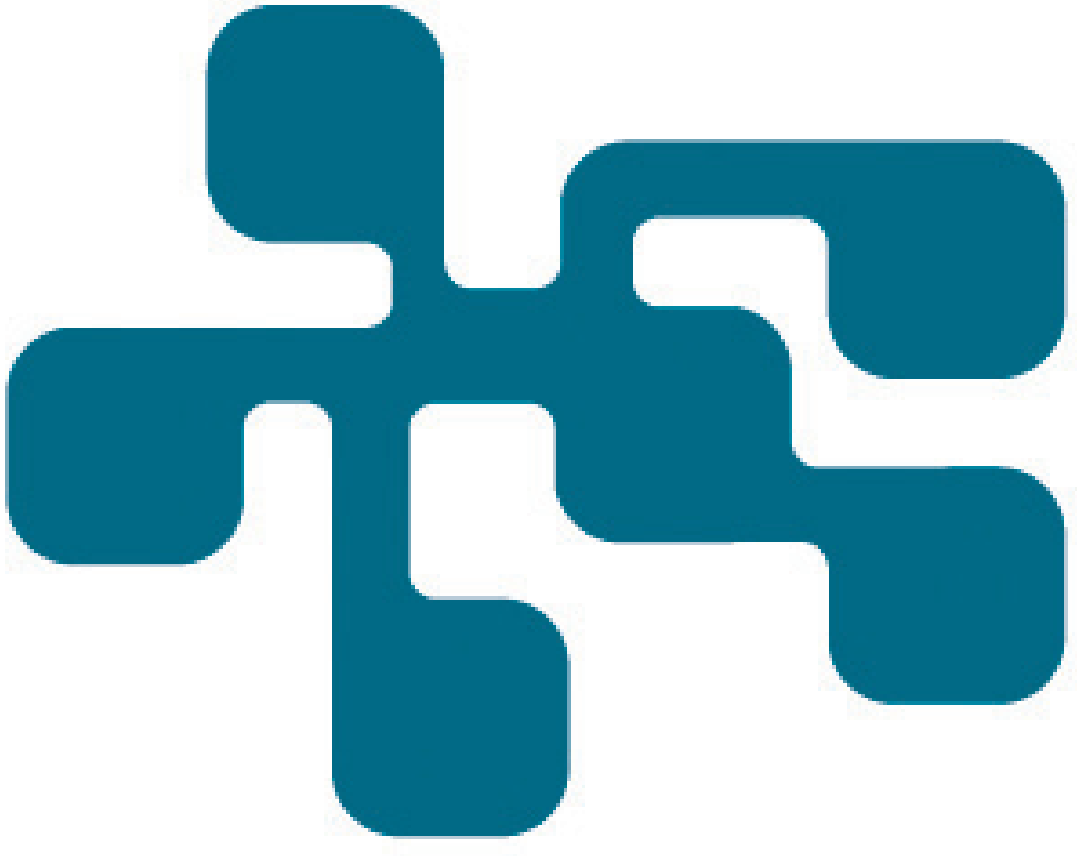
NCS3 - Regelverk och krav inom området industriella informations- och styrsystem

En uppdatering av utvecklingen sedan december 2012

KARIN MOSSBERG SONNEK, FREDRIK LINDGREN

FOI
MSB



FOI-R--4197--SE
MSB 2015-2525
ISSN 1650-1942

December 2015

Karin Mossberg Sonnek, Fredrik Lindgren

NCS3 – Regelverk och krav inom området industriella informations- och styrsystem

En uppdatering av utvecklingen sedan december 2012

Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet

FOI-R--4197--SE

MSB 2015-2525

Titel	NCS3 – Regelverk och krav inom området industriella informations- och styrsystem
Title	NCS3 – Swedish Regulations within the area of Industrial Control Systems
Rapportnr/Report no	FOI-R--4197--SE
Månad/Month	December
Utgivningsår/Year	2015
Antal sidor/Pages	57 p
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	
Projektnr/Project no	E13510
Godkänd av/Approved by	Maria Lignell Jakobsson
Ansvarig avdelning	Försvarsanalys

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

FOI genomförde en studie under 2012, på uppdrag av MSB (Myndigheten för samhällsskydd och beredskap), i syfte att undersöka hur regelverk och krav styr säkerhetsarbetet med industriella informations- och styrsystem. Studien hade fokus på sex sektorer; el, dricksvatten, fjärrvärme och fjärrkyla, kemisk process-industri, spårbunden trafik samt elektroniska kommunikationer. Tre år senare initierade MSB en ny studie för att följa upp vad som hänt inom sektorerna sedan den förra studien. I rapporten presenteras det sammantagna resultatet av båda studierna.

Ett flertal myndigheter har sedan 2012 kommit ut med nya föreskrifter som berör sektorerna. Fler förändringar förväntas till följd av den pågående översynen av säkerhetsskyddslagen och den översyn av föreskrifter som MSB och Strålsäkerhetsmyndigheten genomför. Lagar, förordningar och föreskrifter kan på en övergripande nivå användas för att motivera olika åtgärder inom området, studierna som har genomförts visar dock att de sällan explicit berör säkerheten i informations- och styrsystem.

Generellt visar studierna att uppmärksamheten kring säkerheten i informations- och styrsystem har ökat sedan 2012 men att skillnaden i hur frågorna uppmärksammas inom olika sektorer är stor. Längst har elsektorn och dricksvattensektorn kommit och där är det främst myndigheten Svenska kraftnät och branschorganisationen Svensk Energi samt branschorganisationen Svenskt Vatten som har drivit frågorna.

Nyckelord: Regelverk, krav, informations- och styrsystem, kontrollsystem, SCADA-system, elproduktion, eldistribution, dricksvattenproduktion, vattendistribution, fjärrvärme, fjärrkyla, kemisk processindustri, spårbunden trafik, elektroniska kommunikationer.

Summary

During 2012, FOI carried out a study on behalf of MSB (the Swedish Civil Contingencies Agency) with the aim to investigate how different regulations influence the security work with regard to industrial control systems. The study had focus on six sectors; electricity, drinking water, long distance heating and cooling, chemical processing industry railbound traffic and electronic communications. In 2015, MSB initiated a new study to follow up changes since the last study. The result from both studies are presented in this report.

Several authorities has established new regulations since 2012 that influence the security work in the sectors. More changes are supposed to be implemented as a result of the revision of the security protection law and the revision of MSB's and the Swedish Radiation Safety Authority's regulations. Laws and regulations can all be used to support the security work on a general level. However, the studies have shown that these seldom explicitly mention security in industrial control system.

Taken together, the two studies show that the awareness of security issues in industrial control systems has increased since 2012, but that the variation between sectors is large. The electricity sector and drinking water sector have made most progress. The primary actors in these sectors are the authority Svenska kraftnät and the trade organisation Svensk Energi together with the trade organisation Swedish Water & Wastewater Association.

Keywords: Regulations, industrial control system, SCADA, electricity production, electricity distribution, production of drinking water, water distribution, long distance heating, remote cooling, chemical processing industry, railbound traffic, electronic communications.

Innehåll

1 Inledning

1.1 Bakgrund

Under hösten 2012 gjorde Totalförsvarets forskningsinstitut (FOI), på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB), en genomgång av vilka regelverk och krav som påverkar arbetet med säkerhet i industriella informations- och styrsystem. Genomgången, som omfattade sex olika sektorer, redovisas i Lindgren (2013).[1]

Vid denna tidpunkt gick det att identifiera relativt stora skillnader mellan olika sektorer i hur säkerhet i industriella informations- och styrsystem uppmärksammades i förordningar, föreskrifter och andra regelverk. Inom el- och dricksvattenområdet var frågorna tydligt uppmärksammade och dessutom explicita i de regler och riktlinjer som var styrande för verksamheten, om än med varierande detaljeringsgrad. Inom spårbunden trafik och elektroniska kommunikationer var frågorna också uppmärksammade, men det saknades direkta hänvisningar till krav på säkerhet i informations- och styrsystem i de regelverk som analyserades. Inom fjärrvärme och kemisk processindustri identifierades inga regleringar som tog upp säkerhet i informations- och styrsystem. Resultatet av studien sammanfattas i tabell 1.

Tabell 1. Läget med avseende på uppmärksamhet av säkerheten i industriella informations- och styrsystem och hantering av detta i lagar och regelverk den 1 dec 2012.[2]

Område	Hanteras frågan i regelverk/krav?	Är frågan uppmärksammad?
Elproduktion/-distribution	Ja, explicit	Ja, tydligt
Dricksvatten	Ja, explicit	Ja, tydligt
Fjärrvärme/-kyla	Nej	?
Processindustri (Seveso)	Nej	Delvis
Spårtrafik	Indirekt (?)	Ja
Elektroniska kommunikationer	Indirekt (?)	Ja

[1] Lindgren, F. (2013). Regelverk och krav inom området säkerhet i industriella informations- och styrsystem. FOI Memo 4415.
[2] Ibid.

1.2 Syfte

Under 2015 beslöt MSB att göra en uppföljande studie som syftade till att identifiera förändringar i regelverk och krav som har genomförts efter den 1 december 2012 med bäring på säkerhet i industriella informations- och styrsystem. Studien, vars resultat redovisas i den här rapporten, har omfattat de tidigare kartlagda sektorerna:

- Elproduktion och eldistribution
- Dricksvattenproduktion och vattendistribution
- Fjärrvärme/-kyla – produktion och distribution
- Kemisk processindustri
- Spårbunden trafik
- Elektroniska kommunikationer

Syftet med studien har även varit att se om frågor kring säkerhet har uppmärksammats inom sektorerna utöver det som ingår i regelverk och krav.

1.3 Rapportens disposition

Rapporten har ambitionen att sammanfatta både det nuvarande läget och vad som har hänt inom området de senaste tre åren. Vi har därför valt att återge de delar av texten från den tidigare studien som fortfarande är aktuella och i anslutning till dem kommenterat vad som har förändrats inom området sedan den 1 december 2012. Sådana förändringar handlar oftast om att en tidigare författning har ersatts av en ny eller att det har kommit ut en ny vägledning eller rapport inom området. Avsnitten från den tidigare studien är i de följande kapitlen markerade med en ram. Texten i dessa är direkt citerade[3] från Lindgren (2013).

Rapporten inleds med en kort sammanfattning av studiens resultat. Därefter finns en genomgång av vilka regelverk och krav som är sektorsövergripande och hur frågorna generellt har uppmärksammats. Sedan redovisas hur det ser ut inom varje enskild sektor och inom angränsande områden. Rapporten avslutas med en diskussion. I slutet av rapporten finns det också en ordlista över de juridiska termer som nämns i texten. Referenser står dels i fotnoter i den löpande texten och är dels samlade kapitelvis längst bak i rapporten.

Målgruppen för rapporten är främst verksamma inom de olika sektorerna som arbetar med informationssäkerhet, IT-säkerhet eller styrsystem.

[3] I några fall har vi rättat stavfel eller författningsnummer som har varit fel.

1.4 Metod och avgränsningar

I studien har främst svenska lagar, förordningar och föreskrifter studerats.[4] Bland de rättsakter som EU beslutar om finns *förordningar* (som gäller direkt i svensk lag) och *direktiv* (som innehåller mål som EU-länderna ska följa och där varje land själv avgör vilka lagar som krävs för att uppnå målen).[5] Vissa EU-direktiv påverkar verksamheten inom olika sektorer i hög grad, men dessa har bara tagits med i den mån regeringen har genomfört lagändringar eller tillsatt utredningar till följd av ett sådant.

Utöver en genomgång av regler och krav så har vi också sökt efter rapporter, vägledningar och branschgemensamma handböcker som har getts ut efter den 1 december 2012. Vi har framför allt sökt information på myndigheters och branschorganisationers hemsidor. Vi har inte genomfört några intervjuer, däremot har vi presenterat det preliminära resultatet för MSB och på ett FIDI-SCADA-möte den 26 nov 2015, där ett 15-tal representanter från olika sektorer deltog, och fått värdefulla synpunkter på innehållet. I några fall har vi refererat till vad olika personer har sagt i de sammanhangen.

Genomgången har inte som ambition att vara komplett, men skall ses som en god approximation till hur det ser ut inom de behandlade sektorerna. Speciellt när det rör de avsnitt som beskriver hur säkerhetsfrågorna har uppmärksammats inom olika sektorer finns det skäl att tro att vi har missat sådant som har gjorts inom samverkansgrupper och av enskilda företag eftersom vi inte aktivt letat efter sådana initiativ.

[4] Den främsta källan för dessa är www.notisum.se.
[5] www.eu-upplysningen.se/Om-EU/Om-EUs-lagar-och-beslutsfattande/Olika-typer-av-EU-lagar, 2015-12-01.

2 Sammanfattning av studiens resultat

Generellt har uppmärksamheten kring säkerhet i informations- och styrsystem ökat sedan 2012. Ett exempel på det är den statliga utredningen om informations- och cybersäkerhet i Sverige (SOU 2015:23). Än har dock inga åtgärder som föreslås av utredningen hunnit genomföras. MSB har också bidragit till ökad uppmärksamhet, bland annat genom en ny version av ”Vägledning till ökad säkerhet i industriella informations- och styrsystem” som har fått stor spridning. MSB finansierar också forskningsprojekt inom området. Riksrevisionen har uppmärksammat säkerheten i industriella informations- och styrsystem genom en granskning av hur ändamålsenlig informationssäkerheten är i myndigheter som inom den civila statsförvaltningen utifrån ökade hot och risker och konstaterat att det finns brister, bland annat i förmågan att motstå cyberattacker.

Att enbart uppmärksamma frågorna räcker emellertid inte för att åtgärda bristerna. För att göra det krävs att olika aktörer vidtar åtgärder för att öka säkerheten, vilket ofta är kostsamt och kräver kunskap och resurser. Även om såväl lagar, förordningar och föreskrifter ger stöd för att se över, och vid behov förbättra, skyddet av industriella informations- och styrsystem så är de sällan explicita i vad som behöver göras. Branschorganisationer och företag skulle få ett större stöd i sitt arbete om myndigheternas föreskrifter blev mer specifika. Det har genomförts en del förändringar på regelverkssidan sedan 2012, men de delar som berör informations- och styrsystem är få. Exempel på myndigheter som har gett ut nya föreskrifter är Svenska kraftnät, Livsmedelsverket, MSB, Arbetsmiljöverket, Transportstyrelsen och Post- och telestyrelsen. Det pågår också en översyn av säkerhetsskyddslagen och MSB ser över sina föreskrifter och allmänna råd inom informationssäkerhetsområdet

Skillnaden mellan olika sektorer är fortfarande stor. Elsektorn och dricksvattensektorn har uppmärksammat säkerheten i informations- och styrsystem betydligt mer än övriga sektorer. Så var fallet redan 2012 – och så är det även 2015. Inom elsektorn har myndigheten Svenska kraftnät gjort en stor insats tillsammans med branschorganisationen Svensk Energi. Inom vattensektorn är det främst branschorganisationen Svenskt Vatten som har drivit frågorna. Inom övriga sektorer finns det inte alltid branschorganisationer som har kunnat uppmärksamma problemen. Tabell 2 sammanfattar hur det ser ut i de olika sektorerna.

