Sårbarhetsanalys av ett infrastrukturnätverk

Användning av nätverksteorier för sårbarhetsanalys av komplexa nätverk

Tobias Salomonsson & Mikael Schéele

Department of Fire Safety Engineering
Lund University, Sweden

Brandteknik
Lunds Tekniska Högskola
Lunds universitet

Report 5170, Lund 2005

Sårbarhetsanalys av ett infrastrukturnätverk
Användning av nätverksteorier för sårbarhetsanalys av komplexa nätverk

Tobias Salomonsson & Mikael Schéele

Lund 2005

Sårbarhetsanalys av ett infrastrukturnätverk
Användning av nätverksteorier för sårbarhetsanalys av komplexa nätverk

Vulnerability analysis of an infrastructure network
Using network theories to perform vulnerability analysis of complex networks

Tobias Salomonsson & Mikael Schéele

Report 5170
ISSN: 1402-3504
ISRN: LUTVDG/TVBB-5170-SE

Number of pages: 76
Illustrations: Tobias Salomonsson & Mikael Schéele (If not other stated)

Keywords
Vulnerability analysis, complex networks, network theories, power supply.

Sökord
Sårbarhetsanalys, komplexa nätverk, nätverksteorier, elförsörjning.

Abstract
The aim of this report is to examine the possibilities to use network theories to perform vulnerability analysis on complex networks. The scoop of this work is also to improve the possibilities to chart, analyze and present the vulnerability in a power grid. In this report it has been, using power outage statistics, possible to verify, that network theories can be used to evaluate the vulnerability of an infrastructure network. However further studies to establish values on how vulnerable a network is are needed.

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

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

Förord

Vi vill rikta ett stort tack till alla som hjälpt och stöttat oss under detta examensarbete.

Först vill vi tacka Stefan Andersson på Sydkraft Nät AB i Malmö, som med kort varsel ställde upp som extern handledare. Han har bidragit med kontakter och alltid tagit sig tid när vi kommit med frågor.

Ett stort tack vill vi också rikta till vår handledare doktor Henrik Johansson, på Brandteknik. Trots motgångar och uppförsbacke var vi alltid fulla med entusiasm efter dina ”pep-talk”. Givetvis är vi även djupt tacksam för det dataprogram som Ni tog fram, utan detta program hade detta arbete inte varit möjligt.

Vi vill även tacka WSP för att de ställt upp med lokaler och utrustning. Det inte svårt att vara kreativ på nionde våningen med utsikt över Malmö och norr därom.

Sist men inte minst vill vi tacka våra nära och kära som varit ett stort stöd under arbetets gång.

Denna rapport är en del i FRIVA-projektet (delprojekt 2) som drivs av LUCRAM på uppdrag av Krisberedskapsmyndigheten.

Lund 2005

Tobias Salomonsson Mikael Schéele

Sammanfattning

Under de senaste åren har nätverksteori växt fram som ett nytt vetenskapligt forskningsområde och mängder av artiklar inom nätverksteori har presenterats i vetenskapliga tidskrifter. Forskningsresultaten grundar sig på användning av matematisk grafteori och har visat sig tillämpligt på så vitt skilda områden som elkraftteknik, cellbiologi och sociala nätverk. Samtidigt blir samhället mer och mer beroende av dessa nätverk. Som exempel kan nämnas datanätverk som inte fungerar utan el, där elnätet i sig är ett nätverk. För att hantera hot och risker inom ovan angivna system, har Krisberedskapsmyndigheten bildats. Krisberedskapsmyndigheten har även till uppgift att sprida kunskaper och stärka samhällets krishanteringsförmåga genom att informera och utbilda inom området samhällets sårbarhet.

Syftet med detta arbete är att undersöka möjligheten att göra sårbarhetsanalys av ett infrastrukturnätverk, genom att använda verktyg hämtade från nätverksteori. Detta arbete syftar även till att förbättra möjligheterna att kartlägga, analysera och presentera sårbarheten i ett elnätverk.

Metoden som ligger till grund för detta arbete är studier av litteratur på områden som behandlar matematisk grafteori, nätverksteori samt sårbarhet. Kartläggning och simulering av elnätverk har genomförts med hjälp av datorprogram.

I rapporten presenteras viktiga nätverksbegrepp. Ett enkelt exempel på ett nätverk kan vara ett elnät där stolpar, förgreningar, transformatorer mm är noder och elkablarna mellan dessa är nätverkets länkar. I de simuleringar som genomförts i arbetet har dels noder och dels länkar attackerats i syfte att se hur nätverket klarat dessa påfrestningar. Genom att koppla abonnenter till de noder som innehåller sådana, har en bedömning av nätverkets sårbarhet kunnat göras. Ett kriterium som använts vid dessa simuleringar är nodernas grad. Med grad menas det antal länkar som är kopplade till en nod. Det enklaste måttet som används för att beskriva ett nätverks struktur är nätverkets genomsnittliga grad. Detta bygger på den relativa frekvensen av noder med viss grad. Vid simuleringar har nodens grad använts för att simulera riktade attacker mot nätverket, till exempel terrorhandlingar. Den slutsats som dras med avseende på riktade attacker är att de nät som har noder, med hög grad nära källnoden, uppvisar en högre sårbarhet. Med källnod menas den nod som matar ut ström i nätverket. Alla undersökta nät uppvisade en låg klustringskoefficient. Klustringskoefficienten beskriver hur många av en nods grannar som är förbundna med varandra. En låg klustringskoefficient nära källnoden, leder till färre möjligheter att sammanlänka noder om någon nod skulle attackeras. För att öka robustheten i de studerade elnäten föreslås därför att åtgärder som syftar till att öka klustrings-koefficienten nära källnoden vidtas.

I denna rapport har det, med hjälp av avbrottsstatistik, kunnat verifieras att, verktyg hämtade från nätverksteorin, fungerar för att bedöma sårbarheten av nätverksstruktur. Dock krävs det vidare studier för att

Under arbetets gång har nya frågeställningar, samt fortsättningar där detta arbete slutar dykt upp. Dessa frågeställningar har inte varit möjliga att studera inom ramen för detta arbete. Därför har dessa sammanställts i slutet på detta arbete och det är en förhoppning att detta arbete kan entusiasmera och ligga till grund för fortsatta studier.

Summary

During the last few years network theories have been introduced as a new scientific research field and many articles on the subject have been published. The research takes its ground in using graph theory and has been shown to be applicable in such different fields as power grids, cell biology and social networks. At the same time society becomes more and more reliant of these networks. As an example a computer network can be mentioned, which is dependent of the power grid, which also is a network. To secure the function of these different networks a new department, in Sweden, has been established, Krisberedskapsmyndigheten. This new departments task is to shed light on and strengthen the society's crisis management by informing and educating on the subject of the society's vulnerability.

The scoop of this work is to investigate the possibility to perform vulnerability analyze on a infrastructure network, by using paraphernalia gathered from network theories. The scoop of this work is also to improve the possibilities to chart, analyze and present the vulnerability in a power grid.

To reach the scoop of this work literature regarding graph theories, network theories as well as literature concerning vulnerability has been studied. Mapping of the power grid, and simulations, have been performed with computer software programs.

The report introduces important network concepts. An example of a network is a power grid. The distributors and transformers are nodes and the electrical lines connecting them are links. In the simulations that have been performed, both nodes and links have been attacked to see how the network can cope with these strains. By connecting subscribers to the nodes, it has been possible to evaluate the networks vulnerability. A criterion that has been used during this simulation is the nodes degree. The nodes degree indicates how many links that are connected to a specific node. A way to describe the topology of the network is the average degree of the network. Average degree has been used to see how the network reacts when it is attacked. These attacks can, for example, be acts of terror. All of the examined networks have a low cluster coefficient. The cluster coefficient describes how many of a nodes neighbors are connected to each other. A low cluster coefficient, close to the source, gives less opportunities to connect nodes if a node is to be attacked. To decrease the vulnerability in the examined networks it is proposed to make modifications, which will increase the cluster coefficient close to the source.

In this report it has been, using power outage statistics, possible to verify, that network theories can be used to evaluate the vulnerability of an infrastructure network. However further studies to establish values on how vulnerable a network is are needed.

During the writing of this report new questions have been raised. These new questions have not been able to be examined in this report but have been presented in this work. Hopefully can someone pick up where we left off and explore new aids to perform vulnerability analysis.

Innehållsförteckning

1 Inledning

1.1 Bakgrund

Dagens samhälle är i mångt och mycket uppbyggt på nätverk, exempelvis telenätverk, elnätverk, datanätverk m fl. Nätverk förklaras av att det råder ett beroendeförhållande eller relationer mellan objekt. Objekten kallas inom nätverksteorin ofta för noder och relationer för länkar. Nätverk kan delas upp utefter deras karaktär i, infrastruktur-, organisatoriska- eller sociala nätverk (Karlqvist, 1990). Ett infrastrukturnätverk är uppbyggt för att transportera exempelvis människor, material eller meddelanden. Vägnätet kan ses som praktiskt exempel på ett infrastrukturnätverk, där vägkorsningar är noder och vägarna mellan korsningarna är länkar. Organisatoriska nätverk binder samman individer, segment och arbetsplatser inom produktionssystem, företag och andra organisationer med varandra. De nätverk som behandlar de relationer som förmedlar impulser, idéer eller de känslomässiga band som finns mellan individer brukar kallas sociala nätverk. Ett exempel på socialt nätverk är att se familjemedlemmarna som noder och de känslomässiga band som förbinder dem som länkar.

Samhället är idag mycket beroende av att dessa nätverk. Det visar, om inte annat, följderna av stormen Gudrun i januari 2005, där människor inte kunde transportera sig från sina hem på grund av att vägnätet var utslaget och flera veckor efter stormen var tusentals hushåll fortfarande utan ström och telefon. Detta på grund av att ledningar (länkar), mellan el-stolpen (nod) och abonnenten (nod) har brustit. Därmed borde det vara av stor vikt att kunna bedöma sårbarhet i sådana system.

Den 11 september 2001 inträffade den troligtvis största terrorattacken i modern tid. Konsekvenserna blev stora, inte minst med avseende på mänskligt lidande. Det kaos som uppstod, i samband med dessa attentat och kort därefter, berodde sannolikt inte enkom av terrorhandlingens storlek utan även att flera olika typer av samhällsviktig nät slogs ut samtidigt; infrastruktur (tunnelbane- och telefonnät), organisatoriska (finansnätverk) samt sociala nätverk (företag som förlorade mer än hälften av sina medarbetare). I verkliga nätverk finns det vanligtvis punkter (noder) som är viktigare än andra, i sårbarhetshänseende, beroende på, till exempel, att en och samma plats är nod till flera olika nätverk, som i fallet med World Trade Center. Därmed är nätverkets funktion mycket beroende av att dessa noder är intakta. Terrorism uppfattas idag som ett hot mot samhället där nätverken har en mycket stor betydelse. Liknande kaos, som inträffade den 11 september vid World Trade Center, skulle sannolikt kunna uppstå endast genom att, rikta attacker mot dessa viktiga punkter som beskrivits ovan. Av dessa anledningar är det därmed viktigt att kunna identifiera och skydda dessa.

Som ovan nämnts kan nätverk delas in beroende av dess karaktär. Detta arbete är inriktat på infrastrukturnätverk. Detta på grund av att tyngdpunkten för arbetet är att pröva nätverksteorier för att analysera ett verkligt nätverks sårbarhet. Om sociala eller organisatoriska nätverk hade valts hade sannolikt tyngdpunkten hamnat på att kartlägga nätverket, då dessa ofta är av komplex natur.

Mot bakgrund av terrorhandlingar och katastrofer i allmänhet är det av största vikt att kunna analysera dessa nätverk och på så vis kunna bedöma ett nätverks sårbarhet. För att möjliggöra sådana analyser behöver nätverksteorier studeras och kopplas mot studier i sårbarhetsanalys.

1.2 Syfte

Syftet med detta examensarbete är att undersöka möjligheten att göra sårbarhetsanalys av ett infrastrukturnätverk, genom att använda verktyg hämtade från nätverksteorin. Det nätverk som avses analyseras är ett elnätverk som ägs av Sydkraft.

Detta arbete syftar till att förbättra möjligheterna att kartlägga, analysera och presentera sårbarheten i ett elnät. Denna metod skall ses som ett nytt sätt, alternativt en komplettering av dagens befintliga metoder, för Sydkraft att genomföra sårbarhetsanalys av elnät.

Rapporten syftar vidare till att bidra till spridningen av kunskaper i nätverksteori.

Utformningen på arbetet ska vara på ett sådant sätt att det kan ligga till grund för vidare studier inom området. Härvid skall grund läggas för studier huruvida denna metod även lämpar sig för sårbarhetsanalys av organisatoriska och sociala nätverk.

1.3 Problemformulering

Då nätverken får större och större betydelse för samhället, som redogjorts ovan, och att nätverksteori är ett förhållandevis nytt forskningsområde har vi sett en möjlighet att koppla samman de, sedan tidigare inhämtade kunskaper inom risk- och sårbarhetsanalys, med dessa nya kunskaper.

- Hur ser ett elnätverk ut när det beskrivs som ett nätverk?
- Vilka olika typer av prioriterade kunder finns det i det nät som studeras?
- Hur sårbart är nätverket?
- Hur beskriver man bäst sårbarheten i nätverk med hjälp av nätverksteori?
- Kan metoden överföras på andra typer av nätverk?
- Är denna metod tillräcklig för att bedöma sårbarheten i ett elnätverk?

1.4 Metod

Den huvudsakliga kunskapsinhämtningen om nätverksteori kommer att ske genom studier av i första hand vetenskapliga tidskriftsartiklar hämtade från databasen ELIN, i andra hand från övrig litteratur och examensarbeten. Avseende sårbarhetsanalys kommer tidigare erhållen kompetens inom området kompletteras med studier av examensarbeten hämtade från Avdelningen för brandtekniks, Lunds tekniska högskola, hemsida, vetenskapliga artiklar hämtade på ELIN samt studier av t ex lagstiftning på myndigheters hemsidor via Internet. Exempel på myndigheter är Krisberedskapsmyndigheten, Räddningsverket och Riksdagens hemsida.

Kartläggningen av elnätet kommer att ske genom att sammanställa information från nätkartor, driftsscheman samt dokument som beskriver abonnenttätheten och förekomsten av prioriterade kunder i anslutning till de noder som valts.

Simulering av attacker mot nätverket kommer att genomföras med hjälp av simuleringsprogram tillhandahållet av Dr. Henrik Johansson vid avdelningen för brandteknik,

Lunds tekniska högskola. Programmet analyserar klustringskoefficient (Strogatz & Watts, 1998), inverterad längd (Holme & Kim, 2002) samt attackstrategi.

Slutligen avser vi att analysera denna sårbarhetsanalysmetod och dess validitet.

1.5 Rapportens disposition

För att visa läsaren hur rapportens upplägg ser ut kommer här en kort presentation av de ingående kapitlena. Detta för att läsaren ska kunna förstå hur de olika kapitlena hänger ihop.

Kapitel 2 – Då nätverksteori är en förhållandevis ny vetenskap kommer denna rapport skrivas för tillgodose även den, för nätverksteori, oinsatta. I detta kapitel kommer således teorierna presenteras i en mer populärvetenskaplig synvinkel. Detta syftar till att entusiasmera den oinsatte läsaren och läsaren utan naturvetenskaplig bakgrund.

Kapitel 3 – Här kommer teorierna presenteras djupare och ta en grund i naturvetenskapen. Detta kapitel syftar till att ge läsaren en mer akademisk bakgrund och tar avstamp där forskning befinner sig just nu. Anledningen varför detta avhandlar samma sak som kapitel 2, men ur en annan synvinkel och djup, är att fånga intresset från en bredare publik.

Kapitel 4 – I detta kapitel kommer en beskrivning av studien att genomföras. Härvid kommer alla förutsättningar för denna studie att belysas, bland annat specificeras elnätet och datorprogram för simulering.

Kapitel 5 – De resultat som avser sårbarhetsanalysen av elnätet redovisas här.

Kapitel 6 – I detta, det avslutande kapitlet, kommer de slutsatser som erhålls av sårbarhetsanalysen att redovisas. En diskussion kommer även att föras huruvida sårbarhetsanalys med hjälp av nätverksteori är användbart. Diskussion förs även om denna metod är användbar på andra typer av nätverk. Kapitel redogör också för en känlighets- och osäkerhetsanalys.

Kapitel 7 – Förslag på vidare studier inom ämnet kommer också att ges.

1.6 Avgränsning

Sårbarhetsanalysen kommer endast att genomföras ur ett strukturellt perspektiv. Faktorer som kvalité, underhållsaspekter och ålder på elnätet kommer ej att tas hänsyn till. Det kommer ej heller att ta hänsyn till om nätet består av luft- eller markledning. Antagande har gjorts att finns det en koppling så finns det även ström mellan noderna, vilket är en förenkling. Denna avgränsning är gjord mot bakgrund av att de verktyg som används är framtagna för att analysera struktur.

Dessa typer av elnät (lokalnät) är normalt radiella, vilket betyder att nätet är uppdelat i olika stationer som avskiljs genom att frånskiljare monteras där näten fysiskt sammanlänkas. Stationerna är på liknande vis uppdelade i fack. Möjlighet finns dock att sluta dessa frånskiljare och göra maskade nät, det vill säga, att ett stort nät görs av flera små nät. I detta arbete har elnätet ansetts vara maskat.

Vi avgränsar oss till att endast redovisa abonnenter och i viss mån för samhället sårbara objekt, inte fysiska människor.

2 Bakgrund

Syftet med följande kapitel är att introducera läsaren för nätverksteorier och sårbarhetsanalys. Först kommer bakgrunden till nätverksteorier presenteras och även vissa nyckelord kommer att förklaras. I stycket som behandlar sårbarhetsanalys kommer bakgrunden till ämnet att presenteras.

2.1 Nätverksteorier

De senaste fem åren har studier om nätverk och nätverks system formligen exploderat (Watts, 2003). Med hjälp av billigare men kraftfulla datorer har samband kunnat identifieras mellan problem som tidigare ansetts helt åtskilda. Samtidigt som det finns mer data som beskriver strukturen hos verkliga nätverk, kan dess komplexa struktur analyseras (Barabási et. al., 1999). Det resultat som utkommit av dessa studier, har kallats ”the new science of networks” vilket betyder precis som det låter. Komplexa nätverk har traditionellt studerats genom de grafteorier som Erdós och Rényi presenterade på 1950-talet (Watts, 2003).

2.1.1 Small world

På 1960-talet gjorde psykologen Stanley Milgram ett experiment för att undersöka hur liten världen egentligen är (Milgram & Travers, 1969). Målet med experimentet var att se hur lång kedja (av personer) som krävdes för att vidarebefordra ett brev från en, mer eller mindre, godtycklig startperson till en definierad slutadressat. Milgram skickade ut ett hundratal brev (296 för att vara exakt) till personer i Boston, Massachutes och Omaha, Nebraska. De personerna från Nebraska som deltog i experiment delades in i två grupper. Den ena gruppen (100 personer) bestod av börsmäklare, den andra gruppen var däremot godtyckligt utvald. Brevet skulle skickas till en namngiven person i Boston, en börsmäklare. Om mottagaren kände börsmäklaren skulle givetvis brevet skickas direkt till honom. Kände mottagaren inte börsmäklaren skulle brevet skickas vidare till någon som avsändaren trodde kunde få brevet vidare till börsmäklaren, dock fick brevet endast skickas till personer som avsändaren kände personligen. Resultatet blev att kedjan fullbordades i 64 fall, alltså att brevet skickades från startpersonen till den namngivna börsmäklaren. I dessa 64 fall hade brevet i genomsnitt passerat 5,2 personer. Föga förvånande nådde de kedjor som började i Boston, börsmäklaren snabbare (kortare kedja). Däremot i de fall, där breven startade i Nebraska, kunde ingen skillnad påvisas mellan brev från börsmäklare, vilka kunde förväntas att fullborda kedjan snabbare eftersom de rör sig i samma bransch som måladressaten, och brev från de godtyckligt utvalda experimentdeltagarna. Från resultatet, att det i genomsnitt var 5,2 steg mellan startperson och målet, myntades begreppet ”Six degrees of separation”, och experimentet kallades ”small-world” metoden.

Vid eftertanke är resultatet av Milgrams studie kanske inte så märkvärdigt? Hur många gånger har det inte framkommit vid möten med helt okända personer att det finns gemensamma vänner. Watts (Watts, 2003) presenterar ett tankeexperiment i sin bok *Six degrees – The science of a connected age* i ett försök att förklara detta fenomen. Tänk dig att du har 100 vänner, dina vänner har i sin tur 100 vänner. Redan här, efter två steg av separation, innefattar vi 10 000 personer. Fortsätter vi i fem steg så är vi uppe i 10 miljarder personer, vilket är mer än jordens befolkning.

Samtidigt har det visat sig att flera verkliga nätverk är små världar. Små världar förklaras genom att det i nätverket finns grupper av noder med många länkar, samtidigt som det är korta avstånd mellan de noder som ingår i nätverket. Det är amerikanska elnätet är ett exempel, ett annat är skådespelare som genom att de medverkat i filmer tillsammans är små världar. Studenter vid William and Mary College uppmärksammade att skådespelaren Kevin

Bacon verkade vara filmvärldens centerpunkt. För att undersöka detta tillverkade de ett spel där det går att räkna ut en skådespelares Baconnummer. Har en skådespelare varit med i samma film som Kevin Bacon har denne skådespelare ett Baconnummer som är ett. En skådespelare som inte spelat mot Herr Bacon, men däremot spelat in en film med en skådespelare som varit med i samma film som honom, får ett Baconnummer två, och så vidare (Watts, 2003). Läsaren uppmanas att själv surfa in och testa på The Oracle of Kevin Bacon (http://www.cs.virginia.edu/oracle). En artikel publicerade i Nature av fysikerna Duncan J. Watts och Steven Strogatz kontrollerade att nätverket med skådespelare verkligen var små världar. Detta genom att kontrollera alla vägar, inte bara vägar genom Kevin Bacon. Resultatet visade att varje skådespelare kunde kopplas till en annan skådespelare, i genomsnitt, i mindre än fyra steg av separation (Strogatz & Watts, 1998).

2.1.2 Kluster

Efter ovan nämnda artikel publicerades i Nature 1998, av Strogatz och Watts, ökade intresset för nätverksforskning. Något som Strogatz och Watts presenterade i artikeln var att i verkliga nätverk är vanligtvis en nods grannar ofta även grannar med varandra. För att återgå till exemplet ovan där en person har 100 vänner, dessa 100 i sin tur har 100 vänner, är det stor sannolikhet att många av dessa vänner är gemensamma (Watts, 2003). Detta leder i sin tur att det finns grupper i nätverket som är kopplade till varandra men inte nödvändigtvis kopplade till övriga aktörer i nätverket. Ett tydligt exempel är att inom en familj känner alla varandra men alla känner inte familjemedlemmarnas vänner.

2.1.3 Skalfrihet

Albert och Barabasi fick en artikel publicerad som utgick från Watts och Strogatz tidigare nämnda artikel (Albert och Barabasi, 1999). De ansåg att Watts och Strogatz hade missat en viktig sak i sina antaganden. Watts och Strogatz använde en modell (modellen kommer vidare kallas WS) som visade hur avståndet mellan noder kunde förkortas genom att länkarna mellan noderna godtyckligt kopplas om. Det som Barabasi och Albert invände emot var att i ett verkligt nätverk utökas antal noder med tiden medan WS hade samma antal noder hela tiden. Barabasi och Albert ansåg inte heller att noder kopplas om godtyckligt utan snarare att nya noder i nätverket kommer att kopplas till noder som redan har flera grannar. Detta kan förtydligas genom att återgå till nätverket med skådespelare. En ny nod, skådespelare, i nätverket, kommer troligen att ha en mindre roll i början av sin första produktion. Däremot är sannolikheten stor att huvudrollsinnehavaren i samma produktion redan är länkad till många andra skådespelare. På så viss är sannolikheten större att en ny nod kopplas till en nod som redan har många grannar.

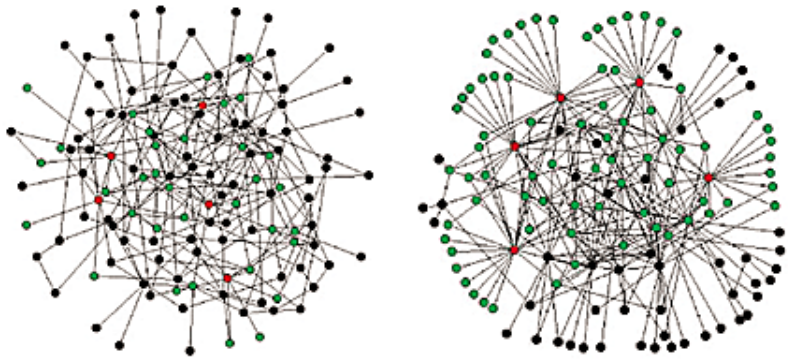


Bild 1 Den högra bilden visar hur nya noder kopplas till noder som redan har flera grannar, vilket karakteriserar skalfrihet. (Computerworld, 2005)

En skalfri fördelning i nätverk förklaras således av att nätverket växer med tiden och att nya noder har en tendens att ansluta sig till noder som redan har flera andra grannar.

2.2 Sårbarhetsanalys

Samhällsutvecklingen de senaste decennierna, där till exempel människan bland annat blivit mer och mer beroende av datorer som i sin tur ställer krav på att eldistributionen fungerar, har gjort samhället mycket sårbart. Även förekomsten av svårare påfrestningar i samhället, så som till exempel de senaste årens närmast årligen återkommande översvämningarna som drabbat olika delar av landet, har gjort att staten höjt ambitionen bland annat genom att bilda Krisberedskapsmyndigheten och stifta ny lag, Lag (2002:833) om extraordinära händelser i fredstid hos kommuner och landsting.

Risk- och sårbarhetsanalys sammanknippas ofta i både litteraturen och i dagligt tal. Sårbarhet och sårbarhetsanalys är, till skillnad mot risk och riskanalys, inte så väldefinierad. Det går att hitta en mängd olika definitioner i olika litteratur. I boken *Risk- och sårbarhetsanalyser - Vägledning för statliga myndigheter* (2003) menar Krisberedskapsmyndigheten att riskanalys fokuserar på felorsakerna och de konsekvenser som uppstår till följd av dessa felorsaker. Sårbarhetsanalysen tar en bredare syn och tittar på konsekvenser även utanför det system som analysen riktar sig. Myndigheten menar också att sårbarheten tar ett annat tidsperspektiv, från det att störningen inträffar till dess stabila tillstånd uppnåtts.

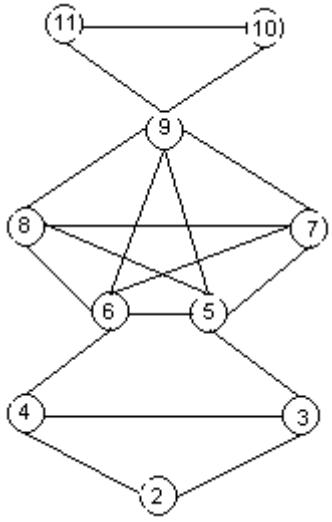
Inom nätverksteorin har verktyg tagits fram för att mäta ett näts känslighet för störningar. Känsligheten kan dels mätas när riktade attacker sker mot de noder som är sammanlänkade till flest andra noder och dels när attackerna sker mot noder rent slumpmässigt. Att koppla dessa verktyg till att mäta sårbarhet i ett elnät har tidigare utförts av Åke Holmgren (Åke Holmgren, 2004a). Det elnät som undersöktes var delar av nät i Sverige, Finland, Norge och Danmark. Resultatet presenterades som ett nordiskt nät då författaren inte blivit tillåten att presentera näten var för sig (Åke Holmgren, 2004b). Dock har det inte, före detta examensarbete, gjorts någon undersökning som ser på antalet utslagna abonnenter vid attack av elnätverket.

3 Teori

I detta kapitel kommer teorin bakom nätverksteori att presenteras. I avsnitt om sårbarhet kommer begreppet definieras och en koppling till styrande lagar kommer att göras.

3.1 Nätverksteori

I ett försök att underlätta för läsaren att följa med i detta kapitel har ett modellnätverk upprättats. Nätverket baseras på ett taktiskt system inom fotboll, 3-5-2, som figur 1 nedan visar. Spelarna i systemet är noder och passningsvägarna mellan spelare blir nätverkets länkar. De olika lagdelarna i systemet, försvar, mittfält och anfall, är tänkta att ses som olika grupper som endast kan interagera genom särskilda mönster. Försvarets passningsvägar går alltid via de två defensiva innermittfältarna, 5 och 6. Alltså är försvar och mittfält sammanlänkat. Vidare är det endast den offensiva mittfältaren, 9, som förser anfallarna, 10 och 11, med passningar.



Figur 2.1.3-1 Modellnätverk i form av ett fotbollslag, 3-5-2.

Som modellen visar kan spelarna inom de olika grupperna spela bollen mellan sig utan några restriktioner. Däremot måste bollen följa vissa vägar när den går från grupp till grupp. Bollen kan dock både passas framåt från back till mittfält till anfall eller i motsatt väg om laget vill maska vid ledning i slutet av match. Nätverket betecknas således som oriktat. Ett exempel på ett riktat nät är ett elnät, där strömmen går från transformatorn till kunden och aldrig tvärtom.

3.1.1 Grafteori

När ordet graf kommer på tal, förknippas detta ofta med en linje som plottas mot x-och y-axeln. Men benämningen graf har vanligtvis en annan betydelse inom matematiken, nämligen en samling noder (punkter) och samling kanter (länkar) som förbinder dessa punkter parvis. (Mathworld, 2005). Eftersom det ännu inte finns någon standard för terminologin inom grafteorin (Bollobás, 1998) kommer rapporten att försöka anpassas till den terminologin som är vanligast i de artiklar som knyter samman grafteori och nätverksteori.

