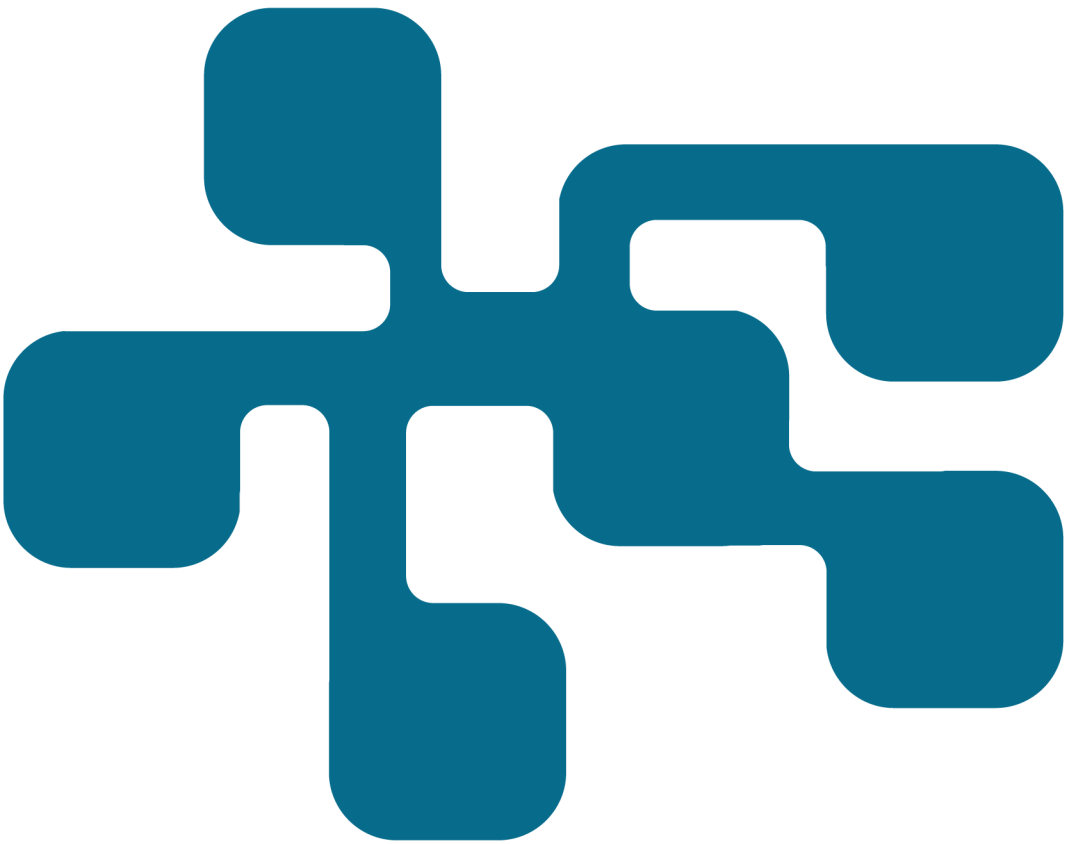
NCS3 2017 – Verksamhetsrapport

Lars Westerdahl

FOI



FOI-R--4957--SE
MSB 2017-405
ISSN 1650-1942

Maj 2020

Lars Westerdahl

NCS3 2017 – Verksamhetsrapport

Titel	NCS3 2017 – Verksamhetsrapport
Title	NCS3 2017 – Activity Report
Rapportnr/Report no	FOI-R--4957--SE
Månad/Month	Maj/May
Utgivningsår/Year	2020
Antal sidor/Pages	22
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	E72151
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är en del av ett program hos *Myndigheten för samhällsskydd och beredskap* (MSB) för 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 2017.

Genom 2017 års överenskommelser har 17 uppdrag utförts under perioden 2017–2018. Dessa uppdrag har utförts av avdelningarna Försvarsanalys respektive Ledningssystem på *Totalförsvarets forskningsinstitut* (FOI). Uppdragen omfattade bland annat tio studier och fem kurstillfällen, samt medvetandehöjande aktiviteter såsom föredrag.

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

Summary

The National Centre for Security in Control Systems for Critical Infrastructure (NCS3) is part of a program at the *Swedish Contingencies Agency* (MSB) for enhancing security in those systems that constitute critical infrastructure. The work that is conducted within NCS3 is regulated through assignments from MSB. In this report, the assignments that were agreed upon in 2017 are summarized.