Ett annat sätt att sammanfatta läget inom området är med de ord som yttrades under FIDI-SCADA-mötet i november 2015 som både andas optimism och pessimism:

> ”Det går framåt – men väldigt långsamt. Utvecklingen i omvärlden går dessvärre fram snabbare, så i realiteten backar vi.”

Tabell 2. Författarnas bedömning av vilka förändringar som skett inom olika sektorer mellan den 1 december 2012 och den 1 december 2015, med avseende på säkerheten i industriella informations- och styrsystem (jämför tabell 1).

Område	Hantering av frågorna i lagar och regelverk[6]	Uppmärksamhet kring frågorna
Elproduktion och eldistribution	Frågorna hanteras explicit. Nya förskrifter: SvK 2013:1 och 2013:2. Strålsäkerhetsmyndigheten ser över sina föreskrifter.	Ökad uppmärksamhet, främst genom att Svenska kraftnät arbetar aktivt med informationssäkerhet, sprider information och stödjer forskning. Även samordningsrådet för smarta elnät har lyft frågan.
Dricksvatten-produktion och vattendistribution	Frågorna hanteras explicit. Nya föreskrifter: LIVSFS 2013:4 och LIVSFS 2013:5.	Ökad uppmärksamhet via branschorganisationen Svenskt Vatten som sprider information och som tagit fram en checklista för SCADA-säkerhet
Fjärrvärme/-kyla, produktion och distribution	Som tidigare (nej)	Som tidigare (oklart)
Kemisk processindustri	Nya föreskrifter: MSBFS 2015:8 och AFS 2014:44	Som tidigare (delvis)
Spårbunden trafik	Nya föreskrifter: TSFS 2013:44 och TSFS 2015:34.	Frågorna har uppmärk-sammats internt inom Trafikverket.
Elektroniska kommunikationer	Ny föreskrift: PTSFS 2015:2	Som tidigare (ja)

[6] Vi har valt att inte lista lagar och förordningar här eftersom det är först när de omsätts i föreskrifter som de specifikt behandlar informations- och styrsystem.

3 Sektorsövergripande

3.1 Säkerhetsskydd

Begreppet säkerhetsskydd omfattar skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet, skydd av uppgifter som rör rikets säkerhet samt skydd mot terroristbrott. De skyddsåtgärder som vidtas ska förebygga att sådana uppgifter obehörigen röjs, ändras eller förstörs (informationssäkerhet), att obehöriga får tillträde till platser där de kan få tillgång till sådana uppgifter eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdes-begränsning) samt att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning).[7] Närmare bestämmelser framgår av säkerhetsskyddsförordningen.[8] (Lindgren, 2013)

Säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordning (1996:633) som Lindgren (2013) refererar till ovan gäller fortfarande. Säkerhetsskyddslagen gäller för ”staten, kommunerna och landstingen; aktiebolag, handelsbolag, föreningar och stiftelser över vilka staten, kommuner eller landsting utövar ett rättsligt bestämmande inflytande; och för enskilda, om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism”. Detta innebär i princip att all samhällsviktig verksamhet berörs av säkerhetsskyddet.

I december 2011 fick en särskild utredare i uppgift att göra en översyn av säkerhetsskyddslagstiftningen i syfte att öka skyddet av verksamhet som har betydelse för rikets säkerhet.[9] Resultatet av utredningen redovisades i mars 2015 i SOU 2015:25[10]. Utredningen föreslår att säkerhetsskyddslagen (1996:627) ersätts av en ny lag som möter de förändrade kraven på säkerhetsskyddet, bl.a. avseende:

- utvecklingen på informationsteknikområdet,
- en ökad internationell samverkan,
- en ökad sårbarhet i samhällsviktiga funktioner,
- det faktum att säkerhetskänslig verksamhet i allt större omfattning bedrivs i enskild regi.

Till dags dato (2015-12-01) har dock ingen ny lag antagits.

I utredningen tas informations- och styrsystem upp generellt som något som är vanligt förekommande inom samhällsviktiga verksamheter. Dessa exemplifieras

[7] Säkerhetsskyddslag (1996:627).
[8] Säkerhetsskyddsförordning (1996:633).
[9] En modern säkerhetsskyddslag (Dir. 2011:94).
[10] En ny säkerhetsskyddslag (SOU 2015:25).

med energiförsörjningen, elektronisk kommunikation, vattenförsörjning, hälso- och sjukvård samt betalningsväsendet.[11] Mer specifikt nämns de under avsnittet om vattenförsörjning och avloppshantering där det noteras att produktionen och distributionen av dricksvatten i hög grad är beroende av att funktionaliteten kan vidmakthållas hos industriella informations- och styrsystem.[12] Även under avsnittet om transporter och kommunikation nämns att styrsystem är viktiga för att upprätthålla transporter. Som exempel lyfts system för styrning av kritiska järnvägsväxlar och dirigering av trafik i luftrummet.[13]

På ett ställe står det att ”[u]nder ett flertal år har brister i säkerheten i s.k. SCADA-system uppmärksammats vilket har lett till förbättringsåtgärder inom flera sektorer”. Detta utvecklas dock inte.[14]

3.2 Informationssäkerhet

Informationssäkerhet är inte begränsat till den relativt snäva betydelse som begreppet har inom säkerhetsskyddslagstiftningen enligt ovan utan handlar om olika aktörers arbete för att skydda information utifrån ställda krav på konfidentialitet, riktighet och tillgänglighet. Flera myndigheter har ett av regeringen särskilt utpekat ansvar för frågor om samhällets informationssäkerhet. Samverkan mellan dessa sker i Samverkansgruppen för informationssäkerhet (SAMFI). Utöver MSB, som även tillhandahåller en kanslifunktion, ingår PTS, Försvarets radioanstalt (FRA), Säkerhetspolisen och Rikskriminalpolisen, Försvarets materielverk (FMV)[15] och Försvarsmakten[16] i SAMFI. (Lindgren, 2013)

Sedan den 1 januari 2015 är det Polismyndigheten, och inte Rikskriminalpolisen[17] som ingår i SAMFI. I det uppdrag som MSB har fått av regeringen ingår att tillsammans med övriga myndigheter i SAMFI ta fram en nationell plan som klargör hur allvarliga IT-incidenter ska hanteras samt att skapa kompletterande tekniska kompetensnätverk av experter som kan stödja samhället vid allvarliga IT-incidenter i syfte att skapa en ökad responsförmåga.[18]

[11] SOU 2015:25, s. 230-231.
[12] SOU 2015:25, s. 299.
[13] SOU 2015:25, s. 301.
[14] SOU 2015:25, s. 514.
[15] Representerat av Sveriges certifieringsorgan för IT-säkerhet (CSEC).
[16] Representerat av Militära underrättelse- och säkerhetstjänsten (MUST).
[17] Rikskriminalpolisen ingår sedan den 1 jan 2015 i Polismyndigheten, www.ne.se, 2015-11-19.
[18] Skr. 2009/10:124.

SAMFI hanterar huvudsakligen frågeställningar inom områdena[19]:

- strategi, handlingsplan och regelverk,
- tekniska frågor och standardiseringsfrågor,
- nationell och internationell utveckling inom informationssäkerhetsområdet,
- informationsaktiviteter,
- övningar och utbildning,
- hantering och förebyggande av IT-incidenter.

SAMFI har en webbplats, informationssäkerhet.se, som vänder sig till myndigheter och organisationer som behöver stöd i sitt informationssäkerhetsarbete.[20]

MSB utfärdar, med stöd av krisberedskapsförordningen (2006:942), föreskrifter för statliga myndigheters informationssäkerhet.[21] Föreskrifterna anger bl.a. enligt vilka standarder myndigheternas arbete ska bedrivas.[22] (Lindgren, 2013)

För att följa upp hur statliga myndigheter har tillämpat MSB:s föreskrifter och i övrigt arbetat med informationssäkerhet så genomförde MSB under 2014 en enkätundersökning. Resultatet av den redovisas i rapporten ”En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter”.[23] Där framgår att myndigheterna önskade stöd inom informationssäkerhetsområdet, bland annat med kravställning, uppföljning, informationsklassning och kontinuitetsplanering, gärna i form av malldokument, utbildningsdokument, vägledningar och praktiska exempel.

MSB har under 2015 tagit fram förslag på nya föreskrifter och allmänna råd inom informationssäkerhetsområdet. Anledningen till det är de standarder som författningen om statliga myndigheters informationssäkerhet (MSBFS 2009:10) hänvisar till har reviderats. Ett annat skäl är att det finns brister i statliga myndigheters informationssäkerhetsarbete, något som blev tydligt i den enkätundersökning som MSB gjorde under 2014. Förslagen har gått på remiss och remissvaren har begärts in under oktober 2015.[24] I förslagen står inget specifikt om industriella informations- och styrsystem.

[19] Publ.nr MSB286.
[20] www.informationssakerhet.se, 2015-10-21.
[21] Föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet (MSBFS 2009:10).
[22] Följande standarder ska tillämpas: Ledningssystem för informationssäkerhet – Krav (SS-ISO/IEC 27001:2006) och Riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 27002:2005)..
[23] MSB Publ.nr: MSB740.
[24] Konsekvensutredning rörande reviderade föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet, MSB dnr 2014-6391.

Försvarsmakten utfärdar, med stöd av säkerhetsskyddsförordningen, föreskrifter om säkerhetsskydd som bl.a. tar upp kategorisering i informationssäkerhetsklasser och krav på hantering av hemliga uppgifter.[25] Dessa föreskrifter gäller även Fortifikationsverket samt de myndigheter som hör till Försvarsdepartementet, utom Kustbevakningen. Inom FMV finns ett certifieringsorgan som utfärdar certifikat enligt standarden Common Criteria för granskning av produkters IT-säkerhet (ISO/IEC IS 15408). Rikspolisstyrelsen utfärdar föreskrifter om säkerhetsskydd som bl.a. tar upp informationssäkerhet för IT-system hos myndigheter, kommuner och landsting.[26] Föreskrifterna ovan är inte analyserade inom ramen för studien. (Lindgren, 2013)

Försvarsmakten har kommit ut med nya föreskrifter om säkerhetsskydd i mars 2015.[27] Föreskrifterna gäller nu för Fortifikationsverket, Försvarshögskolan samt Försvarsmakten och övriga myndigheter som hör till Försvarsdepartementet utom Statens haverikommission. Det bör noteras att Statens haverikommission, MSB och Kustbevakningen sedan 2015 hör till Justitiedepartementet. De hörde tidigare till Försvarsdepartementet.

I november 2013 beslutade regeringen att tillsätta en särskild utredare med uppdrag att föreslå strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och IT-system.[28] Utredningens resultat[29] presenterades i mars 2015 och innehåller ett förslag på en strategi för informations- och cybersäkerhet i staten med sex strategiska mål[30]:

att stärka styrning och tillsyn inom området,
att staten ska ställa tydliga krav vid upphandling på IT-området,
att statliga myndigheter ska kommunicera säkert,
att samtliga statliga myndigheter rapporterar IT-incidenter,
att arbetet med att förebygga och bekämpa IT-relaterad brottslighet stärks
att Sverige ska vara en stark internationell partner

Strategin vänder sig främst till regeringen, Regeringskansliet och statliga myndigheter men indirekt också till den delen av näringslivet och de organisationer som samverkar eller ingår affärsrelationer med staten.[31]

[25] Försvarsmaktens föreskrifter om säkerhetsskydd (FFS 2003:7).
[26] Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd (RPSFS 2010:3, FAP 244-1).
[27] Försvarsmaktens föreskrifter om säkerhetsskydd (FFS 2015:2).
[28] Strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system (Dir. 2013:110).
[29] Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten (SOU 2015:23).
[30] SOU 2015:23, s. 13.
[31] SOU 2015:23, s. 16.

Under det första strategiska målet, att stärka styrning och tillsyn inom området, anser utredningen att det bör inrättas ett Myndighetsråd för informationssäkerhet. Detta i syfte att ytterligare formalisera, utveckla och fördjupa samordningen av informationssäkerhetsarbetet. Myndighetsrådet föreslås ledas av MSB och bestå av företrädare för de relevanta myndigheterna på området. Myndigheten ska ha till uppgift att stödja och utveckla informationssäkerhetsarbetet i samhället.[32]

Industriella informations- och styrsystem (SCADA-system) tas upp på flera ställen i utredningen. Inledningsvis lyfts riskerna med att systemen, från att ha varit leverantörsspecifika och isolerade från omvärlden, numera ofta är direkt eller indirekt uppkopplade mot globala nätverk, vilket innebär att de kan utsättas för angrepp. Det är framför allt antagonistiska hot mot industriella informations- och styrsystem som lyfts i utredningen. Det påpekas också att många samhällsviktiga funktioner är beroende av industriella informations- och styrsystem och att störningar i dessa verksamheter kan leda till stora påfrestningar i samhället. Utredningen uttrycker därför vikten av att sektorsansvariga myndigheter påverkar informationssäkerhetsarbetet inom sina respektive sektorer.[33]

I utredningen redovisas det arbete som görs nationellt idag med fokus på industriella informations- och styrsystem. Bland annat beskrivs att kunskapscentret NCS3[34], som drivs i samverkan mellan MSB och FOI, har en central roll i syfte att höja medvetenheten, kunskapen och förmågan hos olika aktörer. Utredningen påpekar att behovet av medvetandehöjande aktiviteter är stort och att sådana åtgärder skulle behöva öka avsevärt. Även behovet av ytterligare studier lyfts, både inom NCS3 och inom olika sektorer, liksom att övningsverksamheten inom NCS3 bör fortsätta och stärkas.[35]

Utöver att utredningen trycker på att det är centralt att upprätthålla en hög nationell kompetens kring säkerhet i industriella informations- och styrsystem så poängterar de också vikten av internationell samverkan.[36]

Utredningen skickades ut på remiss[37] av Justitiedepartementet i maj 2015 till berörda myndigheter, organisationer och företag. Remissvaren begärdes in till den 15 september 2015 och då detta memo skrivs har inga åtgärder hunnit vidtas till följd av utredningen.

