekommenderade åtgärder kan vara:

- identifierade enskilda områden inom SCADA-systemet som bör förbättras, till exempel förbättrad lösenordshantering
- en ny version av systemet som kan innehålla avsevärda förbättringar från sårbarhetssynpunkt, vilket leder till att rekommendationer om uppdateringar kan ges
- utbyte av SCADA-systemet mot ett annat system som bättre uppfyller kraven om SCADA-systemet bedöms vara osäkert ur sårbarhetssynpunkt och inga väsentliga förbättringar finns i senare versioner.

5.2 Fallbeskrivningar

Avsaknaden av information om cyberattacker mot SCADA-system har lett till att detta säkerhetsskyddsarbete har blivit eftersatt och inte tagits på allvar. Ytterligare bidragande orsaker är att kostnaderna för att komma till rätta med dagens problem troligtvis kommer att vara höga.

För att motivera alla inblandade parter – framförallt leverantörer och användare av SCADA-system samt staten såsom ytterst ansvarig för rikets säkerhet – att ta sitt ansvar i arbetet med att öka säkerheten i och runt systemen så krävs det framtagande av fallbeskrivningar av attacker mot SCADA-system. Dessa kan användas för att skapa medvetenhet om problemen men också skapa förståelse för att det måste avsättas medel för att hantera dessa problem på såväl kort som lång sikt.

Fallbeskrivningarna bör tas fram av en arbetsgrupp med representanter från ett flertal aktörer som kan bidra med sin specifika kompetens. Man kan också behöva ta hjälp av internationell kompetens. Exempel på en enkel men trovärdig fallbeskrivning ges i rapporten Backdoors and Holes in Network Perimeters. A Case Study For Improving Your Control Systems Security från US-CERT Control Systems Security Center (Nash, 2005).

5.3 Kvalitetsgranskning

En konkret och mycket viktig uppgift för staten är att bistå med resurser för att åstadkomma oberoende kvalitetsgranskningar av informationssäkerheten i installerade SCADA-system och dess anläggningar i samhällskritiska verksamheter.

Detta kan exempelvis bestå i att genomföra skarpa penetrationstester av existerande SCADA-system inom utvalda infrastrukturer för att därigenom påvisa kvalitetsbrister när det gäller informationssäkerheten i SCADA-systemen. Om denna typ av aktivitet skall genomföras i skarp miljö eller i testanläggningsmiljö samt hur den skall genomföras och vad som skall genomföras måste noggrant övervägas (Duggan et al, 2005). För att kunna göra det krävs det dock att staten bygger en specialistkompetens inom området.

5.4 Testanläggningar

För att verifiera redan etablerad kunskap och för att kunna ta fram ny kunskap inom SCADA-säkerhetsområdet krävs det testanläggningar. I all IT-utveckling är test-verksamhet en mycket viktig och etablerad aktivitet för att verifiera funktionalitet men också för att identifiera fel. När det gäller SCADA-säkerhet är testning av ännu större betydelse eftersom systemen visserligen består av vanliga IT-komponenter men är mycket komplexa. Dessutom tillfogas komponenter som skall samverka med fysiska processer som ställer helt andra krav på informationen som skall hanteras. Dessutom tillämpas SCADA-system på olika sätt beroende på ett antal faktorer. Det leder till att det i princip är omöjligt att utifrån teoretiska resonemang ta fram generella säkerhetslösningar. Ytterligare en faktor som motiverar behovet av testanläggningar är behovet av att belysa interaktionen mellan försvarare och angripare. Antagonistiska hot innehåller faktorn intention vilket till exempel leder till att nya resurser för skydd som

tillförs påverkar angriparens taktik och tillvägagångssätt. Till detta skall påpekas nyttan av testanläggningar vid utbildning.

Testanläggningarna kan vara olika stora och representera olika verksamheter. Det kan röra sig om omfattande testanläggningar som National SCADA Testbed i USA som består av flera anläggningar vid de olika nationella laboratorierna (Kenchington, 2006). Vid varje sådant laboratorium finns det anläggningar som kan användas för att genomföra olika mindre SCADA-säkerhetstestprojekt. Vid dessa anläggningar genomförs olika typer av testprojekt. I avsnittet 3.3 berörs vilka säkerhetsaspekter som studeras vid testerna som genomförs vid Idaho National Laboratory. För närvarande är urvalsprocessen för vilka system som skall testas något ostrukturerad (Parks, 2006) men det finns utkast till testprogramstruktur där man etablerar vilka huvudområden som skall fokusera på (Parks, 2006):

- säkerhet i SCADA-teknologier
- säkerhet i SCADA-protokoll
- säkerhet i nätverksinfrastruktur som används av SCADA-system.

För att bedöma vilka specifika system (från specifika leverantörer) som skall prioriteras i testprogrammet har man också tagit fram en bedömningslista där det värderade systemet bör få så positiva svar som möjligt för att staten skall anse det prioriterat att testa systemet i National SCADA Testbed. Denna bedömningslista består i översättning av följande frågor (Parks, 2006):

- Används systemet för närvarande?
- Vilken marknadsandel har systemet?
- Används systemet i flera tekniska infrastrukturer?
- Kan säkerhetslösningar hittas?
- Liknar systemet andra system?
- Är systemet nytt för programmet?

Dessa bedömningsfrågor kan med fördel användas även för ett eventuellt svenskt testprogram. En svensk övergripande strategi för tester bör vara att snabbt komma igång i liten skala och testa det som är mest specifikt för svenska förhållanden. Man bör inte alltför ensidigt fokusera på testresultat utan framförallt se till vikten av att bygga

upp den tekniska kompetensen kring SCADA-säkerhet. Dessutom bör man undersöka möjligheter att få ta del av testresultat från de aktörer som sitter inne med denna typ av information.

Samarbete krävs med andra internationella testanläggningar där Sverige kan bidra med specialistkompetens inom vissa områden.

5.5 Utbildning

En av de allra viktigaste aktiviteterna när det gäller att hantera SCADA-säkerhetsfrågor är utan tvekan att tillhandahålla kurser inom området på olika nivåer. Det behövs kurser för personer på ledningsnivå. såväl hos leverantörer som operatörer. Det behövs kurser för de personer som konstruerar SCADA-system och för dem som skall införa systemen och sköta driften av dem. Emellertid är denna typ av utbildningar tyvärr mycket sällsynta. De enda kurser som författarna känner till är de fyra kurser som INL ordnade på uppdrag av DHS vid Sans SCADA Security Summit 2006. Att ta fram kurser är ett mycket krävande arbete. Det är viktigt att notera att det är INL som utvecklar och driver dessa kurser och att man troligtvis kan göra det eftersom man är den aktör som har störst erfarenhet inom SCADA-säkerhetsområdet. Det understryks ytterligare av följande citat (Ananth, 2005):

> *These are the elements – housed in our comprehensive test range, designed to be full-scale in nature, representative of real world infrastructures and capable of being isolated – that uniquely position the federal government, national laboratories, and industry to be successful in identifying and managing risk to our nation's critical infrastructure. To the best of our knowledge, there is no similar facility in the world. And, the cache of over 100 experienced scientists, engineers, and technicians working in INL's SCADA/Cyber Security groups are aware of the great responsibility that comes with managing these resources and the significance of our mission to assist in securing the control systems of our nation's critical infrastructure.*

För svenskt vidkommande handlar det om att i närtid bygga upp en egen kompetens för att kunna sätt ihop egna kurser med hjälp av externa aktörer som till exempel INL och NISCC.