In 2017, 17 assignments were agreed upon and carried out during the period 2017–2018. These assignments were carried out at the *Swedish Defence Research Agency* (FOI), by the division of Defence Analysis and C4ISR respectively. The assignments included ten studies and five course offerings, as well as awareness increasing activities such as talks.

Keywords: NCS3, Industrial Control System, Critical Infrastructure.

Innehållsförteckning

1 Inledning

I denna rapport sammanfattas det arbete som utförts inom de överenskommelser som ingåtts under 2017 rörande arbetet inom *Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet* (NCS3). Arbetet har utförts av avdelningarna Försvarsanalys respektive Ledningssystem på *Totalförsvarets forskningsinstitut* (FOI).

För 2017 års verksamhet upprättades 17 separata överenskommelser. Kunskapsuppbyggnad har varit ett tydligt tema i arbetet, vilket märks genom att fler studier har genomförts jämfört med tidigare. Arbetet inom dessa överenskommelser har genomförts under perioden 2017–2018.

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 är centrerad 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 Myndigheten för samhällsskydd och beredskaps (MSB) nationella program (från 2009 och framåt) som tekniskt inriktad verksamhet avseende IT-säkerhet. Namnet NCS3 etablerades 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 Slutrapportens uppbyggnad

I kapitel 2 presenteras den verksamhet som kategoriseras som medvetandehöjande aktiviteter. Kapitel 3 beskrivs de kunskaps- och förmågehöjande aktiviteter som utförts. Genomförda studier sammanfattas i kapitel 4. Utvecklingen av NCS3:s tekniska och pedagogiska plattform presenteras i kapitel 5. I kapitel 6 beskrivs den övriga verksamhet som kallas för centrumverksamhet. Avslutningsvis i kapitel 7, sammanfattas de leveranser som NCS3 har producerat under 2017 års överenskommelser.

[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 Medvetandehöjande aktiviteter

Medvetandehöjande aktiviteter inom NCS3 syftar till att höja medvetandet om de hot och risker som existerar inom industriella informations- och styrsystem, men även att sprida information om NCS3. Under 2017 deltog medarbetare ur NCS3 i tre olika aktiviteter, vilka beskrivs nedan.

Linköpings Teknologers Studentkår arrangerar årligen ett arbetsmarknads-evenemang på Linköpings universitet. Evenemanget går under namnet *Linköpings teknologers studentkårs arbetsmarknadsdagar* (LARM) och är ett evenemang som är årligen återkommande. Medarbetare ur NCS3 deltog i eventet den 14 februari, genom att bemanna en del av FOI:s monter. Medarbetarna informerade om NCS3, industriella informations- och styrsystem samt visade upp dricksvattendemonstratorn.

MSB anordnade ett lunchseminarium den 4 april. Under detta seminarium presenterades resultat från studien *Styrsystem anslutna till Internet*, en studie som genomfördes 2016.

Den 28 september organiserade Energiföretagen en workshop i syfte att identifiera en målbild för en kommande kurs som de avser skapa för sina medlemmar. NCS3 deltog i denna workshop genom att ge en föreläsning om cyberhot mot informationssystem och industriella informations- och styrsystem. NCS3 deltog även i ett uppföljande möte den 24 november men drog sig därefter ur arbetet då även MSB var representerade där.

3 Kunskaps- och förmågehöjande aktiviteter

Kunskaps- och förmågehöjande aktiviteter avser främst de kurser som ges inom NCS3-arbetet. Under 2017 genomfördes fem kurser: fyra tillfällen med *Säkerhet i industriella informations- och styrsystem* (SI3S) och ett med Praktisk incidenthantering i industriella informations- och styrsystem (I4S).

Kursen SI3S är en grundläggande IT-säkerhetskurs som riktar sig till tekniker och annan personal som arbetar med, eller i anslutning till, industriella informations- och styrsystem. Syftet med kursen är att deltagarna ska kunna arbeta aktivt med säkerhetsfrågor i sina egna system och få ett stöd för att kunna göra detta. Kursen genomförs oftast med inriktning mot en specifik sektor. Kurstillfällen och inriktning redovisas i Tabell 1.

Tabell 1 Tabell 1 SI3S-kurser.

