Analys av sårbarhet med hjälp av nätverksmodeller

Tehler, Henrik; Hassel, Henrik; Johansson, Jonas

2007

Analys av sårbarhet med hjälp av nätverksmodeller

Henrik Johansson
Henrik Jönsson
Jonas Johansson

LUCRAM
Lunds universitets centrum för riskanalys och riskhantering
Lunds universitet

Rapport 1011, Lund 2007

Analys av sårbarhet med hjälp av nätverksmodeller

Henrik Johansson
Henrik Jönsson
Jonas Johansson

Lund 2007

Analys av sårbarhet med hjälp av nätverksmodeller

Henrik Johansson
Henrik Jönsson
Jonas Johansson

Rapport 1011
ISSN: 1404-2983

Antal sidor: 43
Illustrationer: Författarna om inte annat anges.

Sökord: Nätverk, sårbarhetsanalys, teknisk infrastruktur, nätverksanalys eldistributionssystem

Abstract:
This report presents the research concerned with vulnerability analysis of technical infrastructure networks conducted in the research framework programme called FRIVA. The report reviews how network analysis has been used to analyse the vulnerability of systems that are possible to model as networks, such as technical infrastructure systems. In addition, it proposes how these methods can be developed in order to better suit vulnerability analysis conducted with a societal perspective. In order to show the applicability of these methods, they are applied to both hypothetical and real-world systems.

LUCRAM
Lunds universitets centrum för
riskanalys och riskhantering
Lunds universitet
Box 118
221 00 Lund

http://www.lucram.lu.se

LUCRAM
Lund University Centre for
Risk Analysis and Management
Lund University
P.O. Box 118
SE-221 00 Lund
Sweden

http://www.lucram.lu.se

Sammanfattning

I denna rapport redovisas delar av den forskning som handlar om risk- och sårbarhetsanalyser för system som är uppbyggda i form av nätverk. Forskningen har utförts inom ramen för FRIVA (Framework Programme for Risk and Vulnerability Analysis) som är ett ramforskningsprogram finansierat av Krisberedskapsmyndigheten.

Dagens samhälle är starkt beroende av den service som tillhandahålls av ett antal infrastruktursystem, t.ex. eldistributions-, vatten- och avlopps- samt transportsystem. Många av dessa system är uppbyggda i olika typer av nätverksstrukturer och är i de flesta fall geografiskt utspridda samt innehåller ett stort antal komponenter. Avbrott i den service som systemet tillhandahåller kan i många fall leda till allvarliga problem för många av samhällets dagliga aktiviteter. Dessutom kan störningar i infrastrukturer leda till att hanteringen av en kris som av någon anledning har uppstått kraftigt försvåras, t.ex. genom att möjligheten till kommunikation blivit utslagen. Eftersom infrastruktursystemen spelar en så viktig roll i samhället är det viktigt att dessa analyseras ur ett risk- och sårbarhetsperspektiv med syftet att t.ex. undersöka vilka hot som kan skada systemen och hur allvarligt systemet drabbas av hot som realiseras. Med tanke på den stora komplexitet som är förknippad med dessa typer av system är det viktigt att det finns väl utvecklade metoder för sådana analyser. Denna rapport syftar därför till att belysa de metoder som har utvecklats inom området *nätverksanalys* och som har applicerats på infrastruktursystem av olika slag. Rapporten fokuserar på sårbarhetsanalyser, d.v.s. på metoder som kan användas för att undersöka vad som kan hända, hur troligt detta är samt vilka konsekvenserna blir av detta *givet* att ett system utsätts för en specifik påfrestning.

Utgångspunkten för de sårbarhetsanalyser som utförs inom nätverksanalysområdet är att en nätverksmodell (bestående av noder och länkar) av det aktuella systemet tas fram. Genom att slå ut noder och/eller länkar, antingen i en *slumpmässig* ordning eller genom en *riktad* utslagning av en viss typ av komponenter, och sedan uppskatta hur stora de negativa konsekvenserna (som uppskattas genom att mäta någon typ av mått med utgångspunkt i nätverkets struktur) blir till följd av utslagningen kan man få en uppfattning om hur sårbart systemet är. Grovt sett kan metoderna inom området delas in i två huvudkategorier; de som är rent strukturella/statiska och de som försöker ta större hänsyn till underliggande fysikaliska egenskaper (t.ex. att i modellering av ett eldistributionsnät ta hänsyn till laster och kapaciteter i olika noder). Större hänsyn till de underliggande fysikaliska egenskaperna ger givetvis en mer verklighetstrogen modell, men samtidigt blir simuleringarna betydligt mer krävande, både vad gäller den indata och den tid som krävs för att genomföra simuleringarna. Att använda alltför avancerade modeller kan därmed leda till att möjligheten att genomföra en heltäckande och systematisk analys minskar. De lite grövre modellerna kan därför vara ett bra komplement till mer avancerade och detaljerade modeller vid analys av risker och sårbarheter.

I rapporten presenteras även förslag till hur de befintliga metoderna för sårbarhetsanalys kan utvecklas för att de ska vara bättre lämpade för användning ur ett samhälleligt perspektiv, snarare än ett rent tekniskt perspektiv. I rapporten visas sedan exempel på tillämpning av de föreslagna metoderna på eldistributionssystem, men syftet är att metoderna även ska kunna användas för analys av andra typer av infrastruktursystem som kan modelleras i form av nätverk. Givetvis måste t.ex. de mått som används för uppskattning av konsekvenser anpassas till den typ av system som är aktuellt.

Innehållsförteckning

1 INLEDNING 3

1.1 BAKGRUND 3
1.2 SYFTE 5

2 NÄTVERKSANALYS 6

2.1 DEFINITIONER OCH BEGREPP 7

3 ÖVERSIKT AV OLIKA METODER FÖR SÅRBARHETSANALYS AV NÄTVERK 10

3.1 OLIKA TYPER AV PÅFRESTNINGAR 10
3.2 KASKADEFFEKTER 11
3.3 NÅGRA OLIKA TYPER AV NÄTVERKSANALYSER 12

4 NÄTVERKSANALYS SOM EN DEL I EN KOMMUNAL ELLER REGIONAL SÅRBARHETSANALYS 16

4.1 EN METOD FÖR ANALYS AV ETT TEKNISKT SYSTEMS SÅRBARHET 19
4.2 MÅTT PÅ SÅRBARHET 23
4.3 OLIKA TYPER AV PÅFRESTNINGAR 27
4.4 EXEMPEL PÅ SÅRBARHETSANALYS AV ETT LOKALT ELDISTRIBUTIONSSYSTEM 30
4.5 KRAV FÖR ANVÄNDNING AV METODEN 34

5 ANALYS AV VERKLIGA ELNÄT 35

5.1 NÄTVERKSMODELLERING 35
5.2 SIMULERINGSRESULTAT 36

6 SAMMANFATTANDE DISKUSSION 41

REFERENSER 42

1 Inledning

Denna rapport är skriven inom ramen för ramforskningsprogrammet FRIVA[1] (Framework programme for Risk and Vulnerability Analysis) som bedrivs inom Lunds universitets centrum för riskanalys och riskhantering (LUCRAM)[2] och är finansierat av Krisberedskapsmyndigheten. Denna rapport är en direkt följd av arbetet som redovisas i rapporten ”Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv” [1], där bl.a. många av de teoretiska utgångspunkterna för det aktuella arbetet beskrivs. För en djupare förståelse för vissa av de begrepp som används i denna rapport, såsom sårbarhet, hänvisas därför till ovan nämnda rapport.

1.1 Bakgrund

Nätverksstrukturer är något som finns i princip vart man än vänder sig. Genom att använda nätverk kan en stor mängd system av olika slag representeras och modelleras. Som några exempel kan nämnas biologiska (t.ex. näringsväv), sociala (t.ex. vänskapsrelationer mellan individer), teknologiska (t.ex. vattendistributionssystem) och cyber- eller informationsnätverk (t.ex. World Wide Web). I en nätverksmodell av ett system beskrivs och åskådliggörs beroenden och relationer mellan olika delar av systemet genom att använda två grundläggande byggstenar: noder och länkar. (En utförligare introduktion till nätverk och nätverksanalys ges i kapitel 4 av rapporten ”Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv” [1] och till viss del även i nästföljande kapitel). Med hjälp av den verktygslåda som forskningen inom området nätverksteori och nätverksanalys har utvecklat finns sedan möjligheter att utforska de nätverksstrukturer som observeras med syftet att skapa en djupare förståelse för de system som studeras. Ett av de områden som den nätverksanalytiska verktygslådan kan användas på är att analysera systems sårbarhet för olika typer av påfrestningar.

Tekniska infrastruktursystem är en typ av system som i många fall är möjliga att modellera som nätverk. Dessa system, t.ex. eldistributionssystem, väg- och järnvägssystem, telekommunikationssystem, vattendistributionssystem, etc., är ofta uppbyggda med en tydlig nätverksstruktur och är i de flesta fall geografiskt utspridda samt innehåller en stor mängd komponenter. Dessa egenskaper gör systemen mycket svåra att analysera ur ett helhetsperspektiv. Dagens samhälle är i hög grad beroende av dessa system för att kunna fungera. Avbrott i den service som de tekniska infrastrukturerna tillhandahåller kan leda till mycket stora påfrestningar på samhället eftersom det i så hög grad förlitar sig på systemens kontinuerliga funktion, något som inte minst har visat sig vid ett flertal nationella och internationella kriser (t.ex. stormen Gudrun 2005, isstormen i Kanada 1996, Elavbrottet i Auckland 1998 och Orkanen Katrina i New Orleans 2005). Avbrott eller minskad effektivitet i infrastrukturernas service kan även leda till att en befintlig kris som uppstått av samma eller andra orsaker inte kan hanteras på ett lika effektivt sätt som om servicen hade varit normal. Det är alltså viktigt att de tekniska infrastruktursystemen är tillförlitliga och robusta. Faktum är att de tekniska infrastruktursystemen har visat sig vara alltmer tillförlitliga men man får

[1] För mer information om ramforskningsprogrammet hänvisas till följande hemsida: http://www.friva.lucram.lu.se/

[2] För mer information om LUCRAM se följande hemsida: http://www.lucram.lu.se/

inte glömma bort att trenden under denna tid även har varit att samhället blivit alltmer sårbart mot avbrott, då det gjort sig alltmer beroende av dessa system. Det samhället kunde hantera förr har det kanske inte möjlighet att göra idag. Som ett exempel på detta kan nämnas elavbrott som tidigare varit långt mer vanliga än idag. Eftersom dessa skedde relativt ofta tidigare hade människor och organisationer i större utsträckning en beredskap för att klara av ett elavbrott än vad som är fallet idag. Hur framtiden kommer att gestalta sig är givetvis vanskligt att sia om men en trolig utveckling är att beroendet av de tekniska infrastrukturerna i all fall inte kommer att minska under en överskådlig framtid.

Att genomföra riskanalyser och sårbarhetsanalyser på olika typer av system är ett sätt att skaffa kunskap om systemen med syftet att sedan kunna hantera riskerna och sårbarheterna på ett effektivt och rationellt sätt. Medvetna val bör alltså styra de nivåer av tillförlitlighet, robusthet etc. som anses vara lämpliga att uppnå. Lämpligen är det en avvägning mellan de resurser och kostnader som behövs för att skapa robustare system samt den nytta som ett mer robust system innebär för samhället som bör styra vilken den ”optimala” tillförlitligheten och robustheten ska vara. Ett syfte med risk- och sårbarhetsanalyser är att de ska användas för att ta fram det underlag som krävs för att fatta beslut i relation till ovan nämnda avvägning.

I Sverige ställer ett antal olika regelverk krav på att olika verksamheter ska utföra risk- och sårbarhetsanalyser för sin verksamhet. De regelverk som har störst koppling till denna rapport är *Förordningen om krisberedskap och höjd beredskap* (SFS 2006:942), *Lag om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap* (SFS 2006:554) samt *Ellagen* (SFS 1997:857). Sammantaget handlar dessa lagstiftningar om att olika verksamheter (centrala myndigheter, kommuner, landsting samt företag med elnätkoncession (under 220kV)) skall upprätta risk- och sårbarhetsanalyser över sin verksamhet. Kraven på risk- och sårbarhetsanalyser är relativt nya, inte minst kraven i Ellagen, och vad analyserna ska uppfylla är i många fall oklart. Dessutom är det oklart vilka metoder som skall användas i dessa analyser. I denna rapport kommer exempel på metoder att ges, nämligen metoder som är applicerbara på system som är möjliga att modellera i form av nätverk.

Rapporten kommer att fokusera på sårbarhetsanalyser. I rapporten ”Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv” [1] presenterades en operationell definition av sårbarhet och denna kommer att användas även i denna rapport. Sårbarhet definierades där som en uppsättning scenarier samt deras respektive konsekvens och sannolikhet *givet* att systemet utsatts för en specifik påfrestning. Antalet scenarier som skulle kunna inträffa efter att ett system utsatts för en påfrestning kan vara mycket stort eftersom det i många fall är osäkert hur en viss påfrestning påverkar systemet. Det är därför ofta svårt att hitta en lämplig representation av samtliga scenarier i riskscenariorymden[3] genom en rent ”manuell” analys. Genom att använda en nätverksanalytisk ansats där systemen representeras av nätverksmodeller kan problemen förknippade med analysen reduceras. Detta eftersom datorbaserade simuleringar används för att

[3] Begreppet ”riskscenariorymd” förklaras i rapporten ”Risk- och sårbarhetsanalys från ett systemperspektiv” som publicerats av LUCRAM, se [1].

systematiskt gå igenom och generera ett stort antal möjliga scenarier samt uppskatta deras respektive konsekvenser.

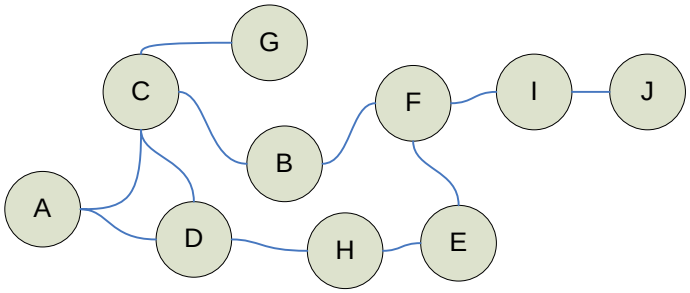
1.2 Syfte

Syftet med denna rapport är att visa hur nätverksmodeller och nätverksanalys kan användas för att analysera sårbarhet. Främst syftar rapporten till att visa hur metoderna kan appliceras på tekniska infrastruktursystem och samtliga exempel i rapporten är kopplade till dessa. Dock finns det inget som hindrar att metoderna generaliseras till att gälla även icke-tekniska system som är möjliga att modellera som nätverk. Mer specifikt är syftet att visa hur många av de svårigheter som är förknippade med risk- och sårbarhetsanalyser av dessa typer av system [1] kan hanteras. De metoder för sårbarhetsanalys som presenteras överensstämmer med den syn på sårbarhet som kort-fattat beskrevs ovan.

2 Nätverksanalys

För att kunna utföra en analys av sårbarheten i ett system måste först en nätverksmodell av systemet skapas. Denna modell representerar olika systemdelar (noder) och relationer mellan dessa (länkarna). Nätverkets struktur beskrivs enklast med en så kallad *kontaktmatris* som har storleken $n \times n$, där n är antalet noder i nätverket. Varje kolumn i matrisen motsvarar en nod (systemdel) i nätverket och om det finns en relation mellan nod v_i och nod v_j representeras detta av värdet 1 på position (i,j), och om det inte finns en relation är värdet 0. Relationer mellan olika systemdelar kan vara olika starka och i så fall kan andra värden än 0 och 1 användas, men för de tillämpningar som diskuteras här räcker det vanligtvis med att ange relationen med hjälp av 1 och 0. Utöver nätverkets struktur måste även de av systemets tillståndsvariabler som har betydelse för konsekvenserna av en påfrestning kunna beskrivas med hjälp av kunskap om nätverkets struktur och systemdelarnas funktion.

