Myndigheten för samhällsskydd och beredskap

FORSKNING/STUDIE

CERCES – Center för resilienta kritiska infrastrukturer

Populärvetenskaplig slutrapport

CERCES

CERCES – Center för resilienta kritiska infrastrukturer

Tidsperiod: september 2015 – augusti 2020
Utförare: KTH
Ansvarig: Henrik Sandberg, Ragnar Thobaben, György Dán, Mads Dam

Kort sammanfattning Om komponenter som övervakar och reglerar samhällets kritiska infrastrukturer, som el- och vattennät, utsätts för cyberattacker kan stora samhällsstörningar följa. Forskare vid KTH har under fem års tid arbetat med att identifiera sårbarheter och utveckla nya säkra tekniklösningar för att stödja säkerhetsarbetet.

© Myndigheten för samhällsskydd och beredskap (MSB)
MSB:s Kontaktpersoner: Carl Önne, 010-2404249, Erik Sundström, 010-2405371

Foto omslag: CERCES logo (Design: Brinton Seashore-Ludlow)
Text: Henrik Sandberg, Ragnar Thobaben, György Dán, Mads Dam
Tryck: DanagårdLiTHO

Publ. nr: MSB1621 – oktober 2020

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

Förord

Under de senaste åren har cyberattacker mot industriell infrastruktur inträffat med stora skador och kostnader som följd. Att detta har kunnat ske beror på att en stor del av den teknik som används i samhällsviktiga verksamheter har digitaliserats. Kombinationen av digitalisering och ökad användning av it ger många fördelar men leder samtidigt till nya risker. En sådan ny risk är att komplexiteten i form av beroenden ökar. Även risken för exponeringen av system ökar när information och applikationer distribueras till fler enheter, externa organisationer och kan bli åtkomlig överallt ifrån.

Samhällsviktig verksamhet - som exempelvis elförsörjning, vattenförsörjning och transporter - är idag beroende av it. Infrastruktur och processer styrs och övervakas av sådan it som kallas industriella informations- och styrsystem, även kallade cyberfysiska system. Avbrott i denna typ av system kan leda till störningar i samhällsviktiga funktioner och även att dyrbar utrustning riskerar att förstöras. Sådana händelser kan medföra allvarliga konsekvenser för samhället. Cybersäkerhet - att införa och förvalta tillräckliga säkerhetsåtgärder för informationssystemen - är därför en fundamental förutsättning för att digitaliseringens möjligheter ska kunna tas tillvara.

På grund av komplexiteten och storleken på dessa industriella informations- och styrsystem är det svårt att skydda dem mot risker och hot som till exempel cyberattacker. Mot bakgrund av de cyberfysiska systemens centrala betydelse för samhället har MSB satsat på utveckling av kunskap om systemens sårbarheter och deras lösningar. Forskningsprojektet CERCES, som MSB har varit med och finansierat, har arbetat inom fyra områden och har gjort stora och viktiga framsteg i vilka säkerhetsåtgärder som måste stärkas för att skydda våra viktiga industriella informations- och styrsystem.

Stockholm, 2020-10-07

Åke Holmgren

Avdelningschef, avdelningen för cybersäkerhet och säkra kommunikationer

Innehåll

INLEDNING **5**
Säkerhet i inbyggda system 6
Trådlös kommunikation 6
Kommunikations- och beräkningsinfrastrukturer 6
Resilient reglering av cyberfysiska system 7

UTVÄRDERING AV CYBERSÄKERHET I INDUSTRIELLA REGLERSYSTEM **7**

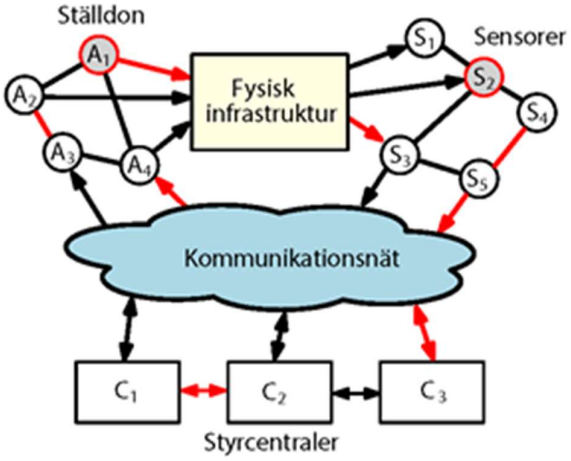
AUTENTISERING, UPPDATERING OCH VERIFIERING I TIDSKRITISKA SYSTEM **10**
Autentisering 11
Verifiering 12
Uppdatering 12

