NCS3: årsrapport 2012

Nationellt centrum för säkerhet i styrsystem
för samhällsviktig verksamhet

JONAS HALLBERG, MIKAEL WEDLIN, DAVID LINDAHL,
JONAS ALMROTH, MATS PERSSON, TEODOR SOMMESTAD

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
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se

FOI-R--3638--SE
ISSN 1650-1942 Januari 2013

Jonas Hallberg, Mikael Wedlin, David Lindahl,
Jonas Almroth, Mats Persson, Teodor Sommestad

NCS3: årsrapport 2012

Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet

Titel	Årsrapport 2012
Title	Annual report 2012
Rapportnr/Report no	FOI-R--3638--SE
Rapporttyp Report Type	FOI-rapport FOI report
Månad/Month	Januari/January
Utgivningsår/Year	2013
Antal sidor/Pages	27 p
ISSN	ISSN 1650-1942
Kund/Customer	MSB
Projektnr/Project no	E32312
Godkänd av/Approved by	Christian Jönsson

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för Informationssystem
Box 1165
581 11 Linköping

FOI, Swedish Defence Research Agency
Information Systems
Box 1165
SE-581 11 Linköping

Sammanfattning

Syftet med *Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet*, NCS3, är att stödja det nationella arbetet rörande säkerhet i industriella informations- och styrsystem. Denna rapport sammanfattar den verksamhet som under 2012 bedrivits inom ramen för NCS3.

Nyckelord: Industriella informations- och styrsystem, IT-säkerhet, kritisk infrastruktur

Summary

The purpose of the *National Center for security in control systems for critical infrastructure*, NCS3, is to support the Swedish national effort on security in industrial information and control systems. This report summarizes the activities performed within the framework of NCS3 during 2012.

Keywords: Industrial control systems, Supervisory control and data acquisition systems, SCADA, IT security, critical infrastructure

Innehåll

1 Inledning

Denna rapport sammanfattar den verksamhet som under 2012 bedrivits inom ramen för *Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet* (NCS3). Verksamheten drivs i projektform av Totalförsvarets forskningsinstitut (FOI) på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB) och utgör en del av MSB:s satsning på ett nationellt program för ökad säkerhet i industriella informations- och styrsystem.

Mål och syfte för verksamheten under 2012 fastställdes gemensamt av MSB och FOI. Enligt denna överenskommelse har projektets fokus under 2012 legat på att:

- bygga upp mer specifik styrsystemskompetens vid NCS3,
- höja medvetenheten om behovet av IT-säkerhet i industriella informations- och styrsystem i samhället,
- uppgradera den tekniska infrastrukturen vid NCS3 samt
- fortsätta arbetet med NCS3:s tekniska inriktning.

1.1 Syfte, mål och omfattning

Verksamheten vid NCS3 syftar till att minska de risker som införandet av nätanslutna industriella informations- och styrsystem för styrning av samhällsviktig infrastruktur medför, speciellt med avseende på avsiktlig störning. NCS3:s vision och strategi återfinns i förkortad version i kapitel 2 och i sin helhet i FOI Memo 4166[1]. Projektets syfte är att utveckla NCS3 enligt denna strategi. Därmed ska projektet, inom området industriella informations- och styrsystem, utveckla kompetens, metodik och tekniska plattformar för

- övningar av IT-försvar
- medvetandehöjning genom tekniska demonstrationer
- utbildning avseende sårbarheter, risker och lösningar
- stöd av experimentbaserad forskning
- analys av aktuella sårbarheter, risker och lösningar.

För att säkerställa att verksamheten har rätt inriktning hålls en kontinuerlig dialog mellan MSB och FOI. Inom ramen för denna dialog bestämdes att projektet under 2012 skulle bestå av följande sju delprojekt.

[1] FOI Memo 4166. *Vision och strategi för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet 2012 till 2017*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

1. Inriktning, samverkan, projektledning
2. Utbildning
3. Utveckling av demostratorer
4. Labbutveckling
5. Kunskapsutbyggnad inom industriella styrsystem
6. Tekniska studier
7. Forskningsfrämjande åtgärder

Under 2012 har ett antal aktiviteter genomförts inom ramen för dessa delprojekt. FOI levererar för varje genomförd aktivitet en enklare dokumentation. Denna årsrapport syftar till att summera årets verksamhet samt att sammanställa dokumentationen av de genomförda aktiviteterna.

1.2 Rapportering

Följande dokumentation har under 2012 tagits fram vid NCS3.

FOI Memo 4166. *Vision och strategi för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet 2012 till 2017*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

FOI Memo 4218. *Detektion av angrepp och förebyggande åtgärder för Siemens S7-serie.* Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

FOI Memo 4315. *Working report on advanced technical security measures for industrial control systems*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

FOI Memo 4317. *Forskningsfrämjande åtgärder vid Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

FOI Memo 4318. *Seminarier om skadlig kod*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

FOI Memo 4330. *Demonstrationer och föreläsningar under 2012 – Utvärderingar*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

FOI Memo 4331. *Tekniska Verken – kartläggning av SCADA-system*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

FOI Memo 4332. *Kursmaterial för SIK oktober och december 2012*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

FOI Memo 4333. *Uppdaterad (programvara och maskinvara) och dokumenterad labbinfrastruktur*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

FOI Memo 4356. *Labb- /kursmoment med PLCer*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

FOI Memo 4357. *Fabriksdemonstratorn v.2.0*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

FOI Memo 4368. *Rapport från 2012 SANS EU SCADA & Process Control Summit*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

FOI Memo 4369. *2013 Digital Bond's SCADA Security Scientific Symposium (S4)*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2013.

