FFI RAPPORT

SÅRBARHET I KRAFTFORSYNINGENS DRIFTS- OG STYRINGSSYSTEMER

RODAL Siv Kjersti

FFI/RAPPORT-2001/04278

FFISYS/769/204.0

Godkjent
Kjeller 4 desember 2001

Jan Erik Torp
Forskningssjef

SÅRBARHET I KRAFTFORSYNINGENS DRIFTS- OG STYRINGSSYSTEMER

RODAL Siv Kjersti

FFI/RAPPORT-2001/04278

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
Postboks 25, 2027 Kjeller, Norge

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
NO-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER	2) SECURITY CLASSIFICATION	3) NUMBER OF PAGES
FFI/RAPPORT-2001/04278	UNCLASSIFIED	26
1a) PROJECT REFERENCE	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE**	
FFISYS/769/204.0	-	

4) TITLE

SÅRBARHET I KRAFTFORSYNINGENS DRIFTS- OG STYRINGSSYSTEMER

VULNERABILITIES IN THE INFORMATION SYSTEMS OF THE ELECTRIC POWER SUPPLY

5) NAMES OF AUTHOR(S) IN FULL (surname first)

RODAL Siv Kjersti

6) DISTRIBUTION STATEMENT

Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) Analysis of vulnerability	a) Sårbarhetsanalyse
b) Electric Power Supply	b) Kraftforsyning
c) Information Security	c) Informasjonssikkerhet
d) Threats	d) Trusler
e) Critical Infrastructure	e) Kritisk infrastruktur

THESAURUS REFERENCE:

8) ABSTRACT

This report presents a short overview of the results from the study of the vulnerability of the information systems in the Norwegian electric power system to physical, electromagnetic and logical threats. Generally, centralised management, with remote control of generation and distribution of power, is performed from system control centers. The operations are supported by SCADA (Supervisory Control And Data Acquisition) systems.

The study shows that the information systems are vulnerable to a multitude of physical, electromagnetic and logical threats, both natural and man-made. Thus, computer failure may lead to short-term local disruptions in the power supply. However, to achieve long-term outages, simultaneous attacks have to be executed at the power infrastructure and at the information systems.

The report contains a scenario, describing the growing dependency on information systems until 2010. A possible large-scale implementation of electronic components in the grid, increased dependency on centralised management and a predicted shortness of skilled personell are key factors in this scenario. This may lead to a more unreliable and vulnerable power system, prone to frequent failures and disruptions.

9) DATE	AUTHORIZED BY	POSITION
	This page only	
4 December 2001	Jan Erik Torp	Director of Research

ISBN-82-464-0560-8

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

INNHOLD

SÅRBARHET I KRAFTFORSYNINGENS DRIFTS- OG STYRINGSSYSTEMER

1 INNLEDNING

Fra siste verdenskrig og frem til i dag har det skjedd en rivende utvikling av samfunnet. Dette er blant annet et resultat av teknologiske nyvinninger og økt globalisering av økonomien. Resultatene er en utstrakt spesialisering og sentralisering av virksomheter, økende avhengighet av internasjonale markeder og en samfunnsstruktur fundamentert på elektronisk utveksling av informasjon gjennom globale telekommunikasjonssystemer.

Utviklingen har gitt økt materiell velstand, men har samtidig gjort samfunnet vesentlig mer sårbart. Informasjonssikkerhet er i ferd med å bli svært sentralt for de fleste prosesstyrte samfunnsfunksjoner. Sentrale funksjoner i samfunnet kan dermed lammes med enkle virkemidler, også uten at landets fysiske grenser krenkes. Dette representerer en ny type trussel mot vår suverenitet og sikkerhet, og representerer nye utfordringer for vår beredskapsstenkning.

Dette gjelder også for kraftforsyningen som både direkte og indirekte avhenger av bruk av informasjonssystemer til distribusjon av elektrisitet og fjernstyring av anlegg. Kraftforsyningen er inne i en rivende utvikling både markedsmessig og teknologisk, og behovet for god informasjonsformidling øker. Informasjonssikkerhet er derfor en sentral og komplisert problemstilling innen sektoren. De mest aktuelle truslene mot kraftforsyningen er derfor i ferd med å bli dramatisk endret.

Denne rapporten belyser sårbarhet i informasjons- og kommunikasjonsteknologi innen norsk kraftforsyning, og inngår i BAS3-prosjektet[1] som ble gjennomført ved FFI i perioden 1999 - 2001. Rapporten identifiserer også mulige sårbarhetsreduserende tiltak, og gir dermed en presentasjon av ulike tiltakskategorier som kan gi norsk kraftforsyning en akseptabel sikkerhet overfor ulike trusler i fred, krise og i krig.

Innholdet i rapporten ligger på et overordnet nivå, og rettes mot ledere og saksbehandlere i Totalforsvaret, samt beredskapsansvarlige i kraftforsyningen. Det er også skrevet en mer omfattende gradert rapport om dette temaet (1).

2 SAMMENDRAG

Produksjon og fordeling av kraft styres i økende grad sentralt ved hjelp av moderne informasjonssystemer[2]. Dette gir effektive løsninger for drift av kraftforsyningen i hverdagen. Et slikt fjernstyringskonsept åpner imidlertid for nye sårbarheter i systemet. Dette gjelder spesielt overfor ekstremsituasjoner hvor mennesker målrettet gjennomfører anslag mot kritiske punkter i kraftsystemet.

[1] BAS3 (Beskyttelse av samfunnet 3 - Sårbarhetsreduserende tiltak innen kraftforsyning) er det tredje i rekken av prosjekter som har satt fokus på sårbarheten i det norske samfunnet.
[2] Fjernstyringssystemer

Analysen viser at informasjonssystemene er sårbare overfor en rekke fysiske, elektroniske og logiske trusler, både overfor tilsiktede og utilsiktede hendelser. For driftssystemene vil dataproblemer alene sannsynligvis kun gi lokale forstyrrelser i kraftsystemet for en kort tidsperiode, mens det kreves flere samtidige anslag mot både den fysiske kraftinfrastrukturen og informasjonssystemene for å forårsake langvarige konsekvenser. Den logiske tilgangen til bedriftenes informasjonssystemer er begrenset, men utro tjenere øker mulighetene for uønsket tilgang til systemene.

Kraftindustrien preges av sterk markedsvekst, internasjonalisering og reduserte marginer der den eksisterende infrastrukturen i økende grad utnyttes maksimalt. Dette gjør at informasjonsutvekslingen blir enda mer kritisk for å opprettholde en stabil kraftforsyning, og gir et økende behov for dataverktøy som automatisk regulerer kraftflyt i kraftnettet. Såfremt teknologien som kommer på markedet i fremtiden gir klare gevinster og økt ytelse av infrastrukturen, er det naturlig å forvente at kraftbransjen tar den i bruk. Kombinert med en forventet mangel på kompetanse og personell i sektoren kan dette gi et mer sårbart kraftsystem.

Samfunnets kritiske avhengighet av en stabil kraftforsyning, samt et fremtidig usikkert trusselbilde, tilsier derfor at det bør iverksettes sårbarhetsreduserende tiltak. Konsekvensene for samfunnet er store ved langvarig strømbortfall, og selv ved kortvarig bortfall stopper mange samfunnsfunksjoner opp.