5.6 Samverkan

Det är viktigt att resurser skapas för att möjliggöra arbetet i olika samverkansgrupper, såväl nationellt som internationellt. Det nationella arbetet i Fidi-SC[21] bör utökas med fler intressenter med ansvar för dessa sektorsövergripande samhällsviktiga funktioner, exempelvis säkerhetspolisen. KBM bör vidare vara moderator och drivande för olika samarbeten mellan organisationer när det gäller ”cyber security”.

Det är dessutom av största vikt att tillräckliga resurser skapas för att både följa och delta i det internationella arbetet som bedrivs. Detta kräver bland annat att man deltar i de internationella möten, konferenser och arbetsgrupper som arrangeras inom området. Ett aktivt deltagande skapar dessutom förutsättningar för ett fördjupat internationellt informationsutbyte.

I detta internationella samarbete bör Sverige kunna ta en ledande roll och bidra med specialistkompetens inom vissa områden. För att kunna göra det bör det dock poängteras att Sverige måste kunna ta fram unik kunskap inom SCADA-säkerhetsområdet som är attraktivt för andra nationer att ta del av.

5.7 Riktlinjer

Ett område där det pågår mycket internationellt arbete (åtminstone tillåts andra nationer delta i olika nationella riktlinjearbeten) är det som handlar om att utarbeta riktlinjer för aktörer som på något sätt påverkar säkerhetsaspekter vid etablering och hantering av SCADA-system. Detta anses som ett viktigt interrimsarbete inom SCADA-säkerhetsområdet, eftersom riktlinjearbetet till stora delar handlar om att hantera redan befintliga system. När bättre säkerhetsstandarder har etablerats och fått fullt genomslag kan riktlinjer förhoppningsvis delvis avvecklas. Hur bra riktlinjerna blir beror mycket på vilka som väljer att delta i arbetet med att ta fram dessa och hur villig man är att dela med sig av sina erfarenheter. Nedan nämns två pågående riktlinje-arbeten inom SCADA-säkerhetsområdet utöver de avslutade som redan nämns i avsnitt 4.3.2 och 4.3.10.

[21] Forum för informationsdelning avseende informationssäkerhet - SCADA.

5.7.1 *NISCC Good Practice Guide Process Control and SCADA Security*[22]

Denna ”god praxis” är framtagen av *PA Consulting Group* för NISCC:s räkning. Guiden spänner över ett mycket stort område som man delar in i sju underområden. Denna rapport är också den första i en serie som utgörs av rapporter som behandlar vart och ett av underområdena. De sju underområdena är:

1. förståelse för affärsrisker (utkast av denna delrapport finns)
2. implementera säker arkitektur
3. etablera en responsfunktion (utkast av denna delrapport finns)
4. förbättra medvetenhet och färdigheter
5. hantera risker kopplade till tredjehandsparter (utkast av denna delrapport finns)
6. involvera olika typer av projekt, framförallt utvecklingsprojekt (utkast av denna delrapport finns)
7. etablera en process för hantering av säkerhetsarbetet.

Efter vad som framgår av listan ovan finns det utkast till delrapporter som NISCC/PA Consulting Group har tagit fram. I skrivande stund (juni 2006) pågår ett aktivt arbete med att ta fram hela serien med delrapporter. NISCC är mycket intresserat av att få synpunkter och förbättringsförslag från aktörer med erfarenheter inom området på de riktlinjer som tas fram.

Hittills har KBM bidragit med kommentarer till de utkast till delrapporter som finns för punkterna 1, 3, 5 och 6.

5.7.2 *The SCADA/Control System Security Project: Common Security Requirement Language for Procurements & Maintenance Contracts*[23]

Detta är ett projekt som drivs och genomförs av framförallt Idaho National Laboratory och ett antal användare av SCADA-system i USA. Projektet påbörjades i mars 2006. Målet med projektet är att utveckla ett gemensamt språkbruk som skall användas vid beskrivning av säkerhetskrav på SCADA-komponenter vid upphandlingar och kontraktsskrivningar. Därmed skall användarna av SCADA-systemen kunna vara säkra

[22] http://www.niscc.gov.uk/niscc/docs/re-20051025-00940.pdf
[23] http://www.cscic.state.ny.us/msisac/scada/

på att de har så säkra system som möjligt. Riktlinjerna skall framförallt beröra upphandling av nya SCADA-system och underhåll av existerande system

Vid den webcastpresentation[24] av projektet som gjordes 18 maj 2006 ges utförligare exempel på typer av frågeställningar som behandlas av de säkerhetsspecifikationer som man för närvarande arbetar fram. Dessutom anges vilka dokument som projektet kommer att ta fram samt en övergripande projektplan för detta. KBM ingår som en av fem internationella aktörer som deltar i den referensgrupp som bidrar med synpunkter på de dokument som projektet tar fram. Projektkoordinatorn är mycket intresserad av att få synpunkter och förbättringsförslag från aktörer med erfarenheter inom området på de riktlinjer som tas fram.

Ytterligare riktlinjer som är värda att nämna finns från Idaho National Laboratory (INL, 2006) och National Institute of Standards and Technology (Stouffer et al., 2006).

För svenskt vidkommande är det viktigt att delta i det pågående riktlinjearbetet. Dels för att tillgodogöra sig de erfarenheter som finns internationellt inom SCADA-säkerhetsområdet, dels för att kunna påverka riktlinjerna eftersom en hel del i dessa kan komma att användas vid utvecklandet av standarder.

[24] http://www.cscic.state.ny.us/msisac/scada/documents/ProcurementProjectWebcastBrief.pdf

REFERENSER

(Abrams et al., 1995) Abrams, M., Joyce, M. 1995, Trusted System Concepts, Computer & Security, Issue 14 1995, pp 45–56.

(Abshier, 2005) Abshier J., Ten Steps to Secure Control Systems, Kema Inc.

(AGA, 2004) Cryptographic Protection of SCADA, Communications Retrofitting Serial Communications, AGA Report No. 12-, Request For Comments, 2004.

(Ananth, 2005) House Committee on Homeland Security, Infrastructure Protection and Cyber Security Hearing on "SCADA and the Terrorist Threat: Protecting the National's Critical Control Systems", Vittnesmål av Dr. K. P. Ananth, Associate Laboratory Director, National & Homeland Security, Idaho National Laboratory, oktober 2005.