FOI-rapport FOI-R--3434--SE. *Application whitelisting, Raises the bar against certain threats but no silver bullet.* Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

FOI-rapport FOI-R--3567--SE. *Möjligheter och problem vid analys av fientlig kod riktad mot Siemens S7-serie.* Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

Genomförda SIK-kurser våren 2012. Diarienummer FOI-2010-1802-3. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

Kartläggning av SCADA-nätverk, Utkast. Diarienummer FOI-2010-1802-6. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

Plan för årets tekniska studier. Diarienummer FOI-2010-1802-7. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

Preliminär årsplanering av demonstrationer. Diarienummer FOI-2010-1802-4. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

Utvecklingsplan demonstratorer - en analys av behovet och kortare beskrivning av nuläge. Diarienummer FOI-2010-1802-8. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

Verktygslåda för S7-kurser. Diarienummer FOI-2013-130. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

1.3 Rapportstruktur

Resterande delar av denna rapport är upplagda enligt följande. I kapitel 2 beskrivs vision och strategi för *Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet*. I kapitel 3 redogörs för de aktiviteter som har genomförts under 2012.

2 Vision och strategi

I detta kapitel presenteras vision och strategi för *Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet* (NCS3), vilket finansieras och inriktas av MSB och byggs upp vid FOI i Linköping. Beskrivningen består av utdrag ur dokumentet FOI Memo 4166[2].

Visionen för NCS3 knyter tydligt an till samhällets övergripande behov av IT-säkerhet i industriella informations- och styrsystem, såsom uttryckt i Nationell Handlingsplan för Samhällets Informationssäkerhet (MSB 2012). Strategin bryter sedan ner det övergripandet behovet i fyra delområden som möjliggör riktade aktiviteter mot centrala målgrupper.

2.1 Vision

> *NCS3 ska vara den naturliga nationella mötesplatsen där aktiviteter som experiment, övningar och studier bedrivs för att höja säkerheten i industriella informations- och styrsystem för samhällsviktig verksamhet.*
>
> *Medarbetarna vid NCS3 ska ha nationellt och internationellt unik kompetens inom området.*

2.2 Strategi

Den övergripande strategin är att bedriva verksamhet inom väl definierade delområden med tydlig koppling till det *Nationella programmet för ökad säkerhet i industriella informations- och styrsystem* och den *Nationella handlingsplanen för samhällets informationssäkerhet*. Strategin utgår från de fyra områdena medvetenhet, kunskap, erfarenhet och samverkan.

Varje område inleds med en övergripande målbild som därefter specificeras och exemplifieras med ett urval av aktiviteter. Alla aktiviteter syftar till att höja säkerheten i industriella informations- och styrsystem. I en sedvanlig årlig projektplanering ska sedan verksamheten prioriteras och aktiviteter med detaljerade, uppföljningsbara mål specificeras.

[2] FOI Memo 4166. *Vision och strategi för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet 2012 till 2017*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

2.2.1 Medvetenhet

Målbild: NCS3 ska fortlöpande bidraga till ökad medvetenhet avseende problematiken och riskerna inom området genom att sprida kunskap till berörda parter.

NCS3 ska vidareutveckla och bredda förmågan att skapa intresse för och öka medvetenheten om aktuella frågor avseende säkerhet i industriella informations- och styrsystem. Centret ska vara den naturliga nationella aktören avseende demonstrationer och kurser inom området.

Exempel på aktiviteter som behövs för att nå målbilden för detta område är att:

- Identifiera prioriterade målgrupper och kanaler för att nå dessa.
- Utveckla målgruppsanpassade demonstratorer som ska skapa medvetenhet om hot, risker och möjliga lösningar.
- Anpassa kursinnehåll för IT-tekniker med fokus på hur industriella informations- och styrsystem fungerar.
- Anpassa kursinnehåll för styrsystemstekniker med fokus på hur IT-system fungerar.

2.2.2 Kunskap

Målbild: NCS3 ska kontinuerligt bygga upp och sprida ny relevant kunskap samt skapa förutsättningar för relevant, experimentell forskning inom området. Den forskning och de egna studier som bedrivs vid NCS3 ska resultera i uppbyggnad och vidmakthållande av internationellt unik kompetens inom området.

Medarbetarna vid NCS3 ska besitta en nationellt och internationellt unik kompetens inom säkerhet i industriella informations- och styrsystem. Kompetensen ska möjliggöra förmåga att analysera aktuella hot och brister samt att kravställa säkerhet för industriella informations- och styrsystem. Vidare ska NCS3 stödja uppbyggnaden av nationell kompetens inom området genom att sprida kunskap till beslutsfattare, utvecklare, tekniker och operatörer samt skapa förutsättningar för experimentell forskning inom området.

Exempel på aktiviteter som behövs för att nå målbilden för detta område är att:

- Utveckla förmåga att analysera fientlig kod riktad mot industriella informations- och styrsystem.
- Utveckla förmåga att analysera utrustning och verktyg för säkerhet i industriella informations- och styrsystem på en teknisk nivå.
- Utveckla den befintliga plattformen för experimentell forskning för att stödja experimentell validering av metoder, verktyg och andra aspekter inom området.
- Öka mängden relevanta publika forskningsdata, genom att publicera resultat och data från verksamhet som har genomförts i centret.

- Följa områdets utveckling, exempelvis genom kurser, konferenser och incidentanalyser.

