Säkra leverantörskedjor för styrsystem

ERIK ZOUAVE, MARGARITA JAITNER

FOI-R--4759--SE
ISSN 1650-1942 Mars 2019

Erik Zouave, Margarita Jaitner

Säkra leverantörskedjor för styrsystem

Titel	Säkra leverantörskedjor för styrsystem
Title	Secure supply chains for ICS
Rapportnr	FOI-R--4759-SE
Månad	Mars
Utgivningsår	2019
Antal sidor	52
ISSN	1650-1942
Kund	MSB
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr	E13641
Godkänd av	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Sammanfattning

En tydlig trend inom inköp, utveckling och drift av industriella informations- och kontrollsystem (ICS) är att leverantörerna representeras av ett stort antal specialister. Detta leder till komplexa leverantörskedjor, vilket innebär ett antal risker för ett ICS, operatören och den övriga verksamheten. Likaså tyder påvisade cyberincidenter på behovet av att ta itu med säkerheten i leverantörskedjorna. Denna rapport inventerar och kategoriserar åtgärder som kan genomföras för att säkra leverantörskedjorna. Rättsliga ramverk samt branschens ”bästa praxis”, så som standarder och vägledningar, utgör underlaget som används för att identifiera sådana åtgärder. Rapporten föreslår dessutom en generisk modell för den typiska livscykeln av ett ICS för att demonstrera när åtgärderna bör genomföras. Många av åtgärderna bör vara på plats redan tidigt i anskaffningsprocessen, medan andra bör genomföras under ett senare skede i ett ICS livscykel. Rapporten konstaterar att åtgärderna som fastställs i de rättsliga ramverken och branschpraxisen kan delas in i fyra kategorier. Dessa kategorier är: utredning av förhållandet mellan operatören och leverantören; genomförande av relevanta analyser; etablering av policy och åtgärdsplaner; samt specificering av säkerhetskrav.

Nyckelord: ICS, SCADA, cybersäkerhet, leverantörskedjor

Summary

Examining the recent trends in industrial control systems (ICS) sourcing and maintenance, a trend towards complex supply chains is detectable. Complex supply chains can pose a number of risks to operators of ICS and their ventures. Further, recently surfaced incidents that involve suppliers, further put supply chain security in focus within the area of cyber security. Based on a number of legal stipulations, norms, and industry best practices and advisory documents, such as standards and guidelines, this report compiles and categorizes activities aimed at securing supply chains for ICS. The report also establishes a generic model representing a typical lifecycle for an ICS. The model presents the phases in which the various activities for securing the supply chain should take place. Many of the activities are to be carried out prior to acquisition of an ICS, whilst others are in focus at different stages throughout the lifetime of an ICS. The report suggests that the chosen legal stipulations and best practices include four main areas of measures that can be carried out in order to secure supply chains. These areas are: defining of the relationship between the operator and the supplier; carrying out required analyses; establishing policy and action plans; and specifying security requirements.

Keywords: ICS, SCADA, supply chain security, cyber security

Innehållsförteckning

1 Inledning

För att ett industriellt informations- och styrsystem (Industrial control system, ICS) ska vara så säkert som möjligt krävs att varje kugge i leverantörskedjan håller en hög nivå i säkerhetsarbete. Ett helt system riskerar bli sårbart om en leverantör brustit i sitt säkerhetsarbete under en produkts framställning och styrsystemets livscykel. Detta ställer krav på leverantörer, på operatörer och inköpare av de industriella informations- och styrsystem.

Myndigheten för samhällsskydd och beredskap (MSB) konstaterar i *Vägledning till ökad säkerhet i industriella informations- och styrsystem* från 2014 att upphandling av industriella informations- och styrsystem har blivit allt mer komplicerad. Enligt Vägledningen har detta delvis att göra med att inköpare ofta möter flera representanter för samma leverantör, var och en med sin specialitet. Tidigare mötte inköpare vanligen en representant som hade kunskap om ett helt system. Att detta förändrats, troligen med hänsyn till systemens ökade komplexitet, försvårar för inköparen av ett ICS att förstå helheten i systemen och därmed att kunna bedöma hur säkert systemet är. I förlängningen riskerar detta att öka osäkerheten och sårbarheten i systemet.

För inköparna av ICS försvåras processen ytterligare av att leverantörerna i sin tur vanligen förlitar sig på underleverantörer för att kunna leverera sina produkter. Det kräver mer av inköparen, som måste förstå komplicerade leverantörskedjor och delvis kunna bedöma om en leverantörs underleverantörer och tillverkare är att anse vara pålitliga. Detta är särskilt viktigt med tanke på att det yttersta ansvaret för informations-, nätverks- och cybersäkerhet vanligen tillfaller operatörer, vilka driftsätter system utan att nödvändigtvis ha insyn i leverantörskedjan bortom förstahandsleverantörer. [1] Reglering, vägledning, standarder och rekommendationer utformas ofta utifrån grundläggande antaganden om att operatörerna äger systemen och är de som först reagerar på en incident, och därför bör åläggas ansvaret för säkerheten. [1]

Flera incidenter har påvisat att grundläggande antaganden om riskfördelning och om de hot och sårbarheter som kan påverkan leverantörskedjan, från leverantör till operatör, behöver omvärderas. Ett exempel är de attacker cyberspionagegruppen Dragonfly, även känd som Energetic Bear, Havex och Croaching Yeti, utfört. Gruppen har varit aktiv sedan 2011 och har bland annat utsatt aktörer inom energisektorn för attacker genom att angripa leverantörernas system och ersätta den genuina styrsystemsmjukvaran med en version som även innehöll skadlig kod. Genom att attackera leverantörer lyckades gruppen även göra skada hos operatören. [2]

Ett annat exempel på att grundläggande antaganden om riskfördelning, hot och sårbarheter kan behöva omprövas, är fall där leverantören kan ha otillbörliga

syften bortom sin verksamhet som leverantör. Med anledning av detta har ett flertal amerikanska underrättelsetjänster varnat för användningen av vissa kinesiska leverantörers produkter och tjänster, då dessa kan utgöra en säkerhetsrisk på grund av företagens kopplingar till den kinesiska staten. [3]

Det kan alltså konstateras att leverantörskedjan och relationen mellan leverantör och operatör har blivit allt mer komplicerad och att det finns ett antal grundantaganden om hot och sårbarheter som kan behöva omprövas. Det är därför nödvändigt att utreda vilka regleringar, standarder, vägledningar och rekommendationer som finns för att vägleda operatörer (och leverantörer) av industriella informations- och styrsystem. Även ansvarsfördelningen mellan operatör och leverantör behöver klargöras för att ytterligare stärka säkerheten i leverantörskedjan.

1.1 Syfte och målsättning

Målsättningen med denna studie är att den ska vara ett kompletterande underlag till MSB:s *Vägledning till ökad säkerhet i industriella informations- och styrsystem* för säkerhet inom leverantörskedjor (Supply Chain Security) i samhällsviktig verksamhet som använder sig av ICS. Därmed stödjer studien även MSB:s arbete med den nationella satsningen på ökad säkerhet i cyber-fysiska system enligt *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019-2022*.

För att uppnå denna målsättning kartlägger studien existerande säkerhetsåtgärder, presenterar en generisk modell för vilka säkerhetsåtgärder som bör implementeras i vilken fas av ett styrsystems livscykel, och förtydligar ansvarsförhållanden mellan operatör och leverantör inom leverantörskedjan. Den innehåller rekommendationer för hur säkerheten i leverantörskedjor för industriella informations- och styrsystem kan förstärkas genom ett styrsystems hela livscykel.

1.2 Frågeställningar

Frågorna som besvaras i denna rapport är:

- Vad innebär leverantörskedjan för säkerheten i industriella informations- och styrsystem?
- Vilka säkerhetsåtgärder finns det och hur kan de användas för samhällsviktiga verksamheter som använder ICS?
- Vilka rekommendationer kan ges till operatörer av ICS för att undvika osäkerhet i leverantörskedjan?

1.3 Metod

Studien grundas på analys av branschpraxis, såsom standarder och vägledningar, samt av rättsliga dokument. För att genomföra analysen har en generisk livscykelmodell skapats för att beskriva ett typiskt styrsystems livscykel. Rekommendationer för åtgärder har främst hämtats ur:

Gällande rätt för informations-, nätverks- och cybersäkerhet. I synnerhet *direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-Direktivet)* och *lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster* till den mån de är normerande för varför operatörer bör vidta säkerhetsåtgärder, hur de bör vidta dem, vem de bör samarbeta med och under vilka principer säkerhetsåtgärder och säkerhetssamarbete bör utformas. Det gäller även *COM(2017) 477 (”Cyber Security Act”)* som fastställer framtida standardisering, ackreditering och certifiering av informations-, och kommunikationsteknologi (IKT) och som skulle medföra att systemoperatörer kan bedöma cybersäkerheten i IKT-produkter och tjänster enligt ett harmoniserat europeiskt format. Båda rättsakterna analyseras också för att förtydliga kontexten, det normativa värdet och möjliga framtida förutsättningar för att utveckla bästa branschpraxis för säkerhet i Europa. Dessa lagar är utvalda för att deras säkerhetskrav kan generaliseras till system i all samhällsviktig verksamhet och därför också är tillämpbara i denna kontext.

Bästa branschpraxis i form av vägledningar och standarder. De vägledningar studien främst bygger på är MSB:s *Vägledning till ökad säkerhet i industriella informations- och styrsystem* och FRA:s *Åtgärdsförslag: Angrepp via tjänsteleverantörer* då dessa utformats av svenska myndigheter med relevant mandat och ansvar för en svensk kontext. Studien använder sig även av vägledningar som utvecklats av andra relevanta aktörer, såsom Europeiska unionens byrå för nät- och informationssäkerhet (ENISA), och ett fåtal myndigheter i andra europeiska länder. Även om det potentiellt sett finns många standarder med rekommendationer som går att tillämpa på säkerhet i leverantörskedjan, bygger den här studien främst på ISO/IEC 27035 som är en standard för förhållanden mellan operatör och leverantör samt på IEC 62443 som är en standard för generaliserade åtgärder riktade till både operatörer och leverantörer i leverantörskedjan.

1.4 Avgränsningar

Studien syftar till att ge en grundläggande överblick av säkerhet i leverantörskedjorna för industriella styrsystem och gör inget anspråk på att vara heltäckande.

Begreppet säkerhet är mycket brett. Denna studie begränsar sig till de aspekter som kan tillskrivas cyber- eller informationssäkerhet. Frågor som rör informationen som tillhandahålls, bearbetas och förs in och ut ur systemet är i

fokus för denna studie. Säkerhetsaspekter inom leverantörskedjan som inverkar på koncept, byggande och drift av ett ICS är också relevanta för denna studie. Frågor om råvaror, förbrukningsmaterial eller dylikt ligger utanför denna studies avgränsning, lika så fysisk säkerhet eller personsäker under leverans.

Det bör noteras att studien inte gör någon skillnad mellan ägaren och operatören av ett ICS, men har genomförts ur ett perspektiv där operatören är den aktör som har det slutliga ansvaret för systemet. I de fallen där en distinktion mellan ägaren och operatören behöver göras, bör de resultat som studien levererar analyseras ytterligare för att kunna göra en gränsdragning över ansvarsområden.

1.5 Definitioner

Risk är ett av de centrala begreppen för denna studie. Det är dock ett begrepp som kan betyda olika saker beroende på kontext. Standardfamiljen ISO 31000, till exempel, definierar risk som ”osäkerhet och effekten av denna på uppsatta mål” [4]; [5] och avser därmed inte själva sannolikheten för en händelse utan potentialen att nå en effekt på verksamhetens mål. Effekten i sin tur kan vara både positiv eller negativ. En sådan definition kan anses vara problematiskt då den går emot gängse uppfattning att begreppet risk övervägande är associerat med ett negativt utfall.

NIS-direktivet, som avser att etablera en hög gemensam nivå på säkerhet i nätverk och informationssystem inom EU och på så sätt är normetablerande, ger en annorlunda syn på innebörden av begreppet risk. Enligt direktivet omfattar risker för informations-, nätverks- och cybersäkerhet rimliga omständigheter och händelser som kan identifieras och som skulle medföra potentiell negativ inverkan på säkerheten i nätverks- och informationssystem. [1]; [6].

Hedtjärn Swaling föreslår att risk kan definieras som en sannolikhetsbedömning av att ett hot kan realiseras, till exempel genom att sårbarheter i ett system exploateras, och därmed negativt påverkar ett skyddsvärde. [7] Kombinationen av skyddsvärden, sårbarhet, och ett hot kan vara en särskilt lämplig modell för risk vid bedömning av antagonistiska hot. [8]. Definitionen bedöms som lämplig för denna rapport.