FÖRDJUPAD LÄSNING **13**

Inledning

Samhällets kritiska infrastrukturer, som elnät och andra distributionsnät, övervakas och regleras med hjälp av industriella informations- och styrsystem, även kallade cyberfysiska system. Om dess komponenter utsätts för cyberattacker riskerar det att leda till stora samhällsstörningar. Forskare inom CERCES-projektet har under fem års tid arbetat med identifiering av nya sårbarheter och utveckling av säkerhetslösningar.

Ett allt mer oroande hot är att storskaliga industriella informations- och styrsystem, som används för övervakning och reglering, utsätts för cyberattacker (se figur 1, [1] och nästa avsnitt för mer detaljer). I värsta fall kan sådana attacker leda till att kritisk infrastruktur såsom elnät och trafiksystem fallerar med stora samhällsskador som följd. Ett exempel på detta kommer från Ukraina där 30 ställverk i elnätet stängdes ner p.g.a. en cyberattack den 23 december 2015. Detta fick till följd att över 200 000 kunder förlorade tillgång till elkraft [2]. Året därpå genomfördes en än mer avancerad attack mot närliggande elnät [3]. Inom projektet CERCES studerades och motverkades denna typ av hot genom utveckling av nya praktiska och teoretiska verktyg. Projektet löpte under åren 2015-2020 och i denna rapport beskrivs några av de mer praktiskt tillämpbara resultaten.



Figur 1. Ett industriellt informations- och styrsystem för kritisk fysisk infrastruktur kan ha många komponenter och kommunikationskanaler som är känsliga för cyberangrepp (indikerade i rött). I CERCES utvecklades nya metoder för att identifiera och skydda sådana känsliga systemelement.

CERCES har varit aktivt i fyra olika teknikområden, vilket avspeglar att säkerhetshoten måste förstås och bemötas på flera nivåer parallellt. Nedan följer en kort sammanställning av arbetet i de olika teknikområdena. Därefter följer två

avsnitt som i mer detalj beskriver problemställningen, tillämpningar av arbetet och hur områdena kompletterar varandra i praktiken.

Säkerhet i inbyggda system

Vi har utvecklat nya verktyg baserade på formell logik [4] för att automatiskt, på matematiskt korrekt sätt, verifiera att program i inbyggda processorer har önskade egenskaper. Till exempel att en angripare inte kan få tillgång till en viss kritisk kryptografisk nyckel, eller att tidsgränser som är viktiga för någon styrfunktion inte överskrids [5]. Verifikationen är dock helt beroende av att modelleringen av den underliggande processorn stämmer med verkligheten. De senaste åren, med framkomsten av ett stort antal hårdvarubaserade sårbarheter såsom Spectre, Meltdown, och Foreshadow, har dock visat att vår kunskap om den faktiska processorhårdvaran är ofullständig, inte minst om s.k. caches. Konsekvensen är att säkerhetsanalysen, om den görs med enbart testning eller med formella metoder, blir felaktig. Under projektets gång har därför modelleringen och analysen av processorhårdvaran blivit en än mer viktig del av forskningsagendan, och resulterat i nya lovande modeller [6] och testmetoder [7].

