Nätverksteori som verktyg vid risk- och sårbarhetsanalys av eldistributionsnät

Sophie Nykvist
Eva Ohlson

Department of Fire Safety Engineering
Lund University, Sweden

Brandteknik
Lunds tekniska högskola
Lunds universitet

Report 5222, Lund 2007

Nätverksteori som verktyg vid risk- och sårbarhetsanalys av eldistributionsnät

Sophie Nykvist & Eva Ohlson

Lund 2007

Nätverksteori som verktyg vid risk- och sårbarhetsanalys av eldistributionsnät
Network theory as a tool for risk and vulnerability analysis of electric distribution networks

Sophie Nykvist
Eva Ohlson

Report 5222
ISSN: 1402-3504
ISRN: LUTVDG/TVBB--5222--SE

Number of pages: 91

Keywords
Risk, vulnerability, electric distribution network, simulation, graph theory, Swedish Electricity Act

Sökord
Risk, sårbarhet, elnät, eldistributionsnät, simuleringsmetod, nätverk, grafteori, ellag.

Abstract
Events such as a storm that hit Sweden in 2005 and caused considerable damage led to a number of new additions in the Swedish Electricity Act. Some of these additions were demands on power distribution companies on a risk and vulnerability analysis and an action plan concerning the reliability of delivery in distribution networks, and also on keeping its customers informed about this. The aim of this master thesis is to investigate how a simulation method based on network theory can be used to perform risk and vulnerability analyses in accordance with these demands. In the analysis two simulation programmes, NetCalc and ACC, were used. With NetCalc, the network is put into strain by removing components one by one in a random or specific order. With ACC, a more detailed analysis of certain risk scenarios is done by analysing all scenarios with one or two simultaneously removed components. The analysis resulted in a set of suggestions on how the methods can be used on electrical distribution networks in accordance with the law. It also showed that the methods were especially useful for electrical distribution networks due to the clear structure and relative stativity of these networks.

Brandteknik
Lunds tekniska högskola
Lunds universitet
Box 118
221 00 Lund

brand@brand.lth.se
http://www.brand.lth.se

Telefon: 046 - 222 73 60
Telefax: 046 - 222 46 12

Department of Fire Safety Engineering
Lund University
P.O. Box 118
SE-221 00 Lund
Sweden

brand@brand.lth.se
http://www.brand.lth.se/english

Telephone: +46 46 222 73 60
Fax: +46 46 222 46 12

Förord

Detta examensarbete är den avslutande delen på civilingenjörsprogrammet i Riskhantering. Examensarbetet har fortgått sedan början av september och motsvarar 2 gånger 20 poäng.

Vi har många personer att tacka för stöd och hjälp under arbetes gång.

Till att börja med vill vi tacka vår handledare Henrik Johansson vid institutionen för Brandteknik samt Jonas Johansson och Henrik Jönsson, forskarstuderande LTH, för idéer och vägledning samt för att vi fått använda de datorprogram de tagit fram i sin forskning.

Ett stort tack vill vi ge till Matz Tapper och referensgruppen vid Svensk Energi, som delat med sig av sin kunskap och sina synpunkter på rapportens innehåll. Ett särskilt tack till Jakob Aldrin på Telge Energi AB för det varma välkomnandet vid vårt besök på företaget, för lån av arbetsplats och för all hjälp med material och svar på frågor. Tack också till alla andra på Telge Energi AB som hjälpte oss under vårt besök.

Sist vill vi tacka Per för att vi fick använda hans algoritm, Carl-Johan för tips och synpunkter, Louise, Jens och Fia för korrekturläsning och Frida för uppehälle under vår vistelse i Södertälje.

Trevlig läsning!

Sophie Nykvist
Eva Ohlson
Lund 2007

Sammanfattning

Stormen Gudrun, som drabbade Sverige år 2005, orsakade stor förödelse och ledde till en insikt om graden av sårbarhet hos den infrastruktur som vi blir allt mer beroende av. Till följd av bland annat detta beslutade riksdagen i slutet av samma år om skärpt lagstiftning angående elsäkerhet. Några av de nya lagkraven var att elnätföretag årligen måste upprätta en risk- och sårbarhetsanalys samt en åtgärdsplan rörande leveranssäkerheten i näten. Elnätföretagen måste även informera elanvändarna om leveranssäkerheten.

En risk- och sårbarhetsanalys kan genomföras utifrån olika angreppssätt. Vilket som väljs beror på hur det system som ska analyseras ser ut. I rapporten diskuteras två angreppssätt som många analysmetoder kan sägas använda, nämligen systembaserat och scenariobaserat. Det som skiljer dessa två åt är att det systembaserade angreppssättet utgår ifrån själva systemet medan det scenariobaserade angreppssättet utgår ifrån en uppsättning scenarier som kan drabba detta.

Ett elnät utgör i de flesta fall ett mycket stort och komplext system. En risk- och sårbarhetsanalys av ett sådant system med hjälp av en systembaserad metod skulle bli mycket omfattande och tidskrävande. Därför är oftast en scenariobaserad metod valet vid analys av stora system. Nackdelen med detta angreppssätt är dock att det kan vara svårt att säkerställa att samtliga relevanta riskscenarier kommer med i analysen.

För att kunna inkludera samtliga relevanta riskscenarier i analysen utan att detta blir alltför tidskrävande föreslås i rapporten att en variant av systembaserad metod, nämligen en simuleringsmetod som utgår från nätverksteori, kan användas. Med denna metod görs en systematisk genomgång av de valda riskscenarierna och eftersom den är datorbaserad blir analysen betydligt mindre tidskrävande än om den hade gjorts för hand. I tidigare studier har metoden visat sig vara användbar vid risk- och sårbarhetsanalyser av elnät. Till följd av detta sågs en möjlighet att använda och utveckla den tidigare kunskap som finns på området till att göra risk- och sårbarhetsanalyser av elnät med hjälp av simuleringsmetoder i enlighet med de nya lagkraven.

Som inledande moment i arbetet gjordes en genomgång av tidigare studier på området. Det som behövde undersökas var hur risk- och sårbarhetsanalys med hjälp av simuleringsmetoder som utgår från nätverksteori tidigare utförts. Det behövde även utredas om det fanns en möjlighet att öka metodernas användbarhet genom att öka detaljeringsgraden i modellerna. Utifrån genomgången beslutades att utreda betydelsen för analysen av två antaganden som inte tagits hänsyn till i tidigare studier, nämligen att antalet avbrott i ledningar är relaterat till ledningslängd och ledningstyp.

I analysen studerades tre nät med olika struktur: ett tätortsnät, ett glesbygdsnät och ett blandat nät. Dessutom användes driftsstörningsstatistik för ett av näten för att bland annat beräkna sannolikheten för avbrott och motivera vissa av de val som gjordes i analysen. För att göra risk- och sårbarhetsanalysen valdes att utgå ifrån ett mått som kallas för CECL (Customer Equivalent Connectivity Loss). Måttet valdes eftersom det inkluderar de faktorer som ansågs relevanta för elnät, nämligen antalet inmatningspunkter, att noderna i nätverket har olika stort värde, och att analysresultatet ska belysa

leveranssäkerheten. För att beräkna CECL behövde ett mått på konsekvensen av avbrott, den så kallade kundekvivalenten, bestämmas. Utifrån vad som bäst ansågs spegla konsekvensen ur såväl samhälls- och ekonomisk synvinkel valdes den årliga förbrukade energin i varje distributionspunkt som kundekvivalent. Med hjälp av CECL kunde ett näts sårbarhet för varje ytterligare utslagen komponent beräknas. Resultatet av analysen kunde redovisas dels som en graf, dels som ett enda tal, SVC (Societal Vulnerability Coefficient). Utöver CECL valdes även att analysera två mått på nätverkets konstruktion, DC_{order} och DC_{path}. Dessutom valdes att visualisera sårbarheten genom att markera sårbara områden i kartor över näten.

Analyserna genomfördes med hjälp av två datorbaserade simuleringsverktyg, NetCalc och ACC (Analysis of Critical Components), som framtagits inom forskningsprojektet FRIVA vid Lunds universitet. Med NetCalc kan en sårbarhetsanalys genomföras utifrån en initial påfrestning som användaren själv bestämmer. Med föresatsen att spegla händelser som kan drabba ett elnät i verkligheten valdes att simulera fyra påfrestningar, slumpmässig utslagning av noder respektive länkar, riktad utslagning av noder med avseende på grad och riktad utslagning av noder med avseende på årlig förbrukad energi. Utifrån de riskscenarier som de initiala påfrestningarna gav upphov till i simuleringarna, gjordes risk- och sårbarhetsanalyser av näten med hjälp av valda robusthetsmått och den driftsstörningsstatistik som fanns tillgänglig. ACC användes för att göra en mer ingående analys av de riskscenarier som i riskanalysen visat sig vara mest sannolika, nämligen ett avbrott och två samtidiga avbrott. Med hjälp av programmet kunde samtliga scenarier med ett och två avbrott analyseras.

Analysen visade att det är lämpligt att ta hänsyn till ledningslängd och typ av ledning i modelleringen av näten, eftersom dessa attribut har betydelse för resultatet av risk- och sårbarhetsanalysen och därmed hur denna speglar verkligheten. Vidare gav analysen resultat som ansågs kunna användas för att uppfylla de nya lagkraven. Risk- och sårbarhetsanalyserna som gjordes med hjälp av NetCalc kan användas för att klassificera ett nät ur sårbarhetssynpunkt. Detta för att kunna jämföra ett näts sårbarhet för olika påfrestningar, eller jämföra olika nät sinsemellan. Även analysen i ACC kan användas för att noggrannare analysera scenarierna ett och två samtidiga avbrott. I en del av analysen markerades sårbara områden i näten på kartor. Med hjälp av dessa kan till exempel framtida åtgärder i nätet motiveras. De kan även användas för att informera abonnenter om deras leveranssäkerhet. Resultatet av ACC kan användas för att motivera förstärkt skydd av vissa punkter, till exempel i en åtgärdsplan.

En analys av metodens användbarhet, utifrån den modellering av elnäten som gjorts, visade att en fördel med simuleringsmetoderna är att behovet av omfattande kunskaper om själva nätet är mindre än vid användande av till exempel scenariobaserade metoder. Detta eftersom metoderna bygger på nätets struktur vilken är ganska enkel att kartlägga och dessutom relativt statisk. Den slutsats som drogs utifrån analysen var att simuleringsmetoder som utgår från nätverksteori är användbara verktyg för att utföra risk- och sårbarhetsanalyser av elnät i enlighet med den nya lagstiftningen. Rapporten visar ett möjligt tillvägagångssätt och pekar även på möjligheterna att utveckla detta ytterligare i fortsatta studier.

Summary

The storm named Gudrun, which hit Sweden in 2005, caused considerable damage and led to an insight about the degree of vulnerability in the infrastructure that all of us have become more and more dependent on. This was one of the reasons that later that year the Swedish parliament decided on harder legislation concerning electric security. This resulted in a number of new demands in the Electricity Act, among others that power distribution companies on a yearly basis have to make a risk and vulnerability analysis concerning the reliability of delivery in the electrical distribution networks and an action plan concerning the reliability improvement. Also, the power distribution companies have to inform its customers about their reliability of delivery.

A risk and vulnerability analysis can be carried through from a number of different approaches. The approach chosen depends on the nature of the system analysed. In the report, two different approaches that many analysis methods use were discussed, the system based and the scenario based approach. The difference between the two is that the system based methods start from the system itself while the scenario based approach considers a set of scenarios that can happen to the system.

An electrical distribution network in most cases forms a very large and complex system both spatially and in the sheer number of components. A risk and vulnerability analysis of such a system with a system based analysis method would become very extensive and time-consuming. Therefore, the choice would in most cases be to use a scenario based method for analysis of large systems. However, the disadvantage with this approach is that it can be hard to ensure that the analysis covers the whole risk scenario space.

A way to include all relevant risk scenarios in the analysis, without it getting too time-consuming is to use a *variant* of system based method, a simulation method based on network theory. With this method, all relevant risk scenarios are systematically gone through and since it is computer based, the analysis will be less time-consuming than if it would had been made by hand. In earlier studies, the method has proved useful for risk and vulnerability analyses of distribution networks. Because of this, we saw an opportunity to use and develop the previous knowledge available on the area to perform risk and vulnerability analyses on distribution networks using simulation methods in accordance with the new demands in the Swedish Electricity Act.

The first part of the analysis was to review previous studies in the area. What had to be investigated was how risk and vulnerability analysis using simulation methods based on network theory previous had been performed. What also had to be investigated was if there was a way to increase the usability of the methods by increasing the degree of accuracy of the models. On the basis of the review, the decision was made to analyze the impact on the analysis of two assumptions that had not been taken into consideration in previous studies: That the frequency of interruptions in cables is related to length and type of cable.

In the analysis, three distribution networks with different structure were modelled: one urban distribution network, one rural distribution network and one that is a mixture of the

two. Also, statistics concerning interruptions in one of the distribution networks was used to calculate the probability of interruptions and motivate certain choices that were made in the analysis.

For the risk and vulnerability analysis, a measure of robustness called CECL (Customer Equivalent Connectivity Loss) was used. This measure was chosen since it included those factors that were considered relevant when it comes to distribution networks, namely the number of inputs, that the nodes in the network have different value and that the result of the analysis should highlight the security of delivery. To calculate CECL, a measure of the consequence of interruptions, the so-called customer equivalent, had to be defined. On the basis of what was considered to give a most accurate reflection of the consequence from a social as well as an economical perspective, the yearly used energy in each distribution node was chosen as customer equivalent. Using CECL, the vulnerability of the distribution networks for every additional removed component could be calculated. The result of the analysis could be presented in form of a graph, or as a single number, the SVC (Societal Vulnerability Coefficient). In addition to this, two measures of the networks' design, DC_{path} and DC_{order} were calculated. Furthermore, the vulnerability of the networks was visualised by indicating vulnerable areas in maps resembling the networks.

The analyses were performed using two computer based simulation tools, NetCalc and ACC, developed in the research project FRIVA at Lund University. With NetCalc, a vulnerability analysis based on an initial event chosen by the user, can be performed. With the intention to resemble strains that can occur to a distribution network in reality, four initial events were chosen to simulate: random removal of nodes and edges, respectively, removal of nodes in decreasing order of initial degree, and removal of nodes in decreasing order of yearly used energy. With the results from these initial events, risk and vulnerability analyses of the networks were performed using available measurements and statistics. ACC was used to make a more detailed analysis of the risk scenarios that turned out to be the most probable according to the risk analysis. Using ACC, critical components and critical combinations of components in the networks could be identified.

The analysis showed that it is appropriate to take into consideration the length and type of cables in the modelling of distribution networks since these attributes make a difference in the results of the risk and vulnerability analysis and hence how this resembles the reality. Furthermore, the analysis showed results that were considered useful to meet with the requirements of the new acts. A risk and vulnerability analysis performed in NetCalc can be used to classify the vulnerability of a network in order to be able to compare different networks or different strains on a network. Also, the analysis in ACC can be used to make a more detailed analysis of the scenarios one and two simultaneous interruptions. Also in the analysis, vulnerable areas of the networks were indicated on maps. These maps can be used to justify planned measures in the networks. They can also be used to inform customers about the reliability of their power delivery. The result of ACC can be used to justify reinforced protection of certain areas in an action plan.

An analysis considering the usefulness of the method, based on the modelling made of the distribution networks, showed that a benefit of using simulation methods is that the need for extensive knowledge regarding the system is less than in using scenario based models. This is since the methods are based on the structure of the networks which is quite easy to map and also relatively static.

The conclusion drawn from the analysis was that simulation methods based on network theory are useful tools for performing risk and vulnerability analysis in accordance with the new demands in the Electricity Act. The report shows a possible procedure for this and suggests how the procedure can be developed in further studies.

Centrala ord och begrepp

Här presenteras de ord förekommande i arbetet som eventuellt kräver en närmare förklaring.

Risk och sårbarhet

emergenta scenarier	I rapporten scenarier som föranleds av till synes enkla inledande händelser men leder till oväntade konsekvenser
leveranssäkerhet	Definieras i rapporten som elnätets förmåga att upprätthålla sin funktion - att förse abonnenterna med el
resiliens	Systemets förmåga att återhämta sig alternativt anta ett nytt, stabilt läge vid en påfrestning
robusthet	Systemets förmåga att förbli mer eller mindre intakt vid en påfrestning
system	Enligt NE "samling element som hänger samman med varandra så att de bildar en ordnad helhet”
tillståndsrymd	innehåller alla tillstånd som ett system kan anta
tillståndsvariabel	Beskriver de olika tillstånd som en komponent i en modell kan anta
union	Enligt NE "matematisk term för en mängd som uppstått genom sammanslagning av två eller flera mängder"

Myndigheter och organ

Elforsk	Branschägt företag för gemensamma forskningssatsningar inom elbranschen
Elsäkerhetsverket	En tillsynsmyndighet som skapar regler inom elsäkerhet samt ser till att dessa efterlevs
Energimyndigheten	Statens kontrollorgan inom energibranschen

Svensk Energi	En bransch- och intresseorganisation som har till uppgift att tillvarata de svenska energiföretagens intressen gällande elnät, elhandel och elproduktion
Svenska Kraftnät	Statligt verk som äger och ansvarar för det svenska stamnätet

Eldistribution

abonnent	Den som innehar abonnemanget för elförsörjning. Kan vara en enskild person, men även en grupp personer eller ett företag.
CMF	*Common Mode Failure*, innebär att en och samma händelse orsakar flera samtidiga fel
DARWIN	*Drift- och avbrottsrapportering*, nationell databas för inrapportering av driftstörningar i elnät
driftstörning	Enligt IEEE ”påtvingad eller obefogat urkoppling som medför att en kraftsystemenhet inte transporterar eller levererar elektrisk energi”.
frånskiljare	Komponent i nätet som kan öppnas för att förhindra att el kan matas längst en ledning. Dessa skiljer sig åt beroende på typ och om de används för friledning eller för jordkabel.
huvudbrytare	Komponent som vid driftstörning kan bryta matningen till elnätet. Är felet tillfälligt kan brytaren åter koppla på matningen.
huvudstation	Station där regionsnätets spänning, 40-70 kV, transformeras ner till distributionsnätets 12-24 kV och sedan fördelas ut till det lokala fördelningsnätet
kaskadeffekt	Då omdistribution av elen till följd av ett avbrott i en komponent leder till överbelastning av andra komponenter som inte klarar av att hantera den extra lasten
maskat nät	Ett nät som har flera inmatningspunkter och där nätstationerna kan få matning från flera håll
nätstation	Där strömmen transformeras från 12-24 kV ner till 0,4 kV och sedan fördelas ut till abonnenterna i fördelningsnätet
nättariff	Fast avgift som ett nätbolag tar ut från sina abonnenter till skillnad från den rörliga energiavgiften som energibolag tar ut

omkopplingstid	Den tid det tar att koppla om matningsvägen vid avbrott så att strömmen kan gå en alternativ väg
radiellt nät	Ett nät som har en trädliknande struktur och matas av en enda inmatningspunkt
slingmatat nät	Ett nät med en inmatningspunkt där nätstationerna ligger i en slinga så att de vid omkoppling kan få matning från två håll
transformator	Komponent som kan transformera upp eller ner spänningen i ett elnät

Nätverksteori

ACC	*Analysis of Critical Components*, ett datorprogram som tar fram kritiska komponenter eller kritiska kombinationer av komponenter i ett nätverk
attribut	Egenskaper som komponenterna tillskrivs som styr deras funktion och hur de interagerar med övriga komponenter i nätverket
CECL	*Customer Equivalent Connectivity Loss*, fraktion kundekvivalenter som förlorat matning vid en viss andel utslagna komponenter i nätet
CL	*Connectivity Loss*, den genomsnittliga minskningen av kopplingar mellan inmatningsnoder och icke inmatningsnoder i ett nätverk
DCorder	*Designkoefficienten med avseende på ordning*, korrelationen mellan den ordning som en distributionsnod förlorar matning och nodens kundekvivalent
DCpath	*Designkoefficienten med avseende på väg*, korrelationen mellan distributionsnodens kortaste väg till inmatningsnod och nodens kundekvivalent
diameter	Den längsta av alla kortaste vägar i nätverket
distributionsnod	I modellen beteckning på en nod där effekt tas ut till en eller flera abonnenter, vanligtvis en nätstation
FRIVA	*Framework for Risk and Vulnerability Analysis*, svenskt ramforskningsprogram inom risk- och sårbarhetsanalys

inmatningsnod	I modellen en beteckning på nod där effekt matas in i nätet från högre spänningsnivå, till exempel huvudstation
intermeditet	Antal kortaste vägar mellan samtliga nodpar som passerar en viss komponent
Inverterad längd, l^{-1}	Inverterade medelvärdet av samtliga kortaste vägar mellan två noder i ett nätverk
Klustringskoefficienten, C	Densiteten trianglar i ett nätverk
komponent	Nod eller länk, som i sin tur kan representera en frånskiljare, transformator, jordkabel eller luftledning
kritisk komponent	Komponent som nätverket är sårbart för utslagning av
Kundekvivalenten, CE	Anger en nods värde enligt vad som avses mätas och kan exempelvis vara antal kunder eller årlig förbrukad energi
Längd, l	Medelvärdet av samtliga kortaste vägar mellan ett nodpar i ett nätverk
länk	Koppling mellan noder, i modellen representerar dessa elledningar
medelgrad	Medelvärdet av samtliga noders grad i nätverket
nav	I rapporten benämning på noder som har en hög nodgrad i förhållande till övriga noder i nätverket
NetCalc	Datorprogram med vars hjälp det går att utföra en sårbarhetsanalys på ett nätverk genom att till exempel utsätta det för olika attackscenarier
nod	Huvudstationer, nätstationer, förgreningar och frånskiljare i modellen
nodgrad	Antal länkar kopplade till en nod

nätverk	Enligt NE ”System av inbördes förbundna enheter vilket liknar ett nät”
oriktat nätverk	Flödet i nätverket kan ske i samtliga riktningar
riktad utslagning	Ordningen för hur en nod eller länk slås ut avgörs av ett visst attribut
riktat nätverk	Flödet i nätverket kan endast ske i en riktning
SVC	*Societal Vulnerability Coefficient*, mått på nätverkets sårbarhet som utgör arean under CECL-kurvan
synergi	Då två eller flera komponenter påverkar ett system så att den totala konsekvensen blir större än summan för de enskilda komponenternas
topologi	Enligt NE "studiet av geometriska objekt där hänsyn endast tas till form och inte avstånd"
utslagning med avseende på attribut	Sannolikheten för utslagning är kopplat till ett attribut

1 Inledning

I detta kapitel beskrivs bakgrunden till examensarbetet, rapportens syfte och avgränsningar samt vilka rapporten vänder sig till.

1.1 Bakgrund

I januari år 2005 drabbades södra Sverige av Gudrun, en storm som medförde stora konsekvenser för såväl människor som natur. Resultatet av stormen blev 75 miljoner kubikmeter fälld skog, ett flertal omkomna och utslagning av viktig infrastruktur med följden att en stor mängd människor isolerades. 30 000 kilometer av eldistributionsnätet[1] blev skadat varav 9 % så svårt att total återuppbyggnad krävdes. 730 000 personer blev utan ström och för en del tog det upp till 45 dygn innan strömmen kom tillbaka. (Svensk Energi, 2005)

Händelser såsom Gudrun ledde till en insikt om hur sårbart vårt samhälle egentligen är. Den 8:e december beslutade riksdagen om skärpt lagstiftning angående elsäkerhet. Ett av de nytillkomna kraven i lagen är att varje företag som innehar nätkoncession[2] årligen måste ”… upprätta en risk- och sårbarhetsanalys avseende leveranssäkerheten i elnätet” Regeringskansliets rättsdatabaser, 3 kap. 9c §).

Det finns i dagsläget många olika metoder för risk- och sårbarhetsanalys. Ett av de viktigaste kriterierna vid val av metod är att den ger möjlighet att utföra så heltäckande analyser som möjligt. Med detta menas att en så stor del som möjligt av de olika riskscenarier som kan inträffa i systemet identifieras. För stora och komplexa system såsom elnät, kan det vara svårt att göra en analys där varje enskild komponent tas i beaktande. Ett alternativ är då att använda en scenariobaserad metod, som utgår ifrån vilka riskscenarier som kan uppstå i systemet. Vid användandet av en sådan metod är det dock extra viktigt att beakta risken att samtliga möjliga riskscenarier inte kommer med i analysen. Detta gäller särskilt sådana scenarier som ännu inte inträffat. Ett möjligt sätt att systematiskt gå igenom hela systemet utan att det ska bli alltför tidskrävande, är att använda sig av en simuleringsmetod som, med hjälp av ett datorbaserat verktyg, simulerar utvecklingen i nätet givet en viss påfrestning.

För att göra en analys med hjälp av en simuleringsmetod krävs dock vissa förenklingar. Om alla möjliga processer som äger rum i nätet skulle tas med skulle analysen, trots att den är datorbaserad, bli mycket omfattande om inte helt omöjlig att genomföra praktiskt. En modellering av nätet tar ner analysen på en hanterbar nivå. En typ av modell, som i flera tidigare studier använts för att analysera sårbarheten i elnät, är en som utgår ifrån ett en modellering av elnätet som ett nätverk (till exempel Albert, Albert & Nakarado, 2004; Crucitti, Latora & Marchiori, 2004 & Holmgren, 2006).

Några av dessa studier har genomförts i Nordamerika (Albert, Albert & Nakarado, 2004) och Italien (Crucitti, Latora & Marchiori, 2004). Resultatet av studierna visade att en

[1] Kallas i fortsättningen för elnätet
[2] Tillstånd från myndighet att bedriva nätverksamhet

simuleringsmetod som använder en modell som bygge på nätverksteori ger en överskådlig bild av hur de olika delarna i nätet påverkar varandra. Även i Sverige finns det en hel del publikationer rörande simuleringsmetoder som bygger på nätverksteori (Holmgren, 2006).

Inom FRIVA (Framework for Risk and Vulnerability Analysis, se bilaga 1), ett ramforskningsprogram vid Lunds universitet, sker bland annat arbete med att ta fram verktyg för risk- och sårbarhetsanalys av nätverk. Två av dessa är simuleringsverktygen NetCalc och ACC (Analysis of Critical Components).

Till följd av de nya lagkraven ses en möjlighet att använda och utveckla den tidigare kunskap som finns på området till att göra risk- och sårbarhetsanalyser av elnät med hjälp av simuleringsmetoder som bygger på nätverksteori.

1.2 Syfte

Examensarbetets syfte är att, med utgångspunkt i tidigare studier på området, utreda om simuleringsmetoder som bygger på nätverksteori kan användas för att utföra risk- och sårbarhetsanalys av elnät i enlighet med de nya kraven i ellagen.

1.3 Frågeställningar

För att kunna uppfylla syftet med rapporten måste ett antal frågeställningar besvaras. Då syftet är att utnyttja kunskapen från tidigare studier ställs först frågan:

- Hur har risk- och sårbarhetsanalys av elnät med hjälp av simuleringsmetoder som bygger på nätverksteori tidigare utförts och vilka resultat har erhållits?

För att utifrån dessa studier finna lämpliga metoder för den aktuella analysen måste även följande problem utredas:

- Vad krävs för att en metod ska vara lämplig för risk- och sårbarhetsanalys av elnät och är det någon av de befintliga metoderna som uppfyller dessa krav?

Vidare undersöks om:

- det finns någon möjlighet att utveckla eller anpassa någon av metoderna så att den blir lämplig för den analys som ska utföras i detta examensarbete?

Enligt syftet ska risk- och sårbarhetsanalysen uppfylla de krav som ställs i den nya ellagen och därför ställs frågan:

- Hur kan en risk- och sårbarhetsanalys utförd med en simuleringsmetod utformas för att analyserna ska uppfylla lagkraven?

De metoder som används för risk- och sårbarhetsanalys kräver att elnäten modelleras med de förenklingar och antagande som detta medför. Det är därför slutligen av stor vikt att besvara:

- Hur påverkar dessa antaganden och förenklingar i modelleringen risk- och sårbarhetsanalysen och är metoden trots detta användbar?

1.4 Generella avgränsningar

I den analys som utfördes i rapporten användes en modell av nätet som har använts i tidigare studie, vilken grundar sig på nätverksteori. I denna modell tas ingen hänsyn till externa aktörers påverkan på nätets robusthet.

Analysen gjordes endast på 12 kV-nivån. Detta eftersom denna ansågs mest intressant att analysera utifrån de historiska data som fanns att tillgå.

I rapporten jämförs inte olika möjliga simuleringsverktyg utan de verktyg som används har valts utifrån tillgänglighet. De algoritmer som används för att utföra beräkningarna beskrivs inte i rapporten.

1.5 Målgrupp

Rapporten vänder sig till företag, organisationer och myndigheter inom elbranschen. Den vänder sig även till andra personer med särskilt intresse för risk- och sårbarhetsanalys av komplexa infrastrukturer, till exempel studenter och forskare.

