2012-03-26
Dnr: 2011/1199

Förstudierapport Svenska Kraftnät 2011

Branschens behov av stöd inom informations-säkerhetsområdet

Övergripande sammanfattning

Förstudien har pågått under hösten 2011 och har under den tiden samverkat med en stor mängd företrädare för elbranschen. Härvid har förstudiens syfte varit att inventera och kartlägga de behov av stöd inom IT- och informationssäkerhetsområdet som föreligger hos svenska elföretag.

Vidare har förstudien samverkat med ett stort antal myndigheter som på olika har beröringspunkter med elbranschen inom säkerhetsområdet. Förstudien har på detta sätt säkerställt att kommunikationsvägar för samverkan är etablerade inför ett införandeprojekt där Svenska Kraftnät skall bemöta de behov som identifierats, och genom samverkan med andra myndigheter validerats, inom ramen för förstudien.

Förstudiearbetet har bedrivits i form av arbetsmöten, seminarier, enkätundersökningar och intervjuer.

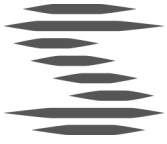
De områden som getts stor tyngd inom ramen för förstudien är följande.

- Riskanalyser
  Ett stort behov av stöd föreligger inom riskanalysområdet. Härvid kan särskilt nämnas att elföretagen brister i tillämpning av riskanalys för att underbygga säkerhetsanalyser enligt 5 § säkerhetsskyddsförordningen (1996:633).

- Förtydliganden av lagar och andra rättsliga krav
  Tolkning och tillämpning av lagar och andra rättsliga krav divergerar stort inom branschen. Förstudien har därför identifierat ett behov av ensning och förtydliganden inom området.

- Instruktioner, checklistor, handböcker och mallar
  Inom ramen för förstudien står det klart att branschen är i ett stort behov av ensade riktlinjer i form av exempelvis mallar, checklistor, handböcker och övriga instruktioner. Denna punkt är även kopplad till föregående punkt om lagar och andra rättsliga krav.

- Säkerhetsarkitektur
  Företrädare för elbolagen efterlyser en referensarkitektur för att bättre kunna utforma och bedöma sina egna IT-arkitekturer. Förstudien bekräftar detta behov och identifierar att Svenska Kraftnät kan utforma funktionella krav på sådana arkitekturer. En renodlad teknisk referensarkitektur bör dock rimligen tas fram av andra aktörer, exempelvis branschorganisationer, med stöd av Svenska Kraftnät.



Innehåll

Bilagor

Bilaga 1 – Lagar och andra rättsliga krav
Bilaga 2 – Rapport från webbenkät
Följande bilagor endast inom SvK
Bilaga 3 – Utkast projektdirektiv
Bilaga 4 – Förteckning över personer som deltagit i eller bidragit till förstudien

1 Inledning

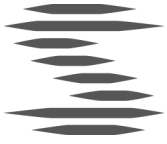
1.1 Bakgrund

Elbolag är beroende av information som hanteras med stöd av IT för centrala verksamhetsprocesser såsom elproduktion och eldistribution, såväl som viktiga stödprocesser som övervakning, fakturering och kontorsautomation. All verksamhet som bedrivs är på ett eller annat sätt beroende av att information hanteras, kommuniceras och bearbetas på ett korrekt sätt. Merparten av informationen hanteras i IT-system men det är härvid viktigt att påpeka att ur ett säkerhetsperspektiv så är IT-säkerhet en delmängd av informationssäkerhet. Mycket av fokus i denna rapport ligger på IT-säkerhet men detta beror till stor del på att den tekniska hotbilden under senare år har eskalerat med oroande hastighet.

Traditionellt så har IT-system som används inom produktion och distribution inom elbranschen varit specialsystem från fackleverantörer. Detta har ändrats över tid då dessa leverantörer valt att nyttja standardkomponenter såsom PC-baserad hårdvara, Windows-baserad mjukvara och TCP/IP-baserad kommunikationsteknologi. Anledningarna till detta är många, bland annat besparingar vid utveckling och underhåll. Denna övergång till standardlösningar innebär samtidigt att de säkerhetsproblem som påverkar kontors-IT-världen nu också kommer över till och påverkar automationsvärlden.

IS/IT-säkerhet är ett ständigt aktuellt område där hotbilden ständigt förändras, nya angreppsmetoder utvecklas konstant och där existerande skydd kan föråldras snabbt. Det är viktigt att se helheten ur ett informationssäkerhetsperspektiv. Det är inte alltid som de bästa åtgärderna är tekniska. De kan lika gärna vara av administrativ eller organisatorisk karaktär. Det viktigaste är att helheten ges erforderlig uppmärksamhet så att inte enskilda åtgärder riskerar att, endera bli verkningslösa på grund av bristande helhetssyn till problematiken eller att de medför hinder för annan verksamhet genom tillförda begränsningar.

Förutom förändringar på hot- och angreppssidan så sker även löpande ändringar i elföretagens verksamheter som är beroende av en sund informationssäkerhet. IT-miljön ute hos elbolag har förändrats, från att styrsystem och driftcentraler varit separerade IT-miljöer till ett nuläge där dessa mer eller mindre integrerats med den ordinarie IT-miljön och den därtill kopplade övriga informationshanteringen. Detta kan bero på behov att skicka ut driftdata såsom miljö- och utsläppsmätningar, statistik eller kostnadsunderlag eller möjligheten att ta in styr- och reglerinformation från



andra system som finns inom organisationen men medför stora utmaningar vad gäller informationssäkerheten.

Den svenska elbranschen, inkluderat myndigheter och energibolag, har under många år aktivt arbetat med olika IS/IT-säkerhetsfrågor. Arbetet har ofta fokuserat på enskilda system av särskild betydelse eller på enskilda riskanalyser.

I ett annat projekt som Svenska Kraftnät genomfört 2011, "Kraftsamling 2011", tillsammans med elföretagen har Svenska Kraftnät undersökt elbranschens olika risker och riskscenarion. En av slutsatserna från detta projekt var att branschen som helhet ansåg att IS/IT-frågorna inte lyfts fram i tillräckligt stor omfattning, vad det gäller hot och risker.

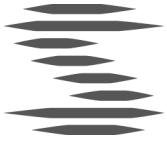
Att IT-system i sig själva är ett mål för aktörsbaserade angrepp är klarlagt. Lika självklart i en modern organisation är att IT-system kan drabbas av oriktade angrepp i form av skadlig kod som bara ”råkat smitta” just dessa system. Samhällskritisk infrastruktur, som elleverans kan betecknas, är ett område som tilldrar sig alltmer intresse som potentiellt mål för olika angripare. Olika internationella och nationella utredningar pekar ut kritisk infrastruktur och kritiskt informationsinfrastruktur som måltavlor.

Förstudien fokuserar på förmåga och funktion för upprätthållande av elleverans, vilket i sin tur är beroende av förmåga och funktion i den befintliga informationshanteringen. Om IT-stöden frånfaller eller om de inte är tillitbara, t.ex. på grund av att datorer är infekterade av skadlig kod, så kommer även funktionen och berörd information att påverkas. För samhällskritisk infrastruktur så måste förmåga och funktion vara högt prioriterade egenskaper.

Myndigheten för samhällsskydd och beredskap slår i sin "strategi för samhällets informationssäkerhet 2010-2015" fast att IT är en bärande komponent inom bl.a. energiområdet. I punkterna fyra och fem, som är utpekade områden, så framhålls att säkerhet i kommunikation och produkter/system som används inom kritiska funktioner är särskilt skyddsvärda.

Utdrag ur strategin.

> *4. Kommunikationssäkerhet*
> *Informationshantering sker regelmässigt mellan fler aktörer vilket ställer krav på säker kommunikation över tele- och datanät. Exempelvis är Internet bärare av en stor andel av vårt informationsflöde.*



Det är viktigt i detta sammanhang att ha robusta kritiska funktioner i infrastrukturen för elektronisk kommunikation och att det finns säkra kryptografiska funktioner och signalskydd. För förtroende- fullt informationsutbyte är det också nödvändigt att elektroniska tjänster bygger på väl fungerande och säkra system.

5. Säkerhet i produkter och system
Långsiktig försörjning av säkra IT-produkter ställer krav på formella ramverk för evaluering och certifiering av säkerhetsegenskaper. Sådana ramverk bör vara nationellt och internationellt accepterade.

Inom området industriella kontrollsystem för samhällsviktiga verksamheter – exempelvis el- och vattendistribution samt spårbunden trafik och petrokemisk industri – används IT-system för att styra och övervaka de centrala fysiska processerna. Det är av stor vikt att dessa system har en hög säkerhet.

Inom förstudien har vi tagit till oss denna övergripande strategi för det svenska samhället och konstaterar att arbetet som Svenska Kraftnät planerar ligger helt i linje med MSB:s strategi. Förstudiens förslag till projektaktiviteter kommer att återspegla detta.

1.2 Syfte och mål

1.2.1 Förstudiens syfte

Att kartlägga elbranschens behov av stöd inom området IS/ITS.