Inom grafteorin brukar en graf beskrivas som $G = (V, E)$, där V är nodmängden $\{v_1, v_2, ..., v_n\}$ och E är kantmängden $\{e_1, e_2, ..., e_m\}$ (Bollobás, 1998). I artikeln av Strogatz

och Watts (Strogatz & Watts, 1998) beskriver n, antalet noder, och m, antalet kanter. I modellnätverket ovan är således n=10 och m=18. En kant som sammanbinder noden $v_1$och noden v_2 och kan då benämnas k_1. Således är v_1 och v_2 ändnoder till denna kant. Två kanter är sammanbundna om de har exakt en gemensam nod. En jämförelse med fotbollslaget ovan ger att spelare 10 och 11, $\{v_{10}, v_{11}\}$, sammanbinds av en kant, $k_{10\text{-}11}$, och att denna kant är sammanbunden med kant, $k_{9\text{-}10}$, mellan spelare 9 och 10, eftersom de har en gemensam nod, v_{10}.

Enligt Bollobás (1998) brukar en väg P anges $v_0, v_1, ..., v_l$, där v_0 och v_l är väg Ps ändnoder. Längden av P blir då $l = e(P)$, alltså antalet kanter mellan start- och slutnod. Vi benämner att P är en väg från v_0 till v_l, eller v_0- v_l. I en oriktad graf är betydelsen densamma om noderna betecknas tvärtom, v_l till v_0. Behövs däremot riktningen specificeras, benämns, t ex, v_0 startnod och v_l slutnod. Avståndet d(v_0,v_l) mellan två noder är längden på den kortaste vägen mellan dem, alltså hur många kanter är det som förbinder dessa noder. Avståndet mellan spelare 2 och spelare 9 i 3-5-2 systemet ovan, blir därmed $d(v_2, v_9) = 3$.

3.1.2 Grad

Grad beskriver hur många länkar som går till eller från en nod och kommer att betecknas som k_i. I modellen kan spelare nummer 5 väljas som exempel. Spelaren har möjlighet att passa eller bli passad av spelarna 3, 6, 7, 8, och 9. Detta betyder att noden 5s grad är $k_5 = 5$. Riktade nätverk skiljs på antalet in- och utgrader, alltså antalet inkommande och utgående länkar från noden.

För att beskriva en graf kan den genomsnittliga graden beräknas samt även gradfördelningen som anger den relativa frekvensen av noder med en viss grad. Den genomsnittliga graden beräknas enligt $\bar{k} = \frac{1}{n}\sum_{i=1}^{n} k_i$ (Bovin, 2003) och för vårat modellnätverk blir den genomsnittliga graden då $\bar{k} = \frac{1}{10}(2+3+3+5+5+4+4+6+2+2) = 3{,}6$.

3.1.3 Klustringskoefficient

Verkliga nätverk brukar innehålla grupper där flera noder är sammanlänkade med varandra. När flera av en nods grannar även är kopplade med varandra anses noden ha en hög klustringsgrad. För att finna ett mått på hur hög klustringsgrad en graf har, har en koefficient definierats, klustringskoeffecienten.

I figuren visas ett exempel på ett nätverk där det går att utläsa att individerna i lagdelarna alltid är sammankopplade. Däremot är inte alla spelare i olika lagdelar sammankopplade. Därmed kommer spelare 8 ha en högre lokal klustringskoefficient än spelare 5. Det kan visas genom att använda nedanstående formel (Bovin, 2003):

$$C_i = \frac{2E}{(k_i - 1)k_i}$$

Nodens grad k_i bestäms som beskrivet i kapitel 3.1.2, och E är hur många nodpar en nod är sammanlänkad med. Spelare 5 är sammanlänkad med spelare 3, 6, 7, 8 och 9. Spelare 3 kan inte bilda ett nodpar med någon av de övriga spelarna, men spelare 6, 7, 8 och 9 kan bilda sex olika nodpar. Således blir $E = 6$ för spelare 5 och $C_i = \frac{2 \cdot 6}{(5-1) \cdot 5} = 0{,}6$.

Klustringskoefficienten för spelare 8 blir på samma vis $C_i = \frac{2 \cdot 6}{(4-1) \cdot 4} = 1$. Spelare 8 har en högre klustringskoefficient eftersom alla dess grannar bildar nodpar.

Genom att beräkna medelvärdet på nodernas klustringskoefficient kan hela grafens klusternivå bestämmas. I vårt fall blir klustringskoefficienten för nätverket,

$$C = \frac{1}{n}\sum_{i=1}^{n} C_i = \frac{1}{10}(1{,}00 + 0{,}33 + 0{,}33 + 0{,}60 + 0{,}60 + 1{,}00 + 1{,}00 + 0{,}47 + 1{,}00 + 1{,}00) = 0{,}73.$$

Verkliga nätverk som uppvisar höga klustringskoefficienter är ofta sociala nätverk. Ett exempel är nätverket av skådespelare (se kap 2.1.1). Elnät däremot har vanligtvis låg klustringskoefficient. Detta beror på att elnätets topologi, med en ledning, länk, som leder mellan transformatorer, noder, inte får lika många sammankopplade grupper där en nods grannar också är grannar sinsemellan. Dock varierar värdet på klustringskoefficienten beroende på om undersökning görs på stam-, regional eller lokalanät.

3.1.4 Kortaste väg

För att beskriva strukturen på ett nätverk kan det kortaste vägen mellan ingående noder mätas. Eftersom den kortaste vägen varierar mellan vilka noder som undersöks, kan ett genomsnittsavstånd användas. Som exempel kan avståndet mellan spelare 3 och 9 i fotbollslaget ovan användas. Spelare 3 är sammanlänkad med spelare 5 som i sin tur är sammanlänkad med spelare 9. Således är det två länkar mellan dessa spelare och den kortaste vägen blir då givetvis 2. Genom att beräkna samtliga avstånd mellan nodpar i grafen kan det genomsnittliga avståndet, l, beräknas. För nätverket som beskriver fotbollsspelarna beräknas $l = 1{,}84$.

Om en graf inte är sammanhängande kan inte den kortaste vägen medelvärdesberäknas eftersom vägen mellan noderna kommer att vara oändlig. Detta problem kan lösas på två sätt. Antingen beräknas den inverterade kortaste vägen eller så beräknas vägar som tillhör samma komponent för sig. Vid beräkning av den inverterande kortaste vägen kan nedanstående formel användas (Holme & Kim, 2002)

$$l^{-1} = \frac{1}{N(N-1)} \sum_{v \in V} \sum_{w \neq v \in V} \frac{1}{d(v,w)}$$

där d är avståndet mellan de olika nodparen och N är antalet noder i nätverket. För fotbollslaget erhålls då den inverterad kortaste väg till 0,66.

3.1.5 Intermeditet

Intermediteten är ett begrepp som kan kopplas till sårbarhetsanalys. Genom att se hur de kortaste vägarna går genom grafen går det att upptäcka om det finns någon nod som är den kortaste vägen mellan många nodpar. Förenklat gör en sådan nod nätverket mer sårbart än övriga eftersom flera nodpars kontakter är beroende av just denna nod. Återgår vi till exemplet med fotbollsspelarna kan det utläsas att spelare 9 är viktig för att anfallsspelet ska fungera. Kommer denna spelare, nod, bort från spelet kommer inga passningar att nå de båda anfallarna.

3.1.6 Nätverksanalys

Begreppen presenterade tidigare kan användas för att beskriva topologin för ett nätverk. Detta medför möjlighet att finna de kortaste vägarna i nätverket, medelgrad osv. Dock beskriver

resultaten bara hur nätverket ser ut när det fungerar. För att se på sårbarheten i nätverket behöver nätverket analyseras på ett annat sätt. Analysen kan, till exempel, bestå av att kontrollera vad som händer om en godtycklig nod kopplas bort eller om den nod som har högst grad slåss ut. Nedan kommer olika attackstrategier för att se på sårbarheten i ett nätverk att presenteras.

3.1.6.1 Attackstrategier

I *Attack vulnerability of complex networks (2002)*, redovisar författarna Holme och Kim hur sårbart ett nätverk är när dess ingående komponenter attackeras. Vid simulering måste beslut tas om attackerna skall ske mot noder eller länkar, eftersom detta ger olika resultat. Slås en nod ut, slås samtidigt de länkar som leder till och från noden ut. Därmed försvinner all förbindelse med den aktuella noden. Samtidigt, med noden, försvinner de kortaste vägar som löpte genom noden. Skulle däremot en länk attackeras försvinner endast den aktuella förbindelsen. Noden kan, beroende på nodens grad och nätverkets topologi, fortfarande vara den kortaste vägen mellan andra nodpar.

3.2 Sårbarhet

I detta avsnitt diskuteras begreppet sårbarhet. Vidare presenteras sårbarhetsmodeller, dels av sårbarhetsanalys i offentlig sektor, dels en modell som redogör för hur en sårbarhetsanalys av ett amerikanskt elnät. Dessa modeller presenteras endast i syfte att ge läsaren ett exempel på en heltäckande sårbarhetsanalys, där analys med hjälp av verktyg hämtade från nätverks-teorien kan vara en del.

3.2.1 Definitioner

Det florerar en mängd olika definitioner på begreppet sårbarhet. Krisberedskapsmyndigheten (KBM), som är den myndighet som av regeringen fått ansvaret för bland annat informera och utbilda inom begreppet sårbarhet, definierar sårbarhet i publikationen *Risk och sårbarhetsanalyser - Vägledning till statliga myndigheter* (2003):

> ”Sårbarhet betecknar hur mycket och hur allvarligt ett system påverkas av en händelse. Graden av sårbarhet bestäms av förmågan att förutse, hantera, motstå och återhämta sig från händelsen.”

I en annan av KBMs publikationer *Kommunal sårbarhetsanalys* (2004) definieras sårbarhet som:

> ”En oförmåga hos ett objekt, system, individ, befolkningsgrupp, m.m. att stå emot och hantera en specifik påfrestning som kan härledas till inre eller yttre faktorer.”

Det finns också en mängd definitioner när sårbarhet är länkad till naturkatastrofer. Som exempel kan nämnas Timmermans (Abrahamsson och Magnusson 2004):

> ”Sårbarhet betecknar den omfattning med vilken ett system reagerar negativt på en exponering från en utlöst riskkälla. Omfattning och styrka av den negativa reaktionen bestäms av systemets motståndsförmåga (ett mått på systemets förmåga att absorbera och återhämta sig från påverkan efter händelsen).”

Vi anser att definitionen som presenteras ovan i KBMs risk och sårbarhetsanalyser – Vägledning till statliga myndigheter (2003), bäst speglar sårbarhet i nätverk.

3.2.2 Sårbarhetsanalys i offentliga sektorn

Sårbarhetsanalyser genomförs på olika nivåer och inom olika organisationer. Förekomsten samt vad sårbarhetsanalyser skall omfatta inom svenska myndigheter styrs av *Förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap*. Den myndighet som fått ansvaret att utbilda och utöva myndighet i fråga om sårbarhet är Krisberedskapsmyndigheten (KBM). I *Förordning (2002:518) med instruktion för Krisberedskapsmyndigheten §4* kan man läsa **"**Krisberedskapsmyndigheten skall sprida kunskap om och stärka samhällets krishanteringsförmåga genom att särskilt samordna kompetensutveckling samt informera och utbilda inom områdena samhällets sårbarhet, krishantering, säkerhetspolitik och totalförsvar."

Sårbarhetsanalys är en förhållandevis ny företeelse och inte många analysmetoder är framtagna, dock har KBM givit ut viss vägledning. I *Risk och sårbarhetsanalyser - Vägledning till statliga myndigheter* (2003) konstaterar KBM att det förekommer stora skillnader mellan risk och sårbarhetsanalysen. Bland annat fokuseras riskanalysen på de fel som kan uppkomma inom ett system (anläggning/verksamhet) och de konsekvenser som kan ske i direkt anslutning till dessa fel medan sårbarhetsanalysen tar en vidare fokusering, även utanför systemet. Sårbarhetsanalysen fokuserar också i högre grad på att minska konsekvenserna och stärka förmågan vid en olyckshändelse eller kris. KBM konstaterar också att sårbarhetsanalysen intar ett mycket längre tidsperspektiv i förhållande till riskanalysen och behandlar förloppet från olycka till dess ett nytt stabilt tillstånd uppnåtts. Risk- och sårbarhetsanalysen skall ses som komplement till varandra, där riskanalysen bör fokuserar på orsaken till att situationen uppstår och sårbarhetsanalysen bör fokusera på de samhälleliga konsekvenserna. I samma publikation slås det fast att analyserna bör omfatta sex steg:

1. Vad kan hända?
2. Varför kan det inträffa och hur ofta?
3. Vilka blir konsekvenserna för samhället?
4. Vad kan förebyggas?
5. Hur kan sårbarheten minskas?
6. Sammanställning av resultaten.

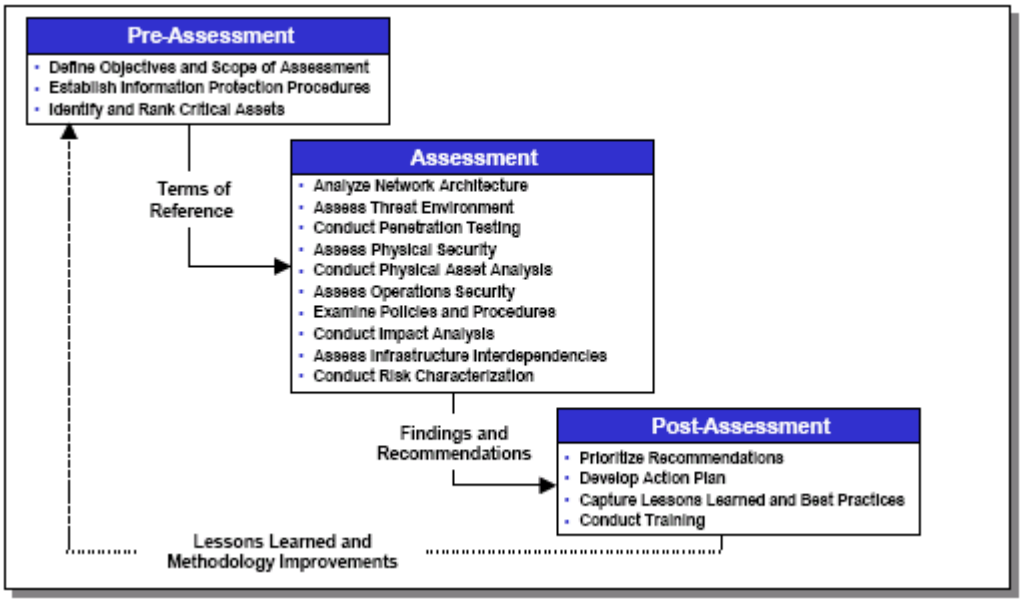
I boken *Kommunal sårbarhetsanalys* stärker författarna uppfattningen om att riskanalysen fokuserar på riskkällan medan sårbarhetsanalysen fokuserar på det skyddsvärda systemet. I denna publikation presenteras en något annorlunda innehåll av sårbarhetsanalys i fem steg:

1. Definiera/fastställa det skyddsvärda och göra avgränsningar i system, rum och tid.
2. Identifiera riskkällor, oönskade situationer och händelser och på vilket sätt dessa kan skada det skyddsvärda.
3. Inventera och kartlägga krishanteringsförmågan.
4. Analysera krishanteringsförmågan i relation till de oönskade händelserna/ situationerna.
5. Diskutera sårbarhetsreducerande åtgärder.

De två ovanstående modellerna på hur sårbarhetsanalys bör/kan genomföras är övergripande och kan tillämpas inom vitt skilda områden. En mer specifik modell för sårbarhetsanalys av elnätverk är utvecklad av U.S. Department of Energy Office of Energy Assurance och beskrivs nedan.

3.2.3 Sårbarhetsanalys av elnätverk

U.S. Department of Energy Office of Energy Assurance redogör för en sårbarhetsanalysmodell i rapporten *Vulnerability Assessment methodology, Electric Power Infrastructure* (2002). Denna modell är indelad i tre skeden; föranalys (Pre-Assessment), analys (Assessment) och efteranalys (Post-Assessment). (Jfr figur 3.2.3).



Figur 3.2.3-1 Sårbarhetsanalysens faser. Bilden hämtad från *Vulnerability Assessment methodology, Electric Power Infrastructure* (2002).

3.2.3.1 Föranalysskedet

Detta skede syftar till att säkerställa att analysen blir så effektiv som möjligt. De uppgifter som ingår i föranalysen är att definiera omfattningen och syftet med analysen, etablera rutiner för informationssäkerheten samt identifiering och värdering av kritiska tillgångar. Arbetet med att definiera omfattningen och syftet kan jämföras med arbetet med att kapitel 1, inledning, i ett vetenskapligt arbete typ detta arbete, vilket innebär:

- att sätta upp mål/problemställning för analysen
- fastställa de metoder som sårbarhetsanalysen kommer att genomföras med
- säkerställa kompetens i form av nyckelpersoner
- säkerställa att rätt information och resurser i övrigt finns att tillgå vid analysarbetet.
- Utarbetande av arbetsplan
- fastställande av vilken typ av analys som skall genomföras. Dessa typer är:

    - **Intern** Sårbarhetsanalysen genomförs av egen personal (expertis) som ofta har fördelen av att känna till organisationen, teknologin, policys och företagsvisioner.
    - **Lednings** Sårbarhetsanalysen genomförs med egen personal men med stöd av utifrån hämtad ledning (t ex konsulter) som förser analysgruppen med ledning och metoder. Personalen kan då koncentrera sig på sin expertis.
    - **Extern** Sårbarhetsanalysen genomförs av extern grupp eller expert. Fördelen med denna typ är att analysen ofta genomförs mer objektivt

än vid t ex en intern. Ofta ökar trovärdigheten av de resultat som analysen kommer fram till.

- **Hybrid** Arbetsuppgifter delas mellan egen personal och utomstående personal, så till vida att vissa uppgifter löses av egen och andra uppgifter löses av utomstående personal.

Arbetet med att identifiera och värdera företagets kritiska tillgångar syftar primärt till att fokusera sårbarhetsanalysen mot de tillgångar som är mest kritiska för företaget. I rapporten betonas vikten av att värderingen (prioriteringen) skall vara allmänt hållen d v s företrädesvis skall alltså värderingen göras genom att analysera helheten i företaget och inte göras verksamhet för verksamhet. Exempel på kritiska tillgångar vid en elkraftsstruktur är:

Fysiskstruktur

- Generatorer
- Understationer
- Transformatorer
- Ledningar
- Övervakningscentraler
- Lager (för t ex utrustning och reservdelar)
- Kontor

IT

- Nätverk
- Databaser
- Affärssystem (t ex försäljning, bokföring mm)
- Telekommunikation

3.2.3.2 Analysskedet

Analysskedet indelas, som synes i figur 3.2.3, i tio punkter:

1. Nätverksstruktur
2. Hotmiljön
3. Penetrationstest
4. Fysiska säkerhetssystem
5. Analys av anläggningstillgångar
6. Produktionssäkerhet
7. Policys och instruktioner
8. Påverkansanalys
9. Infrastruktursberoende
10. Riskvärdering

1 Nätverksstruktur

Under denna punkt analyseras informationssäkerheten i informationsnätverk. De delar som bör ingå i denna typ av analys är nätverks topologi och sammanlänkning, huvudsaklig informations tillgång, samverkans och kommunikations regler, funktion och sammanlänkning av de viktigaste mjuk- och hårdvarorna samt policys och instruktioner som styr säkerheten i nätverk.

I rapporten lyfts tre tekniker att göra sårbarhetsanalysen av nätverksstrukturen fram, nämligen:

1. Analys av nätverks- och systemdokumentation i samband med och efter platsbesök.
2. Intervjua anläggningspersonal, ledning och informationschef, samt
3. Besök och inspektion av nyckelanläggningar.

2 Hotmiljön

Terroristhotet mot elnät kan bestå av hot om angrepp från flera olika håll, bland annat fysiska angrepp eller över datakommunikation i form av t ex virus. Hot kan även komma från individer eller organisationer som drivs av vinstintressen eller tillfredsställelsen av att åsamka skada (t ex hackers). I detta skede ingår att karaktärisering av dessa och andra hot, identifiering av trender samt identifiering av vilka sätt dessa hot gör företaget sårbart.

3 Penetrationstest

Syftet med arbetet är att kartlägga sårbarheten vid intrång i nätverk. Förmågan att möta hot om intrång testas genom att man upprättar en testplan och en strategi för testet. Testet skall omfatta kartläggning av anslutningspunkter till IT-system och kommunikationssystem, modem nätverksanslutningar, anslutningspunkter till servrar (routers) och andra externa anslutningar. Slutligen skall penetrationstesten identifiera sårbarhet särskilt om det finns möjlighet att utifrån skaffa sig kontroll över nätet.
Metoden, med vilken testen genomförs, indelas i tre faser: Sondering, utarbetande av scenarion samt bearbetning.

4 Fysiska säkerhetssystem

Syftet med denna fas är att undersöka och utvärdera de säkerhetssystem som redan finns installerade, eller som man planerar att installera. System som skall ingå är system för inpasserings kontroll, stängsel, lås och nycklar, identitets- och passerkort, detektionsutrustning med tillhörande manöverapparater, TV- övervakning, kommunikationsutrustning mm.

5 Analys av anläggningstillgångar

Syftet är att analysera sina anläggningstillgångar för att utröna huruvida de innehåller några sårbara delar. Detta görs genom att titta på egna data, data utifrån eller en kombination av dessa. De resultat som framkommer av analysen bör innehålla grafer som visar trender. Vid anläggningsbesök bör fokuseringen ligga på punkterna:

- Trender inom olika personalkategorier
- Trender inom underhållsutgifter
- Trender inom infrastrukturs investeringar
- Avbrottsstatistik
- Gränssättande systemkomponenter och potentiella flaskhalsar i systemen.
- Övergripande produktionssystem
- Användningen och beroendet av övervakningkontroll och data inhämtningssystem
- Sammanlänkningen mellan produktionspersonalen och fysiska- och IT säkerhetssytem
- Adekvata policys och instruktioner
- Kommunikationen mellan andra anläggningar
- Kommunikationen till andra företag
- Adekvat organisationsstruktur

6 Informationssäkerhet
Denna punkt analyserar möjligheten för konkurrenter att få tillgång till företagshemligheter, så som t ex kapacitet, inriktningar. Analysen bör innehålla en granskning av säkerhets-utbildningen, utbildning som gör de anställda mer uppmärksam och deltagande, intervjuer av nyckelpersoner samt besök av viktiga anläggningar.

7 Policys och instruktioner
Målet med analysen av policy och instruktionerna är att medvetandegöra hur utarbetandet och implementeringen av ny policys och instruktioner (riktlinjer) medverkar till att skydda en anläggnings viktiga tillgångar. Moment som bör analyseras under denna punkt är:

- Modifiering av nuvarande policy och instruktion.
- Implementeringen av nuvarande policy och instruktion.
- Framtagande och implementering av ny policy och instruktion.
- Acceptans av policys och instruktion.
- Borttagning av policy och instruktion som ej längre är relevant, eller som inte passar in i anläggningens strategi och produktion.

8 Påverkansanalys
Syftet med denna punkt är att analysera vilka konsekvenser ett avbrott skulle få på en ingående del av verksamheten. Exempel på avbrott kan vara elavbrott, avbrott på naturgasledning mm. En detaljerad analys skall bestämma hur en verksamhets produktion påverkas av ett intrång vid en viktig anläggning eller informationssystem.

9 Infrastruktursberoende
Syftet med denna analys är att undersöka och utvärdera den infrastruktur som stödjer viktiga anläggningar, både ur beroende och ur sårbarhetsperspektiv. Exempel på infrastruktur är energi (el, olja, naturgas), telenät, vägnät, vattennät mm.

10 Riskvärdering
Riskvärdering fungerar som ett ramverk vid prioriteringar av åtgärder över hela uppgiftsområdet. Föreslagna åtgärder från varje delområde jämförs mot de kriterier som ställts upp. Syftet är att underlätta för prioriteringar och för att ge organisationen stöd vid beslut om inriktning.

3.2.3.3 Efteranalys

Efteranalysfasen består av prioritering av åtgärder, framtagande av handlingsprogram, tillvaratagande av lärdomar och strategier samt genomförande av träning. Grunden för denna fas bygger på de slutsatser som framkom vid riskvärderingen.

3.2.4 Sårbarhet i nätverksstrukturer

Albert, Albert och Nakarado beskriver en metod för att analysera sårbarheten i nätverk i artikeln *Structural vulnerability of the North American power grid* (2004). De baserade sin studie på 115-765 kV delen i det nordamerikanska elnätet, som bestod av 14 099 noder och 19 657 länkar. Författarna gör i sitt arbete en förenkling som består i att man räknar med att en nod har full ström om det finns en väg mellan den och en källnod. Med källnod menas den nod varifrån strömmen utgår. De bortser alltså från att olika noder kan ha olika kapacitets och/eller andra begränsningar. Den metod de lägger fram inleds med att nodernas gradfördelning bestäms. Därefter analyseras intermediteten och genomsökning av extra sårbara noder som vid utslagning skulle koppla bort delar av näten (bilda nät som ej är

anslutna till någon källnod). Författarna introducerar även ett begrepp benämnt ”förlorad kontakt” (connectivity loss, C_L). Värdet på detta begrepp framräknas med hjälp av formeln,

$$C_L = 1 - \left\langle \frac{N_g^i}{N_g} \right\rangle_i$$

och mäter den minskade möjligheten för transformator att erhålla strömmen från källnoderna. Simuleringar görs sedan för att mäta ”förlorad kontakt”. Dessa simuleringar genomförs dels som riktade och dels som slumpmässiga attacker.

Det nät som Albert et. Al. (2004) beskriver i sin artikel, kan inte jämställas med det nät som denna rapport bygger på. Om man skulle jämställa det amerikanska elnätet med det svenska skulle förmodligen denna rapports elnät ta vid där det amerikanska elnätet slutar.

4 Beskrivning av studien

4.1 Nätet

Det nät som använts i detta arbete är ett av Sydkrafts elnät som finns i ett område i södra Sverige. Nätet är ett lokalnät med en ström på 10 eller 20 kilovolt. Nätet matas av sex stycken stationer som transformerar ner strömmen och distribuerar ut den i nätet. Varje station har i sin tur delats in i fack som distribuerar el ut i en mängd små nät. Den största stationen är uppdelad i tio fack och den som är minst i två, snittet är sju fack per station. Syftet med denna indelning till mindre nät är att en kortslutning inte skall slå ut hela nätet utan endast ett mindre nät, det vill säga så få abonnenter skall drabbas som möjligt. Möjlighet finns att koppla ihop alla dessa små nät till större nät med hjälp av frånskiljare. Denna möjlighet utnyttjas framförallt för skadebegränsande åtgärder vid ett eventuellt fel på nätet genom att koppla bort nätet så nära felet som möjligt. Varje litet nät innehåller, förutom frånskiljare, även förgreningar och transformatorer. Till dessa transformatorer är det kopplat allt mellan en till två hundra abonnenter.

Nätet innehåller både luft och markledningar. Fyra av stationerna är uppbyggd i huvudsak på markledning, beroende på att näten ligger i stadsbebyggelse, medan de övriga näten, som följaktligen i huvudsak är uppbyggd på luftledning, i huvudsak ligger i jordbrukslandskap. En motsvarande uppdelning är gjord av transformatorerna.

4.1.1 Simuleringsnät

Alla stationsnät har kopplats till enda nät som benämns SDS. Detta omfattar 961 och 1017 länkar. Som redogjorts ovan har detta nät en blandning av luft- och markledningar.

FKN är det minsta stationsnätet. Det har endast 44 noder som förbinds med 49 länkar. Detta nät består uteslutande av markledningar.

Station FVK levererar ström till 54 noder via 55 länkar och består nästan uteslutande av markledningar.

SFP omfattar 136 noder och 140 länkar. Nätet består av ungefär lika stor andel luft- och markledningar.

SNR består är en sammanslagning av två stationer SNR och SNRV, men då SNRV endast består av 4 noder har dessa nät, i simuleringen, slagits ihop till ett stationsnät. Nätet består av 53 noder och 62 länkar vilka alla är markledningar.

SLA omfattar 224 noder och 238 länkar och är därmed det näst störst stationsnätet. Ledningarna är både dragna i luften och i marken.

VEE är det största stationsnätet och innehåller 451 noder och 469 länkar. VEE består till nästan 2/3 av luftledning. Detta trots att nätet omfattar den största tätorten i området.

4.2 Simuleringsunderlag

En kartläggning av nätet genomfördes på så sätt att noder definierades som stationer, transformatorer, förgreningar och frånskiljare samt länkar mellan dem. Kartläggningen kompletterades med uppgifter om antal abonnenter, hur noden var beskaffad t ex om noden

var i en stolpe eller på marken samt huruvida länken är luft eller markburen. Kartläggningen sammanställdes i ett exceldokument (se bilaga 1) som sedan låg till grund för de matriser som användes vid simuleringen. Totalt kartlades 961 noder, 1017 länkar och 21752 abonnenter.

Från sammanställningsdokumentet skapades flera *n*x*n* kontaktmatriser, däribland en matris över hela nätet där alla stationer ingick, en matris bestående av två stationer (SNR och SNRV). De övriga matriserna bestod av ett stationsnät vardera. En kontaktmatris, *n*x*n*, karaktäriseras av att varje rad och varje kolumn representeras av en nod. En länk som förbinder två noder markeras med siffran 1 i matrisen, t ex om nod *i* och nod *j* står i förbindelse med varandra noteras det med en 1 i element a_{ij}. Om noder inte står i förbindelse med varann noteras det med siffran 0.

4.3 Datorprogram

I detta arbete har tre datorprogram använts, Microsoft Excel, Netdraw och NetCalc.