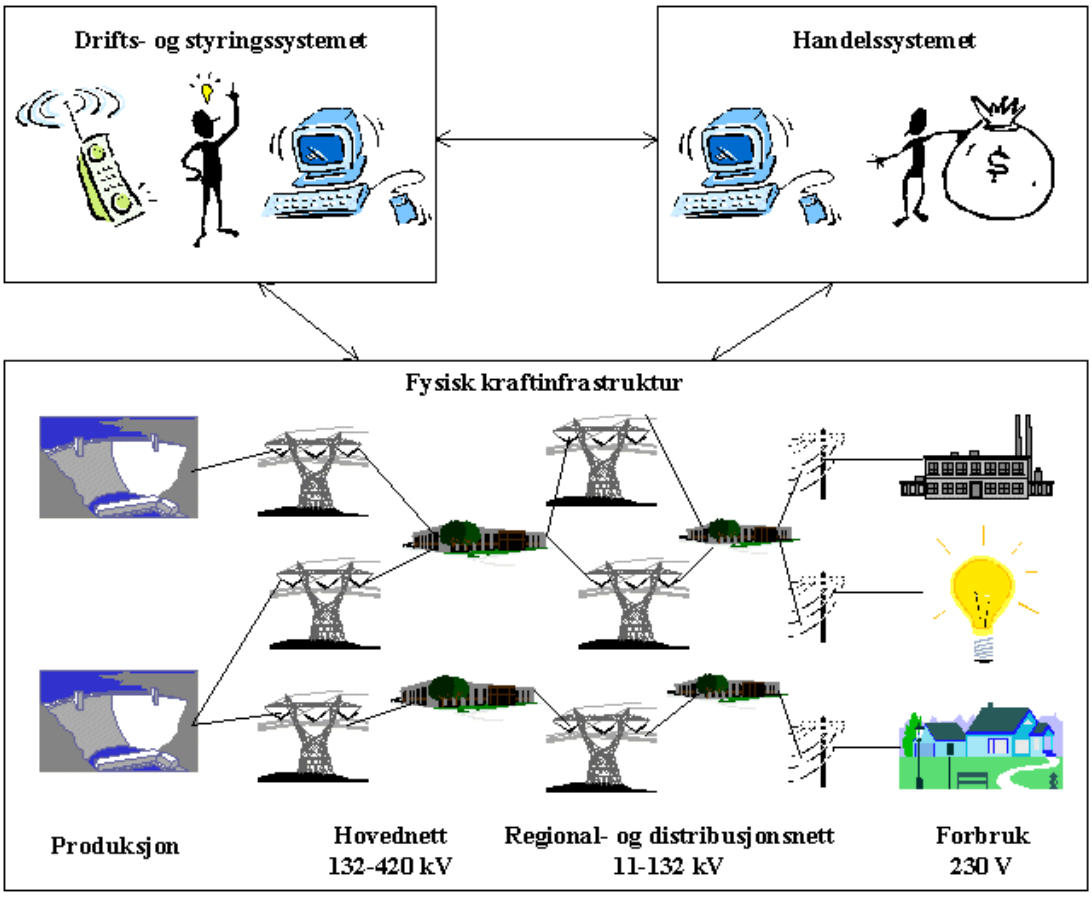
3 INFORMASJONSAVHENGIGE FUNKSJONER INNEN KRAFTFORSYNING

Dette kapitlet gir en kort innføring i kraftsystemets behov for informasjonssystemer.

3.1 Modell av kraftforsyningen

Kraftforsyningen i Norge er et integrert sammenbundet system av regionale og lokale forsyninger. Figur 3.1 viser en modell av dette systemet. I modellen inngår *den fysiske infrastrukturen* som produserer og overfører elektrisk kraft, *drifts- og styringssystemer* som sørger for en effektiv drift av kraftforsyningen, og *handelssystemet* for kjøp og salg av elektrisk kraft (2).

Statnett er i dag systemansvarlig for kraftforsyningen i Norge, slik at systemdriftsansvaret utøves fra Statnetts Landssentral. De store driftssentralene, inkludert Statnetts egne regionale driftssentraler, har derfor rapporteringsplikt til Landssentralen.



Figur 3.1 Modell av norsk kraftforsyning

3.2 Informasjonssystemer

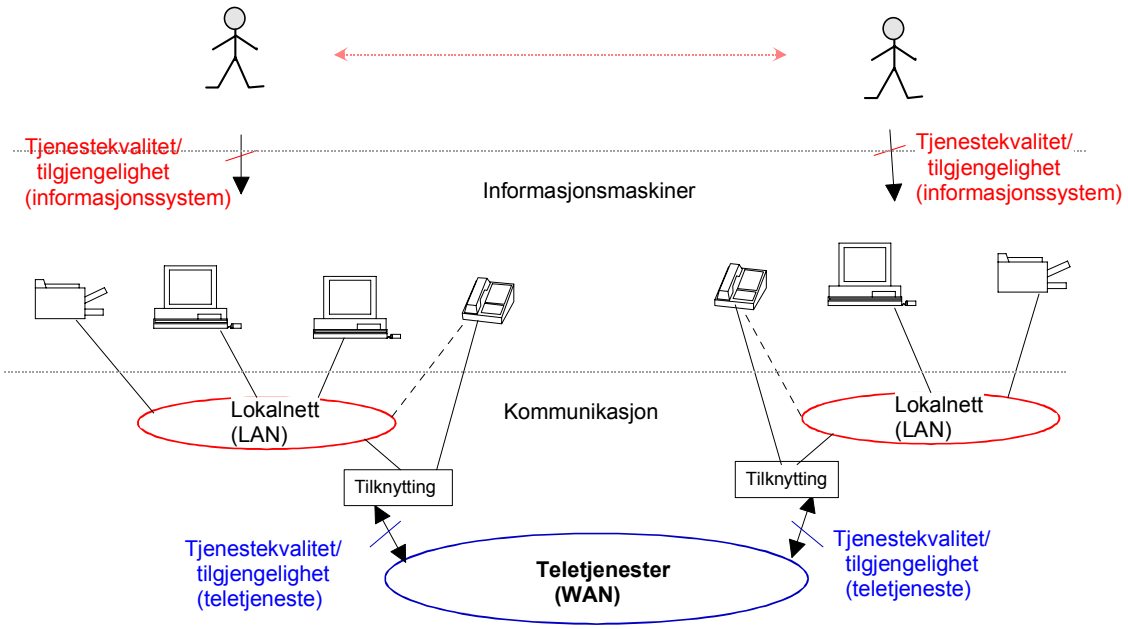
Informasjonssystemer benyttes i dag hovedsakelig til å utføre bestemte automatiske arbeidsoppgaver, og er et medium for utveksling av informasjon. Et informasjonssystem består av en kombinasjon av datamaskiner med tilhørende periferiutstyr, programvare og nødvendige kommunikasjonssystemer (Figur 3.2).

Kommunikasjonssystemet som informasjonsmaskinene i informasjonssystemet tilknyttes kan deles inn i to hovedtyper: Lokalnett (LAN)[3] og telenett (WAN)[4].

Lokalnettet er den delen av kommunikasjonssystemet som står for informasjonsoverføring mellom informasjonsmaskiner innenfor et geografisk begrenset område. Dette begrensede området vil normalt være under brukerens kontroll. *Telenettet* kobler geografiske områder sammen (se Figur 3.2). Gjennom en sammenkopling av lokalnett og telenett utføres informasjonsutveksling med andre deler av foretaket eller eksterne aktører, for eksempel kunder.

Formidling av informasjon via det offentlige telenettet omtales som *telekommunikasjon.*

[3] Local Area Network
[4] Wide Area Network



Figur 3.2 Informasjonssystem

3.3 Kraftforsyningens driftssystem

Norsk kraftforsyning er et *just-in-time system,* der det til enhver tid må være samsvar mellom forbruk og produksjon for at det ikke skal oppstå systemsvikt med påfølgende kraftutfall. Produksjonsstrukturen i Norge er svært desentralisert. Totalt finnes det ca 550 produksjonsanlegg med mer enn 1 MW installert effekt spredt over hele landet (2). Brukerne er også spredt over et stort geografisk område, der de klimatiske forholdene og behovet for fyring og lys varierer over døgnet og over året. Det at produksjonen til en hver tid skal være lik forbruket krever derfor rask kommunikasjon og informasjonsutveksling mellom en rekke aktører. Som følge av dette er kraftforsyningen en kommunikasjonsintensiv bransje.

I de siste årene har moderne informasjons- og kommunikasjonsteknologi blitt tatt i bruk for drift av de ulike delene av kraftforsyningen. Der det tidligere var ansatte på hvert eneste kraftforsyningsanlegg som styrte den aktuelle installasjonen manuelt, fjernstyres nå anleggene fra et fåtall driftssentraler. Dette gjøres ved hjelp av kompliserte IT-systemer og et velfungerende samband.

