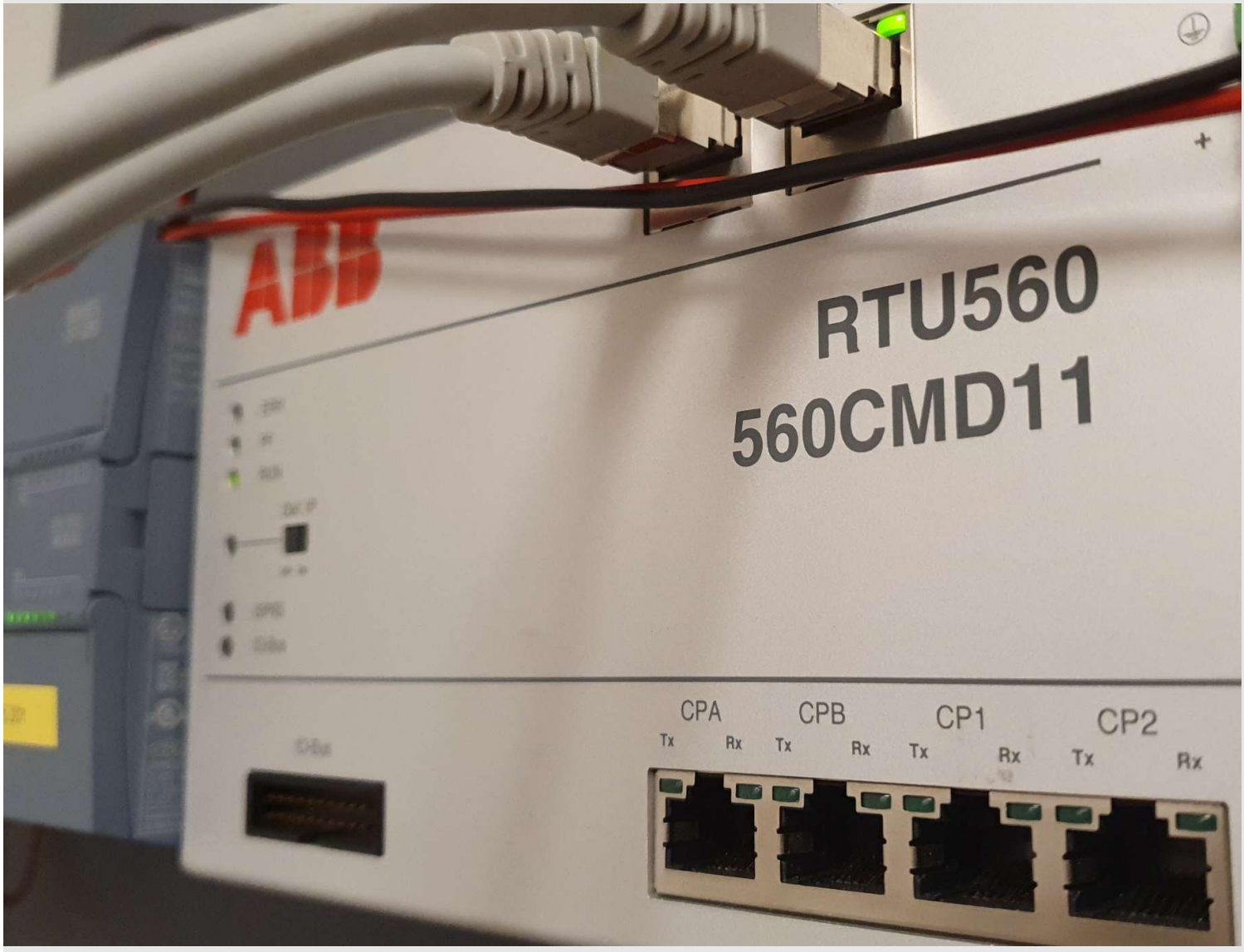
Myndigheten för samhällsskydd och beredskap

FORSKNING/STUDIE

Forskning i CRATE

Resilienta industriella informations- och styrsystem



Forskning i CRATE - Resilienta industriella informations- och styrsystem

Tidsperiod: 2015 - 2020
Utförare: Totalförsvarets forskningsinstitut
Ansvarig: Jonas Hallberg

Kort sammanfattning
Under 2016 till 2020 genomfördes projektet Industriella informations och styrsystem - NCS3 - uppstart av forskningsprogram – fortsättning. Inom projektet har forskningsplattformen RICS-el tagits fram och använts. RICS-el körs i den nationella cyberanläggningen CRATE och är en verklighetstrogen virtuell referensmiljö av de driftmiljöer som återfinns inom den svenska energiförsörjningen.