Relationerna representerar i den här typen av analys vanligtvis beroenderelationer och de är ofta relativt enkla att beskriva. Antag att alla noder i ett nätverk representerar en del i ett system och att varje del är förknippad med en binär tillståndsvariabel som beskriver funktionen hos just den delen (antingen fungerar delen eller så fungerar den inte). En beroenderelation mellan en nod och en uppsättning andra noder kan då innebära att den aktuella noden befinner sig i tillståndet ”fungerar” så länge det finns en väg genom nätverket från den aktuella noden till en annan specifik nod. Funktionen hos delarna av systemet som representeras av nätverket i Figur 1 är exempelvis beroende av att det finns en väg genom nätverket till nod A. Om en sådan väg existerar, och del A fungerar, fungerar också den aktuella delen; om en sådan väg inte finns, eller om del A inte fungerar, fungerar heller inte den aktuella delen. Den här grova beskrivningen av systemets funktion stämmer in på många olika typer av tekniska system där *kontakt* mellan olika systemdelar är avgörande för systemets förmåga att fungera. Exempel på sådana system är elsystem, vattendistributionssystem, järnvägssystem, avloppssystem, etc. Om en viss del av systemet inte har kontakt med en specifik systemdel kommer den delen inte att fungera. Om en nätstation i ett elsystem exempelvis inte har kontakt med en transformatorstation där elektriciteten matas in kan den inte förse de kunder som är kopplade till den med el och om en del av ett vattendistributionssystem inte har kontakt med en inmatningskälla kan inte de fastigheter som är kopplade till den delen få vatten, etc.



Figur 1 **Illustration av ett litet nätverk.**

Funktionen hos de olika verkliga systemen som modelleras med nätverk beror ofta inte enbart på om det finns kontakt med en ”källa” eller ej utan det finns i många fall andra aspekter som kan påverka systemets funktion, exempelvis kapaciteten i de länkar som kopplar ihop olika systemdelar. Att modellera ett fysiskt system på det sätt som precis beskrivits utgör dock en bra första utgångspunkt i en sårbarhetsanalys, och det finns möjligheter att utan alltför avancerade metoder och modeller även ta hänsyn till aspekter såsom kapacitet för noder och länkar.

Syftet med att använda nätverk för att analysera sårbarhet i olika system är att undersöka hela systemet och systemdelarnas relationer med förhoppningen om att kunna uttala sig om *globala* respektive *lokala* egenskaper i nätverket. Med globala egenskaper avses sådana egenskaper som rör hela systemet, exempelvis kan det vara intressant att studera *hur sårbart avloppssystemet i en viss kommun är för en specifik påfrestning*. I detta fall vill man uttala sig om hela avloppssystemet vilket innebär att det är en global analys. I andra fall kan det vara så att man vill uttala sig om *egenskaper hos olika systemdelar i förhållande till varandra* och i så fall handlar det om en lokal analys. Ett exempel skulle kunna vara att undersöka hur sårbara olika områden i ett eldistributionssystem är i förhållande till varandra, d.v.s. vilka områden drabbas värst givet att delar av elnätet slås ut. En annan typ av lokal analys är att identifiera de delar av ett system som är mest kritiska för systemets funktion, d.v.s. som om de av någon anledning inte skulle fungera skulle leda till en kraftigt försämrad funktion för systemet som helhet.

2.1 Definitioner och begrepp

För att analysera av sårbarheten i nätverk måste en del begrepp som härstammar från *grafteori* definieras. Ett nätverk, eller en *graf*[4], G, definieras som en mängd noder V och en mängd länkar E. En individuell nod betecknad v_i och en individuell länk e_i där i är ett index. Länkarna kopplar samman noderna parvis och de kan även ha en riktning, en så kallad riktad graf. Antalet noder i en graf betecknas med n och antalet länkar med m. En graf kan användas för att representera ett system, där de olika delarna i systemet representeras av noderna och relationer mellan delarna representeras av länkar mellan noder.

Grad

Inom analys av nätverk är begreppet *grad* av stor betydelse. En nods (v_i) grad, k_i, är ett mått på hur många länkar som är kopplade till noden. Om nätverket som analyseras är riktat skiljer man på in-grad, och ut-grad. En grafs genomsnittliga grad beräknas som:

$$\langle k \rangle = \frac{1}{n}\sum_{i=1}^{n} k_i = \frac{m}{2n} \tag{1}$$

Klustringskoefficient

Klustringskoefficienten hos en nod är ett mått på hur sammanlänkade nodens grannar är. Om noden v_i har k_i grannar kan det som mest finnas $k_i \cdot (k_i - 1) / 2$ länkar mellan

[4] Graf brukar användas för att beteckna den matematiska representationen, medan nätverk kan användas både för att beteckna det verkliga systemet och den matematiska representationen.

dessa grannar. Klustringskoefficienten C_i är ett mått på hur stor andel av dessa potentiella länkar som existerar och kan beräknas som:

$$C_i = \frac{Antal\ länkar\ mellan\ grannarna\ till\ nod\ i}{Totalt\ antal\ möjliga\ länkar\ mellan\ grannarna\ till\ nod\ i} \qquad (2)$$

Eftersom C_i inte är definierad för de noder som är isolerade eller endast har en granne anges klustringskoefficienten till 0 för dessa noder. Nätverkets klustringskoefficient, C, kan sedan beräknas som medelvärdet av samtliga noders klustringskoefficienter.

Kortaste vägen

I större nätverk kan det vara av intresse att beräkna den så kallade kortaste vägen mellan två noder, v_i och v_j. Den kortaste vägen, $d(v_i, v_j)$, är det minsta antal länkar som måste passeras för att förflytta sig från den ena noden till den andra. Den kortaste vägen mellan två noder kan beräknas med algoritmen som beskrivs av Newman i [2]. När det kortaste avståndet mellan samtliga noder i nätverket beräknats kan det genomsnittliga kortaste avståndet mellan noderna i nätverket, l, beräknas som:

$$l = \frac{1}{1/2 \cdot n(n+1)} \sum_{i \geq j} d(v_i, v_j) \qquad (3)$$

Om nätverket inte är helt sammankopplat, d.v.s. om alla noder inte kan nås från samtliga övriga noder, blir l oändligt stor och då väljer man antingen att bortse från de nodpar som inte kan nå varandra, eller att beräkna den inverterade längden, l^{-1}. Den inverterade längden beräknas som:

$$l^{-1} = \left\langle \frac{1}{d(v_i, v_j)} \right\rangle = \frac{1}{1/2 \cdot n(n+1)} \sum_{i \geq j} \frac{1}{d(v_i, v_j)}, \qquad (4)$$

och då det inte finns någon väg mellan noderna v_i och v_j gäller:

$$\frac{1}{d(v_i, v_j)} = 0 \qquad (5)$$

Intermeditet

I ett nätverk kan det finnas noder som oftare är med i de kortaste vägarna genom nätverket. Sådana noder har olika betydelse beroende på vilken typ av nätverk man studerar (tekniskt, socialt, etc.). Ett mått som används för att mäta hur många av nätverkets kortaste vägar som passerar en speciell nod är *intermeditet* (eng. betweenness). Intermeditet i sociala nätverk kan exempelvis indikera den viktigaste aktören, eller vem som kontrollerar informationsflödet mellan flest andra aktörer. En nods intermeditet, $B(v_i)$, definieras som:

$$B(v_i) = \sum_{v_j \neq v_k \in V} \frac{\sigma_{v_j, v_k}(v_i)}{\sigma_{v_j, v_k}} \text{ [3]}, \qquad (6)$$

där $\sigma_{v_j,v_k}(v_i)$ är antalet kortaste vägar mellan noderna v_j och v_k som passerar genom v_i. σ_{v_j,v_k} är det totala antalet kortaste vägar mellan noderna v_j och v_k. B_i kan beräknas med hjälp av algoritmen som föreslagits av Newman [2] .

Liknande resonemang som förts med avseende på noder kan också appliceras på länkar och en länks intermeditet ges då av, $B(e_i)$:

$$B(e_i) = \sum_{v_j \neq v_k \in V} \frac{\sigma_{v_j,v_k}(e_i)}{\sigma_{v_j,v_k}} \text{ [3],} \qquad (7)$$

där $\sigma_{v_j,v_k}(e_i)$ är antalet kortaste vägar mellan noderna v_j och v_k som passerar länken e_i.

Största komponenten

Begreppet komponent används ibland för att beteckna en uppsättning noder som är sammankopplade, d.v.s. där samtliga noder i uppsättningen kan nå samtliga andra noder. Den största komponenten (eng. giant component) i ett nätverk, S, är den största uppsättningen av sammankopplade noder som tillhör nätverket. Notera att begreppet komponenter i denna rapport även används för att beteckna antingen en nod eller en länk. Begreppet komponent med betydelsen ”en uppsättning noder som är sammanlänkade” används i denna rapport endast i samband med diskussioner kring den största komponenten i ett nätverk.

3 Översikt av olika metoder för sårbarhetsanalys av nätverk

Det finns många olika sätt att genomföra sårbarhetsanalyser för nätverk. Det här kapitlet inleds med en överblick av några sådana metoder som tidigare använts och några olika typer av analyser som genomförts presenteras även. I nästföljande kapitel presenteras sedan ett förslag på utveckling av de befintliga metoderna som passar bättre för att analysera sårbarheten i system av nätverkskaraktär.

Gemensamt för de metoder som beskrivs nedan är att ett antal scenarier, som är resultatet av en påfrestning på systemet, genereras med hjälp av en nätverksmodell av det system som studeras. För varje sådant scenario kan konsekvenserna beräknas med hjälp av ett antal olika mått. Vilken typ av påfrestning som systemets sårbarhet analyseras för kommer att påverka de scenarier som ingår i analysen.

3.1 Olika typer av påfrestningar

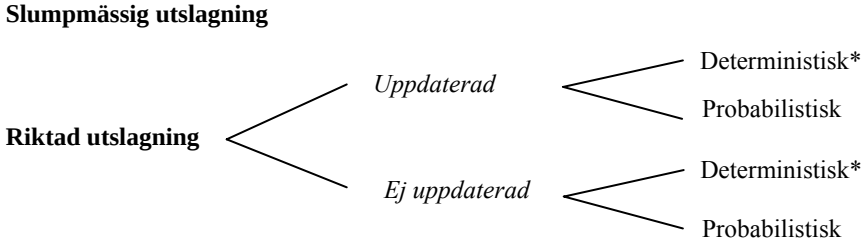
När nätverk används för sårbarhetsanalys går det att skilja på åtminstone två huvudsakliga *typer av påfrestningar*: slumpmässiga och riktade. Den första typen av påfrestning bygger alltså på en helt *slumpmässig utslagning* av noder eller länkar. I analysen undersöks någon typ av mått som syftar till att avspegla konsekvenserna av påfrestningen och sedan utförs mätningar av hur måttet förändras när noder och/eller länkar slås ut slumpmässigt. Tanken är att ju robustare systemet är desto fler nätverkskomponenter skall kunna slås ut innan de negativa konsekvenserna blir alltför stora. Exempelvis kan man definiera ett konsekvensmått som det genomsnittliga avståndet mellan alla noder, l, eller det inverterade avståndet l^{-1}. Avstånden ger en indikation av hur ”lätt” det är att nå de olika noderna från olika positioner i nätverket och kan vara ett bra mått på hur väl vissa nätverk fungerar. Givetvis är väldigt få verkliga påfrestningar helt slumpmässiga, men en slumpmässig utslagningsstrategi används ofta för att representera fenomen som är förknippade med en stor grad av slumpvariation, såsom naturfenomen eller utslitning av tekniska komponenter.

Den andra typen av påfrestning bygger på att någon typ av mått beräknas för samtliga noder eller länkar och sedan beräknas en specifik utslagningssekvens av noderna på basis av detta mått. För att kontrastera med den förstnämnda typen av påfrestning används ofta begreppet *riktad utslagning* som benämning på denna typ av påfrestning. Riktad utslagning kan även användas för att försöka finna de ”värsta” scenarierna som kan drabba nätverket, d.v.s. för att identifiera de påfrestningar som systemet är allra mest sårbart för. Ett exempel på riktad utslagning är att beräkna nodernas grad k och sedan slå ut noderna genom att alltid ta bort den nod som har den högsta graden. Detta motsvarar en situation där någon antagonist systematiskt attackerar de viktiga delarna i nätverket, exempelvis de fördelningsstationer i ett elnät som har flest ledningar kopplade till sig.

Vad gäller riktad utslagning är det möjligt att urskilja två huvudsakliga tillvägagångssätt för att räkna fram måtten som ligger till grund för sekvensen med vilken noderna eller länkarna slås ut. Det första tillvägagångssättet bygger på att måtten beräknas för det ursprungliga nätverket och sedan används dessa mått för att avgöra i

vilken ordning som noderna eller länkarna skall slås ut. Det andra tillvägagångssättet bygger på att man efter varje utslagning av en nod eller länk räknar om måttet som används som utgångspunkt för att bestämma utslagningsordningen och sedan används det omräknade måttet för att bestämma vilken nod eller länk som skall slås ut härnäst. Ett exempel på den här typen av analys är om de noder som har högst intermeditet slås ut först och efter att en nod slagits ut räknas måttet ut igen för samtliga noder i nätverket (nätverket har ju ändrat struktur eftersom en nod slagits ut). Sedan fortsätter utslagningen på samma sätt, d.v.s. den nod med högst intermeditet slås ut och därefter räknas intermediteten om för samtliga noder, o.s.v. Denna typ av påfrestning på ett system representerar förmodligen ett allvarligare fall för nätverket än då endast information från det ursprungliga nätverket används

De utslagningsstrategier som har beskrivits ovan har varit *deterministiska*, d.v.s. den komponent som har det högsta värdet på det beräknade måttet slås ut med säkerhet i varje utslagningsomgång. Ett annat tillvägagångssätt är att låta det beräknade måttet ligga till grund för *sannolikheten* för att en komponent blir utslagen. Istället för en deterministisk typ av utslagning är denna typ av påfrestning *probabilistisk*. Exempelvis korrelerar längden på en elledning ofta väl med sannolikheten för att den ska drabbas av ett avbrott, men man kan ju inte med säkerhet säga att det är den längsta ledningen som kommer att slås ut först då systemet utsätts för en påfrestning. Istället kan elledningarnas längd användas för att göra det troligare att länkar som representerar långa elledningar slås ut än att de som representerar korta ledningar gör det. På samma sätt kan man låta andra mått ligga till grund för sannolikheten för att olika komponenter ska bli utslagna. De olika typerna av påfrestning sammanfattas i Figur 2.



Figur 2 Illustration av olika typer av påfrestningar. * Även om utslagningsstrategin kallas ”deterministisk” kan ett visst mått av slumpmässighet förekomma. Om det exempelvis inte går att avgöra vilken av ett antal noder/länkar som skall slås ut härnäst med hjälp av det mått som man utsett som grund för den riktade utslagningen måste valet mellan dessa noder/länkar ske slumpmässigt.