Prioritera identifierade åtgärdsförslag.

Identifiera Svenska Kraftnäts ansvar och mandat för genomförande av åtgärder.

Ge underlag för kort- och långsiktig verksamhetsplanering.

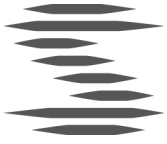
1.2.2 Förstudiens mål

Svenska Kraftnät skall stödja elbranschens fortsatta utveckling inom området IS/ITS

1.3 Bemanning och personal som deltagit i övrigt

1.3.1 Förstudiens bemanning

Den fasta personal som ingått i förstudien har varit



Robert Malmgren	Förstudieledare, konsult Romab
Alireza Hafezi	Informationssäkerhetschef Svenska Kraftnät (uppdragsbeställare)
Thomas Kårgren	Konsult Ekelöw

1.4 Tidplan

Förstudien påbörjades i augusti 2011 och slutlevereras den sista december 2011.

1.5 Leverabler

Resultatet från förstudien sammanställs i detta dokument ”Förstudierapport Svenska Kraftnät 2011 Branschens behov av stöd inom informationssäkerhetsområdet”.

Inom ramen för denna rapport skall även framgå nödvändiga underlag för projektdirektiv för införandeprojekt under 2012.

2 Förutsättningar

2.1 Avgränsningar

Förstudien avgränsas från sådant som relaterar sig till:

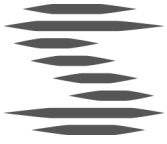
- Fysisk säkerhet
  Anläggningars beskaffenhet med avseende på fysisk säkerhet, i.e. byggnadstekniska skyddsåtgärder och liknande.

- Specifik tillämpning som faller under annan myndighets ansvar.

I övrigt görs inga definitiva avgränsningar då hotbilden ständigt förändras och gränserna exempelvis mellan vad som kan anses utgöra ett styrsystem och vad som är ett kontorsstödjande system får anses vara flytande. Inte minst på grund av den ökade integrationen och systemkonsolideringen.

2.2 Lagar och rättsliga krav

Normerande för Svenska Kraftnäts kravställning mot elsektorns arbete med IT och informationssäkerhet är de befintliga regelverk och rättsliga krav som finns. I bilaga 1 återfinns ett utdrag ur tillämplig lagstiftning och övriga rättsliga krav som påverkar eller kan påverka denna verksamhet. Härvid bör särskilt nämnas att



säkerhetsskyddslagstiftningen endast är tillämplig då berört elföretags verksamhet rör rikets säkerhet eller skyddet mot terrorism. Detta i sin tur vederläggs genom att genomföra en säkerhetsanalys enligt 5 § säkerhetsskyddsförordningen (1996:633).

Inom ramen för förstudien har säkerhetsanalys identifierats som ett problemområde. Detta främst som följd av att tolkningen av hur en sådan analys skall genomföras varierar stort mellan olika elbolag. Det är även ett problem då de säkerhetsanalyser som faktiskt genomförs oftast utförs av säkerhetsskyddschefen och då har fokus på det rent fysiska skyddet och infiltrationsskyddet. Informationssäkerhetsfrågor och IT-säkerhetsfrågor lämnas oftast därhän i detta sammanhang.

Läsaren bör, för att till fullo tillgodogöra sig de resonemang som förs i denna rapport, läsa bilaga 1.

2.2.1 Ändringar i lagstiftningen

Det pågår arbete med att revidera svensk lagstiftning inom de områden som kan ha påverkan för det kommande projektarbetet i allmänhet och IS/IT-säkerhetsfrågorna inom elförsörjningsområdet i stort.

Elberedskapslagen (1997:288)

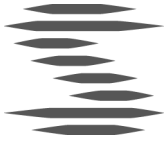
Det pågår sedan 2009-05-28 ett arbete med ändring av elberedskapslagen (1997:288) där Svenska Kraftnät varit drivande i frågan. Nuvarande lagrådsremiss anger följande i 1 §.

> *”Denna lag innehåller bestämmelser om beredskap vid produktion och överföring av el samt vid handel med el. Bestämmelserna reglerar ansvaret för den planering och de övriga åtgärder som behövs för att tillgodose elförsörjningen i landet vid situationer som innebär svåra påfrestningar på samhället.”*

Kursiv text anger förändring mot föregående del av lagtexten med lydelsen ” *höjd beredskap enligt lagen (1992:1403) om totalförsvar och höjd beredskap”*.

Förändringar i elberedskapslagen är ännu inte beslutade men för närvarande tyder allt på att förändringarna kommer att innebära en ändring i syftet med lagen som flyttar fokus från höjd beredskap och krigsfara till just *situationer som innebär svåra påfrestningar på samhället.*

Kommande förändring i elberedskapslagen bedöms få stor påverkan på hur elbolagen måste hantera beredskapsfrågor. I framtiden kan beredskapsåtgärder komma att



sättas in som följd av exempelvis kraftiga stormar, IT-baserade angrepp eller fel, terroraktioner, olyckor m.m. Denna förändring kommer att kräva ett förändrat förhållningssätt till beredskapsfrågor och kommer att ställa högre krav på att insatser och åtgärder kopplade till sådana frågor övas och prövas på en återkommande basis.

Säkerhetsskyddslagstiftningen
Enligt beslut vid regeringssammanträde den 8 december 2011 så kommer en särskild utredare att göra en översyn av säkerhetsskydds-lagstiftningen. Syftet är främst att bättre anpassa lagstiftningen till det som krävs för att skydda verksamhet som har betydelse för rikets säkerhet och till de krav det internationella samarbetet ställer.

Utdrag ur kommittédirektiv 2011:94

”Utredaren ska bl.a.

- *analysera vilka verksamheter som är av betydelse för rikets säkerhet eller som behöver skyddas mot terrorism och därför är i behov av säkerhetsskydd,*
- *föreslå hur reglerna om informationssäkerhet, som en del av säkerhetsskyddet, bör vara utformade,*
- *analysera vilka förändringar som kan behövas för att bättre anpassa lagstiftningen till de krav på säkerhetsskydd som ställs i det internationella samarbetet,*
- *analysera hur ett system med säkerhetsklarering kan utformas för svenska förhållanden,*
- *bedöma inom vilka verksamheter registerkontroll till skydd mot terrorism bör få ske,*
- *analysera behovet av förändringar av bestämmelserna om säkerhetsskyddad upphandling,*
- *ta ställning till om kravet på svenskt medborgarskap i säkerhetsskyddslagen bör förändras och*
- *utarbeta nödvändiga författningsförslag.*

Uppdraget ska redovisas senast den 30 april 2014. ”

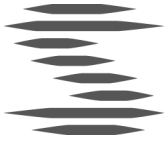
Vidare utdrag ur direktivet.

> *”Arbetsformer och redovisning av uppdraget*
>
> *Utredaren ska hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och utrednings-väsendet, bl.a. Utredningen om förstärkt skydd mot främmande makts underrättelseverksamhet (Ju 2010:03) samt inom internationella organisationer, särskilt EU. Utredaren är oförhindrad att ta upp sådana närliggande frågor som har samband med de frågeställningar som ska utredas.*
>
> *Under genomförandet av uppdraget ska utredaren samråda med och inhämta upplysningar från berörda myndigheter och 19 andra organ, särskilt Säkerhetspolisen, Säkerhets- och integritets-skyddsnämnden, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Post- och telestyrelsen, Affärsverket svenska kraftnät, Transportstyrelsen och Myndigheten för samhällsskydd och beredskap.”*
>
> Svenska Kraftnät har för avsikt att aktivt delta och framställa ändringsbehov kopplade till den problembild som belyses i denna förstudie.

2.3 Hotbild

De hotbilder som i alla snarlika försörjningsverksamheter normalt beaktas är främst olyckor, skadlig kod, miljöpåverkan och sabotage samt kombinationer av sådana hotbilder. I denna förstudierapport redovisas hotbilder översiktligt för att ge en grund för bedömningar som avser behov av skydd i olika nivåer och tillämpningar inom elförsörjningen.

Vad det gäller IS/IT-säkerhet så finns det särskilda omständigheter eller förutsättningar som rör hot. En sådan omständighet är att det hela tiden uppstår ny teknisk utveckling, nya IT-tekniska fenomen, nya användningsfall och därmed också nya hot som uppkommer. Att olika IT-lösningar blir mer och mer komplexa och ogenomträngliga gör det i många fall svårt för gemene man att förstå eller bedöma hotbilder eller konsekvenser. En annan specifik egenskap med IT-hot är potentiell spridningshastighet från det att ett nytt hot har upptäckts tills mängder av system är sårbara för nya attacker.



Olyckor

Detta är ett riskområde som traditionellt sett alltid getts stor uppmärksamhet. I takt med ökade vinstkrav är det dock ofrånkomligt att säkerheten ytterst blir lidande med ökad risk för olyckor som följd.

