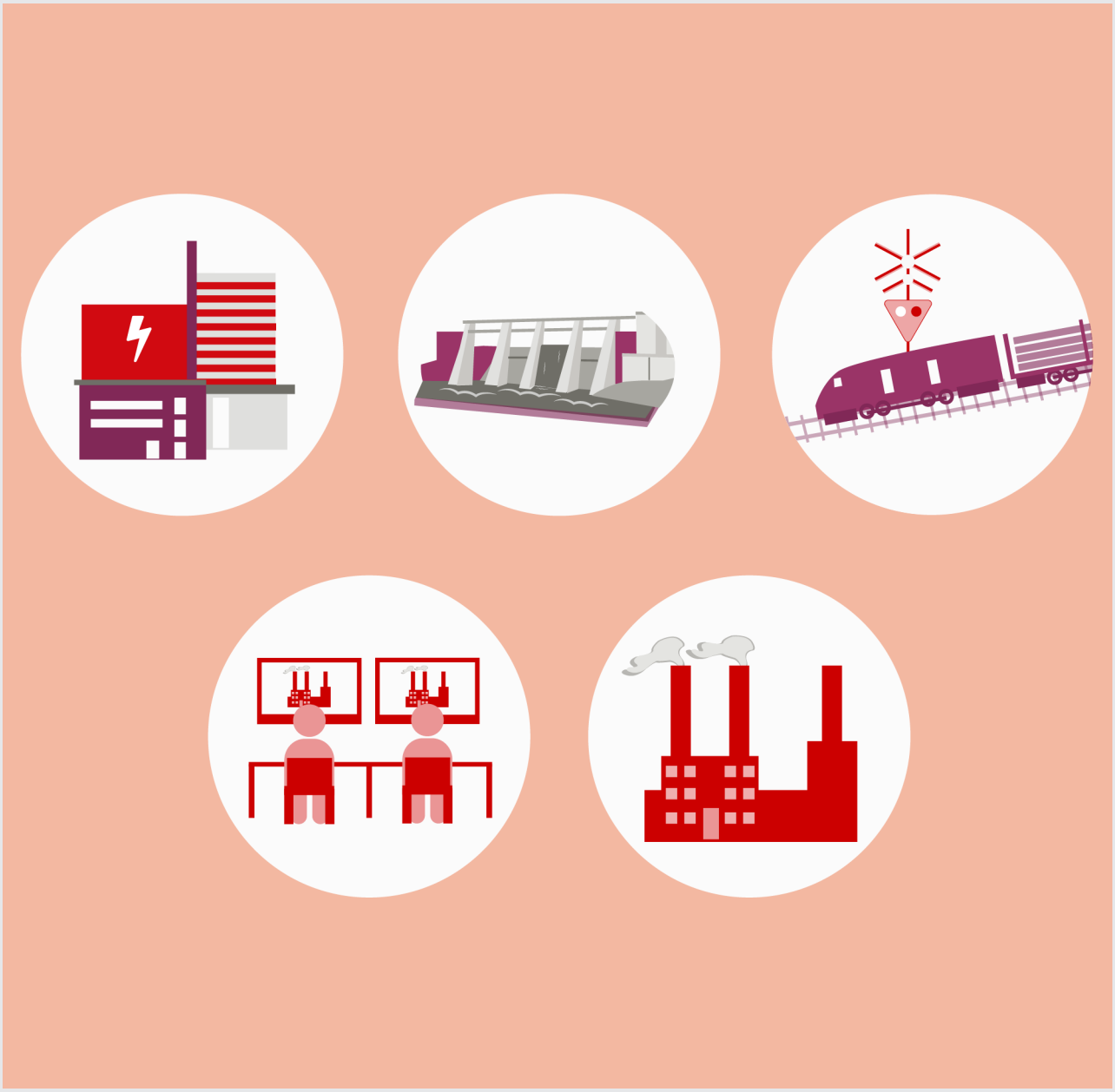
Myndigheten för samhällsskydd och beredskap

VÄGLEDNING

Ökad säkerhet i industriella informations- och styrsystem



Vägledning till ökad säkerhet i industriella informations- och styrsystem

© Myndigheten för samhällsskydd och beredskap (MSB)
Enhet: Enheten för säkerhet i cyberfysiska system/
Avdelningen för cybersäkerhet och säkra kommunikationer

Produktion: Advant

Publikationsnummer: MSB718 - reviderad december 2021
Tidigare utgiven: Juli 2014
ISBN: 978-91-7927-212-8

Förord

Elförsörjning, dricksvattenförsörjning, hälso- och sjukvård och transporter är exempel på samhällsviktiga verksamheter. Ett bortfall eller svår störning i driften av samhällsviktig verksamhet kan leda till att en allvarlig kris inträffar i samhället. Mycket av styrning och övervakning av den infrastruktur och de processer som behövs i samhällsviktiga verksamheter är beroende av industriella informations- och styrsystem.

Syftet med denna vägledning är att bidra med konkreta rekommendationer och stöd till arbetet med att bygga upp samt förbättra säkerheten i industriella informations- och styrsystem.

Denna vägledning är baserad på MSB:s tidigare publicerade vägledning med samma namn[1]. Innehållet syftar till att möta behovet hos aktörer inom industriella informations- och styrsystem och bidra med det stöd som efterfrågas för ökad säkerhet.

Vägledningen innehåller åtta rekommendationer som fokuserar på organisatoriska, tekniska och fysiska säkerhetsåtgärder.

Stockholm i december 2021

Åke Holmgren, avdelningschef

Enheten för säkerhet i cyberfysiska system/
Avdelningen för cybersäkerhet och säkra kommunikationer
Myndigheten för samhällsskydd och beredskap

1. Vägledning till ökad säkerhet i industriella informations- och styrsystem (MSB718 - juli 2014).

Innehåll

Introduktion 7
Bakgrund och läsanvisning 8
Syfte, målgrupp och upplägg 8

Del A
Industriella informations- och styrsystem – en översikt 10

Industriella informations- och styrsystem – vad är det? 11
Huvudmannaskap, driftformer och avreglering 14
Teknik- och tjänsteutveckling 14
Virtualisering 14
Molntjänster 14
Systemberoenden 15
Sensorer och styrenheter 16
Integration mellan drift- och informationsteknik 17
Skillnader mellan informations- och driftteknik 18
Nätverk inom informations- och styrsystem 19
Nätverkssegmentering 19
Filtrera dataflöden 20
Säkerhet på djupet 21
Hot, risker och sårbarheter 21

DEL B
Rekommendationer 24

Bygg upp 1
Implementera en säkerhetsarkitektur i verksamhetens IT- och OT-system 26
1.1. Arbeta med en säkerhetsarkitektur 27
1.2. Övervaka kontinuerligt anslutningar och system för att detektera oönskad trafik 28
1.3. Härda och uppgradera i samverkan med systemleverantörer 29

Bygg upp 2
Genomför regelbundna riskbedömningar och granskningar samt hantera säkerhetsfrågor löpande 30
2.1. Genomför regelbundet, samt vid behov, riskbedömning 31
2.2. Inventera regelbundet inkopplad utrustning och utför teknisk säkerhetsgranskning 32
2.3. Utvärdera regelbundet det fysiska skyddet 33
2.4. Kontrollera regelbundet att endast säkra och relevanta anslutningar existerar 34
2.5. Följ upp incidenter och bevaka händelser i omvärlden 35

Referenser 37

Ordlista 41

Introduktion

Introduktion

Cyberfysiska system kan delas upp i två huvuddelar: industriella informations- och styrsystem (ICS) och sakernas internet (IoT). Denna vägledning hanterar ICS.

ICS används till att samla in data från och om omgivningen, exempelvis varvtal eller flöde, för att exempelvis styra processen som hanterar mängden vätska i en behållare, öka trycket i ett rör eller flytta en hiss till en viss position. I de flesta miljöer där systemen finns är de också övervakade och integrerade med it-system i syfte att effektivisera verksamheten. Därför är ICS allt mer uppkopplade med andra it-system. Integreringen medför exponering mot internet och andra nätverk vilket innebär att ICS i allt större utsträckning ställs inför samma hot och risker som de traditionella it-systemen.

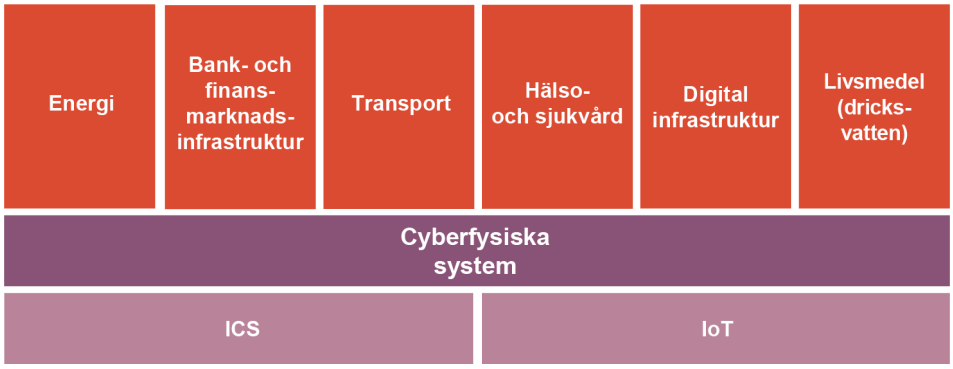
I denna vägledning presenterar vi åtta rekommendationer gällande säkerhetsarbetet i en organisation som nyttjar industriella informations- och styrsystem. De åtta rekommendationerna är uppdelade i två delar:

1. *Arbeta aktivt med en säkerhetsarkitektur (tre rekommendationer)*
   Kartlägg och identifiera de befintliga industriella informations- och styrsystemen. Det är särskilt viktigt att identifiera externa anslutningar. Skapa sedan en zonmodell utifrån principen säkerhet på djupet. Mellan zongränser bör övervakning och detektering av oönskad nätverkstrafik implementeras. De administrativa it-systemen bör endast i undantagsfall integreras med de industriella informations- och styrsystemen och om detta görs ska dessa placeras i en eller flera egna delar av zonmodellen.
2. *Ställ relevanta säkerhetskrav i all upphandling och i serviceavtal (fem rekommendationer)*
   Det finns stora vinster med att hantera säkerhetsfrågor i förväg. Precis som för traditionella it-system är det mycket dyrare att åtgärda säkerhetsproblem i industriella informations- och styrsystem efter att systemen har levererats och implementerats. Genomför en riskbedömning för att kunna ställa relevanta säkerhetskrav baserat på de risker verksamheten identifierat.