3.2 Kaskadeffekter

De ovanstående typerna av påfrestningar kan användas i kombination med en rent statisk ansats eller en ansats som försöker fånga in eventuella kaskadeffekter som kan uppstå. I den rent statiska ansatsen sker inga ytterligare förändringar i nätverkets

struktur efter det att en komponent har blivit utslagen. I många verkliga system kan det dock hända att utslagningen av en viss komponent leder till att belastningen på andra komponenter i nätverket ökar, vilket kan leda till följdfel på grund av överbelastningar – så kallade *kaskadeffekter*. Denna ansats bygger alltså på att noderna eller länkarna i nätverket har en viss kapacitet och att om belastningen på en nod eller länk överskrider dess kapacitet så slås den noden eller länken ut. Ett scenario där belastningen på noder successivt räknas om kan alltså simulera de dominoeffekter som potentiellt kan uppstå i denna typ av system. För att illustrera tillvägagångssättet så anta att varje nod i nätverket har en övre gräns för dess kapacitet. Om en nod eller länk slås ut i nätverket kan man räkna om belastningen på varje nod och undersöka om någon nod/länk belastas med mer än dess kapacitet, i så fall slår man ut den/de också och räknar på nytt om belastningen i nätverket. På detta sätt kan man analysera hur bra nätverket är på att omfördela lasten och man kan också få en förståelse för hur kaskadeffekter påverkar sårbarheten i nätverket.

3.3 Några olika typer av nätverksanalyser

Albert m.fl. [4] presenterar en analys där de utgår ifrån två modellnätverk, ett slumpmässigt nätverk och ett skalfritt nätverk med samma antal noder och länkar (n = 10 000, m = 20 000). I analysen visar de att det skalfria nätverket är mycket mer robust mot slumpmässiga fel, men att det motsatta gäller för attacker riktade mot den nod som har högst grad, k. Skalfria nätverk är en generisk typ av nätverk som betecknas av att nodernas graddistribution följer en ”power-law”-fördelning, d.v.s. de flesta noder har en låg andel länkar kopplade till sig medan ett fåtal noder, som dock inte är försumbara, har ett mycket stort antal länkar kopplade till sig. Vidare presenterar man också en analys av Internets (n = 6 209, m = 12 200) och World Wide Webs (n = 325 729, m = 1 498 353) sårbarhet. I nätverket över Internet representerar noderna olika fysiska komponenter såsom routrar och länkarna representerar olika fysiska kommunikationsmöjligheter mellan dessa komponenter. I nätverket över World Wide Web är noderna hemsidor och länkarna är hypertextlänkar mellan hemsidorna. I uppsatsen presenteras en sårbarhetsanalys av dessa två system där noderna angrips dels slumpmässigt, dels riktat mot den nod som har högst grad. Under tiden som noder slås ut beräknas hur medelvärdet av de kortaste vägarna mellan noderna förändras. Resultaten visar att både Internet och World Wide Web har sårbarhetsegenskaper som överensstämmer med de skalfria nätverkens, d.v.s. de är mycket robusta mot slumpmässiga fel, men sårbara mot riktade attacker.

Holme m.fl. [3] undersöker sårbarheten i fyra modellnätverk: ett slumpmässigt nätverk, ett nätverk genererat med Watts och Strogatz modell för små världar [5], ett skalfritt nätverk [6] samt ett nätverk som genererats med en modifierad modell av den skalfria nätverksmodellen. Vidare analyseras också två verkliga nätverk, ett datornätverk (n = 2 210, m = 4 334) och ett socialt nätverk som visar vilka som samarbetat i en grupp av forskare (n = 2 010, m = 6 614). I sårbarhetsanalysen mäts den inverterade längden, l^{-1}, och storleken på den största komponenten i nätverket, S, som funktion av hur stor andel av noderna respektive länkarna som tagits bort från nätverket. Fyra olika typer av strategier för att ta bort noder och länkar används. En strategi bygger på att graden för

samtliga noder/länkar[5] beräknas och sedan tas den som har högst grad, *k*, bort. Denna procedur upprepas sedan med de noder och länkar som ännu inte blivit utslagna tills dess att ingen ytterligare länk eller nod kan tas bort. En annan strategi bygger på att nodernas/länkarnas ursprungliga intermeditet, *B*, beräknas och sedan tas den nod/länk som har högst intermeditet, *B*, bort. Processen upprepas sedan på samma sätt som vid den föregående strategin. Dessa två strategier bygger på att måtten, grad och intermeditet, beräknas för det *ursprungliga* nätverket. De två sista strategierna som används i uppsatsen bygger på att måtten *uppdateras* efter varje utslagen nod/länk och att nästa nod/länk slås ut baserat på de uppdaterade måtten.

Crucitti m.fl. [7] presenterar en analys som liknar den som Holme m.fl. [3] genomförde. Skillnaden är att i stället för att använda den inverterade längden och storleken hos den största komponenten som konsekvensmått används ett effektivitetsmått [8]. Effektiviteten vid kommunikation mellan två noder definieras som $\varepsilon(v_i, v_j) = 1/ d(v_i, v_j)$ och är alltså omvänt proportionell mot den kortaste vägen mellan de två noderna. Det bör observeras att i ett *viktat nätverk* (där avståndet mellan två noder inte nödvändigtvis är 1) beräknas den kortaste vägen mellan två noder inte genom att räkna hur många länkar som måste passeras mellan två noder utan genom att räkna avståndet eller ”vikten” av de olika länkarna som måste passeras på vägen. *Medeleffektiviteten* av nätverket *G* definieras som:

$$E(G) = \frac{\sum_{i \neq j \in G} \varepsilon\left(v_i, v_j\right)}{n \cdot \left(n-1\right)} = \frac{1}{n \cdot \left(n-1\right)} \cdot \sum_{i \neq j \in G} \frac{1}{d\left(v_i, v_j\right)}. \qquad (8)$$

E(G) kallas också för nätverket *G*:s *globala effektivitet,* E_{Glob}. Genom att definiera medeleffektiviteten *hos en del av nätverket*, $E(G_i)$, nämligen de noder som är grannar till noden v_i, kan nätverkets *lokala effektivitet*, E_{Loc}, beräknas som:

$$E_{Loc} = \frac{1}{n} \cdot \sum_{i \in G} E\left(G_i\right) . \qquad (9)$$

Genom att dividera *E(G)* med effektiviteten hos ett idealt nätverk, $E(G_{id})$, erhålls ett värde mellan 0 och 1. Det ideala nätverket har samtliga av de *n(n-1)* möjliga länkarna mellan noderna. Det globala effektivitetsmåttet kan liknas med den inverterade längden, Γ^1, och den lokala effektiviteten fyller en liknande funktion som klustringskoefficienten, *C*. De strategier som används vid utslagning av noder är slumpmässig utslagning och utslagning baserad på nodernas grad (se ovan).

Albert m.fl. [9] presenterar en analys av det Nordamerikanska elnätet (n = 14 099, m = 19 657) där noderna representerar tre typer av elkraftskomponenter: generatorer, transmissionsstationer och fördelningsstationer. Ett mått som kallas Connectivity Loss,

[5] En länks grad beräknas genom att multiplicera graderna för de noder som länken sammanbinder.

C_L, används för att uppskatta de konsekvenser som uppstår i nätverket givet att det utsätts för en påfrestning. Måttet definieras som:

$$C_L = 1 - \left\langle \frac{N_g^i}{N_g} \right\rangle_i , \tag{10}$$

där N_g är det totala antalet generatorer i nätet och N^i_g är det antalet generatorer som kan nås via nätverket från fördelningsstation i. Från början har samtliga fördelningsstationer (där elektriciteten fördelas vidare ut till kunderna) kontakt med samtliga generatorer och C_L är alltså 0. Genom att slå ut generatorer och transmissionsstationer simulerar man påfrestningar på elnätet. Utslagningen sker antingen slumpmässigt eller riktat genom att alltid slå ut den station som har högst grad eller högst ”belastning”, vilken antas vara proportionell mot nodens intermeditet. Vad gäller utslagning av den nod som har högst belastning så används både en ursprungsstrategi och en uppdateringsstrategi. Den senare kallar författarna för en kaskadbaserad utslagning. Från undersökningen av elnätet drar man slutsatserna att nätet är förhållandevis robust mot slumpmässiga fel (liten ökning av C_L då noder slås ut), men sårbart mot riktad utslagning av noder. Man bör notera att simuleringen av kaskadeffekter egentligen inte beaktar det som normalt förknippas med kaskadfel, nämligen att en omfördelning av lasten leder till att *kapaciteten hos en länk eller nod överskrids*, vilket gör att den också slås ut. I simuleringen ovan slås *alltid* noden som har den högsta belastningen ut, oavsett om den har kapacitet att klara belastningen. I praktiken är det endast benämningen av denna utslagningsstrategi som skiljer den från en av de utslagningsstrategier som Holme m.fl. använde sig av.

Även i Sverige har sårbarhet studerats med hjälp av nätverksmodeller. Holmgren [10] presenterar en analys av det nordiska transmissionsnätet och jämför även detta med transmissionsnätet i västra USA. Dessutom jämför Holmgren sårbarheten för dessa nätverk med två modellnätverk: ett slumpmässigt nätverk och ett skalfritt. För att uppskatta de olika nätverkens funktion använder Holmgren storleken på den största komponenten, S, som fraktion av storleken på hela nätverket, och den genomsnittliga inverterade längden, l^{-1}, för den största komponenten. Två huvudsakliga typer av utslagningsstrategier används i analysen; en för att representera slumpmässiga fel (slumpmässig utslagning av noder) och en för att representera ett antagonistiskt hot (utslagning av noder med högst grad – både utslagning baserad på ursprunglig grad och omräknad grad används). Vad gäller slumpmässig utslagning visade sig de både modellnätverken betydligt mindre sårbara medan när det gäller utslagning av noder med högst grad var det endast det slumpmässiga nätverket som var betydligt mindre sårbart.

De analyser som har beskrivits ovan har varit rent statiska i den bemärkelsen att man inte har explicit försökt modellera de kaskadeffekter som kan tänkas uppstå i nätverket (kaskadeffekter diskuterades i kapitel 3.2). Det finns dock ett antal analyser presenterade i forskningslitteraturen där kapaciteten hos olika noder/länkar att hantera den omfördelade belastningen som en utslagning av en nod/länk medför har tagits hänsyn

till [11-16]. I stort följer dessa analyser samma struktur som de som beskrivits ovan, med skillnaden att det sker en jämförelse mellan kapacitet och belastning i nätverks-modellen. De olika teknikerna som används för att utföra analyserna skiljer sig något åt. I Motter och Lai:s modell [11] slås överbelastade noder ut från nätverket medan i Holmes [15] modell slås överbelastade länkar ut. Crucitti m.fl. [14] använder ett något annorlunda tillvägagångssätt där de istället för att slå ut en överbelastad nod, reducerar kapaciteten för dem. Samma tillvägagångssätt används även av Kinney m.fl. [16]. I samtliga fall antas kapaciteten i de olika komponenterna vara proportionell mot den ursprungliga belastningen på dem. Något som kallas ”Overload tolerance”, α, antas sedan för de olika komponenterna, vilket kan tolkas som hur mycket extra belastning jämfört med den ursprungliga belastningen som komponenter kan hantera.

Sammanfattningsvis kan sägas att ett antal strategier för att slå ut noder eller länkar i ett nätverk har föreslagits av ett antal olika författare. Dessa strategier kan delas in i två huvudgrupper: *slumpmässig utslagning och riktad utslagning.* Vidare är det möjligt att skilja mellan ansatser som är rent statiska/strukturella och ansatser som gör anspråk på att fånga in de kaskadeffekter som kan uppstå. I båda ansatserna är det möjligt att utnyttja de olika typerna av utslagningsstrategier som har beskrivits ovan.

4 Nätverksanalys som en del i en kommunal eller regional sårbarhetsanalys

Nätverksmodeller kan vara mycket användbara i en kommunal, regional, eller nationell sårbarhetsanalys för många typer av tekniska system. Anledningen till att användningsområdet här begränsas till tekniska system är att det är troligt att denna typ av system lämpar sig bättre för nätverksmodellering eftersom de kan bestå av ett stort antal delar mellan vilka relationerna är förhållandevis lätta att kartlägga. Delarnas tillstånd, givet vissa förändringar i systemtillståndet, är också vanligtvis relativt enkla att beskriva (i förhållande till sociala system). Till exempel är det möjligt att beskriva ett elsystem som ett antal noder, vilka är sammankopplade med länkar, där noderna representerar exempelvis nätstationer och länkarna representerar ledningar som kopplar samman stationerna. En nätstation kan sedan betraktas som ”fungerande” om det finns en (eller flera) obrutna vägar genom nätverket från den aktuella nätstationen till en ”inmatningsnod” som representerar antingen en generator, eller punkt i elnätet där det finns en koppling till högre spänningsnivåer (antingen till regionnätet eller till transmissionsnätet). Notera dock att man med en sådan representation av ett elsystem bortser från en stor del av den dynamik som finns i det verkliga systemet. Dock är abstraktioner av detta slag ofrånkomliga om syftet med analyserna är att studera systemen ur ett helhetsperspektiv eftersom hänsyn till dynamiken dels kräver mycket stor datorkraft, dels kräver att mycket information om de tekniska systemen finns tillgänglig.

En förutsättning för att nätverksmodellerna skall kunna användas för analys av sårbarhet enligt den operationella definitionen som presenterades i rapporten ”Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv” [1] är att de negativa konsekvenserna till följd av påfrestningen på systemet kan beskrivas. Beroende på vad som i en specifik analys definieras som negativa konsekvenser kan detta vara mer eller mindre problematiskt. En utgångspunkt för att avgöra vad som är negativa konsekvenser är att studera vilka aktiviteter som möjliggörs på grund av det tekniska systemets funktion. Enligt Little [17-19] är det inte det tekniska systemens funktion i sig som är det viktiga utan snarare de aktiviteter som möjliggörs av systemet:

> ”Although it may be the hardware (i.e. the highways, pipes, transmission lines, communication satellites, and network servers) that initially focuses discussions of infrastructure, it is actually the services that these system provide that is of real value to the public” [19]

De negativa konsekvenserna av en påfrestning på ett tekniskt infrastruktursystem borde, enligt Little, alltså värderas i termer av hur allvarligt påfrestningen drabbar användarna av systemet och inte hur allvarligt det tekniska systemet själv påverkas (trots att det givetvis ofta finns en korrelation mellan de två). Många av de metoder som presenterades i föregående avsnitt fokuserar på systemets funktion, ur ett rent tekniskt perspektiv, och inte på konsekvenserna för användarna och därmed är resultaten från analyserna mindre användbara för sårbarhetsanalyser som har ett samhällsperspektiv, vilket är det perspektiv som är i fokus här. Avsikten är att i det här kapitlet presentera en vidareutveckling av de metoder som tagits upp tidigare. I den

vidareutvecklade metoden läggs större vikt på att konsekvenserna som används i analysen skall vara relevanta för samhällets sårbarhet och inte bara det tekniska systemets sårbarhet, samt att metoderna skall överensstämma med den kvantitativa definitionen av sårbarhet.