Kraftforsyningens driftssystem kan grovt deles inn i to kategorier:

- Styrings- og støttesystemer som står for styring, kontroll og overvåking[5]
- Informasjonssystemer til administrativ bruk

Driftens støttesystem er datasystemer innen teknisk og administrativ del av drift og vedlikehold som inneholder opplysninger om overføringskapasitet og tilknytninger i hovednettet[6] og

[5] Den samlede løsning for dette kalles Energy Management System (EMS), og består bl a av et Supervisory Control and Data Aquisition (SCADA)-system for overvåking og fjernstyring av underliggende stasjoner (prosesstyring), databaser og programmer for lastflytberegninger, optimaliseringer og simulering av dynamiske tilstander.

[6] Det vil si hvilken overføringskapasitet som er tilgjengelig, hvordan den brukes og hvor i nettet den finnes. Dette inkluderer informasjon om planlagte utkoblinger, hvilke komponenter som er operative etc.

distribusjonsnettet[7], administrativ informasjon om for eksempel forbruk, metrologisk data som værdata og snødybde samt geografisk relatert informasjon om kraftsystemets fysiske struktur.

Styringssystemer fjernstyrer ulike prosesser i kraftproduksjon eller nettdrift via dataformidling eller telefoni. Dersom dette svikter er det med enkelte unntak mulig med nærstyring/lokalstyring på anleggene, der nødvendig koordinering skjer via telefoni eller faks. Ved flere anlegg innen et geografisk begrenset område kan også mannskapet kjøre mellom de ulike punktene hvis telefonnettet svikter.

Eksempler på prosesser som kan styres er brytestillinger av koblingspunkt i nettet, effektbrytere og regulering av lastflyt i nettet, trinnoperasjoner på transformatorer og inn- og utkoblinger (brytestillinger) av kompensatorer, ventiler, aggregater, systemvern[8] og komponentvern[9]. Konfigurering av enheter, registrering og sletting av enheter skjer også gjennom drifts- og vedlikeholdssystemer. Selve prosesstyringen kan skje automatisk f eks ved utløsing av vern når fastsatte grenseverdier overskrides, eller besluttes av en beslutningstaker på driftssentralen.

Foruten en slik *prosessorientert informasjon* er det også nødvendig med *administrativ informasjon* for drift av de støttesystemer kraftbransjen trenger for at prosessene skal kunne gå effektivt. Dette innbefatter informasjon om eget personell, ansvarsområder, arbeidstider, lønn, organisatoriske rutiner, forsikringer, serviceavtaler på anlegg samt innkjøp av et bredt spekter av varer og tjenester fra store deler av samfunnet; transport, bank/finans, olje- og drivstoff, industri- og varehandel m m. I sammenheng med sårbarhet i kraftforsyningen er det imidlertid de prosessrelaterte oppgavene som er de mest kritiske.

Driftssystemer lokaliseres på driftsentralen og tilknyttes kraftinfrastrukturen via telenettet. Kraftforsyningen har bygget et eget sambandsnett (telenett), men i flere tilfeller kjøpes kapasitet i det offentlige telenettet. Kraftforsyningens egen nasjonale sambandsinfrastruktur dekkes for det meste av Statnetts telenett[10], men suppleres i noen grad med satellittsamband og leide linjer fra f eks Telenor. Systemene for kontroll og overvåkning av de enkelte nettelementene i telenettet som benyttes bl a for omruting av samband og oppgradering av software er ofte plassert i driftssentralene.

4 KONSEKVENSER FOR KRAFTFORSYNINGEN VED SVIKT I IKT

Den nødvendige koordineringen mellom strømforbruk og produksjon av kraft gjør kraftforsyningen svært sårbart overfor ukontrollerte koblinger i infrastrukturen. Dersom en inntrenger får tilgang til å koble bort ulike komponenter i systemet som linjer, generatorer, vannveier, luker etc, kan likevekten mellom forbruk og produksjon forstyrres, og forsyningen svikte selv i en normaltilstand.

I et velfungerende kraftsystem er det viktig at frekvensen holdes stabil. Såkalt sekundærregulering (ved å slå av og på aggregater) er derfor helt nødvendig for å kunne justere

[7] Det vil i hovedsak si lokalkabler i distribusjonsnett.
[8] Systemvern: Slå av og på vern på generatorer.
[9] Komponentvern: Slå av og på vern ved skader på linjer, transformatorer etc.
[10] WAN som går over store områder.

effekten opp eller ned ved svingninger i forbruket. Uteblir denne reguleringen ved et tidspunkt da forbruket endres betraktelig forandres frekvensnivået. Ustabilt frekvensnivå kan i verste fall medføre at anlegg kobles ut, og at kraftnettet kollapser.

Aggregatenes forhåndsinnstilte systemvern bidrar til å kontrollere kraftproduksjonen. Ut i fra forhåndsinnstillingen kan disse vernene reguleres av operatører på driftssentralene. Hindres dette oppstår normalt kun regionale problemer. Ukontrollerte justeringer av komponentvern er derimot alvorligere. Komponentvern brukes for eksempel til å regulere hvor mye last det kan gå mellom to ulike punkter i nettet. Koordinerte feiljusteringer av lastmengde mellom vernene på flere steder samtidig kan påføre nettkollaps. For å redusere ødeleggelsene er det i en slik situasjon nødvendig for systemleder å kunne foreta de rette koblinger i kraftnettet. Ved svikt er derfor tilgjengelighet til å justere innstillinger på vernene viktig. Uønskede justeringer på disse vernene kan derfor gi store konsekvenser for kraftnettet, men i dag må dette gjøres ved anleggene.

Siden mye av "lastflytinformasjonen" ligger i enhetene i nettet eller ved anleggene er dagens driftssystem først og fremst et viktig hjelpemiddel for å få systemet på fote igjen i tilfelle det oppstår feil. Kortere bortfall av driftssystemet er derfor ikke kritisk for kraftforsyningen i en normalsituasjon, og selv om driftsnettet er nede vil lasten flyte normalt.

Vanligvis kreves det derfor skade på både informasjonssystemene og samtidig fysisk skade på kraftinfrastrukturen før det gir større konsekvenser for driftsfunksjonen. I en slik situasjon er driftsfunksjoner avgjørende for å kunne utnytte den gjenværende kapasiteten i nettet på best mulig måte, og utbedre skadene så raskt som mulig. Selv om feilsøking og beslutninger i verste fall kan gjøres ved hjelp av manuelle metoder er dette svært tidkrevende, og avhenger normalt av talekommunikasjon eller faks. Uten noen form for kommunikasjon vil den nasjonale eller regionale oversikten forsvinne, slik at samkjøring mellom de ulike regionene hindres. Sannsynligheten for å gjøre feiloperasjoner er derfor høy. Manipulering av den sentrale overvåkingen for registrering av lastflyt kan også gi feilinformasjon om belastning i nettet, og dermed medføre overbelastning. En vel fungerende driftsfunksjon er derfor av sentral betydning. Konsekvensene for totalsystemet avhenger imidlertid av hvilke og hvor mange bedrifter som angripes samtidig.

5 TRUSSELEN MOT KRAFTFORSYNINGEN

Norges sikkerhetspolitiske situasjon er i dag overveiende positiv. Forholdene i våre nærområder er relativt stabile, både politisk og militært. Russland er inne i en positiv utvikling, og landet utgjør per i dag en begrenset militær trussel mot Norge. Selv om dette kan endres raskt er det lite sannsynlig med et omfattende angrep mot norsk territorium i overskuelig fremtid (4). Innenfor prosjektets tidshorisont, de nærmeste 10 årene, er det vanskelig å se for seg en krigstrussel mot landet i form av en invasjon.