1.6 Disposition

Inledningsvis ges en kortfattad beskrivning av hotbilden mot leverantörskedjor för ICS. Eftersom rapporten har för avsikt att föreslå åtgärder utifrån de olika stegen som ett ICS genomgår under sin användningstid, introducerar det tredje kapitlet en generisk modell som beskriver en typisk livscykel av ett ICS. I kapitel fyra presenteras en kortfattad genomgång av för området relevanta regleringar, standarder och andra säkerhetskrav. Kapitlet ger även viss inblick i branschpraxis

och några aktörers rekommendationer. Kapitel fem presenterar en genomgång av de säkerhetsåtgärderna som identifierades under studiens gång. Kapitlet ger även rekommendationer gällande ansvarsförhållanden mellan operatör och leverantör av ICS, vilka analyser som bör genomföras, innan anskaffning samt ytterligare organisatoriska och administrativa aspekterna som bör tas i beaktande för att säkra leverantörskedjorna. I samma kapitel presenteras under vilket skede i livscykeln de olika åtgärderna bör genomföras samt i vilken del av livscykeln effekterna av dess åtgärder förväntas uppträda. Det sjätte och avslutande kapitlet sammanfattar rapporten.

2 (O)säkerhet i leverantörskedjan

Industriella informations- och styrsystem präglas av teknisk komplexitet samt mycket varierande ägar- och driftsförhållanden. För att hantera utmaningarna på området krävs ett samlat arbete som inkluderar både privat och offentlig sektor. Arbetet behöver bedrivas kostnadseffektivt och sektorsövergripande. För att uppnå ett adekvat skydd finns det ett behov av ökad samverkan och samarbete mellan systemleverantörer, tekniska konsulter, upphandlare, operatörer, relevanta myndigheter och akademiska miljöer [9].

Säkerhet i leverantörskedjan för industriella informations- och styrsystem är ett strategiskt nationellt säkerhetsintresse. Detta bekräftas av ovanstående citat ur den svenska Nationella strategin för samhällets informations- och cybersäkerhet. Säkerhet börjar inte med operatörerna som sätter styrsystem för samhällsviktig verksamhet i drift och slutar inte heller när produkten lämnar systemleverantörens faciliteter. Ytterst är säkerhet ett delat ansvar där flera aktörer samverkar under ett systems livscykel.

Styrsystem är i många avseenden mycket specifika. De har en förhållandevis lång livstid som sträcker sig över flera generationer av vanliga operativsystem, med en mängd substantiella modifikationer under denna livstid. Det kan också handla om mycket komplexa, skräddarsydda system med eller utan användning av COTS (Commercial-off-the-shelf) komponenter, det vill säga sådana som kan köpas på marknaden i kontrast till egen eller specialutvecklade komponenter. Det handlar även om att industriella informations- och styrsystem i grunden är en del av cyberfysiska system där fel snabbt kan resultera i fysiska konsekvenser som i värsta fall kan ha negativ påverkan på samhället.

Det finns ett flertal tillvägagångssätt för att beskriva och kategorisera potentiella hot mot ICS. Till exempel listar NIST:s [1] *Special Publication 800-82:2, Guide to Industrial Control Systems (ICS) Security* potentiella hot kategoriserat utifrån deras ursprung, det vill säga aktören eller mekanismen bakom hotet. Kategoriseringen samt på vilket sätt hotet kan uppkomma via leverantörskedjan återges i Tabell 1.

[1] National Institute of Standards and Technology (NIST) är en amerikansk federal myndighet som bl.a. har i uppdrag att ta fram standarder.

Tabell 1. Typer av hot mot ICS

Typ av hot	Exempel	Beskrivning	Relevans för säkerhet i leverantörskedjan
Antagonistisk	Individ, grupp eller statlig aktör så som exempelvis missnöjd anställd, konkurrent, (under)leverantör.	Antagonistiska aktörer söker att exploatera organisationens (samhällets) beroende av tjänsten som levereras med hjälp av ICS.	Leverantören själv kan uppträda som en antagonistisk aktör, t.ex. kan f.d. missnöjda anställda använda sig av sin åtkomst till ICS och ICS-nära system för att hämnas på sin arbetsgivare. Alternativt kan leverantören bli ett medel för att nå operatören.
Oavsiktlig	Användare, administratör.	Vanliga misstag som sker inom ramen för användare och administratörs vanliga verksamhet.	Relevansen uppstår när leverantörens personal är verksamma mot ICS och näraliggande systemen, t.ex. vid systemunderhåll.
Strukturell	Systemets komponenter, t.ex. lagring, kommunikation, sensorer, strömförsörjning.	Fel på hård- och mjukvara, exempelvis på grund av åldring och andra aspekter utanför den vanliga driften.	Leverantör kan vara delaktig genom att leverera felaktig hård- och mjukvara, försenas i leverans av uppdatering eller genomfört undermåliga tester innan driftsättning.
Miljö	Naturolyckor och olyckshändelser orsakade av människan.	Påverkan som ligger utanför operatörens kontroll.	Vid extraordinära händelser kan varu- och tjänsteleverans eller drift stanna av.

Osäkra leverantörskedjor kan alltså äventyra ett styrsystems säkerhet ur ett flertal perspektiv där angriparen intar olika positioner i förhållandet till leverantören och de vägar angriparen utnyttjar för att komma åt systemet. Leverantören kan själv stå bakom angreppet genom att, med eller utan uppsåt, presentera intrångsvägar in i operatörens styrsystem. Amerikanska säkerhetstjänster har med anledning av detta varnat för användning av produkter och tjänster som levereras av vissa teknikföretag med hänvisning till företagens nära relationer till stater som ur ett amerikanskt perspektiv betraktas som antagonistiska. I synnerhet kinesiska och ryska företag har pekats ut. Exempelvis har kinesiska Huawei och ryska Kasperski exkluderats från statliga upphandlingar i USA.

Med tanke på mängden olika komponenter i ett it-system, och i styrsystem i synnerhet, är svaret sällan så pass enkelt som att undvika vissa leverantörer. De vardagliga COTS-systemen innehåller en uppsjö av komponenter från en svåröverskådlig mängd leverantörer, men även vid specialtillverkning förlitar sig leverantörerna ofta på delkomponenter från flertalet underleverantörer.

En ytterligare utmaning är att leverantören själv kan bli föremål för ett angrepp som infekterar kunders system. Ett sådant fall, ”Cloud Hopper” eller APT 10, där den skadliga koden har levererats till slutmålet via riktat nätfiske (spear phishing) mot ett antal tjänsteleverantörer. Detta tillvägagångssätt kan delvis jämföras med insiderhot, det vill säga de fall då angriparen har legitimt tillgång till leverantörens gränssnitt mot operatörens styrsystem.

Ett annat exempel på angrepp via leverantör är kryptomasken NotPetya som under 2017 fick spridning i ett antal länder, i synnerhet Ukraina och USA. I detta fall hade uppdateringsmekanismen för det ukrainska skattebokföringsprogrammet M.e.Doc förändrats till att installera maskens skadliga kod istället för att genomföra en autentisk uppdatering. En vanlig uppfattning är att attacken riktade sig mot ukrainska företag, en uppfattning som bara är delvis korrekt eftersom system långt utanför Ukrainas gränser också blev infekterade. Ett av de mest uppmärksammade offren var danska Maersk, för vilket attacken fick stora konsekvenser [11]. I efterhand konstaterade säkerhetsföretag och den officiella ukrainska utredningen att leverantören av M.e.Doc gravt misskött de egna systemen – bland annat hade man sedan 2013 underlåtit nödvändiga uppdateringar och månaderna före attacken hade man utsatts för ett antal intrång [12].

Styrsystem har vanligtvis en mycket lång livslängd som inbegriper ett flertal uppdateringar och modifieringar. Detta ställer ytterligare krav på leverantörerna som bör ha förmåga att långsiktigt kunna tillhandahålla tjänster för styrsystem eller kunna vidareföra kunskap inför en förnyelse av systemet. Detta beroende är förstås ytterligare en osäkerhet för operatörerna att ta hänsyn till i förhållande till leverantörskedjor.

De här ovan presenterade säkerhetsutmaningarna påvisar att det finns ett antal scenarion där leverantören kan ha en negativ inverkan på säkerheten i ett ICS. Det är därför relevant för operatören av ett ICS att analysera och utvärdera sina leverantörer och deras respektive underleverantörer i förhållande till de potentiella risker de kan utgöra.

3 ICS livscykel – en generisk modell

You know you're getting old when you start replacing control systems that you designed/installed earlier in your career [13].

Det finns ett stort antal modeller för att illustrera ett informations- och styrsystems livscykel. En av de mest grundläggande i detta sammanhang är Systems Development Life Cycle (SDLC) som genom sin generella utformning är användbar för att illustrera många olika sorters system. Modellen är cyklisk och sträcker sig över faserna planering, analys, design, implementering och underhåll. Antalet faser och benämningar på dessa beror på systemets användningsområde. Den används bland annat som en modell för utveckling av individuell mjuk- eller hårdvara, men även för system. Modellen är i grunden tillräckligt generisk och skalbar för att kunna användas i ICS-sammanhang. Samtidigt är den inte specifikt anpassad för att illustrera de aspekter som urskiljer ett ICS från vanliga it-system.

Brittiska Centre for the Protection of National Infrastructure (CPNI)[2] använder en egenframtagen livscykelmodell som är specifikt anpassad till ICS. Modellen bygger på fyra generella faser: koncept (design), konstruktion (build), drift (operation) och avveckling (decommissioning). Dessa faser innehåller sedan ett antal aktiviteter för att exempelvis kunna tydliggöra tidpunkter då systemet och kringliggande planering kan (eller bör) verifieras och kontrolleras. Dessa kan ses som en barriärfunktion för att säkerställa att systemet är i fas.[14]

3.1 Livscykelmodellen för ICS

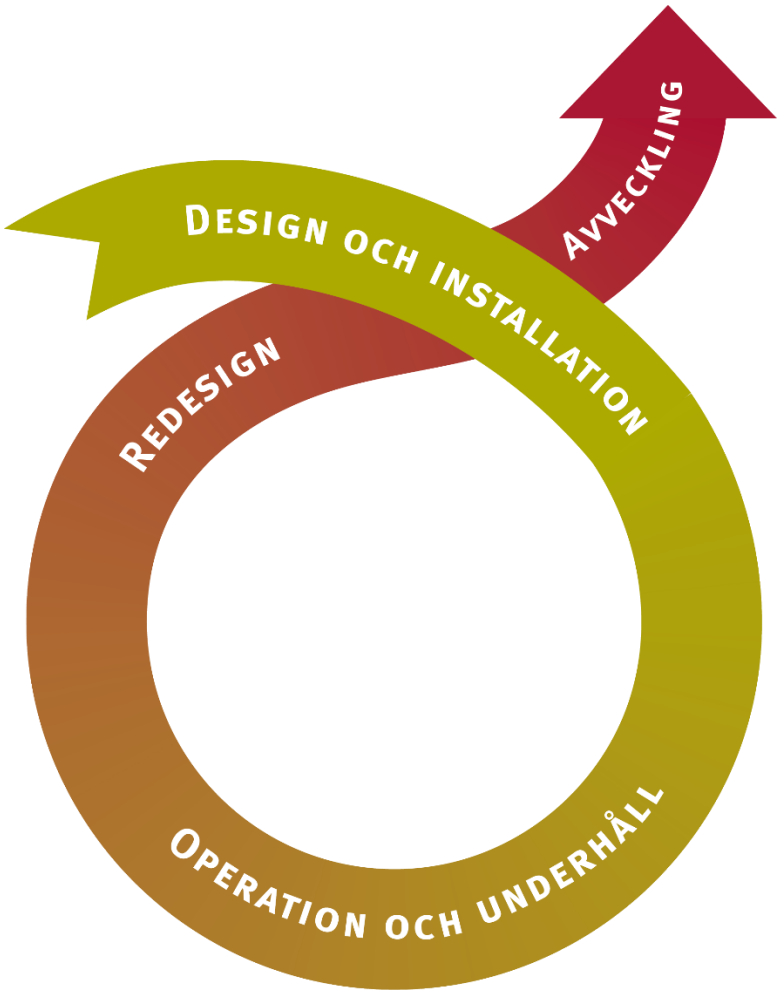
Eftersom leverantörskedjan och relationen mellan operatör och leverantör av ICS är i fokus för denna studie, behövdes det en analysmodell som kan användas cykliskt eller linjärt och beaktar att ett ICS kan genomleva ett större antal iterationer med uppgraderingar och anpassningar. Den föreslagna modellen tar också hänsyn till att även avveckling av systemet kräver en riskanalys.

Modellens grundläggande faser liknar ovan beskrivna modeller. Ett system planeras, konstrueras och installeras. Därpå följer en fas av drift och underhåll som därefter övergår till en ”redesign”-fas. I ”redesign”-fasen måste operatören ta beslut om huruvida systemet ska modifieras och uppgraderas eller avvecklas. Ett antagande är att ett ICS kommer genomgå cykeln ett flertal gånger innan systemet till avvecklas. Modellens faser presenteras översiktligt i Figur 1.

