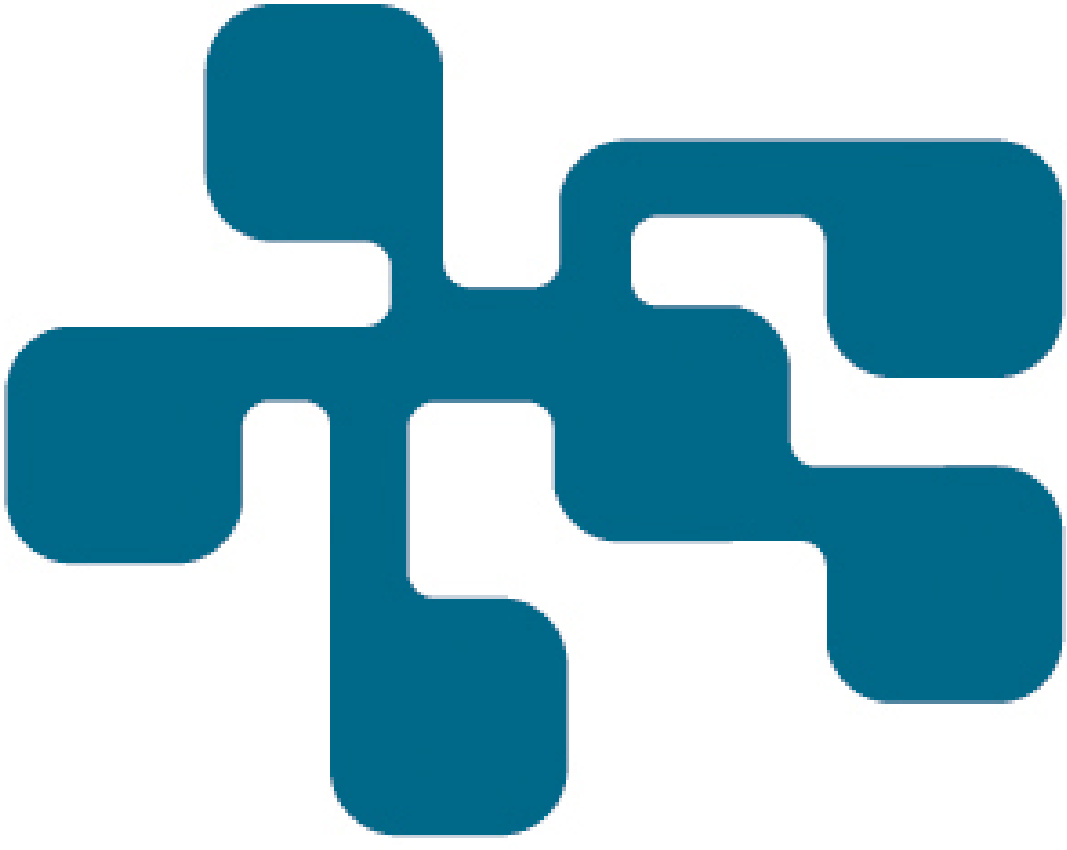
NCS3 Studie – Standardserie ISA/IEC 62443

Användning och erfarenheter bland svenska ICS-aktörer

CHRISTOFFER WEDEBRAND, VIDAR HEDTJÄRN SWALING, ANN-SOFIE STENÉRUS DOVER FOI



FOI-R--4601--SE
MSB 2017-2825 Juni 2018
ISSN 1650-1942

FOI-R--4601--SE

Christoffer Wedebrand, Vidar Hedtjärn Swaling,
Ann-Sofie Stenérus Dover

NCS3 Studie – Standardserie ISA/IEC 62443

Användning och erfarenheter bland svenska ICS-aktörer

FOI-R--4601--SE

Titel	NCS3 Studie – Standardserie ISA/IEC 62443: Användning och erfarenheter bland svenska ICS-aktörer
Title	NCS3 Studie – Standard series ISA/IEC 62443: Use and experiences in the Swedish ICS community
Rapportnr	4601
Månad	Juni
Utgivningsår	2018
Antal sidor	39
ISSN	1650-1942
Kund	MSB
Forskningsområde	5. Krisberedskap och samhällssäkerhet
FoT-område	
Projektnr	E13609
Godkänd av	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Sammanfattning

ISA/IEC 62443 är en standard med fokus på industriella informations- och styrsystem (ICS). Standarden har på senare tid fått ökad uppmärksamhet och används i Sverige såväl som internationellt trots att den i stora delar fortfarande är under utveckling.

Syftet med denna rapport är att ge Myndigheten för samhällsskydd och beredskap (MSB) en ökad förståelse för standardens omfattning och användning i Sverige för att på så vis bidra till ökad kunskap om de förutsättningar som råder inom ICS-området. Standardens användning kartläggs genom intervjuer med aktörer med bred erfarenhet från många olika domäner. Därtill ges en övergripande beskrivning av innehållet i ISA/IEC 62443.

Standardens fördelar anses vara att den är komplett över hela livscykeln, att den är skräddarsydd för ICS samt att den definierar en uppsättning säkerhetsnivåer som kan underkastas olika krav. Andra skäl till att ISA/IEC 62443 används och uppmärksammas anses vara en förändrad kravbild från kunderna som är kopplad till industrins ökade utsatthet för cyberincidenter, samt förväntade åtgärder i och med NIS-direktivet.

Bland utmaningarna nämns att standarden inte är ISO-klassad samt att många delar är under utveckling och att flera av dem riskerar att bli föråldrade. En generell utmaning är att verksamheterna inte alltid ser den ekonomiska nyttan i relation till kostnaderna och därmed är obenägna att implementera standarder inom cybersäkerhet.

Slutligen uppger en majoritet av studiedeltagarna att ISA/IEC 62443 kan och bör kompletteras med andra standarder. Exempelvis kan ISA/IEC 62443 användas på den fysiska detaljnivån med fokus på ICS, och kompletteras med ISO 27000 för den övergripande projektmetodiken.

Nyckelord: 62443, IACS/ICS, standarder, cybersäkerhet, kritisk infrastruktur.

Summary

ISA/IEC 62443 is a standard that focuses on industrial control systems (ICS). Although major parts are still in development, it has already begun to be used in Sweden and internationally.

The purpose of this report is to provide the Swedish civil contingency agency (MSB) with a greater understanding of the extent and application of the standard in Sweden, and thereby contribute to increasing its knowledge of the situation within the area of ICS. The use of the standard in Sweden is mapped through interviews with actors who have broad experience of a variety of areas. In addition, a comprehensive description of the content of ISA/IEC 62443 is provided.

The standard is considered to offer several advantages, including that it is complete over the entire life cycle and is tailor-made for ICS, and that it defines different security levels that can be subjected to different requirements. Other reasons for the use of ISA/IEC 62443 and the attention paid to it are the changed set of requirements from clients, connected to industry's increasing exposure to cyber incidents, as well as the measures expected in the advent of the NIS directive.

Among the challenges that may need to be met, are that it is not ISO-classified and many of its sections are still being developed, while others risk becoming obsolete. A general challenge that has been highlighted is that since the operators do not always see the economic benefits of cyber security standards, they are disinclined to implement them.

Finally, a majority of the study participants state that ISA/IEC 62443 can, and should, be complemented by other standards. For example, ISA/IEC 62443 could be used on the physical level of detail, with focus on ICS, supplemented by ISO 27000 for the overall project methodology.

Keywords: 62443, IACS/ICS, standards, cyber security, critical infrastructure.

Innehållsförteckning

1 Inledning

Det finns för närvarande flera standarder och standardserier inom området industriella informations- och styrsystem (ICS). En av dessa är ISA/IEC 62443 som trots att den fortfarande är under utveckling redan används och uppmärksammas såväl i Sverige som internationellt.

Myndigheten för samhällsskydd och beredskap (MSB) har inom ramen för NCS3[1] uppdragit åt Totalförsvarets forskningsinstitut (FOI) att undersöka hur ISA/IEC 62443 används och uppfattas av svenska aktörer.

1.1 Syfte och mål

Syftet med studien är att ge MSB en ökad förståelse för standardens omfattning och användning i Sverige för att på så vis bidra till ökad kunskap om de förutsättningar som råder inom ICS-området. För att uppfylla syftet har rapporten som mål att besvara följande frågor:

- Hur förhåller sig ISA/IEC 62443 till närliggande standarder?
- Hur används ISA/IEC 62443 av svenska ICS-aktörer?