Trådlös kommunikation

Vi har studerat nya typer av säkerhetslösningar för trådlös kommunikation mellan t.ex. sensorer och regulatorer. Kommersiellt tillgängliga lösningar baseras idag på kryptografi, men dessa kan i praktiken vara svåra att underhålla i ett industriellt informations- och styrsystem. Istället tittade vi på metoder som utnyttjar komponenters och överföringskanalens unika fysikaliska signaturer för att verifiera att kommunikationen är autentisk. I artikeln [8] visar vi att dessa metoder kan garantera en snabb och pålitlig autentisering och därmed klarar av kraven som ställs t.ex. inom tidskritiska tillämpningar. Artikel [9] visar dessutom på stora förbättringar om distribuerade flerantennsystem används för autentiseringen.

Kommunikations- och beräkningsinfrastrukturer

Vi har utvecklat nya säkra algoritmer och protokoll för beräkning i, och kommunikation över, delade infrastrukturer som t.ex. molntjänster. Nya typer av angrepp mot tidssynkroniseringsprotokoll har identifierats, till exempel genom tillgång till switchar i kommunikationsnätet. Nya metoder har utvecklats för detektion av och försvar mot sådana angrepp, genom statistisk analys av mätdata och tidssynkroniseringssignaler, med tillämpning inom t.ex. synkronmätningar i elnät. Vidare har resilient allokering av s.k. virtuella regulatorer för processtyrning studerats. Artiklarna [10] och [11] beskriver arbetet i detalj och inkluderar pekare till ytterligare material.

Resilient reglering av cyberfysiska system

Vi har utvecklat nya metoder för att matematiskt modellera stora cyberfysiska system inklusive olika typer av cyberattacker. Med hjälp av modellerna kan vi effektivt lokalisera särskilt sårbara komponenter (t.ex. ställdon och sensorer) och kanaler i industriella informations- och styrsystem. Sårbarhet i detta sammanhang innebär att en cyberattack kan resultera i stor fysisk skada. Vidare har metoder för kostnadseffektiv allokering av försvarsmekanismer (t.ex. mjuk- och hård-varuredundans) och design av anomalidetektorer tagits fram. Med hjälp av dessa ökas systemets resiliens, d.v.s. dess tålighet och förmåga att återhämta sig efter störningar. Doktorsavhandlingen [12] beskriver och sammanfattar arbetet i detalj och innehåller referenser till forskningsartiklar den är baserad på.

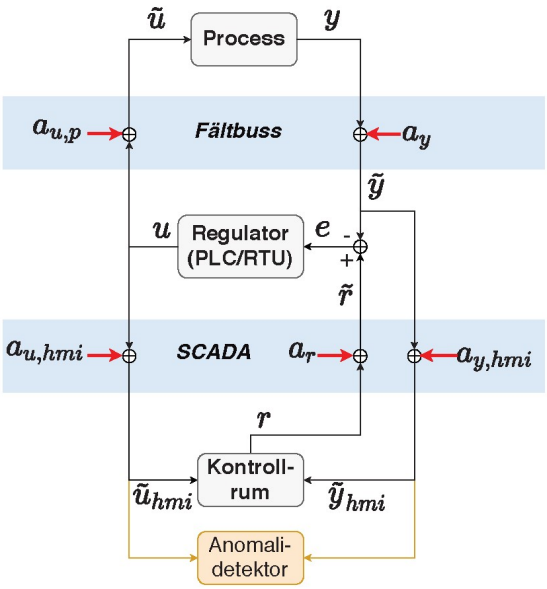
Utvärdering av cybersäkerhet i industriella reglersystem

En öppet tillgänglig simuleringsmiljö har utvecklats för att studera effekten av olika försvarsstrategier i industriella informations- och styrsystem.

Industriella informations- och styrsystem är komplexa infrastrukturer som består av lager av IT-system och fysikaliska processer, se figur 2 och [1]. Systemens roll är att se till att fysikaliska *processer* i t.ex. elnät, vattendistribution och tillverkningsindustri beter sig på önskat vis och inte är en fara för sin omgivning. Fysikaliska processer, t.ex. generation av elkraft, förekommer normalt i en osäker omgivning där t.ex. kunders utnyttjandegrad varierar över tid på ett mer eller mindre oförutsägbart vis. För att ändå se till att processer levererar enligt givna specifikationer används ofta en återkopplingsmekanism där en *regulator* kontinuerligt mäter processens egenskaper och automatiskt korrigerar dess inställningar, se figur 2. Exempelvis så ökas automatiskt elproduktionen i ett elnät om kunders effektuttag ökar. Detta för att hålla elnätets spänning och frekvens på en acceptabel nivå. Reglering så som denna sker ofta över ett datanätverk – en s.k. *fältbuss* (fieldbus) – och regulatorn implementeras då ofta som mjukvara i s.k. PLC (Programmable Logic Controller) eller RTU (Remote Terminal Unit).

