Ett nationellt centrum för SCADA-säkerhet

AMUND HUNSTAD, MIKAEL WEDLIN

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
Informationssystem
Box 1165
581 11 Linköping

Tel: 013-37 80 00
Fax: 013-37 81 00

www.foi.se

FOI-R-2945--SE Underlagsrapport **Informationssystem**
ISSN 1650-1942 November 2009

Amund Hunstad, Mikael Wedlin

Ett nationellt centrum för SCADA-säkerhet

Titel	Ett nationellt centrum för SCADA-säkerhet
Title	A national centre for SCADA security
Rapportnr/Report no	FOI-R-2945--SE
Rapporttyp Report Type	Underlagsrapport
Sidor/Pages	26 p
Månad/Month	11/11
Utgivningsår/Year	2009
ISSN	ISSN 1650-1942
Kund/Customer	Myndigheten för samhällsskydd och beredskap (MSB)
Projektnr/Project no	E53114
Godkänd av/Approved by	

FOI, Totalförsvarets Forskningsinstitut	FOI, Swedish Defence Research Agency
Avdelningen för Informationssystem	Information System
Box 1165	Box 1165
581 11 Linköping	SE-164 90581 11 LInköping

Sammanfattning

Rapporten beskriver viktiga förutsättningar för upprättandet av ett nationellt centrum inom SCADA-säkerhet, samt ger en konkret beskrivning för hur ett sådant centrum kan byggas upp och bemannas.

Nyckelord: Nationellt centrum, SCADA, kontrollsystem

Summary

The report describes important prerequisites for a successful establishment of a Swedish national SCADA security centre, and describes how the centre could be built up and staffed.

Innehållsförteckning

1 Inledning

1.1 Syfte

Syftet med föreliggande rapport är att beskriva en möjlig utveckling av den kompetensgrupp och laborationsinfrastruktur inom SCADA-säkerhet[1] som, genom MSB:s försorg, byggts upp vid FOI:s anläggning i Linköping.

Ett förslag som har framlagts är att med nuvarande verksamhet och infrastruktur som grund bygga upp ett *nationellt centrum* inom området. Rapporten kommer därför att diskutera förutsättningar för en sådan utveckling och olika intressenters synpunkter på detta förslag. För att ge en djupare förståelse för centrumtanken i sig själv diskuteras i rapporten erfarenheter från ett antal existerande nationella centrum.

Rapporten avslutas med att beskriva ett konkret förslag till hur ett nationellt centrum inom SCADA-säkerhet kan byggas upp och bemannas och på vilket sätt samverkan med andra svenska säkerhetsmyndigheter, användare av digitala kontrollsystem och internationella aktörer kan ske.

1.2 Bakgrund

Myndigheten för samhällsskydd och beredskap bildades 1 januari 2009 efter en hopslagning av tidigare Krisberedskapsmyndigheten (KBM), Räddningsverket och Styrelsen för psykologiskt försvar.

Inom avdelningen för informationssäkerhet har myndigheten (tidigare KBM) under flera år bedrivit arbete avseende ökad säkerhet i industriella process- och kontrollsystem.

Industriella process- och kontrollsystem utgör en kritisk del av de verksamheter som försörjer samhället med elektricitet, värme, dricksvatten, bränslen samt transporter av personer och varor. Till skillnad från administrativa IT-system, där informationsbehandlingen i sig ofta är slutmålet, kan störningar i industriella kontrollsystem innebära direkta störningar i den underliggande fysiska processen. Det kan i slutändan leda till leveransavbrott av samhällsviktiga nyttigheter. Moderna industriella kontrollsystem bygger allt oftare på samma tekniker som vanliga IT-system och integreras också med administrativa stödsystem. De görs också i allt högre utsträckning tillgängliga via publika nätverk som Internet. Sammantaget medför den här utvecklingen en förändrad riskbild och nya sårbarheter. Det är samtidigt ett område som kräver samverkan mellan flera olika aktörer och kompetenser, vilket förstärker vikten av olika typer av stödjande aktiviteter och gemensamma forum och projekt. Som en del av det arbetet har MSB finansierat uppbyggnaden och driften av en laborationsinfrastruktur vid Totalförsvarets forskningsinstitut (FOI) i Linköping. Laborationsinfrastrukturen kan användas för såväl utbildning, övningar och tester inom SCADA-området.

1.3 Rapportupplägg

I kapitel 2 beskrivs begreppet nationellt centrum. Relevanta erfarenheter från redan existerande nationella centrum tas upp och de synpunkter som inhämtats från olika aktörer redovisas. Kapitlet avslutas med ett antal rekommendationer som bör beaktas vid skapandet av ett nationellt centrum.

[1] SCADA= Supervisory Control and Data Acquisition. Denna typ av system går även under beteckningen industriella kontrollsystem, digitala kontrollsystem, system för processkontroll o.s.v.

I kapitel 3 presenteras ett konkret förslag på hur ett nationellt centrum inom SCADA-säkerhetsområdet skulle kunna se ut. Slutligen presenteras en kortfattad planering för ett sådant centrums första tre år.

2 Nationellt centrum

2.1 Nationell kompetensgrupp, nationellt centrum – vad kan det innebära?

Under rubriker som nationellt laboratorium, nationellt centrum och liknande benämningar kan ett brett och disparat spektrum av verksamheter noteras existera. Exempel på sådana verksamheter, utan någon annan intention än att indikera mångfalden, är:

- Nationellt vintersportscentrum[2] vid Mittuniversitetet
- Nationellt centrum för flexibelt lärande[3]
- Nationellt resurscentrum för biologi och bioteknik[4]
- MAX-lab, nationellt elektronacceleratorlaboratorium för kärnfysik- och synkrotronljusforskning[5]
- NSC, Nationellt Superdatorcentrum[6]
- Nationella laboratoriet för vedanatomi och dendrokronologi[7]
- Sven Lovén centrum för marina vetenskaper[8]

Verksamheterna beskrivs på sina hemsidor som kompetenskluster och nationella kunskapscentrum. Värdet av verksamheterna beskrivs exempelvis i termer av de synergieffekter de ger, den ökade förståelse av verksamheternas problemområde som uppnås och hur fördjupat forsknings- och utvecklingssamarbete kan främjas av verksamheten. Kompetensutveckling, information, utbildning och rådgivning med utgångspunkt i verksamheters problemområde lyfts också fram som viktigt. Det poängteras också gärna hur nationella laboratorier och centrumbildningar kan utgöra samverkansparter, bidra med analys-, metod- och kompetensstöd, tillhandahålla värdefulla resurser, tjänster och stöd samt främja kontakter kopplade till verksamheten.

