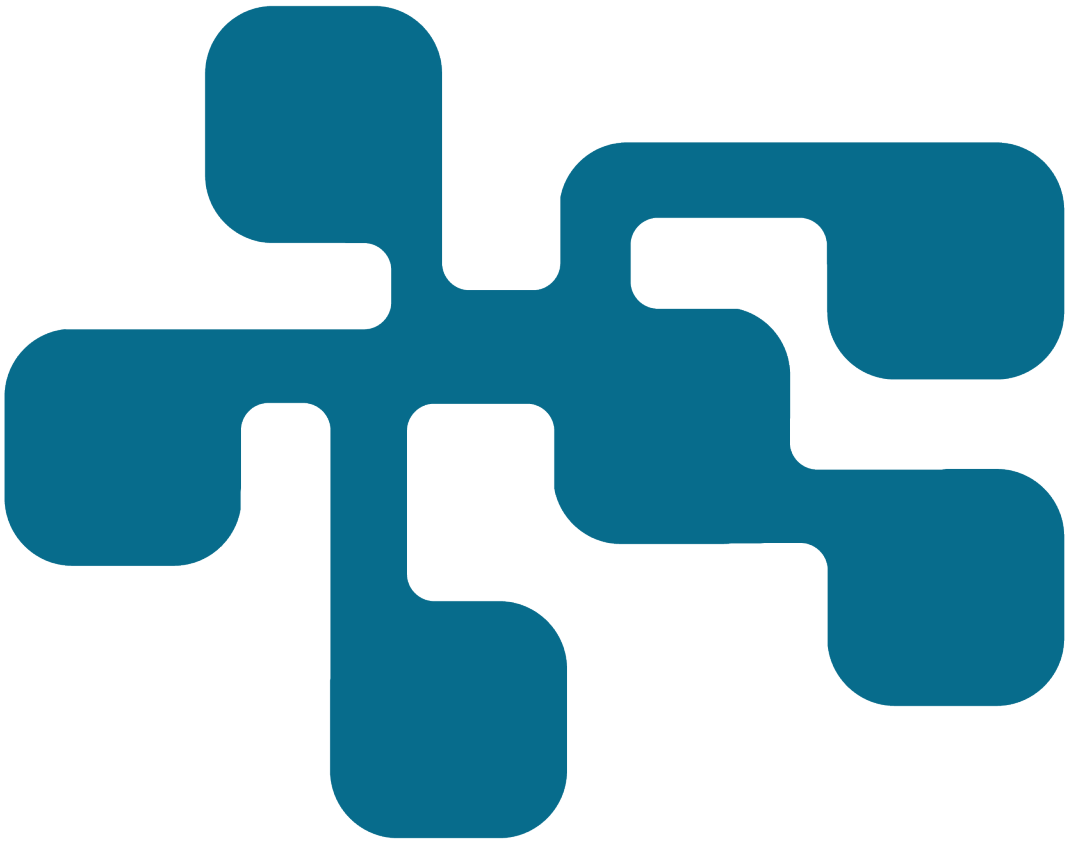


NCS3 2020

Verksamhetsrapport

Lars Westerdahl och Tommy Gustafsson

FOI
MSB



Lars Westerdahl och Tommy Gustafsson

NCS3 2020

Verksamhetsrapport

Titel	NCS3 2020 Verksamhetsrapport
Title	NCS3 2020 Activity Report
Rapportnr/Report no	FOI-R--5290--SE
Månad/Month	Februari
Utgivningsår/Year	2022
Antal sidor/Pages	21
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	E7160781
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.

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

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 bedrivits inom ramen för NCS3 under verksamhetsår 2020.