Alla rekommendationer och råd som finns i vägledningen bygger på branscherfarenheter, samt praxis och standardiserade arbetssätt.Vägledningen hänvisar till relevanta publikationer och källor inom området.

Bakgrund och läsanvisning

Denna vägledning är den del som i bilden nedan visas med den grå rutan ”ICS”. Innehållet är uppdelat med först en illustrerande beskrivning av ICS och de risker som finns, därefter följer åtta rekommendationer för ökad säkerhet i ICS. Notera att denna vägledningen innehåller rekommendationer specifika för ICS-området. För rekommendationer avseende det grundläggande cybersäkerhetsarbetet, exempelvis ledningens engagemang, hänvisar vi till vägledningen ”Grundläggande säkerhet i cyberfysiska system”.
Vi presenterar även ett urval av referenser och tips om var det går att hitta mer information. Det handlar i första hand om standarder, riktlinjer och rekommendationer som går att tillämpa för att skapa ökad säkerhet i industriella informations- och styrsystem.



Figur 1. Denna vägledning fokuserar på industriella informations- och styrsystem (ICS) inom sektorerna ovan (orangea rutor).

Syfte, målgrupp och upplägg

Syftet med denna vägledning är att ge rekommendationer och tillhörande råd för att höja informations- och cybersäkerhetsnivån i ICS. Målet är att öka samhällets förmåga att förebygga it-relaterade störningar och incidenter, samt medvetandegöra risk och sårbarheter mot ICS.

Vägledningen riktar sig till dig som påverkar utformningen och införandet av säkerhetsåtgärder i ICS. Rekommendationerna är även till nytta för dig som arbetar med design, underhåll eller övervakning av ICS.

Del A
Industriella informations- och styrsystem – en översikt

Industriella informations- och styrsystem – vad är det?

Ett industriella informations- och styrsystem används för att styra, kontrollera eller övervaka processer inom bland annat processindustri, elproduktion, dricksvattenproduktion och transporter. Systemen kan exempelvis slå av och på motorer som öppnar en dammlucka, lägga om växlarna på järnvägsrälsen eller ändra belastningen i en transformatorstation. I figur 2 kan du se ett exempel på en principiell uppbyggnad av ett industriellt informations- och styrsystem.

Idag använder många internet och andra nätverk som bärartjänst för data som skickas inom ICS. Det har lett till minskade kostnader och moderniserad styrning och realtidskontroll av systemen. Det har även blivit effektivare än tidigare att övervaka processerna på distans. Detta innebär att de tidigare isolerade industriella informations- och styrsystemen i allt större utsträckning kopplas ihop med den övriga verksamhetens kommunikationsnätverk och administrativa it-system, vilket har skapat fler risker. De industriella informations- och styrsystemen blir vid en sammankoppling nåbara, om än via omvägar, från internet och de administrativa it-systemen.

Driften av systemen har i samband med sammankopplingen till sakernas internet (IoT) blivit allt mer autonom, men även automatiserats med hjälp av maskininlärning (ML) och/eller artificiell intelligens (AI). Utvecklingen innebär en utmaning för upprätthållandet av systemens säkerhet, det vill säga att bibehålla dess tillgänglighet, riktighet och konfidentialitet[2].

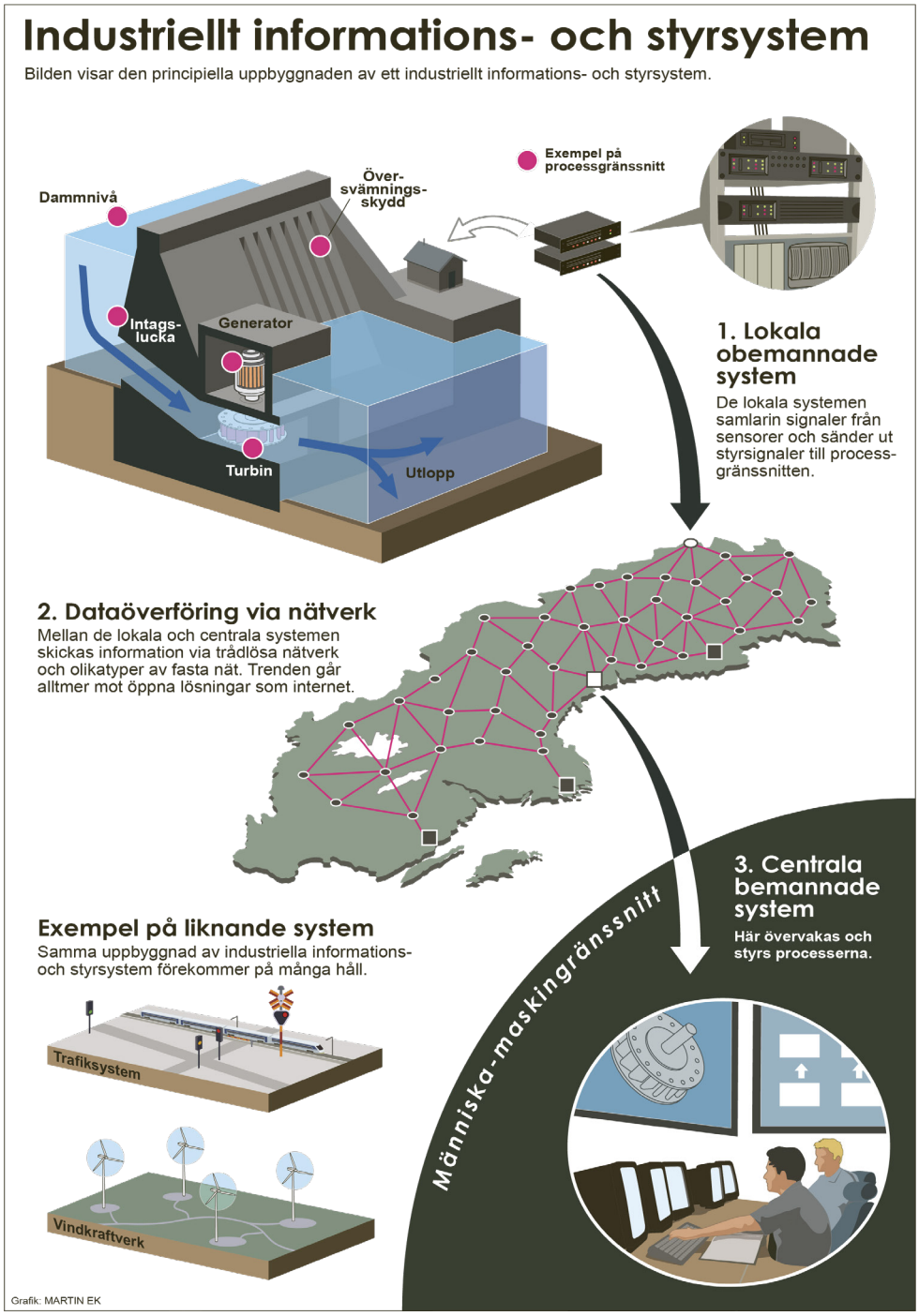
Tabell 1. Exempel på funktioner hos industriella informations- och styrsystem.

Funktion	Beskrivning
Datainsamling	Datalagring, omvandling och skalning, tidsmärkning och rimlighetsbedömning.
Övervakning	Status-, trend-, gränsvärdes-, prestanda- och händelseövervakning samt larmhantering.
Styrning	Direktstyrning, börvärdesstyrning och sekvensstyrning.
Planering och uppföljning	Icke realtidskritisk funktionalitet, planering, loggning och historik, uppföljning och analys.

2. Observera att informationen i cyberfysiska system skyddas utifrån samma säkerhetsprinciper som it-system. Dock är oftast tillgänglighet följt av riktighet viktigast när det gäller cyberfysiska system, till skillnad från it-system där konfidentialitet följt av riktighet ofta är viktigast.

Det är viktigt att de system som styr fysiska processer har definierade säkerhetskrav och lever upp till dessa eftersom konsekvenserna annars kan bli allvarliga. I värsta fall kan de påverka liv och hälsa. Särskilt ICS som används i kritiska samhällsviktiga verksamheter behöver ha en hög driftsäkerhet eftersom avbrott eller störningar kan få stora konsekvenser på samhällsnivå.

Förutsättningarna till ökad säkerhet och minimering av sårbarheter skiljer sig åt mellan it och ICS. Säkerheten är ofta högre i de administrativa it-system än i de industriella informations- och styrsystemen. I en kontorsmiljö är det närmast en självklarhet att uppdatera operativsystemen flera gånger per år för att förbättra säkerheten. I ett driftsatt industriellt informations- och styrsystem kan det dock vara förenat med livsfara att göra förändringar och uppdateringar, särskilt om dessa görs utan att först ha gjort risk- och konsekvensanalys.



Figur 2. Principiell uppbyggnad av ett industriellt informations- och styrsystem.

Huvudmannaskap, driftformer och avreglering

Tidigare ägde staten och kommunerna nästan all samhällsviktig infrastruktur. Idag drivs många samhällsviktiga verksamheter av privata och ibland multinationella bolag. Även inom verksamheter som fortfarande drivs offentligt, till exempel kollektivtrafik och dricksvattenproduktion, läggs delar av driften ut på externa aktörer. Det kan innebära att känslig information om de industriella processerna lagras i ett annat land. I arbetet med att rationalisera verksamheten har säkerhetsfrågorna gällande it-systemen i många fall inte hanterats fullt ut.

Teknik- och tjänsteutveckling

Industriella informations- och styrsystem byggs allt mer av standardkomponenter, så kallade ”Commercial-off-the-shelf”(COTS)-produkter, som är designade utifrån vissa krav. Att komponenter ska ha säker funktionalitet över lång tid är ofta ett krav som saknas eftersom tillgänglighet prioriteras före säkerhet.

Det är allt vanligare med system som bygger på pc-plattformar och kommunikationslösningar byggda på standardprotokoll (TCP/IP). Det innebär att antalet kommunikationsvägar in till de industriella informations- och styrsystemen ökar. Ett exempel är sensorer som automatiskt kontaktar leverantören för underhåll eller i samband med fel i utrustningen.

Före inköp av nya komponenter måste en riskbedömning göras. Annars finns risk att denna typ av komponent med elektroniska kommunikationsmöjligheter har okända ingångar in i infrastrukturen som därmed gör den sårbar för angrepp.