1.6 Metod och disposition

Då examensarbetets syfte bygger på nätverksteori och analyser av eldistributionsnät inleddes arbetet med omfattande litteraturstudier av relevanta skrifter såsom läroböcker, vetenskapliga artiklar, lagtext och information utgiven av diverse branschaktörer. Det finns många tidigare studier på området som går att bygga vidare på. De vetenskapliga artiklarna söktes till största delen fram på databasen ELIN vid Lunds universitetsbibliotek. En del teoretiskt material tillhandahölls även av forskare vid avdelningen för brandteknik på Lunds tekniska högskola.

Informationen som användes i analyserna består av data rörande tre olika elnät, samt driftstörningsstatistik för ett av näten. De data som samlades in för respektive nät var koordinater[3], antal abonnenter och årlig förbrukad energi i de punkter i nätet där uppgifter fanns tillgängliga. För ett av näten hämtades även information om maximal kapacitet för inmatningspunkterna. Den driftstörningsstatistik som behandlas i arbetet användes för att motivera gjorda val såsom vilken del av nätet som skulle analyseras och vilka analyser som skulle göras, samt beräkna sannolikheten för riskscenarier.

Data till två av näten erhölls från tidigare studier inom FRIVA. Data för det tredje nätet, samt driftstörningsstatistik för detta, inhämtades vid besök hos Telge nät AB, ett

[3] Se bilaga 2 för beskrivning hur dessa togs fram

elnätföretag. Under arbetets gång hade författarna fortlöpande kontakt med företaget för att kunna ställa frågor och få återkoppling.

Figur 1 visar rapportens disposition. Rapporten består av tre delar: en teoridel, en empiridel och en avslutande del.

2. Risk och sårbarhet	**Teori**
3. Lagtext	
4. Eldistributionen i Sverige	
5. Metoder för risk- och sårbarhetsanalys i elnät	
6. Nätverksteori och robusthet	
7. Empirisk studie	**Empiri**
8. Slutsatser	**Avslutande del**

Figur 1 Rapportens disposition där de kapitel som tillhör teori, empiri och avslutande del redovisas.

I **teoridelen** presenteras en genomgång av den teori som är relevant för att besvara rapportens frågeställningar. Teoridelen inleds med kapitel två, där begreppen risk och sårbarhet förklaras. Dessutom ges kvantitativa definitioner på de båda begreppen.

De lagkrav som ligger till grund för rapporten beskrivs i kapitel tre. I kapitlet beskrivs hur dessa kom till. Dessutom förklaras den tolkning av lagkraven som gjorts i rapporten.

Kapitel fyra syftar till att skapa en övergripande bild över hur eldistributionen och hanteringen av driftstörningar ser ut i Sverige idag. Detta för att ge en förståelse för de förutsättningar som i dagsläget finns för att göra risk- och sårbarhetsanalyser i enlighet med lagstiftningen.

Med utgångspunkt i kapitel tre och fyra förs i kapitel fem en diskussion kring olika angreppssätt för risk- och sårbarhetsanalys i olika typer av system. Dessutom presenteras tidigare studier inom området. Kapitlets syfte är att motivera varför just simuleringsmetoder valdes för att utföra risk- och sårbarhetsanalyserna i den empiriska studien.

Användandet av simuleringsmetoder innebär att elnäten måste modelleras som nätverk. Därför beskrivs i kapitel sex teori grafteori, som är den matematiska benämningen på nätverksteori, samt olika mått som kan användas för att beskriva ett nätverks sårbarhet. En diskussion förs kring de olika måttens lämplighet för elnät och även kring olika sätt att mäta konsekvensen av oönskade händelser i en risk- och sårbarhetsanalys. Slutligen presenteras de datorprogram som användes i den empiriska studien.

Teoridelen följs av en **empirisk del** som består av metod, resultat och diskussion kring resultatet av risk- och sårbarhetsanalyserna. Denna del inleds med en motivering till

varför vissa avgränsningar gjordes vid analyserna. Här beskrivs även de tre elnät som studerades och hur de modellerades som nätverk.

Därefter presenteras den analys som gjordes för att kunna uppnå rapportens syfte. Analysen bestod av fem delar. I den första delen undersöktes möjligheten att utveckla modelleringen av elnäten genom att analysera betydelsen för risk- och sårbarhetsanalysen av några attribut som inte tagits hänsyn till i tidigare studier, nämligen länklängd och länktyp. Samtliga nät analyserades därför med avseende på attributet länklängd, och ett av näten med avseende på attributet länktyp.

I den andra delen genomfördes en sårbarhetsanalys med hjälp av datorprogrammet NetCalc. Denna utgick från fyra olika initiala påfrestningar som valdes och motiverades i metodbeskrivningen. Sårbarhetsanalysen gjordes för samtliga tre nät varefter resultaten diskuterades och nätens sårbarhet enligt analysen jämfördes.

I den tredje delen gjordes en riskanalys utifrån tillgänglig driftstörningsstatistik och de analysresultat som erhölls från sårbarhetsanalysen. I riskanalysen behandlades endast ett av de tre näten, eftersom driftstörningsstatistiken endast fanns tillgänglig för detta.

I den fjärde delen undersöktes robustheten i de tre nätens konstruktion utifrån analysresultaten från sårbarhetsanalysen. Detta gjordes dels med två smått, och dels med kartor av näten där sårbara områden markerades.

I den femte delen gjordes slutligen en mer ingående analys av två riskscenarier från riskanalysen som ansågs särskilt intressanta att analysera. Detta gjordes genom att kritiska komponenter och komponentpar identifierades med hjälp av datorprogrammet ACC. I denna del behandlades endast ett av de tre näten.

Kapitlet avslutas med en diskussion om analysmetodens användbarhet för att uppfylla lagkraven samt modellens användbarhet ur ett validitetsperspektiv.

I den **avslutande delen** av rapporten presenteras de slutsatser som drogs från studien. Här kopplas resultatet och diskussionen från den empiriska studien till rapportens syfte och frågeställningar. Slutligen ges förslag på fortsatta studier inom området.

2 Risk och sårbarhet

Då begreppen risk och sårbarhet ofta kan tolkas på flera sätt, ges i detta kapitel en redogörelse för begreppens uppkomst och hur deras kvantitativa definition ser ut.

2.1 Risk och kvantitativ riskanalys

Den kvantitativa definitionen av risk av Kaplan och Garrick presenterades 1981. De började med att beteckna scenariorymden, S, som samtliga möjliga scenarier som kan inträffa i ett system. Därefter definierades S_A som riskscenariorymden, vilken innehöll samtliga scenarier i S där oönskade konsekvenser uppstår. Ett enskilt scenario i S_A kallades för S_i. Det scenario där systemet uppför sig som planerat kallades S_0. Risken definierades som:

$$R = \left\{ \left\langle S_i, L_i, X_i \right\rangle \right\}_C \quad \textbf{(1)}$$

där S_i är riskscenario i, L_i sannolikhet eller frekvens och X_i konsekvens. C står för det engelska ordet complete, vilket betyder att samtliga möjliga scenarier ingår i risken. (Kaplan & Garrick, 1981)

Den ursprungliga definitionen utgick ifrån att antalet scenarier var uppräkneliga. I realiteten kan dock varje scenario alltid delas upp i mer specifika scenarier, varför antalet scenarier egentligen utgör ett oupräkneligt antal. Med detta i åtanke förfinades den ursprungliga definitionen av Kaplan, Haimes och Garrick (2001) till:

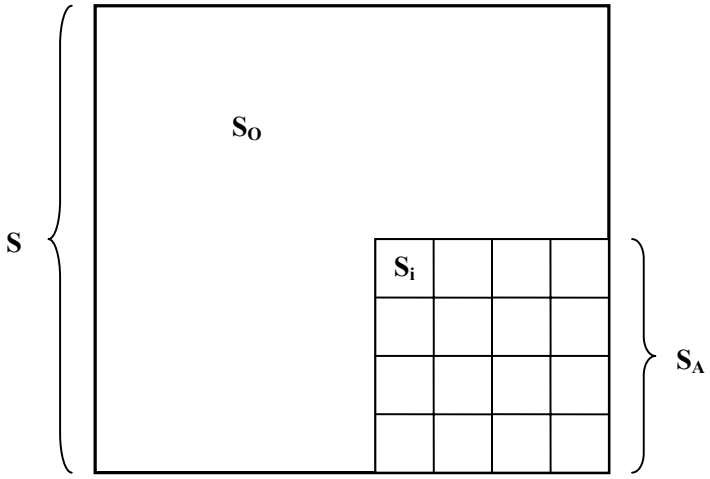
$$R = \left\{ \left\langle S_\alpha, L_\alpha, X_\alpha \right\rangle \right\}, \alpha \in A \quad \textbf{(2)}$$

där α tillhör mängden A vilken är oupräknelig. De enda skillnaden som här gjordes var alltså att ändra antalet scenarier från en uppräknelig till en oupräknelig mängd.

I en riskanalys krävs dock ett uppräkneligt antal riskscenarier. Därför delades mängden S_A för ett specifikt system upp i delmängder S_i. Definitionen av S_i innehöll tre krav. Det första var att uppsättningen S_i skulle vara fullständiga, vilket innebar att $U(S_i) = S_A$, det vill säga unionen av alla delmängder S_i skulle motsvara S_A. Det andra kravet var att S_i skulle vara uppräkneliga och det tredje att de skulle vara disjunkta, det vill säga de olika delmängderna S_i fick inte överlappa varandra. Till följd av denna definition kunde risken skrivas som:

$$R_P = \left\{ \left\langle S_i, L_i, X_i \right\rangle \right\}_P \quad \textbf{(3)}$$

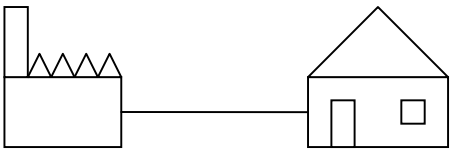
där P står för det engelska ordet partition, eller delning. (Kaplan, Haimes & Garrick, 2001) Figur 2 illustrerar riskbegreppet.



Figur 2 Illustration av scenariorymden, S, som kan delas upp i riskscenariorymden, S_A, och normaltillståndet, S_O. S_A kan i sin tur delas upp i ett antal riskscenarier, S_i.

För att kunna göra en riskanalys krävs alltså en förenkling, en modell, av systemet. Hur detaljerad denna modell, och därmed uppdelningen av riskscenariorymden i riskscenarier enligt formel 3 blir, skiljer sig från fall till fall. Modellen kan bli hur enkel, eller hur detaljerad som helst.

En *tillståndsvariabel* beskriver de olika tillstånd som en komponent i modellen kan anta. (Johansson & Jönsson, 2007) Se figur 3.



Figur 3 Figuren föreställer ett kraftverk (vänster) och en kund (höger) som förses med el från kraftverket.

Figur 3 visar ett kraftverk och en kund som försörjs med el från kraftverket. Kraftverket, kunden och ledningen mellan dem utgör var och en *element* i modellen. Ledningen mellan kraftverket och kunden har, i en mycket enkel modell, en tillståndsvariabel som kan sägas anta två tillstånd: på (den kan leverera el) och av (den kan inte leverera el).

Detaljrikedomen i modellen kan ökas genom att antingen fler tillståndsvariabler läggs till genom att exempelvis öka antalet element, eller genom att öka antalet tillstånd för de befintliga tillståndsvariablerna. Vad som utgör riskscenarier beror av beslutsfattaren. Beslutsfattaren behöver inte vara en specifik person utan det kan även vara en samling värderingar som avgör vad som ska analyseras.(Johansson & Jönsson, 2007)

Ett exempel på system kan vara ett elnät. Alla scenarier som leder till att någon eller några av elnätets komponenter går sönder kan i exemplet utgöra oönskade scenarier. Då kommer alla dessa scenarier ingå i riskscenariorymden S_A. I en riskanalys delas sedan S_A in i riskscenarier S_i. Denna uppdelning kan till exempel göras utifrån antal fallerande komponenter. Till exempel kan då alla scenarier med högst en fallerande komponent ingå

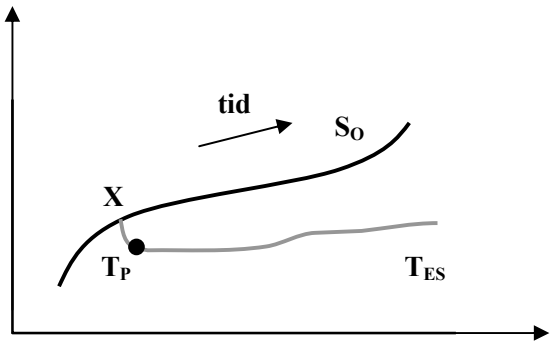
i det första riskscenariot, alla scenarier med högst två fallerade komponenter ingå i det andra, och så vidare.

En **kvantitativ riskanalys** är en sammanställning av samtliga riskscenarier, inklusive deras sannolikhet och konsekvens (Johansson & Jönsson, 2007).

2.2 Sårbarhet och kvantitativ sårbarhetsanalys

En riskanalys resulterar vanligtvis i en storleksuppskattning, kvantitativ eller kvalitativ, på sannolikheten och konsekvensen för ett riskscenario eller en uppsättning riskscenarier. En sårbarhetsanalys sker ur ett något annorlunda perspektiv, den utgår istället från att en händelse skett och sätter denna i relation till ett system. Hallin, Nilsson och Olofsson (2004) definierade sårbarhet som ”… en beskrivning av en relation mellan en specifik händelse, hot eller riskkälla och ett specifikt, mottagligt system”. Enligt Dilley och Boudreau (2001) innehåller begreppet sårbarhet tre grundläggande element: *händelser, känslighet för händelserna*, och *det slutgiltiga resultatet*.

Den kvantitativa definitionen av sårbarhet kan göras utifrån samma teoretiska utgångspunkter som den kvantitativa definitionen av risk. I den kvantitativa definitionen av risk definierades ett systems normaltillstånd som S_0. S_0 kan även sägas vara systemets förväntade väg genom *tillståndsrymden*. Tillståndsrymden innehåller alla möjliga tillstånd som ett system kan ha. Systemets förväntade väg är den väg systemet färdas så länge det inte utsätts för någon påfrestning. Om systemet utsätts för en påfrestning, sker en förflyttning till en ny plats i tillståndsrymden, som leder till ett nytt sluttillstånd. (Johansson & Jönsson, 2007) Se figur 4.



Figur 4 Systemets förändrade väg genom tillståndsrymden då det utsatts för en påfrestning. Den svarta linjen är den väg systemet skulle ha gått i normaltillståndet, den grå är den nya vägen på grund av påfrestningen. (Johansson & Jönsson, 2007)

I figur 4 är T_P det mellanliggande tillstånd som uppkommer på grund av den aktuella påfrestningen. T_{ES} är systemets nya sluttillstånd, som det når till följd av förflyttningen till T_P. Detta kan kopplas till de tre element som nämndes tidigare: händelsen sker i punkten X, systemets känslighet för händelsen orsakar förflyttningen från normaltillståndet till T_P och T_{ES} representerar det slutgiltiga resultatet. Den väg från T_P till T_{ES} som illustreras i figur 4 gäller då det endast finns en väg för systemet att gå efter påfrestningen. I själva verket finns det oftast flera möjliga vägar och sluttillstånd. (Johansson & Jönsson, 2007)

Systemets sårbarhet på grund av en specifik påfrestning kan på detta sätt definieras genom att undersöka skillnaden mellan det nya sluttillståndet och det som skulle ha varit om inte påfrestningen skett. Om det bara finns en väg blir detta relativt enkelt. Om det finns flera möjliga vägar kan sårbarheten beskrivas i likhet med ekvationen för risk med modifieringen att den utgår från att systemet lämnat S_0 och hamnat i T_P: (Johansson & Jönsson, 2007)

$$V_P = \left\{\left\langle S_\alpha, L_\alpha, X_\alpha \right\rangle\right\}, \alpha \in A, S_{\alpha,1} \in T_P \quad \textbf{(4)}$$

där S_α är scenario α, L_α är sannolikheten för scenariot och X_α är konsekvensen som uppstår till följd av påfrestningen och som förflyttar scenariot till T_P. $S_{\alpha,1} \in T_P$ innebär att det första systemtillståndet i samtliga riskscenarier S_α ingår i T_P.

En **kvantitativ sårbarhetsanalys** utgår alltså ifrån att en påfrestning inträffat, varefter riskscenariorymden till följd av denna påfrestning delas upp i riskscenarier och sannolikhet och konsekvens bestäms. I praktiken läggs oftast inte alltför stor vikt vid sannolikheterna för olika händelser utan det är scenarierna och konsekvenserna som är det intressanta. (Johansson & Jönsson, 2007)

Två begrepp som kan ses som komplement till sårbarhet, och som berör systemets krishanteringsförmåga, är *robusthet* och *resiliens*. Ett systems robusthet är dess förmåga att förbli mer eller mindre intakt vid en påfrestning. Robusthet kan ses som motsatsen till sårbarhet. Resiliens är systemets förmåga att återhämta sig alternativt anta ett nytt, stabilt läge vid en påfrestning (Holmgren, 2006).

3 Lagtext

I detta kapitel ges en närmare genomgång av bakgrunden till de lagkrav som rapportens syfte bygger på samt hur de har tolkats i denna rapport.

Bland annat till följd av stormen Gudrun beslutade riksdagen år 2005 om en ny och hårdare ellagstiftning (Svensk Energi, 2005). Tidigare har kravet på risk- och sårbarhetsanalys endast omfattat kommun, landsting och statliga myndigheter enligt *Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap* samt enligt *Förordning (2006:942) om krisberedskap och höjd beredskap*. Enligt den nya lagen ska varje elnätföretag regelbundet utföra risk- och sårbarhetsanalys av sitt elnät. Enligt lagen ska även elnätföretagen utöka informationen rörande abonnenternas leveranssäkerhet och även om eventuella brister i elnät. (Svensk Energi, 2005) Nedan presenteras de lagändringar som fastställdes genom den nya ellagen som är relevanta för rapporten.

Ellag (1997:857)

3 kap. Nätverksamhet m.m.

9c § *Den som bedriver nätverksamhet med stöd av nätkoncession för linje med en spänning som understiger 220 kilovolt eller nätkoncession för område skall årligen upprätta*

1. *en risk- och sårbarhetsanalys avseende leveranssäkerheten i elnätet, och*
2. *en åtgärdsplan som visar hur leveranssäkerheten i det egna elnätet skall förbättras.*

Risk- och sårbarhetsanalysen och åtgärdsplanen skall ges in till den myndighet som regeringen bestämmer. Lag (2005:1110)

9d § *Den som bedriver nätverksamhet med stöd av nätkoncession för linje med en spänning som understiger 220 kilovolt eller nätkoncession för område skall informera elanvändarna om leveranssäkerheten i elnätet och om rätten till avbrottsersättning och skadestånd enligt 10 och 11 kap. Lag (2005:1110)*

Med *leveranssäkerhet* tolkas i rapporten nätets förmåga att upprätthålla sin funktion vilken är att leverera el till abonnenterna. De riskscenarier som risk- och sårbarhetsanalysen utgår från bör alltså utgå ifrån abonnenterna snarare än nätet som sådant.

En *åtgärdsplan* tolkas som en skriftlig redogörelse för vilka områden som i risk- och sårbarhetsanalysen identifierats vara i behov av förstärkt skydd. Det ingår alltså i risk- och sårbarhetsanalysen att skapa underlag för åtgärdsplanen.

Att *informera elanvändarna* om leveranssäkerheten tolkas som att varje abonnent ska informeras om robustheten i den egna elförsörjningen snarare än i nätet som helhet.

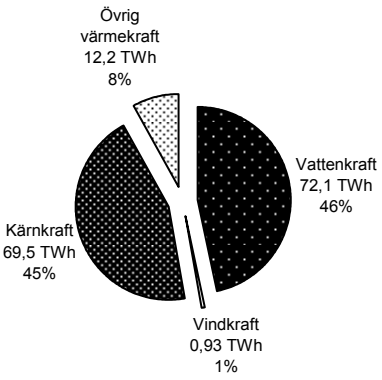
4 Eldistributionen i Sverige

Då rapportens fokus är risk- och sårbarhetsanalyser av elnät ges i detta kapitel en överblick av Sveriges eldistribution och de möjligheter som i dagsläget finns för att övervaka störningar i det svenska elnätet.

4.1 Sveriges elproduktion och distribution

Elkraften kom till Sverige i slutet på 1800-talet, vid denna tid sköttes eldistributionen genom kommunala elverk eller distributionsföreningar. Allt eftersom elbehovet växte i Sverige ökade dock belastningen på elnäten och eldistributionen började skötas av större nätföretag. Dessa var från början runt 5000 stycken men har efter hand minskat till att idag endast omfatta 180 stycken varav 168 är lokala nätföretag (Kungliga Ingenjörsvetenskapsakademin, 2004). År 1996 avreglerades den svenska elmarknaden och därmed blev det fritt för kunderna att köpa sin el från vilket elhandelsföretag som helst. (Nationalencyklopedin, uppslagsord: elmarknadsreformen, 2006) Denna möjlighet finns dock av naturliga skäl inte inom distribution. Där har varje nätföretag ett naturligt monopol inom sitt distributionsområde. Därför är elnätssektorn fortfarande reglerad. (Institutionen för Värme- och Kraftteknik, 2005)

Sverige får sin energitillförsel från importerad olja, kol, naturgas och kärnbränsle, men även från inhemsk produktion i form av kärnkraft, vattenkraft, värmekraft och vindkraft. Den inhemska elproduktionen var år 2005 fördelad enligt figur 5.



Figur 5 Fördelning av Sveriges elproduktion för år 2005 (Svensk Energi, 2005)

Elproduktionen i Sverige ägs till 43 % av staten, 43 % av utländska ägare, 9 % av kommuner och 5 % av övriga ägare. De fem största elproducenterna är Vattenfall, Fortum, Statkraft, E.ON och Skellefteå kraft och dessa stod 2005 för 89 % av Sveriges elproduktion. (Svensk Energi, 2005)

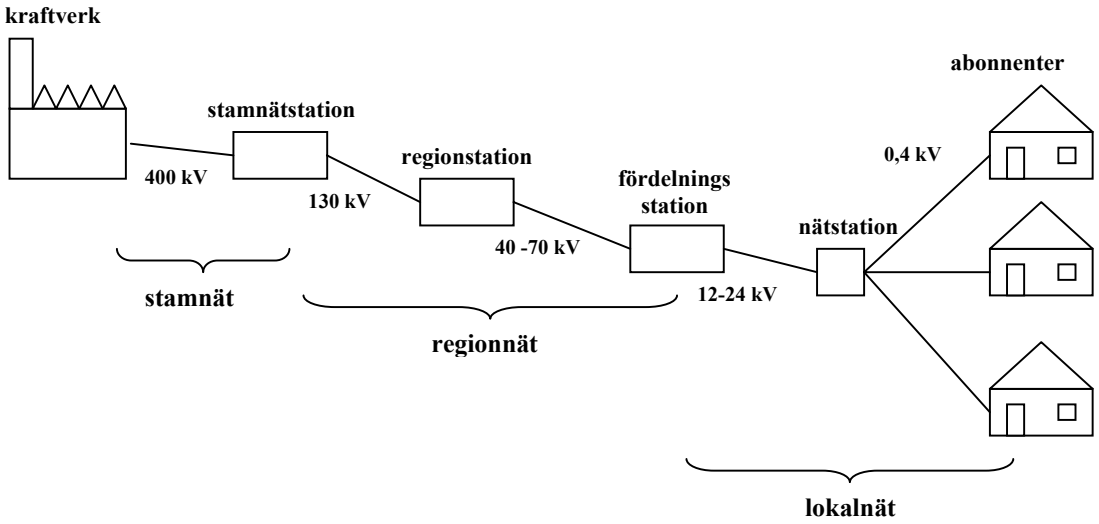
4.2 Aktörer inom elbranschen

Det svenska stamnätet ägs av statliga Svenska Kraftnät som bland annat har till uppgift att ansvara för elnätets stationer samt även de förbindelser Sverige har med utländska elnät (Svenska Kraftnät, 2006). De övriga elnäten ägs av ett antal elnätsföretag där de tre största företagen är E.ON, Vattenfall och Fortum (Svensk Energi, 2005).

Några andra viktiga aktörer inom elnätsbranschen är Svensk Energi, Elforsk, Statens Energimyndighet och Elsäkerhetsverket. Svensk Energi är en bransch- och intresseorganisation, och har till uppgift att tillvarata de svenska energiföretagens intressen gällande elnät, elhandel och elproduktion. Detta sker bland annat genom informations- och kunskapsspridning inom elbranschen (Svensk Energi, 2006). Elforsk ägs av Svensk Energi och Svenska Kraftnät, och bedriver branschgemensam forskning och utveckling inom elbranschen. Energimyndigheten sköter kontrollen inom energibranschen och har bland annat uppgiften att kontrollera att de nättariffer nätföretagen tar ut är rimliga i förhållande till hur företaget ser efter och underhåller sitt elnät. (Statens Energimyndighet, 2006) Elsäkerhetsverket är en myndighet som tar fram regler för en säker elhantering och ser även till att dessa regler följs. De ansvarar även för beredskap då det gäller större och svårare elrelaterade olyckor. (Elsäkerhetsverket, 2006)

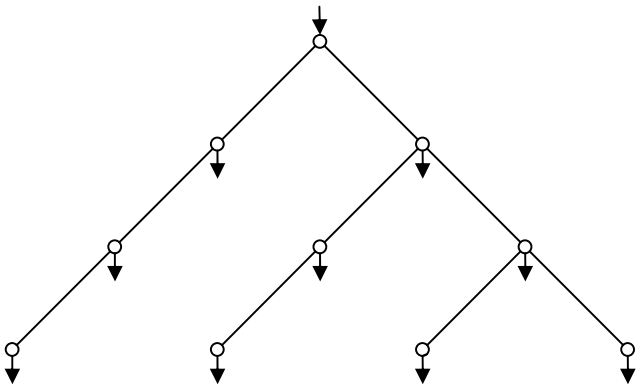
4.3 Det svenska elnätets uppbyggnad och struktur

Sveriges elnät sträcker sig cirka 500 000 km över landet och är uppdelat i stamnät, regionalnät och lokalt fördelningsnät. Stamnätet består av elledningar med en överföringskapacitet på 7000 MW som sträcker sig från norra till södra Sverige. Stamnätet är dessutom ihopkopplat med elnäten i Finland, Norge, Danmark, Polen och Tyskland. På detta sätt kan länderna hjälpa varandra med tillförsel av el vid avbrott och obalanser i nätet. (Elforsk, 2004) Från stamnätet överförs producerad el till det regionala elnätet som förser olika delar av landet med el. Från huvudstationer i det regionala nätet leds strömmen ut till det lokala fördelningsnätet där spänningen sänks från 40-70 kV till 12-24 kV. För att strömmen ska kunna fördelas ut till elabonnenterna måste spänningen sänkas ytterligare, till en nivå på 0,4 kV vilket görs i fördelningsnätets nätstationer. (Kungliga Ingenjörsvetenskapsakademin, 2004) Se figur 6.



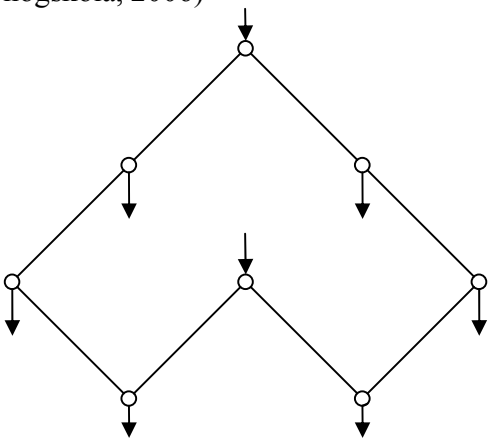
Figur 6 De olika nivåerna i elnätet. Från stamnätet fördelas elen ut i regionnätet och sedan vidare ut i det lokala distributionsnätet för att slutligen nå abonnenterna.

Ett elnät är i huvudsak radiellt, se figur 7, eller maskat, se figur 8.



Figur 7 Ett radiellt nät där inmatning sker i en punkt. Den pil som pekar mot nätet är inmatningspunkt och de pilar som pekar från nätet är punkter där matning sker till abonnenterna.

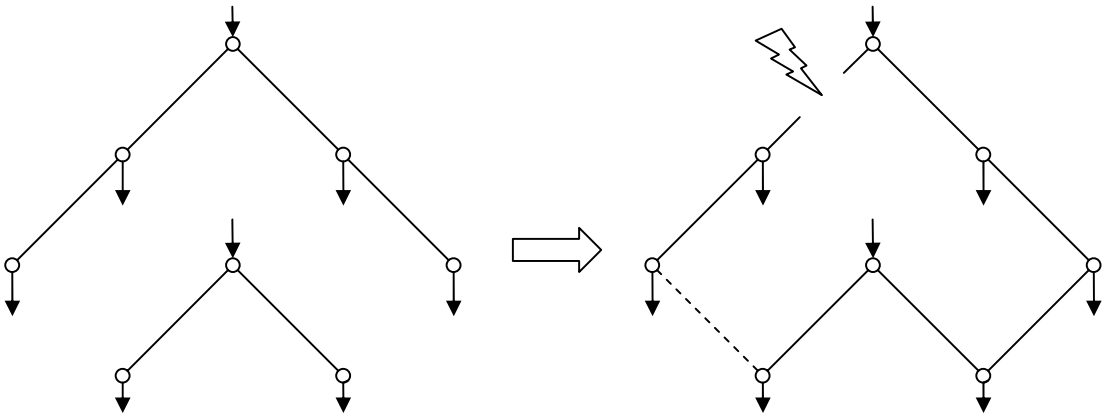
Ett radiellt elnät har en trädliknande struktur och matas av en enda inmatningspunkt. Om ett avbrott sker i ett radiellt elnät förlorar samtliga nätdelar bortom avbrottspunkten matning. Abonnenterna måste därefter vänta till felet blivit avhjälpt innan de kan få ström. Radiell matning är vanligast i glesbygd där abonnenterna ligger långt ifrån varandra och det inte är lönsamt att ha alternativa matningsvägar. (Lunds tekniska högskola, 2006)



Figur 8 Ett maskat nät där inmatning sker i flera punkter. De pilar som pekar mot nätet är inmatningspunkter och de pilar som pekar från nätet är punkter där matning sker till abonnenterna.