Den första frågan besvaras genom en dokumentstudie där ISA/IEC 62443 och andra relevanta standarder ingår. Den andra frågan besvaras genom intervjuer med svenska aktörer. För att få perspektiv på det svenska användandets mognadsgrad och andra intressanta förhållanden, görs även en utblick mot Norge där standarden under de senaste åren tycks ha blivit relativt etablerad inom vissa områden.

1.2 Målgrupp

Studien vänder sig till MSB såväl som till systemägare och produkt- och tjänsteleverantörer som är verksamma inom ICS-området.

1.3 Disposition

I kapitel 2 redovisas metodval. I kapitel 3 sammanfattas och jämförs ISA/IEC 62443 och närliggande standarder utifrån en dokumentstudie. I kapitel 4 analyseras och presenteras användningen av ISA/IEC 62443 utifrån intervjusvaren och i kapitel 5 görs en jämförande utblick mot Norge. I kapitel 6 görs en avslutande sammanställning av studiens resultat.

[1] Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet.

2 Metod

I studien intervjuas ett antal personer som är verksamma inom ICS-området i Sverige och Norge. Den gemensamma nämnaren för deltagarna är att de har utvärderat eller implementerat standarder avsedda för ICS. Urvalet har gjorts bland aktörer med direkt eller indirekt koppling till MSB:s aktörsnätverk FIDI-SCADA.[2]

Intervjuerna har genomförts med hjälp av en intervjuguide (se bilaga 1). Intervjuerna har varit *semistrukturerade*, det vill säga de har inte begränsats strikt till guidens frågor. Både respondenten och intervjuaren har därmed, i viss mån, tillåtits skjuta in nya frågor och ställa följdfrågor som inte redan står i guiden. Svaren har brutits ner utifrån de teman som intervjudeltagarna har tagit upp. Dessa teman speglar delvis intervjuguiden, men i några fall har teman som skär tvärs genom intervjuguidens frågor identifierats. I andra fall har svar under flera frågor grupperats under ett och samma tema. Målet har varit att göra framställningen logisk och samtidigt lätt att följa.

Det ska poängteras att det inte går att generalisera studiens resultat eftersom intervjuerna har varit förhållandevis få.[3] Studien ska ses som en kartläggning och strukturering av ämnesområdet snarare än en uttömmande redogörelse av hur ISA/IEC 62443 används och uppfattas.

Istället för ICS (Industrial Control System) används i litteraturen ibland begreppet IACS (Industrial Automation and Control System). I rapporten används dessa begrepp synonymt.

[2] FIDI-SCADA är ett privatoffentligt samverkansforum som genom informationsutbyte, omvärldsanalys och framtagande av gemensamt material ökar informationssäkerheten i ICS.

[3] Totalt sju intervjuer med nio respondenter, de flesta i ledande positioner inom ICS-säkerhet, men med bred erfarenhet av många olika funktioner (integration, förvaltning, implementering, drift) och verksamheter (gruva, transport, kraftindustri, VA, tillverkningsindustri, med mera).

3 Introduktion till ISA/IEC 62443

ISA/IEC 62443, fortsättningsvis benämnd 62443, är en serie standarder och tekniska rapporter som definierar metoder för implementering av säkra ICS.

Standarden utgår från ANSI/ISA-99 som år 2010 godkändes av IEC och därmed numrerades om för att passa med övriga IEC-standarder. ISA-99 är fortfarande namnet på ISA:s ICS-säkerhetskommitté som utvecklar standarder för publicering i IEC 62443-serien.[4]

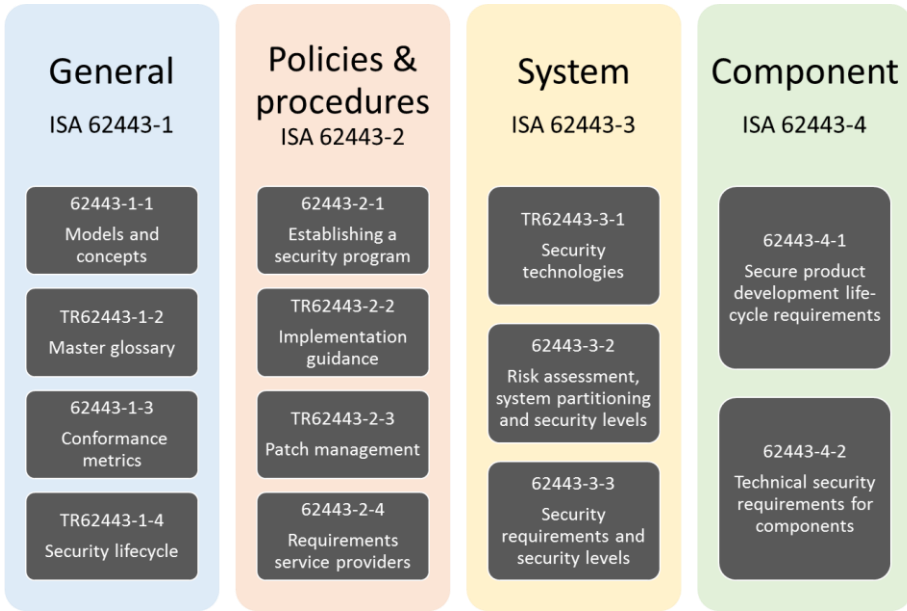
63442 har som syfte att förbättra ICS och ICS-komponenters tillgänglighet, integritet och konfidentialitet, samt att ge kriterier vid anskaffning och implementering av säkra system. Standarden behandlar de beståndsdelar som måste ingå i ett ledningssystem för ICS-säkerhet, och ger samtidigt vägledning för hur ett sådant system kan utvecklas. Dock betonas att vägledningen endast ger exempel och därför måste skräddarsys för att passa den specifika organisationen.[5]

Totalt består serien av fyra övergripande delar. Var och en av dessa innefattar standarder av relevans för såväl system- och anläggningsägare som produkt- och tjänsteleverantörer. De övergripande delarna är i tur och ordning:

- *General*: Behandlar ämnen gemensamma för hela serien, såsom begrepp och mått.
- *Policies and procedures*: Fokuserar på policyer och procedurer kopplade till ICS-säkerhet, såsom ”patch management”.
- *System*: Behandlar krav på systemnivå, såsom systemdesign och analys av säkerhetsrisker.
- *Component*: Behandlar krav för produktutveckling och komponenter för ICS.

Innehållet presenteras översiktligt i Figur 1.

[4] ISA (2018)
[5] ISA/IEC 62443, s. 7, 9



Figur 1: Översikt av innehållet i ISA/IEC 62443. Av utrymmesskäl har titlarna kortats ner.

I Figur 1 har titlarna av utrymmesskäl kortats ner. Prefixet *TR* anger att dokumentet är en teknisk rapport. Delar med nummer 1-4 (*Security life cycle and use cases*) och 2-2 (*Implementation guidance for an IACS security management system*) existerar endast som förslag och presenteras därför inte närmare i denna rapport.

De olika delarna är strukturerade enligt samma logik. Dels finns vissa så kallade *grundläggande krav* för säkerhet, dels en idé om *segmentering* som innebär att olika delar av ett och samma system kan delas in i olika zoner med olika säkerhetsnivåer och därmed olika strikta krav.

De grundläggande kraven är, något förenklat, följande:

- **Identifiering och autentisering**: Att identifiera och autentisera alla användare innan de ges tillträde till kontrollsystemet
- **Användningskontroll**: Att tilldela alla användare rättigheter som styr vilka åtgärder de kan utföra på systemet samt att övervaka användningen.
- **Systemintegritet**: Att säkerställa systemets integritet genom att förhindra otillåten manipulation.
- **Konfidentialitet**: Att säkerställa informationens konfidentialitet genom att förhindra att den avslöjas otillåtet.

- **Begränsat dataflöde**: Att begränsa flödet av data genom att segmentera systemet via zoner och gränsytor/kopplingar.
- **Incidenthantering**: Att svara på säkerhetsöverträdelser genom att varsla rätt instans, rapportera evidens och att vidta korrigerande åtgärder.
- **Tillgänglighet till resurser**: Att säkerställa tillgängligheten till systemets tjänster.

3.1 ISA 62443-1 General

Standardens första del – *General* – behandlar ämnen gemensamma för hela serien, såsom begrepp och mått. Nedan följer en mer detaljerad beskrivning av dess ingående delar. I rubrikerna anges inom hakparentes om respektive del är publicerad, föreligger som utkast eller om den endast finns som förslag.