Design och installationsfasen påbörjar ett ICS livscykel. Vanligtvis genomförs följande steg: En behovsanalys genomförs utifrån en kort- och långsiktigplanering

[2] Del av Communications-Electronics Security Group (CESG) inom UK Government Communications Headquarters (GCHQ)

och ett koncept för det blivande ICS skapas. Konceptet utvecklas till en preliminär design som därefter byggs på med allt fler detaljer. Systemet byggs antigen med hjälp av COTS-komponenter eller som en hybrid av specialtillverkade och standardiserade komponenter. Systemet installeras på plats och dess funktionalitet testas. Leverantörens roll i processen kan exempelvis bero på den blivande operatörens behov, kompetenstillgång och marknadsläge.



Figur 1. Generisk livscykelmodell för ICS

Efter att nödvändiga tester har genomförts driftsätts systemet. Därmed övergår det i enlighet med modellen till nästa fas – *operation och underhåll*. Underhåll säkerställer systemets funktionalitet och innefattar systemuppdateringar och incidenthantering. Beroende på systemets egenskaper och organisatoriska aspekter kan även vissa modifieringar betraktas som en del av operations- och underhållsfasen.

Leverantörer kan på olika sätt vara involverade även i denna fas. Till exempel kan operatören välja att lägga ut delar av underhållet på en eller flera leverantörer eller välja att enbart införskaffa uppdateringar av mjukvara från leverantören. I vissa fall är leverantören även involverad i vidareutveckling av systemet.

Efter en tid åldras vanligtvis ett ICS. Detta kan innebära att systemet inte längre kan uppfylla de krav som omvärlden ställer på det – det kan handla om ny teknologi, att kapacitetsbehovet har växt eller att systemet behöver säkras mot en ny typ av säkerhetshot. Om systemet inte avvecklas går det in i en fas av *redesign*. Den fasen kan innebära att några eller alla steg som den ursprungliga designfasen innehöll genomförs. I ett sådant scenario avslutas fasen med test och driftsättning, för att sedan återgå till operation och drift-fasen som ett ”redesignat” system. Det finns ingen definitiv gräns för när en uppgradering av systemet bör betraktas som en redesign. Därför bör gränssättningen åligga operatören, eventuellt i samråd med leverantören eller leverantörerna. En viktig skillnad gentemot ordinarie drift är att systemet kan betraktas som ”nytt” efter avslutad redesign och återinstallation.

Då ett styrsystem vanligen har en lång livslängd genomgår det ett flertal iterationer av livscykeln innan de slutligen bedöms som föråldrat eller av någon annan anledning tas ur drift. Likt de andra faserna kan *avvecklingsfasen* se olika ut beroende på exempelvis verksamhetsområde, organisation och systemets utformning. Det finns ingen given modell för hur ett system ersätts eller avvecklas utan detta kan variera.

Vid fullständig avveckling av ett system kan det finnas behov av att inkludera cybersäkerhetsaspekter, både från operatören och leverantörens sida. Exempelvis kan system under avveckling innehålla känslig information, exempelvis på systemets lagringsmedia. Även själva systemet och dess uppbyggnad kan avslöja aspekter av operatörens verksamhet och leverantörens förmågor. Exempel på information som kan avslöjas är kunskap- och kompetensnivå bland personal, verksamhetsprocesser av känslig natur eller annan information som kan vara av intresse för en illasinnad aktör eller konkurrent.

4 Regleringar, standarder och säkerhetskrav

Säkerhet och hantering av risker och incidenter i nätverk och informationssystem har i Sverige hittills reglerats tematiskt, sektoriellt och utifrån specialfall. Ikraftträdandet av *direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet)* innebär en mer övergripande och enhetlig säkerhetsreglering för alla samhällsviktiga tjänster inom EU. *Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster* tillämpar direktivet inom Sverige för att åstadkomma en mer enhetlig nationell säkerhetslagstiftning över de samhällsviktiga sektorerna och skapar därmed en gemensam standard mellan leverantörer för samhällsviktiga tjänster.

Innan NIS-direktivet reglerades olika relaterade säkerhetsproblem:

- särskilt för allmänna och elektroniska kommunikationssystem genom lag (2003:389) om elektronisk kommunikation samt Post- och telestyrelsens föreskrifter om krav på driftsäkerhet (PTSFS 2015:2)
- övergripande för personuppgiftsbehandling genom personuppgiftslagen (1998:204) som ersatts av förordning 2016/679 (GDPR)
- myndigheters informationssäkerhet genom MSB:s föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet, MSBFS 2016:1
- vid bevakningsansvariga myndigheter och höjd beredskap genom förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (KBF)
- incidentrapporteringsansvar har reglerats genom förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap avseende rapportering mot MSB, säkerhetsskyddsförordningen (1996:633) avseende rapportering mot Säkerhetspolisen och Försvarsmakten, lag (2003:389) om elektronisk kommunikation, lag (2007:528) om värdepappersmarknaden och i den kommande regleringen i direktiv (EU) 2015/2366 av den 25 november 2016 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (det andra betaltjänstdirektivet).

Dessa regleringsformer omfattar inte samhällsviktig verksamhet på ett enhetligt sätt. På EU-nivå har det därför genomförts flera initiativ, som till exempel programmet för skydd av kritisk infrastruktur (EPCIP) och inrättandet av ett nätverk för varningar om hot mot kritisk infrastruktur (CIWIN) samt en plan för kritisk informationsinfrastruktur för att skapa en mer samspelt syn på säkerhet [15], [16] 2008 antog man också *direktiv 2008/114/EG 2008 om identifiering av,*

och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna för att harmonisera identifieringen av kritisk infrastruktur mellan medlemsstaterna och säkerhetsbehoven utifrån en gemensam begreppsapparat avseende:

a) kritisk infrastruktur: anläggningar, system eller delar av dessa belägna i medlemsstaterna som är nödvändiga för att upprätthålla centrala samhällsfunktioner, hälsa, säkerhet, trygghet och människors ekonomiska eller sociala välfärd och där driftsstörning eller förstörelse av dessa skulle få betydande konsekvenser i en medlemsstat till följd av att man inte lyckas upprätthålla dessa funktioner[…]

b) riskanalys: övervägande av relevanta hotbilder, för att bedöma sårbarhet och potentiella konsekvenser av driftsstörning eller förstörelse av kritisk infrastruktur

c) känslig information om skydd av kritisk infrastruktur: uppgifter om kritisk infrastruktur som, om de avslöjas, skulle kunna användas till att planera och agera för att förorsaka driftsstörning eller förstörelse av kritisk infrastruktur

d) skydd: all verksamhet som syftar till att säkerställa funktion, kontinuitet och okränkbarhet hos kritisk infrastruktur, för att avskräcka, lindra och neutralisera ett hot, en risk eller sårbarhet.

Ur både det svenska lagrummet och de europeiska initiativen kan utrönas att säkerheten i samhällsviktig verksamhet har två grundlager; säkerheten i fysiska system och den logiska säkerheten i informationssystem. Inom viss samhällsviktig verksamhet tillkommer även den personella säkerheten, det vill säga skyddet av personuppgifter, som är mindre framstående just vid skyddet av styrsystem där personuppgifter inte är lika vanligt förekommande som i andra anslutna system som operatörer har. Det personella skyddet förekommer även i NIS-direktivet i den mån det reglerar störningar som påverkar användare av samhällsviktiga tjänster och den allmänna säkerheten.

Regleringarna och de europeiska initiativen har i stort haft den gemensamma utgångspunkten att krav på säkerhet främst ska ställas på leverantörerna som använder sig av informationssystem och nätverk. Detta var en tydlig utgångspunkt för direktiv 2008/114/EG som befäste att ”[d]et yttersta ansvaret för skyddet av europeisk kritisk infrastruktur vilar på medlemsstaterna och infrastrukturens ägare/operatör.” Leverantörer av industriella styrsystem och deras säkerhetsansvar var inte en utgångspunkt i denna utveckling av normer. Normer kring säkerhet i leverantörskedjan har snarare utvecklats genom säkerhetsstandarder som IEC 62443, ackreditering och certifiering som riktar sig mot en bredare mottagargrupp, det vill säga mot operatörer och (under)leverantörer av ICS.

I relation till standardiseringsarbetet innebar EU-insatserna sektorsspecifika samförståndsavtal om utvecklingen av gemensamma standarder [15]. Vad gäller regleringen av standardisering har denna utformats separat genom *förordning (EU) nr 1025/2012 om europeisk standardisering* [17] som fastställer bestämmelser för samarbetet mellan europeiska standardiseringsorganisationer, nationella standardiseringsorgan, medlemsstater och kommissionen. Just i fallet cybersäkerhet föreskriver Europeiska kommissionen ett standardiserings-, ackrediterings- och certifieringssystem för informations och kommunikations-teknologier (IKT) mer generellt, och i styrsystem specifikt genom COM(2017) 477 (”Cyber Security Act”). [18]

4.1 NIS-direktivet

NIS-direktivet fastställer åtgärder för att uppnå en hög nivå på säkerhet i nätverks- och informationssystem hos samhällsviktiga tjänster och digitala tjänste-leverantörer, såväl privata som offentliga, inom EU. Direktivet inbegriper en harmonisering av ländernas säkerhetsreglering och skapar en enhetlig förståelse kring vissa nyckelbegrepp inom nätverk och informationssäkerhet. [1]

Begreppet *säkerhet i nätverks- och informationssystem* syftar till systemens förmåga att med en viss tillförlitlighetsnivå stå emot åtgärder med negativ inverkan på tillgängligheten, integriteten eller konfidentialiteten hos behandlade uppgifter eller de (samhällsviktiga) tjänsterna systemen möjliggör.

Säkerhetsperspektivet i NIS-direktivet är mer övergripande än tidigare då det är neutralt avseende huruvida händelsen som resulterade i en störning eller negativ inverkan är avsiktlig, oavsiktlig, fysisk, logisk, orsakad av naturfenomen eller dylikt. [1]

Direktivet presenterar vissa säkerhetskrav för operatörer. Dessa inbegriper ändamålsenliga och proportionerliga tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem. Åtgärderna ska vara lämpliga i relation till risker eller incidenter. [1] Således medför direktivet en hög grad av subjektivitet för operatörer att själva bedöma lämpligheten av tekniska åtgärder för deras verksamhet. Som klargörs i direktivet, ”bör [direktivets krav på säkerhet] inte innebära krav på att någon särskild kommersiell informations- och kommunikationsteknisk produkt utformas, utvecklas eller tillverkas på ett visst sätt.” [1]

Direktivet utgår däremot från att valet av säkerhetsåtgärder ska ta hänsyn till diverse säkerhetsstandarder [1][3]. Således kan NIS-direktivets implementering komma att bidra till att standarder, som IEC 62443, får större normativt värde som

[3] Direktivet tar sin definition av standarder och deras olika format ur förordning (EU) nr 1025

ett mått på lämpligheten, ändamålsenligheten och proportionaliteten av åtgärder. Direktivet framhåller också betydelsen av frivillig branschpraxis för att anpassa säkerhetsåtgärder till risker. [1] Övergripande kan konstateras att NIS-direktivet inte syftar till detaljerad rättslig reglering av inbyggd säkerhet i system så mycket som att främja befintlig, marknadsdriven bästa praxis för säkerhetsåtgärder. [1]

Förhållandet till standardisering betonas också särskilt av regeringen i propositionen till lag (2018:1174). I Sverige ska myndighetsföreskrifter främja användningen av sådana standarder och specifikationer, vilket innebär att standardiseringsfrämjandet ytterligare institutionaliseras [19]. Enligt propositionen ska leverantörer beakta standarder för att åstadkomma ett systematiskt, riskbaserat, långsiktigt, metodiskt och kontinuerligt säkerhetsarbete. [19]

Slutligen kan noteras att direktivet återskapar de tidigare utgångspunkterna med ett säkerhetsansvar som är riktat mot leverantörer av samhällsviktiga tjänster, det vill säga operatörer av ICS, snarare än tillverkare. Direktivet tilldelar inte heller ansvar för säkerheten i hur system har tillverkats. [1] Direktivet uppmuntrar leverantörer av samhällsviktiga tjänster att upprätta *informella samarbets-mekanismer* för säkerhet och ett bredare samarbete med *berörda parter* [1]. Att *hårdvarutillverkare* och *mjukvaruutvecklare* inte spelar en viktig roll för säkerheten hos tjänsteleverantörerna reflekteras i Skäl 50 av direktivet som också låter påskina att dessa omfattas av befintliga bestämmelser och produktansvar utanför direktivet.