Reaktor 4 vid kärnkraftverket i Tjernobyl som exploderade efter ett felaktigt utfört test natten mot den 26 april 1986. Reaktorn förstördes vid explosionen och fick en oerhörd påverkan på såväl närliggande miljön som Europa och delar av Centralasien. Uppskattningarna om total dödlighet på grund av olyckan varierar mellan kring tusen och kring en miljon.

Ibland uppstår olyckor som ett resultat av mänskliga fel vid IT-användande. I andra fall uppkommer olyckor på grund av system- eller programvarufel. Det kan vara latenta problem som enbart inträffar under väldigt udda och specifika förhållanden.

Bilderna visar vattenreservoaren vid Taum Sauk vattenkraftverk i bergsområdet St. Francois i Missouri Ozarks cirka 140 km söder om St. Louis, USA.

På morgonen den 14 december 2005 brister en triangulär sektion på den nordvästra sidan av det övre magasinet. Detta medför att 4 miljoner m³ vatten okontrollerat rinner ut ur reservoaren under tolv minuter och orsakar en 7 m hög våg nedför Black River.

Enligt AmerenUE (Amerikanskt energibolag) orsakade ett dataprogram problem i reservoaren genom att fortsätta fylla upp reservoaren även om den redan nått sin normala nivå. Vattnet rann över toppen på vallarna vilket leder till katastrof klockan 05:12 då vallen brister helt.

Det fanns i de rättsliga undersökningarna misstanke om att den mänskliga faktorn spelat en roll i olyckan då handgrepp genomfördes för att kompensera för kända fel i den mjukvara som styrde uppfyllnadsgraden av reservoaren.

Skadlig kod

Elektroniska hot har fått en ökad betydelse främst på grund av två huvudsakliga

orsaker. Förekomsten av skadlig kod som påverkar eller kan påverka industriella styrsystem samt det faktum att elbolagen i syfte att kostnadseffektivisera sin verksamhet till en högre grad integrerar industriella styrsystem med sina övriga kontorssystem och därmed får en högre konnektivitet mot andra aktörer och Internet. Detta ökar exponeringen av de industriella styrsystemen och därmed risknivåerna för dessa. Exempel på skadlig kod som specifikt designats för att attackera sådana system är Stuxnet och dess efterföljare Duqu. Stuxnet är en datamask (trojansk häst) som upptäcktes i juli 2010. Masken anfaller bland annat systemet WinCC som skapades av Siemens för övervakning och styrning av industriprocesser och Siemens S7-utrustning. Stuxnet är konstruerad att slå ut specifika mål, utan att synas eller förstöra något på sin spridningsväg genom ett nät. Syftet med Suxnet:s efterföljare Duqu är enligt företaget Symantec att samla in information och tillgångar från specifika enheter, exempelvis tillverkare av industriella styrsystem, i syfte att göra det lättare att genomföra en framtida attack mot en annan tredje part. Angriparna är ute efter information som designdokument som kan hjälpa dem att lansera en attack mot exempelvis industrisystem. Därför, hävdar Symantec, är Duqu i grunden en föregångare till framtida Stuxnet-liknande attacker.

Irans president Mahmoud Ahmadinejad på besök i Natanz anrikningsanläggning med de Pakistantillverkade centrifugerna P-1 som var målet för en riktad attack med den skadliga koden Stuxnet. Centrifugerna påverkades på två sätt. Dels genom att ändra processen så att anrikningen i sig inte fungerade och dels genom att periodiskt överbelasta centrifugerna så att delar av dessa förstördes.

Aurora är en sårbarhet som gör att cyberattacker som kan sabotera kritiska system som ger el inklusive rikstäckande elnätet. Denna sårbarhet påverkar styrsystem för generatorer, pumpar, turbiner och så vidare. Sårbarheten beror delvis på åtgärder som vidtagits av elbolagen att överföra kontrollen över produktion och distribution utrustning från interna nätverk till övervakande kontroll och datainsamling, eller SCADA, system som kan nås via Internet eller genom telefonlinjer. På detta vis exponeras nämnda resurser för det som kallas Aurora-sårbarheten. Det faktum att sårbarheten är, ur angriparens perspektiv, billig att utnyttja gör dock sårbarheten i sådana styrsystem till ett lockande mål för utpressare, terrorister, ovänliga regeringar och andra.

I en dramatisk demonstration av Aurora sårbarheten som genomfördes 2006, visade ingenjörer vid Idaho National Labs, INL, hur sårbarheten kan utnyttjas för att orsaka haveri i en generator ansluten till elnätet. Se länk nedan.

http://www.youtube.com/watch?v=fJyWngDco3g

Bilden visar en dieseldriven elektrisk generator som havererar som följd av att den elektroniska utrustningen för att synkronisera generatorn med elnätet påverkas genom oönskad påverkan så att generatorn kopplas in och ur elnätet ur fas upprepade gånger. Varje gång detta inträffar så påverkas dieselmotorn av den mekaniska belastning som uppstår under den korta period då generatorns rotor av elnätet tvingas rotera eller stå still till dess den kommer i fas med elnätet. Efter sådan oönskad påverkan av maskinaxelns rotationshastighet havererar dieselmotorn.

Miljöpåverkan

Miljöpåverkan är ett hot som ständigt gör sig påmint i branschområdet. I Sverige inskränker sig denna normalt sett till hot kopplade till åsknedslag och motsvarande men händelserna i Japan Fukushima i mars 2011 visar på att oväntade eller eskalerade versioner av kända/väntade händelser måste ges förnyad och förbättrad uppmärksamhet vad avser riskbedömningar. I Sverige har under det senaste årtiondet landet blivit utsatt för stormar som renderat förödelse som tidigare inte skådats. Här kan exempelvis nämnas orkanen Gudrun som orsakade rekordstora skador på skog och el- och telenät. Ett annat mera udda hot manifesterar sig i geomagnetiska stormar eller solstormar som kan påverka elförsörjningen på ett katastrofalt sätt. Smärre jordbävningar eller markuppluckring som följd av extrem nederbörd som medför dammbrott eller motsvarande i vattenmagasin är exempel på potentiella hot i framtiden. Ett annat exempel på miljöpåverkan är isstormar. Sverige har varit förskonat från isstormar sedan 1921 men följder av en sådan i dagsläget skulle kunna bli katastrofala.

Rökutveckling efter en explosion i kärnkraftverket Daiichi i Fukushima efter det att en tsunami slagit in över kärnkraftverket.

Anläggningen drabbades av stora skador från jordbävningen som mätte 9,0 på Richterskalan och den efterföljande tsunami som drabbade Japan den 11 mars 2011. Kärnkraftverket förväntas inte gå att reparera och åter tas i drift.

1998 drabbades Kanada av en stor isstorm vilket ledde till omfattande långa strömavbrott. Miljontals var utan ström från dagar upp till veckor, vilket ledde till mer än 30 dödsfall. Samhällsfunktioner i Montreal och Ottawa stängdes ned och återuppbyggnaden krävde enorma insatser.

Sabotage

Under de senaste tio åren har världen, och Sverige, upplevt en ökning av aktörsrelaterade hot där gärningsman/män har varit drivna av ett syfte bortom rastlöshet och kriminalitet. I de nordiska länderna finns nu erfarenhet av såväl terrorister i form av självmordsbombare (december 2010 Stockholm) som personer som uppsåtligt och överlagt söker skada enskilda personer och grupper av personer. Ett exempel är fallet med Lars Vilks som blivit hotad vid ett flertal tillfällen som följd av publicering av religiöst satiriskt material i Nerikes allehanda 2007. Som följd av en liknande publicering i Jyllandsposten i Danmark ertappades terrorister under en förberedelsefas för att genomföra en attack mot Jyllandsposten och en katastrof kunde undvikas. Vidare måste i sammanhanget nämnas bombattentatet i Norge (Oslo juli 2011) följt av massakern på Utöya, planlagt och genomfört av den inhemske terroristen Anders Behring Breivik. Sammantaget måste slutsatsen dras att terrorism nu är ett närvarande och adekvat hot som i alla avseenden i samband med samhällsviktig verksamhet måste beaktas. Energisektorn är en sårbar bransch där terroraktioner kan nå stor eller mycket stor effekt med små medel. Det får således ses som att till dags dato uteblivna aktioner mot energisektorn får ses som ett tecken på okunskap om befintliga sårbarheter snarare än avsaknad av vilja att göra energisektorn till ett mål för terrorverksamhet. Vidare går det inte att utesluta att demonstrationer och aktioner

initierade av reaktionära samhällsgrupper skulle kunna få oönskade konskevenser för olika typer av anläggningar inom elförsörjningen. Detta skulle exempelvis kunna ske om demonstrationer eller andra aktiviteter går överstyr exempelvis som följd av uppvigling. Aktivistgrupperingar av olika slag har i ökad omfattning använt sig av informationsteknologi för att nå sina mål eller påverka sina mål.

Göteborgskravallerna är en samlande beteckning på en serie kravaller och upplopp i samband med demonstrationer i Göteborg juni 2001 med anledning av EU-toppmötet i Göteborg och besöket av USA:s president. Demonstranters och aktivisters sammandrabbningar med polis var de mest omfattande i Sverige på flera decennier. Sammanlagt skadades 53 polismän och 90 demonstranter och såväl staden som privatpersoner åsamkades omfattande materiella skador. Anmärkningsvärt var att demonstranterna organiserades via en egen ledningscentral och aktivt avlyssnade polisens radiokommunikation.