3.1.1 ISA 62443-1-1 Models and concepts [Utkast]

ISA 62443-1-1 introducerar modeller och begrepp som beskrivs och tillämpas mer utförligt i de delar som följer. Här ingår såväl generella cybersäkerhetsbegrepp som begrepp och modeller specifika för ICS.[6] Det som tas upp är:

- Den omgivning (*situation*) inom vilken ICS används
- Generella begrepp
- En definition av ICS
- Grundläggande krav
- Grundläggande begrepp
- Modeller
- Serie 62443 som sådan

Omgivningen beskrivs som komplex och innefattar affärsmiljön, rådande system och trender samt potentiella konsekvenser. Det framhålls att samtliga säkerhetselement (människor, processer och teknologier) på olika sätt måste beaktas för att säkerhetsutmaningar ska kunna bemötas.[7]

De generella begreppen är säkerhetsomgivning, säkerhetsmål, minimala rättigheter, djupförsvar, analys av hot och risker, samt säkerhet för försörjningskedjor.[8]

[6] Ibid, s. 11
[7] Ibid s. 26-32
[8] Ibid s. 34-37

ICS definieras i termer av funktionalitet, system och gränssnitt, aktivitetsbaserade kriterier, resursbaserade kriterier samt konsekvensbaserade kriterier.[9]

De grundläggande kraven utgör grunden för efterföljande krav i standardserien. Kraven är de som anges i punktlistan på sidan 12 (ovan).[10]

De *grundläggande begreppen* är livscykler, zoner och gränsytor/kopplingar, säkerhetsnivåer, säkerhetsprogram samt säkerhet. Livscykler fokuserar på säkerhetsnivån i en del av systemet över tid, och kan förstås i termer av livscykler för produkter eller för ICS. Zonerna och gränsytor/kopplingarna utgör uppdelningar av aktuellt system i syfte att tilldela dem säkerhetsnivåer och därtill kopplade motåtgärder, och kan förstås i termer av fysiska eller logiska (t.ex. virtuella) zoner och gränsytor/kopplingar. Säkerhetsnivåerna kan förstås i termer av avsedda (önskad nivå), uppnådda (faktiska nivåer) och möjliga (den nivå som kan uppnås när systemen och komponenterna är rätt konfigurerade) nivåer. Säkerhet kan förstås i termer av såväl ”safety” som ”security”, och de båda antas påverka varandra ömsesidigt.[11]

Modellerna underlättar identifieringen av säkerhetsbehov och viktiga egenskaper i omgivningen. Modellerna delas in i kategorierna referensmodeller, arkitekturmodeller, samt zonmodeller. En referensmodell är ett generiskt perspektiv på ett produktionssystem uttryckt som en serie logiska nivåer. En arkitekturmodell beskriver de olika operativa komponenterna och hur de är kopplade sinsemellan. Zonmodeller är härledda ur arkitekturmodeller och grupperar elementen i övergripande enheter.[12]

3.1.2 ISA TR62443-1-2 Master glossary [Utkast]

ISA 62443-1-2 definierar termer och förkortningar. ICS definieras exempelvis som (1) en samling personal, hårdvara och mjukvara som kan påverka hur säker och tillförlitlig en industriell process är, eller (2) en samling personal, hårdvara, mjukvara och policyer som är involverade i driften av en industriell process och som kan påverka hur säker och tillförlitlig driften är.[13]

[9] Ibid s. 34-39
[10] Ibid s. 40-42
[11] Ibid s. 42-71
[12] Ibid s. 71-75
[13] ISA/IEC 62443-1-2

3.1.3 ISA 62443-1-3 Cyber security system conformance metrics [Utkast]

ISA 62443-1-3 specificerar överensstämmelsemått för systemsäkerhet (system security conformance metrics) och deras tillämpning, det vill säga mått att använda inom ett säkerhetsprogram över ett systems livscykel.[14]

Närmare bestämt behandlas följande:

- Ett processbaserat ramverk för utvecklingen av överensstämmelsemått (process-based framework to develop conformity metrics)
- Specificerade kravmåls spårbarhet och relationer (traceability to requirement objectives and relationships)
- Grundläggande dataobjekt (core data objects)
- En minsta uppsättning överensstämmelsemått för specificerade kravmål (minimun set of conformance metrics for specified requirement objectives)

Ramverket innefattar egenskaper för bra överensstämmelsemått, en utvecklings- och implementeringsprocess för måtten, samt en roll- och ansvarsfördelning. Bra mått bör ge kvantifierbar information eller kvalitativa indikatorer, data som understödjer måtten bör vara lättåtkomliga från aktuellt ICS eller andra relevanta källor, endast upprepningsbara processer bör underkastas mätning, och måtten bör vara användbara för att spåra prestanda och inrikta resurser. Utvecklings- och implementeringsprocessen består av att göra nya mätningar eller uppdatera gamla, insamla data, analysera, rapportera, samt löpande förbättra mätningar. Roll- och ansvarsfördelningen avser vem som gör vad och en organisation kan samla flera eller rentav alla dessa roller i en och samma övergripande roll.[15]

Spårbarheten fastställer ett övergripande perspektiv på kravmålen i tillämpliga delar av standardserien. Avsnittet är inte ännu färdigställt, men bland annat framhålls att det behövs en systemmodell innan överensstämmelse i förhållande till kravmålen alls kan mätas. Därför utgår standarden från en modell av ICS bestående av människor, processer och teknologi.[16]

De *grundläggande dataobjekten* behövs för att uppfylla standardens kravmål. Avsnittet är inte färdigställt, men bland annat framhålls att objekten ska specificeras som namngivna objekt och attribut, samt att attributen ska vara antingen primitiva, strukturerade eller listade värdetyper. Primitiva värdetyper saknar intern struktur (värdeegenskaper), strukturerade värdetyper har intern

[14] ISA/IEC 62443-1-3 s. 11
[15] Ibid s. 22-27
[16] Ibid s. 27

struktur (två eller fler värdeegenskaper), medan listade värdetyper har en fastställd uppsättning litteraler.[17]

Den minsta uppsättningen överensstämmelsemått behövs för att uppfylla standardens specificerade kravmål.[18]

3.1.4 ISA TR62443-1-4 IACS Security life cycle and use cases [Förslag]

Dokumentet existerar endast som förslag och presenteras därför inte närmare i denna rapport.

3.2 ISA 62443-2 Policies and procedures

Standardens andra del – *Policies and procedures* – fokuserar på policyer och procedurer kopplade till ICS-säkerhet, såsom exempelvis ”patch management”. Nedan följer en mer detaljerad beskrivning av dess ingående delar. I rubrikerna anges inom hakparentes om respektive del är publicerad, föreligger som utkast eller om den endast finns som förslag.

3.2.1 ISA 62443-2-1 Establishing an industrial automation and control system security program [Publicerad]

ISA 62443-2-1 definierar vilka element som är nödvändiga för etableringen av ett ledningssystem för cybersäkerhet (cyber security management system) och ger vägledning för hur dessa kan utvecklas.[19]

Ett ledningssystem ska omfatta följande element:

- Riskanalys
- Hantering av risker (genom ledningssystemet)
- Övervakning och förbättring av ledningssystemet

Riskanalysen behandlar mycket av den information som utgör input till övriga element i ledningssystemet.[20]

Hantering av risker handlar om merparten av ledningssystemets krav och information och innefattar de underliggande grupperna säkerhetspolicy, organisation och medvetenhet; valda motåtgärder, samt implementering.[21]

[17] Ibid s. 32-39
[18] Ibid s. 39-40
[19] ISA/IEC 62443-2-1
[20] Ibid s. 18-19
[21] Ibid s. 20-36

Övervakning och förbättring av ledningssystemet säkerställer att ledningssystemet efterlevs samt utvärderar dess effektivitet.[22]

3.2.2 ISA TR62443-2-2 Implementation guidance for an IACS security management system [Förslag]

Dokumentet existerar endast som förslag och presenteras därför inte närmare i denna rapport.