Mer begrensede angrepsscenarier kan derimot ikke utelukkes. Europa er preget av et mer sammensatt risikobilde enn under den kalde krigen. I første rekke skyldes dette Norges

engasjement i den pågående bekjempelsen mot terrorsime. I tillegg kan uroligheter på Balkan og andre konflikter spre seg, og dermed få indirekte konsekvenser også for land som Norge (4). Norge kan også være utsatt på grunn av sin strategiske viktige rolle som viktig leverandør av energi. Forsvarets engasjement i fredsoperasjoner i regi av NATO kan også bidra til å eksponere norsk territorium og norske interesser for hevnaksjoner, f eks i form av terrorhandlinger. Det er dermed mulig at Norge kan bli trukket inn i ulike utradisjonelle typer kriser, og at norsk territorium og norske interesser kan rammes av aksjoner.

Frem til nå har det vært få eksempler på sabotasjeaksjoner mot norsk kraftforsyning. Kraftforsyningen i Norge har stort sett bare blitt utsatt for mindre hærverk, med unntak av miljøaksjoner i forbindelse med utbygging av nye produksjonsanlegg. Også i internasjonal sammenheng er kraftforsyningen lite utsatt i fredssituasjoner. I krise øker faren for aksjoner mot kraftforsyningen, og i krig er kraftforsyningen et klart utsatt mål (jfr Golfkrigen og Kosovo-krigen).

Den vanligste årsaken til omfattende strømbrudd i hverdagen er dårlig vær. Naturhendelser kan typisk gi strømbrudd i inntil én uke. En annen årsak som har meldt seg internasjonalt de seneste årene er utilsiktede bivirkninger av deregulering av kraftmarkeder. Dereguleringsregimer med ensidig fokus på effektiv drift gir som regel ingen motivasjon til vedlikehold og investeringer. Dette fører før eller senere til teknisk sammenbrudd i nedslitt utstyr som over lengre tid er presset hardere enn det er konstruert for.

Selv om kraftforsyningen i dag er lite utsatt for angrep, kan dette bildet endres i fremtiden. Et bekymringsfullt utviklingstrekk i så måte er den økende IKT-avhengigheten i kraftforsyningen. Dette tilsier at sannsynligheten for dataangrep mot kraftforsyningens systemer kan øke. Norsk kraftforsyning har imidlertid liten erfaring med denne typen anslag, men det finnes eksempler på at kraftforsyningen i andre land har blitt utsatt for hacking, der utenforstående har klart å manipulere prosesstyringen slik at det har resultert i strømbrudd.

Tidligere analyser vurderer at risikoen for logiske angrep som omfatter bruk av ulike software-teknikker til å innhente etterretning eller ødelegge og degradere informasjonssystemer er stor uansett samfunnstilstand, og kan relateres til alle IT- avhengige funksjoner i samfunnet, deriblant kraftsystemets informasjonssystemer og deres tjenester (1) (3). Den generelle trenden i samfunnet er økende bruk av hacking til ulike formål.

Tabell 5.1 gir en oppsummert vurdering av sannsynligheten for at ulike typer angrep inntreffer innen denne analysens tidshorisont. Sannsynligheten er kvalitativt gitt med følgende definisjoner:

- Lav : sporadiske angrep kan inntreffe
- Middels : systematiske angrep kan inntreffe
- Stor : systematiske og velplanlagte angrep vil inntreffe

	Fysisk trussel[11]	**Elektromagnetisk trussel**[12]	**Logisk trussel**[13]
Fred	Lav	Ikke reell	Lav
Krise	Stor	Lav	Middels
Krig	Stor	Middels	Stor

Tabell 5.1 Trusselsannsynlighet sett ut fra dagens situasjon

Sannsynligheten for fysiske anslag i *krisesituasjoner* anses som stor, mens den tilsvarende logiske trusselen er middels. Dagens erfaringer fra kriger og konflikter viser at hovedvekten av trusler ligger på den fysiske siden. Hittil har det også i fredssituasjoner vært mest vanlig med eksplosiver og fysisk makt ved sabotasjeaksjoner mot kraftforsyningen.

Med tiltakende konfliktnivå er det et stort spenn av virkemidler som kan tenkes brukt mot kraftforsyningen. Likevel er det et viktig moment at kraftforsyningen har en omfattende infrastruktur, som det er ressurskrevende å lamme via fysiske anslag. I en eskalert situasjon er samtidig kraftforsyningen kun ett av mange mulige mål, og det er derfor usikkert hvor store ressurser som faktisk kan tenkes brukt mot kraftsystemet. Samlet kan slike forhold bidra til å gi et skift i sannsynlighetsmatrisen skissert i Tabell 5.1, i form av at logiske trusler øker i betydning sammenlignet med fysiske. Først i de senere årene har det blitt reelt å snakke om en logisk trussel, men på dette området skjer utviklingen fort. *Den skisserte trusselsannsynligheten kan derfor endres i løpet av kort tid*.

6 SÅRBARHET I KRAFTFORSYNINGENS IKT-SYSTEMER

Sårbarhetsvurderingen som gis i de etterfølgende avsnittene er relatert til figurene i kapittel 3 som viser kraftforsyningens og informasjonssystemenes prinsipielle oppbygning.

6.1 Sårbarhet i drifts- og støttesystemer

6.1.1 Sårbarhet i telenettene

Alvorlige og langvarige forstyrrelser av kraftbransjens teleressurser kan medføre at alle teknologiavhengige prosesser innen kraftbransjen stoppes. Kraftbransjens telenett er ikke bygget med tanke på at det skal motstå direkte, systematiske anslag i en krigssituasjon, men er etablert ut fra den forutsetning at offentlige telenett kan bli satt ut av tjeneste. Det er dermed et ønske om å være uavhengig av offentlige teletjenester i driften av norsk kraftforsyning, men dette er ikke fullt ut situasjonen i dag.

Flere steder må kraftforsyningen leie kapasitet av aktører i markedet fordi det blir for kostbart å bygge egen infrastruktur. Dette forholdet vil med stor sannsynlighet forsterkes i fremtiden, slik at en økende bruk av offentlige teletjenester er sannsynlig. Samtidig er offentlige løsninger

[11] Fysiske trusler, m a o direkte fysisk våpenvirkning (konvensjonelle våpen, fysisk sabotasje, eksplosiver, o l).
[12] Elektromagnetiske trusler, m a o jamming og bruk av elektromagnetiske strålingsvåpen.
[13] Logiske trusler, m a o bruk av ulike former for programvare og programvarebasert maskinvare som virkemiddel til å ødelegge eller degradere IT-systemer.

primærsambandet mot eksterne aktører i en krisesituasjon. Mulighetene for å sikre tilgjengelig samband i fremtidens kraftforsyning må derfor ses i sammenheng med de sårbarhetsreduserende tiltak som eventuelt settes inn i offentlig telekommunikasjon. Dessuten kan det på flere punkter dras direkte paralleller mellom Statnetts eget telenett og de offentlige telenettene.

FFI-notatet "Informasjonssikkerhet innen telekommunikasjon" drøfter sårbarhet i forhold til telenett (5). Analysen indikerer at informasjonssystemer innen offentlig telekommunikasjon har svakheter som muliggjør å sette teledriftssystemet og trafikkaviklingen ut av spill. Eksempelvis kan uvedkommende oppnå kontroll med funksjoner som blant annet påvirker tilgjengeligheten til de aktuelle teletjenestene dersom de trenger inn i vitale punkter i den offentlige teleinfrastrukturen. For Statnetts eget telenett kan eksempelvis de proprietære systemene i tilknytning til driftssentralene benyttes for å omrute teletrafikken. I praksis krever dette at en eventuell angriper har insidere innen organisasjonen, evt at en selv inntar en av sentralene og får tilgang til systemene. Når det gjelder selve driftsystemet for telenettene er dette kun et viktig hjelpemiddel for å få systemet på fote igjen i tilfelle det oppstår feil i telenettet. Dessuten kan feilsøking også gjøres ved hjelp av manuelle, om enn litt mer tidkrevende metoder.