3 Genomförande

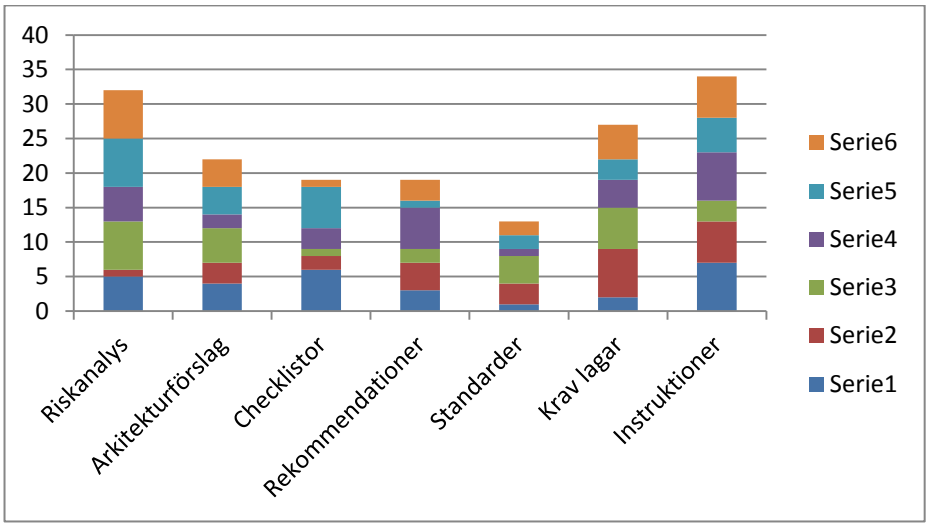
3.1 Enkät EBITS

Tidigt i förstudien genomfördes en presentation av förstudien för EBITS-gruppen (arbetsgruppen för Energibranschens Informationssäkerhet) i samband med ett ordinarie möte på Svenska Kraftnät den 15 september 2011. I samband med denna presentation fick EBITS-företrädarna fylla i en enkel enkät där olika traditionella informationssäkerhetsområden kunde prioriteras utifrån ett bedömt behov av myndighetsstöd.

De områden som presenterades var:

- Riskanalys
- Arkitekturförslag
- Checklistor
- Rekommendationer
- Standarder
- Krav & lagar
- Instruktioner

Utfallet från enkäten sammanställdes i följande diagram där *serie 1…6 avser de personer som deltog i enkäten.*



De slutsatser som kunde dras från denna enkät och som präglat det fortsatta arbetet i förstudien är att följande områden eller sammanslagna områden är förstudiens fokusområden.

- Instruktioner (med stöd av checklistor och rekommendationer)
- Riskanalyser
- Krav och lagar; då främst förtydning av befintliga lagar och krav
- Arkitekturförslag

3.2 Seminarium med branschföreträdare

3.2.1 Allmänt

Den 17 – 18 november 2011 genomfördes ett stort seminarium med företrädare för elbranschen på hotell Arlandia vid Arlanda flygplats utanför Stockholm. I samband med detta redogjorde säkerhetsföreträdare från Svenska Kraftnät för hur Svenska Kraftnät ser på nuläget och framtiden vad avser IS/IT-säkerhet i elbranschen. Vidare fick deltagarna i seminariet möjlighet att under grupparbetsformer formulera problemområden sett från sitt eget perspektiv.

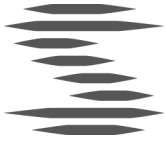
Resultatet av denna övning dokumenterades och redovisas områdesvis nedan.

3.2.2 Område riskanalys

Det föreligger ett behov av en branschgemensam begreppsmodell vad avser riskanalysområdet. Vidare behövs ett metodstöd, framförallt för mindre och medelstora företag. Ett metodstöd bör dessutom lämpa sig för att kunna användas för att skapa underlag som kan ligga till grund för arbete med säkerhetsanalyser[1]. Den spridda uppfattningen vid seminariet var att Svenska Kraftnät bör stå för begreppsmodell, ramverk och eventuellt metodstöd. Några specifika synpunkter som rör riskanalysområdet och som framkom i samband med seminariet är följande.

- Begreppsmodell, ramverk och metodstöd skall omfatta och vara anpassat till SCADA-system.
- Begreppsmodell, ramverk och metodstöd måste ta hänsyn till och i förekommande fall belysa konsekvenser för samhället.
- Metodstödet skall vara lämpligt för att underbygga säkerhetsanalyser.
- Svenska Kraftnät bör ta fram en branschgemensam hotbildsbeskrivning som kan hållas uppdaterad över tiden.
- Ett problem i sammanhanget är att de små bolagen saknar resurser för att på ett tillfredsställande sätt genomföra och hantera riskanalyser. En möjlig lösning som föreslagits är att Svenska Kraftnät tillhandahåller stöd i forma av mallar, checklistor utbildning m.m. Det påpekas dock att ett sådant stöd inte får påverka konkurrenssituationen.

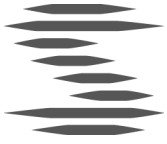
[1] Säkerhetsanalys är ett begrepp som definieras i säkerhetsskyddsförordningen, se vidare avsnitt Lagar och andra rättsliga krav i detta dokument. En säkerhetsanalys underlättas av det finns en övergripande riskanalys som kan ligga till grund för bedömningar inom en säkerhetsanalys.



3.2.3 Område lagar och krav

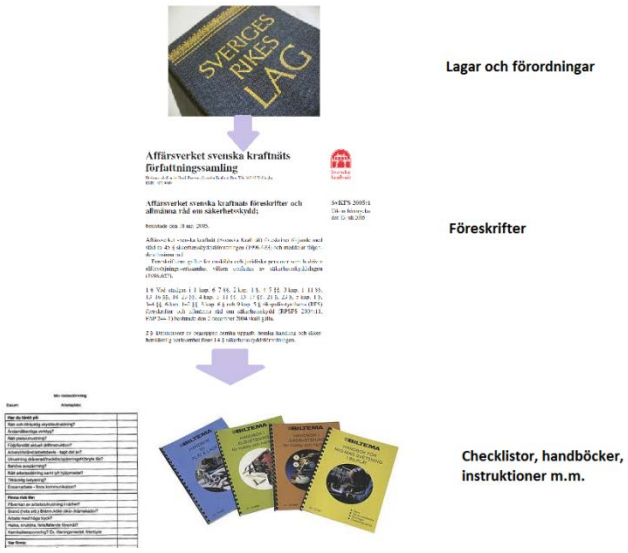
Den allmänna uppfattningen vid seminariet var att det behövs stora insatser för att skapa branschgemensam tolkning av lagar och andra rättsliga krav. Sådan tolkning måste omfatta en nedbrytning från övergripande nivå till en mer detaljerad och mätbar nivå. Det är i detta sammanhang viktigt att en sådan nedbrytning renderar krav på funktion och förmåga, inte specificerar tekniska lösningar. Inom detta område är det dessutom viktigt att titta på andra länder inom Norden och EU då lagstiftning i andra länder kan komma att påverka exempelvis i samband med utlokalisering av elverksamhet. Några specifika synpunkter rörande lagar och krav som framkom i samband med seminariet är följande:

- Tydliga övergångar från lag till föreskrift och vidare till bestämmelser, riktlinjer och handböcker är nödvändiga.
- Det är viktigt att säkerställa att nivån bestämmelser, riktlinjer och handböcker reglerar funktions- och förmågenivåer, inte tekniska lösningar.
- Branschföreträdarna emotser en ökad frekvens på tillsyn och kontroll i detta avseende från Svenska Kraftnät sida.
- Nedbrytningar till nivån bestämmelser, riktlinjer och handböcker bör kompletteras med referensexempel där så är möjligt.



3.2.4 Instruktioner, checklistor och rekommendationer

Detta område hänger samman med det föregående, lagar och krav, då det i allt väsentligt tar upp frågor om hur man skall nå tydlighet i styrande dokumentation. Behovet som påtalades åskådliggörs bäst i följande bild.



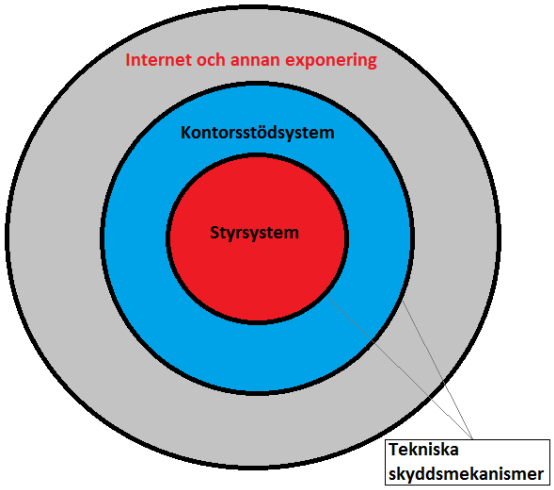
Nedbrytningen av överordnade formella krav till mer lättillgänglig information är en viktig framgångsfaktor för att organisationerna inom elförsörjningen skall förstå, eftersträva och följa dessa krav.