4.2 Cyber Security Act

COM(2017) 477 (”Cyber Security Act”), antagen av EU december 2018, tar vid där NIS-direktivet slutar genom att ta sikte just på informations- och kommunikationsprodukter och tjänster samt inbyggd säkerhet (”security-by-design”). Rättsakten ska skapa en hög nivå av cybersäkerhet, (cyber)-motståndskraft och förtroende för IKT-produkter och tjänster inom unionen. [18] Vidare ska den möjliggöra för systemoperatörer att bedöma säkerheten i IKT-produkter och tjänster redan vid anskaffning enligt kriterier som gäller för hela EU. NIS-direktivet och COM(2017) 477 kan kontrasteras som presenterat i Tabell 2.

Tabell 2. Jämförelse av ansats till branschpraxis och inbyggd säkerhet i NIS-direktivet och Cyber Security Act

NIS-direktivet	**Cyber Security Act**
Främjar bästa praxis inom ramen för industristandard i samhällsviktig verksamhet.	Främjar inbyggd säkerhet i ett bredare spektrum av IKT, inklusive IKT-tillämpning inom samhällsviktig verksamhet.

Rättsakten innebär att unionen därmed också antar sin första bindande ansats till cybersäkerhet. Ansatsen till cybersäkerhet är holistisk och omfattar all verksamhet som krävs för att skydda nätverks- och informationssystem (definierat enligt NIS-direktivet), användare och personer som påverkas av cyberhot. Cyberhoten består av alla potentiella omständigheter eller händelser som kan ha negativ inverkan på ovanstående system, användare och personer. [18]

COM(2017) 477 anger två tillvägagångssätt för att förstärka cybersäkerhet inom unionen. Först förstärker den ENISA:s organisation och mandat. Sedan (och i och med denna förstärkning) inrättar den ett europeiskt system för certifiering av cybersäkerhet i IKT-produkter och tjänster. [18] Det senare är särskilt relevant för denna studie, särskilt i den mån förslaget etablerar en process med minimikrav för säkerhetscertifiering.

Certifieringen i sig är en oberoende och formaliserad utvärdering av IKT-produkter och tjänster som genomförs av ackrediterade organ. [18] Systemet ska harmonisera och effektivisera det som för närvarande är ett lapptäcke av olika nationella certifieringsmekanismer bland de europeiska medlemsstaterna. Konkret kommer detta innebära att gemensamma regler, tekniska krav och standarder inom hela EU säkerställs med ett ackrediteringssystem på unionsnivå. [18]

Det europeiska cybersäkerhetscertifieringssystemet skulle därigenom kunna:

- etablera en process för att utveckla cybersäkerhetscertifiering (artikel 44)
- bedöma säkerheten utifrån ett antal konkreta målsättningar (minimikrav på inbyggd säkerhet) (artikel 45)
- bedöma säkerheten utifrån ett antal säkerhetsnivåer (”assurance levels”) (artikel 46)
- bedöma att cybersäkerhetscertifiering följer vissa formatkrav angående, till exempel, dokumentation och regler (artikel 47)
- ackreditera av nationella organ för att bedöma nationell konformitet mot ovanstående krav (artikel 51).

De aspekter som berör inbyggd säkerhet, det vill säga minimikraven för inbyggd säkerhet och säkerhetsnivåerna, är särskilt relevanta för en analys av möjliga säkerhetsåtgärder riktade mot leverantörskedjan för styrsystem.

4.3 Branschpraxis

Idag finns det en stor mängd standarder för styrsystemssäkerhet och leverantörskedjor. [20] Två illustrativa exempel är det europeiska standardiseringsorganen CEN, verksam inom generell teknisk standardisering, och ETSI, verksam inom telekommunikationsstandardisering - i respektive standardiseringsorgans katalog finns 778 respektive 6542 standarder som innefattar begreppet ”supply chain”, dvs. leverantörskedja. För att ytterligare försvåra för leverantörer och operatörer har specialiserade standarder även olika

definitioner på vad som bör räknas till ”säkerhet i leverantörskedjan” med varierande grad av detalj och styrning.

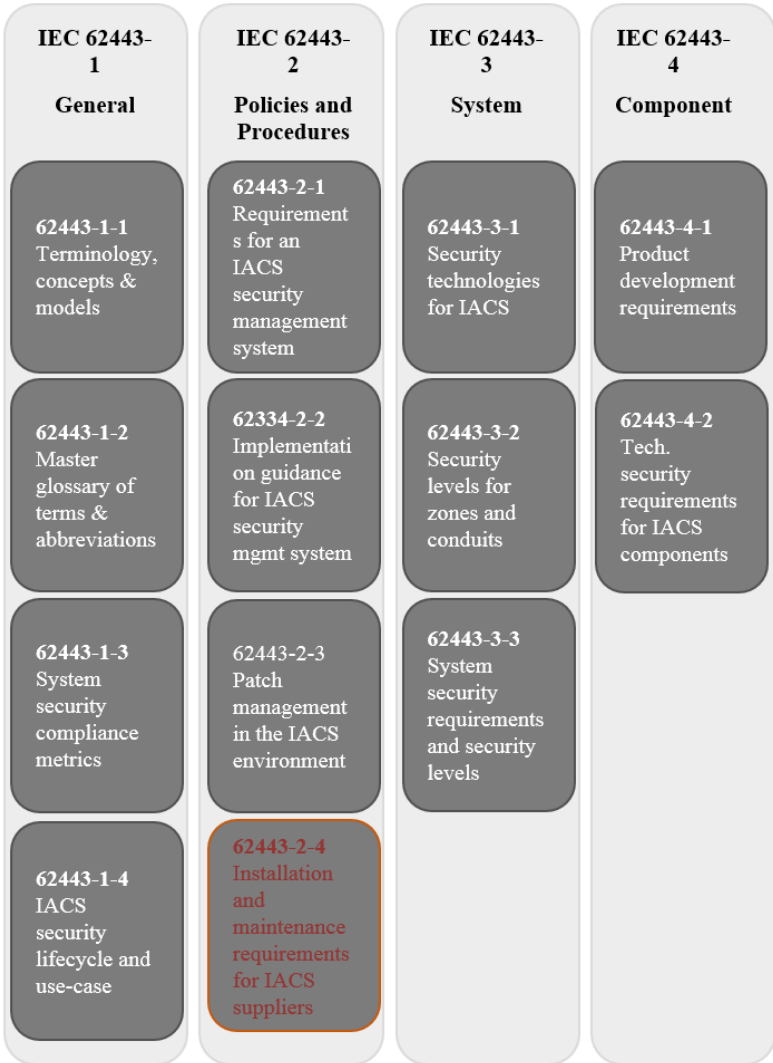
Bland de standarder och vägledningar som den här studien bygger på förekommer följande ansatser till säkerhet i leverantörskedjan:

- **ISA/IEC 62443 –** har en övergripande ansats som riktar sig till tillverkare, tjänsteleverantörer och operatörer av styrsystem
- **ISO/IEC 27036-3** – har en ansats som riktar sig mot förhållandet mellan operatörer och leverantörer
- **ISO 28000:2007** – fokuserar på leverantörskedjorna ur ett lednings- och kontrollsystemsperspektiv
- **MSB:s** *Vägledning till ökad säkerhet i industriella informations- och styrsystem*
- **FRA:s** *Åtgärdsförslag: Angrepp via tjänsteleverantörer*
- **CPNI** *Good Practice Guide Process Control and SCADA Security* **–** har en ansats där operatören är kravställare för leverantörens säkerhet.

Utöver att aktörer inom leverantörskedjan möter betydande utmaningar i att identifiera de för dem viktigaste lärdomarna att dra från det stora utbudet av standarder, kan det stora antalet standarder motverka en effektiv implementering av normerande säkerhetsåtgärder och försvåra för beslutsfattare och lagstiftare att föreslå policys och styrdokument.

4.3.1 ISA/IEC 62443

Standardserien IEC 62443 riktar sig till operatörer och leverantörer av ICS. Ursprungligen skapades standardserien av International Society for Automation, ISA, och publicerades som ANSI/ISA-99, där ANSI står för American National Standards Institute. Numreringen anpassades sedan till nomenklaturen bruklig för International Electrotechnical Commission (IEC) och vidareutvecklas som IEC 62443. Standardseriens struktur introduceras i Figur 2.



Figur 2. IEC 62443 – Standardseriens struktur, 62443-2-4 fokuserar på leverantören

Serien består av fyra övergripande delar som definierar begrepp och mått (*General*), policyer och procedurer (*Policies and procedures*), krav på systemets design och säker integration (*System*) samt produktutvecklingskrav och specifikationer för ICS-komponenter (*Component*). Varje del består av två till fyra standarder som behandlar olika säkerhetsaspekter relevanta för ICS.

Standarden 62443-2-4 *Installation and maintenance requirements for IACS suppliers*, som ingår i standardseriens andra del och således fokuserar på policys, fokuserar på relationen mellan operatören och leverantören. Standarden anger ett

antal olika säkerhetsnivåer, eller mognadsgrader, som bygger på varandra. Standarden är bland annat tänkt att användas vid upphandlingar av ICS-lösningar och tjänster [21]. Även standardens fjärde del, som behandlar krav på komponenter, kan vara av intresse för en leverantör. Den fjärde delen föreslår bland annat en säker produktutvecklingslivscykel för att skapa system präglade av ”security by design”. Den innehåller även detaljerade tekniska krav på komponenter.

4.3.2 ISO/IEC 27000

ISO/IEC 27000 är en serie av säkerhetsstandarder som riktar sig till organisationer som bedriver sin verksamhet med hjälp av it-infrastruktur. Serien innehåller rekommendationer för bästa praxis inom ramen för informationssäkerhets-hanteringssystem (Information Security Management System – ISMS) med hänsyn till bland annat administration, organisation, kravställning och risk-hanteringen för it-system. En fördel med serien är att den är så pass omfattande och flexibel att den kan anpassas till olika typer av verksamheter. Till dato inbegriper serien över 40 separata standarder. I Sverige utvecklas respektive standardserien av Svenska institutet för standarder (SIS).

Standardserien riktar sig inte specifikt mot operatörer av ICS. Istället är det en vanlig uppfattning att denna serie, på grund av sin fokus på vanlig IKT, har mindre relevans för ICS. [21] [22] Det finns dock anledning att studera standardseriens resonemang om relationen mellan operatör och leverantör, vilket är relevant även för ICS. Vissa standarder inom serien behandlar aspekter av relationen mellan operatör och leverantören inom en specifik åtgärd, exempelvis vid incident-hantering. Fyra standarder inom serien är särskilt intressanta i relation till förhållandet mellan operatör och leverantör:

- **ISO 27036-1** behandlar ämnet övergripande och introducerar ett antal koncept för hur relationen kan hanteras
- **ISO 27036-2** introducerar en rad krav för en fungerande relation
- **ISO 27036-3** presenterar en vägledning för säkerhet inom leverantörskedjorna för IKT
- **ISO 27036-4** vägleder för fungerande relationer specifikt med leverantörer av molntjänster.

4.3.3 ISO 28000:2007

Standarden ISO 28000 (även ISO 28000:2007) ”Security Management System for the Supply Chain” är relevant för ökad säkerhet inom leverantörskedjan. Standarden fokuserar främst på hur lednings- och kontrollsystem kan utvecklas för att uppnå förbättrad kontroll av transportflöde och en säker ledning av

internationella leveranser. Standardserien består av fem standarder, varav en delas upp i ytterligare fyra delar:

- **ISO 28000** innehåller specifikationer om rutinerna för säkerhet i leverantörskedjan
- **ISO 28001** innehåller bästa praxis för säkring av leverantörskedjan, bedömningar av och planer för detsamma
- **ISO 28002** syftar till att utveckla leverantörskedjans resiliens
- **ISO 28003** definierar krav på organisationer som certifierar och/eller granskar standardens implementering
- **ISO 28004:1, 28004:2, 28004:3, 28004:4** ger vägledning till implementering av standarder anpassad för exempelvis småföretag.

En av seriens huvudbudskap är att implementationen ger organisationerna förmåga att kontinuerligt följa upp sina skyddsåtgärder. Standarden fokuserar dock i mångt och mycket på fysisk säkerhet.

4.3.4 Vägledningar

Många organisationer som har till uppgift att främja och värna styrsystemens säkerhet har utvecklat vägledningar inom ramen för sitt uppdrag. I detta avsnitt behandlas två vägledningar, ett holistiskt riskhanteringsramverk och CIP-013-1.

Det holistiska ramverket *Holistic Risk Managment Framework* (HRM) bygger på den brittiska regeringens Security Policy Framework. [23] Fokus för ramverket är att skydda tillgångar (människor, information, infrastruktur, faciliteter) och tjänster på ett proportionerligt sätt som stödjer snarare än stör verksamheten.[23]

Ramverket identifierar sju prioriterade områden där en riskhanteringsplan behövs: (1) ledning, (2) identifiering av tillgångar, (3) säkerhet för personal, (4) cybersäkerhet, (5) fysisk säkerhet, (6) sabotage och (7) beredskapskrav. Det finns ett ömsesidigt beroende mellan de olika delarna: en sårbarhet i ett område kan påverka en annan, och därför förespråkas en holistisk syn. Ramverket presenteras översiktligt i Figur 3.