Som illustreras i figur 2 kan en cyberattack mot reglersystem innebära manipulation av mätningar eller automatiska inställningar. Man behöver inte ha mycket fantasi för att förstå att sådan manipulation kan få allvarliga följder för den fysikaliska processen och dess omgivning. Detta bekräftades i den s.k. Stuxnet-incidenten 2010 [13] där centrifuger i en urananrikningsanläggning utsattes för ett cyberangrepp och

ett flertal enheter förstördes. I själva verket har incidenter såsom denna motiverat mycket av arbetet i CERCES.

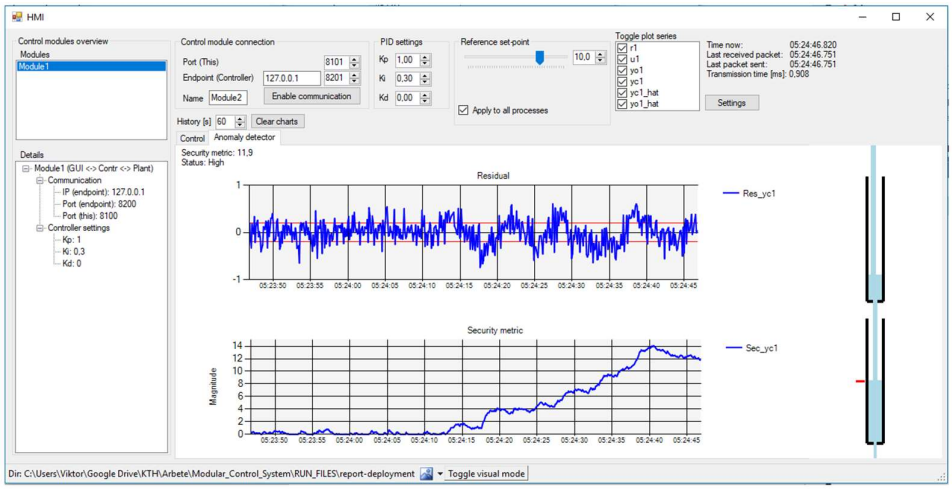


Figur 2. Blockschemat illustrerar hur olika komponenter i ett förenklat industriellt reglersystem kommunicerar och hur potentiella cyberattacker (i rött) kan komma in och störa signalvägar och enheter på olika nivåer. En process' mätsensor kan t.ex. blockeras genom att en angripare injicerar stor mängd data i fältbussen (en s.k. överbelastningsattack). (Adapted/Translated by permission from Springer Nature: Springer eBook [14], © Springer Nature Switzerland AG 2020)

Industriella reglersystem är ofta storskaliga och består av ett stort antal fysikaliska processer och regulatorer. För att övervaka och koordinera dessa används ytterligare ett datanätverk – s.k. *SCADA-system* (Supervisory Control And Data Acquisition) – för att samla in mätdata till och distribuera styrkommandon från ett kontrollrum. I kontrollrummet övervakar operatörer driftläget. Precis som fältbussen kan SCADA-systemet också utsättas för cyberangrepp. I flera dokumenterade fall har angreppen utgått från oskyddade datorer i kontrollrummet och använt SCADA-systemet för att nå ut till de fysikaliska processerna, se [2] och [13]. Till sin hjälp att detektera attacker och fel kan operatörerna använda s.k. *anomalidetektorer* som med hjälp av t.ex. matematiska modeller, regler och AI kan generera alarm om data avviker från förväntade samband och mönster. Inom CERCES har vi bl.a. utvecklat metoder för att hitta och utvärdera inställningar för sådana detektorer [12].