Insatserna för att uppfylla ovan beskrivna roller, eller en delmängd därav, blir lätt betydande både vad gäller personal- och utrustningskostnader. För att garantera verksamhetens fortlevnad och att minska beroendet av finansiering via enskilda uppdrag, eftersträvas gärna en mera långsiktig finansiering. Exempelvis kan detta ske i form av att en statlig instans eller aktör står som garant för verksamheten och laboratoriets eller centrumets status.

I skriften *Vetenskapsrådets guide till infrastrukturen*[9], utgiven av Vetenskapsrådets kommitté för forskningens infrastrukturer, diskuteras frågor avseende stora och dyrbara forskningsanläggningar, databaser och omfattande datanät och annat som kan utgöra forskningsinfrastruktur. Skriften påpekar att där Vetenskapsrådet gör infrastruktursatsningar skall ett brett nationellt intresse och förutsättningar för världsledande forskning finnas. För att prioriteras av Vetenskapsrådet är det vidare av vikt dessa infrastrukturer utnyttjas av ett flertal forskargrupper eller andra användare och att de svårligen kan drivas

[2] Hemsida för Nationellt vintersportcentrum: http://www.miun.se/default____29323.aspx
[3] Hemsida för Nationellt centrum för flexibelt lärande: http://www.cfl.se/
[4] Hemsida för Nationellt resurscentrum för biologi och bioteknik http://www.bioresurs.uu.se/
[5] Hemsida för MAX-lab: http://www.maxlab.lu.se/svenska/index.html
[6] Hemsida för NSC: http://www.nsc.liu.se/
[7] Hemsida för Nationella laboratoriet för vedanatomi och dendrokronologi: http://www.geol.lu.se/dendro/
[8] Ny enhet från 1. januari 2008 bestående av Kristinebergs Marina Forskningsstation, http://www.kmf.kva.se/, Tjärnö marinbiologiska laboratorium, http://www.tmbl.gu.se/ och forskningsfartyget Skagerak.
[9] http://www.vr.se/download/18.2f62b054117692ac43f8000446/Rapport+11.2007.pdf

av enskilda grupper på egen hand. Likaså betonas vikten av långsiktig planering för vetenskapliga mål, finansiering och utnyttjande. Det betonas också av rådet att infrastruktur, insamlade data och resultat skall vara öppna och tillgängliga för forskare.

Vetenskapsrådet påpekar även hur sådana infrastrukturer positivt kan bidra till utbildningssatsningar och metodutveckling, främja tvärdisciplinär forskning och generera kompetens av värde för näringslivet. För att utgöra en tillräcklig volym eller kritisk massa och för att underlätta gemensam användning, pekar detta på nödvändigheten i att dessa infrastruktursatsningar blir nationella eller eventuellt internationella satsningar.

2.2 Erfarenheter av att vara ett nationellt centrum

Kristineberg marinbiologiska forskningsstation, som från nyår 2008 ingår i Sven Lovén centrum för marina vetenskaper, har erfarenheter tillbaka till 1877 och kan i flera hänseenden anses utgöra ett nationellt centrum och laboratorium. Bland annat fyller de en sådan uppgift genom:

- sitt inarbetade namn och renommé
- sin belägenhet vilken möjliggör många olika mätningar och experiment
- stationens utrustning, med bland annat forskningsfartyg
- verksamhetens bredd

För att ge inspiration och ytterligare kunskap om viktiga förutsättningar för uppbyggnaden av ett lyckat nationellt centrum genomförde FOI ett studiebesök vid Kristineberg 6-7 oktober 2008. Under besöket gjordes en rundvandring på stationen och omfattande samtal fördes med stationens administrativa chef Ola Björlin. Medvetet valdes att studera en verksamhet av helt annan art, för att inte hamna i detaljdiskussioner kring problematiken associerad med digitala kontrollsystem, utan istället fokusera på mera generella kvaliteter som ger en nationell statusposition och goda resultat.

Stationen på Kristineberg har 32 seniora forskare och cirka 5 doktorander associerade till sig. Ett antal studenter läser kurser vid Kristineberg. Stationen, betraktad som infrastruktur, finansieras till drygt 50 % via fakultetsanslag och andra långsiktiga anslag. Detta möjliggör för olika forskare och forskningsprojekt att använda stationen med dess utrustning och tjänster som en resurs för sina experiment och studier. Stationens tjänster baserar sig på kunnandet hos en grupp teknisk och administrativ personal som bland annat underhåller laborativ utrustning, forskningsfartyg och så vidare.

Förenklad kan detta formuleras som att teknisk och administrativ personal tillhandahåller stationens bastjänster. Dessa bastjänster utgör den infrastruktur som enskilda forskare utnyttjar för att kunna genomföra sina enskilda projekt, med enskild finansiering, vid stationen.

Vid besöket poängterades vikten av att centrumet lyckas inarbeta och upprätthålla ett namn i folks medvetande, såväl bland expertis som bland den bredare allmänheten. Lyckas men med det är det till exempel lättare att få rollen som kunskapsbank inom det område man arbetar. Det kräver i sin tur arbete med att verkligen söka och fastställa centrumets identitet, i betydelsen att hitta delarna i de begrepp som centrumet utgår ifrån. Det gäller med andra ord att tydligt klargöra vad begreppen står för.

Under besöket lyfte Björlin också fram ett antal viktiga punkter, av varierande art, som tål att tänkas på i arbetet med en eventuell centrumbildning:

- Låt olika grupperingar mötas regelbundet i informella former, gärna med lite kaffe eller mat.
- En centrumbildning har tydliga fördelar, exempelvis identitetsmässigt, genom att vara en informationsnod och rådgivare.

- Utbyte av erfarenheter, exempelvis forskningserfarenheter, bör systematiskt uppmuntras och främjas. Det är till exempel viktigt att undvika att någon skyddar sina egna detaljresultat.
- Det är viktigt att identifiera vilka andra intressenter som existerar på området, både med avseende på konkurrenssituationen och möjliga samarbeten.
- Det är synnerligen viktigt att tala om att man existerar, var man befinner sig och vad man kan och gör.

2.3 Aktörer, aktörsrelaterade frågeställningar och synpunkter

Inför en eventuell uppbyggnad av ett nationellt centrum är det av vikt att inhämta synpunkter på den tänkta verksamheten från olika kategorier av aktörer och intressenter inom området (se 2.2 ovan). Synpunkterna kan exempelvis beröra hur laboratoriet kan stödja och hjälpa aktörerna, vilka arbets-, samverkans- och organisationsformer som är lämpliga, vilka aktiviteter som laboratoriet kan och bör bedriva, på vilket sätt beställningar av arbete från laboratoriet kan ske och rutiner för förvaltning av känslig information.