3.2.3 ISA TR62443-2-3 Patch management in the IACS environment [Publicerad]

ISA 62443-2-3 är en teknisk rapport som beskriver olika krav för systemägare och ICS-leverantörers patch management-program.[23] Rapporten rekommenderar ett fastställt format för distribution av patchar, samt rekommenderar vissa specifika aktiviteter för produktleverantörers utveckling av patchar, liksom för systemägarnas installation av dem.[24]

Följande behandlas:

- Patchning för ICS (industrial automation and control system patching)
- Rekommenderade krav för systemägare (recommended requirements for asset owner)
- Rekommenderade krav för produktleverantörer för ICS (recommended requirements for IACS product supplier)
- Utbyte av patchinformation (exchanging patch information)

Till skillnad från flera andra typer av system riskerar ett bristfälligt patch management-program att leda till mer än endast förlust av data eller driftstopp eftersom även personalens fysiska säkerhet, produktkvalitén, etcetera, kan påverkas.[25] I 62443 framhålls att en mängd information behöver finnas tillgänglig eftersom ICS vanligen bygger på kommersiella operativsystem, som i sin tur kräver regelbundna uppdateringar för att felaktigheter och säkerhetsbrister ska kunna upptäckas och korrigeras. Att implementera ett system för patch management kräver, enligt 62443, bland annat kunskap om vilka patchar som finns tillgängliga, om patcharna är tillämpliga på installerade system, om patcharna har testats gentemot installerade produkter, samt om leverantören rekommenderar att patcharna installeras. I standarden föreslås ett format för

[22] Ibid s. 36-38
[23] ISA/IEC 62443-2-3
[24] ISA/IEC 62443-2-3 s. 8
[25] Ibid s. 8

utbyte av den patch-information som behövs för att kunna identifiera en produkt, en lämplig patch och patchens aktuella status.[26]

3.2.4 ISA 62443-2-4 Security program requirements for IACS service providers [Publicerad]

ISA 2443-2-4 specificerar en uppsättning krav för säkerhetsfunktioner och vänder sig till leverantörer av integration och underhåll av automatiseringslösningar.[27] Standarden innehåller en modell med riktmärken för uppfyllandet av kraven. Riktmärkena definieras i termer av *mognadsnivåer*, där varje nivå är kumulativt mer avancerad än föregående nivå. I samband med begreppsdefinitionerna diskuteras olika sätt på vilka standarden kan användas av tjänsteleverantörer och system- och anläggningsägare, t.ex. i förhandlingar dem emellan.[28]

3.3 ISA 62443-3 System

Standardens tredje del – *System* – behandlar krav på systemnivå, såsom systemdesign och analys av säkerhetsrisker. Nedan följer en mer detaljerad beskrivning av dess delar. I rubrikerna anges inom hakparentes om respektive del är publicerad, föreligger som utkast eller om den endast finns som förslag.

3.3.1 ISA TR62443-3-1 Security technologies for industrial automation and control systems [Utkast]

ISA 62443-3-1 är en teknisk rapport som ger en översikt över verktyg och tekniker som regelbundet används inom modern ICS.[29]

Närmare bestämt behandlas följande:

- Tekniker för autentisering och auktorisering (authentication and authorization technologies)
- Tekniker för nätverksskydd (network protection technologies)
- Krypteringstekniker och datavalidering (encryption technologies and data validation)
- Verktyg för förvaltning, revision, mätning, övervakning och upptäckt (management, audit, measurement, monitoring and detection tools)
- Tekniker för fjärråtkomst (remote access technologies)

[26] Ibid s. 14-15
[27] ISA/IEC 62443-2-4
[28] Ibid s. 14-15
[29] ISA/IEC 62443-3-1

- Cybersäkerhetens programkontext (cybersecurity program context)

3.3.2 ISA 62443-3-2 Security risk assessment, system partitioning and security levels [Utkast]

ISA 62443-3-2 fastställer skilda åtgärder för att vägleda organisationer genom riskvärderingsprocessen och för att vidta motåtgärder (i form av segmentering och säkerhetsnivåer) som minskar identifierade risker till acceptabla nivåer.[30]

Följande behandlas:

- Krav för avgränsningen av ett aktuellt system för ICS (defining a system under consideration, SuC)
- Krav för uppdelning av det aktuella systemet i zoner och gränsytor/kopplingar (partitioning the SuC into zones and conduits)
- Krav för analys av risker för varje zon och kanal (assessing risk for each zone and conduit)
- Krav för fastställande av en säkerhetsnivå för varje zon och kanal (establishing secuirty target for each zone and conduit, SL-T)
- Krav för dokumentation av säkerhetskraven (documenting the security requirements)

3.3.3 ISA 62443-3-3 System security requirements and security levels [Publicerad]

ISA 62443-3-3 tillhandahåller detaljerade tekniska krav för ICS utifrån de grundläggande krav som beskrivs i 62443-1-1.[31] I bilagor diskuteras vektorer för säkerhetsnivåerna, samt hur säkerhetsnivåerna skiljer sig åt och förhåller sig till säkerhetskraven (mapping of SRs and Res to FR SL levels 1-4).[32]

Först beskrivs vissa vanliga säkerhetsbegränsningar hos kontrollsystem, sedan beskrivs krav gällande identifiering och autentisering, användningskontroll, systemintegritet, datakonfidentialitet, begränsat dataflöde (restricted data flow), incidenthantering (timely response to events) samt tillgänglighet av resurser. Kravet gällande *identifiering och autentisering* innebär att identifiera och autentisera alla användare innan de ges tillträde till kontrollsystemet. Kravet gällande *användningskontroll* innebär att genomdriva de tilldelade privilegierna (enforce the assigned privileges) för en autentiserad användare att utföra begärd åtgärd på ICS, samt att övervaka användningen av privilegierna ifråga. Kravet gällande *systemintegritet* innebär att säkerställa ICS integritet för att förebygga

[30] ISA/IEC 62443-3-2
[31] ISA/IEC 62443-3-3
[32] Ibid s. 67-76

otillåten förändring. Kravet gällande *konfidentialitet* innebär att säkerställa att information i kommunikationskanaler och databanker (data repositories) förblir konfidentiell för att förhindra röjning. Kravet gällande *begränsat dataflöde* innebär att segmentera kontrollsystemet via zoner och ledningar för att begränsa ett onödigt flöde av data. Kravet gällande incidenthantering innebär att svara på säkerhetsöverträdelser genom att underrätta rätt instans, rapportera erforderliga bevis på överträdelsen samt att vidta lämpliga korrigerande åtgärder när väl incidenten upptäcks. Kravet gällande *tillgänglighet av resurser* innebär att säkerställa tillgängligheten av kontrollsystemets viktiga tjänster, alltså att säkerställa att kontrollsystemet är resilient mot olika typer av händelser.[33]

3.4 ISA 62443-4 Component

Standardens fjärde del – *Component* – behandlar krav för produktutveckling och komponenter för ICS. Nedan följer en mer detaljerad beskrivning av dess delar. I rubrikerna anges inom hakparentes om respektive del är publicerad, föreligger som utkast eller om den endast finns som förslag.

3.4.1 ISA 62443-4-1 Secure product development life-cycle requirements [Utkast]

ISA-62443-4-1 specificerar skilda processkrav för en säker utveckling av produkter för användning inom ICS.[34] Den fastställer en livscykel (secure development life-cycle, SDL) som innefattar:

- Säkerhetshantering (security management)
- Säkerhetskrav (specification of security requirements)
- Inbyggd säkerhet (security by design)
- Säker implementering (secure implementation)
- Säkerhetsverifiering och valideringstestning (security verification and validation testing)
- Hantering av säkerhetsdefekter (security defect management)
- Hantering av säkerhetsuppdateringar (security update management)
- Riktlinjer för säkerheten (security guidelines)

I standarden beskrivs vissa allmänna principer samt en mognadsmodell. Det huvudsakliga målet med principerna är att tillhandahålla ett ramverk för utformandet, byggandet, bevarandet och utfasandet av ICS-produkter och ICS-system präglat av ”security by design” och djupförsvar. Mognadsmodellen

[33] Ibid s. 24-66
[34] ISA/IEC 62443-4-1

fastställer vissa nivåer för uppfyllandet av standardens krav. Riktlinjerna är ”initial”, ”hanterad” (managed), ”fastställd” (defined), samt ”förbättrande” (improving). ”Initial” avser huruvida organisationen har tillämpat processen åtminstone en gång. ”Hanterad” gäller huruvida det finns en formell procedur som kräver att processen efterlevs. ”Fastställd” gäller huruvida den formella proceduren efterlevs konsekvent. ”Förbättrande” gäller huruvida den formella processen mäts och förbättras.[35]

Standarden anger också ett antal *processer för säkerhetshantering* som är kopplade till de allmänna principerna och stegen i livscykeln. Dessa syftar till att säkerställa att de säkerhetsrelaterade aktiviteterna planeras, dokumenteras och verkställs på ett adekvat sätt genom produktens livscykel.