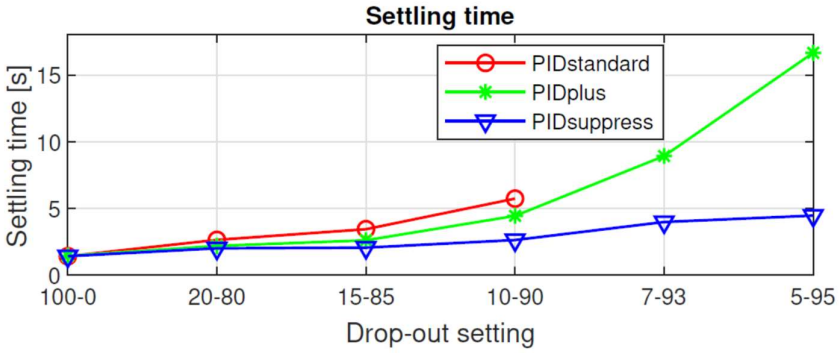
Det kan i praktiken vara mycket svårt att utvärdera potentiella effekter av cyberangrepp och säkerhetsmekanismer i stora industriella informations- och styrsystem. Systemen är ofta komplexa och det kan vara svårt, dyrt eller bryta mot säkerhetsföreskrifter att genomföra fingerade angrepp. För att bistå användare utvecklade vi inom CERCES en testmiljö där industriella reglersystem, fysikaliska processer, angrepp och säkerhetsåtgärder kan simuleras [14]. Ramverket och användarmanual finns fritt tillgängliga. I figur 3 visas ett exempel på hur

operatörsgränssnittet ser ut under en simulerad överbelastningsattack (DoS-attack) mot en mätsensor i regleringen av en vätsketankprocess.



Figur 3. Simulerat operatörsgränssnitt med anomalidetektor under en överbelastningsattack. Signalen "Residual" är ett mått på avvikelse över tid från förväntade mätvärden från den fysikaliska processen. En viss avvikelse förekommer alltid p.g.a. modellfel och störningar men när angreppet startar vid tidpunkten 05:24:10 kan man notera en ökad magnitud som är än mer tydlig i signalen 'Security metric' (en kumulativ summa [CUSUM]) som till slut genererar ett alarm i kontrollrummet [14].

Ett exempel på hur verktygen kan användas för att utvärdera angrepp och försvar visas i figur 4. I [14] beskrivs tre olika algoritmer för att implementera en s.k. PID-regulator som ofta används i reglering av fysikaliska processer. Man kan fråga sig hur känsliga dessa olika implementeringar är mot överbelastningsattacker av varierande intensitet. Resultatet visas i figur 4, där man tydligt kan jämföra de olika algoritmerna och dra slutsatsen att PIDsuppress är den minst känsliga. PIDsuppress är en s.k. händelsestyrd regulator och togs även den fram inom ramen för CERCES.



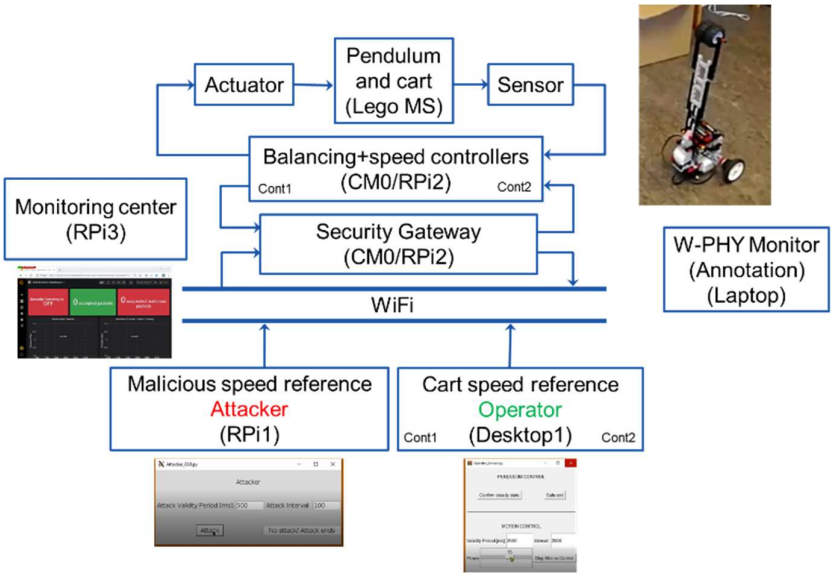
Figur 4. Tre olika PID-algoritmer jämförs under varierande intensitet i en överbelastningsattack [14]. Intensiteten växer längs x-axeln (100-0=inget angrepp, 5-95=max angrepp). Som mått på inverkan på den fysikaliska processen används här insvängningstiden ("Settling time" längs y-axeln) vilket mäter hur lång tid reglersystemet svänger efter en störning. En kort insvängningstid tyder på ett välfungerande system och