Virtualisering

Virtualisering i it-sammanhang innebär att man skapar en virtuell miljö, en mjukvarusimulering eller emulering av en datorresurs på vilken annan mjukvara kan köras som om simuleringen eller emuleringen vore ett verkligt it-system. Systemvirtualisering innebär att mjukvara för hela servrar körs i en virtualiseringsmiljö. Detta är den typ av virtualisering som oftast avses i kontexten industriella informations- och styrsystem.

Virtualisering har blivit populärt för att användning av tekniken kan sänka kostnader eftersom flera system kan nyttja samma hårdvara. Detta innebär ökad tillgänglighet och mer redundanta system. Virtualisering gör ICS-systemen hårdvaruoberoende, man kan byta fysisk hårdvara flera gånger under gästserverns livslängd. Detta gör det möjligt att underhålla ICS-miljön längre än den ursprungliga hårdvarans livslängd.

Virtualisering innebär att realtidskontrollen försämras och att systemen inte längre är isolerade på samma sätt som tidigare. Virtualisering kan vara en tillgång för de system som till exempel inte har hårda realtidskrav. Innan en virtualiseringslösning införs måste dock noggranna konsekvensanalyser göras.

Molntjänster

De senaste åren har det blivit vanligare att drifta it-miljöer via molntjänster vilket innebär att datorkraften är centraliserad och användaren ofta bara behöver en webbläsare eller en mobilapp för att använda tjänsten.

Typiska egenskaper för molntjänster:

- De kan hanteras dygnet runt via internet från flertalet enheter och utan mänsklig interaktion (självbetjäning).
- De erbjuder ofta flexibla betalningslösningar samtidigt som verksamheten slipper betala för outnyttjade resurser.
- Molntjänstleverantören ansvarar för driften av dataresursen (se avsnitt om ansvarsförhållanden).

Ofta har användaren av molntjänsten enbart kunskap om att tjänsten fungerar, men i allmänhet inte någon kontroll över – eller kunskap om – hur resurserna tillhandahålls eller var resurserna finns. Därför behöver stor vikt läggas på att förstå vilka krav på tillgänglighet, riktighet och konfidentialitet som behöver ställas vid upphandling av molntjänster. Det är också viktigt att kontrollera att molntjänsten inkluderar att data kan skyddas och funktionaliteten övervakas kontinuerligt.

I industriella informations- och styrsystem kan molntjänster ge fördelar genom att öppna upp för fler typer av protokoll, spara konfigurationstid mellan hård- och mjukvara samt vara ekonomiskt fördelaktigt. Molntjänster resulterar dock i fler sammankopplingar och större exponering av system som styr de fysiska processerna. Även om molntjänster kan vara lockande rent affärsmässigt krävs det ofta omfattande specialanpassningar för att de ska fungera säkert för industriella informations- och styrsystem. Innan molntjänster tillämpas och används bör de kontrolleras ur tekniska, säkerhetsmässiga, affärsmässiga och juridiska perspektiv.

Systemberoenden

För att uppnå korrekt informationsutbyte mellan lokala enheter och system, och ibland även mellan system belägna på geografiskt och fysiskt skilda platser, behöver ett industriellt informations- och styrsystem en god kommunikationsstruktur. En liten avvikelse i tidsangivelse eller en kort fördröjning av realtidskommunikationen mellan system eller enheter kan leda till att processer drabbas negativt.

En god kommunikationsinfrastruktur är beroende av stabila geografiska, fysiska och logiska förhållanden så att förändringar i ett system inte påverkar ett annat, oavsett var det befinner sig. Exempelvis kan en geografiskt isolerad händelse som påverkar ett lokalt systems drift medföra att funktionen hos ett system beläget långt bort drabbas av allvarliga störningar. Det blir därför kritiskt att dessa system interagerar och kommunicerar felfritt och att de implementerade organisatoriska, fysiska och tekniska säkerhetsåtgärderna inte orsakar avbrott som kan leda till kaskadeffekter på andra sammankopplade system.

Tabell 2. Systemberoenden.

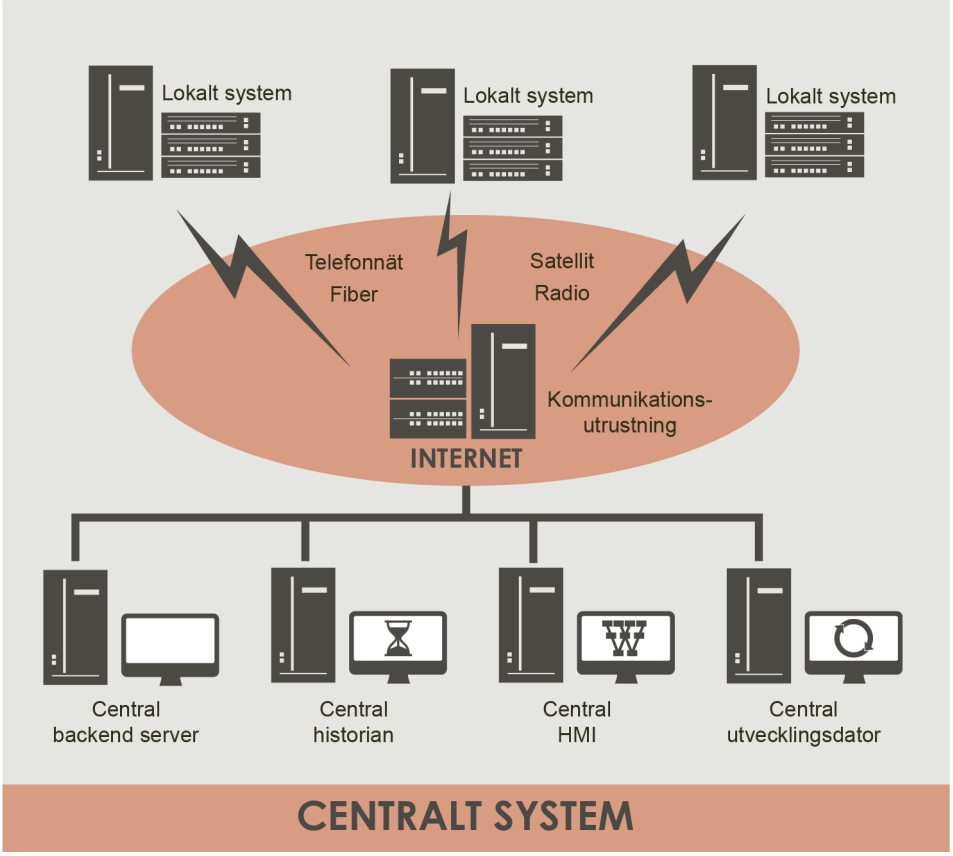
Systemberoenden	Beskrivning
Geografiska	System beroende av att typiska geografiska förhållanden inte avviker.
Fysiska	Flera system som är beroende av varandras processer, exempelvis är slutprodukt från ett system insats till ett annat.
Logiska	Flera system som är beroende av varandras logiska tillstånd, exempelvis avgörande kommandon från HMI (Människa-maskingränssnitt).

Sensorer och styrenheter

Det finns många olika komponenter i ett industriellt informations- och styrsystem, såsom sensorer, styrenheter, kommunikationssystem, säkerhetssystem och gränssnitt mellan systemet och medarbetarna. Gränssnittet där styrsystemet kopplas mot den fysiska processen utgörs av huvudsakligen sensorer för avläsning och av manöverdon för styrning (även kallat ställdon).

De lokala system som samlar in signaler från givare och sänder ut styrsignaler till den fysiska processen innehåller allt fler funktioner och kan ofta även drivas självständigt, exempelvis vid avbrott i kommunikationer med det centrala systemet. De lokala enheterna har ofta både analoga och digitala in- och utgångar och distinktionerna mellan olika typer av enheter – exempelvis IED (Intelligent Electronic Device), PLC (Programmable Logical Controller) och RTU (Remote Terminal Unit) – blir alltmer otydliga.

Från ett eller flera centrala system drivs viktiga funktioner som kräver data från många olika delar av den fysiska processen. I de centrala systemen kan även data lagras och vid hög belastning kan de prioritera vilka systemfunktioner som ska ha företräde.



Figur 3. De centrala systemen tar emot information från de lokala systemen och presenterar processernas tillstånd i grafiska gränssnitt. Via gränssnittet kan operatörerna ändra parametrar och därmed påverka de lokala systemen.

Integration mellan drift- och informationsteknik

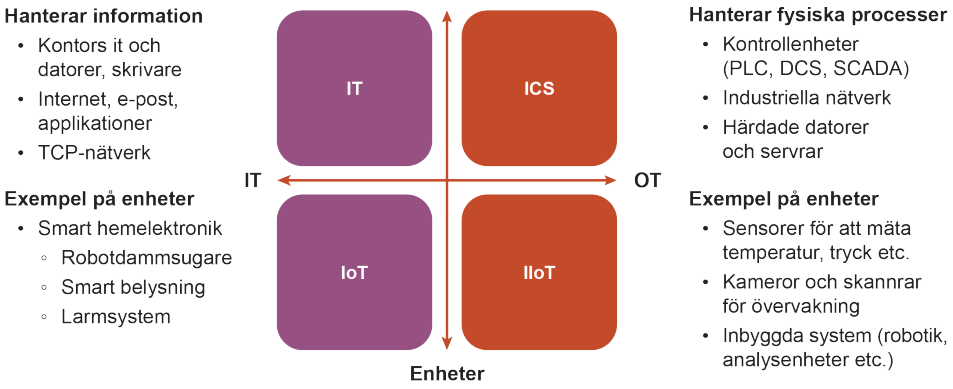
Många industriella processer som tidigare styrts manuellt styrs idag med digitala system. Styrningen kan då också baseras på information som inhämtas från andra system, exempelvis affärssystem, logistiksystem eller från andra driftsystem.

I samband med den ökade digitaliseringen har it- och OT-system under det senaste årtiondet närmat sig varandra och gränserna blivit otydliga. Fler industriella informations- och styrsystem använder exempelvis commercial-of-the-shelf-produkter (s.k. COTS) framtagna främst för it med syfte att minska kostnaderna för utrustning. Det blir även allt vanligare att IoT- och IIoT-enheter (Industriell IoT) integreras med de industriella informations- och styrsystemen för att övervaka och styra driftprocesser via it-systemen. Genom integrering av it- och OT-system möjliggörs snabb – ofta i realtid – inhämtning av underlag till rapporter och möjligheten att omedelbart korrigera och justera driftprocesser samt agera vid signaler om problem. Figur 4 visar systemskillnader mellan it och OT, samt IoT och IIoT.