Ett maskat elnät, däremot, har flera matningsvägar och ofta flera inmatningspunkter. Så länge endast ett avbrott åt gången sker i ett maskat elnät, kan abonnenterna i många fall få matning via en annan väg. Maskade elnät är vanligast i tätort. (Lunds tekniska högskola, 2006)

I realiteten drivs dock även maskade nät radiellt. Se figur 9.



Figur 9 Ett maskat nät som drivs radiellt. I den högra bilden visar den streckade linjen den alternativa matningsvägen vid ett avbrott (Lunds tekniska högskola, 2006)

De ledningar som utgör den alternativa matningsvägen är i normalfallet blockerade med hjälp av öppna frånskiljare. Ett fel i nätet leder till avbrott ända till omkoppling sker genom att den öppna frånskiljaren sluts. Därefter kan abonnenterna få ström via den alternativa matningsvägen. Detta gör att abonnenterna kan återfå matning snabbare än om de hade varit tvungna att vänta tills felet blivit åtgärdat. (Statens Energimyndighet, 2003)

4.4 Driftstörningar

Energimyndigheten har sedan 1996 samlat in driftstörningsstatistik från svenska elnätföretag. För att en driftstörning ska tas upp i statistiken måste den vara längre än tre minuter. Rapporteringen har skett i form av ett antal nyckeltal som årligen beräknas av elnätföretagen. De fyra viktigaste är:

- SAIDI - *System Average Interrupton Duration Index*, genomsnittlig avbrottstid per år och abonnent för samtliga abonnenter
- SAIFI - *System Average Interrupton Frequency Index*, genomsnittlig avbrottsfrekvens per år och abonnent för samtliga abonnenter
- CAIDI - Customer *Average Interrupton Duration Frequency Index*, genomsnittlig avbrottstid per år och abonnent för de abonnenter som berörts av avbrott
- ASAI - *Average Service Available Index*, genomsnittlig tillgänglighet av el för abonnenter

Att enbart rapportera nyckeltal innebär en stor osäkerhet i resultatet eftersom varken tillvägagångssättet eller statistikunderlaget rapporteras. (Svensk Energi, 2004)

På senare tid har ett nytt verktyg för inrapportering av driftstörningsstatistik, DARWIN, tagits fram. Syftet med DARWIN är att skapa en driftstörningsstatistik som har högre tillförlitlighet än den som tidigare funnits. (Statens energimyndighet, 2003) DARWIN omfattar idag 101 elnätföretag och statistiken är hämtad från företagens lokalnät med spänningsnivåer uppdelade i kategorierna 24 kV, 12 kV, <10 kV samt 0,4 kV.

De händelser som kan leda till driftstörning i ett elnät klassificeras enligt DARWIN som:

- Åska
- Övrigt väder
- Åverkan
- Material/metod
- Personal
- Överlast
- Återvändande last
- Säkringsbrott
- Okänd

Data till DARWIN rapporteras in till en central databas hos Svensk Energi och är mer omfattande än rapporteringen till Energimyndigheten. (Svensk Energi, 2004) I DARWIN anges, till skillnad från i Energimyndighetens databas, bland annat avbrottets längd, lokalisering och orsak (Telge nät AB, 2006).

Driftstörningarnas lokalisering i elnätet klassificeras enligt DARWIN som följande komponentdelar:

- Transformatorstation - station som sänker spänningen och som utgör en inmatnings- eller fördelningspunkt i elnätet (Aldrin, 2007)
- Stolpstation - transformator i det lokala distributionsnätet som är belägen uppe i en stolpe
- Nätstation - station i det lokala distributionsnätet som sänker spänningen från 12 kV till 0,4 kV (Aldrin, 2007)
- Oisolerad luftledning
- Isolerad luftledning
- Hängkabel - totalisolerad ledning som är upphängd i stolpar (Aldrin, 2007)
- Jordkabel - totalisolerad ledning som är belägen under marken (Aldrin, 2007)
- Annan ledning
- Avgrenings- eller kabelskåp - skåp i lågspänningsnätet där ledningar kan kopplas bort eller kopplas om (Aldrin, 2007)
- Säkrings- eller apparatlåda - komponent som innehåller säkringar och manuella brytare (Aldrin, 2007)
- Okänd

I regel drabbas luftledningar oftare av driftsstörningar än jordkabel. Dock är reparationstiden längre för jordkabel än luftledning. (Svensk Energi, 2005; Kungliga Ingenjörsvetenskapsakademin, 2004)

5 Metoder för risk- och sårbarhetsanalys i elnät

I detta kapitel beskrivs övergripande olika angreppssätt som en risk- och sårbarhetsanalys kan ha. Därefter presenteras en metod för att avgöra användbarheten hos den modellering av systemet som måste göras för att genomföra en analys. Sedan diskuteras tidigare studier på området och slutligen motiveras valet av den analysmetod som ligger till grund för rapportens empiriska studie.

5.1 Systembaserat och scenariobaserat angreppssätt

Eftersom risk- och sårbarhetsanalyser är rätt lika till angreppssättet diskuteras metoderna med utgångspunkten att samma resonemang gäller för såväl risk- som sårbarhetsanalyser.

De metoder som idag finns för risk- och sårbarhetsanalys kan grovt delas upp i två kategorier[4]: scenariobaserade[5] och systembaserade[6]. Den fundamentala skillnaden mellan dessa två är, som namnen antyder, att systembaserade analyser utgår från en noggrann kartläggning av själva systemet, medan scenariobaserade metoder utgår från en samling riskscenarier som kan tänkas uppstå i systemet. Scenariobaserade metoder är vanliga i mycket stora system, där riskscenarier ofta får konsekvenser som påverkar många olika delar av systemet och där olika aktörer är en del av systemet, till exempel en kommun. Systembaserade metoder är vanligast i tekniska system, till exempel en kemisk process. (Johansson & Jönsson, 2007)

Scenariobaserade metoder går ut på att samla en grupp personer med stor erfarenhet av det aktuella systemet för att sedan genom diskussion identifiera de hot som systemet kan utsättas för. När dessa identifierats görs en djupare analys av varje hot för att försöka ta fram sannolikhet, konsekvens, vilka aktörer som blir inblandade i scenariot och systemets beredskap för hotet. (Krisberedskapsmyndigheten, 2006)

En systembaserad metod inleds med att kartlägga det system som analysen ska genomföras på[7]. Hur noggrant detta ska göras beror på analysens syfte. Efter denna kartläggning skiljer sig de olika metoderna något åt. Till exempel kan en systematisk genomgång av alla systemets komponenter göras, där frågeställningarna ”Vad kan hända i denna komponent?” eller ”Vad händer i denna komponent om en avvikelse sker?” försöker besvaras. En systembaserad metod kan också koncentrera sig på enskilda händelser i systemet, och försöka bryta ner orsakerna till, eller konsekvenserna av, dessa till önskad detaljnivå. (Davidsson, 2003)

Det finns även en variant på systembaserade metoder som tar hjälp av något slags simuleringsverktyg, så kallade simuleringsmetoder. Dessa kan antingen användas för att simulera utvecklingen av ett visst riskscenario i en viss komponent, eller för att beskriva

[4] Det förekommer metoder som ligger utanför denna kategorisering. För en mer fullständig genomgång av metoder rekommenderas till exempel (Johansson & Jönsson, 2007)
[5] Till exempel MVA, ROSA och GDG (Krisberedskapsmyndigheten, 2006)
[6] Till exempel grovanalys, Hazop, What-if, FMEA, FTA, och ETA (Davidsson, 2003)
[7] En av de systembaserade metoderna, grovanalys, skiljer sig från denna arbetsgång eftersom den kan utföras utan en kartläggning av systemet

den dynamiska utvecklingen i ett system för ett större antal riskscenarier. En simuleringsmetod kan till exempel gå till så att de regler som gäller för ett systems dynamiska utveckling beskrivs i ett datorprogram, varefter en dator får beräkna hur systemet, givet ett visst utgångsläge, kommer att agera. (Johansson & Jönsson, 2007)

Med systembaserade metoder görs en noggrann genomgång av systemet vilket innebär att risken för utelämnande av riskscenarier och konsekvenser minskar. Dessa metoder utgör även ofta ett bra underlag för att beräkna sannolikhet och konsekvens hos riskscenarier (Johansson & Jönsson, 2007). Dock kan en analys med någon av dessa metoder, i större och mer komplexa system, bli alltför omfattande. Av dessa orsaker kan en scenariobaserad metod vara att föredra i större system. Vid en analys med en sådan metod är det dock viktigt att vara uppmärksam på svårigheten att få med alla relevanta riskscenarier. En uppsättning erfarna personer vars sammanlagda kunskap ger en så komplett bild av systemet som möjligt, kan bidra till att minska detta problem. Dock kvarstår svårigheten att identifiera scenarier som aldrig inträffat. En simuleringsmetod kan både öka analysens täckningsgrad och möjliggöra identifiering av riskscenarier som ännu inte inträffat.

Nackdelen med simuleringsmetoder är att de inte tar någon hänsyn till om det finns externa faktorer som kan mildra eller åtgärda fel då de inträffar, till exempel reparatörer och om abonnenterna har tillgång till egen reservkraft. Därför kan det vara lämpligt att kombinera en scenariobaserad metod med en simuleringsmetod som simulerar utvecklingen i systemet givet ett ursprungsscenario.

5.2 Modellering av systemet

Oavsett vilken analysmetod som väljs för att utföra en risk- och sårbarhetsanalys krävs först att det system som ska analyseras definieras och avgränsas i en modell. Detta kräver alltid en viss del förenklingar och antaganden. För att säkerställa att den modell som skapas trots detta är användbar kan ett par frågeställningar formulerade av Johansson & Jönsson (2007) angående detta besvaras:

- Kan samtliga konsekvenser som identifierats som viktiga beskrivas med systemet?
- Kan samtliga relevanta riskscenarier beskrivas med systemet?
- Finns samtliga relevanta riskscenarier med i riskscenariorymden?
- Beskriver riskscenarierna verkligheten på ett korrekt sätt?

Den första frågan syftar på att för att kunna få konsekvenser av riskscenarier måste dessa finnas beskrivna i systemet. Om till exempel den konsekvens som eftersöks i analysen är antal strömlösa kunder vid ett elavbrott, måste information om antal kunder som är utan ström vid olika systemtillstånd definieras, till exempel med hjälp av en tillståndsvariabel. (Johansson & Jönsson, 2007)

Den andra frågan syftar till att klargöra om modellen är tillräckligt detaljerad för att de riskscenarier som är relevanta för analysen ska kunna beskrivas. Den tredje frågan berör

huruvida samtliga relevanta riskscenarier överhuvudtaget finns med i riskscenariorymden. (Johansson & Jönsson, 2007)

Den sista frågan är troligtvis den mest svåra att besvara. Det är omöjligt att exakt spegla verkligheten i en modell men det är samtidigt nödvändigt att säkerställa att de slutsatser som dras utifrån modellen även stämmer överens med verkligheten. Det krävs att en händelse i modellen som motsvaras av en verklig händelse, leder till en konsekvens i modellen som motsvarar den verkliga konsekvensen och inte en helt annan. (Johansson & Jönsson, 2007)

5.3 Tidigare studier

Eftersom användningen av simuleringsmetoder fortfarande är relativt ny, finns det ännu mycket som är oklart rörande hur simuleringarna ska gå till. Axelrod (1997) beskrev i sin översikt av simuleringsmodellers användningsområden, vilka riktlinjer som bör beaktas i användningen av simuleringsmetoder för att resultatet ska bli så bra som möjligt. Han menade bland annat att ett simuleringsprogram bör besitta tre egenskaper: *validitet, användbarhet och möjlighet till utveckling*. Med validitet menade Axelrod programmets förmåga att korrekt implementera modellen. Med användbarhet menades möjligheten för användarna att förstå programmet och de utdata som programmet genererar. Möjlighet till utveckling innebar möjligheten för framtida användare att utveckla programmet.

Som tidigare nämnts är simuleringsmetoder, som simulerar utvecklingen i systemet då det utsätts för en påfrestning, ett sätt att inkludera samtliga möjliga riskscenarier i en risk- och sårbarhetsanalys. De kan även användas till att upptäcka scenarier som ännu inte inträffat. Axelrod (1997) nämnde även detta i sin studie då han påpekade att så kallade *emergenta* scenarier, som föranleds av till synes enkla inledande händelser men leder till oväntade konsekvenser, vore mycket svåra att upptäcka utan hjälp av en simuleringsmetod.

Crucitti, Latora och Marchiori (2004) visade i sin analys av det italienska stamnätet på svårigheten att kunna förutse och motverka emergenta scenarier såsom exempelvis kaskadeffekter vid avbrott. Författarna pekade på en rad incidenter, bland annat det största elavbrottet i USA:s historia 2003 som gjorde miljontals abonnenter strömlösa i upp till 15 timmar, och ett avbrott i Schweiz 2003 som utöver att drabba landets södra del dessutom släckte ner nästan hela Italien. Båda började som ett enda avbrott men spred sig till att omfatta stora områden och i det schweiziska fallet till och med ett annat land. Crucitti, Latora och Marchiori använde sig i analysen av en topologisk nätverksmodell av det italienska stamnätet för att simulera effekten av utslagningar av noder i nätet.

Albert, Albert och Nakarado (2004) studerade i sin analys det nordamerikanska stamnätet ur ett liknande nätverksperspektiv. De fann bland annat att det, liksom flera tidigare studerade elnät, bestod av ett fåtal punkter som utgjorde viktiga nav och att en utslagning av dessa medförde stora konsekvenser för eldistributionen. Författarna menade därför att det var av stor vikt att i en risk- och sårbarhetsanalys bland annat identifiera om nätverket är beroende av ett litet antal nav.

Holmgren (2006) påpekade i sin topologiska studie av det nordiska och amerikanska stamnätet att modellering och simulering av elnät är ett hjälpmedel för att skapa en bredare förståelse för de mekanismer som styr nätets beteende. Holmgren menade vidare att målet med en sårbarhetsanalys inte skulle vara att helt eliminera sårbarheten i systemet utan snarare att öka förmågan att hantera riskscenarier när de uppkommer och att simuleringsmodeller är ett verktyg för att göra detta.

De flesta tidigare studier rörande lämpligheten hos simuleringsmetoder, som bygger på nätverksteori, för risk- och sårbarhetsanalys av elnät har gjorts på stamnät. Johansson, Jönsson och Johansson (2006) menade dock i sin studie baserad bland annat på de stora konsekvenser som orsakades av stormen Gudrun, att dessa metoder även bör tillämpas på distributionsnivå. Detta eftersom händelser såsom Gudrun visade att skador på denna nivå kan få omfattande och långvariga konsekvenser.

5.4 Val av angreppssätt i rapporten

För den risk- och sårbarhetsanalys av elnät som gjordes i rapporten valdes att använda en simuleringsmetod som simulerar den dynamiska utvecklingen i systemet efter att en påfrestning skett. Med en sådan metod kan samtliga riskscenarier till följd av påfrestningen systematiskt gås igenom. En analys med hjälp av en simuleringsmetod kräver dock vissa förenklanden. Om alla möjliga processer som äger rum i ett nät tas med skulle analysen, trots att den är datorbaserad, bli alltför omfattande att genomföra praktiskt. I många tidigare studier på området studerades näten därför ur ett topologiskt perspektiv. Modelleringen av näten utgick från nätverksteori och näten modellerades då som nätverk med noder och länkar.

Ett strikt topologiskt perspektiv innebär att ingen hänsyn tas till avstånd utan endast till form. Den modellering av näten som gjordes i rapporten utgick från tidigare studier där det topologiska perspektivet användes. Utöver detta undersöktes dock även möjligheten att utveckla modelleringen ytterligare genom att ta hänsyn till attribut som kan öka analysmetodens användbarhet.

6 Nätverksteori och robusthet

En simuleringsmetod kräver indata i form av en modell av det system som ska analyseras. De nätverk som analysernas i rapporten modelleras med utgångspunkt i det topologiska perspektivet, vilket bygger på nätverksteori eller grafteori som den matematiska benämningen är. Därför behandlar detta kapitel grundläggande grafteori och olika robusthetsmått som bygger på nätverksteori.

6.1 Grafteorins uppkomst

Nätverk förekommer så gott som överallt. En del är synliga, som infrastrukturen och olika tekniska nätverk. Andra är inte är lika uppenbara, till exempel sociala, ekonomiska och informationsnätverk. Det finns även gott om naturliga nätverk. Den biologiska näringskedjan är ett exempel på detta och vårt eget nervsystem ett annat.

Den person som brukar få äran för grafteorins första teorem är den schweiziske matematikern Leonhard Euler. År 1736 publicerade han en artikel baserad på det numera klassiska matematiska problemet *Königsbergs sju broar*. Staden Königsberg bestod av ett antal mindre öar förbundna med sammanlagt sju broar. Problemet gick ut på att finna en promenadväg genom staden, där varje bro passerades exakt en gång. Euler formulerade problemet som ett nätverk, och kunde på det sättet bevisa att en sådan promenadväg inte existerade. (Weisstein, 2005)

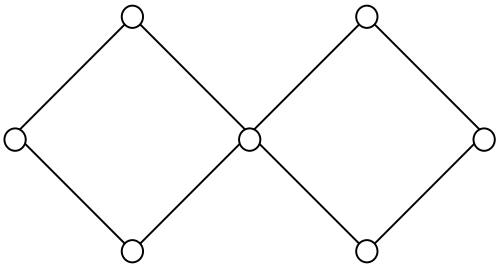
1852 presenterade Francis Guthrie ett problem som bestod i att färglägga en karta, vilken som helst, med hjälp av endast fyra olika färger. Varje land skulle ha en färg och två angränsande länder fick inte hade samma färg. Problemet fick inte sin lösning förrän mer än hundra år senare men under tiden hade många viktiga och fundamentala grafteoretiska teorem framtagits. (Weisstein, 2003) Efter detta tog forskningen fart på allvar och numera påträffas grafteori inom en mängd olika specialiteter. (Nationalencyklopedin, uppslagsord: grafteori, 2006)

6.2 Grundläggande grafteori

Ett nätverk beskrivs enklast som ett sammanlänkat system av punkter. Punkterna kan vara personer eller saker och dessa kallas med ett gemensamt namn för *noder*. *Länkarna* är relationer, abstrakta eller konkreta, mellan noderna. Matematiskt kallas nätverket för en *graf*:

$$G = (V, E) \quad \textbf{(5)}$$

där G är grafen, V är en uppsättning noder med antal n och E är en uppsättning länkar med antal m. Se figur 10 för illustration.



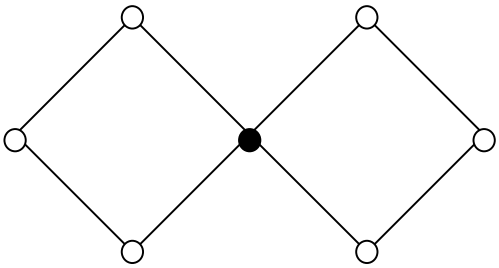
Figur 10 En enkel graf med n = 7 och m = 8

Grafen kan vara *riktad* eller *oriktad*. En riktad graf innebär att flödet mellan två noder endast sker åt ett håll. Motsatsen, oriktad graf, innebär att flöden kan ske i båda riktningar. (Holme et al., 2002)

Om grafen är oriktad kan det största möjliga antalet länkar, m_{max}, i grafen räknas ut med:

$$m_{\max} = \frac{1}{2} n(n-1) \qquad \textbf{(6)}$$

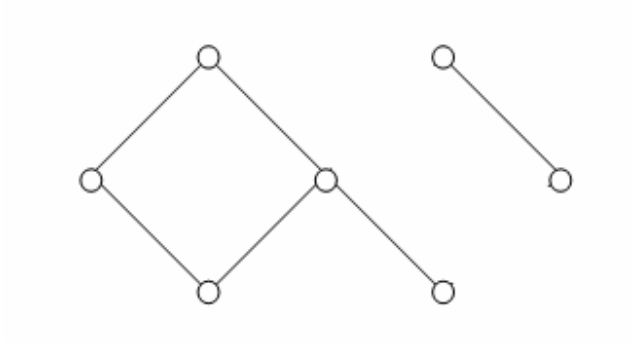
där n är det totala antalet noder i grafen. En nods *grad* anger hur många länkar som är kopplade till den. Ju fler länkar som är kopplade till noden, desto högre nodgrad har den. Se figur 11 för illustration.



Figur 11 En enkel graf där den svarta noden har grad 4

Medelgraden är det genomsnittliga värdet av samtliga noders grad i nätverket. (Newman, 2003)

En graf kan bestå av en eller flera separata *grafkomponenter*. Den största sammankopplade grafkomponenten brukar kallas *S* vars värde till exempel kan uttryckas som antalet noder den sammanbinder. (Holme, 2004) Se figur 12.



Figur 12 En enkel graf som består av två grafkomponenter där S = 5

Såväl noderna som länkarna kan ha olika *attribut* kopplade till sig. Detta är egenskaper som komponenterna tillskrivs och som styr deras funktion och hur de interagerar med övriga noder och länkar i nätverket. (Newman, 2003)

En egenskap som kan observeras i många verkliga system utformade som nätverk är att ett fåtal noder utgör så kallade nav i nätverket, vilket betyder att de har en relativt hög nodgrad, medan majoriteten av noderna har en låg nodgrad. Detta leder ofta till att fördelningen av nodernas grad följer en så kallad *power law-fördelning* vilket innebär att sannolikheten P(k) att en nod ska vara ansluten till k stycken andra noder är:

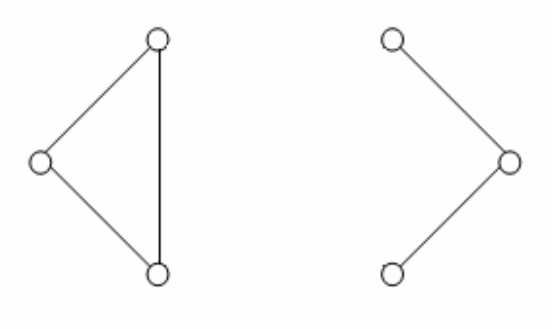
$$P(k) = ak^{-\gamma} \qquad \textbf{(7)}$$

där *a* och γ är konstanter (Holme, 2004). Nätverk där fördelningen av nodernas grad följer en power law-fördelning har i flera studier visat sig vara robusta för slumpmässiga attacker men mycket sårbara för attacker mot de noder som utgör nav i nätverket (Albert, Albert & Nakarado, 2004).

Klustringskoefficienten är ett mått som mäter densiteten av trianglar i nätverket. Om nod A är länkad till nod B och nod B är länkad till nod C, bildas en triangel om även A och C är länkade till varandra. Sociala nätverk, till exempel, har ofta en hög klustringskoefficient. Klustringskoefficienten, *C*, beräknas som:

$$C = \frac{3 \times antal\ trianglar\ i\ nätverket}{antal\ tripletter\ i\ nätverket} \qquad \textbf{(8)}$$

Med *triplett* menas i detta fall tre sammanlänkade noder som inte behöver bilda en triangel. (Newman, 2003) Se figur 13.



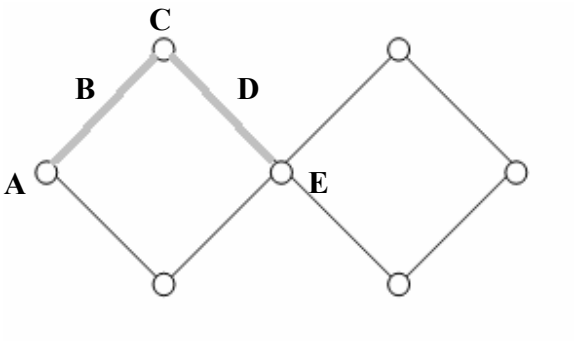
Figur 13 Skillnaden mellan en triangel (vänster) och en triplett (höger)

För en viss nod n_i kan klustringskoefficienten, C_i, beräknas som:

$$C_i = \frac{antal\ trianglar\ \ förbundna\ med\ nod\ n_i}{antal\ tripletter\ centrerade\ på\ nod\ n_i} \quad (9)$$

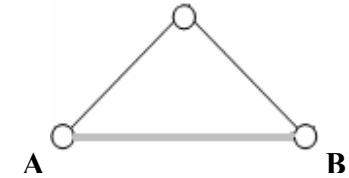
En hög klustringskoefficient tyder på att det finns många alternativa vägar i nätverket. (Newman, 2003)

En *väg* är sträckan från en nod till en annan i grafen. Vägen innehåller de noder och länkar som skiljer de två noderna åt. Se figur14.



Figur 14 En enkel graf där vägen från nod A till nod E består av länk B, nod C och länk D

Då det finns flera alternativa vägar att gå från en nod till en annan kan det vara intressant att veta den *kortaste vägen* mellan dessa två noder. Se figur 15.



Figur 15 En enkel graf där den kortaste av två möjliga vägar mellan A och B är gråmarkerad

Den *längsta* av samtliga kortaste vägar i nätverket kallas för nätverkets *diameter*.

Medelvärdet av de kortaste vägarna kallas nätverkets *längd, l,* och beräknas som:

$$l = \frac{1}{n(n-1)} \sum_{v \in V} \sum_{w \neq v \in V} d_{vw} \quad \textbf{(10)}$$

där n är antal noder i grafen och d_{vw} är den kortaste vägen mellan nod v och nod w (Holme et al., 2002). Diametern och längden är två mått på hur sammanhängande nätverket är. De kan även sägas beskriva hur effektivt flödet är mellan noderna. Dessa mått fungerar dock endast när nätverket består av en enda grafkomponent. Om det består av flera fristående grafkomponenter, kommer det att finnas noder som inte har någon länk alls mellan sig och såväl diametern som medelvärdet blir oändligt stort. (Newman, 2003) Ett alternativ är då att beräkna den *inverterade längden*:

$$l^{-1} = \frac{1}{n(n-1)} \sum_{v \in V} \sum_{w \neq v \in V} \frac{1}{d_{vw}} \quad \textbf{(11)}$$

där $\frac{1}{d_{vw}} = 0$ eftersom d_{vw} går mot oändligheten om nod v och nod w saknar länk (Holme et al., 2002).

Det kan vara betydelsefullt ur sårbarhetssynpunkt att veta om många av de kortaste vägarna i nätverket passerar en viss nod eller länk, eftersom denna då ”kontrollerar” en stor del av flödet i nätverket och avlägsnande av denna nod eller länk antagligen ökar nätverkets inverterade längd. En nods *intermeditet* anger hur många kortaste vägar som passerar noden. Rent matematiskt kan den definieras som:

$$B(u) = \sum_{v \in V} \sum_{w \neq v \in V} \frac{\sigma_{vw}(u)}{\sigma_{vw}} \quad \textbf{(12)}$$

där σ_{vw} är antal kortaste vägar mellan nod v och nod w, och $\sigma_{vw}(u)$ är antalet kortaste vägar mellan nod v och nod w som passerar nod u. En länks intermeditet definieras efter samma princip. (Holme, 2004)

6.3 Några mått på nätverkets robusthet

Ett robusthetsmått mäter hur väl systemet kan stå emot en eventuell påfrestning. En del robusthetsmått syftar till att bedöma systemets robusthet utifrån dess ursprungliga struktur. Andra används för att mäta systemets sårbarhet då det utsätts för en påfrestning.

Den genomsnittliga nodgraden används ibland som ett robusthetsmått. En hög genomsnittlig nodgrad indikerar att det finns många länkar i förhållande till noder i nätverket vilket innebär många alternativa vägar mellan noderna och därför en högre robusthet.

Klustringskoefficienten kan användas för att jämföra olika nätverks robusthet. En hög klustringskoefficient innebär en hög densitet av trianglar i nätverket vilket medför många alternativa vägar mellan noderna.

Förändringen av den största grafkomponenten och nätverkets inverterade längd vid utslagning av noder eller länkar i nätverket har ofta studerats i sårbarhetsanalyser. Om de minskar snabbt betyder det att nätverket sannolikt inte är särskilt robust.

För nätverk som matas med ett flöde, till exempel infrastrukturella nätverk för el, vatten och värme, är det viktigt att ta hänsyn till matning från inmatningsnoder vid analys av nätverkets robusthet. Tre mått som gör detta genom att analysera nätets sårbarhet då det utsätts för ett visst riskscenario är *CL (connectivity loss)*, *CECL (customer equivalent connectivity loss)* och *DC (designkoefficienten)*. CL och CECL illustreras som kurvor i ett diagram medan DC är ett korrelationsmått.

