Vägledning till ökad säkerhet i digitala kontrollsystem i samhällsviktiga verksamheter

Forum för informationsdelning avseende informationssäkerhet – SCADA och processkontrollsystem (FIDI-SC)

KRISBEREDSKAPS MYNDIGHETEN

Vägledning till ökad säkerhet i digitala kontrollsystem i samhällsviktiga verksamheter

Titel: Vägledning i ökad säkerhet i digitala kontrollsystem i samhällsviktiga verksamheter
Utgiven av Krisberedskapsmyndigheten (KBM)
Omslagsfoto: Ablestock, Mikael Bertmar/Nordic Photos, Ablestock
Foto, inlaga: s. 7 och 39 Ablestock, s. 19 Mikael Bertmar/Nordic Photos, s. 13 Alessandro Della Bella/Keystone/Scanpix, Thomas Hernikssson/Scanpix, Kaspel Dudzik/Scanpis, Malin Hoelstad/SvD/Scanpix, Thomas Henriksson/Scanpix samt Cornelius Poppe/Scanpix
Upplaga: 1 000 ex

ISBN: 978-91-85797-21-9
KBM:s dnr: 0451/2008
Grafisk form: AB Typoform

Skriften kan erhållas kostnadsfritt från
Krisberedskapsmyndigheten, materielförvaltning
E-post: bestallning@kbm-sema.se

Skriften kan laddas ner från Krisberedskapsmyndighetens webbplats
www.krisberedskapsmyndigheten.se

Innehåll

Förord

Digitala kontrollsystem utgör en kritisk del av de system som försörjer samhället med elektricitet, värme, dricksvatten, bränslen samt transporter av personer och varor. Till skillnad från administrativa IT-system, där informationsbehandlingen i sig ofta är slutmålet, kan störningar i digitala kontrollsystem innebära direkta störningar i den underliggande fysiska processen. Det kan i slutändan leda till leveransavbrott av samhällsviktiga nyttigheter.

Dagens kontrollsystem görs i allt högre utsträckning tillgängliga via publika nätverk som Internet. De bygger allt mer på samma teknik som vanliga IT-system och integreras med administrativa IT-system. Sammanfattningsvis medför den här utvecklingen en radikalt förändrad riskbild.

Krisberedskapsmyndigheten (KBM) driver sedan 2005 forumet FIDI-SC för att öka säkerheten i digitala kontrollsystem. Gruppens arbete bygger på en modell för förtroendebaserad informationsdelning som den brittiska säkerhetsmyndigheten CPNI (Centre for the Protection of National Infrastructure) har utvecklat.

Representanter för flera branscher som använder digitala kontrollsystem träffas regelbundet för att dela information och utbyta erfarenheter. I dag deltar följande organisationer i FIDI-SC: Banverket, E.ON AB, Fortum AB, KBM, Norrvatten, Preem Petroleum AB, AB Storstockholms Lokaltrafik (SL), Stockholm Vatten AB, Affärsverket Svenska Kraftnät (SvK), Säkerhetspolisen och Vattenfall AB.

Syftet med det här dokumentet är att öka medvetandet kring behovet av ökad säkerhet i digitala kontrollsystem. De rekommendationer som ges här stöds av medlemmarna i FIDI-SC och arbetet med dokumentet har underlättats väsentligt av den generösa hjälp som erhållits från forumets representanter.

Vägledningen till ökad säkerhet i digitala kontrollsystem är framtagen av Åke J. Holmgren (Informationssäkerhetsenheten, KBM), Erik Johansson (Industriella informations- och styrsystem, KTH) och Robert Malmgren (Robert Malmgren AB). Författarna ansvarar själva för den slutliga texten.

STOCKHOLM 2008-10-01

Arvid Kjell

ENHETSCHEF, INFORMATIONSSÄKERHETSENHETEN, KBM

Syfte

Syftet med det här dokumentet är att ge stöd i arbetet med att öka säkerheten i digitala kontrollsystem. Kontrollsystem förekommer vanligtvis inom exempelvis el- och dricksvattenförsörjningen, petrokemisk industri och spårtrafik.

Säkerhet i digitala kontrollsystem har fått stor uppmärksamhet under de senaste åren och i dag finns många internationella rekommendationer och praxis.

Det här dokumentet ger grundläggande rekommendationer kring säkerhet i digitala kontrollsystem. Dokumentet tipsar också om var det går att finna ytterligare information. De rekommendationer som vi ger ansluter väl till internationellt erkända rekommendationer, praxis och standardiserade arbetssätt.

Den inledande delen av dokumentet vänder sig till dig som arbetar med säkerhetsfrågor på ledningsnivå. Sedan följer något mer detaljerade avsnitt som huvudsakligen riktar sig till dig som arbetar praktiskt med säkerhet i digitala kontrollsystem.

Omfattning och urval av referenser

Det här dokumentet behandlar säkerhet i digitala kontrollsystem och ger inte specifika råd kring IT-säkerhetsfrågor.

Vi refererar främst standarder, riktlinjer och rekommendationer som går att tillämpa generellt för att skapa ökad säkerhet i digitala kontrollsystem. Vi har gett företräde till referenser som enligt vår bedömning inte är branschspecifika. Urvalet av refererade dokument är även begränsat till svenska och engelska dokument, som i möjligaste mån är fritt tillgängliga via Internet.

Dokumentet består av tre delar:

Del A

Förutsättningar och sammanfattande rekommendationer

Del B

Detaljerad vägledning till rekommendationer och etablerade riktlinjer

Del C

Referenslista med kommentarer

Ytterligare information

Dokumentet kommer att revideras regelbundet och synpunkter på innehållet tas gärna emot.

Kontakta FIDI-SC och Krisberedskapsmyndigheten på följande e-postadress: `scada@kbm-sema.se`

Del A

Förutsättningar och sammanfattande rekommendationer

Digitala kontrollsystem

I dag är samhällsviktiga verksamheter, såsom distribution av elektricitet och dricksvatten, fjärrvärme och spårbunden trafik, beroende av datorbaserade system för styrning, reglering och övervakning av de centrala fysiska processerna.

Sammanfattningsvis finns ett antal mer eller mindre överlappande benämningar på de här datorbaserade styr- och kontrollsystemen. Här använder vi benämningen *digitala kontrollsystem*, men systemen kallas även SCADA-system (Supervisory, control, and data acquisition), processkontrollsystem, industriella informations- och styrsystem, process-IT, tekniska IT-system, distribuerade kontrollsystem, inbyggda realtidssystem (RTE) och så vidare. I vissa avseenden finns tekniska skillnader, men de betonar vi inte alltid.

Figur 1 visar den principiella uppbyggnaden av ett kontrollsystem. Den bakomliggande *fysiska processen* kan innehålla ett mycket stort antal mätpunkter som kan vara spridda över stora geografiska områden. *Processgränssnittet*, det vill säga sättet att kommunicera verkligheten, utgörs huvudsakligen av sensorer för avläsning och manöverdon för styrning (styrutrustning).

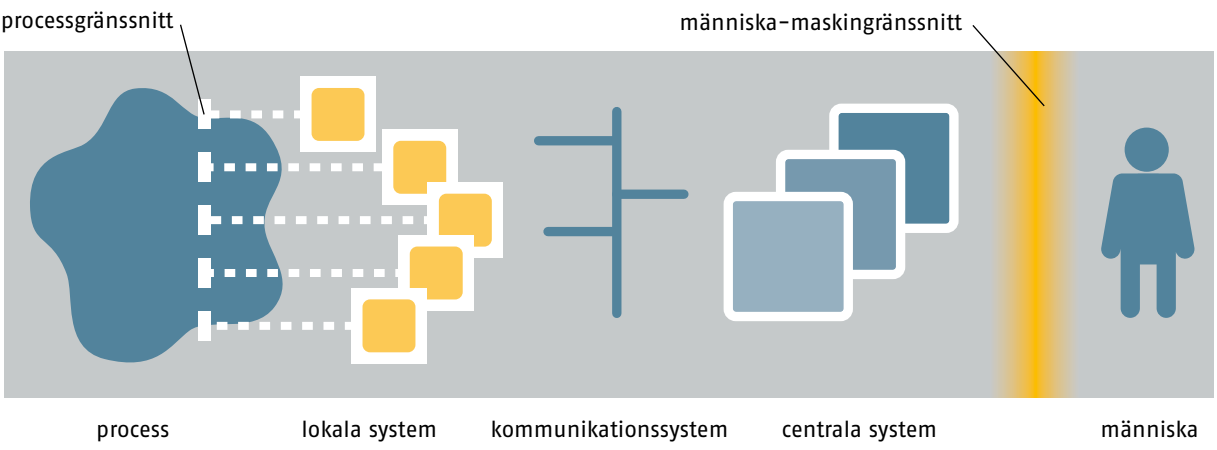
De *lokala system* som samlar in signaler från givare och sänder ut styrsignaler till styrutrustningen innehåller allt fler funktioner och kan ofta även verka självständigt vid exempelvis avbrott i kommunikationer med det centrala systemet. De lokala enheterna har ofta både analoga och digitala in- och utgångar och distinktionerna mellan olika typer av enheter – exempelvis IED (Intelligent electronic device), PLC (Programmable logic controller) och RTU (Remote terminal unit) – blir alltmer otydliga.

Viktiga funktioner, till exempel sådana som kräver stor beräkningskapacitet och data från många olika delar av processen, kan realiseras i en eller flera *centrala system*. Här kan även data lagras och vid hög belastning kan centrala enheter prioritera vilka systemfunktioner som ska ha företräde.

Kommunikationerna mellan de olika delarna av kontrollsystemet kan ske på en mängd olika sätt, både via obundna media (till exempel trådlösa nätverk) och bundna media (till exempel optisk fiber och telefonnät).

För att presentera data och interagera med systemet behövs *människa-maskingränssnitt*. Några av de viktigaste användningsområdena för dessa systemdelar är driftagning av systemet (att definiera processdata och funktioner), drift av processen (att styra och övervaka) samt underhåll av kontrollsystemet (att förändra och uppdatera systemet).

Figur 1: Schematisk uppbyggnad av ett digitalt kontrollsystem [figuren modifierad från Cegrell och Sandberg (1994)]



Vi kan sammanfatta de viktigaste funktionerna hos digitala kontrollsystem i nedanstående punkter:

- **Datainsamling** (datalagring, omvandling och skalning, tidsmärkning, rimlighetsbedömning och så vidare)
- **Övervakning** (statusövervakning, trendövervakning, gränsvärdesövervakning, prestandaövervakning, händelse- och larmhantering och så vidare)
- **Styrning** (direkt styrning, börvärdesstyrning, sekvensstyrning och så vidare)
- **Planering och uppföljning** (icke-realtidskritisk funktionalitet; planering, loggning och historik, uppföljning och analys och så vidare)
- **Underhåll och förändring** (i och urtagning av drift, uppgradering, hantering av utvecklingsmiljöer och så vidare).

MER INFORMATION

Boyer, S. A. (2004) *SCADA: Supervisory control and data acquisition.* The Instrumentation, systems, and automation society (ISA), Research Triangle Park, N.C.

Cegrell, T. & Sandberg, U. (1994) *Industriella styrsystem.* SIFU förlag, Borås.

Varför är säkerhet i digitala kontrollsystem viktigt?

Nedan följer ett antal observationer som alla pekar på behovet av en ökad uppmärksamhet på säkerhet i digitala kontrollsystem. Observationerna är inte givna i prioritetsordning och de överlappar varandra till viss del.

Samhällsviktiga verksamheter är beroende av digitala kontrollsystem

Digitala kontrollsystem utgör en kritisk del av de system som försörjer samhället med elektricitet, värme, dricksvatten, bränslen samt transporter av personer och varor. Till skillnad från administrativa IT-system, där informationsbehandlingen i sig är slutmålet, kan störningar av kommunikationer, datorsystem eller applikationer i digitala kontrollsystem innebära direkta störningar i den underliggande fysiska processen. Det kan i slutändan leda till leveransavbrott av samhällsviktiga nyttigheter.