MSB:s Kontaktpersoner: Erik Sundström, 010-240 5371,

Foto omslag: Tommy Gustafsson
Text: Tommy Gustafsson och Johan Bengtsson
Tryck: DanagårdLiTHO

Publ. nr: MSB1803 – juni 2021

MSB har beställt och finansierat genomförandet av denna forskningsrapport (alt. studierapport). Författarna är ensamma ansvariga för rapportens innehåll.

Förord

I denna slutrapport beskrivs resultaten från projektet Industriella informations- och styrsystem - NCS3 - uppstart av forskningsprogram – fortsättning. Projektet har genomförts av Totalförsvarets forskningsinstitut (FOI) och har varit ett stödprojekt till forskningsprojekten CERCES (Center for Resilient Critical Infrastructures) och RICS (Resilient Information and Control Systems).

Inom ramen för projektet har forskargruppen vid FOI bland annat utvecklat en forskningsplattform samt genomfört en utforskande cybersäkerhetstävling. Utöver stödet till de två forskningsprojekten, har projektet också bidragit med kunskap till nationella och internationella cybersäkerhetsövningar såsom iPilot och Locked Shields.

Forskargruppen vill rikta ett särskilt tack till projektgrupperna CERCES och RICS för många givande samarbeten och dialoger under projektet. Forskargruppen vill också tacka ABB för att ha möjliggjort RICS-el genom att tillhandahålla hård- och mjukvara samt till ABB:s personal som har stöttat projektet med sin kunskap. Avslutningsvis vill vi tacka handläggarna på Myndigheten för samhällsskydd och beredskap (MSB) och styrgruppens medlemmar som har bistått projektet med idéer, handläggning och stöd.

Linköping, 2021-02-19

Innehåll

Sammanfattning

I denna slutrapport beskrivs resultaten från projektet Industriella informations- och styrsystem - NCS3 - uppstart av forskningsprogram – fortsättning. Projektet har genomförts av Totalförsvarets forskningsinstitut (FOI) och har varit ett stödprojekt till forskningsprojekten CERCES och RICS.

Inom projektet har forskningsplattformen RICS-el utvecklats, en referensmiljö för de driftmiljöer som återfinns inom den svenska energiförsörjningen. Plattformen är en modul i cyberanläggningen CRATE (Cyber Range And Training Environment) och har under projektet gett examensarbetare, doktorander och forskare möjligheten att genomföra avancerade experiment som leder till förbättrad cybersäkerhet för Sveriges energiförsörjning.

Den kunskap som har byggts upp inom projektet har också använts för att utveckla övningsmiljöer och scenarier i flera nationella och internationella cybersäkerhetsövningar. Under år 2020 genomfördes den utforskande cybersäkerhetstävlingen 20/20 CTF inom ramen för projektet. Vid tävlingen, som arrangerades över internet, medverkade 450 deltagare fördelade i 174 lag. Under tävlingen samlades data i form av enkätsvar och nätverkstrafik in som kan användas i framtida forskning.

Inledning

Myndigheten för samhällsskydd och beredskap (MSB) utlyste år 2014 medel för ett forskningsprogram inom området industriella informations- och styrsystem, nedan kallat forskningsprogrammet. Utöver de två forskningsprojekten *Center för resilienta kritiska infrastrukturer* (CERCES) och *Resilient Industrial Control Systems* (RICS) finansieras ett tredje projekt vid Totalförsvarets forskningsinstitut (FOI). Syftet med det sistnämnda projektet har varit att FOI ska stödja såväl utformningen som genomförandet av de båda forskningsprojekten. En speciell aspekt av detta är att ta tillvara de resultat som framkommer under forskningsprogrammet och se över hur de kan nyttiggöras inom ramen för verksamheten vid *Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet* (NSC3).

