Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv

Tehler, Henrik; Hassel, Henrik

2007

Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv

Henrik Johansson
Henrik Jönsson

LUCRAM
Lunds universitets centrum för riskanalys och riskhantering
Lunds universitet

Rapport 1010, Lund 2007

Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv

Henrik Johansson
Henrik Jönsson

Lund 2007

Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv

Henrik Johansson
Henrik Jönsson

Rapport 1010
ISSN: 1404-2983

Antal sidor: 110
Illustrationer: Om inte annat anges, författarna.

Sökord:
Riskanalys, sårbarhetsanalys, risk- och sårbarhetsanalys, definition av sårbarhet, beroenden, systemsyn, komplexa adaptiva system

Abstract:
An operational definition of vulnerability is proposed. The definition is used to describe and analyse different methods for risk and vulnerability analysis. Several problems related to analysing the vulnerability of a complex sociotechnical system to a specific perturbation are identified and discussed. Suggestions of how risk- and vulnerability analyses can be performed for such systems are presented.

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.brand.lth.se/english

SAMMANFATTNING

Risk- och sårbarhetsanalyser genomförs idag för olika typer av system, exempelvis kommuner, regioner och myndigheter, och det finns ett antal olika metoder som en sådan analys kan genomföras med. Ett syfte med den här rapporten är att presentera några av dessa metoder och göra en beskrivning av dem utifrån en och samma terminologi. För att göra detta är det nödvändigt att ha en operationell definition av vad risk är och vad sårbarhet är. En sådan definition finns när det gäller begreppet risk, men saknas när det gäller sårbarhet. I ett av de första kapitlen i rapporten presenteras därför en sådan definition för sårbarhet.

Definitionen bygger på en sedan tidigare föreslagen operationell definition av risk. Den största skillnaden mellan de båda begreppen risk och sårbarhet, såsom de används i rapporten, är att vid analys av risken i ett system är det underförstått att systemet befinner sig i ett tillstånd som betraktas som normalt och analysen genomförs med målet att ta reda på hur systemet kan avvika från det normala tillståndet, hur sannolikt det är och vad konsekvenserna i så fall blir. När det gäller ett systems sårbarhet måste det analyseras med utgångspunkt i någon typ av påfrestning och analysen är alltid betingad av att den aktuella påfrestningen har inträffat, d.v.s. systemet befinner sig inte i ett tillstånd som betraktas som normalt.

Den operationella definition av sårbarhet som presenteras i rapporten innebär att ett systems sårbarhet för en specifik påfrestning är svaret på tre frågor:

- Vad kan hända, givet en specifik påfrestning?
- Hur sannolikt är det, givet påfrestningen?
- Vad blir konsekvenserna?

I praktiken kommer det inte bara att finnas ett svar på de olika frågorna eftersom det är möjligt att en påfrestning kan ge upphov till olika händelseutvecklingar i det aktuella systemet. Varje svar som kan ges på den första frågan motsvarar en typ av händelseutveckling, eller riskscenario, och för varje sådant som identifieras i en sårbarhetsanalys skall också de övriga två frågorna besvaras. Denna samling svar utgör systemets sårbarhet för den aktuella påfrestningen.

Med utgångspunkt i de operationella definitionerna av risk och av sårbarhet presenteras sedan en beskrivning av ett antal metoder för risk- och sårbarhetsanalys som grovt kan delas in i typerna *scenariobaserade* och *systembaserade* metoder. Skillnaderna mellan typerna är att de scenariobaserade metoderna inte explicit utgår från en systemmodell när olika typer av riskscenarier analyseras. De systembaserade typerna av metoder utgår från att en sådan modell skapas och sedan används för att systematiskt analysera möjliga sätt som fel kan uppkomma i systemet.

De operationella definitionerna av risk och av sårbarhet samt beskrivningen av de olika metoderna för risk- och sårbarhetsanalys används sedan som utgångspunkt för att identifiera ett antal potentiella problem som kan uppkomma då risk- och sårbarhetsanalyser genomförs för komplexa sociotekniska system, exempelvis en kommun.

De viktigaste av dessa potentiella problem bedöms vara:

- Problem som kan inträffa på grund av att systemmodellen som används i analysen inte definierats.
- Problem som kan inträffa på grund av att osäkerhet när det gäller vilket/vilka riskscenarier som kommer att inträffa inte hanterats på ett adekvat sätt.
- Problem som har att göra med att vissa typer av händelseförlopp med negativa konsekvenser inte representeras av de riskscenarier som identifierats i analysen (täckningsgradsproblemet).
- Problem som har att göra med detaljeringsgraden i beskrivningen av olika riskscenarier.
- Problem som har att göra med sannolikhetsskattningar.
- Problem som har att göra med överensstämmelsen mellan systemmodellen och verkligheten.

Rapporten avslutas med tre förslag på hur sårbarhetsanalyser kan genomföras med utgångspunkt i den operationella definitionen av sårbarhet som föreslagits i rapporten:

- *Grov analys av olika typer av fel*, vilket innebär en analys där fokus ligger på att skapa en lämplig systemmodell och att systematiskt gå igenom de olika elementen i systemet för att undersöka vilka riskscenarier som kan inträffa om just det aktuella elementet inte skulle fungera normalt.
- *Kvalitativ analys av sårbarhet*, vilket innebär en analys där fokus ligger på att ta fram en uppsättning riskscenarier som utgör svaret på den första frågan i den operationella definitionen av sårbarhet (se ovan). Svaren på de två övriga frågorna behandlas kvalitativt.
- *Kvantitativ analys av sårbarhet,* vilket är samma sak som en kvalitativ analys av sårbarhet med skillnaden att sannolikheter och konsekvenser kvantifieras.

INNEHÅLLSFÖRTECKNING

1 Inledning

1.1 Bakgrund

Lunds universitets centrum för riskanalys och riskhantering (LUCRAM) har mellan 2004 och 2007 drivit ett projekt som heter FRIVA (Framwork Programme for Risk and Vulnerability Analysis) finansierat av Krisberedskapsmyndigheten. I den här rapporten presenteras delar av resultaten från den forskning som bedrivits inom delprojekt 2 (Metoder för risk- och sårbarhetsanalys) i FRIVA[1].

Det finns många olika metoder för risk- och sårbarhetsanalys där vissa av dem är av mycket specifik karaktär, d.v.s. de kan bara användas för att analysera mycket specifika system eller mycket specifika påfrestningar. Andra metoder är mer generella och kan anpassas för att användas på en rad olika system och typer av påfrestningar. En relevant fråga är om olika analysmetoder är likvärdiga, d.v.s. spelar det någon roll för resultatets användbarhet vilken metod som används i en risk- och sårbarhetsanalys? Detta är en mycket angelägen fråga att svara på eftersom vissa metoder tar förhållandevis lite resurser i anspråk medan andra kräver betydligt mer och om metoderna är likvärdiga är det slöseri med resurser att använda de mer krävande metoderna. Bakom denna till synes enkla fråga döljer sig ett antal intressanta frågeställningar som exempelvis ”Hur kan det avgöras om en analysmetod är lämplig eller ej?” och ”Vilka krav bör ställas på en metod som skall användas för ett specifikt syfte?”. Det finns ett behov att klargöra vad olika metoder för risk- och sårbarhetsanalyser *syftar till att göra*, samt att analysera metoderna med avseende på *hur väl de uppfyller syftena*. Utifrån en sådan kartläggning och analys av metoder för risk- och sårbarhetsanalys bör de frågor som formulerats ovan åtminstone delvis kunna besvaras.

För att kunna göra en beskrivning av olika metoder för risk- och sårbarhetsanalys och för att kunna göra utvärderingar av sådana metoder måste man ha *operationella definitioner* av vad risk och sårbarhet är. En operationell definition innebär i det här sammanhanget en definition som inkluderar en beskrivning av hur risken eller sårbarheten i ett system kan bestämmas. Om man inte har det blir det mycket svårt att avgöra hur användbar en specifik metod är för att analysera dessa begrepp. Befintliga definitioner av sårbarhet såsom ”...en oförmåga hos ett objekt, system, individ, befolkningsgrupp, m.m. att stå emot och hantera en specifik påfrestning som kan härledas till inre eller yttre faktorer.” [1] ger inte mycket vägledning för att bedöma om exempelvis resultatet av en sårbarhetsanalys ger en bra uppfattning om ett systems sårbarhet. När det gäller begreppet risk finns en operationell definition, som föreslagits av Kaplan och Garrick [2, 3], vilken ger god vägledning för att avgöra om resultatet av en riskanalys representerar risken i det aktuella systemet. En målsättning i den här rapporten är att utveckla den

[1] Mer information om FRIVA-projektet finns på LUCRAMs hemsida: http://www.friva.lucram.lu.se/.

definitionen så att den även kan användas för begreppet sårbarhet. Det skall dock noteras att definitionen av sårbarhet som citeras ovan stämmer överens med den som senare används i rapporten, skillnaden är dock att den definition som föreslås här är mer detaljerad och ger ett förfarande för hur sårbarhet skall beskrivas. Vidare bör det noteras att även om sårbarheten i en analys inte kvantifieras så kan idéerna som ligger till grund för definitionen vara nyttiga, exempelvis att sårbarheten i ett system beror av vilka riskscenarier som kan uppkomma om den specifika påfrestningen inträffar.

Traditionella riskanalysmetoder tillämpas normalt på system som är förhållandevis enkla att avgränsa, d.v.s. gränsen mellan vad som utgör ”systemet” och ”omgivningen” är tydlig. Ett exempel är en kemisk reaktortank och dess tillhörande utrustning. Vidare mäts de negativa konsekvenserna av en oönskad händelse vanligtvis i termer av systemets ”kapacitet”, exempelvis ”förlust av kylkapacitet”, eller genom något mått på hur systemet påverkar sin omgivning, exempelvis antal döda människor. Det vore fel att säga att det är enkelt att beskriva dessa konsekvenser som funktion av diverse olika påfrestningar som kan tänkas drabba systemet, men det finns i alla fall bra kunskap om de mekanismer som ger upphov till de oönskade konsekvenserna. Tillämpning av risk- och sårbarhetsanalyser på den typen av system är beprövad och använd för allt ifrån mycket begränsade system till omfattande sådana, exempelvis PSA-analyser för kärnkraftsreaktorer.

Tillämpningen av metoder för risk- och sårbarhetsanalys är ännu så länge relativt oprövad när det gäller system:

- som är svåra att avgränsa,
- som involverar ett stort antal människor vars reaktioner på diverse oönskade händelser är svåra att beskriva men som i hög grad påverkar systemet,
- där det råder oklarhet rörande vilka konsekvensmått som är lämpliga att använda, samt
- där en stor mängd beroenden mellan olika delar av systemet spelar stor roll för systemets beteende vid en påfrestning. Detta gäller åtminstone då exempelvis beroenden beaktas explicit.

Den här rapporten utgör ett steg i riktningen mot att kunna genomföra välgrundade och trovärdiga risk- och sårbarhetsanalyser för dessa typer av system. Frågan är om samma typ av metoder som kan användas för risk- och sårbarhetsanalys för mindre komplexa system även kan vara användbara för sådana med mycket hög grad av komplexitet. Är det möjligt att exempelvis hantera den stora mängden beroenden mellan olika aktörer, och mellan olika aktörer och tekniska system, med alla metoder? Dessa beroendens betydelse för ett systems sårbarhet har under senare tid blivit alltmer uppmärksammade, exempelvis i samband med stormen Gudrun, i olika forskningsrapporter [1, 4], i rapporter rörande IT och sårbarhet [5] samt i Krisberedskapsmyndighetens Hot- och riskrapporter [6, 7]. En viktig del av den här

rapporten handlar om de problem som uppkommer då system med ett stort antal beroenden och ett stort antal aktörer skall analyseras. Det finns ett behov av att klargöra vilka svårigheter som tillkommer då man i stället för att analysera förhållandevis ”enkla” tekniska system försöker använda risk- och sårbarhetsanalysmetoder för att analysera komplexa socioteknisk a system. Om dessa svårigheter kan identifieras och beskrivas kan de också användas som utgångspunkt för att göra de befintliga metoderna för risk- och sårbarhetsanalys mer lämpliga för analys av sådana system.

1.2 Perspektiv

Rapporten är skriven med ett ingenjörsmässigt perspektiv, vilket innebär att avsikten med materialet är att det skall vara tillämpbart för risk- och sårbarhetsanalys i praktiken. Rapporten syftar därmed inte till att *förklara* hur olika typer av system uppför sig vid en kris utan snarare till att föreslå en plattform utifrån vilken risk- och sårbarhetsanalyser kan genomföras. Detta innebär att de fenomen som kan uppstå i komplexa system i en kris och som diskuteras i rapporten, exempelvis självorganisation, berörs mycket kortfattat och ofta med enbart exempel som utgångspunkt.

Rapporten är också skriven ur ett systemperspektiv med utgångspunkt i en operationell definition av risk som presenterats av Kaplan och Garrick [2, 3]. Det finns andra perspektiv på risk och sårbarhet som skulle kunna ha använts som utgångspunkt, men författarna har bedömt att det aktuella perspektivet ger störst möjligheter att nå fram till lösningar på hur risk- och sårbarhetsanalyser skall kunna genomföras i praktiken.

1.3 Syften

Rapporten har ett antal syften, vilka kan beskrivas med följande punkter:

- Ett syfte med rapporten är att föreslå *en operationell definition* av sårbarhet, d.v.s. en definition som inkluderar ett förfarande (en operation) som kan användas för att avgöra hur sårbarheten i ett system kan bestämmas. Detta syfte behandlas i Kapitel 2.

- Ett annat syfte med rapporten är att presentera en *inventering av metoder för risk- och sårbarhetsanalys* samt att, med hjälp av den föreslagna definitionen av sårbarhet, analysera dessa metoder med avseende på bland annat vilka syften metoderna har, hur de uppnår syftena, samt hur användbara de är för att analysera sårbarhet. Detta syfte behandlas i Kapitel 3.

- Vidare syftar rapporten till att, med utgångspunkt i den föreslagna operationella definitionen av sårbarhet, presentera en analys av potentiella problem som kan uppkomma då en risk- och sårbarhetsanalys för ett

förhållandevis komplext socioteknisk system (exempelvis en kommun eller region) genomförs. Detta syfte behandlas i kapitel 3 och 4.

- Syftet är också att, med utgångspunkt i ovan nämnda analys, föreslå hur de svårigheter som identifierats kan hanteras i en risk- och sårbarhetsanalys. Detta syfte behandlas i kapitel 4.

1.4 Avgränsningar

Risk- och sårbarhetsanalyser kan genomföras med en mängd olika metoder och med en mängd olika syften. Sedan förordningen om åtgärder för fredstida krishantering och höjd beredskap (SFS 2002:472)[1] tillkom har en mängd risk- och sårbarhetsanalyser presenterats av olika myndigheter. Det har i en utvärdering av dessa kunnat konstateras att den metodik som används kan variera mellan olika myndigheter [8]. En målsättning med den här rapporten är att presentera en inventering av olika metoder för risk- och sårbarhetsanalys. Efter att arbetet med att identifiera olika metoder inletts framkom det att det finns ett antal svårigheter med att inventera metoder för risk- och sårbarhetsanalys. Det förefaller som om det finns en hel del metoder som inte finns publicerade av någon organisation eller i vetenskapliga tidskrifter. I rapporten har inte denna typ av metoder tagits med eftersom det är ett rimligt krav att det finns en skriftlig beskrivning av en metod som skall användas för risk- och sårbarhetsanalys. Publicerade metoder kan trots det vara svåra att finna. Exempelvis finns det metoder för risk- och sårbarhetsanalys som publiceras inom teknikområden, såsom telekommunikation och vattendistributionssystem. För att finna dessa måste en stor mängd olika forskningsområden sökas igenom, vilket tar mycket tid. På grund av dessa två problem är den inventering av metoder för risk- och sårbarhetsanalys som presenteras i rapporten inte fullständig. Ambitionen har snarare varit att försöka göra *klassificeringen* av metoder så fullständig som möjligt, d.v.s. arbetet har gått ut på att försöka hitta ett sätt att beskriva metoder på som passar alla olika metoder och samtidigt är tillräckligt detaljerad för att fånga upp väsentliga olikheter.