Två användbara begrepp i arbetet med att försöka anpassa metoderna är *hjälpbehov* [20] och *samhällsviktig verksamhet*. En sårbarhetsanalys för ett tekniskt system med hjälp av nätverk bör inledas med att undersöka om det finns risk att en påfrestning på det aktuella systemet kan orsaka störningar i *samhällsviktig verksamhet* (se definition i [21]). Om så är fallet bör ett eller flera konsekvensmått kunna uttryckas med hjälp av kunskap om vad som utgör den samhällsviktiga verksamheten. Exempelvis kan en samhällsviktig verksamhet vara *att energiförsörja* en kommun och denna verksamhet kan hotas av en påfrestning på elsystemet. Vid en sårbarhetsanalys av elsystemet måste lämpliga konsekvensmått som på ett bra sätt representerar konsekvenserna av att energiförsörjningen till kommunen begränsas konstrueras. Detta kan exempelvis innebära att konsekvenserna mäts genom att beräkna det maximala antalet abonnenter utan elförsörjning under riskscenarierna, eller genom att beräkna summan av tiderna som de olika abonnenterna är utan elförsörjning i riskscenarierna. Vilket/vilka konsekvensattribut som används beror dels på vilken samhällsviktig verksamhet som avses i analysen, dels på möjligheten att få fram information om attributet. I vissa fall kan det vara svårt eller omöjligt att få fram tillräcklig information angående olika konsekvensmått som bedömts som relevanta i en sårbarhetsanalys. Av pragmatiska skäl kan i dessa fall en variabel som ersätter eller representerar konsekvensmåttet användas (en s.k. proxyvariabel). Exempelvis kan det vara svårt att uppskatta hur många *personer* som är utan vattenförsörjning på grund av ett avbrott och då kan det vara lättare att definiera konsekvensen som antalet *abonnenter* som är utan vatten vid en viss tidpunkt efter påfrestningens början. Antal abonnenter blir då en proxyvariabel för antal personer.

Även om en påfrestning på ett tekniskt system inte ger upphov till avbrott i samhällsviktiga verksamheter kan det finnas andra konsekvenser som är viktiga att beakta i en sårbarhetsanalys. Ett sätt att komma fram till lämpliga konsekvensmått för en sådan analys är att fundera över vilka *hjälpbehov* som en påfrestning på ett tekniskt system kan ge upphov till. Om exempelvis elsystemet slås ut, men de flesta kommuninvånare har tillgång till reservkraft, uppstår ett begränsat hjälpbehov och därmed blir påfrestningen på krishanteringsorganisationen inte lika stor som den hade blivit om invånarna inte hade haft tillgång till reservkraft. Därmed är sårbarheten lägre för påfrestningar i elsystemet i en kommun där de flesta invånarna har tillgång till reservkraft än i en kommun där de inte har det, förutsatt att konsekvenserna av påfrestningen definieras som antal personer utan elförsörjning. På samma sätt går det att i en analys av något annat tekniskt system undersöka vad syftet med systemet är och vilka hjälpbehov som kan uppkomma om systemet inte fungerar som det är tänkt. En sådan analys kan vara anledningen till att man i en sårbarhetsanalys väljer att fokusera på olika grupper av människor som är beroende av det aktuella systemet. Exempelvis kan man tänka sig att äldre och handikappade människors hjälpbehov är större än andra människors hjälpbehov vid ett elavbrott (detta är dock inte säkert eftersom det visat sig att många äldre som bor själva utanför städer kan klara ett bortfall av elförsörjning

förvånansvärt bra, t.o.m. bättre än barnfamiljer, vilket stormen Gudrun illustrerade på ett tydligt sätt). I sådana fall kan man definiera ett konsekvensattribut för var och en av grupperna i analysen.

Anledningen till att just nätverksmodellerna är lämpliga i det här sammanhanget är att man kan låta ett datorprogram generera riskscenarierna för det system som man är intresserad av och på så vis reducera arbetet som måste läggas ner på analysen. Om inte datorprogrammet kan generera riskscenarierna samt deras konsekvenser och sannolikheter måste detta göras manuellt vilket kan ta mycket lång tid för stora system. Datorprogram kan också konstrueras så att de utgår ifrån den operationella definitionen av sårbarhet och sedan presenterar sårbarheten för en specifik påfrestning på ett mer lättförståeligt och överskådligt sätt än vad annars hade varit möjligt. Definitionen av sårbarhet innebär ju en lista med en uppräkning av de riskscenarier som kan bli resultatet av påfrestningen, samt deras respektive sannolikhet (givet påfrestningen) och konsekvens. Denna lista kan bli mycket lång för stora system. En sådan lista kan därför vara svår att tolka och genom att ett datorprogram förenklar presentationen av resultatet underlättas även tolkningen av resultatet.

För att kunna konstruera lämpliga mått på konsekvenser, d.v.s. att koppla nätverkets struktur till dess funktion, är det viktigt att domänkunskap finns om systemen. Hur systemets tillståndsvariabler beror av varandra har nämligen att göra med vilken typ av tekniskt system som studeras. En vanlig typ av system är sådana där en systemdels funktion bestäms av om den har kontakt med en eller flera speciella systemdelar, exempelvis huruvida en fastighet i ett vattendistributionsnät har fysisk kontakt (d.v.s. det kan flöda vatten mellan delarna) med vattentornet via ledningsnätverket, eller huruvida en nätstation i ett elsystem har kontakt med en inmatningspunkt. I sådana system kan en nätverkmodell för systemet tas fram och funktionen hos de olika delarna kan bestämmas med hjälp av nätverksmodellen och kunskap om den påfrestning som sårbarheten i systemet skall analyseras för.

I föregående avsnitt beskrevs två huvudsakliga typer av påfrestningar som nätverks-modellerna kan användas för att analysera: slumpmässig utslagning av systemets komponenter och riktad utslagning av systemets komponenter. Beskrivningarna av påfrestningarna definierar vanligtvis inte systemets tillstånd entydigt, d.v.s. det finns flera olika systemtillstånd som stämmer överens på beskrivningarna. Om man exempelvis är intresserad av att undersöka ett systems sårbarhet för ”slumpmässig utslagning av 10% av systemets delar” finns det många systemtillstånd som stämmer överens med den beskrivningen. Om systemet har 10 delar finns det närmare bestämt 10 systemtillstånd som stämmer överens med beskrivningen. I den operationella definitionen av sårbarhet [1] som används i denna rapport betecknas en påfrestning som T_P. Notera att denna påfrestning på systemet inte behöver vara ett enskilt systemtillstånd utan kan vara en *uppsättning* systemtillstånd, vilket alltså stämmer väl överens med användningen av begreppet påfrestning i detta kapitel. Systemets sårbarhet för påfrestningen definieras, i enlighet med den operationella definitionen av sårbarhet, som ett antal riskscenarier och deras respektive sannolikhet (betingat på påfrestningen) och konsekvens. Eftersom det för stora system kan vara svårt att få en överblick över en sådan uppsättning scenarier är det ofta svårt att presentera resultatet från en

sårbarhetsanalys genom att endast rada upp dessa scenarier. Därför brukar i stället de *förväntade konsekvenserna* givet den aktuella påfrestningen användas då resultatet från analysen presenteras. Detta innebär att om en viss påfrestning på ett system kan ge upphov till ett antal olika riskscenarier analyseras den förväntade konsekvensen genom att beräkna produkten av sannolikheten och konsekvensen för varje riskscenario och sedan summera dessa produkter för samtliga riskscenarier. Det är denna teknik som kommer att användas här och som också används av merparten av de metoder som beskrivits tidigare i kapitlet. Andra sätt att presentera sårbarheten är att även visa på spridningen i de möjliga utfallen, exempelvis genom att presentera kumulativa sannolikhetsfördelningar, analoga med FN-kurvorna som används flitigt inom risk-analys, eller att presentera konfidensintervall. Skillnaden är att kurvorna när det gäller sårbarhetsanalys är betingade på att systemet är utsatt för en specifik påfrestning.

Det kanske mest användbara måttet i det här sammanhanget som föreslagits är *Connectivity loss*, C_L, [9] som använts vid analys av elnätverk. Måttet mäter hur stor andel av det totala antalet generatorer i ett elnätverk som har kontakt med en viss fördelningsstation. Även om det är ett förhållandevis bra mått kan det förbättras genom att man utgår från vad som är syftet med systemet, nämligen att leverera elektricitet till abonnenter. Det är när det sker elavbrott för abonnenter som ett möjligt hjälpbehov uppstår och därför vore det bättre att ha ett mått som mäter hur många abonnenter som inte är i kontakt med en inmatningspunkt. Måttet förutsätter att alla abonnenter, ur ett konsekvensperspektiv, kan betraktas som lika. Det viktiga är huruvida det finns en väg genom nätet till *åtminstone* en inmatningspunkt. Genom att göra antagandet att en oavbruten väg genom nätet till en abonnent medför att elektricitet kan levereras bortser man ifrån de tekniska problem, exempelvis överbelastning av komponenter och stabilitet, som kan uppkomma och som kan medföra att elektricitet inte kan levereras till en abonnent trots att en fysisk förbindelse finns genom elnätet. Att alla abonnenter i ett elnätverk skulle vara likvärdiga ur ett konsekvensperspektiv är inte sant vilket utvecklas senare i kapitlet då kopplingen mellan social sårbarhet och nätverksanalys diskuteras.

4.1 En metod för analys av ett tekniskt systems sårbarhet

För att inte bara vara begränsade till att analysera elsystem måste analystekniken som presenteras här på något sätt beskrivas med generella termer som passar in på flera tekniska system med relevans för krishantering. Utifrån en sådan generell beskrivning kan man sedan formulera användbara mått på vad som menas med sårbarhet i ett specifikt systemen. Många tekniska system (el, vatten, avlopp, etc.) kan ses som nät-verk som tillhandahåller någon typ av resurs till människor eller organisationer. I det här sammanhanget använder vi begreppet *agent* för att representera den/de som är i behov av den aktuella resursen. En analys av ett tekniskt system bör inledas med att bestämma hur konsekvenserna av påfrestningen skall mätas. Ett sätt att göra detta är att ta reda på vilka agenter som är beroende av det aktuella systemet och om det finns skäl att dela in dessa i olika grupper. Indelning i grupper kan vara aktuellt om agenterna, ur ett konsekvensperspektiv, inte kan betraktas som likvärdiga. Om en sårbarhetsanalys genomförs för ett vattendistributionssystem i en kommun och de agenter som är beroende av systemet är privata hushåll, olika företag och organisationer kan det vara

klokt att dela in agenterna i exempelvis grupperna ”privata hushåll”, ”företag” och ”övriga organisationer”. Anledningen är att konsekvenserna, beroende på vilka värderingar som ligger till grund för analysen, kan uppfattas som olika om en agent av typen ”hushåll” står utan vatten än om en agent av typen ”företag” står utan vatten. Antalet agenter av typen *j* som är beroende av systemet betecknas som $N_{j,dep}$, och antal agenter av typen *j* som inte har tillgång till systemet betecknas som $N_{j,loss}$. Meningen med att dela in agenterna i olika typer är alltså att kunna göra skillnad på konsekvenserna som drabbar olika typer av agenter i olika riskscenarier, d.v.s. att en agent av en typ saknar funktionen hos det tekniska systemet behöver inte vara lika illa som att en agent av en annan typ saknar funktionen.

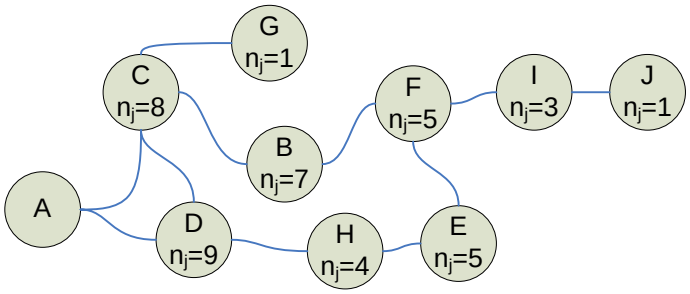
I många fall kan det hända att det finns andra konsekvensattribut som är mer intressanta än att uppskatta hur många av de olika agenterna som inte har tillgång till den service som systemet normalt förser dem med. Denna typ av konsekvensattribut, d.v.s. antal agenter av en viss typ som det tekniska systemet inte fungerar för, bör dock kunna fungera som bra ersättningsattribut (proxyvariabel) för en stor del av de typer av konsekvenser som kan vara mer intressanta. Exempelvis är konsekvensen ”totalt antal omkomna personer under riskscenariot” eller ”totala kostnader till följd av riskscenarier” som kanske är de verkligt intressanta attributen i en analys. Men på grund av att det är svårt att beskriva dessa konsekvensattribut med hjälp av modellen av det tekniska systemet används i stället ersättningsattributet ”maximalt antal agenter av typen *j* som inte har tillgång till det fungerande tekniska systemet under riskscenariot”. Om ersättningsattributet är bra eller ej avgörs av hur väl det samvarierar med de ”optimala” konsekvensattributen för de olika riskscenarierna. Om ersättningsattributet alltid korrelerar väl med det konsekvensattribut det ersatt, med avseende på konsekvensernas allvarlighetsgrad, är attributet bra. Om det däremot inte finns någon korrelation mellan ersättningsattributet och det konsekvensattribut som ersatts är ersättningsattributet inte bra. Att ha en hög grad av samvariation mellan konsekvensattributet och ersättningsattributet har delvis att göra med hur noggrann indelningen av agenterna i olika grupper utförs. Om man exempelvis antar att äldre människor har mycket högre sannolikhet att omkomma på grund av att ett visst tekniskt system inte fungerar kan samvariationen mellan konsekvensattributet ”totalt antal omkomna personer under riskscenariot” och ”maximalt antal agenter utan tillgång till det tekniska systemet under riskscenariot” vara relativt låg. Om däremot agenterna delas in i grupperna ”gamla människor” och ”övriga människor” kan man åstadkomma en hög samvariation mellan variablerna ”totalt antal omkomna personer under riskscenariot” och ”maximalt antal agenter av en viss typ (d.v.s. gamla människor) utan tillgång till det tekniska systemet under riskscenariot”.

Ett kompletterande mått på konsekvenserna av en påfrestning än antal agenter av typen *j* som inte har tillgång till ett specifikt system, $N_{j,loss}$, är det normerade konsekvensmåttet C_j, se ekvation 11. Måttet har som fördel att det är lättare att jämföra system som försörjer olika många agenter om konsekvenserna alltid normeras till ett värde mellan 0 och 1. Dock kan man även förlora intressant information om de konsekvenser som uppstår, då man omvandlar konsekvenserna från absoluta tal till ett ratio.

$$C_j = \frac{N_{j,loss}}{N_{j,dep}} \tag{11}$$

Nästa steg i analysen är att göra en nätverksmodell av det tekniska systemet, d.v.s. representera det med hjälp av noder och länkar. Alla noder (och ibland även länkarna) har en tillståndsvariabel, t_i, som representerar huruvida den aktuella systemdelen fungerar eller ej. Vad ”fungerar” innebär har att göra med vilken typ av tekniskt system som analyseras. Om exempelvis ett eldistributionssystem analyseras avser ”fungerar” att el kan distribueras genom den aktuella delen och ”fungerar ej” avser att distributionen inte är möjligt. Systemet beskrivs enklast genom en så kallad kontakt-matris (se tidigare i detta kapitel).

Med hjälp av nätverksmodellen kan sårbarheten för olika typer av påfrestningar analyseras, exempelvis slumpmässig utslagning av en viss andel av noderna eller länkarna. Ett datorprogram kan generera alla systemtillstånd, eller åtminstone ett tillräckligt stort urval av möjliga systemtillstånd, som den aktuella påfrestningen kan innebära och kan dessutom beräkna sannolikheten för de olika tillstånden givet påfrestningen. I Figur 3 presenteras samma nätverk som återfinns i Figur 1, men med skillnaden att varje nod (utom A) är förknippad med ett visst antal agenter som är beroende av just den systemdelen, n_j.



Figur 3 En nätverksmodell av ett tekniskt system med ett visst antal agenter (n_j) kopplade till de olika delarna av systemet.