Figur 3. Det integrerade ramverket för områden där en riskhanteringsplan behövs

Varje område innefattar ett antal krav. Av dessa är de som är föreskrivna ledningen de viktigaste, då ledningen har huvudansvar såväl som tillsynsansvar över ett antal områden. Ledningen ska säkerställa en korrekt implementering av riskhanteringsplanen, att säkerhetskontroller utförs kontinuerligt och att relevant personal får den utbildning som behövs. Det krävs också att leverantörer har tillräcklig kunskap och att säkerhetspolicys utvärderas och uppdateras fortlöpande. Utöver detta är identifiering av tillgångar viktig, då skyddsvärda resurser inom cyberstrukturer, fysiska tillgångar och information bör kartläggas. Dessa kan i sin tur klassificeras efter skyddsvärde.

När det gäller cybersäkerhet och ägare av system, så bör operatören ha god överblick över sina tillgångar. Dessutom bör det finnas en säker kodningspraxis för internt utvecklad programvara. De bör även granska program som köps in från tredje part för att försäkra att säkerhetskraven överensstämmer. För operatörer föreslås identifiering av incidenter och lagring av information om dessa, att kontroller utvecklas och implementeras för att undvika otillbörlig tillgång till konton och system samt att sårbarhetsanalyser genomförs. Beredskapskrav innefattar att det ska finnas personal med tydliga beredskapsroller, både för hantering av fysiska och cyberrelaterade incidenter. Beredskapsplaner ska testas regelbundet.

CIP-013-1 är en pålitlighetsstandard (reliability standard) för hantering av cybersäkerhet i leverantörskedjor av hårdvara, mjukvara, dataanvändning och nätverkstjänster för industriella kontrollsystem associerade med Bulk Electric System (BES). Ambitionen med standarden är att varje organisation och verksamhet ska utveckla och implementera säkerhetskontroller utefter en objektiv standard. Standarden kan delas upp i fyra delar: (1) integritet och äkthet hos mjukvaran, (2) fjärråtkomst för leverantören, (3) planering av informationssystem, och (4) riskhanterings- och anskaffningskontroller hos leverantören [24]. CIP-013-1 hanterar således relevanta cybersäkerhetsrisker i leverantörskedjor i planerings-, anskaffnings-, och implementeringsfasen av livscykeln hos system som identifierats och kategoriserats utefter kraven i CIP-002-5 eller motsvarande standard [25].

CIP-013-1 är uppdelad i tre krav (requirements), R1 till R3. R1 föreskriver att utveckling av ett eller flera styrinstrument för att säkerställa cybersäkerheten i leverantörskedjorna, till exempel riskhanteringsplaner. Uppskattning av potentiella cybersäkerhetsrisker och sårbarheter ska tillgodoses i såväl planeringen som införskaffandet av system. [25] R2 föreskriver implementeringen av R1, med särskilt fokus på kontrakt med nya leverantörer. R3 behandlar hur de risk-hanteringsplaner som specificerats i R1 skall granskas och godkännas. Godkännandet ska ges av en CIP Senior Manager var 15:e månad, vilket motiveras av att varje ansvarig kontinuerligt ska granska nya risker och tillgängliga dämpande åtgärder som finns på marknaden. [25]

5 Rekommendationer för säkerhetsåtgärder i leverantörskedjor inom ICS-området

Risker, hot, sårbarheter, och incidenter ska bemötas med lämpliga åtgärder. Det är ett tankesätt som återspeglas av informations-, nätverks- och cybersäkerhetssektorn, från högsta policynivå ner till operatörers säkerhetschefer. Men vilken karaktär brukar åtgärderna ha, och vilka typer av åtgärder brukar förordas för operatörer respektive leverantörer av industriella styrsystem? Dessa frågor besvaras i det här kapitlet.

En allmänt vedertagen syn på säkerhetsåtgärder är att de ska vara ändamålsenliga för bevarandet av konfidentialitet, integritet, och tillgänglighet av

- information inom systemen (*informationssäkerhet)*,
- logiska och regelstyrda processer eller funktioner som utförs av systemet (*logisk säkerhet*),
- systemen i sig (*fysisk säkerhet*) och
- användarna (*personsäkerhet*). [1]; [6]; [9]; [18]

Ett huvudantagande är att om sådana åtgärder kommer till stånd så kan man bättre säkra kontinuiteten i samhällsviktiga tjänster som använder ICS. [1] En av de mest grundläggande orsakerna till att behov av informations-, nätverks- och cybersäkerhetsåtgärder uppstår är just sammanslutningen och uppkopplingen av system, direkt eller indirekt mot internet (nätverkssäkerhet). [26]

Ett ytterligare synsätt är att säkerhetsåtgärder ska vara både tekniska och organisatoriska, samt att de ska förebygga, upptäcka, hantera och minimera verkningarna av risker, hot, sårbarheter och incidenter. [1]; [6]; [9] Den traditionen följer av koncept kring inbyggd integritet, och som följd till integritet, *inbyggd säkerhet*. Säkerhet måste alltså realiseras proaktivt, holistiskt och i ett tidigt skede genom exempelvis tydligt dokumenterade organisatoriska prioriteringar, efterlevnad av standarder samt genom design av logiska processer och protokoll som integrerar säkerhet i teknologin som standard och kärnfunktion. [27]; [28]; [29: s1-88] Konkretare vägledning, särskilt kring inbyggd säkerhet, har också potential att minska ovisshet hos operatörer och leverantörer, och därmed öka tilliten aktörer emellan. [30]; [31]

Följande rekommendationer riktar sig till aktörer inom leverantörskedjan för industriella styrsystem. Den utgår ifrån att ledningen inom organisationer redan är engagerad för att förstärka säkerhet och att det finns organisatoriska och personella resurser tillgängliga för dessa ändamål [32: s32]. Först och främst rekommenderas att tydliggöra ansvarsförhållandet mellan operatör och leverantör. För att förtydliga aspekterna som bör beaktas i detta arbete föreslår författarna en komprimerad modell som presenteras i Avsnitt 5.1. Därefter bör nödvändiga

analyser genomföras samt policyer och planer etableras. Slutligen bör tydliga säkerhetskrav specificeras.

5.1 Ansvarsförhållanden

Med anledning av att det finns många olika sätt varor och tjänster kan levereras på finns det ingen given formel för ansvarsfördelning för säkerhetsåtgärder som passar alla. Som tidigare påvisat (se kap. 4: Regleringar, standarder och säkerhetskrav) är ofta det rättsliga antagandet att huvudansvaret för säkerhetsåtgärder ligger hos operatörerna som köper in, äger och driftsätter styrsystem. Standarder ger sällan en samlad syn på ansvarsfördelning.

Generellt sett finns det ett fåtal bindande ansvarsformer och ett mycket större antal frivilliga ansvarsformer. Lagkraven för nätverks- och informationssäkerhet är bara bindande såtillvida att operatörer som levererar samhällsviktiga tjänster måste vidta vissa identifierade och specifika organisatoriska åtgärder, exempelvis kartläggningar av egna system, riskanalyser och incidenthanteringsplaner. [1] Operatören har alltså det yttersta ansvaret att se till att en lämplig ansvarsfördelning implementeras gentemot leverantörerna, till exempel genom att välja operatörer från länder med lämpliga lagkrav på säkerhet, avtal och dokumenterade användarkrav på system, komponenter och tjänster. [33]

Inbyggd säkerhet i form av övriga gemensamma och specifika organisatoriska och tekniska åtgärder för leverantörer av samhällsviktiga tjänster tenderar snarare att förekomma som frivilliga inslag, till exempel genom standardisering. Frivilliga ansvarsformer kan medföra flexibilitet och främja tilliten mellan operatörer och leverantörer, men kan också medföra oförutsägbarhet som minskar tilliten. Särskilt utvalda standardkrav får en särställning inom vissa typer av verksamhet, vissa nationaliteter, eller vissa grupper av operatörer och leverantörer. Exempel på detta är amerikansk bästa praxis [34] som riktar sig mot upphandling av styrsystem, och norsk bästa praxis för olje- och gasindustri som särskilt riktar sig mot tillverkare av styrsystem användbara för sektorn [35]. Sådana standardkrav kan öka förutsägbarheten och tilliten inom vissa operatörs- och leverantörsförhållanden. Samtidigt kan dessa framstå som godtyckliga och kostsamma i relation till andra likartade operatörs- och leverantörsförhållanden.

Både operatörer och leverantörer bör ingå i dialog om lämplig praxis. Dialogen bör föras både inom forum såsom NIS-direktivets informella samarbetsmekanismer för att åstadkomma bred relevans för samhällsviktiga sektorer och industrin [1] och i ett tidigt skede av upphandling mellan operatör och leverantör för åstadkomma särskild relevans för enskilda förhållanden. [33]

Fördelningen av det faktiska ansvaret mellan den som äger och driftsätter ett system och den som levererar varor eller tjänster för ett system, ska också bidra

till att säkerhetsåtgärderna blir ändamålsenliga och lämpliga [1]; [6]; [9]; [18]. Ansvarsförhållandet bör också baseras på det faktiska riskförhållandet mellan operatör och leverantör [33]. Därför rekommenderas följande principer för att fördela ansvar för att implementera säkerhetsåtgärder:

- Ansvarsfördelningen ska vara *proportionerlig* i förhållande till riskfördelningen. (Se även [1]). Fördelningen av ansvar för säkerhetsåtgärder bör alltså reflektera den grad av risk som en leverantör i leverantörskedjan medför för operatören med sin tjänst, komponent eller system, den grad av beroende operatören har till leverantören, samt den grad av tillgång och behörighet en leverantör i leverantörskedjan har till operatörens faciliteter och system. [33]
- Ansvarsfördelningen bör vara *funktionell*. Ansvar för säkerhet bör endast fördelas i syfte att åstadkomma höjd säkerhet. Om en leverantör i leverantörskedjan inte tillhandahåller en tjänst, komponent eller system där säkerhetskrav kan implementeras funktionellt, bör de inte heller ansvara för säkerheten.
- Ansvarsfördelningen bör vara *adekvat* (lämplig för ändamålet). Om en leverantör i leverantörskedjan ska ansvara för säkerhetsåtgärder bör ansvaret avse funktionella krav som angivits i lag, standard eller bästa praxis. Säkerhetsåtgärden som fördelas bör vara utvald för att den sannolikt kommer att höja säkerheten i systemet. Detta betyder också att leverantörer som inte kan implementera säkerhetsåtgärder på ett adekvat sätt bör väljas bort.

I hänseende till proportionalitet föreslår rapporten en ansvarsfördelningsstrategi för frivilliga åtgärder. Riskfördelningen i denna strategi bedöms enligt förhållandemodellen mellan operatören och leverantören, operatörens förtroendenivå för leverantören samt operatörens riskuppfattning. En övergripande modell beskrivs i Tabell 3.

Tabell 3. Övergripande modell av möjliga ansvarsförhållanden mellan operatör och leverantör

Ansvarsfördel-ningsstrategi	**Lågt leverantörsansvar, operatören tar huvudsakligt och proaktivt ansvar för säkerheten**	**Måttligt leverantörsansvar, operatören delar proaktivt ansvar för säkerheten**	**Högt leverantörsansvar, operatören delar proaktivt ansvar för säkerheten**
Leverantörens inflytande	Låg grad av inflytande	Måttligt inflytande	Högt inflytande
Operatörens riskuppfattning	Låg risk	Måttlig risk	Hög risk
Förtroende för leverantörens säkerhet	Låg garanti för efterlevnad med branschpraxis för inbyggd säkerhet kan accepteras	Måttlig garanti för efterlevnad med branschpraxis för inbyggd säkerhet kan accepteras	Hög garanti för efterlevnad med branschpraxis för inbyggd säkerhet med specialiserade säkerhetsanpassningar krävs

5.1.1 Förhållandemodeller för operatörer och leverantörer

Ansvarsfördelningen måste baseras på en verklighetsnära och nyanserad modell av hur förhållandet mellan operatörer och leverantörer ser ut. Rapportförfattarna utgår ifrån en reviderad modell med utgångspunkt i ISO/IEC 27035 [33] och dess empiriska redovisning av hot mot leverantörskedjan. Modellen graderas efter leverantörens generella proportion av inflytande i styrsystemets livscykel och i operatörens verksamhet. Modellen förhåller sig både till styrsystemen, deras teknologi och komponenter samt informations- och kommunikationsteknologin (IKT) och de komponenter som gör styrsystemen integrerade eller uppkopplade. Modellen beskrivs i Tabell 4.