- Processerna för *specificering av säkerhetskrav* används för att dokumentera säkerhetsfunktioner, såsom autentisering, kryptering, etcetera, som krävs för en produkt i förhållande till den förväntade produktsäkerhetskontexten, såsom den fysiska säkerhetsnivån.
- Processerna för *inbyggd säkerhet* används för att säkerställa att produkten är ”secure by design”, avseende alla steg i produktdesignen.
- Processerna för *säker implementering* används för att säkerställa att produktens egenskaper implementeras säkert.
- Processerna för säkerhetsverifiering och valideringstestning används för att dokumentera den testning som krävs för (1) att säkerställa att alla produktens säkerhetskrav har uppfyllts, (2) att produktsäkerheten bibehålls när produkten används i sin produktsäkerhetskontext, samt (3) att produkten konfigureras för att använda sin djupförsvarsstrategi.
- Processerna för *hantering av säkerhetsdefekter* används för att hantera säkerhetsrelaterade fel hos en produkt som har konfigurerats för en viss produktsäkerhetskontext.
- Processerna för *säkerhetsuppdatering* används för att säkerställa att säkerhetsuppdateringar för produkterna testas för regression och görs tillgängliga för produktanvändarna.
- Processerna för *vägledning för säkerhet* används för att tillhandahålla dokumentation för hur integration, konfiguration och upprätthållande av produktens djupförsvarsstrategi i enlighet med dess produktsäkerhetskontext ska gå till.[36]

[35] Ibid s. 21-24
[36] Ibid s. 24-53

3.4.2 ISA 62443-4-2 Technical security requirements for IACS components [Utkast]

ISA-62443-4-2 tillhandahåller detaljerade tekniska krav för komponenter till kontrollsystem (detailed technical control system component requirements) utifrån de sju ovan nämnda grundläggande krav (foundational requirements).[37]

Följande områden behandlas:

- Vanliga säkerhetsbegränsningar hos kontrollsystem
- Identifiering och autentisering
- Användningskontroll
- Systemintegritet
- Datakonfidentialitet
- Begränsat dataflöde
- Incidenthantering
- Tillgång till resurser
- Krav för mjukvaruapplikationer (software application requirements)
- Krav för inbäddade enheter (embedded device requirements)
- Krav för värdenheter (host device requirements)
- Krav för nätverksenheter (network device requirements)

Standarden tillhandahåller detaljerade tekniska krav för komponenter till kontrollsystem utifrån de ovan nämnda grundläggande kraven.[38]

I stort är standarden densamma som ISA 62443-3-3, men till skillnad från denna behandlar ISA-62443-4-2 *komponenter* till kontrollsystem snarare än hela system. Komponenter inkluderar i standarden även *mjukvaruapplikationer*, *inbyggda enheter* (embedded devices), samt *nätverk*.[39]

3.5 Relaterade standarder

Det finns flera standardserier, och standardliknande dokument, som ligger mer eller mindre nära 62443. Under intervjuerna nämndes ISO 27000, IEC 62351, NIST Cyber Security Framework (NIST CSF) och NERC CIP:

- *ISO 27000* behandlar ledningssystem för informationssäkerhet. Standarderna beskriver krav på ledningssystem för informationssäkerhet och för certifieringsorgan, men beskriver även olika generella processer

[37] ISA/IEC 62443-4-2 (ej sidnumrerad)
[38] ISA/IEC 62443-4-2 (ej sidnumrerad)
[39] Ibid (ej sidnumrerad)

och ger vägledning för exempelvis införandet av sådana ledningssystem.[40]

- *IEC 62351* behandlar informationssäkerhet för styrsystem inom kraftområdet (power system control operations). Serien är utformad för att främja säkerheten i enlighet med olika kommunikationsprotokoll fastställda av TC 57, en kommitté inom IEC som utvecklar standarder för informationsutbyte riktade till kraftsystem och närliggande områden.[41]
- NIST CSF är ett ramverk som behandlar cybersäkerhet hos kritisk infrastruktur. Ramverket är leverantörsneutralt och bygger på och hänvisar till flera redan föreliggande standarder och vägledningar.[42] NIST 800-82, *Guide to Industrial Control System (ICS) Security*, som gavs ut i maj 2015, beskriver hur en mängd olika typer av ICS ska säkras mot cyberattacker med samtidigt beaktande av ICS-specifika krav på prestanda, tillförlitlighet och säkerhet.[43]
- *NERC CIP* behandlar cybersäkerhet hos stamnät och produktionsanläggningar, typiskt på nationell nivå.[44]

Dokumenten har bland annat jämförts inom ramen för EU-projektet ESCoRTS[45], vars analys har kompletterats av anställda vid ABB.[46] Tre parametrar undersöks där. För det första huruvida standarden (eller motsvarande) är relevant för IT och/eller ICS, för det andra huruvida den har djup och/eller bredd, det vill säga om den fokuserar på tekniska detaljer eller på processer, och för det tredje om den är relevant för operatörer och/eller leverantörer.

Analysen ger vid handen att 62443 och NIST CSF är relevanta för ICS och 27000 främst för IT, medan NERC CIP och 62351 är relevanta specifikt för energisektorn.

Analysen ger vidare att 62443 är både detaljerad och heltäckande, att 62351 är detaljerad men inte särskilt heltäckande medan NERC CIP, NIST CSF och ISO 27000 är heltäckande men inte särskilt detaljerade.

[40] SS-EN ISO/IEC 27000:2017
[41] TS IEC 62351-1: 2007
[42] National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity
[43] Wikipedia (2018)
[44] NERC: North American Electric Reliability Corporation. CIP: Critical Infrastructure Protection.
[45] ESCoRTS: European Network for the Security of Control and Real Time Systems, 16 June 2008-15 December 2010: Publishable Summary.
[46] Lindström, Tomas. Cyber Security for Process Control Systems: ABB's view. https://ics.kaspersky.com/media/ics-conference-2017/Tomas-Lindstrom-Cyber-Security-for-Process-Control-Systems.pdf.

Slutligen ger analysen att 62443 har en tonvikt mot operatörer även om den också är relevant för leverantörer. 62351 tycks omvänt ha en tonvikt mot leverantörerna, även om den också är relevant för operatörerna. NERC CIP, NIST CSF och ISO 27000 tycks ha en klar tonvikt mot operatörerna.

4 Användningen i Sverige

Nedan redovisas analysen av intervjuerna om hur 62443 används och uppfattas i Sverige. Framställningen bygger helt på intervjusvaren och det som presenteras är författarnas tolkning av hur studiedeltagarna upplever att saker och ting är. Författarna ansvarar fullt ut för eventuella feltolkningar.

4.1 Skäl till att 62443 uppmärksammas och används

Studiedeltagarna uppger flera skäl till att 62443 har börjat uppmärksammas och användas, antingen inom den egna organisationen eller av andra. De uppger också några skäl som i framtiden skulle kunna leda till att serien uppmärksammas och används i högre grad än vad som nu är fallet.

Några nämner verksamheternas ökade utsatthet för cyberincidenter. Enligt dem beror utsattheten på att systemen alltmer kopplas upp och digitaliseras, att man använder samma protokoll och switchar som IT-världen, att man har drabbats av cyberangrepp, etcetera.

Några nämner det faktum att serien uttalat behandlar just ICS. Standarder utformade för IT-säkerhet är mindre tillämpbara på ICS, medan 62443 upplevs ta hänsyn till rätt saker och vara anpassad till de omständigheter som ofta råder runt sådana system. Här avses, vad författarna förstår, bland annat segmenteringslogiken i 62443, där olika delar av systemet kan underkastas olika säkerhetskrav beroende på vad delarna klarar av och har för behov.

Några nämner att serien bidrar med en gemensam nomenklatur och att det är bra att ha termer definierade och skrivna krav och rekommendationer som man kan föra en diskussion runt, dels i dialogen mellan operatörer och leverantörer, dels inom den egna organisationen.

Några nämner en förändrad kravbild från kunderna. Den förändrade kravbilden är kopplad till industrins ökade utsatthet för cyberincidenter, men även till introduktionen av den amerikanska standarden NERC-CIP 2009 inom ICS-området.

En studiedeltagare nämner förväntade åtgärder i och med NIS-direktivet. Verksamheterna vill ha en standard att luta sig mot eftersom direktivet kan medföra nya krav än de som råder i dagsläget.

En annan nämner seriens övergång till IEC. Ursprungligen betecknades serien ISA99 (International Society for Automation) men sedermera har den anpassats till och godkänts av IEC (International Electrotechnical Commission). Denna övergång har bidragit till att serien uppmärksammas.

Några nämner att förändrade lagkrav skulle kunna leda till att serien uppmärksammas och används i framtiden. I Tyskland är industrin underkastad lagkrav som ligger nära serie ISO 27000, vilket upplevs främja denna.