[32] SOU 2015:23, s. 15, 17, 218.
[33] SOU 2015:23, s. 65, 71-73.
[34] NCS3 – Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet.
[35] SOU 2015:23, s. 161-162, 164, 273.
[36] SOU 2015:23, s. 161.
[37] Ju2015/2650/SSK.

3.3 Hur frågorna har uppmärksammats

MSB gav under 2014 ut en ny version av sin vägledning till ökad säkerhet i industriella informations- och styrsystem.[38] Vägledningen vänder sig främst dem som arbetar inom samhällsviktiga verksamheter och syftar till att öka medvetenheten om behovet av en högsäkerhet i industriella informations- och styrsystem. Vägledningen har även översatts till engelska.[39]

MSB har gett ut en vägledning för fysisk informationssäkerhet i IT-utrymmen.[40] Vägledningen tar inte specifikt upp skydd av SCADA-system men bör vara till hjälp till arbetet med att öka säkerheten för industriella informations- och styrsystem.

I MSB:s handlingsplan för skydd av samhällsviktig verksamhet står det[41]:

> ”I dag är samhällsviktig verksamhet beroende av system för att bearbeta, lagra, kommunicera och mångfaldiga information. Genom industriella informations- och styrsystem har även de fysiska processerna integrerats i informationshanteringen inom samhällsviktig verksamhet. För att ta tillvara IT-utvecklingens möjligheter och skydda samhällsviktig verksamhet krävs ett systematiskt arbete med informationssäkerhet i hela samhället.”

I handlingsplanen föreslås ett antal åtgärder såsom vägledning för kontinuitetshantering och sektorsvisa planer. En åtgärdspunkt handlar om att genomföra projekt eller studier som identifierar befintlig lagstiftning och övriga regelverk som har koppling till arbetet med skydd av samhällsviktig verksamhet. MSB ansvarar tillsammans med sektorsansvariga för den punkten och räknar med att vid årsskiftet vara klar med sektorerna Energi, Transporter, Livsmedel och Hälso- och sjukvård samt omsorg.[42]

MSB driver också sedan 2005 ett privat-offentligt samverkansforum för informationsdelning kring säkerhet i industriella informations- och säkerhetssystem, FIDI-SCADA.[43] Inom forumet träffas representanter för flera branscher regelbundet för att dela information och koordinera arbetet inom området. MSB finansierar dessutom två femåriga forskningsprogram inom området sedan 2015; CERCES – (Center for Resilient Critical Infrastructures)[44] som leds av KTH och

[38] Vägledning till ökad säkerhet i industriella informations- och styrsystem, publ.nr: MSB718 - juli 2014.
[39] Guide to Increased Security in Industrial Information and Control Systems, Order No: MSB766 - November 2014.
[40] Vägledning för fysisk informationssäkerhet i it-utrymmen, 2013, MSB629.
[41] Handlingsplan för skydd av samhällsviktig verksamhet, 2013, MSB597.
[42] Personlig kommunikation med Jan-Olof Olsson, MSB.
[43] FIDI-SCADA, Forum för informationsdelning kring säkerhet i industriella informations- och styrsystem, publ.nr: MSB889, augusti 2015.
[44] www.kth.se/en/ees/omskolan/organisation/avdelningar/ac/research/cerces, 2015-11-16.

RICS (Resilient Information and Control Systems)[45] som leds av Linköpings universitet.

Inom den nationella risk- och förmågebedömning (NRFB) som MSB ansvarar för har FOI tagit fram exempelscenarier som beskriver möjliga händelser som berör informations- och cybersäkerhet. Ett av dessa beskriver ett angrepp mot SCADA-system.[46] Exempelscenariot borde kunna användas i medvetandehöjande syfte, men vi inte hittat något exempel på att det har gjorts.

Riksrevisionen har granskat om arbetet med informationssäkerhet i den civila statsförvaltningen är ändamålsenligt utifrån ökande hot och risker.[47] Granskningsrapporten, som konstaterar att det finns brister i informationssäkerheten i den civila statsförvaltningen, lyfter riktade cyberattacker som ett av flera hot. Rapporten tar specifikt upp angrepp mot industriella informations- och styrsystem. Den exemplifierar hoten med STUXNET-attacken mot en iransk kärnkraftsanläggning 2010 och attacken mot det kommunala bostadsbolaget Platens fastigheter i Motala samma år, då någon hackade sig in den datacentral som reglerar fjärrvärmen till bolagets fastigheter.

[45] www.rics.se, 2015-11-16.
[46] Veibäck, E., Malmberg Andersson F. och Carlsson, E. (2014) Informations- och cybersäkerhet i nationell risk- och förmågebedömning – diskussion och presentation av en tankemodell, FOI memo 5100.
[47] Informationssäkerheten i den civila statsförvaltningen, RiR 2014:23.

4 Elproduktion och eldistribution

4.1 Tillämplig lagstiftning

Den grundläggande lagstiftningen inom området, ellagen (1997:857), innehåller ingen särskild reglering avseende krisberedskap men pekar ut affärsverket Svenska Kraftnät (SvK) som systemansvarig nationell myndighet för eldistribution. Det finns en separat elberedskapslag (1997:288) som innehåller bestämmelser om beredskap vid produktion och överföring av el samt vid handel med el. Elberedskapslagen innebär skyldigheter för den som bedriver sådan verksamhet att vidta beredskapsåtgärder, dvs. åtgärder som behövs för att förebygga, motstå och hantera sådana störningar i elförsörjningen som kan medföra svåra påfrestningar på samhället. Sådana åtgärder beslutas av regeringen eller den i elberedskapsförordningen (1997:294) utpekade elberedskapsmyndigheten (SvK) som därmed har rätt att meddela föreskrifter om beredskapsåtgärder.

Exempel på beredskapsåtgärder med bäring på industriella informations- och styrsystem inkluderar skyddsåtgärder i och av anläggningar (t.ex. förstärkt skalskydd inkl. teknisk bevakning) och åtgärder för ökad tillgänglighet ur beredskapssynpunkt (t.ex. komplettering och förstärkning av styr- och reglersystem samt kommunikationsförbindelser och installation av reservkraft).[48]

(Lindgren, 2013)

Föreskriften om åtgärder som kan utgöra beredskapsåtgärder enligt elberedskapslagen (SvKFS 2000:2 och 1997:2), som refereras till i stycket ovan, har ersatts av en ny föreskrift (SvKFS 2013:2).[49] I föreskriften står det specifikt att en beredskapsåtgärd för att motstå störningar är att göra styrsystem mer robusta.

4.2 Övriga regler och bestämmelser

För att stamnätet ska fungera driftsäkert måste anslutna anläggningar uppfylla ställda krav vad gäller funktionalitet. SvK upprättar föreskrifter med kravställningar som gäller för alla anläggningar samt tekniska riktlinjer för stamnätet. Dessa tekniska riktlinjer gäller även anläggningar som är direkt anslutna till stamnätet. Detta gäller bland annat olika typer av produktionsanläggningar (gasturbinaggregat, kondenskraftverk, kraftvärmeverk och vattenkraftstationer).

[48] SvKFS 2000:2, Föreskrifter om ändring av Affärsverket svenska kraftnäts föreskrifter (SvKFS 1997:2) om åtgärder som kan utgöra beredskapsåtgärder enligt elberedskapslagen (1997:288).
[49] Affärsverket svenska kraftnäts föreskrifter och allmänna råd om elberedskap (SvKFS 2013:2).

För kärnkraftverken finns ytterligare föreskrifter som styr utformningen (mer om det nedan).

I föreskrifterna om driftsäkerhetsteknisk utformning av produktionsanläggningar finns bland annat krav på störningstålighet vid kraftiga variationer (avvikelser) i frekvens och/eller spänning. Det finns också generella krav på att anläggningar av en viss storlek ska kunna lämna realtidsinformation till Svenska Kraftnät avseende spänning, effekt och driftstatus.[50] Det finns även ett krav på att sådana anläggningar efter en driftstörning inom 15 minuter ska kunna styras manuellt antingen lokalt eller via fjärrstyrning. Det sägs inget specifikt om industriella informations- och styrsystem i dessa föreskrifter.

Bland de tekniska riktlinjerna finns en uppsättning riktlinjer för kontroll-anläggningar, med bland annat riktlinjer för Standarder och generella krav, Datorer i kontrollanläggning, Fjärrkontroll och RTU[51]:er, Människa-Maskin-Kommunikation och Dokumentation av kontrollutrustningar. [52] Riktlinjerna för fjärrkontroll och RTU:er tar bland annat upp hur kommunikation ska ske med över- och underordnade system (protokoll m.m.) men det sägs inget specifikt om säkerhetsaspekter. Det finns även tekniska riktlinjer för IT-säkerhet.[53]

(Lindgren, 2013)

Ovanstående uppgifter gäller fortfarande.

För kärnkraftverken styrs utformningen även av de krav som finns i Strål-säkerhetsmyndighetens föreskrifter, vilka i sin tur utgår ifrån lagen och förordningen om kärnteknisk verksamhet.[54] I dessa föreskrifter finns en separat paragraf om datoriserade system:

> ”Datoriserade system av betydelse för anläggningens säkerhet inklusive det fysiska skyddet ska vara skyddade mot obehörig åtkomst och dataintrång.”

Av de allmänna råd om tillämpning av föreskriften som myndigheten utarbetat framgår att kravet gäller såväl processdatorer som datorsystem som används för tillträdeskontroll och larmfunktioner. Det görs också ett förtydligande av att skyddsåtgärder ska vidtas för att skydda dessa system både från obehörig

[50] SvKFS 2005:2, Affärsverket svenska kraftnäts föreskrifter och allmänna råd om driftsäkerhetsteknisk utformning av produktionsanläggningar.
[51] RTU = Remote Terminal Units
[52] TR2-03-2 Standarder och generella krav, TR2-03-3 Datorer i kontrollanläggning, TR2-04-3 Fjärrkontroll och RTU:er, TR2-04-2 Människa Maskin Kommunikation, TR2-10-1 Dokumentation kontrollutrustningar.
[53] TR4-02, Tekniska riktlinjer IT-säkerhet.
[54] Strålsäkerhetsmyndighetens föreskrifter om fysiskt skydd av kärntekniska anläggningar (SSMFS 2008:12), 11 §.

åtkomst, t.ex. genom tillträdesbegränsningar till berörda lokaler, och från dataintrång t.ex. genom brandväggar eller fysisk separation från administrativa datanät.

I fall det inträffar en incident med betydelse för säkerheten vid en kärnteknisk anläggning eller om förhållanden av betydelse för säkerheten i en anläggning upptäcks ska detta rapporteras till Strålsäkerhetsmyndigheten. Detta bör innebära att eventuella incidenter som rör industriella styr- och informationssystem dokumenteras och rapporteras till en statlig myndighet.

(Lindgren, 2013)

Utöver de av Strålsäkerhetsmyndighetens utfärdade föreskrifter som refereras till ovan (SSFMS 2008:12) finns det fler som berör säkerheten i kärntekniska anläggningar.[55] Ingen av dem nämner dock specifikt industriella informations- och styrsystem. Som en följd av förändringar i omvärlden och ett nytt EU-direktiv om strålskydd och kärnsäkerhet pågår sedan 2013 en översyn av föreskrifterna i Strålsäkerhetsmyndighetens författningssamling (SSMFS). Översynen förväntas pågå fram till 2018. Enligt uppgift[56] innefattar föreskrifterna även informationssäkerhet. Strålsäkerhetsmyndigheten arbetar dessutom med att ta fram ett förslag till ny strålskyddslag och ny strålskyddsförordning där EU:s strålskyddsdirektiv, 2013/59/Euratom, ska implementeras.[57] Utöver det tar myndigheten fram nya föreskrifter om konstruktion av kärnkraftreaktorer där instrumentation and control (I&C), som är kärnkraftsbranschens närliggande benämning på styrsystem, ska få ett eget avsnitt[58].

För vattenkraftstationerna finns det utöver krav på utformning av vattenkraftaggregaten även olika bestämmelser kopplade till dammsäkerhet, bland annat bestämmelser om farlig verksamhet i lagen om skydd mot olyckor.[59] Även kraven i elberedskapslagen på verksamhetsutövaren att genomföra risk- och sårbarhetsanalyser och informera om störningar är till för att öka säkerheten. Ur ett säkerhetsperspektiv måste en vattenkraftanläggning analyseras som en integrerad helhet. (Lindgren, 2013)

Ovanstående uppgifter gäller fortfarande.

[55] Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om säkerhet i kärntekniska anläggningar (SSMFS 2008:1), Strålsäkerhetsmyndighetens föreskrifter om konstruktion och utförande av kärnkraftsreaktorer (SSMFS 2008:17) och Föreskrifter om ändring i Strålsäkerhetsmyndighetens föreskrifter (SSMFS 2008:1) om säkerhet i kärntekniska anläggningar (SSMFS 2014:3).
[56] Personlig kommunikation med Kristina Blomqvist, MSB, 2015-11-20.
[57] http://www.stralsakerhetsmyndigheten.se/Lagar-forfattningar/Oversyn-av-Stralsakerhetsmyndighetens-foreskrifter, 2015-11-16.
[58] Personlig kommunikation med Kristina Blomqvist, MSB, 2015-12-04.
[59] Lag (2003:778) om skydd mot olyckor.

SvK är även, enligt säkerhetsskyddslagen (1996:627), säkerhetsskyddsmyndighet för elförsörjningen. Den som bedriver elförsörjningsverksamhet som omfattas av säkerhetsskyddslagen är skyldiga att utse en säkerhetsskyddschef som utövar kontroll över säkerhetsskyddet. Vem som är säkerskyddschef, och dennes ersättare, ska rapporteras till SvK. Utöver säkerhetsskyddschef finns det ett antal andra anställningar som innebär inplacering i säkerhetsklass, exempelvis personal som i sitt arbete med IT-system eller tele/datakommunikation kan få en sådan insyn i överföringssystem av el att de kan få del av hemliga uppgifter när de utför sitt arbete. Vid sådana anställningar ska registerkontroll genomföras.