Microsoft Excel är ett kalkyleringsprogram som lämpar sig väl när stora mängder data skall organiseras. Programmet användes i detta arbete dels vid sammanställningen av kartläggningen av nätverket och dels när resultaten av simuleringarna skulle presenteras. Vid sammanställningen gavs varje nod en egen rad på vilken dess attribut sammanställdes. De attribut som noterades var nodens namn, nodens tillhörighet (vilken station och fack), vilka typer av objekt (station, transformator, förgrening, frånskiljare, stolpe), vilken typ av länk (luft- eller markledning), hur många abonnenter samt vilka andra noder noden stod i kontakt med. För att kunna presentera resultaten av simuleringarna på ett överskådligt sätt användes Excel och då framför allt möjligheten att skapa diagram.

Netdraw är ett program framtaget av Analytic Technologies för att visualisera nätverk. Detta program har följaktligen använts för att skapa en visualiserad bild på hur nätverket ser ut. Programmet har en mängd olika funktioner och möjligheter för visualisering, bland annat finns möjlighet att åskådliggöra noders olika attribut med hjälp av storlekar och färger. Erfarenheten visar dock att bildskärmens storlek är den komponent som sätter begränsningen vid visualiseringen av stora nätverk.

NetworkCalc är ett program som är framtaget av Dr Henrik Johansson vid avdelningen för brandteknik, Lunds tekniska högskola. Programmet har använts till att skapa kontaktmatris utifrån ett exceldokument, beräkning av klusterkoefficient, medelgrad, medel inverterad längd, samtliga noders grad samt simulering av attacker. Programmet erbjuder två olika typer av analys; analys av inverterade längden och sammanlänkningsanalys samt två olika attackstrategier; slumpmässig eller högsta grad. Attacker kan antingen ske mot noder eller mot länkar. Analys av inverterade längden är mycket beräkningskrävande och ställer följaktligen mycket stora krav på processorerna vid simulering av stora nätverk. Varför den inverterade längden beräknas och inte den kortaste vägen beror på att vid simuleringarna kan stora delar av nätet tappas tidigt vilket skulle innebära att nätet skulle delas upp i mindre komponenter utan kontakt med varandra. Simulering av hur den inverterade längden förändras vid attacker på nätverket visar hur avstånden mellan noder i nätverket förändras. De resultat som erhålls vid simulering är:

- när enskilda noder tappar kontakten med källnod, med källnod menas den nod varifrån strömmen utgår. I dessa simuleringar är de olika stationerna källnoder.
- hur den inverterade längden förändras när noder plockas bort.
- utslagningssekvens av noder.

Till dessa noder kan sedan kopplas olika attribut, så som t ex abonnenter. Dessa beräknas kumulativt så att resultat av utslagning presenteras som tappade abonnenter per utslagen nod. På detta sätt kan resultatet av olika sekvenser studeras och beräkning av sårbaraste nät fastställas.

4.4 Simulering

De simuleringar som har gjorts bygger på två tänkta scenarier. Det ena scenariot studerar effekterna av en terrorhandling och den andra relaterar mer till vardagliga funktionsbortfall, beroende på, till exempel, en storm. Dessutom tillkom simuleringar som syftade till att studera antalet källnoder betydelse för nätets robusthet samt simuleringar för känslighets-analys

4.4.1 Terror

I detta scenario har det förutsatts att en terrorist har som mål att med sin handling lamslå hela eller delar av samhället. För att handlingen skall bli så effektiv som möjligt, i terroristens ögon, kommer han/hon att slå mot de noder som har flest förbindelser. Alltså de noder som har högst grad. Dessa noder skulle kunna vara stora stationer eller transformatorer där det är enkelt att förstå att effekten blir stor. Sådana stationer skulle kunna kännetecknas av att de antingen är svåra att tillträda, genom att där finns höga staket och/eller kraftiga lås, bevakning i form av vaktbolag eller att området är kameraövervakat. En annan karakteristika, på en nod med många förbindelser, är att det visuellt går att avgöra att många ledningar leder till och från platsen. En terrorist strävar sannolikt att få så stor effekt av så få handlingar som möjligt, då hans möjligheter att lyckas minskar markant med tiden efter den utlösande händelsen beroende på att samhället kan mobilisera motåtgärder.

4.4.2 ”Vardagligt bortfall”

Ett elnät, likt andra tekniska system, kommer å ena sidan alltid att påverkas av yttre faktorer, såsom väder och vind. Vid till exempel en storm kan vissa stolpar komma att falla vid, till synes, låga vidhastigheter och andra stolpar kommer att stå kvar även vid höga. Detta kan förklaras med ojämn kvalité på ledningsstolpar, dåligt underhåll av ledningsgator etc. Om inte stormen är alltför omfattande kan denna utslagning till synes ske slumpvis. Å andra sidan går det sannolikt att förutse de platser, stråk och delar i nätet som är mer sårbara än andra. Till exempel är luftledning troligen mer sårbar än markledning och att en luftledning är mer sårbar i en skog än ute på en åker. För att testa dessa påfrestningar på näten i undersökningen simuleras slumpvis utslagning av länkar respektive slumpvis utslagning noder. Syftet med dessa simuleringar är att undersöka hur strukturen på nätet påverkas av de vardagliga bortfall som presenterats ovan.

4.4.3 Simuleringsmoment

Utifrån ovanstående scenarier har en simuleringsmomentbeskrivning tagits fram, vilken presenteras nedan. Simuleringsbeskrivningen utgår från de olika inställningar som kan göras i Netcalc och syftar till att underlätta för den som vill kontrollera resultaten i simuleringarna. På grund av att simuleringarna producerar en mängd data i kombination med att Excel har begränsningar i hur många rader som kan hanteras, kommer de simuleringsmoment som simuleras 1000 gånger att delas upp i fyra stycken simuleringar á 250 gånger.

En analys av de olika näten kommer också att göras. Denna analys kommer att omfatta antal noder och länkar, medelgrad, fördelning av medelgrad, inverterad längd (medelvärde) samt klustringskoefficient.

1 Sammanlänkningsanalys, antal simuleringar: 1000, simuleringsstrategi: Högst grad, mål: noder, nät: SDS

2 Sammanlänkningsanalys, antal simuleringar: 1000, simuleringsstrategi: högst grad, mål: noder, nät: stationsnät, a)VEE, b)FVK, c)SNR, d)SLA, e)FKN, f)SFP

3 Analys av inverterad längd, antal simuleringar: 10, simuleringsstrategi: högst grad, mål: noder, nät: stationsnät, a)VEE, b)FVK, c)SNR, d)SLA, e)FKN, f)SFP

4 Sammanlänkningsanalys, antal simuleringar: 1000, simuleringsstrategi: slumpvis, mål: noder, nät: SDS

5 Sammanlänkningsanalys, antal simuleringar: 1000, simuleringsstrategi: slumpvis, mål: länkar, nät: SDS

6 Sammanlänkningsanalys, antal simuleringar: 1000, simuleringsstrategi: slumpvis, mål: noder, nät: stationsnät, a)VEE, b)FVK, c)SNR, d)SLA, e)FKN, f)SFP

7 Sammanlänkningsanalys, antal simuleringar: 1000, simuleringsstrategi: slumpvis, mål: länkar, nät: stationsnät, a)VEE, b)FVK, c)SNR, d)SLA, e)FKN, f)SFP

8 Analys av inverterad längd, antal simuleringar: 10, simuleringsstrategi: slumpvis, mål: noder, nät: stationsnät, a)VEE, b)FVK, c)SNR, d)SLA, e)FKN, f)SFP

5 Resultat

I detta kapitel kommer de resultat som erhölls vid simuleringarna av attacker mot studerat nätverk att presenteras.

5.1 Resultat av nätanalys

Vid analys av de olika näten erhölls resultat som beskriver de olika nätens utseenden.

Nät	Antal noder	Antal länkar	Medelvärde av nodgrad	Inventerad längd	Klustrings-koefficient
SDS	961	1071	2,12	0,035	0,00173
FKN	44	49	2,27	0,256	0
FVK	54	55	2,04	0,183	0
SFP	136	140	2,06	0,114	0
SLA	224	238	2,13	0,095	0
SNR	53	62	2,34	0,244	0
VEE	451	469	2,08	0,065	0,00370

Tabell 5-1 Analys av nät.

I ovanstående tabell är hela nätet redovisat som SDS. De övriga näten är olika stationsnät som ingår i SDS. Av tabellen går det att utläsa att VEE utgör nästan 50 % av de noder som ingår i SDS. Detta näts uppbyggnad kommer därmed att spela stor roll för hela nätets robusthet. Medelvärde av nodgrad sprider sig från, 2,04 för FVK, till, 2,34 för SNR. Detta betyder att alla nät har en väldigt lik nodgrad. Inverterad längd skiljer sig däremot mer mellan de olika näten. Vid en jämförelse visar det sig att desto fler noder ger ett lägre värde på inverterad längd. Klustringskoefficienten för elnätet, SDS, beräknas till 0,00173 enligt NetCalc. Detta värde är lägre än det som erhölls vid studie av ett elnät i USA. Detta amerikanska elnät hade enligt Watts en klustringskoefficient av 0,080 (Watts, 2004). Vad denna skillnad beror på är svår att avgöra då ingen information finns om hur detta amerikanska elnät är uppbyggt.

Nät\Grader	1	2	3	4	5	6	7	8	9	10
SDS	211	477	240	25	4	1	0	1	1	1
FKN	5	30	6	1	1	0	0	1	0	0
FVK	13	28	11	2	0	0	0	0	0	0
SFP	28	76	28	4	0	0	0	0	0	0
SLA	40	118	59	4	0	1	0	0	0	0
SNR	6	32	8	5	2	0	0	0	0	0
VEE	119	193	128	9	1	0	0	1	0	0

Tabell 5-2 Sammanställning av gradfördelning i nät.

I ovanstående tabell redovisas den gradfördelning som de olika näten har. Fördelningen har en tyngdpunkt mot de lägre nodgraderna, där nodgraderna 1, 2 och 3 står för drygt 97 % av alla noder. SDS borde vara summan av de övriga noderna men eftersom vissa länkar tillkommer för att sammanknyta de olika näten, ökar graden för vissa noder.

Nätet visar inga tecken på att vara skalfritt. Anledningen till detta är sannolikt att det undersökta nätverket är för litet.

5.2 Simulering

5.2.1 Simuleringsmoment 1

Denna simulering genomfördes på hela nätet genom att de noder med högst grad angreps först. Simuleringen indelas i två moment, dels ett där källnoderna inte fick slås ut och ett där de fick slås ut. Dessa två moment motiveras med antagandet att alla abonnenter tidigt kommer att tappa strömmen då källnoderna naturligt är de noder med högst grad och därför kommer att slås ut först.

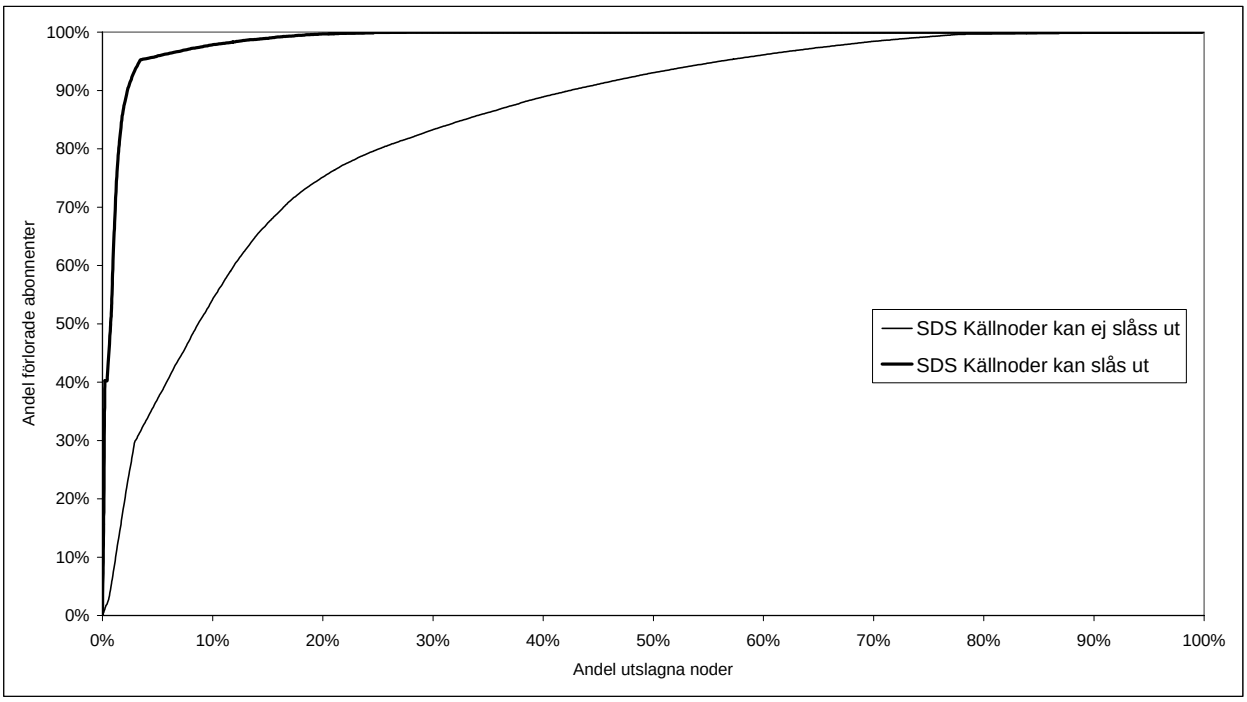


Diagram 5.2-1 Simuleringsmoment 1, noder med högst grad attackeras först, medelvärde av 1000 simuleringar

Diagrammet ovan visar andelen förlorade abonnenter som funktion av andelen utslagna noder. Kurvorna visar ett medelvärde av 1000 simuleringar. Det ovan angivna antagandet verifieras i diagrammet genom att samtliga abonnenter förlorats när endast en femtedel av noderna slagits ut, om källnoderna tillåts attackeras. Om källnoderna ej tillåts att attackeras förloras samtliga abonnenter först när nästan fyra femtedelar av noderna slagits ut. Kurvan, när källnoder ej tillåts slås ut, kan indelas i tre delar. Dels går det att konstatera att 30 % av abonnenterna förlorats när endast 3 % av noder slagits ut, dels att kurvan efter detta får en något flackare utseende mellan 3 till 20 % där ytterligare 45 % av abonnenterna förloras. I det sista stadiet planar kurvan ytterligare och för att förlora den sista fjärdedelen av abonnenterna krävs det att nästan 80 % av noder slås ut.

Denna simulering anser vi visa konsekvensen av att låta källnoderna slås ut. Vid samtliga simuleringar hädanefter kommer källnoderna inte tillåtas slås ut.

5.2.2 Simuleringsmoment 2

I detta moment genomförs samma simulering som i moment 1, det vill säga de noder med högst grad slås ut först, med den skillnaden att simuleringarna genomförs med stationsnätens data som underlag.

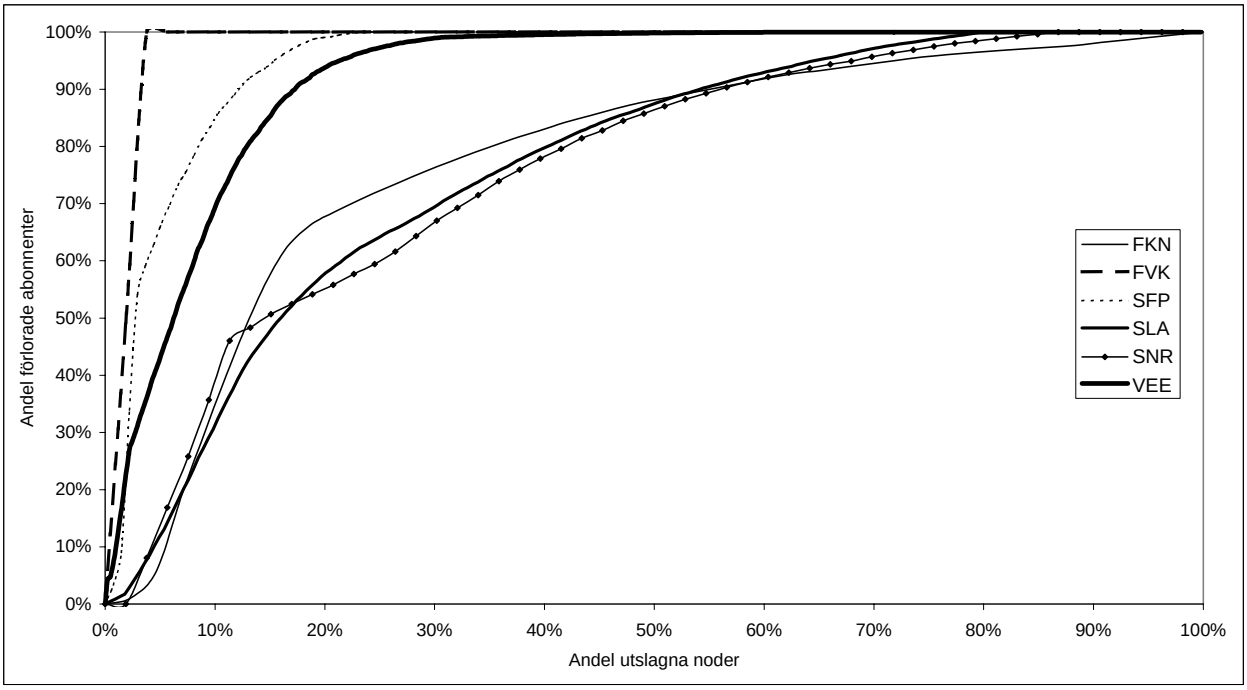


Diagram 5.2-2 Simuleringsmoment 2, medelvärde av 1000 simuleringar där noder med högst grad attackeras först.

I diagrammet ovan presenteras ett medelvärde av de resultat som erhölls vid simuleringsmoment 2. Stationsnäten kan här indelas i två huvudgrupper, dels de nät som vid relativ låg utslagning av noder tappar alla abonnenter. Dessa nät representeras av FVK, SFP och VEE. Den andra huvudgruppen består av FKN, SLA samt SNR och denna grupp karaktäriseras av att när 75 % av alla noder slagits ut har nätet fortfarande abonnenter kvar. Det nät som klarar flest antal utslagna noder är FKN och det nät som slås ut först är FVK, som tappar alla sina abonnenter redan när endast 6 % av noderna slagits ut.

Station	Nod	Sårbara objekt
FKN	T 026	Daghem
FVK	T 388, T 352	
SFP	T 328	
SLA	T 016, T 336	Daghem
SNR	T 022, T009, T015, T 019	Lantbruk, daghem, flerbostadshus direktverkande eluppvärmning, mindre industri
VEE	T 024	Lantbruk, daghem

Tabell 5-3 Tabell över sårbara objekt som slås ut först

I tabellen ovan beskrivs de konsekvenser, i form av utslagna objekt som kan antas vara viktiga för samhället, som uppkommer efter det att första noden slagits ut. I näten FVK, SLA,

SNR, VEE är det flera noder med samma höga gradtal vilket innebär att någon av de beskrivna noderna kommer att slås ut först. Som kan utläsas blir konsekvensen störst vid attack mot SNR där bl a lantbruk, mindre industrier daghem eller flerbostadshus som värms med direktverkande el kan komma att slås ut. De noder som kommer att slås ut först vid attack mot noder med högst grad i näten FVK och SFP saknar för samhället viktiga objekt.

5.2.3 Simuleringsmoment 3

Simuleringen undersöker hur längden på vägarna mellan noderna förändras då de noder med högst grad plockas bort. Syftet med simuleringen är att se hur nätet reagerar i jämförelse med om noder borttages slumpvis. Denna simulering görs i simuleringsmoment 8.

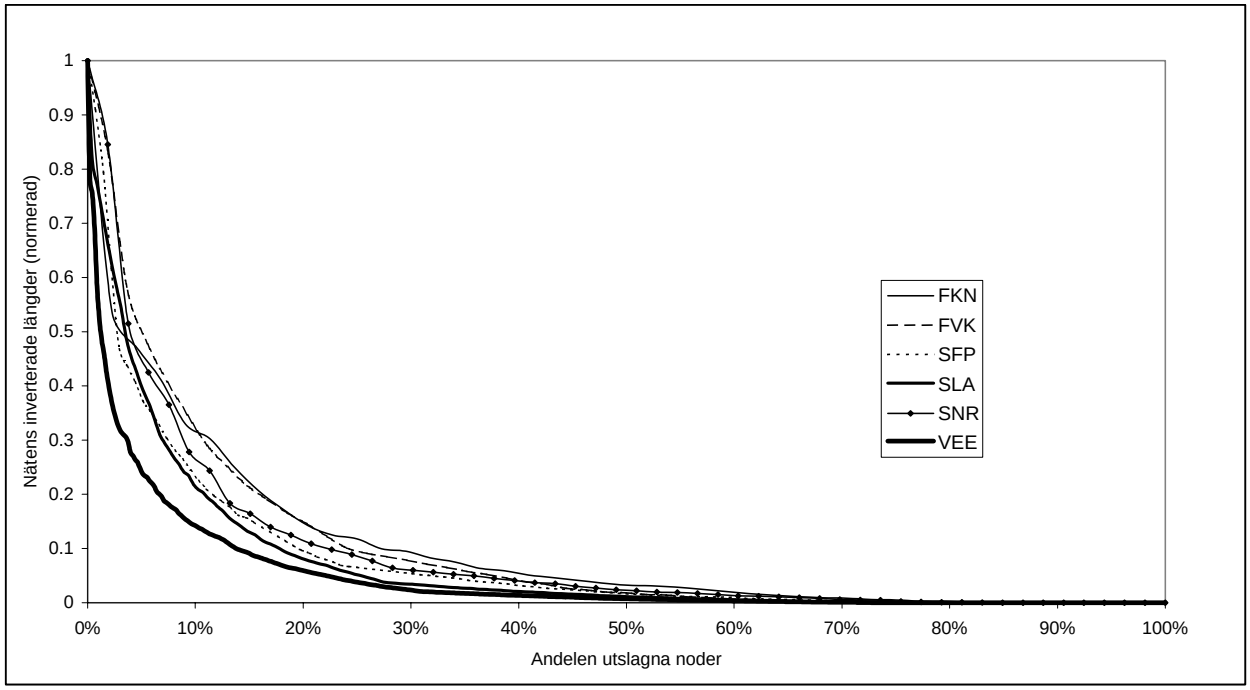


Diagram 5.2-3 Simuleringsmoment 3, beskriver hur den inverterade längden förändras när noder med högst grad attackeras.

Det ovanstående digrammet visar att även få utslagna noder ger snabbt påtaglig förändring. Det kännetecknas av att kurvan inledningsvis erhåller en brant lutning. Därefter planar kurvorna ut för att i det närmaste följa x-axeln. Det som även kan observeras är att de mindre näten erhåller högst värde och de största näten lägre. Skillnaden är dock liten.

5.2.4 Simuleringsmoment 4

Simuleringen visar hur nätet, SDS, reagerar när noder borttages slumpvis.

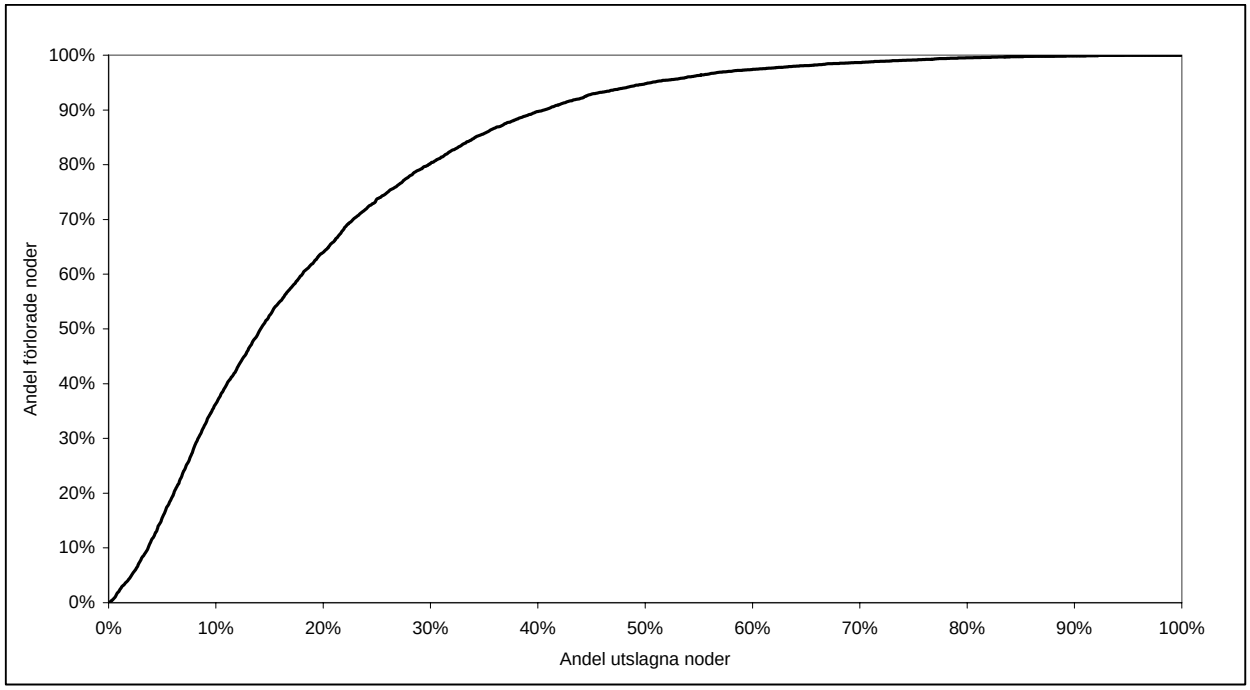


Diagram 5.2-4 Simuleringsmoment 4, slumpvis borttagning av noder.

Diagrammet ovan visar hur samtliga abonnenter har tappats när 80 % av alla noder har slagits ut. När endast 15 % av noderna är utslaget har kontakten tappats med hälften av nätets abonnenter.

5.2.5 Simuleringsmoment 5

Denna simulering är snarlik simuleringen i moment 4 med skillnaden att målen för dessa attacker är länkar och inte noder.

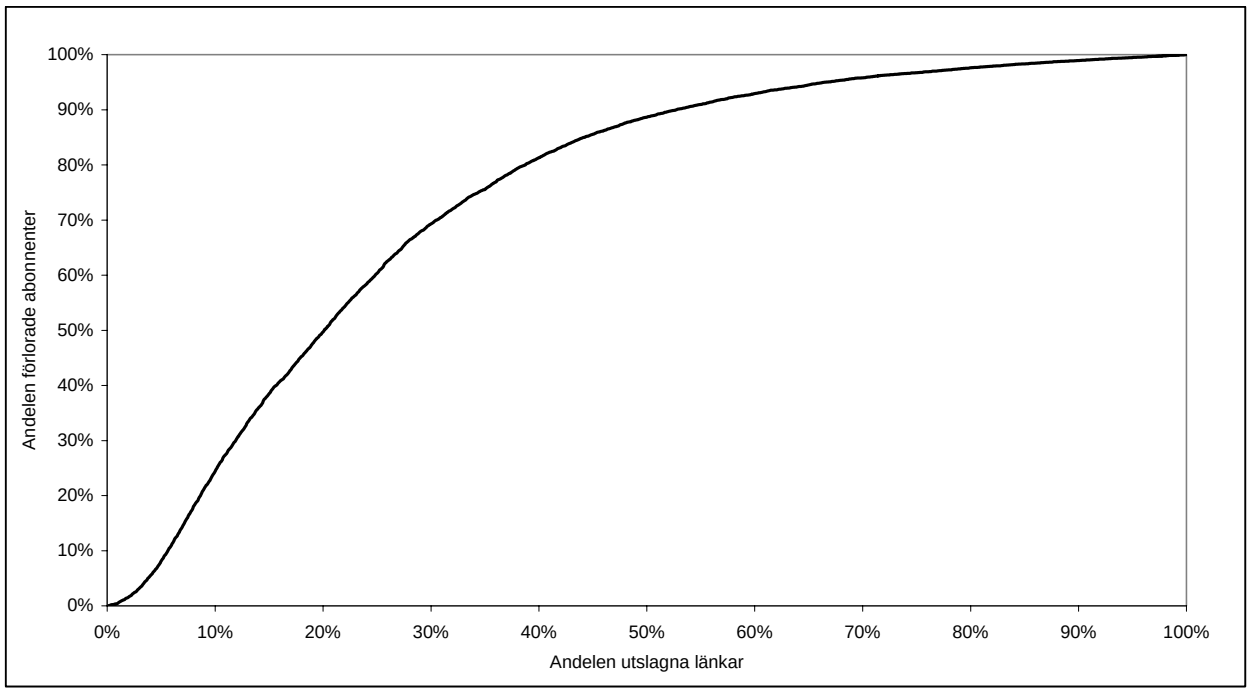


Diagram 5.2-5 Simuleringsmoment 5, slumpvis utslagning av länkar

Diagrammet ovan visar att kurvans lutning marginellt avviker från den kurva som presenteras under Diagram 5.2-4, utslagning av noder. Hälften av abonnenterna är tappade vid 20 % länkutslagning och alla abonnenter tappas när 95 % av alla länkar är utslagna.

5.2.6 Simuleringsmoment 6

Denna simulering visar hur näten reagerar när noder slås ut slumpvis. Det som presenteras är hur många abonnenter som behåller kontakten med källnoder när noder attackeras.

