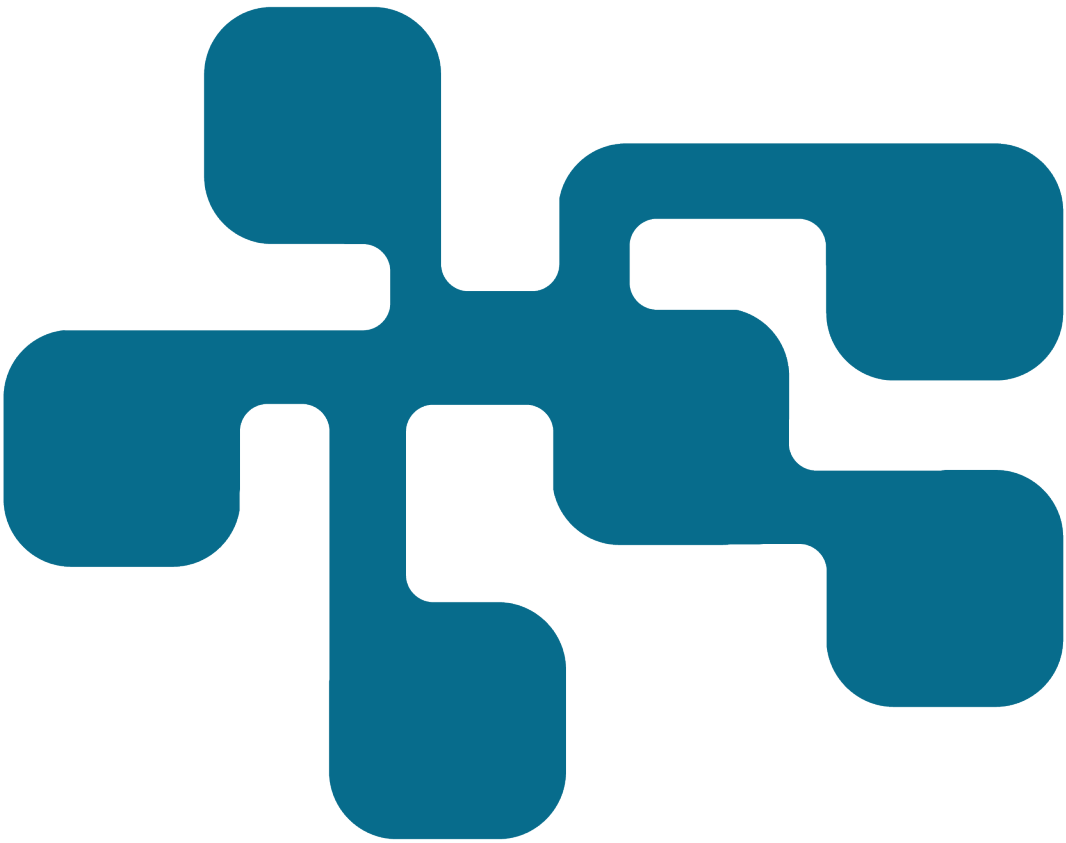
NCS3 2019
Verksamhetsrapport

Lars Westerdahl

FOI
MSB



FOI-R--5176--SE
MSB 2019-00646
ISSN 1650-1942

Januari 2022

Lars Westerdahl

NCS3 2019
Verksamhetsrapport

Titel	NCS3 2019 Verksamhetsrapport
Title	NCS3 2019 Activity Report
Rapportnr/Report no	FOI-R--5176--SE
Månad/Month	Januari
Utgivningsår/Year	2022
Antal sidor/Pages	20
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	E72289
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen. The content has been reviewed and does not contain information which is subject to Swedish export control.

Sammanfattning

Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett samarbete mellan Myndigheten för samhällsskydd och beredskap (MSB) och Totalförsvarets forskningsinstitut (FOI) i syfte att stärka säkerheten i de system som utgör kritisk infrastruktur. Det arbete som utförs inom NCS3 regleras via uppdrag från MSB. I denna rapport sammanfattas de uppdrag som överenskommits under 2019.