därmed är PIDsuppress den algoritm som är minst påverkad av angreppet. (Reprinted by permission from Springer Nature: Springer eBook [14], © Springer Nature Switzerland AG 2020)

Autentisering, uppdatering och verifiering i tidskritiska system

En viktig aspekt vid övervakning och styrning av fysikaliska processer är att de kan vara tidskritiska. Med detta menas att motåtgärder måste sättas in snabbt efter det ett angrepp inletts för att förhindra skador. Givet systemens komplexitet är detta en stor utmaning och CERCES har därför testat nya tekniker i en testbädd.

Trådlös kommunikation är en attraktiv, flexibel lösning i och med att man kan undvika höga kostnader för kablar och underhåll. Trådlös kommunikation kan t.ex. användas i kommunikationen mellan kontrollrum, regulatorer, sensorer och ställdon (se figur 1 och 2). En säkerhetsutmaning är att trådlös kommunikation sker över ett delat medium, vilket förenklar och möjliggör nya attacker. T.ex. kan en störsändare blockera kommunikationen mellan två enheter. Särskilt utmanande är att använda trådlösa kanaler i övervakning och styrning av tidskritiska fysikaliska processer som lätt fallerar vid störningar. För att studera säkerhetslösningar i en trådlös miljö utvecklade CERCES en testbädd, se figur 5.

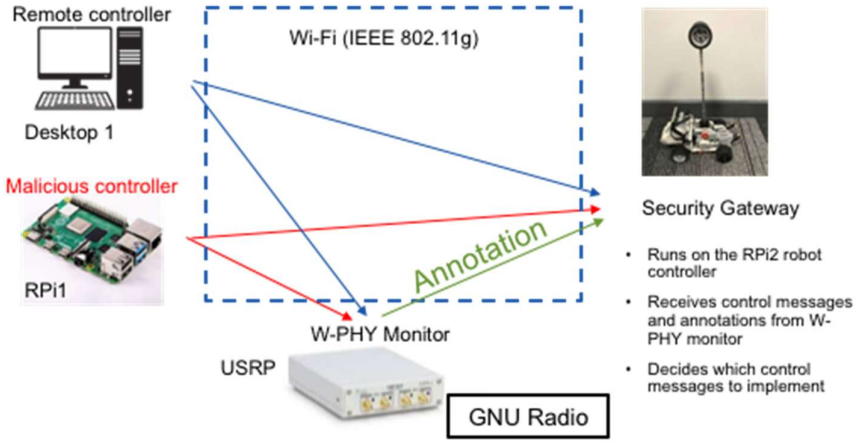


Figur 5. Blockschemat illustrerar alla komponenter och kommunikationsvägar i CERCES' trådlösa testbädd.