För verksamhetsåret finns åtta överenskommelser som beskriver de uppdrag som har beställts. Dessa är *Sedelärande berättelser*¹, *Cyberfysiska sårbarheter i tunga fordon*², *Kursutveckling och –genomförande*³, *Internetanslutna styrsystem, del 3*⁴, *Elektromagnetiska hot mot trådlösa system*⁵, *Industriella informations- och styrsystem i kris och krig*⁶, *Regelverk och krav inom området industriella informations- och styrsystem*⁷ samt *Förstudie Medicintekniska produkter*⁸. Dessa uppdrag har utförts av avdelningarna Försvarsanalys samt Ledningssystem på FOI. Uppdragen omfattade bland annat sju studier och tre kurstillfällen, varav två ingick i införandet av en ny kunskapshöjande kurs.

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

¹ FOI-2020-205:3 resp. MSB 2020-04058

² FOI-2020-205:4 resp. MSB 2020-04055

³ FOI-2020-205:6 resp. MSB 2020-04057

⁴ FOI-2020-205:9 resp. MSB 2020-06443

⁵ FOI-2019-606:1 resp. MSB 2019-04982

⁶ FOI-2019-773:1 resp. MSB 2019-05348

⁷ FOI-2020-205:1 resp. MSB 2020-04491

⁸ FOI-2020-829:1 resp. MSB 2020-08183

Summary

The National Center for Security in Control Systems for Critical Infrastructure (NCS3) is a collaboration between the Swedish 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 2020.

The assignments have been performed by the Department of Defense Analysis and the Department of C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) at FOI. The topics of the studies performed during 2020 included *Vulnerabilities in cyberphysical systems in heavy vehicles*, *Internet attached ICS systems in Sweden*, *Electromagnetical threats to wireless systems*, *Legislation and regulations*, and *ICS in medtech*. Three training sessions were also arranged by NCS3 during the year.

Keywords: NCS3, Industrial Control System, Critical Infrastructure.

Innehållsförteckning

1	Inledning	7
1.1	Om NCS3	7
1.2	Verksamhetsrapportens uppbyggnad	8
2	Medvetande-, kunskaps- och förmågehöjande verksamhet	9
2.1	Medvetandehöjande verksamhet	9
2.2	Kunskaps- och förmågehöjande verksamhet.....	9
3	Studier	11
3.1	Cyberfysiska sårbarheter i tunga fordon	11
3.2	Sedelärande berättelser	12
3.3	Internetanslutna system, del 3	12
3.4	Elektromagnetiska hot mot trådlösa system	13
3.5	Industriella informations- och styrsystem i kris och krig.....	13
3.6	Regelverk och krav inom området industriella informations- och styrsystem.....	14
3.7	Förstudie Medicintekniska produkter	15
4	Kursutveckling	16
5	Leveranser	18
5.1	Projektkoordinering och centrumverksamhet.....	18
5.2	Genomförande av påbyggnadskurs SI3S september 2020.....	18
5.3	Kursutveckling	18
5.4	Cyberfysiska sårbarheter i tunga fordon	19
5.5	Sedelärande berättelser	19
5.6	Internetanslutna system, del 3	20
5.7	Elektromagnetiska hot mot trådlösa system	20
5.8	Industriella informations- och styrsystem i kris och krig.....	20
5.9	Regelverk och krav inom området industriella informations- och styrsystem.....	21
5.10	Förstudie - medicintekniska produkter	21

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 2020. Arbetet har utförts av avdelningarna Försvarsanalys respektive Ledningssystem på FOI under perioden 2020–2021.

1.1 Om NCS3

NCS3 är ett kunskapscentrum som startades år 2007 med fokus på IT-säkerhet relaterad till industriella informations- och styrsystem inom samhällsviktig verksamhet. Mycket av centrumets verksamhet är 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 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*.⁹

⁹ Wedlin, M. & Hallberg, J. (2012). Vision och strategi för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet 2012 till 2017 (FOI Memo 4166).

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 kursutveckling och införandet av en ny kurs presenteras i kapitel 4. En sammanställning av samtliga leveranser från FOI till MSB presenteras i kapitel 5.

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 medverkade en forskare i ett reportage i Östgöta Correspondenten som bland annat beskrev verksamheten vid NCS3. Övrig medvetandehöjande verksamhet utgick till följd av restriktioner under pandemin.