CL är den genomsnittliga minskningen av kopplingar mellan inmatningsnoder och övriga noder i nätverket och beskriver alltså antalet kvarstående möjligheter för noderna att få matning från inmatningsnod. CL är ett värde mellan noll och ett och beräknas som:

$$CL = 1 - \left\langle \frac{N_{gi}}{N_g} \right\rangle_i \qquad \textbf{(13)}$$

där N_g är det totala antalet inmatningsnoder i nätet och N_{gi} antalet inmatningsnoder som noden *i* fortfarande är ansluten till. (Albert, Albert & Nakarado, 2004)

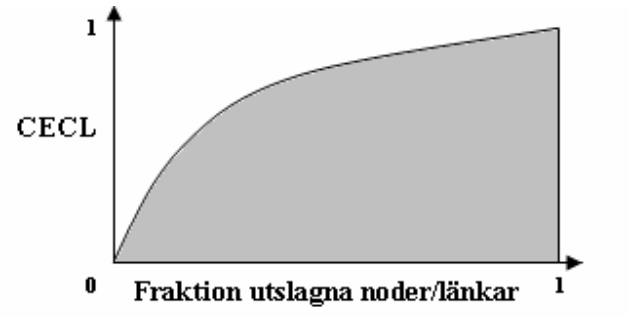
CECL mäter konsekvenserna av ett riskscenario som fraktionen *kundekvivalenter* som förlorat matning. Kundekvivalenten är ett kvantitativt mått på en nods *värde*. Detta kan till exempel vara antal abonnenter knutna till noden. Vilket värde som väljs på kundekvivalenten beror dels på vilken information som finns tillgänglig, dels på vilket perspektiv analysen ska göras utifrån. Om analysen till exempel ska göras utifrån ett ekonomiskt perspektiv bör en kundekvivalent som speglar varje nods ekonomiska värde väljas.

För CECL antas att så länge det finns minst en inmatningsnod kopplad till noden kommer den att kunna upprätthålla sin funktion. CECL är ett värde mellan noll och ett och beräknas på följande sätt:

$$CECL = \frac{CE_{loss}}{CE_{tot}} \qquad \textbf{(14)}$$

där CE_{loss} är mängden kundekvivalenter som förlorat samtliga kopplingar till inmatningsnoder och CE_{tot} är den totala mängden kundekvivalenter för nätet.

Arean under den kurva som illustrerar CECL som funktion av fraktion utslagna noder eller länkar kallas för *SVC (societal vulnerability coefficient)* och kan vara ett värde mellan noll och ett. Se figur 16.



Figur 16 Illustration av en CECL-kurva. Det grå området är SVC, arean under kurvan.

Ju närmre noll SVC är, desto långsammare bryts nätet ner och desto mer robust är nätet enligt CECL. SVC tar inte någon hänsyn till lokala variationer i kurvan och därför kan ett nät enligt CECL-kurvan till exempel vara mer robust än ett annat för små påfrestningar men mindre robust för större utan att detta syns på SVC-värdet. Därför bör inte SVC studeras fristående från CECL. (Johansson, Jönsson & Johansson, 2006)

Vid slumpmässigt avlägsnande av noder eller länkar i nätverket kommer noderna att förlora koppling till inmatningsnod i en viss ordning. Korrelationen mellan denna ordning och nodens kundekvivalent är ett mått på hur väl nätverket är designat och kallas för DC. DC kan ligga mellan -1 och 1. Det bästa, sett till nätverkets design, är om noder med hög kundekvivalent förlorar koppling till inmatningsnod sist vilket indikeras av ett högt DC. (Johansson, Jönsson & Johansson, 2006)

6.4 Val av robusthetsmått

I valet av robusthetsmått är det viktigt att utgå ifrån vilken sorts analys som ska göras och hur riskscenarierna ska definieras. Det är dessutom viktigt att beakta det system som ska beskrivas. Ett elnät består av noder och länkar som troligen är olika skyddsvärda, vilket bör tas hänsyn till. Det matas med ett flöde varför inmatningspunkterna bör inkluderas i robusthetsmåttet. Slutligen är det nätets leveranssäkerhet, det vill säga dess förmåga att leverera el till abonnenterna, som är av betydelse i analysen. Ett robusthetsmått som möjliggör uppdelning av konsekvenser i lämpliga riskscenarier, som tar hänsyn till nodernas och länkarnas olika värde samt antalet inmatningsnoder, och som fokuserar på nätets förmåga att leverera el till abonnenterna, är ett lämpligt robusthetsmått för elnät. Nedan diskuteras tidigare nämnda robusthetsmått utifrån deras lämplighet för elnät.

Den genomsnittliga nodgraden och klustringskoefficienten beskriver nätets ursprungliga struktur. Dessa mått kan vara bra för att få en indikation om huruvida systemet har många länkar i förhållande till noder och därmed kommer att vara robust för en påfrestning. Nätverkets diameter och inverterade längd kan vara intressanta att veta för att få en uppfattning om hur väl sammanlänkat nätverket är. I en risk- och sårbarhetsanalys kan förändringen av diametern och den inverterade längden användas som ett mått på konsekvensen av olika riskscenarier. Inget av de fyra måtten tar dock hänsyn till antalet inmatningsnoder eller distributionsnodernas värde. För en risk- och sårbarhetsanalys av eldistributionsnät är de därför inte särskilt intressanta. De kan dock användas för att ge en första indikation om robustheten i nätets struktur och därför valdes den genomsnittliga nodgraden och den inverterade längden att studeras vid en inledande analys.

Med CL kan konsekvenserna av ett riskscenario mätas i en simulering. Det går dock inte att, med CL, ta hänsyn till att noderna har olika betydelse. Det går däremot att göra med CECL eftersom detta mått använder kundekvivalenten som konsekvensmått. Till följd av detta valdes CECL och SVC att använda för att göra risk- och sårbarhetsanalys i den empiriska studien.

DC är ett korrelationsmått som baseras på i vilken ordning noderna förlorar kontakt med inmatningsnod. För att ta fram DC krävs ett simuleringsverktyg. En enklare variant på DC, som inte kräver simulering, kan dock härledas från ett högst troligt samband, nämligen att det finns en korrelation mellan en nods avstånd till inmatningsnod, och nodens sårbarhet. Detta samband är troligt eftersom en nod som ligger långt bort från inmatningsnod borde ha större sannolikhet att förlora matning än en som ligger nära då den är beroende av att fler mellanliggande komponenter fungerar för att den ska få matning. Som bilaga 3 visar kunde sambandet även iakttas i den empiriska studien. Med denna bakgrund är det inte särskilt bra om betydelsefulla distributionsnoder, det vill säga noder med hög kundekvivalent, ligger i elnätets periferi. Det kan därför vara relevant att analysera sambandet mellan en distributionsnods kundekvivalent och avståndet denna har till närmaste inmatningsnod. I den empiriska studien valdes därför att analysera dessa två mått. För att särskilja dem från varandra valdes det mått som tas fram genom simulering att kallas för DC_{order}, och det som tas fram genom att mäta avståndet från till inmatningsnod för DC_{path}. DC_{order} och DC_{path} tar hänsyn till både antalet inmatningsnoder och distributionsnodernas kundekvivalent. Dock bör de, eftersom de är korrelationsmått, användas som komplement till CECL.

6.5 Val av värde på kundekvivalenten

Vilket värde som väljs på kundekvivalenten beror på vad som anses viktigt att mäta och hur resultatet ska användas. Utifrån den information som fanns tillgänglig i indata valdes att undersöka två alternativ: antal abonnenter knutna till noden och årlig förbrukad energi i noden. Med dessa alternativ har endast distributionsnoder något värde. Utifrån rapportens syfte valdes sedan att analysera dessa två alternativ dels ur samhällsperspektiv, dels ur ett ekonomiskt perspektiv. Detta eftersom båda dessa ansågs viktiga att ta hänsyn till när det handlar om elnät.

Det bästa ur ett samhällsperspektiv kan tyckas vara att så få abonnenter som möjligt blir strömlösa vid ett avbrott. Detta argument talar för att antal abonnenter ska väljas som värde på kundekvivalenten. De enskilda abonnenterna skiljer sig dock väldigt mycket åt i energiförbrukning. En abonnent behöver inte vara ett privat hushåll, den kan även vara en större verksamhet som är mycket viktigt ur samhällssynpunkt, till exempel ett sjukhus. Detta talar för att årlig förbrukad energi ska väljas som värde på kundekvivalenten.

Ur ett ekonomiskt perspektiv är argumentet för att välja årlig förbrukad energi den inkomst som nätföretaget går miste om till följd av matningsbortfall vid ett avbrott. Relativt nya bestämmelser i ellagen innebär dock höga böter för nätföretagen vid långa elavbrott (se bilaga 4) vilket talar för att antal strömlösa abonnenter kan vara ett bättre mått på kundekvivalenten ur ett ekonomiskt perspektiv.

En sammanvägning av de två faktorerna skulle antagligen ge det bästa värdet på kundekvivalenten. Dock valdes detta att inte göras då bedömningen gjordes att tillräckligt underlag för hur de skulle vägas samman saknades vid rapportens skrivande.

I rapporten valdes istället att använda årlig uttagen energi som värde på kundekvivalenten. Detta eftersom det ansågs att denna faktor, baserat på ovanstående argument, speglade konsekvensen av matningsbortfall något bättre än antal strömlösa abonnenter.

6.6 Verktyg

För att utföra analyserna i den empiriska delen av rapporten användes två simuleringsverktyg, NetCalc och ACC, och ett visualiseringsverktyg, Net Draw.

6.6.1 NetCalc

I NetCalc studeras ett nätverk genom att det modelleras i en Excelfil som en graf med noder och länkar. För att kunna utföra modelleringen krävs viss information angående nätverket. Denna är nodernas position i form av koordinater, de andra noder som varje nod är kopplat till samt värdet för varje nod angivet i kundekvivalenter. Förutom detta måste det i filen även anges vilka noder som utgör inmatningsnoder. Excelfilen konverteras sedan till en skv-fil som NetCalc kan läsa. (Johansson, 2006)

Programmet kan utifrån de koordinater som angivits i indatafilen beräkna avståndet mellan noderna i nätverket. Beräkningen av avståndet sker utifrån Pythagoras sats och blir därför ”fågelvägen” mellan noderna. (Johansson, 2006)

Netcalc kan sedan dels utföra en analys av det befintliga nätverket, dels utsätta det för en av flera möjliga attackstrategier. Analysen sker genom att programmet räknar fram olika typer av mått som beskriver egenskaperna hos nätverket. Exempel på sådana mått är klustringskoefficienten och den inverterade längden. Analysen ger även en så kallad distansmatris över nätverket som anger avståndet mellan samtliga noder i nätverket. Detta avstånd kan i dagsläget dock endast anges i antal länkar mellan noderna. (Johansson, 2006)

Sårbarheten hos nätverket studeras genom att utsätta nätverket för olika attackstrategier. I programmet väljer användaren att slå ut antingen länkar eller noder. I dagsläget går det inte att slå ut både noder och länkar i samma simulering. Följande attackstrategier är möjliga med programmet:

- *Utslagning med avseende på grad* - nod med högst antal länkar kopplat till sig slås ut först.
- *Utslagning med avseende på attribut* - nod eller länk med högst värde på ett visst attribut slås ut först. Vilket attribut väljer användaren själv.
- *Slumpmässig utslagning* - noder eller länkar slås ut helt slumpmässigt.
- *Slumpmässig utslagning med avseende på attribut* – noder eller länkar slås ut slumpmässigt men sannolikheten är viktad efter ett visst attribut som användaren själv väljer.
- *Kontinuerlig omräkning* - nod eller länk med högst intermeditet slås ut först och för varje ny utslagning beräknas intermediteten om. Finns det fler noder eller länkar med samma intermeditet sker utslagningen av dessa slumpmässigt.

För ett elnät kan de två första attackstrategier, utslagning med avseende på grad eller attribut, representera riktade antagonistiska attacker, exempelvis ett terroristangrepp. Den tredje attackstrategin, slumpmässig utslagning, kan representera de driftstörningar som normalt drabbar ett elnät till följd av till exempel väder, mindre åverkan, materialfel och handhavandefel samt säkringsbrott. Den fjärde, slumpmässig utslagning med avseende på attribut, kan användas då det kan anses att en viss nod eller länk i elnätet har större sannolikhet att slås ut eftersom denna är mer utsatt i förhållande till resten av elnätet. Den sista attackstrategin, kontinuerlig omräkning, kan användas för att beskriva exempelvis kaskadeffekter i elnätet. (Johansson, 2006)

I NetCalc slås komponenter ut en efter en medan konsekvensen av varje ytterligare utslagen komponent beräknas. Detta sker tills samtliga komponenter är utslagna. Resultatet av simuleringen ges som en textfil som även kan öppnas i Excel. I resultatfilen anges bland annat komponenternas utslagningsordning samt konsekvensen av varje ytterligare utslagen komponent i de storheter som användaren angivit i indatafilen. Om flera simuleringar gjorts anges även medelvärdet av simuleringarna. (Johansson, 2006)

Eftersom NetCalc fortfarande är under utveckling fanns viss möjlighet till uppgraderingar och anpassningar av programmets egenskaper och då programmet är framtaget inom Lunds universitet fanns dessutom möjlighet till full insyn i hur det fungerar.

6.6.2 ACC

För att beräkna *kritiska komponenter* eller *kritiska komponentpar* i elnätet används datorprogrammet ACC som är framtaget i Matlab.

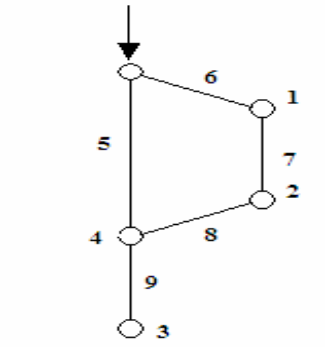
Med kritiska komponenter menas komponenter som nätet är sårbart för utslagning av. Kritiska komponentpar är par av komponenter som nätet är sårbart för en samtidig

utslagning av. Ett kritiskt komponentpar kan bestå av två noder, två länkar, eller en nod och en länk. (Jönsson, Johansson & Johansson, 2007)

Ju mer sårbart nätverket är för utslagning av en komponent eller ett par, desto mer kritisk är denna. Vid framtagning av kritiska komponenter och komponentpar i ACC tas även hänsyn till kapacitetsbegränsningar. Detta innebär att även om en distributionsnod har koppling till inmatningsnod är det inte säkert att den kan få matning från denna om inmatningsnodens kapacitet inte är tillräckligt stor. Detta är en egenskap hos ACC som saknas i NetCalc. (Jönsson, Johansson & Johansson, 2007)

Indatafilen till programmet ser i princip likadan ut som den för NetCalc. Eftersom hänsyn tas till kapacitetsbegränsningar måste dock även inmatningsnodernas kapacitet finnas med som indata. I ACC slås en komponent ut i taget, varefter konsekvensen för varje utslagning beräknas. Detta gäller även för flera samtidiga utslagningar. Sedan rangordnas komponenterna och komponentparen efter hur kritiska de är, det vill säga efter den konsekvens de ger upphov till. Programmet beräknar även den eventuella synergi som kan uppkomma då flera komponenter slås ut samtidigt. (Johansson, 2006)

För att tydligare illustrera vad som menas med kritiska komponenter kan ett mindre nätverk, som illustreras i figur 17, studeras.

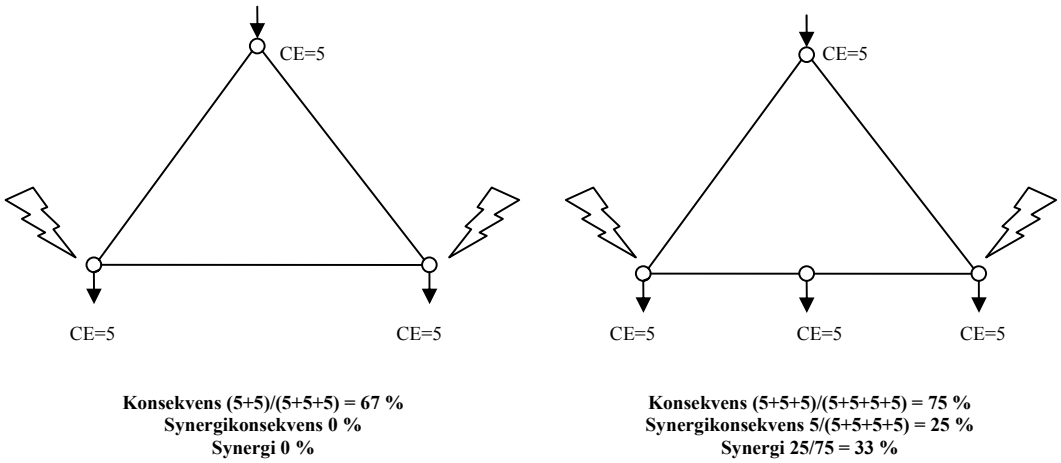


Figur 17 Ett mindre nätverk med tio komponenter

Som figur 17 visar medför utslagning av vissa komponenter större konsekvenser än andra. Noden längst upp i figuren är en inmatningsnod. Utslagning av denna nod orsakar störst konsekvens och den är därmed den mest kritiska punkten i nätet. Slås exempelvis komponent 4 ut innebär detta att även komponent 3 förlorar matning. Slås däremot komponent 2 ut bidrar inte detta med en större konsekvens än dess egna direkta, eftersom matningen kan omdirigeras till en annan väg. (Jönsson, Johansson & Johansson, 2007)

Utslagning av fler komponenter följer samma resonemang. Dock kan även synergi uppkomma vid utslagning av fler komponenter. Detta uppkommer då exempelvis komponent 7 och 5 slås ut. Summan av konsekvenserna för utslagning av de enskilda komponenterna 7 och 5, vilken är noll, är mindre än konsekvenserna av en samtidig utslagning av dessa.

Figur 18 visar principen för synergi.



Figur 18 Två fel utan synergi (till vänster) och två fel med synergi (till höger)

Skulle endast en av de två noderna i den högra figuren i figur 18 ha slagits ut, så hade inte noden i mitten påverkats. Det två samtidiga utslagningarna leder till synergi som är den andel av det totala matningsbortfallet som kan härledas till den mittersta noden.

Eftersom ACC är framtaget inom Lunds universitet fanns möjlighet till full insyn i hur programmet fungerar.

6.6.3 Net Draw

Net Draw är ett datorprogram med vars hjälp det går att rita upp ett nätverk utifrån givna koordinater. Programmet kan läsa flera typer av filer eller spara ner nätverket som en karta i form av olika typer av bildfiler. Förutom att rita upp nätverket kan programmet även färgmarkera eller förstora vissa komponenter med hänsyn till något attribut kopplat till dessa. Till exempel kan storleken på noder i ett elnätverk variera med antalet kunder som är kopplat till noden. På detta sätt kan fördelningen av ett visst attribut i nätverket på ett överskådligt sätt visualiseras. Net Draw är skrivet av Steve Borgatti och går att ladda ner gratis via mjukvarudistributören Analytic Technologies. (Analytictech, 2007)

7 Empirisk studie

I detta kapitel beskrivs utförandet och resultaten av den risk- och sårbarhetsanalys som gjordes för att illustrera hur en simuleringsmetod kan användas i enlighet med den nya lagstiftningen.

7.1 Val av nät

De tre elnät som användes i studien bestod av ett tätortsnät ett blandat nät och ett glesbygdsnät. Syftet med att studera tre olika nätstrukturer var att undersöka hur sårbarheten för dessa skiljer sig åt för olika påfrestningar. I analysen studerades nät på 12 kV-nivån, det vill säga distributionsnätet. Motiveringen till detta var att antalet strömlösa abonnenter och abonnentavbrottstimmar, enligt driftstörningsstatistiken från DARWIN som fanns tillgänglig för det blandade nätet, var störst på 12 kV-nivån. Se tabell 1.

	0,4 kV	12 kV	24 kV
Antal avbrott	411	371	62
Andel avbrott	49%	44%	7%
Antal strömlösa abonnenter	3 975	59 923	54 443
Andel strömlösa abonnenter	3%	51%	46%
Antal abonnentavbrottstimmar	6 773	186 102	58 724
Andel abonnentavbrottstimmar	3%	74%	23%

Tabell 1 Avbrott fördelade på spänningsnivå

7.2 Beskrivning av valda nät

Samtliga tre elnät består av en enda grafkomponent. Detta innebär att varje nätstation i ursprungsläget kan få matning från vilken som helst av inmatningspunkterna. Som tabell 2 visar, har alla tre näten en fördelning av nodernas grad som stämmer bra överens med en power law-fördelning.

Glesbygdsnät		Blandat nät		Tätortsnät	
$Y = 1473{,}9x^{-3{,}2034}$		$Y = 407{,}86x^{-2{,}6988}$		$Y = 81{,}557x^{-1{,}7467}$	
$R^2 = 0{,}8432$		$R^2 = 0{,}7821$		$R^2 = 0{,}7573$	
Nodgrad	**Antal noder**	**Nodgrad**	**Antal noder**	**Nodgrad**	**Antal noder**
1	430	1	101	1	22
2	285	2	225	2	59
3	401	3	113	3	35
4	17	4	8	4	13
5	5	6	1	5	5
6	3	8	1	8	1
8	1	10	1	9	1
10	1			13	1

Tabell 2 Fördelningen av nodernas grad hos de tre näten. Y är fördelningen av nodernas grad. R^2 är ett värde mellan 0 och 1 som anger hur väl fördelningen stämmer överens med en power law-fördelning där 1 är fullständig överensstämmelse.

Detta är av intresse eftersom tidigare studier har visat att denna egenskap medför att nätverken är robusta för slumpmässiga attacker men sårbara för riktade attacker på noder med högst grad (Albert, Albert & Nakarado, 2004).

Tätortsnätet består av ett elnät med till största delen maskad karaktär och jordkabel. Strömmen kan därmed matas på flera alternativa vägar och nätet ligger mer skyddat för väderpåverkan. Hela tätortsnätet består av 12 kV-ledningar.

Det blandade nätet består av ett tätortsnät med omgivande landsbygdsnät. De delar som ligger i tätort är till största delen maskade och består av jordkabel medan de delar som utgör landsbygdsnät har radiell karaktär och består av luftledning.

Glesbygdsnätet har en mer radiell struktur än tätortsnätet. Detta beror på att glesbygdsnätet har färre abonnenter som dessutom bor långt ifrån varandra vilket i regel gör det olönsamt att bygga in alternativa matningsvägar. De långa avstånden gör också att majoriteten av ledningarna är luftburna, bland annat eftersom detta är billigare än jordkabel. Glesbygdsnätet består av spänningsnivåerna 12 och 24 kV.

Tabell 3 visar en sammanställning över de tre näten.

	Tätortsnät	Blandat nät	Glesbygdsnät
Antal abonnenter	8 370	5 768	7 919
Total uttagen energi/år (kWh)	183 585 084	99 294 673	106 864 361
Antal noder	137	450	1 143
Antal länkar	176	473	1 166
Antal inmatningsnoder	3	5	5
Medelgrad	2,569	2,102	2,040
Inverterad längd	0,199	0,064	0,052

Tabell 3 Data för de tre näten

Som tabell 3 visar har tätortsnätet högst medelgrad, därefter kommer det blandade nätet och sist glesbygdsnätet. Detta indikerar att tätortsnätet har flest länkar i förhållande till noder vilket innebär störst andel alternativa matningsvägar. Eftersom tätortsnätet har en struktur som i högre grad än de andra två näten är maskad, är detta en rimlig slutsats.

Glesbygdsnätet har minst inverterad längd vilket tyder på att det är mer utspritt än det blandade nätet och tätortsnätet. Även detta är rimligt, eftersom glesbygdsnätet i högre grad än de andra två är förlagt till landsbygd och därmed har längre avstånd mellan noderna.

Utifrån denna information kan antagandet göras att glesbygdsnätet sannolikt är mest sårbart av de tre näten, medan tätortsnätet troligtvis är mest robust. Detta eftersom tätortsnätet både har högst medelgrad och störst inverterad längd.

7.3 Modellering av näten

Elnäten modellerades som nätverk med noder och länkar. Vid modellering av näten antogs det finnas tre typer av noder. Dessa var:

- *Inmatningsnoder* - fördelningsstationer där inmatning av el från regionnätet sker
- *Distributionsnoder* - nätstationer som fördelar elen via lågspänningsnätet ut till slutabonnenterna
- *Förgreningsnoder* - där ledningarna förgrenar sig för att kunna mata olika områden med el

I det blandade nätet modellerandes även frånskiljare, komponenter som kan öppnas för att förhindra att el kan matas längst en ledning, som noder.

Ett antal antaganden gjordes för att förenkla modelleringen av näten. Till att börja med antogs att om en ledning på kartan förelåg mellan två noder kunde det gå ström igenom den (i ursprungsläget). Detta är inte nödvändigtvis sant i verkligheten då det kan finnas flera orsaker till att en ledning är ur funktion, den kan till exempel vara nedlagd eller under konstruktion eller reparation. Det antogs vidare att det endast fanns en länk mellan varje nodpar. I verkligheten kan det finnas flera ledningar mellan två komponenter. Distributionsnoder antogs vara seriekopplade. Det innebär att om någon av dessa slogs ut kunde inte den del av nätet som ligger bortom denna punkt matas med ström.

Dessutom antogs i NetCalc att samtliga noder och länkar hade obegränsad kapacitet för strömöverföring. Då alla komponenter i ett elnät är mer eller mindre begränsade kapacitetsmässigt är även detta en förenkling av verkligheten. Detta antagande gjordes eftersom det vid analysens genomförande inte var möjligt att ta hänsyn till kapacitetsbegränsningar i programmen.

Inmatningsnoder antogs inte kunna slås ut. Anledningen till att detta antagande gjordes var att inmatningsnoderna ansågs vara mer skyddade än övriga noder. En utslagning av en inmatningsnod ger stora konsekvenser för nätet och det gör att ett elbolag kan antas ha hög prioritet i att skydda denna.

Där näten inte var naturligt avgränsade gjordes detta genom att frånskiljare i lämpliga avgränsningspunkter modellerades som permanent öppna. Övriga frånskiljare i nätet modellerades som slutna. Detta är en förenkling som kan tolkas som att den tid det tar att koppla om matningen vid ett avbrott är försumbart kort. Förenklingen gjordes eftersom det vid analysens genomförande inte var möjligt att ta hänsyn till omkopplingstid i programmen. Se bilaga 5 för en analys av vad förenklingen betyder för sårbarheten.

Längden på länkarna beräknades i NetCalc baserat på nodernas koordinater. Resultatet blev ”fågelvägen” mellan noderna och alltså inte den verkliga längden av länkarna. Denna approximation gjordes eftersom det är väldigt svårt och tidskrävande att ta reda på den verkliga länklängden.

7.4 Metod

Den första delen av analysen syftade till att utveckla en modell som tidigare studerats genom att pröva om det går att ta hänsyn till vissa attribut. Utifrån diskussionen i kapitel 6.4, ”Val av robusthetsmått”, valdes CECL (med SVC) som verktyg för att göra en sårbarhetsanalys och en riskanalys i den andra och tredje analysdelen. För att analysera nätens konstruktion studerades i den fjärde analysdelen DC_{path}, DC_{order} och dessutom kartor över näten där sårbara områden markerades. Som sista analysdel valdes att göra en djupare analys av två av de riskscenarier som analyserades i risk- och sårbarhetsanalysen.

De empiriska studierna utfördes med hjälp av de datorbaserade verktyg som beskrevs i kapitel 6.6, ”Verktyg”. Analyserna ”Utveckling av modellen”, ”Sårbarhetsanalys” och ”Riskanalys” gjordes med hjälp av NetCalc. Analysdelen ”Nätens konstruktion” gjordes med hjälp av NetCalc och Net Draw. Kritiska komponenter togs fram med hjälp av ACC.

7.4.1 Utveckling av modellen

Tidigare studier på området utgick från en nätverksmodell ur ett topologiskt perspektiv. För att öka simuleringsmetodens användbarhet sågs en möjlighet att utveckla detaljeringsgraden i modellen ytterligare. Eftersom felfrekvensen hos länkarna i elnätet antogs vara delvis kopplad till längd och typ av länk studerades betydelsen av att ta hänsyn till dessa attribut i modelleringen i näten. Valet av attribut gjordes dels utifrån egna antaganden och dels med bakgrund av tidigare studier.

Betydelsen av attributet länklängd analyseras eftersom det antogs att ledningar drabbas av fler driftstörningar ju längre de är då sträckan som kan drabbas av ett fel ökar. Sambandet antogs vara linjärt. Attributet länktyp[8] studerades eftersom tidigare studier visade att sannolikheten för fel generellt är större i luftledning än i jordkabel (Wallnerström, 2005 och Statens Energimyndighet, 2006). Denna analys utfördes endast för det blandade nätet, eftersom det endast var för detta nät som information fanns angående vilka ledningar som var av respektive typ.

I de simuleringar då hänsyn togs till länklängd slogs länkarna ut slumpmässigt men med högre sannolikhet ju längre länken var. I det fallet då inte hänsyn till länklängd togs, slogs länkarna ut helt slumpmässigt och alla länkar hade lika stor sannolikhet att bli utslagna. För att se om längden på länkarna hade betydelse beräknades sedan den avvikelse som uppstod till följd av hänsyn till länklängden. Varje fall simulerades 1000 gånger och därefter beräknades medelvärdet utifrån dessa.