1.5 Fallstudier

Arbetet som rapporten är baserad på har bedrivits med hjälp av empiriskt material rörande sociala och tekniska system från tre kommuner: Stenungsund, Ljungby och Vellinge. Det arbete som bedrivits i dessa kommuner benämns fallstudier och många av de förslag på hur idéerna i rapporten skall tillämpas i praktiken kommer från författarnas arbete i dessa kommuner.

[1] Denna förordning är numera upphävd och istället är det förordningen om krisberedskap och höjd beredskap (SFS 2006:942) som reglerar myndigheters risk- och sårbarhetsanalyser. Liknande krav på risk- och sårbarhetsanalyser för kommuner finns i Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.

1.6 Målgrupp

Rapporten riktar sig till dem som har ett intresse av den praktiska tillämpningen av risk- och sårbarhetsanalys, men som även har ett intresse för de teoretiska utgångspunkterna för dessa typer av analyser. Vidare riktar den sig till personer som är intresserade av de problem (och möjligheter) som finns med att tillämpa risk- och sårbarhetsanalyser på komplexa sociotekniska system.

Personer som bara är intresserade av den praktiska tillämpningen av risk- och sårbarhetsanalyser och som vill ha förslag på hur sådana kan genomföras för komplexa sociotekniska system bör framförallt läsa avsnitt 4.3.

Rapporten är bitvis skriven med ett abstrakt språk och med många ekvationer. Detta gör att den kan upplevas som krånglig och inte speciellt praktiskt orienterad. Vår ambition har dock hela tiden varit att försöka exemplifiera de abstrakta resonemangen med konkreta exempel. Tyvärr finns det vissa delar som kräver ett stort inslag av abstrakta resonemang, exempelvis kapitel 2. I dessa fall har dock mycket energi lagts ner på att försöka förklara idéerna bakom resonemangen, vilket innebär att dessa delar kan fungera som en introduktion för läsare som inte tidigare är bekanta med exempelvis Kaplan och Garricks definition av risk (kapitel 2). Vi anser dock att man bör vara bekant med riskbegreppen sedan tidigare för att kunna tillgodogöra sig dessa avsnitt.

För den som är intresserad av en mer kompakt och enklare beskrivning av några av områdena som behandlas i rapporten hänvisas till de informationsblad som producerats inom FRIVA (se exempelvis FRIVA:s hemsida, www.friva.lucram.se).

1.7 Disposition av rapporten

Rapporten inleds i kapitel 2 med en presentation av de teoretiska utgångspunkterna för diskussionerna i rapporten. Här ges en beskrivning av Kaplan och Garricks definition av risk och här presenteras också ett förslag på en operationell definition av sårbarhet. Kapitlet beskriver också utgångspunkten för hur begreppet system uppfattas och vad som avses med scenarier, negativa konsekvenser mm.

I kapitel 3 presenteras en inventering av metoder för risk- och sårbarhetsanalys. Dessutom presenteras en analys av metoderna med avsikten att beskriva metodernas syfte, hur de uppfyller syftet, vilka förutsättningar som måste vara uppfyllda för att metoden skall kunna användas, och vilka begränsningar som finns vid användningen av resultatet från analysen.

Kapitel 4 behandlar beroenden mellan olika delar i ett system och hur man kan hantera sådana beroenden i risk- och sårbarhetsanalyser. Kapitlet behandlar också system i vilka det finns agenter (vanligtvis personer) som har förmåga att anpassa sig till sin omgivning och ett antal exempel ges på hur sociala system kan vara mycket viktiga för utvecklingen av en kris. Kapitlet avslutas med ett förslag på hur

en sårbarhetsanalys med fokus på beroenden mellan olika agenter och artefakter (vanligtvis resurser som agenter kan använda) kan genomföras.

Kapitel 5 innehåller slutsatser och diskussion.

1.8 Positionering av arbetet inom forskningen rörande krishantering

Det finns ett behov av att på något sätt beskriva olika typer av forskningsinsatser när det gäller området krishantering. En anledning till att göra det är att det kan ställas olika krav på forskning inom området beroende på vilken typ av forskningsinsats det rör sig om.

Ett förslag på hur man kan karaktärisera olika forskningsinsatser är att använda FEMA:s (Federal Emergency Management Agency) indelning av krishantering i fyra faser som utgångspunkt och låta dessa faser representera en dimension som beskriver vilken typ av forskning som bedrivs. En annan dimension som är intressant för beskrivningen är huruvida forskningen är deskriptiv eller preskriptiv/normativ. Den deskriptiva forskningen syftar till att beskriva olika fenomen i världen, att klassificera, att förklara, etc. Inom krishanteringsområdet kan forskning som syftar till att förstå exempelvis ledningsproblematik vid kriser betraktas som deskriptiv forskning. Den preskriptiva/normativa forskningen handlar om att lägga fram argument eller förslag på hur saker och ting bör eller skall genomföras i praktiken och på den typen av forskning kan man ställa lite annorlunda krav på än vad man kan göra på deskriptiv forskning. Motsvarande exempel till det som gavs ovan inom det preskriptiva/normativa området kan vara forskning som går ut på att föreslå hur ledning bör eller skall genomföras vid kriser.

Med utgångspunkt i dessa två dimensioner går det att klassificera forskning inom krishanteringsområdet i åtta klasser som motsvarar de åtta fälten i Tabell 1. I tabellen finns ett antal exempel på frågor som kan tänkas vara av intresse för de olika typerna av forskning.

Tabell 1 *Indelning av krishanteringsforskningen i åtta kategorier med tillhörande exempel på frågeställningar.*

		Krishanteringens faser			
		Förebyggande	**Förberedande**	**Akut avhjälpande**	**Återuppbyggande**
Typ av forskning	**Deskriptiv**	Hur bedrivs det förebyggande arbetet inom olika regioner?	Hur förbereder olika aktörer sig för kriser?	Vilka faktorer har betydelse för ”god ledning”?	Vad karaktäriserar en specifik insats för att återuppbygga ett krisdrabbat område?
	Normativ / Preskriptiv	Hur bör investeringar för att undvika kriser värderas?	Hur kan risk- och sårbarhetsanalyser användas vid förberedelser inför en kris?	Hur bör olika aktörer agera i en kris?	Hur bör återuppbyggnaden av krisdrabbade områden organiseras för att arbetet skall bli så effektivt som möjligt?

Det är möjligt att den föreslagna klassificeringen bör kompletteras med andra dimensioner, eller en mer detaljerad indelning av de nuvarande dimensionerna. I dess nuvarande form är den dock tillräcklig för att beskriva inom vilka områden som den aktuella rapporten bör placeras. Målsättningen har varit att rapporten skall placeras i de områdena som är nere till vänster i matrisen, d.v.s. rapporten har en normativ/preskriptiv karaktär, och dess huvudsakliga fokus ligger i den förebyggande och förberedande fasen. Visserligen finns det material i rapporten som kommer från den deskriptiva sidan i den akut avhjälpande fasen, men det materialet är inte särskilt tongivande i rapporten och det är heller inte rapporterat på det sätt man skulle kunna kräva om rapportens fokus hade varit deskriptivt.

2 Teoretiska utgångspunkter

Innan olika metoder för risk- och sårbarhetsanalys presenteras och analyseras är det nödvändigt att beskriva de teoretiska utgångspunkterna som används i rapporten. Med teoretiska utgångspunkter avses i det här sammanhanget hur begrepp såsom ”sårbarhet”, ”risk” och ”system” uppfattas och används. Materialet som ligger till grund för det här kapitlet kommer framförallt från den operationella definition av risk som presenterats av Kaplan och Garrick [2, 3] och som vidareutvecklats av Kaplan, Garrick och Haimes [9] samt från området systemvetenskap (se exempelvis Lars Ingelstams genomgång av området i [10]). Området systemvetenskap är stort och det är i huvudsak begrepp från områdena beslutsteori, cybernetik och komplexa adaptiva system som används.

2.1 System och systemavgränsningar

Utgångspunkten för den här rapporten är att det finns någon typ av *system* som det är intressant att göra en risk- och sårbarhetsanalys för. Begreppet system används för att beteckna en ”...samling element som hänger samman med varandra så att de bildar en ordnad helhet...”[3]. Definitionen säger inget om vad elementen i systemet är och inte heller något om vad en ”ordnad helhet” är. Eftersom storskaliga komplexa system kan modelleras på flera olika sätt, vilka samtliga kan vara acceptabla modeller av systemet (se exempelvis [11] s. 95), kan man inte definiera vad som utgör ett systems delar innan man vet vilken typ av system som skall analyseras. Detta bör i stället styras av de resurser som finns tillgängliga för analysen och dess målsättningar. Haimes ger ett antal exempel på indelningar av system:

> For example, an economic system may be decomposed into geographic regions or activity sectors. An electric power management system may be decomposed according to the various functions of the system (e.g., power generation units, energy storage units, transmission units, etc.) or along geographical/political boundaries. Another decomposition might be a timewise decomposition into planning periods. [11]

Analysmetoden Hierarkisk Holografisk Modellering (HHM) [11] som utvecklats av Haimes, och som kommer att behandlas senare i rapporten, fokuserar specifikt på det faktum att verkligheten kan modelleras på olika sätt genom att använda olika perspektiv i analysen.

Utgångspunkten i den här rapporten är att verkligheten kan beskrivas som ett system och att den beskrivningen, i en risk- och sårbarhetsanalys, beror på vad analysens syfte är och vilka värderingar som utgör grunden för analysen. Exempel på värderingar kan vara att ”antal döda personer” uppfattas som de enda negativa konsekvenserna av olyckor och kriser i ett system. Dessa värderingar kan vara en

[3] Hämtat från Nationalencyklopedin, www.ne.se, 2007-04-04, uppslagsord: ”system”.

persons, men de kan lika gärna vara en grupp eller en organisations. Anledningen till att det är viktigt att beakta analysens syfte och värderingarna som utgör grunden är att det påverkar vad som uppfattas som systemets avgränsningar (se nedan), vilka de viktiga elementen i systemet är och vad som är oönskade konsekvenser för systemet. Det är viktigt att skilja på det ”verkliga systemet” och det system som i analysen används för att representera verkligheten. Om inget annat anges avser begreppet system i fortsättningen det system som används för analys av verkligheten, d.v.s. modellen.

Beroende på analysens syfte, vilka värderingar som används som utgångspunkt och på hur mycket resurser som finns för en risk- och sårbarhetsanalys kommer elementen som används för att definiera systemet att kunna vara olika. Om exempelvis en kommun gör en risk- och sårbarhetsanalys rörande allvarliga stormar kan systemdefinitionen vara annorlunda jämfört med om ett företag gör en liknande analys för deras verksamhet. I kommunens analys kan *ett element* vara det aktuella företaget medan i företagets analys kan elementen exempelvis vara olika delar av företaget. Att definiera vad som är det aktuella systemet är mycket viktigt för en analys av risk och sårbarhet. Utan en tydlig systemavgränsning blir det svårt att genomföra en riskanalys och framförallt svårt att kommunicera resultatet med andra personer. Ofta kan systemavgränsningarna vara implicita, d.v.s. det är underförstått att analysen bara gäller exempelvis ett visst tekniskt system. Trots detta är det ändå lämpligt att konkretisera vad som avses med systemet eftersom risken annars ökar att olika personer uppfattar systemet, och därmed analysen, på olika sätt. Det inte självklart om en analys av ett tekniskt system, exempelvis ett vattendistributionssystem, inkluderar personalen som sköter driften eller inte. Det som i slutändan styr hur systemet definieras är framförallt vad som uppfattas som de möjliga negativa konsekvenserna för systemet. Om exempelvis de negativa konsekvenserna skall beskrivas i termer av antalet personer som omkommer och risk- och sårbarhetsanalysen gäller stormar i en kommun bör människorna i kommunen vara en del av systemet som analyseras. Förutom att definitionen av ett system innebär att ta ställning till vilka element som ingår i systemet innebär det också att ta ställning till hur detaljerat systemet skall beskrivas. Ofta kan verkligheten beskrivas med hierarkier där ett element i en viss systemmodell i sig själv kan beskrivas som ett system bestående av ett antal element. Exemplet med risk- och sårbarhetsanalysen för stormar ovan illustrerar detta. Där beskrivs företaget som ett element i ett system, men detta element kan i sin tur beskrivas som ett system bestående av ett antal element, exempelvis olika byggnader, anställda, o.s.v. Vilken detaljeringsnivå som används i en analys är något som måste bestämmas då systemet definieras. Diskussionen om systemdefinition återkommer efter att den teoretiska utgångspunkten för hur scenarier och konsekvenser förhåller sig till varandra har klargjorts.

För att beskriva att olika element i ett system kan förändras och befinna sig i olika tillstånd används *tillståndsvariabler*, t_1, t_2,..., t_n. Dessa variabler kan vara

numeriska, exempelvis hastigheten i km/h som en bil färdas med, men de kan också vara av annan typ, exempelvis kan en pumps tillstånd beskrivas som antingen ”på” eller ”av”. *Systemets tillstånd* beskrivs av samtliga tillståndsvariablers tillstånd och kan alltså ses som en vektor bestående av de n olika variablerna, $T = (t_1, t_2, ..., t_n)$. Inom cybernetik definieras ett system som en uppsättning tillståndsvariabler [12] (s. 40). I den definition av system som används i den här rapporten, d.v.s. att ett system är en uppsättning element som bildar en helhet, kan elementen beskrivas av ett antal tillståndsvariabler och därmed innebär definitionerna i praktiken samma sak.

När en risk- eller sårbarhetsanalys utförs är *systemavgränsningarna* något av det första som bör klargöras. Systemavgränsningar har i det här sammanhanget att göra med vad som omfattas av systemet och vad som inte gör det och därmed betraktas som systemets *omgivning*. Som påpekats ovan är det viktigt att skilja på det verkliga systemet och modellen av systemet. En modell av ett verkligt system kan konstrueras på i princip ett oändligt antal sätt eftersom:

> ”*...every material object contains no less than an infinity of variables and therefore of possible systems*.” [12], s. 39.

Detta har ett samband med definitionen av risk [9] där riskscenariorymden, S_A, betraktas som oupräknelig (detta diskuteras utförligare senare i rapporten). Det går alltså alltid att finna en mer detaljerad beskrivning av ett riskscenario eller ett system. Att etablera systemavgränsningar har att göra med hur modellen av systemet byggs upp och inte med några verkliga avgränsningar.

Systemavgränsningarna som används beror till stor del på syftet med den aktuella analysen, de resurser som finns tillgängliga och vad som definierats som oönskade konsekvenser. Om syftet exempelvis är att göra en riskanalys för en kommun med avseende på översvämningar och de oönskade konsekvenserna utgörs av antal människor som omkommer måste människorna på ett eller annat sätt vara en del av systemet. Om konsekvenserna även skall mätas i termer av vattenskadade byggnader måste givetvis även byggnaderna vara med i analysen. Att både byggnader och människor bör vara en del av systemet i det fallet är självklart med tanke på hur de oönskade konsekvenserna definierats. Det är däremot inte självklart hur resten av systemet skall definieras, utan detta styrs till stor del av vad analysen skall användas till samt vilka resurser som finns tillgängliga. Är analysen exempelvis tänkt att ligga till grund för beslut om hur mycket sandsäckar som skall finnas till hands i kommunen, eller är den tänkt att kunna användas för att utvärdera olika strategier för en räddningsinsats i händelse av en översvämning? En grov systemavgränsning skulle kunna bestå av tre element: Byggnader, Människor och Vattendrag i kommunen. Elementet Byggnader har en tillståndsvariabel som representerar antalet byggnader med vattenskador, elementet Människor har en tillståndsvariabel som representerar antalet omkomna människor och elementet Vattendrag i kommunen har en variabel som representerar vattenståndet i

kommunen. I arbetet med analysen måste de olika tillstånden som variablerna kan anta definieras, exempelvis vilka tillstånd som vattenståndet i kommunen kan anta.