2.2 Kunskaps- och förmågehöjande verksamhet

I inledningen av 2020 genomförde FOI en specialframtagen kurs för MSB:s traineer som dels beskrev FOI och samarbetet med MSB och dels gav en introduktion till säkerhet i industriella styrsystem.

Under året har också *Påbyggnadskurs: Säkerhet i industriella informations- och styrsystem* (Pk-SI3S) genomförts vid två tillfällen.

Påbyggnadskursen gavs för första gången under hösten 2019. Normalt genomförs kursen med 16 deltagare men till följd av de restriktioner som gällde under pandemin begränsades antalet deltagare och genomfördes i enlighet med detaljerna i Tabell 1. Tillsammans med pilotutbildningarna har cirka 85 personer hittills genomfört påbyggnadskursen.

Tabell 1 Deltagare på påbyggnadskurs SI3S under 2020

Datum	Deltagare	Män/kvinnor
8-10 september	12	11/1
15-17 september	13	11/2

Deltagarna utgjordes av en blandad grupp med ursprung ifrån statliga och kommunala verksamheter samt till viss del även privata aktörer. Utvärdering av kurstillfällena avrapporteras i ett FOI Memo¹⁰.

Enligt överenskommelsen planerades också två genomföranden av *Grundkurs: Säkerhet i industriella informations- och styrsystem* (Gk-SI3S) men dessa fick ställas in till följd av coronarestriktioner. Istället omfördelades dessa medel till utvecklingen av incidenthanteringskursen i enlighet med kapitel 4.

¹⁰ Westerdahl, L. (2020). *Kursutvärdering Påbyggnadskurs: Säkerhet i industriella informations- och styrsystem, september 2020*. (FOI Memo 7314)

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 2020 genomfördes sju studier, samtliga med en teknisk eller administrativ inriktning.

3.1 Cyberfysiska sårbarheter i tunga fordon

Inom projektet genomfördes en studie med fokus på cyberfysiska sårbarheter i tunga fordon. Syftet med studien var att utveckla och bygga vidare på den analys som gjordes år 2017 och ge en indikation på sårbarheten hos tunga fordon av betydelse för civilförsvaret. Målet med studien var att utvärdera vilka risker som finns med tredjepartssystem samt vilka konsekvenser dessa risker kan få. Ytterligare ett mål med studien var att ge en överblick av berörda intressenters medvetandegrad gällande cybersäkerhet i tunga fordon.

Fordon blir allt mer digitaliserade och förses med olika gränssnitt för uppkoppling mot internet och annan digital utrustning. Detta gäller inte minst tunga fordon, där olika påbyggnader från tredje part ytterligare ökar gränssytor mot omvärlden. Samtidigt utgör en stor del av den tunga fordonsflottan en viktig del av samhällsviktig verksamhet. MSB initierade därför en studie av cybersäkerhet i tunga fordon, med särskild inriktning mot fordon av vikt för civilförsvaret, för att belysa aktuell status och framtida trender inom området.

Studien bygger på en litteraturstudie inom området samt intervjuer med personal på olika befattningar inom räddningstjänsten och fordonstillverkare.

Resultatet visar att cybersäkerhetsarbetet inom branschen ännu är i sin linda, men att tillverkningssidan har börjat anamma cybersäkerhetsprinciper vid nyutveckling. Trots att cybersäkerhetsnivån i tunga fordon är låg samtidigt som angreppsytor ökar motverkar delvis det traditionella fokuset på tillförlitlighet och personsäkerhet (eng. *safety*) och sannolikheten för framgångsrika angrepp. Forskarnas bedömning är att för närvarande utgör något slags tillgänglighetsangrepp det största hotet.

Projektets resultat redovisas i en rapport¹¹ samt ett presentationsmaterial och underlag till ett informationsblad.