Även länktypens inverkan studerades genom att göra simuleringar dels med och dels utan hänsyn till attributet. Eftersom information om driftstörningsfrekvenser hos respektive ledningstyp inte fanns att tillgå specifikt för nätet, behövdes data för viktningen tas fram på annan väg. Tidigare studier har gjorts på nät med snarlik karaktär som det blandade nätet där driftstörning i luftledning, baserat på statistik, antogs vara 10 gånger vanligare än jordkabel (Wallnerström, 2005). För att undersöka hur mycket olika val av proportioner påverkar analysen, valdes dock att göra fem olika simuleringar där

[8] I analysen luftledning och jordkabel

driftstörning i luftledning antogs vara mellan 5-25 gånger mer frekvent än i jordkabel. Detta gjordes genom att längden på de länkar som var luftledningar multiplicerades med 5, 10, 15, 20 och 25. Simuleringar gjordes sedan med slumpmässig utslagning av länkar där sannolikheten för utslagning var viktad mot länklängden. På så sätt hade länkar bestående av luftledning högre sannolikhet att slås ut än de av jordkabel. Simuleringarna jämfördes sedan med de utan hänsyn till länktyp och avvikelsen mellan simuleringarna beräknades. Varje fall simulerades 1000 gånger. Därefter beräknades medelvärdet av dessa.

7.4.2 Sårbarhetsanalys

Som initiala påfrestningar i sårbarhetsanalysen valdes fyra olika attackstrategier som simulerades i NetCalc. Dessa valdes eftersom de bedömdes som mest relevanta för elnät. Det fyra initiala påfrestningarna blev då:

- *Slumpmässig utslagning av noder respektive slumpmässig utslagning av länkar* som avsåg illustrera de driftstörningar som eldistributionsnät i de flesta fall drabbas av och som resulterar i ett avbrott. Det antogs att dessa avbrott skedde slumpmässigt för noder och slumpmässigt men viktat mot attributen ledningslängd och ledningstyp för länkar.

- *Riktad utslagning med avseende på nodgrad* som avsåg undersöka hur väl det teoretiska antagandet om att nätet var mycket sårbart för riktad utslagning av noder som utgör nav stämde in på de tre näten.

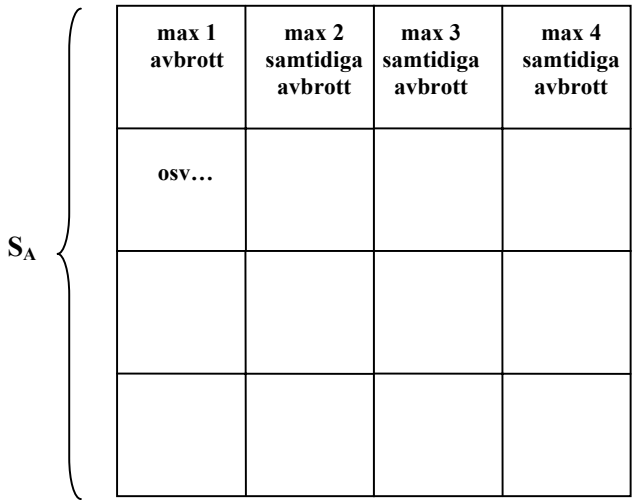
- *Riktad utslagning med avseende på årlig förbrukad energi* som skulle illustrera en antagonistisk attack av en aktör med viss kunskap om effektuttagen i nätet och som därför attackerar de distributionsnoder där den årliga förbrukade energin är som högst.

Ett riskscenario är en successiv utslagning av hela nätet till följd av en initial påfrestning. För de påfrestningar som innebär riktade utslagningar finns endast ett riskscenario i riskscenariorymden. För de blandade utslagningarna utgörs riskscenariorymden dock av samtliga möjliga utslagningsordningar i nätet. Det är inte svårt att inse att detta leder till en enorm mängd riskscenarier. För att analysen skulle bli genomförbar gjordes därför en approximation som innebar att 1000 riskscenarier simulerades för varje påfrestning som innebar slumpmässig utslagning. I sårbarhetsanalysen är det konsekvensen av en initial påfrestning som är av intresse och därför analyserades inte sannolikheten för de olika påfrestningarna utan endast konsekvensen mätt i CECL och SVC, som för de slumpmässiga utslagningarna utgjordes av ett medelvärde.

SVC beräknandes även för de 10 % första riskscenarierna, det vill säga upp till 10 % av de först utslagna noderna eller länkarna. Anledningen var att det är mindre troligt att mer än 10% utav komponenterna slås ut samtidigt. (Telge nät AB, 2006).

7.4.3 Riskanalys

I riskanalysen delades riskscenariorymden upp efter maximalt antal samtidiga avbrott. Detta gjordes eftersom information om hur vanliga dessa riskscenarier varit historiskt kunde härledas ut driftsstörningsstatistiken från DARWIN. Se figur 19.



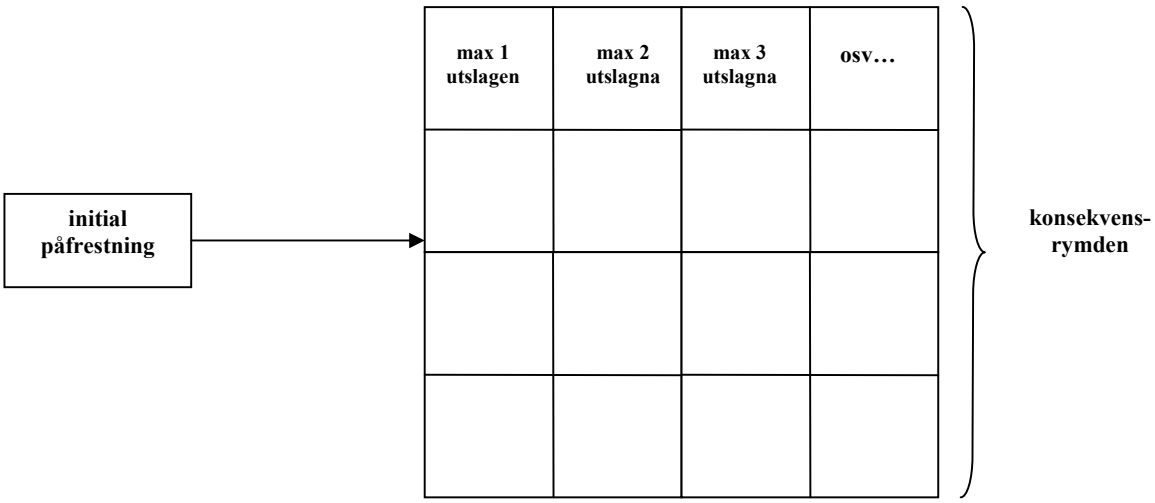
Figur 19 Uppdelning av riskscenariorymden S_A i riskscenarierna maximalt 1 avbrott, maximalt 2 samtidiga avbrott, och så vidare.

Varje riskscenario i riskscenariorymden innehåller samtliga scenarier som kan beskrivas som riskscenariot. Exempelvis innehåller riskscenariot ”max ett avbrott” samtliga sätt som ett avbrott kan uppstå på, vilket är lika många som det finns komponenter. ”Max två samtidiga avbrott” innehåller samtliga möjliga fall där avbrott sker i två komponenter samtidigt, och så vidare.

Sannolikheten för varje riskscenario togs fram baserat på historiska data från databasen DARWIN. Detta bedömdes vara lämpligt att göra för att visa hur historiska data kan användas i en riskanalys. Sannolikheten för ett riskscenario byggde på hur stor del av den totala tiden som kunde härledas till scenariot. Beräkningen av sannolikheten inleddes med att den totala tid som kunde härledas till varje riskscenario togs fram. Denna tid beräknades, med hjälp av en algoritm[9], ur driftstörningsstatistiken från DARWIN (Ohlson, 2006). Därefter dividerades varje tid med den totala tid som statistiken sträckte sig över. På så sätt erhölls den del av den totala tiden som ett visst scenario varade för. Detta kan ses som sannolikheten för att det scenariot ska inträffa.

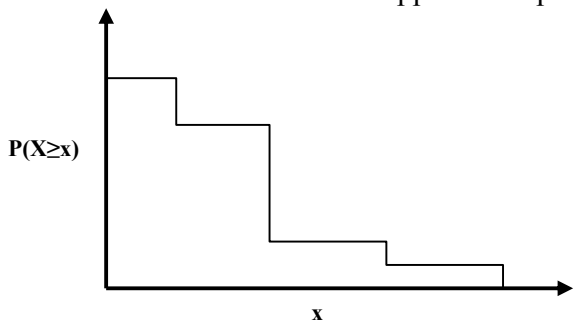
För att beräkna konsekvensen för varje riskscenario användes de konsekvenser som erhölls från simuleringarna av de slumpmässiga utslagningarna i sårbarhetsanalysen. Eftersom utslagningarna var slumpmässiga ansågs deras konsekvens vara vad som bäst speglade den verkliga konsekvensen av de olika riskscenarierna i riskscenariorymden. Se figur 20.

[9] Tillvägagångssättet hos denna beskrivs ej, se kapitel 1.4 ”Generella avgränsningar”.



Figur 20 Konsekvensföljden till följd av en initial påfrestning delas upp i antal utslagna komponenter

För att illustrera den totala riskens storlek ritades den kumulativa frekvensen för avbrott som funktion av konsekvensen upp i en riskprofil. Se figur 21.



Figur 21 Utseende hos en riskprofilkurva.

På x-axeln i figur 21 finns de konsekvenser som ingår i konsekvensrymden. På y-axeln finns sannolikheten för att konsekvensen är större eller lika med värdet på x-axeln, det vill säga den kumulativa sannolikheten. Denna typ av kurvor används bland annat för att beskriva samhällsrisk vid riskanalys av områden och anläggningar, och då med antal dödsfall som x och den kumulativa frekvensen av x eller fler dödsfall på y-axeln (Davidsson, 2003). Ofta bestäms då även en övre gräns för det område där risken är tolererbar (Davidsson, 2003). För elnät kan riskprofilen användas för att beskriva genomsnittligt matningsbortfall med x och den beräknade frekvensen för att matningsbortfallet ska bli x eller mer på y-axeln.

7.4.4 Nätens konstruktion

För att analysera nätens konstruktion valdes att analysera korrelationsmåtten DC_{path} och DC_{order}. Dessutom valdes att använda informationen om utslagningsordning och avstånd till inmatningsnod till att markera de mest och minst sårbara noderna i kartor över näten. Detta gjordes för att enkelt kunna identifiera särskilt sårbara och robusta områden i nätet och även, i kombination med kundekvivalenten, kunna motivera förstärkt skydd av vissa områden.

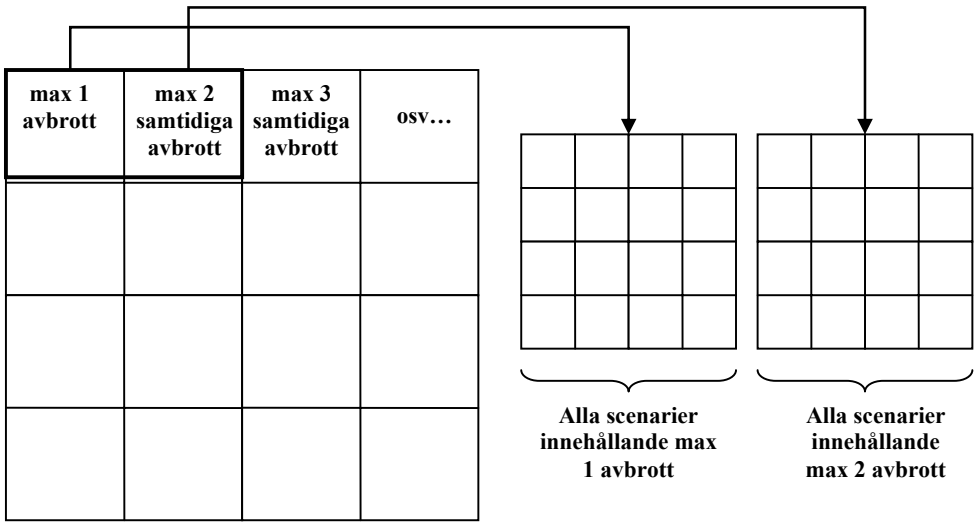
DC_{order} beräknades som korrelationen mellan i vilken ordning en distributionsnod förlorar matning och dess kundekvivalent. Utslagningsordningen erhölls från samma simuleringar som användes för sårbarhetsanalysen. DC_{path} beräknades utifrån nätets ursprungliga struktur som den negativa korrelationen mellan distributionsnodens avstånd till inmatningsnod, och distributionsnodens kundekvivalent. Korrelationen var negativ eftersom ju högre kundekvivalent en distributionsnod har, desto närmre bör den ligga en inmatningsnod för att nätet ska anses ha en robust konstruktion. För DC_{path} gjordes, till skillnad från DC_{order}, en del förenklingar. Dels togs inte hänsyn till den verkliga längden mellan noderna, utan varje länk hade längden ett. DC_{path} tog inte heller hänsyn till länktyp. Orsaken till detta är att DC_{path} beräknades utifrån den avståndsmatris som erhölls i analysen i NetCalc. I denna kunde vid analysens genomförande inte hänsyn tas till länklängd och länktyp. I framtida studier skulle dock faktiska avstånd mycket väl kunna användas för att beräkna $DC_{path.}$

För att kunna markera de mest och minst sårbara punkterna i elnäten på en karta användes datorprogrammet Net Draw. De mest sårbara punkterna var de som förlorat matning först i analysen och de minst sårbara punkterna var de som förlorat matning sist vid analysen. Vidare markerades även de noder med längst och kortast avstånd till en inmatningsnod i kartor. Visualiseringen gjordes genom att nätverken analyseras i NetCalc varpå resultatet sparades ner som så kallade VNA-filer. Därefter kunde nätverken öppnas med Net Draw och där visas som kartor. Kartorna sparades sedan ner som bilder där de mest sårbara och minst sårbara punkterna markerades med hjälp av ett ritprogram.

7.4.5 Kritiska komponenter

I riskanalysen delades riskscenariorymden upp efter maximalt antal samtidiga avbrott. Eftersom konsekvensen för varje riskscenario togs från de slumpmässiga simuleringarna i NetCalc blev denna ett medelvärde. Eftersom utslagning av olika komponenter i ett elnät i realiteten leder till olika allvarliga konsekvenser kan det dock vara intressant att dela upp riskscenariorymden ytterligare och istället för att dela upp riskscenariorymden i antal avbrott låta varje enskilt avbrott utgöra ett eget riskscenario. Istället för riskscenariot ”ett avbrott” där alla scenarier med ett avbrott ingår skulle då varje scenario med ett avbrott utgöra ett eget riskscenario.

Om detta gjordes för samtliga riskscenarier skulle dock analysen bli enorm. Ett sätt att begränsa analysens omfattning vore att utgå från driftstörningsstatistiken (Telge nät AB, 2006). Enligt denna är det nämligen ett par riskscenarier som dominerar, ett avbrott och två samtidiga avbrott. För att minska ner den detaljerade analysen kan den begränsas till att endast studera scenarier innehållande ett avbrott och två samtidiga avbrott. Se figur 22.



Figur 22 De scenarier som innehåller maximalt ett respektive två samtidiga avbrott lyfts ut och analyseras mer detaljerat.

I analysdelen ”Kritiska komponenter” valdes därför att analysera samtliga scenarier som innehåller en eller två utslagna komponenter med syfte att ta fram konsekvens för dessa. För att göra detta användes datorprogrammet ACC. I analysen simulerades endast ett av de tre näten, det blandade nätet. Detta gjordes eftersom den första riskanalysen endast behandlade detta nät.

Nätet modellerades på samma sätt som vid simuleringar i NetCalc, dock med vissa tillägg. För det första antogs att inmatningsnoder kunde slås ut. Inmatningsnoderna tillskrevs dessutom en maxkapacitet som var den högsta effekten som noderna kunde leverera till nätet. Vidare valdes distributionsnodernas kundekvivalent som toppeffekt per timme. Toppeffekten är den maximala effekt som levereras till abonnenterna. Genom tilläggen i modellen kunde hänsyn till kapacitetsbegränsningar tas vid simulering i ACC.

Konsekvensen beräknades i andel förlorad maximal effekt och enskilda kritiska komponenter rangordnades efter denna konsekvens. Kritiska kombinationer gav även upphov till synergi[10] och därför beräknade programmet även synergikonsekvensen samt synergi som är den del av den totala konsekvensen som är synergikonsekvens.

[10] Se kapitel 6.6.2, ”ACC”

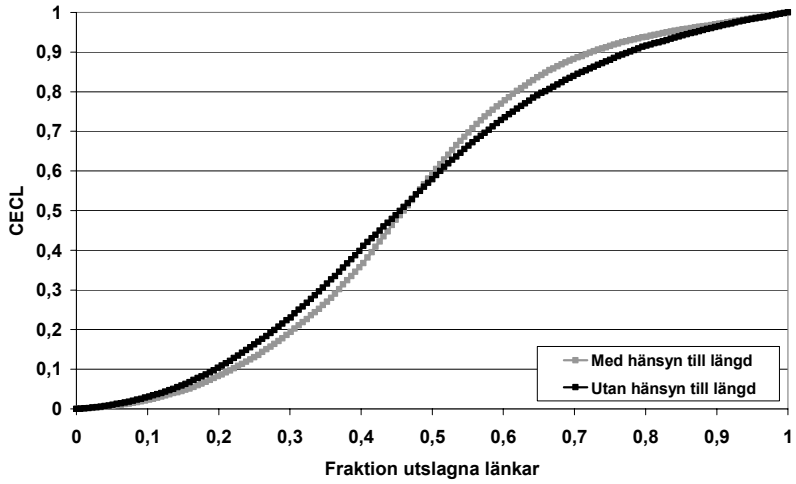
7.5 Resultat och diskussion

Med bakgrund i val av och metod för de empiriska studierna presenteras här resultatet och en diskussion kring detta.

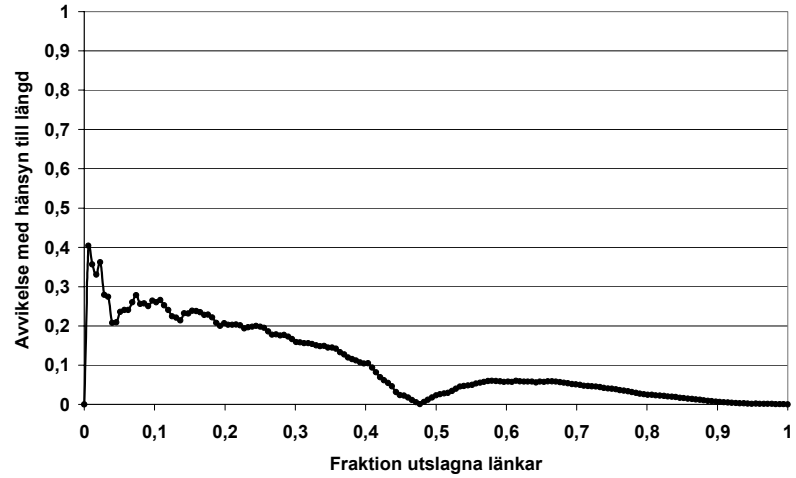
7.5.1 Utveckling av modellen

För att försöka utveckla modellen simulerades näten med och utan hänsyn till länklängd, samt med och utan hänsyn till länktyp.

I figur 23 och 24 presenteras resultaten från simuleringarna med och utan hänsyn till länklängd för tätortsnätet. Figur 24 visar den grå kurvans relativa avvikelse från den svarta då hänsyn togs till länklängd.



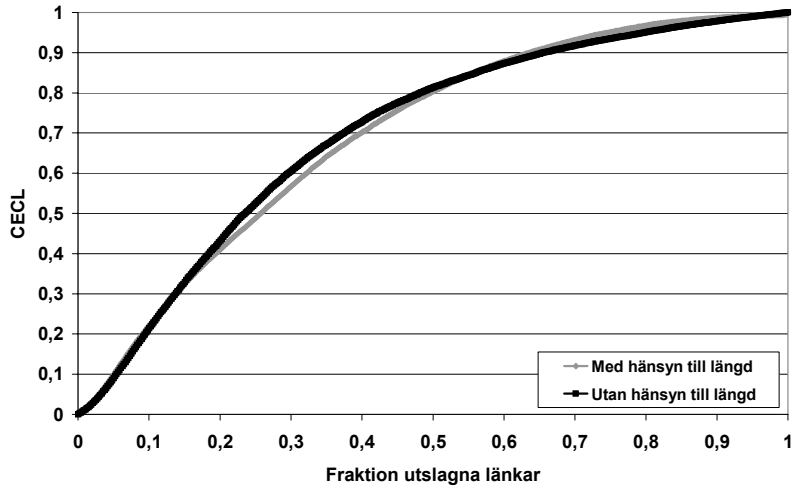
Figur 23 Tätortsnätet: CECL som funktion av fraktion utslagna länkar med och utan hänsyn till längd



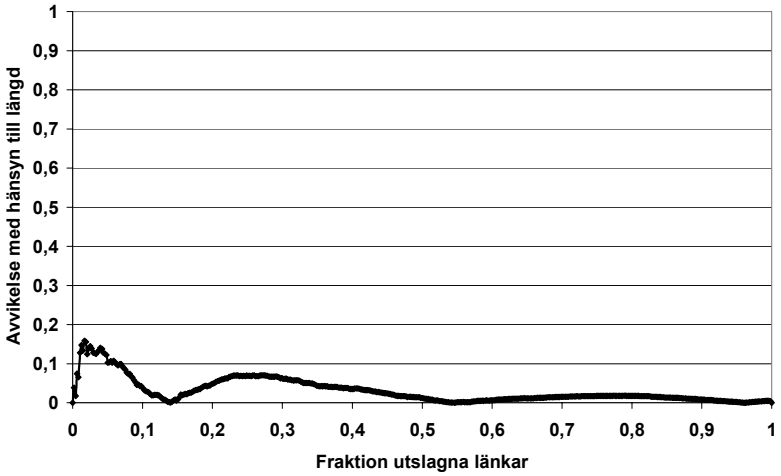
Figur 24 Tätortsnätet: Den relativa absoluta avvikelsen då hänsyn tas till längd

Som figur 23 och 24 visar, minskade konsekvensen av utslagningarna i början på simuleringen när hänsyn till längden togs, vilket tyder på att långa länkar generellt är kopplade till noder med lägre kundekvivalent än korta i tätortsnätet.

Figur 25 och 26 visar resultaten från simuleringarna med och utan hänsyn till länklängd för det blandade nätet. Figur 26 visar avvikelsen då hänsyn togs till länklängd.



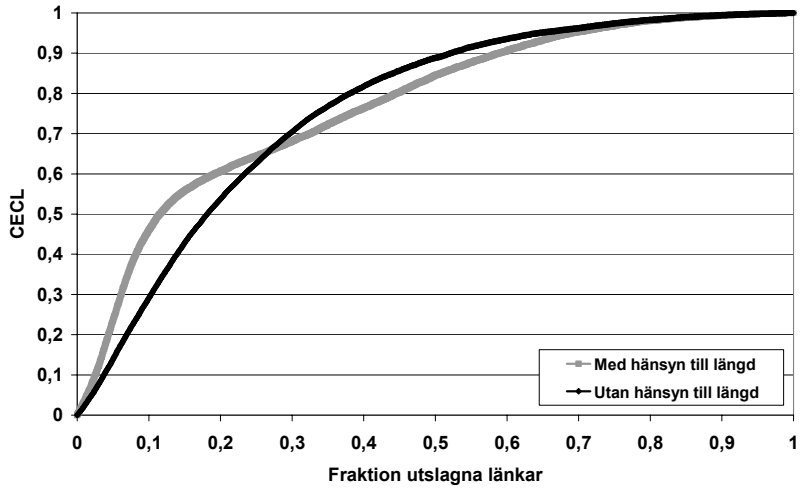
Figur 25 Det blandade nätet: CECL som funktion av fraktion utslagna länkar med och utan hänsyn till längd



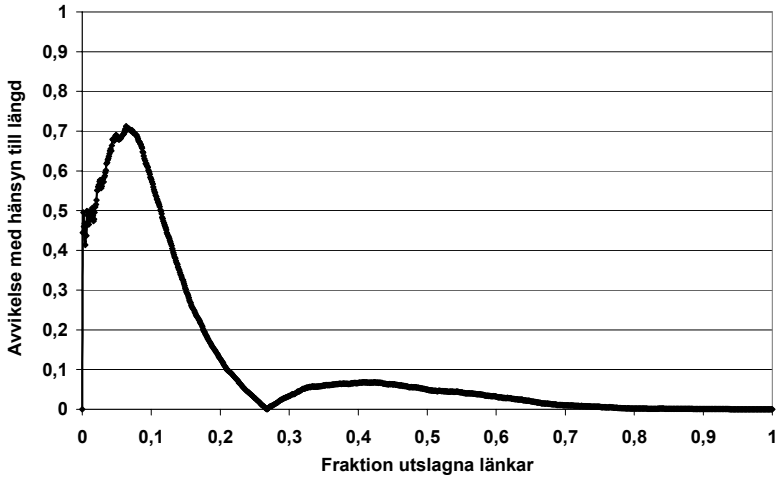
Figur 26 Det blandade nätet: Den relativa absoluta avvikelsen då hänsyn tas till längd

Som figur 25 och 26 visar, blev skillnaden i simuleringsresultaten för det blandade nätet inte så stor då hänsyn togs till länklängd. Detta beror antagligen på att glesbygdsdelen och tätortsdelen av nätet ”tog ut” varandra i simuleringen, i och med att långa ledningar främst förekommer i glesbygd och har mindre kundekvivalent medan korta ledningar främst förekommer i tätort och har större kundekvivalent.

Figur 27 och 28 visar resultaten från simuleringarna med och utan hänsyn till längd för glesbygdsnätet. Figur 28 visar avvikelsen då hänsyn togs till länklängd.



Figur 27 Glesbygdsnätet: CECL som funktion av fraktion utslagna länkar med och utan hänsyn till längd



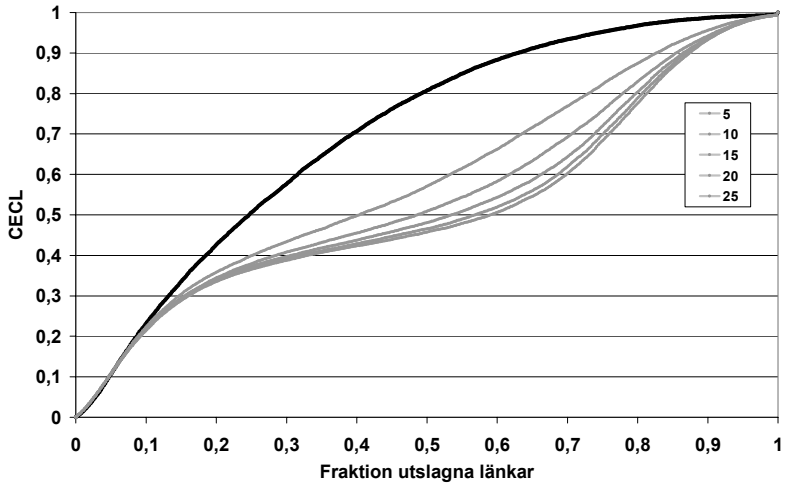
Figur 28 Glesbygdsnätet: Den relativa absoluta avvikelsen då hänsyn tas till längd

Som figur 27 och 28 visar, ökade glesbygdsnätets sårbarhet då hänsyn togs till länklängd i simuleringen. Detta kan härledas till att glesbygdsnätet innefattar både 12 kV- och 24 kV-ledningar. Ledningarna på 24 kV är längre än de på 12 kV, vilket gjorde att 24 kV-ledningarna hade en högre sannolikhet att slås ut i början av simuleringarna. Eftersom 24 kV-ledningarna i de flesta fall är överordnade 12 kV-ledningarna påverkar avbrott på den högre nivån automatiskt lägre nivåer och ger därmed större konsekvenser.

För samtliga nät blev det alltså skillnad i resultaten då hänsyn till länklängd togs. För tätortnätet (figur 24) uppgick den procentuella avvikelsen till maximalt 40 %. För det blandade nätet (figur 26) var denna avvikelse 16 % och för glesbygdsnätet (figur 28) var den maximala avvikelsen 71 %. Skillnaden var störst i början av simuleringarna.

Eftersom länklängden enligt analysen har betydelse för sårbarheten enligt CECL blir slutsatsen att hänsyn bör tas till längden vid modelleringen av näten.