Vissa objekt kan utifrån bestämmelserna i skyddslagen[60] beslutas vara skyddsobjekt. Detta gäller bland annat ”byggnader, andra anläggningar och områden som används eller är avsedda för ledning av räddningstjänsten eller totalförsvarets civila delar i övrigt eller för fredstida krishantering, energiförsörjning, vattenförsörjning, elektroniska kommunikationer, transporter eller försvarsindustriella ändamål”.[61] SvK har en förteckning över vilka anläggningar som, efter beslut av länsstyrelsen, är klassade som skyddsobjekt.[62] Utifrån ett sådant underlag bör det gå att dra slutsatser om vilken typ av anläggningar som klassas som skyddsobjekt och hur stor andel av anläggningarna inom elsystemet som skyddslagens bestämmelser omfattar.

Även personer som deltar i verksamhet vid skyddsobjekt ska enligt SvK:s föreskrifter genomgå registerkontroll.[63] För kärnkraftverken gäller detta bl.a. alla anställda samt personer som med tillträde till kontrollrum, telerum eller datarum eller i övrigt får insyn i kärnkraftsblockens säkerhetsskydd. För verksamhet vid övriga anläggningar som är skyddsobjekt gäller kravet bl.a. personer som äger tillträde till kontrollrum, telerum eller datarum och personer som äger tillträde till driftcentral varifrån skyddsobjektet styrs och övervakas.

(Lindgren, 2013)

Svenska kraftnäts föreskrifter om säkerhetsskydd (SvKFS 2005:1), som refereras till i stycket ovan, ersattes den 1 juli 2013 av en ny föreskrift (SvKFS 2013:1).[64] Revideringen av föreskrifterna ger nu bland annat företagen skyldighet att informera Svenska kraftnät vid incidenter som har betydelse för säkerhetsskyddet. Skyldigheten att informera gäller också om uppgifter som rör rikets säkerhet eller skydd mot terrorism har röjts eller om det finns en misstanke om

[60] Skyddslag (2010:305).
[61] Skyddslag (2010:305), 4 §, pt 4..
[62] SvK:s tekniska riktlinjer, Tillträdes- och fotobestämmelser för Svenska Kraftnäts anläggningar, TR 9-14 .
[63] Affärsverket svenska kraftnäts föreskrifter om säkerhetsskydd (SvKFS 2005:1).
[64] Affärsverket svenska kraftnäts föreskrifter och allmänna råd om säkerhetsskydd (SvKFS 2013:1).

att sådana uppgifter har röjts.[65] Uppgifterna om registerkontroll ovan har inte ändrats.

> Utöver de krav myndigheterna ställer på anläggningarna i elnätet finns det sedan några år tillbaka även ett så kallat funktionskrav i ellagen (1997:857) som innebär att oplanerade avbrott i elöverföringen inte får överstiga tjugofyra timmar. Det finns också regler om ersättning till de kunder som drabbas av ett längre avbrott i sin elleverans. Detta krav bör innebära ett incitament för nätföretagen att vidta åtgärder för att minska risken för driftstörningar. (Lindgren, 2013)

Ovanstående uppgifter gäller fortfarande.

[65] Risk- och sårbarhetsanalys för år 2014, Affärsverket svenska kraftnät, 2014-11-11, Dnr: Svk 2013/2082.

4.3 Hur frågorna har uppmärksammats inom sektorn

Beroendet av industriella informations- och styrsystem inom elförsörjningens drift och förvaltning och frågor om risker och robusthet i sådana system har uppmärksammats inom sektorn. SvK finansierar bland annat doktorandprojekt vid KTH inom området.[66] Det pågår även arbete med mer övergripande informationssäkerhetsfrågor inom branschen som rimligen bör ha kopplingar till industriella informations- och styrsystem.[67] (Lindgren, 2013)

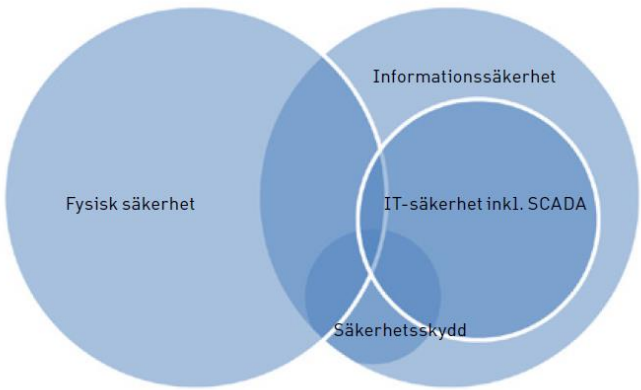
Svenska kraftnät bedriver och stöttar forskningsprojekt samt stödjer doktorandprojekt och examensarbeten vid de tekniska högskolorna i Sverige. Den totala budgeten för forskning och utveckling under 2015 är 40 miljoner kronor.[68] I Svenska kraftnäts forsknings- och utvecklingsplan för 2015-2017 lyfts ”Informations- och IT-säkerhet” som ett av sju områden som anses ha störst behov av FoU de närmaste tre åren.[69] Inom området ryms även driftkritiska system (SCADA) för central styrning och övervakning av kraftnätet och produktionen. SCADA-systemen beskrivs som kritiska för styrning och övervakning av elnätet och det framhålls ett behov av att stärka den digitala säkerheten, den s.k. cybersäkerheten, för sådana system.[70] I FoU-planen påpekas att många av SCADA-systemen är sammankopplade eller utbyter information med andra typer av system och att det därför är av yttersta vikt att skydda information och funktionalitet i samtliga typer av it-system.[71]

Under den period FoU-planen spänner över (2015-17) finns det även en intention att starta upp ett projekt som lägger fokus på att ”utnyttja delar av data som finns inom organisationen men som insamlats av andra skäl än underhåll, exempel på sådan data är strömmar, spänningar samt brytar- och frånskiljarrörelser ur SCADA-systemet”.[72]

[66] SvK, Beslut om Svenska Kraftnäts FoU-plan 2012-2014 (dec 2011).
[67] Förstudierapport Svenska Kraftnät 2011 – Branschens behov av stöd inom informationssäkerhetsområdet, dnr 2011/1199, 2012-03-26.
[68] www.svk.se/om-oss/organisation/forskning-och-utveckling, 2015-11-16.
[69] Forsknings- och utvecklingsplan 2015 – 2017, Svenska kraftnät, www.svk.se/contentassets/24899fc22f6c4c51b76affeda839da0f/141217-fou-plan-2015-2017.pdf, 2015-11-16.
[70] Ibid, s.23.
[71] Ibid, s.17.
[72] Ibid, s. 31.

Svenska kraftnät arbetar också mer övergripande med informationssäkerhetsfrågor och tog tillsammans med representanter från Svensk Energi fram en vägledning för informations- och IT-säkerhet samt säkerhetsskydd under 2014.[73] Vägledningen syftar till att hjälpa företag verksamma inom elförsörjningen med säkerhetsarbetet, både i allmänhet och mer specifikt med det som berörs i SvKFS 2013:1.

I vägledningen definieras SCADA-säkerhet som en delmängd av IT-säkerhet, som i sin tur definieras som ”sådan säkerhet som rör tekniskt skyddande funktioner av exempelvis system”.[74] Figur 1 visar hur vägledningen ser på överlappet mellan de olika säkerhetsområdena.



Figur 1. Vägledning för informations- och IT-säkerhet samt säkerhetsskydd, mars 2014, Svenska kraftnät, figur 4, s.16.

I vägledningen påpekas att säkerhet i styrsystem och SCADA-säkerhet är av yttersta vikt för elbranschen då i stort sett alla produktions- och distributionsanläggningar är direkt beroende av sådana system för sin funktion. I takt med att integrationen mellan styrsystem och andra typer av IT-system ökar så ökar också kraven på att säkerheten i dessa system motsvarar den i andra skyddsvärda IT-system. Med äldre system kan detta vara problematiskt då säkerheten i dessa ofta har baserats på att de varit åtskilda från övriga system.[75]

[73] Vägledning för informations- och IT-säkerhet samt säkerhetsskydd, mars 2014, Svenska kraftnät, www.energisakerhetsportalen.se/media/1054/vaegledning-informations-och-it-saekerhet-samt-saekerhetsskydd.pdf.
[74] Ibid, s. 11.
[75] Ibid, s. 16..

Svenska kraftnät har också gett ut en vägledning om IT-säkerhetsarkitektur.[76] I den står det mycket med bäring på ICS/SCADA-system. Bland annat lyfts ett antal problem, som att mjukvaruuppdateringar kan vara svåra att genomföra, att äldre leverantörsspecifik hård- och mjukvara inte alltid stöds av moderna antivirusprogram och att leverantören av ICS/SCADA-lösningar inte alltid tillåter att tredjepartsprogram installeras. Det nämns också lösningar på problemen, som hur man hanterar viruskontroller och hur man kan använda sig av så kallade vitlistor (listor på godkända program) snarare än svartlistor (listor på blockerade program). Vägledningen refererar till Open Security Architectures modellösning för industriella kontrollsystem som innehåller 34 säkerhetskontroller för ICS/SCADA.[77]

Svenska Kraftnät har, tillsammans med representanter från Svensk Energi, tagit fram en hotkatalog[78] som är en sammanställning av säkerhetsproblem som förekommer i samhället i allmänhet och mot aktörer inom elsektorn i synnerhet. I arbetet har särskild vikt lagts på att belysa IT-relaterade hot och risker och i anslutning till dessa beskrivningar nämns SCADA-system på ett flertal ställen.

I Svenska kraftnäts risk- och sårbarhetsanalys för 2014 tas antagonistiska hot som sabotage och terrorangrepp upp som ett möjligt hot mot strategiska anläggningar inom elförsörjningen, vilket skulle kunna resultera i omfattande och långvariga elavbrott.[79]

> ”Angrepp mot elförsörjningen kan utöver fysiska attacker också ske i form av IT-attacker och dataintrång, där till exempel system för styrning och övervakning (SCADA-system) eller information om en organisations kritiska system kan utgöra ett mål.”[80]

Under avsnittet ”Genomförda, pågående och planerade åtgärder” nämns att ett antal säkerhetshöjande åtgärder har genomförts under 2014 inom ramen för riktade beredskapsåtgärder för att öka skyddsförmågan mot fysiskt sabotage, intrång och skador i prioriterade anläggningar samt IT-attacker (SCADA- och affärssystem). Vilka dessa åtgärder är nämns dock inte. Inom förmågebedömningen identifierades även behovet av att öka kunskapen inom informationssäkerhetsområdet och för att åtgärda det så togs vägledningen för informationssäkerhet och säkerhetsskydd, som nämns ovan, fram tillsammans med Svensk

[76] IT-säkerhetsarkitektur, en vägledning för elbranschen med typexempel och referenslösningar, 2015-03-15.
[77] www.opensecurityarchitecture.org/cms/library/0802control-catalogue, 2015-11-16.
[78] Hotkatalog för Elbranschen Hot mot IT-, informations¬hantering, processkontroll och automation, Version 1.0, Svenska kraftnät, dnr: 2012/331.
[79] Risk- och sårbarhetsanalys för år 2014, Affärsverket svenska kraftnät, 2014-11-11, Dnr: Svk 2013/2082.
[80] Ibid. s. 17.

Energi. Därutöver har en utbildning i säkerhets- och medvetandehöjande åtgärder påbörjats under 2014 med hjälp av ett interaktivt utbildningsverktyg.[81] Svenska kraftnät har även i sin risk- och sårbarhetsanalys för 2015 lyft cyberattacker mot SCADA-system på ett flertal ställen.[82]

Svenska kraftnät, Svensk Energi och Energimyndigheten driver tillsammans Energisäkerhetsportalen[83] som är en samlingsplats för relevanta styr- och stöddokument samt för kommunikation av för branschen aktuella händelser och nyheter.

Samordningsrådet för smarta elnät[84] har på uppdrag av regeringen lämnat ett slutbetänkande SOU 2014:84[85] som bland annat lyfter behovet av att inkludera IT- och styrsystem i arbetet med risk- och sårbarhetsanalyser inom elsektorn:[86]

> ”I takt med ett ökat elberoende ökar också behovet av sårbarhets- och risk-analyser som också tar hänsyn till den ökade integrationen av IT-system. Men föreskrifterna för genomförandet av risk- och sårbarhetsanalyser fokuserar fortfarande i stor utsträckning på leveranssäkerhet och bör därför kompletteras med särskilt hänseende på IT- och styrsystem.”

I en rapport från Energimarknadsinspektionen behandlas funktionskrav på framtidens elmätare. Den innefattar både styrsystem och säkerhetsaspekter även om den inte specifikt tar upp begreppet SCADA-säkerhet.[87] Det gör däremot en rapport av Malmgren och Johansson som berör säkerheten i smarta elnät.[88] Författarna använder begreppen cybersäkerhet, IT-säkerhet och SCADA-säkerhet som synonymer. De visar på hur antalet sårbarheter hos SCADA-system har ökat de senaste fyra åren, ger exempel på incidenter och diskuterar åtgärder. Bland annat pekar de på CPNI (Centre for the Protection of National Infrastructure) i Storbritannien som har gett ut ett flertal relevanta publikationer om SCADA-säkerhet. De föreslår också att Sverige ska inrätta en CERT-funktion för ICS/SCADA-system.

[81] Ibid. s. 34.
[82] Risk- och sårbarhetsanalys för år 2015, Svenska kraftnät, ärendenr: 2015/1763.
[83] www.energisakerhetsportalen.se, 2015-11-16.
[84] www.swedishsmartgrid.se, 2015-11-16.
[85] Planera för effekt! Slutbetänkande från Samordningsrådet för smarta elnät (SOU 2014:84).
[86] SOU 2014:84, s. 83-84.
[87] Norstedt, D., Persson, S. och Ny, T., Funktionskrav på framtidens elmätare, Energimarknadsinspektionen, R2015:09.
[88] Malmgren, R. och Johansson, E., Rapport rörande säkerhet i smarta elnät, 2014.

5 Dricksvattenproduktion och vattendistribution

5.1 Tillämplig lagstiftning

Inom det samlade området vattenförsörjning och avlopp utgör lag (2006:412) om allmänna vattentjänster (även kallad LAV) grunden för det nationella regelverket. Även miljöbalken (1998:808) och förordning (1998:899) om miljöfarlig verksamhet och hälsoskydd ligger till grund för bestämmelser inom området. Om det med hänsyn till skyddet för människors hälsa eller miljön behöver ordnas vattenförsörjning eller avlopp i ett större sammanhang har kommunen enligt LAV ett ansvar att tillhandahålla allmänna vattentjänster.

I fråga om den del av området som rör dricksvattenkvaliteten är det i första hand livsmedelslagen (2006:804) och den därtill knutna livsmedelsförordningen (2006:813) som reglerar verksamheten. Ansvarig nationell myndighet är Livsmedelsverket.