Under 2019 års överenskommelser har 10 uppdrag utförts under perioden 2019–2020. Dessa uppdrag har utförts av avdelningarna Försvarsanalys respektive Ledningssystem på FOI. Uppdragen omfattade bland annat fyra studier och fyra kurstillfällen, varav två ingick i införandet av en ny kunskapshöjande kurs.

Nyckelord: NCS3, industriella informations- och styrsystem, industriella kontrollsystem, kritisk infrastruktur.

Summary

The National Center for Security in Control Systems for Critical Infrastructure (NCS3) is a collaboration between the Swedish Civil Contingencies Agency (MSB) and the Swedish Defense Research Agency (FOI) to strengthen the security of the systems that constitute critical infrastructure. The work carried out within NCS3 is regulated through assignments from MSB. This report summarizes the assignments agreed upon during 2019.

Under the 2019 agreements, 10 assignments were performed during the period 2019–2020. These assignments have been performed by the Departments of Defense Analysis and Management Systems at FOI. The assignments included, among other things, four studies and four courses, two of which were part of the introduction of a new knowledge-enhancing course.

Keywords: NCS3, Industrial Control System, Critical Infrastructure.

Innehållsförteckning

1 Inledning

Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kunskapscentrum vars verksamhet genomförs i samarbete mellan *Myndigheten för samhällsskydd och beredskap* (MSB) och *Totalförsvarets forskningsinstitut* (FOI). I denna rapport sammanfattas det arbete som utförts inom de överenskommelser som ingåtts under år 2018. Arbetet har utförts av avdelningarna Försvarsanalys respektive Ledningssystem på FOI under perioden 2018–2020.

1.1 Om NCS3

NCS3 är ett kunskapscentrum som startades 2007 med fokus på IT-säkerhet relaterad till industriella informations- och styrsystem inom samhällsviktig verksamhet. Mycket av centrumets verksamhet kretsar kring en teknisk laborativ miljö och dess kringverksamhet som finns vid FOI i Linköping, men en del av arbetet utförs även vid FOI i Stockholm.

NCS3 och dess verksamhet syftar till att minska de risker som nyttjandet av digitala system för styrning av samhällsviktig infrastruktur medför, speciellt med avseende på avsiktlig störning. Vidare syftar kunskapscentrumet till att bibehålla en hög statlig kompetens inom området. Uppdragen har bestått av såväl stöd till MSB:s enhet för cyberfysiska system som till tekniskt inriktad verksamhet avseende IT-säkerhet. Namnet NCS3 etablerades år 2010.

Det långsiktiga målet med NCS3:s verksamhet är att öka säkerheten i industriella informations- och styrsystem och därigenom öka förmågan att förebygga och hantera störningar i samhällsviktig verksamhet och kritisk infrastruktur i Sverige. För att uppnå detta mål krävs ett långsiktigt säkerhetsarbete som inkluderar:

- medvetenhet om sårbarheter, risker och möjliga åtgärder
- kompetens avseende säkerhet i industriella informations- och styrsystem
- förmåga att analysera aktuella risker och brister
- förmåga att kravställa säkerhet i industriella informations- och styrsystem.

NCS3:s vision och strategi återfinns i sin helhet i dokumentet Vision och strategi för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet 2012 till 2017.[1]

De viktigaste målgrupperna för NCS3:s verksamhet är

- aktörer som äger och driver samhällsviktig verksamhet och kritisk infrastruktur som är beroende av industriella informations- och styrsystem
- sektors- och tillsynsmyndigheter (bland annat inom Samverkansområde teknisk infrastruktur, SOTI)
- myndigheterna i Samverkansgruppen för informationssäkerhet (SAMFI).

All verksamhet inom centrumet bygger på en nära samverkan mellan FOI och MSB. Samarbetet regleras genom överenskommelser vilka ingås under varje budgetår.