3.2.5 Område IT-arkitektur

I samband med seminariet på Arlandia framkom att branschföreträdarna var positivt inställda till en referensarkitektur. En sådan referensarkitektur skulle kunna belysa möjliga lösningar på de funktions- och förmågekrav som formuleras när tolkning och nedbrytning av krav och lagar sker. Vidare skulle en sådan referensarkitektur kunna belysa hur zonmodellen kan implementeras i olika sammanhang och på olika nivåer. Några av synpunkterna återges här.

- Det bör utredas hur befintliga standarder ställer sig i förhållandet till IT-arkitekturer i tillämpning i elbranschen i allmänhet och referensarkitektur i synnerhet.
- Zonmodellen bör framgå med tydlighet och bra exempel.
- Arkitekturbeskrivningar bör vara av typen *(eng.)*Best practice.
- Arkitekturbeskrivningar skall vara utformade så att de är leverantörsoberoende.
- Inom detta område bör ett förtydligande av betydelseklasser B1-B4 göras.

Figur: exempel på zonmodell



3.2.6 Område övrigt

Elbolagens inneboende konflikt mellan vinst och verkan påverkar säkerheten i all tillämpning. Tydlighet vad avser skyldigheter i enlighet med elberedskapslagen efterfrågas.

Det påtalas att en ensad kravbild från myndigheternas sida är ett axiom för att kunna uppfylla krav på säkerhet. Härvid har Svenska Kraftnät en framträdande roll såsom tillsynsmyndighet.

Branschföreträdarna efterlyser stöd för att medvetandegöra bolagsledningar om skyldigheter som kan kopplas till säkerhetsproblematik.

Dokumentation som tas fram av Svenska Kraftnät inom det reglerande området bör vara översatt till engelska så att en gemensam tolkning och översättning existerar i stället för att respektive bolag gör sina egna översättningar.

3.3 Samverkan med myndighetsföreträdare

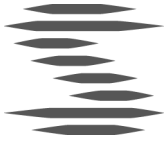
3.3.1 Samverkansmöte med myndighetsföreträdare

2011-12-12 genomfördes inom ramen för förstudien ett informations- och samverkansmöte om förstudiens aktiviteter med Myndigheten för samhällsskydd och beredskap (MSB), Säkerhetspolisen (SÄPO), Strålsäkerhetsmyndigheten (SSM), Energimarknadsinspektionen och Elsäkerhetsverket. Till mötet var ett antal andra myndigheter kallade som valde att inte delta.

Vid mötet diskuterades bland annat brister i elbolagens säkerhetsanalyser och att dessa ofta saknar en bred underbyggnad från riskanalyser som spänner över hela verksamhetsområdet.

Som en följd av sådana brister är det vanligaste scenariot att säkerhetsanalyser, i den mån de utförs, präglas av organisationens säkerhetsskyddschefs värderingar och därmed oftast får ett fokus som i säkerhetssammanhang brukar kallas ”lås och larm”. Med detta avses att det saknas en övergripande syn på säkerheten där IT-systemens och den administrativa informationshanteringens betydelse finns med.

En annan brist som diskuterades var hur säkerhetsanalyser och motsvarande skyddsvärd information hanterades av de berörda bolagen. Dessa hämmas av det faktum att de inte kan sekretessbelägga information enligt offentlighets och sekretesslagen (2009:400). Således kan information som av en myndighet skulle klassificeras som hemlig uppgift hanteras olika och i förekommande fall inte i enlighet



med den skyddsnivå som informationens skyddsvärde egentligen kräver. Vidare föreligger brister i möjligheten att genomföra kontroller (motsvarande SUA och registerkontroll) av utländsk personal som får tillgång till skyddsvärda uppgifter om den svenska elförsörjningen.

En kommande förändring av säkerhetsskyddslagstiftningen (se vidare avsnitt 2.2.1 Ändringar i lagstiftningen) kan möjligen avhjälpa eller minska problem enligt ovanstående stycke.

3.3.2 Kompletterande samverkansmöte med myndighetsföreträdare

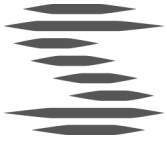
Energimyndigheten

Den 10:e januari 2012 genomfördes ett samverkansmöte med en företrädare för Energimyndigheten i Eskilstuna. Från förstudiens håll orienterades om förstudiens syfte, mål och arbetsgång samt om att förstudien skall följas upp med ett projekt under 2012.

Från energimyndighetens sida gavs tips om samverkanspunkter inom olika gränsöverskridande beredskapsorganisationer såsom NORDBER och EPCIP.

NORDBER är ett samarbete om beredskap inom elförsörjningsområdet i Norden. Samarbetet har som mål att:

- ge en god förståelse mellan parterna om ländernas beredskapsverksamhet och krishantering
- främja en effektiv kommunikation mellan parterna i händelse av en krissituation och därmed öka parternas förutsättningar till en bättre koordinering mellan inblandade i den nationella krishanteringen,
- följa utvecklingen, utväxla erfarenheter och synpunkter om frågor som är relevanta för elförsörjningens beredskap avseende nationella och internationella förhållanden,
- skapa förutsättningar för samordning av gemensamma projekt/verksamheter som är relevanta för elförsörjningens beredskap och krishantering samt
- bidra till förmedling av relevant information och därmed bidra till ökat samarbete mellan berörda inom elförsörjningen inom respektive land.



Organisationerna bildar ett nordiskt beredskapsforum, benämnt NordBER. Samarbetet sker dels genom möten i forumet, dels genom att beredning- och/eller arbetsgrupper tillsätts för särskilda ändamål.
Utdrag från NORDBER hemsida http://www.nsr.is/Nordber/index.aspx?groupid=3

EPCIP, European Programme for Critical Infrastructure Protection, är ett EU-program för säkerhetsarbete relaterat till kritisk elförsörjning inom EU. Svenska Kraftnät har representation i detta program.

Energimyndigheten har tillhandahållit Översiktlig risk- och sårbarhetsanalys över energisektorn i Sverige år 2011 vilken har färgat delar av hotbildsbeskrivningen i detta dokument.

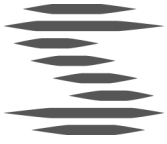
Energimyndigheten genomförde 2004 HEL-projektet, En helhetssyn på den svenska elförsörjningens säkerhet. Denna kompletterades år 2008 med bedömningar kopplade till klimathot.

Ingångsvärden från Energimyndigheten kommer att tas med i det kommande projektarbetet.

3.4 Kompletterande intervju med branschföreträdare

Då företrädare för Vattenfalls centrala säkerhetsstab inte kunde medverka på den gemensamma workshopen, så utfördes en särskild intervju med Vattenfalls informationssäkerhetschef. Nedan sammanfattas de områden som diskuterades och de önskemål som framfördes:

- Svenska Kraftnät måste bistå med handfast och konkret assistans och hjälp till elföretagen i deras dagliga frågeställningar om IS/IT-säkerhetsfrågor och IT-relaterade säkerhetsskyddproblem.
- Svenska Kraftnät måste tillhandahålla lättillgänglig och förståelig information på svenska och engelska som beskriver myndighetskrav, information, IS/IT-hjälpmedel, etc.
- Svenska Kraftnät kan vara en aktör för att se till att det finns informationsdelning mellan aktörer inom elbranschen.
- Vad det gäller utformande av IT- och IT-säkerhetsarkitektur för branschen så måste Svenska Kraftnät bli en drivande kraft. Det går inte att utesluta att samarbete med andra myndigheter, t.ex. MSB kommer att krävas.



- Svenska Kraftnät behöver utföra mera uppföljning, t.ex. mot mindre anläggningar. Det finns mycket att göra inom det området, inte minst på grund av det stora symbolvärdet mot verksamhetsföreträdare.
- Fortsätt att göra uppföljningar och granskningar av anläggningar. Svenska Kraftnät och SSM har tillsammans med andra myndigheter inspekterat kärnkraftsanläggningar. Det är viktigt att detta samarbete fortsätter, då de granskar verksamhet och skydd utifrån olika lagrum och perspektiv.

3.5 Webbenkät

Då inbjudan till workshopen på Arlanda i princip enbart besvarades av de tre stora elbolagen, så kompletterades informationsinhämtningen med ett utskick till samtliga elbolagsföretag i Sverige. Utskicket bestod av en enkät med tio allmänt hållna frågor skickades ut till samtliga medlemsföretag i Svensk Energi, ca 250 stycken.

Med hjälp av enkäten kompletterades den tidigare utförda datainsamlingen för att få en mer komplett översikt av vad de olika organisationerna inom den svenska elbranschen har för behov av stöd.