Integrationen mellan digitala kontrollsystem och administrativa informationssystem ökar kraftigt

Processkontrollsystem har tidigare uppnått höga säkerhetskrav genom isolation från omvärlden och god fysisk säkerhet. Dagens krav på processorientering ur ett affärsperspektiv leder till en ökad integrering mellan de digitala kontrollsystemen och de administrativa informationssystemen, exempelvis system för logistik och ekonomi. För att uppnå hög flexibilitet och effektivitet görs digitala kontrollsystem även i en allt högre grad tillgängliga via Internet och andra publika nätverk. Denna integration exponerar de digitala kontrollsystemens sårbarheter för de hot som exempelvis finns på Internet.

Digitala kontrollsystem moderniseras sakta och hela system byts sällan ut samtidigt

Digitala kontrollsystem ingår i systemlösningar med lång livslängd och kan innehålla tekniska lösningar från flera generationer av kontrollsystem (så kallade legacy systems). Väl installerade är avsikten att kontrollsystemet ska ha en hög tillgänglighet och ha en bra funktionsgrad i många år. Inom många organisationer finns det därför en ovilja att förändra systeminställningar, systemkomponenter och liknande i produktionssatt utrustning, det vill säga efter de har tagit systemet i skarp drift. Detta kan leda till att de inte åtgärdar kända IT-säkerhetshål eller att det tar mycket lång tid innan de gör det.

Användandet av standardkomponenter förändrar leverantörernas roll och ökar kraven på användarna

Leverantörerna av processkontrollsystem har traditionellt sett oftast fungerat som en helhetsleverantör, det vill säga att de både har designat och byggt de system de har tillhandahållit. I dag används alltmer standardiserade tekniker och komponenter från den traditionella IT-världen (ofta benämnda Commercial-off-the-shelf, COTS) i digitala kontrollsystem. Några exempel på COTS-produkter som används är operativsystem från Microsoft, IP-baserad kommunikationsteknik och databaslösningar från Oracle. På grund av omställningen till standardkomponenter ändras leverantörernas roll från systemleverantörer till systemintegratörer. Det kan i sin tur leda till att de får minskad insyn och kontroll över viktiga delar i det integrerade systemet. I förlängningen kräver detta en ökad kunskap om säkerhet i digitala kontrollsystem hos slutanvändare av systemen.

Cyberattacker mot digitala kontrollsystem är ett trovärdigt hot

Säkerhet ur ett antagonistperspektiv (angriparperspektiv) har inte varit en avgörande fråga för utvecklingen av digitala kontrollsystem. Säkerhetsmedvetenheten hos såväl utrustnings-, system- och programleverantörer som upphandlare och beställare är ofta svag. Detta innebär att kravställningen kan bli bristfällig och system inte utformas att hantera säkerhet på ett lämpligt sätt. I dag finns sofistikerade verktyg för IT-attacker lätt åtkomliga via Internet. När digitala kontrollsystem i allt högre grad kopplas ihop i nätverk, och allt oftare bygger på IT-komponenter av standardtyp, så löper de allt större risk för att bli utsatta för cyberattacker.

Digitala kontrollsystem har god tillgänglighet – vanliga IT-säkerhetsproblem kan leda till driftsstörningar

Eftersom digitala kontrollsystem används för att övervaka och styra fysiska processer i realtid, så har systemet utvecklats för att upprätthålla en mycket hög tillgänglighet. Traditionella IT-säkerhetsproblem, såsom skadlig kod eller datorintrång, kan i processkontrollsammanhang påverka kontrollsystemens tillgänglighet och dess driftsmässiga säkerhetsaspekter. Till exempel kan ett virusdrabbat system få svarstider som är oacceptabla. Det kan i sin tur leda till att insamlingsvärden, larm eller kommandon inte tas emot på det sätt som de ursprungliga konstruktörerna har avsett.

Arbetet med säkerhet i digitala kontrollsystem leder till kulturkrockar i säkerhetsorganisationen

För att uppnå hög säkerhet i digitala kontrollsystem krävs både kunskap om traditionell IT-säkerhet samt kunskap om processkontrollsystem och den underliggande fysiska processen. Säkerhetsarbetet kräver därför samarbete mellan personer från olika kulturer med olika säkerhetstraditioner och organisatoriska hemvister. Sedvanlig IT-säkerhetskunskap går inte direkt att överföra till processkontrollsystem. Många nyproducerade dokument med säkerhetstips uttrycker sig i termer, eller ger rekommendationer, som kan vara svåra att tillämpa direkt på kontrollutrustningen. Att exempelvis härda ett system – det vill säga ta bort onödig, okänd eller oanvänd programvara, samt konfigurationsmässigt förbättra den programvara som man använder – är ett mycket svårt moment i ett produktionssatt kontrollsystem. Ofta går det inte att göra – både av tekniska och juridiska skäl – på annat sätt än att systemleverantören, efter en noggrann utvärdering, genomför dessa förändringar.

Säkerhet i digitala kontrollsystem uppmärksammas alltmer och detta leder till externa säkerhetskrav

I dag pågår ett flertal internationella initiativ för att ta fram standarder och rekommendationer för hur man skapar säkerhet i digitala kontrollsystem. Området har även fått stor uppmärksamhet hos många statliga aktörer. Genom att tillämpa ett proaktivt säkerhetsarbete redan i dag kan användare och leverantörer av digitala kontrollsystem aktivt vara med och påverka vilka säkerhetskrav som kommer att ställas på de här systemen i framtiden. Det kan även vara en konkurrensfördel att införa ett systematiskt säkerhetsarbete. I vissa branscher finns redan säkerhetskrav, exempelvis förväntas elbolag i USA att följa standarden NERC CIP.

Säkerhet i digitala kontrollsystem är lönsamt, men kräver en god säkerhetskultur och ett långsiktigt engagemang

Säkerhet i digitala kontrollsystem är inte främst ett tekniskt problem. Det handlar huvudsakligen om att få till en bra avvägning mellan risker och kostnader i organisationen. Att bygga upp en säkerhetskultur anpassad för att hantera nutida IT-relaterade hot är en långsiktig omställningsprocess som organisationen måste utföra med den högsta ledningens stöd. Det finns dock stora vinster med att hantera säkerhetsfrågor i förväg. Precis som för traditionella IT-system är det mycket dyrare att åtgärda säkerhetsproblem i digitala kontrollsystem efter att systemen har levererats. Den ökade integrationen mellan administrativa informationssystem och kontrollsystem innebär dock inte bara ökade säkerhetsproblem. En ökad integration kan även ge ökad effektivitet och förbättrad lönsamhet, tack vare bättre optimerade produktionsprocesser.

MER INFORMATION

Johansson, E., Christiansson, H., Andersson, R., Björkman, G. & Vidström, A. (2007) *Aspekter på antagonistiska hot mot SCADA-system i samhällsviktiga verksamheter.* Krisberedskapsmyndigheten, Stockholm. Rapporten kan laddas ned från:
`www.krisberedskapsmyndigheten.se/upload/SCADA_studie%20_070903.pdf`

Shaw, W. T. (2006) *Cybersecurity for SCADA systems.* PennWell Corp., Tulsa.


SJ
1348
1348


BIOGAS

Skillnader mellan administrativa IT-system och digitala kontrollsystem

Trots en ökande konvergens mellan administrativa IT-system och digitala kontrollsystem finns det fortfarande många betydande skillnader. I tabell 1 sammanfattar vi några av de viktigaste. Jämför även med de observationerna som vi presenterade i föregående avsnitt.

För att skapa säkerhet i digitala kontrollsystem krävs en god kännedom om deras respektive särdrag. Det är dock mycket viktigt att hålla i minnet att många välkända IT-attacker, konceptuella attackmetoder samt olika alternativ för att missbruka IT-system – sådana som är klassiska eller standardmässiga i administrativ IT-miljö – även fungerar i digitala kontrollsystem.

MER INFORMATION

NIST (2007) *Guide to Industrial Control Systems (ICS) Security.* SP 800-82, National Institute of Standards and Technology (NIST), Gaithersburg. Rapporten kan laddas ned från:
`http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf`

Tabell 1: Väsentliga skillnader mellan administrativa IT-system och digitala kontrollsystem [Tabellen är modifierad av författarna från NIST (2007)]

Kategori	Administrativa IT-system	Digitala kontrollsystem
Prestationskrav	Ej realtid	Realtid
	Respons måste vara konsekvent	Respons är tidskritisk
	Höga krav på utförandehastighet	Moderat utförandehastighet acceptabel
	Fördröjning och jitter kan vara acceptabelt	Fördröjning och jitter är allvarliga problem
Tillgänglighetskrav	Respons i form av omstart är acceptabelt	Respons i form av omstart kan vara oacceptabelt p.g.a. tillgänglighetskrav i industriprocessen
	Tillgänglighetsavvikelser kan ofta tolereras, beroende på systemets operationella krav	Störningar måste planeras och schemaläggas dagar/veckor i förväg
Riskhanteringskrav	Datasekretess (konfidentialitet) och riktighet (integritet) är viktigast	Säkerhet (safety) är viktigast, både när det gäller människor och produktionssystem
	Feltolerans är mindre viktig – tillfälligt driftstopp är oftast inte en allvarlig risk	Feltolerans är mycket viktig, även kortare driftstopp är oacceptabla
	Största risk är störningar i affärsverksamheten	Största risk är förlust av liv, processutrustning eller produktionskapacitet
Säkerhetsarkitektur	Primärt fokus är att skydda datorrelaterade tillgångar och information som lagras eller sänds	Primärt fokus är att skydda ändutrustning (t.ex. styrutrustning såsom PLC:er)
	Centrala servrar kan behöva extra skydd	Skydd av centrala servrar fortfarande viktigt
Säkerhetslösningar	Säkerhetslösningar är designade för typiska IT-system	Säkerhetsverktyg måste testas för att garantera att de inte äventyrar kontrollsystemets normala drift

Kategori	Administrativa IT-system	Digitala kontrollsystem
Tidskritisk interaktion	Mindre kritiskt med interaktion i nödlägen	Respons på mänsklig eller annan interaktion i nödlägen är kritisk
	Access till systemresurser kan begränsas och kontrolleras i önskad grad	Access till kontrollsystem bör kontrolleras strikt – får dock ej störa människa-maskin-interaktion (speciellt viktig i nödlägen)
Systemoperation och Change Management	Systemen är designade för att använda sig av vanliga operativsystem	Specifika och specialanpassade operativsystem samt vanliga operativsystem
	Uppgradering är enkelt och görs i enlighet med säkerhetspolicy och rutiner – automatiska verktyg finns tillgängliga	Uppgradering av programvara bör ske stegvis och kräver ofta medverkan av systemleverantör, exempelvis p.g.a. modifierad hårdvara och programvara
Resursbegränsningar	Tillräckliga systemresurser finns för att stödja tillägg av tredjepartsapplikationer (säkerhetslösningar)	Systemen är designade för specifika industriella processer varför minnekapacitet och beräkningsresurser kan begränsa möjliga säkerhetslösningar
Kommunikationer	Kommunikationsprotokoll av standardtyp	Många skräddarsydda kommunikationsprotokoll (kommersiella), men även standardprotokoll
	Främst trådbundna nätverk och lokala trådlösa nätverk	Många olika typer av media för kommunikation, t.ex. optofiber, radiolänk, satellit (även privata nät)
	Kommunikationsnätverken bygger på typisk IT-nätverkspraxis	Kommunikationsnätverken är komplexa och kräver teknisk kunskap om kontrollsystem
Support	Många olika varianter och leverantörer	Vanligtvis endast ett fåtal leverantörer
Livslängd	Komponenter och system har kort livslängd (typiskt 3–5 år)	Komponenter och system har lång livslängd (typiskt 15–20 år)
Fysisk tillgång	Komponenter är oftast lokalt placerade och enkla att nå	Komponenter kan vara isolerade, geografiskt avlägsna och svåra att nå

God säkerhetskultur – en grundförutsättning

För att skapa ett väl fungerande arbete med säkerhet i digitala kontrollsystem behöver organisationen ha en god säkerhetskultur, det vill säga en fungerande generell riskhantering och ett systematiskt informationssäkerhetsarbete. Figur 2 nedan illustrerar relationerna mellan de aktiviteter som bör ingå i en systematisk riskhantering.