Driftteknik (eng. Operational Technology, OT) beskrivs ofta som hård- och mjukvara som används för att övervaka eller styra fysiska processer. OT är vanligt förekommande inom industriella informations- och styrsystem, där SCADA-system är vanligt förekommande. Inom samhällsviktig verksamhet används OT för att styra bl.a. kraftverk och transportsystem. I samband med den pågående digitaliseringen närmar sig OT de tidigare avskilda administrativa it-systemen.

Informationsteknik (it) används för att beskriva datateknik, både hård- och mjukvara. Exempelvis är e-post en informationstyp som faller inom ramarna för begreppet it. Denna typ av teknik är inte lika vanligt förekommande i industriella processer, men utgör likväl ofta den tekniska ryggraden i ett företag eller organisation. Denna typ av enheter och information har låg grad av autonomitet och dess programvara uppdateras kontinuerligt.

Integration av it- och OT-systemen ger upphov till nya risker. Ett exempel på det är att industriella informations- och styrsystem görs tillgängliga för attacker via it-system. Det gör det viktigt att verksamheten är medveten om att varje enskild enhet som kopplas upp mot internet, eller ett nätverk med tillgång till internet, utgör en risk. En cyberattack mot en OT-enhet kan ha katastrofala konsekvenser – både ur ett för verksamheten ekonomiskt perspektiv och ett personskade-perspektiv eftersom det även kan orsaka fysiska skador på människor.



Figur 4. Skillnader på system och enhetsnivå mellan it och OT, samt IoT och IIoT.

Skillnader mellan informations- och driftteknik

Både it- och OT-systemen hanterar idag information i digital form. Skillnaden ligger i syftet med informationsbearbetningen. I en traditionell it-miljö ligger fokus på att informationen behandlas för att förädlas, medan informationen i en OT-miljö används för styrning av fysiska processer. Nedan följer en tabell som belyser några av de huvudsakliga skillnaderna mellan informations- och driftteknik:

Tabell 3. Skillnader i funktion mellan it- och OT-system.

Variabel	Informationsteknik	Driftteknik
Funktion	Dynamisk	Deterministisk
Område	Affärsfokus	Industrifokus
Primära användare	Folk i allmänhet.	Ingenjörer, tekniker och produktionsledare.
Processkrav (svarstid)	Minuter till dagar.	Millisekunder till sekunder.
Gränssnitt	Webbläsare, tangentbord och enheter.	Sensorer, kodad data, skärmar eller tillgång via pekskärm.
Uppdateringsfrekvens	Konstant, i samband med mjukvaruuppdatering. Avbrott för underhåll är acceptabelt och kan utföras utanför normal kontorstid.	Uppdatering måste testas i förväg och noggrant granskas. Det leder oftast till avbrott eller omstart av system vilket påverkar tillgängligheten negativt.
Livscykel	Kort, 3–5 år.	Lång, 15–30 år
Attackyta	Flera nätslussar.	Få nätslussar.
Huvudfokus	Konfidentialitet (C-I-A)	Tillgänglighet (A-I-C)
Fokus	Informationslagring och överföring.	Processkontroll
Dataflöde (mängd)	Hög	Låg
Antivirus	Vanligt och enkelt att implementera.	Komplicerat att implementera.
Protokoll	Standard TCP-/IP-protokoll där autentisering och kryptering kan appliceras.	Nätverksprotokoll, ofta utan säkerhet på grund av funktionella krav och begränsningar som finns inom OT.
Påverkan	Vanligtvis ingen risk för miljöpåverkan eller risk för mänskligt liv.	Risk för skada på natur och människa samt risk för mänskligt liv.
IT-säkerhetsmedvetenhet (generellt)	Hög	Låg
Komponenter	Vanligtvis lokalt placerade, med kontrollerad miljö (temperatur).	Lokalt eller isolerat, samt avskilt. Placerade i dynamisk miljö med hög/låg temperatur och hög/låg lufttryck/luftfuktighet.

Nätverk inom informations- och styrsystem

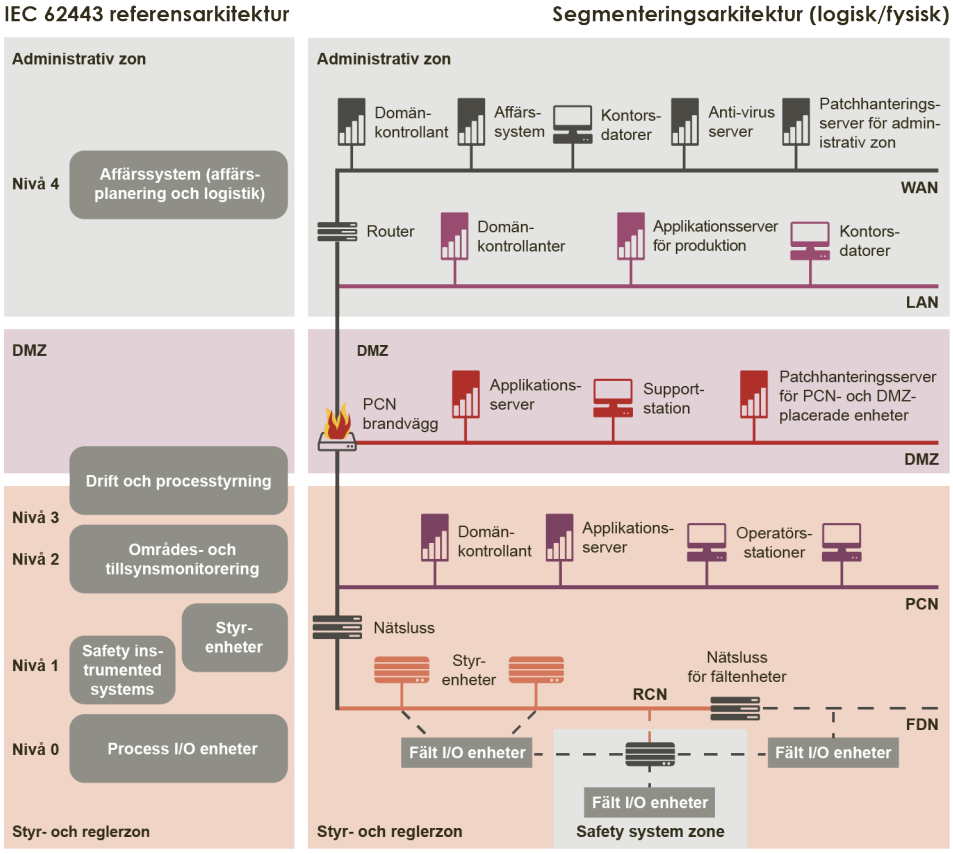
Till skillnad från traditionell it utnyttjar industriella informations- och styrsystem vanligtvis flera olika protokoll för realtidskommunikation och dataöverföring mellan olika komponenter.

Funktion och typ av nätverkstrafik skiljer mellan industriella informations- och styrsystem och traditionella kontorsnätverk. Internetåtkomst, FTP, e-post och fjärråtkomst tillåts vanligtvis inom kontorsnätverk men bör undvikas inom industriella informations- och styrsystem. Följaktligen krävs annorlunda säkerhetskrav för informations- och styrsystem samt noggrann reglering av ändringskontroll, konfiguration och programvaruändringar i dess nätverk och system.

Nätverkssegmentering

Nätverkssegmentering innebär att nätverk delas upp i flera mindre zoner för att begränsa och filtrera nätverkstrafiken mellan segmenten. Exempelvis är det olämpligt att informations- och styrsystem finns i samma segment som kontorsystem. Genom nätverkssegmentering minskar risken för att skadlig kod eller felaktigheter sprids till samtliga enheter som är uppkopplade på nätverket. Skadan kan begränsas till en zon eller ett segment. Likaså ökar svårigheten för en angripare att få åtkomst till OT-miljön även om denne fått åtkomst till den traditionella it-miljön.

En riskbedömning ska ligga till grund för val av lämplig zon- och nätverkssegmentering, men traditionellt sett tillämpas segmentering vid nätslussar mellan nätverksdomäner där nätverkstrafiken begränsas av logisk- eller fysisk segmentering. Av säkerhetsskäl finns vanligtvis flera nätverksdomäner inom industriella informations- och styrsystemsnätverk, exempelvis flera lokala och operativa nätverk, samt kontorsnätverk.



Figur 5. Referensmodell för nätverkssegmentering enligt 62443-2-1. Förklaringar av förkortningar går att finna i ordlistan.

Filtrera dataflöden

Att filtrera dataflöden mellan nätverkssegment, och i vissa fall mellan enskilda enheter, är en grundläggande säkerhetsåtgärd. Ofta görs detta med hjälp av brandväggar, men det finns även andra sätt.

Att konfigurera brandväggar med rätt filtreringsregler i industriella informations- och styrsystem kan vara komplext på grund av mängden protokoll och dess olika sårbarheter. Många filtrerande nätverksprodukter är också främst avsedda för en traditionell it-miljö vilket gör att stöd för att sätta brandväggsregler med protokoll som används i OT-miljön inte finns, eller är begränsat. Exempel på filtreringsregler:

- Obehörig trafik (dvs. trafik från exempelvis internet) ska inte ges tillgång till nätverket.
- Trafik ska enbart kunna flöda från OT-miljön till it-miljön, inte omvänt.

Bortsett från uppenbara regler som att utomstående inte ska få tillgång till nätverket, bör man generellt sträva efter att både portspecifika och adresspecifika regler implementeras, samt att ett fåtal enheter, adresser, tillåts. Exempelvis bör inte slutanvändare, en tredjepartsenhet eller en IoT-enhet som inte krävs för ICS-systemets funktion kunna kopplas till nätverket. Att använda kommersiella COTS-enheter bör beaktas med försiktighet då de ofta är konfigurerade att underlätta användning och inte för att uppnå säkerhet och därför inte är lämpliga för ICS-nätverket. Det finns även risker med avsaknade av insyn i leveranskedjan för COTS där produkterna kan ha utsatts för exempelvis skadlig kod.

Säkerhet på djupet

För ökad säkerhet i industriella informations- och styrsystem behöver säkerhetsmekanismer implementeras enligt principen säkerhet på djupet (eng. defence-in-depth). I korthet innebär principen att säkerhetsåtgärder fungerar överlappande och skyddet byggs i flera lager. Om en säkerhetsfunktion visar sig vara otillräcklig, ska andra säkerhetsfunktioner finnas som upprätthåller ett skydd, om än inte fullt ut, tills den fallerande säkerhetsfunktionen är åtgärdad.