2.2 Scenarier och risk

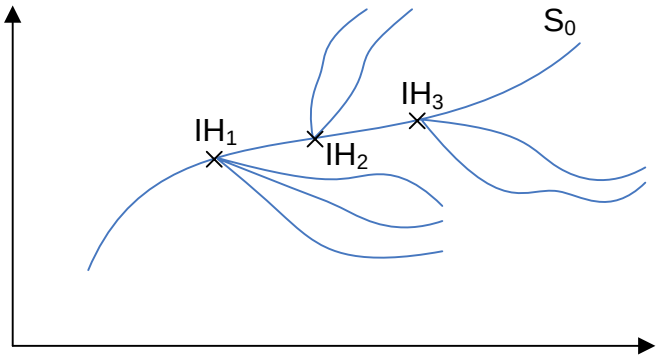
Risk- och sårbarhetsanalyser behandlar *möjliga* scenarier som *kan* inträffa i framtiden. Alla metoder för risk- och sårbarhetsanalys behandlar inte explicit scenarier, det är i stället underförstått att sådana kan inträffa. Scenarierna i en risk- och sårbarhetsanalys kan medföra negativa konsekvenser för det aktuella systemet. Vad som är en negativ konsekvens beror på vilket perspektiv som analysen har, eller vilka värderingar som används i analysen. En negativ konsekvens för en person/organisation behöver inte vara det för en annan person/organisation. Detta är en anledning till varför det är viktigt att redan från början i en risk- och sårbarhetsanalys klargöra vilka negativa konsekvenser som avses.

Ett *scenario* är en väg genom systemets tillståndsrymd (eng. state space), vilket betyder att ett scenario kan beskrivas som en vektor bestående av ett antal olika systemtillstånd som följer på varandra. I Kaplan och Garricks definition av risk [2, 3, 9] betecknas samtliga scenarier som kan inträffa i systemet för *scenariorymd* (eng. scenario space), *S*. För att tydliggöra att man i en risk- och sårbarhetsanalys är intresserad av scenarier som är oönskade används begreppet *riskscenario* och alla sådana scenarier kallas *riskscenariorymden* (eng. risk space), S_A. Ett enskilt scenario i S_A kallas för S_i och det är vanligt att man även identifierar det så kallade S_0-scenariot, vilket innebär att systemet uppför sig ”som planerat”. Ett riskscenario, S_i, består av ett visst antal systemtillstånd, T_j, som följer på varandra, $S_i = (T_1, T_2,..., T_k)$. I den ursprungliga kvantitativa definitionen av risk [2, 3] uppfattas antalet riskscenarier som utgör riskscenariorymden som en uppräknelig mängd och begreppet risk, *R*, definieras som den fullständiga uppsättningen scenarier S_i, deras sannolikhet eller frekvens L_i, samt deras konsekvenser X_i. Detta framgår i Ekvation 1, där *c* står för ”complete”, d.v.s. att uppsättningen riskscenarier skall vara ”fullständig”.

Ekvation 1

$$R = \{<S_i, L_i, X_i>\}_c$$

I Figur 1 illustreras S_0-scenariot och olika riskscenarier som kan uppkomma, vilket innebär att systemet avviker från det normala (S_0-scenariot). Det som inleder ett riskscenario kallas för initierande händelse (eng. initiating event) och kan exempelvis vara att en brand uppstår. Att analysera risk enligt definitionen ovan innebär att man försöker identifiera så många olika sätt som möjligt på vilka systemet kan avvika från S_0-scenariot och att man sedan beskriver de riskscenarier som kan uppkomma på grund av dessa avvikelser.



Figur 1 *Illustration av S_0-scenariot och olika initierande händelser (IH) som kan få systemet att avvika från det.*

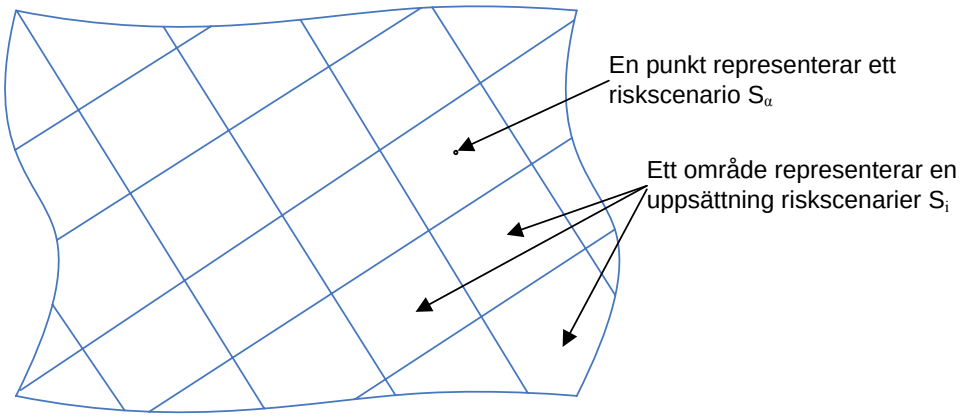
Den ursprungliga definitionen av risk har förfinats av Kaplan, Haimes och Garrick [9] och i den nya definitionen innehåller riskscenariorymden en oupräknelig mängd scenarier. Den gamla definitionen av risk kan illustreras med de rationella talen, vilka är uppräkneliga, medan den nya definitionen av risk kan illustreras med de reella talen, vilka utgör en oupräknelig mängd. Den nya definitionen av risk (Ekvation 2) innebär att risk definieras som en beskrivning av varje scenario, S_α, scenariots sannolikhet eller frekvens, L_α samt dess konsekvenser, X_α, för alla α som tillhör mängden A. Mängden A är oupräknelig och S_A representerar uppsättningen av alla riskscenarier.

Ekvation 2

$$R = \{<S_\alpha, L_\alpha, X_\alpha>\}, \alpha \in A$$

Förfiningen av riskdefinitionen innebär att varje scenario kan delas upp i mer detaljerade scenarier och alltså kan varje scenario S_i i den klassiska definitionen av risk representeras av en delmängd av scenarierna i S_A, eller en uppsättning riskscenarier. Exempel 1 och Figur 2 illustrerar detta.

> Exempel 1 - Uppdelning av scenarier
> Ett riskscenario som kan inträffa i en kommun är att en brand uppkommer i en byggnad någonstans i kommunen. Detta scenario kan delas upp i de två scenarierna ”En brand uppkommer i en byggnad som är en skola” och ”En brand uppkommer i en byggnad som inte är en skola”. Vidare kan scenariot med branden i en skola delas upp i ”En brand uppkommer i skola A” och ”En brand uppkommer i skola B”, o.s.v.



Figur 2 *Geometrisk representation av mängden A av alla riskscenarier S_α. (Från [9])*

I praktiken innebär den utvecklade definitionen av risk att en riskanalys bland annat går ut på att göra en uppdelning av mängden av alla riskscenarier S_A för ett specifikt system i ett antal delmängder S_i (det som i den ursprungliga riskdefinitionen kallades för riskscenarier). Enligt Kaplan m.fl. [9] skall uppsättningen delmängder S_i vara (1) *fullständiga* i bemärkelsen att $U(S_i) = S_A$, där $U(S_i)$ innebär unionen av mängderna S_i, (2) *uppräkneliga*, och (3) *disjunkta*, vilket innebär att $S_i \cap S_j = \emptyset$ för alla $i \neq j$, d.v.s. det får inte finnas något ”överlapp” mellan delmängderna S_i. Efter en specifik uppdelning av S_A definieras risken på samma sätt som i den ursprungliga definitionen, men med tillägget att risken beror på uppdelningen av S_A. Se Ekvation 3, där ”P” syftar på det engelska ordet ”partition”, eller delning. Risken, givet en specifik uppdelning av S_A , d.v.s. R_P, är resultatet av en riskanalys och är en approximation av R enligt Ekvation 2. Notera att S_i egentligen inte är ett riskscenario utan en uppsättning eller klass av riskscenarier, exempelvis ”En brand i en skolbyggnad” (se exempel 1 ovan). I fortsättningen av rapporten används dock begreppet *ett* riskscenario, men det är då underförstått att riskscenariot representerar ett antal mer detaljerat beskrivna riskscenarier, exempelvis ”Brand i en mellanstadieskola”, ”Brand i en högstadieskola”, etc.

Ekvation 3

$R_P = \{<S_i, L_i, X_i>\}_P$

Användningen av Ekvation 2 som definitionen av risk kan tyckas abstrakt och praktiskt svårhanterlig. I praktiken behöver man dock ofta inte bekymra sig om Ekvation 2, men den är viktig för resonemang rörande risk- och sårbarhetsanalyser i allmänhet och mer specifikt för att analysera *metoder* för risk- och sårbarhetsanalys. Den praktiska tillämpningen av idéerna som återges här kan vara problematisk, exempelvis när det gäller att skatta sannolikheter eller frekvenser för

händelser som aldrig tidigare inträffat, eller när det gäller risk- och sårbarhetsanalyser för system som är mycket komplexa och svåra att beskriva. Några av dessa problem belyses i kapitel 3.

Detaljrikedomen som kan användas när riskscenariorymden delas upp i ett antal riskscenarier beror på hur detaljerad modellen av systemet är. Som beskrevs ovan innehåller riskscenariorymden, S_A, en ouppräknelig mängd riskscenarier. Detta gäller dock bara det verkliga systemet, inte den *modell* av systemet som måste skapas i en riskanalys. Detaljrikedomen i modellen av det verkliga systemet påverkar hur detaljerad uppdelningen av riskscenariorymden kan göras, d.v.s. hur många riskscenarier som kan användas för att approximera den verkliga risken. Detaljrikedomen i modellen kan ökas på två sätt, dels genom att fler tillståndsvariabler läggs till modellen, exempelvis genom att utöka antalet element i modellen, dels genom att utöka antalet möjliga tillstånd som de befintliga tillståndsvariablerna kan anta.

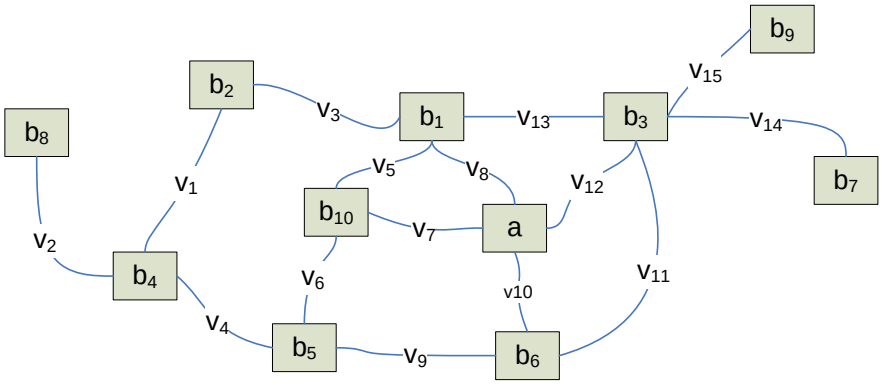
> *Exempel 2 - Analys av brandrisk i en fabrik*
> Antag att en riskanalys gällande bränder skall genomföras för en fabrik och att modellen som används för systemet består av *ett* element, fabriken och att detta element har *en* tillståndsvariabel. Tillståndsvariabeln beskriver fabriken som antingen ”normal”, ”rökskadad på grund av brand” eller ”förstörd av brand”, d.v.s. tillståndsvariabeln har tre tillstånd. Med den här grova modellen av systemet finns endast tre tillstånd för systemet som helhet, vilket medför att de scenarier som kan inträffa i *den verkliga fabriken* (ett oändligt antal) inte kan beskrivas speciellt utförligt med modellen. Om det antas att tillståndet ”rökskadad på grund av brand” alltid inträffar innan ”förstörd av brand” blir *riskscenarierna* som kan beskrivas med modellen två stycken, d.v.s. ett scenario där fabrikens tillstånd blir ”rökskadad på grund av brand” och ett scenario där först tillståndet ”rökskadad på grund av brand” inträffar och därefter inträffar tillståndet ”förstörd av brand”.
>
> Ett sätt att utöka detaljrikedomen i modellen är att dela upp elementet ”fabrik” i två nya element ”brandcell 1” och ”brandcell 2” och dessutom lägga till en tillståndsvariabel, för varje element, som beskriver om sprinklersystemet i brandcellerna fungerar som tänkt eller ej. Förutom detta läggs ytterligare ett element till i modellen, brandcellsgränsen mellan brandcell 1 och brandcell 2. Brandcellsgränsen har en tillståndsvariabel som beskriver dess förmåga att hindra en brand att sprida sig från en brandcell till den andra. Tillståndsvariabeln har tillstånden ”fungerar” och ”fungerar ej”. Med denna mer detaljerade modell av systemet är det möjligt att skapa betydligt fler riskscenarier, vilket betyder att indelningen av riskscenariorymden blir mer detaljerad (fler rutor i Figur 2). Det verkliga systemet är dock fortfarande oförändrat.

Detaljrikedomen i systemmodellen som används i exemplet ovan är förhållandevis grov. Nedan följer ett exempel med en något mer detaljerad systemmodell, vilken finns illustrerad i Figur 3.

Exempel 3 - Riskanalys för ett fiktivt samhälle
Ett exempel på ett system som skulle kunna vara intressant att göra en risk- och sårbarhetsanalys för är ett litet fiktivt samhälle som består av tio invånare (i_1 till i_{10}) som bor på olika geografiska platser och som kan röra sig mellan sina hem och sin arbetsplats (alla jobbar på samma ställe), a, genom att följa ett vägnät som består av ett antal vägsträckor (v_1 till v_{15}). Byggnaderna som invånarna bor i betecknas b_1 till b_{10}. I samhället finns två personer som, för enkelhetens skull, antas kunna genomföra räddningsinsatser av olika slag (släcka bränder, ge akut sjukvård, transportera personer, röja vägar o.s.v.). Personerna som har möjlighet att genomföra räddningsinsatser, r_1 och r_2, befinner sig vanligtvis på samma geografiska position som de övriga invånarnas arbetsplats, a.

I det system av personer (12 stycken), vägsträckor (15 stycken) och byggnader (11 stycken då räddningspersonalen antas vistas i samma byggnad som de övriga personerna arbetar i) som utgör modellen av samhället finns ett antal tillstånd för systemet som helhet. Ett tillstånd för systemet som helhet utgörs av *en* kombination av de olika tillståndsvariablerna i systemet. I det här exemplet finns det en tillståndsvariabel för varje person som förknippas med deras geografiska position. Variabeln kan vara i tillstånden v_1, v_2,...,v_{15}, b_1, b_2,...,b_{10} och a. Dessutom finns en variabel för varje person som beskriver personens fysiska tillstånd, variabeln kan ha tillstånden ”normal”, ”sjuk” och ”död”. Varje vägsträcka har en variabel som beskriver framkomligheten på just den sträckan, variabelns tillstånd är ”framkomlig” och ”ej framkomlig”. Förutom dessa variabler har byggnaderna i systemet en variabel som beskriver om personerna kan bo respektive arbeta i en byggnad, variabelns tillstånd är ”beboelig/möjligt att arbeta i” och ”obeboelig/omöjligt att arbeta i”.

I modellen av systemet som presenterats finns alltså 38 element/delar (byggnader, vägsträckor och personer) och 50 tillståndsvariabler. Figur 3 illustrerar byggnaderna och vägsträckorna, samt relationerna mellan dem, d.v.s. från vilka vägsträckor man kan nå vilka byggnader och tvärt om.