Några nämner att rekommendationer till berörda aktörer skulle kunna leda till att serien uppmärksammas och används i framtiden. De som arbetar med serien gör det av eget intresse, inte för att någon har pekat ut den som lämplig. De anser att det därför behövs mer reklam för serien, bland annat från myndighetshåll.

Studiedeltagarna uppger även flera skäl till att serie 62443 *inte* uppmärksammas eller används.

En studiedeltagare nämner att verksamheterna är känsliga för driftavbrott och därför obenägna att implementera nya standarder. Om man startar en ny verksamhet är det lättare att implementera nya standarder, medan även korta driftavbrott i en verksamhet som redan finns kan stoppa processer som kan ta lång tid att få igång igen.

Några nämner att verksamheterna inte alltid ser den ekonomiska nyttan i relation till kostnaderna, varför de är obenägna att implementera standarder inom cybersäkerhet. Det beror på stränga ekonomiska ramar, en önskan om avkastning på investeringar tillsammans med ekonomiska vinster med att koppla upp systemen mot internet.

En studiedeltagare nämner svårigheterna att certifiera sig och sin organisation eftersom certifieringskurserna är förenade med höga kostnader dessutom bara går i utlandet.

4.2 Vilka delar av 62443 används och varför?

En majoritet av studiedeltagarna uppger att det är oklart om och hur 62443 används av andra aktörer än dem själva. Detsamma gäller andra standarder. Standarder överlag uppges snarast fungera som inspiration och målbild, eller också görs hänvisningar till dem mest av slentrian. En uppfattning var att vissa leverantörer påstår sig ha funktionsuppfyllnader inom säkerhetsområdet som man inte har.

Flera studiedeltagare uppger att eftersom inte alla delar av serien är publicerade ännu (somliga föreligger endast som utkast) används heller inte alla delar. Angående de delar som faktiskt används uppger flera studiedeltagare att de väljer de delar och föreskrifter som är relevanta och applicerbara. Vilka delar som används skiftar beroende på om man är systemägare, produkt- eller tjänsteleverantör, liksom beroende på vad man själv eller ens leverantörer klarar av eller har råd med.

Det finns inga lagkrav på att man ska använda alla standardens delar, eller ens delarna i sin helhet. En studiedeltagare uppger att man implementerar delsegment

för att kunna bygga vidare på dem senare. Standardserien är för omfattande för att det ska vara praktiskt möjligt att implementera den fullt ut. Den är ju heller inte färdig än. Man väljer därför ut delar, exempelvis genom att segmentera och klassificera systemet i termer av viktigaste zoner, för att eventuellt kunna nå en mer fullödig implementering i framtiden. Exempel på delar som studiedeltagarna uttalat använder är 2-4 (Security program requirements for IACS service providers) och 3-3 (System security requirements and security levels).

4.3 I vilken grad är föreskrifterna i 62443 tillämpliga?

Några studiedeltagare uppger att föreskrifterna måste tolkas innan de kan tillämpas. Serien ses som ett arbetssätt eller en metodik, och ett försök att standardisera begrepp, snarare än en checklista. Det är därför inte helt trivialt att avgöra vad man faktiskt måste göra för att uppfylla en given föreskrift. Tillämpningen blir därför något subjektiv.

Flera studiedeltagare uppger att tillämpningen av 62443 måste anpassas efter den specifika verksamheten och att detta beror på att betingelserna i de olika verksamheterna och programvarorna är olika. Det beror också på att somliga krav är för dyra för att bygga in i verksamheten.

4.4 Används 62443 ensam eller med andra standarder?

En majoritet av studiedeltagarna uppger att 62443 brukar kompletteras, eller kan och bör kompletteras, av andra standarder. En studiedeltagare kompletterar exempelvis 62443 med ISO 27000, där den senare används för den övergripande projektmetodiken, medan den 62443 används på den fysiska detaljnivån och med fokus på just ICS. En annan studiedeltagare menar att det vore naturligt att förena 62443 med ISO 27000, där den senare skulle kunna användas för krav på systemägaren själv, medan 62443 skulle kunna användas som krav på dennes leverantörer.

En studiedeltagare uppger att hur standarderna kombineras skiftar från aktör till aktör. En annan studiedeltagare uppger dock att 62443 inte verkar kompletteras av andra cybersäkerhetsstandarder. Däremot kompletteras 62443 av standarder som gäller andra omständigheter, exempelvis elsäkerhetsföreskrifter. Som framgår ovan delas dock inte denna bild av alla studiedeltagare.

4.5 Särdrag, styrkor och svagheter

Studiedeltagarna nämner flera *särdrag* hos 62443.

En studiedeltagare nämner att jämfört med ISO 27000, som främst fokuserar på IT, fokuserar 62443 på ICS. ISO 27000 används mer av de som arbetar med ”vanlig IT-säkerhet”, även om den också används och kan utgöra ett bra ramverk vid säkerhetsarbetet för ICS, särskilt avseende de frågor som relaterar till IT-aspekter. ISO 27000 går dock inte in på de mer tekniska krav som är specifika för ICS, till skillnad från 62443.

En annan nämner att jämfört med ISO 27000, som certifierar organisationer, certifierar 62443 även komponenter och system. Eftersom ISO 27000 certifierar organisationer kan man inte certifiera det som levereras till organisationen. Snarare än att systemet certifieras, certifieras istället kunden där systemet installeras, till skillnad från med 62443. I linje med detta nämner en studiedeltagare att jämfört med ISO 27000, som är relevant för systemägare, är 62443 även relevant för leverantörer.

Några studiedeltagare anger att jämfört med ISO 27000, som fokuserar på datas konfidentialitet, fokuserar 62443 på datas tillgänglighet och integritet (riktighet). Därmed är 62443 mer riktad mot industriell verksamhet.

En studiedeltagare nämner att jämfört med ISO 27000, som berättar vad man ska göra, berättar 62443 även *varför och hur* man bör göra något. ISO 27000 förklarar inte varför serien innehåller vissa föreskrifter eller hur man uppfyller dem. Till viss del i strid med detta nämner några studiedeltagare att jämfört med IEC 62351 fokuserar 62443 mer generellt på vad som ska göras. 62351 är mycket detaljrik men gör inte anspråk på att ha ett helhetsperspektiv, den är mer av en hur-standard medan 62443 är mer en vad-standard. 62351 kan därför appliceras på vissa delar i en produkt men inte på ett helt system, till skillnad från 62443.

Studiedeltagarna nämner också flera *styrkor* hos serie 62443.

Några studiedeltagare nämner exempelvis att serien kan användas över ett systems hela livscykel.

Några nämner att serien skiljer mellan, och täcker in, både komponenter och system, systemägare och leverantörer. Serien är alltså relativt komplett och som sådan relevant för flera olika typer av aktörer.

En studiedeltagare nämner att serien inte ställer för höga krav. Inom cybersäkerhetsområdet finns en tendens att kräva för mycket, medan föreskrifterna i 62443 är rimliga krav att ställa.

En studiedeltagare nämner att serien kan medföra transparens och förutsägbarhet i leverantörsledet. Som sådan kan serien förhindra att leverantörerna undviker relevanta säkerhetskrav.

Flera studiedeltagare nämner att serien skapar en gemensam nomenklatur. Standarder gör det lättare att tala samma språk, vilket är bra såväl i dialogen med kunder och leverantörer som inom den egna organisationen. Eftersom 62443 inte bara är en lång lista med krav, utan uppdelad i *kategorier av krav*, gör den det även möjligt att tala på flera olika nivåer – från detaljnivå upp till en högre abstraktionsnivå. Ibland saknas dock kunskap om att serien är uppdelad på det sättet, varför aktörer ibland begär att man ska uppfylla 62443 i sin helhet. Något sådant går dock inte enligt studiedeltagaren, eftersom inte alla seriens delar är relevanta för alla aktörer.

Studiedeltagarna nämner också flera *svagheter* hos 62443:

En studiedeltagare nämner att serien inte är färdig än och tar tid att utveckla. Eftersom serien inte är färdig än kan inte heller någon påstå att man uppfyller den, och då flera aktörer är inblandade blir arbetet med att ta fram serien lite långsamt.