(Lindgren, 2013)

Sedan december 2014 kopplas ansvarsfördelningen, befogenheterna och sanktionsmöjligheterna enligt livsmedelslagen ihop med EU-lagstiftningen via SFS 2014:1526 (Tillkännagivande om de EU-bestämmelser som kompletteras av livsmedelslagen (2006:804)).[89]

Övriga berörda myndigheter är Havs- och Vattenmyndigheten (centralt tillsynsansvar för frågor om skydd av dricksvattenförekomster, vattenskyddsområden och dricksvattentäkter) och Socialstyrelsen (med centralt tillsynsansvar för enskilda anläggningar, lokalt tillsynsansvar vilar på kommunernas Miljö- och hälsoskyddskontor.) Även Boverket (i fråga om installationer i fastigheter), Kemikalieinspektionen (KemI) och SSM berörs i någon mån av vattenfrågor. I LAV anges att länsstyrelsen har ett tillsynsansvar över att kommunerna fullgör sina skyldigheter. Sammantaget är det frågor om vattenkvalitet som utgör tyngdpunkten i tillsynsarbetet. Vid en tidigare genomlysning av krisberedskapen inom dricksvattenområdet konstaterade Riksrevisionen att den ordinarie tillsynen

[89] Nationell plan för kontrollen i livsmedelskedjan 2015-2018. Del 4, Organisation, revision och fördjupning inom planens olika områden. Planen har utarbetats av Livsmedelsverket, Jordbruksverket, Statens veterinärmedicinska anstalt, Länsstyrelsen, Sveriges Kommuner och Landsting samt Generalläkaren. Det står inget årtal eller rapportnummer i dokumentet.

inte täcker in alla områden som är viktiga ur beredskapssynpunkt och att det saknas en central funktion för incidentbevakning.[90]

Vissa anläggningar och områden som används för vattenförsörjning kan enligt bestämmelserna i skyddslagen beslutas vara skyddsobjekt vilket bl.a. innebär tillträdesförbud för obehöriga.[91]

(Lindgren, 2013)

Ovanstående uppgifter gäller fortfarande.

5.2 Övriga regler och bestämmelser

Livsmedelsverket beslutar om föreskrifter inom dricksvattenområdet samt vägledningar till dessa föreskrifter. [92] (Lindgren, 2013)

Den 1 juli 2013 trädde en mindre ändring av föreskrifterna i kraft (LIVSFS 2013:4). I den finns en ny definition av begreppet ”distributionsanläggning” och det finns också ett förtydligande över vilka anläggningar för dricksvatten-försörjning som omfattas av föreskrifterna. Ändringarna av föreskrifterna innebär inga ändringar i sak.

Av särskilt intresse för skydd av industriella informations- och styrsystem är Livsmedelsverkets föreskrifter (LIVSFS 2008:13) om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar. Föreskriften innehåller krav på åtgärder för att förebygga skadeverkningar samt upptäcka sabotage och avhjälpa skadeverkningar. Detta ska bl.a. annat göras genom att säkerställa att obehöriga personer inte kan bereda sig tillträde till ett vattenverk och att distributionsanläggningar skyddas från obehörig åtkomst. Som en specifik punkt lyfts även skyddet av industriella informations- och styrsystem fram:

> ”Den som producerar dricksvatten eller tillhandahåller dricksvatten från en distributionsanläggning ska vidta de administrativa och tekniska åtgärder som behövs för att säkerställa att system för drift och övervakning av dricksvattenproduktionen och dricksvattendistributionen skyddas mot obehörig åtkomst. Även handlingar som är av betydelse för driften och övervakningen ska skyddas mot obehörig åtkomst.”[93]

(Lindgren, 2013)

[90] Riksrevisionen, Dricksvattenförsörjning – beredskap för stora kriser, RiR 2008:8
[91] Skyddslag (2010:305), 4 §, pt 4.
[92] Bl.a. Livsmedelverkets föreskrifter (SLVFS 2001:30) om dricksvatten (ändrad LIVSFS 2011:3) som införlivar ett EG-direktiv om minimikrav på dricksvattenkvaliteten.
[93] Livsmedelsverkets föreskrifter (LIVSFS 2008:13) om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar, 6 §.

Även här har en mindre ändring i föreskrifterna (LIVSFS 2013:5), som berör definitionen av begreppet ”distributionsanläggning”, trätt i kraft den 1 juli 2013.

Livsmedelsverket har även tagit fram vägledningar till sina föreskrifter. I föreskriften om åtgärder mot sabotage och annan skadegörelse tas såväl generell informationssäkerhet som säkerhet i vattenverkens styr- och reglersystem upp. I den senare delen diskuteras bl.a. risker med integration till kontorsnätverk, krav på behörigheter, regler för inloggning och loggning av aktiviteter.[94]

Det bör noteras att Livsmedelsverkets föreskrifter ovan gäller ”sabotage och skadegörelse som kan påverka kvaliteten på dricksvatten”. Mängden vatten tas inte upp explicit. I vägledningen till föreskriften anges dock att åtgärder mot sabotage och skadegörelser även påverkar den mängd vatten som kan levereras. I LAV anges att kommunen, om vissa förutsättningar är uppfyllda i ett område, har ett ansvar att tillhandahålla allmänna vattentjänster, dvs. att ordna vatten-försörjningen i ett större sammanhang och tillhandahålla dricksvatten. Det saknas specifika krav på att en viss mängd vatten måste tillhandahållas per dygn, däremot måste kvantiteten vara tillräcklig för att inte sanitära olägenheter eller annat hot mot människors hälsa ska uppstå.[95] Branschorganisationen Svenskt Vatten, som företräder vattentjänstföretagen, har tagit fram råd och riktlinjer i anslutning till Livsmedelsverkets föreskrifter med fokus på fysiskt skydd.[96] I Svenskt Vattens generella råd och riktlinjer för ansvariga inom dricksvatten-produktion finns ett avsnitt om säkerhetsanalys där områden som lås-, larm-, drift- och övervakningssystem och IT-säkerhet omnämns, men inte utvecklas närmare.[97] Där finns dock en hänvisning till en särskild säkerhetshandbok som Svenskt Vatten tagit fram.[98]

(Lindgren, 2013)

Ovanstående uppgifter gäller fortfarande. Den säkerhetshandbok som Svenskt vatten har tagit fram innehåller ett kapitel som enbart handlar om säkerhets-aspekter i industriella kontrollsystem. [99]

[94] Livsmedelsverket, Vägledning: Dricksvatten – åtgärder mot sabotage och annan skadegörelse, 2012-02-17.
[95] Se 33 § i förordning (1998:899) om miljöfarlig verksamhet och hälsoskydd, under rubriken Särskilda bestämmelser till skydd mot olägenheter för människors hälsa. ”I syfte att hindra uppkomst av olägenhet för människors hälsa skall en bostad särskilt; ha tillgång till vatten i erforderlig mängd och av godtagbar beskaffenhet till dryck, matlagning, personlig hygien och andra hushållsgöromål”.
[96] Svenskt Vatten, Råd och riktlinjer – Fysiskt och tekniskt skydd för dricksvatten, december 2011.
[97] Svenskt Vatten, Råd och riktlinjer för ansvariga inom dricksvattenproduktion.
[98] Svenskt Vatten, Säkerhetshandbok för dricksvattenproducenter.
[99] Ibid, s. 49-57.

5.3 Hur frågorna har uppmärksammats inom sektorn

Frågan om säkerhet i industriella styr- och informationssystem har på flera sätt uppmärksammats inom sektorn. MSB och Svenskt Vatten stödde gemensamt genomförandet av en studie som under 2009 och 2010 gjorde en kartläggning av säkerheten i sådana system.[100] Livsmedelsverket har nyligen också reviderat vägledningen till föreskrifterna om åtgärder mot sabotage och annan skadegörelse och där lagt till avsnitt om behörighetskontroll, rutiner för tillträde till lokaler, intrångsdetektering och intern incidentrapportering.[101] (Lindgren, 2013)

På sin hemsida har Svenskt Vatten en checklista för ökad SCADA-säkerhet (även kallad ”blå listan”) som baseras på resultat från den studie som gjordes av MSB och Svenskt vatten 2009-10 (se ovan).[102] Checklistan ska kunna användas av organisationer för att inventera den egna verksamheten, men också som diskussionsunderlag inför systemförändringar och upphandlingar. Svenskt vatten har också anordnat säkerhetsseminarium som bland annat innefattat informationssäkerhet.[103]

FOI har inom ramen för NCS3 utvecklat en demonstrator (fysisk modell) av en dricksvattenanläggning och dess produktionskedja, från råvatten till distribution av dricksvatten. Demonstratorn är ett pedagogiskt hjälpmedel för att visa var de industriella informations- och styrsystemen används och vilken påverkan de kan få på produktionen.[104]

[100] MSB och Svenskt Vatten, Kartläggning av SCADA-säkerhet inom svensk dricksvattenförsörjning, december 2010, (framtagen inom MSB:s program, författad av Erik Johansson vid KTH)
[101] Den första versionen av vägledningen utarbetades under 2008.
[102] www.svensktvatten.se/Vattentjanster/Dricksvatten/Kris/SCADA, 2015-11-16.
[103] www.trippus.se/eventus/userfiles/63343.pdf, 2015-11-16.
[104] www.foi.se/sv/Var-kunskap/Informationssakerhet-och Kommunikation/NCS3/Demonstratorer1/Dricksvatten, 2015-11-16.

6 Fjärrvärme/-kyla – produktion och distribution

Nästan alla fjärrvärmeverk producerar även el och därför gäller samma föreskrifter för dem som för de företag och bolag som producerar el. Svenska Kraftnät är dock bara tillsynsmyndighet mot elproduktionen, inte mot energiproduktion.[105]

6.1 Tillämplig lagstiftning

Den specifika nationella lagstiftningen inom området – fjärrvärmelagen (2008:263) – handlar i första hand om att stärka fjärrvärmekundernas ställning och öka insynen i fjärrvärmeverksamhet för att kunna bedöma om prissättningen är rimlig, bl.a. genom att fjärrvärmeföretagen ska lämna uppgifter om drift- och affärsförhållanden. Lagen innehåller inga specifika krav på utformning och drift av anläggningar för produktion eller distribution. Fjärrkyla omfattas inte av bestämmelserna i lagen.

Fjärrvärmelagens skydd för konsumenter mot avbrott i distributionen av fjärrvärme innebär att fjärrvärmeföretaget ska ersätta skada som en konsument orsakas genom att distributionen av fjärrvärme avbryts utan att det beror på konsumentens försummelse eller utan att fjärrvärmeföretaget har rätt att avbryta distributionen. Godtagbara skäl för att avbryta distributionen är om avbrottet är nödvändigt för att genomföra en åtgärd som syftar till att undvika personskada eller omfattande sakskada, bygga ut fjärrvärmeverksamheten eller en god distributionssäkerhet. Det finns inte som på elsidan någon reglering av leveranssäkerheten till kund såsom maximal tid för oplanerade avbrott eller ersättning för elavbrott som varar en viss tid.

I övrigt är det i första hand arbetsmiljölagen (SFS 1977:1160) som är av stor betydelser för fjärrvärmeområdet. Även jordabalken (SFS 1970:994), miljöbalken (SFS 1998:808) och brottsbalken (1962:700) innehåller bestämmelser som påverkar verksamheten.

Energimarknadsinspektionen är tillsynsmyndighet gentemot fjärrvärmeföretagen enligt fjärrvärmelagen.[106] Det är därmed till Energimarknadsinspektionen som fjärrvärmeföretagen lämnar uppgifter om affärs- och driftförhållanden. Dessa rapporter innehåller dock inga uppgifter som relaterar till styr- och informationssystem kopplade till driften. I fråga om tillsyn av själva produktionen och

[105] Kommentar som kom upp på FIDI-SCADA-mötet den 26 nov 2016.
[106] Förordning (2007:1118) med instruktion för Energimarknadsinspektionen, 1 §, pt 1.

distributionen av fjärrvärme synes den handla om hur verksamheten bedrivs i förhållande till bestämmelserna i arbetsmiljö- och miljölagstiftningen.

(Lindgren, 2013)

Ovanstående uppgifter gäller fortfarande.

6.2 Övriga regler och bestämmelser

Övriga regler och bestämmelser inom fjärrvärmeområdet utgår från det faktum att fjärrvärmeanläggningarna, vilka schematiskt delas in i produktionsdelar, distributionsnät och fjärrvärmecentraler, består av trycksatta anordningar för vilket det finns specifika regler genom föreskrifter från Arbetsmiljöverket.[107] Av föreskrifterna framgår bl.a. krav på riskbedömningar, tillsyn och larmrutiner.

I de allmänna råd från Arbetsmiljöverket som är knutna till föreskrifterna listas ett antal exempel på särskilda risker. Ingen av dessa är relaterade till industriella informations- och styrsystem. Branschorganisationen Svensk Fjärrvärme har utifrån myndigheternas föreskrifter tagit fram en handbok för riskbedömning.[108] I denna handbok nämns ingenting om risker och hot specifikt knutna till industriella styr- och informationssystem.

Som stöd för en effektiv och säker drift vid de svenska fjärrvärmeanläggningarna ger branschorganisationen Svensk Fjärrvärme ut *Tekniska Bestämmelser* och annat informationsmaterial som enligt Svensk Fjärrvärme ”utgör fjärrvärme-branschens samlade kunskap och kompetens inom distribution och fjärrvärme-centraler. Bestämmelserna bör användas vid planering, upphandling och utförande av fjärrvärmesystem och omfattar handlingar för komponenter, anvisningar, certifiering och garanti. I bestämmelserna framgår funktions- och utförandekrav med målsättningen att få god funktion, säkra system och långsiktig hållbarhet”.[109] De tekniska bestämmelserna handlar om olika komponenter som ingår i system och anläggningar. Några bestämmelser som specifikt tar upp industriella styr- och informationssystem har inte identifierats.

(Lindgren, 2013)

Ovanstående uppgifter gäller fortfarande.

[107] Arbetsmiljöverket. Användning av trycksatta anordningar AFS 2002:1.
[108] Svensk Fjärrvärme, Säkerhet i fjärrvärmeanläggningar – Regler och råd för riskbedömning, 2004:2.
[109] Svensk Fjärrvärmes webbplats (http://www.svenskfjarrvarme.se/Rapporter--Dokument/Rapporter_och_Dokument/Tekniska-bestammelser/), per 2012-11-22.