1.2 Verksamhetsrapportens uppbyggnad

I kapitel 2 presenteras de utåtriktade aktiviteterna som genomförts. Exempel på utåtriktade aktiviteter är sådana aktiviteter där föredrag och kurser ges. I kapitel 3 sammanfattas de studier som genomfört under året. Arbetet med införandet av en ny kurs presenteras i kapitel 4. En sammanställning av samtliga leveranser från FOI till MSB presenteras i kapitel 5.

[1] Wedlin, M. & Hallberg, J. (2012). Vision och strategi för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet 2012 till 2017 (FOI Memo 4166).

2 Medvetande-, kunskaps- och förmågehöjande verksamhet

Arbetet inom NCS3 består dels av utåtriktade aktiviteter såsom kurser och föreläsningar, samt mer internt arbete såsom att genomföra studier. Den utåtriktade verksamheten delas in i medvetande-, kunskaps- och förmågehöjande verksamhet.

2.1 Medvetandehöjande verksamhet

I början av året blev MSB och FOI gemensamt intervjuade för tidningen Energi. Fokus för intervjun var hur energibolag kan träna på att skydda sina system mot angrepp och den övningsverksamhet som genomförs inom NCS3-samarbetet.[2]

Myndigheten Trafikanalys anordnade under hösten en kortare workshop i syfte att informera sig om cybersäkerhetsfrågor inom deras ansvarsområde. Vid detta tillfälle presenterades de två rapporter som tagits fram i studier om tung trafik och om informationssystem för hantering av farligt gods.

2.2 Kunskaps- och förmågehöjande verksamhet

Under året har två ordinarie kurser genomförts vid fyra tillfällen. Vid två av dessa tillfällen gavs *Grundläggande kurs: Säkerhet i industriella informations- och styrsystem*, och två andra tillfällen den nya kursen *Påbyggnadskurs: Säkerhet i industriella informations- och styrsystem*.

Den grundläggande kursen har genomförts sedan år 2009 och har som helhet haft drygt 500 deltagare över åren. Målsättningen är att ha 16 deltagare per kurstillfälle vilket det oftast är (Tabell 1).

Tabell 1 Deltagare på grundläggande kurs SI3S under 2019

Datum	Deltagare	Män/kvinnor
30–31 oktober	16	15/1
5–6 november	15	14/1

[2] Isaksson, P. (2019). Träning mot it-attacker. *Tidningen Energi*, (2), ss.39–42.

Påbyggnadskursen gavs för första gången under hösten. Även denna kurs har som mål att ha 16 deltagare per tillfälle (Tabell 2). Tidigare under våren gavs även kursen som en pilotserie men då som en del i utvecklingsarbetet av kursen, se kapitel 4 för mer detaljer om kursutvecklingen. Tillsammans med pilotutbildningarna har cirka 60 personer hittills genomfört påbyggnadskursen.

Tabell 2 Deltagare på påbyggnadskurs SI3S under 2019

Datum	Deltagare	Män/kvinnor
12–14 november	17	16/1
19–21 november	14	13/1

Deltagarna under både den grundläggande och påbyggnadskursen utgjordes av en blandad grupp med ursprung ifrån statliga och kommunala verksamheter samt till viss del även privata aktörer.

3 Studier

Inom NCS3 genomförs studier i syfte att bättre förstå den miljö där industriella informations- och styrsystem används men även för att studera hur en teknik eller process kan tillämpas inom området. På en övergripande nivå delas studierna in i sektor- respektive tekniska studier men inom tekniska studier kan även administrativa åtgärder inkluderas. Under år 2019 genomfördes fyra studier, samtliga med en teknisk eller administrativ inriktning.

3.1 Verklighetsbaserade tidiga tecken på IT-angrepp mot ICS

Inom projektet studerades ett antal stora cyberangrepp mot ICS-system för att se om det gick att hitta gemensamma tecken på intrång i ett tidigt skede av angreppet. De utvalda angreppen var alla allmänt kända och det fanns öppet tillgänglig information om angreppen att tillgå. Tidsspannet för angreppen var dock stort, från år 2009 till år 2019, vilket å andra sidan möjliggjorde upptäckt av bestående parametrar för tidigt upptäckt.