Datum	**Inriktning**
28 februari–1 mars	Kommuner
7–8 mars	Kommuner
15–16 november	Trafikverket
21–22 november	Blandad

Kursen I4S genomfördes 7–10 november och är riktad mot IT-tekniker vilka arbetar i, eller i anslutning till, en miljö med industriella informations- och styrsystem. Målet med kursen är att teknikerna ska identifiera och analysera incidenter i ett IT-system med kopplingar till ett produktionsnätverk och föreslå åtgärder. Kursen har en bredare målgrupp jämfört med kursen SI3S och kräver fler kompetenser för att ge ett optimalt arbetslag under övningspassen.

4 Studier

Tio studier av varierande omfattning har genomförts under 2017.

4.1 Förstudie fjärrvärme

Denna studie syftar till att beskriva fjärrvärmebranschen och dess utveckling på medellång sikt. I detta arbete igår främst att studera industriella informations- och styrsystem och säkerhetsaspekter kopplat till dessa, men även branschen som helhet. Därför tas även frågor om aktörer, ekonomi och juridik upp i förstudien.[2]

Fjärrvärme är en av de vanligaste uppvärmningsformerna för hus i Sverige, särskilt för flerbostadshus och lokaler där det bedrivs verksamhet. Produktion och distribution av fjärrvärme är oftast lokal även om det kan finnas flera källor som bidrar till värmen i nätet. Det är ännu dock vanligast att alla källor tillhör en gemensam ägare. Produktionen är ofta automatiserad i hög grad vilket innebär behov av övervakning, både lokalt och via fjärranslutning. Den direkta hotbilden mot fjärrvärmesystem bedöms som låg, främst genom att det anses vara en miljövänlig teknik samt att effekterna av ett angrepp endast blir lokala. Anläggningar är dock uppkopplade vilket innebär att det finns behov av ett grundläggande skydd mot internetbaserade hot.

4.2 Förstudie risker med IPv6 inom ICS

För att kunna kommunicera via internet måste varje enhet gå att adressera på ett unikt sätt. Fortfarande används en uppsättning adresser kallad IPv4, som redan i början på 1990-talet insågs vara för liten. Det gör att olika typer av lösningar för att kringgå begränsningen har behövt tas fram, vilka dock komplicerar kommunikationen. Därför antog Internet Engineering Task Force (IETF) 1994 ett förslag om en ersättning för IPv4, vilken fick namnet IPv6. Förutom en mycket utökad adressrymd (från 4,3*109 till 3,4*1038 adresser) i IPv6, åtgärdas även en del brister som finns i IPv4. I och med den enorma expansion av internetanslutna enheter, främst inom industriella informations- och styrsystem, som sakernas internet (eng. Internet of Things, IoT) innebär kommer en övergång till IPv6 behöva genomföras inom en snar framtid. I detta memo problematiseras införandet och användning av IPv6 inom industriella informations- och styrsystem (eng. Industrial Control Systems, ICS).[3]

---

[2] Valassi, C., Hunstad, A.G. & Westerdahl, L. (2019). *NCS3 – Förstudie fjärrvärme* (FOI-R--4738--SE).

[3] Karresand, M. (2017). *Risker med IPv6 inom industriella informations- och styrsystem* (FOI Memo 6114).

Resultatet av problematiseringen visar att övergången från IPv4 till IPv6 kan ge problem, dock främst för att all utrustning i kommunikationskedjan måste stödja IPv6. Dessa problem kan därför betraktas som logistiska. Användningen av IPv6 medför dock problem i och med att protokollet inte är anpassat för resurssvaga enheter och den speciella kommunikationsstruktur som återfinns inom industriella informations- och styrsystem. Det pågår dock flera projekt för att utöka IPv6 med tillägg som löser dessa problem. Likaså kräver möjligheten att i IPv6 direkt adressera en enhet även ett nytt sätt att tänka säkerhetsmässigt, till skillnad från IPv4 där lösningarna för att virtuellt utöka adressrymden har medfört ett visst skydd mot angrepp.