För ett nationellt centrum om säkerhet i SCADA-system har följande aktörer eller aktörskategorier identifierats:

- Användare av digitala kontrollsystem (i första hand stora användare inom samhällsviktiga verksamheter)
- Underrättelse- och säkerhetsmyndigheter
- Myndigheten för samhällsskydd och beredskap (MSB)
- Sektorsmyndigheter (av särskild vikt Svenska Kraftnät, Banverket och Livsmedelsverket)
- Internationella samarbetspartners (exempelvis INL[10] och liknande verksamhet inom EU)

(Till denna lista kan läggas leverantörer av system.)

I samband med identifierande av aktörerna har även en uppsättning generella frågor av vikt att studera identifierats:

1. Hur kan ett nationellt centrum hjälpa olika aktörer (speciellt industriella aktörer och olika myndigheter) att hantera säkerhetsfrågor relaterade till industriella kontrollsystem och samhällsviktiga verksamheter?
2. Under vilka former bör ett nationellt centrum samarbeta med industrin (inklusive andra industriella centrum/laboratorium) och med olika myndigheter?
3. Vilka typer av aktiviteter bör kunna genomföras för att gynna aktörer och sektorsintressen? Följdfråga: Vilka krav och förväntningar ställer detta på bemanning och utrustning?
4. Skall olika aktörer tillåtas att göra extrabeställningar? Hur ska detta gå till för att inte favorisera vissa aktörer eller tränga ut ordinarie verksamhet?
5. Behövs några speciella hänsyn för att kunna samverka med leverantörer av digitala kontrollsystem och komponenter för dessa?
6. Hur hanteras sekretess?

[10] Idaho National Laboratory

Under 2008 har dialog förts med olika aktörer för att inhämta synpunkter rörande dessa frågor och relaterade avvägningar. Denna dialog har genomförts dels i form av samtal (formella och informella) med olika aktörsrepresentanter och dels i form av deltagande vid MSB:s (tidigare KBM:s) arbetsgrupp FIDI-SC, där de viktigaste industriella aktörerna inom området finns representerade.

Det är rimligt att dialogen på olika sätt pågår även i fortsättningen, eftersom det är svårt att ta ställning till en del detaljsvar innan ett eventuellt centrum är inrättat. Detta har i viss mån präglat dialogen så här långt, men – vilket bör påpekas – detta är inget bekymmer i sig.

Mycket förenklad och utan att detaljredovisa dialogen, ges nedan en sammanställning av de svar som kan ges på respektive fråga, med hänsyn tagen till de synpunkter som inhämtats:

1. Ett nationellt centrum kan hjälpa olika aktörer att hantera säkerhetsfrågor relaterade till industriella kontrollsystem och samhällsviktiga verksamheter i form av:
    - Informations- och utbildningsverksamhet
    - Testnings- och studieverksamhet
    - Kunskapsförvaltning
    - Utveckling och forskning

Informations- och utbildningsverksamhet kan genomföras i form av kurser, seminarier och demonstrationer rörande säkerhet i digitala kontrollsystem. Det är här av vikt att höja kompetensen hos olika aktörer, speciellt avseende IT-säkerhetsaspekter på industriella kontrollsystem.

Testnings- och studieverksamheten bör vara inriktad på att kontinuerligt vidareutveckla en teknisk expertis på området digitala kontrollsystem, men bör däremot inte vara inriktad på aktiviteter som ackreditering och certifiering. Denna tekniska expertis kan exempelvis bidra vid utformning av relevanta policies, värdera kvalificerad information, bidra till utveckling av en kunskapsbank och bidra till områdesrelaterad utveckling och forskning.

Återkommande har det i dialogen med olika aktörer poängterats att en kunskapsbank är intressant. Detta är i enlighet med i flera sammanhang[11] poängterade behov av informationsutbyte rörande säkerhet i digitala kontrollsystem. Samtidigt kan det observeras att det här existerar en balansgång mellan behov av informationsutbyte och behov av lämplig grad av informationshantering med sekretess, vilket kräver utveckling av lämpliga rutiner för att såväl hantera öppen som icke öppen information.

Utveckling och forskning bör steg för steg byggas upp på området. Tänkbara områden för forskning kan vara forskning kring säkerhetshot och säkerhetsrisker respektive säkerhetslösningar, värderingsmetoder och värderingsverktyg för industriella kontrollsystem och aspekter i kedjan riskperception[12] – riskanalys – IT-säkerhetsanalys (exempelvis rörande interaktion mellan mänskliga aktörer och kontrollsystemen).

2. Samarbete med industrin (inklusive andra industriella centrum/laboratorier) och med olika myndigheter förutsätts ske konkurrensneutralt, särskilt för att inte prismässigt utkonkurrera privata aktörer. Inom en statlig ramfinansiering för centrumet är det rimligt att som utgångspunkt eftersträva öppet

[11] Exempelvis framkom detta tydligt vid flera presentationer under SANS Process Control & SCADA Security Summit Europé i Amsterdam, 8-11 september 2008, http://files.sans.org/summit/euscada08/..
[12] Innebörden av riskperception och relaterade begrepp diskuteras närmare i KBM (2008b).

informationsutbyte, om inte sekretess är av vikt för de flesta aktörerna, med andra ord på nationell nivå.

Motsvarande bör all verksamhet inom statlig ramfinansiering vara av intresse för de flesta av aktörerna. Med enskild finansiering kan även andra verksamheter pågå under den för den enskilda verksamhetens lämpliga samarbetsformer.

3. Med avseende på typer av aktiviteter har frågan redan besvarats under punkt 1 i denna svarslista. Rörande utrustningsbehov redovisar Wedlin (2008) de behov som för närvarande bedöms vara aktuella. Bemanningsbehov diskuteras i nästkommande kapitel, och sammanfattas i avsnitt 3.3 i en tabell över personalbehov under säkerhetscentrumets första tre år.
4. Se svar under fråga 2.
5. Samverkan med leverantörer bör så långt möjligt präglas av ett öppet informationsutbyte mellan centrumet och leverantörer, men, där så krävs, med sekretess utåt. Det är av vikt att balansera fördelar med sekretess mot fördelar av öppet tillgänglig information.
6. FOI har utvecklade och använda rutiner för ärendehantering med sekretess, vilket där så krävs kan användas.