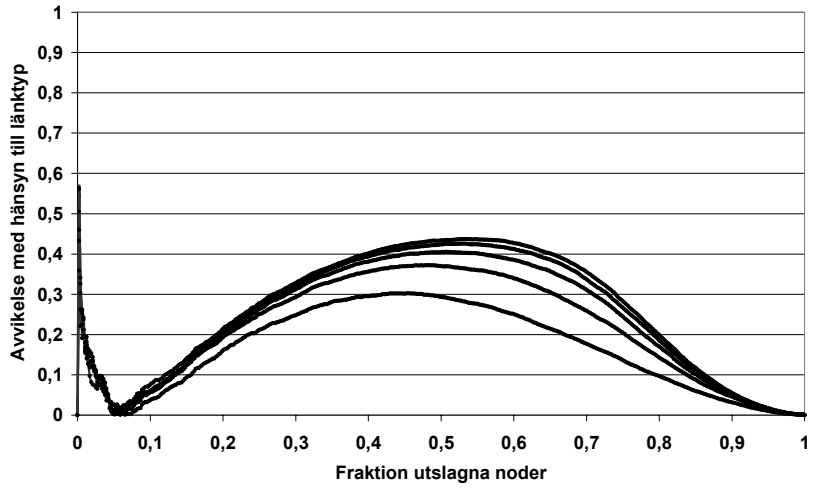
I figur 29 och 30 presenteras resultaten från simuleringarna med och utan hänsyn till länktyp. För denna analys simulerades endast det blandade nätet. Figur 29 visar CECL som funktion av fraktion utslagna länkar i en slumpmässig utslagning. Simuleringarna bestod av ett fall där hänsyn inte togs till länktyp, och fem där hänsyn togs till länktyp. I de fem fall där hänsyn togs till länktyp antogs utslagning av luftledning ha 5-25 gånger högre sannolikhet än jordkabel.



Figur 29 CECL som funktion av fraktion utslagna länkar vid slumpmässig utslagning av länkar i det blandade nätet, med och utan hänsyn till länktyp. En simulering utan (svart) och fem med (grå) hänsyn till länktyp. Simuleringarna med hänsyn till länktyp kommer i den ordning som förklaringsrutan visar.

Som figur 29 visar, ökar avvikelsen mellan fallet utan hänsyn till länktyp och de med hänsyn till länktyp ju mer skillnaden i avbrottsfrekvens mellan luftledning och jordkabel ökar. Precis i början ökade sårbarheten enligt CECL då hänsyn till länktyp togs men sedan blev den mindre. Det faktum att sårbarheten i nätet minskar då hänsyn tas till länktyp pekar på att värdefulla noder i högre grad är kopplade till jordkabel, vilket bidrar till att dessa noder har mindre sannolikhet att slås ut. Eftersom analysen är gjord på det blandade nätet är det sannolikt så att de mest värdefulla noderna finns i tätortsdelen, som till största delen består av jordkabel.

Figur 30 visar den relativa avvikelsen då hänsyn tas till länktyp.



Figur 30 Den relativa absoluta avvikelsen då hänsyn tas till länktyp

Som figur 30 visar uppgick avvikelsen som mest till 56 % för den simulering där luftledning antogs vara 25 gånger mer sårbar än jordkabel.

Resultatet visar tydligt att länktyp har betydelse för resultatet av sårbarhetsanalysen. Därför bör hänsyn till länktyp tas vid modelleringen av näten. Eftersom generaliserbar information om proportionen mellan avbrott i jordkabel och luftledning saknades måste ett antagande om detta göras. I en tidigare rapport på ett nät som på många sätt liknade det blandade nätet användes en frekvens för fel i luftledning som var 10 gånger den för jordkabel (Wallnerström, 2005). Efter noggrannare undersökning framgick dock att denna i realiteten sannolikt var högre (Wallnerström, personlig kommunikation, 2006). Därför valdes i fortsatta analyser att låta avbrott i luftledning ha 15 gånger högre sannolikhet än i jordkabel.

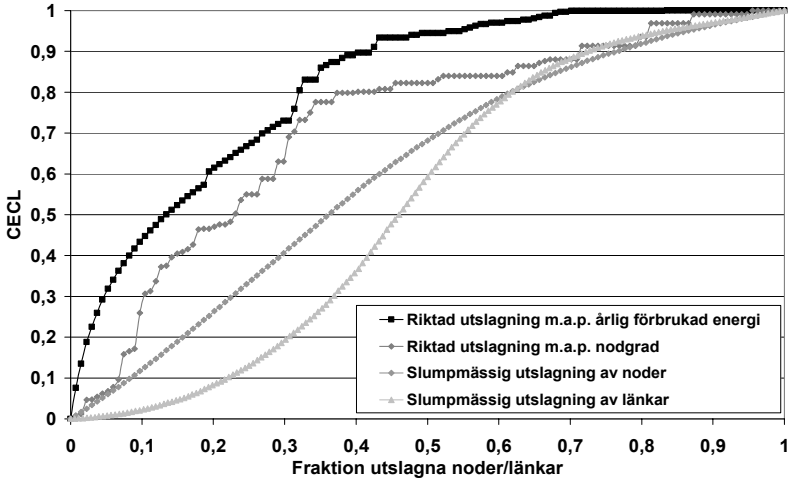
7.5.2 Sårbarhetsanalys

CECL används för att beräkna hur snabbt nätet bryts ner vid utslagning av noder eller länkar efter ett visst scenario, och få ett värde på konsekvensen för varje ytterligare avlägsnad nod eller länk. De fyra initiala påfrestningar som simulerades var riktad utslagning med avseende på längd, riktad utslagning med avseende på grad, slumpmässig utslagning av noder och slumpmässig utslagning av länkar.

I utslagningen av länkar togs hänsyn till attributet länklängd för samtliga nät, och till attributet länktyp för det blandade nätet. Detta gjordes med bakgrund av resultaten från kapitel 7.5.1, ”Utveckling av modellen”.

SVC beräknas som arean under CECL-kurvan. SVC redovisas för samtliga riskscenarier men även för de första 10 % utslagna komponenterna eftersom det är dessa scenarier som är mest troliga att inträffa i verkligheten, se kapitel 7.6.3, ”Riskanalys”. Ju närmre noll SVC är, desto långsammare bryts nätet ner och desto mer robust är det enligt SVC.

Figur 31 visar resultaten av sårbarhetsanalysen av tätortsnätet för de fyra initiala påfrestningarna. Tabell 4 visar SVC för hela analysen och för de första 10 %.

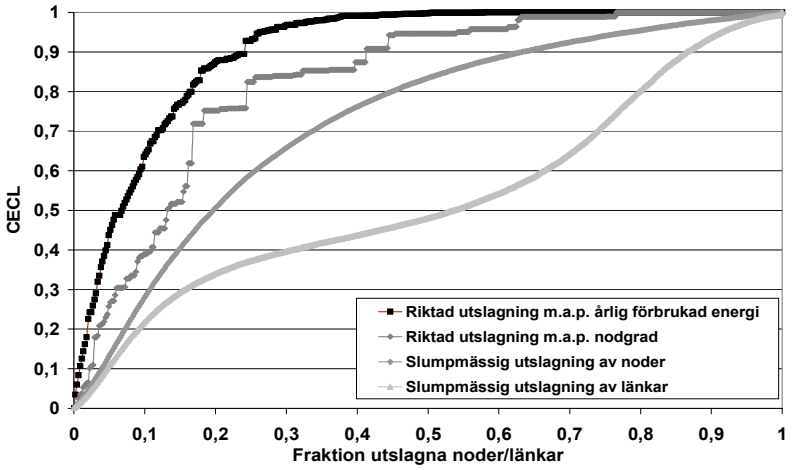


Figur 31 Tätortsnätet utsatt för utsatt för fyra olika initiala påfrestningar

	Riktad utslagning noder m.a.p. effekt	Riktad utslagning noder m.a.p. nodgrad	Slumpmässig utslagning noder	Slumpmässig utslagning länkar
SVC	0,822	0,722	0,610	0,535
SVC (10 %)	0,305	0,109	0,066	0,010

Tabell 4 SVC och SVC 10 % för tätortsnätet utsatt för fyra olika initiala påfrestningar

Figur 32 visar resultaten av sårbarhetsanalysen av det blandade nätet för de fyra initiala påfrestningarna. Tabell 5 visar SVC för hela analysen och för de första 10 %.

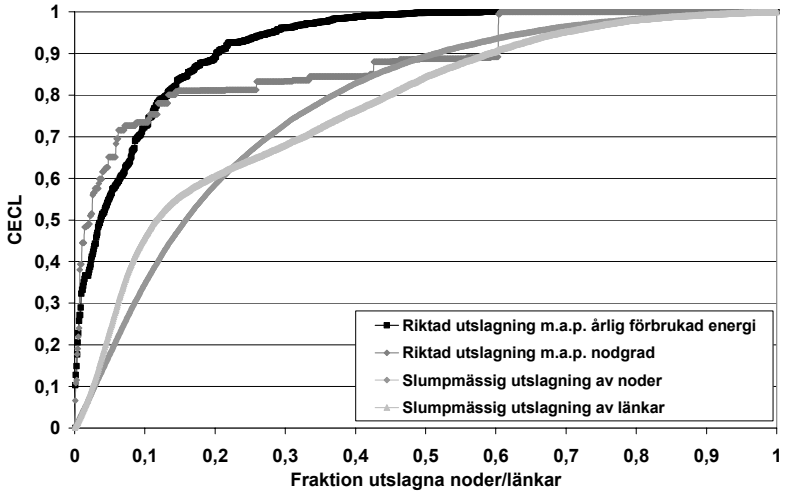


Figur 32 Det blandade nätet utsatt för fyra olika initiala påfrestningar

	Riktad utslagning noder m.a.p. effekt	Riktad utslagning noder m.a.p. nodgrad	Slumpmässig utslagning noder	Slumpmässig utslagning länkar
SVC	0,906	0,831	0,731	0,532
SVC (10 %)	0,397	0,230	0,140	0,111

Tabell 5 SVC och SVC 10 % för det blandade nätet utsatt för fyra olika initiala påfrestningar

Figur 33 visar resultaten av sårbarhetsanalysen av glesbygdsnätet för de fyra initiala påfrestningarna. Tabell 6 visar SVC för hela analysen och för de första 10 %.



Figur 33 Glesbygdsnätet utsatt för utsatt för fyra olika initiala påfrestningar

	Riktad utslagning noder m.a.p. effekt	Riktad utslagning noder m.a.p. nodgrad	Slumpmässig utslagning noder	Slumpmässig utslagning länkar
SVC	0,925	0,882	0,779	0,771
SVC (10 %)	0,522	0,605	0,178	0,236

Tabell 6 SVC och SVC 10 % för glesbygdsnätet utsatt för fyra olika initiala påfrestningar

Som figur 31, 32 och 33 visar är resultatet för de tre näten ganska likt i fråga om rangordning av de fyra påfrestningarna. Att riktad utslagning av noder med avseende på årlig förbrukad energi är den mest skadliga initiala påfrestningen var väntat, eftersom årlig förbrukad energi är det värde som även valdes som kundekvivalent.

Även utslagning av noder med avseende på grad visade sig i simuleringarna vara en allvarlig påfrestning. Detta stämmer bra överens med vad som visades i tidigare studier, att nätverk där nodernas grad följer en power law-fördelning är sårbara för riktade attacker mot de noder som utgör nav. Framför allt glesbygdsnätet bröts snabbt ner till följd av denna påfrestning. I början var den faktiskt mer skadlig än riktad utslagning med avseende på årlig förbrukad energi. Detta beror antagligen på att glesbygdsnätet har bättre passning till power law-fördelningen än de andra två näten, se kapitel 7.2 ”Beskrivning av valda nät”. I samtliga nät har inmatningsnoderna högst grad av alla noder. I denna analys slogs inmatningsnoder inte ut men om detta skett så hade antagligen näten varit ännu mer sårbara för riktad utslagning av noder med avseende på grad.

Påfrestningen slumpmässig utslagning av noder bröt i simuleringen ner näten snabbare än slumpmässig utslagning av länkar i samtliga fall utom precis i början för glesbygdsnätet. Detta beror troligtvis på att länkarna, till skillnad från noderna, inte har någon kundekvivalent. Därför gav utslagning av länkar i många fall ingen direkt, utan endast indirekt konsekvens. Att glesbygdsnätet var mer sårbart för utslagning av länkar än av

noder i början av utslagningarna kan tyda på att glesbygdsnätet i högre grad har noder med hög kundekvivalent kopplade till långa länkar.

Sårbarhetsanalysen bekräftar det som antogs i kapitel 7.2, ”Beskrivning av valda nät”. Glesbygdsnätet visade sig vara mest sårbart av de tre näten för samtliga påfrestningar. Därefter kom det blandade nätet och sist tätortsnätet. Att glesbygdsnätet var mest sårbart beror på dess radiella struktur, att det är så utspritt och att det till största delen består av luftledning.

7.5.3 Riskanalys

För att göra en riskanalys krävs vetskap om sannolikhet eller frekvens för de riskscenarier som riskscenariorymden delats upp i. Utifrån tillgänglig data valdes i analysen att dela upp riskscenariorymden i riskscenarier utifrån antal samtidiga avbrott. Sannolikheten för riskscenarierna är beräknad utifrån det totala antal minuter som varje scenario pågår, och är alltså inte baserad på frekvensen av varje riskscenario. Sannolikheten redovisas i tabell 7.

Riskscenario (antal samtidiga avbrott)	Total tid (minuter)	Sannolikhet (total tid scenario/ total tid samtliga scenarier)
1	159 878	11,08%
2	25 661	1,78%
3	2 402	0,17%
4	1 543	0,11%
5	474	0,03%
6	856	0,06%
7	238	0,02%
8	317	0,02%
9	430	0,03%
10	1 636	0,11%
11	218	0,02%
12	388	0,03%
13	111	0,01%
14	317	0,02%
15	1 246	0,09%
16	464	0,03%
17	381	0,03%
18	182	0,01%
19	169	0,01%

Tabell 7 Sannolikhet för varje riskscenario enligt statistik från DARWIN där riskscenarierna är antal samtidiga avbrott (Ohlson, 2006)

Som tabell 7 visar, delas riskscenariorymden upp i kategorierna 1 - 19 samtidiga avbrott. Detta görs eftersom 19 är det maximala antalet samtidiga avbrott som kan identifieras, enligt den driftstörningsstatistik som finns tillgänglig från DARWIN. Som tabellen visar minskar sannolikheten ju fler samtidiga avbrott som avses, vilket var väntat. Enligt statistiken var nätet fritt från avbrott 86,35 % av tiden.

För ett radiellt nät kan ett avbrott leda till stora konsekvenser om det sker så att en stor del, eller värdefulla delar av nätet kopplas bort från inmatningspunkten. Ett maskat nät kan i de flesta fall hantera ett fel åt gången, eftersom det har egenskapen att matningen vid ett avbrott kan omdirigeras till en annan väg. 97,43 % av tiden skedde enligt statistiken inga eller högst ett avbrott i nätet.

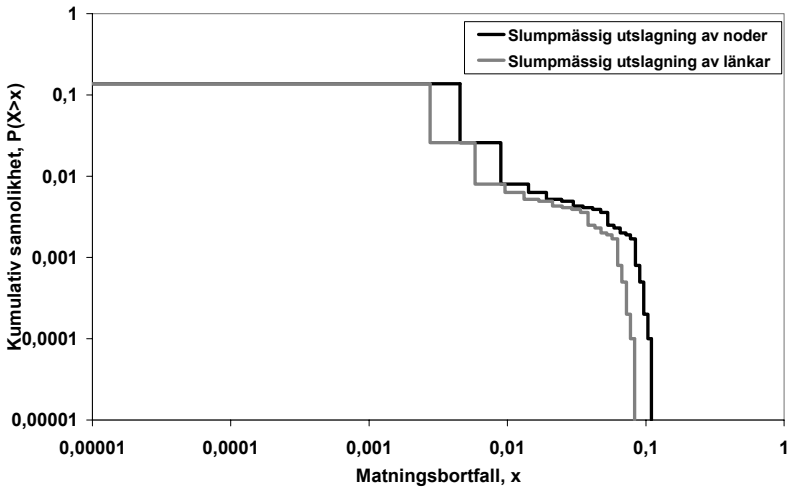
Två eller fler avbrott är mer kritiska för maskade nät eftersom de kan leda till att delar av nätet kopplas bort från samtliga inmatningspunkter. Två samtidiga avbrott förekom enligt statistiken 1,78 % av tiden medan övriga samtidiga avbrott endast stod för 0,79 % av tiden.

Konsekvensen av riskscenarierna enligt den konsekvensrymd som erhölls i de slumpmässiga utslagningarna av noder respektive länkar i sårbarhetsanalysen (se kapitel 7.5.2 ”Sårbarhetsanalys”) redovisas i tabell 8. Alla konsekvenser är därför medelvärden.

Riskscenario	Konsekvens	
	Slumpmässig utslagning noder	Slumpmässig utslagning länkar
1	0,45%	0,28%
2	0,90%	0,58%
3	1,42%	0,96%
4	1,91%	1,32%
5	2,46%	1,68%
6	2,99%	2,11%
7	3,53%	2,49%
8	4,14%	2,92%
9	4,73%	3,38%
10	5,30%	3,81%
11	5,90%	4,29%
12	6,54%	4,75%
13	7,18%	5,22%
14	7,75%	5,72%
15	8,41%	6,26%
16	9,06%	6,72%
17	9,66%	7,24%
18	10,34%	7,75%
19	10,96%	8,29%

Tabell 8 Konsekvens för varje riskscenario mätt i andel matningsbortfall

Figur 34 visar nätets riskprofil utifrån de beräknade sannolikheterna och konsekvenserna.



Figur 34 Riskprofilkurvor för det blandade nätet med konsekvensrymden av slumpmässig utslagning av noder respektive länkar som konsekvens.

Riskanalysen visar hur risken för ett elnät kan visualiseras för att exempelvis göra jämförelser mellan olika nät. I analysen beräknades sannolikheten för riskscenarierna med hjälp av driftsstörningsstatistik, men denna kan även tas fram genom uppskattning av experter eller på annat lämpligt sätt. Sannolikheten beräknades även utifrån sammanlagd tid för varje riskscenario, vilket var en approximation då information om frekvensen saknades. Konsekvensen erhölls från simuleringarna i sårbarhetsanalysen, och bygger på medelvärdet av konsekvenserna från samtliga simulerade riskscenarier. Även konsekvensen kan tas fram på andra sätt, till exempel från historiska data.

7.5.4 Nätens konstruktion

DC_{order} och DC_{path} är mått på hur väl nätet är designat. De kan ligga mellan -1 och 1. Ju närmre 1 värdet ligger, desto bättre designat är nätet med avseende på att försörja kunder med el. I tabell 9 visas resultaten av DC_{order} för slumpmässig utslagning av noder och länkar. Eftersom DC_{path} utgår från nätets ursprungliga struktur blir måttet detsamma oavsett vilken attackstrategi som avses.

	Slumpmässig utslagning noder			Slumpmässig utslagning länkar med attribut		
	Tätort	Blandat	Glesbygd	Tätort	Blandat	Glesbygd
DCorder	0,270	0,490	0,304	0,268	0,634	0,388
DCpath	0,241	0,353	0,186	0,241	0,353	0,186

Tabell 9 DC_{order} och DC_{path} för slumpmässig utslagning av noder och länkar i de tre näten

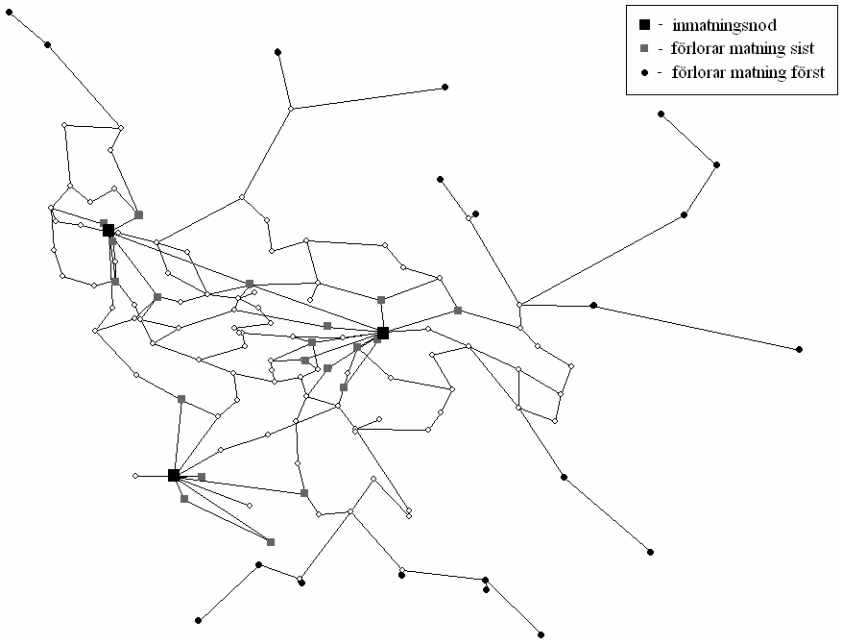
Enligt tabell 9 hade det blandade näten det största värdet på DC_{order}. I detta nät tenderar distributionsnoder med låg kundekvivalent att slås ut tidigare och distributionsnoder med hög kundekvivalent att slås ut senare vid en simulering. Det blandade nätet har även det högsta värdet på DC_{path}, vilket indikerar att distributionsnoder med hög kundekvivalent i högre grad ligger nära inmatningsnoderna än vad de gör i tätorts- och glesbygdsnätet. Att

näten rangordnas olika för DC_{order} och DC_{path} beror troligen på de förenklingar som gjorts i beräkningen av DC_{path}.

DC_{order} och DC_{path} bör ses som komplement till CECL och SVC. Ett högt värde på DC_{order} och DC_{path} är ofta en indikation på att nätet är bättre designat, men inte alltid. DC_{order} kan till exempel bli lika högt oavsett om noder med hög kundekvivalent slås ut tidigt eller sent i simuleringen, så länge de slås ut efter noder med lägre kundekvivalent.

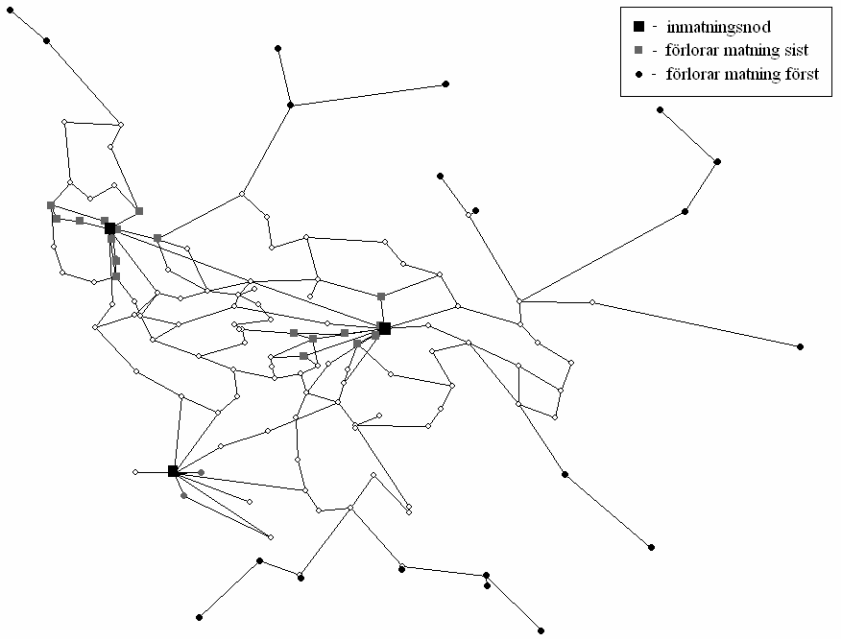
I figur 35-43 visas kartor över de tre näten där de mest och minst sårbara distributionsnoderna vid slumpmässig utslagning av noder respektive länkar, samt de distributionsnoder med längst och kortast avstånd till inmatningsnod, finns markerade. I samtliga figurer kan det i vissa fall se ut som om en nod är omarkerad som borde vara markerad. Detta beror på att noder och länkar i flera fall överlappar varandra så att det kan se ut som om två noder ha en länk mellan sig trots att de inte har det egentligen.

Figur 35, 36 och 37 visar kartor över tätortsnätet. Figur 35 visar de mest och minst sårbara distributionsnoderna vid slumpmässig utslagning av noder.



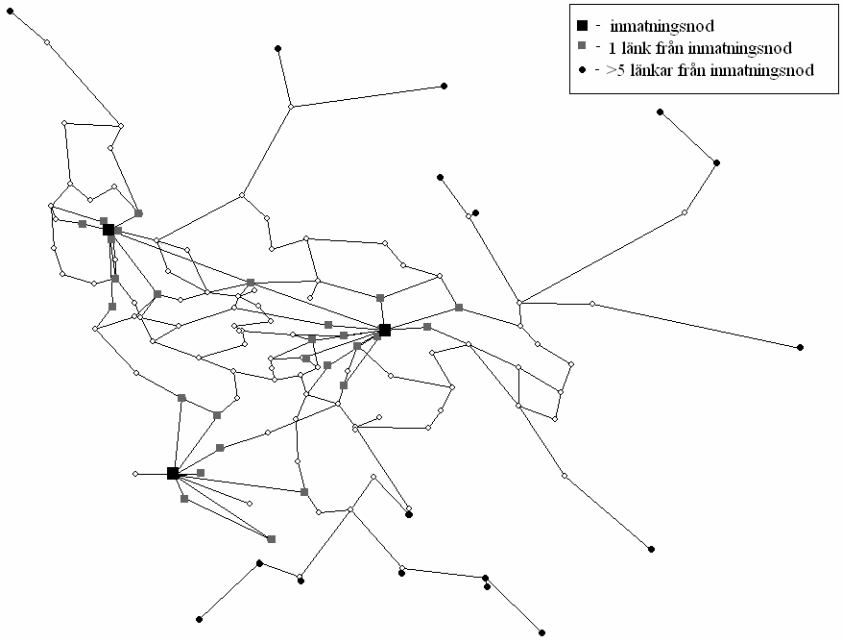
Figur 35 Tätortsnätet där de 20 distributionsnoder som förlorar matning först och sist vid slumpmässig utslagning av noder är markerade.

Figur 36 visar de mest och minst sårbara distributionsnoderna i tätortsnätet vid slumpmässig utslagning av länkar



Figur 36 Tätortsnätet där de 20 distributionsnoder som förlorar matning först och sist vid slumpmässig utslagning av länkar är markerade.

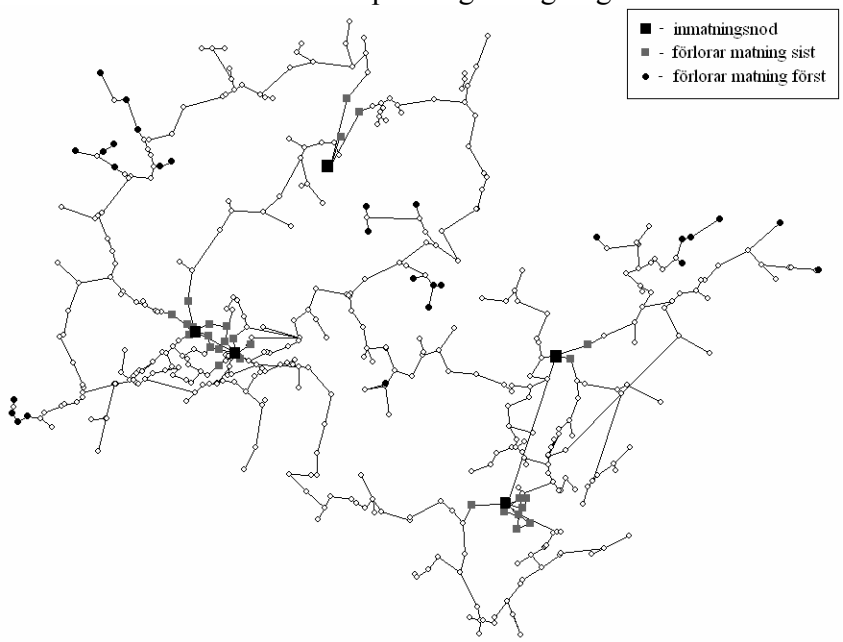
Figur 37 visar de distributionsnoder med längst och kortast avstånd till inmatningsnod i tätortsnätet.



Figur 37 Tätortsnätet med distributionsnoder som har ett avstånd från inmatningsnod på >5 och de med ett avstånd på 1 är markerade.

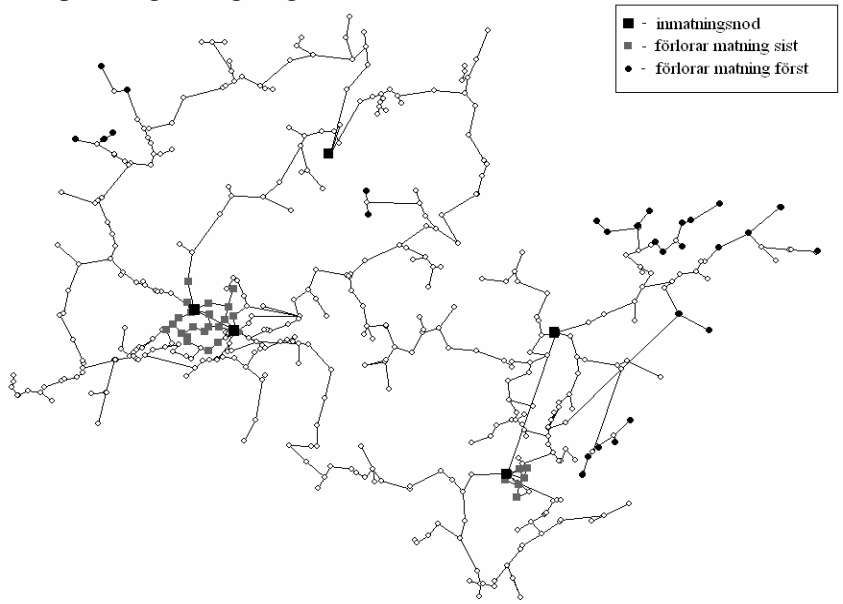
I tätortsnätet sammanfaller nästan samtliga mest och minst sårbara distributionsnoder, både enligt simuleringarna och enligt avstånd till inmatningsnod. Som figur 35, 36 och 37 visar ligger alla de mest sårbara punkterna i tätortsnätet i nätets periferi, i de få delar som har radiell struktur.