(ANSI, 2004) Ansi/ISA-TR99.00.02-2004, Integrating Electronic Security into the Manufacturing and Control Systems Environment, oktober 2004.

(Assante et al., 2006) Assante, M., Hoffman, R., Larsen, J., What is the Real Threat to SCADA Systems? SANS Webcast Presentation, februari 2006.

(BCIT, 2004) BCIT Group for Advanced Information Technology, NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, National Infrastructure Coordination Center, London, UK, July 2004.

(BCIT, 2004) BCIT Group for Advanced Information Technology, NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, National Infrastructure Coordination Center, London, UK, July 2004.

(BCIT/NISCC, 2005) BCIT Group for Advanced Information Technology, NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, National Infrastructure Coordination Center, London, UK, July 8, 2004

(Berg, 2005) Berg M., J. Stamp, A Reference Model for Control and Automation Systems in Electric Power, SAND 2005-1000C, 2005.

(Byres et al, 2002) Byres E., Hoffman, D., IT security and the plant floor, www.76.isa.org/intech, december 2002.

(Byres et al, 2004a) Byres E., M. Franz, D. Miller, The Use of Attack Trees in Accessing Vulnerabilities in SCADA Systems, International Infrastructure Survivability Workshop (IISW '04), IEEE, Lisbon, Portugal, december 2004.

(Byres et al, 2004b) Byres E., M. Franz, D. Miller, The Use of Attack Trees in Accessing Vulnerabilities in SCADA Systems, International Infrastructure Survivability Workshop (IISW '04), IEEE, Lisbon, Portugal, december 2004.

(Byres et al, 2004c)	Byres J., and J. Lowe, The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, VDE Congress, VDE Association For Electrical, Electronic & Information Technologies, Berlin, oktober 2004.
(Byres et al, 2004d)	Byres J., and J. Lowe, The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, VDE Congress, VDE Association For Electrical, Electronic & Information Technologies, Berlin, oktober 2004.
(Byres et al., 2004e)	Byres, E., Lowe, J., The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, 2004.
(Byres et al, 2005a)	Byres E., M. Franz, D. Miller, The Use of Attack Trees in Accessing Vulnerabilities in SCADA Systems, International Infrastructure Survivability Workshop (IISW '04), IEEE, Portugal, december 2004.
(Byres et al., 2005b)	Byres, E., Lowe, J., Insidious threat to control systems, januari 2005, hämtat 20060111 från: http://www.isa.org/InTechTemplate.cfm?Section=Article_Index1&template=/ContentManagement/ContentDisplay.cfm&ContentID=41080
(Byres, 2005)	Byres E., Finding the Holes in Your Control System Before the Hackers Do, Vulnerabilities in Modern Control Systems – Infragard 2005
(Carlson et al., 2005)	Carlson, R. E., Dagle, J. E., Shamsuddin, S. A., Evans, R. P., A Summary of Control System Security Standards Activities in the Energy Sector, 2005
(CC, 1999)	CC (1999), Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version 2.1, CCIMB-99-031, augusti 1999.
(Cegrell, 1994)	Cegrell T., U. Sandberg, Industriella Styrsystem, 1994.
(Cherkashin, 2005)	Cherkashin V., G. Feifer, Spy Handler, Memoir of a KGB officer. The true story of the man that who recruited Robert Hanssen and Aldrich Ames, Basic Books, 2005.
(Christiansson, 2004)	Christiansson, H., Värdering av IT-säkerhetsanalysmetodiker inom samhällsviktig infrastruktur; FOI-R--1350--SE, 2004
(CiDX, 2004)	CiDX, Cybersecurity Practices, Standards, and Technology - Cybersecurity Reference Model, 2004.
(Davidson et al., 2004)	Davidson, J. R., Permann, M. R., Rolston, B., Schaeffer, S. J., INEEL National Security Division, ABB SCADA/EMS System INEEL Baseline Summary Test Report, INEEL/EXT-04-02423, november 2004.
(DHS, 2005)	DHS, Control Systems Cyber Security Awareness, US-CERT Informational Focus Paper, 7 juli 2005.
(DoE, 2003a)	US Department of Energy, Office of Energy Assurance, Meeting Brief DOE/DHS SCADA Meeting, juli 2003
(DoE, 2003b)	U.S. Department of Energy, Office of Energy Assurance, 21 Steps to Improve Cyber Security of SCADA Networks, 2003.

(DoE, 2006) U.S. Department of Energy, Office of Energy Assurance, Roadmap to Secure Control Systems in the Energy Sector, januari 2006.

(Duggan et al, 2005) Duggan, D. P., Berg, M., Dillinger, J., Stamp, J., Sandia National Laboratories' Center for SCADA Security, Penetration Testing of Industrial Control Systems g, oktober 2005.

(DMEA, 2006) Dutch Ministery of Economic Affairs, (In)security of SCADA systems: a role for the Government, 2006 (confidential)

(Dzung et al., 2004) Dzung D., M. Naedele, T.P. von Hoff, och M. Crevatin, Security for Industrial Communication Systems, 2004.

(Dzung et al., 2005) Dzung D., M. Naedele, T.P. von Hoff, och M. Crevatin, Security for Industrial Communication Systems, Proceedings of the IEEE, vol. 93, no. 6, juni 2005.

(Eloff et al., 2000) Eloff, von Solms (2000), Information Security Management: An Approach to Combine Process Certification And Product Evaluation, Computers & Security, Volume 19, Issue 8, pp 698-709, 2000.

(Franz, 2003) Franz, M., Vulnerability Testing of Industrial Network Devices, Cisco Critical Infrastructure Assurance Group (Ciag), ISA Industrial Network Security Conference, oktober 2003.

(GAO, 2004) GAO, Challenges and Efforts to Secure Control Systems, GAO-04-354, mars 2004.

(Haimes, 2003) Haimes Y., Accident Precursors, Terrorist Attacks, and Systems Engineering, 2003.

(Hildick-Smith, 2005) Hildick-Smith, A., Security for Critical Infrastructure SCADA Systems, 2005.

(Hildick-Smith, 2005) Andrew Hildick-Smith, Security for Critical Infrastructure SCADA Systems, GSEC Practical Assignment, Version 1.4c, Option 1, SANS Institute, februari 2005.

(IBM, 2006) IBM Report om Cybercrime, hämtad 060323 från http://www.itsecuritymagazine.com/its/News%20Documents/2006/Jan/IBM%20releases%20cybercrime%202006%20report.htm, 2006.

(INEEL, 2004) A comparison of Electrical Sector Cyber Security Standards and Guidelines, INEEL/EXT-04-02428, 2004.

(INL, 2006) External Report # INL/EXT-06-11478, Control Systems Cyber Security: Defense in Depth Strategies, May 2006

(ISA, 2005) ISA, dISA 99.00.02 Draft 1 Edit 5, ISBN: 1-55617-976-6, september 2005.