3.2 Sedelärande berättelser

Under år 2020 har ett antal incidenter relaterade till industriella styrsystem studerats. Studiens syfte var att ta fram incidentbeskrivningar för pedagogiska syften genom att beskriva incidenterna samt hur berörda organisationer hanterat dessa. Dessa berättelser har relaterats med referenser till MSB:s *Vägledning till ökad säkerhet i industriella informations- och styrsystem* från år 2014 samt till en teoretisk referensmiljö för att underlätta förståelsen. Incidentbeskrivningarna utgör sedelärande berättelser som är tänkta att fungera som underlag för diskussioner i kurser och övningar och finns beskrivna i ett separat FOI Memo¹².

3.3 Internetanslutna system, del 3

Under verksamhetsåret 2020 har en tredje etapp av studien Internetanslutna system genomförts. Under 2016 kartlagdes industriella informations- och styrsystem (vanligen benämnda som ICS, efter engelskans *Industrial Control System*) som är anslutna till internet genom sökningar på tjänster som Shodan och Censys. Arbetet fortsatte under år 2018 med en fortsättningsstudie och en studie med en problematisering avseende kartläggning av ICS till MSB. I den senare studien undersöktes tolv fabrikat som är vanliga i Sverige i syfte att se om dessa fångas upp av ett avgränsat antal publika sökmotorer.

Under år 2020 genomfördes en tredje studie inom området. Syftet med uppdraget var att stödja MSB i sin roll att stärka skyddet av ICS för svensk kritisk infrastruktur. Detta med kunskap kring hur man kan bygga en aktiv skanner för att detektera samhällskritiska internetanslutna ICS. Målet för uppdraget var att ta fram ett verktyg för att kunna göra egna skanningar och därmed kunna identifiera exponerade ICS i Sverige. De data som verktyget samlar in kan sedan ligga till grund för analyser av hur sårbara svenska system är.

¹¹ Valassi, C. & Karresand, M. (2020). *Cyberfysiska sårbarheter i tunga fordon* (FOI-R--5067--SE).

¹¹ Valassi, C. (2020). *Presentationsunderlag samt informationsblad – Cyberfysiska sårbarheter i tunga fordon* (FOI Memo 7463).

¹² Hunstad, A., Lindahl, D., Valassi, C. (2021). *Sedelärande berättelser* (FOI Memo XXXX)

Studiens upplägg beskrivs mer utförligt i ett FOI Memo¹³. Avrapportering sker i två FOI Memo^{14,15}. Vidare beskrivs rättsliga aspekter av nätverksskanning i ett separat FOI Memo¹⁶.

3.4 Elektromagnetiska hot mot trådlösa system

Under år 2019 och år 2020 genomfördes en studie med fokus på elektromagnetiska hot mot cyberfysiska system. Studien presenteras i en FOI-rapport¹⁷ som kortfattat beskriver hotbilden mot samhällsviktig verksamhet och ger exempel på både avsiktliga och oavsiktliga störningar i Sverige. Rapporten redogör även för hypotetiska störningsscenarier och åtgärder mot elektromagnetiska hot, baserade på erfarenheter från berörda svenska myndigheter. Slutligen sammanfattar rapporten kort de bestämmelser som utvecklats för att främja elektromagnetisk säkerhet. Merparten av de åtgärder som studien identifierar är av förebyggande karaktär eller ingår som en del i ett strategiskt och mer övergripande arbete för att främja medvetenhet, samarbete och säkerhet. Utifrån de samlade resultaten föreslås ett antal områden för vidare studier.

3.5 Industriella informations- och styrsystem i kris och krig

Under år 2019 beställdes en studie med målen att kartlägga regelverk samt att fånga utmaningar och problem med prioritering och fördelning av ICS-relaterade resurser när det råder brist i kris eller krig. Studien avrapporteras i en FOI-rapport¹⁸.