Tabell 4. Inflytande i relationen mellan operatör och leverantör

Leverantörens inflytande	Låg grad av inflytande	Medelgrad av inflytande	Hög grad av inflytande
Övergripande	Styrsystemen och IKT ägs, driftsätts och hanteras av operatören men delar av system, eller tjänster har tillhandahållits av leverantören	Styrsystemen och IKT, ägs och driftsätts av operatören men hanteras delvis eller helt av en leverantör	Styrsystemen och IKT ägs eller driftsätts och hanteras helt eller till hög grad av leverantörer
Utveckling & installation	Styrsystemet eller ansluten IKT är utvecklat (och installerat) av en leverantör. Operatören har haft betydande inflytande över utvecklingsprocessen	Styrsystemet eller ansluten IKT är utvecklat (och installerat) av en leverantör som även initierar vidareutvecklingen. Operatören har haft inflytande över processen	Styrsystemet eller ansluten IKT är utvecklat och installerat av en leverantör. Operatören har haft lågt eller inget inflytande över utvecklingsprocessen
Drift	Både styrsystemet och IKT driftsätts endast av operatören. Uppdateringar sker helt på operatörens initiativ utan ett inflytande från leverantören	Både styrsystemet och IKT används driftsätts av operatören med stöd av leverantören. Uppdateringar i drift och tillämpning sker på leverantörens initiativ	Styrsystemet eller ansluten IKT ägs och driftsätts av leverantören alternativt att systemen delvis ägs av operatören men driften är helt beroende av leverantörens medverkan
Förnyelse & avveckling	Operatören förnyar eller avvecklar sina system samt etablerar nya leverantörsförhållanden på eget initiativ	Systemen förnyas eller avvecklas samt nya leverantörsförhållanden etableras på operatörens initiativ med stöd från leverantören	Systemen avvecklas och/eller förnyas på leverantörens initiativ. Operatörens förutsättningar att etablera nya leverantörsförhållanden är begränsade
Leverantörs-ansvar	Lågt leverantörsansvar	Måttligt leverantörsansvar	Högt leverantörsansvar

5.1.2 Riskuppfattning i förhållandet mellan operatör och leverantör

Ansvarsfördelningsstrategin påverkas av vilken risknivå som operatören uppfattar i sin verksamhet generellt, och särskilt vilken risk operatören uppfattar i sitt förhållande till leverantören. Operatörens riskuppfattning i förhållandet till leverantören graderas till exempel i ISO/IEC 15408-3:2008(E) och beskrivs i Tabell 5.

Tabell 5. Riskuppfattning i relationen mellan operatör och leverantör

Risk-uppfattning	**Låg riskuppfattning**	**Måttlig riskuppfattning**	**Hög riskuppfattning**
ISO/IEC 15408-3:2008(E)	Behovet av självständig garanti om inbyggd säkerhet enligt bästa branschpraxis är låg hos operatör och leverantör	Behovet av självständig garanti om säkerhet enligt bästa branschpraxis är måttligt hos operatör och leverantör. Operatör/leverantör är redo att utöka den ekonomiska investeringen för säkerhet	Risken bedöms som hög eller extremt hög. Behovet av självständig garanti om inbyggd säkerhet enligt bästa branschpraxis är högt hos operatör och leverantör. Utökad ekonomisk investering för säkerhet krävs
Leverantörs-ansvar	Lågt leverantörsansvar	Måttligt leverantörsansvar	Högt leverantörsansvar

Operatörens riskuppfattning bör baseras på analyser om hotbild, sårbarhet, konfidentialitet och risk generellt (se 5.2).

5.1.3 Förtroendet mellan operatör och leverantör

Det finns inga uttömmande eller objektiva metoder för att klassificera förtroendegrader i förhållande till en leverantör. Däremot representerar standardisering ett sätt att skapa tydlighet och förutsägbarhet kring vilken nivå av säkerhetsgaranti (assurance/evaluation assurance/maturity level) som en certifierad leverantör, produkt eller tjänst kan uppfylla [18]. Därmed representerar nivåerna den lämpligaste modellen i förhållande till bästa branschpraxis för cybersäkerhet. Nivåerna är inte en skildring av faktisk säkerhet eller någon garanti för fullständig hantering av hot och risker, utan snarare en representation av hur genomgripande leverantörens ansvarstagande för cybersäkerhet är och till vilken grad operatören kan verifiera det. Säkerhetsgarantinivåerna relaterar till förhållandemodellen och riskuppfattningen på så sätt att låga garantier endast bör accepteras vid låg riskuppfattning och låg grad av inflytande från leverantören. De olika nivåerna presenteras i Tabell 6. Det finns flera olika försök att representera säkerhetsgarantinivåer inom auktoritativa instrument för att forma branschpraxis kring cybersäkerhet, till exempel:

- **COM(2017) 477** (”Cyber Security Act”) syftar till en förutsägbar, europeiskt allmän modell där europeiska kompetenta myndigheter bedömer IKT-produkter och tjänsters förtroende utifrån särskilda standardkrav (grundläggande nivå till hög nivå av garanti).
- **ISO/IEC 15408-3:2008(E)** syftar till att bedöma hur stringent den inbyggda säkerheten i IKT kan bedömas i relation till hot och risk.
- **IEC 62443-4:2018(E)** syftar till att bedöma säkerheten i relation till säkerhetsriktmärken hos leverantören, särskilt till organisatoriska riktmärken.

Tabell 6. Förtroendenivåer i relationen mellan operatör och leverantör

Förtroendenivåer		
Låg Garanti	**Måttlig Garanti**	**Hög Garanti**
Leverantören och/eller dess nationella rätts- och standardiseringssystem inger begränsat förtroende för efterlevnad med branschpraxis för hög cybersäkerhet i produkter/tjänster. Produkten/tjänsten har begränsad anpassning till operatörens säkerhetspolicy och operatören har begränsad tillgång till dokumentation angående inbyggd säkerhet.	Leverantören och/eller dess nationella rätts- och standardiseringssystem inger förtroende för efterlevnad med branschpraxis för hög cybersäkerhet i produkter/tjänster. Produkten/tjänsten är anpassad till operatörens säkerhetspolicy och operatören har tillgång till dokumentation angående inbyggd säkerhet.	Leverantören och/eller dess nationella rätts- och standardiseringssystem inger högt förtroende för efterlevnad med bästa branschpraxis för hög cybersäkerhet i produkter/tjänster. Produkten/tjänsten påvisar en hög grad av anpassning till operatörens säkerhetspolicy med specialiserad och prövad inbyggd säkerhet, samt åtgärder för utvärdering och uppdatering av säkerhetsåtgärder.
Förtroendenivåer enligt Cyber Security Act		
Garantinivå grundläggande	**Garantinivå väsentlig**	**Garantinivå hög**
Begränsat förtroende för cybersäkerheten hos en IKT-produkt eller tjänst med hänvisning till tekniska specifikationer, standarder och säkerhetshantering, inklusive tekniska kontroller, vars syfte är att minska risken för cybersäkerhetsincidenter.	Väsentligt förtroende för cybersäkerheten hos en IKT-produkt eller tjänst med hänvisning till tekniska specifikationer, standarder och säkerhetshantering, inklusive tekniska kontroller, vars syfte är att minska risken för cybersäkerhetsincidenter.	Högt v förtroende för cybersäkerheten hos en IKT-produkt eller tjänst med hänvisning till tekniska specifikationer, standarder och säkerhetshantering, inklusive tekniska kontroller, vars syfte är att minska risken för cybersäkerhetsincidenter.

Förtroendenivåer enligt ISO/IEC 15408-3:2008(E)		
Funktionellt prövad	**Metodologiskt utvecklad, prövad och utvärderad**	**Metodologiskt utvecklad, prövad och utvärderad**
Produkten eller tjänsten har en begränsad anpassning till [operatörens] säkerhetspolicy med hotbilden bedöms som ringa. Produkten säkerhet är utvärderad.	Produkten påvisar en mycket hög inbyggd säkerhet och en fullständig säkerhetsanalys och produktutvärdering, inklusive oberoende prövning.	Produkten påvisar mycket specialiserade säkerhetsanspassningar, en fullständig säkerhetsanalys och produktutvärdering, inklusive oberoende prövning, är genomförd.
Förtroendenivåer enligt IEC 62443-4:2018(E)		
Initial	**Hanterat/dokumenterat**	**Optimerande**
Produktutvecklingen sker till hög grad med oplanerad, odokumenterat, och inkonsekventa säkerhetsprocesser som inte kan repeteras.	Produktsäkerhet hanteras utifrån dokumenterade policy och mål, samt med personal som genomgått träning utifrån dessa. Produktutvecklingen sker utifrån dokumenterat inövade processer som kan repeteras.	Leverantören kan redovisa förbättring i produktsäkerhet baserat på lämpliga mätvärden.
Ansvarsfördelningsstrategi		
Låg garanti accepteras när leverantören har låg grad av inflytande över verksamheten och risken uppfattas som låg. Operatören har huvudsakligt och proaktivt ansvar för säkerheten.	Måttlig garanti accepteras när leverantören har måttlig grad av inflytande över verksamheten och risken uppfattas som måttlig. Operatören delar proaktivt ansvar för säkerheten med leverantören.	Hög garanti krävs när leverantören har hög grad av inflytande över verksamheten och risken uppfattas som hög. Operatören delar proaktivt ansvar för säkerheten med leverantören.

5.1.4 Relationen mellan leverantör och operatör under livscykeln

Som regel fastställs relationen mellan operatören och leverantören under de initiala förhandlingarna om design, köp och installation. Det huvudsakliga arbetet med dessa frågor sker tidigt under designfasen, förmodligen innan avtalen skrivs. Även då operatören avser att engagera en tredje leverantör för drift, bör förhandlingarna ske redan under designfasen. Under redesignfasen, i synnerhet vid leverantörsbyte, bör operatören fundera kring vilket slags relation operatören i framtiden vill ha till sina leverantörer. Då ICS typiskt har en mycket lång livslängd är det troligt att en operatör behöver byta leverantör under livscykeln. I dessa fall etableras relationen med den nya leverantören under operations- och underhållsfasen eller under redesignfasen. Utredningen kring förhållanden mellan operatör och leverantör bör alltså generellt genomföras under livscykelns samtliga faser, men i synnerhet under design och redesignfasen (se Figur 1).

5.2 Nödvändiga Analyser

Behovet av analyser uppstår bland annat genom rättsliga krav och branschpraxis kring hanteringen av hot, sårbarhet och risker [1] [6] [18]. Analyser av hot, sårbarheter, tillgångar, konfidentialitet och risker anses vanligen som en central del av en riskhanteringsprocess [8] [36] [37]. I FOI:s och MSB:s studie *IoT-relaterade risker och strategier* [38] är hot och sårbarheter starkt kopplade till risken att en incident ska förverkligas.

En övergripande inventering av branschpraxis visar att analyserna bör täcka hot, sårbarheter, konfidentialitet, risker och säkerhetsbehov kopplat till information, logiska processer, nätverk, fysisk infrastruktur såväl som användare.

Det finns ingen universell analysmetod, men branschpraxis föreslår ett antal viktiga aspekter som bör ingå i analysarbetet. I Tabell 7 presenteras ett urval av sådana aspekter.

Tabell 7. Faktorer inom en sårbarhetsanalys

Analysinriktning	Innehåll för analysen
Hotbildsanalys	SS-ISO/IEC 27005:2018: resursägaren bör utgå ifrån en kvalitativ karaktärisering med en sannolikhetsbedömning som är förankrad hos olika experter inom organisationen. IEC 62443-4-1 2018(E): hotmodeller bör framställas redan i utvecklingen av produkter som ska användas i anslutning till styrsystem.
Sårbarhetsanalys	ISO/IEC 27000:2018(E): Analys av tekniska attackvektorer. SS-ISO/IEC 27005:2018(E): Analys av generella faktorer så som svagheter inom organisationen, i processer och rutiner eller den fysiska miljön.
Analys av konfidentialitetsbehov	Identifiering av information, som av olika anledningar inte bör spridas eller behandlas av utomstående; kan omfatta företagshemligheter, personuppgifter, och uppgifter som omfattas av sekretess och tystnadsplikt. [38]
Riskanalys	ISO/IEC 27000:2018(E): organisationer bör särskilt bedöma sannolikheten av fysiska och funktionella systemfel, samt operativa hot, hot mot driftskontinuitet och intressenters intressen till följd av, exempelvis antagonistiska intressen mot organisationen, naturkatastrofer, och fallerande tjänster inom leverantörskedjan. SS- ISO/IEC 27005:2018: innehåller riskbedömningar och inverkansbedömningar.