De rekommendationer som vi ger i det här dokumentet ansluter till ISO:s informationssäkerhetsstandarder (27000-serien), exempelvis den ledningsmodell för informationssäkerhet som presenteras i *ISO/IEC 27001* (SIS, 2006).

Det finns en stor mängd analysmetoder för riskanalyser av IT-system. Krisberedskapsmyndigheten har givit ut BITS, Basnivå för informationssäkerhet [KBM (2006)], och ett tillhörande verktyg för informationssäkerhetsanalys (BITS Plus). BITS och BITS Plus gör det enklare att starta upp informationssäkerhetsarbetet i en organisation, för att sedan gå vidare med att exempelvis införa ISO-standarderna ovan. Ytterligare exempel är den amerikanska myndigheten NIST:s rapport *SP 800-30* som beskriver en generell modell för risk-analys av IT-system, samt *SP 800-34* som behandlar kontinuitetsplanering i IT-system (NIST, 2002a; NIST, 2002b).”

I dagsläget finns inga, som författarna känner till, väletablerade riskanalysmetoder som specifikt behandlar IT-säkerhet i digitala kontrollsystem.

MER INFORMATION

IEC (1995) *Dependability management – part 3: application guide – section 9: risk analysis of technological systems.* International Electrotechnical Commission (IEC), Geneva.

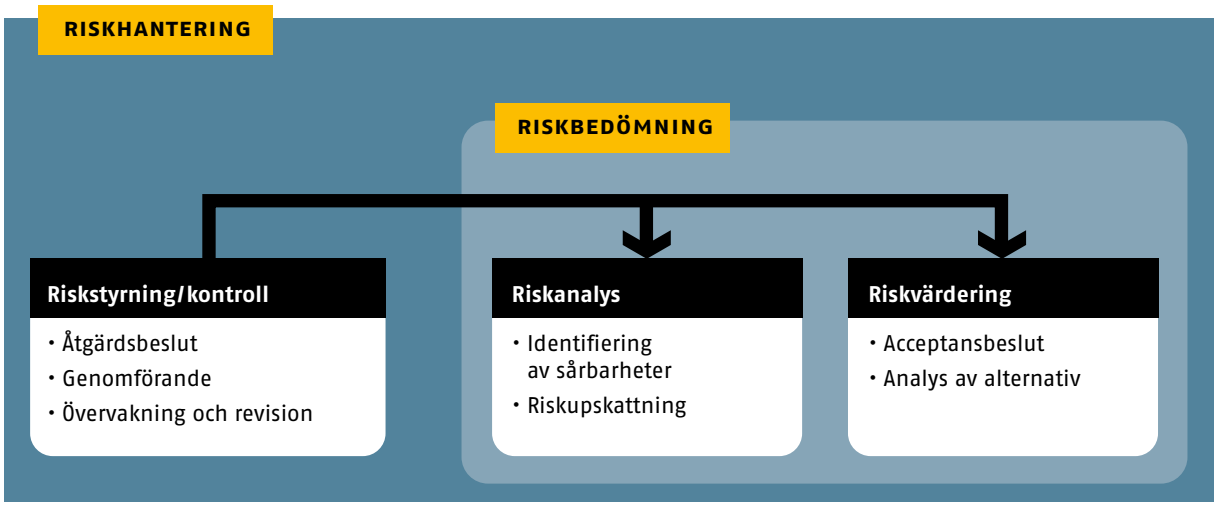
KBM (2006) *Basnivå för informationssäkerhet (BITS).* KBM rekommenderar 2006:1, Krisberedskapsmyndigheten (KBM), Stockholm. Rapporten kan laddas ned från: `http://www.krisberedskapsmyndigheten.se/upload/8043/bits_rek_2006_I.pdf`

NIST (2002a) *Risk Management guide for information technology systems.* SP 800-30, National Institute of Standards and Technology (NIST), Gaithersburg.Rapporten kan laddas ned från: `http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf`

NIST (2002b) *Contingency planning guide for information technology systems. SP 800-34*, National Institute of Standards and Technology (NIST), Gaithersburg. Rapporten kan laddas ned från: `http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf`

SIS (2006) *Ledningssystem för informationssäkerhet – Krav*, SS-ISO/IEC 27001:2006, Swedish Standards Institute (SIS).

Figur 2: Riskhantering [figuren modifierad av författarna från IEC (1995)]



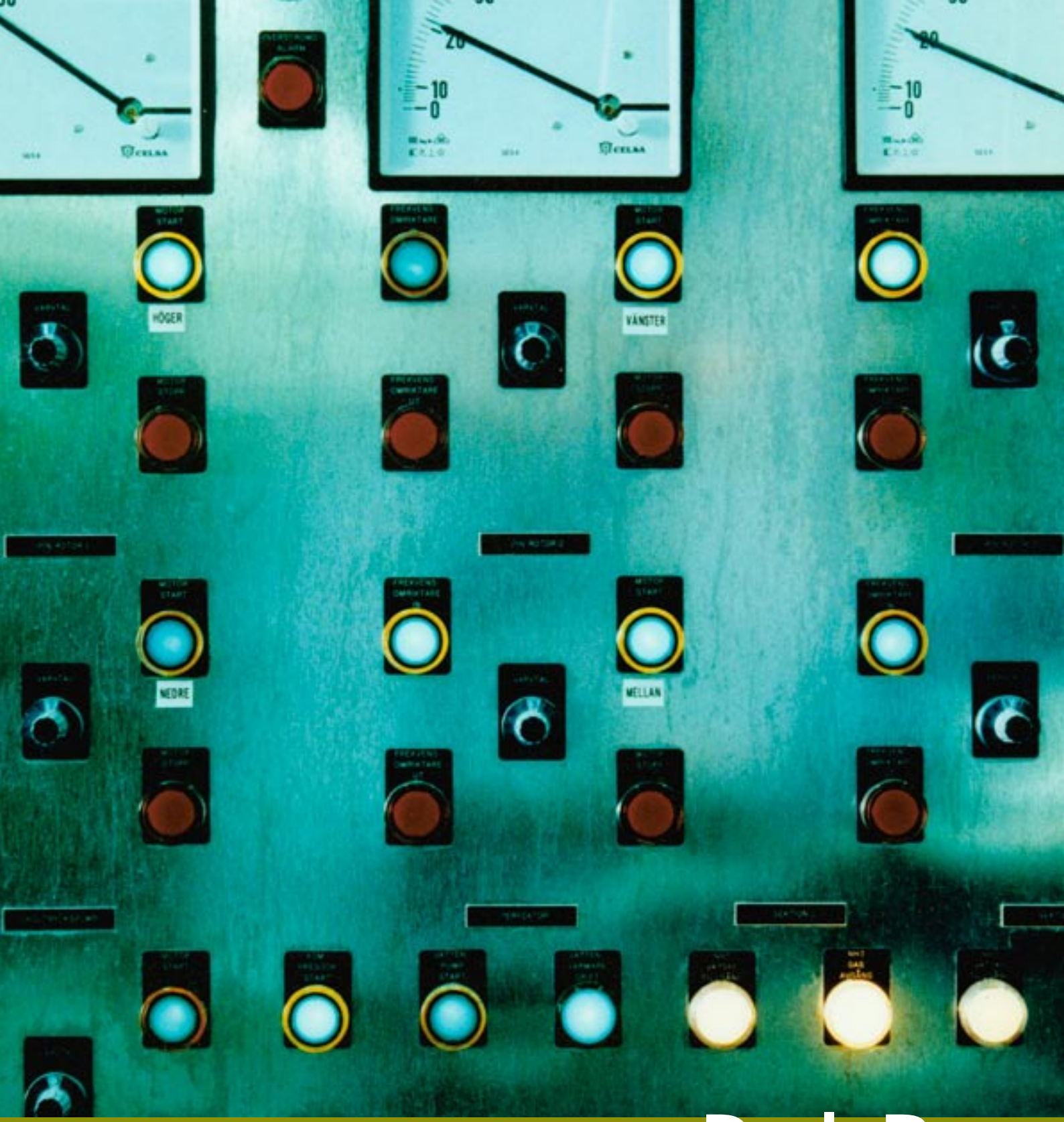
Sammanfattande rekommendationer för ökad säkerhet i digitala kontrollsystem

I avsnitt B ger vi en mer detaljerad vägledning till rekommendationer och etablerade riktlinjer. Här sammanfattar vi de viktigaste rekommendationerna.

Urvalet bygger på diskussioner inom FIDI-SC samt erfarenheter från forskning och praktiska projekt som författarna har deltagit i. Det har även stöd i internationella rekommendationer och i välkänd praxis.

Nedanstående rekommendationer utgör ett första steg i arbetet med att öka säkerheten i digitala kontrollsystem.

1. **Öka medvetandet i hela organisationen om behovet av säkerhet i digitala kontrollsystem.**
   Detta är en verksamhetskritisk fråga och därför bör högsta ledningen involveras i ett tidigt skede.
2. **Genomför grundläggande utbildning kring säkerhet i digitala kontrollsystem.**
   Operatörer av kontrollsystem behöver öka sin kunskap om traditionell IT-säkerhet. IT-personal behöver mer kunskap om processkontrollsystem och den underliggande fysiska processen. Även personer som är inblandade i upphandling och verksamhetsplanering behöver utbildning i dessa frågor.
3. **Håll digitala kontrollsystem separerade från administrativa IT-system i så hög grad som möjligt.**
   Kartlägg befintliga digitala kontrollsystem och identifiera externa anslutningar till dem. Digitala kontrollsystem bör endast i undantagsfall integreras med administrativa IT-system. Det kräver en mycket kvalificerad logisk separering av systemen.
4. **Ställ säkerhetskrav i all upphandling av digitala kontrollsystem och i serviceavtal.**
   Det finns stora vinster med att hantera säkerhetsfrågor i förväg. Precis som för traditionella IT-system är det mycket dyrare att åtgärda säkerhetsproblem i digitala kontrollsystem efter att systemen har levererats.



Del B

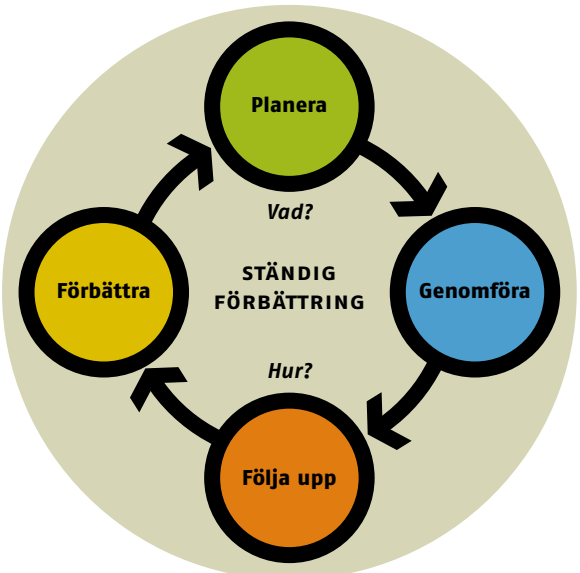
Detaljerad vägledning till rekommendationer och etablerade riktlinjer

Utgångspunkt för rekommendationer

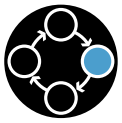
I detta avsnitt ger vi rekommendationer för att öka säkerheten i digitala kontrollsystem. Urvalet av rekommendationer bygger på diskussioner inom FIDI-SC samt erfarenheter från praktiska projekt som författarna deltagit i. Det har även stöd i internationella rapporter och i välkänd praxis. Rekommendationerna är inte givna i prioritetsordning och i vissa avseenden överlappar de varandra.