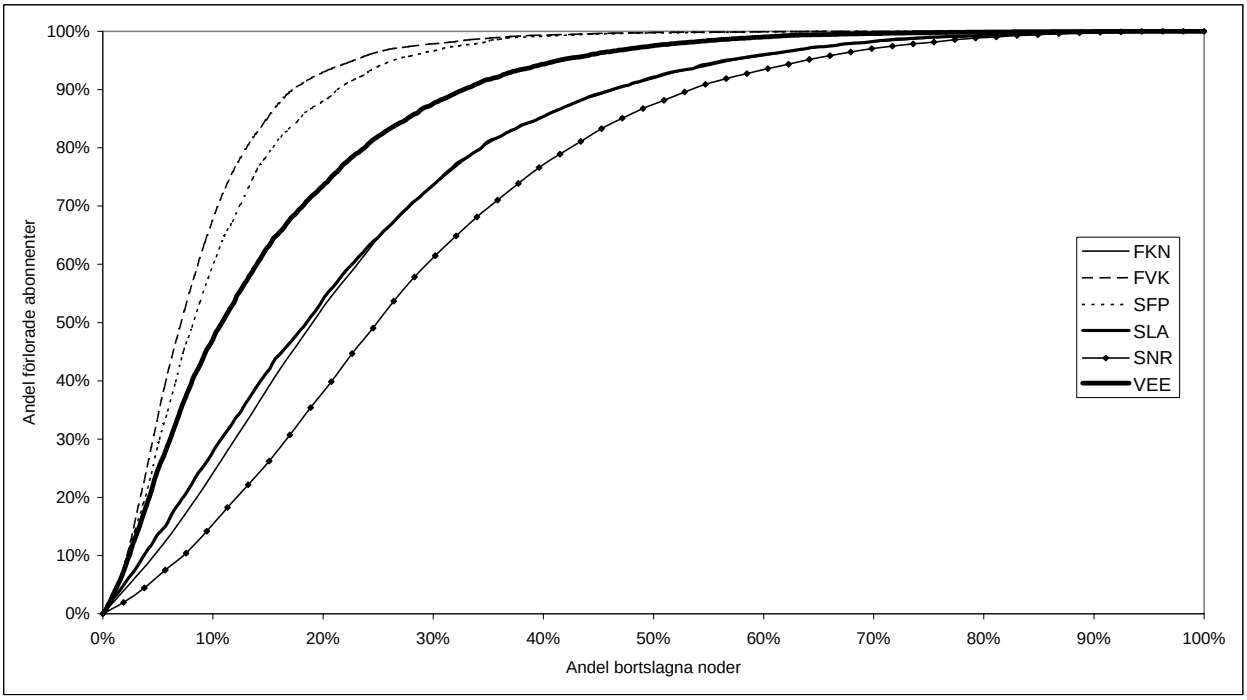


Diagram 5.2-6 Simuleringsmoment 6, slumpvis utslagning av noder

Resultaten visar att näten kan delas in i tre grupper utifrån hur de reagerar på attackerna. En grupp bestående av FVK och SFP kännetecknas av att deras kurva antar en brant lutning och de tappar alla abonnenter innan hälften av noderna är utslagna. Den andra tydliga gruppen, bestående av FKN, SLA och SNR, karakteriseras av en något flackare kurva och en total utslagning efter det att 75 % av alla noder slagits ut. Emellan dessa grupper finns nät VEE, som inledningvis, 0 till 5 % nodutslagning, intar en mycket brant lutning, likt den grupp bestående av FVK och SFP, därefter planas kurvan ut och alla abonnenter tappas strax innan 70 % utslagna noder.

Nät	**Nod**	**Sårbara objekt**
FKN	T 024	Daghem
FVK	T 166	Flerbostadshus, daghem
SFP	T 208	Lantbruk, daghem
SLA	S 1152	
SNR	T 001	
VEE	T 043	Lantbruk, daghem

Tabell 5-4 Tabell över objekt som i snitt slåss ut först

I ovanstående tabell presenteras en sammanställning av de konsekvenser, i form av utslagna objekt som kan antas vara viktiga för samhället, som sker efter av att första noden slagits ut. Att notera är att i nät SLA och SNR slås inledningsvis inga för samhället sårbara objekt ut.

5.2.7 Simuleringsmoment 7

Strategin för denna simulering var att slumpvis slå ut de länkar som förbinder noder i stationsnäten. Resultaten redovisas i diagrammet nedan.

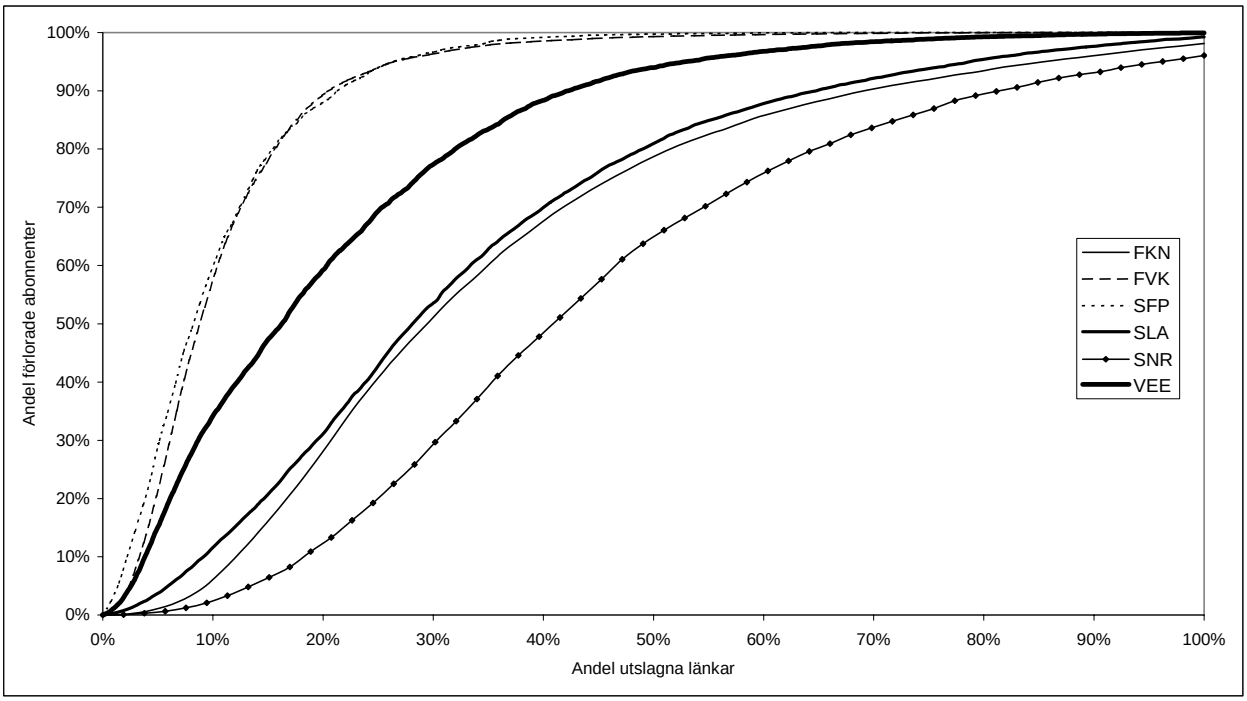


Diagram 5.2-7 Simuleringsmoment 7, slumpvis utslagning av länkar.

Resultaten visar på samma fenomen som simulering 6, där attacker skedde mot noder, att stationsnäten kan delas in i tre olika grupper. Av dessa grupper erhåller gruppen, bestående av, FKN, SLA och SNR, kurvor som har ett flackare utseende på samma vis som i simulering 6. Även i denna simulering tappar FVK och SFP alla abonnenter när hälften av är utslagna.

Nät	**Nod**	**Sårbara objekt**
FKN	T 024	Daghem
FVK	T 166	Flerbostadshus, daghem
SFP	T 208	Lantbruk, daghem
SLA	S 1152	
SNR	T 053	Daghem
VEE	T208	Lantbruk

Tabell 5-5 Tabell över sårbara objekt som i snitt slåss ut först

Tabellen ovan ger i princip samma resultat som i Tabell 5-4. De enda näten som uppvisar ett annorlunda resultat, jämfört med simuleringsmoment 6, är nät SNR och VEE.

5.2.8 Simuleringsmoment 8

I detta simuleringsmoment undersöktes hur den inverterad längden förändrades då noder plockades bort slumpvis.

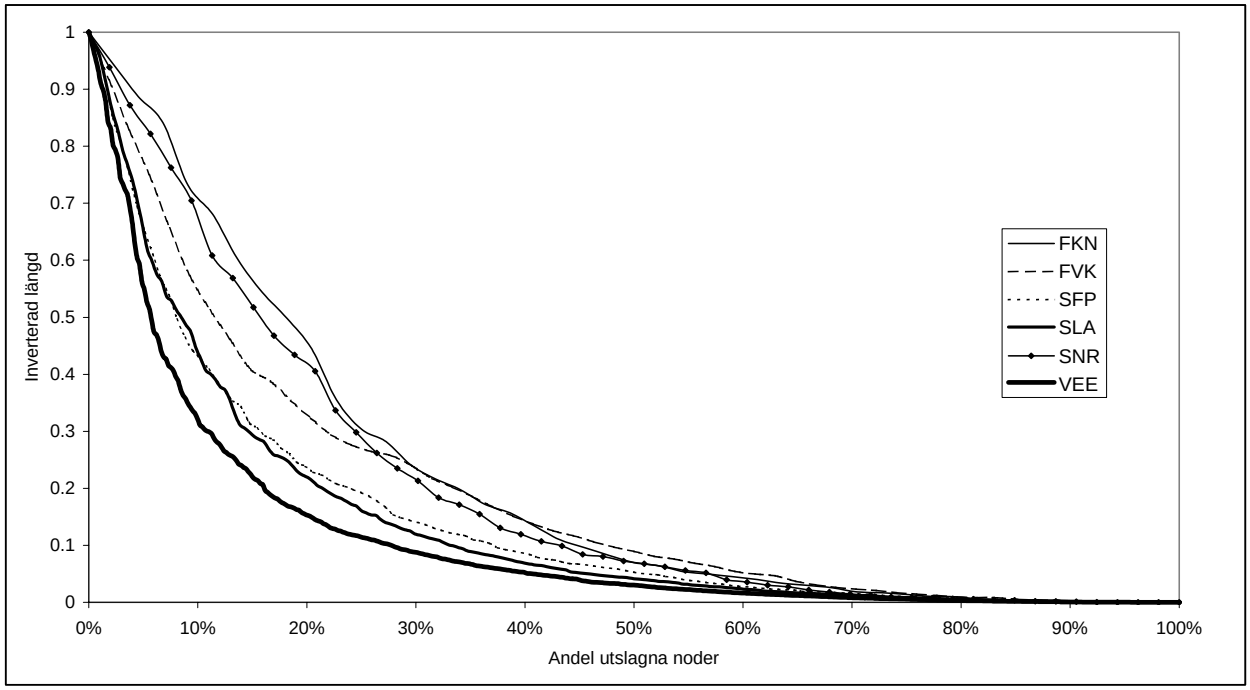


Diagram 5.2-8 Simuleringsmoment 8, förändring av inverterad längd vid slumpvis borttagning av noder.

Vid en jämförelse med resultat i moment 3 går det att utläsa att vid slumpmässig bortplockning av noder erhålls en betydligt flackare kurva.

5.3 Resultat av känslighetsanalys

För att verifiera att tillräckligt många simuleringar genomförts för att erhålla ett resultat som är tillförlitligt har en känslighetsanalys gjorts på simuleringsmoment 2, 3, 6, 7 och 8. För att kunna jämföra resultaten har ett av näten valts ut som underlag för känslighetsanalysen, SFP.

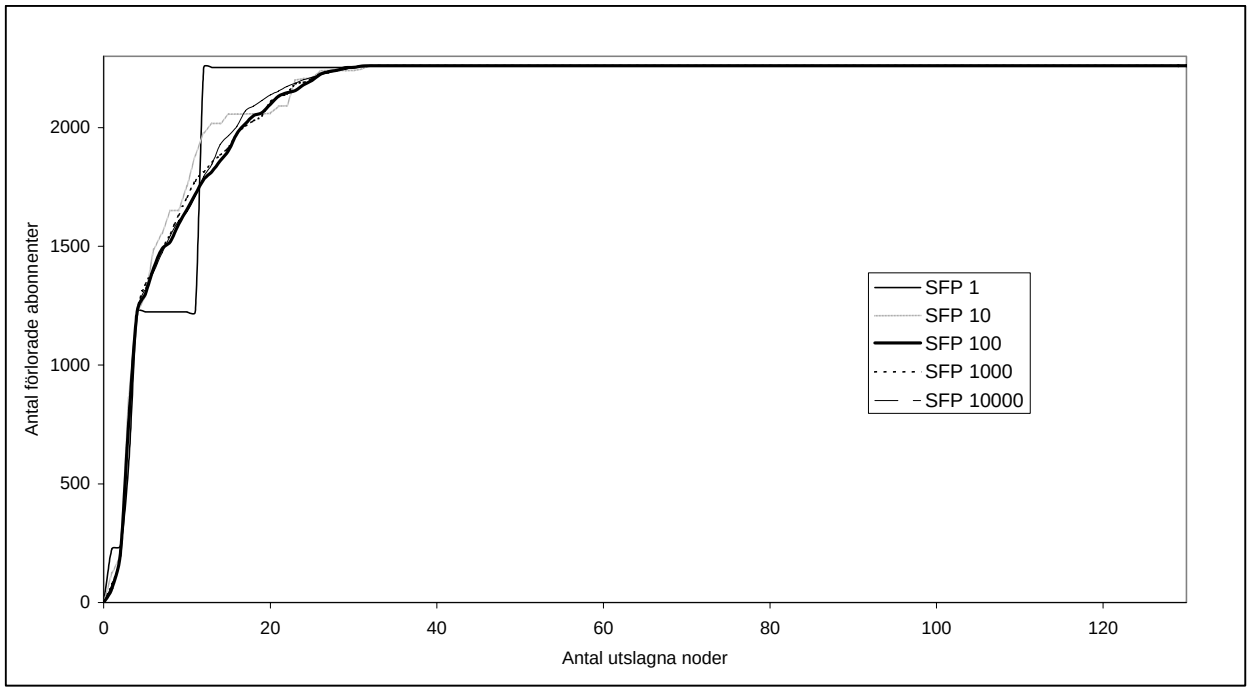


Diagram 5.3-1 Känslighetsanalys simulering 2 nät SFP

Resultat visar att endast 1 simulering ger en kurva som är väldigt oregelbunden. Redan vid 10 simuleringar erhålls en jämnare kurva och mellan 100 och 10000 simuleringar visar resultaten på små avvikelser.

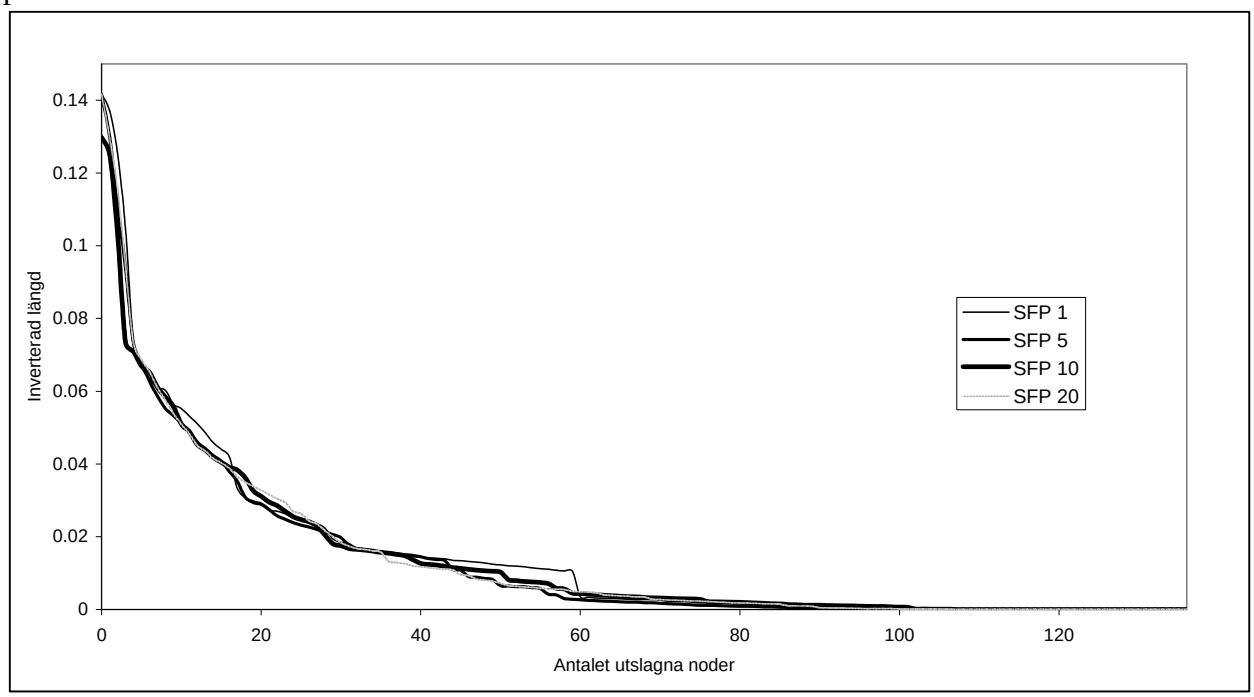


Diagram 5.3-2 Känslighetsanalys simulering 3 nät SFP

Diagram 5.3-2 visar resultatet av känslighetsanalysen för simuleringsmoment 3 där stationsnätens förändrade inverterad längd beräknades när noder med högst grad attackerades. Kurvan som beskriver resultatet av 1 simulering är av oregelbunden karaktär. De övriga simuleringarna visar på en mindre variation mellan resultaten.

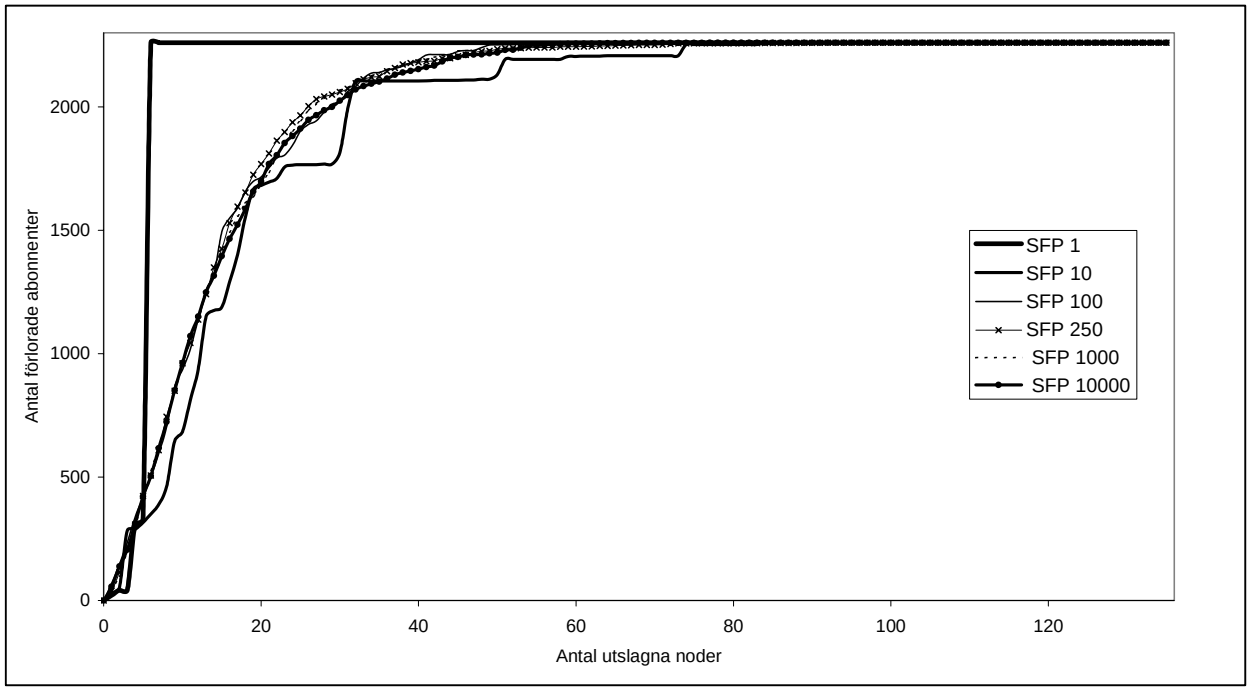


Diagram 5.3-3 Känslighetsanalys simulering 6 nät SFP

Likt tidigare känslighetsanalyser ger få simuleringar resultat med stora variationer. Däremot är det endast mindre avvikelser mellan 100 simuleringar upp till 10000 simuleringar.

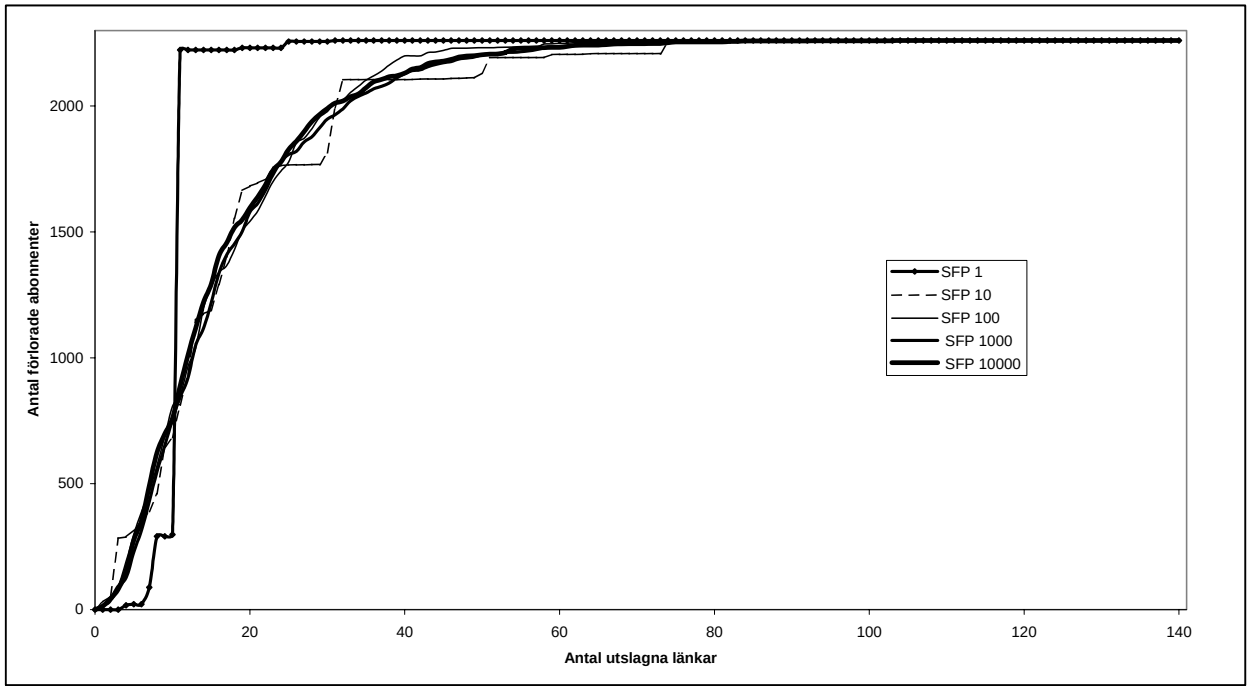


Diagram 5.3-4 Känslighetsanalys simulering 7 nät SFP

I diagrammet ovan kan viss avvikelse utläsas när 100 simuleringar jämförs med 1000 och 10000 simuleringar. Däremot visar resultaten endast på små avvikelser mellan 1000 och 10000 simuleringar.

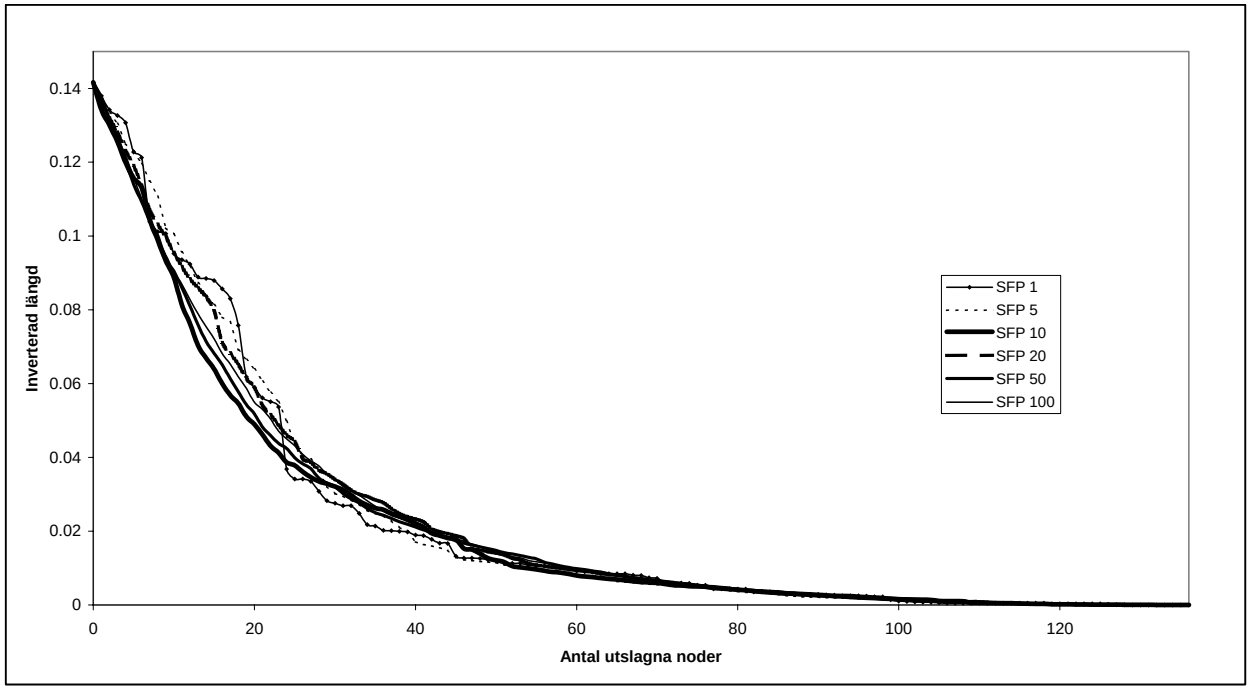


Diagram 5.3-5 Känslighetsanalys simulering 8 nät SFP

Mellan 10, 50 och 100 simuleringar visar resultaten på små avvikelser. Däremot uppvisar 20 simuleringar ett resultat med större variationer. Mindre antal simuleringar än 10 ger, som i känslighetsanalyser, resultat med stora variationer.

5.4 Avbrottsstatistik

Sydkraft har dokumenterat de avbrott som skett i näten. Man har till viss del även dokumenterat anledningen till avbrotten. Den statistik som legat till grund för detta arbete är hämtad under åren 2000 och 2001.

Nät	Antal abonnenter	Kund-avbrottstid (h)	Kund-avbrottstid/ abonnent	Antal drifts-störningar	Antal drifts-störningar/ nod
FKN	3408	0	0	0	0
FVK	2161	7642	3,54	10	0,19
SFP	2260	2308	1,02	14	0.1
SLA	5346	736	0,14	7	0,03
SNR	2411	672	0,28	2	0,04
VEE	6238	17850,8	2,86	46	0.1

Tabell 5-6

Tabellen ovan beskriver de avbrott och den kundavbrottstid i timmar som ägde rum under åren 2000 och 2001. I syfte att likställa näten och därmed ges möjlighet att jämföra näten sinsemellan, presenteras även avbrottstiden per abonnent. Det nät som hade längst

avbrottstid/abonnent var FVK och FKN hade lägst. Kunder i FKN nätet hade inte en enda avbrottstimme under 2000 och 2001. Även när en jämförelse görs avseende antalet driftsstörningar i förhållande till antalet noder toppar FVK med 0,19 driftsstörningar per nod.

6 Diskussion

6.1 Nät

Vid en analys av stationsnäten går det att utläsa att det finns stora likheter mellan dem. De har alla en låg klustringskoefficient, varav de flesta inte har någon klustring alls, samt att de har låga värden på inverterad längd.

6.1.1 Klustringskoefficient

Tidigare undersökningar av elnät påvisar samma sak, att klustringskoefficienten i elnät vanligtvis är låg. Vid en undersökning av ett elnät i västra USA beräknades klustringskoefficienten till 0,080 (Strogatz & Watts, 1998) vilket är betydligt högre än 0,00173 som blev resultatet av analysen av nät SDS. Resultaten är dock svåra att jämföra då det inte finns någon information om vilken typ av nät som Strogatz och Watts undersökt i de amerikanska studierna.

Vad betyder då en låg klustringskoefficient och varför har just vårat elnät ett lågt värde på den samma? Om uppbyggnaden på nätet studeras är det lättare att förstå det låga värdet. Exemplet nedan visar strukturen på stationsnätet FKN.