I bilaga A och B redovisas ett antal specifika synpunkter från två enskilda intressenter.

2.4 Rekommendationer och utgångspunkter för ett SCADA-säkerhetscentrum

Avseende svenska prioriteringar på området säkerhet i industriella kontrollsystem, är det, med utgångspunkt i de resonemang som hittills förts, rimligt att en svensk satsning på säkerhet i industriella kontrollsystem tar sin utgångspunkt i begreppet *nationellt centrum*. Där kan viktig kompetens samlas och vidareutvecklas i samverkan med övriga relevanta aktörer inom landet. Ett *nationellt centrum* indikerar en bredare verksamhet än det smalare begreppet *nationellt laboratorium*, exempelvis indikerar *centrum* att hela spektret i resonemangskedjan riskperception – riskanalys – IT-säkerhetsanalys är av intresse att studera och hantera.

Som en sammanfattning utgående ifrån detta kapitels resonemang och tidigare inhämtade kunskaper formuleras följande generella rekommendationer för organisering av, och utgångspunkter för, en satsning på ett nationellt centrum för säkerhet i SCADA-system:

- Hela resonemangskedjan riskperception – riskanalys – IT-säkerhetsanalys bör beaktas i arbetet med säkerhet i industriella kontrollsystem.
- Det aktuella problemområdet kan delas i två delproblem:
  - Kritikalitet[13] relaterad till industriella kontrollsystem
  - Kritikalitet relaterad till samhällsviktiga verksamheter och viktiga infrastrukturer
- Ett centrum är en lämplig form för att samla kompetens, verksamhet och samarbete rörande säkerhet i industriella kontrollsystem.
- Centrumet bör vara nationellt, där statliga och icke-statliga aktörer samverkar och samarbetar. Grundfinansieringen bör dock vara statlig.

[13] Innebörden av begreppet kritikalitet diskuteras närmare i KBM (2008b).

3 Principskiss för ett nationellt centrum inom SCADA-säkerhet

Med utgångspunkt i de rekommendationer som redovisades i föregående kapitel, formuleras i detta kapitel en principskiss av hur ett säkerhetscentrum inom området säkerhet i industriella kontrollsystem i samhällsviktiga verksamheter kan förverkligas.

Viktiga egenskaper för det tänkta säkerhetscentrumet är:

- En substantiell, långsiktig, medveten och målinriktad satsning
- Kompetensmässig bredd tvärs över olika organisationer och verksamheter
- Gemensam nationell satsning med statlig finansiering av centrumets basverksamhet
- Säkerhetscentrumet skall utgöra en delad resurs i form av att vara en kunskapsbas, informationsnod och rådgivare

3.1 Centrumbildning som infrastruktur

Hur olika andra nationella centrum och laboratorium har organiserats och byggts upp har gett inspiration till centrumförslaget. Särskilt har det tidigare beskrivna studiebesöket på Kristinebergs marinbiologiska forskningsstation bidragit med idéer. En bärande idé för att uppnå flexibilitet och att satsa medel där de gör bäst nytta och för flest möjliga aktörer, är att definiera säkerhetscentrumet som primärt en uppsättning bas- eller stödfunktioner på liknande sätt som vid Kristineberg. Samlat utgör dessa bas-/stödfunktioner en infrastruktur som ytterligare aktiviteter kan grundläggas på. Bildligt kan centrumet ses som ett träd med stam och grenar (infrastrukturen), men inga löv. Löven skulle här vara de projekt och verksamheter som med enskild finansiering nyttiggör centrumets grundläggande infrastruktur.

Att bygga upp centrumet som en infrastruktur på detta sätt ger en betydande flexibilitet. Inom en ramfinansiering för centrumet kan de för intressenterna gemensamt intressanta uppgifterna lösas. Samtidigt möjliggör det även att specialuppdrag av intresse för en eller ett fåtal aktörer kan ges till centrumet, men med enskild finansiering.

Personalstyrkan för centrumet är den baspersonal som krävs för att som infrastruktur realisera, upprätthålla och vidareutveckla centrumets stödfunktioner. Utöver baspersonalen kan med separat finansiering ytterligare personal arbeta med olika till centrumet associerade projekt. Baspersonalen bedöms behövas för att lösa följande kategorier av uppgifter:

1. Centrumadministration och -ledning
2. Informations- och utbildningsverksamhet
3. Testning och studier, operativ
4. Kunskapsförvaltning
5. Uppbyggande, förvaltning och underhåll av laborativ miljö

Närmare specificering krävs vid senare tillfälle av vilka enskilda uppgifter som ingår i de olika kategorierna. Till exempel är detta av vikt vid behov av nyrekrytering av personal för att täcka kompetensbehov inom centrumet.

I de olika uppgiftskategorierna, särskild kategorierna 2-4, ingår även dokumentation, rapport- och artikelförfattande som en central och viktig verksamhet för att bidra till

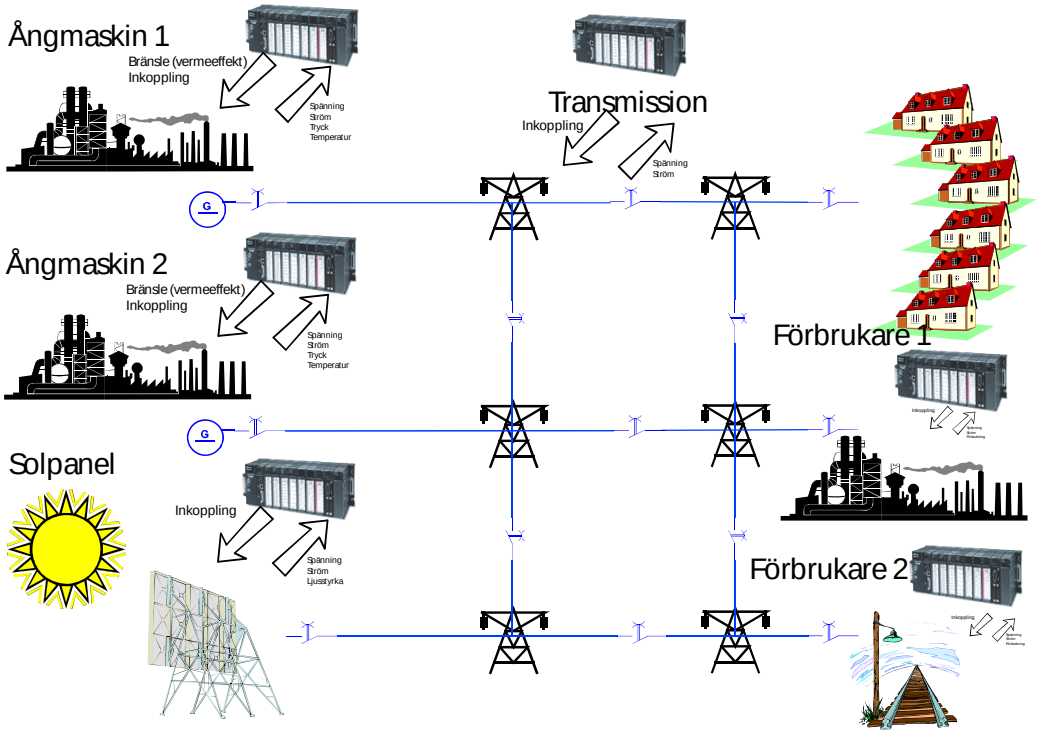
områdets vidare utveckling och forskning, säkra kontinuitet respektive underlätta uppföljning och granskning av verksamheten.