De aktiviteter som vi föreslår i följande rekommendationer är en del i ett löpande kvalitetsarbete. För att tydliggöra vikten av att aktiviteterna är en del av ett *kontinuerligt förbättringsarbete* relaterar vi dessa till den välkända Demings kvalitetscykel (Figur 3), även kallad PDCA-modellen (Plan, do, check, act). Man tillämpar även PDCA-modellen i flera internationella standarder, exempelvis i ISO/IEC 27000-serien om ledningssystem för informationssäkerhet. Målsättningen är att organisationens arbete med säkerhet i digitala kontrollsystem på detta sätt ska kunna få en naturlig koppling till det övriga informations-, säkerhets- och kvalitetsarbetet.

Figur 3: Vi använder PDCA-modellen (Demings kvalitetscykel) i detta dokument, dels för att betona vikten av att arbetet består av ständiga förbättringar, dels för att strukturera rekommendationerna.



Planeringsfasen
omfattar att upprätta policy, mål, processer och rutiner.



Genomförandefasen
omfattar att införa och driva policy, åtgärder, processer och rutiner.

Uppföljningsfasen
omfattar att övervaka och granska genom att bedöma, mäta och rapportera.

Förbättringsfasen
omfattar att underhålla och förbättra – det vill säga att vidta korrigerande förbättrande åtgärder.

I de följande avsnitten ger vi tips på var man kan hitta mer information. De etablerade riktlinjer och standarder som vi hänvisar till, beskriver vi närmare i **Del C**. Nedan skriver vi dem kortfattat på följande sätt:

NERC CIP	Cyber security standard CIP-002-1 – 009-1
NIST 800-82	Guide to industrial control systems (ICS) security
CPNI GPG	Good practice guide process control and SCADA security
DOE 21 Steps	21 steps to improve cyber security of SCADA networks
OLF 104	Krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer
PL	Cyber security procurement language for control systems

Rekommendationer för en ökad säkerhet i digitala kontrollsystem

01 Tydliggör roller och ansvar för säkerheten i digitala kontrollsystem.

02 Etablera en process för att kartlägga digitala kontrollsystem och för att genomföra riskanalyser.

03 Etablera en process för förändringshantering i digitala kontrollsystem.

04 Etablera processer för kontinuitetsplanering och incidenthantering i digitala kontrollsystem.

05 Inkludera säkerhetskrav i digitala kontrollsystem från början i all planering och upphandling.

06 Skapa en god säkerhetskultur och höj medvetandet om behovet av säkerhet i digitala kontrollsystem.

07 Skapa ett djupledsförsvar i digitala kontrollsystem.

08 Inför intern och extern intrångsdetektering och incidentövervakning dygnet runt i digitala kontrollsystem.

09 Genomför riskanalyser av digitala kontrollsystem.

10 Genomför regelbunden teknisk säkerhetsgranskning av digitala kontrollsystem och anslutna nätverk.

11 Utvärdera löpande digitala kontrollsystems fysiska skydd.

12 Se till att endast säkra och relevanta anslutningar till digitala kontrollsystem existerar.

13 Härda och uppgradera digitala kontrollsystem i samverkan med systemleverantörer.

14 Följ upp incidenter i digitala kontrollsystem och bevaka säkerhetsproblem i omvärlden.

15 Samverka i användarföreningar, standardorgan och andra nätverk för att öka säkerheten i digitala kontrollsystem.

01 Tydliggör roller och ansvar för säkerheten i digitala kontrollsystem

NERC CIP (003-1) **NIST SP 800-82** (Kap. 4.2, 6.1, 6.2) **CPNI GPG** (GPG 4, GPG 7)
DOE 21 Steps (No. 12, 16, 20) **OLF 104** (No. 1, 3)

I många organisationer är processorienterad styrning vanligt när det gäller administrativa informationssystem. I denna styrmodell finns ofta utsedda systemägare, informationsägare, förvaltningsansvariga, driftsansvariga, systemadministratörer eller liknande.

När det gäller kontrollsystem saknas ofta denna *roll- och ansvarsfördelning*, det vill säga både ansvarsområden och styrmodeller saknas. Ibland är leverantörsrepresentanter det närmaste en IT-tekniker eller systemadministratör som finns att tillgå. Dessutom kan processingenjörer, utan kunskaper om logisk säkerhet i kontrollsystem, vara de som praktiskt förvaltar systemen. Det här leder till att den egna organisationen har litet eller inget kunnande om de digitala kontrollsystemens IT-tekniska egenskaper. Det i sin tur leder till minskad kontroll och förmåga att styra tekniken och dess användning.

Ansvarsfördelningen för dessa säkerhetsfrågor tydliggörs enklast genom att skapa en *säkerhetspolicy för digitala kontrollsystem*. Denna policy kan antingen vara ett separat dokument, som i så fall måste relateras till organisationens övriga policydokument, eller så kan frågan lösas genom tillägg i organisationens informationssäkerhetspolicy.

Roll- och ansvarsfördelningen hos de administrativa informationssystemen och kontrollsystemen bör samordnas. Det bör tydligt framgå vilka system som organisationens centrala IT-stöd förvaltar och vilka system som förvaltas lokalt ute i produktionen. Hur detta rent praktiskt genomförs har koppling till hur organisationen väljer att införa skydd och nivåer av skyddsbarriärer i sin totala IT-miljö. Även om en stor del av de processnära systemen förvaltas lokalt så är det nödvändigt att organisationens centrala IT-stöd ansvarar för den totala integrationen och skapar en sammanhållen syn på säkerhetsfrågorna. Ett viktigt skäl till att det krävs en *sammanhållen syn på organisationens informationssäkerhet* är det blir alltmer vanligt med omfattande datautbyten mellan kontrollsystem och administrativa system.

Exempel på risker och problem

Om ingen är utsedd att vara systemägare, systemförvaltare respektive systemadministratör för ett kontrollsystem så är det stor sannolikhet för att löpande säkerhetsarbete – exempelvis att uppdatera program eller att spärra före detta entreprenörers konton – inte genomförs, eller inte genomförs i tid.

Vid händelse av ett säkerhetsproblem, exempelvis en infektion av skadlig kod, finns det ingen som känner ansvar eller vet vilka befogenheter de har för att hantera incidenten. Detta kan fördröja det skadebegränsande arbetet och leda till att verksamheten påverkas mer än nödvändigt.

02 Etablera en process för att kartlägga digitala kontrollsystem och för att genomföra riskanalyser

NERC CIP (002-1) **DOE 21 Steps** (No.13) **OLF 104** (No. 2, 3, 11)

För att skapa säkerhet i digitala kontrollsystem är det viktigt att det finns en etablerad process för att kartlägga och förstå verksamhetens informationsflöden och systemberoenden, det vill säga de samband som finns mellan olika typer av system och verksamheten.

Det är väsentligt att verksamhetens processer, system och information analyseras baserat på en förståelse för vilka konsekvenser en felaktig eller störd funktion kan innebära både för processen och för organisationen. Detta är en viktig förutsättning för att skapa en relevant riskvärdering och en klassificering av vilka system som är mest kritiska respektive vilken information som är mest kritisk.

En verksamhets- och systemkartläggning bör resultera i listor över åtkomst- och anslutningsmöjligheter, systemklassificeringar samt driftsmässiga prioriteringsindelningar. Det bör finnas tillgängliga diagram över de digitala kontrollsystemen med tillräcklig detaljeringsgrad för att göra det möjligt att identifiera kritiska komponenter och system. Exempel på information som bör finnas tillgängliga i *systemdiagram* är uppgifter om operativsystem hos datorresurser, IP-adresser, kommunikationsprotokoll, tekniska uppgifter om lokala enheter, såsom PLC:er och så vidare. För att kunna fastställa den elektroniska säkerhetsperimetern måste alla anslutningar till digitala kontrollsystem identifieras. Här ingår, förutom intranät, exempelvis fjärranslutna kopplingar till samarbetspartners, leverantörer och Internet. Observera att alla trådlösa anslutningar bör behandlas som fjärranslutna punkter. Anslutningar till organisationens administrativa informationssystem (intranät) bör betraktas som externa anslutningar.

Organisationens kritiska tillgångar bör identifieras genom att tillämpa ett riskbaserat synsätt. Baserat på denna analys identifieras sedan de *kritiska datorbaserade tillgångarna*. Det här kräver att det finns en dokumenterad process för hur riskanalyser ska genomföras och under vilka förutsättningar de ska uppdateras. Valet av riskanalysmetod bör anpassas efter analysens syfte och den tillgängliga informationen. För att göra det smidigt att uppdatera riskanalyserna, välj inte en onödigt avancerad riskanalysmetod.

Exempel på risker och problem

Om organisationen saknar en standardiserad process för riskanalys och kartläggning av kontrollsystem, blir det svårare att jämföra och övervaka hur verksamhetens risker förändras över tiden.

Om organisationen saknar en anpassad riskbedömning kan det innebära att viktiga kontrollsystem är oskyddade. Då satsar man i stället onödigt stora resurser på att skydda andra informationsresurser, som inte är kritiska för verksamhetens överlevnad.

03 Etablera en process för förändringshantering i digitala kontrollsystem

■ **NERC CIP** (003-1) ■ **DOE 21 Steps** (No. 17) ■ **OLF 104** (No. 10, 15)

En *kontrollerad hantering av förändringar* och versioner av parametersättningar, inställnings- och datafiler eller program är viktig för att undvika störningar, onödig felsökning eller allvarliga problem i digitala kontrollsystem. System och applikationer som organisationer ska använda under lång tid, exempelvis inom industriprocesser, medför särskilda krav på strikt kontroll över förändringshanteringen.

Uppgradering av programvara bör ske stegvis och kräver ofta medverkan av systemleverantörer, både på grund av juridiska och tekniska krav. I processkontrollmiljöer är det viktigt att alla inblandade parter – leverantörer, systemansvariga och användare – har en korrekt och gemensam förståelse av den aktuella konfigurationen och driftstatusen hos systemet. Separata test-, utvecklings- och driftsmiljöer är vanliga när det gäller administrativa informationssystem. Tyvärr gäller inte detta digitala kontrollsystem. Därför kan det krävas extra ekonomiska resurser för att skapa förutsättningar för en god förändringshantering i de här systemen.

Det bör finnas en formell process som talar om hur man får tillstånd att göra förändringar i digitala kontrollsystem. Inga förändringar bör vara tillåtna utan att ett formellt tillstånd har givits. Detta bör även gälla tillfälliga förändringar och förändringar av stödutrustning. För att upprätthålla en god säkerhet i kritiska system bör i princip allt som inte är explicit tillåtet vara förbjudet.

Den formella processen för förändringshantering bör åtminstone omfatta en procedur för få tillstånd att göra förändringar, en beskrivning av hur *tester före och efter en förändring* ska genomföras (inklusive en beskrivning av vilka förändringar som kräver tester i separat testmiljö), krav på hur dokumentation ska uppdateras efter förändringar, samt krav på hur personal ska ta del av förändringar (exempelvis i vilka fall det krävs särskild träning av operatörer).

Exempel på risker och problem

En leverantör verifierar förändringar i ett testsystem som installationsmässigt avviker mot kundens faktiska system. När förändringarna så småningom införs i det driftssatta systemet, uppträder oväntade systemhändelser och kontrollsystemet blir instabilt.

Lokala förändringar i ett kontrollsystem meddelas inte till leverantören. Vid nästa programuppgradering försvinner funktionalitet, rättningar av säkerhetsproblem faller bort, och parametersättningar återgår till ordinarie fabriksinställningar.

Digitala kontrollsystem har i många fall en mer statisk programvarustatus än informationssystem och löpande säkerhetskopiering utförs därför inte lika ofta. Ibland sker säkerhetskopiering enbart vid systemdrifttagande eller större förändringar. Därför finns risken att man tappar bort små förändringar eller glömmer bort att återföra dem i samband med en eventuell återinstallation från säkerhetskopian.