2.2.3 Erfarenhet

Målbild: NCS3 ska genomföra regelbunden övning och träning av ansvarig personal med syfte att vidmakthålla och höja den operativa kompetensen avseende IT-försvar av kritiska styrsystem.

NCS3 ska bidra till större nationella övningar med metodik och tekniska plattformar framtagna vid centret. Vidare ska centrets övningsplattform utnyttjas vid större internationella övningar. Mindre övningar ska regelbundet genomföras med centrets övningsplattform som grund.

Exempel på aktiviteter som behövs för att nå målbilden för detta område är:

- Övningsplattformen ska vidareutvecklas för att erbjuda större flexibilitet, förbättrad överblick av händelseförlopp och ytterligare möjligheter till uppföljning av genomförda övningar.
- Standardiserade övningar ska tas fram för att minska behovet av förberedelser inför övningar. Ett sätt att åstadkomma detta är framtagande av scenarion med inspel och händelser som medför realistiska övningsmoment.
- Metoder för observation och dokumentation samt metodik för övningsutvärdering ska utvecklas.
- Övningsplattformen ska anpassas för att kunna genomföra övningar riktade mot olika intressenter från olika branscher och med olika kompetenser.
- Demonstratorer relaterade till industriella informations- och styrsystem ska integreras i övningarna.

2.2.4 Samverkan

Målbild: NCS3 ska arrangera och stödja genomförandet av evenemang som syftar till att öka samverkan mellan de nationella aktörerna på en teknisk nivå inom området samt aktivt delta i relevanta internationella nätverk.

Målen är att centret ska vara den naturliga samlingsplatsen för relevanta aktörer för att skapa såväl ett väl fungerade nationellt nätverk som relevanta internationella kontakter och samarbeten inom området. Vidare ska synergier med andra verksamheter skapas för att uppnå en total verksamhet som ger mervärde för alla involverade behovsägare. Andra verksamheter kan exempelvis utgöras av forskningsprojekt eller övningar.

Exempel på aktiviteter som behövs för att nå målbilden för detta område är:

- Studiebesök hos relevanta aktörer.
- Seminarier med relevanta aktörer.
- Verksamhet med bas i labbet och övningsplattformen finansierad av andra aktörer.
- Ha aktiva kontakter med relevanta behovsägare och knyta dessa till centrets verksamhet.
- Aktivt deltagande i nationella och internationella nätverk.
- Samarbete med leverantörer av industriella informations- och styrsystem.
- Etablera kontakter och samarbeten med centrala internationella aktörer inom området, exempelvis italienska JRC och amerikanska Idaho National Laboratory, INL.

3 Verksamhet 2012

I detta kapitel beskrivs de under 2012 genomförda delprojekten med avseende på syfte, genomförande och resultat. Syftet med respektive delprojekt beskrivs med utgångspunkt i den förväntade effekt som specificerats i överenskommelsen mellan MSB och FOI. Delprojektens genomförande och resultat kopplas till de leverabler som specificeras i överenskommelsen mellan MSB och FOI.

3.1 Inriktning, samverkan, projektledning

Detta delprojekt syftar till att uppnå följande effekt.

- Ökad nationell praktisk samverkan kring it-säkerhet i industriella informations- och styrsystem.
- De kontaktnät som idag är kopplade till NCS3 upprätthålls och utvecklas.
- Ökad kännedom om NCS3 i samhället.
- En ökad förståelse för hur olika aktörer kan stöttas i sitt arbete att öka it-säkerheten i industriella styrsystem.
- En strategisk inriktning för Projektet och ett väl sammanhållet projekt.

Följande delavsnitt motsvarar de leverabler som specificerats för delprojektet.

3.1.1 Visions- och strategidokument

Under 2012 togs vision och strategi för NCS3 fram. Dessa beskrivs i sin helhet i FOI Memo 4166[3] och i förkortad version i kapitel 2 i denna rapport.

3.1.2 Årsrapport

För att sammanställa rapporteringen av verksamheten vid NCS3 under 2012 har en årsrapport (denna rapport) tagits fram.

3.1.3 Kommunikationsplan

Arbetet med kommunikationsplanen har pågått under hela året, men inte lyckats landa i ett färdigt dokument. Den största anledningen till att arbetet har tagit längre tid än planerat är en initial underskattning av komplexiteten i hur projektets kommunikationsplan skulle förhålla sig till hela programmets plan.

[3] FOI Memo 4166. *Vision och strategi för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet 2012 till 2017*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

Mycket arbete är därför nedlagt på att synkronisera de båda planerna. Arbetet kommer därför att fortsätta under 2013.

3.1.4 Samverkan med externa aktörer

Inom ramen för arbetet med NCS3 bjöds den internationellt erkända säkerhetsforskaren Dr. Bencsáth Boldizsár in till Sverige under hösten 2012[4]. Dr. Boldizsár är verksam vid Laboratory of Cryptography and System Security (CrySyS) vid Budapest Universitet och har tillsammans med sina medarbetare vid CrySyS gjort betydande insatser inom analys av skadlig kod, såsom Duqu, Stuxnet och Flame.

Under ett par intensiva dagar, 2012-10-18 – 2012-10-19, anordnades tre seminarier och ett flertal möten med representanter för NCS3 och SAMFI-myndigheterna samt forskare från andra organisationer. Därmed fick närmare 60 personer från en rad olika organisationer möjlighet att höra det allra senaste kring jakten på avancerad skadlig kod.

3.2 Utbildning

Detta delprojekt syftar till att uppnå följande effekt.