Vissa av säkerhetscentrumets bas-/stödfunktioner utgår ifrån tjänster som finns som allmänt forskningsstöd vid FOI Linköping. Bland annat rör det sig om bibliotekstjänster, fältservice respektive verkstads- och elmonteringsresurser. För centrumets informations- och undervisningsverksamhet är tillgången till undervisningslokalerna i de kurscentrum FOI har byggt upp av särskild vikt.

FOI:s kompetensgrupp inom IT-säkerhet har omfattande erfarenheter av laborativ verksamhet med IT-säkerhetsfokus. För uppbyggnaden av säkerhetscentrumet är detta kompetens av stor vikt, dels vad det gäller att hitta personer som kan utgöra centrumets personal och dels för att bygga ut den laborativa miljön efter centrumets behov. Detaljer avseende utbyggnaden av den laborativa miljön har redovisats separat i tidigare rapport (Wedlin, 2008).

Den laborativa miljön är inte i sig själv viktig, men den blir oerhört viktig i och med att den möjliggör lösandet av centrumets uppgifter. Av de ovan fem listade uppgiftskategorierna är en väl utformad laborativ miljö, tillsammans med kompetent personal och finansiering, helt avgörande för att lösa andra, tredje respektive fjärde uppgiftskategorin.[14]

Vad gäller informations- och utbildningsverksamhet har ett mobilt demonstrationssystem, i form av en modelljärnväg i miniatyrskala med styrsystem tagits fram (Wedlin, 2008). Med hjälp av detta kan sårbarheter, hot och risker med digitala kontrollsystem illustreras på ett konkret sätt som höjer publikens medvetenhet.



Figur 1: En simulerad infrastruktur – generering, överföring och användning av el, (Wedlin, 2008).

[14] Uppgiftskategori 1 (Centrumadministration och –ledning) är minimalt beroende av den laborativa miljön. Uppgiftskategori 5 (Uppbyggande, förvaltning och underhåll av laborativ miljö) är uppenbart beroende av existensen av en laborativ miljö, men utöver denna enkla observation och att övriga uppgiftskategorier drar fördelar av att miljön byggs upp, förvaltas och underhålls, är det inte nödvändigt av att ta upp kategorin till ytterligare diskussion här.

.
FOI:s IT-säkerhetsgrupp förfogar över ett datorkluster med 200 datornoder (Wedlin, 2008). Detta kan användas i undervisningssyfte för att exempelvis simulera en infrastruktur för energiproduktion, -distribution och -användning, (se

Figur 1). En operatörsplats likartad med vad som finns i kommunikations- och ledningscentraler (se Figur 2), tillsammans med enklare operatörsplatser och klassuppsättningar av datorer (Wedlin, 2008) möjliggör ytterligare realism i undervisningssituationer.

Den första undervisningsverksamheten, som genomförs i regi av säkerhetscentrumet, är en heldagskurs där processtyrningskunnig personal, efter pass med demonstrationer av IT-osäkerheter och föreläsningar för att ge grundläggande nätverkskunskap, ges möjlighet att med enkla nätverktyg undersöka och göra intrång i centrala delar av ett fullständigt isolerad nät. Se bilaga C för ytterligare detaljer.

I fråga om operativ testning och studier öppnar de relativt omfattande beräkningsresurser som datorklustret medger för ett brett spektrum av testnings- och studieverksamhet med fokus på säkerhet i operativa digitala kontrollsystemmiljöer. Icke minst är det en fördel att kunna genomföra sådan verksamhet i en rent laborativ miljö, där negativa effekter på samhällsviktiga verksamheter är eliminerade. Testning och studier är beroende av en adekvat och realistisk uppfattning av hur samhällsviktiga verksamheter blir utförda. Existensen av den laborativa miljöns operatörsplatser möjliggör att i rimlig omfattning skapa en sådan uppfattning. Det är tänkbart att senare utveckling av säkerhetscentrumets verksamhet och uppgifter kan peka på behov av kompletterande utrustning för andra typer av testning och studier.

Adekvat kunskapsförvaltning är en förutsättning för centrumets framgång. De erfarenheter informations- och utbildningsverksamhet tillsammans med testning och studieverksamhet ger, bidrar till att bygga upp en kunskapsbas. Rätt förvaltad inom säkerhetscentrumet är den en värdefull resurs vid upphandlingar, kvalitetssäkringsarbete, utveckling, forskning och så vidare. Likaså kan en sådan kunskapsbas bidra till att allmänt höja medvetenhet och kunskap om säkerhet i industriella kontrollsystem. För att uppnå detta är den laborativa miljön synnerligen viktig.

Figur 2: Exempel på operatörsplats under uppbyggnad.