(Johansson et al., 2005) Johansson E., et al., "The Enterprise Information Security Assessment Method - an approach for credible and efficient assessments applied in an European Energy Company", 29th European Safety, Reliability & Data Association (ESReDA) Seminar on Systems Analysis for a More Secure

World, European Commission Joint Research Centre (JRC), IPSC, Ispra, Italy, oktober 2005.

(Johansson, 2005) Johansson E., "Assessment of Enterprise Information Security – How to make it Credible and efficient", Doktorsavhandling framlagd vid Kungliga Tekniska högskolan (KTH), Stockholm, december 2005.

(Johansson et al., 2006) Johansson E., P. Johnson and T. Cegrell, Assessment of Information Security in Electric Utilities - The Importance of Prioritization, CIGRE 2006.

(JRC, 2005) JRC, The future of ICT for power systems: emerging security challenges, report on the Workshop held in Brussels, februari 2005.

(Kenchington, 2006) Presentation av Hank Kenchington, DoE, Securing Control Systems in the Energy Sector, SANS SCADA Security Summit, Orlando, mars 2006.

(Kilman et al., 2005) Kilman, D., Stamp, J., Framework for SCADA Security Policy, 2005

(Kilman et al., 2005) Kilman, D., J. Stamp, Framework for SCADA Security Policy, (SAND 2005-1002C), 2005.

(Larsen, 2006) Larsen, J., Understanding the Threat, SANS SCADA Security Summit, Orlando, mars 2006.

(Maynor et al., 2006) Maynor, Graham, SCADA Security and Terrorism: We're not crying wolf (Internet Security Systems, ISS), Black Hat Federal 2006.

(Melton et al., 2004) Melton, R., Fletcher, T., Earley, M., System Protection Profile – Industrial Control Systems Version 1.0, 2004.

(Mitratek, 2005) Mitratek Systems Inc, Process Control Systems Forum Formational Meeting, 2005.

(Naedele et al., 2005a) Naedele, M., D. Dzung,, Industrial information system security Part 1: IT security in industrial plants - an introduction, ABB Review 2/2005.

(Naedele et al., 2005b) Naedele, M., R. Vahldieck, Industrial information system security Part 2: Malware protection for industrial automation systems, ABB Review 2/2005.

(Nash, 2005) T. Nash, US-Cert Control Systems Security Center, Backdoors and Holes in Network Perimeters. A Case Study For Improving Your Control Systems Security, Case Study Series 1.1, augusti 2005.

(NISCC, 2004) NISCC, The electronic Attack (eA) Threat to Supervisory Control and Data Acquisition (SCADA) Control & Automation Systems, NISCC Briefing 02/04, juli 2004.

(NTSB, 2002) National Transportation Safety Board, Pipeline Accident Report, Pipeline Rupture and Subsequent Fire in Bellingham, Washington, June 10, 1999, Oktober 2002.

(Ober, 2006) Presentation av Jan Ober, vid polska Institute of Biocybernetics and Biomedical Engineering (IBBE), vid EU PASR-projektet Vital Infrastructure Threats and Assurance (VITA) möte i Madrid 2006-05-17.

(Parks et al., 2005) Parks, R., Hills, J., Smith, S., Davis, T., Baros, A., Cordeiro, P., Sandia National Laboratories' Center for SCADA Security, Network Security Infrastructure Testing, Version 1.2, 2005

(Parks, 2006) Presentation av Raymond Parks, SNL, National Control System Security Testing Plan, SANS SCADA Security Summit, mars 2006, Orlando

(PCSF, 2005) Process Control Systems Forum 2005 Spring Meeting, Research Interest Group, maj 2005.

(Polsen, 2002) Polsen, K., FBI Issues Water Supply Cyberterror Warning, 2002.

(Rodriguez et al, 2006) Rodriguez, J. G., Maio, V., Beitel, G. A., The Cyber Security Risk Of Current And Future Generation Process Control And SCADA Systems, International Workshop on "Complex Networks and Infrastructure Protection", mars 2006.

(Rolston, 2005) Rolston, B., US-CERT Control Systems Security Center, Attack Methodology Analysis: Emerging Trends in Computer-Based Attack Methodologies and Their Applicability to Control System Networks, INL/EXT-05-00477, juni 2005.

(Stamp et al., 2003) Stamp J., Campbell, P., DePoy, J., Dillinger, J., Young, W., Sustainable Security for Infrastructure SCADA, 2003.

(Stamp et al., 2005) Stamp J., Berg, M., Baca, M., Reference Model for Control and Automation Systems in Electrical Power version 1.2, 2005.

(Stamp et al., 2002) Stamp J., J. Dillinger, W. Young, Common Vulnerabilities in Critical Infrastructure Control Systems (SAND 2002-0435C), 2002.

(Stamp et al., 2003) Stamp J., P. Campbell, J. Depoy, J. Dillinger, W. Young, Sustainable Security for Infrastructure SCADA (SAND 2003-4670C), 2003.

(Stouffer et al., 2004) Stouffer, K., Falco, J., Proctor, F., The NIST process control security requirements forum (PCSRF) and the future of industrial control system security, 2004.

(Stouffer et al., 2006) K. Stouffer, J. Falco, K. Kent, Special Publication 800-82 Initial Public Draft, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, Recommendations of the National Institute of Standards and Technology, september 2006.

(Torstensson et al., 2003) Torstensson, D., Wedlin, M., IT-relaterade sårbarheter inom vattenförsörjning, 2003.

(US-C PSOTF, 2004) U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, april 2004.

(US-CERT CSSC, 2005) US-Cert Control Systems Security Center, Cyber Incidents Involving Control Systems, INL/EXT-05-00671, oktober 2005.

(Wells, 2006a) Presentation av Rita Wells, INL, Technology Panel 1: Testing the Security of Industrial Control Systems: Reducing the Risk for the Asset Owners, Sans SCADA Security Summit, Orlando, mars 2006.

(Wells, 2006b) Presentation av Rita Wells, INL, Measurement: Testing the Security of Industrial Control Systems: Reducing the Risk for the Asset Owners, SANS SCADA Security Summit, Orlando, mars 2006.

(Young, 2003) Young, J. DePoy, Relative Risk Assessment for Water Utility SCADA systems (SAND 2003-1772C), 2003.