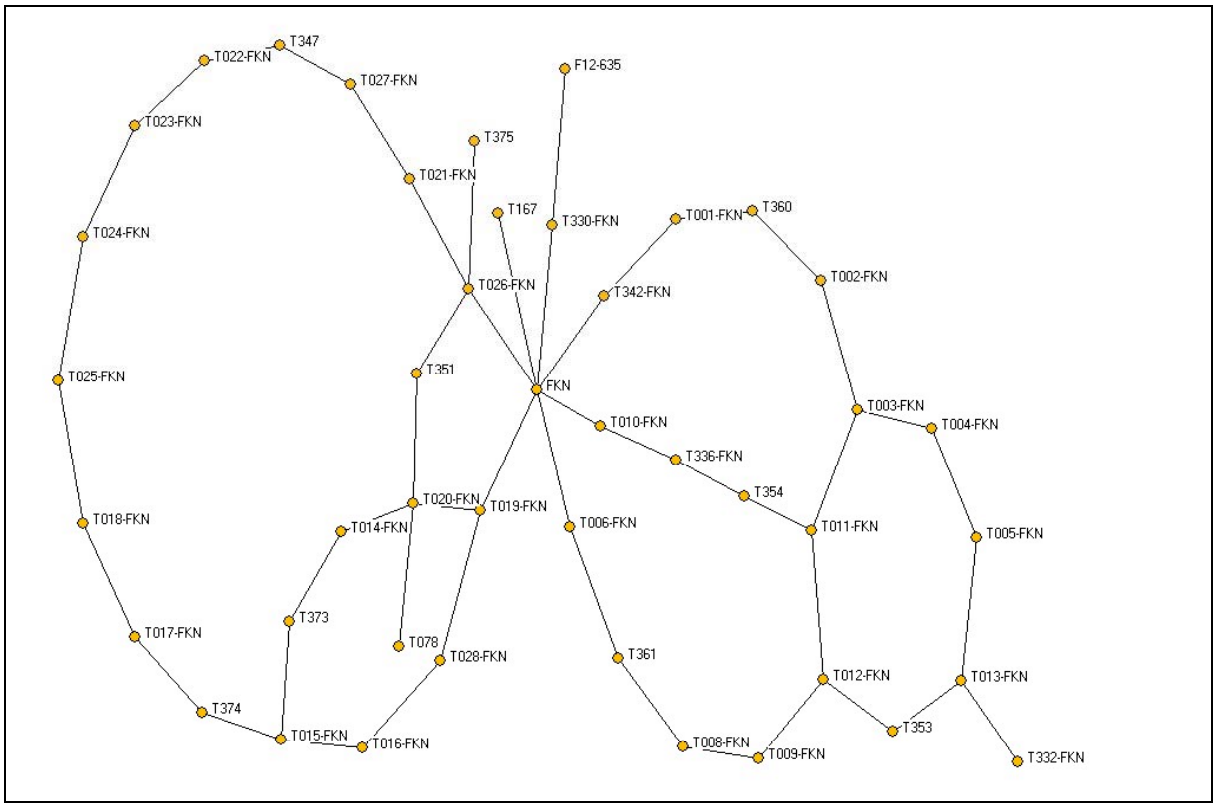


Bild 6.1.1-1 Schematisk bild av stationsnät, FKN. Notera hur noderna är kopplade längs en linje med få genvägar mellan noderna.

Elnätets struktur kan lättast förklaras genom att säga att varje nod ligger efter varandra längs en linje. En nods grannar är aldrig grannar med varandra vilket just är definitionen på klustringskoefficient. Nätverk som däremot brukar ha höga klustringskoefficienter är sociala nätverk. Bilden nedan beskriver en uppdelning som ofta sker på en fest där alla personer inte

känner varandra. Exemplet kan förklaras genom att beskriva de tre personerna i mitten som värdar. Värdarna skickar inbjudningar till sina vänner i sin tur, som då blir en del i festnätverket. Det sociala nätverket, nedan, erhåller därför flera kopplingar som tillsynes går kors och tvärs. Det i sin tur leder till att flera noders grannar är grannar sinsemellan och nätverket erhåller därmed en högre klustringskoefficient.

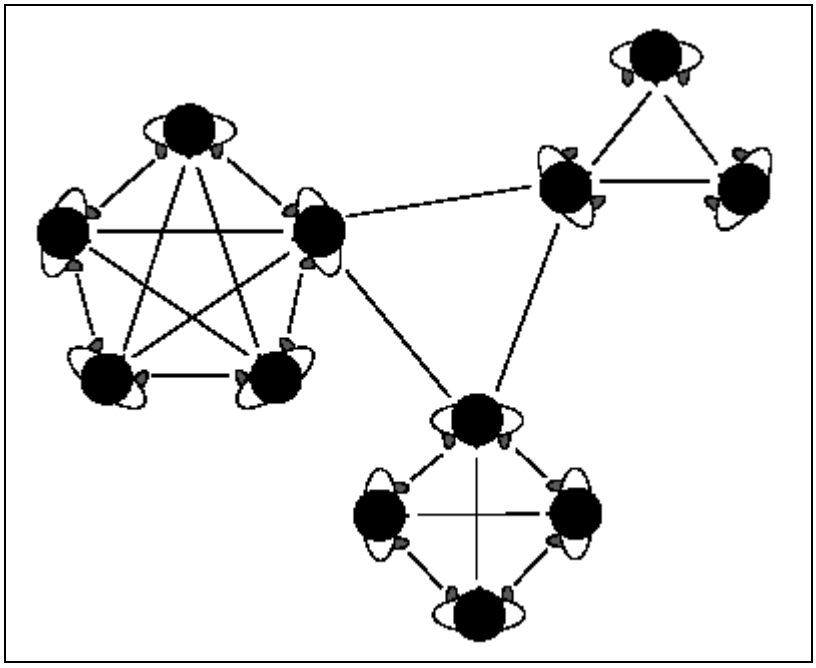


Bild 6.1.1-2 Schematisk bild som beskriver ett socialt nätverk på en fest (sedd ovanifrån). Bilden är hämtad från Komplexa nätverk (Bovin, 2003)

Vad är nyttan med en hög klustringskoefficient i syfte att minska sårbarheten? För att återgå till exemplet ovan, visar det sociala nätverket upp en större möjlighet att sammanlänka noder även om någon nod skulle attackeras. Eftersom en nods grannar är grannar med varandra kan, i elnätets fall, ström ta en annan väg för att nå sin abonnent. Detta exempel är givetvis enbart så här enkelt i teorin. I verkligheten måste även faktiska problem som att ström inte kan gå vilken väg som helst beaktas, ekonomiska aspekter o.s.v. Men att öka ett elnäts klustring är likväl ett sätt att göra elnätet robustare.

6.1.2 Inverterad längd

Som nämnts ovan visar alla näten upp ett lågt värde på inverterad längd. Även detta kan förklaras med att de flesta noder ligger på rad och endast är kopplade till två noder. Därmed finns det få ”genvägar” mellan noder som kan göra det genomsnittliga avståndet, mellan dem, mindre.

Vid en jämförelse med resonemanget angående klustringskoefficienten förstås det att dessa två mått hänger ihop. Ett nätverk med hög klustring har även kortare genomsnittligt avstånd mellan nätverkets noder. Således är ett hög klustrat nätverk med korta genomsnittliga avstånd mer anpassningsbart vid attacker eftersom det kommer att finnas flera alternativa vägar mellan noder. Gällande elnät som är riktade nätverk, på grund av att strömmen utgår från en källnod, förutsätts att den höga klustringen skall ske nära källnoden för att ovanstående resonemang skall gälla.

6.2 Slutsatser av simuleringar

Simuleringar har genomförts i syfte att analysera sårbarheten i de elnät som stått till förfogande. Härvid har två olika scenarier använts som grund för simuleringarna, dels ett scenario för analys av sårbarheten vid ett terrorangrepp och dels ett scenario för analys av sårbarheten vid vardagsbortfall t ex vid storm.

6.2.1 Slutsatser av terrorangrepp

För att kunna genomföra sårbarhetsanalys av de lokala elnätverk som stått till vårt förfogande, har tre olika moment simulerats. Dels har sammanlänkningsanalys med attack mot de noder som har högst grad genomförts mot såväl hela nätet, SDS, som mot delnäten och dels har analys av inverterad längd med attack mot noder med högsta grader i delnäten.

I majoriteten av delnäten är stationen den nod som har högst grad. Slutsatsen av detta konstaterande samt det faktum att strömmen matas från dessa noder (näten är alltså riktade), är att alla nät slås ut omedelbart. Med andra ord är de mycket sårbara. Simuleringarna genomfördes, efter denna analys, med tillägget att källnoderna ej fick slås ut. Slutsatserna av resultaten efter dessa simuleringar är att näten FKN och SNR uppvisat resultat av att vara mest robust. Nätet SNR matas från två noder, SNR och SNRV. För att se om ovanstående slutsats även var giltig om nätet, likt de andra näten, endast innehöll en källnod, gjordes ytterligare två simuleringar där endast en av stationerna åt gången, fungerade som källnod.

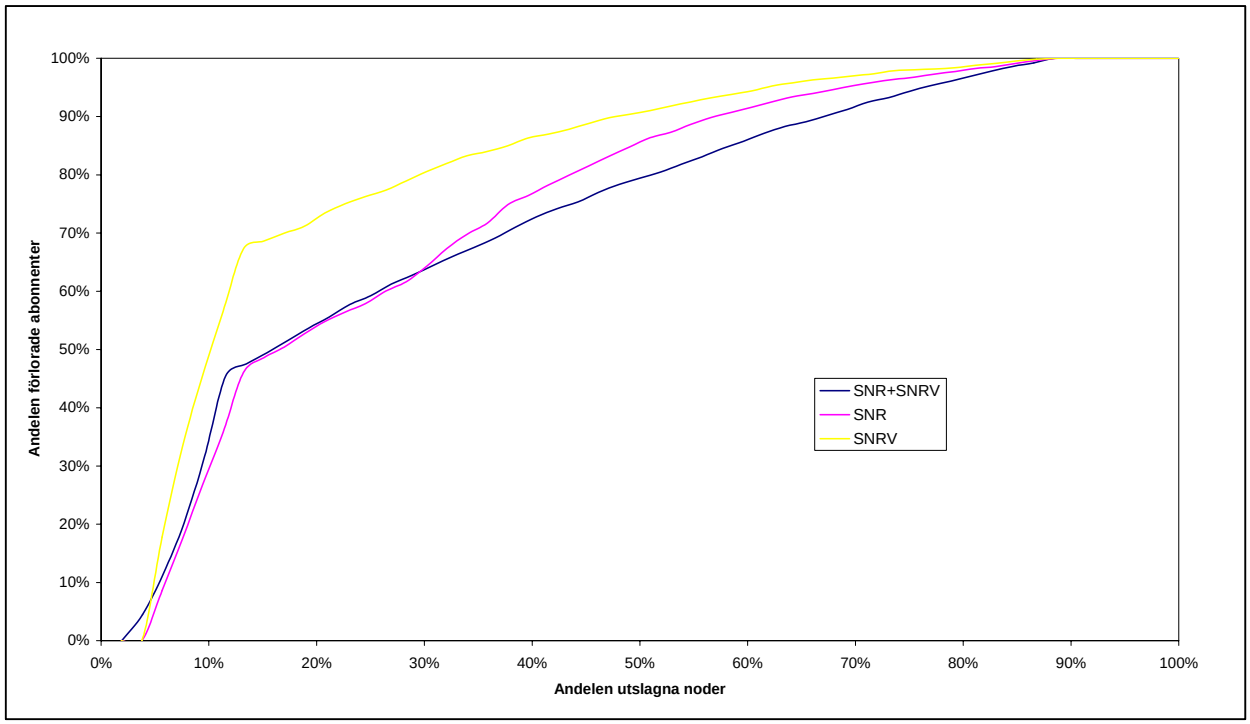


Diagram 6.2-1 Simuleringsmoment 2 med både SNR och SNRV som källnoder.

Slutsatserna vi drar är att vid simulering med SNRV som källnod förloras fler abonnenter (ca 20%) under de första 15% utslagning av noder. Vid simulering med SNR som källnod förändras kurvans utseende inte nämnvärt, jämfört med resultaten med två källnoder (SNR+SNRV), vilket leder till slutsatsen att det faktum att detta nät matas från två noder, istället för en likt de andra delnäten, inte påverkar slutsatsen att detta nät är mer robust är många andra nät.

Avseende nät SLA, har det ett bra resultat i moment 2, sammanlänkningsanalysen, medan nätet uppvisar sämre resultat i moment 3, inverterade längsta väg. Omvänt förhållande uppvisar nätet FVK som har ett bra resultat i moment 3, inverterade längsta väg, medan ett dåligt i moment 2, sammanlänkningsanalysen. Skillnaderna i resultaten i moment 2 kan förklaras med att titta på stationernas grader, där station SLA har ett gradtal på 6 medan station FVK har grad 1, samtidigt som de noderna som är kopplade till SLA har låga gradtal, vilket innebär att de står långt ner på listan för utslagning, medan den nod som är kopplad till FVK (T388) har hög grad, vilket innebär att den attackeras tidigt. (Se bilderna 6.2.1 och 6.2.2) Skillnaderna i moment 3 Inverterad längd analys, kan förklaras med de olika startförutsättningarna, där FVK har nästan dubbelt så högt värde på inverterad längd (0,183) jämfört med SLA (0,095). Vid denna typ av simulering studeras endast nätets struktur och ingen vikt läggs på vilket håll nätet är riktat, d v s inga källnoder är specificerade.

De slutsatser som är viktiga att poängtera är stationernas betydelse för näten. Denna slutsats stärks vid en jämförelse av resultaten i Diagram 5.2-1, där man kan konstatera att en terrorist skulle slå ut 95 % av alla abonnenter om han tilläts slå ut 5 % av alla noder, stationer inräknade. Motsvarande abonnentutslagning, om stationerna inte slås ut, är 35 %. Som redan redogjorts i tidigare kapitel är nätet som studerats (SDS) uppdelat i en mängd mindre nät, med hjälp av frånskiljare. Möjligheten finns dock att sammankoppla alla dessa mindre nät till större för att därigenom minska sårbarheten. Detta gäller inte SLA, då detta nät inte är sammankopplingsbart med de övriga studerade näten.

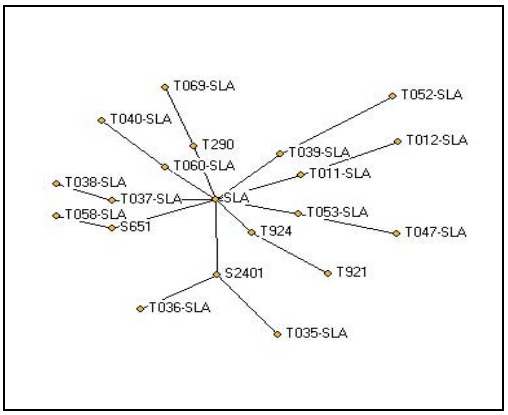


Bild 6.2.1-1 Del av nät SLA.

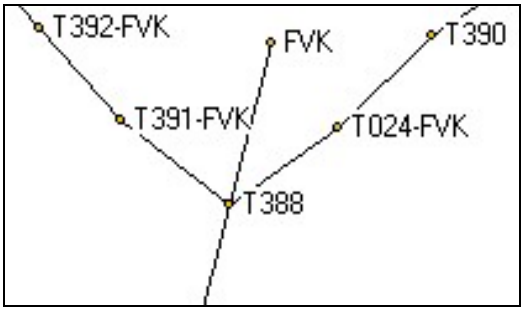


Bild 6.2.1-2 Del av nät FVK.

6.2.2 Slutsats av vardagsbortfall

För att studera detta scenario har fem olika simuleringsmoment genomförts. Två olika moment har genomförts mot hela nätet (SDS), dels en sammanlänkningsanalys med slumpvisa attacker mot noder och dels en motsvarande mot länkar. Två simuleringsmoment innehållande sammanlänkningsanalys med slumpvisavisa attacker mot dels noder och dels mot länkar. Ett simuleringsmoment har genomförts med analys av inverterad längd, slumpvisa attacker mot noder.

Vid en jämförelse mellan riktad utslagning, högsta grad, och slumpvis utslagning av noder i nät SDS kan det konstateras att kurvan som visar den riktade utslagningen inledningsvis har ett brantare utseende. När 3 % av noderna slagits ut, i den riktade attacksimuleringen, rätas kurvan ut och när drygt en tredjedel av noderna slagits ut så tappas abonnenterna i snabbare takt vid de slumpvisa attackerna. (Se Diagram 5.2-1) Resultatet förklaras av att de noder med grad 4 eller högre, är 3 % av den totala nodantalet. Noder med grad tre eller högre är 30 % av

det totala nodantalet. När attackerna är riktade slås noderna med hög grad ut först vilket gör att abonnenterna tappas snabbt. När så de noder med hög grad är utslagna tappas abonnenterna i lägre takt, d v s kurvans lutning mattas. Vid slumpvis utslagning blandas noder med hög och låg grad, vilket gör att utslagningen (kurvans lutning) sker mer konstant. Kurvan av simuleringen med slumpvis utslagning av länkar, ligger under de båda kurvorna när noder slås ut. Detta beror på att en nod med t ex grad 4, kan få tre av dessa länkar utslagna utan att för den skull sluta att fungera.

Vi drar slutsatsen av ovanstående jämförelser att nätet är sårbart, framförallt när attackerna är riktade. Nätet måste anses vara sårbart när drygt 6500 abonnenter förlorar strömmen när mindre än 30 noder slagits ut. Detta konstaterande görs utan att någon av noderna är av typen station, då skulle konsekvensen, i tappade abonnenter, blivit avsevärt större.

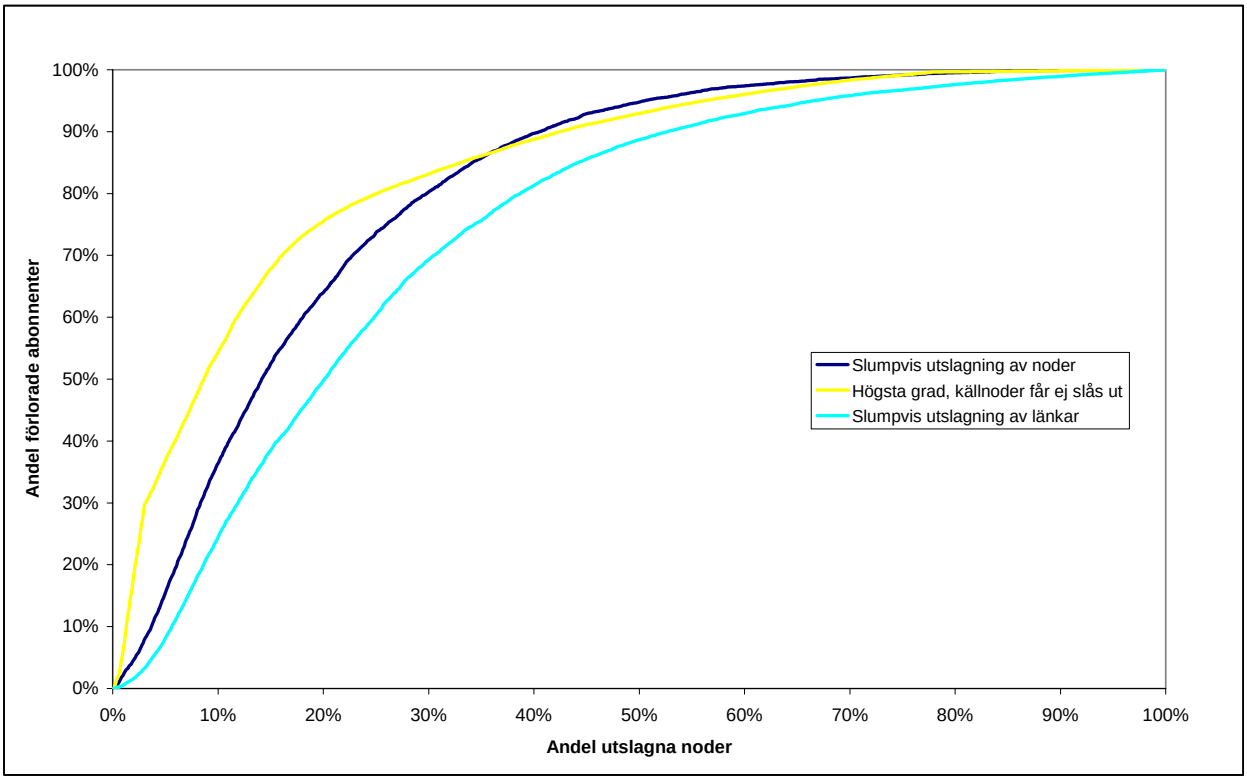


Diagram 6.2-2 Jämförelse av olika simuleringsmoment, nät SDS.

Liksom i simuleringsmoment 2 (sammanlänkningsanalys, attacker mot noder med högst grad) så uppvisar resultaten från simuleringsmoment 6 (sammanlänkningsanalys, slumpvisa attacker mot noder) och simuleringsmoment 7(sammanlänkningsanalys, slumpvisa attacker mot länkar) motsvarande slutsatser. FVK och SFP är de nät som uppvisar sämst resultat, d v s är sårbarast, medan SLA, FKN och SNR är de nät som är mest robust. FVK och SFP tappar drygt 90 % av sina abonnenter när endast en femtedel av noderna/länkarna slagits ut. Dessa värden kan jämföras mot de nät som uppvisat bäst resultat, där mindre än hälften av abonnenterna tappats när 20 % av noderna slagits ut. Avseende resultaten i moment 7 har SNR endast tappat en femtedel av abonnenterna när 20 % av länkarna blivit utslagna, jämför Tabell 6-1. Dessa slutsatser förstärks av den avbrottsstatistik som presenteras i Tabell 5-6, där det framgår att SLA endast hade en kundavbrottstid av 0,14 timmar/abonnent, SNR hade 0,28 timmar/abonnent och FKN saknade avbrott under den tid kundavbrottsstatistiken är hämtad.

Motsvarande kvittens erhålls när vi tittar på de sårbaraste näten FVK med kundavbrottstiden 3,54 timmar/abonnent och SFP på 1,02 timmar/abonnent.

Nät	Utslagna noder								
	10%	20%	30%	40%	50%	60%	70%	80%	90%
SNR	3%	12%	30%	48%	65%	76%	84%	90%	93%
FVK	58%	90%	96%	98%	99%	100%	100%	100%	100%

Tabell 6-1 Jämförelse mellan två nät, simuleringsmoment 7, som uppvisar det bästa och sämsta resultatet. Tabellen visar andelen utslagna abonnenter i förhållande till utslagna noder

6.3 Känslighetsanalys

För att undersöka hur stor påverkan antalet simuleringar har vid användandet av simuleringsprogrammet NetCalc genomfördes en känslighetsanalys. Som presenterats i kapitel 4.4.3 genomfördes 1000 simuleringar vid sammanlänkningsanalys och 10 simuleringar vid analys av inverterad längd. För att erhålla resultat som är oberoende av antal simuleringar kontrollerades var denna gräns låg. Nät SFP valdes ut som exempelnätverk för känslighetsanalysen eftersom detta nät ligger i mitten vid en jämförelse av mängd ingående noder i de olika stationsnäten.

Diagrammet nedan visar känslighetsanalys av simuleringsmoment 8, som simulerar hur den inverterade längden förändras när noder borttages slumpvis. I diagrammet går det att utläsa att vid få simuleringar, mindre än fem, får kurvan ett oregelbundet utseende som visar att det finns stora osäkerheter i resultatet. Vid tio simuleringar eller fler erhåller kurvan ett jämnare utseende vilket tyder på att resultat är mer oberoende av antalet simuleringar. En jämförelse där 100 simuleringar gjorts tyder endast på små avvikelser från tio simuleringar. Därför anses det att tio simuleringar ger ett resultat som är pålitligt.

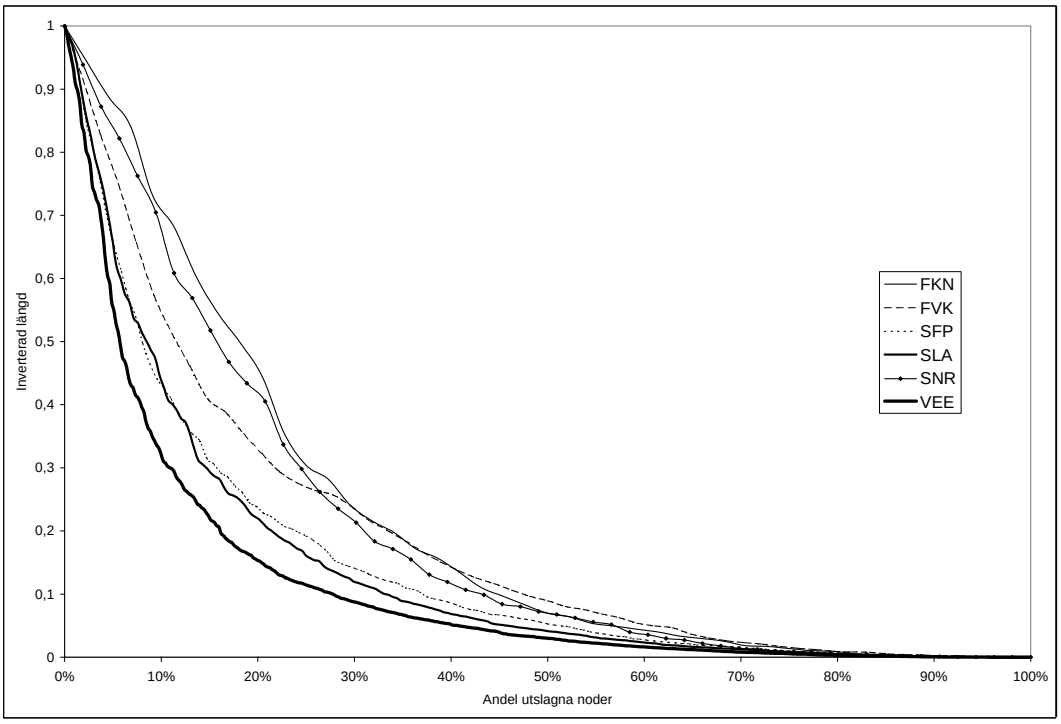


Diagram 6.3-1 Känslighetsanalys av simuleringsmoment 8.

En känslighetsanalys har även gjorts för sammanlänkningsanalys där noder borttagits slumpvis. Även här visar diagrammet (se nedan) att vid få simuleringar kommer resultatet påvisa stora osäkerheter. Kurvan som beskriver 100 simuleringar uppvisar en mer jämn kurva, och därmed ett resultat med mindre osäkerheter. I analysen redovisas också resultatet av 1000 och 100000 simuleringar. Dessa kurvor sammanfaller, med små avvikelser, med resultat av 100 simuleringar. Därmed anses det att 1000 simuleringar ger ett resultat med god pålitlighet.

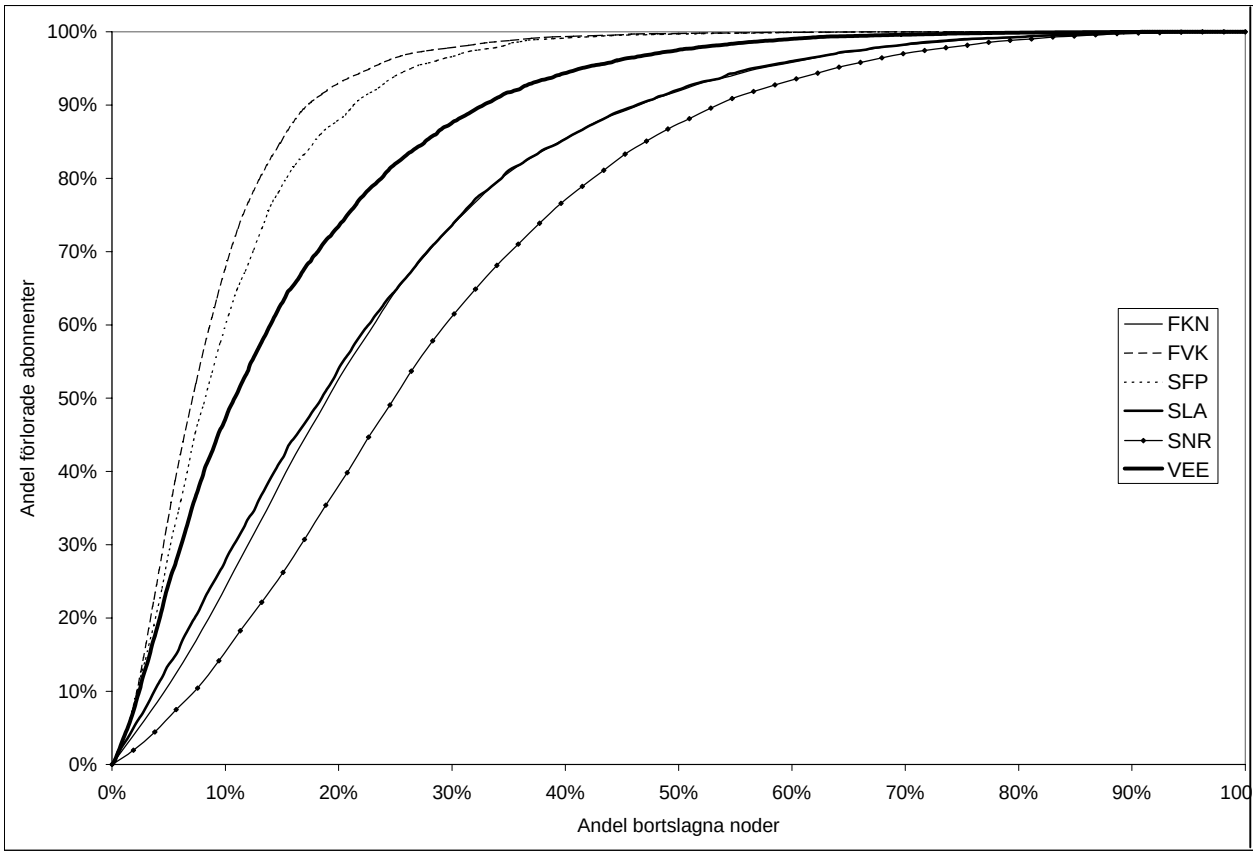


Diagram 6.3-2 Känslighetsanalys av simuleringsmoment 6.

En känslighetsanalys har även gjorts gällande simuleringar där strategin varit att slå ut de noder som hade högst grad. Analysen visar på samma resultat som ovan och därför anses det att samma antal simuleringar ger ett pålitligt resultat även för denna typ av simulering.