Figur 3 *Illustration av modellen som representerar det fiktiva samhället.*

Med hjälp av modellen över systemet är det möjligt att illustrera vad som menas med exempelvis en väg genom tillståndsrymden och riskscenariorymden, S_A. Tillståndsrymden för det aktuella systemet utgörs av alla möjliga kombinationer av tillståndsvariablerna och om det antas att alla kombinationer av dessa kan uppkomma (exempelvis att en person kan vara i en byggnad trots att den har tillståndet ”obeboelig / omöjligt att arbeta”) finns det ungefär 3,4 $*10^{30}$ olika tillstånd för systemet. Ett scenario i det aktuella exemplet är en väg genom denna tillståndsrymd. Antag exempelvis att systemets tillstånd beskrivs med en vektor där de olika positionerna i vektorn motsvarar tillståndsvariablerna. Ett scenario där personen i_9 blir sjuk, och får hjälp av personen r_1, men trots det omkommer skulle kunna beskrivas som följande väg genom tillståndsrymden där $r_{1,p}$ är tillståndsvariabeln som representerar positionen för person r_1, och $i_{9,f}$ är tillståndsvariabeln som representerar person i_9:s fysiska tillstånd och punkterna (...) innebär att alla andra tillståndsvariabler är i sina ursprungslägen (vägarna är framkomliga invånarna är i sina bostäder, o.s.v.): ($i_{1,f}$ = ”normal”, $r_{1,p}$ = ”a”,...), ($i_{1,f}$ = ”sjuk”, $r_{1,p}$ = ”a”,...), ($i_{1,f}$ = ”sjuk”, $r_{1,p}$ = ”v_{12}”,...), ($i_{1,f}$ = ”sjuk”, $r_{1,p}$ = ”b_3”,...), ($i_{1,f}$ = ”sjuk”, $r_{1,p}$ = ”v_{15}”,...), ($i_{1,f}$ = ” sjuk”, $r_{1,p}$ = ”b_9”,...), ($i_{1,f}$ = ”död”, $r_{1,p}$ = ”b_9”,...).

Beroende på vilka värderingar som är utgångspunkten för analysen (vem som är beslutsfattare) kommer riskscenariorymden att se annorlunda ut. Om exempelvis beslutsfattaren betraktar alla scenarier där någon av invånarna omkommer som ett oönskat scenario kommer samtliga scenarier som resulterar i omkomna invånare att ingå i S_A. En sådan uppsättning scenarier representeras av ett område i S_A.

En riskanalys innebär en uppdelning av riskscenariorymden i ett antal riskscenarier (delmängder) och i det aktuella exemplet kan denna uppdelning ske genom att alla riskscenarier där en invånare omkommer kallas S_1, alla riskscenarier där två invånare omkommer kallas S_2, o.s.v. En sådan uppdelning ger en lista med riskscenarier som, om man också skattar sannolikheten för dessa (L_1 till L_{12}), kan användas som en approximation av risken (se Ekvation 3):

S_1, L_1, 1 död
S_2, L_2, 2 döda
.
.
.
S_{12}, L_{12}, 12 döda

En lista liknande den som presenteras i exemplet ingår normalt i en kvantitativ riskanalys och enligt Kaplan och Garricks definitionen av risk representerar listan risken, eller en approximation av risken i systemet.

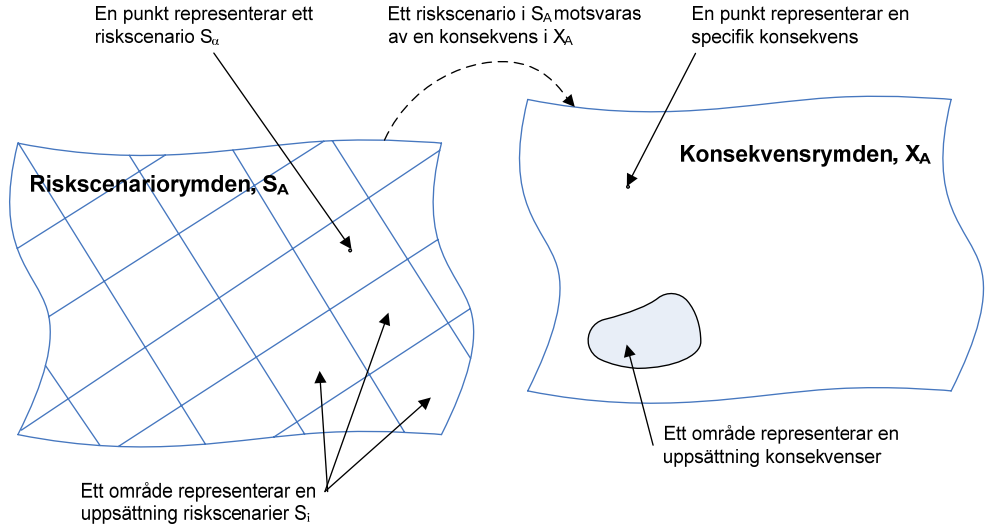
I exemplet ovan är modellen över det verkliga systemet troligtvis mer detaljerad än vad som skulle behövas för att komma fram till listan över riskscenarier, exempelvis förekommer inte vägarna i beskrivningen av scenarierna (S_1 till S_{12}) och inte heller förekommer de i konsekvensbeskrivningen. Modellen skulle dock kunna användas för en mer detaljerad approximation av risken, exempelvis genom att ta med riskscenarier som innebär att vissa vägar är oframkomliga samtidigt som någon/några behöver hjälp av personerna som kan genomföra räddningsinsatser. Vilka element och tillståndsvariabler som används för att beskriva det verkliga systemet har att göra med vilka systemavgränsningarna är. I en analys kan man välja att inte ta med vägarna i systemet, förutsatt att deras möjliga tillstånd inte är förknippade med de oönskade konsekvenserna som studeras.

Det är vanligt att en riskanalys genomförs med avseende på något specifikt hot, exempelvis brand, storm eller farligt gods-transporter, och i de fallen ”krymper” riskscenariorymden, d.v.s. det är bara de riskscenarier som faktiskt har en koppling till det aktuella hotet som skall ingå i analysen.

2.3 Konsekvenser

En viktig komponent i definitionen av risk är de negativa konsekvenserna för varje riskscenario, X_i (se Ekvation 3). Vad som betraktas som negativa konsekvenser för ett system beror på vems värderingar som används och vad som är syftet med riskanalysen. Det är därför lämpligt att i det första steget av en riskanalys bestäms vilka negativa konsekvenser som är av intresse.

I Ekvation 3 är X_i, d.v.s. konsekvensen på grund av riskscenario S_i, inte nödvändigtvis endimensionell utan kan bestå av i princip hur många dimensioner som helst. Det är dock vanligt att den består av en eller ett fåtal dimensioner, exempelvis antal döda personer eller kostnaderna på grund av riskscenarierna. De olika konsekvensdimensionerna kan också kallas för konsekvensattribut. På samma sätt som *riskscenariorymden* utgörs av samtliga riskscenarier som kan inträffa i systemet innehåller *konsekvensrymden*, X_A, samtliga konsekvenser som, på grund av riskscenarierna, kan uppkomma i systemet. Ett specifikt scenario i S_A motsvaras av en konsekvens i X_A. Ibland kan flera scenarier i S_A motsvaras av en konsekvens i X_A, exempelvis om den enda konsekvens som är av intresse är antalet omkomna personer och flera olika scenarier leder till samma antal omkomna personer. På grund av detta kan ett område i S_A motsvaras av antingen ett område eller en punkt i X_A, (se illustration i Figur 4).



Figur 4 *Illustration av Riskscenariorymden och Konsekvensrymden.*

När en beslutsfattare bestämmer vilka attribut eller dimensioner som skall användas för att beskriva konsekvenserna av riskscenarierna är det viktigt att dessa är mätbara, d.v.s. att varje riskscenario går att relatera till en konsekvens enligt de olika attributen/dimensionerna. För att testa om detta går kan man tänka sig en synsk person[4] som kan se in i möjliga framtider och därmed också kan observera alla riskscenarier. Om en sådan person kan observera scenarierna och därefter entydigt säga vad konsekvensen enligt det aktuella attributet blir för vart och ett av riskscenarierna är attributet mätbart, annars inte. Om attributet inte är mätbart måste attributet preciseras bättre. Ett exempel på ett icke mätbart attribut är ”antal sjuka personer”. Om en synsk person skall svara på frågan vilket värde attributet har för ett specifikt riskscenario får han eller hon problem eftersom antalet sjuka personer kan variera under scenariot. Bättre definierade attribut är ”maximalt antal sjuka (i en specifik sjukdom) vid samma tidpunkt inom en månad från riskscenariots början”, eller ”totalt antal insjuknade en månad efter riskscenariots början”.

När konsekvenserna av ett riskscenario är mätbara enligt de konsekvensattribut som beslutsfattaren anser representera de oönskade konsekvenserna för systemet har riskscenariot nått ett så kallat *sluttillstånd* (eng. end-state), se Figur 5. Det är inte nödvändigt att alla konsekvensattributen blir mätbara samtidigt i ett riskscenario. Om så är fallet når riskscenariot sitt sluttillstånd först då *samtliga* konsekvensattribut är mätbara.

[4] Normalt används exemplet med en synsk person när sannolikheter för olika händelser skall skattas. I det fallet kallas det ”the Clarity test” (se exempelvis Howard, R.A., Decision Analysis: Practice and Promise*, Management Science*, 1988, Vol. 34, No. 6, s. 679-695).

2.4 Sannolikheter

En viktig del av definitionen av risk är sannolikheterna eller frekvenserna för de olika riskscenarierna, L_i. I det aktuella sammanhanget betraktas sannolikheter och frekvenser som ”subjektiva” i enlighet med den Bayesianska traditionen (se exempelvis [13]). Detta innebär att en sannolikhet beror av de ”bevis” som finns tillgängliga rörande den händelse som sannolikheten skattas för. Om man exempelvis vill skatta sannolikheten för att ett specifikt lag vinner en fotbollsmatch kan skattningen baseras på information om lagens tidigare resultat, spelarnas dagsform, mm. Det är dock inte nödvändigt att lagen har mötts tidigare för att skattning enligt den Bayesianska traditionen ska kunna göras, vilket passar bra in i det aktuella sammanhanget eftersom många av de riskscenarier som är av intresse aldrig tidigare har inträffat. I det här avsnittet kommer sannolikheter inte att behandlas mer utförligt eftersom fokus i den här rapporten inte är på att kunna beräkna sannolikheten för olika riskscenarier utan snarare på hur man kan analysera olika risk- och sårbarhetsanalysmetoder samt på hur man kan ta hänsyn till beroenden mellan olika krishanteringsfunktioner när man bedömer risker och sårbarheter.

2.5 Sårbarhet

Den operationella definitionen av risk som används som utgångspunkt i den här rapporten är förhållandevis väl etablerad[5]. När det gäller sårbarhetsanalys och definitionen av sårbarhet råder inte samma förhållande (se [1] s. 16-18). En definition av sårbarhet som används i krishanteringslitteraturen innebär att sårbarhet ses som en relation mellan ett system och en riskkälla eller händelse [14, 15]. Sårbarhet skall enligt den definitionen alltså inte ses som någon egenskap som existerar oberoende av riskkällor utan måste alltid relateras till en sådan, d.v.s. en person, byggnad, samhälle, etc. måste vara sårbar för något. Dilley och Boudreau [14] identifierar tre fundamentala element för att definiera begreppet sårbarhet; händelser, mottaglighet (susceptibility) för händelserna och det slutliga resultatet (outcome). Dessa element kan relateras till den teoretiska utgångspunkt som används här. Händelser motsvaras i det här sammanhanget av inledningen på ett riskscenario (vilket diskuteras senare i detta kapitel), eller en uppsättning scenarier. Mottaglighet för händelserna har dels att göra med vilka negativa konsekvenser som beaktas för det aktuella systemet, dels med vad som händer i systemet efter den initierande händelsen. Den initierande händelsen i kombination med vad som händer i systemet efter den initierande händelsen definierar ett eller flera riskscenarier och vart och ett av dessa motsvaras av en punkt i konsekvensrymden, d.v.s. vart och ett av riskscenarierna resulterar i en konsekvens.

[5] När det gäller olika veteskapliga discipliner finns ingen gemensam definition. Områden såsom ekonomi, psykologi, sociologi, etc. använder olika definitioner. När det gäller att dimensionera diverse tekniska system eller analysera riskerna med en viss verksamhet, exempelvis transport av farligt gods, drift av kärnkraftsverk eller kemisk industri, finns dock en större likhet och den definition som presenteras här är den vanligast förekommande inom dessa områden.

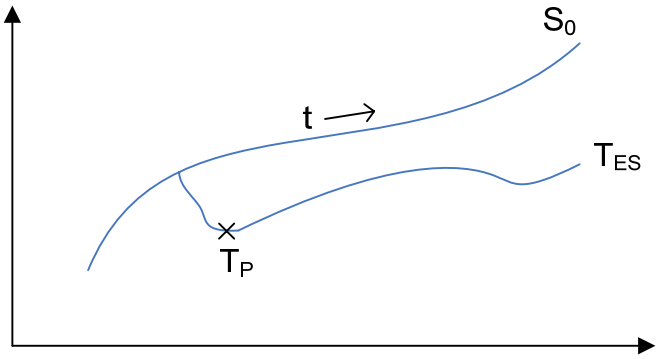
Det bör noteras att begreppet sårbarhet även kan syfta på *ett tillstånd* eller *ett förhållande* som gör att de negativa konsekvenserna i ett system blir stora om en specifik påfrestning inträffar:

> ”Vulnerability is the manifestation of the inherent states of the system (e.g., physical, technical, organizational, cultural) that can be exploited to adversely affect (cause harm or damage to) that system.” [16]

För att identifiera *en sårbarhet* är det rimligt att man utgår från någon typ av sårbarhetsanalys eller riskanalys. Ett exempel på detta är om en analys av en byggnads sårbarhet för bränder skall genomföras. I det fallet är det intressant att studera hur byggnaden kan motstå en brand och resultatet blir en analys av byggnadens *sårbarhet för brand*. Efter analysen av byggnadens sårbarhet för brand kan det konstateras att en orsak till att byggnaden är mycket sårbar för den påfrestningen är att det finns oskyddade stålpelare i byggnaden, vilka med stor sannolikhet kommer att vika sig om de blir påverkade av brand och innebära att taket rasar in. I det fallet utgör de oskyddade stålpelarna *en sårbarhet*. I fortsättningen av rapporten används begreppet sårbarhet då ett systems oförmåga att motstå en specifik påfrestning avses.

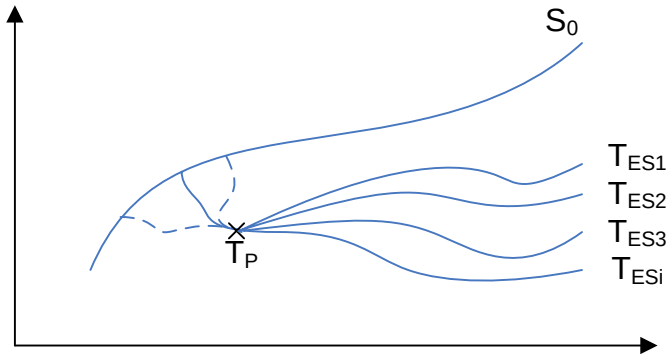
Med utgångspunkt i det teoretiska ramverk som presenterats i det här kapitlet kan faran eller hotet ses som orsaken till en uppsättning riskscenarier, S_α, enligt Ekvation 2. Att sådana riskscenarier existerar är underförstått eftersom om det inte fanns några skulle ”hotet” inte vara något hot för systemet. Att ett system är mer sårbart för ett specifikt hot indikerar att konsekvenserna om hotet skulle realiseras, d.v.s. ett riskscenario skulle inträffa, blir värre än om sårbarheten i systemet var mindre. Ett problem med denna formulering är att ett riskscenario syftar på systemets ”hela” väg genom tillståndsrymden, d.v.s. från det att systemet avviker från vad som är normalt tills dess att ett så kallat sluttillstånd inträffat. Detta innebär alltså att systemets sluttillstånd är definierat i riskscenariot och det kan då alltså inte bero på sårbarheten. Istället måste sårbarheten relateras till delen av ett riskscenario som inträffar innan sluttillståndet har nåtts, men efter det att hotet realiserats. På vägen från S_0 till ett sluttillstånd för systemet, T_{ES}, finns ett antal mellanliggande tillstånd (mid-states), T_{MS} [9]. Det är förhållandet mellan dessa mellanliggande tillstånd och sluttillstånden som säger något om systemets sårbarhet för just den aktuella *påfrestningen* som fick systemet att förflyttas till ett visst mellanliggande tillstånd. En *påfrestning* på systemet definieras alltså som en händelse som förflyttar systemets position i tillståndsrymden från en position inne i området som definieras som S_0 (kom ihåg att alla scenarier S_i egentligen är uppsättningar av scenarier, se avsnitt 2.2) till ett mellanliggande tillstånd. Det mellanliggande tillståndet som uppkommer som följd av den aktuella påfrestningen kallas T_P. Systemets sårbarhet för påfrestningen beror av konsekvenserna av det sluttillstånd, T_{ES}, som systemet når efter att ha befunnit sig i T_P. Sårbarare system

kommer att ge upphov till allvarligare negativa konsekvenser då systemet når sluttillståndet. Figur 5 illustrerar hur en påfrestning ser ut när den flyttar systemets tillstånd bort från den väg genom tillståndsrymden som definieras av S_0.