LÄNKAR TILL ANDRA VIKTIGA KÄLLOR PÅ NÄTET

http://csrp.inl.gov/

http://www.esisac.com/library-guidelines.htm

http://www.inl.gov/SCADA/

http://www.nerc.com/

http://www.nerc.com/cip.html

http://www.niscc.gov.uk/niscc/SCADAen.html

http://www.sandia.gov/SCADA/

http://www.securityfocus.com/print/news/11351

http://www.tswg.gov/tswg/ip/ip_ma.htm

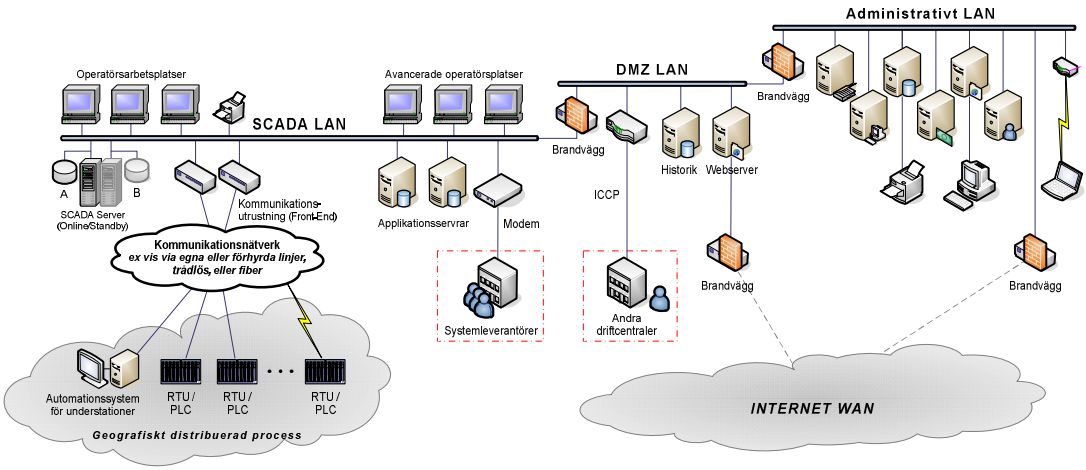
http://www.tswg.gov/tswg/ip/SCADA.htm

APPENDIX A - UPPBYGGNAD OCH KONSTRUKTION AV SCADA-SYSTEM

I detta appendix presenteras en mer ingående teknisk beskrivning av SCADA-systemens uppbyggnad. Beskrivningen innehåller följande avsnitt:

Principiell uppbyggnad av ett modernt SCADA-system

Moderna SCADA-system som är avsedda för geografiskt utbredda processer har en principiell uppbyggnad som presenteras i Figur 18 nedan. Följande avsnitt avser att ge inblick i hur dessa system är uppbyggda.



Figur 18. Principiell uppbyggnad av typiskt SCADA-system.

Processanknytning

I den övervakade processen finns givare och styrdon som kan mäta primära processtorheter och styra olika typer av utrustningar. Dessa givare och styrdon ansluts till elektronisk utrustning som oftast placeras i naturliga knutpunkter i processen. Sådana knutpunkter kan till exempel vara en kraft- eller transformatorstation eller en telekommunikationsväxel.

Den elektroniska utrustningen är datorbaserad. Dess främsta uppgift är att omvandla de uppmätta mätsignalerna till digital information och sända den vidare till den centrala driftcentralen. Utrustningen skall också motta styrorder från driftcentralen och ställa ut styrdon i processen. Oftast betecknas dessa elektroniska enheter som RTU:er (Remote Terminal Unit). Mätsignalerna varierar i antal från några tiotal till några tusental per RTU. Signalerna ansluts av tradition parallellt genom en kabel från varje givare till en RTU-ingång via ett korskopplingsskåp. Tre typer av ingångssignaler används: digital in, analoga in och pulsräknare.

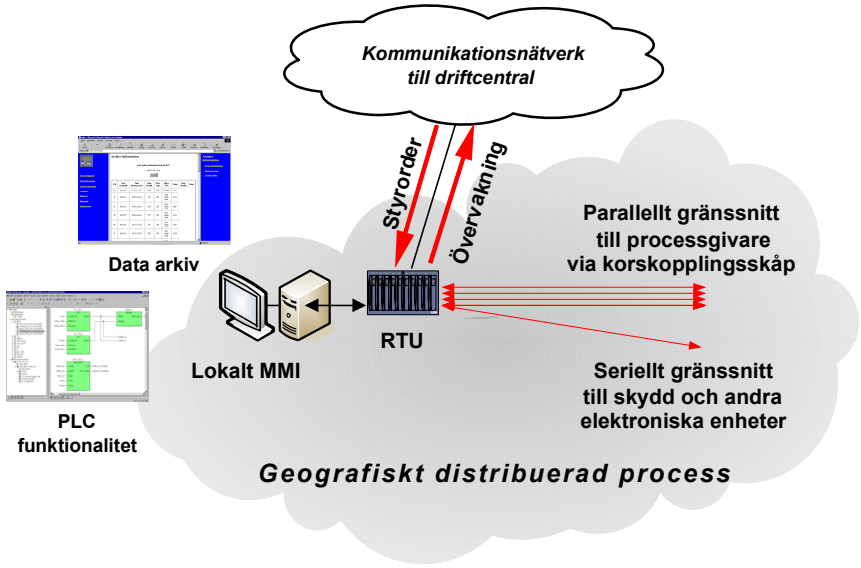
På senare år har det blivit allt vanligare att RTU:en också ansluts till en seriell stationsbuss. I en sådan är olika typer av sekundär stationsutrustning, till exempel skyddsreläer kopplade. Dessa utrustningar (numer också elektroniska) innehåller information om processens tillstånd och processtorheter. Informationen kan hämtas direkt från dessa enheter via stationsbussen och skickas till driftcentralen utan att behöva använda dubbla givare och extra kabeldragning. Ett internationellt standardiseringsarbete har pågått under ett antal år som resulterat i ett antal standarder för stationsbussar. IEC 870-5-103 är idag en etablerad standard för kommunikation på stationsbussar och IEC 61850 är en kommande standard med större ambition och omfattning. Avsikten med denna standardisering är naturligtvis att kunna installera utrustning från olika tillverkare som kan kommunicera med varandra och med överliggande system.

Moderna RTU:er kan innehålla lokal programmerbar logik som antingen kan agera på egen hand, till exempel förreglingskontroller, eller innehålla sekvenser som startas på kommando från driftcentralen. Dessutom finns ofta lokala arkiveringsfunktioner och möjlighet till lokal utskrift.

Moderna kraft- och transformatorstationer har ofta numera egna lokala SCADA-system. Systemen innehåller operatörsarbetsplatser med människa-maskinkommunikation för att möjliggöra lokal styrning av stationen. Dessa lokala SCADA-system har tillgång till all lokal information i stationen via stationsbussen. Anslutningen till det

centrala, överordnande SCADA-systemet, och översändning av information till detsamma sker då endast via en kommunikationsnod (gateway). Den omvandlar information från stationsbussen till ett kommunikationsprotokoll mot den överordnade driftcentralen.

Principerna för de olika typerna av processanslutning framgår av nedanstående bild (Figur 19).



Figur 19. Olika typer av processanslutning till stationsutrustning (RTU).