¹³ Westerdahl, L. (2020). *NCS3 2020: Förstudie – Internetanslutna styrsystem, del 3*. (FOI Memo 7212)

¹⁴ Westerdahl, L., Lundholm, K., Westring, E. (2021). *Detektion av industriella informations- och styrsystem på internet*. (FOI Memo 7482)

¹⁵ Lundholm, K., Westerdahl, L. (2021). *Detektion av 104-trafik med Nmap*. FOI Memo H2291)

¹⁶ Zouave, E. (2020). *Rättsliga aspekter av nätverksskanning* (FOI Memo 7435)

¹⁷ Odell, A., Zouave, E., Jaitner, M. (2020). *NCS3 - Elektromagnetiska hot mot trådlösa system*. (FOI-R--4838—SE)

¹⁸ Eckersand, U., Stenérus Dover, A. (2020). *NCS3 – Industriella informations- och styrsystem i kris och krig*. (FOI-R--4935—SE)

I det tidigare totalförsvaret fanns en företagsplanläggning för att säkerställa god leveranssäkerhet vid kris och krig. Särskilt kris- och krigsviktiga företag (så kallade K-företag) ingick i denna planläggning. Även idag ska näringsidkare delta i totalförsvarsplaneringen så att samhällsviktig verksamhet fungerar i krig.

I intervjuer med såväl leverantörer av ICS-relaterade resurser som myndigheter med ansvar för ICS-tung verksamhet lyfts önskemål om vägledningar och riktlinjer för prioritering och fördelning av ICS-resurser som behövs för att upprätthålla samhällsviktig verksamhet i händelse av en samhällsstörning. Det lyfts exempel på prioriteringsmodeller i intervjuerna, bland annat styr-el, prioriteringsmodellen för elnätet.

Studien utmynnade efter litteraturstudier och intervjuer i några förslag på lösningar av de identifierade utmaningarna. I rapporten föreslås att en nationell eller regional modell för prioritering tas fram. Vidare föreslås att om den motorreparationstjänst som fanns tidigare återinförs bör ICS-resurser ingå som en del av tjänsten.

3.6 Regelverk och krav inom området industriella informations- och styrsystem

Syftet med denna studie var att ge en uppdaterad bild av regelverk och krav och den baserades på två tidigare studier som genomfördes inom ramen för NCS3 åren 2012 och 2015. Studien från 2012 avrapporterades i FOI Memo 4415¹⁹ och studien från 2015 i en FOI-rapport²⁰. De ursprungliga studierna omfattade sektorerna elproduktion och eldistribution, dricksvatten, fjärrvärme och fjärrkyla, kemisk processindustri, spårbunden trafik, samt elektroniska kommunikationer.

I studien identifierades att regelverk och krav som styr säkerhetsarbetet med industriella informations- och styrsystem sedan 2015 har genomgått omfattande reformer. Detta gäller i synnerhet med antagandet av NIS-direktivet, cybersäkerhetsakten och nya säkerhetsskyddslagen. Studiens resultat redovisas i

¹⁹ Lindgren, F. (2013). Regelverk och krav inom området säkerhet i industriella informations- och styrsystem. FOI Memo 4415.

²⁰ Mossberg Sonnek, K och Lindgren, F. (2015). NCS3 – Regelverk och krav inom området industriella informations- och styrsystem. FOI-R--4197--SE

en FOI-rapport²¹ som på övergripande nivå beskriver regelverk och krav för industriella informations- och styrsystem. Förutom tidigare kartlagda sektorer har studien utökats med sektorn hälso- och sjukvård.

3.7 Förstudie Medicintekniska produkter

Under år 2020 genomfördes en förstudie med fokus på medicintekniska produkter. I en del av studien med fokus på CE-märkning och certifiering beskrivs hur regelverket kring certifiering av medicintekniska produkter kan påverka patientsäkerhet och cybersäkerhet.

Målet med studien var att presentera en faktaöversikt om regelverk och standarder för medicintekniska produkter och ta fram frågeställningar som ska användas i en intervjustudie med planerat genomförande under år 2021. Studien avrapporterades i ett FOI Memo²² som utgör ett underlag att utgå från i en kommande intervjustudie.