Figur 5 *Illustration av olika vägar genom systemets tillståndsrymd. En väg genom tillståndsrymden motsvarar ett scenario. Scenariot S_0 innebär att systemet uppför sig normalt, det scenarierna som avviker från S_0 är ett riskscenario. T_P är det tillstånd som systemet hamnar i när det utsatts för en specifik påfrestning och detta tillstånd är ett mellanliggande tillstånd på vägen mot ett sluttillstånd, T_{ES}.*

I praktiken är det ofta omöjligt att med säkerhet veta hur systemet kommer att utvecklas i tillståndsrymden efter att T_P har inträffat (jämför med diskussion om probabilistiska tillståndsförändringar i avsnitt 2.6) och på samma sätt som i definitionen av risk kan därför ett antal riskscenarier inträffa som kan leda till olika sluttillstånd, T_{ES1} till T_{ESi} i Figur 6. Det är även ofta så att flera händelser kan leda till samma påfrestning T_P, vilket illustreras med hjälp av de streckade linjerna i Figur 6.



Figur 6 *Illustration av påfrestningen, T_P, och ett antal möjligt sluttillstånd ES_1 till ES_i.*

Hur kan då ett systems sårbarhet definieras med hjälp av den terminologi som används här? Först och främst kan det konstateras att frågan måste preciseras för att kunna besvaras, eftersom ett systems sårbarhet måste ses i relation till någon typ av *påfrestning* som kan uppkomma på grund av någon typ av hot eller fara. Ett systems sårbarhet på grund av en viss påfrestning kan dock definieras. Om systemet antas vara *deterministiskt*, i bemärkelsen att en specifik påfrestning T_P bara kan ge upphov till *en* väg genom tillståndsrymden och därmed bara ett sluttillstånd (se Figur 5), bör systemets sårbarhet på grund av påfrestningen definieras genom att undersöka skillnaden i konsekvens för systemet mellan S_0 och det scenario som blir resultatet av störningen. Att jämföra två systems sårbarhet för en viss störning kan åstadkommas genom att jämföra de konsekvenser som blir resultatet av systemens väg genom tillståndsrymden på grund av störningen. Eftersom konsekvenserna av en väg genom tillståndsrymden kan beskrivas med fler än en dimension är jämförelser mellan olika kombinationer av konsekvensattribut inte alltid enkelt, men det går att göra exempelvis med multiattributmetoder från området beslutsteori (se exempelvis [17]).

Om systemet däremot inte är deterministiskt, vilket betyder att ett specifikt tillstånd på grund av en påfrestning, T_P, inte leder till ett unikt sluttillstånd för systemet utan kan leda till flera (se Figur 6), blir definitionen av sårbarhet något mer komplicerad. Det är dock denna situation som är mest praktiskt intressant eftersom det för de flesta verkliga system som är av intresse är praktiskt omöjligt att veta exakt hur systemet kommer att utvecklas på grund av en påfrestning och därför finns det alltså flera olika möjliga vägar genom tillståndsrymden. Eftersom det råder osäkerhet rörande systemets sluttillstånd efter påfrestningen kommer en definition liknande den som används för definition av risk (Ekvation 2) att användas.

Det är inte nödvändigtvis så att en påfrestning på ett system entydigt definierar systemtillståndet, utan påfrestningen kan ge upphov till en *uppsättning* systemtillstånd som alla stämmer överens med beskrivningen av påfrestningen. T_P bör därför uppfattas som en *mängd* systemtillstånd, men givetvis är det möjligt att denna mängd endast innehåller ett enda systemtillstånd och i så fall är innebörden av T_P samma som presenterats ovan. Ett exempel är någon typ av process som är beroende av två servrar, Server 1 och Server 2, för att fungera. En påfrestning på systemet kan vara ”en av servrarna slås ut” och den påfrestningen kan beskrivas med (åtminstone) två systemtillstånd där det ena innebär att Server 1 slås ut och det andra att Server 2 slås ut. I det fallet består alltså T_P av dessa två systemtillstånd. En annan påfrestning på systemet är ”Server 1 slås ut”. Denna påfrestning kan beskrivas med ett systemtillstånd, vilket också innebär att T_P bara innehåller det tillståndet.

Ett riskscenario definierades tidigare som en väg genom systemets tillståndsrymd. Ett specifikt systemtillstånd kan beskrivas som en kombination av de olika

tillståndsvariablerna, $T = (t_1, t_2,..., t_n)$ och *ett riskscenario* är en vektor av systemtillstånd från det första tillståndet T_1 till det sista, d.v.s. sluttillståndet T_{ES}, $S_i = (T_1, T_2,..., T_{ES})$. Det första systemtillståndet i riskscenario *i* betecknas $T_{1,i}$, det andra betecknas $T_{2,i}$, o.s.v. De riskscenarier som är intressanta för definitionen av sårbarhet är alla de scenarier som innehåller något av systemtillstånden i T_P, vilka kan uppstå på grund av den aktuella påfrestningen. Systemets sårbarhet för att förflyttas till något av systemtillstånden T_P kan uttryckas som V_P enligt Ekvation 4, där den enda förändringen jämfört med definitionen av risk (Ekvation 2) är villkoret att något av systemtillstånden i T_P är det första systemtillståndet i riskscenarierna som ingår i definitionen. Definitionen av sårbarhet är alltså samma som definitionen för risk med modifikationen att den är *betingad* av att systemet lämnat S_0 och hamnat i något av tillstånden T_P efter en påfrestning. Hur systemet hamnat i något av tillstånden T_P är ointressant. A i ekvationen är en ouppräknelig mängd.

Ekvation 4

$$V_P = \{<S_\alpha, L_\alpha, X_\alpha>\} : \alpha \in A, T_{1,\alpha} \in T_P$$

Definitionen av sårbarhet stämmer väl överens med uppfattningen att ”Sårbarhet kan således ses som en beskrivning av en relation mellan en specifik händelse, hot eller riskkälla och ett specifikt mottagligt system...” [1]. Det specifika hotet eller riskkällan motsvaras i Ekvation 4 av orsaken till påfrestningen på systemet som gör att systemet hamnar i tillståndet(en) T_P. Relationen mellan påfrestningen och systemet beskrivs sedan av den/de möjliga vägarna genom tillståndsrymden som systemet kan ta efter påfrestningen. Om det finns fler än en möjlig väg för systemet representeras detta av flera riskscenarier i Ekvation 4. Slutligen leder detta/dessa riskscenario(-er) fram till det så kallade sluttillståndet, då konsekvenserna för systemet på grund av påfrestningen kan beskrivas.

Precis som när det gäller den operationella definitionen av risk kan inte sårbarhetsdefinitionen uttryckas med ett enda värde utan att man gör en kraftig förenkling. Om man däremot vill ha ett enklare mått på sårbarhet kan man med hjälp av definitionen ovan komma fram till sådana, exempelvis genom att beräkna de förväntade konsekvenserna på grund av riskscenarierna.

När en sårbarhetsanalys görs i praktiken måste en uppdelning av riskscenariorymden göras, på samma sätt som då en riskanalys utförs. Eftersom man inte kan ha en oändlig mängd riskscenarier i sin analys använder man en uppdelning i olika riskscenarier som en *approximation* av sårbarheten i systemet, se ekvation 5, där index *i* indikerar att riskscenariorymden är uppdelad i ett uppräkneligt antal riskscenarier.

Ekvation 5

$$V_P \approx \{<S_i, L_i, X_i>\} : T_{1,i} \in T_P$$

När man gör en sårbarhetsanalys för ett system i praktiken är det viktigt att beskriva påfrestningen för vilken systemets sårbarhet skall utvärderas, d.v.s. beskriva det systemtillstånd som man utgår ifrån då möjliga scenarier beskrivs, T_P. Genom att först definiera sitt system och tillståndsvariablerna blir denna beskrivning lättare, se exempel 2 ovan. En sårbarhetsanalys handlar om att dela upp den betingade riskscenariorymden (betingad av att den aktuella påfrestningen inträffat) i ett lämpligt antal riskscenarier och bestämma sannolikhet och konsekvens för dessa. I praktiken fokuserar dock en sårbarhetsanalys vanligtvis inte så mycket på sannolikheterna för olika scenarier utan är mer inriktad på scenariobeskrivningar och konsekvensbeskrivningar.

Ett enklare sätt att beskriva definitionen är att ett systems sårbarhet för en specifik påfrestning är svaret på följande tre frågor:

- Vad kan hända, givet en specifik påfrestning?
- Hur sannolikt är det, givet påfrestningen?
- Vad blir konsekvenserna?

Den första frågan motsvarar S_i i ekvation 5, d.v.s. det är en beskrivning av ett eller flera riskscenarier. Den andra frågan motsvarar L_i i ekvationen, d.v.s. sannolikheten att ett specifikt riskscenario inträffar givet att påfrestningen har inträffat och den tredje frågan motsvarar X_i i ekvationen, d.v.s. konsekvenserna på grund av ett specifikt riskscenario.

I praktiken innebär definitionen att för att analysera ett systems sårbarhet för en specifik påfrestning måste först ett antal riskscenarier som kan uppkomma som en följd av påfrestningen beskrivas. Sedan måste, för vart och ett av scenarierna, sannolikheten att just det scenariot inträffar givet påfrestningen skattas. Slutligen skall konsekvenserna beskrivas för vart och ett av riskscenarierna. Denna uppsättning svar på frågorna utgör alltså systemets sårbarhet för den aktuella påfrestningen.

2.6 Tillståndsförändringar

Ett begrepp som kommer att användas senare i rapporten och som är viktigt när dynamiken i ett system studeras är *tillståndsförändring*. En tillståndsförändring är en beskrivning av hur systemet ändras från ett tillstånd till ett annat. Ett scenario, eller riskscenario är en uppsättning systemtillstånd som följer på varandra och mellan varje sådant tillstånd sker ofta en förändring, d.v.s. en tillståndsförändring. Detta innebär att ett scenario eller riskscenario kan betraktas som ett antal tillståndsförändringar. Tillståndsförändringar kan dels ses som ”regler” för hur ett system uppför sig, d.v.s. de talar om vilka tillstånd som följer efter att systemet befunnit sig i ett specifikt tillstånd, dels som beskrivningar av vad som sker i ett system.

För att beskriva skillnaden mellan tillståndsförändring och scenario används ett enkelt exempel. Antag att ett system består av en metallkula som hänger i en tråd och där systemtillståndet beskrivs av två variabler, kulans position, t_1 (1 betyder att kulan befinner sig en meter över marken, 0 betyder att den ligger på marken), och huruvida tråden är avklippt eller ej, t_2 (0 betyder att den inte är avklippt och 1 betyder att den är avklippt). Systemtillståndet kan då beskrivas med en vektor bestående av de två tillståndsvariablerna, (t_1, t_2). En tillståndsförändring beskriver hur systemet förändras givet att det befinner sig i ett specifikt tillstånd. Exempelvis är (1, 1)→(0, 1) en tillståndsförändring som innebär att om metallkulan befinner sig en meter ovan mark och tråden är avklippt kommer systemet att förflyttas till ett tillstånd som innebär att kulan befinner sig på marken och tråden är avklippt. Pilen mellan de två systemtillstånden illustrerar att det sker en förändring i systemet och är den symbol som används för att illustrera en tillståndsförändring. Den dynamik som precis beskrevs i systemet skulle också kunna beskrivas som ett scenario. Tillstånd 1 definieras som att metallkulan hänger i en tråd som är hel, T_1 = (1,0), tillstånd 2 definieras som att metallkulan befinner sig i luften men tråden är avklippt, T_2 = (1,1) och tillstånd 3 definieras som att metallkulan befinner sig på marken och tråden är avklippt, T_3 = (0,1). Ett scenario, S_1, kan då definieras som att de tre tillstånden följer på varandra, S_1 = (T_1, T_2, T_3). I detta scenario ingår tillståndsförändringen som diskuterades ovan då systemet förflyttas mellan T_2 och T_3. Ett scenario kan alltså innehålla flera olika tillståndsförändringar.

Tillståndsförändringar kan vara antingen *deterministiska* eller *probabilistiska*. Deterministiska tillståndsförändringar är sådana som illustrerats ovan, d.v.s. det råder ingen osäkerhet om vilket ett systems nästa tillstånd kommer att vara. Probabilistiska tillståndsförändringar innebär att det inte går att veta vilket av ett antal olika tillstånd som blir resultatet av att systemet befinner sig i ett specifikt tillstånd. För att illustrera detta kan man använda en tabell med sannolikheter för olika tillståndsförändringar (eng. matrix of transition probabilities) [12]. Ett exempel på en sådan visas i Tabell 2 där den övre raden representerar de tillstånd som systemet kan befinna sig i innan tillståndsförändringen (d.v.s. 1, 2 och 3). I den första kolumnen står de tillstånd som systemet kan befinna sig i efter tillståndsförändringen, vilka är samma som det kunde befinna sig i innan förändringen. Siffrorna i tabellen representerar hur sannolikt det är att systemet skall förflyttas från ett tillstånd till ett annat och av dessa framgår att systemet, förr eller senare, kommer att befinna sig i tillstånd 3. Anledningen är att om systemet väl kommit till det tillståndet är sannolikheten 1 att det även kommer att vara kvar där i fortsättningen.

Tabell 2 *Tabell med tillståndsförändringssannolikheter för att system med tre tillstånd (1,2 och 3).*

↓	**1**	**2**	**3**
1	0,5		
2	0,5	0,5	
3		0,5	1

En probabilistisk tillståndsförändring har stora likheter med ett händelseträd eftersom båda metoderna tillåter att systemets utveckling beskrivs med ett antal möjliga utvecklingar i stället för med en enda. Att använda sig av probabilistiska tillståndsförändringar kan vara ett sätt att minska tillståndsrymden för ett system. Detta kan ske genom att ta bort ett stort antal element och komplexa interaktioner i systemet och ersätta det med en probabilistisk tillståndsförändring. Ett exempel som illustrerar detta är om man vill beskriva en olycka med en gasolvagn som välter. Tanken skulle i det här fallet kunna beskrivas med en stor mängd tillståndsvariabler som har att göra med materialet i olika punkter i tanken och den påfrestning som exempelvis ett vasst föremål som tränger in i tanken medför. Det skulle förmodligen bli mycket resurskrävande att gå igenom alla möjliga riskscenarier där tanken utsätts för en påfrestning och beräkna om ett hål uppstår och i så fall hur stort det blir. I stället för att göra detta kan man ersätta alla dessa tillståndsvariabler med en tillståndsvariabel som indikerar storleken på hålet i tanken och exempelvis anta att hålet kan ha tre storlekar. Om det blir ett hål, och i så fall vilken storlek hålet har, bestäms sedan av en probabilistisk tillståndsförändring där det finns en viss sannolikhet att hålet får en viss storlek givet att tanken utsätts för påfrestning (detta är ett vanligt tillvägagångssätt i riskanalyser för farligt gods-transporter). Den förenkling som görs när alla de tillståndsvariabler som annars skulle ha behövts för att beräkna hålstorleken reduceras bort kan endast genomföras om den nya tillståndsförändringen representerar verkligheten på ett korrekt sätt och om detaljeringsgraden i systemet är tillräckligt för att utsagor om konsekvenserna av de olika riskscenarierna kan göras. Huruvida tillståndsförändringen representerar verkligheten på ett korrekt sätt har att göra med om fördelningen av hålstorlekarna i olika tankar som blivit påfrestade på samma sätt som motsvaras av den aktuella påfrestningen i systemet överensstämmer med de sannolikheter som antagits i modellen.