6.3 Hur frågorna har uppmärksammats inom sektorn

Det finns ytterst få exempel på att säkerhet inom industriella informations- och styrsystem har lyfts inom sektorn. Mer allmänt har både Energimyndigheten och Svensk Fjärrvärme lyft området säker värmeförsörjning, men de nämner inget specifikt om informationssäkerhet.[110,111]

MSB har under 2015 initierat en studie inom NCS3 om hur industriella informations- och styrsystem används inom fastighetsautomation.[112] Studien kan möjligen öka medvetenheten inom fjärrvärme/-kyla-sektorn, men riktar sig inte till den specifikt.

[110] www.lansstyrelsen.se/orebro/SiteCollectionDocuments/Sv/manniska-och-samhalle/krisberedskap/Dokumentation/Energimyndigheten%20Varmeberedskap.pdf, 2015-11-16.
[111] www.svenskfjarrvarme.se/Nyheter/Nyhetsarkiv/2015/Saker-varmeforsorjning---viktig-bade-i-Sverige-och-EU, 2015-11-16.
[112] Mossberg Sonnek, K. och Lindgren, F., Industriella informations- och styrsystem inom fastighetsautomation – en förstudie, 2015, FOI Memo 5405.

7 Kemisk processindustri

7.1 Tillämplig lagstiftning

För att förebygga allvarliga olyckor inom kemisk processindustri och andra anläggningar med farlig industriell verksamhet finns det så kallade Sevesoregler. Dessa regler syftar även till att begränsa följderna för människor och miljö ifall en olycka ändå skulle inträffa. Reglerna tillämpas för verksamheter där farliga ämnen vid ett och samma tillfälle förekommer i vissa mängder.

Huvudlagstiftningen inom området utgörs av lagen om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor (även kallad Seveso-lagen)[113] med tillhörande förordning.[114]

(Lindgren, 2013)

Förordningen SFS 1999:382 (till vilken hänvisas ovan) upphävdes den 1 juni 2015 och ersattes av SFS 2015:236 (Förordning om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor). Regeringen har antagit den nya förordningen som ett led i att genomföra EU:s så kallade Seveso[115] III-direktiv som antogs den 4 juli 2012.[116] De huvudsakliga förändringarna i Seveso III-direktivet, jämfört med tidigare – Seveso II – är en anpassning till EU:s förordning om klassificering och förpackning av ämnen och blandningar och att kraven på information till och samråd med allmänheten har skärpts.[117]

[113] Lagen (SFS 1999:381) om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor.
[114] Förordning (SFS 1999:382) om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor.
[115] Direktivet har fått sitt namn från en allvarlig kemikalieolycka som inträffade 1976 i Seveso i Italien. Den och andra olyckor under 70-talet drev fram ny lagstiftning inom EU - det första Sevesodirektivet 1982. (www.seveso.se, 2015-11-19).
[116] Europaparlamentets och rådets direktiv 2012/18/EU.
[117] Konsekvensutredning avseende förslag till myndigheten för samhällskydd och beredskaps föreskrifter om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor, MSB, dnr 2014-5577.

Lagstiftningen medför skyldigheter för såväl verksamhetsutövare som myndigheter. Även miljöbalken och förordningar knutna till den innehåller bestämmelser som är relevanta för denna typ av verksamhet.[118] Lagstiftningen inom arbetsmiljöområdet ställer också krav på hur denna typ av verksamhet bedrivs.[119] (Lindgren, 2013)

Förordningen SFS 1998:900 (till vilken hänvisas ovan) upphävdes den 1 mars 2011 och ersattes av SFS 2011:13 (Miljötillsynsförordning).

Verksamheter som omfattas av Sevesolagstiftningen är i de flesta fall att betrakta som farlig verksamhet enligt lagen om skydd mot olyckor[120] med närmare bestämmelser i den tillhörande förordningen.[121] Beroende på vilken typ av ämnen som hanteras kan även lagstiftningen om brandfarliga och explosiva varor vara tillämplig.[122] (Lindgren, 2013)

Ovanstående uppgifter gäller fortfarande.

7.2 Övriga regler och bestämmelser

Denna typ av industriell verksamhet faller under ett antal olika lagstiftnings-områden och därmed är flera nationella myndigheter berörda och kan utfärda föreskrifter som är relevanta för sådan verksamhet, bl.a. Arbetsmiljöverket, MSB, Naturvårdsverket och Sprängämnesinspektionen.

Ett sådant exempel på föreskrifter är Räddningsverkets föreskrifter (vilka numera förvaltas inom MSB) som är knutna till Sevesolagen.[123] Där specificeras att den säkerhetsrapport som ska förnyas vart femte år och lämnas till tillsyns-myndigheten bl.a. ska innehålla uppgifter om riskkällor och en beskrivning av verksamhetens processer, inklusive styrning och kontroll, vid normal drift och vid förutsägbara störningar. Några uttalade krav på hur denna styrning och

[118] Miljöbalken (SFS 1998:808), förordningen (SFS 1998:899) om miljöfarlig verksamhet och hälsoskydd, förordningen (SFS 1998:900) om tillsyn enligt miljöbalken, förordningen (SFS 1998:901) om verksamhetsutövarens egenkontroll.
[119] Arbetsmiljölagen (SFS 1977:1160) samt arbetsmiljöförordningen (SFS 1977:1166).
[120] Lag (SFS 2003:778) om skydd mot olyckor.
[121] Förordning (SFS 2003:789) om skydd mot olyckor.
[122] Lag (SFS 2010:1011) om brandfarliga och explosiva varor samt Förordning (SFS 2010:1075) om brandfarliga och explosiva varor.
[123] Räddningsverkets föreskrifter (SRVFS 2005:2) om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor.

kontroll ska ske anges inte. Begreppet säkerhetsrapport förekommer även i Arbetsmiljöverkets föreskrifter inom området.[124]

(Lindgren, 2013)

Räddningsverkets föreskrifter SRVFS 2005:2 är upphävda den 1 juni 2015 och ersattes av MSBFS 2015:8 (Myndigheten för samhällsskydd och beredskaps föreskrifter om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor). Anledningen är anpassningen till det s.k. Seveso III-direktivet som antogs av EU den 4 juli 2012.[125]

Som en del i anpassningen till Seveso III-direktivet har det tillkommit fyra paragrafer om tillsyn. Den första av dem nämner att tekniska system samt organisations- och driftsystem som tillämpas vid verksamheten ska granskas systematiskt och att åtgärder ska vidtas för att förebygga allvarliga kemikalieolyckor och för att begränsa följderna av sådana olyckor.[126] Uppgifterna (ovan) om vad en säkerhetsrapport skulle innehålla enligt SRVFS 2005:2 finns inte med i MSBFS 2015:8.

Likaså upphävdes föreskrifterna AFS 2005:19 (till vilka hänvisas ovan) vid utgången av maj 2015 genom AFS 2014:44 (Arbetsmiljöverkets föreskrifter om upphävande av föreskrifterna om förebyggande av allvarliga kemikalieolyckor). Även om det inte går att hitta någon information om varför föreskriften inte har ersatts med en annan så är det gissningsvis för att MSBFS 2015:8 täcker även innehållet i dessa.

MSB är central tillsynsmyndighet enligt Sevesolagen. Även länsstyrelser och kommuner utövar tillsyn. I de delar där arbetsmiljölagstiftningen kräver tillsyn är Arbetsmiljöverket ansvarigt för den operativa tillsynen. Säkerhet i informations- och styrsystem nämns inte specifikt i de ovan nämnda föreskrifterna och torde därför heller inte vara föremål för riktad tillsyn från berörda myndigheter. (Lindgren, 2013)

Ovanstående uppgifter gäller fortfarande.

[124] Arbetsmiljöverkets författningssamling AFS 2005:19 förebyggande av allvarliga kemikalieolyckor.
[125] Europaparlamentets och rådets direktiv 2012/18/EU
[126] MSBFS 2105:8, 11 §.

7.3 Hur frågorna har uppmärksammats inom sektorn

På uppdrag av enheten för samordning av samhällets krisberedskap på Justitiedepartementet, Ju/SSK, har FOI skrivit en rapport om hur länsstyrelserna kan samordna sina personalresurser vid tillsyn av Sveriges 375 Sevesoverksamheter.[127] Rapporten går igenom Sevesolagstiftningen och lyfter säkerhet (security) på ett flertal ställen, men diskuterar inte informationssäkerhet eller industriella informations- och styrsystem.

I övrigt har studien inte hittat fler exempel där frågorna uppmärksammas.

[127] Roffey, R., Ryghammar, L. och Trané, C., Förslag till regional samordning av tillsyn för Sevesoverksamheter, 2014, FOI Memo 5083.

8 Spårbunden trafik

8.1 Tillämplig lagstiftning

Lagstiftningen inom området skiljer på järnväg respektive tunnelbana och spårväg. I såväl järnvägslagen som den tillhörande förordningen finns separata kapitel om krav på järnvägssystem inklusive krav på säkerhet.[128] Det finns också krav på säkerhetsstyrningssystem för infrastrukturförvaltare och järnvägsföretag. Med säkerhet avses i lagstiftningen främst frågor om att förebygga och undvika olyckor och skador till följd av järnvägsverksamhet. De olika delsystem och komponenter som ingår i järnvägssystemet ska utöver säkerhet i denna mening även uppfylla krav på bland annat tillförlitlighet och tillgänglighet. Motsvarande lagstiftning med krav på säkerhet finns även för tunnelbane- och spårvägssystem.[129] Anläggningar som används för transporter kan, i likhet med infrastruktur inom andra samhällssektorer, klassas som skyddsobjekt.[130] (Lindgren, 2013)

Ovanstående uppgifter gäller fortfarande

8.2 Övriga regler och bestämmelser

Berörda nationella myndigheter är främst Transportstyrelsen och Trafikverket. Transportstyrelsen är central tillsynsmyndighet inom området och ska övervaka järnvägssystemens säkerhet. Transportstyrelsen utformar föreskrifter och regler, kontrollerar regelefterlevnad och utfärdar olika typer av tillstånd. Trafikverket ansvarar för långsiktig planering av transportsystemet för alla trafikslag samt för byggande, drift och underhåll av statliga vägar och järnvägar. I de regelverk som Transportstyrelsen ansvarar för inom området ingår det föreskrifter om säkerhetsstyrningssystem och övriga säkerhetsbestämmelser.[131] För tunnelbana och spårväg finns motsvarande regler om en så kallad säkerhetsordning.[132] I dessa föreskrifter finns inga direkta hänvisningar till de informations- och styrsystem som utnyttjas i spårbunden trafik. I trafikföreskrifterna ingår regler

[128] Järnvägslag (2004:519), 2 kap samt järnvägsförordning (2004:526).
[129] Lag (1990:1157) om säkerhet vid tunnelbana och spårväg och förordning (1990:1165) om säkerhet vid tunnelbana och spårväg.
[130] Skyddslag (2010:305), 4 §, pt 4.
[131] Järnvägsstyrelsens föreskrifter (JvSFS 2007:1) om säkerhetsstyrningssystem och övriga säkerhetsbestämmelser för järnvägsföretag och Järnvägsstyrelsens föreskrifter (JvSFS 2007:2) om säkerhetsstyrningssystem och övriga säkerhetsbestämmelser för infrastrukturförvaltare.
[132] Järnvägsstyrelsens föreskrifter (JvSFS 2007:4) om säkerhetsordning för tunnelbana och spårväg.

om signaler och signalsystem, men dessa handlar i huvudsak om hur signalering ska ske i systemet.[133]

Utöver de krav på sektorn som följer av lagar och förordningar görs det också affärsmässiga överväganden om säkerhet och tillförlitlighet i de system som används för drift och styrning av trafiken. Robusta styrsystem med skydd mot otillbörlig påverkan bidrar till att minska risken för störningar och förseningar i trafiken.

(Lindgren, 2013)

Föreskriften JvSFS 2007:2 (till vilken hänvisas ovan) ersattes först av TSFS 2013:43 som sedan upphävdes den 1 juli 2015 och ersattes av TSFS 2015:34 (Transportstyrelsens föreskrifter om säkerhetsstyrningssystem och övriga säkerhetsbestämmelser för infrastrukturförvaltare med säkerhetstillstånd samt järnvägsföretag med säkerhetsintyg). Likaså har förordningen JvSFS 2007:4 (till vilken hänvisas ovan) upphävts och ersatts av TSFS 2013:44 (Transportstyrelsens föreskrifter om säkerhetsstyrning och säkerhetsordning med säkerhetsbestämmelser inom tunnelbana och spårväg). Ingen av dessa nya föreskrifter innehåller något specifikt om informations- och styrsystem.

Järnvägssektorn är även styrda av EU-direktiv för de delar av järnvägsnätet som sitter ihop med det europeiska järnvägsnätet. Exempelvis finns driftkompabilitetsdirektivet[134], direktivet om säkerhet på gemensamma järnvägar[135] och kommissionens förordning om antagande av en gemensam säkerhetsmetod (CSM-RA)[136] som alla syftar till att det ska vara lättare för järnvägstrafiken att passera nationsgränserna. Direktiven handlar framför allt om säkerhetsfrågor (safety) och standardisering. De nämner ingenting om IT-säkerhet, men indirekt finns det kopplingar dit.[137]

8.3 Hur frågorna har uppmärksammats inom sektorn

Trafikverket har under 2013 gjort en revision av hur myndighetens styrande dokument för informationssäkerhet har efterlevts med fokus på kritiska operativa system för trafikledning och eldrift. Under våren 2013 blev systemen för trafikledning rent formellt klassificerade som it-system inom Trafikverket. Dessa är primärt byggda för att ha hög driftsäkerhet. Informationssäkerhet har inte varit

[133] Järnvägsstyrelsens trafikföreskrifter (JvSFS 2008:7), bilaga 3 Signaler, system.
[134] Europaparlamentets och rådets direktiv 2008/57/EG.
[135] Europarådets och parlamentets direktiv 2004/49/EG.
[136] Kommissionens förordning (EG) nr 352/2009.
[137] Personlig kommunikation med Johan Andersson, Trafikverket, 2015-12-06.

prioriterat. I och med att systemen bli mer exponerade mot yttervärlden genom att de i större utsträckning kopplas ihop med andra system, och i och med övergången till IP-kommunikation, så finns det skäl att se över informationssäkerheten. Revisionen resulterade i totalt 21 observationer varav merparten berör brister beträffande informationssäkerhetsanalyser, riskhantering och kontinuitetsplanering. Dessutom noterades allvarliga brister avseende bemanning av systemtekniker, hantering av behörigheter och konton samt i datorhallar.[138]

Inom ramen för NCS3 har en kartläggning genomförts av vilka informations- och styrsystem som behövs för att bedriva järnvägstrafik på Trafikverkets järnvägsnät. Rapporten beskriver övergripande hur den spårbundna trafiken utnyttjar olika typer av informations- och styrsystem, vilken information som flödar mellan systemen och vilka potentiella sårbarheter som finns.[139]

[138] Revisionsrapport. Informationssäkerhet i operativ verksamhet, Trafikverket, 2014, TRV 2013/86848.