Anta att det är intressant att studera hur sårbart systemet, som illustreras i Figur 3, är för någon typ av påfrestning. Påfrestningen kan beskrivas genom att precisera exakt vilken del av nätverket som slås ut, exempelvis ”Systemdel B slås ut”, eller genom att beskriva påfrestningen mer generellt, exempelvis ”1 av 10 systemdelar slås ut”. Sårbarheten för den första typen av påfrestning kan beskrivas enkelt med hjälp av den operationella definitionen av sårbarhet. Den uppsättning riskscenarier som utgör sårbarheten är i det fallet ett enda. Scenariot innebär att del B slås ut och att de 7 agenter som är beroende av den aktuella delen därmed blir utan den resurs som systemet förser dem med. Sannolikheten för detta scenario givet påfrestningen är 1 och konsekvenserna är $N_{j,loss} = 7$ eller $C_j = 0.16$ beroende på om konsekvenserna normeras eller inte.

För den andra typen av påfrestning finns det flera möjliga systemtillstånd som överensstämmer med beskrivningen av påfrestningen och därmed består mängden systemtillstånd i T_P av fler än ett tillstånd. I det aktuella fallet motsvaras påfrestningen av 10 möjliga systemtillstånd och vart och ett av dessa systemtillstånd ger upphov till ett specifikt riskscenario[6]. Ett systemtillstånd kan ses som en vektor, T, av de olika tillståndsvariablerna t_A, t_B, o.s.v., vilka antar värdet 0 om den systemdel som de representerar inte fungerar och värdet 1 om den fungerar, d.v.s. $T = (t_A, t_B, t_C, t_D, t_E, t_F, t_G, t_H, t_I, t_J)$. Detta innebär att T_P innehåller följande systemtillstånd:

$T_P =$ *[(0, 1, 1, 1, 1, 1, 1, 1, 1, 1),*
(1, 0, 1, 1, 1, 1, 1, 1, 1, 1),
(1, 1, 0, 1, 1, 1, 1, 1, 1, 1),
(1, 1, 1, 0, 1, 1, 1, 1, 1, 1),
(1, 1, 1, 1, 0, 1, 1, 1, 1, 1),
(1, 1, 1, 1, 1, 0, 1, 1, 1, 1),
(1, 1, 1, 1, 1, 1, 0, 1, 1, 1),
(1, 1, 1, 1, 1, 1, 1, 0, 1, 1),
(1, 1, 1, 1, 1, 1, 1, 1, 0, 1),
(1, 1, 1, 1, 1, 1, 1, 1, 1, 0)]

Varje systemtillstånd i T_P ger upphov till ett riskscenario, d.v.s. till en väg genom tillståndsrymden. Denna väg kan bestämmas med hjälp av de enkla regler som används för systemet, d.v.s. att en systemdel fungerar så länge det finns en väg genom nätverket till nod A. Genom att använda exempelvis algoritmen som beskrivs av Newman [2] kan alla de noder som inte har en väg genom nätverket till nod A identifieras, vilket i sin tur gör det möjligt att beskriva sluttillståndet för de olika riskscenarierna, d.v.s. de som har kontakt med noden A efter påfrestningen fungerar och de som inte har kontakt fungerar inte. I Tabell 1 visas resultatet av analysen, d.v.s. en beskrivning av de olika riskscenarierna, S_i, som kan inträffa som resultat av påfrestningen (en pil, →, innebär att systemets tillstånd förändras från det som beskrivs till vänster om pilen till det som är till höger om den), sannolikheten för de olika riskscenarierna, L_i, samt konsekvenserna av riskscenarierna, X_i.

[6] Eftersom det här exemplet inte involverar några kaskadutslagningseffekter eller någon annan typ av dynamik i systemet blir antalet riskscenarier per systemtillstånd i T_P lika med 1, men så behöver det inte vara om modellen innehåller mer dynamik och det inte är möjligt att avgöra vilket riskscenario som blir resultatet av ett specifikt systemtillstånd i T_P.

Tabell 1 **Beskrivning av resultatet från en sårbarhetsanalys av påfrestningen ”10% av systemdelarna slås ut” på systemet som illustreras i Figur 3. S_i är en beskrivning av de olika riskscenarierna som kan orsakas av påfrestningen, L_i är deras respektive sannolikhet (givet att påfrestningen inträffat) och X_i är en beskrivning av konsekvenserna i termer av hur många agenter av typen *j* som inte har tillgång till systemet.**

i	S_i	L_i	X_i
1	*(0, 1, 1, 1, 1, 1, 1, 1, 1, 1) → (0, 0, 0, 0, 0, 0, 0, 0, 0, 0)*	*1/10*	$N_{j,loss} = 43$
2	*(1, 0, 1, 1, 1, 1, 1, 1, 1, 1) → (1, 0, 1, 1, 1, 1, 1, 1, 1, 1)*	*1/10*	$N_{j,loss} = 7$
3	*(1, 1, 0, 1, 1, 1, 1, 1, 1, 1) → (1, 1, 0, 1, 1, 1, 0, 1, 1, 1)*	*1/10*	$N_{j,loss} = 9$
4	*(1, 1, 1, 0, 1, 1, 1, 1, 1, 1) → (1, 1, 1, 0, 1, 1, 1, 1, 1, 1)*	*1/10*	$N_{j,loss} = 9$
5	*(1, 1, 1, 1, 0, 1, 1, 1, 1, 1) → (1, 1, 1, 1, 0, 1, 1, 1, 1, 1)*	*1/10*	$N_{j,loss} = 5$
6	*(1, 1, 1, 1, 1, 0, 1, 1, 1, 1) → (1, 1, 1, 1, 1, 0, 1, 1, 0, 0)*	*1/10*	$N_{j,loss} = 9$
7	*(1, 1, 1, 1, 1, 1, 0, 1, 1, 1) → (1, 1, 1, 1, 1, 1, 0, 1, 1, 1)*	*1/10*	$N_{j,loss} = 1$
8	*(1, 1, 1, 1, 1, 1, 1, 0, 1, 1) → (1, 1, 1, 1, 1, 1, 1, 0, 1, 1)*	*1/10*	$N_{j,loss} = 4$
9	*(1, 1, 1, 1, 1, 1, 1, 1, 0, 1) → (1, 1, 1, 1, 1, 1, 1, 1, 0, 0)*	*1/10*	$N_{j,loss} = 4$
10	*(1, 1, 1, 1, 1, 1, 1, 1, 1, 0) → (1, 1, 1, 1, 1, 1, 1, 1, 1, 0)*	*1/10*	$N_{j,loss} = 1$

Tabell 1 består av 10 rader – en rad per riskscenario. Om systemet som analyserades i stället hade innehållit 50 systemdelar (i stället för 10) som representeras av noder i nätverket hade antalet riskscenarier varit 2 118 760[7], givet att 10% av systemdelarna slås ut. Antalet riskscenarier som måste analyseras ökar alltså mycket fort då system-storleken ökar och det är en anledning till att analys av sårbarhet med hjälp av den metod som beskrivs här i praktiken måste utföras av ett datorprogram. Men även om ett datorprogram kan beräkna konsekvensen och sannolikheten för de olika riskscenarierna är det svårt för användaren att dra några slutsatser rörande systemets sårbarhet med hjälp av en lista med riskscenarier som kan vara mycket lång.

4.2 Mått på sårbarhet

Ett sätt att reducera problemet förknippat med det stora antalet riskscenarier är att utifrån den operationella definitionen av sårbarhet definiera olika *sårbarhetsmått* som är lättare använda. Ett sådant mått är de *förväntade konsekvenserna* av påfrestningen. För att kunna beräkna de förväntade konsekvenserna måste konsekvenserna uttryckas med hjälp av ett numeriskt konsekvensattribut. De förväntade konsekvenserna, $E(X)$, av en påfrestning med n riskscenarier kan då beräknas enligt ekvation 12, där L_i är sannolikheten för riskscenario i (givet att den specifika påfrestningen inträffar) och X_i är konsekvensen för detta scenario. I ekvationen förutsätts att konsekvenserna är uttryckta med någon typ av numeriskt attribut.

[7] Antalet möjliga kombinationer av komponenter som kan slås ut beräknas som: $\binom{50}{5} = \frac{50!}{45!\cdot 5!} = \frac{50\cdot 49\cdot 48\cdot 47\cdot 46}{5\cdot 4\cdot 3\cdot 2\cdot 1} = 2118760$

$$E(X) = \sum_{i=1}^{n} L_i \cdot X_i \tag{12}$$

De förväntade konsekvenserna av påfrestningen på systemet som redovisas i Figur 3 är 9,2 agenter som förlorar systemfunktionen. I stället för att använda väntevärdet för konsekvensmåttet *E(X)* som mått på sårbarhet kan man använda väntevärdet för det normerade konsekvensmåttet i ekvation 11, $E(C_j)$, se ekvation 13, där $C_{j,i}$ är de normerade konsekvenserna för agenter av typen *j* då riskscenario *i* inträffar.

$$E(C_j) = \sum_{i=1}^{n} L_i \cdot C_{j,i} \tag{13}$$

I exemplet ovan blir[8] *E(C)* = 0,21, d.v.s. den förväntade andelen agenter som förlorar tillgången till systemet vid den aktuella påfrestningen är 21%.

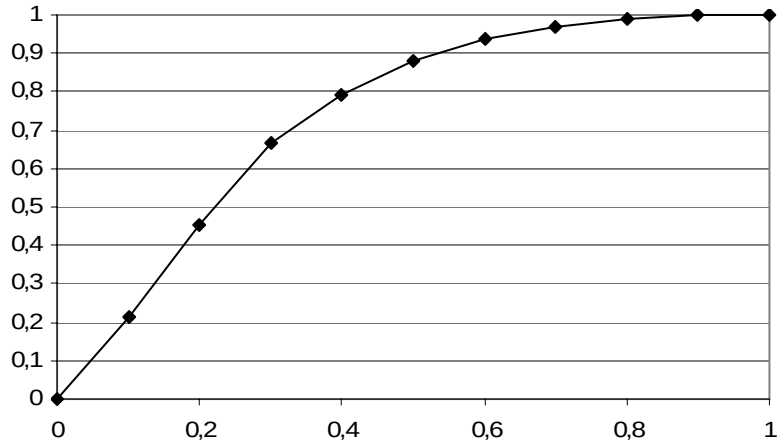
Då en sårbarhetsanalys genomförs för ett tekniskt system måste påfrestningen som är utgångspunkten för analysen specificeras (se ovan), men det är inte alltid lätt att veta om systemet skall analyseras för en påfrestning då 10% av systemdelarna slås ut, eller kanske då 5% slås ut, eller 1%. I stället för att bestämma exakt vilken påfrestning som systemet skall analyseras för kan man analysera ett antal påfrestningar och sedan jämföra resultaten, i termer av de förväntade konsekvenserna, för olika nivåer av påfrestningen.

Den metod för att göra detta som presenteras här går ut på att beräkna den förväntade konsekvensen för olika grader av påfrestningar. Den första graden av påfrestning är ”1 systemdel slås ut”, den andra är ”2 systemdelar slås ut”, o.s.v. till den sista typen som är ”alla systemdelar slås ut”. Resultatet från sårbarhetsanalysen av var och en av dessa påfrestningar kan presenteras med hjälp av det normerade konsekvensmåttet i ekvation 11. Genom att i ett diagram rita ut väntevärdet för det normerade konsekvensmåttet som funktion av andelen systemdelar som slås ut i den aktuella påfrestningen kan en bra illustration av systemets sårbarhet för olika grader av påfrestning skapas. Diagrammet visar hur stora konsekvenserna förväntas bli för påfrestningar av olika allvarlighetsgrad (hur många delar av systemet som slås ut).

Att räkna fram den nödvändiga informationen för ett sådant diagram manuellt är praktiskt omöjligt för stora system. Även för ett datorprogram kan det vara tidsödande att räkna fram detta diagram exakt för stora system och därför kan man använda sig av Monte Carlo-simulering i stället. Simuleringen ger en approximativ lösning genom att simulera ett stort antal riskscenarier och sedan beräkna väntevärdet för konsekvenserna i dessa scenarier. I Figur 4 illustreras resultatet från en analys av systemet i Figur 3. I figuren visas det förväntade normerade konsekvensmåttet, eller den förväntade andelen agenter som inte har tillgång till systemet, som funktion av hur många noder som är utslagna i systemet, d.v.s. påfrestningens storlek. Som väntat går kurvan från punkten

[8] Om enbart *en* grupp av agenter analyseras kan indexet *j* utelämnas.

(0,0), som representerar systemet utan någon påfrestning till punkten (1,1), som representerar systemet då samtliga noder slagits ut. Det intressanta med diagrammet är hur snabbt kurvan stiger upp mot 1, d.v.s. hur stor andel av noderna som måste slås ut för att en stor del av agenterna skall förlora tillgång till systemet.



Figur 4 **Det förväntade normerade konsekvensmåttet som funktion av andelen noder som slagits ut i systemet (storleken på påfrestningen).**

Ibland kan det även vara intressant att inte bara studera de förväntade konsekvenserna av en påfrestning utan även spridningen av de konsekvenser som är möjliga givet en viss påfrestning. Detta kan göras på (åtminstone) två sätt. För det första skulle man utöver kurvan som gäller den förväntade konsekvensen i Figur 4 kunna presentera konfidensintervall för konsekvenserna, t.ex. inom vilket intervall konsekvenserna hamnar med 95% säkerhet givet en viss påfrestning. För det andra skulle sannolikheterna för att konsekvenserna överstiger vissa specifika nivåer givet påfrestningen också kunna presenteras.

Den typ av diagram som illustreras i Figur 4 är bra för att ge en överblick över hur systemet klarar av att stå emot olika typer och storlekar av påfrestningar, men det kan vara svårt att göra jämförelser mellan två system, eller mellan två olika utformningsalternativ för samma system. Anledningen är att det kan vara svårt att jämföra två kurvor med varandra. Så länge en kurva alltid är placerad över den/de andra kurvan/kurvorna bör det inte vara något problem att avgöra vilket system som är mest robust mot den aktuella typen av påfrestning, men om kurvorna korsar varandra kan detta vara svårare.

Sårbarhetskoefficient
För att göra det lättare att jämföra olika system ur sårbarhetssynpunkt kan måttet *Societal Vulnerability Coefficient* (SVC), eller *sårbarhetskoefficient*, användas [22]. SVC är arean under grafen som bildas av *E(C)* som funktion av andelen utslagna

noder, *f*, d.v.s. en sådan graf som illustreras i Figur 4. SVC är ett mått mellan 0 och 1 där ett högre värde betyder att den förväntade normerade konsekvensen ökar snabbt när påfrestningen på systemet ökar (andelen utslagna noder ökar). SVC för exemplet som illustreras i Figur 4 är 0,79. SVC föreslogs ursprungligen som ett lämpligt mått för sårbarhet i eldistributionsnät, men måttet kan användas även för andra system som har liknande egenskaper, d.v.s. som har en nätverksstruktur och ett antal agenter som betjänas av systemet.