- Ökad medvetenhet om behovet av it-säkerhet i industriella informations- och styrsystem hos berörda aktörer.
- Ökade tekniska kunskaperna om it-säkerhet i industriella informations- och styrsystem hos de som äger och driver samhällsviktig verksamhet och kritisk infrastruktur, samt hos sektors- och tillsynsmyndigheter.
- De personer som genomgår utbildning sprider kunskaperna i sina organisationer och branscher. Den utbildnings som ges ökar inspiration hos deltagarna så att säkerhetsarbetet fortsätter när de kommit tillbaka till sina respektive organisationer.
- En nära praktisk samverkan med prioriterade aktörer.

Följande delavsnitt motsvarar de leverabler som specificerats för delprojektet.

3.2.1 Anpassning av kursen Säkerhet i industriella kontrollsystem

Under 2012 har kursen Säkerhet i Industriella Kontrollsystem (SIK) anpassats för sektorerna kärnkraft, transport samt vatten- och avloppsförsörjning.

[4] FOI Memo 4318. *Seminarier om skadlig kod*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

Anpassningen för Kärnkraftssektorn bestod bland annat i att textstycken och exempel byttes ut i det utdelade materialet för att bättre täcka in för kursdeltagarna relevanta områden. Vidare tryckte föreläsarna på de aspekter av säkerhet som berör kärnkraftssektorns speciella förutsättningar och hotbild. Kursutvärderingen var positiv.

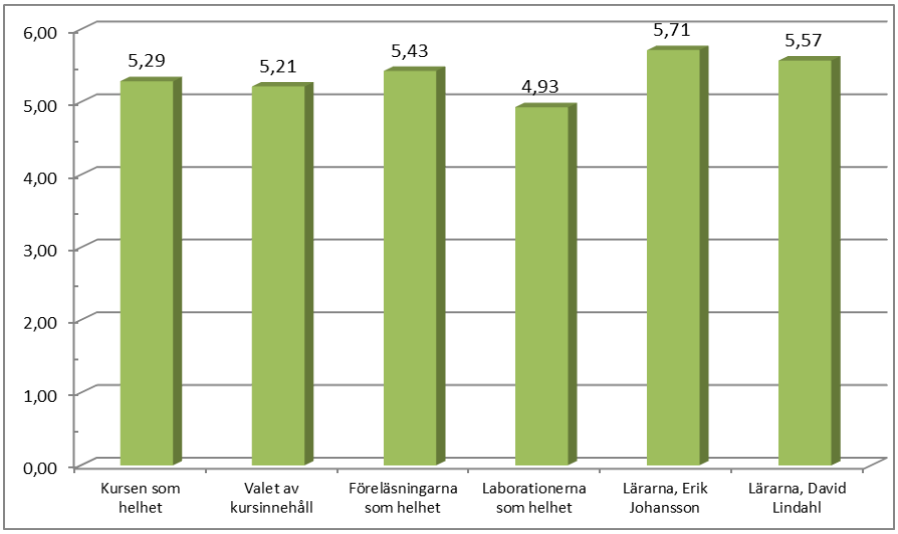
Anpassningarna för transport respektive vatten- och avloppsförsörjning redovisas i FOI Memo 4332[5] med bilaga. Kursmaterialet användes vid de kurser som gavs med start 2012-10-24 respektive 2012-12-05. Bilagan omfattar det som delades ut i pärmformat till kursdeltagarna. Kurserna individualiserades genom att exempel och diskussioner tog upp branschspecifika problem och erfarenheter för att passa deltagarnas bakgrund. Enligt kursutvärderingar fungerade detta bra, men deltagarna efterlyste kursmaterial som är anpassat efter bakgrund så att de med tekniska arbeten kunde använda det utdelade materialet som referensmaterial i efterhand.

3.2.2 Genomförande av kursen Säkerhet i industriella kontrollsystem

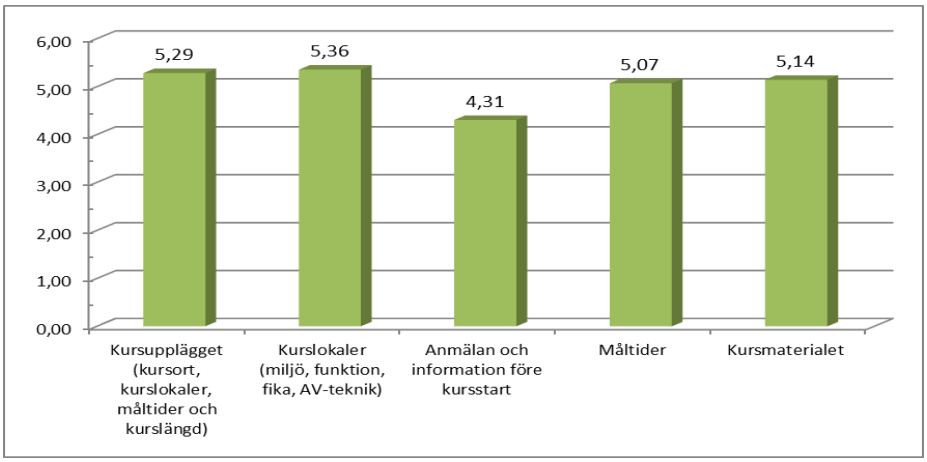
Under 2012 genomfördes kursen Säkerhet i Industriella Kontrollsystem (SIK) fyra gånger. Det första tillfället riktades mot en bred målgrupp. Det tre följande tillfällena riktades mot kärnkraftsbranschen, transportsektorn respektive vatten- och avloppsförsörjning med de anpassningar av kursmaterialet som beskrivs i avsnitt 3.2.1.