[139] Mossberg Sonnek, K., Holm, H., Lindgren, J., Lindgren, F. och Westring, E., NCS3 – Informations- och styrsystem inom spårbunden trafik, 2015, FOI-R--4029—SE, MSB 2014-1131.

9 Elektroniska kommunikationer

Även om de system som används för drift och styrning av elektroniska kommunikationer inte omedelbart påverkar några fysiska processer så kan avbrott i tele- eller datatrafik indirekt innebära störningar inom andra sektorer. Underlaget i detta avsnitt ger en kortfattad orientering av arbetet med säkerhet i styr- och informationssystemen inom sektorn. (Lindgren, 2013)

Ovanstående uppgifter gäller fortfarande.

9.1 Tillämplig lagstiftning

Lagen om elektronisk kommunikation reglerar hur information ska hanteras i elektroniska medier och vänder sig främst till telekommunikationsoperatörer.[140] Enligt lagen ska den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ”vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet”.[141] Det ställs också krav på åtgärder för att skydda uppgifter som hanteras i de elektroniska näten med hänsyn till användarnas integritet. (Lindgren, 2013)

Ovanstående uppgifter gäller fortfarande.

9.2 Övriga regler och bestämmelser

Ansvarig nationell myndighet är Post- och Telestyrelsen (PTS), som utifrån bestämmelserna i lagen om elektronisk kommunikation utarbetat allmänna råd om god funktion och teknisk säkerhet.[142] De allmänna råden tar upp vikten av ett systematiskt säkerhetsarbete, riskanalys och hantering samt planering för avbrott och störningar, men anger inte några specifika råd om drift- och styrsystemen. På sin webbplats lyfter PTS fram ”intrång i teleoperatörernas styr- och övervakningsnät med stödsystem” som ett fredstida hot mot landets telekommunikationer.[143] (Lindgren, 2013)

I juni 2015 fattade PTS styrelse beslut om nya föreskrifter om driftsäkerhet. Förordningen PTSFS 2007:2 (till vilken hänvisas ovan) kommer därför att

[140] Lag (2003:389) om elektronisk kommunikation.p
[141] Ibid, 5 kap., 6b §.
[142] Post- och Telestyrelsens allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid, PTSFS 2007:2.
[143] www.pts.se/sv/Bransch/Internet/Robust-kommunikation/Hotbilder, 2015-11-16.

upphävas den 1 januari 2016 och ersattes av PTSFS 2015:2 (Post- och telestyrelsens föreskrifter om krav på driftsäkerhet).

De nya föreskrifterna förtydligar vilka åtgärder som tillhandahållare av elektroniska kommunikationsnät och -tjänster ska vidta för att leva upp till lagens krav på en grundläggande driftsäkerhet. I föreskrifterna finns generella krav som gäller för samtliga tillhandahållare och som berör ansvarsförhållanden, dokumentation, skyldighet att vidta skyddsåtgärder och att genomföra kontinuitetsplanering, behörighetsrutiner och övervakning. De generella kraven träder i kraft den 1 januari 2016.

I föreskrifterna finns också mer specifika krav för tjänsteleverantörer, kommunikationsoperatörer och leverantörer av mobila kommunikationsnät och kommunikationstjänster. Dessa krav har bedömts ta längre tid att implementera och därför behöver de inte vara genomförda förrän efter fem år från det att föreskrifterna beslutades, dvs. i juni 2020. De specifika kraven rör redundans och reservkraft och är olika skarpt formulerade beroende på hur många aktiva anslutningar som skulle drabbas av en störning eller avbrott till följd av att en resurs slutar att fungera. Inte heller i de nya föreskrifterna nämns informations- och styrsystem specifikt.[144]

9.3 Hur frågorna har uppmärksammats inom sektorn

Examensarbetet ”Mobil kommunikation och högre tillgänglighet vid längre elavbrott, exemplet stormen Dagmar och 4G-kommunikation inom smarta elnät” av Mattias Lindgren nämner krav på SCADA för ökad tillgänglighet, men tar inte upp något om informationssäkerhet.[145]

PTS:s risk- och sårbarhetsanalys för sektorn elektronisk kommunikation, 2015, tar upp en virusattack som en oönskad händelse. Rapporten nämner att tekniska system kan drabbas men diskuterar inte specifikt informations- och styrsystem.[146]

[144] www.pts.se/sv/Bransch/Internet/God-funktion-och-teknisk-sakerhet, 2015-11-09.
[145] Lindgren, M., Mobil kommunikation och högre tillgänglighet vid längre elavbrott, exemplet stormen Dagmar och 4G-kommunikation inom smarta elnät, 2013, Uppsala universitet, ISSN: 1650-8319, UPTEC STS13 003.
[146] 2015-års risk- och sårbarhetsanalys för PTS och dess ansvarsområden, 2015, PTS, dnr 15-4951.

10 Lagar och bestämmelser inom andra områden

Även inom andra områden kan det finnas lagar som kan påverka vilka krav som ställs på såväl informationssäkerhet i allmänhet som säkerhet i industriella styr- och kontrollsystem. Nedan listas några sådana exempel som dock inte varit föremål för någon närmare analys inom studiens ram:

- Brottsbalkens bestämmelser om *dataintrång*[147], enligt vilka det är förbjudet att olovligen bereda sig tillgång till en uppgift som är avsedd för automatiserad behandling eller att olovligen ändra, utplåna, blockera eller i register föra in en sådan uppgift. Det är heller inte tillåtet att olovligen allvarligt störa eller hindra användningen av en sådan uppgift.
- Lag om skydd för *företagshemligheter*[148] ,dvs. sådan ”information om affärs- eller driftförhållanden i en näringsidkares rörelse som näringsidkaren håller hemlig och vars röjande är ägnat att medföra skada för honom i konkurrenshänseende”. Det bör noteras att denna lag inte omfattar så kallade insiders som medvetet väljer att skada företaget utan endast obehöriga angrepp.
- Lagen om *offentlig upphandling* (LOU) som bland annat reglerar hur kravställning kan göras i offentliga upphandlingar.[149] Frågor av intresse att analysera närmare är i vilka situationer som LOU ska tillämpas och om det finns lägen där andra än myndigheter och kommuner ska tillämpa LOU, t.ex. i egenskap av operatör av en offentligt finansierad verksamhet.
- För *upphandling inom områdena vatten, energi, transporter och posttjänster* finns det en särlagstiftning.[150] Flera av de branscher som ingår i studien omfattas av denna lagstiftning. På motsvarande sätt som vid en genomgång av LOU bör de möjliga formerna för kravställning analyseras samt vilka aktörer som berörs i olika situationer.
- Offentlighets- och sekretesslagen (2009:400).
- Personuppgiftslagen/PUL (1998:204).

(Lindgren, 2013)

Ovanstående uppgifter gäller fortfarande.

[147] Brottsbalk (1962:700), 4 kap 9c §).
[148] Lag (1990:409) om skydd för företagshemligheter.
[149] Lag (2007:1091) om offentlig upphandling och Upphandlingsförordning (2011:1040).
[150] Lag (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster.

11 Diskussion

Elsektorn och vattensektorn har uppmärksammat frågorna om säkerhet i informations- och styrsystem mer än andra sektorer. Det beror enligt flera deltagare i FIDI-SCADA på att det finns enskilda individer som driver frågorna och att dessa har kunnat använda sina respektive branschorganisationer som en plattform i arbetet. Inom elsektorn finns det också ett långt drivet arbete i USA som har fungerat som förebild.

Det är positivt att elsektorn och dricksvattensektorn har uppmärksammat frågorna, men det skulle också vara önskvärt att höja uppmärksamheten inom de övriga sektorerna. Många människor är exempelvis beroende av fjärrvärme, speciellt under vintern, och stora datorhallar är beroende av fjärrkyla under varma sommarperioder. Även om det finns möjlighet att lagra värme och kyla under en viss tid så kan ett längre avbrott få stora konsekvenser. Likaså kan längre avbrott inom den spårbundna trafiken och i elektroniska kommunikationer få stora samhällskonsekvenser.

Utöver myndigheten Svenska kraftnät har branschorganisationerna Svensk Energi och Svenskt Vatten arbetat mycket med frågorna. Sektorerna kemisk processindustri och spårbunden trafik har inte några tydligt utpekade bransch-organisationer vilket kan vara en förklaring till att det är svårare att ta ett samlat grepp kring säkerhetsfrågan där. Utöver myndigheter och branschorganisationer gör även samverkansgrupper och enskilda företag insatser, men det har inte rymts inom ramen för den här studien att kartlägga sådana initiativ.

Den här studien har kartlagt regelverk och krav som är styrande inom olika sektorer. Det skulle vara intressant att även följa upp i vilken grad myndigheterna bedriver tillsyn, det vill säga följer upp att föreskrifterna följs, samt hur det påverkar arbetet inom sektorerna. Det skulle också vara intressant att göra en fördjupad studie i hur olika myndigheter tar upp aspekter av skydd (safety) och säkerhet (security), där det senare inkluderar antagonistiska angrepp, inom ramen för sina föreskrifter. Ytterligare en fråga som skulle kunna belysas djupare är vilka EU-standarder som styr verksamheten inom olika sektorer och hur dessa påverkar arbetet med säkerhet i informations- och styrsystem. En intervjustudie med företrädare för olika branscher, företag och bolag skulle kunna ge en större insikt i dessa frågor.

Det finns samhällssektorer som inte har berörts i den här studien som också är beroende av informations- och styrsystem. En genomgång av regelverk och krav inom dessa sektorer skulle kunna ge en mer heltäckande bild av hur det ser ut i det svenska samhället idag.

Ordlista, juridiska termer

Begrepp	Förklaring
Författning	En *författning* är en av behörig myndighet utfärdad, generellt förpliktande föreskrift. Ordet täcker både *lagar*, som beslutas av riksdagen, och *förordningar*, som beslutas av regeringen, samt *föreskrifter* med skilda beteckningar som beslutas av lägre statliga eller kommunala myndigheter.[151]
Lag	*Lagar* antas av riksdagen och publiceras i SFS (*Svensk författningssamling*). Lagar är de viktigaste *författningarna* i Sverige. Innehållet i en lag är ganska generellt. I förarbetet *proposition* förklaras vad riksdagen vill med lagen.[152]
Förordning	*Förordningar* kompletterar *lagen* och är mer detaljerade. De antas av regeringen. Förordningar publiceras i SFS (*Svensk författningssamling*). [153]
Föreskrift	Vissa statliga myndigheter (drygt hundra enligt lagrummet.se) har av riksdag och regering fått rätt att besluta om *föreskrifter* inom sitt verksamhetsområde. Föreskrifterna kompletterar *lagen* och *förordningarna* och är mer detaljerade än dessa. Föreskrifterna publiceras i myndighetens *författningssamling*.[154,155]
Instruktion	*Instruktionen* är en *författning* som regeringen utfärdar till en myndighet med regler om dess organisation, arbetssätt m.m.[156]
Myndighets författningssamling	*Författningssamlingar* innehåller *föreskrifter* som utges av myndigheter.[157]
Kommittédirektiv	När regeringen tillsätter en statlig utredning för att utreda en fråga så anger de utgångspunkterna för arbetet i ett så kallat *kommittédirektiv*.[158]

[151] www.ne.se, 2015-10-21.
[152] www.notisum.com/News.aspx?itemid=5478, 2015-10-21.
[153] www.notisum.com/News.aspx?itemid=5478, 2015-10-21.
[154] www.notisum.com/News.aspx?itemid=5478, 2015-10-21.
[155] www.lagrummet.se/rattsinformation/myndigheters-foreskrifter, 2015-10-21.
[156] www.ne.se, 2015-10-21.
[157] www.ne.se, 2015-10-21.
[158] www.regeringen.se/ordlista, 2015-10-21.

Statens offentliga utredningar, SOU	Innan regeringen lägger fram ett lagförslag tillsätts ofta en särskild utredare eller en kommitté, som får i uppdrag att utreda en viss fråga. Resultatet samlas i en rapport som kallas betänkande och som publiceras i serien *Statens offentliga utredningar, SOU*.[159]
Proposition	*Propositionen* är ett förslag från regeringen till riksdagen. Propositionerna är riksdagens viktigaste arbetsmaterial och utgör utgångspunkt för flertalet riksdagsbeslut i lagstiftnings- och budgetfrågor.[160]
Regleringsbrev	*Regleringsbrevet* är en skrivelse från regeringen till en myndighet som beskriver hur de anslag som riksdagen har beviljat ska förfogas av myndigheten.[161]
Svensk författningssamling, SFS	*Svensk författningssamling*, *SFS*, innehåller gällande *lagar* och *förordningar*, d.v.s. författningar utgivna av riksdagen och regeringen.[162]
EU-förordning	Gäller direkt som *lag* i ett medlemsland.[163]
EU-direktiv	Innehåller gemensamma mål. Varje land avgör själv vilka *lagar* som krävs för att uppnå målen. [164]

[159] www.regeringen.se/ordlista, 2015-10-21.
[160] www.ne.se, 2015-10-21.
[161] www.ne.se, 2015-10-21.
[162] www.riksdagen.se/sv/Dokument-lagar/lagar/svenskforfattningssamling, 2015-10-21.
[163] www.eu-upplysningen.se/Om-EU/Om-EUs-lagar-och-beslutsfattande/Olika-typer-av-EU-lagar 2015-12-01.
[164] www.eu-upplysningen.se/Om-EU/Om-EUs-lagar-och-beslutsfattande/Olika-typer-av-EU-lagar, 2015-12-01.

Referenser

Inledning

Rapporter, artiklar och dokument

Lindgren, F. (2013). Regelverk och krav inom området säkerhet i industriella informations- och styrsystem. FOI Memo 4415.