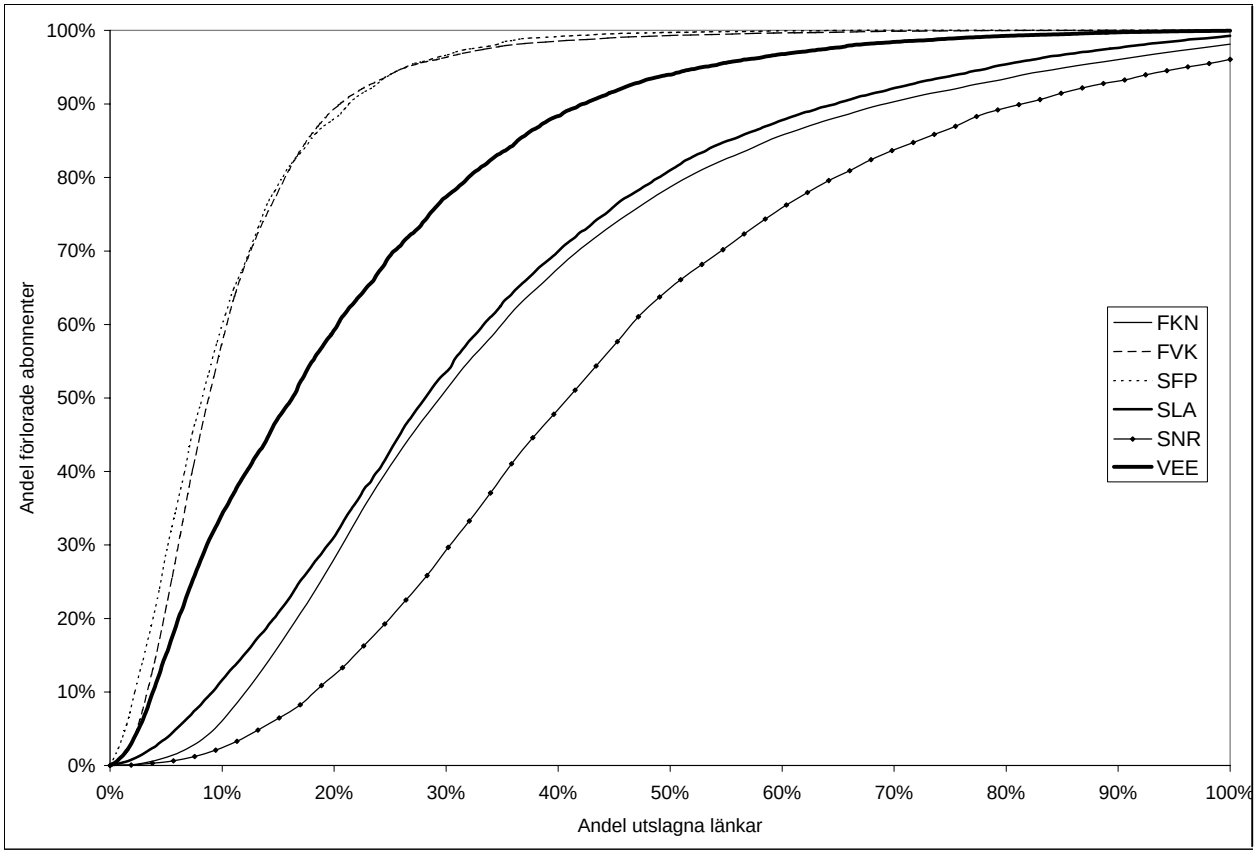


Diagram 6.3-3 Känslighetsanalys av simuleringsmoment 7.

Diagrammet ovan visar en känslighetsanalys av moment 7 där länkar slumpvis bortplockades. Likt tidigare ger få simuleringar resultat med stor variation vilket resulterar i en ojämn kurva. Även vid denna typ av simulering minskar variationen vid 100 simuleringar och 1000 simuleringar har små avvikelser från 10000 simuleringar. Därmed anses 1000 simuleringar ge ett acceptabelt resultat.

6.4 Osäkerhetsanalys

6.4.1 Indata

Det ligger en hel del osäkerhet i de data som används i denna analys. De kopplingsscheman som använts för att kartlägga och skapa simuleringsunderlag har varit av skiftande noggrannhet, såtillvida att vissa scheman innehållit uppgifter om typ av ledning, stolpar mm medan andra endast innehållit uppgifter om transformatorer. Vi kan heller inte utesluta att förändringar i näten utförts, utan att de tagits upp i de kopplingsscheman som kartläggningen grundar sig på. Då kartläggningen innefattat uppgifter om nästan tusen noder, typ av nod, typ av länk samt vilka noder som är sammanlänkade, kan det inte uteslutas att fel smugit sig in vid kartläggningen. En annan osäkerhet ligger i det faktum att vi simulerar ett större nät än vad som normalt sätt drivs verkligheten. Som poängteras tidigare i rapporten är lokalnätet uppdelade i stationsnät som i sin tur består av olika fack. Därmed är stationsnäten uppdelade i mindre nät. Vid våra simuleringar vi utgått från stationsnäten, vilket alltså är en förenkling av verkligheten. Denna förenkling är också en källa till osäkerhet. Detsamma gäller när simuleringar genomförts med lokalnätet som helhet (SDS).

6.4.2 Kundavbrottstid

Det underlag avseende kundavbrottstid som ställts till detta arbetes förfogande omfattade bl a total kundavbrottstid, antal driftsstörningar samt vad avbrotten berott på t ex bristande underhåll, vind mm. I det statistiska underlaget framgår det inte om avbrotten skett i hela det nät som statistiken omfattar eller bara en del av den samma. Vidare framgår det ej om det funnits något tröskelvärde för avbrottstiden, t ex hela timmar. Den störta osäkerheten med detta underlag ligger dock i det faktum att statistiken endast är hämtad från åren 2000-2001.

6.4.3 Diskussion runt osäkerheter

De osäkerheter som presenterats ovan kan tyckas vara stora och omfattande. Huvudsyftet med detta arbete är dock att studera och utveckla en metod att göra sårbarhetsanalys och då anser vi att dessa osäkerheter inte är för stora. Vi är övertygade att dessa osäkerheter endast marginellt påverkar våra möjligheter att dra slutsatser huruvida denna metod är bra eller ej.

6.5 Diskussion runt förekomsten av VIP-kunder

I det underlag som ställdes till förfogande för detta arbete ingick en kategorisering av olika kunder kopplade till vissa noder. Exempel på kategorier är; mindre industri, med eller utan elvärme, lantbruk, daghem, flerbostadshus med eller utan fjärrvärme, flerbostadshus med eller utan elvärme m fl. I lagen Ellag 1997:857 framgår det att nätbolagen ICKE får prioritera vissa kunder före andra. Detta är givetvis en demokratiskt riktig bedömning men vi ifrågasätter om detta är den bästa för samhället i stort, med sårbarhet i fokus. Vi anser att det vore rimligt att till exempel kommunen hade möjlighet att prioritera samhällsviktiga objekt vid återställning efter avbrott. Sådana objekt kan vara ålderdomshem, daghem, vattenverk, reningsverk, m fl. Ett annat exempel skulle kunna vara denna enda industrin i det lilla samhället, då dennas drift kan vara en förutsättning för att samhället ska leva vidare.

Vi vill betona att denna kundprioritering ska ligga hos kommunen (länstyrelsen eller motsvarande) och inte hos nätbolagen då ekonomiska intressen kan gå före i bedömningen.

6.6 Slutdiskussion

Av de simuleringar som gjorts har vi kunnat dra slutsatsen att nätet FVK är ett av de nät som är mest sårbart. Vi har även kunnat verifiera denna slutsats med den kundavbrottstid som nätet hade under 2000-2001. Dock, så vet vi efter den kartläggning som utförts, att FVK är ett av de nät som har högst andel markledning. Med erfarenheter av tidigare stormar, nu senast stormen Gudrun, vet vi att luftledning är betydligt mer sårbar i dessa sammanhang än ledning nedgrävd i mark. Därför är sannolikheten mindre att FVK kommer attackeras på grund av väder och vind. Det är därför av stor vikt att vid fortsatta studier på området inkludera fler parametrar vid simulering som beskriver nätets verkliga beskaffenhet. Dessa parametrar kan vara om nätet består av mark- eller luftledningar, vilket material ledningarna har, vilken kvalitet nätet har i övrigt. Det skulle även vara möjligt att lägga in parametrar som vanligtvis finns i ledningssystem, så som till exempel underhållsfrekvens, kvalitet på underhåll, förekomst av underhållsrapportering och uppföljning, etc. För att göra sårbarhetsanalysen så heltäckande som möjligt bör även funktionen av nätet inkluderas i analysen. I vår analys har vi antagit att finns det en koppling så finns det även ström mellan noderna. Detta är en förenkling och för en fullständig analys bör även dessa aspekter inkluderas.

Vi anser att intermeditet är ett viktigt begrepp vid analys av sårbarhet i komplexa nätverk. I detta arbete har dock ej intermeditet studerats. Detta på grund av att verktyg i form att beräkningsprogram ej funnits att tillgå. Som tidigare redogjorts i denna rapport går

intermediteten ut på att beräkna hur ofta en nod ingår i den kortaste vägen mellan andra noder. De noder som erhåller högst intermeditetsvärde torde vara de mest sårbara noderna för nätverket. Detta ligger till grund för vår slutsats att fortsatta studier bör göras inom detta område med syfte att försöka fastställa ett sårbarhetsgränsvärde på intermediteten.

Vi anser att detta är en bra metod för att genomföra sårbarhetsanalys på ett nätverk, dock är ett nätverk endast ett verktyg för att transportera något från en punkt till en annan, i detta fall elektricitet. För att göra en sårbarhetsanalys över eldistribution ska denna metod ses som en del av en större analys, jämför kapitel 3.2.3.

Vi ser ingenting som tyder på att det inte skulle gå att använda dessa verktyg även på andra typer nätverk, till exempel organisatoriska eller sociala. Men vi vill återigen poängtera att metoden endast ska ses som en del av en sårbarhetsanalys.

Eftersom ett elnätverk finns i fysisk form är de möjligt att visualisera nätverket. Detta kan göras genom att, till exempel, använda GIS-applikationer. Fördelarna att använda GIS-applikationer för ett elnätsbolag torde vara flera. Möjligheten finns då att, vid ett avbrott, direkt kunna skicka ut en reparatör och vägleda honom via GPS till platsen för avbrottet. Detta betyder att användningen av GIS-applikationer är något som kan användas i det dagliga underhållsarbetet, men att elnätsbolaget samtidigt får ett underlag för att genomföra sårbarhetsanalyser på elnätverk med hjälp av nätverksteorier. Detta maximerar nyttan av en investering i GIS-mjukvara.

6.6.1 Återkoppling

I problemformuleringen ställdes några frågeställningar upp som legat till grund för detta arbete. I denna avslutande återkoppling kommer ett försök att besvara ställda frågeställningar.

Utseendet på elnät när det beskrivs som ett nätverk kan liknas med det som kan ses utanför bilfönstret, en stolpe (nod) som förbinds med en elledning (länk). Det kan också konstaterats det typ av elnät som studerats, lokalnät, är lågklustrat med långa avstånd.

Då det i Ellagen (1997:857) regleras att nätbolag inte får ha några prioriterade kunder står det klart att inga prioriterade kunder existerar. Vi anser dock att vissa kunder rimligen borde prioriteras och att det bör redas ut hur denna prioritering skall utformas. Detta anser vi är det svåra då det är svårt att finna en opartisk beslutsfattare.

Den typ av nätverk vi studerat, elnät, är riktade, det vill säga strömmen utgår från en källnod. Detta gör nätverket sårbart för riktade attacker, då relativ få noder behöver attackeras för att tappa hela nätet. Det som kunnat konstaterats i detta sammanhang är att källnoden är sårbarast.

Vår förhoppning är framtida studier kommer att leda gränsvärden på sådan begrepp som klusterkoefficient och kortaste väg/inverterad längd. Ett begrepp som vi hoppas kommer att undersökas mer i framtiden är intermeditet, eftersom vi anser att detta begrepp är starkt kopplat till sårbarhet.

Av de resultat som vi erhållit vid skrivandet av denna rapport anser vi att det inte finns något som tyder på att metoden inte skulle kunna användas på andra typer av nätverk.

Som vi nämnt i rapporten skall analysen av nätverk endast ses som ett komplement till sårbarhetsanalys. Dock anser vi att nätverksteorier är en viktig del för att sårbarheten i ett komplext nätverk skall kunna bedömas.

7 Förslag på vidare studier

För att gå vidare och utveckla möjligheten att använda nätverksteorier vid genomförandet av sårbarhetsanalyser på komplexa nätverk vill vi här ge lite förslag vad framtida rapporter kan inrikta sig på.

Nätet som studerats i denna rapport är av karaktären lokalnät. Som tidigare beskrivits kan nätet liknas med ett långt snöre med knutar, där knutarna representeras av noder och snöret av länkar. Vi tror att det svenska stamnätet har en annan topologi och att en studie av detta skulle ge andra resultat på klustringskoefficient och inverterade längder. I en analys av det svenska stamnätet skulle det även vara av intresse att undersöka hur funktionen i nätet förändras när en nod eller länk attackeras. Till exempel skulle kaskadeffekter studeras.

Vidare studier bör genomföras i syfte att utröna möjligheten att även använda dessa verktyg på sociala och organisatoriska nätverk. Vi anser oss inte finna några bevis för att dessa verktyg inte skulle fungera för att bedöma sårbarheten i dessa typer av nätverk, men då vi inte analyserat dessa nät har vi inga belägg som styrker dessa antaganden.

Fortsatta studier hur intermediteten inverkar på nätets sårbarhet bör genomföras i syfte att finna ett sårbarhetsgränsvärde för intermediteten.

Då vi tidigare i denna rapport pekat på andra aspekter som sannolikt påverkar sårbarheten, så som t ex underhållsfrekvensen och kvaliteten på underhållet, mark- eller luftledning, materialet på ledningen, skulle fortsatta studier om dessa vara mycket värdefulla. Studierna skulle t ex kunna syfta till att hitta värden på hur mycket sårbarare luftledning är i förhållande till markledning och/eller hur dessa värden skall användas i beräkningar.

Referenslista

Abrahamsson, M & Magnusson, S E (2004) *Användning av risk- och sårbarhetsanalyser i samhällets krishantering* LUCRAM, Lund

Albert I., Albert R. & Nakarado G. L. (2004) Structural vulnerability of the North American power grid *Physical Review E 69, 025103-1*

Barabasi A-L., Albert R., Jeong H. (1999) Mean-field theory for scale-free random networks, *Physica A 272* 173-187

Bollobás, B. (1998). *Modern Graph Theory*. New York: Springer Verlag

Bovin, J. (2003) *Komplexa nätverk,* Avdelningen för epidemiologi, Smittskyddsinstitutet

Ellagen (1997:857)

Förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap.

Förordning (2002:518) med instruktion för Krisberedskapsmyndigheten

Hallin P-O., Nilsson J. och Olofsson N (2004) *Kommunal sårbarhetsanalys* Krisberedskapsmyndigheten Stockholm

Holmgren, Å. (2004a) *Vulnerability Analysis of Electric Power Delivery Networks, Licentiate Thesis,* KTH Land and Water Resoursces Engineering

Holmgren, Åke (2004b) Graph Modeling and Vulnerability Analysis of Electric Power Grids, Royal Institute of Technology (KTH) and the Swedish Defence Research Agency (FOI).

Holme, P., Kim, B.J., Yoon, Chang No & Han, Seung Kee, (2002) Attack vulnerability of complex networks, *Physical Review E 69,* 056109-1

http://mathworld.wolfram.com/Graph.html 2005-03-22.

http://www.cs.virginia.edu/oracle 2005-05-27

http://www.computerworld.com/networkingtopics/networking/story/0,10801,75539,00.html 2005-05-27

Karlqvist, A (1990) *Nätverk. Teorier och begrepp i samhällsvetenskapen.* Värnamo: Gidlunds Bokförlag

Krisberedskapsmyndigheten (2003) *Risk- och sårbarhetsanalyser – Vägledning för statliga myndigheter* Krisberedskapsmyndigheten Stockholm

Lag (2202:833) om extraordinära händelser i fredstid hos kommuner och landsting

Travers, J., Milgram, S., (1969) An Experimental Study of the Small World Problems, *Sociometry, Vol.32, No. 4*, 425-443

U.S. Department of Energy Office of Energy Assuransce (2002) *Vulnerability Assessment Methodology. Electric Power Infrastructure* U.S. Department of Energy Office of Energy Assuransce:USA

Watts, Duncan J. (2003) *Six degrees – The science of a connected age* London: Vintage

Watts, Duncan J., & Strogatz, Steven (1998) Collective dynamics of ”small-world” networks, *Nature* 393:440.

Bilaga 1

Nedan presenteras det dokument som användes för att beskriva elnätet som undersöks i rapporten. Varje nod gavs ett individuellt nummer för identifikation. I kolumnerna beskrivs vilka olika beskaffenheter som de olika noderna kan ha. Har en nod en etta i någon av kolumnerna betyder det att noden har den beskaffenheten. I abonnent kolumn anges antal abonnenter som är direkt beroende av noden och i sista kolumnen, grannar, visas till vilka noder som är sammanlänkade.

					Objekt				Länk						Grannar				
Nummer		Identitet	Tillhörighet	Fack	Station	Transformator	Frånskiljare	Stolpe	Mark	Luft	Abonnent								
0	FVK				1	0	0	0	1	0	0	451	780	780					
1	VEE				1	0	0	0	1	0	0	2	76	110	117	219	277	388	70
2	S1991	VEE		17	0	0	0	1	0	1	0	1	3						
3	S1994	VEE		17	0	0	0	1	0	1	0	2	4	5					
4	T102-VEE	VEE		17	0	1	0	1	0	1	7	3							
5	T098	VEE		17	0	1	0	1	0	1	6	3	6						
6	F22-629	VEE		17	0	0	1	1	0	1	0	5	7						
7	T090	VEE		17	0	1	0	1	0	1	3	6	8	18					
8	S2025	VEE		17	0	0	0	1	0	1	0	7	9	15					
9	F22-630	VEE		17	0	0	1	1	0	1	0	8	10						
10	S2033	VEE		17	0	0	0	1	0	1	0	9	11	12					
11	T366	VEE		17	0	1	0	1	1	0	4	10							
12	S2035	VEE		17	0	0	0	1	0	1	0	10	13	14					
13	T100	VEE		17	0	1	0	0	1	0	11	12							
14	T101-VEE	VEE		17	0	1	0	1	0	1	6	12							
15	S2048	VEE		17	0	0	0	1	0	1	0	8	16						
16	T099	VEE		17	0	1	0	0	1	0	49	15	17						
17	T359	VEE		17	0	1	0	1	1	0	10	16							
18	T250	VEE		17	0	1	0	1	0	1	4	7	19						
19	F22-533	VEE		17	0	0	1	1	0	1	0	18	20						
20	S2062	VEE		17	0	0	0	1	0	1	0	19	21	37					
21	OF22-534	VEE		17	0	0	1	1	0	1	0	20	22						
22	S2176	VEE		17	0	0	0	1	0	1	0	21	23	25					
23	S2604	VEE		17	0	0	0	1	0	1	0	22	24						
24	T091	VEE		17	0	1	0	0	1	0	8	23							
25	S2181	VEE		17	0	0	0	1	0	1	0	22	26	30					
26	T092	VEE		17	0	1	0	1	0	1	6	25	27						
27	S2203	VEE		17	0	0	0	1	1	0	0	26	28						
28	S2204	VEE		17	0	0	0	1	1	0	0	27	29						
29	T153	VEE		17	0	1	0	1	0	1	2	28							
30	S2187	VEE		17	0	0	0	1	0	1	0	25	31	32					
31	T093	VEE		17	0	1	0	1	0	1	8	30							
32	S2190	VEE		17	0	0	0	1	1	0	0	30	33						
33	T095	VEE		17	0	1	0	0	1	0	40	32	34						

34	T096	VEE	17	0	1	0	0	1	0	25	33	35			
35	T211	VEE	17	0	1	0	1	0	1	14	34	36			
36	T212-VEE	VEE	17	0	1	0	1	0	1	6	35				
37	F22-535	VEE	17	0	0	1	1	0	1	0	20	38			
38	S2071	VEE	17	0	0	0	1	0	1	0	37	39	42		
39	S2074	VEE	17	0	0	0	1	0	1	0	38	40	41		
40	T134-VEE	VEE	17	0	1	0	1	0	1	3	39				
41	T094	VEE	17	0	1	0	1	0	1	17	39				
42	S2104	VEE	17	0	0	0	1	0	1	0	38	43	45		
43	T236-VEE	VEE	17	0	1	0	1	0	1	4	42	44			
44	T097	VEE	17	0	1	0	1	0	1	12	43				
45	F22-529	VEE	17	0	0	1	1	0	1	0	42	46			
46	S2117	VEE	17	0	0	0	1	1	0	0	45	47			
47	S2118	VEE	17	0	0	0	1	0	1	0	46	48			
48	S2120	VEE	17	0	0	0	1	0	1	0	47	49	50		
49	T186	VEE	17	0	1	0	1	0	1	5	48				
50	S2127	VEE	17	0	0	0	1	1	0	0	48	51			
51	S2128	VEE	17	0	0	0	1	0	1	0	50	52	53		
52	T187	VEE	17	0	1	0	1	1	0	16	51				
53	S2131	VEE	17	0	0	0	1	0	1	0	51	54	57		
54	S2242	VEE	17	0	0	0	1	0	1	0	53	55	56		
55	T188	VEE	17	0	1	0	1	0	1	5	54				
56	T207	VEE	17	0	1	0	1	0	1	20	54				
57	F22-537	VEE	17	0	0	1	1	0	1	0	53	58			
58	S2137	VEE	17	0	0	0	1	0	1	0	57	59	63		
59	S2252	VEE	17	0	0	0	1	0	1	0	58	60	61		
60	T191	VEE	17	0	1	0	1	0	1	10	59				
61	S2705	VEE	17	0	0	0	1	1	0	0	59	62			
62	T190	VEE	17	0	1	0	1	1	0	14	61				
63	T192	VEE	17	0	1	0	1	0	1	4	58	64			
64	S2143	VEE	17	0	0	0	1	0	1	0	63	65	66		
65	T338-SFP	SFP	16	0	1	0	0	1	0	72	64	866	867	868	
66	S2165	VEE	17	0	0	0	1	0	1	0	64	67	68		
67	T073	VEE	17	0	1	0	0	1	0	27	66	386			
68	T193	VEE	17	0	1	0	1	0	1	2	66	69			
69	F22-570	VEE	17	0	0	1	1	0	1	0	68	374			
70	S2442	VEE	15	0	0	0	1	1	0	0	1	71			
71	S2448	VEE	15	0	0	0	1	0	1	0	70	72			
72	T184	VEE	15	0	1	0	0	1	0	56	71	73			
73	T151-VEE	VEE	15	0	1	0	0	1	0	119	72	74	106		
74	T004-VEE	VEE	15	0	1	0	0	1	0	132	73	75	81		
75	T003-VEE	VEE	15	0	1	0	0	1	0	49	74	76			
76	T204-VEE	VEE	15	0	1	0	0	1	0	1	75	77	1	79	130
77	T001-VEE	VEE	15	0	1	0	0	1	0	48	76	78			
78	T002-VEE	VEE	15	0	1	0	0	1	0	45	77				
79	T369	VEE	15	0	1	0	0	1	0	108	76	80			
80	T363	VEE	15	0	1	0	0	1	0	65	79				
81	T139-VEE	VEE	15	0	1	0	0	1	0	356	74	82	83		
82	T136-VEE	VEE	15	0	1	0	0	1	0	112	81				
83	T029-VEE	VEE	15	0	1	0	0	1	0	95	81	84			
84	S2457	VEE	15	0	0	0	1	0	1	0	83	85			

85	T358	VEE	15	0	1	0	1	0	1	31	84	86	
86	S2450	VEE	15	0	0	0	1	1	0	0	85	87	
87	T233-VEE	VEE	15	0	1	0	0	1	0	87	86	88	
88	T232-VEE	VEE	15	0	1	0	0	1	0	53	87	89	
89	T181	VEE	15	0	1	0	0	1	0	62	88	90	122
90	T240-VEE	VEE	15	0	1	0	0	1	0	148	89	91	
91	T182	VEE	15	0	1	0	0	1	0	102	90	92	118
92	T251	VEE	15	0	1	0	0	1	0	4	91	93	
93	T381	VEE	15	0	1	0	0	1	0	99	92	94	
94	T005-VEE	VEE	15	0	1	0	0	1	0	40	93	95	
95	T333-VEE	VEE	15	0	1	0	0	1	0	139	94	96	
96	T379	VEE	15	0	1	0	0	1	0	55	95	97	
97	T183	VEE	15	0	1	0	0	1	0	219	96	98	104
98	T213-VEE	VEE	15	0	1	0	0	1	0	206	97	99	
99	T904	VEE	15	0	1	0	0	1	0	1	98	100	102
100	T237-VEE	VEE	15	0	1	0	0	1	0	2	99	101	118
101	T176	VEE	15	0	1	0	0	1	0	168	100	102	103
102	T175	VEE	15	0	1	0	0	1	0	82	101	99	
103	T174	VEE	15	0	1	0	0	1	0	208	101	104	112
104	T173	VEE	15	0	1	0	0	1	0	49	97	103	105
105	T179	VEE	15	0	1	0	0	1	0	19	104	106	107
106	T355	VEE	15	0	1	0	0	1	0	15	105	73	
107	T395-VEE	VEE	15	0	1	0	0	1	0	7	105	108	
108	T180	VEE	15	0	1	0	0	1	0	72	107	109	
109	T338-VEE	VEE	15	0	1	0	0	1	0	72	108	110	
110	T103-VEE	VEE	15	0	1	0	0	1	0	64	109	1	111
111	T137-VEE	VEE	15	0	1	0	0	1	0	128	110	112	113
112	T902	VEE	15	0	1	0	0	1	0	0	111	103	
113	T165	VEE	16	0	1	0	0	1	0	3	111	114	115 388
114	S2623	VEE	16	0	0	0	1	0	1	0	113	391	
115	S2470	VEE	16	0	0	0	1	0	1	0	113	116	
116	T157	VEE	16	0	1	0	1	0	1	1	115	117	
117	S2461	VEE	15	0	0	0	1	1	0	0	116	1	
118	T164	VEE	15	0	1	0	0	1	0	8	100	91	119
119	S424	VEE	15	0	0	0	1	1	0	0	118	120	446
120	S425	VEE	15	0	0	0	1	0	1	0	119	121	
121	T115	VEE	16	0	1	0	1	0	1	12	120		
122	T231-VEE	VEE	15	0	1	0	0	1	0	56	89	123	
123	T384	VEE	15	0	1	0	0	1	0	1	122	124	129
124	T906	VEE	15	0	1	0	0	1	0	1	123	125	
125	S2362	VEE	15	0	0	0	1	1	0	0	124	126	127
126	F22-599	VEE	15	0	0	1	1	0	1	0	125	135	
127	T026-VEE	VEE	15	0	1	0	1	0	1	28	125	128	129
128	T030-VEE	VEE	15	0	1	0	1	0	1	3	127	129	
129	S2373	VEE	15	0	0	0	1	0	1	0	127	128	123
130	S2299	VEE	15	0	0	0	1	1	0	0	76	131	
131	F22-633	VEE	25	0	0	1	1	0	1	0	130	132	133
132	T344-VEE	VEE	25	0	1	0	1	0	1	1	131		
133	S2307	VEE	25	0	0	0	1	0	1	0	131	134	135
134	T033-VEE	VEE	25	0	1	0	1	0	1	7	133		
135	S2324	VEE	25	0	0	0	1	0	1	0	133	126	136 153

136	S2327	VEE	25	0	0	0	1	0	1	0	135	137	138
137	T370	VEE	25	0	1	0	1	1	0	2	136		
138	S2343	VEE	25	0	0	0	1	0	1	0	136	139	140
139	T368	VEE	25	0	1	0	1	1	0	4	138		
140	KGP		25	0	0	0	0	1	0	0	138	141	451
141	T109	VEE	25	0	1	0	1	1	0	13	140	142	
142	S0122	VEE	25	0	0	0	1	0	1	0	141	143	
143	T112-VEE	VEE	25	0	1	0	1	0	1	5	142	144	
144	S0140	VEE	25	0	0	0	1	0	1	0	143	145	146
145	F22-595	VEE	25	0	0	1	1	0	1	0	144	449	
146	F22-510	VEE	25	0	0	1	1	0	1	0	144	147	
147	S0145	VEE	25	0	0	0	1	1	0	0	146	148	
148	T110	VEE	25	0	1	0	1	0	1	8	147	149	
149	S0151	VEE	25	0	0	0	1	1	0	0	148	150	
150	S0153	VEE	25	0	0	0	1	0	1	0	149	151	152
151	T135-VEE	VEE	25	0	1	0	1	0	1	27	150		
152	T138-VEE	VEE	25	0	1	0	1	0	1	8	150		
153	OF22-527	VEE	25	0	0	1	1	0	1	0	135	154	
154	S2390	VEE	25	0	0	0	1	1	0	0	153	155	158
155	S2405	VEE	25	0	0	0	1	0	1	0	154	156	157
156	T199	VEE	25	0	1	0	1	0	1	23	155		
157	T227-VEE	VEE	25	0	1	0	1	0	1	10	155		
158	F22-634	VEE	25	0	0	1	1	0	1	0	154	159	
159	S2392	VEE	25	0	0	0	1	0	1	0	158	160	161	162
160	T025-VEE	VEE	25	0	1	0	1	0	1	3	159		
161	T387	VEE	25	0	1	0	1	1	0	3	159		
162	S2399	VEE	25	0	0	0	1	0	1	0	159	163	169
163	S2412	VEE	25	0	0	0	1	0	1	0	162	164	
164	T024-VEE	VEE	25	0	1	0	0	1	0	12	163	165	
165	HK001		25	0	0	0	1	1	0	0	164	166	167
166	T201-VEE	VEE	25	0	1	0	1	1	0	10	165		
167	S2423	VEE	25	0	0	0	1	0	1	0	165	168	
168	T200	VEE	25	0	1	0	1	0	1	13	167		
169	F22-579	VEE	25	0	0	1	1	0	1	0	162	170	
170	T023-VEE	VEE	25	0	1	0	1	0	1	17	169	171	173
171	F22-604	VEE	25	0	0	1	1	0	1	0	170	172	
172	T202-VEE	VEE	25	0	1	0	1	0	1	16	171		
173	T022-VEE	VEE	25	0	1	0	1	0	1	1	170	174	
174	F22-591	VEE	25	0	0	1	1	0	1	0	173	175	
175	S0646	VEE	25	0	0	0	1	0	1	0	174	176	187
176	T017-VEE	VEE	25	0	1	0	1	0	1	5	175	177	
177	S0695	VEE	25	0	0	0	1	0	1	0	176	178	184
178	S0700	VEE	25	0	0	0	1	1	1	0	177	179	
179	S0701	VEE	25	0	0	0	1	0	1	0	178	180	
180	S0705	VEE	25	0	0	0	1	0	1	0	179	181	182
181	T391-VEE	VEE	25	0	1	0	0	1	0	9	180		
182	T365	VEE	25	0	1	0	1	0	1	2	180	183	
183	T018-VEE	VEE	25	0	1	0	1	0	1	30	182		
184	T019-VEE	VEE	25	0	1	0	1	0	1	3	177	185	
185	S0716	VEE	25	0	0	0	1	1	0	0	184	186	
186	T020-VEE	VEE	25	0	1	0	1	0	1	8	185		