Figur 38, 39 och 40 visar det blandade nätet. Figur 38 visar de mest och minst sårbara distributionsnoderna vid slumpmässig utslagning av noder.



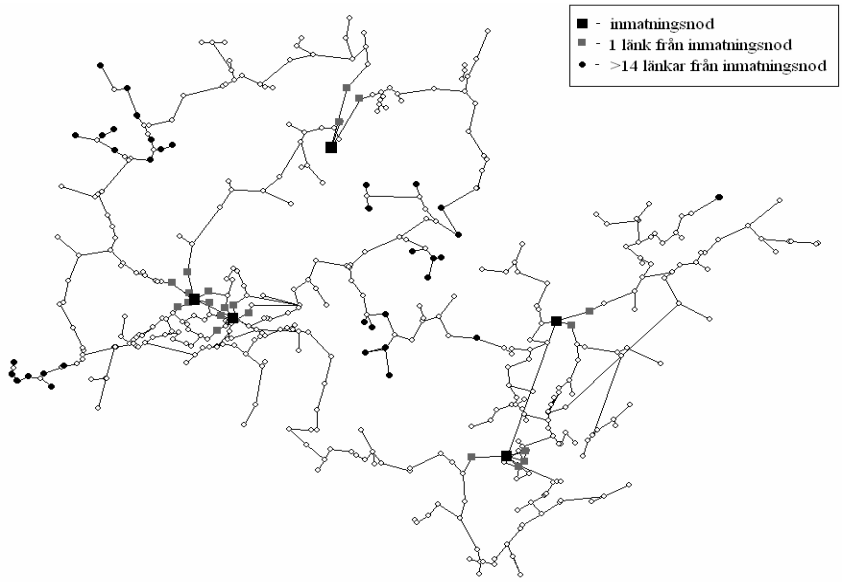
Figur 38 Det blandade nätet där de 10 % av distributionsnoderna som förlorar matning först och sist vid slumpmässig utslagning av noder är markerade.

Figur 39 visar de mest och minst sårbara distributionsnoderna i det blandade nätet vid slumpmässig utslagning av länkar.



Figur 39 Det blandade nätet där de 10 % av distributionsnoderna som förlorar matning först och sist vid slumpmässig utslagning av länkar är markerade.

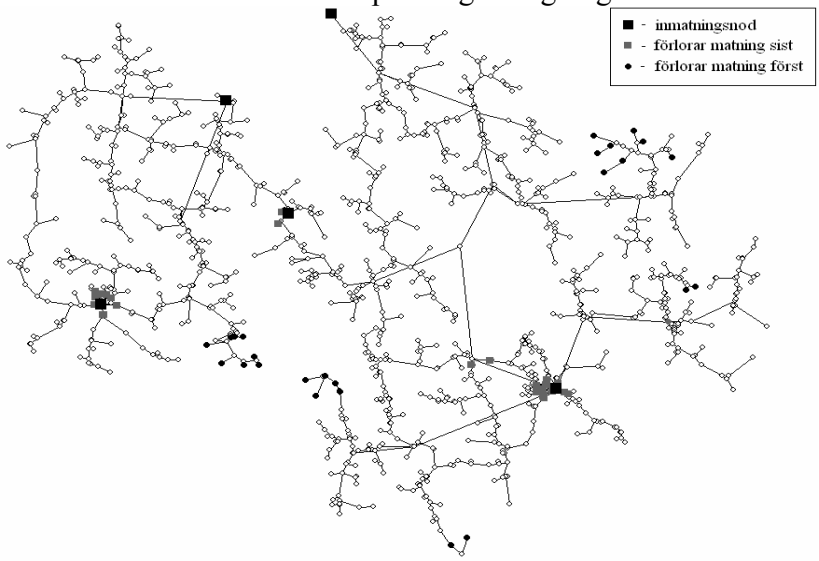
Figur 40 visar de distributionsnoder med längst och kortast avstånd till inmatningsnod i tätortsnätet.



Figur 40 Det blandade nätet där de distributionsnoder som har ett avstånd från inmatningsnod på >14 och de med ett avstånd på 1 är markerade.

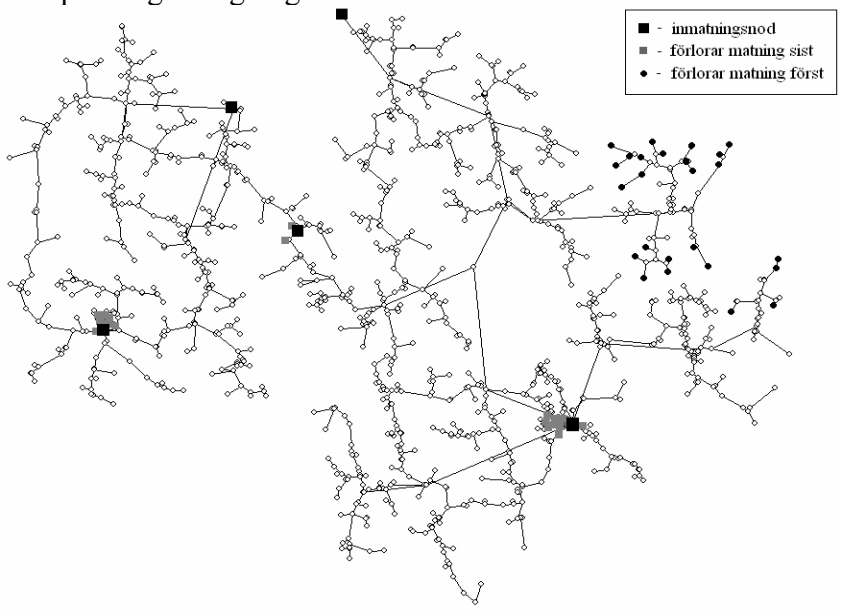
I det blandade nätet blev det en viss skillnad mellan de olika figurerna. Detta beror troligtvis på att hänsyn tagits till länktyp och länklängd i den simulering som illustreras i figur 39, slumpmässig utslagning av länkar. I de två andra, figur 38 och 40, har inte hänsyn tagits till länktyp och alla länkar har antagits ha längden ett. Därför är dessa två mer lika varandra.

Figur 41, 42 och 43 visar glesbygdsnätet. Figur 40 visar de mest och minst sårbara distributionsnoderna vid slumpmässig utslagning av noder.



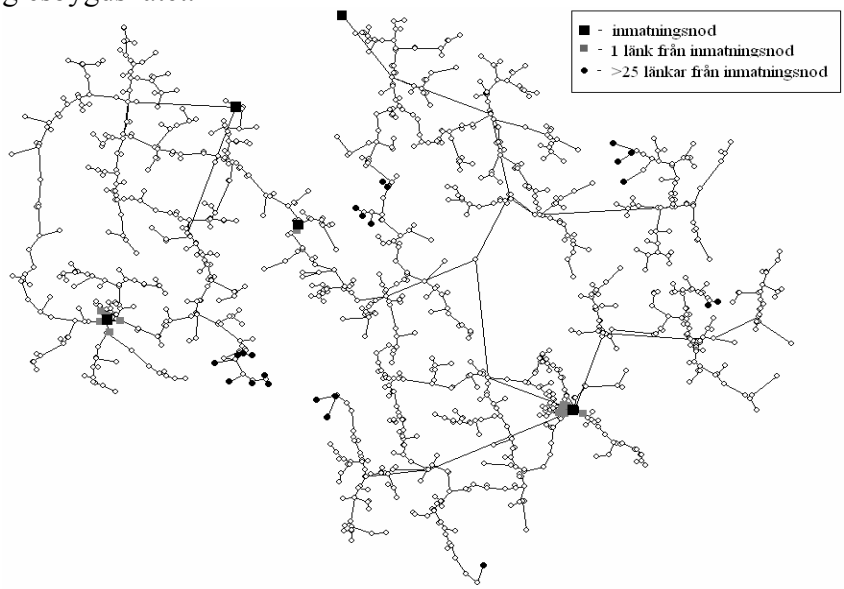
Figur 41 Glesbygdsnätet där de 25 distributionsnoder som förlorar matning först och sist vid slumpmässig utslagning av noder är markerade.

Figur 42 visar de mest och minst sårbara distributionsnoderna i glesbygdsnätet vid slumpmässig utslagning av länkar.



Figur 42 Glesbygdsnätet där de 25 distributionsnoder som förlorar matning först och sist vid slumpmässig utslagning av länkar är markerade.

Figur 43 visar de distributionsnoder med längst och kortast avstånd till inmatningsnod i glesbygdsnätet.



Figur 43 Glesbygdsnätet där de distributionsnoder som har ett avstånd från inmatningsnod på >25 och de med ett avstånd på 1 är markerade.

I simuleringen med slumpmässig utslagning av länkar, figur 42, har hänsyn tagits till länklängd. För glesbygdsnätet hade länklängden stor betydelse för sårbarheten, se kapitel 7.5.1, ”Utveckling av modellen”, och det är orsaken till att kartorna över glesbygdsnätet ser något olika ut.

7.5.5 Kritiska komponenter

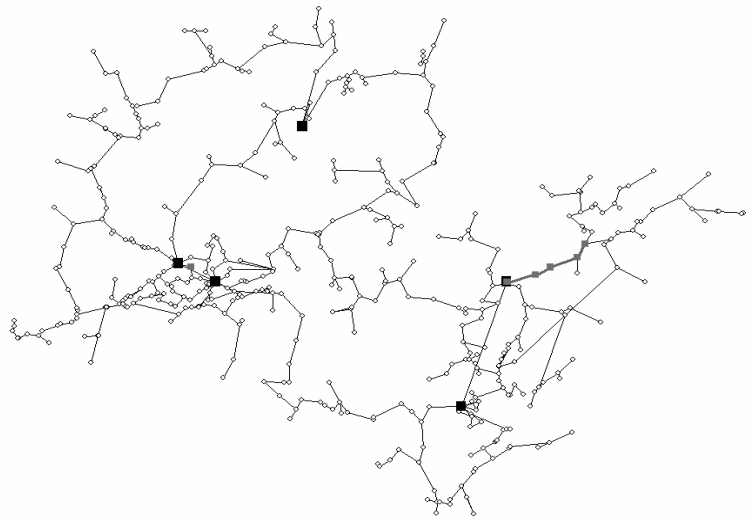
Som tidigare nämnts, är ett och två samtidiga avbrott enligt driftstörningsstatistiken de vanligaste riskscenarierna. Därför finns det en anledning till att studera dessa scenarier mer detaljerat. Analysen av kritiska komponenter gjordes, på grund av tidsbegränsning, endast för det blandade nätet.

De 10 mest kritiska enskilda komponenterna, det vill säga de som enligt simuleringen i ACC gav störst konsekvens då de slogs ut, redovisas i tabell 10.

Komponent	Konsekvens
91	3,31%
245	3,27%
295	3,27%
716	3,27%
296	3,21%
767	3,21%
297	3,17%
768	3,17%
299	3,07%
770	3,07%

Tabell 10 De 10 mest kritiska komponenterna enligt ACC

Enligt tabell 10 orsakade en utslagen komponent maximalt 3,31 % matningsbortfall. Den komponent som toppar listan är samma som slogs ut först i den riktade utslagningen med avseende på årlig uttagen energi i sårbarhetsanalysen. Anledningen till att konsekvensen skiljer sig något åt mellan analyserna[11] är att kundekvivalenten här definieras som toppeffekt under ett år, baserat på velanderkoeffecienten istället för den årliga förbrukade energin. Figur 44 visar de 10 mest kritiska komponenterna i det blandade nätet.



Figur 44 Det blandade nätet där de 10 mest kritiska komponenterna är gråa och inmatningsnoderna är svarta.

[11] 3,43 % i sårbarhetsanalysen och 3,31 % i detta kapitel

Det matningsbortfall som utslagning av den mest kritiska komponenten orsakade är endast den direkta konsekvensen av den utslagna noden. Som figur 44 visar, ligger övriga nio komponenterna på rad längs en väg i den radiella delen av nätet. En utslagning av någon av dessa nio komponenter ledde i simuleringen till att en stor del av nätet kopplades bort eftersom inga alternativa matningsmöjligheter fanns. Det faktum att de ligger på ungefär samma plats är orsaken till att de nio komponenterna gav ungefär samma konsekvens vid utslagning.

Kombinationer av fel kan delas upp i sådana med och utan synergi. Kombinationer utan synergi är i många fall ganska enkla att förutse utan simulering, särskilt för någon som känner till nätet väl. Kombinationer med synergi kan dock vara svårare att upptäcka.

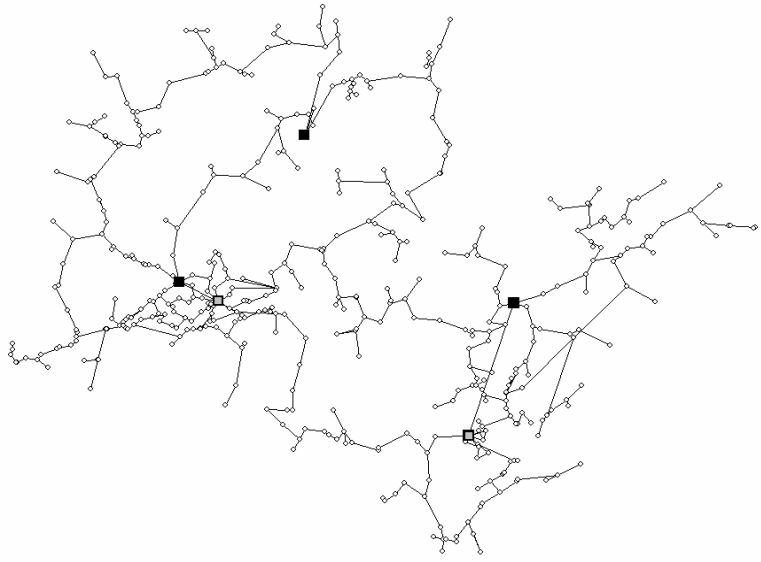
För två utslagna komponenter undersöktes och rangordnades konsekvenserna med och utan synergi i en simulering. De 20 mest kritiska kombinationerna med synergi redovisas i tabell 11. De komponenter markerade i fetstil är inmatningsnoder.

Komponent 1	Komponent 2	Konsekvens	Synergikonsekvens	Synergi
92	**366**	34,54%	34,54%	100%
1	**92**	16,54%	14,83%	90%
92	103	10,05%	8,99%	89%
92	458	10,05%	10,05%	100%
92	102	8,99%	7,61%	85%
92	573	8,99%	8,99%	100%
81	119	8,06%	3,88%	48%
1	119	7,49%	3,31%	44%
245	293	6,58%	3,10%	47%
245	294	6,58%	3,31%	50%
245	377	6,58%	3,31%	50%
245	765	6,58%	3,31%	50%
245	766	6,58%	3,31%	50%
95	102	6,50%	5,12%	79%
98	102	6,50%	3,82%	59%
102	565	6,50%	5,12%	79%
197	**337**	6,47%	6,47%	100%
197	345	6,47%	6,41%	99%
197	809	6,47%	6,47%	100%
198	**337**	6,47%	6,47%	100%

Tabell 11 De 20 mest kritiska komponentparen med synergi. Komponenter i fetstil är inmatningsnoder.

Den kolumn i tabell 11 som heter konsekvens är den totala konsekvensen av utslagningen av komponentparet. Synergikonsekvens är den totala synergikonsekvensen av utslagningen. Synergi är den del av den totala konsekvensen som kan härledas till synergikonsekvens. Det komponentpar som ligger överst i tabell 10 visade sig ge upphov till hela 34 % matningsbortfall. Vidare kan ses att denna konsekvens endast uppstår då dessa två komponenter fallerar samtidig, det vill säga 100% synergi. Därefter sjunker konsekvenserna ganska snabbt till lägre nivåer.

Inmatningsnoder finns med ganska frekvent bland de 20 mest kritiska komponentparen. Detta beror på att inmatningsnoderna har hög nodgrad och därmed utgör viktiga nav i nätverket. Figur 45 visar det mest kritiska komponentparet i det blandade nätet.



Figur 45 Det blandade nätet där det mest kritiska komponentparet är gråa och inmatningsnoder är svarta.

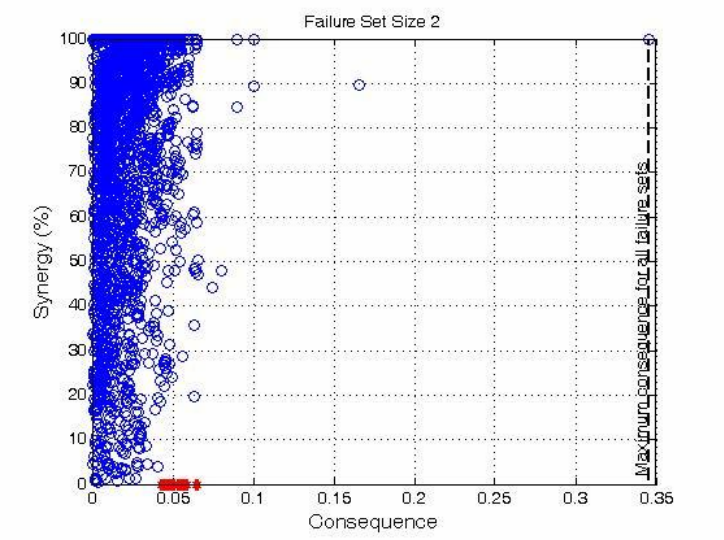
De 20 mest kritiska kombinationerna utan synergi redovisas i tabell 12. Komponenterna markerade i fetstil är inmatningsnoder.

Komponent 1	Komponent 2	Konsekvens
91	**245**	6,58%
91	295	6,58%
91	716	6,58%
91	296	6,51%
91	767	6,51%
91	297	6,48%
91	768	6,48%
91	299	6,38%
91	770	6,38%
91	140	5,96%
91	154	5,96%
91	155	5,96%
91	612	5,96%
91	624	5,96%
91	156	5,92%
91	625	5,92%
140	**245**	5,92%
140	295	5,92%
140	716	5,92%
154	245	5,92%

Tabell 12 De 20 mest kritiska komponentparen utan synergi. Komponenter i fetstil är inmatningsnoder.

De som toppar denna lista är, som väntat, kombinationer av de 10 mest kritiska enskilda komponenterna som listades i tabell 9. Dessa kombinationer orsakade i simuleringen betydligt lägre konsekvenser än de kombinationer som innehåller synergi.

För att på ett tydligt sätt visualisera konsekvenserna av de mest kritiska komponentparen, genererades även med hjälp av ACC ett spridningsdiagram innehållande samtliga komponentpar med synergi och de 1000 mest kritiska komponentparen utan synergi. Se figur 46.



Figur 46 Konsekvens och synergi för samtliga komponentpar med synergi (blå) och de 1000 mest kritiska utan synergi (röda).

I figur 46 återfinns synergin på y-axeln och den totala konsekvensen på x-axeln. De blå punkterna representerar komponentpar med synergi och de röda punkterna representerar komponentpar utan synergi.

7.5.6 Analysmetodens koppling till lagen

Baserat på rapportens syfte valdes de delar av analysresultatet som kan användas för att uppfylla lagkraven.

Den risk- och sårbarhetsanalys som gjordes i analysen kan användas för att klassificera nät ur risk- och sårbarhetssynpunkt. De grafer som sammanställdes visar överskådligt analysens resultat för en viss påfrestning eller en uppsättning riskscenarier. Även SVC som beräknades i sårbarhetsanalysen kan användas för att klassificera nät. Det som krävs för att kunna göra en sådan klassificering är att en definition görs angående vad som är ett ”bra” respektive ”dåligt” värde på risken eller sårbarheten. Detta kan till exempel göras med en stor mängd analyser av olika nät, eller genom att utnyttja experter.

Den analys där kritiska komponenter och komponentpar togs fram med hjälp av ACC borde också vara intressant ur risksynpunkt. En sådan analys skulle kunna utformas så att de mest kritiska komponenterna, exempelvis de vars konsekvens i analysen överstiger 5 %, identifieras varefter sannolikheten eller frekvensen för utslagning av dessa tas fram

med hjälp av antingen experter eller statistik. Med hjälp av ACC kan dessutom beredskapen vid ett avbrott ökas. Vetskapen om vilka komponenter som tillsammans bildar en kritisk kombination kan hjälpa till vid beslut om vilka åtgärder som ska vidtas vid ett avbrott. Om två komponenter tillsammans utgör en kritisk kombination kan det vara lämpligt att, om den ena slås ut, snabbt säkerställa att tillräckliga åtgärder vidtas för att inte den andra också ska slås ut och därmed orsaka ett stort avbrott.

I de nya tilläggen i lagen finns även ett krav på att en åtgärdsplan ska lämnas in. Detta krav tolkas i rapporten som en skriftlig redogörelse för vilka områden som i risk- och sårbarhetsanalysen identifierats vara i behov av förstärkt skydd.

För att identifiera områden som bör få förstärkt skydd, och som därför bör omnämnas i en åtgärdsplan, kan till exempel kartorna över näten, där sårbara områden finns utmärkta, användas tillsammans med kundekvivalenten. På så sätt kan värdefulla noder som ligger i ett sårbart läge, och därmed bör förses med extra skydd, identifieras. Vidare bör kanske även de mest kritiska komponenterna och komponentparen som identifieras med hjälp av ACC förses med förstärkt skydd om dessa visar sig ha hög sannolikhet för utslagning.

Information till abonnenter skulle kunna utformas med hjälp av kartorna över näten. Sårbara områden skulle, liksom visats i kapitel 6.5.4, ”Robustheten i nätens konstruktion”, kunna markeras med på ett sätt medan robusta områden skulle kunna markeras på ett annat. Ett alternativ om det vore olämpligt att visa hela kartor kunde vara att använda samma data men istället endast tala om för abonnenterna vilken robusthet deras leveranssäkerhet har på någon slags skala.

7.5.7 Modellens och metodens användbarhet

I kapitel 4.1, ”Systembaserat och scenariobaserat angreppssätt”, beskrevs fyra frågeställningar som ansågs vara viktiga att ta hänsyn till vid avgörandet om den modell som används vid risk- och sårbarhetsanalysen är tillräckligt användbar. Den första frågan löd ”Kan samtliga konsekvenser som identifierats som viktiga beskrivas med systemet?” I analysen valdes att använda den så kallade kundekvivalenten som ett mått på konsekvensen av riskscenarierna. Eftersom denna valdes som årlig förbrukad energi, och i den sista analysdelen maximal uttagen effekt, kan samtliga konsekvenser som i rapporten bedömts som viktiga beskrivas med systemet.

Den andra frågan som ställdes var ”Kan samtliga relevanta riskscenarier beskrivas med systemet?” I modelleringen av näten gjordes ett antal förenklingar. Bland annat antogs frånskiljare som slutna och näten avgränsade permanent i vissa punkter där det i realiteten kunde ha varit möjligt att få matning vid behov. Det har även gjorts andra antaganden och förenklingar i modellen. Avgränsningar och förenklingar har dock gjorts med avsikten att samtliga relevanta riskscenarier i så hög grad som möjligt ska kunna beskrivas med systemet.

Den tredje frågan löd ”Finns samtliga relevanta riskscenarier med i riskscenariorymden?” Samtliga relevanta scenarier innebär i en slumpmässig utslagning att samtliga möjliga utslagningsordningar ska ingå in analysen. På grund av den omfattning det skulle

innebära att simulera samtliga möjliga utslagningsordningar valdes istället att simulera varje påfrestning 1000 gånger varefter medelvärdet av simuleringarna beräknades. Detta bedömdes ge en tillräckligt bra approximation av samtliga riskscenarier. I den första riskanalysen valdes riskscenarierna som antal samtidiga avbrott. Omfattningen valdes efter historiska data. Denna bedömdes inte vara helt komplett, och riskanalysen bör därför kompletteras med mer tillförlitlig data om riskanalysen ska anses innehålla alla relevanta riskscenarier. I den mer ingående riskanalysen däremot, där kritiska komponenter och kritiska komponentpar togs fram, gjordes en systematisk genomgång av samtliga riskscenarier som ansågs vara relevanta i analysen. Denna analys kan därmed anses vara komplett.

Den sista frågan var ”Beskriver riskscenarierna verkligheten på ett korrekt sätt?”. Svaret på denna fråga beror på modelleringen av näten, val av initiala påfrestningar i sårbarhetsanalysen, och val av riskscenarier i riskanalysen. För samtliga tre faktorer har val och antaganden gjorts för att analyserna så väl som möjligt ska spegla verkligheten. För att ytterligare öka sannolikheten för detta gjordes dessutom en mer detaljerad analys av de riskscenarier som ansågs mest relevanta. Det finns dock möjlighet att utveckla modelleringen av näten ytterligare, vilket diskuteras vidare i kapitel 8.2, ”Fortsatta studier”.

De simuleringsmetoder som användes i analysen är inte särskilt svåra att använda. Det som tar mest tid i anspråk är själva modelleringen av näten vilket är det som till största delen avgör analysens tillförlitlighet och därför bör göras med eftertanke. I sårbarhetsanalysen illustrerar CECL och SVC på ett tydligt sätt nätets sårbarhet för en viss typ av initial påfrestning. I och med detta ges en möjlighet att jämföra olika nät mot varandra utifrån en specifik påfrestning eller bedöma ett näts robusthet för olika möjliga påfrestningar. En riskanalys kan vara svår att genomföra om inte tillräckligt statistiskt material eller experter finns tillgängliga för att ta fram sannolikhet för riskscenarier. En indikation på vilka riskscenarier som är mest sannolika och som bör analyseras närmre kräver inte lika mycket beslutsunderlag och kan vara ett alternativ då inte tillräckligt med material för att göra en fullständig riskanalys finns tillgängligt.

Av de verktyg som använts för att bedöma nätens konstruktion är kanske de figurer som visualiserar sårbara områden mest intressanta att använda. Dessa visar på ett tydligt och pedagogiskt sätt var sårbara punkter finns till följd av en viss initial påfrestning och i kombination med kundekvivalenten ger de en indikation på vart nätet behöver förstärkt skydd. En analys av kritiska komponenter, slutligen, bedömer nätets sårbarhet på en mer detaljerad nivå i och med att den identifierar de komponenter och komponentpar som nätet är mest sårbart för en utslagning av.

7.6 Resultatets tillförlitlighet

För att visa att åtgärder vidtagits för att öka resultatets tillförlitlighet diskuteras nedan validitet, reliabilitet och objektivitet. Vidare görs en kritisk granskning av källmaterialet.

7.6.1 Validitet, reliabilitet och objektivitet

Validitet anger huruvida eller med vilken grad det som avses mätas verkligen mäts (Ejvegård, 2003). Validiteten hos den modelleringsmetod som använts diskuteras i kapitel 7.5.7, ”Modellens användbarhet”. För att öka validiteten i arbetet fördes i de fall då flera alternativ fanns att tillgå en diskussion kring de olika alternativen och orsaken till varför ett specifikt val gjordes motiverades. Detta gjordes bland annat vid val av robusthetsmått i kapitel 6.4 och val av kundekvivalent i kapitel 6.5. För att göra de risk- och sårbarhetsanalyser som presenterats i rapporten, var vissa antaganden och förenklingar nödvändiga. Därför var det viktigt att försöka se till att resultatet av simuleringen i så hög grad som möjligt speglade de konsekvenser som ett verkligt system skulle ha gett upphov till. För att öka sannolikheten för detta undersöktes i kapitel 7.5.1, ”Utveckling av modellen”, möjligheten att anpassa modellen genom att tillskriva länkarna fler attribut. Troligtvis finns det fler attribut som skulle öka validiteten ytterligare om de togs med men som till följd av tidsbegränsningen inte analyserades.

Reliabilitet anger precisionen i mätningen, det vill säga om resultatet kan förväntas bli detsamma vid en upprepad mätning (Ejvegård, 2003). För att öka reliabiliteten eftersträvades att modellera de tre näten som ingick i analysen så snarlikt som det bara var möjligt. Metoden för modelleringen och de antaganden och begränsningar som gjordes beskrevs noggrant i kapitel 7.3, ”Modellering av näten” och 7.4, ”Metod”, för att studien skulle kunna upprepas. För att öka reliabiliteten hos de analyser där medelvärdet av simuleringar användes gjordes 1000 simuleringar eftersom detta ansågs tillräckligt för att ge tillförlitliga värden.

Objektivitet avser inflytandet av egna värderingar eller andra personers åsikter i arbetet (Ejvegård, 2003). Genom att en diskussion med såväl forskare inom området som verksamma inom elbranschen fördes kontinuerligt under arbetets gång, gavs möjligheten till återkoppling på metodval och dragna slutsatser.