Som tidskritisk fysikalisk process valdes en elmotordriven vagn med en inverterad pendel. På vagnen finns två regulatorer som dels balanserar pendeln och dels ser till att vagnen rör sig med föreskriven hastighet. Dessa regulatorer antar rollen en PLC har i ett industriellt reglersystem (jfr figur 2). I testbädden motsvaras kontrollrummet av en desktop-PC som kommunicerar trådlöst (över Wi-Fi) med regulatorerna på vagnen. I PC:n kan man ställa in önskad vagnhastighet som skickas till vagnen, men även ta emot sensorvärden och visa för operatören. En attack kan få vagnen att välta t.ex. genom att skicka manipulerade trådlösa kommandon. Vi har i denna miljö studerat tre olika attackscenario och motsvarande lösningar.

Autentisering

För att visa att komponenters och kanalens fysikaliska egenskaper lämpar sig för en snabb och pålitlig autentisering och filtrering av trådlösa kommandon har CERCES implementerat en Wi-Fi-monitor (W-PHY Monitor i figur 5) baserad på en experimentell USRP-radioplattform. Egenskaperna som används för att skilja legitima kommandon från en attack består av frekvensförskjutningar vid mottagaren (som är typisk för sändaren) och dämpningen (som är typisk för överföringskanalen), se figur 6. Baserat på en statistisk modell beräknar W-PHY Monitor attacksannolikheten för varje mottaget datapaket. Våra experiment bekräftar att denna metod är pålitlig och snabb. I de genomförda experimenten lyckades attackeraren inte med att skicka in falska kommandon och därmed inte med att välta vagnen. Den uppmätta fördröjningen låg på endast 20 ms. Vi förväntar oss att fördröjningen ytterligare kan reduceras i en kommersiell implementering.



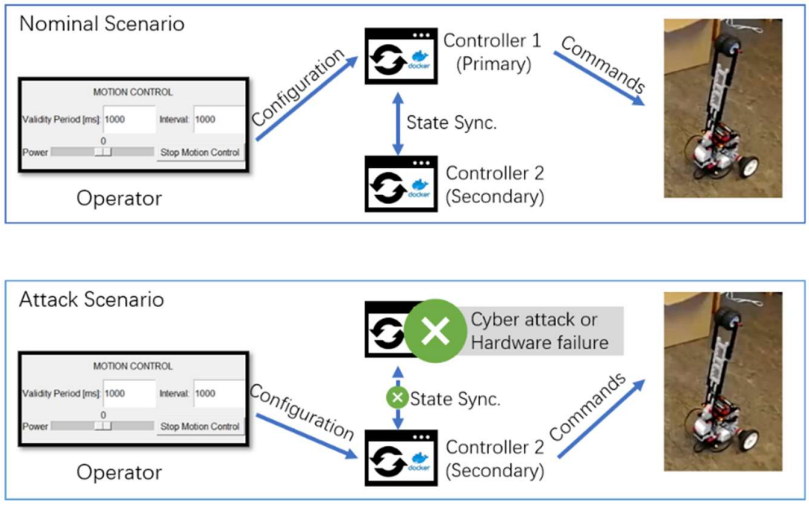
Figur 6. W-PHY monitorn inspekterar alla datapaket över Wi-Fi-nätverket och flaggar (”annotation”) misstänkt kommunikation.

Verifiering

I CERCES-testbädden demonstrerar vi även verifikation av kod på binär nivå. Som exempel studerar vi verifikation av exekveringstidsgränser. Detta är viktigt i säkerhetssammanhang eftersom variationer i tidsförbrukning i princip kan användas till att läcka kryptografisk information, och specifikt för testbädden, eftersom regleringen är tidskritisk. Vi kan därmed garantera vid en uppdatering av styrprogrammet att de säkerhetskritiska tidsgränserna respekteras. Vi har implementerat styrprogrammet på en processor (Cortex-M0) där en klockcykelexakt formell modell finns tillgänglig. Analysen använder sig av s.k. symbolisk exekvering där en enkel exekvering av en symbolisk modell kan motsvara en mycket stor mängd exekveringar i den fysiska processorn.