187	F22-578	VEE	25	0	0	1	1	0	1	0	175	188		
188	S0640	VEE	25	0	0	0	1	0	1	0	187	189	190	
189	T015-VEE	VEE	25	0	1	0	1	0	1	21	188			
190	S0632	VEE	25	0	0	0	1	0	1	0	188	191	192	195
191	T027-VEE	VEE	25	0	1	0	1	0	1	3	190			
192	S678	VEE	25	0	0	0	1	0	1	0	190	193	194	
193	T028-VEE	VEE	25	0	1	0	1	1	0	1	192			
194	T169	VEE	25	0	1	0	1	0	1	5	192			
195	S0626	VEE	25	0	0	0	1	0	1	0	190	196	198	
196	S0614	VEE	25	0	0	0	1	1	0	0	195	197		
197	T234-FVK	FVK	17	0	1	0	0	1	0	109	196	466		
198	F22-576	VEE	25	0	0	1	1	0	1	0	195	199		
199	S1889	VEE	25	0	0	0	1	0	1	0	198	200	201	
200	T214-VEE	VEE	25	0	1	0	1	0	1	4	199			
201	S1872	VEE	25	0	0	0	1	0	1	0	199	202	203	
202	T143-VEE	VEE	25	0	1	0	1	0	1	10	201			
203	S1989	VEE	25	0	0	0	1	1	0	0	201	204		
204	S1660	VEE	25	0	0	0	1	0	1	0	203	205		
205	S1654	VEE	25	0	0	0	1	1	0	0	204	206	207	
206	T170	VEE	25	0	1	0	1	0	1	6	205			
207	HG01	VEE	25	0	0	0	0	1	0	0	205	208	209	
208	T382	VEE	25	0	1	0	1	0	0	5	207			
209	HG02	VEE	25	0	0	0	0	1	0	0	207	210	211	
210	T132-VEE	VEE	25	0	1	0	1	1	0	6	209			
211	S1648	VEE	25	0	0	0	1	0	1	0	209	212	213	
212	T386	VEE	25	0	1	0	0	1	0	1	211			
213	S1647	VEE	25	0	0	0	1	0	1	0	211	214	215	
214	T039-VEE	VEE	25	0	1	0	1	1	0	4	213			
215	S1644	VEE	25	0	0	0	1	0	1	0	213	216	217	
216	T040-VEE	VEE	25	0	1	0	1	0	1	12	215			
217	T038-VEE	VEE	25	0	1	0	1	0	1	2	215	218		
218	F22-636	VEE	25	0	0	1	1	0	1	0	217	260		
219	S1398	VEE	14	0	0	0	1	0	1	0	1	220	238	
220	T394-VEE	VEE	14	0	1	0	0	1	0	1	219			
221	S1404	VEE	14	0	0	0	1	0	1	0	238	222	223	
222	F22-545	VEE	14	0	0	1	1	0	1	0	221	279		
223	S1527	VEE	14	0	0	0	1	0	1	0	221	224	225	
224	T396-VEE	VEE	14	0	1	0	1	1	0	2	223			
225	S1529	VEE	14	0	0	0	1	0	1	0	223	226	228	
226	T162	VEE	14	0	1	0	1	1	0	6	225	227		
227	T163	VEE	14	0	1	0	1	1	0	2	226			
228	S1538	VEE	14	0	0	0	1	1	0	0	225	229		
229	S1540	VEE	14	0	0	0	1	0	1	0	228	230	231	
230	T178	VEE	14	0	1	0	1	0	1	3	229			
231	S1548	VEE	14	0	0	0	1	1	0	0	229	232		
232	T140	VEE	14	0	1	0	0	1	0	16	231	233	234	
233	T376	VEE	14	0	1	0	0	1	0	8	232			
234	S1568	VEE	14	0	0	0	1	0	1	0	232	235		
235	S1572	VEE	14	0	0	0	1	0	1	0	234	236	242	
236	S1664	VEE	14	0	0	0	1	0	1	0	235	237	239	
237	T032-VEE	VEE	14	0	1	0	1	0	1	6	236			

238	F22-611	VEE	14	0	0	1	1	0	1	0	219	221		
239	S1673	VEE	14	0	0	0	1	1	0	0	236	240		
240	T034-VEE	VEE	14	0	1	0	1	1	0	2	239	241		
241	T035-VEE	VEE	14	0	1	0	1	1	0	7	240			
242	F22-551	VEE	14	0	0	1	1	0	1	0	235	243		
243	T141-VEE	VEE	14	0	1	0	1	0	1	10	242	244		
244	T036-VEE	VEE	14	0	1	0	1	0	1	20	243	245		
245	F22-592	VEE	14	0	0	1	1	0	1	0	244	246		
246	S1755	VEE	14	0	0	0	1	1	0	0	245	247	250	
247	F22-552	VEE	14	0	0	1	1	1	0	0	246	248		
248	T142-VEE	VEE	14	0	1	0	1	0	1	32	247	249		
249	T203-VEE	VEE	14	0	1	0	1	0	1	7	248			
250	S1600	VEE	14	0	0	0	1	1	0	0	246	251		
251	T070	VEE	14	0	1	0	1	0	1	2	250	252		
252	S1606	VEE	14	0	0	0	1	0	1	0	251	253	257	258
253	F22-553	VEE	14	0	0	1	1	0	1	0	252	254		
254	S1735	VEE	14	0	0	0	1	0	1	0	253	255	256	
255	T046-VEE	VEE	14	0	1	0	1	0	1	15	254			
256	T047-VEE	VEE	14	0	1	0	1	0	1	3	254			
257	F22-593	VEE	14	0	0	1	1	0	1	0	252	341		
258	T045-VEE	VEE	14	0	1	0	1	0	1	3	252	259		
259	F22-554	VEE	14	0	0	1	1	0	1	0	258	260		
260	S1622	VEE	14	0	0	0	1	0	1	0	259	261	218	262
261	T037-VEE	VEE	14	0	1	0	1	0	1	3	260			
262	T041-VEE	VEE	14	0	1	0	1	0	1	6	260	263		
263	F22-587	VEE	14	0	0	1	1	0	1	0	262	264		
264	S1775	VEE	14	0	0	0	1	1	0	0	263	265	270	
265	T044-VEE	VEE	14	0	1	0	0	1	0	37	264	266		
266	S1788	VEE	14	0	0	0	1	0	1	0	265	267		
267	S1797	VEE	14	0	0	0	1	0	1	0	266	268	269	
268	T208-VEE	VEE	14	0	1	0	1	0	1	4	267			
269	T209	VEE	14	0	1	0	1	0	1	3	267			
270	S1823	VEE	14	0	0	0	1	1	0	0	264	271	274	
271	S1855	VEE	14	0	0	0	1	0	1	0	270	272		
272	S1862	VEE	14	0	0	0	1	1	0	0	271	273		
273	T042-VEE	VEE	14	0	1	0	0	1	0	28	272			
274	F22-588	VEE	14	0	0	1	1	0	1	0	270	275		
275	S1841	VEE	14	0	0	0	1	1	0	0	274	276		
276	T043-VEE	VEE	14	0	1	0	0	1	0	15	275			
277	S1001	VEE	23	0	0	0	1	0	1	0	1	278		
278	F22-623	VEE	23	0	0	1	1	0	1	0	277	279		
279	S1002	VEE	23	0	0	0	1	0	1	0	222	278	280	
280	S1007	VEE	23	0	0	0	1	0	1	0	279	281	282	
281	T154-VEE	VEE	23	0	1	0	1	0	1	9	280			
282	S1014	VEE	23	0	0	0	1	0	1	0	280	283	289	
283	F22-544	VEE	23	0	0	1	1	1	0	0	282	284		
284	T088	VEE	23	0	1	0	1	1	0	14	283	285		
285	S1118	VEE	23	0	0	0	1	0	1	0	284	286		
286	S1123	VEE	23	0	0	0	1	0	1	0	285	287	288	
287	T155-VEE	VEE	23	0	1	0	1	0	1	3	286			
288	T156	VEE	23	0	1	0	1	0	1	6	286			

289	T087	VEE	23	0	1	0	1	0	1	32	282	290	
290	S1031	VEE	23	0	0	0	1	1	0	0	289	291	292
291	T086	VEE	23	0	1	0	1	1	0	11	290		
292	S1033	VEE	23	0	0	0	1	0	1	0	290	293	
293	T161	VEE	23	0	1	0	1	0	1	3	292	294	
294	S1135	VEE	23	0	0	0	1	0	1	0	293	295	376
295	OF22-542	VEE	23	0	0	1	1	0	1	0	294	296	
296	S1051	VEE	23	0	0	0	1	0	1	0	295	297	298
297	T172	VEE	23	0	1	0	1	0	1	35	296		
298	S1074	VEE	23	0	0	0	1	0	1	0	296	299	300 306
299	T067-VEE	VEE	23	0	1	0	1	0	1	8	298		
300	S1201	VEE	23	0	0	0	1	0	1	0	298	301	302
301	T068-VEE	VEE	23	0	1	0	1	1	0	8	300		
302	F22-566	VEE	23	0	0	1	1	0	1	0	300	303	
303	T081-VEE	VEE	23	0	1	0	1	0	1	1	302	304	
304	T133-VEE	VEE	23	0	1	0	1	0	1	6	303	305	
305	T069-VEE	VEE	23	0	1	0	1	0	1	13	304		
306	S1085A	VEE	23	0	0	0	1	1	0	0	298	307	
307	T080	VEE	23	0	1	0	0	1	0	48	306	308	
308	T145	VEE	23	0	1	0	0	1	0	50	307	309	
309	T079	VEE	23	0	1	0	0	1	0	16	308	310	
310	S1089	VEE	23	0	0	0	1	0	1	0	309	311	313
311	S1240	VEE	23	0	0	0	1	1	0	0	310	312	
312	T013-VEE	VEE	23	0	1	0	0	1	0	13	311		
313	OF22-562	VEE	23	0	0	1	1	0	1	0	310	314	
314	T031-VEE	VEE	23	0	1	0	1	0	1	8	313	315	
315	S1097	VEE	23	0	0	0	1	0	1	0	314	316	343
316	S1103	VEE	23	0	0	0	1	0	1	0	315	317	319
317	S1357	VEE	23	0	0	0	1	1	0	0	316	318	
318	T058-VEE	VEE	23	0	1	0	1	1	0	27	317		
319	F22-619	VEE	23	0	0	1	1	0	1	0	316	320	
320	S1929	VEE	23	0	0	0	1	1	0	0	319	321	329
321	T053-VEE	VEE	23	0	1	0	1	0	1	6	320	322	
322	F22-618	VEE	23	0	0	1	1	0	1	0	321	323	
323	S1939	VEE	23	0	0	0	1	0	1	0	322	324	325
324	T054	VEE	23	0	1	0	1	1	0	11	323		
325	S1949	VEE	23	0	0	0	1	0	1	0	323	326	327
326	T055-VEE	VEE	23	0	1	0	1	0	1	5	325		
327	S1957	VEE	23	0	0	0	1	1	0	0	325	328	
328	T056-VEE	VEE	23	0	1	0	1	1	0	7	327		
329	S1931	VEE	23	0	0	0	1	0	1	0	320	330	
330	F22-617	VEE	23	0	0	1	1	0	1	0	329	331	
331	T050-VEE	VEE	23	0	1	0	1	1	0	9	330	332	339
332	S1894	VEE	23	0	0	0	1	0	1	0	331	333	
333	F22-556	VEE	23	0	0	1	1	0	1	0	332	334	
334	S1902	VEE	23	0	0	0	1	0	1	0	333	335	336 337
335	T049-VEE	VEE	23	0	1	0	1	0	1	13	334		
336	T051-VEE	VEE	23	0	1	0	1	0	1	1	334		
337	T052-VEE	VEE	23	0	1	0	1	0	1	4	334	338	
338	T210-VEE	VEE	23	0	1	0	1	0	1	3	337		
339	S1712	VEE	23	0	0	0	1	0	1	0	331	340	

340	T206-VEE	VEE	23	0	1	0	1	0	1	1	339	341	
341	S1704	VEE	23	0	0	0	1	0	1	0	257	340	342
342	T048-VEE	VEE	23	0	1	0	1	0	1	8	341		
343	T059-VEE	VEE	23	0	1	0	1	0	1	15	315	344	
344	F22-559	VEE	23	0	0	1	1	0	1	0	343	345	
345	S1249	VEE	23	0	0	0	1	0	1	0	344	346	350
346	F22-596	VEE	23	0	0	1	1	0	1	0	345	347	
347	T061-VEE	VEE	23	0	1	0	1	0	1	3	346	348	
348	T060-VEE	VEE	23	0	1	0	1	0	1	2	347	349	
349	T076	VEE	23	0	1	0	1	0	1	6	348		
350	S1253	VEE	23	0	0	0	1	0	1	0	345	351	352
351	T062-VEE	VEE	23	0	1	0	1	0	1	12	350		
352	F22-561	VEE	23	0	0	1	1	0	1	0	350	353	
353	S1265	VEE	23	0	0	0	1	0	1	0	352	354	355
354	T063-VEE	VEE	23	0	1	0	1	0	1	5	353		
355	S1278	VEE	23	0	0	0	1	0	1	0	353	356	358
356	T064-VEE	VEE	23	0	1	0	1	1	0	6	355	357	
357	T393	VEE	23	0	1	0	0	1	0	34	356		
358	S1281	VEE	23	0	0	0	1	0	1	0	355	359	360
359	T065-VEE	VEE	23	0	1	0	1	0	1	39	358		
360	F22-568	VEE	23	0	0	1	1	0	1	0	358	361	
361	T066-VEE	VEE	23	0	1	0	1	0	1	6	360	362	960
362	F22-569	VEE	23	0	0	1	1	0	1	0	361	363	
363	S1289	VEE	23	0	0	0	1	0	1	0	362	364	365
364	T198	VEE	23	0	1	0	1	0	1	9	363		
365	S1292	VEE	23	0	0	0	1	0	1	0	363	366	367
366	T371	VEE	23	0	1	0	1	1	0	5	365		
367	S1297	VEE	23	0	0	0	1	0	1	0	365	368	369
368	T197	VEE	23	0	1	0	1	0	1	4	367		
369	S1298	VEE	23	0	0	0	1	1	0	0	367	370	371
370	T196	VEE	23	0	1	0	1	0	1	8	369		
371	S1305	VEE	23	0	0	0	1	0	1	0	369	372	
372	S1308	VEE	23	0	0	0	1	0	1	0	371	373	374
373	T195	VEE	23	0	1	0	1	1	0	18	372		
374	S1313	VEE	23	0	0	0	1	0	1	0	69	372	375
375	T194	VEE	23	0	1	0	1	0	1	7	374		
376	OF22-541	VEE	23	0	0	1	1	0	1	0	294	377	
377	T071-VEE	VEE	23	0	1	0	1	1	0	3	376	378	
378	T083	VEE	23	0	1	0	1	0	1	3	377	379	
379	S1152	VEE	23	0	0	0	1	0	1	0	378	380	382
380	S1167	VEE	23	0	0	0	1	1	0	0	379	381	
381	T085	VEE	23	0	1	0	0	1	0	6	380		
382	S1157	VEE	23	0	0	0	1	1	0	0	379	383	384
383	T075	VEE	23	0	1	0	1	1	0	3	382		
384	T350	VEE	23	0	1	0	0	1	0	121	382	385	
385	T072-VEE	VEE	23	0	1	0	0	1	0	49	384	386	
386	T077	VEE	23	0	1	0	0	1	0	110	67	385	387
387	T367	VEE	23	0	1	0	0	1	0	34	386		
388	T400	VEE	25	0	1	0	0	1	0	1	1	113	
389	T104-VEE	VEE	16	0	1	0	0	1	0	58	391		
390	T105-VEE	VEE	16	0	1	0	0	1	0	71	392		

391	S2477	VEE	16	0	0	0	1	0	1	0	114	389	392
392	S2483	VEE	16	0	0	0	1	0	1	0	390	391	393
393	S2487	VEE	16	0	0	0	1	0	1	0	392	394	398
394	S2518	VEE	16	0	0	0	1	1	0	0	393	395	
395	T340-VEE	VEE	16	0	1	0	0	1	0	34	394	396	
396	S2519	VEE	16	0	0	0	1	0	1	0	395	397	
397	T106-VEE	VEE	16	0	1	0	1	0	1	51	396		
398	S2497	VEE	16	0	0	0	1	0	1	0	393	399	400
399	T107	VEE	16	0	1	0	1	0	1	1	398		
400	F22-518	VEE	16	0	0	1	1	0	1	0	398	401	
401	S2501	VEE	16	0	0	0	1	0	1	0	400	402	404
402	S2528	VEE	16	0	0	0	1	1	0	0	401	403	
403	T108	VEE	16	0	1	0	0	1	0	26	402		
404	S2503	VEE	16	0	0	0	1	0	1	0	401	405	407
405	T380	VEE	16	0	1	0	0	1	0	53	404	406	
406	T383	VEE	16	0	1	0	0	1	0	113	405		
407	S2508	VEE	16	0	0	0	1	1	0	0	404	408	
408	T121-VEE	VEE	16	0	1	0	0	1	0	26	407	409	
409	S1485	VEE	16	0	0	0	1	0	1	0	408	410	
410	S1490	VEE	16	0	0	0	1	0	1	0	409	411	412
411	T120-VEE	VEE	16	0	1	0	0	1	0	5	410		
412	S1504	VEE	16	0	0	0	1	0	1	0	410	413	414
413	T129-VEE	VEE	16	0	1	0	1	0	1	1	412		
414	S1516	VEE	16	0	0	0	1	1	0	0	412	415	416
415	T122-VEE	VEE	16	0	1	0	1	0	1	8	414		
416	T117-VEE	VEE	16	0	1	0	0	1	0	57	414	417	
417	T119-VEE	VEE	16	0	1	0	0	1	0	74	416	418	
418	T118	VEE	16	0	1	0	0	1	0	114	417	419	
419	S350	VEE	16	0	0	0	1	0	1	0	418	420	
420	S346	VEE	16	0	0	0	1	0	1	0	419	421	422
421	T021-VEE	VEE	16	0	1	0	1	0	1	7	420		
422	S331	VEE	16	0	0	0	1	0	1	0	420	423	425
423	T392-VEE	VEE	16	0	1	0	1	1	0	2	422	424	
424	T218-VEE	VEE	16	0	1	0	1	0	1	1	423		
425	S326	VEE	16	0	0	0	1	0	1	0	422	426	427
426	T217-VEE	VEE	16	0	1	0	1	1	0	3	425		
427	F22-514	VEE	16	0	0	1	1	0	1	0	425	428	
428	T116	VEE	16	0	1	0	1	0	1	6	427	429	
429	S279	VEE	16	0	0	0	1	0	1	0	428	430	431
430	T150	VEE	16	0	1	0	1	0	1	11	429		
431	S271	VEE	16	0	0	0	1	0	1	0	429	432	433
432	T149	VEE	16	0	1	0	1	0	1	4	431		
433	T148	VEE	16	0	1	0	1	0	1	6	431	434	
434	S225	VEE	16	0	0	0	1	0	1	0	433	435	436
435	T147	VEE	16	0	1	0	1	0	1	12	434		
436	OF22-508	VEE	16	0	0	1	1	0	1	0	434	437	
437	T146	VEE	16	0	1	0	1	0	1	5	436	438	
438	S203	VEE	16	0	0	0	1	0	1	0	437	439	442
439	S212	VEE	16	0	0	0	1	0	1	0	438	440	441
440	T160	VEE	16	0	1	0	1	0	1	6	439		
441	T159	VEE	16	0	1	0	1	0	1	9	439		

442	S197	VEE	16	0	0	0	1	0	1	0	438	443	445	447	
443	T111-VEE	VEE	16	0	1	0	1	1	0	22	442	444			
444	T158	VEE	16	0	1	0	1	1	0	14	443				
445	F22-624	VEE	16	0	0	1	1	0	1	0	442	446			
446	T113	VEE	16	0	1	0	1	0	1	3	119	445			
447	S190	VEE	16	0	0	0	1	0	1	0	442	448	449		
448	T114	VEE	16	0	1	0	1	0	1	21	447				
449	S185	VEE	16	0	0	0	1	0	1	0	145	447	450		
450	T131-VEE	VEE	16	0	1	0	1	0	1	4	449				
451	T388	FVK	17	0	1	0	0	1	0	0	0	452	455	779	140
452	T391-FVK	FVK	17	0	1	0	0	1	0	10	451	453			
453	T392-FVK	FVK	17	0	1	0	0	1	0	22	452	454			
454	T126-FVK	FVK	17	0	1	0	0	1	0	22	453				
455	HG-05	FVK	17	0	0	0	0	1	0	0	451	456	457		
456	T025-FVK	FVK	17	0	1	0	1	1	0	5	455				
457	T394-FVK	FVK	17	0	1	0	0	1	0	14	455	458	459		
458	T235-FVK	FVK	17	0	1	0	0	1	0	21	457				
459	T364	FVK	17	0	1	0	1	1	0	7	457	460			
460	T395-FVK	FVK	17	0	1	0	0	1	0	9	459	461			
461	T008-FVK	FVK	17	0	1	0	0	1	0	95	460	462	466		
462	HG-06	FVK	17	0	0	0	0	1	0	0	461	463	464		
463	T307-FVK	FVK	17	0	0	0	1	1	0	38	462				
464	T356	FVK	17	0	1	0	0	1	0	108	462	465			
465	T171	FVK	17	0	1	0	0	1	0	127	464	767			
466	T346	FVK	17	0	1	0	0	1	0	74	197	461	467		
467	T311	FVK	17	0	1	0	1	1	0	3	466	468			
468	HG-07	FVK	17	0	0	0	0	1	0	0	467	469	470		
469	T396-FVK	FVK	17	0	1	0	0	1	0	1	468				
470	T313	FVK	17	0	1	0	1	1	0	5	468	471	472		
471	T310	FVK	17	0	1	0	1	1	0	4	470				
472	T907	FVK	17	0	1	0	0	1	0	1	470	473			
473	T908	FVK	17	0	1	0	0	1	0	1	472				
474	SNR			1	0	0	0	1	0	0	475	513	518	521	525	957
475	T051-SNR	SNR	13	0	1	0	0	1	0	51	474	476				
476	T037-SNR	SNR	13	0	1	0	0	1	0	1	475	477				
477	T019-SNR	SNR	13	0	1	0	0	1	0	45	476	478	483	479	
478	T020-SNR	SNR	13	0	1	0	0	1	0	3	477				
479	T017-SNR	SNR	13	0	1	0	0	1	0	13	477	480			
480	HK-002	SNR	13	0	0	0	0	1	0	0	479	481	482		
481	T053-SNR	SNR	13	0	1	0	0	1	0	4	480				
482	T013-SNR	SNR	13	0	1	0	0	1	0	102	480	483	484		
483	T033-SNR	SNR	13	0	1	0	0	1	0	84	477	482			
484	T031-SNR	SNR	13	0	1	0	0	1	0	59	482	485			
485	T015-SNR	SNR	13	0	1	0	0	1	0	158	484	486	491	497	
486	T049-SNR	SNR		0	1	0	0	1	0	1	485	487			
487	T003-SNR	SNR		0	1	0	0	1	0	1	486	488			
488	T036-SNR	SNR		0	1	0	0	1	0	1	487	489	959		
489	T002-SNR	SNR		0	1	0	0	1	0	1	488	490			
490	T039-SNR	SNR		0	1	0	0	1	0	1	489	491	501		
491	T004-SNR	SNR		0	1	0	0	1	0	1	485	490	492		
492	T030-SNR	SNR		0	1	0	0	1	0	1	491	493			

493	T048-SNR	SNR		0	1	0	0	1	0	1	492	494						
494	T005-SNR	SNR		0	1	0	0	1	0	1	493	495						
495	T042-SNR	SNR		0	1	0	0	1	0	1	494	496						
496	T006-SNR	SNR		0	1	0	0	1	0	1	495	501						
497	T014-SNR	SNR		0	1	0	0	1	0	1	485	498						
498	T016-SNR	SNR		0	1	0	0	1	0	1	497	499						
499	T027-SNR	SNR		0	1	0	0	1	0	1	498	500						
500	T052-SNR	SNR		0	1	0	0	1	0	1	499	501						
501	SNRV			1	0	0	0	1	0	0	490	496	500	502	522			
502	T050-SNR	SNR		0	1	0	0	1	0	1	501	503						
503	T008-SNRV	SNRV		0	1	0	0	1	0	69	502	504	519					
504	T034-SNRV	SNRV		0	1	0	0	1	0	1	503	505						
505	T009-SNR	SNR		0	1	0	0	1	0	103	504	506	509	511				
506	T040-SNR	SNR		0	1	0	0	1	0	60	505	507	508					
507	T018-SNR	SNR		0	1	0	0	1	0	18	506							
508	T041-SNR	SNR		0	1	0	0	1	0	82	506	509						
509	T010-SNR	SNR		0	1	0	0	1	0	94	505	508	510	516				
510	T023-SNR	SNR		0	1	0	0	1	0	110	509	512						
511	T035-SNR	SNR		0	1	0	0	1	0	204	505	516	517					
512	T029-SNR	SNR		0	1	0	0	1	0	32	510	513						
513	T022-SNR	SNR		0	1	0	0	1	0	87	474	512	514	515				
514	T044-SNR	SNR		0	1	0	0	1	0	4	513							
515	T024-SNR	SNR		0	1	0	0	1	0	37	513							
516	T028-SNR	SNR		0	1	0	0	1	0	101	509	511						
517	T032-SNR	SNR		0	1	0	0	1	0	97	511	518						
518	T021-SNR	SNR		0	1	0	0	1	0	73	474	517						
519	T111-SNR	SNR		0	1	0	0	1	0	74	503	520						
520	T011-SNR	SNR		0	1	0	0	1	0	93	519	521						
521	T047-SNR	SNR		0	1	0	0	1	0	38	474	520						
522	T012-SNRV	SNRV		0	1	0	0	1	0	204	501	523						
523	T026-SNR	SNR		0	1	0	0	1	0	144	522	524						
524	T045-SNR	SNR		0	1	0	0	1	0	25	523	525						
525	T025-SNR	SNR		0	1	0	0	1	0	125	474	524						
526	SLA			1	0	0	0	1	0	0	527	543	549	554	555	584	585	684	701
527	T060-SLA	SLA	4	0	1	0	0	1	0	107	526	528						
528	T040-SLA	SLA		0	1	0	0	1	0	113	527	529						
529	T041-SLA	SLA		0	1	0	0	1	0	122	528	530						
530	T059-SLA	SLA		0	1	0	0	1	0	127	529	531	536					
531	T061-SLA	SLA		0	1	0	0	1	0	25	530	532						
532	T334-SLA	SLA		0	1	0	0	1	0	9	531	533						
533	S552	SLA		0	0	0	1	0	1	0	532	534						
534	T240-SLA	SLA		0	1	0	1	0	1	9	533	535						
535	F12-346	SLA		0	0	1	1	0	1	0	534	644						
536	T062-SLA	SLA		0	1	0	0	1	0	80	530	537						
537	T063-SLA	SLA		0	1	0	0	1	0	74	536	538						
538	T082	SLA		0	1	0	0	1	0	58	537	539						
539	T081-SLA	SLA		0	1	0	0	1	0	76	538	540						
540	T295	SLA		0	1	0	0	1	0	26	539	541	544					
541	T294	SLA		0	1	0	0	1	0	43	540	542						
542	T069-SLA	SLA		0	1	0	0	1	0	93	541	543						
543	T290	SLA		0	1	0	0	1	0	91	526	542						