Webbsidor

www.eu-upplysningen.se
www.notisum.se

Sammanfattning och slutsatser

Sektorsövergripande

Lagar

SFS 1996:627	Säkerhetsskyddslag

Förordningar

SFS 1996:633	Säkerhetsskyddsförordningen

Föreskrifter

Försvarsmakten	
FFS 2015:2	Försvarsmaktens föreskrifter om säkerhetsskydd
MSB	
MSBFS 2009:10	Föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet
Rikspolisstyrelsen	
RPSFS 2010:3, FAP 244-1	Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd

Upphävda föreskrifter

Försvarsmakten	
FFS 2003:7	Försvarsmaktens föreskrifter om säkerhetsskydd (ersatt av FFS 2015:2)

Utredningar

SOU 2015:23	Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten
SOU 2015:25	En ny säkerhetsskyddslag

Kommittédirektiv

Dir. 2011:94	En modern säkerhetsskyddslag
Dir. 2013:110	Strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system

Skrivelser

Skr. 2009/10:124	Samhällets krisberedskap – stärkt samverkan för ökad säkerhet
Ju2015/2650/SSK	Remiss av betänkandet SOU 2015:23 Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten

Rapporter, artiklar och dokument

MSB (2013:1). Vägledning för fysisk informationssäkerhet i it-utrymmen, MSB629.

MSB (2013:2). Handlingsplan för skydd av samhällsviktig verksamhet, MSB597.

MSB (2014:1). Samverkansgruppen för informationssäkerhet, SAMFI, faktablad, publ.nr. MSB286.

MSB (2014:2). En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter, publ.nr. MSB740.

MSB (2014:3). Konsekvensutredning rörande reviderade föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet, dnr 2014-6391.

MSB (2014:4). Vägledning till ökad säkerhet i industriella informations- och styrsystem, publ.nr: MSB718.

MSB (2014:5). Guide to Increased Security in Industrial Information and Control Systems, Order No: MSB766.

MSB (2015). FIDI-SCADA, Forum för informationsdelning kring säkerhet i industriella informations- och styrsystem, publ.nr: MSB889.

Riksrevisionsverket (2014). Informationssäkerheten i den civila statsförvaltningen, RiR 2014:23.

Veibäck, E., Malmberg Andersson F. och Carlsson, E. (2014). Informations- och cybersäkerhet i nationell risk- och förmågebedömning – diskussion och presentation av en tankemodell, FOI memo 5100.

Webbsidor

www.informationssakerhet.se
www.kth.se
www.notisum.se
www.rics.se

Elproduktion och eldistribution

Lagar

SFS 1996:627	Säkerhetsskyddslag
SFS 1997:288	Elberedskapslag
SFS 1997:857	Ellag
SFS 2003:778	Lag om skydd mot olyckor
SFS 2010:305	Skyddslag

Förordningar

SFS 1997:294	Förordning om elberedskap

Föreskrifter

Svenska kraftnät

SvKFS 2005:2	Affärsverket svenska kraftnäts föreskrifter och allmänna råd om driftsäkerhetsteknisk utformning av produktionsanläggningar
SvKFS 2013:1	Affärsverket svenska kraftnäts föreskrifter och allmänna råd om säkerhetsskydd
SvKFS 2013:2	Affärsverket svenska kraftnäts föreskrifter och allmänna råd om elberedskap

Strålsäkerhetsmyndigheten

SSMFS 2008:1	Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om säkerhet i kärntekniska anläggningar
SSMFS 2008:12	Strålsäkerhetsmyndighetens föreskrifter om fysiskt skydd av kärntekniska anläggningar
SSMFS 2008:17	Strålsäkerhetsmyndighetens föreskrifter om konstruktion och utförande av kärnkraftsreaktorer

SSMFS 2014:3	Föreskrifter om ändring i Strålsäkerhetsmyndighetens föreskrifter (SSMFS 2008:1) om säkerhet i kärntekniska anläggningar

Upphävda föreskrifter

Svenska kraftnät

SvKFS 1997:2	Upphävd av SvKFS 2013:2
SvKFS 2000:2	Upphävd av SvKFS 2013:2
SvKFS 2005:1	Upphävd av SvKFS 2013:1

Utredningar

SOU 2014:84	Planera för effekt! Slutbetänkande från Samordningsrådet för smarta elnät

Rapporter, artiklar och dokument

Malmgren R. och Johansson, E. (2014). Rapport rörande säkerhet i smarta elnät.

Norstedt, D., Persson, S. och Ny, T. (2015). Funktionskrav på framtidens elmätare, Energimarknadsinspektionen, R2015:09.

Svenska kraftnät (2011:1). Beslut om Svenska Kraftnäts FoU-plan 2012-2014.

Svenska kraftnät (2011:2). Förstudierapport Svenska Kraftnät 2011 – Branschens behov av stöd inom informationssäkerhetsområdet, dnr 2011/1199.

Svenska kraftnät (2013). Hotkatalog för Elbranschen Hot mot IT-, informationshantering, processkontroll och automation, Version 1.0, dnr: 2012/331.

Svenska kraftnät (2014:1). Risk- och sårbarhetsanalys för år 2014, Affärsverket svenska kraftnät, Dnr: Svk 2013/2082.

Svenska kraftnät (2014:2). Forsknings- och utvecklingsplan 2015 – 2017, Svenska kraftnät, nr 2014/2257.

Svenska kraftnät (2014:3). Vägledning för informations- och IT-säkerhet samt säkerhetsskydd.

Svenska kraftnät (2015:1). Risk- och sårbarhetsanalys för år 2015, ärendenr: 2015/1763.

Svenska kraftnät (2015:2). IT-säkerhetsarkitektur. En vägledning för elbranschen med typexempel och referenslösningar.

Svenska kraftnäts tekniska riktlinjer:

TR2-03-2	Standarder och generella krav
TR2-03-3	Datorer i kontrollanläggning
TR2-04-2	Människa Maskin Kommunikation
TR2-04-3	Fjärrkontroll och RTU:er
TR2-10-1	Dokumentation kontrollutrustningar
TR4-02	Tekniska riktlinjer IT-säkerhet
TR 9-14	Tillträdes- och fotobestämmelser för Svenska Kraftnäts anläggningar

Webbsidor

www.svk.se
www.energisakerhetsportalen.se
www.opensecurityarchitecture.org
www.stralsakerhetsmyndigheten.se
www.swedishsmartgrid.se

Dricksvattenproduktion och vattendistribution

Lagar

SFS 2006:412	Lag om allmänna vattentjänster
SFS 2006:804	Livsmedelslag
SFS 2010:305	Skyddslag

Förordningar

SFS 1998:808	Miljöbalk
SFS 1998:899	Förordning om miljöfarlig verksamhet och hälsoskydd
SFS 2006:813	Livsmedelsförordning
SFS 2014:1526	Tillkännagivande om de EU-bestämmelser som kompletteras av livsmedelslagen

Föreskrifter

Livsmedelsverket

SLVFS 2001:30	Livsmedelsverkets föreskrifter om dricksvatten
LIVSFS 2008:13	Livsmedelsverkets föreskrifter om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar

LIVSFS 2011:3	Föreskrifter om ändring i Livsmedelsverkets föreskrifter (SLVFS 2001:30) om dricksvatten
LIVSFS 2013:4	Föreskrifter om ändring i Livsmedelsverkets föreskrifter (SLVFS 2001:30) om dricksvatten
LIVSFS 2013:5	Föreskrifter om ändring i Livsmedelsverkets föreskrifter (LIVSFS 2008:13) om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar

Rapporter, artiklar och dokument

Johansson, E. (2010). Kartläggning av SCADA-säkerhet inom svensk dricksvattenförsörjning, framtagen inom MSB:s program tillsammans med Svenskt Vatten.

SLV, SJV, SVA, Länsstyrelsen, SKL samt Generalläkaren. Nationell plan för kontrollen i livsmedelskedjan 2015-2018. Del 4, Organisation, revision och fördjupning inom planens olika områden. Det står inget årtal eller rapportnummer i dokumentet.

Riksrevisionen (2008). Dricksvattenförsörjning – beredskap för stora kriser, RiR 2008:8.

SLV (2012). Vägledning: Dricksvatten – åtgärder mot sabotage och annan skadegörelse, Livsmedelsverket.

Svenskt Vatten (2011:1). Råd och riktlinjer – Fysiskt och tekniskt skydd för dricksvatten.

Svenskt Vatten (2011:2). Råd och riktlinjer för ansvariga inom dricksvattenproduktion.

Svenskt Vatten (2012). Säkerhetshandbok för dricksvattenproducenter.

Webbsidor

www.svensktvatten.se
www.foi.se

Fjärrvärme/-kyla – produktion och distribution

Lagar

SFS 1977:1160	Arbetsmiljölag
SFS 2008:263	Fjärrvärmelag

Förordningar

SFS 1962:700	Brottsbalk
SFS 1970:994	Jordabalk
SFS 1998:808	Miljöbalk
SFS 2007:1118	Förordning med instruktion för Energimarknadsinspektionen

Föreskrifter

Arbetsmiljöverket

AFS 2002:1	Användning av trycksatta anordningar

Rapporter, artiklar och dokument

Mossberg Sonnek, K. och Lindgren, F. (2015). Industriella informations- och styrsystem inom fastighetsautomation – en förstudie, FOI Memo 5405.

Svensk Fjärrvärme (2004). Säkerhet i fjärrvärmeanläggningar – Regler och råd för riskbedömning, rapport nr 2004:2.

Webbsidor

www.lansstyrelsen.se
www.svenskfjarrvarme.se

Kemisk processindustri

Lagar

SFS 1977:1160	Arbetsmiljölag
SFS 2003:778	Lag om skydd mot olyckor
SFS 2003:789	Förordning om skydd mot olyckor
SFS 1999:381	Lag om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor
SFS 2010:1011	Lag om brandfarliga och explosiva varor

Förordningar

SFS 1977:1166	Arbetsmiljöförordning
SFS 1998:808	Miljöbalk
SFS 1998:899	Förordning om miljöfarlig verksamhet och hälsoskydd
SFS 1998:901	Förordning om verksamhetsutövares egenkontroll
SFS 2010:1075	Förordning om brandfarliga och explosiva varor
SFS 2011:13	Miljötillsynsförordning
SFS 2015:236	Förordning om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor

Upphävda förordningar

SFS 1998:900	Upphävd av SFS 2011:13
SFS 1999:382	Upphävd av SFS 2015:236

Föreskrifter

Arbetsmiljöverket

AFS 2014:44	Arbetsmiljöverkets föreskrifter om upphävande av föreskrifterna (AFS 2005:19) om förebyggande av allvarliga kemikalieolyckor

MSB

MSBFS 2015:8	Myndigheten för samhällsskydd och beredskaps föreskrifter om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor

Upphävda föreskrifter

Arbetsmiljöverket

AFS 2005:19	Upphävd av AFS 2014:44, ersatt av MSBFS 2015:8

Räddningsverket

SRVFS 2005:2	Upphävd av MSBFS 2015:8

EU-direktiv

2012/18/EU	Europaparlamentets och rådets direktiv 2012/18/EU, det s.k. Seveso III-direktivet

Rapporter, artiklar och dokument

MSB (2014). Konsekvensutredning avseende förslag till myndigheten för samhällsskydd och beredskaps föreskrifter om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor, dnr 2014-5577.

Roffey, R., Ryghammar, L. och Trané, C. (2014). Förslag till regional samordning av tillsyn för Sevesoverksamheter, FOI Memo 5083.

Webbsidor

www.seveso.se

Spårbunden trafik

Lagar

SFS 1990:1157	Lag om säkerhet vid tunnelbana och spårväg
SFS 2004:519	Järnvägslag
SFS 2010:305	Skyddslag

Förordningar

SFS 1990:1165	Förordning om säkerhet vid tunnelbana och spårväg
SFS 2004:526	Järnvägsförordning

Föreskrifter

Transportstyrelsen

JvSFS 2007:1	Järnvägsstyrelsens föreskrifter om säkerhetsstyrningssystem och övriga säkerhetsbestämmelser för järnvägsföretag
JvSFS 2008:7	Järnvägsstyrelsens trafikföreskrifter
TSFS 2013:44	Transportstyrelsens föreskrifter om säkerhetsstyrning och säkerhetsordning med säkerhetsbestämmelser inom tunnelbana och spårväg
TSFS 2015:34	Transportstyrelsens föreskrifter om säkerhetsstyrningssystem och övriga säkerhetsbestämmelser för infrastrukturförvaltare med säkerhetstillstånd samt järnvägsföretag med säkerhetsintyg

Upphävda föreskrifter

Transportstyrelsen

JvSFS 2007:2	Ersatt av TSFS 2013:43 som sedan upphävdes genom TSFS 2013:34
JvSFS 2007:4	Ersatt av TSFS 2013:44
TSFS 2013:43	Upphävd genom TSFS 2013:34

EU-direktiv

Europaparlamentets och rådets direktiv 2008/57/EG
Europarådets och parlamentets direktiv 2004/49/EG
Kommissionens förordning (EG) nr 352/2009

Rapporter, artiklar och dokument

Mossberg Sonnek, K., Holm, H., Lindgren, J., Lindgren, F. och Westring, E. (2015). NCS3 – Informations- och styrsystem inom spårbunden trafik, FOI-R--4029—SE, MSB 2014-1131.

Trafikverket (2014). Revisionsrapport. Informationssäkerhet i operativ verksamhet, TRV 2013/86848.

Elektroniska kommunikationer

Lagar

SFS 2003:389	Lag om elektronisk kommunikation

Föreskrifter

Post- och telestyrelsen

PTSFS 2007:2	Post- och telestyrelsens allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid; upphävs den 1 jan 2016 av PTSFS 2015:2
PTSFS 2015:2	Post- och telestyrelsens föreskrifter om krav på driftsäkerhet; gäller fr.o.m. den 1 jan 2016

Rapporter, artiklar och dokument

Lindgren, M. (2013). Mobil kommunikation och högre tillgänglighet vid längre elavbrott, exemplet stormen Dagmar och 4G-kommunikation inom smarta elnät, Uppsala universitet, ISSN: 1650-8319, UPTEC STS13 003.

PTS (2105). 2015-års risk- och sårbarhetsanalys för PTS och dess ansvarsområden, dnr 15-4951.

Webbsidor

www.pts.se

Lagar och bestämmelser inom andra områden

Lagar

SFS 1990:409	Lag om skydd för företagshemligheter
SFS 1998:204	Personuppgiftslag
SFS 2007:1091	Lag om offentlig upphandling
SFS 2007:1092	Lag om upphandling inom områdena vatten, energi, transporter och posttjänster
SFS 2009:400	Offentlighets- och sekretesslag

Förordningar

SFS 1962:700	Brottsbalk
SFS 2011:1040	Upphandlingsförordning

Diskussion

Ordlista

Webbsidor

www.eu-upplysningen.se
www.lagrummet.se
www.ne.se
www.notisum.se
www.regeringen.se
www.riksdagen.se

Security in Industrial Control Systems

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

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

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

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

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

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

www.msb.se