En avgörande faktor för om risk- och sårbarhetsanalyser för stora komplexa system ska kunna utföras är om sådana förenklingar av systemet är möjliga att finna, som gör att det går att ersätta en stor mängd tillståndsvariabler med ett fåtal probabilistiska tillståndsförändringar.

3 Metoder för risk- och sårbarhetsanalys

En metod är ett ”planmässigt tillvägagångssätt för att uppnå visst resultat”[6] och i det här sammanhanget är en metod för risk- och sårbarhetsanalys ett tillvägagångssätt som ger en beskrivning av risken eller sårbarheten i någon typ av system. Det finns många metoder för att göra risk- och sårbarhetsanalyser och ett av syftena med detta kapitel är att, med hjälp av de teoretiska utgångspunkter som diskuterades i föregående kapitel, presentera ett sätt att beskriva och analysera sådana metoder. Ytterligare ett syfte med kapitlet är att presentera en kartläggning av olika metoder för risk- och sårbarhetsanalys samt en analys av dessa. Det sista syftet med kapitlet är att göra en värdering av hur lämpliga metoderna är för analys av olika typer av system och för att uppfylla olika syften[7].

Notera att sårbarhetsanalys i det här sammanhanget används för att beteckna en analys av ett systems egenskap, d.v.s. systemets oförmåga att hantera en specifik påfrestning. Begreppet används inte för att avse en identifiering av *sårbarheter i systemet* (se diskussion i avsnitt 2.5). Det förefaller rimligt att om en identifiering av ett systems sårbarheter skall genomföras måste den bygga på, alternativt genomföras samtidigt som, en analys av systemets sårbarhet.

För att här betrakta ett tillvägagångssätt som en metod krävs det att:

1) det måste finnas *dokumenterat och publicerat*;
2) det måste framgå vilket *resultat* som tillvägagångssättet genererar;
3) det måste framgå vad *syftet* med tillvägagångssättet är;
4) det måste framgå *vad som krävs* (exempelvis information, resurser, etc.) för att använda tillvägagångssättet och för vilken typ av system det är tillämpbart.

Det första kravet, att tillvägagångssättet är dokumenterat och publicerat, är nödvändigt av tillgänglighets- och transparensskäl.

Det andra kravet har att göra med att kunna avgöra vad som de som skapat metoden anser vara dess resultat. Anledningen till att detta är viktigt i det aktuella sammanhanget är att om man vill analysera hur bra en metod för risk- och sårbarhetsanalys är för ett visst ändamål, måste man veta vad som *utges* för att vara

[6] Hämtat från Nationalencyklopedin, www.ne.se, 2007-04-04, uppslagsord: ”metod”.

[7] I kapitlet behandlas både metoder för *riskanalys* och metoder för *sårbarhetsanalys*. Eftersom den teoretiska skillnaden mellan en riskanalys och en sårbarhetsanalys inte är särskilt stor (se föregående kapitel) och att det ibland kan vara svårt att veta om en metod är en riskanalysmetod eller sårbarhetsanalysmetod (beroende på användningen av metoden kan den vara bådadera) används begreppet *risk- och sårbarhetsanalys* i det här avsnittet då båda typerna avses.

metodens resultat. Därefter kan man utvärdera hur väl tillämpningen av metoden faktiskt kan generera det önskade resultatet. Detta är också skälet till det tredje kravet, d.v.s. att det måste framgå vilket syfte metoden har. För vissa metoder framgår det ganska klart vad deras resultat är, men det kan vara mindre klart vad resultatet kan användas till. Att resultatets användbarhet skall framgå har att göra med möjligheten att bedöma lämpligheten i att använda en specifik metod för ett specifikt syfte.

Det sista kravet är formulerat på så sätt att det skall vara möjligt att bedöma inom vilka områden som en specifik metod är tillämpbar. Vissa metoder har ett ganska smalt tillämpningsområde och detta måste man vara medveten om då man utvärderar dessa. Det är också en fördel för analysarbetet om man har kännedom om vad som krävs för att använda metoden.

Trots att punkterna ovan formulerats som krav betraktas även tillvägagångssätt som bara uppfyller några av kraven som en metod för risk- och sårbarhetsanalys, i dessa fall görs en *tolkning* av exempelvis syftet med metoden.

3.1 Karaktärisering av metoder

Analysen av metoderna för risk- och sårbarhetsanalys utförs genom att undersöka ett antal attribut som belyser de mest betydande likheterna och skillnaderna mellan metoderna.

3.1.1 Syfte

En viktig aspekt som kan användas för att karaktärisera och utvärdera metoder för risk- och sårbarhetsanalys är vilka syften som de kan användas till. En metod för risk- och sårbarhetsanalys kan vara bra att använda för att uppnå ett syfte, men dålig då den används för att uppnå ett annat. Det är exempelvis stor skillnad på om en metod används med syftet att ”bara” producera en beskrivning av ett eller några stycken riskscenarier eller om den används som underlag för att prioritera hur resurser för risk- och sårbarhetsreduktion skall fördelas.

Ofta framgår inte syftet med att använda en metod av själva metodbeskrivningen, en sådan beskrivning är vanligare att finna då man studerar en faktisk analys som genomförts med någon metod. Det kan därför vara svårt att avgöra vad syftet med att använda en specifik metod är. Om inte syftet med användning av metoden framgår görs i rapporten en tolkning av olika möjliga syften och en diskussion förs rörande vilka syften som den aktuella metoden är lämplig för.

3.1.2 Resultat

Metoder för risk- och sårbarhetsanalys kan kategoriseras med avseende på det resultat som de åstadkommer. Resultatet är det som uppkommer då en viss metod används, eller ”produkten” som genereras då man använder en viss metod. Vilket resultat som åstadkoms då man använder en metod för risk- och sårbarhetsanalys är

troligtvis det mest väsentliga för att kunna avgöra om en viss metod är lämplig att använda eller ej. Ett exempel på resultat är en uppräkning av ett antal riskscenarier, deras konsekvenser och sannolikhet, d.v.s. det som ingår i den operationella definitionen av risk som används här (se kapitel 2). Ett annat resultat av att göra en risk- och sårbarhetsanalys för en viss organisation är att man genom det ökar personalens medvetenhet rörande risk- och sårbarhetsfrågor och detta kan leda till bättre riskreducerande arbete. Problemet med den typen av resultat är dock att det är mycket svårt att visa att resultatet faktiskt uppkommit då man använt metoden.

3.1.3 Beskrivning av systemet

Ett attribut som kan användas för att karaktärisera olika metoder för risk- och sårbarhetsanalys är hur noggrant systemet som riskanalysen eller sårbarhetsanalysen fokuserar på beskrivs. I föregående kapitel finns flera avsnitt som handlar om systemsyn i risk- och sårbarhetsanalyssammanhang. Där presenteras ett sätt att betrakta verkligheten med hjälp av en indelning i tillståndsvariabler och element. En fullständig beskrivning av systemet är med detta synsätt en beskrivning av alla ingående element och tillståndsvariabler samt en beskrivning av *hela* tillståndsrymden. I det här sammanhanget är det mycket viktigt att komma ihåg att varje beskrivning av verkligheten som ett system är subjektiv eftersom verkligheten kan beskrivas på ett i princip oändligt antal sätt (se diskussion i föregående kapitel). Vad som avses med huruvida hela tillståndsrymden är beskriven har att göra med om det i den *modell* av verkligheten som den aktuella analysmetoden använder sig av framgår vilka samtliga tillstånd som systemet kan anta är (notera återigen att ”systemet” avser den modell av verkligheten som används i analysmetoden).

Ett exempel som illustrerar olika detaljeringsgrad avseende beskrivningen av systemet är skillnaden mellan ”traditionella” riskanalysmetoder som FMEA (Failure Modes and Effects Analysis), Hazop (Hazard and Operability) samt händelseträdsanalys, och scenariobaserade seminarieövningar (exempelvis MVA-metoden). Med scenariobaserade seminarieövningar avses en analys där en grupp människor som har kunskap om ett visst område samlas för att analysera ett fåtal riskscenarier som kan tänkas uppkomma i systemet. I en traditionell riskanalys, enligt de metoder som räknats upp, identifieras samtliga komponenter i systemet och deras möjliga tillstånd beskrivs också (exempelvis som ”fungerar” eller ”fungerar ej”, men det förekommer också större variationer). En scenariobaserad seminarieövning resulterar visserligen i en ofta mycket noggrann genomgång av en del av riskscenariorymden genom att man successivt behandlar olika händelser som följer på varandra i det område som man är intresserad av, exempelvis konsekvenserna av en storm i en kommun. En skillnad mellan de båda angreppssätten är dock att man i den scenariobaserade seminarieövningen vanligtvis inte explicit beskriver hur man uppfattar systemet och framförallt inte går igenom samtliga tillstånd som systemet kan ha. Denna skillnad i angreppssätt

beskrivs nedan då termerna *systembaserat* och *scenariobaserat* angreppssätt introduceras.

3.1.4 Hantering av riskscenariorymden

Ett annat attribut som kännetecknar metoder för risk- och sårbarhetsanalys är deras *hantering av riskscenariorymden*. Riskscenariorymden är det begrepp som används för samtliga riskscenarier som kan uppkomma i det aktuella systemet (se föregående kapitel). När det gäller begreppet ”hantering” avses i det här sammanhanget framförallt fyra aspekter:

- Hur avgränsad är riskscenariorymden?
- Sker en fullständig uppdelning av riskscenariorymden?
- Hur detaljerad är uppdelningen av riskscenariorymden?
- Är uppdelningen av riskscenariorymden disjunkt?

Den första aspekten har att göra med hur stor variation i riskscenarier som ”täcks in” i analysen. Exempelvis har en metod som specifikt behandlar brandrisker en snävare avgränsning av riskscenariorymden är en metod som behandlar brand- och explosionsrisker. Ibland kan det vara en fördel att ha en snävt avgränsad riskscenariorymd eftersom det ger möjlighet att behandla de ingående riskscenarierna mer i detalj, men det finns även problem som kräver en vidare avgränsning av riskscenariorymden för att kunna analyseras på ett adekvat sätt. I många fall har man inte möjlighet att bedöma hur avgränsad riskscenariorymden är för en specifik *metod*, utan det har snarare att göra med hur metoden används.

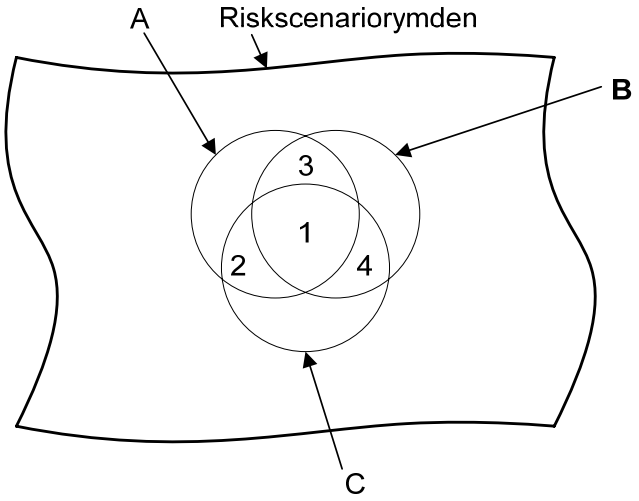
En fullständig uppdelning av riskscenariorymden har att göra med om metoden ”täcker in” alla möjliga scenarier som kan inträffa givet avgränsningarna av riskscenariorymden. Ett exempel på när en metod inte gör en fullständig uppdelning av riskscenariorymden är en metod som gör anspråk på att kunna användas för analys av bränder i en byggnad och där det vid användningen av metoden finns brandscenarier som inte beskrivs av de riskscenarier som identifieras. Om byggnaden exempelvis innehåller två lokaler och samtliga riskscenarier som identifierats innebär att en brand inträffar i den ena lokalen finns det brandscenarier som inte täcks in av alla riskscenarier, d.v.s. bränder som börjar i den andra lokalen. Ett enkelt sätt att gardera sig mot att man har täckt in hela riskscenariorymden är att ha med ett scenario som är ”övriga bränder”. Att ha med detta riskscenario innebär dock inte att detaljrikedomen i riskscenariot räcker för att uppfylla syftet med analysen, vilket är den aspekt som diskuteras härnäst. Innan den diskussionen är det dock lämpligt att notera att ibland är det inte metoden för risk- och sårbarhetsanalys *i sig* som medför en mer eller mindre fullständig uppdelning av riskscenariorymden utan det har att göra med den faktiska tillämpningen av metoden.

Hur detaljerad uppdelningen av riskscenariorymden är har att göra med antalet riskscenarier som ingår i risk- och sårbarhetsanalysen, fler riskscenarier ger en mer detaljerad uppdelning. I samband med att man analyserar detaljeringsgraden bör man också undersöka om den aktuella metoden ger upphov till olika detaljrikedom i olika delar av riskscenariorymden. Om man noterar en sådan olikhet avseende detaljrikedomen bör man reflektera över vad det får för effekter på analysens resultat. Det är dock inte nödvändigt att olika detaljrikedom i olika delar av riskscenariorymden är något negativt utan det kan vara helt naturligt att det blir så. Exempelvis kan det, i en analys av brandriskerna i en byggnad, vara klokt att ta med ett stort antal brandscenarier som börjar i eller i anslutning till lokaler där många människor förväntas vistas. Brandscenarier som börjar i delar av byggnaden där det inte vistas så många människor och där möjligheten för en brand att sprida sig är små behöver i så fall inte beskrivas med en stor mängd riskscenarier, utan det kan räcka med ett eller ett fåtal. Anledningen till varför det är lämpligt att göra en mer detaljerad analys i de områden av byggnaden där fler människor kan drabbas av branden är att en uppdelning av riskscenarier där kan ge en mer nyanserad bild av konsekvenserna av en brand än vad en uppdelning av riskscenarier där bränder uppstår i delar av byggnaden med låg persontäthet ger. Resonemanget bygger på att konsekvenser mäts i termer av hur många människor som utsätts för brandgaser under ett brandscenario. Om en uppdelning av riskscenariot ”brand i den obefolkade delen av byggnaden” delas upp i två nya riskscenarier: ”brand i bensin i den obefolkade delen” och ”brand i övriga bränslen i den obefolkade delen” så kommer (förmodligen) inte konsekvenserna att skilja så mycket mellan dessa två riskscenarier (troligen kommer antalet personer som påverkas av brandgaser i riskscenarierna att vara litet i båda scenarierna). En uppdelning av ett riskscenario i den del av byggnaden där en stor mängd personer befinner sig kan dock ge upphov till flera riskscenarier som skiljer sig markant när det gäller konsekvenserna på grund av riskscenarierna och i det fallet är det mer motiverat med en uppdelning av riskscenariorymden.

Den sista punkten ”Är uppdelningen av riskscenariorymden disjunkt?” innebär att man undersöker om olika riskscenarier ”överlappar” varandra. Överlapp mellan riskscenarier innebär att scenarierna inte är ömsesidigt uteslutande, d.v.s. de kan inträffa samtidigt. Om man vill använda en risk- och sårbarhetsanalys till exempelvis förmågebedömning eller prioritering av risk- och sårbarhets-reducerande åtgärder så måste man vara medveten om att ett antal svårigheter uppstår om så är fallet. Ett exempel är en risk- och sårbarhetsanalys där man identifierat de två riskscenarierna ”allvarlig storm i kommunen” och ”storbrand i samlingslokal med många döda”. Dessa riskscenarier är inte disjunkta, d.v.s. det kan inträffa en storbrand i en samlingslokal med många döda *samtidigt* som en allvarlig storm drabbar kommunen. Om de två riskscenarierna inträffar samtidigt kan konsekvenserna av det ”nya” riskscenariot mycket väl bli värre än summan av de två riskscenarierna som beskrivits tidigare, d.v.s. man har underskattat risken. En annan fara som leder till precis motsatt resultat, d.v.s. en överskattning av

risken är om man i en analys har identifierat ett antal riskscenarier som i princip är samma riskscenario. Ett, något överdrivet, exempel är följande situation. Antag att man i en analys av sårbarheten för en allvarlig storm i en kommun identifierat tre riskscenarier (A, B och C) som kan inträffa vid en sådan storm: A) Stormen slår ut elnätet och orsakar översvämningar i ett antal källare, B) Stormen slår ut elnätet och några personer omkommer på grund av nedfallande träd, C) Stormen slår ut elnätet och järnvägarna i kommunen blir oframkomliga. Dessa tre riskscenarier är inte disjunkta eftersom det är möjligt att ett riskscenario där elnätet slås ut, järnvägarna blockeras, några personer omkommer på grund av nedfallande träd och det uppstår översvämningar i ett antal källare mycket väl kan inträffa. Faran i den här situationen är att man med utgångspunkt i sårbarhetsanalysen kan få uppfattningen att sannolikheten att elnätet slås ut givet att kommunen drabbas av en allvarlig storm är större än den faktiskt är. Anledningen till detta är att händelsen att elnätet slås ut förekommer i alla tre riskscenarier.