4.3 Förstudie SI3S fortsättningskurs

Kursen Säkerhet i industriella informations- och styrsystem (SI3S) har getts sedan 2009. Inledningsvis definierades den som en kunskapshöjande kurs vilket stämde bra med den allmänna medvetandegraden i början av 2010-talet. Sedan dess har medvetandegraden om hot mot industriella informations- och styrsystem ökat vilket har resulterat i ett behov av en nyare kurs. En förstudie har genomförts i syfte att undersöka vilka förutsättningar som finns för att skapa en ny kurs och hur en sådan kurs skulle kunna utformas. Under förstudien identifierades nationella och internationella initiativ som kan utgöra konkurrens och en analys genomfördes av olika pedagogiska upplägg. Resultatet av förstudien dokumenterades i FOI Memot *Förstudie SI3S fortsättningskurs*.[4]

4.4 Förstudie smarta system i tunga fordon i kommersiell trafik

Målet med denna studie var att ge en överskådlig bild av de komponenter och teknologier som används för att bygga elektroniska styrsystem i tunga fordon, hur komponenterna kommunicerar med varandra och hur de kommunicerar med omvärlden. Resultatet av förstudien dokumenterades i FOI Memot *NCS3 - Kartläggning av elektroniska styrsystem i tunga fordon*.[5]

Studien visar att tillverkarna endast på senare tid har tagit hänsyn till cybersäkerhet vid konstruktion av systemen i tunga fordon. Utvecklingen av protokoll och system har fokuserat på robusthet och tillförlitlighet och i många fall har man inte övervägt de hot som kommer från en illvillig person som vill påverka fordonet. Systemen har setts som isolerade från omvärlden. Att ett

[4] Westerdahl, L. (2017). *Förstudie SI3S fortsättningskurs* (FOI Memo 6095).

[5] Gustafsson, T. (2018). *NCS3 - Kartläggning av elektroniska styrsystem i tunga fordon* (FOI Memo 6358).

uppvaknande har skett kan dock observeras, dels genom att tillverkare av tunga fordon idag har dedikerade cybersäkerhetsexperter för systemen i fordonen och dels genom hur dessa frågeställningar hanteras i aktuella projekt såsom utvecklingen inom V2X och uppkopplade fordon.

Studien visar också att det finns ett antal olika protokoll och tekniska lösningar med vilka kommunikationen inom ett fordon sker samt att dessa protokoll ofta saknar relevanta cybersäkerhetsmekanismer. Vilka protokoll och lösningar som finns inom ett visst fordon varierar stort varför det är svårt att generellt besvara frågan om hur känsliga tunga fordon är för cyberattacker. Det verkar dock vanligt att ett fordon innehåller flera olika nätverk för olika funktioner. I många fordon finns det också en viss segmentering mellan olika funktioner som delar nätverk, till exempel den så kallade CAN-bussen. Det är dock oklart hur effektivt skydd denna segmentering egentligen utgör och om hur svårt det är att kringgå denna. Ytterligare ett problem som har identifierats men där omfattningen är okänd är hur olika tredjeparts-system används och hur de påverkar integriteten för de aktuella kommunikationsprotokollen. Ett exempel på sådana system är färdskrivare och så kallade Fleet Management Systems som används för att hantera och optimera användningen av fordonen. Det är oklart hur och i vilken omfattning dylika system riskerar att påverka exponeringen av fordonsinterna system samt vilka konsekvenser denna exponering kan få.

4.5 Förstudie styrsystem i drivmedelskedjan

Studien, som resulterade i ett memo[6], syftade till att översiktligt beskriva drivmedelskedjan samt var och med vilket syfte som informations- och styrsystem används. Syftet var också att utifrån kartläggningen analysera eventuella systemrisker. Studien genomfördes med hjälp av intervjuer med ett urval aktörer inom drivmedelskedjan (företrädesvis fossilbränslebranschen), från produktion, till förädling, distribution och lagring. Resultaten visade att styrsystem används inom alla steg i drivmedelskedjan. I en del fall kan verksamheten bedrivas utan fungerande styrsystem då det finns alternativa, om än mer omständliga och resurskrävande, lösningar. I andra fall är verksamheten, som exempelvis raffineringsprocessen, helt beroende av fungerande styrsystem. Studien visar också att det finns en uppsjö av leverantörer av styrsystem för aktörerna inom drivmedelskedjan, vilket kan vara positivt ur ett säkerhets-perspektiv då aktörer som fyller liknande funktion inte använder samma typ av system/leverantör. En potentiell risk å andra sidan är att flera av respondenterna uppger att de låter leverantörer och konsulter koppla upp sig mot organisationens styrsystem för att bland annat genomföra uppgraderingar. Ingen av

[6] Stenérus Dover, A-S., Lindgren, J. & Andersson, P. (2018). *NCS3 - Styrsystem i drivmedelskedjan* (FOI Memo 6387).

respondenterna uttryckte dock någon större oro inför framtiden relaterat till styrsystem ur ett säkerhetsperspektiv.