Kommunikation

RTU:er och stationskontrollsystem kommunicerar med driftcentralen via olika typer kommunikationsnätverk och med hjälp av många typer av medier. Traditionellt har processägaren också varit ägare av dessa kommunikationsnätverk. Man har önskat äga nätverken för att säkerställa att kommunikationen, speciellt vid större störningar, ständigt är tillgänglig. Som tidigare nämnts har dessa nätverk kännetecknats av relativt låga överförningshastigheter, normalt 1 200 till 2 400 bits per sekund. En tydlig trend finns för närvarande mot mer fiberbaserad kommunikation med betydligt högre kommunikationshastigheter. Detta kommer förmodligen att på sikt medföra

förändringar i systemstrukturen och i funktionsfördelning mellan driftcentral och stationsutrustning men denna trend är långsam.

De medier som idag används för kommunikation mellan RTU och driftcentral är

- bärvåg överlagrad på kraftledning (Power Line Communication för elnät)
- privat telefonkabel
- mikrovåg
- fiber (även med Wide Area Networks och TCP/IP kommunikation)
- uppringda förbindelser
- GSM/GPRS (fortfarande relativt ovanligt).

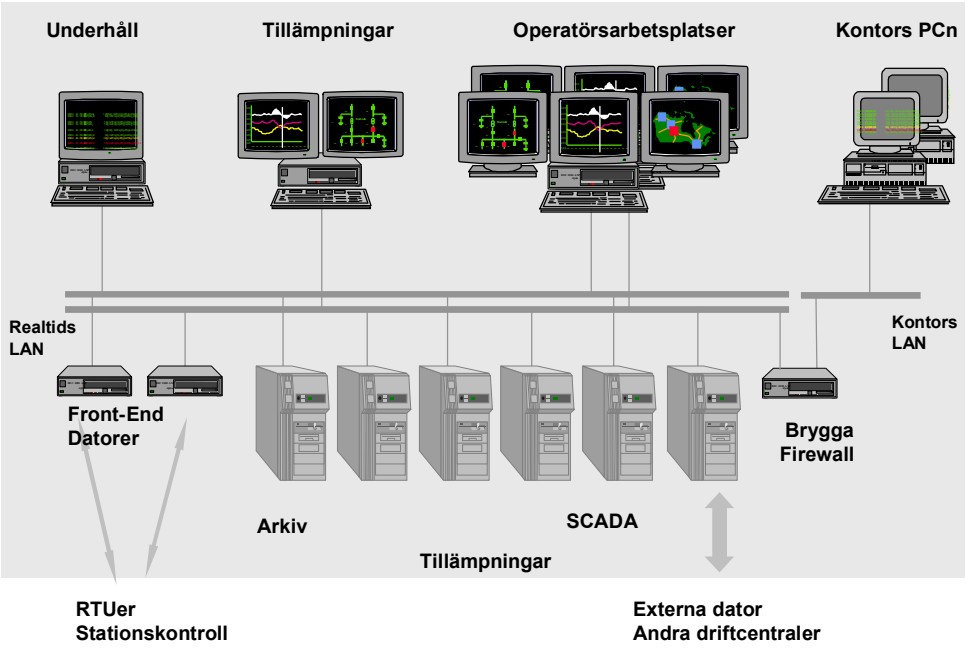
Vanliga kommunikationsstrukturer är

- punkt till punkt
- redundanta linjer
- multidrop
- stjärnkopplingar med datakoncentratorer
- slingor.

På grund av den låga kommunikationshastigheten och de stora kraven på datasäkerhet har SCADA-system av tradition använt egna specialkonstruerade kommunikations-protokoll mellan driftcentral och RTU:er. Eftersom inget telegram får vara felaktigt, speciellt vid styrning av processen, har protokollen haft många paritetsbitar (stora hammingavstånd). Regeln har varit att alla enbitsfel kan korrigeras och alla tvåbitsfel upptäckas. Eftersom dessa protokoll har varit leverantörsspecifika har det varit svårt att blanda RTU:er från olika tillverkare i samma system. Detta faktum har drivit fram ett standardiseringsförfarande för RTU-protokoll. Idag understödjer de flesta nyinstallerade SCADA-system och moderna RTU:er inom elbranschen de båda internationella standarderna IEC 870-5-101 och IEC 870-5-104 (TCP/IP baserat) samt de-factostandarderna DNP3.0 och Modbus. På grund av den långa livslängden för RTU-installationer (uppåt 30 år) finns dock mängder av äldre typer av leverantörsspecifika protokoll fortfarande i drift.

Driftcentral

Driftcentralsystemet är numera uppbyggt runt ett lokalt nätverk, ett så kallat Local Area Network (LAN), som alla anslutna enheter kommunicerar via. Detta LAN kan vara enkelt eller dubbelt men är ofta av tillgänglighetsskäl dubblerat. Av samma skäl är också samtliga applikationsdatorer (servrar) dubblerade och arbetsstationer så utformade att de kan ta över uppgifter från varandra om någon skulle gå sönder. Man vill i driftcentralkonfigurationen helt enkelt undvika att enkelfel skall kunna slå ut hela driftcentralen. Figur 20 nedan visar en typisk driftcentralkonfiguration.



Figur 20. Typisk driftcentral konfiguration

Front-end-datorer

Dubblerade front-end-datorer är ansvariga för kommunikationen med RTU:er och stationskontrollsystem. De avsöker fältutrustningen kontinuerligt, sänder informationen vidare till en realtidsdatabas samt ansvarar för övervakning och styrningen av

datainsamlingsnätverket. Det är i front-end-datorerna som de olika kommunikations-protokollen är installerade, vare sig det gäller standardprotokoll som IEC 870 eller leverantörsspecifika protokoll. Oftast avlastar front-end-datorerna de huvudsakliga SCADA-datorerna med viss preprocessing av den insamlade informationen innan den sänds vidare. Det kan till exempel vara omvandling av rå digital mätvärdesavläsning till ingenjörsvärden via olika typer och konverteringsrutiner samt översättning av hårdvaruadresser i RTU:erna till logiska namn i driftcentralen.

I den mån TCP/IP-baserade protokoll används, exempelvis IEC 870-5-104, kan insamling ske direkt i SCADA-datorerna via en kommersiell WAN-router ansluten till det lokala nätverket.

SCADA-datorer

Informationen från front-end-datorerna samlas i en realtidsdatabas i SCADA-datorerna. Dess uppgift är att avbilda den övervakade processen så nära verkligheten som möjligt inklusive följa processens ändringar i realtid. SCADA-datorerna är normallt kommersiellt tillgängliga serverar baserade på Unix eller Windows med en leverantörsspecifik realtidsdatabas och omfattande applikationsprogramvara. Anledning till att i stort sett alla större SCADA-system använder leverantörsunika realtidsdatabaser är att prestanda i processavbildning och i operatörspresentation inte kan lösas med dagens teknik i kommersiella relationsdatabaser.

SCADA-datorernas uppgift är också att övervaka processinformationen för att finna signifikanta förändringar och att uppmärksamma operatörerna om dessa förändringar. En sådan signifikant förändring kan vara en ventil i ett gasnät som har stängts spontant emedan en mindre tryckändring inom tillåtna gränser i en gasledning registreras men inte behöver påkalla speciell uppmärksamhet. Förändringar samlas i händelse- och larmlistor tillsammans med tidpunkter för förändringen. Händelselistor innehåller registrering av allt som sker i och runt processen. Larmlistor fordrar en aktiv kvittering av operatörerna för att konfirmera att de uppmärksammat förändringen.