04 Etablera processer för kontinuitetsplanering och incidenthantering i digitala kontrollsystem

NERC CIP (008-1, 009-1) **NIST 800-82** (Kap. 6.2.3) **CPNI GPG** (GPG 3)
DOE 21 Steps (No. 19) **OLF 104** (No. 7, 16)

För att säkerställa verksamhetens fortlevnad vid allvarligare störningar krävs en kontinuitetsplanering som innehåller tydliga beskrivningar av roller och ansvar vid nödlägen. Exempel på detta är avbrott i kraftförsörjningen, haveri av styrsystem, sjukdom hos operativa nyckelpersoner och så vidare.

Förutom att kontinuerligt följa upp och uppdatera kontinuitetsplaner är det viktigt att personalen får öva sin beredskap och att man regelbundet testar att verksamheten skulle kunna fungera tillfredsställande i händelse av en kris. För digitala kontrollsystem är det extra viktigt att kontrollera att *backuper* är utförda och kan användas för att återställa systemen. Några viktiga punkter som bör ingå i kontinuitetsplaneringen är

- rutiner för att sköta verksamheten manuellt (driva processen utan datorstöd)
- rutiner för att återställa data och konfigurationsinställningar samt återstarta processen
- kontaktuppgifter till operatörer, drifttekniker, övrig personal, leverantörer och support
- beskrivning av hur centrala komponenter i kontrollsystemet återanskaffas
- beskrivning av hur, och varifrån, nöddrift genomförs om störningen är allvarlig.

Alla *oväntade händelser* som leder till att en störning uppträder i de digitala styrsystemen, exempelvis att en tjänst inte är tillgänglig eller har reducerad funktionalitet, *måste dokumenteras* för att senare kunna analyseras. En av svårigheterna med incidenthanteringen är att finna en balanserad struktur över hur incidenter ska kunna fångas in utan att det uppfattas som hindrande i den normala arbetsprocessen. Vidare är det viktigt att motivera organisationen genom att kommunicera syftet med rapporteringen av incidenter samt att återkoppla resultaten av incidenthanteringen. Utan denna kommunikation kan det bli svårt att bevara motivationen att rapportera incidenter och svagheter.

Exempel på risker och problem

En verksamhet drabbas av stor störning och tvingas att återställa ett verksamhetskritiskt kontrollsystem fullständigt. Man har gjort regelbunden backup av systemet, men inte hanterat backupbanden på ett varsamt sätt. Därför har de åldrats så pass att en återställning inte är möjlig.

Den person som ansvarar för de digitala kontrollsystemen i en verksamhet avlider under sin semester. Det primära problemet är att ingen i organisationen kan ta över hans arbetsuppgifter. Sedan visar det sig även att han var den enda som kände till de viktigaste lösenorden för vissa systemförändringsmöjligheter och hur några av de centrala systemen konfigurerats.

05 Inkludera säkerhetskrav i digitala kontrollsystem från början i all planering och upphandling

NIST 800-82 (Kap. 6.1.3) **CPNI GPG** (GPG 6) **OLF 104** (No. 8, 9) **PL** (Alla kapitel)

En verksamhet är det mycket viktigt att säkerhetsfrågor inkluderas i planeringen i ett så tidigt skede som möjligt.

Det är svårt och dyrt att uppnå en godtagbar säkerhetsnivå i kontrollsystem i efterhand. Därför bör säkerhetskrav inkluderas från allra första början i systemspecifikationer och behovsanalyser. Eftersom många systemlösningar helt eller delvis upphandlas från externa parter, så krävs en särskild uppmärksamhet på säkerhetsfrågorna i upphandlingsarbetet.

Säkerhet i digitala kontrollsystem bör behandlas uttryckligen i upphandlingsunderlag, test- och överlämnandehantering, kontrakt och styrdokument för underhåll eller driftsuppdrag. Upphandling kan omfatta såväl nyinstallation som hel- eller delvis modernisering av befintliga lösningar. Säkerhetskrav bör ingå som en viktig del i alla leverantörsavtal, även service- och underhållsavtal. Ett bra tekniskt stöd i all upphandling av kontrollsystem är *Cyber security procurement language for control systems* (PL).

I samband med moderniseringar av kontrollsystem krävs en särskild hänsyn till IT-säkerhetsfrågor. Detta för att förändringarna med största sannolikhet kommer att påverka det befintliga kontrollsystemet på ett sätt som de ursprungliga konstruktörerna inte hade tänkt på. Exempelvis är det ofta ett underförstått antagande i äldre kontrollsystem att åtkomst till utrustning enbart kan ske via lokal fysisk närvaro. I dag är dock fysisk separation i många situationer inte längre möjlig, utan det handlar snarare om att skapa en logisk separation mellan olika delar av processkontrollsystemen.

Kravinsamling bör ske i form av olika kartläggningar samt hot- och riskanalyser. Förutom att leva upp till detaljerade krav på säkerhets- och skyddsfunktioner i system och applikation, bör leverantören även kunna redovisa vilka egna metoder eller processer (exempelvis interna utvecklarhandböcker) som används för att garantera kvaliteten på det egna säkerhetsarbetet.

Exempel på risker och problem

Försummade säkerhetskrav vid upphandling leder till dyra tilläggsbeställningar samt ogenomtänkta och krångliga tekniska säkerhetslösningar i efterhand.

Missade säkerhetskrav vid upphandling kan innebära att systemet är onödigt sårbart under hela sin livscykel.

06 Skapa en god säkerhetskultur och höj medvetandet om behovet av säkerhet i digitala kontrollsystem

NERC CIP (004-1) **DOE 21 Steps** (No. 21) **OLF 104** (No. 5)

Det är viktigt att skapa en förståelse för att säkerhet i digitala kontrollsystem är en verksamhetskritisk fråga. Förståelse och attitydpåverkan kräver långsiktiga insatser och högsta ledningens engagemang är, som alltid när det gäller säkerhetsfrågor, mycket viktigt. Dels för att säkerhet i digitala kontrollsystem kräver ökade resurser ,dels för att det kräver en samverkan mellan delar av organisationen som inte alltid brukar samarbeta.

För att uppnå hög säkerhet i digitala kontrollsystem krävs både *kunskap om traditionell IT-säkerhet, kunskap om processkontrollsystem* och den underliggande fysiska processen. Säkerhetsarbetet kräver därför ett samarbete och ett förtroende mellan personer från olika kulturer med olika säkerhetstraditioner och organisatoriska hemvister. Detta kräver regelbunden utbildning och träning, både av IT-personal och av kontrollsystems operatörer.

Digitala kontrollsystem ingår i systemlösningar som är mycket långlivade. Det är särskilt viktigt att försöka tänka på hur man kommer att använda, eller missbruka, systemen i framtiden. Många normala aktiviteter kan, på grund av okunskap eller otydliga rutiner, leda till potentiella säkerhetsproblem.

Organisationen bör etablera ett administrativt säkerhetsprogram för att skapa ett generellt förhållningssätt till IT. Det ger ett bra säkerhetsmedvetande, uppmuntrar till ett kritiskt tänkande samt skapar en positiv attityd till att arbeta med sådant som höjer säkerheten.

Exempel på risker och problem

En operatör tillbringar en lugn stund vid en ordinarie driftsituation med att på en operatörsdator följa ett sportevenemang via Internet (strömmande ljud- och bildutsändningar). Samtidigt chattar han med kompisar via IRC. Detta leder till att spyware drabbar operatörsdatorn, vilket i sin tur gör datorn obrukbar.

Några drifttekniker arbetar med en leverantörs fältpersonal ute i en anläggning i produktionssystemet och behöver oplanerat flytta program och data mellan två olika IT-miljöer. Man brukar vanligen flytta data mellan dessa nät via en speciell löstagbar hårddisk. För att slippa hämta hårddisken, drar de en nätverkskabel mellan de två datorerna i de vanligtvis separerade näten. Efter arbetsdagens slut glömmer de att ta bort nätverkskabeln och den operatör som brukar sitta vid datorn tror att kabeln ska vara kvar. Kontrollsystemet är nu inte längre fysiskt separerat, utan i stället direkt kopplat till företagets intranät. Eftersom kontrollsystemet alltid har varit fysiskt isolerat har organisationen inte ansett sig behöva installera några IT-säkerhetsmekanismer.

07 Skapa ett djupledsförsvar i digitala kontrollsystem

NERC CIP (005-1, 007-1) **CPNI GPG** (GPG Firewall Deployment) **DOE 21 Steps** (No. 5, 15)
OLF 104 (No. 4, 13) **PL** (Alla kapitel)

En grundläggande princip för att skydda moderna IT-system är att utforma ett *försvar i djupled* (defence-in-depth), det vill säga att använda flera nivåer av skydd och överlappande säkerhetsmekanismer. Skyddsmekanismerna kan vara av samma typ, exempelvis flera brandväggar. De kan också bestå av olika typer av kompletterande skyddsmekanismer, exempelvis en brandvägg som nätverkssäkerhetsskydd kombinerad med en stark autentisering för åtkomst till IT-systemet.

En stark drivkraft inom alla typer av organisationer är en alltmer effektiv informationshantering. Detta innefattar bland annat att koppla ihop informationssystem på ett sådant sätt att dubbelarbete undviks – information i ett IT-system ska inte behöva skrivas in manuellt i ett annat system. Äldre kontrollsystem, eller digitala komponenter som finns i processmiljöer, är ofta utvecklade under en tid då fysiskt skydd var det enda de behövde. Logiska skydd var inte ens påtänkta. Kända brister och sårbarheter som åtgärdats i den administrativa IT-miljön för många år sedan finns vanligtvis kvar i processkontrollsystem. Sammankopplingar mellan olika nät kan därför exponera digitala kontrollsystem för hot som de saknar skydd mot och alla externa kopplingar till dessa system medför avsevärda risker. En grundlig riskanalys bör därför föregå en integration av kontrollsystem och administrativa IT-system. Ihopkopplingen av systemen kräver dessutom ett IT-säkerhetsskydd av extremt god kvalitet.

Ett moment som förr eller senare måste utföras är att skapa en elektronisk säkerhetsperimeter (logiskt skalskydd) runt processkontroll- och driftsystemen. Det är viktigt att på en konceptuell nivå kunna skilja mellan det som logiskt bildar ett systemlandskap och de övriga systemen inom organisationen.

Digitala kontrollsystem bör vara uppdelade i flera olika zoner med skyddsnivåer som anpassats efter hur kritiska de olika systemen är. Det betyder att nätverksarkitekturen bör vara segmenterad med överlappande säkerhetsmekanismer, och osäkra tjänster och anslutningar bör placeras i så kallade demilitariserade zoner (DMZ).

Datautväxling mellan digitala kontrollsystem via en DMZ till andra system i omvärlden, exempelvis affärssystem, bör ske på ett begränsat och kontrollerat sätt. Utgående kommunikation från kontrollsystem till affärssystem bör vara begränsad då det gäller tjänster och portar. Det kan även vara lämpligt att använda olika kommunikationsprotokoll för kommunikationen mellan olika delar av nätverket. Om ett protokoll används för kommunikationen mellan kontrollsystemet och en DMZ, så bör ett annat protokoll användas för den vidare kommunikationen mellan DMZ och organisationens administrativa informationssystem.

Även kommunikationen inom ett kontrollsystem kan behöva skyddas. Kommunikationen mellan fältutrustning, exempelvis PLC:er, och lokala system baseras i de flesta system på industriella protokoll med låg eller obefintlig säkerhet.

Exempel på risker och problem

Eftersom man har förstått att "security by obscurity" (säkerhet genom förvanskning eller fördöljande) inte är någon fungerande säkerhetslösning, så implementerar organisationen ett perimeterskydd (logiskt skalskydd), som man tror är starkt och omfattande. En anställd ansluter en arbetsstation till Internet via en osäker uppkoppling och skapar på så sätt ett hål i perimeterskyddet. Väl inne i systemet finns det inga säkerhetsmekanismer (inget djupförsvar) som kan hindra att skadlig kod, eller en hacker, ställer till med en omfattande skada.