7.6.2 Källgranskning

De vetenskapliga artiklar som källhänvisas till i rapporten hämtades till stor del från databasen ELIN vid Lunds universitetsbibliotek. En del hämtades även via sökmotorer på Internet, men dessa blev i så fall dessförinnan antingen rekommenderade av de forskare vid universitetet som författarna varit i kontakt med, eller hänvisade till i en artikel som författarna tidigare läst. Övrig litteratur bestod av informationsmaterial från aktörer inom elbranschen och från myndigheter, lagboken, samt läroböcker som använts i kurser vid Lunds universitet. Begreppsdefinitioner hämtades från Internetkällor som bedömdes som tillförlitliga.

Indata till de tre näten tillhandahölls dels av forskare vid Lunds tekniska högskola, och dels av Telge nät AB. De data som kom från Telge nät AB sammanställdes specifikt för

denna rapport och kom huvudsakligen från en intern databas på företaget. Vid sammanställning av dessa data upptäcktes en del mindre fel som till den största delen försöktes åtgärdas genom kontakt med Telge nät AB. Det finns dock en möjlighet att samtliga fel inte upptäckts.

Den driftstörningsstatistik som analyserades i rapporten kom från DARWIN, en databas som endast funnits i ett fåtal år. I den statistik som författarna fick tillgång till var i många fall orsaken till avbrottet okänd. Detta visar på brister i rapporteringen av elavbrott. I rapporten användes driftstörningsstatistiken bland annat för att motivera val av vissa metoder. Detta ansågs den vara tillräckligt tillförlitlig för. Statistiken låg även till grund för riskanalysen. Till följd av osäkerheten i indata ansågs att samtliga slutsatser angående nätets risk bör dras med försiktighet och att analysen snarare bör användas som ett exempel på hur risken med hjälp av driftstörningsstatistik och tillgängliga verktyg kan beräknas i ett elnät.

Slutligen bör belysas att för att de data som använts i den empiriska studien ska anses som helt tillförlitliga behöver de samlas in under stabila förhållanden. Det innebär att inga väsentliga förändringar i nätet får ha skett under tiden. Detta kan inte tas för givet i rapporten eftersom förändringar, såväl planerade som oplanerade, ständigt sker i ett elnät.

8 Slutsatser

I detta kapitel kopplas erhållna resultat till rapportens syfte och frågeställningar. Därefter ges förslag på fortsatta studier inom området.

8.1 Resultatets koppling till syftet och frågeställningarna

I de nytillkomna ändringarna i ellagen finns krav på att elnätföretag ska utföra risk- och sårbarhetsanalyser rörande leveranssäkerheten i näten. För att utföra risk- och sårbarhetsanalys av ett elnät krävs ett angreppssätt som inte är alltför tids- och resurskrävande men som ändå täcker in alla relevanta riskscenarier. Det angreppssätt som vanligtvis används för stora system såsom elnät är en scenariobaserad metod. Problemet med denna metod är svårigheten att säkerställa att samtliga relevanta riskscenarier kommer med i analysen. Rapportens syfte är att undersöka om en simuleringsmetod kan användas, till exempel som komplement till en scenariobaserad metod, för att utföra risk- och sårbarhetsanalys av elnät i enlighet med de nya kraven i ellagen.

För att visa detta behövde inledningsvis undersökas hur risk- och sårbarhetsanalys av elnät med hjälp av simuleringsmetoder som bygger på nätverksteori tidigare utförts. De tidigare studierna använde varierande attackstrategier för att simulera påfrestningar på näten. De använde även olika robusthetsmått för att mäta nätens sårbarhet för attackstrategierna. *Alla studier visade dock att en simuleringsmetod som simulerar utvecklingen i nätet givet en initial påfrestning är ett bra verktyg för att göra systematiska risk- och sårbarhetsanalyser av stora och komplexa system. En anledning till detta är att systematiken i metoden ökar sannolikheten att samtliga relevanta riskscenarier, även sådana som inte inträffat tidigare, kommer med i analysen. Simuleringsmetoderna visade sig vara mycket användbar när det gällde att identifiera emergenta riskscenarier, det vill säga scenarier som föranleds av till synes enkla inledande händelser men leder till oväntade konsekvenser till följd av komplexiteten i systemets struktur.*

Det är viktigt att, vid val av simuleringsmetod, ta hänsyn till hur det nätverk som ska analyseras ser ut. För att en simuleringsmetod ska vara lämplig för risk- och sårbarhetsanalys av elnät krävs att de egenskaper som utmärker just denna typ av nätverk tas i beaktande. Därför var det viktigt att utreda vilka dessa egenskaper var och vad som skulle krävas av en simuleringsmetod för att den skulle anses lämplig för att genomföra analyser enligt syftet. *Slutsatsen blev att metoden bör ta hänsyn till antal inmatningsnoder, att distributionsnoderna värderas olika och att det är nätets leveranssäkerhet som bör vara av betydelse i risk- och sårbarhetsanalysen.*

Utifrån dessa krav valdes lämpliga simuleringsmetoder för risk- och sårbarhetsanalysen. I de tidigare studier som gjorts med de valda simuleringsmetoderna användes modeller av nät som utgick från ett topologiskt perspektiv. Detta innebar att ingen hänsyn togs till komponenternas egenskaper. För att utreda möjligheten att öka tillförlitligheten i analysresultaten undersöktes dock som första analys i den empiriska studien möjligheten att utveckla modelleringen. Detta gjordes genom att ta hänsyn till att kablar och ledningar tenderar att ha högre sannolikhet att drabbas av fel ju längre de är, och att luftledningar

tenderar att drabbas av fler fel än jordkabel. *Slutsatsen blev att såväl längd som typ av ledning hade betydelse för resultatet av risk- och sårbarhetsanalysen och därför valdes att ta hänsyn till dessa i fortsatta analyser.*

I efterföljande delar av den empiriska studien undersöktes hur en risk- och sårbarhetsanalys utförd med de valda simuleringmetoderna kan utformas för att uppfylla de nya krav som tillkom i ellagen år 2005. De krav som behandlades i analysen var krav på en risk- och sårbarhetsanalys rörande leveranssäkerheten, krav på upprättande av en åtgärdsplan och krav på information till abonnenter. Analysen utgick ifrån en tolkning av lagkraven som gjordes i rapportens inledande del. *Resultatet blev en samling förslag på hur simuleringsmetoderna kan användas för att utföra analyser som kan användas för att uppfylla de tre kraven i lagen. För att uppfylla det första kravet föreslogs att den risk- och sårbarhetsanalys som utfördes med hjälp av NetCalc, samt den riskanalys som utfördes med hjälp av ACC kunde användas. För åtgärdsplanen föreslogs att de kartor som togs fram samt resultatet från analysen i ACC kunde användas för att motivera förstärkt skydd av vissa områden. Kartorna ansågs slutligen även kunna användas för att informera abonnenterna om leveranssäkerheten i den egna elförsörjningen.*

Vid modellering av verkliga system krävs oundvikligen vissa antaganden och förenklingar. Därför är det viktigt att utreda hur dessa påverkar risk- och sårbarhetsanalysen och om modellen trots dessa förenklingar är användbar. Detta görs genom att klargöra om de simulerade resultaten verkligen speglar de konsekvenser som ett verkligt riskscenario skulle ha gett upphov till. För att undersöka användbarheten hos de modeller som gjorts av näten analyserades dessa utifrån fyra frågeställningar. *Slutsatsen av analysen var att modellens användbarhet delvis beror på användarnas kompetens angående elnät. Detta för att kunna avgöra hur de antaganden och förenklingar som görs påverkar modellen. Modellens användbarhet beror även på tillgången av indata. Dessa påverkar graden av tillförlitlighet i simuleringsresultaten. Eftersom ett elnäts fysiska struktur är ganska enkel att kartlägga och dessutom relativt statisk*[12] *är dock behovet av specifik kompetens mindre vid användandet av en simuleringsmetod, än vid användandet av till exempel en scenariobaserad metod.*

Simuleringsmetoden är inte särskilt tidskrävande förutom i den initiala modelleringen av näten. Resultaten av risk- och sårbarhetsanalyser utförda med metoden möjliggör dessutom överskådliga jämförelser mellan olika riskscenarier i ett nät eller mellan olika nät eftersom dessa ges som funktionskurvor, tabeller och kartor. *Till följd av detta blir slutsatsen att simuleringsmetoder som bygger på nätverksteori är användbara för att göra risk- och sårbarhetsanalyser av elnät i enlighet med lagstiftningen, eventuellt tillsammans med en annan metod som även tar hänsyn till externa skyddsåtgärder. I rapporten har ett möjligt tillvägagångssätt som bedöms uppfylla kraven i ellagen illustrerats.*

[12] Jämfört med till exempel ett socialt nätverk

8.2 Fortsatta studier

I fortsatta studier kan det vara lämpligt att se till möjligheten att utveckla modelleringen av näten ytterligare. Kundekvivalenten bör kunna anpassas bättre för syftet genom att använda en sammanvägning av faktorer som anses vara betydelsefulla. Om tillförlitlig information om felfrekvenser för olika komponenter finns kan utslagningen av alla komponenter, inte bara luftledning och jordkabel, i en fortsatt studie viktas efter dessa. Möjligheten att ta hänsyn till kapacitetsbegränsningar i NetCalc, både hos inmatningsnoder och i komponenter skulle också kunna ses över i en fortsatt studie.

Eftersom en storm var det som till största delen gav upphov till den nya lagstiftningen, vore det intressant om en sådan kunde simuleras i en sårbarhetsanalys. En storm kan sägas ge upphov till så kallade *Common Mode Failures*, då en händelse orsakar flera samtidiga konsekvenser. Detta skulle till exempel kunna simuleras genom att öka sannolikheten för en komponent att slås ut om dess granne blivit utslagen.

Slutligen kan interdependens mellan olika infrastrukturer, till exempel elnätet och telenätet, analyseras i en fortsatt studie. Detta för att inkludera sekundära riskscenarier till följd av en påfrestning på elnätet i analysen. Då konsekvensen mäts i energi eller effekt, som den gjordes i denna rapport, är interdepens inte så intressant men om den till exempel mättes i samhällskostnad skulle den vara desto mer intressant.

9 Referenser

Här redovisas det material som refereras till i rapporten.

9.1 Vetenskapliga artiklar

Albert, R., Albert, I. & Nakarado, G. L. (2004). Structural vulnerability of the North American power grid. *Physical review, 69,* 045104.

Axelrod, R. (1997). Advancing the art of simulation in the social sciences. *Complexity, 3(2),* 16-22.

Barabási, A-L & Albert, R. (1999). Emergence of scaling in random networks. *Science, 286*, 509-512.

Crucitti, P., Latora & Marchiori, M. (2004). A topological analysis of the Italian electric power grid. *Physica A: Statistical Mechanics and its Applications, 338(1-3),* 92-97.

Dilley, M. & Boudreau, T. E. (2001). Coming to terms with vulnerability: a critique of the food security definition. *Food Policy, 26(3),* 229-247.

Holme, P, et al. (2002). Attack vulnerability of complex networks. *Physical review, 65*, 056109.

Holmgren, Å. J. (2006). Using graph models to analyse the vulnerability of electric power networks. *Risk analysis, 26(4),* 1-14.

Johansson, H., Johansson, J. & Jönsson, H. (2006). Analysing Social Vulnerability to Perturbations in Electric Distribution Systems. *Complex Network and Infrastructure Protection*, CNIP06, Rome, 2006.

Kaplan, S. & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis, 1981(1),* 11-27.

Kaplan, S., Halmes, Y. & Garrick, B. J. (2001). Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk, *Society for risk analysis*, *21(5)*, 807-819.

9.2 Rapporter

Barabási, A-L., Albert, R. & Jeong, H. (1999). *Scale-free characteristics of random networks: The topology of the world wide web.* Notre-Dame: University of Notre-Dame.

Hallin, P-O., Nilsson, J. & Olofsson, N. (2004). *Kommunal sårbarhetsanalys* (KBM:s forskningsserie nr 3). Stockholm: Krisberedskapsmyndigheten.

Holme, P. (2004). *Form and function of complex networks*. Umeå: Umeå Universitet: Department of Physics.

Johansson, H., Johansson, J. & Jönsson, H. (2007). *Identifying critical components in electrical power systems: a network analytic approach.* Lund: Lunds tekniska högskola.

Krisberedskapsmyndigheten (2006). *Risk- och sårbarhetsanalyser. Vägledning för kommuner och landsting.* (KBM:s utbildningsserie 2006:2) Stockholm: Krisberedskapsmyndigheten.

Lövgren, K. et al. (2004). *Landsbygdens eldistribution –en livsviktig infrastruktur.* Stockholm: Kungliga Ingenjörsvetenskapsakademin.

Newman, M. E. J. (2003) *The structure and function of complex networks*. Ann Arbor: University of Michigan, Department of Physics & Santa Fe: Santa Fe Institute.

Statens energimyndighet (2003). *HEL-projektet, Inriktning och ambitioner för elföretagens säkerhet och beredskap*. Stockholm: Statens Energimyndighet.

Svensk Energi (2004). *DARWIN – driftstörningsstatistik 2004.* Stockholm: Svensk Energi.

Svensk Energi (2005). *Elåret 2005*. Stockholm: Svensk Energi.

Nordel (2002). *Nordels riktlinjer för klassificering av driftstörningar.*

9.3 Böcker

Davidsson, G. (2003). *Handbok för riskanalys*. Östervåla: Elanders Tofters AB.

Ejvegård, R. (2003). *Vetenskaplig metod.* Lund: Studentlitteratur.

Institutionen för Värme- och Kraftteknik (2005). *Säkerhet och sårbarhet i elsystemen* (2005). Polen.

9.4 Elektroniska referenser

Analytic technologies. http://www.analytictech.com. 2007-01-08.

Elsäkerhetsverket. www.elsäkerhetsverket.se. 2006-12-06.

FRIVA. http://www.friva.lucram.lu.se. 2006-09-06.

Lunds tekniska högskola, institutionen för elektroteknik och automation. www.iea.lth.se/et/G5_05.pdf. 2006-12-18.

Math World. www.mathworld.wolfram.com. Uppslagsord: four color theorem. 2006-09-04.

Math World. www.mathworld.wolfram.com. Uppslagsord: köningsberg bridge problem. 2006-09-04.

Nationalencyklopedin. www.ne.se. Uppslagsord: elmarknadsreformen. 2006-09-08.

Nationalencyklopedin. www.ne.se. Uppslagsord: grafteori. 2006-09-04.

Nationalencyklopedin. www.ne.se. Uppslagsord: nätverk. 2007-01-31.

Nationalencyklopedin. www.ne.se. Uppslagsord: system. 2007-01-29.

Nationalencyklopedin. www.ne.se. Uppslagsord: topologi. 2006-09-04.

Nationalencyklopedin. www.ne.se. Uppslagsord: union. 2007-01-29.

Regeringskansliets rättsdatabaser. http://lagen.nu. 2006-09-06.

Statens Energimyndighet. www.stem.se. 2006-09-01.

Svensk Energi. www.svenskenergi.se. 2006-09-01.

Svenska Kraftnät. www.svk.se. 2006-09-01.

9.5 Personlig kommunikation

Aldrin, J. (2007). Personlig kommunikation. 2007-01-29.

Johansson, H. (2006). Personlig kommunikation. Fortlöpande sep - dec 2006.

Johansson, J. (2006). Personlig kommunikation. 2006-11-22.

Wallnerström, C-J. (2006). Personlig kommunikation. 2006-11-10.

9.6 Övrigt

Elforsk (2004). *Guide för elanvändare och allmänt sakkunniga inom området*. Stockholm.

Johansson, H. & Jönsson, H (2007). *Metod för risk och sårbarhetsanalys ur ett systemperspektiv*. Utkast. Lund: Lunds Tekniska Högskola.

Ohlson, P. (2006). *Algoritm för beräkning av antal samtidiga fel.* Skapad 2006-11-29.

Telge nät AB (2006). *Driftstörningsstatisktik från DARWIN.* 2006-09-03.

Wallnerström, C-J. (2005). *En jämförande studie av tillförlitlighetsmetoder för elnät - en utvärdering av nätnyttomodellens tillförlitlighetsmetod*. Examensarbete. Kungliga tekniska högskolan, institutionen för Elektrotekniska System.

Bilagor

Här återfinns de bilagor som refererats till i rapporten.

Bilaga 1 FRIVA

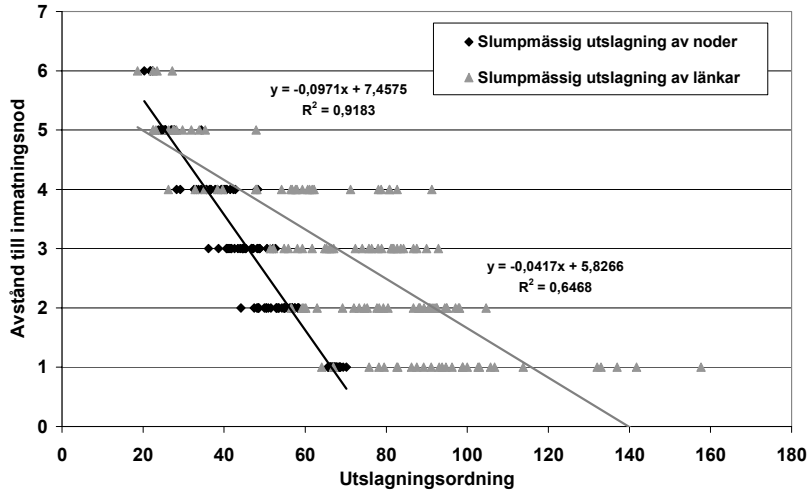
De båda verktygen NetCalc och ACC är framtagna inom ramforskningsprogrammet FRIVA som bedrivs inom ramen för LUCRAM (Lunds University Centre for Risk Analysis) och finansieras av Krisberedskapsmyndigheten. Tanken med FRIVA är att förbättra kompetensen kring, och metoderna för, utförande av risk- och sårbarhetsanalys. En viktig del i forskningsprojektet är att utveckla verktyg för att analysera konsekvenser av och interdependens mellan stora händelser, till exempel elavbrott. Tanken är att verktygen utvecklade i projektet, utöver elnätsystem, även ska gå att använda för andra betydelsefulla infrastrukturer såsom vattenförsörjning och telesystem. (FRIVA, 2006)

Bilaga 2 Framtagning av koordinater

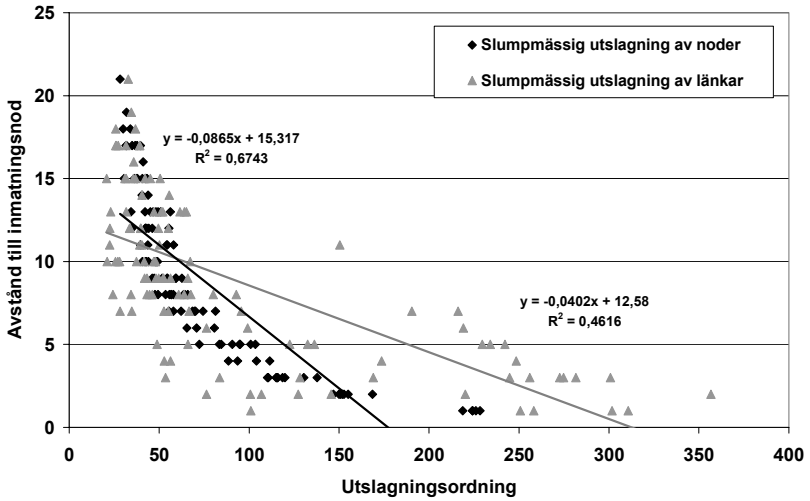
Nodernas position i de tre näten togs fram på två olika sätt. Data för tätorts- och glesbygdsnätet hämtades från tidigare studier där nodernas koordinater togs fram genom att leta upp deras position på en karta över elnäten. Koordinaterna för noderna i det blandade nätet togs däremot fram i denna rapport och hämtades ur en databas. För noder som representerade frånskiljare och förgreningar saknades dock uppgifter om koordinater. Dessa togs därför fram genom följande approximationer: För noder som var kopplade till tre andra noder med existerande koordinater togs nodens koordinater fram i den beräknade tyngdpunkten hos triangeln som bildades av de tre angränsade noderna. För noder som enbart var kopplade till två noder med existerande koordinater, gavs koordinaterna i den punkt som låg mittemellan de två noderna. De noder som var kopplade till fyra eller fler andra noder gavs koordinater i den punkt som utgjorde tyngdpunkten hos triangeln som bildades av tre utav de angränsande koordinaterna. De noder som endast var kopplade till en annan nod gavs koordinater 50 meter i den riktning som noden låg i förhållande till i den första noden i linjeschemat, detta eftersom underlag för mer exakt approximation saknades.

Bilaga 3 Samband mellan avstånd till inmatningsnod och utslagningsordning

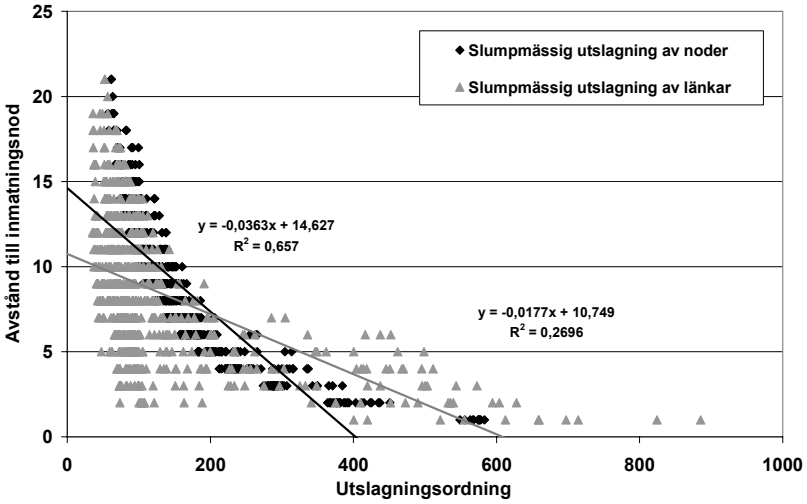
Figur 1, 2 och 3 visar sambandet mellan distributionsnodernas avstånd till inmatningsnod och utslagningsordningen vid simulering i NetCalc för de tre näten. Sambandet plottades för både utslagning av noder och länkar.



Figur 1 Sambandet för tätortsnätet vid slumpmässig utslagning av noder och länkar



Figur 2 Sambandet för det blandade nätet vid slumpmässig utslagning av noder och länkar



Figur 3 Sambandet för glesbygdsnätet vid slumpmässig utslagning av noder och länkar

Som figurerna visar, finns det ett samband mellan distributionsnodernas avstånd till inmatningsnod och den ordning i vilken de förlorar matning i en slumpmässig utslagning. Sambandet är störst för nodutslagningarna, detta beror sannolikt på att ingen hänsyn togs till länklängd och länktyp vid dessa simuleringar. Vid utslagningen av länkar i glesbygdsnätet finns i princip inget samband alls vilket visar att hänsyn till länklängd har stor betydelse för resultatet av sårbarhetsanalysen.

Bilaga 4 Lagtext

Enligt nya bestämmelser i ellagen har en elabonnent rätt till ersättning för avbrott längre än 12 timmar.

Ellag (1997:857)

10 kap. Avbrottsersättning

10 § *Om överföringen av el avbryts helt under en sammanhängande period om minst tolv timmar har elanvändaren rätt till avbrottsersättning. Elanvändaren har inte rätt till avbrottsersättning om*

1. *avbrottet beror på elanvändarens försummelse,*
2. *överföringen av el avbryts för att vidta åtgärder som är motiverade av elsäkerhetsskäl eller för att upprätthålla en god drift- och leveranssäkerhet och avbrottet inte pågår längre än åtgärden kräver,*
3. *avbrottet är hänförligt till ett fel i en koncessionshavares ledningsnät och felet beror på ett hinder utanför den koncessionshavarens kontroll som koncessionshavaren inte skäligen kunde förväntas ha räknat med och vars följder koncessionshavaren inte heller skäligen kunde ha undvikit eller övervunnit, eller*
4. *avbrottet är hänförligt till ett fel i ett ledningsnät vars ledningar har en spänning om 220 kilovolt eller mer. Lag (2005:1110)*

11 § *Avbrottsersättning skall betalas av den som har koncession för det elnät till vilket elanvändaren är direkt ansluten. Lag (2005:1110)*

12 § *När avbrottsersättning beräknas skall en period med avbruten överföring av el (avbrottsperiod) anses avslutad vid den tidpunkt då avbrottet upphört, om överföringen därefter har fungerat oavbrutet under de närmast följande två timmarna.*

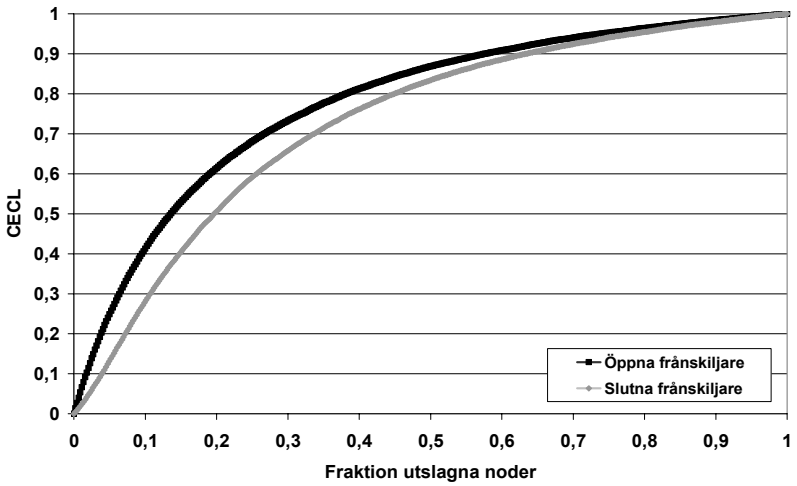
Avbrottsersättningen skall för en avbrottsperiod om minst tolv timmar och högst tjugofyra timmar betalas med 12,5 procent av elanvändarens beräknade årliga nätkostnad, dock lägst 2 procent av prisbasbeloppet enligt lagen (1962:381) om allmän försäkring avrundat till närmast högre hundratal kronor.

Om avbrottsperioden är längre än tjugofyra timmar skall för varje därefter påbörjad tjugofyratimmarsperiod ytterligare ersättning betalas med 25 procent av elanvändarens beräknade årliga nätkostnad, dock lägst 2 procent av prisbasbeloppet avrundat till närmast högre hundratal kronor.

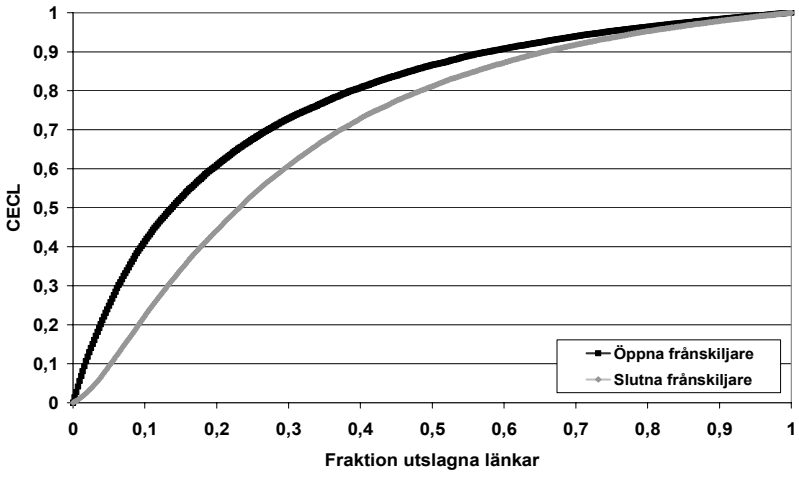
Avbrottsersättningen skall för en avbrottsperiod uppgå till högst 300 procent av elanvändarens beräknade årliga nätkostnad. Lag (2005:1110)

Bilaga 5 Betydelse av försummad omkopplingstid

I modelleringen försummades omkopplingstiden i elnäten. För att undersöka hur stor betydelse detta har på resultatet gjordes simuleringar med öppna och slutna frånskiljare för det blandade nätet. Detta gjordes för slumpmässig utslagning av noder respektive länkar. Med öppna frånskiljare menas att dessa modelleras som normalläget, det innebär att frånskiljare som är slutna i normalläget även är slutna i den ”öppna” simuleringen. Varje scenario simulerades 1000 gånger i NetCalc varefter ett medelvärde beräknades. Resultaten av simuleringarna presenteras i figur 1 och 2.



Figur 1 Simulering med öppna och slutna frånskiljare vid slumpmässig utslagning av noder



Figur 2 Simulering med öppna och slutna frånskiljare vid slumpmässig utslagning av länkar.

Enligt figurerna var nätets sårbarhet enligt CECL högre då frånskiljarna modellerades som öppna. Detta visar att möjligheten till alternativa matningvägar har stor betydelse för hur robust nätet är vid ett avbrott. I dagsläget är det inte möjligt att ta hänsyn till omkopplingstid i de simuleringsmetoder som användes i analysen men det är något som vore intressant att titta på i framtida studier.