Design koefficient

Ett annat mått som också ursprungligen föreslogs för elsystem, men som också kan vara användbart för andra typer av system är *design coefficient*, DC [22]. DC har att göra med i vilken ordning de olika noderna i nätverket tenderar att slås ut då antalet utslagna noder går från 0 till samtliga noder. Tanken är att i en ”robust” design av systemet så skall de noder som flest agenter är beroende av slås ut sist och de som har få agenter skall slås ut först när systemet drabbas av en påfrestning. Varje nod, v_i, har ett antal agenter som är beroende av att just den noden fungerar, n_i, vilket betyder att om den aktuella noden slås ut förlorar agenterna den funktion som representeras av nätverket (exempelvis leverans av elektricitet i ett elnätverk). För en nod v_i är attributet n_i lika med 0 om det inte finns några agenter kopplade till noden. Vid en analys av DC slås noder och eller länkar ut slumpmässigt eller med någon typ av riktad strategi (se genomgången tidigare i detta kapitel). Andelen noder/länkar av det totala antalet som måste slås ut för att en specifik nod skall förlora sin funktion (exempelvis förlora kontakten med en inmatningskälla i ett elnätverk) betecknas f_i. Eftersom analysen bygger på ett antal simuleringar, som kan vara slumpmässiga, behöver inte värdet f_i vara lika vid två olika simuleringar. Därför är medelvärdet av f_i över ett antal simuleringar, $\overline{f}_i$, ett bättre mått på hur snabbt en specifik nod förlorar sin funktion när nätverket attackeras. Ett mått på sårbarhet då konsekvenserna mäts i termer av hur många agenter som saknar funktionen av det aktuella systemet blir då Pearsons korrelationskoefficient (r) beräknad med avseende på n_i och $\overline{f}_i$ för de noder där $n_i \neq 0$. N är antalet noder där $n_i \neq 0$, se ekvation 14.

$$DC = \frac{\sum_{n_i \neq 0} \left(n_i \cdot \overline{f}_i \right) - \frac{\sum_{n_i \neq 0} n_i \cdot \sum_{n_i \neq 0} \overline{f}_i}{N}}{\sqrt{\left(\sum_{n_i \neq 0} n_i^2 - \frac{\left(\sum_{n_i \neq 0} n_i \right)^2}{N} \right) \cdot \left(\sum_{n_i \neq 0} \overline{f}_i^{\,2} - \frac{\left(\sum_{n_i \neq 0} \overline{f}_i \right)^2}{N} \right)}} \qquad (14)$$

Koefficienten ger ett mått på hur väl attributen ”antal agenter beroende av noden v_i”, n_i, och ”hur länge noden v_i i medeltal behåller funktionen då fler och fler noder i nätverket

slås ut”, $\overline{f}_i$, korrelerar. Detta är ett globalt mått för nätverket och om DC har värden som är nära -1 innebär det att noder som har stor andel agenter kopplade till sig slås ut tidigt vid påfrestningen och om DC har ett värde nära 1 slås dessa noder ut sist.

Det finns ett annat sätt att beräkna en design koefficient än det som precis redovisats. I det sätt som redovisats ovan förutsätts att alla noderna i systemet förr eller senare slås ut, d.v.s. i en simulering inleder man med att slå ut en nod och notera vilka andra noder som slutat fungera, sen slår man ut nästa, o.s.v. I stället för att utgå från att alla noder skall slås ut kan man utgå från någon annan typ av påfrestning när design koefficienten beräknas. Antag exempelvis att man vill beräkna design koefficienten för den påfrestning och det system som resulterade i Tabell 1. Eftersom påfrestningen som analyseras endast innebär utslagning av 10% av noderna finns inga beräkningar av $\overline{f}_i$, d.v.s. hur stor andel noder som i medeltal måste slås ut för att nod v_i skall sluta fungera. I stället för att analysera korrelationen mellan antal agenter som är beroende av en specifik nod, n_i, och $\overline{f}_i$ kan man analysera korrelationen mellan, n_i, och *sannolikheten* att en specifik nod fortfarande fungerar efter riskscenarierna som uppkommer på grund av en specifik påfrestning, $P(t_i = 1 | T_P)$. Sannolikheten att en specifik nod fortfarande fungerar efter en påfrestning kan beräknas med hjälp av den operationella definitionen av sårbarhet. Exempelvis kan sannolikheten att de olika noderna i systemet som illustreras i Figur 3 slutar fungera på grund av att 10% av noderna slås ut beräknas med hjälp av Tabell 1. För att göra det summerar man sannolikheten, L_i, för alla de risk-scenarier där den aktuella noden fortfarande fungerar, d.v.s. de riskscenarier där variabeln som motsvarar den aktuella nodens funktion i vektorn som representerar systemets tillstånd är 1. Resultatet om Tabell 1 används som grund för att beräkna koefficienten är 0,79, d.v.s. noder som många agenter är beroende av har också hög sannolikhet att fungera efter påfrestningen. Den här typen av design koefficient kan sägas vara betingad av en specifik påfrestning, P, och därför benämns den DC_P.

4.3 Olika typer av påfrestningar

Tidigare i det här kapitlet har påfrestningar beskrivits genom att ange hur många, eller hur stor andel av det totala antalet, noder eller länkar i ett nätverk som slås ut. Då är det underförstått att alla kombinationer av länkar/noder som stämmer överens på beskrivningen skall ingå i T_P och att de olika systemtillstånden är lika sannolika. De systemtillstånd som då ingår i T_P kan sägas utgöra svaret på frågan ”vilka kombinationer av noder kan slås ut om x antal noder skall slås ut i nätverket?”. Det kan dock vara intressant att undersöka andra typer av påfrestningar än bara slumpmässig utslagning av noder och länkar, exempelvis sådana påfrestningar som i högre grad drabbar kritiska komponenter i ett system. En sådan typ av påfrestning benämns riktad påfrestning (se avsnitt 3.1). Ett exempel på en sådan påfrestning är att slå ut de noder som har högst *intermeditet*, $B(v_i)$, först. Intermeditet är ett mått på hur många kortaste vägar mellan två noder i nätverket som passerar den aktuella noden och om de noderna med högst intermeditet slås ut innebär det att flest kortaste vägar mellan olika noder i nätverket bryts. Detta kan sägas representera en allvarlig typ av påfrestning på nätverk där nätverkets funktion i hög grad bestäms av hur många av noderna som har kontakt

med varandra, exempelvis ett nätverk som representerar möjligheten till kommunikation mellan olika agenter och där alla agenter kommunicerar med varandra.

I tekniska nätverk av den typ som illustreras i Figur 3, d.v.s. där funktionen hos de olika noderna beror på om det finns en väg genom nätverket till en eller flera specifika noder, är dock inte intermediteten ett lika bra mått för att identifiera de noder som gör störst skada på nätverket om de slås ut. Ett bättre sätt är i stället att beräkna antalet kortaste vägar mellan samtliga noder och en *specifik grupp av noder*, som benämns *källnoder*. I ett elnät, exempelvis, motsvarar källnoder de noder där elektriciteten matas in i nätverket. Detta sätt att beräkna intermeditet innebär att bara de kortaste vägarna i nätverket som går mellan noderna i nätet och någon av de noder som klassas som källnoder ingår i beräkningen av måttet. För att skilja detta mått från ”normal” intermeditet benämns det *källnodsintermeditet,* $B_S(v_i)$, och kan beräknas genom att göra en liten ändring av algoritmen som föreslagits av Newman [2], vilken innebär att bara de kortaste vägarna som går till en källnod används i beräkningen.

Att slå ut noder som har hög *källnodsintermeditet* innebär att noder som är mycket viktiga för ett nätverks funktion (om nätverket är av den typ som illustreras i Figur 3) slås ut först och detta utgör mycket allvarligare attacker på nätverk av den här typen än om noder med hög intermeditet skulle slås ut först.

Att analysera sårbarheten i ett system på grund av en påfrestning av den här typen innebär vanligtvis att mängden systemtillstånd som ingår i T_P är mindre än om typen av påfrestning vore slumpmässig. Om exempelvis nätverket i Figur 3 analyseras med avseende på påfrestningar som innebär att de noder med högst källnodsintermeditet slås ut först kommer resultatet att skilja sig väsentligt från det som erhölls då nätverket analyserades med avseende på slumpmässig utslagning av noder. I Tabell 2 presenteras källnodsintermediteten för de olika noderna i nätverket.

Tabell 2 Källnodsintermediteten för de olika noderna i nätverket i Figur 3.

Nod	Källnodsintermeditet
A	10
B	4
C	6
D	3
E	1
F	3
G	1
H	2
I	2
J	1

En påfrestning på nätverket som definieras som ”Utslagning av de x noder som har högst källnodsintermeditet, $B_S(v_i)$.” har en mindre mängd systemtillstånd i T_P än då påfrestningen är ”Slumpmässig utslagning av x noder.”. I Tabell 1 illustreras att T_P då x = 1 och påfrestningen är slumpmässig består av 10 stycken systemtillstånd. Då utslagningen sker av de noder med högst källnodsintermeditet och x = 1 är $T_P = [(0, 1,$

1, 1, 1, 1, 1, 1, 1, 1)], d.v.s. T_P består enbart av ett enda systemtillstånd. Utslagning av noder med hög källnodsintermeditet skulle kunna representera en antagonistisk attack mot nätverket där attacken utgår från att förstöra de delar av nätverket som, utifrån global information om nätverksstrukturen, verkar vara de viktigaste.

En annan påfrestningstyp som kan vara användbar är ”Utslagning av de x noder som har högst grad, k_i.”. En nods grad är ett mått på hur många länkar som finns kopplade till noden och denna typ av påfrestning är också vanligtvis allvarligare än en slumpmässig påfrestning. Utslagning av noder med hög grad skulle kunna representera en antagonistisk attack mot nätverket där attacken utgår från att förstöra de delar av nätverket som, utifrån enbart lokal information rörande noderna, verkar vara de viktigaste.

I Tabell 3 presenteras graden för de olika noderna i nätverket som illustreras i Figur 3. Då påfrestningen på systemet innebär att de noder med högst grad slås ut först och antalet noder som slås ut (x) är 1 kommer T_P att bestå av ett enda systemtillstånd, nämligen *(1, 1, 0, 1, 1, 1, 1, 1, 1, 1)*.

Tabell 3 **Nodernas grad i nätverket som illustreras i Figur 3.**

Nod	Grad
A	2
B	2
C	4
D	3
E	2
F	3
G	1
H	2
I	2
J	1

Båda typerna av påfrestningar, utslagning av noder baserat på källnodsintermeditet och baserat på nodernas grad, ger vanligtvis upphov till en reduktion av antalet systemtillstånd i T_P och därmed också till en reduktion i antalet riskscenarier jämfört med den slumpmässiga påfrestningstypen. I Tabell 4 och Tabell 5 finns de riskscenarier (S_i) som de olika påfrestningarna som diskuterats ovan resulterar i, samt deras respektive sannolikhet givet påfrestningen (L_i), och konsekvenser (X_i). Notera att båda påfrestningarna innebär samma antal utslagna noder i nätverket som den påfrestning som resulterade i Tabell 1, men antalet riskscenarier är bara ett jämfört med Tabell 1 som innehåller tio.

Tabell 4 **Resultatet från en sårbarhetsanalys av systemet som illustreras i Figur 3. Påfrestningen som är utgångspunkten för analysen är: ”Utslagning av den nod med högst källnodsintermeditet”.**

i	S_i	L_i	X_i
1	*[0, 1, 1, 1, 1, 1, 1, 1, 1, 1] → [0, 0, 0, 0, 0, 0, 0, 0, 0, 0]*	*1*	$N_{j,loss} = 43$

Tabell 5 **Resultatet från en sårbarhetsanalys av systemet som illustreras i Figur 3. Påfrestningen som är utgångspunkten för analysen är: ”Utslagning av den nod som har högst grad”.**

i	S_i	L_i	X_i
1	$[1, 1, 0, 1, 1, 1, 1, 1, 1, 1] \rightarrow [1, 1, 0, 1, 1, 1, 0, 1, 1, 1]$	1	$N_{j,loss} = 9$

Resultaten från sårbarhetsanalyserna illustrerar att ett system kan vara mer eller mindre sårbart för en specifik typ av påfrestning. Tabell 4 och Tabell 5 visar exempelvis att det aktuella systemet är mer sårbart för påfrestningar som innebär att den nod som har högst källnodsintermeditet slås ut än påfrestningar som innebär att den som har högst grad slås ut.

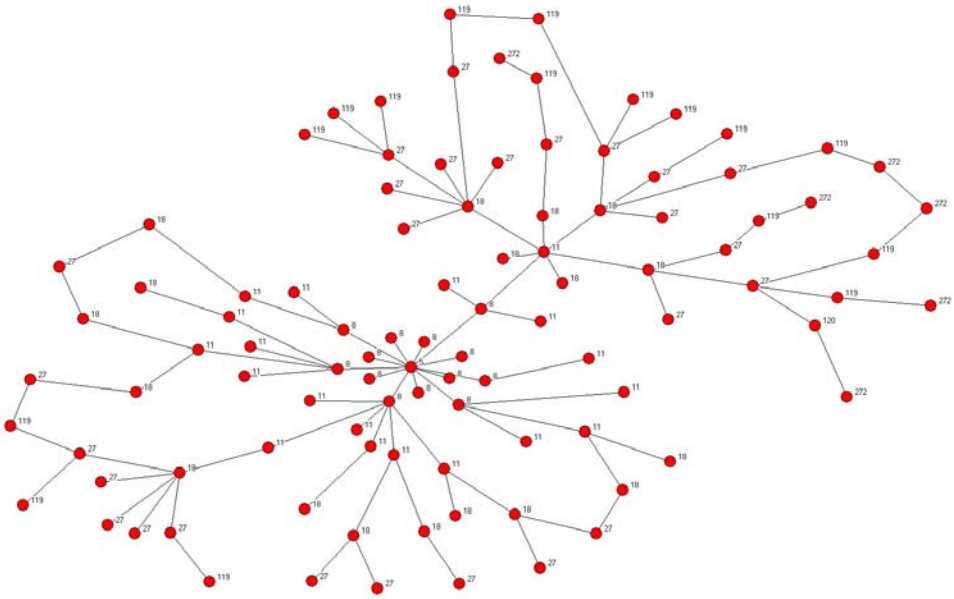
4.4 Exempel på sårbarhetsanalys av ett lokalt eldistributionssystem

Tillämpningen av sårbarhetsmåtten som presenterats ovan kan konkretiseras genom att visa ett exempel på hur en analys kan se ut. För det mesta är det troligt att den här typen av analys kommer att genomföras för agenter av typen ”kunder”. En anledning är att det kan vara lättare att få information om hur många kunder som är kopplade till ett visst system än t.ex. hur många människor som bor i de hushåll som motsvarar en kund. Anta att man är intresserad av att undersöka robustheten i eldistributionssystemet i en mindre kommun och att en kartläggning av systemet har genomförts och att det nu finns en nätverksmodell av elnätet som innehåller uppgifter om hur många kunder som är kopplade till de olika nätstationerna.

I Figur 5 illustreras ett fiktivt elnät i en mindre stad med 5000 abonnenter. För att skapa nätverket genererades först ett nätverk med 100 noder med hjälp av modellen för skalfria nätverk [6]. Därefter adderades ett antal länkar för att skapa looparna i nätet. Normalt finns det frånskiljare och brytare som gör att dessa loopar inte är slutna, men i en sårbarhetsanalys kan man anta att dessa frånskiljare och brytare är slutna om tiden det tar att ändra frånskiljarnas och brytarnas lägen är betydligt mindre än den tid det tar att reparera nätet. Slutligen fördelades 5000 abonnenter över nätet. De flesta abonnenter placerades nära punkten där nätet antas matas (den centrala nod som har 12 länkar kopplade till sig). Ju längre bort från inmatningspunkten en nod är, desto färre abonnenter har den.