De parametrar som identifierades för tidig upptäckt av intrång delades in i tre grupper: avvikande kommunikationsmönster, avvikande systembeteende samt avvikande mejl. I sex av sju fall förekom det avvikelser i det normala kommunikationsmönstret mellan ICS-enheterna, något som i dylika miljöer bedöms extra lätt att detektera på grund av den (relativt) statiska normala kommunikationen mellan enheterna. I fem av sju fall började även ICS-enheterna och hela systemet att bete sig annorlunda än normalt, till exempel i form av en förändrad ljudbild i processen. Även dylika beteenden torde vara lätta att upptäcka för erfarna operatörer, de måste dock även vara införstådda med (och uppmuntrade till) att rapportera dylika avvikelser. Det är även vanligt att det i samband med det första intrångsförsöket inkommer avvikande mail till (nyckel)personer i organisationen. Här gäller också uppmärksamhet hos personalen i kombination med utbildning för att möjliggöra så tidig upptäckt som möjligt av eventuella intrång. Dock är variationen på legitima mejl stor och det är därför svårare att avgöra vad som faktiskt är ett riktat nätfiskeförsök och vad som inte är det.

Projektrapporten[3] avslutas med en lista med råd till systemägare för att försvåra framgångsrika intrång och underlätta upptäckt av (försök till) dylika. Ett kondensat av råden är att ha god IT-säkerhet, samt ha utbildad och uppmärksam personal.

3.2 Elektromagnetiska hot mot trådlös kommunikationsutrustning kopplat till samhällsviktiga tjänster

Trådlös kommunikation har länge varit ett sätt att kostnadseffektivt kunna kommunicera över stora avstånd. I modernare system är även trådlös kommunikation en viktig del i hur organisationer kommunicerar lokalt. Tekniken för trådlös kommunikation är dock sårbar, exempelvis genom att den är radiobaserad och kan därmed exempelvis störas även utan att angriparen nödvändigtvis förstår vad som sägs på nätverket.

Studien Elektromagnetiska hot mot trådlös kommunikationsutrustning kopplat till samhällsviktiga tjänster genomfördes med målet att öka kunskapen om sårbarheter kring trådlös kommunikation, samt ge rekommendationer över åtgärder för att minska dessa sårbarheter. Resultat från studien baseras på en litteraturstudie, en workshop, samt intervjuer.

Litteraturstudien syftade till att identifiera rapporterade störningsincidenter samt att studera vilka rekommendationer som angivits för att motverka dessa. Den fortsatta inventeringen kompletterades med kunskap inhämtad från en workshop som genomfördes i oktober samt från enskilda intervjuer med utvalda personer baserat på forskarnas bedömning. Inventeringen kompletterades också med kunskap baserade på verkliga fall.

Resultat från de olika inhämtningsdelarna sammanställdes i en rapport[4]. I rapporten presenteras en hotbild mot samhällsviktig verksamhet avseende trådlös kommunikation samt exempel på avsiktliga och oavsiktliga störningar i Sverige. Vidare tas även mer hypotetiska exempel upp baserade på erfarenheter från svenska myndigheter. Avslutningsvis ges ett antal rekommendationer i syfte att stödja aktörer i deras arbete att skydda sina system.

[3] Valassi, C. & Karresand, M. (2020). *IT-angrepp mot industriella informations- och styrsystem* (FOI-R--4929--SE).

[4] Odell, A., Zouave, E. & Jaitner, M. (2020). *NCS3 - Elektromagnetiska hot mot trådlösa system* (FOI -R--4838--SE).