De frågor som ställdes i webbenkäten var:

1. Hur många anställda har ert/era företag?

2. Hur många personer ingår i SÄKERHETSORGANISATIONEN i [Företag]?

3. Hur många personer ingår i funktionen/rollen som arbetar med IT-SÄKERHET OCH INFORMATIONSSÄKERHET i [Företag]?

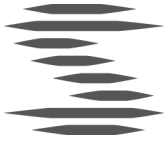
4. När gjorde ni senast en säkerhetsanalys enligt säkerhetsskyddsförordningen § 5?

5. Vad känner ni till om er organisations interna IT-relaterade säkerhetsincidenter?

6. Vilket behov har er organisation av stöd inom IT- och informationssäkerhetsområdet?

7. Inom vilka delområden har er organisation ett behov av stöd inom IT- och informationssäkerhetsområdet?

8. Vilken prioritet för framtagande/vidareutveckling av de olika delmomenten anser du skall gälla?



9. Vad bör sektorsmyndigheten fokusera stödet inom informations- och IT-säkerhet på?

10. Vad bör branschorganisationer fokusera stödet inom informations- och IT-säkerhet på?

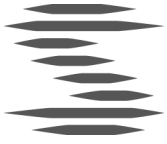
Enkäten var tillgänglig för medlemsföretagen att besvara under perioden december 2011 tills januari 2012. Information om själva enkätens spridning, svarsfrekvens, etc., finns i tabellen nedan.

Mottagare	247
Ej kontaktbara	2
Svarande	120
Svarsfrekvens	49%

utskick- och svarsfrekvens finns i tabellen nedan

Utifrån det besvarade frågematerialet går det att dra ett antal enkla slutsatser, bland annat:

- Mer än 2/3 av alla tillfrågade organisationer har aldrig gjort en säkerhetsanalys enligt säkerhetsskyddsförordningen 5 § och för 14% så var det längre än 24 månader sedan. D.v.s. det är mindre än 1/5 av organisationerna som har en aktuell säkerhetsanalys.
- Mer än 90% av de tillfrågade organisationerna har behov av stöd i någon omfattning
- Över 70% av de tillfrågade önskade checklistor eller annat stöd för riskanalys, hotbedömningar, säkerhetsarbete, mm
- Mer än hälften önskade sig förtydliganden av lagar, förordningar eller andra rättsliga krav, men också tillgång till mallar och branschgemensamma hotbilder/hotkataloger



- Majoriteten av de tillfrågade anser att sektormyndigheten Svenska Kraftnät bör prioritera förebyggande IT- och informationssäkerhetsåtgärder i stödjande syfte.
- Majoriteten av de tillfrågade anser att även branschorganisationer som representerar elbranschen ska satsa på förebyggande åtgärder, inte minst inom utbildning och kompetensutveckling.

Skillnaden mellan elbolagens olika behov framgår om man jämför resultat från arbetsmötet på Arlandia, där framförallt de tre stora elbolagen (Vattenfall, Fortum, E.ON) var representerade, med webbenkäten där de små och mellanstora elbolagen är representerade. Ett tydligt exempel är att de stora bolagen inte anser sig ha behov av mallar eller checklistor, medan detta efterfrågas starkt av de mindre bolagen främst p.g.a. resursbrist.

På vissa punkter finns det en samstämmighet mellan såväl stora elbolag och de mindre aktörerna. En klar sådan punkt är förtydligande och nedbrytning av gällande lagar, förordningar och regler.

Rapporten med sammanställningen från undersökningen finns tillgänglig som bilaga 2.

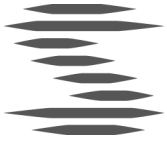
3.6 Övriga reflektioner

3.6.1 Integritet – personlig integritet för elkunder

Förstudien inleddes med ett fokus på skydd av IT-system mot aktiva angrepp eller andra typer av attacker. Under arbetets gång har andra områden uppmärksammats, inte minst hantering av elkundernas personinformation och den därtill hörande personliga integriteten.

Frågor rörande den personliga integriteten har ökat i samband med införandet av mer IT-teknik i de tjänster som elföretag erbjuder sina slutkunder. Befintliga tjänster av typen automatiserad fjärravläsning av elmätare (s.k. smart meter eller AMR) hämtar in förbrukningsinformation med hög detaljnoggrannhet. Frågan är känslig och det finns personer och grupper[Ref.1] som av olika anledningar inte vill ha automatiserad mätdatainhämtning.

Olika undersökningar utförda eller beställda av olika länders myndigheter[Ref.2][Ref.3] och säkerhetsforskare [Ref.4][Ref.5] har påvisat att det går



att få fram information om användningsmönster, identifiering av användning av enskild strömförbrukande utrustning, med mera.

Införandet av denna typ av teknologi har i vissa länder föranlett till omtolkning av lagstiftning[Ref.6] och nya branschkrav från sektorsmyndigheter[Ref.7] där särskilda krav på IT-säkerhet och skydd av personlig integritet explicit pekas ut. I andra länder utreds och bereds frågan för att modifiera den befintliga lagstiftningen och rättsliga krav.

3.6.2 Internationell utveckling

En internationell utblick visar att många länder ser över sitt skydd av kritisk samhällsinfrastruktur, inte minst grundläggande funktioner som elförsörjning.

USA

I USA förkommer mycket arbete inom området IS/IT-säkerhet i elbranschen, då man identifierat det som en kritisk infrastrukturkomponent.

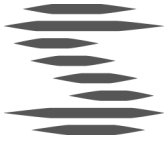
Den amerikanska standardiseringsorganisationen NIST har publicerat ett antal dokument, så kallade ”special publications”, som är relevant för området, bland annat:

- NIST 800-53 *“Recommended Security Controls for Federal Information Systems and Organizations”* [Ref.8] och
- NIST 800-82 "*Guide to Industrial Control Systems (ICS) Security*"[Ref.9]

Dessa har används som förlaga i många dokument rörande IS/IT-säkerhet inom området industriella styr- och kontrollsystem.

Department of Energy, DoE, har via sina olika ramprogram producerat ett antal strategiska dokument, policyinriktningar samt tekniska beskrivningar. En strategiöversikt (*eng. roadmap*) kallad *"Roadmap to Achieve Energy Delivery Systems Cybersecurity*"[Ref.10][Ref.11] framtagen av Energy Sector Control Systems Working Group (ESCSWG) beskriver tillvägagångssättet för att skapa en säkrare energiförsörjning i USA där skydd mot olika typer av IT-hot beaktats och hanterats.

Ett stort arbete som utförts i USA är den gemensamma kravkatalog som används vid specifikation, projektkravställning och upphandling av IT-lösningar. Denna kravkatalog, kallad *”Department of Homeland Security: Cyber Security Procurement Language for Control Systems”* [Ref.12] har kommit att i allt större utsträckning vara standardkrav vid all ny upphandling och kravställning.



En annan viktig satsning i USA har letts av *North American Electric Reliability Corporation,* NERC, som styr över det amerikanska stamnätet. Genom sitt regelverk NERC CIP, Critical Infrastructure Protection[Ref.13], så läggs grundläggande IS/IT-säkerhetskrav på alla organisationer som skall vara anslutna till stamnätet.

NERC själva beskriver sitt IT-säkerhetsreglemente som ett övergripande ramverk:

> *"NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System."*

Ett par viktiga koncept som introduceras med NERC CIP är:

- *Critical Cyber Asset Identification,* och
- *Electronic Security Perimeter(s)*

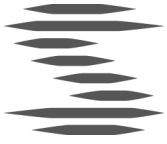
Tack vare dessa koncept så ökas inriktningen med säkerhetsarbetet på kritiska IT-relaterade komponenter i anläggningen samt det ger signalvärden att IT är likvärdigt med fysiskt skydd i många hänseenden, exempelvis skal- och områdesskydd.

Det existerar ett otal andra, mer specifika, program och aktiviteter för att arbeta med IS/IT-säkerhetsfrågor inom områden såsom Smart Grid, Smart Metering, mikrogenerering av el, nya tjänster, etc. såsom exempelvis ENTSOE, European Network of Transmission System Operators for Electricity. I sådana program är stabilitet, systemtillit och hög nivå av god informationshantering viktiga egenskaper.

Tyskland

I Tyskland pågår flera olika aktiviteter och projekt på såväl policynivå som rörande tekniska detaljer. På en övergripande nivå så pågår arbete inom standardiseringsorganet DIN för med att skapa en elbranschanpassad variant [Ref.14] av SIS/IEC-standarden 27002 "*ledningssystem för informationssäkerhet*" som fokuserar på styrning och kontroll av industriprocessen.

Vad det gäller tekniska detaljer så arbetar t.ex. elbranschen tillsammans med ansvariga myndigheter att ta fram *Common Criteriabaserad* s.k. *protection profile* [Ref.15] för kommunikationsutrustning som används för kundplacerad utrustning för inhämtning av uppgifter om aktuell förbrukning.