5.2.1 Analyser under livscykeln

Mycket av analysarbetet föregår rimligtvis konceptualiseringen, beställningen och installationen av styrsystemet. Dessa analyser kan vara separata eller ingå i ett paket av behovsanalyser, marknadsanalyser och övriga analyser som inte är

relaterade till säkerhet. På grund av dess långa livslängd och potentiellt mångtaliga modifikationer, är det viktigt att med jämna mellanrum revidera de genomförda analyserna. Händelser som kan innebära ett förnyat analysbehov kan till exempel vara ett förändrat säkerhetspolitiskt läge, detekterade sårbarheter inom styrsystemet eller näraliggande system.[4] Även signifikanta förändringar hos leverantören, som exempelvis ett byte av underleverantörer, kan innebära ett förnyat analysbehov. Också vid avverkning av styrsystemet kan det finnas ett analysbehov, särskilt gällande skydd av intellektuell egendom eller annan skyddsvärd information, nedstängning av potentiella fjärråtkomstmöjligheter och skydd av kvarvarande system. En rekommendation är således att analys genomförs under livscykelns alla faser, men i synnerhet under design och installation, operation och underhåll samt redesign (se Figur 1).

5.3 Policy och planering

Ett sätt för leverantörer och operatörer att sprida kunskap inom den egna organisationen och påvisa att lag- och standardkrav efterlevs är att anta relevanta verksamhetsanpassade policyer. [41] För operatörer av samhällsviktiga tjänster måste det säkerhetsrelaterade arbete dokumenteras i flera skeden. [6] [42] Det är viktigt att förtydliga både externa och interna ansvarsförhållanden för organisationer, och att upprätthålla transparens. [40] Det bör i dokumentationen tydligt framgå operatörens eget säkerhetsansvar (och rollfördelning för det säkerhetsansvaret), likväl som leverantörens säkerhetsansvar.

5.3.1 Informationssäkerhetspolicy och åtgärdsplan

Svenska operatörer som levererar samhällsviktiga tjänster ska anta en informationssäkerhetspolicy. [42] Ett krav på en informationssäkerhetspolicy är att den förtydligar mål och regler för organisationens informationssäkerhetsarbete. [42]

Operatörer som levererar samhällsviktiga tjänster måste också fastställa en åtgärdsplan för sina kontinuerliga riskanalyser. [6] Åtgärdsplanen ska fastställa tekniska och organisatoriska åtgärder som är lämpliga vid incidenter och bör fastställa vilken funktion inom organisationen som ansvarar för åtgärden. [42] Incidenter är händelser med en faktisk negativ inverkan på säkerheten i nätverks- och informationssystem. Åtgärdsplanen bör koppla risker, åtgärder, ansvar och fördelning av resurser för incidenthantering till den nivå av skydd som krävs vid en incident samt den nivå av konsekvenser incidenten skulle medföra. [42]

[4] Ett bra exempel är säkerhetshål som blev kända under namnen Spectre och Meltdown och berör många olika system. https://spectreattack.com/

Operatören bör, redan vid avtalsskrivning med en tjänsteleverantör, avtala vilka av åtgärderna som leverantören ska vidta. [42] De avtalade åtgärderna bör förslagsvis överensstämma eller komplettera de mål och regler som informationssäkerhetspolicyn identifierar samt svara mot de skyddsnivåer som fastställs i åtgärdsplanen. Leverantören ska dessutom förse operatören med information om misstänkta eller inträffade incidenter, avvikelser och sårbarheter, samt vilken kunskap och kompetens som leverantören måste ha för att hantera sådana incidenter, avvikelser och sårbarheter [42].

5.3.2 Policy och planering under livscykeln

Det är inte ovanligt att diskussioner kring policyer och dokumentationen sker tidigt i ett systems livscykel, och det är bra att ha dessa på plats i samband med styrsystemets driftsättning. Den fullständiga systemdokumentationen hör oftast till leveransen vid inköp. Det är dock under operations- och underhållsfasen som policyer och dokumentation tillämpas mest. Det är just under drift system, planer och policy stresstestas i händelse av incidenter. Incidenter ger i sin tur upphov till reflektion och revision, vilket förlägger det huvudsakliga arbetet med policy, planer och dokumentation till operations- och underhållsfasen. Det inkluderar även uppdatering av dessa typer av dokument. (Se Figur 1). I idealfallet borde uppdateringen av policy och åtgärdsplaner ingå i de aktiviteter som i vanliga fall anses vara ”business as usual”, så som övrig verksamhetsutveckling. [45]

5.4 Specificering av cybersäkerhetskrav

Cybersäkerhetskrav bygger ytterst på identifiering av åtgärder som måste vidtas för att höja säkerhetsnivån i hänsyn till cybersäkerhet. Medan det finns få vedertagna definitioner för cybersäkerhet, föreslår COM(2017) 477 (”Cyber Security Act”) att cybersäkerhet är all verksamhet som krävs för att skydda nätverks- och informationssystem (definierat enligt NIS-direktivet) samt användare och personer som påverkas av cyberhot. Cyberhot är omständigheter med potentiell negativ inverkan på systemen, användare och personer. [18] Som tidigare beskrivits kan cybersäkerhet dessutom kopplas till informationssäkerhet, logisk säkerhet, nätverkssäkerhet, fysisk säkerhet och personsäkerhet. [1] [6] [9] [18] [43]

Specificering av säkerhetskrav är en väsentlig del av säkerhetshanteringen. [37] Dessa krav ska omfatta både tekniska och organisatoriska åtgärder och bör alltså stå i proportion till den bedömda risken för verksamheten och de berörda nätverks- och informationssystemen. [1] Aspekter av proportionalitet kan alltså vara att säkerhetskrav ska väljas utifrån sin funktionalitet. Detta innebär att de ska syfta till att uppnå en högre grad av säkerhet emot identifierade hot, sårbarheter och risker.

Det finns således få universellt giltiga säkerhetsåtgärder som passar alla tänkbara förhållandemodeller mellan operatörer och leverantörer. (Se till exempel [6])

Tabell 8. Råd för specificering av säkerhetskrav

Säkerhetsaspekt	Åtgärder
Informationssäkerhet	Tillgodose begränsad uppkoppling av systemarkitektur. [50] Tillgodose begränsad centralisering av datalager. [28] Tillgodose säker kommunikation och lagring av information, till exempel genom att säkerställa att system och organisation kan hantera kryptering och krypteringsnycklar. [28] [47] Tillgodose anonymisering och pseudonymisering om konfidentialiteten eller sekretessen härrör till skyddade identiteter eller personuppgifter. [28] Loggad behandling av datat [50]
Personell säkerhet	IEC 62443-1-1: • **Kontroll över identifiering,** autentisering och säkerhet vid åtkomst till systemet. • **Kontroll över användning** säkerställer att endast nödvändiga rättigheter tilldelas användare av systemet och övervakning av systemanvändning. Organisatoriska åtgärder: registerkontroller, säkerhetsprövningar samt att tillämpa uppförandekoder och avtal för konfidentialitet. [29] [44] [47] [50]
Nätverkssäkerhet	Kontrollera metoder för åtkomst till osäkrade nätverk samt neka åtkomst till sådana nätverk. [47] [50] Förmåga att auktorisera, övervaka och tillämpa användningsbegränsningar för trådlös anslutning enligt accepterad branschpraxis. [47] [50] Konfigurera kontroll och restriktioner för mobila och portabla enheter enligt risk för skada. [47] [50] Generera loggar för granskning av systemsäkerhet, till exempel åtkomstkontroll, säkerhetskopiering och konfigurationsändringar. [47] [50]
Logisk säkerhet	Säkerställa användning av mjukvara som är lämplig för uppgifterna som ska utföras. [36] Processerna, protokollen och rutinerna baseras på fullständig och korrekt data eller att bristande funktioner inte korrumperar viktig data. [47] Mjukvara kan identifieras på ett unikt sätt, autentiseras och dess privilegier mot systemet kan kontrolleras. [47]
Fysisk säkerhet	Skydd av systemets hårdvara samt skydd från fysiska hot och således även i förläning skydd av faciliteter för verksamhetskritiska system. [36] [43] [47] [50] [51]

Svenska operatörer och leverantörer bör uppmärksamma europeiska och internationellt accepterade standarder och specifikationer [46] samt följa eventuella föreläggande och föreskrifter som MSB publicerar angående implementeringen av NIS-direktivet och systematiskt och riskbaserat informationssäkerhetsarbete. [6] [46] Detta måste genomföras kontinuerligt allteftersom denna branschpraxis publiceras.

Branschpraxisen redogör för flera åtgärder för att höja säkerheten. Tabell 8 redogör för ett antal utvalda åtgärder.

5.4.1 Säkerhetskrav under livscykeln

Många av säkerhetskraven fastställs under de initiala förhandlingarna om anskaffning, design och installation av ett system. Detta innebär att en stor del av arbetet sker redan innan avtalen som ligger till grund för förvärv skrivs. Med tanke på den ofta mycket långa livslängden hos ett ICS, kan dock den verklighet som operatören och leverantörerna verkar i förändras signifikant. Ett exempel skulle kunna vara nya tekniker som antagonister kan utnyttja till sin fördel.[5] Därutöver kan operatörens utveckling av den egna verksamheten eller tillkomna lagkrav resultera i förändrade behov och nya säkerhetskrav. Även den geopolitiska situationen kan förändras med tiden och i sin tur kräva en förnyad analys av säkerhetsaspekterna. Detta gör att säkerhetskrav behöver justeras även under operations- och underhållsfasen. Även under avvecklingsfasen kan det finnas behov att etablera säkerhetskrav med tanke på vilken information som kan bli tillgänglig eller om viss information behöver arkiveras för framtiden när styrsystemet fysiskt lämnar operatörens faciliteter. Specificering av säkerhetskrav, även gentemot leverantören, bör alltså ske i livscykelns samtliga faser (se Figur 1).

[5] T.ex. har s.k. air gap för inte alltför länge sedan ansetts vara ett bra sätt för att säkra IT-system. Sedan några år tillbaka har det blivit tydligt att även ett air gap är överkomligt för en antagonist. https://cyber.bgu.ac.il/media/malware-escapes-from-faraday-cages-and-air-gapped-computers/

6 Slutsatser

Vad innebär leverantörskedjan för säkerheten i industriella informations- och styrsystem?

Ett flertal nutida incidenter har demonstrerat behovet att stärka säkerheten i leverantörskedjorna till industriella informations- och styrsystem, till exempel kryptomasken NotPetya, som spreds via en leverantör. Sådant arbete påverkas av komplexiteten som uppstår då operatören behöver ge åtkomst till, och kunskap om sina system till sina leverantörer, vilka i sin tur underhåller egna leverantörskedjor. Målet för denna rapport har varit att inventera tillämpliga säkerhetsåtgärder för att höja säkerheten i leverantörskedjan, att integrera dessa i ett styrsystems fullständiga livscykel och att förtydliga hur ansvaret för sådana åtgärder kan fördelas mellan operatörer och leverantörer. Detta med syftet att stödja MSB:s arbete för ökad säkerhet i industriella information- och styrsystem i enlighet med den nationella handlingsplanen.

För att kunna resonera kring användbarhet av de olika föreslagna åtgärderna i livscykelns olika skeden, skapades en generisk livscykelmodell bestående av fem faser (se Figur 1). Modellen speglar ett styrsystems ofta mycket långa livslängd och tillgodoser möjligheten att styrsystemet modifieras signifikant i flera iterationer med uppgraderingar och anpassningar. Ett antagande modellen gör är att ett ICS kommer genomgå cykeln ett flertal gånger innan systemet till slut avvecklas. Modellen är dock så pass generiskt och flexibel att den i framtiden även kan användas för att illustrera andra aspekter av säkerheten i industriella informations- och styrsystem. I den här rapporten används modellen för att tydliggöra de olika skeden i ett styrsystems liv då en åtgärd för att säkra leverantörskedjan bör genomföras.

Vilka säkerhetsåtgärder finns det och hur kan de användas för samhällsviktiga verksamheter som använder ICS?

Säkerheten i styrsystem regleras i flertalet lagar som operatörer behöver förhålla sig till. Detta gäller i synnerhet verksamheter som levererar samhällsviktiga tjänster. Det finns även rekommendationer för hur arbetet kan läggas upp i många standarder, vägledningar och annan branschpraxisdokumentation. Många av kraven och rekommendationerna, som i grunden riktar sig mot operatörer, kan appliceras även på förhållandet mellan operatör och leverantör. En grundläggande fråga i detta är hur mycket ansvar för ett styrsystem och dess funktionalitet operatören är beredd att lämna ifrån sig, och vilka kontrollmekanismer för att säkerställa säker drift finns att tillgå. Förslagsvis kan dessa aspekter balanseras. Samtidigt bör påpekas att till exempel operatörens tillgång till kompetens, ekonomiska eller rättsliga förutsättningar kan begränsa möjligheterna för att nå en sådan balans. Tilliten gentemot leverantören blir således en viktig faktor. Många aspekter påverkar tilliten, det kan till exempel handla om att leverantören är certifierad i sin roll som leverantör, eller förhåller sig till samma rättsliga krav som

operatören, men det kan även handla om kulturellt samförstånd eller det vedertagna sättet att verka inom sitt område. Centralt för att säkra leverantörskedjorna blir alltså att stänga gapet mellan kontrollmekanismerna och den rimliga tilliten gentemot leverantören. Nedan presenteras de tillvägagångssätten som kan rekommenderas utifrån studiens resultat.