Data, hårdvara, källkod och nätverkstrafik är exempel på information och utrustning som kan vara skyddsvärd och kräva säkerhetsåtgärder samt säker hantering. Vilka säkeråtgärder och vilken grad av skydd i förhållande till behov och kostnad som är lämpligt varierar. Detta bör verksamheten utvärdera genom att genomföra riskbedömning av verksamhetens kartlagda informationstillgångar i relation till en omvärlds- och verksamhetsanalys.

I vägledningen *"Grundläggande säkerhet i cyberfysiska system"* hittar du mer information och exempel på områden som omfattas av säkerhetsarbete enligt principen säkerhet på djupet.

Hot, risker och sårbarheter

En incident, oavsett om den är orsakad av en attack, ett misstag eller ett handhavandefel, kan få svåra konsekvenser. En incident kan resultera i manipulation av styrdon och sensorer vilket kan påverka den fysiska miljön eller processen som styrs. Det kan i sin tur leda till svåra konsekvenser i form av utsläpp av farliga ämnen, produktions- och processfel, explosion eller att de industriella informations- och styrsystemen förstörs.

En incident kan även leda till att känslig information sprids till obehöriga, ändras eller förstörs. Detta kan få stora konsekvenser för organisationen eftersom resurser behöver läggas på skademinimering och återskapande av det som ändrats eller förstörts.

Säkerhet ur ett angriparperspektiv har inte varit någon prioriterad fråga vid utvecklingen av industriella informations- och styrsystem. Medvetenheten kring den här typen av säkerhet är därför låg hos såväl utrustnings-, system- och programleverantörer som upphandlare och beställare. Oförståelsen leder till otydlig kravställning och system som inte är utformade för att hantera it-relaterad säkerhet. Problematiken förvärras av att det idag finns möjlighet att beställa angrepp på internet (attack as a service). Det finns också beskrivningar av sårbarheter i industriella informations- och styrsystem samt verktyg och instruktioner för hur skadlig kod kan skapas.

Den 23 december 2015 drabbades ett energibolag i Ukraina av ett driftavbrott efter en cyberattack där BlackEnergy 3 (en form av skadlig kod) användes för att få tillgång till bolagets it- och senare OT-system. Driftavbrottet resulterade i att uppskattningsvis 225 000 abonnenter hade strömavbrott under cirka tre timmar. Denna cyberattack var den första allmänt kända incidenten som resulterade i strömavbrott och attack mot samhällsviktig verksamhet. Analyser av händelsen tyder på att angriparen hade djup kunskap om systemen och koordinerade flera olika mekanismer och verktyg för till slut kunna slå ut driften. Det ukrainska bolaget utsattes för en nätfiskekampanj (eng. *spear phishing*) och den skadliga koden, BlackEnergy, planterades i bolagens datorer redan ett halvår före avbrottet.

Under tiden före avbrottet kunde aktören bakom nätfiskekampanjen samla in information om bolagets systemuppbyggnad och identifiera svagheter.

Vid avbrottet utfördes en koordinerad DoS-attack mot företagets kundtjänst och lyckades stoppa bolagets kommunikation med sina kunder. Väl inne i ICS-systemen startades KillDisk[3] för att radera viktig data, vilket förhindrade personalen att återställa eller styra systemen på distans. Attacken lyckades också inaktivera två av anläggningarnas reservgeneratorer. Strömmen kunde till slut återställas genom att personalen manuellt slog på strömbrytarna på plats på de olika substationerna.

En ytterligare, uppföljande attack, mot det ukrainska energisystemet utfördes ett år senare, 2016. Attackerna mot det ukrainska energisystemet visar tydligt att det är möjligt att skada infrastruktur och stoppa drift av samhällsviktig verksamhet genom cyberattacker. Det är inte osannolikt att vi framöver kommer att få fler liknande attacker. Ett färskt exempel är att coronaviruspandemins många distansarbetare verkar ha lett till att antalet nätfiskekampanjer har ökat signifikant. Sammantaget stärks bilden av att det finns ett stort behov av ökad säkerhet i industriella informations- och styrsystem.

Ett paradigmskifte avseende hoten mot de industriella informations- och styrsystemen

I juli 2010 upptäcktes Stuxnet, vilket var en avancerad form av skadlig kod som angrepp ICS-system. Stuxnet använde flera olika mekanismer för att sprida sig (bland annat via USB-minnen) för att till slut nå fram till de industriella informations- och styrsystemen. Genom att manipulera grundläggande programmeringsblock kunde Stuxnet därmed förändra och skada den fysiska processen utan att processoperatörerna kunde se att något var fel. Enligt de flesta bedömare var Stuxnet skräddarsydd för att angripa och slå ut ett specifikt mål – en urananrikningsanläggning i Iran – utan att förstöra något annat.

3. KillDisk är en programvara för att rensa och radera information på hårddiskar eller annat lagringsmedium.

DEL B
Rekommendationer

Rekommendationer

Rekommendationerna är uppdelade i två delar och innehåller råd på sådant du kan implementera för att öka säkerheten i dina industriella informations- och styrsystem. För att underlätta säkerhetsarbetet är rekommendationerna kategoriserade utifrån tre olika delområden baserat på typ av åtgärd och var inom verksamheten de ska införas. Eftersom det ofta är olika roller som arbetar med olika typer av delområden är avsikten att kategoriseringen ska underlätta den interna dialogen.Vi vill understryka att det inte finns några färdiga recept för hur säkerheten bör eller ska utformas. Det är verksamhetens behov som avgör vad som behövs. Det finns dock ett antal vedertagna arbetsmetoder och rekommendationer som vägledningens rekommendationer utgår ifrån.

Organisatoriska åtgärder
Organisatoriska åtgärder består av en organisations regelverk, policyer, rutiner, bemanning och arbetssätt. Syftet med denna typ av åtgärder är att exempelvis medarbetare ska erbjudas stöd och regler i sitt arbete för att säkerställa att det utförs på ett säkert sätt.

Fysiska åtgärder
Detta är åtgärder som fysiskt begränsar eller förhindrar åtkomst till it-system eller utrymmen där cyberfysiska system är placerade.

Tekniska åtgärder
Tekniska åtgärder består av hård- eller mjukvara samt konfigurationsinställningar vars syfte är att skydda it-system och resurser.

Avsikten med att definiera säkerhetsåtgärder utifrån olika delområden är att underlätta dialogen inom organisationen eftersom det ofta är olika roller som arbetar med de olika delområdena.

Bygg upp 1
Implementera en säkerhets-arkitektur i verksamhetens IT- och OT-system

Bygg upp 1

1.1. Arbeta med en säkerhetsarkitektur

En säkerhetsarkitektur är ett ramverk på strategisk nivå som innehåller koncept, styrande säkerhetsprinciper och en gemensam struktur för var, när och hur säkerhetsåtgärder införs, förvaltas och hanteras. Denna säkerhetsarkitektur är också relaterad och anpassad utifrån it- och OT-arkitekturen för att säkerställa att exempelvis valda säkerhetsåtgärder eller principer placeras på rätt ställe – på ett strukturerat och systematiskt sätt.

En säkerhetsarkitektur ska utgå från ett antal principer, exempelvis djupledsförsvar, vilket kan ställa krav på att säkerhetsåtgärder är redundanta. Åtgärder som till exempel flera brandväggar, eller en kombination av intrångs-detekteringssystem, brandväggar, kryptering av nätverkstrafik och data, samt behörighets- och inloggningsmekanismer.

En del av säkerhetsarkitekturen är segmentering i zoner där skyddsmekanismer fungerar som gräns. De olika zonerna utgör grupperingar av komponenter och system med olika säkerhetsmässiga eller funktionsmässiga kriterier. Dataflöden över zongränser filtreras och begränsas.

Rekommendationer

- Utforma säkerhetsarkitekturer utifrån it- och OT-miljöerna, mönsterkatalogen och katalogen med säkerhetsåtgärder och som omfattar
  - nätverkssäkerhet
  - systemsäkerhet
  - applikationssäkerhet
  - driftoperativa säkerhetsfrågor.
- Dela upp de industriella informations- och styrsystemen i olika zoner (samt ev. subzoner) med skyddsnivåer som anpassats efter hur kritiska de olika systemen är.
- Dela upp nätverket utifrån funktion.
- Nätverksarkitekturen bör vara segmenterad med överlappande säkerhetsmekanismer, enligt principen säkerhet på djupet.
- Dataflöden över zongränser ska begränsas, filtreras, övervakas och loggas. För vissa typer av it-miljöer kan det vara bra att använda datadioder och dataslussar.
- Undvik att ansluta it-system och dess stödfunktioner (t.ex. datalagring) till flera zoner parallellt (så kallad multihoming), eftersom det kortsluter zon-uppdelningen och aktivt motverkar zonmodellen som säkerhetskoncept.
- Placera osäkra tjänster och andra externa anslutningar i demilitariserade zoner (DMZ). Tillåt inga andra direkta anslutningar genom ett DMZ, utan använd proxytjänster, betrodda nätverk eller datorer, exempelvis en hoppserver som genom kontrollerad åtkomst kan hantera data eller värdar mellan zoner.
- Bygg upp ett logiskt skalskydd runt de industriella informations- och styrsystemen. De administrativa it-systemen ska ligga utanför detta skalskydd.
- Använd gärna olika kommunikationsprotokoll mellan olika delar av nätverket. Om ett protokoll används mellan styrsystemet och en DMZ, så bör ett annat protokoll användas för den vidare kommunikationen mellan DMZ:n och organisationens administrativa it-system.
- Säkerställ att tekniska skyddsåtgärder som implementeras i och skyddar zongränser administreras antingen från zonen med det högre skyddsvärdet eller genom ett separat skyddat nätverk.

1.2. Övervaka kontinuerligt anslutningar och system för att detektera oönskad trafik

Verksamheten rekommenderas att kontinuerligt övervaka sina system och anslutningar för att kunna detektera oönskad trafik som kan påverka cybersäkerheten. Att övervaka de egna systemen och dess kommunikationer ger tillsammans med omvärldsbevakningen en bättre förståelse för aktuella hot, förändrade attacktrender och aktuell skadlig kod. Denna övervakning bör ske både internt, inom verksamhetens egna system, och externt för att övervaka attacker mot externa anslutningar.