Operatörerna kan använda SCADA-systemet för att sända styrorder till processen. De använder då processbilder i arbetsstationerna för att begära öppning av en brytare eller för att sända ett nytt börvärde till en lokal processutrustning. Styrordern skickas via front-end-datorer över kommunikationsnätverket till RTU:er och stationskontroll-utrustning innan den verkställs. Automatiska styrorder via ”close-loop- reglering” förekommer samt möjligheten att definiera automatiskt utförda styrordersekvenser.

SCADA-datorerna används också för att, på operatörernas begäran, skapa olika typer av utdrag av processinformationen, styra och kontrollera operatörernas behörighet, övervaka och larma om problem i själva driftcentralsystemet samt säkerställa och verkställa spontana och manuella överkopplingar mellan redundant enheter i drift-central eller i stationerna.

Det är vanligt att en driftcentral är en del av en styrhierarki inom bolaget eller landet. Till exempel kan en regional driftcentral vara underordnad en nationell central. Det sker då ett datautbyte mellan centralerna via standardiserade driftcentralprotokoll där det vanligaste idag är ICCP Intercenter Communication Protocol (eller TASE.2). Dessa protokoll innehåller funktioner för datainsamling samt processtyrning och är också, i likhet med RTU-protokoll, normallt inte krypterade.

Slutligen finns ibland någon typ av uppkoppling direkt till leverantören av SCADA-systemet som möjliggör fjärrdiagnostik samt fjärruppdatering av felrättningar. Dessa uppkopplingar är normallt bara inkopplade vid speciella tillfällen för felsökning eller vid korrigering av felaktigheter. Via dessa uppkopplingar kan hela systemet, inklusive databaser och programsystem, nås och påverkas.

Arkivfunktioner

Som tidigare nämnts är en viktig uppgift för SCADA-systemen att registrera och arkivera allt väsentligt som händer i och runt processen, till exempel alla operatörsåtgärder. För detta använder man speciella arkivdatorer oftast baserade på en kommersiell relationsdatabas, till exempel Oracle. Tack vare den kommersiella relationsdatabasen finns här en uppsjö av rapport- och programmeringsverktyg tillgängliga för olika typer av användare, från normala kontrollrumsoperatörer till systemanvändare och tillämpningsexperter.

Arkivfunktionen har kapacitet att registrera all information som kommer från processen via RTU:er, stationsdatorer samt andra driftcentraler plus händelse- och larmlistor samt beräkningsresultat. Arkivfunktionen är kopplade till olika medier, till exempel DVD eller taperobotar, för automatisk långtidslagring när utrymmet i själva arkivdatorn inte längre räcker till. På detta sätt åstadkommer man obegränsat lagringsutrymme.

Arkivet kan användas för att:

- lagra processdata, händelser, larm, operatörsingripanden, beräkningsresultat, etc.
- lagra framtida planer, till exempel produktionsplaner for alla producerade enheter
- spela upp processförlopp i förgången tid i normala enlinjescheman i kontrollrummet
- definiera och presentera grafer och rapporter.
- på ett enkelt sätt ställa frågor (queries); till exempel kan man via en enkel SQL-fråga få veta vilka av mina gasledningar som har en tillgänglighet på mindre än 80 procent under de senaste fem åren
- programmera avancerade statiska applikationer som använder historiska realtidsdata för att visa trender och förändringar i processens egenskaper.

Kontorsanslutning

I dag är det vanligt att kontorsnät ansluts till SCADA-systemen via routrar och bryggor för att möjliggöra att normala pc-användare anknutna till kontorsnäten kan nå data från SCADA-system och arkiv. Detta möjliggör att bygga kundunika rapporter och tillämpningar som arbetar direkt med realtids- och historiska data. Också för kontorsanvändare är en strikt behörighetskontroll nödvändig. På allra senaste tid har införandet så kallade ”Demilitarized Zones” (DMZ) börjat krävas. Detta innebär att en datakopia av realtidsdatabasen och det historiska arkivet placeras i en DMZ skyddad av brandväggar och skild från realtidsnätverket för att skydda ursprungsdata från yttre användning.

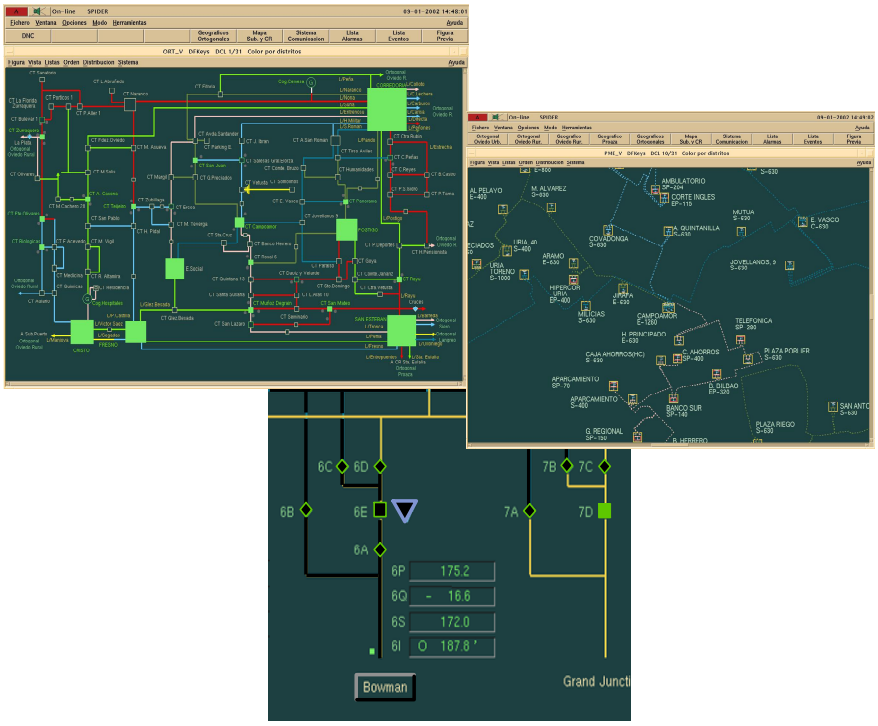
Människa-maskin-kommunikation

Människa-maskin-arbetsplatserna är operatörernas verktyg för att övervaka och styra processen. De är vanligen baserade på persondatorer. Med hjälp av modern fullgrafisk presentationsteknik kan information om processen presenteras i olika vyer i många fönster. Informationen på operatörsarbetsplatserna hålls ständigt och automatiskt uppdaterad av SCADA-datorerna så fort någon signifikant förändring upptäcks i processen. Modern presentationsteknik som informationszoom (declutter) är vanlig för

att ge mer processdetaljer ju djupare operatörerna zoomar in i processbilderna. Figur 21 åskådliggör några exempel på olika typer av processbilder för grundläggande driftcentralfunktioner.