Det är viktigt att få en balanserad avvägning mellan hur mycket arbete och resurser som används för fysiska respektive logiska skydd. Det är lätt att föredra fysiska skydd, till exempel dubblering av datorer eller en ståldörr, på bekostnad av logiska skydd som är mycket mer abstrakta. En tankemiss i det fysiska skyddet kan leda till att både primärsystem och sekundärsystem blir drabbade av ett logiskt fel, exempelvis en broadcaststorm på nätverket, eller ett fysiskt fel, exempelvis ett hårdvarufel i en central nätverkskomponent.

08 Inför intern och extern intrångsdetektering och incidentövervakning dygnet runt i digitala kontrollsystem

NERC CIP (005-1) **DOE 21** Steps (No. 8)

Till skillnad från incidentuppföljning (omvärldsbevakning) och uppdatering av riskanalyser syftar intrångsdetektering och säkerhetsövervakning till att analysera angreppsförsök och angrepp mot den egna organisationen. Omvärldsbevakningen tillsammans med en god övervakning av de egna systemen och dess kommunikationer ger en god totalförståelse av hotbilder, såsom förändrade attacktrender och aktuell skadlig kod.

Det finns två typer av *intrångsdetekteringssystem* (IDS). Dels finns system som känner igen attackförsök via analys av kommunikationsströmmar (nätbaserade intrångsdetekteringssystem, NIDS), dels finns system som övervakar händelser i ett datorsystem eller användningsmönster i en applikation (värddatorbaserade intrångsdetekteringssystem, HIDS). En utvecklad variant av dessa system är så kallade intrångsförhindrande system (IPS), som inte bara kan upptäcka attackförsök, utan även aktivt agerar för att avstyra angrepp.

Observera att installation av IPS i kontrollsystem vid felaktig angreppsklassificering, kan leda till att korrekt trafik blockeras (så kallade falska positiver). Att säkerhetssystemet oförutsägbart går in och blockerar styrkommandon eller resultatkoder är inte acceptabelt i digitala kontrollsystem.

Så kallade honungsfällor kan också användas för att indikera pågående angreppsförsök. En enkel lösning som kan vara lämplig i kontrollsystem, är att installera en dator i nätverket som normalt inte mottar någon trafik och som slår larm om så sker (en sådan honungsfälla kallas ibland Canary eller försåtsminering). Redan försök till kommunikation med den här datorn kan vara skäl till att misstänka ett pågående attackförsök eller att en angripare försöker förbereda en attack genom att inventera nätverket.

Det är viktigt att *loggar och spårdata* från intrångsdetekteringssystem sparas under så pass lång tid att de finns tillgängliga när en eventuell efterforskning sätts igång. Det kan i många fall ske månader efter det initiala problemet.

Exempel på risker och problem

Ett IDS-system missar attacker och attackförsök eftersom det inte är byggt att förstå de speciella kommunikationsprotokoll som nyttjas i digitala kontrollsystem.

Ett nätbaserat IPS-system agerar felaktigt på kommunikation och blockerar legitim trafik, vilket leder till driftstörningar.

09 Genomför riskanalyser av digitala kontrollsystem

NERC CIP (002-1) **NIST SP 800-82** (Kap. 3.2-3.6) **DOE 21** Steps (No. 14, 18) **OLF 104** (No. 2)

En av säkerhetsorganisationens viktigaste verksamheter är att regelbundet uppdatera och utvärdera de riskanalyser som har genomförs. Riskanalysen är det viktigaste underlaget för att fatta beslut om vilka åtgärder som bör genomföras för att undvika driftstörningar, produktionsbortfall eller i värsta fall person- och miljöskador.

Den grundläggande utgångspunkten som bör gälla vid all riskbedömning av IT-system är att fienden känner till systemet (Shannons maxim). När det gäller kontrollsystem antar många tyvärr ofta det motsatta – att ingen utomstående känner till detaljer om de leverantörsspecifika lösningarna. Detta kallas ibland för säkerhet genom förvanskning eller fördöljande (security by obscurity), något som sällan lyckas då angriparen har mycket stora valmöjligheter när det exempelvis gäller angreppssätt och angreppstidpunkt. Leverantörsspecifika kommunikationsprotokoll, krypteringslösningar eller operativsystem innebär därför inte på något sätt några säkerhetsgarantier. Snarare är resultatet ofta det omvända – att de inte skulle hålla måttet för en öppen granskning av forskare eller tekniska specialister.

En riskanalys kan utföras för ett avgränsat delsystem eller för en mer övergripande verksamhet. Organisationen ska uppdatera riskanalyserna i enlighet med de metoder som tidigare har fastställts och dokumenterats. Vilken riskanalysmetod som används i det specifika fallet beror på syftet med analysen, samt vilken information som finns tillgänglig om det aktuella systemet, inklusive hoten mot systemet. Att uppdatera riskanalysen kan kräva en uppdatering av systemkartläggningen, men målsättningen är att systemdiagram och dylikt ständigt ska vara aktuella. Utifrån den verksamhetsanalys som organisationen har genomfört tidigare bör man även ha definierat vilka system, och vilka informationsresurser, som är verksamhetskritiska.

Riskanalysen ska dokumenteras på ett förutbestämt sätt. En sådan dokumentation bör åtminstone omfatta upptäckta sårbarheter, bedömning av risker, samt beskrivning och prioritering av möjliga åtgärder bör ingå. För att genomföra en riskanalys kan följande information behövas: Incident- och störningsdata (loggar och material från omvärldsbevakningen), resultat från genomförda säkerhetsgranskningar (säkerhetstester och administrativa revisioner), samt checklistor.

Exempel på risker och problem

Eftersom en riskanalys inte uppdaterats på mer än ett år tar den inte hänsyn till de omfattande systemförändringar som nyligen har gjorts i ett av organisationens produktionssystem. Resultatet blir att ett numera verksamhetskritiskt kontrollsystem har för låga behörighetskrav. Exempelvis kan administrativ personal logga in i systemet och påverka känsliga delar av anläggningen samt att systemleverantörer kan få tillgång till och förändra mer än sitt eget system via servicekonton.

10 Genomför regelbunden teknisk säkerhetsgranskning av digitala kontrollsystem och anslutna nätverk

DOE 21 Steps (No. 9, 11)

Genom att utföra praktiska säkerhetsgranskningar och tekniska kontroller går det att skapa en mer realistisk bild av säkerheten i system och installerade funktioner.

Det finns vissa mycket viktiga skillnader mellan praktiska säkerhetstester av administrativa IT-system och den IT-utrustning som nyttjas inom digitala kontrollsystem. En stor del av den utrustning som nyttjas i kontrollsystem (exempelvis fältutrustning som PLC:er och RTU:er) har dåliga säkerhetskvaliteter. Utrustningen går ofta att störa eller angripa på grund av triviala programfel. En resulterande krasch, omstart eller ett felaktigt uppförande hos testenheten, som svar på ett enklare säkerhetstest, är tyvärr inte ovanligt. I vissa fall är den enda existerande installationen den som är produktionssatt, och det saknas en test- eller utvecklingsmiljö som man kan använda för praktiska säkerhetstester.

En noggrann planering bör föregå ett praktiskt säkerhetstest av digitala kontrollsystem, inklusive en genomgång av hur eventuella störningar till följd av testet ska hanteras. Verksamhetens ledning bör godkänna testplanen. Grundprincipen är att lita på enkla basmetoder och intervjuer i stället för automatiska verktyg för penetrationstester av traditionella IT-system. Få IT-konsulter har tillräckliga kunskaper om hur man testar digitala kontrollsystem. Många produktionsmiljöer är högst specialiserade , vilket kräver en förståelse för andra tekniker än de som finns i IP-baserade nätverk. Av denna anledning kan det även vara en god idé att meddela systemleverantörer före ett säkerhetstest.

När det gäller kartläggning av kontrollsystem för att identifiera värddatorer, noder och nätverk kan traditionella metoder som Ping sweep störa systemet. En inventering av kontrollsystemet är dock ett mycket viktig steg i testprocessen. 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. När det gäller att inventera tjänster och sårbarheter hos olika tjänster så bör aktiva scanningsmetoder (såsom portscanning och sårbarhetsscanning med verktyg som exempelvis Nmap och Nessus) undvikas i ett produktionssystem som är i skarp drift. Använd i stället passiva metoder och undersök exempelvis manuellt hur routers är konfigurerade. Gör aktiva tester i ett separat testsystem eller i ett kontrollsystem som inte är i drift.

Exempel på risker och problem

En test av en PLC utförs i en produktionssatt miljö. Själva testmetoden stör driftstatusen hos utrustningen, som därför missar viktiga styrkommandon eller låser sig.

11 Utvärdera löpande digitala kontrollsystems fysiska skydd

NERC CIP (006-1) **NIST 800-82** (Kap. 6.2.2) **DOE 21 Steps** (No. 10) **PL** (Kap. 9, 11)

Digitala kontrollsystem, speciellt de centrala anläggningarna, har historiskt sett haft ett omfattade fysisk skydd och i många branscher finns etablerade krav på hur viktiga anläggningar ska skyddas fysisk.

Digitala kontrollsystem är ofta geografiskt utspridda (decentraliserade), vilket gör det svårare att upprätthålla ett bra fysiskt skydd i de avlägsna anläggningarna. Attacker mot digitala kontrollsystem kan ske från utrustning i fält. I dag kan lokala enheter som PLC:er och RTU:er vara mycket sofistikerade. Exempelvis kan en modern RTU innehålla en webbserver och en Ethernet-port (eller Bluetooth) och den bör därför ha ett tillräckligt fysiskt skydd. Kablar 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 access till digitala kontrollsystem. Logisk och fysisk säkerhetsperimeter måste därför ovillkorligen följas åt.

Fysiskt skydd bör utföras i flera led – även här gäller principen om djupledsförsvar – och det bör bland annat inkludera

- skydd av känsliga lokaler (fysiskt skalskydd, tillträdesskydd, inbrottslarm, kameraövervakning och bevakning, brandskydd och så vidare)
- behörighetskontroll (se till att endast behöriga personer har tillgång till känslig information och viktiga driftslokaler)
- spårbarhet som gäller personer och tillgångar (se till att både personer och utrustning stannar i behörigt område – exempelvis bör inte bärbar utrustning såsom laptops för programmering av PLC:er lämnas obevakade)
- kontroll av miljöfaktorer (exempelvis ventilation och kraftförsörjning).

Observera att även säkerhetsklassad personal bör granskas kontinuerligt. De bör också genomgå en tillträdeskontroll om de önskar tillgång till kontrollanläggningar.

Exempel på risker och problem

En anställd tar med sin bärbara arbetsdator hem. Ett av barnen spelar spel via Internet och datorn blir infekterad av skadlig kod. Tillbaka på arbetet kopplar den anställde in datorn på det interna nätverket och den skadliga koden exekveras. Det resulterar i att en angripare nu opererar innanför den elektroniska säkerhetsperimetern (det logiska skalskyddet).

12 Se till att endast säkra och relevanta anslutningar till digitala kontrollsystem existerar

CPNI GPG (GPG 2, GPG Firewall Deployment) **DOE 21 Steps** (No. 1, 2, 3, 7) **OLF 104** (No. 10, 12) **PL** (Kap. 10, 11)

Traditionellt har kontrollsystem varit fysiskt isolerade och få, eller inga, kommunikationsanslutningar mot omvärlden har förekommit. Effektiviseringar och integrationsbehov har lett till fler kopplingar mellan administrativa informationssystem och digitala kontrollsystem. Alla typer av anslutningar ska vara identifierade och försedda med skyddsmekanismer som är anpassade till organisationens säkerhetskrav och till de verksamhetskrav som ställs på de olika kontrollsystemen.