Efter genomförda kurser utför deltagarna alltid en omfattande kursutvärdering. Denna ger värdefull information om vad som fungerar och vad som kan behöva förbättras till nästa gång. Figur 1 och Figur 2 nedan sammanfattar deltagarnas utvärderingar från kurstillfället för kärnkraftsindustrin i juni 2012. Sammanställning av utvärderingarna från alla fyra kurstillfällena under 2012 återfinns i FOI Memo 4330[6].

[5] FOI Memo 4332. *Kursmaterial för SIK oktober och december 2012*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.
[6] FOI Memo 4330. *Demonstrationer och föreläsningar under 2012 – Utvärderingar*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.



Figur 1: Det samlade betyget om kursen. Högsta möjliga betyg är 6. Deltagarna är överlag positiva till hur kursen genomförts.



Figur 2. Det samlade betyget kring de administrativa delarna av kursen. Högsta möjliga betyg är 6. Det finns förbättringspotential avseende ”Anmälan och informationen före kursstart”.

Efter vårens två kurstillfällen genomfördes en intern utvärdering för att belysa möjligheterna till förbättringar inför framtiden baserat på återkoppling och kursledningens egna erfarenheter. Kurserna har generellt avlöpt väl och får återigen bra betyg med ett snitt på mellan fem och sex av sex möjliga. Kritiken begränsades till förekomst av och längd på raster. I fortsättningen ska

hållpunkterna i schemat hållas bättre. Förslagsvis sätter vi upp fasta rasttider och uppmuntrar då även deltagarna att lämna rummet så att det kan återluftas.

Kursformatet är väl inarbetat och kursutvärderingarna visar att deltagarna är mycket positiva till genomförandet, men det finns som sagt fortfarande punkter med förbättringspotential. Baserat på vår egen erfarenhet listas nedan ett antal olika punkter där det finns klara förbättringsmöjligheter.

- **Kommunikation**
  Det är viktigt att möjligheterna till att skapa medvetandehöjning i sin organisation kommuniceras tydligt till verksamheter som är kritiska för samhället. Annars riskerar vi att kurserna inte fylls i tid och att värdefulla utbildningsplatser då går till spillo trots att behovet av dessa i samhället är stort.
- **Hemsida**
  På kursens hemsida behövs tydligare information om vilket kurstillfälle som anmälningen avser. Vid ett tillfälle under året erhölls sex stycken anmälningar som visade sig vara till senare kurstillfällen än det aktuella.
- **Logi**
  Inför varje kurstillfälle bör vi genomföra en kontroll av vilka hotellalternativ som finns och framförallt kontrollera om kurstillfället kolliderar med några andra stora evenemang i Linköping. Under våren 2012 hade ett företag valt att förlägga en nationell konferens till Linköping vilket gjorde att det var svårt för en del av kursdeltagarna att få tag på hotellrum.
- **Personberoende**
  Kursen har två skickliga föreläsare, men saknar delvis redundans. Om någon av huvudföreläsarna inte kan medverka finns ingen naturlig ersättare tillgänglig som kan ta hand om deras respektive kursdelar. För att minska detta personberoende bör ytterligare personer från enheten delta på kursen som observatörer. Dessa observatörer kan då även få till uppgift att fungera som kritiker för att förbättra föreläsningarna ytterligare.
- **Anmälningstid**
  Det måste finnas en hård deadline senast två veckor innan ett kurstillfälle. Den dagen fattas beslut om aktuellt kurstillfälle skall hållas eller inte. Om det av någon anledning är ytterst få deltagare kan kursen eventuellt fyllas på med fler deltagare i efterhand (från en eventuell reservlista). Ett beslut senast två veckor innan krävs för att kursadministrationen skall fungera (tryckeriet och synkning mellan förberedelser och föreläsare) samt för att deltagarna ska kunna ges möjlighet att avboka sin eventuella resa.
- **Personligt kursmaterial**
  Om vi inte löser problemen med sena anmälningar måste vi troligen frångå principen med att ge kursdeltagarna personligt namngivna kursmuggar och anteckningsblock vilket varit uppskattat av deltagarna. I

stället kan vi ta fram muggar med ett mer påkostat SIK-tryck (eller kanske NCS3) och pärmarna kan vi fortfarande lätt förse med deras namn på framsidan. Generellt material förenklar även då vi kan beställa ett större antal i förväg och även ha som buffert för sena anmälningar eller andra aktiviteter. Under alla omständigheter bör vi ha ett lager av generella kursmuggar och annat material.

- **Belysning**
  Ljuset i lokalerna har fungerat otillfredsställande vid ett par tillfällen. Det måste rimligen gå att slå på och av ljusen i en föreläsningssal utan att två av tre lampor slumpmässigt slocknar. Detta är inte något som kursdeltagarna har störts av, men det bör ändå kontrolleras och åtgärdas innan nästa kurstillfälle.
- **AV-utrustning**
  Projektorutrustningen i lokalerna har fungerat otillfredsställande. Det går exempelvis inte att använda båda VGA-ingångarna vilket vore praktiskt för att snabba på bytet mellan olika föreläsare. Detta bör åtgärdas innan nästa kurstillfälle.
- **Luncher**
  De som ansvarar för den laborations- och demonstrationsutrustning som används under kursen bör delta i de luncher som föreläsarna genomför med kursdeltagarna. Detta ger ytterligare tillfälle för deltagarna att interagera med kursarrangörerna.