3.3 Kommande cybersäkerhet inom uppkopplade fordon i Sverige

Automatisering i trafiken är en trend som har fått fart under de senare åren och troligtvis kommer att ha en stor inverkan på vårt samhälle. Trenden bär med sig förändringar, anpassningar och nya utmaningar för vägtrafiken. Den framskridande automatiseringen av fordon innebär både en allt svårare överskådlig komplexitet, men även att teknologin ytterst kommer att direkt påverka människans liv och hälsa. Detta sätter i sin tur frågan om cybersäkerheten, och dess reglering i nytt fokus. Denna studie har kartlagt ett flertal lagrum och bestämmelser som är relevanta för cybersäkerheten i uppkopplade, automatiserade fordon. Lagrummen identifierades utifrån tidigare utredningar om lagstiftning och reglering. Följande lagrum låg i fokus för studien: civilrätten för smart robotteknik, dataskyddsbestämmelser, nätverks- och informationssäkerhet i samhällsviktig verksamhet (NIS), säkerhetsskyddsbestämmelser, förslag om IKT-standardiseringsbestämmelser, bestämmelser om intelligenta transportsystem (ITS och C-ITS), produktansvars- och produkt- prövningsbestämmelser, fordonskontrollsbestämmelser samt försäkringsbestämmelser. Cybersäkerhetsregleringen för transportsektorn i sin helhet utgörs av en fragmenterad och komplex lagstiftning. Olika lagrum fyller olika syften, med krav som ofta riktas till olika typer av aktörer och verksamhet. Medan det inte finns harmoniserade cybersäkerhetskrav mellan olika lagrum finns det ett antal åtgärder som är återkommande. Dessa innefattar att anmäla verksamhet till behöriga myndigheter, bedöma risker och vidta säkerhetsåtgärder, samt rapportera säkerhetsincidenter.

Inom ramen för studien genomfördes även en workshop i september 2019 med deltagare från myndigheter och civila aktörer. Resultat från studien finnas sammanfattade i en rapport[5], vilken även har redovisats för i ett slutseminarium i januari 2020.

3.4 Kartläggning av resursförmåga vid kris och ofred

Tillgången till resurser inom industriella informations- och styrsystem (fortsättningsvis förkortat ICS baserat på den engelska benämningen *Industrial*

[5] Zouave, E., Wennberg, S. & Jaitner, M. (2019). Lag och cybersäkerhet i smart vägtrafik (FOI-R--4811--SE).

Control Systems) upplevs god vid normalförhållanden och mindre störningar, men inför allvarliga samhällsstörningar är planeringen inte lika god.

I studien *Kartläggning av resursförmåga vid kris och ofred* var målet att kartlägga regelverk samt att fånga utmaningar och problem med prioritering och fördelning av ICS-relaterade resurser vid brist i kris eller krig.

Efter en litteraturstudie genomfördes intervjuer med ICS-leverantörer och myndigheter med ansvar för samhällsviktig verksamhet som är beroende av ICS-relaterade resurser, såväl komponenter och system som personal.

Studien utmynnade därefter i några förslag på lösningar av de identifierade utmaningarna. Bland annat föreslås att någon form av övergripande nationell eller regional prioriteringsmodell tas fram, för att leverantörer ska veta hur de ska prioritera kunder i både kris, när avtal gäller, och i krig, när andra lagar kan gå in och styra. Vidare föreslås att om den motorreparationstjänst som fanns tidigare återinförs bör ICS-resurser ingå som en del av tjänsten. I intervjuerna lyfts också vikten av att hålla lager i kombination med *just-in-time*-principen. Lager kan hållas på flera nivåer, såväl hos ICS-ägarna såväl som hos leverantörerna och andra aktörer i leveranskedjan, men det skulle också kunna finnas komponenter lagrade i nationella beredskapslager. Resultaten från studien finns sammanställda i en rapport[6].

[6] Eckersand, U. & Stenerus, A-S. (2020). *NCS3 – Industriella informations- och styrsystem i kris och krig* (FOI-R--4935--SE).