I denna slutrapport presenteras projektet som har genomförts vid FOI samt de resultat som åstadkommits inom ramen för projektet. Arbetet har genomförts enligt en årligen uppdaterad plan som har fastslagits av projektets styrgrupp och har fördelats enligt följande arbetspaket:

- Arbetspaket 1 och 2: FOI-NCS3-stöd till RICS och CERCES.
- Arbetspaket 3: NCS3-aktiviteter.
- Arbetspaket 4: Erfarenheter och rekommendationer.
- Arbetspaket 5: Network manager i CRATE.
- Arbetspaket 6: 20/20 CTF – Tillkom år 2020.

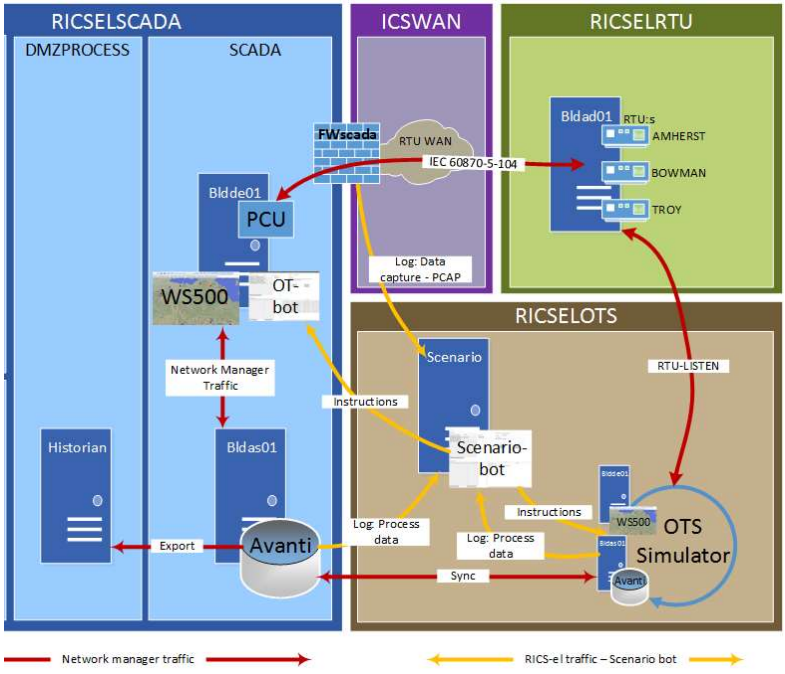
Detta arbetssätt har gjort det möjligt att kontinuerligt anpassa projektet för att hantera forskningsprojektens behov. En betydande del av arbetet inom projektet har varit att ge forskningsprojekten tillgång till cyberanläggningen CRATE samt att tillsammans med dem utveckla forskningsmiljön RICS-el. Inom ramen för projektet har också forskningsresultaten sammanställts och förmedlats till NCS3. Under år 2020 genomfördes dessutom en cybersäkerhetstävling inom ramen för projektet.

Projektresultat

I detta avsnitt presenteras resultat som har åstadkommits inom projektet. Notera att utöver nedanstående konkreta exempel har samverkan mellan FOI, de akademiska lärosätena involverade i CERCES och RICS samt industrin medfört ett betydande icke-mätbart resultat från projektet.

RICS-el

RICS-el är en forskningsplattform i den nationella cyberanläggningen CRATE och utgör en virtuell referensmiljö över de driftmiljöer som återfinns inom den svenska energiförsörjningen. Figur 1 visar hjärtat av RICS-el som är en simulerad industriell process där produktion, transmission och distribution av el hanteras med riktiga industriella informations- och styrsystemen. Precis som i en riktig driftmiljö återfinns i RICS-el både IT-system (såsom klienter och servrar) och industriella informations- och styrsystem (såsom SCADA-system och styrdatorer). Med hjälp av RICS-el är det möjligt att studera cyberangrepp och skyddsåtgärder på riktigt, men utan att riskera några allvarliga konsekvenser för samhället.