Norden

Arbete pågår i de olika nordiska länderna med att förbättra IS/IT-säkerheten inom elförsörjningsområdet. I exempelvis Norge arbetar bland annat *Norges vassdrags- og energidirektorat,* NVE, med att ta fram nya krav och hantering av IT-inriktad kris. Andra norska myndigheter som *Oljedirektoratet* och *Petroleumtilsynet* har fokus på och reglerar den delen av energiområdet där SCADA-system och industriella kontroll- och styrsystem används inom petroleumindustrin.

3.6.3 Utlokalisering av kritisk elverksamhet

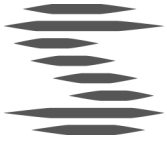
Under hösten 2011 har en utredning genomförts vid Svenska Kraftnät avseende utlokalisering av kritisk elverksamhet till utlandet. Utredningen har beröringspunkter med denna utredning i det avseende att det i dagsläget saknas ett rättsligt stöd för att för elbolagen reglera att de skall ha styrcentraler och motsvarande funktioner kvar i landet. Detta kan tyckas vara ett uppenbart axiom att den tekniska styrförmågan måste finnas i landet även om den till daglig dags hanteras från annat land men rättsligen finns inte detta stöd explicit.

En besvärande faktor i sammanhanget är att det saknas en tydlig definition av vad som utgör kritisk elverksamhet, då i synnerhet vad avser styr- och reglerförmåga. I nämnda utredning ansätts en definition för detta enligt följande.

> *Funktioner, personal och teknisk utrustning som är avgörande för elbolagens förmåga att styra och reglera sina processer för elförsörjning av Sverige även under förhållanden som präglas av icke ordinära händelser.*
>
> En förutsättning som råder för ovan nämnda definition är:
> *Sådan styrning och reglering skall vara möjlig även under sådana förhållanden som innebär att elektronisk kommunikation över rikets gränser inte längre är möjlig.*

Det bör särskilt påpekas att ovanstående definition syftar enbart på styr- och reglerförmåga.

På en mera implicit nivå kan man av elberedskapslagen och övrig tillämplig lagstiftning i kombination med dagens rådande hotbild där aktörsdrivna hot, särskilt cyberhot och hot som hänför sig till sabotage, ges en högre grad av uppmärksamhet än tidigare utläsa följande.



Ur beredskapssynpunkt så måste elbolagen säkerställa att de har styr- och reglerförmåga inom landet oavsett vilket läge som råder.

Av detta kan man därefter dra ett antal implicita slutsatser som t.ex. *att elbolagen måste ha nationell kompetens och erforderlig teknisk utrustning på plats*. Detta kan också innebära att vissa styrcentraler inte kan avvecklas vad avser deras tekniska funktion, de kan möjligen vara obemannade under det ordinarie verksamhetsläget då kris eller motsvarande inte råder.

Ändringar i tillämplig lagstiftning är planerade men ännu inte genomförda. Det synes rimligt att dessa ändringar kommer att ge ett tydligare mera explicit stöd för att säkerställa elbolagens förmåga att styra och reglera elförsörjningen under olika former av kris och incidenter.

De slutsatser och därtill kopplade aktiviteter som nämns i utredningsrapporten är delvis överförda till förslag på aktiviteter som skall ingå i det projekt som följer på denna förstudie.

4 Sammanfattning och slutsatser

4.1 Sammanfattning

Under denna rubrik sammanfattas de områden som genom förstudien tydligt varit tongivande i att de är problematiska och att det därtill finns ett stort behov av insatser av olika slag från Svenska Kraftnät inom ramen för det projekt som skall följa på denna förstudie. Med mottagare avses i denna sammanfattning företrädesvis elbolagens företrädare inom respektive tillämpligt område, exempelvis IT, Juridiska avd., Adm.

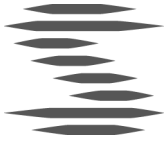
Inom flera av de områden som vi pekar ut så är arbetsinsatserna i projektet snarlika.

- Framtagande av en för mottagarna tydligare och mer tillämplig vägledande och styrande information.
- *Spridande* av informationen, exempelvis elektroniskt eller i arbetsgruppsform.
- *Hjälp och stöd* i form av *grundutbildning* och *vidare kompetensutveckling*, exempelvis som branschspecifik komplettering av säkerhetsutbildning.

En annan aspekt är att resultaten från det framtida projektarbetet bör stämmas av mot motsvarande arbete som utförs i främst de övriga nordiska länderna, då flera av de större aktörerna inom elförsörjning har pan-nordisk utsträckning. I och med denna utsträckning så bör exempelvis metodstöd och referensmodeller harmoniseras görligaste mån.

4.1.1 Riskanalyser

Redan tidigt i förstudien framstod riskanalysområdet som prioriterat. Det finns ett stort behov av tydliggöranden inom området såväl som styrning i tillämpning av riskanalyser. Ett tydligt exempel på behov av riktlinjer och annan tydlighet inom området är det divergerande arbetssätt på vilket säkerhetsanalys enligt 5 § säkerhetsskyddsförordningen genomförs på, om den överhuvudtaget genomförs. En säkerhetsanalys bör enligt praxis bygga på, och föregås av, en riskanalys som övergripande tittar på en verksamhet ur ett helhetsperspektiv. Detta i syfte att säkerställa att säkerhetsanalysen inte endast fokuserar på traditionellt säkerhetsskydd såsom lås, larm och övrigt fysiskt skydd utan även beaktar administrativa,



organisatoriska och tekniska aspekter. Det sistnämnda är särskilt viktigt sett mot den ökande hotbilden kring cyberattacker.

Det saknas i dagsläget en branschgemensam begreppsmodell och samsyn på hur riskanalyser skall utformas och genomföras samt vilket fokus de bör ha, särskilt i samband med säkerhetsanalyser.

Ett behov som har påtalats inom ramen för förstudien är behovet av en branschgemensam hotinventering. Resultatet från en sådan inventering kan ses som en hotkatalog men bör hanteras dynamiskt över tiden för att inte bli inaktuell.

4.1.2 Lagar och andra rättsliga krav

En central del i arbetet med att skydda anläggningar, processer, system och information är att följa de externa krav som redan existerar.

Branschen har idag svårt att ta till sig, fullt ut förstå samt korrekt tillämpa lagar och andra rättsliga krav. Detta visar sig inte minst i resultatet från webbenkäten (avsnitt 3.5 i detta dokument) ställd till branschorganisationens medlemmar, där mer än två tredjedelar av de svarande uppger att de aldrig har genomfört en säkerhetsanalys. I många fall har det bekräftats att de svarande inte kände till vad en säkerhetsanalys var för något.

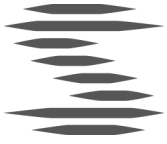
Det faktum att lagar och andra rättsliga krav tolkas individuellt av varje företag och andra branschorganisationer leder ofrånkomligen till inkonsistenser såväl vad avser själva tolkningarna som tillämpningarna, eller allvarligare avsaknaden av tillämpning.

Branschföreträdare har tydligt angett behov av en utökad styrning och tydlighet från Svenska Kraftnät vad avser detta område. Främst i form av olika typer av nedbrytning till en mer begriplig och tillämplig nivå av regelverk såsom exempelvis bestämmelser, riktlinjer och handböcker, se vidare avsnitt 4.1.4 nedan.

4.1.3 Arkitektur

Information av det mer IT-tekniska slaget som återkommande efterfrågades under förstudien rörde IT-arkitektur och säkerhetsarkitektur. Denna typ av information, som får anses vara av den mer handgripliga slaget, är olika typer av scenariobeskrivningar, typfall av IT-arkitekturer, exempelkataloger på IS/IT-säkerhetsarkitektur, etc.

Bland de moment som kan ingå i området ”arkitektur” är:



- Beskrivningar av vad som är vedertagna skydd och skyddstekniker inom processnära IT-system inom elförsörjning. Exempelvis envägstrafik, skydd av känsliga IT-komponenter, skydd av inbyggda system, etc.
- Beskriva nödvändiga eller prioriterade IT-funktioner och komponenter för att kunna skapa god IT- och informationssäkerhet i en IT-miljö, exempelvis behörighetskontroll, tidssynkronisering, logghantering, etc.
- Beskrivning av separerande kommunikationslösningar, i form av indelning av interna nätverk i olika säkerhetszoner
- Sammanställningar över vanliga frågor- och svar (*eng*. FAQ) som hjälper beslutsfattare, IT-tekniker, processingenjörer och andra i sitt arbete att skapa säkrare IT-miljöer inom den elförsörjningen

4.1.4 Instruktioner, checklistor, mallar och handböcker

Elbranschens företrädare har efterfrågat insatser med att ta fram hjälpmedel i form av informationsmaterial och metodstöd. Metodstödet kan bestå i att ta fram metoder, instruktioner och handböcker, checklistor, mallar och liknande som förenklar införande och genomförande av olika arbetsmoment som berör IS/IT-säkerhet inom de olika organisationerna.

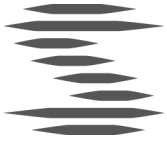
Förtydligande vad gäller hur elberedskap och säkerhetsskydd påverkar eller påverkas av IT-användning skall vara genomgående i det material som tas fram.