I en andra del av studien kontrollerades avvikelshantering i medicintekniska produkter (MTP). Syftet med delstudien var att analysera orsaker bakom de medicintekniska produktavvikelser som rapporteras till den nationella avvikelседatabasen *reidarMTP*. Dess mål var att analysera om inrapporteringen av avvikelser förändras över tid, om antalet datorrelaterade och ej datorrelaterade avvikelser förändras över tid samt om det finns rapporter i databasen om hot, risker, sårbarheter eller attacker mot cybersäkerheten i de medicintekniska produkterna. Studien ska ses som en förstudie som ligger till grund för en fortsatt fördjupande intervjustudie där representanter för vårdgivare samt föreskrifts- och tillsynsmyndigheter intervjuas under år 2021. Som hjälp för detta tas förslag på intervjufrågor fram. Studien avrapporterades i ett FOI Memo²³.

²¹ Appelgren, J och Zouave, E. (2021). NCS3 - Regelverk och krav inom området industriella informations- och styrsystem. En uppdatering av utvecklingen sedan december 2015. (FOI-R--5073--SE)

²² Eckersand, U., Wahrenberg, J. (2020). NCS3 – CE-märkning och certifiering av medicintekniska produkter. (FOI Memo 7428)

²³ Eckersand, U., Wahrenberg, J. (2021). NCS3 – Medicintekniska produkter. Avvikelsehantering. (FOI Memo 7474).

4 Kursutveckling

Under verksamhetsåret har kursutvecklingen genomförts i tre spår, begränsad uppdatering av *Grundkurs: Säkerhet i industriella informations- och styrsystem* (Gk-SI3S), framtagande av *Chefskurs: Säkerhet i industriella informations- och styrsystem* (Ck-SI3S) samt utveckling av kursen *Praktisk incidenthantering för industriella informations- och styrsystem* (I4S).

Uppdateringen av Gk-SI3S har syftat till att modifiera kursen samt att positionera den i relation till påbyggnadskursen. Resultatet redovisas i ett separat FOI Memo²⁴ och inkluderar i princip en begränsad översyn av samtliga föreläsningsmoduler. De praktiska kursmomenten i form av laborationer, demonstrationer och övning är dock oförändrade och i behov av uppdatering.

Ck-SI3S är en ny kurs som har tagits fram under år 2020. Kursen är planerad att genomföras under tre timmar och är primärt inriktad mot beslutsfattare på den nivå som motsvarar chefer till de som brukar delta i grundläggande och påbyggnadskurs (Gk-SI3S resp. Pk-SI3S). Målet med kursen är att uppnå förståelse för vad informationssäkerhet inom industriella informations- och styrsystem innebär. Detta i syfte att förstå att informationssäkerhet är ett verksamhetsproblem. Då mycket av innehållet i kursen överensstämmer med föreläsningsmaterialet från Gk-SI3S har arbetet samordnas med uppdateringen av den senare. Ck-SI3S finns beskriven i ett FOI Memo²⁵.

Den tredje utvecklingsaktiviteten fokuserar på att uppdatera kursen *Praktisk incidenthantering för industriella informations- och styrsystem* (I4S). I första hand hade övningsmodulen kring vilken den gamla kursen kretsade blivit föråldrad, men under förarbetet identifierades också brister i kursens pedagogiska upplägg. Därför inleddes arbetet med att ta fram ett uppdaterat upplägg för kursen baserat på dess målgrupp och lärandemål. Ett schema med ett tydligare fokus på incidenthanteringsmetod med föreläsningar, träning i form av laborationer samt tre avslutande övningar togs fram. I samband med detta förlängs kursen också från 3,5 dagar till fyra dagar. Förarbetet och de övergripande tankarna med laborationer och övningar finns beskrivet i ett FOI Memo²⁶. Utvecklingen av kursen har fortsatt under 2021 och under oktober 2021

²⁴ Westerdahl, L. (2021). *Sammanfattning av utfört arbete – kursutveckling av Gk-SI3S*. (FOI Memo 7499)

²⁵ Westerdahl, L. (2020). *Chefskurs för säkerhet i industriella informations- och styrsystem*. (FOI Memo 7411)

²⁶ Westerdahl, L. (2020). *Planerad utveckling av NCS3-kursen I4S 2020*. (FOI Memo 7200)

kommer två pilotgenomföranden att ske. De senare har fördröjts på grund av coronarestriktioner.