Mer allvarliga fel kan inträffa om man gör en riskanalys på ovanstående sätt och på något vis skattar frekvensen eller sannolikheten för riskscenarierna. Om man med utgångspunkt i en sådan analys sedan vill beräkna exempelvis den förväntade konsekvensen på grund av stormar, sannolikheten att konsekvenserna blir större än ett specifikt värde, etc. riskerar man att överskatta risken. Eftersom riskscenarierna inte är disjunkta blir dessa värden för höga. Detta kan man illustrera med en bild som visar riskscenariorymden i Figur 7. I bilden finns de tre icke disjunkta riskscenarier illustrerade som cirklar i riskscenariorymden (A, B och C). Ytan inom cirkeln A representerar alla riskscenarier som kan beskrivas som ”Stormen slår ut elnätet och orsakar översvämningar i ett antal källare”, och på samma sätt representerar ytorna inom cirklarna B och C scenarierna som kan beskrivas med hjälp av de övriga scenarierna. De ytor där det står siffror representerar olika kombinationer av de tre riskscenarierna som beskrivits ovan, exempelvis representerar yta 1 riskscenarier där en storm inträffar som slår ut elnätet och där några personer omkommen på grund av nedfallande träd och där järnvägarna i kommunen blir oframkomliga. Felet man kan göra om man slår ihop sannolikheten eller frekvensen för riskscenario A, B och C är att då har man överskattat sannolikheten för vissa riskscenarier. Genom att tänka sig frekvensen av de olika riskscenarierna som ytorna innanför de respektive områden kan man förstå varför det blir fel. Om man summerar ytorna för A, B och C så kommer den sammanlagda ytan att bli större än området som täcks in av de tre cirklarna (på grund av att det finns överlapp mellan dem).



Figur 7 Illustration av riskscenariorymden och ett antal olika riskscenarier.

Vissa metoder för risk- och sårbarhetsanalys är konstruerade just för att undvika problem med disjunkta riskscenarier (exempelvis händelseträd) medan andra är konstruerade på så vis att disjunkta riskscenarier kan uppkomma (exempelvis Hierakisk Holografisk Modellering). Då metoderna analyseras kommer denna aspekt att vara viktig för att dela in metoderna i olika typer.

3.1.5 Beskrivning av konsekvenser

Metoderna hanterar beskrivningarna av konsekvenserna på grund av olika riskscenarier olika. En del ger ingen vägledning rörande vad som skall ingå i konsekvensbeskrivningen, medan andra ger betydligt mer vägledning. En annan aspekt som bör diskuteras i samband med konsekvensbeskrivning är om metoden i fråga ger vägledning när det gäller avvägningar mellan olika konsekvenstyper, eller om den kan användas för att på annat sätt rangordna olika riskscenarier utefter hur allvarliga de är.

3.1.6 Hantering av osäkerhet i analysen

Hur metoderna hanterar osäkerhet är en annan viktig aspekt som skiljer metoderna för risk- och sårbarhetsanalys. Med ”hantering” av osäkerhet avses hur hänsyn tas till att framtiden, och därmed vilka riskscenarier som faktiskt inträffar, är osäker. Vissa metoder hanterar detta genom att använda numeriska sannolikhetsskattningar för de olika riskscenarierna, medan andra använder sig av en klassificering av sannolikheten för olika riskscenarier i grupper (exempelvis ”trolig” och ”icke trolig”).

Man kan ibland få uppfattningen när det gäller sårbarhetsanalyser att osäkerheter (läs sannolikheter) är irrelevanta. Detta är dock felaktigt. Det som är irrelevant i en sårbarhetsanalys är *sannolikheten eller frekvensen att den påfrestning som man vill*

analysera uppkommer. Detta innebär *inte* att man kan bortse från att det råder osäkerhet rörande vilket riskscenario som kommer att inträffa *givet* att påfrestningen har inträffat. Oavsett om metoden som analyseras är en riskanalysmetod eller en sårbarhetsanalysmetod så måste osäkerheter hanteras.

3.1.7 Simulering av riskscenarier

Simulering innebär ”… att representera ett system med ett annat i avsikt att studera dess dynamiska uppförande…”[8] och i det här fallet innebär simulering att en modell av verkligheten används för att studera ett systems dynamiska uppförande antingen då systemet lämnar eller är på väg att lämna det så kallade S_0-scenariot (se kapitel 2), eller då systemet utsätts för en specifik påfrestning.

Skillnaden mellan metoder för risk- och sårbarhetsanalys som använder sig av simulering för att analysera riskscenarier och de som inte gör det är att metoderna i den första gruppen använder sig av regler för hur systemet beter sig (tillståndsförändringar) och sedan kan man med hjälp av dessa regler (och vanligtvis en dator) förutsäga hur systemet kommer att uppföra sig, givet att systemet befinner sig i ett visst tillstånd. När metoder från den andra gruppen används, d.v.s. de som inte använder sig av simulering, genereras de olika riskscenarierna inte genom att explicit utgå ifrån ett antal regler för systemets uppförande. Dessa metoder genererar i stället riskscenarierna genom att exempelvis använda experter för att bedöma systemets utveckling givet att det befinner sig i ett visst tillstånd.

Gränsen mellan när en metod för risk- och sårbarhetsanalys använder simulering eller ej är vag. Det går att hävda att även metoder som förmodligen inte skulle betraktas som simuleringsmetoder, exempelvis scenariobaserade seminarie-övningar, i viss mån utnyttjar sig av simulering. Under en seminarieövning då en grupp människor med kunskap om ett visst system försöker resonera sig fram till hur systemet kommer att uppföra sig givet en viss påfrestning kan gruppmedlemmarna använda sig av ”simulering” för att dra slutsatser om riskscenariots fortsatta utveckling. Vad som avses är att de personer som har kunskap om systemet känner till de ”regler” som gäller för hur systemet uppför sig och därmed kan dra slutsatser rörande systemets framtida tillstånd givet ett visst utgångstillstånd. Vanligtvis är dock inte dessa regler explicit uttryckta, vilket är en skillnad jämfört med de mer traditionella simuleringsmetoderna.

Förutom att simuleringsmodeller kan användas för att generera information om vilka riskscenarier som kan inträffa kan vissa av dem också användas för att ta fram information rörande sannolikheten för olika riskscenarier.

[8] Hämtat från Nationalencyklopedin, www.ne.se, 2007-04-04, uppslagsord: ”simulering”.

3.1.8 Överensstämmelse mellan analysen och verkligheten

Även om den metod som används för en risk- och sårbarhetsanalys är den mest lämpade för uppgiften kan själva analysen utföras på ett sätt som gör att dess användning blir mycket begränsad. Något som påverkar detta i hög grad är hur stor överensstämmelsen är mellan verkligheten och den modell (system) som man använder sig av i analysen. Detta är visserligen något som mer handlar om hur bra en specifik analys är och inte hur bra metoden i sig är, men det finns ändå skäl att ta upp det här eftersom valet av metod kan påverka möjligheterna att skapa en modell som stämmer väl överens med verkligheten.

Det finns åtminstone fyra olika förhållanden mellan en risk- och sårbarhetsanalys och verkligheten som är relevanta för att bedöma användbarheten av en analys. Förhållandena finns beskrivna som frågor i Tabell 3 och där framgår också vilken del av risk- och sårbarhetsanalysen som måste förändras om svaret på någon av frågorna är nej.

Tabell 3 Förhållanden mellan systemet och verkligheten som avgör hur väl analysen stämmer överens med verkligheten.

Förhållande mellan systemet och verkligheten	**Del av risk- och sårbarhetsanalysen som ger svaret på frågan**
Kan samtliga konsekvenser som identifierats som viktiga beskrivas med systemet?	Systemet
Kan samtliga relevanta riskscenarier beskrivas med systemet?	Systemet
Finns samtliga relevanta riskscenarier med i riskscenariorymden?	Riskscenariorymden
Beskriver riskscenarierna verkligheten på ett korrekt sätt?	Riskscenariorymden / Systemet

Den första frågan är ”Kan samtliga konsekvenser som identifieras som viktiga beskrivas med systemet?” och har att göra med detaljrikedomen i systembeskrivningen. För att man skall kunna analysera olika riskscenarier med avseende på en viss konsekvens måste konsekvensen kunna gå att beskriva med systemmodellen. Om exempelvis ”Antalet omkomna människor på grund av en pandemi” är den konsekvens som man är intresserad av måste man i den systemmodell som används kunna få fram information om antalet människor som omkommit på grund av pandemin. Antingen får man informationen genom att ha en tillståndsvariabel som motsvarar konsekvensen eller så får man den genom ett antal tillståndsvariabler. Om det inte går att få fram informationen måste systemmodellen justeras så att det går.

Nästa fråga är ”Kan samtliga relevanta riskscenarier beskrivas med systemet?” och den har att göra med om systemmodellen är tillräckligt detaljerad för att beskriva de riskscenarier som man vill att modellen skall kunna beskriva. Vilka riskscenarier som bör kunna beskrivas har att göra med vad man vill använda

analysen till. Antag att det är intressant att göra en riskanalys för ett system som består av en pump, ett kärl och en ventil. De negativa konsekvenser som man är intresserad av att beakta i analysen är överfyllning av kärlet, vilket innebär att vätska läcker ut från (det öppna) kärlet. För att göra en adekvat systembeskrivning behöver man alltså en (eller flera) tillståndsvariabler som beskriver fenomenet ”vätska rinner över kanten på kärlet”. I det här fallet räcker det med att definiera en tillståndsvariabel som motsvarar vätskenivån i kärlet. Om vätskenivån är högre än kanten på kärlet uppträder konsekvensen som är av intresse, annars inte. Systemet med en tillståndsvariabel räcker i det här fallet för att beskriva den konsekvens som man är intresserad av, d.v.s. om vätskan rinner över kanten eller ej, men den är inte tillräcklig för analys av vad det är som kan leda fram till att vätskenivån blir så hög att läckage uppstår. För att göra det behövs ett mer detaljerat system. Detta kan man beskriva med andra ord genom att använda begreppet *tillståndsförändring* (se sid 32 i referens [12]). En tillståndsförändring innebär att man beskriver vad som händer i systemet givet att systemet befinner sig i ett visst tillstånd.

När det gäller systemet med kärlet, pumpen och ventilen kan man inte med hjälp av tillståndsvariabeln som motsvarar vätskenivån i tanken beskriva orsakerna till att vätskenivån blir för hög. Detta innebär att man inte kan beskriva en tillståndsförändring som resulterar i det tillstånd som motsvarar den konsekvens som man är intresserad av. Exempelvis kan tillståndsvariabeln som motsvarar vätskenivån kallas $t_{nivå}$ och den kan anta tillstånden $t_{nivå} = 0$, vilket innebär att vätskenivån är lägre eller lika med kärlets kant, och $t_{nivå} = 1$, vilket innebär att vätskenivån är högre än kärlets kant. Det går då att beskriva en tillståndsförändring som leder till den konsekvens som är av intresse som: $t_{nivå} = 0 \rightarrow t_{nivå} = 1$. Denna tillståndsförändring är dock felaktig eftersom det ganska lätt genom att observera verkligheten (eller helt enkelt tänka efter hur verkligheten fungerar) går att konstatera att om vätskenivån i kärlet är lägre än kärlets kant så leder inte detta automatiskt till att vätskenivån blir högre än kärlets kant, alltså saknas något för att kunna beskriva tillståndsförändringen som leder till konsekvensen $t_{nivå} = 1$. I det här fallet är alltså systembeskrivningen inte adekvat för den aktuella tillämpningen. Det går dock att utveckla systembeskrivningen så att den blir det genom att lägga till två tillståndsvariabel som heter t_{pump} och t_{ventil}. t_{pump} har värdet 1 om pumpen är igång och värdet 0 om pumpen inte är igång. t_{ventil} har värdet 1 om ventilen är öppen och värdet 0 om den är stängd. Med hjälp av denna nya uppsättning tillståndsvariabler går det att beskriva tillståndsförändringen som leder till det tillstånd som motsvarar den aktuella konsekvensen, nämligen ($t_{pump} = 1$, $t_{ventil} = 0$, $t_{nivå} = 0$) $\rightarrow$ ($t_{pump} = 1$, $t_{ventil} = 0$, $t_{nivå} = 1$). Notera att systemet skulle kunna ha beskrivits mycket mer detaljerat, exempelvis genom att ange systemtillståndet vid olika tidpunkter och beskriva mängden vätska som strömmar ut ur karet som en funktion av vätskenivån, pumpens kapacitet, etc. I det aktuella fallet behövs dock inte den noggrannheten eftersom systemet med de tre tillståndsparametrarna kan beskriva det (de) tillstånd som motsvarar de konsekvenser som är av intresse och det går att beskriva den tillståndsförändring som leder till de (dessa) tillstånd med

hjälp av tillståndsvariablerna. Vidare överensstämmer tillståndsförändringen som presenterats ovan med verkligheten eftersom om pumpen är på och ventilen stängd så kommer (förr eller senare) vätskenivån i karet att bli högre än karets kant. Det är även möjligt att det finns andra tillståndsförändringar som leder till de aktuella konsekvenserna, exempelvis om pumpen är på och ventilen är öppen (om utflödet ut karet inte räcker för att kompensera för den mängd vätska som pumpen pumpar in). Om det är så att systemet (modellen) inte kan beskriva vissa riskscenarier som anses vara relevanta är *systemet otillräckligt*. Även om systemet inte är otillräckligt kan riskscenariorymden vara otillräcklig, vilket förklaras närmare nedan.

En fråga som är relaterad till den föregående är ”Finns samtliga relevanta riskscenarier med i riskscenariorymden?”. Denna fråga är i princip samma som den föregående, men där den föregående handlade om huruvida *det går* att beskriva de relevanta riskscenarierna med systemet handlar denna fråga om huruvida dessa riskscenarier faktiskt *finns med i* riskscenariorymden. Om de inte finns med är *riskscenariorymden otillräcklig* och bör utvecklas så att riskscenarierna kommer med.