3.2.3 Kursmaterial och kurs-PM för ny kursmodul, reglerteknisk utrustning (PLC)

Utvecklingen av de nya fabrikerna har möjliggjort nya, mer avancerade kursmoment. För bytet av hårdvara från de gamla fabrikerna till de nya har vi dels justerat de gamla laborationsuppgifterna något så att de passar de nya fabrikerna, dels påbörjat en vidarutveckling av laborationsuppgifter som bättre utnyttjar potentialen hos de nya fabrikerna[7]. Slutligen har projektet färdigställt en "Verktygslåda för S7-kurser" i form av en CD[8] med verktyg för att demonstrera och laborera med sårbarheter i fabrikernas PLCer. Verktygslådan innehåller följande.

- Två olika DoS-attacker mot S7-1200 (fungerar mot både v2 och v3 firmware).

[7] FOI Memo 4356. *Labb- /kursmoment med PLCer*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.
[8] *Verktygslåda för S7-kurser*. Diarienummer FOI-2013-130. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

- Ett verktyg för att avkoda lösenord till klartext från inspelade S7-400-sessioner.
- Ett verktyg som plockar ut alla 160-bitars challenge och response från S7-1200-sessioner (v2 och v3 firmware).
- Ett verktyg som hämtar ordernummer, firmware-version och serienummer från S7-1200 PLC:er (v2 och v3 firmware) utan att man behöver ange lösen, även om det är satt.
- Ett verktyg som återspelar S7-1200-sessioner för v2 firmware.
- Ett verktyg som återspelar S7-1200-sessioner för v3 firmware genom att kringgå återspelningsskyddet som Siemens har lagt till.

3.2.4 Demonstrationer med egenutvecklade demonstratorer

Under 2012 har ett antal demonstrationer med egenutvecklade demonstratorer genomförts. Nedan beskrivs sex av dessa demonstrationer.

- NCS3 deltog på konferensen *Informationssäkerhet för offentlig sektor* 21-22 augusti där en monter med informationsmaterial och demonstrationsutrustning bemannades.
- Tre demonstrationer genomfördes i Stockholm, Revinge och Umeå för av länsstyrelserna inbjuden publik. Övriga föreläsare var FRA, Romab, Safeside och MSB. NCS3:s del fick genomgående höga betyg och hade heller inga negativa omdömen i kommentarerna på någon ort[9].
- Samma föredrag som vid länsstyrelserna gavs också för trafiksektorn i Stockholm den 8 november. Även där var kunden nöjd och meddelade att många positiva kommentarer hade kommit spontant från de medarbetare som deltagit.
- NCS3 deltog med en demonstration på en konferens för oljesektorn i Bergen, *Datasikkerhet onshore/offshore*, anordnad 7-8 november. Utvärderingen efteråt gav oss betyget 4,3 på innehåll (faglig) och 4,0 på framförandet. Detta på en 5-gradig skala. På denna konferens invigde vi den nya fabriksdemonstratorn.
- En liknande presentation inledde även på IBC euroforums konferens *SCADA-säkerhet 2012*, 20-21 november i Stockholm. Denna konferens är en av de få återkommande konferenserna i Sverige som specifikt adresserar området och vi har varit ett återkommande inslag på alla de konferenser som varit hittills. I år fick vi betyget 4,48 på innehållet och 4,34 på framförandet (6-gradig skala).

[9] FOI Memo 4330. *Demonstrationer och föreläsningar under 2012 – Utvärderingar*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

- Ett av ytterst få internationella seminarier som behandlar området SCADA-säkerhet på en djupare teknisk nivå är den årliga SCADA Security Scientific Symposium (S4). Den 15-19 januari 2013 deltog NCS3 i konferensen dels för att identifiera vad som sker inom området samt dels för att demonstrera resultat från NCS3[10]. Demonstratorn baserad på de nya fabrikerna rönte stor uppskattning och omnämndes bland annat som den hittills bästa demonstratorn som setts.

3.2.5 Alumniträff för SIK

Den 22:a november hölls en alumniträff för de som gått någon av de tidigare hållna SIK-kurserna. Under dagen presenterades nya resultat avseende säkerhet i industriella informations- och styrsystem, hotbild och genomförande av experiment. Dessutom diskuterades vilken utveckling som kan förväntas i framtiden. I arrangemanget deltog ungefär 25 av de tidigare kursdeltagarna.

3.2.6 Workshop med teknisk personal från Samverkansgruppen för informationssäkerhet (SAMFI)

Inom ramen för de seminarier om skadlig kod som genomfördes tillsammans med Dr. Bencsáth Boldizsár under hösten 2012[11] ingick ett seminarium med teknisk personal från Samverkansgruppen för informationssäkerhet (SAMFI).

3.3 Utveckling av demonstratorer

Detta delprojekt syftar till att uppnå följande effekt.

- En ny portabel teknisk demonstrator, och två uppdaterade demonstratorer, gör det möjligt att nå ytterligare målgrupper för att öka medvetandet om behovet av ökad it-säkerhet i industriella styrsystem.
- Tydligt dokumenterade demonstratorer gör det lättare att skräddarsy demonstrationer med avseende på målgrupp och önskat budskap.

Följande delavsnitt motsvarar de leverabler som specificerats för delprojektet.

[10] FOI Memo 4369. *2013 Digital Bond's SCADA Security Scientific Symposium (S4)*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2013.
[11] FOI Memo 4318. *Seminarier om skadlig kod*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

3.3.1 Utvecklingsplan för demonstratorer

Under 2012 togs en utvecklingsplan för demonstratorer vid NCS3[12] fram och redovisades för MSB.