3.2 Verksamhet associerat till centrumet

När centrumets bas- och stödfunktioner har kommit igång, är det dags att initiera olika verksamheter som är associerade till centrumet, men som inte definieras ingå som del i centrumet betraktat som infrastruktur. Bildligt kan detta ses som att ovan omtalade infrastrukturträd börjar få löv (associerade enskilda projekt med enskild finansiering som nyttjar centrumets bas-/stödfunktioner). Forskning och utveckling är verksamheter som det är naturligt att associera till centrumet med dess stödfunktioner. Med utgångspunkt i centrumets tänkta fokus, föreslogs i resonemangen i kapitel 2 tre huvudområden för forskning och utveckling:

- Värderingsmetoder/-verktyg för digitala kontrollsystem
- Sårbarheter, säkerhetshot/-risker respektive säkerhetslösningar
- Övriga aspekter i kedjan riskperception – riskanalys – IT-säkerhetsanalys (exempelvis rörande interaktion mellan mänskliga aktörer och kontrollsystemen)

Argumentation för dessa områden kan utgå från följande observationer: Komplexiteten i kedjan riskperception – riskanalys - IT-säkerhetsanalys understryker vikten av tillgång till adekvata värderingsmetoder och -verktyg. IT-säkerhet låter sig inte enkelt mätas, och den måste även sättas in i en betydelsegivande sammanhang, som ges av exempelvis organisatoriska och operativa förutsättningar. Utbudet av metoder för bedömning och värdering av IT-säkerhet är begränsat, och därmed följer behovet för vidare forskning och utveckling på området. Förbättrade mått på vad som utgör kritiska egenskaper och hur dessa skall hanteras behövs. För detta måste mål för vad som skall mätas och bedömas definieras, relevanta frågor utgående ifrån målet formuleras och metriker som underlättar besvarandet av frågorna väljas.

Värdering är ett viktig steg på vägen mot förbättrad säkerhet, genom att associera sårbarheter, säkerhetshot och säkerhetsrisker till säkerhetslösningar och därmed underlätta valet av lösningar. Implementerade säkerhetslösningar skall hantera risker och hot som kan uppträda i berörda system och verksamheter, och därmed följer behovet av forskning och utveckling kring aktuella respektive tänkbara sårbarheter, hot och risker och handhavande av dessa. Med avseende på industriella kontrollsystem i samhällsviktiga verksamheter, är sambanden mellan IT-säkerhet[15] och drifts- och katastrofsäkerhet[16] mera komplex än i många andra sammanhang. Medvetna aktörer kan realisera IT-säkerhetshot som även kan ha mycket tydliga och problematiska effekter på driftssäkerheten i den verksamhet som styrs av det industriella kontrollsystemet.

Komplexiteten i kedjan riskperception – riskanalys - IT-säkerhetsanalys medför också att interaktionen mellan mänskliga aktörer och kontrollsystemen är en bland flera aspekter som utgör utgångspunkt för utveckling och forskning. De föreslagna forsknings- och utvecklingsområden utgår i betydande grad från digitala kontrollsystem, deras uppbyggnad, funktionssätt och påverkan. Händelser i digitala kontrollsystem har dock följdeffekter i berörda verksamheter och infrastrukturer som inte är begränsade till tekniska effekter. I uppbyggnadsfasen av centrumet torde en tyngdpunkt ligga på tekniska avvägningar och faktorer, men nämnda följdeffekter nödvändiggör att också aktivt involvera kompetens avseende riskanalys respektive interaktion mellan mänskliga aktörer och de olika tekniska system som ingår.

3.3 Årsvis planering för SCADA-centrumet

Med utgångspunkt i en ramfinansiering omfattande tre år för SCADA-säkerhetscentrumet, skisseras här en grov planering för utvecklingen av centrumets tänkta verksamhet:

[15] Vad som på engelska omnämns ”IT security” och huvudsakligen berör intentionella hot.
[16] Vad som på engelska omnämns ”safety” och i utgångspunkten berör icke-intentionella hot

År 1:

Uppbyggnad av SCADA-säkerhetscentrum, speciellt med fokus på labmiljön.

Igångsättande av centrumets basaktiviteter

Identifiera och säkra kompletterande finansieringsmöjligheter utöver för forskning och utveckling

År 2:

Verksamhet inom basaktiviteterna fortgår och vidareutvecklas

Forskning och utvecklingsprojekt startas

Utredning av tänkbar fortsättning för SCADA-säkerhetscentrumet efter ramfinansieringens år 3

År 3:

Verksamhet inom basaktiviteterna fortgår och vidareutvecklas

SCADA-centrumets vidare forskning och utveckling inom ramfinansieringen

Planera fortsättning efter ramfinansieringens år 3

Identifiera lämplig inriktning för forskning och utveckling efter år 3 och söka finansiering för detta

Med utgångspunkt i denna grova planering har följande bedömning av personalbehoven inom ramfinansieringen växt fram:

Tabell 1: Personalbehov [17]

	Personal-behov, år 1 [personår]	**Personal-behov, år 2 [personår]**	**Personal-behov, år 3 [personår]**
Centrumsadministration och –ledning	0,5	0,5	0,5
Informations- och utbildningsverksamhet	1	1	1
Kunskapsförvaltning	0,5	0,5	0,5
Testning och studier, operativt	1	2-3	2-3
Uppbyggande, förvaltning och underhåll av laborativ miljö	1-2	1-2	1-2
Totalt (exkl. FoU)	4-5	5-7	5-7
Forskning och utveckling (FoU utanför ramfinansiering)	-	0,5-1	0,5-1,5
Totalt (inkl. FoU)	**4-5**	**5,5-8**	**5,5-8,5**

[17] FoU: Forskning och utveckling

4 Litteraturlista

KBM (2005), Samhällsviktigt! Ett första förslag till definition av samhällsviktig verksamhet ur ett krisberedskapsperspektiv. Krisberedskapsmyndigheten

KBM (2008a) Vägledning till säkerhet i digitala kontrollsystem i samhällsviktiga verksamheter. Krisberedskapsmyndigheten

KBM (2008b) Digitala kontrollsystem i samhällsviktiga verksamheter - Att bedöma SCADA- och processkontrollsystems kritikalitet. Krisberedskapsmyndigheten

Wedlin, M., (2008) Laborativ utrustning för SCADA-säkerhetscentrum – Beskrivning av uppbyggnaden av en grundläggande undervisnings- och laborationsmiljö för nationell och internationell samverkan kring SCADA-säkerhet. FOI Memo 2615, Totalförsvarets forskningsinstitut

Bilaga A: Synpunkter från industriell aktör

Energibranschens Informations- & IT-säkerhetsforum (EBITS) har vid ett sammanträde i maj 2008 diskuterat roller och arbetsuppgifter för ett tänkt SCADA-laboratorium vid FOI. För att sammanfatta dessa synpunkter har EBITS-dokumentets synpunkter omarbetats något och sammanfattats i fyra kategorier (kolumnerna) av synpunkter i nedanstående tabell.

Det kan observeras att tre av de fyra kategorierna har fokus på hur nå ut till användare av SCADA-system i form av information och utbildning, hur kunskap skall förvaltas och vilka avvägningar som bör göras rörande känslig information. I dessa tre kategorier är teknisk kunskap synnerligen viktigt, men det är inte där fokus ligger.