4.6 IoT-relaterade hot

Studien identifierar och analyserar risker relaterade till IoT, samt föreslår strategier för att motverka och begränsa dem. Strategierna riktas i första hand till MSB och andra myndigheter.

Till grund för analysen ligger en studie av vetenskapliga skrifter. Analysen görs med hjälp av ett ramverk baserat i riskanalytisk metod. De element som ingår i ramverket är skyddsvärden, sårbarheter, attackvektorer, risker och strategier. Attackvektorerna beskrivs på en djupare teknisk nivå än de andra delarna och har därför lagts i en bilaga.

Slutsatserna som presenteras i en rapport[7] är att MSB bör agera mot fysisk exponering, bristfällig lösenordshantering och design utan säkerhetstänk, samt prioritera ordinärt IT- och ICS-säkerhetsarbete för hantering av de relevanta konsekvenserna. MSB bör även verka för transparens inom IoT där syftet med uppkopplingen kommuniceras och där information om händelser och sårbarheter kan delas utan att kommersiella incitament äventyras.

4.7 Krypterad kommunikation inom industriella informations- och styrsystem

Studien undersöker behov, nyttjande samt relevans av kryptografiska funktioner som skydd mot cyberangrepp för industriella informations- och styrsystem. Totalt genomfördes tre informationsinhämtningsmoment, två litteraturstudier och en intervjuserie. Litteraturstudierna delades i sin tur in i (1) identifiering av lagkrav och standarder för kryptografiska funktioner inom industriella informations- och styrsystem och (2) identifiering av lämpliga kryptografiska funktioner i kontexten av industriella informations- och styrsystem. Intervjuer genomfördes med två styrsystemsoperatörer inom branscher med olika skyddskrav samt en intervju med en leverantör av styrsystemsprodukter. Studiens resultat[8] visar att respondenterna motsätter sig kryptering av de interna nätverken eftersom detta avsevärt försvårar övervakning av dessa nätverk. Övervakning av dessa nätverk prioriteras högt då det för systemägaren är viktigt att se innehållet i kommunikationen som färdas mellan enheter i nätverket. Istället för kryptering ses starka autentiseringsmekanismer som det mest kritiska för att säkerställa de

[7] Swaling, V.H. & Johansson, J. (2018). *IoT-relaterade hot och strategier* (FOI-R--4591--SE).

[8] Valassi, C., Lindahl, D. & Westerdahl, L. (2018). *Kryptografiska funktioner inom industriella informations- och styrsystem* (FOI-R--4596--SE).

interna nätverken, dock kan kryptografiska funktioner så som digitala signaturer användas för autentisering. Baserat på studiens resultat rekommenderas även kryptering av all extern kommunikation samt all lagrad data.

4.8 Molntjänster inom industriella informations- och styrsystem

Allt fler leverantörer av industriella informations- och styrsystem erbjuder även molntjänster med olika innehåll och servicenivå. De erbjudna servicenivåerna skiljer sig åt och omfattar allt från att vissa administrativa funktioner placeras i ett moln till lösningar där i stort sett allt utom den processintegrerade hårdvaran läggs i molnet. Utvecklingen går snabbt och medför inte bara förbättringar utan introducerar även nya säkerhetsrisker. I rapporten presenteras molntjänstkonceptet och dess säkerhetsmässiga utmaningar för industriella informations- och styrsystem, både nuvarande och kommande.[9] Rapporten avslutas med en uppsättning råd till den som planerar att börja nyttja en molntjänst.

Resultaten som presenteras i rapporten pekar på olika säkerhetsmässiga övervägningar som bör göras vid en övergång till molnet. Främst handlar det om att kontrollen över känslig information delegeras till en extern part, samt att åtkomsten till informationen äventyras i och med de längre och mer komplexa kommunikationsvägarna. Det uppstår därför nya risker för avbrott i verksamheten, samtidigt som andra risker minskar. Slutsatsen är att en övergång måste förberedas noga, men på intet sätt behöver avrådas från.

4.9 Standard ISA/IEC62443 – dess användning och utbredning i Sverige

Syftet med studien var att ge MSB en ökad förståelse för standardens omfattning och användning i Sverige för att på så vis bidra till ökad kunskap om de förutsättningar som råder inom ICS-området. Standardens användning kartläggs genom intervjuer med aktörer med bred erfarenhet från många olika domäner. Därtill ges i rapporten[10] en övergripande beskrivning av innehållet i ISA/IEC 62443.