3.3.2 Nyutvecklad demonstrator

Eftersom det under 2012 konstaterades att fördjupad behovs- och genomförandeanalyser är nödvändiga innan utvecklingen av nya demonstratorer kan inledas sköts denna aktivitet på framtiden. Resurserna lades istället på att utveckla de befintliga demonstratorer som har visat sig fungera väl under hittills genomförda demonstrationer.

3.3.3 Uppdaterade demonstratorer

Våra demonstratorer har genomgående fått olika ansiktslyft under året. Störst förändring har dock skett med fabrikerna som har gjorts om helt och hållet och nu förutom att använda ”riktiga” PLC:er också är betydligt mer mobila än tidigare[13].

3.4 Labbutveckling

Detta delprojekt syftar till att uppnå följande effekt.

- En väl fungerande och dokumenterad labbinfrastruktur, vilken är en bas i det praktiska arbetet med att öka säkerheten i industriella informations- och styrsystem i samhällsviktig verksamhet och kritisk infrastruktur.

Följande delavsnitt motsvarar de leverabler som specificerats för delprojektet.

3.4.1 Uppdaterad och dokumenterad labbinfrastruktur

En viktig del av NCS3 är att tillhandahålla en övningsanläggning för utbildning och forskning. Övningsanläggningen utgör del av det IT-labb på FOI som sedan 2012 kallas för CRATE, Cyber Range And Training Environment. Då den tekniska utrustningen i övningsanläggningen består av donationer med ca 10 år gammal hårdvara, var det en nödvändighet att förnya denna för att säkra anläggningens framtida förmåga.

[12] *Utvecklingsplan demonstratorer - en analys av behovet och kortare beskrivning av nuläge*. Diarienummer FOI-2010-1802-8. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.
[13] FOI Memo 4357. *Fabriksdemonstratorn v.2.0*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

Nedan beskrivs den uppdaterade infrastrukturen kortfattat. En mer omfattande beskrivning återfinns i FOI Memo 4333[14].

Mellan 2010 och 2011 köptes 160 nya noder in till datorklustret. Dessa har under 2012 kompletterats med ytterligare 120 nya noder med tillhörande infrastruktur i form av bl.a. switchar.

Under våren 2012 började en helt ny övningsmiljö att byggas i klustret. Arbetet med denna nya miljö (CRATE) genomfördes i följande huvudsteg.

1. Införande av nytt skriptsystem
2. Uppbyggnad av ny routerinfrastruktur
3. Design av virtuella målmaskiner
4. Design av målnät
5. Konstruktion av användarskript, så kallade *bottar*
6. Konstruktion av övervakningssystem för målnäten

3.5 Kunskapsutbyggnad inom industriella styrsystem

Detta delprojekt syftar till att uppnå följande effekt.

- NCS3 fortsätter vara en trovärdig och kompetent samarbetspartner i det nationella arbetet med att öka it-säkerheten i industriella informations- och styrsystem.
- Medarbetarna inom NCS3 ökar den tillämpade kompetensen inom industriella informations- och styrsystem, samt ökar förståelsen för säkerhetsrelaterade frågor kopplade till industriella informations- och styrsystem.

Följande delavsnitt motsvarar de leverabler som specificerats för delprojektet.

3.5.1 Metodbeskrivning, fördjupat studiebesök

Ett utkast till en metodbeskrivning över teknisk kartläggning av industriella informations- och styrsystem har tagits fram. Den utgick från att vi skulle genomföra en djupstudie av någon anläggning under en veckas tid samtidigt som denna dokumenterades med hjälp av ett verktyg för att metodisk modellera

[14] FOI Memo 4333. *Uppdaterad (programvara och maskinvara) och dokumenterad labbinfrastruktur*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

säkerhetsegenskaper, CySeMoL[15]. Ett försök att använda metoden gjordes också vid Tekniska Verken i Linköping. Det visade sig dock att syftet med att skapa en högre förståelse för hur dessa anläggningar är uppbyggda uppfylls betydligt effektivare av kortare studiebesök. Det är därför inte meningsfullt att gå vidare med metoden som den är utformad idag.

3.5.2 Rapportering från studiebesök

Den 5:e och 6:e november 2012 gjordes två studiebesök hos Tekniska verkens avdelning för el-distribution. Studiebesöken beskrivs i FOI Memo 4331[16] och innehöll följande aktiviteter.

- En översiktlig genomgång av SCADA-systemet för el-distributionen hos Tekniska verken samt diskussioner om elnät och IT-system.
- Besök och studie av kontroll- och övervakningsrum.
- Studie av serverrum.
- En diskussion med IT-tekniker från IT-driften, som har hand om kontorsnät, nätverk och brandväggar.
- Besök på två 130 000- och 10 000-volts kopplingsstationer i Linköping.

3.6 Tekniska studier

Detta delprojekt syftar till att uppnå följande effekt.

- Resultat från de tekniska studierna utgör en del i arbetet med att öka it-säkerheten i industriella informations- och styrsystem. I förlängningen skapas en bättre förståelse för risker, sårbarheter och skydd.
- Den tekniska kompetensen kring it-säkerhet i industriella informations- och styrsystem vid NCS3 ökar.
- NCS3 skapar en förmåga att hantera plötsligt uppkomna behov inom området.

Följande delavsnitt motsvarar de leverabler som specificerats för delprojektet.