Det finns i huvudsak två typer av intrångsdetekteringssystem (IDS):

- Nätbaserade intrångsdetekteringssystem (NIDS) – detekterar attackförsök via analys av kommunikationsströmmar.
- Värddatorbaserade intrångsdetekteringssystem (HIDS) – övervakar händelser i ett datorsystem eller analyserar användningsmönster i en applikation.

En utvecklad variant av dessa IDS-system är så kallade intrångsförhindrande system (IPS) som även kan agera för att avstyra angrepp. Observera att IPS i industriella informations- och styrsystem kan leda till att korrekt trafik blockeras vid felaktig angreppsklassificering. Att ett säkerhetssystem oförutsägbart går in och blockerar styrkommandon eller resultatkoder är inte acceptabelt i industriella informations- och styrsystem.

Ett komplement till ovan system är honungsfällor (eng. Honey pots) vilka ofta är inriktade på att även samla in information om en angripare eller inkräktare. En enkel lösning som kan vara lämplig i industriella informations- och styrsystem är att installera en dator som normalt inte tar emot någon trafik i nätverket och som larmar om så sker (en sådan honungsfälla kallas ibland Canary eller försåtsminering). Försök till kommunikation med den här datorn kan vara skäl till att misstänka ett pågående attackförsök eller att en angripare förbereder en attack genom att kartlägga nätverket.

För små och medelstora operatörer erbjuder MSB Skyddspaket ICS/SCADA.[4] Genom skyddspaketet får operatörerna tillgång till ett grundskydd i sina ICS- och SCADA-miljöer och verktyg för att enkelt och snabbt komma igång med säkerhetshöjande åtgärder.

Rekommendationer	
	• Övervaka kontinuerligt externa anslutningar och interna system för att detektera alla former av oönskad trafik. • Analysera kontinuerligt loggar och spårdata från intrångsdetekteringssystem. • Spara loggar och spårdata från intrångsdetekteringssystem långsiktigt. Dessa behövs när en eventuell efterforskning påbörjas, vilket kan dröja lång tid efter att det initiala problemet uppstod. • Det bör finnas en person (roll) med ansvar att hantera och analysera eventuella varningar från de tekniska systemen.

4. Varje enskild verksamhet ansvarar för att välja och implementera skyddsåtgärder utifrån genomförd riskbedömning och verksamhetskrav. För mer information, besök https://www.informationssakerhet.se

1.3. Härda och uppgradera i samverkan med systemleverantörer

Målet är att minska informationssystemens exponering för attacker vilket innebär att ha minsta möjliga mängd aktiva tjänster, protokoll och nätverkskopplingar, samt att konfigurationen för respektive informationssystem är anpassad efter valda och beslutade säkerhetsåtgärder.

Härdning innebär till exempel att komponenter installeras och konfigureras på ett säkert sätt där önskad funktionalitet är aktiverad och oönskad eller osäker funktionalitet är avinstallerad, avstängd eller blockerad. Härdning kan även innebära ändring av standardinställningar- och lösenord, säkerhetsuppgradering (patchning) och begränsning av behörigheter i systemkonton. Det är viktigt att härdningen genomförs enligt den process som etablerats för förändringshantering.

För att genomföra lyckad härdning av systemutrustning, applikationer och operativsystem krävs information från leverantörerna. Utan samverkan med system- och applikationsleverantörer kan förändringar av utrustning eller programvaruinställningar (inkl. uppgraderingar) leda till driftstörningar, orsaka instabilitet i styrsystemen samt ge avtalsmässiga konsekvenser.

Rekommendationer	• Härda och uppgradera industriella informations- och styrsystem. • Underhåll systemens säkerhet fortlöpande. Kända sårbarheter ska hanteras genom att till exempel uppgradera, blockera eller införa särskild övervakning för att upptäcka om sårbarheten utnyttjas. • Dokumentera alla förändringar som genomförs för att säkerställa spårbarhet. Logga gärna detta i en konfigurationsdatabas. Rekommendationerna gäller även alla kringliggande system och hjälpmedel – exempelvis bärbara datorer som används av supporttekniker – för att underhålla och driva funktionen. • Vid byte av utrustning eller delkomponenter bör alla nya komponenter härdas vid installationen. All härdning och uppgradering ska hanteras enligt rutiner för förändringshantering (för råd se rekommendation 2.2 i vägledningen ”Grundläggande säkerhet i cyberfysiska system”). • Säkerställ vid uppdatering av hård- eller mjukvara att kravställd konfigurering inte påverkats (nollställts).

Bygg upp 2
Genomför regelbundna riskbedömningar och granskningar samt hantera säkerhetsfrågor löpande

Bygg upp 2

2.1. Genomför regelbundet, samt vid behov, riskbedömning

För verksamhetens säkerhet är det viktigt att regelbundet, samt vid behov, identifiera, värdera och analysera risker. Riskbedömningen ska ses som ett viktigt underlag vid beslut om vilka åtgärder som behöver genomföras för att undvika driftstörningar, produktionsbortfall eller i värsta fall person- och miljöskador.

En utgångspunkt när det gäller risker baserade på hot från angripare ska vara att dessa har kunskap om verksamhetens system, dvs. utgå inte från att systemens komplexitet gör angrepp omöjliga att genomföra (eng. security by obscurity). En angripare har stora valmöjligheter avseende till exempel angreppssätt och tidpunkt, vilket innebär att leverantörsspecifika kommunikationsprotokoll, krypteringslösningar eller operativsystem utan tillförda säkerhetsåtgärder kan anses vara sårbara. Säkerhetstester (även kallade ”penetrationstester”) och tekniska säkerhetsgranskningar kan genomföras för att få underlag till riskbedömning.

Det är viktigt att riskbedömningar genomförs innan förändringar införs i en verksamhet. Eftersom industriella informations- och styrsystem kan ha inbyggda beroenden som inte alltid är självklara bör du kritiskt analysera tänkbara indirekta effekter av förändringar.

Det behöver finnas processer för att fånga upp risker som uppdagas när en formell riskbedömning inte pågår så att dessa kan hanteras.

Rekommendationer

- Genomför riskbedömningar av industriella informations- och styrsystem. En riskbedömning ska utföras för ett avgränsat delsystem samt för miljön och verksamheten i stort.
- Uppdatera riskbedömningarna i enlighet med de metoder som tidigare har fastställts och dokumenterats.
- Uppdatera systemkartorna (systemdiagram, konfigurationsdatabaser och liknande) så att dessa är aktuella när riskbedömningen genomförs.
- Den verksamhetsanalys som organisationen tidigare genomfört bör ligga till grund för vilka system och vilka informationsresurser som anses verksamhetskritiska och därmed prioriterade i riskbedömningen.
- Dokumentera riskbedömningen. Dokumentationen bör omfatta upptäckta sårbarheter, bedömning av risker samt beskrivning och prioritering av möjliga åtgärder. Informera ledningen om riskerna så att de ska kunna leda, styra och tilldela resurser till verksamheten.
- Använd information från inträffade incidenter och andra störningar som underlag i riskbedömningen, information från omvärldsbevakningen, resultat från genomförda säkerhetsgranskningar samt checklistor. (Se rekommendation 2.5 om incidentuppföljning och omvärldsbevakning.)

2.2. Inventera regelbundet inkopplad utrustning och utför teknisk säkerhetsgranskning

Kartläggningen av it- och OT-miljön måste kontinuerligt vara uppdaterad så att verksamheten är medveten om vilken utrustning som används. Som minimum bör det föras en förteckning över nätverksadresser, maskinnamn, syfte och ansvarig ägare. Varje nätverksansluten enhet som har en ip-adress på nätverket ska vara med i förteckningen.

Var uppmärksam på att när det gäller kartläggning av informations- och styrsystem så kan traditionella metoder som ”pingsweep” störa systemen. När det gäller att inventera tjänster och sårbarheter hos olika tjänster bör aktiva skanningsmetoder (såsom portskanning och sårbarhetsskanning med verktyg som exempelvis Nmap och Nessus) undvikas i ett produktionssystem som är i skarp drift. I stället för att använda automatiska verktyg handlar det ofta om att granska dokumentationen noga och även ge sig ut i processen och studera fysiska kopplingar och datorer på plats.

Fältutrustning som PLC:er och RTU:er har ofta begränsade förmågor att korrekt svara på enklare säkerhetstest. Mjukvaran i utrustningen är ibland utvecklad på ett sätt som leder till att utrustningen kraschar, gör en omstart eller annat felaktigt uppförande. Dessa begränsningar medför att det är svårt att använda sig av automatiska verktyg för penetrationstester som används i miljöer med traditionella it-system. Gör helst dessa tester i separat testsystem eller i styrsystem som inte är i drift.

Få it-konsulter har tillräckliga kunskaper om hur man testar industriella infor-mations- och styrsystem. Av denna anledning kan det även vara en god idé att diskutera med systemleverantörer före ett säkerhetstest. Alternativt utföra testet tillsammans med systemleverantören.

En noggrann planering bör föregå ett praktiskt säkerhetstest av industriella informations- och styrsystem, inklusive en genomgång av hur eventuella störningar till följd av testet ska hanteras. Verksamhetens ledning bör godkänna testplanen.

Rekommendationer

- Genomför regelbunden teknisk säkerhetsgranskning av industriella informations- och styrsystem och anslutna nätverk.
- Praktiska tester kan negativt påverka styrsystem och processer, därför bör dessa enbart utföras efter noggranna förberedelser och efter att man har förstått vilka konsekvenser testerna kan medföra. Använd i stället passiva metoder och undersök manuellt hur till exempel routrar och nätverksansluten utrustning är konfigurerade.
- Om aktiva tester ska genomföras, gör då dessa i separat testsystem eller i styrsystem som inte är i drift.
- Genomför helst en kontinuerlig omvärldsbevakning och omvärldsanalys för att få kunskap om uppdagade sårbarheter som kan påverka era egna informations- och styrsystemen.
- Kontrollera periodiskt att ingen icke-auktoriserad hårdvara, exempelvis USB-enhet eller modem, är ansluten.

2.3. Utvärdera regelbundet det fysiska skyddet

Industriella informations- och styrsystem, speciellt de centrala anläggningarna, har historiskt sett haft ett omfattande fysiskt skydd. I många branscher finns etablerade krav på hur viktiga anläggningar ska klassas och skyddas fysiskt. Det är den egna verksamhetens ansvar att vara medveten om vilka krav som gäller för deras verksamhet.

Industriella informations- och styrsystem är ofta geografiskt utspridda (decentra¬liserade), vilket gör det svårare att upprätthålla ett bra fysiskt skydd i de avlägsna anläggningarna. Angrepp mot industriella informations- och styrsystem kan ske från utrustning i fält, exempelvis genom användning av störsändare.