Teleoperatørenes sammenkoblinger av sine telenett for å oppnå samtrafikk[14] åpner de enkelte operatørenes telenett for aktører utenfor bedriften, og øker dermed sannsynligheten for at uvedkommende får tilgang til vitale punkter i telenettene. Samtrafikk mellom teleoperatører øker og gir verdensomspennende nett. Det stilles imidlertid ofte for få sikkerhetsmessige krav til de ulike partene, samtidig som de tekniske prinsippene bak samtrafikk i utgangspunktet ikke bygger på sikkerhet. Uønskede hendelser i samtrafikkpunkter kan dermed gi store konsekvenser for trafikkavviklingen[15]. Til i dag har imidlertid erfaringer vist at samtrafikk ikke representerer større sikkerhetsproblemer selv om det har vært brukt over landegrensene i flere år. Dette kan sannsynligvis forandres, og eksempelvis Telenor tar i dag denne trusselen på alvor (5).

I tillegg til disse driftsrelaterte sårbarhetene finnes det en rekke tekniske sårbarheter i kraftbransjens ulike sambandsløsninger (1). Kraftforsyningen trekker ofte frem dublerte samband som et viktig og nødvendig tiltak for å sikre mot at enkeltinstallasjoner skal oppleve sambandssvikt. Det finnes imidlertid flere eksempler i bransjen på at dubleringstanken er vanskelig å følge fullt ut.

6.1.2 Sårbarhet i lokalnettene

I utgangspunktet skal kun den administrative delen av driften innen kraftforsyningen kobles til offentlige nett[16], slik at administrativ brukerdata og prosessorientert driftsdata normalt går i separate nett. Økende behov for utveksling av data og ønske om bruk av felles interne resurser krever allikevel ofte en fysisk forbindelse mellom disse domenene. Slike koblinger utsetter i økende grad driftssystemene for logiske angrep utenfra. Samtidig reduseres oversikten over

[14] For å utveksle tjenester.
[15] Mulige konsekvenser ved uønskede operasjoner i telesystem er forstyrrelser og redusert driftsstabilitet, reduksjon av systemets evne til å takle enkeltfeil, driftsforstyrrelser med sperr og redusert fremkommelighet, manipulasjon og ødeleggelse av tjenester for eksempel ved å sette opp falske viderekoplinger, økonomisk svindel som for eksempel forfalskning av data for å oppnå vinning, påvirkning av tjenestetilbud samt avlytting eller tapping av operatørenes nett og kompromittering av interne data (trafikkdata, abonnentdata).
[16] Det administrative domenet har kontakt utad til eksterne aktører som NVE, markedsoperatører (Nordpool), systemoperatører, leverandører, nettoperatører og produsenter.

hvem som har tilgang til ulike tjenester innad i bedriften, og gjør dermed driftsdelen mer sårbar for utro tjenere. Dette har imidlertid ikke vært noe stort problem så langt.

I tillegg har leverandører og hjemmevakt normalt tilgang inn til visse deler av driftsdomenet ved bruk av oppringte linjer. Leverandører kan for eksempel ha behov for å styre og optimalisere systemene samt å drive service. Ulempen er at oppringt datasamband ofte reduserer oversikten i datanettverk, og reduserer dermed informasjonssikkerheten.

Informasjonssystemene som brukes bygger gjerne på såkalte åpne[17] standardiserte plattformer. Dette er fordelaktig funksjonsmessig, men gjør samtidig systemene mer åpne og tilgjengelige overfor hacking. Kommer alt datautstyret fra samme leverandør med identisk programvare, øker i tillegg sjansene for større og mer omfattende skader.

I dag brukes vanligvis sikkerhetsprodukter og rutiner til å sikre grensesnittene mellom interne og eksterne domener. Sikringen mellom ulike domener *innenfor* bedriften er imidlertid beskjeden. Dette kan skyldes vegring mot å redusere funksjonaliteten i informasjonssystemene. Kraftforsyningen er i dag en økonomidreven industri, der økonomisk tenkning i økende grad tar over. Faren er derfor tilstede for at sikkerhetstiltak omgås av økonomiske årsaker. Det er også kjent at de fleste sikkerhetsprodukter uansett kvalitet kan forseres med litt hackerferdigheter (5). De fleste bedriftene innen kraftforsyningen er derfor sårbare overfor målbevisste og kompetente hackere med nok ressurser og tid.

6.1.3 Utro tjenere

Driften av kraftinfrastrukturen kan være utsatt for utro tjenere som har muligheter til å foreta sabotasje innenfra. Utro tjenere kan eksempelvis plante feil og legge inn virus som kan være svært vanskelig å avdekke. Situasjonen forverres også dersom en utro tjener sitter med kompetanse på drift av kraftforsyningen, og samtidig har tilgang til driftssystemet. Det bør også nevnes at utviklingsingeniører hos utstyrsleverandører som produserer systemer for kraftbransjen har inngående kjennskap til programvarestrukturene og mekanismer i driftssystemer.

Det er opp til hver enkelt leder å avgjøre hvorvidt en ansatt skal sikkerhetsklareres, selv om bedriften er viktige for Totalforsvaret. Kraftforsyningens retningslinjer (RSK) påpeker imidlertid at kun personer med tjenestelige behov gis adgang til høyt graderte opplysninger. Allikevel blir vanligvis ansatte kun kontrollert av ledelsen gjennom samtaler og taushetserklæring. Sikkerhetsklarering av personell gir imidlertid ingen garanti mot at utro tjenere eller andre kan plante feil eller legge inn virus.

6.1.4 Mangel på personell og kompetanse

Personell og kompetanse blir kritisk i årene fremover. Ansatte rasjonaliseres vekk til fordel for IKT-løsninger. Slik systemet er i dag kan kraftforsyningen driftes manuelt i en mulig krisesituasjon, men dette krever tilgang til arbeidskraft og riktig kompetanse. Det er lite sannsynlig at dette behovet kan dekkes dersom utviklingen fortsetter som i dag. Samme forhold

[17] Betegnelsen ”åpne systemer” brukes gjerne på anerkjente standarder som kan knytte sammen ulike typer informasjonssystemer.

vil også påvirke evnen til å reetablere kraftforsyningen etter skader i fremtiden.

Parallelt med dette skiftes fokus fra tradisjonell teknisk kraftkompetanse til kompetanse innen informasjonssystemer. Økende informasjonsavhengighet og kompleksitet forårsaker ofte dårligere helhetsforståelse, og som følge av dette feil beskyttelse av informasjonssystemene. Eksempelvis kan sviktende kompetanse ved valg av ny teknologi medføre at feil og mangler ikke oppdages under testing. Det kan derfor tenkes at policyen og tankene om egen kompetanse og sikkerhet ikke alltid henger sammen med de praktiske tekniske tiltak som er implementert. Ulike tester har også vist at det er mulig å trenge inn i informasjonssystemer, selv der sikkerhetsmekanismer er implementert.

Kraftbransjens outsourcing av tjenester på IT-siden reduserer kompetansen i hver enkelt bedrift. Selv om det er få selskaper som per dags dato har satt bort slike tjenester, er dette noe som meget vel kan komme til å skje i flere selskaper i fremtiden. De eksterne leverandørene er imidlertid profesjonelle når det gjelder datasikkerhet, og dersom bedriftene selv ikke klarer å rekruttere kompetent IT-personell er det nødvendig. Likevel gjør dette at flere mennesker enn tidligere har tilgang til driftssystemene.

6.2 Sårbarhet på grunn av sentralisering

Det er stor forskjell mellom kraftselskapene når det gjelder behovet for ekstern kommunikasjon med egne anlegg og installasjoner. De store regionale selskapene har et mye større kommunikasjonsbehov i vanlig drift enn små lokale selskaper med nærhet til egne installasjoner og anlegg. Følgelig er de små selskapene mindre sårbare overfor kommunikasjonsbrudd enn de store.

Trenden går allikevel mot større og færre aktører innen kraftforsyningen, og en naturlig følge av dette er færre men større driftssentraler som håndterer mange underliggende anlegg. Konsentrasjon og sentralisering har vært nøkkelord for utviklingen innen kraftforsyningen de siste ti årene. Den enkelte driftssentral bli dermed viktigere for kraftforsyningens evne til å fungere, og øker mulighetene til å svekke større deler av kraftsystemet ved få anslag.