Anslutningarna till kontrollsystem kan bestå av uppringda modem eller ISDN, fasta och trådlösa nätverksförbindelser eller Internetbaserade anslutningar. Exempel på nätverksanslutningar är

- serviceingångar för leverantörsrepresentanter
- anslutningsmöjligheter för jourpersonal som behöver snabb tillgång till processkontrollsystemet
- anslutningsmöjligheter för fjärrdrift av anläggningar
- anslutningsmöjligheter för fjärravläsning av givare i anläggningar
- anslutningsmöjligheter för åtkomst till tilläggsfunktionalitet eller kringsystem i anläggningen, såsom kameraövervakning, larmanläggningar, kort- och åtkomstskydd, brandlarm och så vidare.

Organisationen bör regelbundet praktiskt granska att enbart relevanta anslutningar till de digitala kontrollsystemen existerar, samt att dessa är så säkra som möjligt. En av de allra viktigaste säkerhetshöjande åtgärderna är att eliminera onödiga anslutningar.

Fjärråtkomst för leverantörer eller åtkomst för personal med jourtjänstgöring kräver särskild hänsyn. 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 och till vilka datorer dessa kan nyttjas.

Exempel på risker och problem

En okänd koppling existerar mellan ett styrsystem i processmiljön och ett administrativt datorsystem. En Internetmask infekterar en dator på ekonomiavdelningen som sedan sprider sig och orsakar omfattande driftstörningar i produktionen.

13 Härda och uppgradera digitala kontrollsystem i samverkan med systemleverantörer

CPNI GPG (GPG 5) **DOE 21 Steps** (No. 4, 6) **OLF 104** (No. 6, 10, 12, 13) **PL** (Kap. 2)

Härdning av datorlösningar, systemkomponenter och applikationer innebär att man tar bort oanvända, onödiga eller okända delar av programvara och konfiguration samt att man installerar säkerhetsuppgraderingar (patchar). Detta skapar en begränsad angreppsyta och en minskad riskexponering. Härdning är en standardåtgärd när det gäller att förbättra säkerheten i traditionella IT-system. Målet är att alltid använda den säkraste varianten av systemuppsättning och inställningar. Det är viktigt att härdningen genomförs enligt den process som etablerats för förändringshantering. Ett systems angreppsyta kan minskas genom att exempelvis

- ändra fabriksinställningar, exempelvis byta ut standardlösenord
- välja säkrare alternativ och inställningar i applikationer, nätverksfunktioner eller operativsystem
- stänga av oanvända funktioner i applikationer, nätverksfunktioner eller operativsystem
- blockera inloggningsmöjligheter för användare som inte längre ska ha tillgång till system, eller begränsa användares inloggningsmöjligheter och rättigheter
- åtgärda kända säkerhetsproblem genom uppgraderingar (patchning).

Härdning och manuell uppsäkring av systemutrustning, applikationer och operativsystem, som säkerhetsdokument för digitala kontrollsystem ibland nämner, går normalt inte att genomföra utan starkt stöd från leverantörssidan. Att förändra utrustning eller programvaruinställningar (inklusive patchning) utan att samverka med system- och applikationsleverantörer kan leda till driftstörningar, skapa instabiliteter i kontrollsystem samt ge avtalsmässiga konsekvenser.

Exempel på risker och problem

En systemleverantör har baserat funktioner i ett kontrollsystem på osäkra nättjänster och systemkomponenter. Flera av de osäkra funktioner som används i systemet går därför inte att deaktivera och systemet kan inte härdas i den omfattning som är önskvärt.

Om personer utan djupare kunskaper om ett kontrollsystem utför en systemhärdning kan systemet bli instabilt. De tar av misstag bort komponenter som sällan används av systemet, men som ändå fyller en funktion.

En falsk känsla av säkerhet kan infinna sig om en systemhärdning genomförs, men inte är så fullständig som de som utför den tror, utan sårbara delar av systemet fortfarande är aktiva.

14 Följ upp incidenter i digitala kontrollsystem och bevaka säkerhetsproblem i omvärlden

NERC CIP (008-1, 009-1) **NIST 800-82** (Kap. 6.2.3) **CPNI GPG** (GPG 3)
DOE 21 Steps (No. 19) **OLF 104** (No. 16)

En viktig förutsättning i allt förbättringsarbete är att organisationen rapporterar, dokumenterar och drar lärdom av inträffade incidenter och säkerhetserfarenheter – både sådana som inträffar i den egna organisationen och i omvärlden.

Erfarenhets- och incidentrapporteringen bör ligga till grund för att uppdatera riskbedömningar (riskanalyser). Den bör även kunna leda till åtgärder och till att fördelningen av resurser omprioriteras.

För att upptäcka incidenter krävs en kontinuerlig uppföljning och övervakning av verksamhetens säkerhetsrutiner och dess tillstånd. Genom att övervaka och följa upp dessa kan verksamheten bättre hantera hot och upptäcka nya säkerhetsbrister – såväl från den egna som från andra organisationer. Även incidenter och händelser i omvärlden som kan påverka verksamheten bör uppmärksammas. Fysiska incidenter kan vara relaterade till IT-incidenter. Exempelvis kan ett inbrott som har resulterat i en stulen laptop vara en del i den informationsinsamling som föregår ett logiskt angrepp.

Genom att hålla verksamheten uppdaterad kring vilka incidenter och säkerhetsproblem som människor upptäcker i omvärlden, är det enklare att ständigt upprätthålla en god beredskap mot nya hot och sårbarheter i digitala kontrollsystem.

Ett kunskaps- och analysmässigt problem är att det förekommer en ytterst begränsad mängd öppen information om inträffade störningar i digitala kontrollsystem. I dagsläget finns det få forum och kommunikationskanaler där information är lättillgänglig för system- och anläggningsägare.

Som ett led i omvärldsbevakningen bör organisationen etablera en grupp som samlas för att diskutera incidenter och riskproblem, och analysera hur dessa kan påverka säkerheten i organisationens kontrollsystem. Gruppen bör träffas regelbundet och ska bestå av representanter från både processkontroll- och IT-sidan.

Exempel på risker och problem

Om incidenter inte rapporteras är det svårt att upptäcka brister i befintliga säkerhetsrutiner, exempelvis felkonfigurerade brandväggar eller trasiga enheter.

Om mindre incidenter inte uppmärksammas kan de utvecklas till skador och leda till kritiska driftstörningar hos verksamheten.

15 Samverka i användarföreningar, standardorgan och andra nätverk för att öka säkerheten i digitala kontrollsystem

För närvarande pågår många internationella initiativ för att ta fram standarder och rekommendationer för att skapa säkerhet i digitala kontrollsystem. Många statliga aktörer i Europa, Nordamerika och Asien prioriterar området högt. Genom att delta aktivt i detta säkerhetsarbete kan användare och leverantörer av digitala kontrollsystem vara med och påverka vilka säkerhetskrav som kommer att ställas på de här systemen i framtiden.

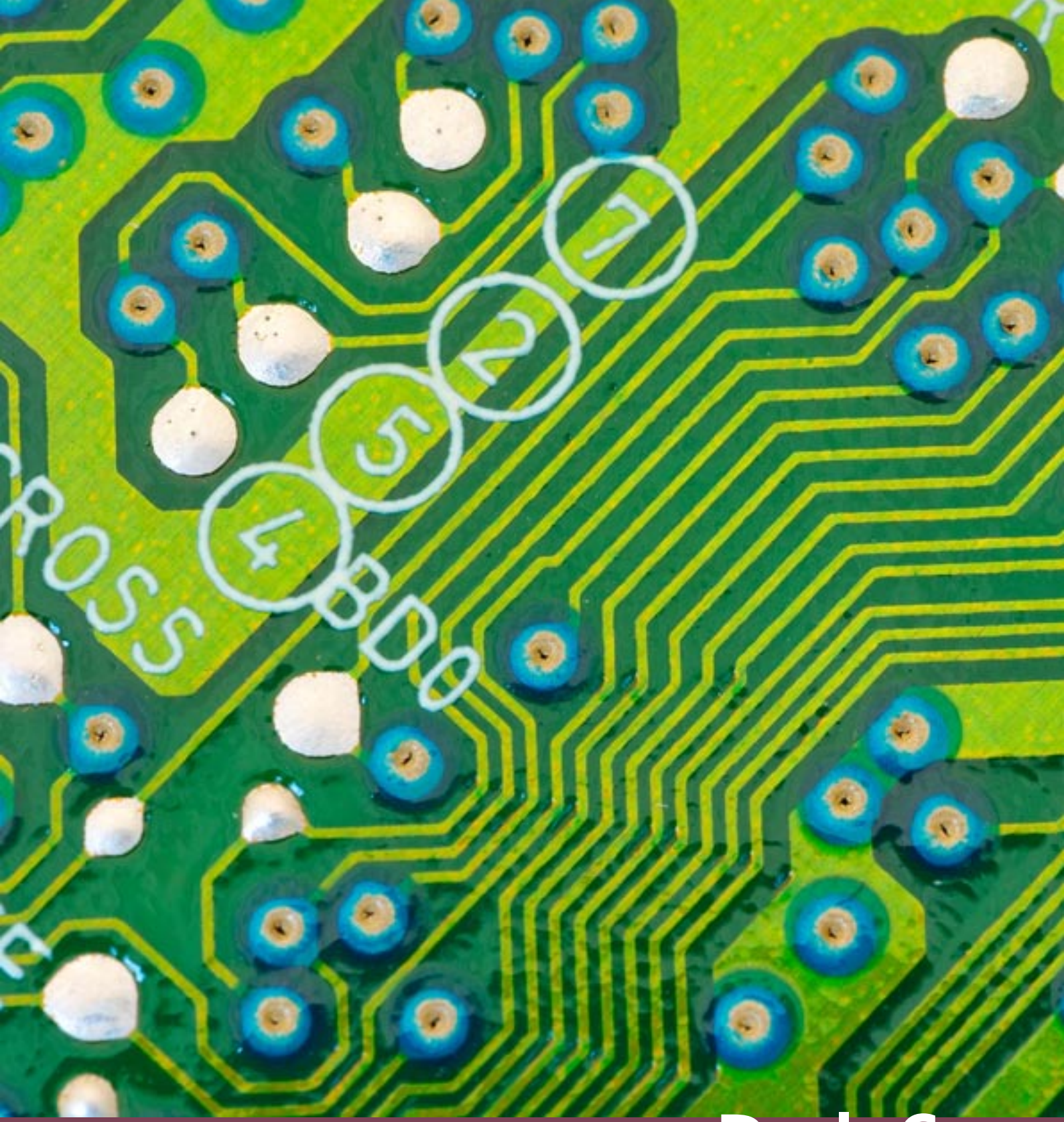
Genom att som användare av digitala kontrollsystem verka genom olika nationella och internationella organisationer och intressegrupper går det att ställa högre, tydligare och mer samlade säkerhetskrav på leverantörer, systemintegratörer och applikationsutvecklare.

Genom att som leverantör av digitala kontrollsystem, applikationer eller annan utrustning, delta i säkerhetsarbetet går det att skapa en konkurrensfördel. Redan i dag finns dock etablerade säkerhetskrav i vissa branscher, exempelvis förväntas elbolag i USA följa standarden NERC CIP. På sikt är det med största sannolikhet en förutsättning för att få leverera både maskin- och programgramvara.

Att samverka genom användarföreningar, standardorgan och andra nätverk är ett ekonomiskt realistiskt alternativ för många små och medelstora användare och leverantörer. I Sverige finns exempelvis Elbranschens informations- och IT-säkerhetsforum (EBITS), ett nätverk för Svensk Energis, Svensk Fjärrvärmes, Svenskt Vattens och Svenska Kraftnäts samordning av frågor knutna till informations- och IT-säkerhet.

Exempel på risker och problem

Genom ett svagt deltagande i standardiserings- och säkerhetsarbetet från antingen leverantörer eller användare, utvecklas obalanserade säkerhetskrav eller tekniskt inkompetenta krav.