De typer av bilder som operatörerna använder sig av för att styra och övervaka processen och styrsystemet är framförallt

- schematiska och geografiska enlinjescheman
- händelse- och larmlistor
- grafer och rapporter
- tabellbilder
- styrsystembilder
- underhålls- och diagnostikbilder



Figur 21. Typiska bilder för grundläggande driftcentralfunktioner.

Speciella operatörsarbetsplatser reserveras för underhåll av data och bilder. När processen byggs ut eller förändras måste motsvarande förändringar införs i SCADA-systemens datamodeller och bilder. Detta är ett omfattande arbete eftersom de övervakande processerna ständigt förändras. Som exempel kan nämnas ett elnät för distribution av 110 kV ned till 0,4 kV i en större stad. Där kan upp till 20 ombyggnader av nätstrukturen (nya transformatorer, etc.) ske dagligen med hjälp av olika team som arbetar ute på fältet. Alla dessa ombyggnader måste planeras, testas och övervakas av kontrollrumspersonalen som ansvarar för nätets stabilitet och säkerhet.

Processmodeller

Hittills har vi bara diskuterat SCADA-system som rena insamlings- och styrsystem. Varje punkt som insamlas är oberoende av alla andra punkter och processkunskapen. Det vill säga hur de olika punkterna hänger ihop eller är grupperade finns bara inritat i processbilderna som definieras per implementering. Samma SCADA-system kan användas oberoende av vilken process som övervakas eftersom de grundläggande SCADA-egenskaperna, alltså insamling, styrning, händelse och larmrapportering, behövs i alla de övervakade processerna.

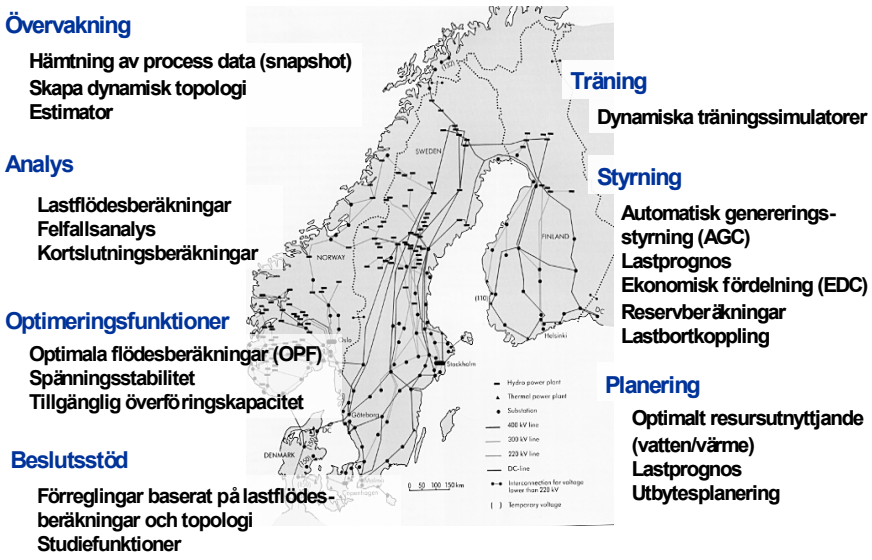
Om vi vill att SCADA-systemet skall kunna ha en mer intelligent uppfattning om den övervakade processen måste vi införa modeller av de olika processobjekten i databasen. Dessa modeller blir olika beroende på vilken typ av process som modelleras. Det är skillnad på en brytare i ett elnät och en ventil i ett gasnät eller på en trycktank i ett gasnät och ett kondensatorbatteri i elnäten. Det är också viktigt att införa konnektivitet. Med det menas hur de olika objekten i den övervakade processen statiskt är kopplade till varandra, till exempel på vilken buss i vilken station en brytare eller frånskiljare är inkopplad. Att definiera dessa modeller är ett omfattande arbete eftersom antalet övervakade objekt är så stort. Särskilda hjälpmedel är utvecklade av SCADA-leverantörerna för att hjälpa användarna att definiera och underhålla dessa modeller på ett effektivt sätt. Det sker bland annat via import från andra datorsystem där objekten kan finnas beskrivna, till exempel underhållssystem (*Asset Management*).

Avancerade applikationer

Baserat på de processmodeller som diskuterades i föregående avsnitt är det möjligt att utföra avancerade matematiska applikationer specialanpassade för respektive

processtyp. De kanske mest tydliga exemplen på avancerade applikationer finns på elkraftsidan där det sedan mycket länge funnits relativt enkla och precisa matematiska modeller för hur elnät uppför sig (det vill säga Ohms och Kirchhoffs lagar). Figur 22 visar en palett med applikationer som vanligtvis används inom övervakning och styrning av elnät.

Det är inte syftet med denna rapport att diskutera olika typer av applikationer i detalj. Men en kort beskrivning av hur dessa applikationer fungerar inom elnätsidan kan ge en bättre förståelse för deras användning och betydelse.



Figur 22. Exempel på avancerade funktioner i SCADA-system för elnät.

Med hjälp av insamlade brytarlägen kan en dynamiskt uppdaterad topologibeskrivning av det aktuella kopplingsläget erhållas. Genom att lägga till en icke fullständig mätvärdesinformation (alla punkter i nätet har inte givare) kan en fullständig lastflödesinformation räknas fram (tillståndsestimering) . Den innehåller det aktiva och reaktiva effektflödet i all punkter i nätet. Denna lastflödesbild kan användas för att simulera lastflödet efter förändringar i nätet, till exempel efter planerat underhåll eller efter andra omläggningar av nätet. Detta görs normallt i en parallell databas, en så kallad studiedatabas. Genom att simulera alla tänkbara fel som kan inträffa i nätet (N-1

analys) kan lastflödet räknas ut efter varje felfall och varningar och rekommendationer om driftomläggning kan göras innan felfallet eventuellt inträffar.

Det går att räkna fram det optimala lastflödet för att, till exempel, minimera de aktiva förlusterna och därigenom spara stora belopp.

På motsvarande sätt kan en optimal produktionsplanering med hänsyn till bästa möjliga resursutnyttjande (kärnkraft, olja, gas, vatten) räknas fram och applikationer för att automatisk styrning generande enheter enligt beräknade produktionsplaner finns tillgängliga.

Modellerna och applikationer kan också användas for att åstadkomma realistisk operatörsträning med instruktörsarbetsplatser och operatörer som skall tränas vid de normala tillfälligt omkopplade arbetsplatser. I detta fall kompletteras vanligen modellerna med viss dynamisk information.

Vi kan avslutningsvis konstatera att ju mer processresurserna utnyttjas mot sina fysiska gränser, desto mer omfattande SCADA-system krävs med avancerade styrfunktioner och matematiska modeller.