Ved koordinering av kraftinfrastrukturen i en krisesituasjon kan sentralisering derimot være en fordel. Under isstormen i Canada i 1998 ble det trukket frem som viktig for beslutnings- og koordineringsevnen at det bare var ett stort selskap i det rammede området. Dessuten fører dagens komplekse systemer til et betydelig større behov for kompetanse enn tidligere, og en konsentrasjon av komplekse systemer er derfor en fordel for operatørene siden denne kompetansen trengs på færre steder.

Driftssentralenes fysiske krav til sikringstiltak rettes vanligvis mot brann og innbrudd, det vil si låsing, alarmer og alternative kontrollrom. Mulighetene for å innta en slik bygning uten store ressurser er likevel tilstede.

Siden kravet om sikring mot elektromagnetisk pulsvåpen i flere tilfeller ikke er oppfylt, selv ikke for de viktigste anleggene, kan elektronisk utstyr raskt ødelegges ved bruk av slike våpen. Sikring mot elektromagnetisk pulsvåpen er forbundet med store kostnader, men for hovednettet

vil alle deler av styringssystemet være sikret mot deler av denne typen våpen om kort tid.

Ved distribuerte driftssentralløsninger for store aktører kan også andre driftssentraler ta over prosesstyringen dersom en av sentralene faller bort. Dette er mulig å løse rent teknisk, men er ikke tatt i bruk i dag. Normalt kan derfor ikke en driftssentral drifte andre driftssentralers understasjoner. Enkelte aktører vurderer imidlertid å innføre slike løsninger.

6.3 Konkurransens rolle i et sårbarhetsperspektiv

Kraftsystemet er tett sammenkoplet med handelssystemet for kjøp og salg av kraft (6). Det norske kraftmarkedets deregulering i 1991 endret i stor grad rammevilkårene for aktørene. Fri konkurranse ble innført på produksjons- og forbrukernivå, mens nettenhetene måtte operere under monopolkontroll for å sikre samfunnsøkonomisk optimal drift.

Dagens monopolregulering reduserer mulighetene til å tjene penger innenfor kjerneområdet, og stimulerer derfor bedriftene til å finne nye inntjeningsmuligheter via såkalt bransjekonvergens. Etter hvert som bedriftene i kraftmarkedet i større utstrekning også inkluderer annen tjenesteproduksjon vil det totale informasjonsbehovet, og dermed antall aktører tilknyttet kraftbransjens informasjonssystemer øke. Dersom kraftbransjens informasjonssystem kobles opp mot de andre tjenestene bedriften betjener kan det bli vanskelig å ”nødstoppe” informasjonssystemene ved behov.

Aktørene i markedet trenger tilgang på informasjon om tilstanden i kraftsystemet for å kunne operere i markedet. Dette er et potensielt sikkerhetsproblem av to grunner. I tillegg til at driftsdelen åpnes for angrep utenfra, blir det et økende press om at sensitiv driftsinformasjon gjøres offentlig tilgjengelig for aktørene i markedet.

6.4 Samlet sårbarhetsvurdering

Det er en betydelig mengde informasjon som skal utveksles mellom et stort antall aktører for at både driftsdelen og kraftmarkedet skal fungere i en ordinær driftssituasjon. Utviklingen tilsier at informasjonsutvekslingsbehovet i fremtiden vil øke ytterligere. Alle sårbarhetselementene over indikerer at informasjonssystemene har svakheter overfor et bredt spekter av trusler.

For å oppnå effekt på totalsystemet bør angrepene sannsynligvis helst rettes mot datakommunikasjonssystemene i driftsnettet til de større aktørene. I tillegg vil personer med kompetanse og innsikt i mekanismene i Statnetts telenett, og som har tilgang til det rette utstyret utvilsomt kunne forårsake stor skade. Angrep mot mindre informasjonssystemer har liten effekt på totalsystemet, og får sannsynligvis kun lokal virkning i en kort periode. Konsekvensene for totalsystemet avhenger imidlertid av hvor mye som angripes samtidig.

7 FREMTIDSTRENDER

7.1 Økende avhengighet av informasjonssystemer

Frem mot 2010 vil sannsynligvis datakommunikasjon ta over mye av den informasjonsflyten som i dag går via telefoni og faks. Det vil si at mer av informasjonsflyten skjer automatisk, og avhengigheten av datakommunikasjon øker.

Økende automatisering av kraftsystemet øker kompleksiteten, og gjør systemene enda mer dynamiske. Med en slik utvikling vil det kreves mye kompetanse av systemansvarlig for å kunne ha en overordnet oversikt og forståelse uten hjelp fra datamaskiner. Dette øker behovet for en elektronisk beslutningsstøtte som tar hensyn til denne kompleksiteten, og som dermed kan kontrollere stabiliteten i systemet. Et slikt støtteverktøy (simulator) gir råd om beslutninger, og anbefaler systemansvarlig hvilke operasjoner som bør gjøres. Det er sannsynlig at IT-baserte beslutningsstøttesystemer for kraftforsyningen i økende grad tar over for menneskelige beslutninger og vurderinger i fremtiden. Selv om det trengs personer til å betjene verktøyene, går den generelle utviklingen mot mer teknologi og elektronisk utstyr til å styre og drifte kraftforsyningen. Sannsynligheten er derfor til stede for at systemtilstanden med målinger, estimeringer og vurderinger som driver systemene, styres helt automatisk innen analysen tidshorisont i 2010.

Hvis kraftforsyningen satser på en slik utvikling, kan dette medføre at en overgang til manuell drift vil være vanskelig i fremtiden fordi systemansvarlig ikke har mulighet til å ta beslutninger uten hjelp fra datamaskiner. I dag er IKT-avhengigheten betydelig, mens den vil være svært stor og tidskritisk i en situasjon som vist i dette fremtidsscenariet.

Som tidligere nevnt er det naturlig å anta at kraftforsyningens avhengighet av offentlig telekommunikasjon vil øke i fremtiden. Den viktigste årsaken til dette er utviklingen mot mer kapasitetskrevende tjenester, såvel på driftssiden som rent administrativt. Overgangen til standardiserte, IP[18]-baserte driftsløsninger og utviklingen mot en tettere integrasjon mellom driftssystemer og administrative systemer bidrar til å forsterke dette.

Trenden innen offentlig telekommunikasjon går mot såkalt konvergens der tale, data og bilde overføres over samme infrastruktur. Dermed blir sektorgrenene mellom tele og IT blir mindre tydelige, og overføringsteknologien fremover vil sannsynligvis i stor grad baseres på IP-protokollen. I dag gir imidlertid ikke denne protokollen garantert kvalitet og integritet ved dataoverføring i nettene, samtidig som kravet til telenettene øker.

Det antas også at Internett i løpet av få år overtar mange av de samfunnskritiske tjenestene som de offentlige teletjenestene tradisjonelt i dag utfører (7). Dersom denne utviklingen også gjelder kraftforsyningen vil dermed de sikkerhetsmessige problemene overfor logiske angrep øke i fremtiden, ikke minst på grunn av alle sårbarhetselementene ved bruk og utvikling av Internett.

[18] Internett Protokoll

8 SÅRBARHETSREDUSERENDE TILTAK

Kraftforsyningen har et meget omfattende beredskapsregelverk. Vårt tradisjonelle trusselbilde har vært fokusert mot krig, bruk av konvensjonelle våpen og fysisk ødeleggelse. Dette bærer også dagens regelverk preg av. I dagens og fremtidens informasjonssamfunn representerer den logiske trusselen en klar utfordring, ikke bare for den norske beredskapslovgivningen rettet mot kraftforsyningen, men også for internasjonal konflikthåndtering generelt.

Det foreligger nå en ny sikkerhetslov som omhandler informasjonssikkerhet i samfunnsviktige funksjoner[19], og som dermed kan bidra til å øke kraftforsyningens informasjonssikkerhet. Sikkerhetsloven med forskrifter skal erstatte blant annet sikkerhetsinstruksen, datasikkerhetsdirektivet, tempestdirektivet, kryptosikkerhetsdirektivet og personellsikkerhetsdirektivet. Loven gjelder Forsvaret, hele kommunal- og statsforvaltningen og bedrifter som leverer varer eller tjenester til forvaltningen i forbindelse med sikkerhetsgraderte anskaffelser. Sikkerhetsloven vil nå kunne gjøres gjeldende for enhver som får tilgang til sikkerhetsgradert informasjon, uavhengig av om det dreier seg om offentlige organer, forvaltningsorganer eller annen virksomhet.