Uppdatering

Under de senaste åren har virtualisering lett till en omvandling av mjukvaruindustrin och den är nu på väg att förändra även processindustrin. I ett virtualiserat reglersystem kan regulatorer implementeras i form av virtualiserad mjukvara och kan därmed köras i olika plattformar i nätverket. I testbädden körs kontrollrummet som en virtualiserad process. Den implementerar algoritmer och protokoll för att demonstrera hur nedsatt prestanda i regulatorprocessen kan upptäckas och hur regulatorn kan startas om på en annan plattform vid behov, utan att den fysiska processen påverkas. Lösningen är baserad på två komponenter, å ena sidan pågår det en kontinuerlig synkronisering av information mellan en huvudregulator och en reservregulator, å andra sidan använder vi algoritmer som vi har utvecklat för effektiv placering och flytt av virtualiserade regulatorer, se figur 7.



Figur 7. När huvudregulatorn utsätts för anfall kan den snabbt ersättas av en reservregulator utan att den fysikaliska processen påverkas.

Fördjupad läsning

Innehållet i denna rapport baseras på de vetenskapliga artiklar som forskningsprojektet har skrivit och fått publicerat.

[1] ”Vägledning till ökad säkerhet i industriella informations- och styrsystem”, MSB, 2014 (Länk: https://www.msb.se/ribdata/filer/pdf/27425.pdf)

[2] ”Cyber-Attack Against Ukrainian Critical Infrastructure”, CISA, US Department of Homeland Security, 2016 (Länk: https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01)

[3] “'Crash Override': The Malware That Took Down a Power Grid”, Wired, 2017 (Länk: https://www.wired.com/story/crash-override-malware/)

[4] A. Lindner, R. Guanciale, R. Metere, “TrABin: Trustworthy analyses of binaries”, Science of Computer Programming vol. 174, pp. 72-89, 2019

[5] R. Guanciale, H. Nemati, M. Dam, C. Baumann, “Provably secure memory isolation for Linux on ARM”, Journal of Computer Security, 2016

[6] R. Guanciale, M. Balliu, M. Dam, “InSpectre: Breaking and Fixing Microarchitectural Vulnerabilities by Formal Analysis”, to appear in Proc. 2020 ACM Conference on Computer and Communications Security, 2020

[7] H. Nemati, P. Buiras, A. Lindner, R. Guanciale, S. Jacobs, “Validation of Abstract Side-Channel Models for Computer Architectures”, Proc. 32nd International Conference on Computer Aided Verification, CAV, pp. 225-248, 2020

[8] H. Forssell, R. Thobaben, H. Al-Zubaidy, J. Gross, "Physical layer authentication in mission-critical MTC networks: A security and delay performance analysis", IEEE Journal on Selected Areas in Communications, vol. 37, no. 4, pp. 795-808, 2019

[9] H. Forssell, R. Thobaben, J. Gross, "Performance analysis of distributed SIMO physical layer authentication", in Proc. IEEE International Conference on Communications (ICC), 2019

[10] P. Zhao, G. Dán, "A Benders Decomposition Approach for Resilient Placement of Virtual Process Control Functions in Mobile Edge Clouds", IEEE Trans. on Network and Service Management, vol. 15., no. 4., pp. 1460-1472, 2018

[11] E. Shereen, M. Delcourt, S. Barreto, G. Dán, J.-Y. Le Boudec, M. Paolone, "Feasibility of Time Synchronization Attacks against PMU-based State-Estimation", IEEE Trans. on Instrumentation and Measurement, vol. 69., no. 6., pp. 3412-3427, 2020

[12] J. Milosevic, "Security metrics and allocation of security resources for control systems", doktorsavhandling, KTH, 2020 (Länk: diva2:1411558)

[13] K. Zetter, "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon", Crown, 2014

[14] V. Tuul, H. Sandberg, "Testbed Evaluation of DoS Attacks on PID-controllers", in: Nadjm-Tehrani S. (eds) Critical Information Infrastructures Security. CRITIS 2019. Lecture Notes in Computer Science, vol. 11777. Springer, Cham., 2020 (Länk: https://doi.org/10.1007/978-3-030-37670-3_17)

Myndigheten för samhällsskydd och beredskap

I samarbete med:

© Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1621 – oktober 2020