Några studiedeltagare nämner att serien är för omfattande och komplex. Serien verkar exempelvis inte förutsätta att det redan föreligger något ledningssystem för informationssäkerhet. Snarare verkar den ha en ambition att vara heltäckande och som sådan kunna lösa alla problem. Man menar att det hade varit bättre om man riktat in serien mot ett specifikt område, exempelvis komponenter. Som framgår ovan verkar dock andra studiedeltagare betrakta seriens heltäckande karaktär som en styrka, och inte heller måste man som en viss typ av aktör beakta samtliga av seriens delar – de enskilda delarna har olika relevans för olika typer av aktörer.

En studiedeltagare nämner att serien till viss del har en oklar relation till ISO 27000 och att seriens del 2-1 (*Establishing an industrial automation and control system security program*) är snarlik ISO 27000. Deltagaren upplever det visserligen som rätt att delen finns med i serien, men ser det inte som självklart att styrsystemavdelningen tar med sig denna del till IT-avdelningen och meddelar att det är denna standard man ska arbeta efter.

En annan studiedeltagare nämner att serien inte är en ISO-standard. I Sverige är vi mer vana vid ISO, medan serie 62443 är en ISA/IEC-standard.

En studiedeltagare nämner att serien avhåller sig från detaljer. Som nämns ovan är det inte helt trivialt att avgöra vad man faktiskt måste göra för att uppfylla en given föreskrift.

4.6 Betydelse i relation till leverantörer och kunder

En studiedeltagare uppger att 62443 är viktig med tanke på rådande hotbild. Men deltagaren ser det som ett problem att så få kollegor och kunder förstår vilka risker som finns. I dialogen med kunder har de ännu inte mognadsgraden att förstå att deras verksamhet faktiskt kan bli utsatt för attacker.

Några studiedeltagare uppger att serien har eller kan ha betydelse i förhållande till leverantörerna. Flera studiedeltagare uppger dock att serien saknar eller har liten betydelse i förhållande till kunderna. I motsats till detta menar några studiedeltagare att serien har eller kan ha betydelse också i förhållande till kunderna. Å ena sidan skapar serien ett gemensamt språk för kunder och leverantörer. Eftersom serien behandlar hela systemets livscykel finns det tydliga dokument som kan hjälpa till i aktörernas kravställningar gentemot varandra. Å andra sidan drivs försäljningen mycket av vilka lagar som gäller hos kunden. Vid internationell försäljning används därför ISO 27000 mycket mot Tyskland, medan NERC-CIP används mycket mot USA.

4.7 Certifiering

Ingen av studiedeltagarna uppger att deras organisation eller det de levererar har certifierats. En studiedeltagare menar dock att certifiering nu i högre grad än tidigare efterfrågas av kunderna. Enligt några studiedeltagare finns det två stora certifieringsorgan för 62443; TÜV SÜD och ISA Secure.[47] En av studiedeltagarna uttrycker en förhoppning om att dessa certifieringsprogram ska uppfattas som likvärdiga i kundernas ögon, men har samtidigt farhågan att de kommer att efterfråga certifiering utförd av det ena eller andra certifieringsorganet.

[47] Siemens är ett av de företag som lyfter fram att de har varit tidiga med att certifiera produkter enligt 62443. (Siemens, 2018)

5 Utblick Norge

För att komplettera den bild som de svenska aktörerna givit om användningen av 62443 intervjuades även två norska aktörer. Dessa tillhör delvis samma bransch och samarbetar också sedan ett par år inom ett initiativ taget av Det Norske Veritas (DNV) för att ta fram en best practice-guide för tillämpning av 62443 inom olje- och gasindustrin.[48] Respondenterna hade båda praktisk erfarenhet av 62443.

De norska studiedeltagarna uppgav flera anledningar till att 62443 har börjat användas. I flera fall överensstämmer dessa med de anledningar som de svenska deltagarna uppgav, exempelvis att 62443 så specifikt behandlar just ICS och att det är viktigt med en gemensam nomenklatur inom området. Därtill svarade en av studiedeltagarna att det finns flera stora aktörer inom deras område som stödjer och använder 62443 vilket skapar en drivkraft för att själv använda den. Den andra studiedeltagaren svarade också att organisationen undersökte vilka standarder som dess huvudleverantörer nyttjade, vilket ofta just varit 62443. Genom att själva använda samma standardserie erhålls både en bild av huvudleverantörernas förståelse för cybersäkerhet och en gemensam terminologi.

De delar av serien som väsentligen används av de norska aktörerna är

- 2-1: Establishing an industrial automation and control system security program
- 2-4: Security program requirements for IACS service providers
- 3-2: Security risk assessment, system partitioning and security levels
- 3-3: System security requirements and security levels

Dessa delar upplevs utifrån den egna verksamheten vara de mest relevanta. I dagsläget finns 3-2 visserligen endast som utkast men den används till viss del ändå utifrån avstämningar med utgivaren. De svenska studiedeltagarna uppgav att de främst använde delarna 2-4 och 3-3.

Utmaningen med serien anses vara att den beskriver *vad* man ska göra, men inte *hur* man bör göra det. Den är således ingen ”kokbok för exakt vad man ska göra”. Detta är också anledningen att de norska aktörerna arbetat fram den best practice-guide som nämns ovan. Eftersom serien är så omfattande beskriver respondenterna att det finns ett behov av att plocka ut vissa krav, vilket också

[48] DNVGL-RP-G108 *Cyber security in the oil and gas industry based on IEC 62443*. Guiden finns för nedladdning på https://www.dnvgl.com/oilgas/download/dnvgl-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html.

görs inom ramen för den nämnda best practice-guiden. Detta är en uppfattning som delas av svenska studiedeltagare.

Båda de intervjuade respondenterna nämner att ISO 27000-serien och 62443 kompletterar varandra väl, där ISO 27000 är till för en kontorsmiljö med fokus på konfidentialitet, och 62443 är till för ICS där istället tillgänglighet och riktighet är viktigare. Även svenska studiedeltagare ser 62443 som mer fokuserad på tillgänglighet och riktighet, och menar att ISO 27000 och 62443 kan komplettera varandra.

Standardserier framhålls i sammanhanget som färskvaror i det att de måste reflektera dagens utmaningar. Aktörer väljer med andra ord den som är mest aktuell. En av respondenterna lyfte till exempel att NIST-ramverket för några år sedan det mest uppdaterade och det man istället använde sig av.

Att standarder är färskvaror framhåller de norska respondenterna som problematiskt även när det gäller certifiering. En av dem påpekade att en gammal certifiering inte är värd någonting. Det faktum att det dessutom finns flera olika initiativ till certifieringsprocesser i USA och Europa uppges kunna bli ett framtida problem när det finns flera standarder att förhålla sig till. En svensk studiedeltagare uttrycker samma farhåga. Certifieringar betraktas av respondenterna dessutom inte som odelat positivt då det både är kostsamt att certifiera sig och det beskrivs som osäkert vilken egentlig nytta man får av att kräva certifieringar. En certifiering gällande tekniska krav kan till exempel visa sig vara otillräcklig om man inte också beaktar de processer som omger tekniken.

Studiedeltagarnas uppfattning om styrkorna och svagheterna med 62443 delas av flera svenska studiedeltagare och kan sammanfattas enligt följande:

- Styrkor är att serien är komplett över hela livscykeln, att den är skräddarsydd för ICS, att det finns en beskrivning utifrån säkerhetsnivåer och att viktiga leverantörer är med i de kommittéer som tar fram standardserien.
- Svagheter är att serien fortfarande har många delar under utveckling som dessutom snabbt kommer att bli föråldrade, att roll- och ansvarsaspekter saknas och att serien är väldigt omfattande och tekniskt orienterad. Det uppges dock finnas uppgifter om att ett nytt avsnitt om skyddsnivåer, som i sin tur är summan av säkerhetsnivåer och mognadsnivåer, är under utveckling. I detta skulle enligt uppgift även MTO-perspektivet tas omhand.[49]

[49] MTO: Människa, teknik, organisation.

6 Avslutande sammanställning

Denna rapport har dels beskrivit strukturen i standardserie 62443, dels dess förhållande till andra standarder. Fokus har emellertid varit på hur standarden används av ett urval aktörer i Sverige och Norge.

ISA/IEC 62443 riktar sig till både operatörer och leverantörer inom ICS-området och består av fyra övergripande delar: En generell del med bland annat begreppsförklaringar, en med policyer och tekniker (bland annat rörande patch management), en som behandlar design och säkerhet på systemnivå och slutligen en som behandlar krav för produktutveckling och komponenter.

Samtliga delar är strukturerade enligt ett antal grundläggande säkerhetskrav samt en segmenteringsprincip som innebär att olika delar av ett och samma system kan tilldelas olika säkerhetsnivåer och därmed olika strikta krav. De grundläggande kraven avser identifiering och autentisering, användningskontroll, systemintegritet, konfidentialitet, begränsat dataflöde, incidenthantering och säkerställande av tillgänglighet.