Sikkerhetskrav fra forsikringsselskapene kan også bli en viktig driver til å øke kraftforsyningens informasjonssikkerhet. I tillegg sørger den alminnelige etterspørselen etter strøm for et visst sikkerhetsnivå. Markedet alene vil imidlertid ikke sikre at samfunnets behov for kraftforsyning sikres ved en krise- eller krigssituasjon. I dette kapitlet diskuteres ulike sikkerhetstiltak utover det som er nødvendig for vanlig drift.

8.1 Fysisk beskyttelse av informasjonssystemer

Lokaler med mulighet for pålogging til drift av kraftsystemet og funksjoner for telenettet bør sikres i henhold til et minimumskrav. Dette kravet bør inkludere sikring mot både fysiske våpenvirkninger, elektromagnetiske våpen, sabotasje og innbrudd, der sikring av bygningsmasse, overvåkingssystemer og adgangskontroll inngår som sentrale virkemidler. Det bør også kontrolleres at driftssentraler har den nødstrømskapasitet som kreves ut fra RSK.

8.2 Beskyttelse av kommunikasjonsveier

Sikkerhet i kommunikasjonsløsningene for kraftbransjen er svært viktig for en sikker informasjonsflyt. Derfor må det vurderes tiltak som forsterker sambandsløsningene inn til de enkelte driftssentraler. Et viktig tiltak er å etablere fysisk redundans i kritiske kommunikasjonsveier. Det er også behov for alternative sambandsløsninger til andre aktører som myndighetene, støttefunksjoner og markedet. Et alternativt nødsamband kan være satellittkommunikasjon. Foruten disse tiltakene kan også de ulike komponenter i de forskjellige sambandsløsningene sikres i den grad det er mulig.

8.3 Distribuerte driftssentralløsninger

Statnetts driftssentralstruktur er lagt opp slik at hver regionssentral styrer anleggene innen sin

[19] Lov av 20.03.1998 nr 10. Loven ble gyldig våren 2001, bortsett fra bestemmelsene om objektsikkerhet som kan tre i kraft 01.01.2002. Det vises også til Sikkerhetslovens forarbeider, Ot prp nr 49 av 1996-97.

region, men kan ikke overta styringen innen andre regioner. En ringstruktur blant regionssentralene, der alle sentralene i praksis kan styre alle underlagte anlegg, vil redusere avhengigheten av den enkelte sentral. Et slikt distribuert driftsentralkonsept er derfor hensiktsmessig overfor krise- og krigssituasjoner.

8.4 Sikring av informasjon

Risiko- og sårbarhetsanalyser for å identifisere kritiske funksjoner innen informasjonssystemene bør gjennomføres regelmessig i hver enkelt bedrift, og danne grunnlag for krav og iverksettingen av tiltak innen kraftforsyning. Aktørene i kraftbransjen må bygge opp gode og sikre datanettverk ut fra rutiner og prinsipper[20]. De viktigste parametrene for et godt nettverk er hvilke komponenter som inngår, samt hvordan de er satt sammen. Aktørene bør derfor utvikle og etablere standarder og prosedyrer for IT-sikkerhet.

Det finnes en rekke sikkerhetsprodukter for datanettverk på markedet, og det er viktig at disse tas i bruk der det er nødvendig. Det er dermed viktig med full oversikt over antall grensesnitt og veier inn til lokalnettene. Det foreslås at alle sikkerhetsprodukter sertifiseres slik at de oppfyller spesifikke krav (såkalt "common criteria"[21]). Driftsystemene bør også ha forskjellige former for kontrollfunksjoner, slik at feilsituasjoner ikke så lett forplantes ukontrollert innover i nettet.

I tillegg er det viktig med holdningsskapende arbeid, opplæring av ansatte innen datasikkerhet, og god sikkerhetspolicy hos ledelsen. Det er viktig å sørge for at "brukere" innen bedriften er klar over sårbarhetene i informasjonssystemene, og dermed har mulighet til å bidra til å redusere sårbarheten. Dette kan for eksempel øke bevisstheten overfor insidere.

8.5 Kompetanse

Tekniske IKT-tiltak bør i utgangspunktet tas hånd om i den enkelte bedrift ut fra deres behov. Det anbefales derfor at de større aktørene har en sikkerhetsansvarlig i egen organisasjon, mens mindre bedrifter kan leie slik kompetanse.

Det er kritisk med god kompetanse når komponenter skal settes sammen og et datanett skal utvikles. Teknisk sikring av informasjonssystemene krever derfor høy kompetanse, både for å forstå hva som kreves og hvor tiltak skal implementeres. Det kan derfor være behov for å styrke kompetansen innen informasjonssikkerhet i kraftbransjen. Utdanning innen informasjonssikkerhet bør derfor prioriteres. Det er også mulig at de ansvarlige for drift av informasjonssystemer har for liten eller foreldet utdanningsbakgrunn. Det er derfor også viktig at det legges opp til videre- og etterutdanning innen dette området der det trengs. Foruten god kompetanse på IT-sikkerhet bør også krafttilbydere til enhver tid være tilknyttet personer med dokumentert formell kompetanse på driftssystemene.

[20] "Best practises"-prinsipp
[21] Produktstandarder

8.6 Beredskapspersonell

En av de store utfordringene for driften av kraftforsyningen i årene fremover blir å sikre tilgjengelighet til personell som kan bemanne underliggende anlegg i tilfelle fjernstyringen fra driftssentralen bryter sammen i en større krisesituasjon.

Gitt at utviklingen går mot ytterligere personellreduksjoner hos aktørene i kraftbransjen, må det vurderes løsninger som muliggjør bruk av arbeidskraft med minimumskompetanse. En mulighet er å iverksette en utdanningsordning som utdanner personell for manuelt arbeid i ulike deler av kraftforsyningen. Slikt personell vil være forbeholdt for innsats ved svikt/skade i kritiske situasjoner, og er tenkt å fungere under tilsyn av en faglært arbeidsleder.

8.7 Samøvelser

Dersom samfunnet stilles overfor ekstraordinære utfordringer, må alle aktørene som samhandler i hverdagen være i stand til å takle utfordringene. Det er derfor viktig med samarbeid og samøvelser mellom aktørene, hvor rutiner og prosedyrer som anses viktige i en beredskapssituasjon prøves ut. Det bør i tillegg etableres samarbeid og gjensidig tillit mellom de ulike aktørene, og mellom aktørene og myndighet for utveksling av informasjon. For eksempel vil et forum for informasjonsutveksling og samarbeid som bygger på gjensidig tillit, både mellom virksomheter innen kraftbransjen og mellom ulike typer bransjer være viktig.

8.8 Kompetansesenter for informasjonssikkerhet

Selv om selve utførelsen av de ulike tiltakene i vesentlig grad bør settes ut til virksomheter som har dette som spesialfelt, er det viktig at noen har et overordnet ansvar for å gjennomføre de tiltakene som er nevnt tidligere. Dette inkluderer for eksempel utvikling av en generell metodikk for risiko- og sårbarhetsanalyser og krav for ”best practises”. For å oppnå en god informasjonsberedskap i kraftbransjen er det viktig med god veiledning for sikring av informasjonssystemer. Det vil si et godt regelverk innen informasjonssikkerhet som er regelmessig oppdatert av kompetent personell, og som er felles for hele bransjen.

Selv om de store aktørene i bransjen har bevisste holdinger til informasjonssikkerhet ut fra kommersielle interesser, er det motsatte ofte tilfellet for mellomstore og mindre aktører. Men også store aktører må vurdere nytten av "tungvinte" beskyttelsestiltak opp mot funksjonelle løsninger tilpasset konkurransemarkedet. Innkjøpte IT-sikkerhetstjenester er heller ikke nødvendigvis dimensjonert mot trusselen fra en målrettet aktør som har gjennomført langvarig informasjonsinnhenting i forkant av et angrep.