Figur 1: En översikt över segmenten i RICS-el. Röda pilar visar nätverkstrafik som relaterar till styrningen av processen och gula pilar visar data som hämtas in under forskningsförsöken.

Den industriella processen kontrolleras av ABB Network Manager – ett system för övervakning och styrning av elnät. Det standardiserade protokollet IEC 60870-5-104 används för att hantera de tre styrdatorer som finns emulerade i miljön. ABB

Operator Training Simulator används för att simulera realistiska elnätsscenarier. Ett sextiotal virtuella datorer används för att emulera den IT-miljö som omger processen i RICS-el.

Det som gör RICS-el unikt är de specialutvecklade program där det är möjligt att skapa och genomföra experiment och som sparar data från experimenten. Dessa program kallas botar. Det finns tre olika typer av botar i RICS-el: IT-botar, OT-botar och scenario-botar. IT-botar simulerar kontorspersonal som arbetar med dokument, skickar e-post och surfar på internet. OT-botar simulerar operatörer som hanterar elproduktion och eldistribution. Scenario-botar gör det möjligt att kombinera händelser i IT- och OT-botarna till en kedja av händelser som i sin tur möjliggör avancerade experiment. Efter ett genomfört experiment kan miljön enkelt återställas, händelseflödet eller dess omgivning justeras och experimentet upprepas med nya eller samma förutsättningar. I RICS-el finns fördefinierade scenarier såsom överbelastningsattacker, man-i-mitten-attacker, avancerade intrång och extrahering av data via dolda kanaler. RICS-el är således en plattform som kan användas för att studera alltifrån detaljer i protokoll till hela händelseförlopp.

Inom ramen för projektet har RICS-el använts för att skapa dataset för forskning som bedrivits inom RICS, för ett flertal examensarbeten samt för att skapa så kallade flaggor för cybersäkerhetstävlingen 20/20 CTF. Det finns även planer att i framtiden använda plattformen för att träna tekniker i incidenthantering för industriella informations- och styrsystem inom energisektorn. Det finns också planer på att nyttja plattformens förmåga för att genomföra forskning under träning och övning där personal från flera verksamhetsnivåer tränas samtidigt, exempelvis tekniker och beslutsfattare.

Uppbyggnad och nyttjande av kunskap

Uppbyggnaden av kunskap som kan nyttjas inom NCS3 och övrig verksamhet som FOI bedriver har utgjort ett stort bidrag från projektet. I första hand har den kunskap som har byggts upp genom framtagandet och nyttjandet av RICS-el använts.

Vid de nationella cybersäkerhetsövningarna iPilot 2017 och SAFE Cyber 2019 utnyttjades övningsmiljöer som baserades på RICS-el inklusive SCADA-miljön ABB Network Manager. Övningsdeltagarna fick hantera ett scenario där olika incidenter uppstod i dessa miljöer.

Vid de internationella cybersäkerhetsövningarna Locked Shields 2018 och 2019 användes kunskapen om protokollet IEC 60870-5-104 för att bygga upp den övningsmiljö och det angreppsscenario som användes under övningarna. Under år 2021 kommer denna kunskap också att användas vid genomförandet av Nationell Teknisk Övning (NTÖ).

20/20 CTF

Under hösten år 2020 genomfördes inom ramen för projektet en utforskande cybersäkerhetstävling kallad 20/20 CTF. Med utforskande menas att syftet inte endast var att arrangera själva tävlingen utan att även samla in kunskap och data för att besvara ett antal forskningsfrågor. Tävlingen genomfördes som en så kallad Capture The Flag (CTF), ett format som används för att bedöma deltagarnas färdigheter inom cybersäkerhet och hantering av IT-system. Genomförandet skedde över internet och deltagarna fick via en webbportal tillgång till ett antal uppgifter som skulle lösas inom en viss tid. I varje uppgift fanns en flagga i form av en krypterad eller på annat sätt dold textsträng. Deltagaren tilldelades poäng genom att hitta flaggan och redovisa dess innehåll via webbportalen. Det lag som hade flest poäng när tiden var slut vann.