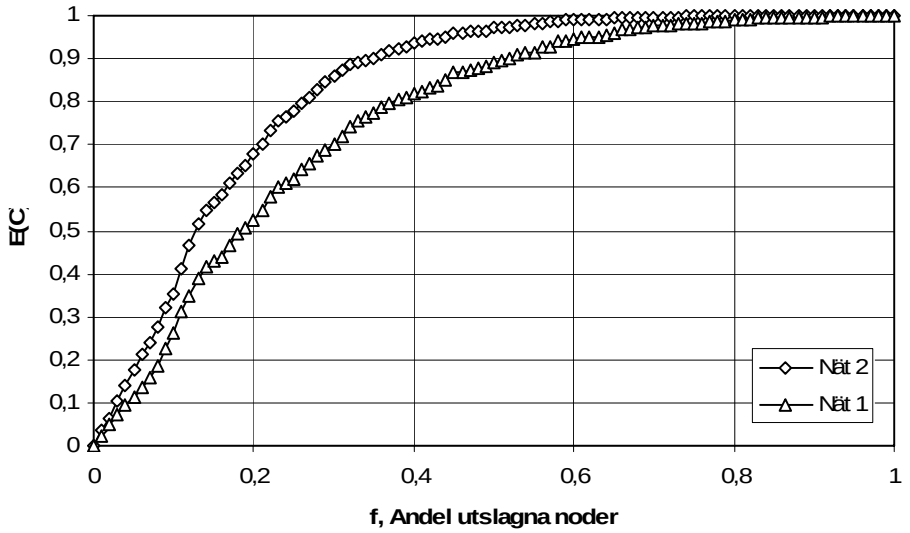
Ett andra nät med identisk struktur skapades också. Det andra nätet har dock en annan fördelning av abonnenterna än det första. I det andra nätet är det fler abonnenter i nätets ytterkanter (de noder som är långt bort från inmatningspunkten).

Figur 5 **Nät 1. Ett fiktivt elnät i en mindre stad. Fördelningen av abonnenter (siffrorna vid noderna) är koncentrerad till nätets inmatningspunkt (noden med 12 länkar).**



Figur 6 **Nät 2. Ett fiktivt elnät i en mindre stad. Fördelningen av abonnenter (siffror vid noderna) är koncentrerad till nätets yttre noder.**

Genom att göra en analys av slumpmässiga attacker mot elnätet kan man se hur väntevärdet för det normerade konsekvensmåttet, *E(C)* (inget index används eftersom det bara är ett nät som analyseras och bara en typ av agent), ökar som en funktion av andelen noder som slås ut, *f*. 50 simuleringar användes som underlag för att beräkna de förväntade konsekvenserna och i Figur 7 visas resultatet av dessa.

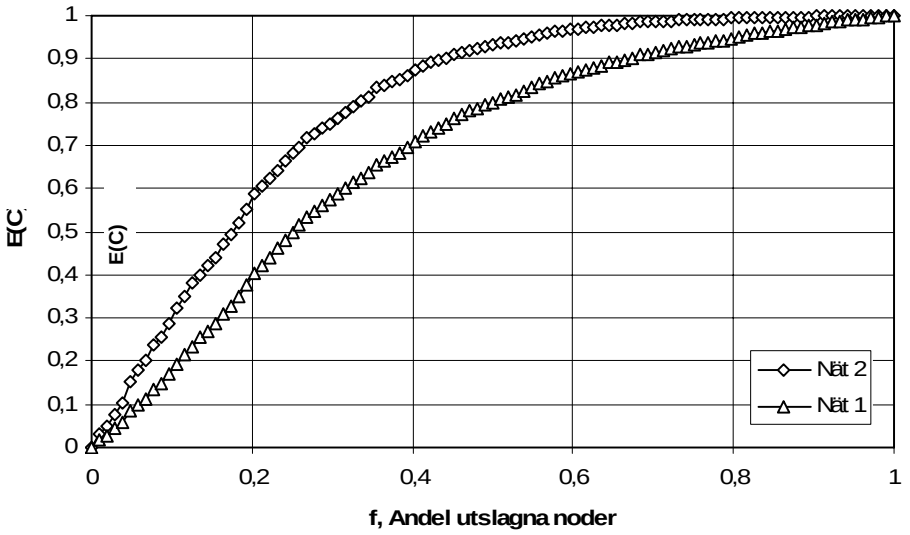


Figur 7 **Resultat från simuleringar av slumpmässiga attacker mot noderna i de båda elnäten i Figur 5 och Figur 6. Diagrammet visar medelvärdet för *C* över 100 simuleringar.**

Figur 7 är ett exempel på resultat som ger en indikation på sårbarheten i nätverket för slumpmässiga fel riktade mot noderna i nätet. De två nät som analyserats uppvisar skillnader när det gäller sårbarhet eftersom abonnenterna i det ena nätet (nät 2) förlorar kontakten med inmatningspunkten snabbare än abonnenterna i nät 1. Eftersom nätverkens strukturer är identiska uppkommer denna skillnad i sårbarhet av att abonnenterna i näten är fördelade på olika sätt mellan noderna. Sårbarhet i ett tekniskt system, då konsekvenserna definieras som antalet agenter som inte har tillgång till systemet, är alltså inte bara beroende på det tekniska systemet i sig utan även på hur agenterna är placerade i systemet.

Exemplet ovan visar hur en analys av ett tekniskt system kan genomföras med hjälp av nätverksanalys. Förutom att analysera slumpmässig utslagning av noder kan man även analysera slumpmässig utslagning av länkarna (ledningarna). Resultaten från en sådan simulering illustreras i Figur 8, där det framgår att resultatet liknar det som erhölls vid den föregående analysen, d.v.s. att nät 2 är mer sårbart (för slumpmässig utslagning av länkar) än nät 1. Det går också att genomföra analyser av riktade attacker mot nätverken, men i det här fallet blir resultatet inte så intressant eftersom elförsörjningen till samtliga abonnenter kommer att försvinna om noden där elen matas in i nätet försvinner. Inmatningsnoden kommer att vara den första som slås ut om man använder strategin att alltid slå ut den nod som har flest länkar. I ett verkligt distributionsnät är

simulering av antagonistiska attacker av intresse eftersom det i dessa fall kan finnas kopplingar till regionnät på flera ställen, alternativt om regionnätet ingår i analysen så kan det finnas flera kopplingar till stamnätet. Det är heller inte säkert att noderna som är kopplade till regionnät respektive stamnätet är de som har flest antal länkar, och i så fall ger analyser av antagonistiska attacker mot nätet bra information om sårbarheten.



Figur 8 **Resultat från simuleringar av slumpmässiga attacker mot länkarna i de båda elnäten i Figur 5 och Figur 6. Diagrammet visar medelvärdet för *E(C)* i 100 simuleringar.**

En analys av *DC* för nätverk 1 och 2 (se Figur 5 och Figur 6) ger resultatet *DC* = 0,95 för nät 1 och *DC* = -0,55 för nät 2 (slumpmässig utslagning av noder). Analysen bekräftar alltså de resultat som man kan ana genom att studera fördelningen av abonnenter i näten (Figur 5 och Figur 6), d.v.s. att noder med fler agenter slås ut tidigare i nät 2 än i nät 1 då fler och fler noder slås ut slumpmässigt i nätverket.

I beräkningen av *DC* används medelvärdet av hur stor andel av noder/länkar som måste slås ut innan en specifik nod förlorar sin funktion, f_i. f_i är ett lokalt mått, d.v.s. det mäter en egenskap hos en specifik nod och ibland kan sådana mått vara intressanta ur en sårbarhetsaspekt. Framförallt gäller detta då man vill illustrera vilka områden i nätverket som har en ”sämre position”, d.v.s. som slås ut tidigare än andra områden då nätverket utsätts för en specifik påfrestning. Genom att studera fördelningen av f_i över samtliga noder kan man få en sådan överblick. Det är även intressant att kombinera informationen om f_i med andra mått för de olika noderna, exempelvis antalet människor som berörs om noden slås ut.

4.5 Krav för användning av metoden

För att kunna använda den metod för sårbarhetsanalys av tekniska system som presenterats här krävs att ett antal villkor är uppfyllda. Först och främst måste systemet gå att beskriva i form av ett nätverk där strukturen på nätverket tillsammans med systemets tillstånd kan användas för att ta fram olika riskscenarier. Att ta fram riskscenarier innebär dels att påfrestningen för vilken systemets sårbarhet skall analyseras kan beskrivas som ett eller en mängd systemtillstånd, dels att det finns regler som kan användas för att ta reda på vad som kommer att hända i systemet efter att påfrestningen har påverkat systemtillståndet. I det exempel som illustrerats ovan har påfrestningen kunnat beskrivas genom att olika noder i nätverket slås ut. Utifrån denna beskrivning av en påfrestning har sedan regeln om att en nod som inte har kontakt med en speciell typ av nod (noden där elektriciteten matas in i exemplet ovan) inte fungerar och att alla som har kontakt med en sådan nod fungerar kunnat användas för att räkna ut effekten av påfrestningen, d.v.s. ett riskscenario.

Förutom att systemet måste kunna representeras i form av ett nätverk måste det också gå att identifiera ett eller flera lämpliga konsekvensattribut för systemet. Dessa konsekvensattribut bör vara numeriska för att beräkningarna som redovisas ovan skall fungera. Vidare måste det eller de konsekvensattribut som används gå att beräkna för varje systemtillstånd som kan uppkomma. Notera att vilka konsekvensattribut som är lämpliga i en viss kontext beror på de värderingar som ligger till grund för analysen. Konsekvensattribut som är lämpliga ur en kommuns perspektiv behöver därför exempelvis inte vara lämpliga ur nätägarens perspektiv. Detta berörs mer i detalj i rapporten ”Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv” [1].

Om dessa förutsättningar är uppfyllda går det att analysera påfrestningar som är mycket generellt formulerade, exempelvis ”10% av delarna i systemet slås ut”, och via ett datorprogram räkna fram de olika riskscenarierna, deras respektive sannolikhet och konsekvens, samt sammanställa resultatet på ett sätt som gör det lättöverskådligt.

5 Analys av verkliga elnät

Metoden som beskrivs ovan har även tillämpats på två verkliga elnät. Dessa sårbarhetsanalyser utfördes på elnäten i två svenska kommuner, båda med ca 30 000 invånare, och redovisas i sin helhet i [22]. Målet med studien var att analysera sårbarheten för distributionsnivån av elnäten, vilket inkluderar spänningsnivåer från 10 kV till 50 kV. Som konsekvensmått användes andel abonnenter utan elförsörjning, vilket motsvarar C_j i ekvation 11. Alla abonnenter betraktas alltså som likvärdiga ur ett konsekvensperspektiv.

5.1 Nätverksmodellering

Eldistributionssystemet representerades av ett nätverk bestående av tre nodtyper; nätstationer, transmissionsnoder och källnoder. I nätstationerna är abonnenterna inkopplade, oftast via ett 400V nät, och där transformeras elektriciteten i regel ner från 10kV till 400V. Lågspänningsnätet, 400V, modellerades inte i denna analys eftersom syftet med analysen var att undersöka sårbarheten i distributionsnätet. Transmissionsnoder är noder som varken har abonnenter kopplade till sig eller utgör inmatningspunkter, t.ex. en förgrening i nätverket. Källnoder är alla noder som kopplar samman distributionsnätet med spänningsnivåer på över 20 kV. Distributionssystemet är till viss del byggt maskat men drivs radiellt, vilket innebär att ett fel som uppstått drabbar alla abonnenter nedströms i nätet. Maskningen möjliggör dock omkopplingar vid eventuella fel vilket innebär att fördelningsstationer kan erhålla matning från alternativa inmatningspunkter om den normala vägen skulle vara ur funktion. I denna analys antogs det, liksom i föregående avsnitt, att omkopplingen tar betydligt kortare tid än att reparera felen. Det innebär att konsekvenserna som uppstår fram tills att omkopplingen är genomförd försummas. Följden för nätverksmodellen av elsystemet är att samtliga normalt öppna frånskiljare och brytare modelleras som slutna. I Tabell 6 presenteras relevant information om de två eldistributionsnäten.

Tabell 6 Information om de två elnäten.

Nätverksdata	System A	System B
Antal källnoder	7	8
Antal transmissionsnoder	191	442
Antal nätstationer	568	830
Totalt antal noder	766	1280
Totalt antal länkar	822	1342
Genomsnittlig grad	2.15	2.10
Genomsnittlig inverterad längd	0.0453	0.0437
Klustringskoefficient	0.00218	0.00461

Sårbarhetsanalyserna utfördes med avseende på sju typer av påfrestningar, slumpmässig nodutslagning, slumpmässig länkutslagning, utslagning av noder med högst grad (ursprunglig), utslagning av noder med högst källnodsintermeditet (se avsnitt 4.3 för förklaring av begreppet), samt utslagning av länkar med högst källnodsintermeditet. Den typ av påfrestning som innebär utslagning av noder/länkar med högst källnodsintermeditet delas vidare upp i två typer av påfrestningar, en som betecknas ”ursprunglig” och en som betecknas ”uppdaterad”. Den ursprungliga innebär att käll-

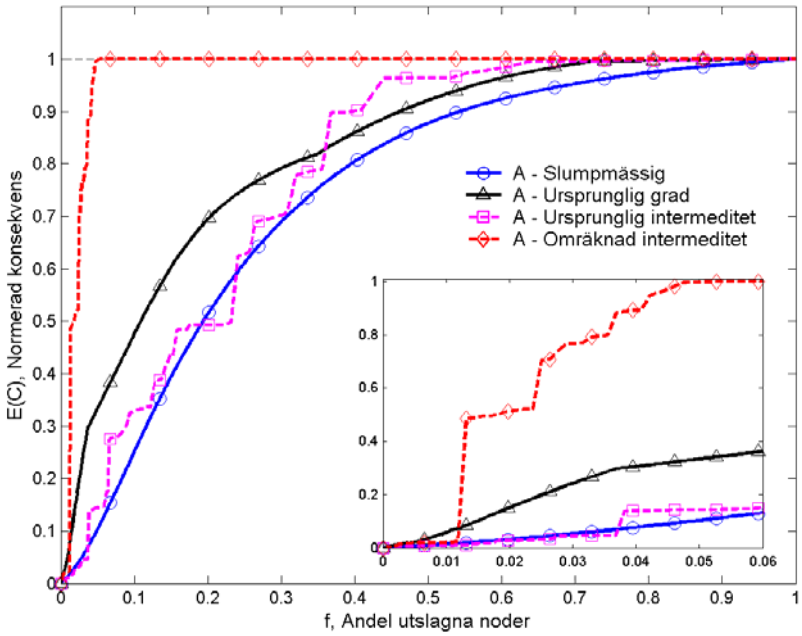
nodsintermediteten beräknas på samma sätt som beskrivs i avsnitt 4.3. Den uppdaterade innebär att de noder som skall slås ut bestäms genom att fortlöpande analysera alla noders källnodsintermeditet och låta de som har högst värde ingå bland de noder som skall slås ut först (om det finns fler noder med lika källnodsintermeditet sker valet mellan dem slumpmässigt). En uppdatering av källnodsintermeditet för samtliga noder med hänsyn taget till att vissa noder har blivit utslagna sker alltså baserat på den ”nya” strukturen på nätverket.

En *specifik* påfrestning på systemet definieras dels genom *typen av påfrestning*, dels genom påfrestningens storlek, d.v.s. genom att ange hur *stor andel av noderna/länkarna som slås ut*. En specifik påfrestning motsvaras av en uppsättning systemtillstånd T_P. För varje specifik påfrestning kan man beräkna det förväntade normerade konsekvensmåttet *E(C)*, d.v.s. i det här fallet väntevärdet för andelen abonnenter utan ström. Beräkningar av *E(C)* kan sedan utföras för olika andel utslagna noder/länkar. Resultatet ger en uppfattning om systemens sårbarhet för en viss typ av påfrestning men vid olika allvarlighetsgrad och kan sammanfattas i diagram som liknar det i Figur 4.