Idag kan lokala enheter som PLC:er och RTU:er vara mycket sofistikerade. Exempelvis kan en modern RTU innehålla såväl en webbserver som modernare kommunikationsmetoder (Bluetooth, Ethernetport, WLAN) och den behöver därför ha ett tillräckligt fysiskt skydd. Kablar och korskopplingsutrymmen bör förläggas så att obehöriga personer förhindras att fysiskt komma åt dem och koppla in sig på nätverket.

Fysisk tillgång till en systemkomponent gör det mycket enklare att få logisk åtkomst till industriella informations- och styrsystem. Logiska och fysiska säkerhetsperimeter måste därför upprätthållas. Olika branscher omfattas av olika lagar och krav, håll koll på vad gäller för din verksamhet.

Rekommendationer

- Anpassa det fysiska skyddet utifrån gjord riskbedömning i samtliga anläggningar och utrymmen. Balansera de fysiska och logiska skydden så att de är på samma ambitionsnivå. Fysisk säkerhet utan motsvarande insatser på logisk säkerhet, eller det omvända, kan urholka de insatser som gjorts.
- Behörighetskontroll – se till att endast behöriga personer har tillgång till känslig information och viktiga driftlokaler.
- Fysiskt skydd bör inkludera
  - skalskydd och tillträdesbegränsning för verksamhetens lokaler
  - tekniska system för att larma vid obehörigt tillträde till verksamhetens lokaler
  - indelning av verksamhetens lokaler i fysiskt separerade zoner.
- Spårbarhet som gäller personer och tillgångar – se till att både personer och utrustning stannar i behörigt område – exempelvis bör inte bärbar utrustning såsom datorer för programmering av PLC:er lämnas obevakade.
- Kablar för kommunikation – minimera risken för att kablar och korskopplingsutrymmen utsätts för avlyssning eller manipulation.
- Genomför kontroll av miljöfaktorer – exempelvis ventilation och kraftförsörjning.
- Säkerställ att de it-system som hanterar och styr det fysiska skyddet är skyddade på minst samma säkerhetsnivå som de system som de ska skydda.

2.4. Kontrollera regelbundet att endast säkra och relevanta anslutningar existerar

Alla typer av anslutningar och kommunikationskanaler till och från de industriella informations- och styrsystemen ska vara identifierade och försedda med skydds¬mekanismer som är anpassade till organisationens säkerhetskrav och till de verk¬samhetskrav som ställs på de olika styrsystemen.

Anslutningarna till industriella informations- och styrsystem kan bestå av uppringda modem eller ISDN, fasta och trådlösa nätverksförbindelser eller internetbaserade anslutningar. Exempel på nätverksanslutningar:

- serviceingångar för leverantörsrepresentanter
- anslutningsmöjligheter för jourpersonal som behöver snabb tillgång till de industriella informations- och styrsystemen
- anslutningsmöjligheter för fjärrdrift av anläggningar
- anslutningsmöjligheter för fjärravläsning av givare i anläggningar
- anslutningsmöjligheter för åtkomst till tilläggsfunktionalitet eller kringsystem i anläggningen, som exempelvis kameraövervakning, larmanläggningar, kort- och åtkomstskydd, och brandlarm.

Rekommendationer	
	• Säkerställ regelbundet att enbart relevanta anslutningar till de industriella informations- och styrsystemen existerar, samt att dessa är tillräckligt säkra. • Eliminera onödiga anslutningar. Alla anslutningar som finns ska vara formellt sanktionerade av behörig ansvarig roll. • Fjärråtkomst för leverantörer eller åtkomst för personal med jourtjänstgöring kräver särskild tillsyn. För att skapa en godtagbar säkerhet bör kombinationer av olika metoder användas, exempelvis motringning, begränsningar i uppkopplingstiden, förstärkt autentisering samt inskränkningar i vilka kommunikationsmetoder som kan användas till vilka datorer. • Alla användar- och systemkonton ska endast ha nödvändiga behörigheter. Tillgång till filer, applikationer och systemresurser bör nekas om de inte är explicit tillåtna. Alla konton bör vara försedda med stark autentisering.

2.5. Följ upp incidenter och bevaka händelser i omvärlden

Incidenthantering består inte enbart av det arbete som utförs för att hantera en uppkommen situation när en incident redan inträffat. För effektiv incidenthantering behöver minst följande aspekter ingå:

- Utforma ansvar (roller och mandat) och rutiner.
- Skapa förmåga att upptäckta incidenter genom utbildning av användare och tekniska system för övervakning av funktioner.
- Främja kultur och skapa rutiner för intern och extern incidentrapportering.
- Förmåga att ta emot och bedöma anmälningarna utifrån organisationens definierade bedömningskriterier.
- Hantera incidenter så att verksamhetens funktion återställs.
- Rutiner och förmåga att utreda orsakerna till incidenter så att åtgärder kan vidtas så att incidenten inte inträffar igen.
- Arbetssätt för att utvärdera incidenthanteringen och ta tillvara erfarenheter för att förbättra det förebyggande informations- och cybersäkerhetsarbetet samt incidenthanteringen.

Omvärldsbevakning innebär att vara uppdaterad kring vilka incidenter och säkerhetsproblem som rapporteras från den egna, och andra, branscher eller relaterad till den teknik man använder. Det kan vara så enkelt som att prenumerera på nyhetsutskick från leverantörer, säkerhetsföretag och relevanta myndigheter (även utländska sådana). Omvärldsbevakningen ska ge underlag till riskbedömningar, inriktning av säkerhetsarbetet och ge förutsättningar att upprätthålla en god beredskap mot nya hot och sårbarheter i industriella informations- och styrsystem.

Rekommendationer	
	• Sätt ihop en grupp som regelbundet samlas för att diskutera incidenter och riskproblem, och analysera hur dessa kan påverka säkerheten i er organisations informations- och styrsystem. • Gruppen bör bestå av representanter från ledningen samt från både OT- och it-sidan. • Det är viktigt att skapa en kultur där medarbetare vågar berätta om incidenter och säkerhetsbrister utan att hängas ut som ”syndabockar”. • Bevaka även säkerhetsproblem i vanliga it-säkerhetskomponenter eftersom dessa ofta är grunden eller delkomponenter i de it-lösningar som styr de industriella informations- och styrsystemen.

Referenser

Referenser

Nedan följer en lista på rekommendationer för vidare läsning.

Källa	Beskrivning	Kostnadsfri
NERC CIP	North American Electric Reliability Corporation: Critical Infrastructure Protection	X
NIST 800-82	National Institute of Standars and Technology: Guide to Industrial Control Systems (ICS) Security	X
CPNI	Centre for the Protection of National Infrastructure: Good Practice Guide Process Control and SCADA Security	X
DOE 21 Steps	Department of Energy: 21 Steps to Improve Cyber Security of SCADA Networks	X
Norwegian Oil & Gas	Information security baseline requirements for process control, safety and support ICT systems	
PL	Cyber Security Procurement Language for Control Systems	
IAEA	Nuclear security series #17 (Computer Security at Nuclear Facilities)	X
2700[X]	SS-ISO/IEC 27000-serien: Ledningssystem för informations-säkerhet	
ISA95	Manufacturing Enterprise Systems Standards and User Resources	
IEC 62443 [X-X]	IEC 62442-serien: Security Guidelines and User Resources for Industrial Automation and Control Systems	

Rekommendation	Referens- och informationsmaterial
Bygg upp 1	
1.1 Arbeta med en säkerhetsarkitektur	NERC CIP (005-4. 007-4) CAPSS DOE 21 Steps (No.5, 15) Norwegian Oil & Gas (No. 4, 13) PL (alla kapitel) IAEA (Kap. 5.5, 2.3.3) 27002 (Kap. 12, 14) ISA-95 IEC 62443-3 (Kap. 9.4)
1.2 Övervaka kontinuerligt anslutningar och system för att detektera intrångsförsök	NERC CIP (005-4) DOE 21 Steps (No. 8) PL (Kap. 2.2, 3.2, 3.3, 4.4) 27002 (Kap. 12, 14) IEC 62443-3-1 (Kap. 8.4) IEC 62443-3-3 (Kap. 10.4)
1.3 Härda och uppgradera i samverkan med systemleverantörer	CAPSS DOE 21 Steps (No. 4, 6) Norwegian Oil & Gas (No. 6, 10, 12, 13) PL (Kap. 2) 27002 (Kap. 14)

Rekommendation	Referens- och informationsmaterial
Bygg upp 2	
2.1 Genomför regelbundet, samt vid behov, riskbedömning	NERC CIP (002-4) NIST 900-82 (Kap. 3.1–3.3) DOE 21 Steps (No. 14, 18) Norwegian Oil & Gas (No. 2) 27002 (Kap. 14.1.1) 27005 IAEA (Kap. 6) IEC 62443-1-1 (Kap. 5.6) IEC 62443-3-2-1 (Kap. 4.2, 4.3)
2.2 Genomför regelbundet teknisk säkerhetsgranskning	DOE 21 Steps (No. 9, 11) 27002 (Kap. 18) IEC 62443-2-1 (Kap. 3.4.2.5, A.3.4.2.4.2, A.3.4.2.4.3)
2.3 Utvärdera löpande det fysiska skyddet	NERC CIP (006-4) NIST 800-82 (Kap. 6.2.11) DOE 21 Steps (No. 10) PL (Kap. 9, 11) 27002 (Kap. 11) IAEA (Kap. 5.2.1) IEC 62443-1-1 (Kap. 5.9) IEC 62443-2-1 (Kap. A.3.3.3, A.2.3.3.8.9) IEC 62443-3-1 (Kap. 10)
2.4 Kontrollera regelbundet att endast säkra och relevanta anslutningar existerar	CAPSS DOE 21 Steps (No. 1, 2, 3, 7) Norwegian Oil & Gas (No. 4, 10, 12) PL (Kap. 10, 11) 27002 (Kap.9) 27033
2.5 Följ upp incidenter och bevaka säkerhetsproblem i omvärlden	NERC CIP (008-4, 009-4) NIST 800-82 (Kap. 6.2.6) CAPSS DOE 21 Steps (No. 19) Norwegian Oil & Gas (No. 16) 27002 (Kap. 16) IEC 62443-2-1 (Kap. 4.3.4.5)