6.1 Rekommendationer

Vilka rekommendationer kan ges till operatörer av ICS för att undvika osäkerhet i leverantörskedjan?

Rapporten presenterar ett antal åtgärder, eller tillvägagångssätt, för att säkra leverantörskedjorna för ICS. Dessa kan kategoriseras utifrån fyra områden:

Reda ut ansvarsförhållanden: Redan i designfasen bör det utredas vilken typ av förhållande operatören och leverantören kan och bör ha. Hänsyn bör tas till hur mycket inflytande leverantören kommer att ha på operatörens system, hur operatören uppfattar risken i sin verksamhet, samt vilken nivå av förtroende gentemot leverantören som är rimlig. Detta ger möjlighet till ansvarsfördelning som passar den situationen som operatören och leverantören befinner sig i, t.ex. med hänsyn till verksamhetsområde, säkerhetskultur och efterlevnad av lagstiftning.

Genomför nödvändiga analyser: Ett flertal analyser är kopplade till säkerheten i leverantörskedjan. Hotbildsanalys, sårbarhetsanalys och riskanalys bör genomföras med hänsyn till information, logiska processer, nätverk, fysisk infrastruktur och användare av styrsystemet.

Skapa policyer och planering: Policyer och planer för hantering av systemet i daglig drift och vid incidenter bör etableras. Relationen till leverantörer bör uppmärksammas vid utvecklingen av policy och planering. Kraven bör vara proportionerliga till ansvaret som leverantören de facto har över systemet. Policyer och planer är kopplade till och nyttiggör resultaten från de tidigare nämnda analyserna. Åtgärdsplaner ingår i de krav som numera ställs på leverantörer av samhällsviktiga tjänster enligt *Lag 2018:1174 om informationssäkerhet i samhällsviktiga och digitala tjänster*.

Specificera säkerhetskrav: Säkerhetskraven är en grundbult för att höja säkerheten i system och för att säkra information, personer, logisk och fysisk infrastruktur. Säkerhetskraven som åläggs leverantören bör stå i proportion till den typen av ansvar som leverantören har över systemet. Kraven bör omfatta såväl tekniska som organisatoriska åtgärder och behöver stå i proportion till de identifierade riskerna.

Referenser

[1] EU (2016) *Europaparlamentets och Rådets 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.* ISO/IEC 27036-3 2013. Brussels: EU. Tillgänglig via https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX%3A32016L1148

[2] Symantec Security Response Response (2014) *Dragonfly: Western Energy Companies under Sabotage Threat.* Inhämtad 190304, tillgänglig via https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

[3] U.S. Senate Select Committee on Intelligence (2018) *Open Hearing: Nomination of Gina Haspel to be the Director of the Central Intelligence Agency*. Washington, D.C.: The U.S. Government Publishing Office. Tillgänglig via: https://www.intelligence.senate.gov/hearings/open-hearing-nomination-gina-haspel-be-director-central-intelligence-agency# Inhämtad 190212.

[4] Swedish Standards Institute, SIS, ISO 31000:2009 *Riskhantering – Principer och riktlinjer*.

[5] Swedish Standards Institute, SIS, ISO 73:2009 *Risk management – Vocabulary*.

[6] SFS 2018:1174 *Lag om informationssäkerhet för samhällsviktiga och digitala tjänster*.

[7] Hedtjärn Swaling, V. (2018) *IoT-related risk: prevention and management*. FOI Memo 6503. Stockholm: Totalförsvarets Forskningsinstitut

[8] Swedish Standards Institute, SIS, ISO/IEC 27000:2018 *Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Översikt och terminologi*

[9] Skr 2016/17:213 *Nationell strategi för samhällets informations- och cybersäkerhet.* Stockholm: Regeringskansliet

[10] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. & Hahn, A. (2015): *Guide to Industrial Control (ICS) Security – Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)*. Washington, D.C.: National Institute of Standards and Technology, NIST, U.S. Department of Commerce

[11] Olenick, D. (2018) SC Magazine: *NotPetya attack totally destroyed Maersk's computer network: Chairman*. Inhämtad 190304, tillgänglig

via https://www.scmagazine.com/home/security-news/ransomware/notpetya-attack-totally-destroyed-maersks-computer-network-chairman/

[12]Cimpanu, C. (2017) Bleeping Computer: *M.E.Doc Software Was Backdoored 3 Times, Servers Left Without Updates Since 2013*. Inhämtad 190305, tillgänglig via https://www.bleepingcomputer.com/news/security/m-e-doc-software-was-backdoored-3-times-servers-left-without-updates-since-2013

Department of Cyberpolice Ukraine (2017) Прикриттям наймасштабнішої кібератаки в історії України став вірус Petya (Diskcoder.C). (The largest cyberattack in Ukraine's history hid behind Petya) Inhämtad 190305, tillgänglig via https://cyberpolice.gov.ua/news/prykryttyam-najmasshtabnishoyi-kiberataky-v-istoriyi-ukrayiny-stav-virus-diskcoderc-881/

[13]Klein, M. (2017) *SCADA Life Cycle – A Look Back and Ahead*. Inhämtad 190304, tillgänglig via http://goconcentric.com/resources/scada-life-cycle-a-look-back-and-ahead/

[14]Davidsson, G., Haeffler, L., Ljundman, B. & Frantzich, H. (2003) Räddningsverket: *Handbok för riskanalys*. Stockholm: Räddningsverket.

[15]Commission of the European Communities (2006) *Communication from the Commission on a European Programme for Critical Infrastructure Protection*. COM (2006) 786 final. Brussels: Commission of the European Communities

[16]European Commission (2009) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"* COM (2009) 149. Brussels: European Commission.

[17]EU (2012) *Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG Text av betydelse för EES*. OJ L 316, 14.11.2012, p. 12–33. Brussels: Europaparlamentet

[18] EU (2017) *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").* COM/2017/0477 final - 2017/0225 (COD). Brussels: European Parliament

[19] Proposition 2017/18:205: *Informationssäkerhet för samhällsviktiga och digitala tjänster.* Inhämtad 190305, tillgänglig via https://www.regeringen.se/rattsliga-dokument/proposition/2018/04/prop.-201718205/

[20] European Union Agency for Network and Information Security, ENISA (2011) *Annex III. ICS Security Related Standards, Guidelines and Policy Documents*. Inhämtad 190305, tillgänglig via https://www.enisa.europa.eu/publications/annex-iii

[21] Wedebrand, C., Hedtjärn Swaling, V. & Stenérus Dover, A-S. (2016) *NCS3 Studie – Standardserie ISA/IEC 62443 – Användning och erfarenheter bland svenska ICS-aktörer*. FOI-R--4601--SE. Stockholm: Totalförsvarets Forskningsinstitut, FOI.

[22] Norsk Forening for Elektro og Automatisering, NFEA (2018) Konferens, *Cyber Security 2018*. Oslo 25-26 April 2018.

[23] McFarland, M. & Stewart, A. (2017) National Institute of Standards and Technology, NIST, U.S. Department of Commerce: *Great River Energy – Managing Supply Chain Risks Holistically*. Washington, D.C.: U.S. Department of Commerce. Inhämtad 190305, tillgänglig via https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-GRE-Cyber-SCRM-Case-Study.pdf

[24] North American Transmission Forum, NATF (2018) *Implementation Guidance.* Charlotte, NC: North American Transmission Forum.

[25] North American Electric Reliability Corporation, NERC (2017) *Cyber Security Supply Chain Risk Management Plans – Implementation Guidance for CIP-013-1*. Atlanta, GA: NERC

[26] Hedtjärn Swaling, V. & Mossberg Sonnek, K. (2015) *NCS3 – Beroenden till industriella informations- och styrsystem – En förstudie*. FOI-R--2480--SE Stockholm: Totalförsvarets Forskningsinstitut117

[27] Cavoukian, A. (2016) *Privacy by Design – The 7 Foundation Principles – Implementation and Mapping of Fair Information Practices.* Inhämtad 190212, tillgänglig via: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[28] European Network and Information Security Agency, ENISA (2014) *Privacy and Data Protection by Design.* Heraklion: ENISA

[29] EU (2016) *Europaparlamentets och Rådets Förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (Text av betydelse för EES).* Bryssel: Europeiska unionens officiella tidning.

[30] UK Department for Digital, Culture, Media & Sport (2018) *Secure by Design: Improving the cyber security of consumer Internet of Things Report.* Inhämtad 190305, tillgänglig via: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf London: UK Department for Digital, Culture, Media & Sport.

[31] Regeringskansliet (2017) *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi.* N2017/03643/D. Stockholm: Regeringskansliet Inhämtad 190305, tillgänglig via https://www.regeringen.se/informationsmaterial/2017/05/for-ett-hallbart-digitaliserat-sverige---en-digitaliseringsstrategi/

[32] Myndigheten för samhällsskydd och beredskap (MSB) (2014) *Vägledning till ökad säkerhet i industriella informations- och styrsystem.* Publ.nr: MSB718. Stockholm: MSB

[33] Swedish Standards Institute, SIS, ISO 27036-3:2013, IDT. *Informationsteknik – Säkerhetstekniker – Informationssäkerhet vid leverantörsrelationer – Del 3: Riktlinjer för informations- och kommunikationssäkerhet i leverantörskedjor.*

[34] Department of Homeland Security, DHS (2009) *Cyber Security Procurement Language for Control Systems*. Washington, D.C.: DHS

[35] Norsk Olje & Gass (2016) *Recommended guidelines for information security baseline requirements for process control, safety and support ICT systems*. No. 104, revision no. 6. Inhämtad 190305, tillgänglig via: https://www.norskoljeoggass.no/en/working-conditions/retningslinjer/integrated-operations/104-recommended-guidelines-for-information-security-baseline-requirements-for-process-control-safety-and-support-ict-systems-new-revision-05122016/

[36] Swedish Standards Institute ISO/IEC 27005:2018 *Informationsteknik – Säkerhetstekniker – Riskhantering för informationssäkerhet.*

[37] International Electrotechnical Commission IEC 62443-4:2018 *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements.*

[38] Hedtjärn Swaling, V. & Johansson, J. (2018) NCS3 Studie - *IoT-relaterade risker och strategier – Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem*. FOI-R--4591--SE, MSB 2017-1554. Stockholm: Totalförsvarets Forskningsinstitut.

[39] Hedtjärn Swaling, V. (2018) IoT-related risk: prevention and management. FOI Memo 6503. Stockholm: Totalförsvarets Forskningsinstitut.

[40] Swedish Standards Institute, SIS, ISO 28000:2007 *Specification for security management systems for the supply chain.*

[41] Danezis, G., Schiffner, S., Hansen, M., Tirtea, R., Domingo-Ferrer, J., Le Métayer, D. & Hoepman, J-H. (2014) European Network and Information Security Agency, ENISA: *Privacy and Data Protection by Design – From Policy to Engineering.* Heraklion: ENISA

[42] MSBFS 2018:8 (2018) *Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster.* Stockholm: Myndigheten för samhällsskydd och beredskaps författningssamling.

[43] CEN/CENELEC Cybersecurity Focus Group (2017) *Rec#2 – Definition of Cybersecurity*. Berlin: CEN/CENELEC/ETSI CSCG Secretariat

[44] International Electrotechnical Commission, IEC 62443-3-3:2013 *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels.*

[45] Centre for the Protection of National Infrastructure (CPNI) (odaterad) *Good Practice Guide – Process Control and SCADA Security. Guide 7. Establish ongoing governance.* London: CPNI.

[46] SFS 2018:1175 *Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster.*

[47] Swedish Standards Institute IEC TS 62443-1-1:2009(E) *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models.*

[48] Swedish Standards Institute, SIS, SIS-TR 50:2015 *Terminologi för informationssäkerhet.*

[49] Myndigheten för samhällsskydd och beredskap, MSB (2016) *Terminologi och begrepp inom informationssäkerhet – Hur man skapar en språkgemenskap.* Stockholm: MSB

[50] Försvarets radioanstalt, FRA (2017) *Åtgärdsförslag: Angrepp via tjänsteleverantörer.* Stockholm: FRA.

[51] Swedish Standards Institute, SIS, IEC 62443-4-1:2018 *Security for industrial automation and control systems – Part 4-1: Secure Product development lifecycle requirements.*

[52] Ben Gurion University of the Negev (2018) *Malware Escapes from Faraday Cages and Air-Gapped Computers.* Inhämtad 190306, tillgänglig via https://cyber.bgu.ac.il/media/malware-escapes-from-faraday-cages-and-air-gapped-computers/

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se