Det material som idag finns framtaget hos Svenska Kraftnät bör gås igenom och uppdateras för att innehålla rätt mängd IS/IT-säkerhetsrelaterat material.

Av intervjuer och enkätsvar drar vi slutsatsen att små och medelstora elföretag har ett större behov av stöd inom detta område än de stora elbolagen. Den främsta anledningen förefaller att de mindre organisationerna har mindre resurser och inte orkar prioritera arbetet med säkerhetsfrågorna.

4.2 Slutsatser

Slutsatser redovisas här utifrån förstudien som helhet och mot föregående sammanfattning.



4.2.1 Riskanalyser - slutsatser

Svenska Kraftnät bör ta fram vägledning för området riskanalys tillsammans med en branschgemensam begreppsmodell i syfte att ensa fackspråk kring riskanalyser och de bedömningar som görs kopplade till sådana analyser.

Svenska Kraftnät bör särskilt tydliggöra hur processen med säkerhetsanalys enligt 5 § säkerhetsskyddsförordningen skall hanteras. En tydlig koppling till Svenska Kraftnät tillämpliga föreskrifter bör finnas med liksom en beskrivning av riskanalysens roll i detta sammanhang.

Det bör företas en hotinventering som på ett övergripande, och över tiden hållbart, sätt beskriver sådana hotbilder som i varje avseende, men i synnerhet i samband med säkerhetsanalyser, måste beaktas.

För de mindre elbolagen, som av resursskäl inte har möjlighet att ta fram egna metodstöd och andra tillämpliga resurser inom riskanalysområdet, bör Svenska Kraftnät arbeta med metodstöd, se kap 4.2.4 ”Instruktioner, checklistor, mallar och handböcker - slutsatser”.

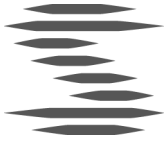
4.2.2 Lagar och andra rättsliga krav – slutsatser

En omfattande genomlysning av tillämpliga lagar och andra rättsliga krav bör företas. Denna genomlysning skall syfta till att ge underlag för att uttrycka innebörden på ett samlat och, för juridiska lekmän, överskådligt och begripligt sätt.

Arbetet med att förtydliga lagar och andra rättsliga krav måste ske så att korrelationer mellan olika tillämpliga lagrum adresseras på ett korrekt sätt. Här kan exempelvis nämnas kopplingen mellan säkerhetsskyddslagstiftningen och lagar som rör terrorbrott.

Utfallet från arbetet med att *förtydliga* lagar och andra rättsliga krav måste rendera underlag som svarar upp mot minst följande egenskaper.

- Det skall vara lätt att hitta information som eftersöks om ett specifikt ämne eller problemområde.
- Det måste finnas adekvata länkar från ett ämne till sådan information som i olika tillämpningsområden kan påverka ett arbete i någon särskild riktning eller av annat skäl ge ytterligare belysande information.



- Dubbletter av information skall inte finnas. Varje instans av en information skall vara unik och om den behövs i en annan del av underlaget så skall detta ske med länkar och referenser.

Ett efterfrågat område är *exempelsamlingar och kopplingar mot vardagsliga säkerhetsfrågeställningar* hos elbolagen. Att koppla de juridiska kraven mot dessa vardagsfrågor kan förenkla och förbättra säkerhetsarbetet hos företagen inom den svenska elförsörjningen.

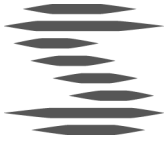
4.2.3 Arkitektur – slutsatser

Svenska Kraftnät bör verka för att ta fram funktionskrav på vissa IS/IT-säkerhetslösningar eller säkerhetskoncept som är acceptabla, antingen som miniminivåer eller som skydd för vissa särskilt skyddsvärda funktioner. Att ha exempelkataloger eller referensmaterial underlättar inom många verksamheter där det idag saknas kunskap eller resurser att själva ta fram detta. Svenska Kraftnät bör om möjligt samarbeta med Svensk Energi och andra berörda aktörer för att en sådan teknisk referensarkitektur arbetas fram.

Fördelar för Svenska Kraftnät att ta fram funktionskrav till referensarkitektur är många, bland annat.

- Det förenklar för de elföretag som inte har stark kompetens inom IT eller IT-säkerhet att skapa viss grundsäkerhet i sina IT-miljöer. Detta oavsett om de själva utvecklar och driver IT-lösningarna eller om de kravställer och upphandlar det hela som en funktion.
- Elföretag med egen intern kompetens kan stämma av de egna lösningarna mot öppna och gemensamma lösningsförslag.
- Att det vid olika typer av tillsyn och myndighetsutövning går att stämma av befintliga IT-lösningar mot dessa funktionskrav.

Då delar av IT-infrastrukturen för elförsörjning är under stark förändring, inte minst de delar som har med smart mätare eller smarta elnät att göra, så finns det ett behov för Svenska Kraftnät att såväl i linjeform som inom ramen för kommande projekt ha fortsatt bevakning av standardisering, både de facto och faktiskt arbete inom internationella standardiseringsorgan, inom området.



4.2.4 Instruktioner, checklistor, mallar och handböcker - slutsatser

Svenska Kraftnät bör inleda ett arbete med att ta en portfölj av olika dokument och material som understödjer arbetet med förbättrad IS/IT-säkerhet inom elförsörjningen.

Genom att ta fram mallar, checklistor och ett enklare metodstöd så säkerställer Svenska Kraftnät att även de mindre aktörerna på marknaden ges en möjlighet att genomföra adekvata riskanalyser och säkerhetsanalyser.

Det bör klargöras vilket arbete som bäst utförs av Svenska Kraftnät, andra myndigheter med arbete inom området samt andra intressenter, främst branschorganisationen Svensk Energi och elföretagen själva.

Ett särskilt område som bör täckas in av det framtagna materialet är hantering av integritetskänslig information i de nya typer av tjänster som elbranschen utvecklar, främst smarta mätare och smarta elnät Detta kan innebära nya typer av myndighetskontakter, främst med datainspektionen.

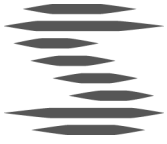
Det material som tas fram bör i görligaste mån framställas på både svenska och engelska då elföretagen idag lever i en situation med internationella leverantörer eller supportpersonal. Eller där företagen är uppbyggda så att delar av de organisationer påverkar svensk elförsörjning bemannas av personal utomlands.

4.2.5 Utvecklingsmått

Vi föreslår att Svenska Kraftnät följer upp utvecklingen och förändringen rörande IS/IT-säkerhetsmognaden inom den svenska elförsörjningen, så att det går att analysera hur projektets leverabler tas emot. Ett konkret förslag är att ta fram metoder som tillåter Svenska Kraftnät att följa IS/IT-säkerhetsutvecklingen inom sitt sektorsansvar.

4.2.6 Utredning om utlokalisering av kritisk elverksamhet

Den utredning som omnämns i avsnitt 3.6.2, *Utlokalisering av kritisk elverksamhet,* innehåller slutsatser och förslag på åtgärder och aktiviteter som bör genomföras för att bemöta berörd problematik. Tillämpliga delar av dessa förslag har inarbetats som aktivitetsförslag.



5 Referenser

[Ref.1]
http://stopsmartmeters.org/

[Ref.2]
http://www.tno.nl/downloads/Assessment%20of%20the%20implementation%20regulations%20for%20Smart%20Meters.pdf

[Ref.3]
http://www.google.com/url?sa=t&rct=j&q=dutch%20smart%20metering%20law&source=web&cd=3&sqi=2&ved=0CDgQFjAC&url=http%3A%2F%2Fwww.rijksoverheid.nl%2Fbestanden%2Fdocumenten-en-publicaties%2Frapporten%2F2010%2F10%2F25%2Fsmart-meters-in-the-netherlands%2F10-1193-final-report-smart-metering-ez-draft-v1.pdf&ei=hcQfT97PLoOusgaW9IG7DA&usg=AFQjCNEw4ZWR3aW5t-68W4mWZnJOobhupQ

[Ref.4]
"28c3: Smart Hacking for Privacy" video från konferensen 28c3 http://www.youtube.com/watch?v=YYe4SwQn2GE

[Ref.5]
http://cees.delaat.net/rp/2007-2008/p33/report.pdf

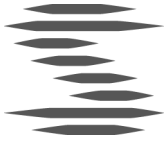
[Ref.6] sid 6
http://www.energiened.nl/_upload/bestellingen/publicaties/355_320005%20-%20PS%20M%20Main.pdf

[Ref.7]
http://www.energiened.nl/_upload/bestellingen/publicaties/288_Dutch%20Smart%20Meter%20%20v2.1%20final%20Main.pdf

[Ref.8]
http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[Ref.9]
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[Ref.10]
http://www.us-cert.gov/control_systems/pdf/Cross-Sector_Roadmap_9-30.pdf



[Ref.11]
http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf

[Ref.12]
http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf

[Ref.13]
http://www.nerc.com/page.php?cid=2%7C20

[Ref.14]
http://www.nia.din.de/projekte/DIN+SPEC+27009/en/146942293.html

[Ref.15]
https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html