[9] Hunstad, A.G. & Karresand, M. (2018). *Molntjänster inom industriella informations- och styrsystem - En översikt av säkerhetsaspekter* (FOI-R--4597--SE).

[10] Wedebrand, C., Swaling, V.H. & Stenérus Dover, A-S. (2018). *NCS3 Studie – Standardserie ISA/IEC 62443 – Användning och erfarenheter bland svenska ICS-aktörer* (FOI-R--4601--SE).

Standardens fördelar anses vara att den är komplett över hela livscykeln, att den är skräddarsydd för ICS samt att den definierar en uppsättning säkerhetsnivåer som kan underkastas olika krav. Andra skäl till att ISA/IEC 62443 används och uppmärksammas anses vara en förändrad kravbild från kunderna som är kopplad till industrins ökade utsatthet för cyberincidenter, samt förväntade åtgärder i och med NIS-direktivet. Bland utmaningarna nämns att standarden inte är ISO-klassad samt att många delar är under utveckling och att flera av dem riskerar att bli föråldrade. En generell utmaning är att verksamheterna inte alltid ser den ekonomiska nyttan i relation till kostnaderna och därmed är obenägna att implementera standarder inom cybersäkerhet.

4.10 Virtualisering inom industriella informations- och styrsystem

Rapporten[11] presenterar hur virtualisering i ökande grad framträder som en smidig och attraktiv lösning för industriella informations- och styrsystem, men att det är nödvändigt att göra säkerhetsmässiga avvägningar vid en övergång till virtualiserad datordrift. Huvudtyper av virtualiseringslösningar och relaterade säkerhetsutmaningar diskuteras, vilket leder fram till säkerhetsrelaterade rekommendationer för systemägare och operatörer. Rekommendationerna fokuserar på planering avseende ansvarsfrågor, incidenthantering respektive risk- och sårbarhetsanalys.

[11] Hunstad, A.G., Valassi, C. & Lindahl, D. (2018). *Virtualisering inom industriella informations- och styrsystem* (FOI-R--4603--SE).

5 Teknisk utveckling

Den tekniska utvecklingen inom NCS3 avser utveckling av både tekniska och pedagogiska plattformar.

5.1 Kursstöd

En uppdatering av presentationsmaterialet till kurserna genomfördes innan kurserna gavs för året. Dels anpassades bildspelet till FOI:s nya mall för bildspel, dels gjordes en genomgång av bildmaterialet för att säkerhetsställa upphovsrätt.

Den kursutvärdering som görs av deltagare efter SI3S och I4S har hittills genomförts på papper. En digitalisering av pappersmallen genomfördes med stöd av det verktyg som används för utvärdering av andra FOI-kurser.

I samband med SI3S-kurserna i november genomfördes även en internutbildning med målet att öka redundansen av möjliga lärare för kursen. Det finns nu två parallella lärarlag för SI3S vilket ökar leveranssäkerheten för kursen.

5.2 Demonstratorer

Ångmaskinsdemonstratorn med tillhörande nätverk utgör en viktig komponent i de laborationer som genomförs i SI3S-kursen. En svaghet med ångaskins-demonstratorn har varit att deltagarna endast sett sin egen nätverkstrafik, vilket innebär att det inte finns något behov av att prioritera vilken nätverkstrafik som är viktig och vilken som är ”brus”. En bot liknande de som används i kursen I4S nätverk i syfte att skapa bakgrundstrafik i ångmaskinsnätverket installerades därför i demonstratorn.

5.3 Kursmoduler

Två längre föreläsningspass baserade på de tidigare studierna *Industriella protokoll* samt *Monitorering och övervakning* har tagits fram. Föreläsningspassen är cirka 45 minuter långa och är tänkta att antingen kunna utgöra en lektion i en kurs eller att fungera som fristående föreläsningar.

Föreläsningen om industriella protokoll innehåller en presentation av de vanligast förekommande kommunikationsprotokollen i Sverige och dess egenskaper inom industriella informations- och styrsystem. Föreläsningen om monitorering och övervakning presenterar en genomgång av digitala övervakningsmetoder för att upptäcka intrångsförsök, anpassade för industriella informations- och styrsystem.