Syftet med arrangemanget var att bygga upp kunskap om CTF-formatet, hur det kan nyttjas för att väcka intresse för cybersäkerhet och hur formatet kan användas inom ramen för forskning. Som arrangemang blev 20/20 CTF en framgång där både tekniska plattformar och uppgifter höll måttet, trots det oväntat stora antalet deltagare. Totalt kämpade 174 lag med totalt 450 deltagare för att lösa de uppgifter som tävlingsledningen vid FOI hade skapat. Baserat på lösningsgraden tillhörde ett simulerat dataläckage med hjälp av ett SCADA-protokoll och ett Bacon-chiffer de svårare uppgifterna. Den svåraste uppgiften visade sig dock vara en reverseringsuppgift för det mobila operativsystemet Android.

Under tävlingen samlades data in för framtida forskning, både i form av den trafik som genererades mot de tjänster som användes för vissa uppgifter och i form av den enkät som deltagarna besvarade. Forskarteamet bakom övningen lyckades också uppnå CTF-konceptets gyllene mått på framgång – att alla uppgifter löstes av någon, men att ingen löste alla uppgifter.

Då 20/20 CTF lockade betydligt fler deltagare än förväntat och där många deltagare i en enkät svarade att de gärna ser fler svenska CTF:er planeras en uppföljare under år 2021.

Publikationslista

Projektets uppgift har inte i första hand varit att producera egen forskning utan att stödja forskningsprojekten CERCES och RICS. Projektet har även fungerat som en länk mellan forskningsprojekten och NCS3 samt relaterad verksamhet inom FOI. Således inkluderar publikationslistan i Tabell 1 huvudsakligen dokumentation relaterat till detta stödjande arbete snarare än vetenskapliga publikationer.

Tabell 1: En lista över de publikationer som producerats under projektet.

Rapportnummer	Titel	Författare	Utgiven
FOI MEMO 5956	Forskningsbehov inom NCS3	Jonas Hallberg, Johan Bengtsson	2016-12-31
FOI MEMO 6186	Samverkan mellan NCS3 och de två forskningsprojekten RICS och CERCES	Jonas Hallberg, Johan Bengtsson	2017-11-01
FOI-S--6240--SE	RICS-El-Building a National Testbed for Research and Training on SCADA Security	Peter Andersson, Jonas Hallberg, Erik Westring, Magnus Almgren, Gunnar Björkman, Mathias Ekstedt, Simin Nadjm-Tehrani	2020-06-02
FOI MEMO 6471	Forskningsresultat från RICS och CERCES - Relevansen för NCS3 och CRATE	Johan Bengtsson, Jonas Hallberg	2018-09-21
FOI-S--6302--SE	Using serious gaming to train operators of critical infrastructure: an industry/experience report	Tommy Gustafsson, Lars Westerdahl	2019-09-23
IB-307:1/2020	20/20 CTF - En tävling i cybersäkerhet	Tommy Gustafsson	2020-08-17
IB-308:1/2020	20/20 CTF - En tävling i cybersäkerhet	Tommy Gustafsson	2020-09-03
FOI-S--6283--SE	CRATE Exercise Control - A cyber defense exercise management and support tool	Tommy Gustafsson, Jonas Almroth	2020-11-05
FOI Memo 7320	Erfarenheter kring samverkan mellan NCS3 och de två forskningsprojekten RICS och CERCES	Johan Bengtsson, Tommy Gustafsson	2020-11-05
IB-309:1/2020	Tävlingsresultat 20/20 CTF – 2020	Johan Bengtsson	2020-11-13
FOI Memo 7343	Sammanställda forskningsresultat från RICS och CERCES med relevans för NCS3 och CRATE	Tommy Gustafsson, Johan Bengtsson	2020-11-17
FOI Memo 7344	20/20 CTF	Tobias Lundberg	2020-11-17

Myndigheten för samhällsskydd och beredskap

I samarbete med:

FOI Totalförsvarets forskningsinstitut

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1803 – juni 2021