Det er mange funksjoner som bør ivaretas av et tiltak som skal heve IT-sikkerheten innen kraftbransjen:

- Et grunnlag for IT-sikkerhetsarbeid må legges, og skrives inn i RSK

- Ut fra dette må det fortløpende spres informasjon om IT-sikkerhet, gode tekniske løsninger/sikkerhetsprodukter og trusselbildet

- Sikkerheten i eksisterende systemer må evalueres, både passivt gjennom risiko- og sårbarhetsanalyser og aktivt gjennom penetrasjonstester

- Nylig gjennomførte og mulig forestående angrep mot bransjen må varsles, ut fra statistikker av innrapporterte hendelser og trusselvurderinger

- Kompetanse og systemer i tilknytning til prosesstyringen må sertifiseres

I praksis er det behov for et høykompetent miljø som fortløpende arbeider med disse problemstillingene, og som bransjen kan bruke for å bedre sikkerheten i egne IT-systemer. Et nasjonalt senter for informasjonssikkerhet er for tiden under arbeid (8). Hvordan senteret vil se ut i sin endelige form er vanskelig å si, men det vil ivareta flere av de skisserte oppgavene, i alle fall på overordnet nivå. Inspirert av dette er det mulig å tenke seg et mindre kompetansemiljø om IT-sikkerhet "skreddersydd" for kraftforsyningen. Grunnlaget for dette senteret må være en revidert utgave av RSK, som skisserer hensiktsmessige generelle retningslinjer for informasjonssikkerhet i kraftforsyningen. Senteret vil ivareta den løpende håndtering av IT-sikkerhet i bransjen, gjennom å bistå med informasjon, varsle om kommende angrep, organisere penetrasjonstester o l. Det kan skisseres flere modeller for hvor senteret bør høre hjemme organisatorisk, men et rent tilsyn bør unngås for å få til tilstrekkelig åpenhet om problemene.

Erfaringer fra andre frivilligbaserte fellesprosjekter på IT-siden mellom myndighet og bransjen har vist at det er vanskelig å få stilt tilstrekkelige ressurser til disposisjon. Det må derfor sannsynligvis tilføres økonomiske midler og/ eller gis lovbestemte oppgaver for kraftforsyningen.

I det videre arbeidet blir det en viktig oppgave å foreta en vurdering av hvor mange systemer som er eller eventuelt skulle vært sikret av hensyn til rikets sikkerhet, og om disse systemene er sikret i samsvar med datasikkerhetsdirektivet/sikkerhetsloven[22], eller i samsvar med egne bestemmelser for kraftforsyningen.

Sammen med andre relevante tiltak for å fysisk sikre kraftforsyningen har BAS identifisert de mest kosteffektive driftsrelaterte tiltakene og funnet frem til strategier[23] for beskyttelse av norsk kraftforsyning. Strategiene presenteres i egen rapport (9).

[22] Som nevnt blir datasikkerhetsdirektivet opphevet når sikkerhetsloven trer i kraft og nye bestemmelser gjøres gjeldende også for sikkerhet i datamaskinbaserte informasjonssystemer.
[23] Pakker av beredskapstiltak.

Litteratur

(1) Rodal S K et al. (2001): Sårbarhet i kraftforsyningens informasjonssystemer, FFI/RAPPORT-2001/01868, Begrenset

(2) Hagen J M et al (2000): NORSK KRAFTFORSYNING - Dagens system og fremtidig utvikling. FFI/RAPPORT-2000/04450, ugradert

(3) INFOOPS-gruppen (2000): Statusrapport - Trussel og sårbarhet mot samfunnsvitale informasjonssystemer, Begrenset

(4) Forsvarsdepartementet (2001): Omleggingen av det norske forsvaret i perioden 2002-2005. Stortingsproposisjon nr 45 2000/01

(5) Rodal S K (2001): Informasjonssikkerhet innen telekommunikasjon. FFI/NOTAT-2001/04276, Begrenset

(6) Rutledal F et al (2000): Kraftmarkedets føringer for sårbarheten i norsk kraftforsyning, FFI/RAPPORT-2000/03451**,** Offentlig

(7) Silkoset O, Johansen O-A og Spilling P (2000): Sårbarhet og beredskap relatert til internett. Versjon 0.6 datert 21 august 2000, Scanpower A/S, Halden.

(8) Nærings- og handelsdepartementet (Oktober, 2000): Samfunnets sårbarhet som følge av avhengighet til IT

(9) Fridheim H et al (2001): Analyse av sårbarhetsreduserende tiltak innen kraftforsyning, FFI/RAPPORT-2001/01864, Begrenset

FORDELINGSLISTE

FFISYS **Dato:** 4 desember 2001

RAPPORTTYPE (KRYSS AV)	RAPPORT NR.	REFERANSE	RAPPORTENS DATO
X RAPP ☐ NOTAT ☐ RR	2001/04278	FFISYS/769/204.0	4 desember 2001

RAPPORTENS BESKYTTELSESGRAD	ANTALL EKS UTSTEDT	ANTALL SIDER
UGRADERT	80	26

RAPPORTENS TITTEL	FORFATTER(E)
SÅRBARHET I KRAFTFORSYNINGENS DRIFTS- OG STYRINGSSYSTEMER	RODAL Siv Kjersti

FORDELING GODKJENT AV FORSKNINGSSJEF:	FORDELING GODKJENT AV AVDELINGSSJEF:

EKSTERN FORDELING

ANTALL	EKS NR	TIL
1		Justisdepartementet
1		v/ Karen Melander
1		v/ May Kristin Ensrud
		Postboks 8005 Dep, 0030 Oslo
1		Olje- og energidepartementet
1		v/ Per Høisveen
1		v/ Kåre Rudsar
		Postboks 8148 Dep, 0033 Oslo
1		Direktoratet for sivilt beredskap
1		v/ Arthur Gjengstø
1		v/ Tonje Grunnan
		Postboks 8136 Dep, 0033 Oslo
1		Norges vassdrags- og energidirektorat
10		Avdeling for konsesjon og tilsyn
1		v/ Tor Langrud
1		v/ Truls Sønsteby
1		v/ Bjarne Larsen
		Postboks 5091 Majorstua, 0301 Oslo
1		Statnett
1		v/ Leif Vikane
1		v/ Kjell Sand
		Husebybakken 28B, 0379 Oslo
1		Statkraft SF
1		v/ Jon Ingvaldsen
		Postboks 494, 1323 Høvik
1		Post- og teletilsynet
1		v/ Torgeir Alvestad
		Postboks 447 Sentrum, 0104 Oslo

INTERN FORDELING

ANTALL	EKS NR	TIL
14		FFI-Bibl
1		Adm direktør/stabssjef
1		FFIE
1		FFISYS
1		FFIBM
1		FFIN
1		Ragnvald Solstrand, FFISYS
1		Bent Erik Bakken, FFISYS
1		Jan Erik Torp, FFISYS
1		Janne M Hagen, FFISYS
1		Håvard Fridheim, FFISYS
1		Kjell Olav Nystuen, FFIE
1		Gry Hege Rodal, FFISYS
1		Siv Kjersti Rodal, FFISYS
1		Frode Rutledal, FFISYS
17		Avdelingskontor FFISYS
		FFI-veven

EKSTERN FORDELING			INTERN FORDELING		
ANTALL	EKS NR	TIL	ANTALL	EKS NR	TIL
		Telenor			
1		Konsernstab Sikkerhet og miljø			
1		v/ Frits A Ødegaard			
		Pb 6701 St Olavsplass, 0030 Oslo			
1					
1		Samferdselsdepartementet			
1		v/ Kariann Skar Sørdahl			
		Postboks 8010 Dep, 0030 Oslo			
		www.ffi.no			

FFI-K1 Retningslinjer for fordeling og forsendelse er gitt i Oraklet, Bind I, Bestemmelser om publikasjoner for Forsvarets forskningsinstitutt, pkt 2 og 5. Benytt ny side om nødvendig.