6 Centrumverksamhet

Inom det övergripande arbetet har tre aktiviteter genomförts. Verksamheten inleddes med en kick-off i Norrköping 25–26 januari. Kick-offen organiserades av MSB och under denna deltog tio NCS3-medarbetare från FOI:s avdelningar Försvarsanalys samt Ledningssystem. Under kick-offen presenterades genomfört arbete från föregående år och förutsättningar för kommande år diskuterades.

En medarbetare deltog i en förvaltningskurs för IT. Kursen gavs som en intensivkurs av Nordic Forum for Information (NFI) och genomfördes den 11–12 maj under namnet *Ledning och styrning av IT*.

NCS3-medarbetare deltog under en av dagarna på MSB:s konferens *Informationssäkerhet för offentlig sektor*. Konferensen är återkommande och årets konferens genomfördes den 5–6 september.

Nio medarbetare från Försvarsanalys deltog i en anpassad variant av SI3S-kursen den 22 november. Aktiviteten var ett led i att bredda kompetensbasen inom avdelningens NCS3-verksamhet.

Ett kortare FOI Memo[12] på engelska togs fram baserat på rapporten *Effekten av kurser inom ICS-säkerhet*.[13]

[12] Stenérus Dover, A-S. (2017). *The influence on an organization´s security work of training and exercises in ICS* (FOI Memo 6042).

[13] Stenérus Dover, A-S. & Trané, C. (2017). *Effekten av kurser inom ICS-säkerhet* (FOI-R--4433--SE).

7 Leveranser

Leveranser från NCS3 utgörs i huvudsak av rapporter och memon samt olika typer av aktiviteter.

7.1 Skriftliga leveranser

Nedan redovisas NCS3:s skriftliga leveranser sorterat under de överenskommelser som efterfrågat leveranserna.

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **NCS3 - Förstudie: Smarta system i tunga fordon i kommersiell trafik** (FOI-2017-89, MSB 2017-11442)

- Gustafsson, T (2018). *NCS3 - Kartläggning av elektroniska styrsystem i tunga fordon* (FOI Memo 6358).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **NCS3 - Delbeställning: Förstudie SI3S fortsättningskurs** (FOI-2017-89, MSB 2017-1625)

- Westerdahl, L (2017). *Förstudie SI3S fortsättningskurs* (FOI Memo 6095).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **Delbeställning: Deltagande i övergripande arbete** (FOI-2017-88, MSB 2017-403)

- Stenérus Dover, A-S. (2017). *The influence on an organization´s security work of training and exercises in ICS* (FOI Memo 6042).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **Delbeställning: Deltagande i övergripande arbete för FOI Ledningssystem** (FOI-2017-89, MSB 2017-404)

- Westerdahl, L (2017). *Anteckningar från Fjärrvärmedagarna 2017* (FOI Memo 6058)
- Westerdahl, L (2017). *Statusrapport för ÖK deltagande i övergripande arbete* (FOI Memo 6091)
- Westerdahl, L (2017). *Statusrapport för ÖK Deltagande i övergripande arbete* (FOI Memo 6265).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **NCS3 - Delbeställning: Projektkoordinering och centrumverksamhet vid NCS3s tekniska plattform i Linköping** (FOI-2017-89, MSB 2017-405)

- Westerdahl, L (2017). *Statusrapport NCS3 2017 kvartal 1* (FOI Memo 6046)
- Westerdahl, L (2017). *Statusrapport NCS3 2017 kvartal 2* (FOI Memo 6092)
- Westerdahl, L (2017). *Statusrapport NCS3 2017 kvartal 3* (FOI Memo 6143)
- Westerdahl, L (2018). *Statusrapport NCS3 2017 kvartal 4* (FOI Memo 6357)
- Westerdahl, L (2020). *NCS3 2017 - verksamhetsrapport* (FOI-R--4957--SE).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **Genomförande av grundläggande kurs – SI3S** (FOI-2017-89, MSB 2017-96)

- Westerdahl, L (2017). *Kursredovisning SI3S 2017 februari–mars* (FOI Memo 6039).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **NCS3 - Delbeställning: Molntjänster inom industriella informations- och styrsystem** (FOI-2017-89, MSB-2017-1620)

- Hunstad, A.G. & Karresand, M. (2018). *Molntjänster inom industriella informations- och styrsystem - En översikt av säkerhetsaspekter* (FOI-R--4597--SE).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **NCS3-studie Krypterad kommunikation inom industriella informations- och styrsystem** (FOI-2017-89, MSB-2017-1623)