4 Teknisk utveckling

Den tekniska utvecklingen som genomfördes under år 2019 avsåg att realisera och testa kursen *Påbyggnadskurs: Säkerhet i industriella informations- och styrsystem* (Pk-SI3S). Arbetet med att planera kursen och framtagningen av kursmoduler påbörjades redan under år 2018 men målet under år 2019 var att testa den kompletta kursen inför publik.

Inledningsvis genomfördes ett par informella försök utanför överenskommelsen genom att genomföra en tidig version av kursens övningsdelar och en laboration. Övningsdelen i kursen utgörs av ett brädspel där deltagarna i flera steg tillämpar den kunskap de erhållit under föreläsningar och laborationer. Målet med övningen är att deltagarna stegvis ska förbättra skyddet av ett system. I samband med ett studiebesök på FOI, testades även en av kursen laborationer på enhet från MSB.

Det fösta planerade pilotförsöket genomfördes internt inom FOI i slutet av april. Huvudfokus för pilotförsöket var att testa och få återkoppling på det spel som tagits fram för övningsdelen av kursen, vilket medförde att det tog det mesta av tiden. Deltagarna utgjordes mestadels av projektmedlemmar från NCS3-projekt men även några andra medarbetare vid FOI med vana av brädspel deltog. I samband med detta försök testades även en annan laboration än den tidigare.

En komplett version av kursen testades med externa deltagare under två tillfällen i maj. Kursdeltagarna var inbjudan till en vanlig kurs men med förbehållet att detta är en pilotversion och att det förväntas en mer utförlig utvärdering av kursen än vad som är normalt. Båda pilotkurserna genomfördes med gott resultat och den återkoppling som kom var till god hjälp för fortsatt utveckling av kursen. Det visade sig exempelvis att övningsmomentet gjorde sig mycket bra som ett brädspel. En av tankarna kring övningsmomentet var ursprungligen att initialt utveckla övningsmetoden med en pappersversion (som ett brädspel) för att senare när metoden verifierats, överföra övningen i mer digital form. Motivet med den tänkta utvecklingen var att säkerhetsställa att övningsmetodiken är hållbar innan den byggs in i ett system som inte är så lätt att förändra. De erfarenheter som drog från pilotgenomföranden var dock att brädspelformatet gav en god överblick över de komponenter som ingår (systemplan, tillgängliga systemkomponenter, med mera) och därmed goda diskussionsmöjligheter kring olika förbättringsalternativ. Just dessa diskussioner är huvudsyftet med övningen, varvid stor vikt fästes vid detta inför den fortsatta utvecklingen.

Erfarenheterna från de tre pilotutbildningarna sammanfattades i ett FOI Memo[7], vilket även innehöll en handlingsplan för vad som behövdes förbättras innan kursen var mogen för att genomföras som en ordinarie NCS3-kurs.

[7] Westerdahl, L. (2019). Kursutvärdering och handlingsplan (FOI Memo 6775). Stockholm: Totalförsvarets forskningsinstitut

5 Leveranser

I detta kapitel listas de överenskommelser som upprättades under år 2019 samt de skriftliga leveranser som gjorts under respektive överenskommelse.

5.1 Projektkoordinering och centrumverksamhet vid NCS3s tekniska plattform i Linköping

Överenskommelse: Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2019 NCS3, Delbeställning: Projektkoordinering och centrumverksamhet vid NCS3s tekniska plattform i Linköping

MSB dnr: MSB 2019-00646

Tabell 3: Leverabler som färdigställts inom ramen för denna överenskommelse

Referens	Titel
FOI Memo 6789	Statusrapport NCS3 2019 för perioden januari–maj
FOI Memo 6851	NCS3 statusrapport juni-september 2019
FOI Memo 6987	Statusrapport NCS3 2019 för perioden oktober–december
FOI-R--5176--SE	Verksamhetsrapport 2019

5.2 Deltagande i övergripande arbete för FOI Ledningssystem

Överenskommelse: Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2019 NCS3, Delbeställning: Deltagande i övergripande arbete för FOI Ledningssystem

MSB dnr: MSB 2019-00644

Uppdraget har inga fasta leverabler. Aktiviteter inom denna överenskommelse rapporteras huvudsakligen i de statusrapporter som redovisas under 5.1.