3.6.1 Rapport från förra årets studie av alternativa skydd

Under 2011 studerades vitlistning av applikationer (även känt som ”application control”) och deras möjliga nytta i styrsystemsmiljöer. Resultatet beskrivs i en

[15] http://www.vikingproject.eu/new2/attachments/210_A1_CySeMoL.pdf
[16] FOI Memo 4331. *Tekniska Verken – kartläggning av SCADA-system*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

rapport[17]. Slutsatsen är att vitlistning bör betraktas som ett användbart komplement till andra säkerhetslösningar, men inte en ersättare för uppdatering av sårbar mjukvara. Dessutom konstateras att den utbredda idé som finns angående vitlistnings förmågor att blockera skadlig kod och otillåtet användande stämmer dåligt överens med hur skyddet fungerar i praktiken.

3.6.2 Planering av årets studier

Under våren 2012 gjordes en grov planering av studierna för 2012[18]. Planen var att:

1. Skapa en engelsk ”kappa” till de tekniska studierna som på ett övergripande sätt beskrev tekniska skydd som upplevs som lovande i styrsystemsammanhang. Denna skall sedan uppdateras vid behov.
2. Undersöka ”insidan” av en eller flera Programmable Logic Controlers (PLC) för att identifiera typiska lösningar på hur kod skapas, laddas in och exekveras i dessa.
3. Studera kända sårbarheter i styrsystemkomponenter för att identifiera generella designsårbarheter och ytterliga förbättra centrets kunskap om tekniska lösningar i styrsystemens insida.

3.6.3 Genomförda tekniska studier

De tre studierna genomfördes enligt plan. Den första aktiviteten resulterade i en ”kappa” för tekniska studier[19].

Studie två och tre syftade främst till att förbereda inför eventuellt framtida arbete med incidentanalys och analys av skadlig kod. För att ge ett konkret fall att hänga upp arbetet på fokuserades det på Siemens lösningar och den skadliga PLC-koden i Stuxnet. Målet var att i slutet uppnå den nivå som skulle behövas för att analysera PLC-delarna av Stuxnet och få en allmän förståelse för vilka svårigheter som kan uppstå ifall liknande fall dyker upp i framtiden. Resultatet beskrivs i en FOI-rapport[20] och i ett FOI-memo[21]. Som dessa två publikationer

[17] FOI-rapport FOI-R--3434--SE. *Application whitelisting, Raises the bar against certain threats but no silver bullet.* Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.
[18] *Plan för årets tekniska studier*. Diarienummer FOI-2010-1802:7. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.
[19] FOI Memo 4315. *Working report on advanced technical security measures for industrial control systems*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.
[20] FOI-rapport: FOI-R--3567--SE. *Möjligheter och problem vid analys av fientlig kod riktad mot Siemens S7-serie*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.
[21] FOI Memo 4218. *Detektion av angrepp och förebyggande åtgärder för Siemens S7-serie*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

indikerar gav studierna en god insikt i hur Siemens PLC-lösningar kan se ut på insidan.

3.7 Forskningsfrämjande åtgärder

Detta delprojekt syftar till att uppnå följande effekt.

- Investeringen i NCS3 merutnyttjas för att stödja experimentell forskning kopplad till it-säkerhet i industriella informations- och styrsystem.
- NCS3 ökar sin tekniska kompetens
- NCS3 blir väletablerat bland forskningsaktörerna inom området.
- En ökad mängd experimentell forskning inom området och en ökad samverkan mellan olika forskningsgrupper.

Följande delavsnitt motsvarar de leverabler som specificerats för delprojektet.

3.7.1 Praktisk samverkan med forskargrupper

Eftersom NCS3 finansieras med beredskapsmedel inkluderar verksamheten inte någon akademisk forskning. Däremot ska NCS3 ge praktiskt stöd till akademiska institutioner som nyttjar dess resurser för träning, övning och experiment inom sin forskningsverksamhet. Möjligheten att kombinera NCS3:s verksamhet med akademisk forskning ger utmärkta tillfällen för forskare att samla data vars insamlande annars skulle kräva alltför omfattande resurser.

Som beskrivs i FOI Memo 4317[22], har arbetet med att skapa goda förutsättningar för forskning avseende informationssäkerhet i industriella informations- och styrsystem under 2012 i huvudsak inriktats på att:

- utveckla forskningsinfrastrukturen vid NCS3
- marknadsföra infrastrukturen
- aktivt samarbeta med forskningsaktörer.

Exempel på aktiviteter som har genomförts för att främja forskningen inom området är:

- utveckling av den tekniska infrastrukturen vid NCS3 så att förutsättningarna för att samla forskningsdata från träning, övning och experiment förbättras

[22] FOI Memo 4317. *Forskningsfrämjande åtgärder vid Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet*. Totalförsvarets forskningsinstitut, Linköping, Sverige, 2012.

- marknadsföring av infrastrukturen vid NCS3 som forskningsplattform, bland annat vid The 17th Nordic Conference on Secure IT Systems (NordSec) i Karlskrona
- samverkan med ICS vid KTH, bland annat genom utveckling av mer verklighetstrogen simulering av användare i datornät som byggs upp med hjälp av infrastrukturen vid NCS3
- deltagande i referensgruppen för projektet Informationssäkerhet i SCADA-system som finansierar doktoranderna Hannes Holm och Markus Buschle vid ICS
- deltagande i handledargrupp för doktorand Matus Korman vid ICS
- handledning av examensarbetare från Linköpings universitet
- stöd till forskning om HCI vid KTH.

3.7.2 Rapport utförd samverkan

Under 2012 genomförd samverkan har rapporterats i form av FOI Memo 4317[22].