I den fjärde kategorin är dock fokus rätt tydlig på tekniken i SCADA-systemen i form av testning och kontroll av dessa. I denna kategori ligger de verksamheter som eventuellt först associeras till laboratorieverksamhet.

Kategorin förvaltning av känslig SCADA-information är inte så mycket ett eget självständigt område. Det är mera tal om ett sätt att hantera och genomföra övriga kategoriers aktiviteter på ett sätt som inte röjer känslig information för obehöriga.

Informations- och utbildningsverksamhet	Kunskapsförvaltning	Förvaltning av känslig SCADA-information	Testning och kontroll (operativt men även metodutveckling)
Arrangera utbildningar med stöd av SCADA-labbet för personal (användare av SCADA-system respektive test-/kontrollpersonal)	Kunskapsbank inför upphandlingar, kvalitetssäkringar m.m. (rörande olika system och fabrikat)	Regler och rutiner för hantering av känslig information i kunskapsbanken	Kontroll av att leverantörer följer standarder och fastställda regelverk
Arrangera utbildningar med stöd av SCADA-labbet för personal: Testning av företagens idéer och testmetoder i kontrollerad labmilljö	FOI:s kompetens-höjande roll kring SCADA-säkerhetsfrågor	Sekretesshantering inom myndigheter som FOI	Testning av idéer och testmetoder (uppdrag till FOI från kommersiella oberoende aktörer)
Mobilt demonstrations-system (Målgrupp : Företag som använder SCADA-system)			Framtagning av testmetoder för SCADA-system (FOI och företag i samverkan)
Möjlighet att med FOI-stöd utnyttja/låna labbet för intressenternas personal och material (för att öka personalens kunskaper kring SCADA-säkerhetsfrågor)			Framtagning av testmetoder för SCADA-system (FOI-regi)
FOI:s kompetenshöjande effekt kring SCADA-säkerhetsfrågor			Möjlighet att med FOI-stöd utnyttja/låna labbet för intressenternas personal och material (för test av utrustning)

Vad indikerar detta rörande uppbyggandet av ett SCADA-laboratorium? Ett sådant bör enligt synpunkterna vara betydligt mera än en ren teknisk provverksamhet för SCADA-teknisk utrustning. Med utgångspunkt i synpunkterna kan man tänka sig två huvud-alternativ för att realisera signalerad önskad bredd i verksamheten:

- SCADA-laboratoriet är centrerad kring en teknisk provverksamhet som därmed utgör en bas och kärna för verksamheten. Därigenom styr den tekniska provverk-samheten hur övrig verksamhet blir.

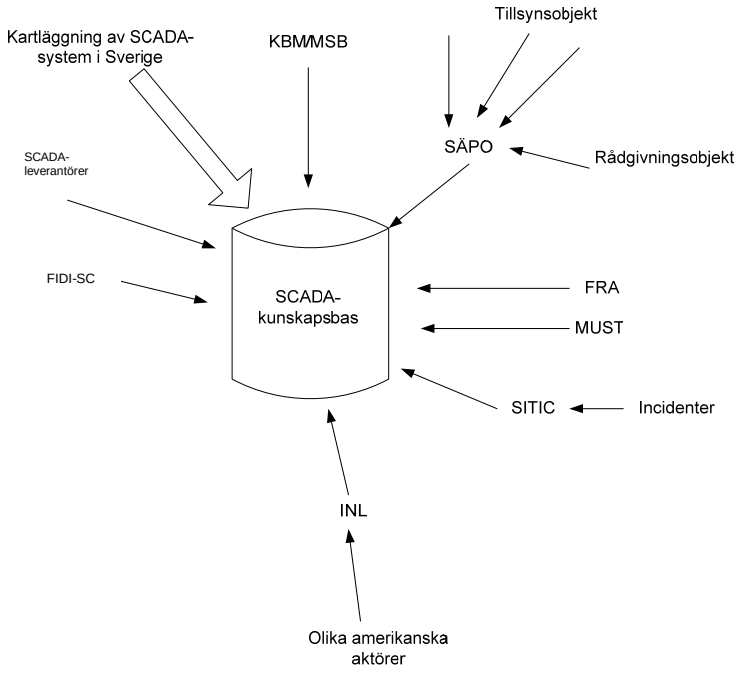
- Den tekniska provverksamheten är en av flera jämställda verksamheter inom SCADA-laboratoriet. Förmodligen kan ett holistiskt perspektiv på SCADA-problematiken lättast utgå från detta alternativ, men det torde kräva mera resurser. I övrigt har IT-säkerhetsgruppen vid FOI en teknisk tyngdpunkt med nuvarande sammansättning.

Bilaga B: Synpunkter Säkerhetspolisen

Vid ett samtal med en representant för SÄPO framkom synpunkterna nedan. Tyngdpunkten i resonemanget var på behovet av en kunskapsbas om digitala kontrollsystem.

Labbet kan/bör utgöra en kontaktpunkt mot svenska producenter av SCADA-utrustning och SCADA-programvara. Detta underlättar handel/utbyte av information med andra SCADA-lab och -aktörer.

Huruvida man kan ha ett informationsutbyte togs upp till relativt omfattande diskussion. Det poängterades som viktigt att ett nationellt lab/centrum utgör en kunskapsbas (se figur), som tar tillvara, analyserar och vidareutvecklar SCADA-erfarenheter från olika aktörer. Vidare diskuterades möjligheter att få in andra aktörers inhämtade kunskaper till en sådan central kunskapsbas. I sammanhangen är det av vikt att ta fram rutiner och praxis för att dela information med andra aktörer.



Figur 3: Nationellt centrums roll som kunskapsbas

Det poängterades att rörande tester bör fokus vara på testning utifrån svenska testbehov, vilket delvis kan baseras på tidigare utredningar och inventeringar, men även på kompletterande nya.

Det är viktigt att som myndighet inte prismässigt utkonkurrera privata aktörer.

Undervisningsinsatser bör rikta sig in på intressenter i ett mellanskikt mellan teknik och organisation, där man fortfarande har en påverkan på tekniken.

Omfattning på verksamheten: Bedöms vara svårt att yttra sig om, men minst två på heltid. Inget problem att ha 3-4 på heltid.

FOI får gärna ta fram ”guidelines” och ”best practice”-dokument.