5.3 Deltagande i övergripande arbete för FOI Försvarsanalys

Överenskommelse: Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2019 NCS3, Delbeställning: Deltagande i övergripande arbete för FOI Försvarsanalys

MSB dnr: MSB 2019-00642

Uppdraget har inga fasta leverabler. Aktiviteter inom denna överenskommelse rapporteras huvudsakligen i de statusrapporter som redovisas under 5.1.

5.4 Införande av kunskapshöjande kurs

Överenskommelse: Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2019, Delbeställning: Införande av kunskapshöjande kurs

MSB dnr: MSB 2019-04601

Tabell 4: Leverabler som färdigställts inom ramen för denna överenskommelse

Referens	Titel
FOI Memo 6775	Kursutvärdering och handlingsplan
FOI Memo 6988	Uppdaterat kursunderlag: Påbyggnadskurs SI3S

5.5 Verklighetsbaserade tidiga tecken på IT-angrepp mot ICS

Överenskommelse: Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2019, Delbeställning: Verklighetsbaserade tidiga tecken på IT-angrepp mot ICS

MSB dnr: MSB 2019-04684

Tabell 5: Leverabler som färdigställts inom ramen för denna överenskommelse

Referens	Titel
FOI-R--4929--SE	IT-angrepp mot industriella informations- och styrsystem

FOI Memo 7500	Presentationsunderlag samt informationsblad – Verklighetsbaserade tidiga tecken på IT-angrepp mot ICS

5.6 Genomförande av påbyggnadskurs SI3S november 2019

Överenskommelse: Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2019, Delbeställning: Genomförande av påbyggnadskurs SI3S november 2019

MSB dnr: MSB 2019-07612

Tabell 6: Leverabler som färdigställts inom ramen för denna överenskommelse

Referens	Titel
FOI Memo 6984	Kursutvärdering påbyggnadskurs (Pk-SI3S) november 2019

5.7 Genomförande av grundläggande kurs SI3S oktober–november 2019

Överenskommelse: Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2019, Delbeställning: Genomförande av grundläggande kurs SI3S oktober–november 2019

MSB dnr: MSB 2019-07609

Tabell 7: Leverabler som färdigställts inom ramen för denna överenskommelse

Referens	Titel
FOI Memo 6985	Kursutvärdering Grundläggande kurs SI3S (Gk-SI3S) oktober–november 2019

5.8 Elektromagnetiska hot mot trådlös kommunikationsutrustning kopplat till samhällsviktiga tjänster

Överenskommelse: NCS3 Studie: Elektromagnetiska hot mot trådlös kommunikationsutrustning kopplat till samhällsviktiga tjänster

MSB dnr: MSB 2019-04982

Tabell 8: Leverabler som färdigställts inom ramen för denna överenskommelse

Referens	Titel
FOI-R--4838--SE	NCS3 - Elektromagnetiska hot mot trådlösa system

5.9 Kommande cybersäkerhet inom uppkopplade fordon i Sverige

Överenskommelse: NCS3 Studie: Kommande cybersäkerhet inom uppkopplade fordon i Sverige

MSB dnr: MSB 2019-04983

Tabell 9: Leverabler som färdigställts inom ramen för denna överenskommelse

Referens	Titel
FOI-R--4811--SE	Lag och cybersäkerhet i smart vägtrafik

5.10 Kartläggning av resursförmåga vid kris och ofred

Överenskommelse: NCS3 Studie: Kartläggning av resursförmåga vid kris och ofred

MSB dnr: MSB 2019-05348

Tabell 10: Leverabler som färdigställts inom ramen för denna överenskommelse

Referens	Titel
FOI-R--4935--SE	NCS3 – Industriella informations- och styrsystem i kris och krig

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se