544	T057	SLA		0	1	0	0	1	0	95	540	545	546
545	S0214	SLA		0	0	0	1	0	1	0	544	665	
546	T042-SLA	SLA		0	1	0	0	1	0	214	544	547	
547	T013-SLA	SLA		0	1	0	0	1	0	88	546	548	550
548	T052-SLA	SLA		0	1	0	0	1	0	323	547	549	552
549	T039-SLA	SLA		0	1	0	0	1	0	215	526	548	
550	T048-SLA	SLA		0	1	0	0	1	0	27	547	551	
551	T922	SLA		0	1	0	0	1	0	1	550	557	
552	T055-SLA	SLA		0	1	0	0	1	0	145	548	553	567
553	T012-SLA	SLA		0	1	0	0	1	0	485	552	554	
554	T011-SLA	SLA		0	1	0	0	1	0	101	526	553	
555	T924	SLA		0	1	0	0	1	0	1	526	556	
556	T921	SLA		0	1	0	0	1	0	1	555	581	
557	T071-SLA	SLA		0	1	0	0	1	0	60	551	558	
558	T043-SLA	SLA		0	1	0	0	1	0	54	557	559	
559	T335-SLA	SLA		0	1	0	0	1	0	7	558	560	
560	T072-SLA	SLA		0	1	0	0	1	0	34	559	561	562
561	T338-SLA	SLA		0	1	0	0	1	0	50	560	567	
562	T293	SLA		0	1	0	0	1	0	14	560	563	564
563	T022-SLA	SLA		0	1	0	0	1	0	311	562	570	
564	T018-SLA	SLA		0	1	0	0	1	0	43	562	565	566
565	T066-SLA	SLA		0	1	0	0	1	0	29	564	573	
566	T070-SLA	SLA		0	1	0	0	1	0	137	564	571	
567	T014-SLA	SLA		0	1	0	0	1	0	133	552	561	568
568	T298	SLA		0	1	0	0	1	0	52	567	569	
569	T015-SLA	SLA		0	1	0	0	1	0	95	568	570	579
570	T068-SLA	SLA		0	1	0	0	1	0	33	563	569	
571	T067-SLA	SLA		0	1	0	0	1	0	57	566	572	
572	T065-SLA	SLA		0	1	0	0	1	0	79	571	573	579
573	T023-SLA	SLA		0	1	0	0	1	0	66	565	574	572
574	T064-SLA	SLA	17	0	1	0	0	1	0	42	573	575	578
575	S2417	SLA	17	0	1	0	0	1	0	0	574	685	
576	F12-301	SLA	17	0	1	0	0	1	0	0	685	687	
577	T024-SLA	SLA	17	0	1	0	0	1	0	44	686	688	
578	F12-597	SLA	17	0	1	0	0	1	0	0	574	689	
579	T016-SLA	SLA		0	1	0	0	1	0	62	569	572	580 582
580	T918	SLA		0	1	0	0	1	0	1	579	581	
581	T020-SLA	SLA		0	1	0	0	1	0	18	556	580	
582	T017-SLA	SLA		0	1	0	0	1	0	117	579	583	
583	T047-SLA	SLA		0	1	0	0	1	0	68	582	584	
584	T053-SLA	SLA		0	1	0	0	1	0	161	526	583	
585	S651	SLA	7	0	0	0	1	0	1	0	526	586	
586	T058-SLA	SLA	7	0	1	0	1	0	1	6	585	587	
587	S656	SLA	7	0	0	0	1	0	1	0	586	588	589
588	T337	SLA	7	0	1	0	1	1	0	5	587		
589	T219	SLA	7	0	1	0	1	0	1	1	587	590	
590	S680	SLA	7	0	0	0	1	0	1	0	589	591	592
591	T220	SLA	7	0	1	0	1	1	0	4	590		
592	F12-343	SLA	7	0	0	1	1	0	1	0	590	593	
593	S324	SLA	7	0	0	0	1	0	1	0	592	594	616
594	S321	SLA	7	0	0	0	1	0	1	0	593	595	596

595	T221	SLA	7	0	1	0	1	1	0	4	594	
596	F12-340	SLA	7	0	0	1	1	0	1	0	594	597
597	S311	SLA	7	0	0	0	1	0	1	0	596	598	599
598	T222	SLA	7	0	1	0	1	0	1	6	597	
599	T223	SLA	7	0	1	0	1	0	1	7	597	600
600	S233	SLA	7	0	0	0	1	0	1	0	599	601	608
601	F12-337	SLA	7	0	0	1	1	0	1	0	600	602
602	S246	SLA	7	0	0	0	1	0	1	0	601	603	604
603	T226	SLA	7	0	1	0	1	0	1	2	602	
604	T227-SLA	SLA	7	0	1	0	1	0	1	11	602	605
605	S267	SLA	7	0	1	0	1	0	1	0	604	606	607
606	T229	SLA	7	0	1	0	1	0	1	9	605	
607	T228	SLA	7	0	1	0	1	1	0	4	605	
608	F12-336	SLA	7	0	0	1	1	0	1	0	600	609
609	S1190	SLA	7	0	0	0	1	0	1	0	608	610	612
610	T224	SLA	7	0	1	0	1	0	1	2	609	611
611	T242-SLA	SLA	7	0	1	0	1	0	1	8	610	
612	T225	SLA	7	0	1	0	1	0	1	2	609	613
613	F12-333	SLA	7	0	0	1	1	0	1	0	612	614
614	T210-SLA	SLA	7	0	1	0	1	0	1	2	613	615
615	S1152	SLA	7	0	0	0	1	0	1	0	614	
616	F12-347	SLA	7	0	0	1	1	0	1	0	593	617
617	S345	SLA	7	0	0	0	1	0	1	0	616	618	621
618	T330-SLA	SLA	7	0	1	0	1	0	1	1	617	619
619	S388	SLA	7	0	0	0	1	1	0	0	618	620
620	T218-SLA	SLA	7	0	1	0	0	1	0	24	619	
621	S350	SLA	7	0	0	0	1	0	1	0	617	622	623
622	T217-SLA	SLA	7	0	1	0	1	0	1	2	621	
623	S354	SLA	7	0	0	0	1	0	1	0	621	624	625
624	T235-SLA	SLA	7	0	1	0	1	0	1	8	623	
625	S362	SLA	7	0	0	0	1	0	1	0	623	626	627
626	T216	SLA	7	0	1	0	1	0	1	5	625	
627	F12-350	SLA	7	0	0	1	1	0	1	0	625	628
628	T215	SLA	16	0	1	0	1	0	1	2	627	629
629	S368	SLA	16	0	0	0	1	0	1	0	628	630	631
630	T214-SLA	SLA	16	0	1	0	1	0	1	9	629	
631	S380	SLA	16	0	0	0	1	0	1	0	629	632	670
632	F12-338	SLA	16	0	0	1	1	0	1	0	631	633
633	S382	SLA	16	0	0	0	1	1	0	0	632	634
634	S1575	SLA	16	0	0	0	1	0	1	0	633	635	636
635	T236-SLA	SLA	16	0	1	0	1	1	0	34	634	
636	S1570	SLA	16	0	0	0	1	1	0	0	634	637
637	S527	SLA	16	0	0	0	1	0	1	0	636	638	641
638	S1561	SLA	16	0	0	0	1	0	1	0	637	639	640
639	T241-SLA	SLA	16	0	1	0	1	0	1	18	638	
640	S1310	SLA	16	0	0	0	1	0	1	0	638	
641	F12-310	SLA	16	0	0	1	1	0	1	0	637	642
642	T237-SLA	SLA	16	0	1	0	1	0	1	7	641	643
643	S540	SLA	16	0	0	0	1	0	1	0	642	644	645
644	T239	SLA	16	0	1	0	1	0	1	3	643	535
645	T238	SLA	16	0	1	0	1	1	0	9	643	646

646	S2005	SLA	16	0	0	0	1	0	1	0	645	647		
647	F12-342	SLA	16	0	0	1	1	0	1	0	646	648		
648	S2012	SLA	16	0	0	0	1	0	1	0	647	649	650	
649	T282	SLA	16	0	1	0	1	0	1	13	648			
650	T281	SLA	16	0	1	0	1	1	0	7	648	651		
651	S2026	SLA	16	0	0	0	1	0	1	0	650	652	659	
652	T111-SLA	SLA	16	0	1	0	1	1	0	3	651	653		
653	T112-SLA	SLA	16	0	1	0	1	1	0	2	652	654		
654	T299	SLA	16	0	1	0	0	1	0	1	653	655	656	
655	T331-SLA	SLA	16	0	1	0	0	1	0	6	654			
656	T332-SLA	SLA	16	0	1	0	1	0	1	3	654	657		
657	S420	SLA	16	0	0	0	1	1	0	0	656	658		
658	T336-SLA	SLA	16	0	1	0	0	1	0	1	657	736	747	748
659	T283	SLA	16	0	1	0	1	0	1	2	651	660		
660	S2028	SLA	16	0	0	0	1	0	1	0	659	661	662	
661	T284	SLA	16	0	1	0	1	0	1	5	660			
662	F12-332	SLA	16	0	0	1	1	0	1	0	660	663		
663	T056-SLA	SLA	16	0	1	0	1	0	1	16	662	664		
664	S218	SLA	16	0	0	0	1	0	1	0	663	665	666	
665	T046-SLA	SLA	16	0	1	0	1	0	1	24	545	664		
666	S167	SLA	16	0	0	0	1	1	0	0	664	667		
667	T345-SLA	SLA	16	0	1	0	0	1	0	12	666	668		
668	T045-SLA	SLA	16	0	1	0	1	0	1	13	667	669		
669	T044-SLA	SLA	16	0	1	0	0	1	0	76	668			
670	F12-341	SLA	16	0	0	1	1	0	1	0	631	671		
671	T230	SLA	16	0	1	0	1	0	1	6	670	672		
672	S482	SLA	16	0	0	0	1	0	1	0	671	673	674	
673	T245	SLA	16	0	1	0	1	0	1	1	672			
674	S485	SLA	16	0	0	0	1	0	1	0	672	675	676	677
675	T232-SLA	SLA	16	0	1	0	1	0	1	3	674			
676	T231-SLA	SLA	16	0	1	0	1	0	1	7	674			
677	F12-344	SLA	16	0	0	1	1	0	1	0	674	678		
678	S487	SLA	16	0	0	0	1	0	1	0	677	679	680	
679	T234-SLA	SLA	16	0	1	0	1	0	1	34	678			
680	T233-SLA	SLA	16	0	1	0	1	0	1	31	678	681		
681	S0609	SLA	16	0	0	0	1	1	0	0	680	682		
682	T333-SLA	SLA	16	0	1	0	0	1	0	2	681	683		
683	T038-SLA	SLA	16	0	1	0	0	1	0	4	682	684		
684	T037-SLA	SLA	16	0	1	0	0	1	0	15	526	683		
685	S2418	SLA	17	0	0	0	1	0	1	0	575	576	686	
686	S2500	SLA	17	0	0	0	1	1	0	0	685	577		
687	S2424	SLA		0	0	0	1	0	1	0	576	704		
688	S2501	SLA		0	0	0	1	0	1	0	577	690		
689	S2413	SLA		0	0	0	1	0	1	0	578	696	700	
690	T025-SLA	SLA		0	1	0	1	0	1	7	688	691		
691	S2516	SLA		0	0	0	1	0	1	0	690	692	693	
692	T026-SLA	SLA		0	1	0	1	0	1	26	691			
693	S2532	SLA		0	0	0	1	1	0	0	691	694		
694	T027-SLA	SLA		0	1	0	1	0	1	1	693	695		
695	T028-SLA	SLA		0	1	0	1	0	1	9	694			
696	S2475	SLA		0	0	0	1	0	1	0	689	697	698	699

697	T032-SLA	SLA	0	1	0	1	0	1	1	696		
698	T033-SLA	SLA	0	1	0	1	0	1	1	696		
699	T034-SLA	SLA	0	1	0	1	0	1	7	696		
700	T035-SLA	SLA	0	1	0	1	0	1	13	689	701	
701	S2401	SLA	0	0	0	1	1	0	0	526	700	702
702	T036-SLA	SLA	0	1	0	1	0	1	16	701	703	
703	T292	SLA	0	1	0	1	1	0	19	702		
704	S2425	SLA	0	0	0	1	0	1	0	687	705	
705	S2429	SLA	0	0	0	1	0	1	0	704	706	707
706	T029-SLA	SLA	0	1	0	1	0	1	5	705		
707	S2437	SLA	0	0	0	1	0	1	0	705	708	709
708	T031-SLA	SLA	0	1	0	1	0	1	28	707		
709	T296	SLA	0	1	0	1	0	1	7	707	710	
710	S2448	SLA	0	0	0	1	1	0	0	709	711	
711	T030-SLA	SLA	0	1	0	0	1	0	45	710	712	
712	S2378	SLA	0	0	0	1	0	1	0	711	713	714
713	T136-SLA	SLA	0	1	0	1	0	1	3	712		
714	S2369	SLA	0	0	0	1	1	0	0	712	715	716
715	T135-SLA	SLA	0	1	0	1	0	1	10	714		
716	S2367	SLA	0	0	0	1	0	1	0	714	717	
717	S2361	SLA	0	0	0	1	0	1	0	716	718	719
718	T141-SLA	SLA	0	1	0	1	0	1	4	717		
719	F12-349	SLA	0	0	1	1	0	1	0	717	720	
720	S2353	SLA	0	0	0	1	0	1	0	719	721	725
721	F12-330	SLA	0	0	1	1	0	1	0	720	722	
722	T137-SLA	SLA	0	1	0	0	1	0	1	721	723	
723	T138-SLA	SLA	0	1	0	0	1	0	1	722	724	
724	T139-SLA	SLA	0	1	0	0	1	0	1	723		
725	S2328	SLA	0	0	0	1	0	1	0	720	726	731
726	F12-348	SLA	0	0	1	1	0	1	0	725	727	
727	S2339	SLA	0	0	0	1	0	1	0	726	728	729
728	T134-SLA	SLA	0	1	0	1	0	1	4	727		
729	S0077	SLA	0	0	0	1	1	0	0	727	730	
730	T144	SLA	0	1	0	1	0	1	6	729		
731	T133-SLA	SLA	0	1	0	1	1	0	2	725	732	
732	T286	SLA	0	1	0	1	0	1	23	731	733	
733	S2321	SLA	0	0	0	1	1	0	0	732	734	742
734	T132-SLA	SLA	0	1	0	0	1	0	55	733	735	
735	T285	SLA	0	1	0	1	0	1	20	734	736	
736	S2578	SLA	0	0	0	1	0	1	0	658	735	737
737	S2589	SLA	0	0	0	1	0	1	0	736	738	739
738	T344-SLA	SLA	0	1	0	0	1	0	1	737		
739	S2595	SLA	0	0	0	1	0	1	0	737	740	741
740	T131-SLA	SLA	0	1	0	1	0	1	3	739		
741	T260	SLA	0	1	0	1	0	1	4	739		
742	S2312	SLA	0	0	0	1	0	1	0	733	743	745
743	S132	SLA	0	0	0	1	1	0	0	742	744	
744	T143-SLA	SLA	0	1	0	1	1	0	14	743		
745	S2311	SLA	0	0	0	1	1	0	0	742	746	
746	S2310	SLA	0	0	0	1	0	1	0	745	747	
747	S2301	SLA	0	0	0	1	1	0	0	658	746	

748	S120	SLA		0	0	0	1	0	1	0	658	749								
749	T142-SLA	SLA		0	1	0	1	0	1	11	748									
750	T166	FVK	16	0	1	0	0	1	0	95		751								
751	T343-FVK	FVK	16	0	1	0	0	1	0	21	750	752								
752	T378	FVK	16	0	1	0	0	1	0	17	751	753								
753	T304	FVK	16	0	1	0	0	1	0	131	752	754	755							
754	T185	FVK	16	0	1	0	0	1	0	85	753									
755	T334-FVK	FVK	16	0	1	0	0	1	0	89	753	756								
756	T303	FVK	16	0	1	0	0	1	0	117	755	757	770							
757	T021-FVK	FVK	16	0	1	0	0	1	0	60	756	758								
758	T335-FVK	FVK	16	0	1	0	0	1	0	52	757	759								
759	T352	FVK	16	0	1	0	0	1	0	1	758	760	761	769						
760	T349	FVK	16	0	1	0	0	1	0	1	759									
761	T241-FVK	FVK	16	0	1	0	0	1	0	57	759	762								
762	T242-FVK	FVK	16	0	1	0	0	1	0	71	761	763								
763	T243	FVK	16	0	1	0	0	1	0	79	762	764	765							
764	T357	FVK	16	0	1	0	0	1	0	60	763									
765	T012-FVK	FVK	16	0	1	0	0	1	0	139	763	766	768							
766	T345-FVK	FVK	16	0	1	0	0	1	0	114	765	767								
767	T306-FVK	FVK	16	0	1	0	0	1	0	113	766	465								
768	T301	FVK	16	0	1	0	0	1	0	128	765	769								
769	T016-FVK	FVK	16	0	1	0	0	1	0	154	768	759								
770	T128-FVK	FVK	16	0	1	0	0	1	0	1	756	771								
771	T302	FVK	16	0	1	0	0	1	0	1	770	772	773							
772	T013-FVK	FVK	16	0	1	0	0	1	0	1	771									
773	T339-FVK	FVK	16	0	1	0	0	1	0	1	771	774								
774	T168	FVK	16	0	1	0	0	1	0	1	773	775								
775	T331-FVK	FVK	16	0	1	0	0	1	0	1	774	776								
776	T127-FVK	FVK	16	0	1	0	0	1	0	1	775	777								
777	T377	FVK	16	0	1	0	0	1	0	1	776	778								
778	T390	FVK	16	0	1	0	0	1	0	1	777	779								
779	T024-FVK	FVK	16	0	1	0	0	1	0	1	778	451								
780	FKN			1	0	0	0	1	0	0	781	795	781	801	815	819	0	0	955	956
781	T026-FKN	FKN	7	0	1	0	0	1	0	33	780	782	798	780	958					
782	T021-FKN	FKN	7	0	1	0	0	1	0	81	781	783								
783	T027-FKN	FKN	7	0	1	0	0	1	0	82	782	784								
784	T347	FKN	7	0	1	0	0	1	0	52	783	785								
785	T022-FKN	FKN	7	0	1	0	0	1	0	88	784	786								
786	T023-FKN	FKN	7	0	1	0	0	1	0	104	785	787								
787	T024-FKN	FKN	7	0	1	0	0	1	0	71	786	788								
788	T025-FKN	FKN	7	0	1	0	0	1	0	68	787	789								
789	T018-FKN	FKN	7	0	1	0	0	1	0	53	788	790								
790	T017-FKN	FKN	7	0	1	0	0	1	0	45	789	791								
791	T374	FKN	7	0	1	0	0	1	0	58	790	792								
792	T015-FKN	FKN	7	0	1	0	0	1	0	63	791	793	800							
793	T016-FKN	FKN	7	0	1	0	0	1	0	94	792	794								
794	T028-FKN	FKN	7	0	1	0	0	1	0	63	793	795								
795	T019-FKN	FKN	7	0	1	0	0	1	0	119	794	796	780							
796	T020-FKN	FKN	7	0	1	0	0	1	0	69	795	797	798	799						
797	T078	FKN	7	0	1	0	1	1	0	1	796									
798	T351	FKN	7	0	1	0	0	1	0	90	796	781								

799	T014-FKN	FKN	7	0	1	0	0	1	0	60	796	800	
800	T373	FKN	7	0	1	0	0	1	0	42	799	792	
801	T006-FKN	FKN	14	0	1	0	0	1	0	119	780	802	
802	T361	FKN	14	0	1	0	0	1	0	110	801	803	
803	T008-FKN	FKN	14	0	1	0	0	1	0	137	802	804	
804	T009-FKN	FKN	14	0	1	0	0	1	0	65	803	805	
805	T012-FKN	FKN	14	0	1	0	0	1	0	88	804	806	816
806	T353	FKN	14	0	1	0	0	1	0	39	805	807	
807	T013-FKN	FKN	14	0	1	0	0	1	0	165	806	808	809
808	T332-FKN	FKN	14	0	1	0	0	1	0	101	807		
809	T005-FKN	FKN	14	0	1	0	0	1	0	168	807	810	
810	T004-FKN	FKN	14	0	1	0	0	1	0	99	809	811	
811	T003-FKN	FKN	14	0	1	0	0	1	0	114	810	812	816
812	T002-FKN	FKN	14	0	1	0	0	1	0	101	811	813	
813	T360	FKN	14	0	1	0	0	1	0	85	812	814	
814	T001-FKN	FKN	14	0	1	0	0	1	0	116	813	815	
815	T342-FKN	FKN	14	0	1	0	0	1	0	119	814	780	
816	T011-FKN	FKN	14	0	1	0	0	1	0	142	811	817	805
817	T354	FKN	14	0	1	0	0	1	0	42	816	818	
818	T336-FKN	FKN	14	0	1	0	0	1	0	115	817	819	
819	T010-FKN	FKN	14	0	1	0	0	1	0	64	818	780	
820	SFP			1	0	0	0	1	0	0	821	954	
821	OF22-210	SFP	16	0	0	1	1	0	1	0	820	822	
822	S5045	SFP	16	0	0	0	1	1	0	0	821	823	
823	S5050	SFP	16	0	0	0	1	0	1	0	822	824	
824	S5065	SFP	16	0	0	0	1	1	0	0	823	825	
825	T130	SFP	16	0	1	0	0	1	0	66	824	826	873
826	T129-SFP	SFP	16	0	1	0	0	1	0	80	825	827	828
827	T011-SFP	SFP	16	0	1	0	0	1	0	131	826		
828	T127-SFP	SFP	16	0	1	0	0	1	0	86	826	829	
829	T300	SFP	16	0	1	0	1	1	0	21	828	830	
830	T131-SFP	SFP	16	0	1	0	0	1	0	84	829	831	870
831	T132-SFP	SFP	16	0	1	0	0	1	0	68	830	832	
832	S5070	SFP	16	0	0	0	1	0	1	0	831	833	
833	F22-622	SFP	16	0	0	1	1	0	1	0	832	834	
834	S5074	SFP	16	0	0	0	1	0	1	0	833	835	836
835	T106-SFP	SFP	16	0	1	0	1	0	1	5	834		
836	S5079	SFP	16	0	0	0	1	0	1	0	834	837	
837	S5082	SFP	16	0	0	0	1	0	1	0	836	838	839	840
838	T104-SFP	SFP	16	0	1	0	1	0	1	6	837		
839	T105-SFP	SFP	16	0	1	0	1	0	1	7	837		
840	T103-SFP	SFP	16	0	1	0	1	0	1	4	837	841	
841	F22-615	SFP	16	0	0	1	1	0	1	0	840	842	
842	S5098	SFP	16	0	0	0	1	1	0	0	841	843	844
843	T101-SFP	SFP	16	0	1	0	1	0	1	3	842		
844	S5099	SFP	16	0	0	0	1	0	1	0	842	845	
845	T102-SFP	SFP	16	0	1	0	1	0	1	4	844	846	
846	S5107	SFP	16	0	0	0	1	1	0	0	845	847	
847	T264	SFP	16	0	1	0	0	1	0	37	846	848	
848	T266	SFP	16	0	1	0	0	1	0	26	847	849	
849	S5108	SFP	16	0	0	0	1	0	1	0	848	850	

850	F22-614	SFP	16	0	0	1	1	0	1	0	849	851		
851	S574	SFP	16	0	0	0	1	1	0	0	850	852		
852	TRE	SFP	16	0	1	1	0	1	0	0	851	853	927	
853	S1014	SFP	16	0	0	0	1	0	1	0	852	854	855	
854	T201-SFP	SFP	16	0	1	0	1	0	1	3	853			
855	T202-SFP	SFP	16	0	1	0	1	0	1	17	853	856		
856	S1042	SFP	16	0	0	0	1	0	1	0	855	857	859	
857	T203-SFP	SFP	16	0	1	0	1	0	1	6	856	858		
858	T204-SFP	SFP	16	0	1	0	1	0	1	5	857			
859	F22-314	SFP	16	0	0	1	0	0	1	0	856	860		
860	T205	SFP	16	0	1	0	1	0	1	1	859	861		
861	T213-SFP	SFP	16	0	1	0	1	0	1	6	860	862		
862	S1064	SFP	16	0	0	0	1	0	1	0	861	863	865	
863	S1204	SFP	16	0	0	0	1	1	0	0	862	864		
864	T212-SFP	SFP	16	0	1	0	0	1	0	32	863			
865	T206-SFP	SFP	16	0	1	0	1	0	1	5	862	866		
866	S1114	SFP	16	0	0	0	1	1	0	1	865	65		
867	T917	SFP	16	0	1	0	0	1	0	1	65			
868	T342-SFP	SFP	16	0	1	0	0	1	0	7	65	869		
869	T208-SFP	SFP	16	0	1	0	1	1	0	7	868			
870	T339-SFP	SFP	16	0	1	0	0	1	0	14	830	871		
871	T010-SFP	SFP	16	0	1	0	0	1	0	351	870	872		
872	T341	SFP	16	0	1	0	0	1	0	123	871	873		
873	T328	SFP	16	0	1	0	0	1	0	36	872	874	825	876
874	T340-SFP	SFP	16	0	1	0	0	1	0	164	873	875		
875	T343-SFP	SFP	16	0	1	0	1	1	0	27	874			
876	S724	SFP	16	0	0	0	1	0	1	0	873	877		
877	S728	SFP	16	0	0	0	1	0	1	0	876	878	898	
878	S731	SFP	16	0	0	0	1	0	1	0	877	879	880	
879	T151-SFP	SFP	16	0	1	0	1	0	1	10	878			
880	S737	SFP	16	0	0	0	1	0	1	0	878	881	886	
881	OF22-309	SFP	16	0	0	1	1	0	1	0	880	882		
882	T154-SFP	SFP	16	0	1	0	1	1	0	6	881	883		
883	S3031	SFP	16	0	0	0	1	0	1	0	882	884		
884	S3037	SFP	16	0	0	0	1	1	0	0	883	885		
885	T155-SFP	SFP	16	0	1	0	1	1	0	18	884			
886	T152	SFP	16	0	1	0	1	0	1	5	880	887		
887	F22-246	SFP	16	0	0	1	1	0	1	0	886	888	889	
888	F22-237	SFP	16	0	0	1	1	0	1	0	887	928		
889	F22-243	SFP	16	0	0	1	1	0	1	0	887	890	943	
890	S1132	SFP	16	0	0	0	1	0	1	0	889	891	892	
891	T119-SFP	SFP	16	0	1	0	1	0	1	3	890			
892	F22-222	SFP	16	0	0	1	1	0	1	0	890	893		
893	S1146	SFP	16	0	0	0	1	0	1	0	892	894	899	906
894	S1313	SFP	16	0	0	0	1	0	1	0	893	895	897	
895	S1321	SFP	16	0	0	0	1	0	1	0	894	896		
896	T930	SFP	16	0	1	0	1	0	1	1	895			
897	F22-231	SFP	16	0	0	1	1	0	1	0	894	898		
898	F22-234	SFP	16	0	0	1	1	0	1	0	897	877		
899	S1325	SFP	16	0	0	0	1	0	1	0	893	900	901	
900	T117-SFP	SFP	16	0	1	0	1	0	1	21	899			

901	F22-191	SFP	16	0	0	1	1	0	1	0	899	902	
902	T125	SFP	16	0	1	0	1	0	1	16	901	903	
903	S1344	SFP	16	0	0	0	1	0	1	0	902	904	905
904	S305	SFP	16	0	0	0	1	0	1	0	903		
905	T288	SFP	16	0	1	0	1	0	1	3	903		
906	F22-200	SFP	16	0	0	1	1	0	1	0	893	907	
907	S512	SFP	16	0	0	0	1	0	1	0	906	908	910
908	F22-198	SFP	16	0	0	1	1	0	1	0	907	909	
909	T291	SFP	16	0	1	0	1	0	1	23	908		
910	F22-195	SFP	16	0	0	1	1	0	1	0	907	911	
911	S490	SFP	16	0	0	0	1	1	0	0	910	912	921
912	S5130	SFP	16	0	0	0	1	0	1	0	911	913	
913	T268	SFP	16	0	1	0	1	0	1	6	912	914	
914	F22-616	SFP	16	0	0	1	1	0	1	0	913	915	
915	S5134	SFP	16	0	0	0	1	0	1	0	914	916	917
916	T267	SFP	16	0	1	0	1	0	1	5	915		
917	T269	SFP	16	0	1	0	1	0	1	3	915	918	
918	S5146	SFP	16	0	0	0	1	1	0	0	917	919	
919	T270	SFP	16	0	1	0	1	1	0	6	918	920	
920	T271	SFP	16	0	1	0	1	1	0	1	919		
921	S458	SFP	16	0	0	0	1	1	0	0	911	922	
922	S457	SFP	16	0	0	0	1	0	1	0	921	923	
923	S455	SFP	16	0	0	0	1	0	1	0	922	924	925
924	T262	SFP	16	0	1	0	1	0	1	5	923		
925	T261	SFP	16	0	1	0	1	0	1	14	923	926	
926	S1243	SFP	16	0	0	0	1	1	0	0	925	927	
927	S1244	SFP	16	0	0	0	1	0	1	0	926	852	
928	KUP	SFP	26	0	0	1	0	1	0	0	888	929	
929	T306-SFP	SFP	26	0	1	0	0	1	0	57	928	930	
930	T324	SFP	26	0	1	0	0	1	0	70	929	931	
931	T307-SFP	SFP	26	0	1	0	0	1	0	35	930	932	
932	T327	SFP	26	0	1	0	0	1	0	46	931	933	
933	T329	SFP	26	0	1	0	0	1	0	63	932	934	935
934	T325	SFP	26	0	1	0	0	1	0	17	933		
935	T321	SFP	26	0	1	0	0	1	0	104	933	936	
936	T322	SFP	26	0	1	0	0	1	0	79	935	937	938
937	T326	SFP	26	0	1	0	0	1	0	4	936		
938	T323	SFP	26	0	1	0	0	1	0	79	936	939	
939	F22-219	SFP	26	0	0	1	1	0	1	0	938	940	
940	S1111	SFP	26	0	0	0	1	0	1	0	939	941	944
941	S1118	SFP	26	0	0	0	1	0	1	0	940	942	943
942	T124	SFP	26	0	1	0	1	0	1	8	941		
943	F22-240	SFP	26	0	0	1	1	0	1	0	941	889	
944	F22-603	SFP	26	0	0	1	1	0	1	0	940	945	
945	T120-SFP	SFP	26	0	1	0	1	0	1	16	944	946	
946	S1094	SFP	26	0	0	0	1	0	1	0	945	947	948 950
947	T121-SFP	SFP	26	0	1	0	1	0	1	17	946		
948	S1279	SFP	26	0	0	0	1	1	0	0	946	949	
949	T126-SFP	SFP	26	0	1	0	1	1	0	6	948		
950	T122-SFP	SFP	26	0	1	0	1	0	1	3	946	951	
951	S1078	SFP	26	0	0	0	1	0	1	0	950	952	953

952	T128-SFP	SFP	26	0	1	0	1	0	1	4	951	
953	OF22-213	SFP	26	0	0	1	1	0	1	0	951	954
954	S1003	SFP	26	0	0	0	1	1	0	0	953	820
955	T167	FKN		0	1	0	0	1	0	80	780	
956	T330-FKN	FKN		0	1	0	0	1	0	0	780	957
957	F12-635	FKN		0	0	1	1	1	0	0	956	474
958	T375	FKN		0	1	0	0	1	1	3	781	
959	T001-SNR	SNR		0	1	0	0	1	0	0	488	
960	T905	VEE	23	0	1	0	0	1	0	1	361	