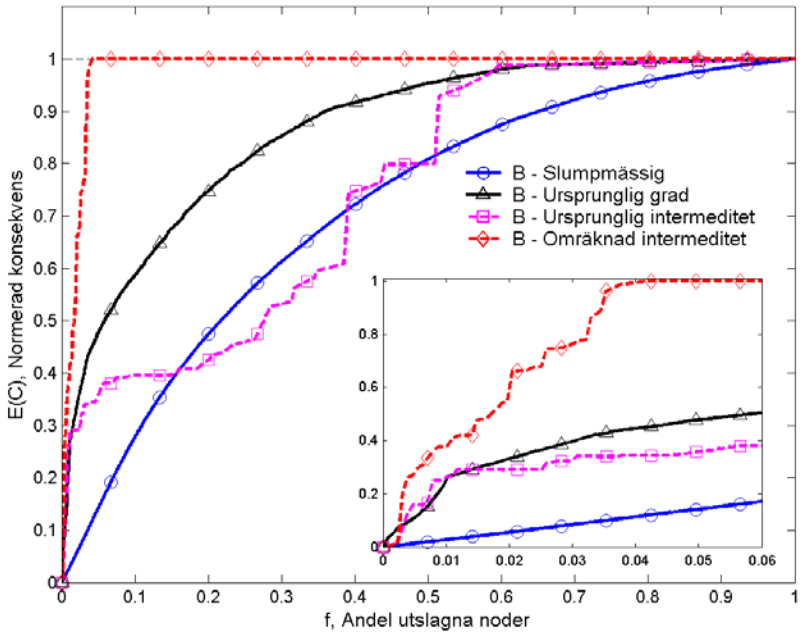
E(C) beräknades genom Monte Carlo-simulering. I simuleringarna antogs att källnoderna inte var utslagningsbara och resultaten baseras på medelvärden för 1000 simuleringar för slumpmässig utslagning och 100 simuleringar för övriga utslagningsstrategier. Här presenteras endast resultat för nodutslagning eftersom skillnaderna mellan nod- och länkutslagning var små.

5.2 Simuleringsresultat

I Figur 9 och Figur 10 presenteras simuleringsresultaten för system A respektive B. För båda systemen var uppdaterad intermeditet den mest skadliga utslagningsstrategin. Efter utslagning av ca 5 % (system A) och 4 % (system B) av noderna har samtliga abonnenter förlorat elförsörjningen. Att denna utslagningsstrategi är den mest skadliga är väntat eftersom den syftar till att slå mot de mest kritiska komponenter i nätet. Intressant, och något oväntat, är att utslagning av noder enligt påfrestningen som innebär att noder med hög ursprunglig källnodsintermeditet slås ut först endast är en något mer skadlig strategi än den slumpmässiga för system A och endast mer skadlig vid mindre påfrestningar (under 10% utslagna noder) för system B. Det finns dock en naturlig förklaring till detta, nämligen att efter hand som noder slås ut förändras nätverkstopologin. Det som ursprungligen var en kritisk nod är inte nödvändigtvis det då nätverkstopologin har förändrats, t.ex. efter att en nod ”uppströms” har blivit utslagen.



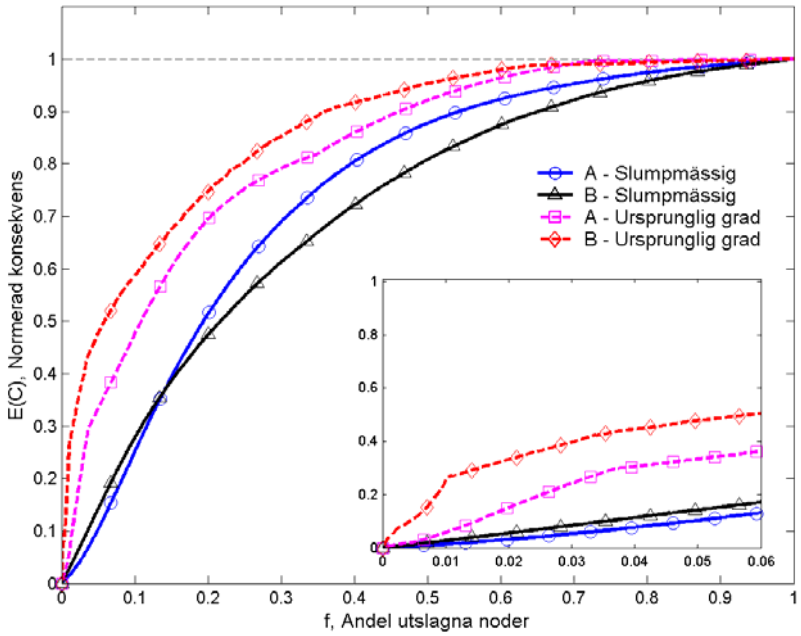
Figur 9 **Den normerade konsekvensen, E(C), för olika utslagningsstrategier som en funktion av fraktionen utslagna noder, f, för system A.**



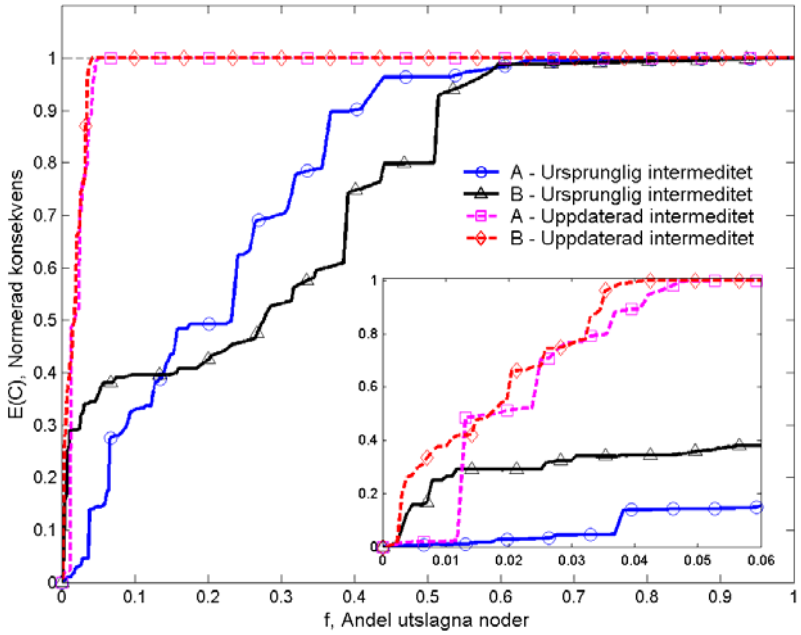
Figur 10 **Den normerade konsekvensen, E(C), för olika utslagningsstrategier som en funktion av fraktionen utslagna noder, f, för system B.**

En jämförelse mellan systemen (Figur 11 och Figur 12) visar att det inte generellt går att säga vilket av systemen som är mest robust, utan detta beror helt enkelt på typ av påfrestning, påfrestningens storlek, och till viss del även på hur robustheten mäts. Även om man bestämmer sig för att mäta ett systems robusthet genom att mäta den förväntade normerade konsekvensen, *E(C)*, kan man inte säga vilket system som är mest robust utan man måste i så fall specificera vilken storlek på påfrestningen (och typen) som man avser. När det gäller utslagning av noder med högst grad först är det tydligt att system B är mer sårbart, vilket både diagrammen och sårbarhetskoefficienten (se Tabell 7) visar. Resultaten från den slumpmässiga utslagningen leder dock till en något tvetydig slutsats kring sårbarheten. Det visar sig att system B är mer sårbart vid små påfrestningar (under ca. 10%) men mer robust vid större påfrestningar. Slutsatsen som kan dras är att det inte bara kan vara svårt att uttala sig generellt om sårbarheten i ett system utan även att det kan vara svårt att uttala sig generellt om sårbarheten för en specifik *typ* av påfrestning, vilket SVC-måttet gör. För att entydigt kunna uttala sig om sårbarheten måste påfrestningens storlek alltså specificeras, vilket exempelvis görs i den operationella definitionen av sårbarhet som beskrivs utförligt i rapporten ”Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv” [1] och i den metod för sårbarhetsanalys som beskrivs i kapitel 4. Samma fenomen uppstår när det gäller utslagning enligt ursprunglig källnodsintermeditet, d.v.s. att system B är mer sårbart för små påfrestningar men mer robust för stora (över ca 15%). När det gäller typen av påfrestning som kallas uppdaterad källnodsintermeditet är system A mer robust för alla storlekar av påfrestningen.

Designkoefficienten (DC) visar entydigt (för samtliga påfrestningar) att system B har en ”bättre” distribution av abonnenterna i nätverket, alternativ är bättre designat med abonnentdistributionen i åtanke. Tendensen för båda systemen är att noder med många abonnenter har en mer tillförlitlig elförsörjning än noder med färre abonnenter (eftersom samtliga DC-mått är positiva), men denna tendens är alltså starkare för system B.



Figur 11 **Jämförelse mellan system A och B för två utslagningsstrategier: slumpmässig utslagning av noder och utslagning av noder i fallande ordning av nodens grad.**



Figur 12 **Jämförelse mellan system A och B för två utslagningsstrategier: utslagning av noder i fallande ordning av ursprunglig och uppdaterad intermeditet presenteras.**

Tabell 7 **SVC och DC för olika strategier för utslagning av noder.**

Mått	Utslagningsstrategi	System A	System B	Jämförelse [a]
SVC	Slumpmässig	0.749	0.716	B
	Ursprunglig grad	0.830	0.868	A
	Ursprunglig intermeditet	0.792	0.750	B
	Uppdaterad intermeditet	0.979	0.983	A
DC	Slumpmässig	0.354	0.467	B
	Ursprunglig grad	0.274	0.279	B
	Ursprunglig intermeditet	0.315	0.469	B
	Uppdaterad intermeditet	0.231	0.451	B

[a] Bokstaven i kolumnen hänvisar till det system som har det bästa värdet (ur sårbarhetssynpunkt) på det aktuella måttet.

Analyser av den här typen ger mått på sårbarhet för olika typer av påfrestningar för tekniska system. Det är dock viktigt att ha i åtanke att måtten och analyserna inte ger någon förklaring till varför sårbarheten i olika system skiljer sig. En analys av orsaken till skillnader i sårbarhet, enligt de mått som använts här, är ett bra komplement till sårbarhetsanalysen.

6 Sammanfattande diskussion

I denna rapport har vi presenterat en metod för sårbarhetsanalys som kan användas på olika typer av tekniska system. Den metod som har föreslagits här utgår från en uppsättning befintliga metoder inom området. Dessa metoder har anpassats och vidareutvecklats mot bakgrund av den problembild man ställs inför då sårbarhetsanalyser ska utföras för storskaliga tekniska system. Vidare har metoden utvecklats för att passa in i den operationella definition av sårbarhet som föreslagits i rapporten ”Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv” [1].

För att kunna använda de metoder som föreslagits och beskrivits i denna rapport måste (åtminstone) följande villkor vara uppfyllda:

- Systemet måste vara möjligt att representera med ett nätverk som kan användas för att generera olika riskscenarier. Med hjälp av nätverksstrukturerna ska det alltså vara möjligt att uttala sig om hur väl systemet fungerar givet vissa betingelser, t.ex. hur väl systemet fungerar då tre kritiska noder är utslagna till följd av en påfrestning.

- Det måste vara möjligt att fastställa ett eller flera konsekvensmått som fångar in de dimensioner av konsekvenser som anses vara av intresse att studera, d.v.s. som stämmer överens med de värderingar som utgör grunden för analysen. Konsekvensmåtten måste även vara numeriska.

Genom att representera det tekniska system med en nätverksrepresentation reduceras en del av komplexiteten med systemen. Mycket av den underliggande fysiken abstraheras bort vid denna representation, t.ex. detaljer som har med det elektriska flödet i ett elsystem att göra. Det är dock möjligt att även ta hänsyn till den underliggande fysiken i varierande grad, exempelvis genom att ta hänsyn till laster på noder och länkar samt deras kapaciteter. Det finns heller inte något som hindrar att man kombinera en nätverksanalytisk ansats med en mer detaljerad modellering av de tekniska systemen. Givetvis ställer detta betydligt högre krav på indatan om de tekniska systemen samt den datorkraft och tid som krävs för att analysera riskscenarierna inom en rimlig tidsrymd. Oavsett vilken detaljeringsgrad som används måste den som använder metoderna vara medveten om att ett antal förenklingar måste göras med syftet att i någon mån kunna fånga in helheten.

Referenser

1. Johansson, H. och Jönsson, H. (2007), *Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv*, LUCRAM, Rapport 1010, Lunds universitet, Lund.
2. Newman, M. E. J. (2001), ”Scientific collaboration networks. II. Shortest paths, weighted networks, and centrality”, *Physical Review E*, **64:**016132.
3. Holme, P., Kim, B. J., Yoon, C. H. och Han S. K. (2002), “Attack vulnerability of complex networks”, *Physical Review E*, **65**:056109.
4. Albert, R., Jeong, H. och Barabási A.-L. (2000), “Error and attack tolerance of complex networks”, *Nature*, **406**(6794): 378-382.
5. Watts, D. J. och Strogatz, S. H. (1998), “Collective dynamics of 'small-world' networks”, *Nature*, **393**(6684): 440-442.
6. Barabási, A.-L. och Albert, R. (1999), “Emergence of Scaling in Random Networks, *Science*, **286**(5439): 509-512.
7. Crucitti, P., Latora, V., Marchiori, M. och Rapisarda, A. (2003), “Efficiency of scale-free networks: error and attack tolerance”, *Physica A*, **320**: 622-642.
8. Latora, V. och Marchiori, M. (2001) “Efficient Behaviour of Small-World Networks”, *Physical Review Letters*, **87**(19).
9. Albert, R., Albert, I. and Nakarado, G. L. (2004) “Structural vulnerability of the North American power grid, *Physical Review E*, **69**(025103(R)).
10. Holmgren, Å. (2006), “Using Graph Models to Analyze the Vulnerability of Electric Power Networks”, *Risk Analysis*, **26**(4): 955-969.
11. Motter, A. E. och Lai, Y.-C. (2002), “Cascade-based attacks on complex networks”, *Physical Review E*, **66**(065102).
12. Moreno, Y., Gómez, J. B., och Pacheco, A. F. (2002), “Instability of scale-free networks under node-breaking avalanches”, *Europhysics Letter*, **58**(4): 630-636.
13. Moreno, Y., Pastor-Satorras, R., Vázquez, A. och Vespignani, A. (2003), “Critical load and congestion instabilities in scale-free networks”, *Europhysics Letters*, **62**(2): 292-298.
14. Crucitti, P., Latora, V. och Marchiori, M. (2004), “Model for cascading failures in complex systems”, *Physical Review E*, **69**(4).
15. Holme, P. (2002), “Edge overload breakdown in evolving networks”, *Physical Review E*, **66**(036119).
16. Kinney, R., Crucitti, P., Albert, R. och Latora, V. (2005), “Modeling cascading failure in the North American power grid”, *The European Physical Journal B*, **46**(1): 101-107.
17. Little, R. (2002), “Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures”, *Journal of Urban Technology*, **9**(1): 109-123.
18. Little, R.G. (1999), “Educating the Infrastructure Professional: A New Curriculum for a New Discipline”, *Public Works Management and Policy*, **4**(2): 93-99.
19. Little, R.G. (2003), “Toward more robust infrastructure: observations on improving the resilience and reliability of critical systems”, *Proceedings of the 36th Annual Hawaii International Conference on System Sciences, Hawaii*.

20. Buckle, P. (1998), “Re-defining community and vulnerability in the context of emergency management”, *Australian Journal of Emergency Management*, **13**(4): 21-26.
21. Krisberedskapsmyndigheten (2006), *Samhällsviktigt! Ett första förslag till definition av samhällsviktig verksamhet ur ett krisberedskapsperspektiv*, Krisberedskapsmyndigheten, Stockholm.
22. Johansson, J., Jönsson, H., och Johansson, H. (2007), “Analysing the Vulnerability of Electric Distribution Systems: a Step Towards Incorporating the Societal Consequences of Disruptions”, *International Journal of Emergency Management*, **4**(1): 4-17.