- Valassi, C., Lindahl, D. & Westerdahl, L. (2018). *Kryptografiska funktioner inom industriella informations- och styrsystem* (FOI-R--4596--SE).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **NCS3 - Delbeställning: Virtualisering inom industriella informations- och styrsystem** (FOI-2017-89, MSB-2017-1624)

- Hunstad, A.G., Valassi, C. & Lindahl, D. (2018). *Virtualisering inom industriella informations- och styrsystem* (FOI-R--4603--SE).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **Delbeställning: Genomförande av kurs – I4S** (FOI-2017-89, MSB-2017-3103)

- Westerdahl, L (2018). *Kursutvärdering I4S* (FOI Memo 6334).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **NCS3 - Delbeställning: Test av miljö** (FOI-2017-89, MSB-2017-3185)

- Westerdahl, L. (2018). *Test av miljö* (FOI Memo 6457).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **Delbeställning: Förstudie – Risker med IPv6 inom ICS** (FOI-2017-89, MSB-2017-3508)

- Karresand, M. (2017). *Risker med IPv6 inom industriella informations- och styrsystem* (FOI Memo 6114).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **Delbeställning: Förstudie fjärrvärme** (FOI-2017-89, MSB-2017-4121)

- Valassi, C., Hunstad, A.G. & Westerdahl, L. (2019). *NCS3 – Förstudie fjärrvärme* (FOI-R--4738--SE).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **Delbeställning: Kursutveckling** (FOI-2017-89, MSB-2017-4856)

- Westerdahl, L (2018). *Kursutveckling: Anpassning av bildspel* (FOI Memo 6332)
- Westerdahl, L (2018). *SI3S november 2017* (FOI Memo 6333)
- del Ama Garcia, V. (2018). *Kursutveckling: Bot för ångmaskinsnätet* (FOI Memo 6335)
- Karresand, M. (2018). *Presentationsunderlag - Kursmodul Monitorering och övervakningssystem för industriella informations- och styrsystem* (FOI Memo 6478)
- Eidenskog, D. (2018). *Presentationsunderlag - Industriella protokoll i kritisk infrastruktur* (FOI Memo 6487).

NCS3 Förstudie: Styrsystem inom drivmedelskedjan (FOI-2017-422, MSB 2017-1621)

- Stenérus Dover, A-S., Lindgren, J. & Andersson, P. (2018). *NCS3 - Styrsystem i drivmedelskedjan* (FOI Memo 6387).

NCS3 Studie - IoT-relaterade hot (FOI-2017-798, MSB 2017-1554)

- Swaling, V.H. & Johansson, J. (2018). *IoT-relaterade hot och strategier* (FOI-R--4591--SE).

NCS3: Standard ISA/IEC 62443 - dess användning och utbredning i Sverige (FOI-2017-797, MSB 2017-2825)

- Wedebrand, C., Swaling, V.H. & Stenérus Dover, A-S. (2018). *NCS3 Studie – Standardserie ISA/IEC 62443 – Användning och erfarenheter bland svenska ICS-aktörer* (FOI-R--4601--SE).

7.2 Övriga leveranser

Utöver skriftliga rapporter och memon har även nedanstående aktiviteter genomförts under 2016.

7.2.1 Föredrag, presentationer och deltagande

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **Delbeställning: Deltagande i övergripande arbete för FOI Ledningssystem** (FOI-2017-89, MSB 2017-404)

Datum	Aktivitet	Event
4 april	Föredrag	Lunchseminarium
28 september	Föredrag	Energiföretagen
24 november	Planeringsmöte	Energiföretagen

7.2.2 Kurser

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **Genomförande av grundläggande kurs – SI3S** (FOI-2017-89, MSB 2017-96)

Datum	Kurs	Inriktning
28 februari–1 mars	SI3S	Kommuner
7–8 mars	SI3S	Kommuner

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **Delbeställning: Kursutveckling** (FOI-2017-89, MSB-2017-4856)

Datum	**Kurs**	**Inriktning**
15–16 november	SI3S	Trafikverket
21–22 november	SI3S	Blandad

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2017, **Delbeställning: Genomförande av kurs – I4S** (FOI-2017-89, MSB-2017-3103)

Datum	**Kurs**	**Inriktning**
7–10 november	I4S	Blandad

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