Bilaga C: SCADA-laboration

Motivation

Det finns två distinkt olika målgrupper för kursverksamhet inom IT-säkerhet på SCADA-området. Dels behöver traditionell processtyrningsspersonal förstå konsekvenserna av att använda kontorsanpassad IT-teknik i styrsystemssammanhang. Både ur aspekten att de har en högre hotbild i form av att de är betydligt generellare och ur aspekten att användande av dessa standardprodukter inbjuder till att koppla ihop administrativa nät med styrsystemsnät. Den andra gruppen som behöver utbildas är traditionella IT-tekniker som behöver utbildning i de speciella krav som ställs på SCADA-system i och med att operativsystemen ofta inte går att underhålla och uppdatera på sedvanligt sätt för att hantera upptäckta sårbarheter. Likaså gör strängare tidskrav att många vanliga skyddsåtgärder inte går att införa i dessa system. Denna grupp behöver främst undervisning i alternativa skyddsstrategier.

Laborationskursen som beskrivs i denna bilaga riktar sig framför allt till den första gruppen, de processstyrningskunniga. En svårighet vi upplever här är att IT-säkerhet på den tekniska nivån är genuint svår att förstå för någon som inte är datorkunnig med ett avsevärt tekniskt djup. Vi har tidigare främst hanterat detta genom att bygga på tillrättalagda demonstrationer där mycket kraft har lagts på den pedagogiska utformningen. Utvecklingen de senaste åren bland tillgängliga intrångsverktyg har varit att dessa blivit betydligt enklare att använda och verktyg som *nmap* och *nessus* har vi redan använt i laborationer under en längre tid. Uppkomsten av *Metasploit* med dess användarvänliga gränssnitt gör att det nu borde vara möjligt att införa moment där hela kedjan från kartläggning av sårbarheter till faktiska intrång exemplifieras.

Vad vi vill undersöka vid detta första provtillfälle är om antagandet att verktygen idag är tillräckligt enkla håller och att en normalt processstyrningskunnig förstår tillräckligt mycket av kurstillfället för att det skall ge bestående insikter.

Kursupplägg

Kursen kommer att vara en heldagskurs enligt följande schema:

08:30-09:00	Registrering med kaffe och fralla
09:00-09:45	Demonstration av IT-osäkerhet
10:00-10:45	Grundläggande nätverkskunskap
11:00-11:45	Nätverksarkitektur
12:00-13:00	Lunch
13:00-13:45	Genomgång av labbmiljön och verktygen
14:00-17:00	Laboration

Demonstration av IT-osäkerhet

Genomför en vanlig ”Tivoliföreställning” med fokus på demonstrationer som illustrerar att det finns en mängd kommunikationer som är dolda för användaren. Ta med momenten:

Lakritstrollet[18]

[18] Samma dokument visar olika information beroende på vilken version av Windows som används.

DCOM[19]

Förändrat virus[20]

Grundläggande nätverkskunskap

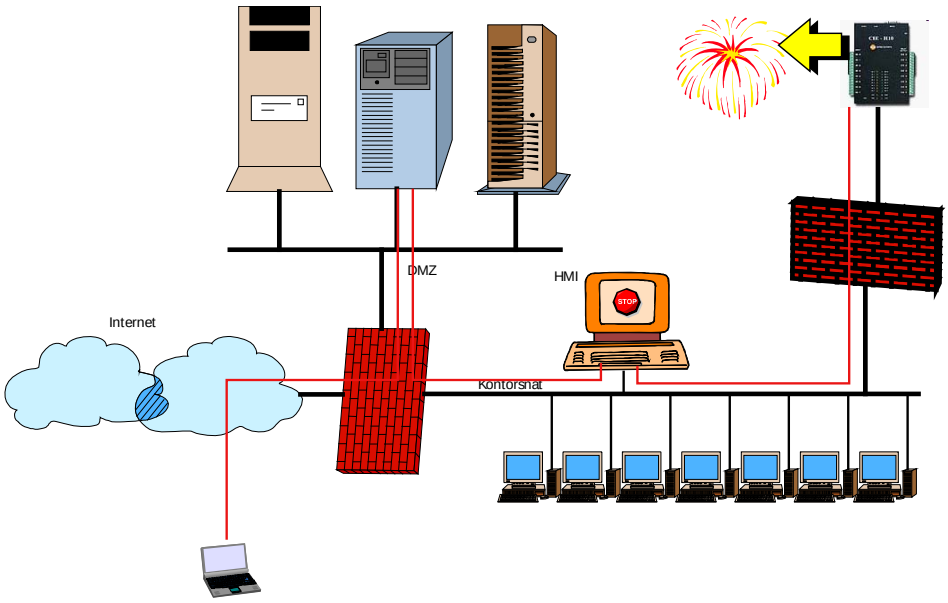
Plocka passet om nätverk från HKES[21]. Skall ge deltagarna en grundläggande förståelse för IP-adressering, portar, protokoll, OSI-modellen och MAC-adresser.

Grundläggande arkitektur

Nyutvecklat moment som skall ge deltagarna en grundläggande förståelse för hur man oftast bygger upp en nätverksarkitektur med begrepp som brandvägg, DMZ, kontorsnät och styrsystemsnät. Skissera upp nätet som kommer att användas i labben.

Genomgång av labbmiljön

Deltagarna kommer att ha var sin laptop med programmen *nmap* och *nessus* installerad under Windows. *Metasploit* körs med en BackTrack under VMWare player. Nätkonfiguration enligt nedan i så många exemplar som det finns deltagare.



Figur 4

Genomförande

Labben genomförs i flera faser:

1. Deltagaren får sig tilldelat ett nät och scannar detta med *nmap*.
2. Datorerna på DMZ-nätet syns.

[19] Intrång via nätverk via en sårbarhet i en nätverkstjänst
[20] Demonstrerar hur enkelt det är att lura ett virusskydd
[21] Högre Kurs i Elektronisk Säkerhet. Kurs omfattande 1 vecka som ges vid FOI, Linköping.

3. Webservern skannas med *Nessus* och en sårbarhet identifieras. Skanna övriga servers i mån av tid.
4. Intrång i webservern med meterpreter.
5. Sätt upp metasploitrouting genom webservern.
6. Leta igenom nätet innanför för att hitta HMI-stationen.
7. Ta reda på vad den är för något och metasploita den. Använd VNC.
8. Tryck på knappen och tårtfontänen går av.
9. Extrauppgift: Hitta developmentstationen med det extra interfacet till styrsystemsnätet och gör intrång i denna. Routa vidare och kartlägg vad som finns i övrigt på detta nät.

Deltagarna har ett labbkompendium av fylleriformat som är tänkt att leda deltagaren genom alla moment utan att någon riskerar att misslyckas. Viktigt är också att uppmuntra till egen aktivitet runt omkring.