Del C

Referenslista med kommentarer

NERC CIP-002-1 till CIP-009-1

Typ av dokument: Standard
Utgivare: North American Reliability Council (NERC), U.S.
Version: Slutversion (giltig från 2006-06-01)
Omfattning: 53 sidor (totalt)

`http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html`

Standarderna i NERC CIP (CIP 002-1 till 009-1) är allmänt formulerade och går att använda inom andra verksamhetsområden än elkraftsområdet.

NERC CIP 002-1 kräver att den ansvariga organisationen identifierar de kritiska tillgångarna genom att tillämpa ett riskbaserat synsätt. Baserat på denna analys identifierar de sedan de kritiska datorbaserade tillgångarna (Critical cyber assets).

NERC CIP 003-1 kräver att den ansvariga organisationen etablerar någon form av administrativt säkerhetsprogram (Minimun security management controls) för att skydda kritiska datorbaserade tillgångar.

NERC CIP 004-1 kräver att den ansvariga organisationen ska se till att personal (inklusive extern personal av olika slag) som de ger logisk access, eller obevakat fysiskt tillträde, till kritiska datorbaserade tillgångar har nödvändig träning och ett säkerhetsmedvetande.

NERC CIP 005-1 kräver att den ansvariga organisationen ska identifiera och skydda så kallade elektroniska säkerhetsperimetrar inom vilka de kritiska datorbaserade tillgångarna finns, samt identifiera och skydda alla accesspunkter i dessa perimetrar.

NERC CIP 006-1 kräver att den ansvariga organisationen implementerar ett program för att fysiskt skydda kritiska datorbaserade tillgångar.

NERC CIP 007-1 kräver att den ansvariga organisationen definierar metoder, processer och procedurer för att säkra de system de har fastställt vara kritiska datorbaserade tillgångar. Detta gäller även de icke-kritiska, datorbaserade tillgångar som befinner sig innanför någon av de så kallade elektroniska säkerhetsperimetrarna.

NERC CIP 008-1 kräver att den ansvariga organisationen ser till att de identifierar, klassificerar, besvarar samt rapporterar säkerhetsincidenter relaterade till kritiska datorbaserade tillgångar.

NERC CIP 009-1 kräver att den ansvariga organisationen etablerar återhämtningsplaner (Recovery plans) för kritiska datorbaserade tillgångar och att dessa planer följer etablerade praxis och tekniker för beredskaps- och kontinuitetsplanering.

NIST SP 800-82 – Guide to Industrial Control Systems (ICS) Security

Typ av dokument: Rekommendation
Utgivare: National Institute for Standards and Technology (NIST), U.S.
Version: Second Public Draft (september 2007)
Omfattning: 157 sidor (inklusive bilagor)

`http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf`

NIST SP 800-82 är allmänt formulerad och går att tillämpa inom alla områden där de använder digitala kontrollsystem. Dokumentet består av sex huvudsakliga avsnitt:

Sektion 1: Avsnittet redogör för rekommendationens syfte, omfattning och målgrupp.

Sektion 2: Avsnittet ger en generell beskrivning av digitala kontrollsystem och förklarar betydelsen av dessa system.

Sektion 3: Avsnittet innehåller en diskussion kring skillnaderna mellan digitala kontrollsystem och traditionella IT-system, samt ger en beskrivning av hot, sårbarheter och inträffade incidenter.

Sektion 4: Avsnittet ger en översiktsbeskrivning av säkerhetsprogram för att minska riskerna med de sårbarheter som ni har identifierat i sektion 3.

Sektion 5: Avsnittet ger rekommendationer för hur säkerhet kan integreras i traditionella nätverksarkitekturer hos digitala kontrollsystem. Det betonar speciellt praxis för segmentering av nätverk.

Sektion 6: Avsnittet tillhandahåller rekommendationer kring hur de olika formerna av kontroll (lednings-, operationell och teknisk kontroll), som har identifierat i NIST SP 800-53 (*Recommended security controls for federal information systems*) kan tillämpas för digitala kontrollsystem.

Dokumentet innehåller även sex appendix (A till F) som ger referenser, listar förkortningar, tillhandahåller en ordlista, beskriver olika amerikanska aktiviteter som syftar till att öka säkerheten i digitala kontrollsystem och så vidare.

CPNI Good Practice Guide Process Control and SCADA Security

Typ av dokument: Rekommendationer
Utgivare: Centre for the Protection of National Infrastructure (CPNI), U.K.
Version: Slutversioner (olika datum)
Omfattning: 14–42 sidor (beroende på dokument)

`http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx`

Dokumenten är allmänt formulerade och går att använda inom alla områden där digitala kontrollsystem används. Serien består för närvarande av en sammanfattande guide och åtta specifika dokument:

- Good Practice Guide Process Control and SCADA Security
- Good Practice Guide Process Control and SCADA Security. Guide 1. Understand the business risk
- Good Practice Guide Process Control and SCADA Security. Guide 2. Implement secure architecture
- Good Practice Guide Process Control and SCADA Security. Guide 3. Establish response capabilities
- Good Practice Guide Process Control and SCADA Security. Guide 4. Improve awareness and skills
- Good Practice Guide Process Control and SCADA Security. Guide 5. Manage third party risk
- Good Practice Guide Process Control and SCADA Security. Guide 6. Engage projects
- Good Practice Guide Process Control and SCADA Security. Guide 7. Establish ongoing governance
- Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks

21 Steps to Improve Cyber Security of SCADA Networks

Typ av dokument: Rekommendation
Utgivare: Department of Energy (DOE), U.S.
Version: Slutversion (september 2002)
Omfattning: 10 sidor

`http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf`

Det här dokumentet diskuterar mycket kortfattat följande rekommendationer:

1. ”Identify all connections to SCADA networks.
2. Disconnect unnecessary connections to the SCADA network.
3. Evaluate and strengthen the security of any remaining connections to the SCADA network.
4. Harden SCADA networks by removing or disabling unnecessary services.
5. Do not rely on proprietary protocols to protect your system.
6. Implement the security features provided by device and system vendors.
7. Establish strong controls over any medium that is used as a backdoor into the SCADA network.
8. Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring.
9. Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns.
10. Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security.
11. Establish SCADA “Red Teams” to identify and evaluate possible attack scenarios.
12. Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.
13. Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.
14. Establish a rigorous, ongoing risk management process.
15. Establish a network protection strategy based on the principle of defense-in-depth.
16. Clearly identify cyber security requirements.
17. Establish effective configuration management processes.
18. Conduct routine self-assessments.
19. Establish system backups and disaster recovery plans.
20. Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance.
21. Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.”

Krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer

Typ av dokument: Rekommendation (Retningslinje Nr. 104)
Utgivare: OLF
Version: Revisjon Nr: 01 Dato skrevet: 1.4.2007
Omfattning: 6 sidor (Norsk version), 32 sidor (engelska version)

`http://www.olf.no/hms/retningslinjer/?50I82.pdf`

Det engelska dokumentet diskuterar följande rekommendationer:

1. "An Information Security Policy for process control, safety, and support ICT systems environments shall be documented.
2. Risk assessments shall be performed for process control, safety, and support ICT systems and networks.
3. Process control, safety, and support ICT systems shall have designated system and data owners.
4. The infrastructure shall be able to provide segregated networks, and all communication paths shall be controlled.
5. Users of process control, safety, and support ICT systems shall be educated in the information security requirements and acceptable use of the ICT systems.
6. Process control, safety, and support ICT systems shall be used for designated purposes only.
7. Disaster recovery plans shall be documented and tested for critical process control, safety, and support ICT systems.
8. Information security requirements for ICT components shall be integrated in the engineering, procurement, and commissioning processes.
9. Critical process control, safety, and support ICT systems shall have defined and documented service and support levels.
10. Change management and work permit procedures shall be followed for all connections to and changes in the process control, safety, and support ICT systems and networks.
11. An updated network topology diagram including all system components and interfaces to other systems shall be available.
12. ICT systems shall be kept updated when connected to process control, safety, and support networks.
13. Process control, safety, and support ICT systems shall have adequate, updated, and active protection against malicious software.
14. All access requests shall be denied unless explicitly granted.
15. Required operational and maintenance procedures shall be documented and kept current.
16. Procedures for reporting of security events and incidents shall be documented and implemented in the organisation."

Cyber Security Procurement Language for Control Systems

Typ av dokument: Rekommendation
Utgivare: Idaho National Laboratory och U.S. Department of Homeland Security
Version: Augusti 2008
Omfattning: 111 sidor (totalt)

`http://www.us-cert.gov/control_systems/pdf/SCADA_Procurement_DHS_Final_to_Issue_08-I9-08.pdf`

Det här dokumentet är tänkt att användas för att ställa säkerhetskrav i upphandlingen av digitala kontrollsystem. För varje huvudområde ges exempel på kravspecifikationer inklusive teståtgärder. Dokumentet utvidgas kontinuerligt och för närvarande ingår följande avsnitt:

Härdning av system: Avsnittet behandlar exempelvis krav på borttagande av onödiga program, konfigurering av maskinvara samt uppdatering av OS.

Perimeterskydd: Avsnittet behandlar exempelvis krav på brandväggar och nätverks-IDS:er.

Konton och lösenord: Avsnittet behandlar exempelvis krav på gästkonton, lösenord och autentisering, loggning samt rollbaserad accesskontroll.

Programmeringspraxis: Avsnittet behandlar krav på dokumentering av leverantörsutvecklad kod.

Felhantering: Avsnittet behandlar exempelvis krav på meddelanden och dokumentation från leverantören samt problemrapportering.

Skadlig kod: Avsnittet behandlar exempelvis krav på detektering och skydd mot skadlig kod.

Nätverksadressering: Avsnittet behandlar krav på adresseringen i nätverk och konfigurering av DNS-servers.

Lokala enheter: Avsnittet behandlar krav på säkerhet i IED, PLC, RTU och så vidare.

Fjärråtkomst: Avsnittet behandlar krav på olika anslutningar till kontrollsystem.

Fysisk säkerhet: Avsnittet behandlar fysiska säkerhetskrav, exempelvis då det gäller tillgänglighet till digitala komponenter.

Nätverkspartitionering: Avsnittet behandlar krav på nätverksenheter och arktitektur.

Informationsresurser (urval)

Det pågår ett omfattande internationellt arbete kring säkerhet i digitala kontrollsystem. Ett bra sätt att hålla sig uppdaterad är att regelbundet följa vad som skrivs på några av de etablerade webbsidorna. Följande sidor är en bra start:

Centre for the Protection of National Infrastructure (CPNI), U.K.
`http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx`

Department of Homeland Security, US-CERT, Control Systems Security Program, U.S.
`http://www.us-cert.gov/control_systems/`

Process Control Systems Forum (PCSF), U.S.
`https://www.pcsforum.org/`

SCADA Blog (Digital Bond), U.S.
`http://www.digitalbond.com/`

Digitala kontrollsystem utgör en kritisk del av de system som försörjer samhället med elektricitet, värme, dricksvatten, bränslen samt transporter av personer och varor. Till skillnad från administrativa IT-system, där informationsbehandlingen i sig ofta är slutmålet, kan störningar i digitala kontrollsystem innebära direkta störningar i den underliggande fysiska processen. Det kan i slutändan leda till leveransavbrott av samhällsviktiga nyttigheter.

Dagens kontrollsystem görs i allt högre utsträckning tillgängliga via publika nätverk som Internet. De bygger allt mer på samma teknik som vanliga IT-system och integreras med administrativa IT-system. Sammanfattningsvis medför den här utvecklingen en radikalt förändrad riskbild.

Det här dokumentet ger grundläggande rekommendationer kring säkerhet i digitala kontrollsystem. Dokumentet tipsar också om var det går att finna ytterligare information och sammanfattar internationellt erkända rekommendationer.

ISBN 978-91-85797-21-9

Krisberedskapsmyndigheten

Box 599
101 31 Stockholm

Tel 08-593 710 00
Fax 08-593 710 01

kbm@kbm-sema.se

www.krisberedskaps
myndigheten.se