Ordlista

Ordlista

Administrativa it-system	It-system som används för administrativ databehandling, kontorsautomation eller affärssystem.
Börvärdestyrning	Bör värdet, *referensvärdet*, anges av operatören eller ett överordnat reglersystem. Det jämförs med aktuell utsignal, mätvärdet, och därefter kan systemets utsignal styras mot det önskade värdet.
COTS	*(Eng. Commercial off-the-shelf.)* Färdiga standardkomponenter till skillnad mot skräddarsydda produkter eller leverantörsunika lösningar.
Cyberfysiska system	Med cyberfysiska system menas gränssnittet mellan en digital miljö och en fysisk process. Ett cyberfysiskt system kan antingen vara ett industriellt informations- och styrsystem eller ett IoT-system (eng. Internet of Things).
Cybersäkerhet	Cybersäkerhet är all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot möjliga handlingar, omständigheter, eller händelser som på ett negativt sätt påverkar nätverks- och informationssystemen och människor. Cybersäkerhet handlar främst om att möta antagonistiska hot.
Data	Data kan syfta på information eller rådata (uppgifter som ej bearbetats eller analyserats).
Datadiod	En datadiod är en elektronisk komponent som bara släpper igenom ström i en riktning. Data kan alltså bara överföras i en riktning varav det är ett kraftigt verktyg för säker överföring av data ut ur ett skyddat nätverk.
Datasluss	*(Eng. Gateway.)* En datasluss används för att på ett säkert sätt kunna överföra data mellan två separerade nätverk. Dataslussen filtrerar och kontrollerar data enligt fördefinierade regler för att säkerställa att ingen oönskad data överförs mellan nätverken.
DCS (eng. Distributed Control System)	*(Sv. distribuerat kontrollsystem.)* Ofta ett överordnat styrsystem som autonomt fungerar i loopar med datainsamling och kontroll av processer och operationer. Kan inkluderas övervakning och analysverktyg.
Direktstyrning	Styrning av ett enhet utan mellanhand eller proxy.
Driftteknik	*(Eng. Operationtechnology, OT.)* Datorsystem som styr och övervakar fysiska processer.
DMZ	(Eng. DeMilitarized Zone.) Ett isolerat subnät som placeras utanför det administrativa nätet och endast innehåller system som behöver exponeras mot omvärlden.
FDN	*(Eng. Field Device Network.)* Ett nätverk som kopplar ihop sensorer och aktuatorer med utrustning för kontroll.

Fysisk säkerhet	Informationstillgångar och system skyddas fysiskt från till exempel obehörigt tillträde, brand och vattenskador.
Nätsluss	Nätsluss på svenska. En anordning som kopplar samman nätverk med olika protokoll.
HMI	(Eng. Human Machine Interface.) (Sv. Människa-maskingränssnitt). En komponent som presenterar data för operatörer, ofta med funktion att styra och övervaka processen.
Händelse	Avgränsat, iakttagbart skeende som inte är möjligt att (helt) förutse eller kontrollera och som ofta är anmärkningsvärt på något sätt.
Härdning	(Inom it.) Processer och rutiner som syftar till att minska systemets attackyta och därmed bättre motstå angrepp och angreppsförsök.
ICS	(Eng. Industrial Control Systems.) En vanligt förekommande förkortning som ibland används synonymt med industriella informations- och styrsystem.
IED	(Eng. Intelligent Electronic Device.) Term som förekommer inom elbranschen för att beskriva mikroprocessorbaserade system för styrning av kraftsystemets olika delar, exempelvis frånskiljare.
Inbyggda system	Datorer eller datorliknande system som ingår i enheter som har en eller ett fåtal speciella funktioner, ofta med någon form av realtidskrav. Mjukvaran i ett inbyggt system ligger oftast lagrat i ROM-minne eller flashminne. Inbyggda system är ofta en del av en apparat eller maskin inklusive hårdvara och mekaniska delar. Inbyggda system förekommer ofta i industriella informations- och styrsystem. Kallas även inbäddade system.
Incident	En oönskad händelse som kan leda till negativ påverkan på verksamheten.
Industriella informations- och styrsystem	Industriella informations- och styrsystem är ett begrepp som samlar flera typer av styrsystem, bl.a. SCADA-system (Supervisory Control and Data Acquisition). Andra benämningar kan vara processkontrollsystem, processautomation, process-it, OT-system (operational technology), tekniska it-system, anläggnings-it, distribuerade kontrollsystem och inbyggda realtidssystem (RTE).
IoT	Internet of Things, IoT (sv. sakernas internet) är ett begrepp som används för att beskriva att allt fler föremål, både för privat och industriellt bruk, utrustas med möjligheten att anslutas till internet och andra nätverk.
IIoT	Användning av IoT inom industrin benämns IIoT (Industrial Internet of Things) och är enheter som används för mätning och övervakning, eller system och enheter för styrning som kopplas samman med övriga informationsnätverk.
Information	En mängd data som har betydelse.
Informationssäkerhet	Informationssäkerhet handlar om att skydda information så att den alltid finns när vi behöver den (tillgänglighet), att vi kan lita på att den inte är manipulerad eller förstörd (riktighet), att endast behöriga personer får ta del av den (konfidentialitet). Informationssäkerhet handlar om att skydda informationen i sig, oavsett vilket medium den förmedlas på. Informationssäkerhet uppnås genom att vidta administrativa, organisatoriska, tekniska och fysiska åtgärder.

Konfigurationsdatabas	En databas som innehåller information om hur ett it-system eller cyberfysiskt system är konfigurerat, vilka resurser som finns i systemet och hur de är kopplade till varandra. Databasen är till för att underlätta återställning av system efter en incident. Konfigurationsdatabasen har ett högt skyddsvärde.
Kommunikationssystem	Kommunikationen mellan system och komponenter kan ske med en mängd olika kommunikationsprotokoll och över många olika bärartjänster. Både traditionell och specifik nätverksutrustning används, exempelvis radioteknik, fiber, kopparkabel och telefonnät.
LAN	*(Eng. Local Area Network.)* Ett lokalt nätverk som kopplar ihop och möjliggör kommunikation mellan datorer som befinner sig inom ett avgränsat område.
Lokalt system	System som styr en fysisk process, till exempel en damm-lucka, järnvägsbom eller vattenpump.
Logiskt skydd	Skydd av logisk infrastruktur, till exempel systemfunktioner eller nätverksfunktionalitet. Logiskt skydd existerar parallellt med fysiska skydd.
Maskininlärning	Maskininlärning är en process som använder algoritmer som möjligör lärande från befintlig data i syfte att förutse framtida skeenden/resultat.
Molntjänster	Tjänst som tillhandahålls av leverantör via internet från ett nätverk av servrar, till exempel datalagring på distans via internet.
Organisatorisk säkerhet	Det finns personal som har tid, kompetens och förmåga att arbeta med informations- och cybersäkerhet. Alla medarbetare i organisationen har en grundläggande förståelse för informationssäkerhet och inom organisationen gällande regelverk.
PLC	*(Eng. Programmable Logic Controller.)* Digital dator som används för automation. Ofta avancerad enhet som kan utökas eller programmeras att utföra nya uppgifter och styra fysisk interaktion med systemkomponenter (t.ex. ställdon).
PCN	*(Eng. Process Control Network.)* Ett nätverk som används till att överföra instruktioner och data mellan styr- och mätenheter och SCADA-system.
RCN	*(Eng. Regulatory control network.)* Typ av kontrollnätverk.
Redundans	Dubbel eller flerdubbel uppsättning av viktiga komponenter, information, utrustning eller data för att det ska fungera eller vara korrekt även om något går sönder eller förändras på något sätt.
Riskbedömning	En riskbedömning utgörs av tre olika delar: riskidentifiering, riskanalys och riskvärdering.
RTE	*(Eng. Real Time and Embedded.)* Inbyggda system med stort fokus på realtidsapplikationer (jämför inbyggda system).
RTU	*(Eng. Remote Terminal Unit.)* Digital styrsystemskomponent som interagerar med den fysiska processen genom att avläsa eller styra denna. Den utväxlar telemeletriuppgifter med överliggande kontrollsystem, ofta ett SCADA-system.
Samhällsviktig verksamhet	MSB definierar samhällsviktig verksamhet som verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet.

SCADA	*(Eng. Supervisory, Control and Data Acquisition.)* Ett övergripande, ofta geografiskt distribuerat, industriellt styrsystem för övervakning och styrning av processer för industriellt bruk.
Sekvensstyrning	Styrning genom utförandet av förprogrammerad sekvens.
Säkerhetsfunktioner	*(Eng. Safety Instrumented Systems, SIS.)* Funktioner för nödstopp i händelse av allvarliga fel eller katastrofer. Dessa är kritiska komponenter och måste skyddas därefter. Utveckling går från mekaniska komponenter till digitala och IT-baserade lösningar.
Sårbarhet	Brist i skyddet av en tillgång eller av en säkerhetsåtgärd som kan utnyttjas av ett eller flera hot.
Säkerhetsperimeter	Logiskt eller fysiskt skalskydd. Logiskt skalskydd utgörs av segment eller domän som avgränsar område, exempelvis åtskiljer OT- från it-arkitektur.
Säkerhet på djupet	Ett omfattande försvar som utgörs av flera lager av säkerhetsmekanismer. Detta innebär att flera samverkande eller kompletterande skyddsmekanismer existerar och därmed motverkar att fel i eller manipulation av enstaka skydd får omfattande konsekvenser.
Teknisk säkerhet	Säkerhetsåtgärder som införs i it-miljön och den industriella informations- och styrsystemsmiljön t.ex. autentisering, nätverkssegmentering, kryptering, filtrering av nätverkstrafik osv.
TCP/IP	*(Eng. Transmission Control Protocol/Internet Protocol.)* Standardiserat datakommunikationsprotokoll som används som bärartjänster såväl på internet som inom industriella lösningar.
Virtualisering	Virtualisering i it-sammanhang innebär att man skapar en virtuell miljö, en mjukvarusimulering eller emulering av en datorresurs på vilken annan mjukvara kan köras som om simuleringen eller emuleringen vore ett verkligt it-system. Systemvirtualisering innebär att mjukvara för hela servrar körs i en virtualiseringsmiljö (Eidenskog & Karresand, 2017). Detta är den typ av virtualisering som oftast avses i kontexten industriella informations- och styrsystem.
WAN	*(Eng. Wide Area Network.)* Ett nätverk som täcker ett större geografisk område genom att ansluta flera lokala nätverk.

Myndigheten för
samhällsskydd
och beredskap

© Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB718 - reviderad december 2021 ISBN 978-91-7927-212-8