6.1 Jämförelse med andra standarder

Följande sammanställning visar vilka standarder som har omnämnts som närliggande samt i korthet vad de behandlar:

- *ISO 27000*: Ledningssystem för informationssäkerhet.
- *IEC 62351*: Informationssäkerhet för styrsystem inom kraftområdet.
- *NIST CFS*: Cybersäkerhet hos kritisk infrastruktur.
- *NERC CIP*: Cybersäkerhet hos stamnät och produktionsanläggningar på nationell nivå.

Tabell 1 sammanställer dessa standarders tillämpningsområde, deras täckningsgrad vad gäller processer samt teknisk detaljeringsgrad.

Tabell 1: En sammanställning av olika standarders tillämpningsområde, deras täckningsgrad vad gäller processer samt teknisk detaljeringsgrad.

Standard	ICS	IT	Heltäckande	Detaljerad
ISO 27000		*x*	*x*	
IEC 62351	*x (energi)*			*x*
NIST CSF	*x*		*x*	
NERC CIP	*x (energi)*		*x*	
ISA/IEC 62443	*x*		*x*	*x*

En majoritet av studiedeltagarna uppger att 62443 brukar kompletteras, eller kan och bör kompletteras, med andra standarder. Exempelvis uppges att 62443 kan användas på den fysiska detaljnivån med fokus på ICS, kompletterat med ISO 27000 för den övergripande projektmetodiken. Ett annat exempel gör gällande att 62443 kan användas för krav på leverantörer jämte ISO 27000 för krav på operatören själv.

6.2 Styrkor och svagheter

Uppfattningar om 62443-seriens styrkor och svagheter delas i stort sett av de svenska och norska studiedeltagarna. De styrkor som framhålls är bland annat att:

- serien är komplett över hela livscykeln
- serien är skräddarsydd för ICS
- det finns en beskrivning utifrån säkerhetsnivåer
- viktiga leverantörer är med och tar fram standardserien
- serien är relevant för flera olika typer av aktörer
- kraven i 62443 är rimliga, när det inom cybersäkerhetsområdet finns en tendens att kräva för mycket
- serien kan medföra en transparens och förutsägbarhet i leverantörsledet.

De svagheter med 62443 som framhålls är bland annat att roll- och ansvarsaspekter saknas samt, enligt några studiedeltagare, att serien är för omfattande och tekniskt komplex. Serien verkar exempelvis inte förutsätta att det redan föreligger något ledningssystem för informationssäkerhet.

6.3 Motiv till användande

Bland de skäl som anges till att 62443 används återfinns följande:

- En förändrad kravbild från kunderna, som är kopplad till industrins ökade utsatthet för cyberincidenter.
- Introduktionen av den amerikanska standarden NERC-CIP 2009.
- Förväntade åtgärder i och med NIS-direktivet. Verksamheterna vill ha en standard att luta sig mot eftersom direktivet kan medföra nya krav än de som råder i dagsläget.
- Seriens övergång till IEC.

De norska studiedeltagarna anger att flera viktiga aktörer inom deras område stödjer och använder 62443 vilket skapar en drivkraft för att själv använda den.

Några av studiedeltagarna nämner att förändrade lagkrav skulle kunna leda till att serien uppmärksammas och används även i framtiden.

Som skäl till att 62443 *inte* används uppger studiedeltagarna att verksamheterna är känsliga för driftavbrott och därför obenägna att implementera nya standarder samt (i ett fall) svårigheterna att certifiera sig.

6.4 Utmaningar

Nedan listas ett antal utmaningar som kan behöva bemötas om standarden ska vara fortsatt framgångsrik.

- Serien är inte ISO-klassad.
- Eftersom 62443 inte bara är en lång lista med krav, utan är uppdelad i kategorier av krav, gör den det möjligt att tala på flera olika nivåer – från detaljnivå upp till en högre abstraktionsnivå. Ibland saknas dock kunskap om att serien är uppdelad på det sättet, varför aktörer ibland begär att 62443 ska uppfyllas i sin helhet. Något sådant går dock inte, eftersom inte alla av seriens delar är relevanta för alla aktörer.
- En utmaning enligt både svenska och norska studiedeltagare är att serien beskriver vad som ska göras, men inte hur det ska göras. Detta är också anledningen att de norska aktörerna har arbetat fram den best practice-guide.
- Serien har fortfarande många delar under utveckling och många av dessa kommer snabbt att bli föråldrade. Att standarder är färskvaror framhåller de norska respondenterna som problematiskt även när det gäller certifiering, det vill säga att en gammal certifiering inte är mycket värd.
- Det faktum att det dessutom finns flera olika initiativ till certifieringsprocesser i USA och Europa uppges kunna bli en framtida utmaning när det finns flera organ att förhålla sig till.

- En generell utmaning som lyfts är att verksamheterna inte alltid ser den ekonomiska nyttan i relation till kostnaderna, och därmed att de är obenägna att implementera standarder inom cybersäkerhet.

Referenser

ISA (2018). *ISA-99*. Tillgänglig på: https://www.isa.org/isa99/. Besökt 2018-06-03.

ISA/IEC 62443-1-1. *Models and concepts*. Draft 6. Edit 4. 2017.

ISA/IEC 62443-1-2. *Master glossary*. Draft 1. Edit 6. 2017.

ISA/IEC 62443-1-3. *Cyber security system conformance metrics*. Draft 1. Edit 19. 2015.

ISA/IEC 62443-2-1. *Establishing an industrial automation and control system security program*. Edition 1.0. 2010.

ISA/IEC 62443-2-3. *Patch management in the IACS environment*. Edition 1.0. 2015.

ISA/IEC 62443-2-4. *Security program requirements for IACS service providers*. Edition 1.0. 2017.

ISA/IEC 62443-3-1. *Security technologies for industrial automation and control systems*. Revision 2. Odaterad.

ISA/IEC 62443-3-2. *Security risk assessment, system partitioning and security levels*. Draft 7. Edit 1. 2017.

ISA/IEC 62443-3-3. *System security requirements and security levels*. Edition 1.0. 2013.

ISA/IEC 62443-4-1. *Secure product development life-cycle requirements*. Draft 3. Edit 11. 2016.

ISA/IEC 62443-4-2. *Technical security requirements for IACS components*. Draft 4. Edit 1. 2017.

Lindström, Tomas. *Cyber Security for Process Control Systems: ABB's view*. 2017. https://ics.kaspersky.com/media/ics-conference-2017/Tomas-Lindstrom-Cyber-Security-for-Process-Control-Systems.pdf, hämtad 180205.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.0. 2014.

Siemens (2018). Tillgänglig på: https://www.siemens.com/press/en/pressrelease/?press=/en/pressrelease/2016/digitalfactory/pr2016110078dfen.htm&content[]=DF. Besökt 2018-06-03.

SS-EN ISO/IEC 27000:2017. *Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Översikt och terminologi*. Utgåva 1. 2017.

TS IEC 62351-1. *Communication network and system security – Introduction to security issues*. First edition. 2007.

Wikipedia (2018). *Cyber security standards*. Tillgänglig på: https://en.wikipedia.org/wiki/Cyber_security_standards. Besökt 2018-06-03.

Bilaga 1: Intervjuguide

1. Vilka arbetsuppgifter har du och hur har du arbetat med standarder närmare bestämt?

2. Varför uppmärksammade eller började man använda standardserie ISA 62443?

3. För publicerade delar av standardserien, använder man alla eller ett urval?

   → Om urval, varför använder man vissa delar men inte andra?

4. För använda delar av standardserien, följer man samtliga av delarnas krav och föreskrifter eller ett urval?

   → Om urval, varför följer man vissa krav och föreskrifter men inte andra?

5. I vilken grad är delarnas krav och föreskrifter tillämpliga sådana de är och i vilken grad behöver de skräddarsys efter verksamheten?

6. Jämfört med närliggande standarder, vad täcker standardserien in respektive vad täcker den inte in?

7. Använder man standardserien ensam eller kompletteras den av andra standarder?

   → Om kompletteras, hur förenar man standarderna sinsemellan?

8. Hur genomförs certifieringsprocessen och vilka aktörer är inblandade?

9. Vilka styrkor och svagheter har standardserien i förhållande till andra standarder?

10. Vilken betydelse har standardserien i förhållande till leverantörer och kunder?

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

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

www.msb.se