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

Överenskommelse: Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2020 NCS3, Delbeställning: Kursutveckling och - genomförande

MSB dnr: MSB 2020-04057

Referens	Titel
FOI-R-5290-SE	Verksamhetsrapport

5.2 Genomförande av påbyggnadskurs SI3S september 2020

Överenskommelse: Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2020, Delbeställning: Kursutveckling och - genomförande

MSB dnr: MSB 2020-04057

Referens	Titel
FOI Memo 7314	Kursutvärdering Påbyggnadskurs: Säkerhet i industriella informations- och styrsystem, september 2020

5.3 Kursutveckling

Överenskommelse: Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2020, Delbeställning: Kursutveckling och - genomförande

MSB dnr: MSB 2020-04057

Referens	Titel
FOI Memo 7200	Planerad utveckling av NCS3-kursen I4S 2020
FOI Memo 7411	Chefskurs för säkerhet i industriella informations- och styrsystem
FOI Memo 7499	Sammanfattning av utfört arbete - kursutveckling av Gk-SI3S

5.4 Cyberfysiska sårbarheter i tunga fordon

Överenskommelse: Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2020, Delbeställning: Cyberfysiska sårbarheter i tunga fordon

MSB dnr: MSB 2020-04055

Referens	Titel
FOI-R--5067--SE	NCS3: Cyberfysiska sårbarheter i tunga fordon
FOI Memo 7463	Presentationsunderlag samt informationsblad

5.5 Sedelärande berättelser

Överenskommelse: Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2020, Delbeställning: Sedelärande berättelser

MSB dnr: MSB 2020-04058

Referens	Titel
FOI Memo 7623	Sedelärande berättelser

5.6 Internetanslutna system, del 3

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

MSB dnr: MSB 2020-06443

Referens	Titel
FOI Memo 7212	NCS3 2020: Förstudie – Internetanslutna styrsystem, del 3
FOI Memo 7435	Rättsliga aspekter av nätverksskanning
FOI Memo 7482	Detektion av industriella informations- och styrsystem på internet
FOI Memo H2291	Detektion av 104-trafik med Nmap

5.7 Elektromagnetiska hot mot trådlösa system

Överenskommelse: NCS3 Studie: Elektromagnetiska hot mot trådlösa system

MSB dnr: MSB 2019-04982

Referens	Titel
FOI-R--4838--SE	NCS3 - Elektromagnetiska hot mot trådlösa system. En studie av incidenter, möjliga hot och åtgärder

5.8 Industriella informations- och styrsystem i kris och krig

Överenskommelse: NCS3 Studie: Industriella informations- och styrsystem i kris och krig

MSB dnr: MSB 2019-05348

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

5.9 Regelverk och krav inom området industriella informations- och styrsystem

Överenskommelse: NCS3 - Delbeställning: Regelverk och krav inom området industriella informations- och styrsystem

MSB dnr: MSB 2020-04491

Referens	Titel
FOI-R--5073--SE	NCS3 - Regelverk och krav inom området industriella informations- och styrsystem. En uppdatering av utvecklingen sedan december 2015

5.10 Förstudie - medicintekniska produkter

Överenskommelse: NCS3 - Medicintekniska produkter – incidentrapportering och CE-märkning samt övergripande NCS3-arbete

MSB dnr: MSB 2020-08183

Referens	Titel
FOI Memo 7428	NCS3 - CE-märkning och certifiering av medicintekniska produkter
FOI Memo 7474	NCS3 - Medicintekniska produkter. Avvikelsehantering.



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 cybersäkerhetsaspekter 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

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

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

www.msb.se