Den sista frågan är förmodligen den svåraste att svara på och den har att göra med hur väl de olika riskscenarierna som utgör riskscenariorymden faktiskt beskriver verkligheten på ett korrekt sätt. När man skapar en systemmodell som sedan används för att genomföra en risk- och sårbarhetsanalys gör man det med avsikten att modellen skall avspegla verkligheten. Det är omöjligt att avspegla verkligheten exakt, d.v.s. in i allra minsta detalj, men det viktiga är att man får med de förhållanden i verkligheten som betyder något för den analys som man gör. En bra systemmodell kan användas för att förutsäga utvecklingen i verkligheten givet ett visst utgångsläge. När det gäller risk- och sårbarhetsanalyser har detta oftast att göra med att kunna förutsäga utvecklingen i ett system när något oönskat inträffar. Den systemmodell som används innehåller information om hur systemet utvecklas givet att det befinner sig i ett visst tillstånd. Kalla det ursprungliga systemtillståndet för A och det systemtillstånd som blir resultatet av att systemet befinner sig i A för systemtillstånd B. För att systemmodellen skall vara bra måste verkligheten om den befann sig i ett tillstånd som *motsvaras* av A i systemmodellen förflytta sig till ett tillstånd som *motsvaras* av B i systemmodellen. Ett exempel som illustrerar vad som avses är följande:

Antag att det finns en systemmodell som används för att analysera riskerna med farligt gods-transporter på en viss vägsträcka. I den modellen finns tillståndsvariabler som beskriver transporterna, d.v.s. tankbilarna, hur stort hål som uppstår i tanken på en tankbil om den är inblandad i en olycka, hur många människor som omkommer, o.s.v. Det finns också ett antal riskscenarier som beskriver händelseförlopp då en tankbil krockar, hål uppstår i tanken, det giftiga ämnet släpps ut och människor omkommer. Om de riskscenarier som finns med i modellen förutsäger andra konsekvenser än de som skulle bli resultatet om

motsvarande olycka inträffade i verkligheten är systemmodellen och riskscenarierna inte bra. Att validera systemmodeller kan vara mycket svårt, framförallt när man är intresserad av hur många människor som omkommer om ett specifikt riskscenario inträffar. I sådana fall får man i stället använda sig av experter och information från ”närliggande” områden för att beskriva vad som händer i de olika riskscenarierna. Ett exempel är att använda sig av information om hur dödliga vissa kemikalier är för djur och med hjälp av expertbedömningar försöka anpassa den informationen till människor.

De frågor som finns i Tabell 3 utgör ett instrument för att kritiskt granska den systemmodell som man använder sig av i en risk- och sårbarhetsanalys. Vanligtvis innebär en sådan granskning att det är en faktisk analys som granskas, inte en metod. Det finns dock metoder som ger mer eller mindre bra förutsättningar att genomföra en analys enligt de fyra områdena som representeras av frågorna i tabellen.

3.2 Beskrivning av olika metoder för risk- och sårbarhetsanalys

I detta avsnitt presenteras ett antal metoder för risk- och sårbarhetsanalys[9] med fokus på de vanligaste *typerna* av metoder. Beskrivningarna av metoderna är endast kortfattade, för ytterligare information om dem hänvisas till referenserna som ges i texten.

3.2.1 Seminariebaserade scenariometoder

Denna rapport tar upp tre metoder som klassas som *seminariebaserade scenariometoder*, IBERO [18], ROSA [19] och MVA-metoden [1] (informationen om MVA-metoden kommer även från metodens hemsida[10]). En seminariebaserad scenariometod är en metod för risk- och sårbarhetsanalys som bygger på användning av gruppdiskussioner för att resonera sig fram till olika riskscenarier som kan inträffa i ett system (vanligtvis en kommun eller region). De tre metoderna har stora likheter, åtminstone om man utgår från den dokumentation av metoderna som finns tillgänglig. Det finns dock en del skillnader, framförallt fokuserar de olika starkt på olika områden i risk- och sårbarhetsanalysen.

Kort beskrivning av metoderna

MVA-metoden (Municipal Vulnerability Analysis) är en metod för sårbarhetsanalys som utvecklats av en forskargrupp vid Lunds universitet. Det finns stöd i form av programvara för att genomföra analyser med MVA. Det finns även programstöd för IBERO, men när det gäller ROSA framgår det inte av dokumentationen om det finns någon tillgänglig mjukvara som stödjer en analys.

[9] Precis som påpekats tidigare i rapporten handlar det snarare om metoder för risk- *eller* sårbarhetsanalys.

[10] http://www.keg.lu.se/forsa/metoder/MVA/index.asp (2006-11-29).

Metoderna ger en förhållandevis övergripande beskrivning av hur man kan utforma arbetet med risk- och sårbarhetsanalys och de behandlar inte bara själva produktionen av en risk- och sårbarhetsanalys. Dokumentationen till alla tre metoderna betonar vikten av att betrakta själva arbetet med risk- och sårbarhetsanalys i en kommun eller region som en viktig del av resultatet. En annan tydlig gemensam nämnare är metodernas fokusering på att bedöma olika aktörers *förmåga* att genomföra olika uppgifter.

Man kan grovt beskriva metoderna som att arbetet med att genomföra en risk- och sårbarhetsanalys inleds med att en grupp människor samlas för att diskutera olika möjliga riskscenarier som kan inträffa i det aktuella systemet. Detta kan kallas för en *grovanalys*. Metoderna förefaller skilja sig lite i detta inledande skede, framförallt eftersom MVA-metoden och IBERO utgår från en *inventering* av olika skyddsvärda objekt i det aktuella systemet medan en analys med ROSA inleds med att identifiera olika hot eller riskscenarier som kan inträffa i systemet.

Grovanalysen resulterar i en lista med olika riskscenarier (alternativt hot) som kan inträffa i systemet. Utifrån denna lista väljer man sedan vilka scenarier som man skall fortsätta att göra en mer detaljerad analys av. Den detaljerade analysen går ut på att försöka kartlägga systemets aktörers förmåga att hantera det aktuella riskscenariot och även att bedöma konsekvenserna av det. Resultatet från analyserna kan sedan användas för att diskutera hur man kan förbättra sin förmåga att hantera de olika riskscenarierna.

Syfte
De huvudsakliga syftena med att genomföra en analys med metoderna är att bedöma olika aktörers förmåga att hantera en påfrestning samt att stimulera arbetet med risk- och sårbarhetsfrågor hos olika aktörer.

Vidare förefaller syftet med användningen av metoderna även vara att kunna prioritera åtgärder för att reducera sårbarheten i systemet som studeras.

Resultat
Det konkreta resultat som metoderna genererar är en beskrivning av olika aktörers förmåga att hantera en eller flera specifika påfrestningar. I samband med detta presenteras också uppskattningar av konsekvenserna på grund av påfrestningen.

Ett indirekt resultat av användningen av den här typen av metoder som förs fram i dokumentationerna är att medvetenheten om risk- och sårbarhetsrelaterade frågor ökar hos de aktörer som deltar vid seminarieövningarna och att de personliga nätverken mellan personer som har ansvar för risk- och sårbarhetsrelaterade frågor stärks.

Beskrivning av systemet
En analys med MVA-metoden inleds med en inventering av vad som är skyddsvärt i det aktuella systemet och vad som eventuellt kan skada det skyddsvärda. Metoden lägger stor vikt vid att identifiera *elementen* i systemet (exempelvis tekniska försörjningssystem), men den fokuserar inte på att försöka identifiera de olika elementens möjliga tillstånd. Därmed kan man inte säga att det är en systembaserad metod, även om den innehåller moment som påminner om det systembaserade angreppssättet. Detta förefaller inte gälla de andra två metoderna, d.v.s. de fokuserar direkt på att inventera olika riskscenarier som kan skada systemet utan att först kartlägga detta. Detta gör att dessa två metoder är scenariobaserade angreppssätt. I dokumentationen till ROSA-metoden används begreppet *typhändelse*, vilket med den terminologi som används i den här rapporten skulle motsvaras av en klass eller uppsättning riskscenarier som passar in på en viss beskrivning, exempelvis ”översvämningar”.

Hantering av riskscenariorymden
Samtliga metoder involverar aktiviteter då en uppsättning hot och risker som kan skada systemet identifieras. Detta kan man se som att riskscenariorymden till en början är mycket stor, d.v.s. den kan rymma en stor mängd olika riskscenarier. Denna stora mängd reduceras sedan ner då man väljer att gå vidare i analysen med ett fåtal av de ursprungliga riskscenarierna.

Det är svårt att avgöra om metoderna gör en fullständig uppdelning av riskscenariorymden eftersom det förmodligen beror på den enskilda analysen. Det framgår inte om det finns något stöd i någon av metoderna för att genomföra en fullständig uppdelning. Det verkar snarare som om metoderna är fokuserade på att göra en grundlig utredning av en eller ett fåtal riskscenarier snarare än att kraft ägnas åt att fundera över andra möjliga riskscenarier. En fullständig uppdelning av riskscenariorymden har alltså att göra med att utreda om man missat några viktiga riskscenarier i sin analys. Det skulle kunna ses som en typ av ”känslighetsanalys”. Exempelvis kan man tänka sig att i en analys av en kommuns sårbarhet för ett långvarigt elbortfall så innebär ett av de identifierade riskscenarierna att en specifik aktör ser till att ett antal reservkraftverk fraktas ut till några kommunala byggnader så att de kan fungera som värmestugor under elavbrottet. Om man i det här fallet inte funderat över vad konsekvenserna blir om aktören inte lyckas få ut reservkraftverken kan man påstå att riskscenariorymden inte är fullständig.

Av dokumentationerna att döma är detaljrikedomen när det gäller riskscenariobeskrivning inte speciellt hög. Det verkar mest handla om att bedöma förmåga och eventuellt också konsekvenser. Förmodligen sker en diskussion vid de seminarier där riskscenarierna diskuteras från vilken man kan få fram hur systemet utvecklas vid de olika scenarierna. En orsak till att man inte gör en särskilt detaljerad beskrivning av scenarierna kan vara att beskrivningen av systemet har en låg detaljeringsgrad, möjligtvis med undantag av MVA-metoden som ju inleder en

analys med en beskrivning av åtminstone det som betraktas som skyddsvärt och det som kan tänkas vara en utlösande faktor till en kris. Det bör noteras att analysmetoderna förmodligen innebär en grundlig genomgång av aktörers förmåga att genomföra olika uppgifter, men detta är inte samma sak som att göra en grundlig (detaljerad) genomgång av riskscenariorymden. En detaljerad genomgång av riskscenariorymden handlar om att beskriva *riskscenarierna* på ett detaljerat sätt, inte att beskriva förmåga. Dessa två begrepp hänger dock ihop eftersom en aktörs förmåga påverkar utgången av ett riskscenario. Om man i stället diskuterar sig fram till en bedömning av en aktörs förmåga *via* en beskrivning av olika riskscenarier borde man ha större möjlighet att komma fram till en bättre bedömning av en aktörs förmåga.

Hantering av konsekvenser
Varken MVA-metoden eller ROSA utgår från några på förhand definierade konsekvensdimensioner. På seminarierna med deltagarna diskuteras vilka dimensioner som kan vara relevanta att använda för att beskriva konsekvenserna. Metoderna ger inget stöd för hur man kan göra avvägningar mellan olika konsekvensdimensioner och inte heller något stöd för värdering av hur allvarligt ett enskilt scenario är. IBERO skiljer sig från de övriga metoderna när det gäller konsekvensbedömningar. I den metoden skall de som genomför analysen bedöma konsekvenserna av olika riskscenarier i termer av fem attribut: Människoliv, Hälsa, Hjälpbehov, Miljöskador och Ekonomi. Attributen graderas med en femgradig skala: Katastrofala, Mycket stora, Stora, Måttliga och Inga. En trolig anledning till att IBERO styr bedömningen av konsekvenser är att den metoden är i högre grad inriktad på att möjliggöra jämförelser mellan olika system och i så fall är det en fördel om analyserna använder sig av samma konsekvensattribut och samma kriterier vid bedömningar. IBERO ger dock ingen vägledning när det gäller att bedöma vad exempelvis ”Mycket stora” konsekvenser innebär, vilket kan leda till olika bedömningar. I stället framgår att den som genomför analysen skall utgå från de lokala förhållandena.

Hantering av osäkerhet
MVA-metoden ger ingen specifik vägledning för hur man skall hantera osäkerheten rörande framtida riskscenarier. Sannolikheten för de olika riskscenarierna bedöms inte. Inte heller bedöms sannolikheten att ett givet riskscenario inträffar, givet att en viss påfrestning har inträffat (se definitionen av sårbarhet i avsnitt 2.5). Under tiden som ett riskscenario utarbetas kan det tänkas att osäkerhet behandlas i gruppen som gör arbetet genom att de ”provar” alternativa utvecklingar för ett riskscenario och sedan går vidare med den utvecklingen som verkar mest sannolik. Detsamma gäller även de andra metoderna, d.v.s. osäkerheten rörande vad som händer efter en specifik påfrestning har ingen framträdande roll.

Simulering av riskscenarier
Ingen av metoderna innebär att simulering används vid framtagande av riskscenarier.

Överensstämmelse mellan analysen och verkligheten
Överensstämmelsen mellan de riskscenarier som behandlas under analysen och verkligheten beror på kunskap hos seminarieövningarnas deltagare.

3.2.2 Traditionella riskanalysmetoder

Begreppet ”traditionella” riskanalysmetoder används här för metoderna Felträd, Händelseträd, Grovanalys, Hazop, What if-metoden och FMEA. Dessa metoder har använts under lång tid för analys av framförallt tekniska system, men även i viss mån för de övriga systemtyperna (se föregående kapitel). En bra redogörelse för metoderna återfinns i Räddningsverkets ”Handbok för riskanalys” [20].

Kort beskrivning av metoderna
Metoderna som beskrivs ovan är förhållandevis olika, men i det här sammanhanget (när de jämförs med de seminariebaserade scenariometoderna) finns ändå tillräckligt med likheter för att placera dem i samma grupp av metoder. Både händelseträdsmetoden och felträdsmetoden används för att identifiera och strukturera riskscenarier samt att beräkna sannolikheten för dessa. Grovanalys, FMEA, What if-metoden och Hazop är mer inriktade på att identifiera riskscenarier och inte så mycket på själva kvantifieringen av sannolikheter. Gemensamt för dessa metoder är, möjligtvis med undantag för Grovanalys, att de ofta utgår från en systemmodell när de används för att komma fram till riskscenarier. Ett exempel på detta är att då Hazop-metoden används genomförs en systematisk genomgång av olika komponenter i systemet och för varje komponent utreder man vad konsekvenserna blir om dess funktion skulle avvika från det normala. Med den terminologin som används i den här rapporten innebär det att man går igenom tillståndsrymden för systemet och undersöker vilka möjliga tillstånd för de olika elementen som kan leda till riskscenarier. Den viktiga skillnaden i jämförelse med de scenariobaserade metoderna är att kartläggningen av systemet och systemets tillståndsrymd har en central plats vid framtagandet av riskscenarier. Grovanalysen utgör ett undantag från detta eftersom den ofta kan tillämpas utan att först göra en systembeskrivning.

Syfte
Syftet med att använda felträdsanalys är, precis om beskrevs ovan, att identifiera olika riskscenarier som kan leda till en oönskad händelse. Vidare är också syftet att beräkna sannolikheten för denna oönskade händelse (den så kallade topphändelsen). Sannolikheten kan sedan användas i en annan analys, exempelvis en händelseträdsanalys.

Syftena med händelseträdsanalys kan vara många, men ett vanligt syfte i det här sammanhanget är att skatta risken i ett system, d.v.s. svara på frågorna: Vad kan hända? Hur troligt är det? Och vad blir konsekvenserna? Svar på alla dessa frågor kan åskådliggöras med ett händelseträd och det är också möjligt att beräkna olika riskmått som sedan kan användas för jämförelser mellan olika system och i förlängningen också för att utvärdera investeringar i riskreducerande åtgärder (se exempelvis [21]).

Syftet med de övriga metoderna är vanligtvis att identifiera olika riskscenarier som kan leda till oönskade händelser.

Resultat
Resultatet från en felträdsanalys är sannolikheten (eller frekvensen) att en specifik händelse inträffar i ett system, den så kallade topphändelsen. Vidare kan man erhålla en uppsättning riskscenarier som kan leda till den aktuella topphändelsen. Detta innebär att riskscenariorymden är förhållandevis liten när det gäller en felträdsanalys eftersom alla riskscenarier som finns med involverar en specifik händelse. Eftersom felträdsanalys används för att beräkna sannolikheten för en specifik händelse, d.v.s. en uppsättning tillstånd i tillståndsrymden för systemet, kan man inte säga att dessa utgör risken eller sårbarheten i systemet (om inte den aktuella händelsen är det enda som kan inträffa i systemet). Felträd används i stället ofta för att beräkna sannolikheten för en händelse som ingår i ett eller flera av de riskscenarier som utgör risken eller sårbarheten i systemet.

Händelseträdet är mycket lämpligt för att beräkna/beskriva risken i ett system. Dess uppbyggnad gör att de olika grenarna i händelseträdet enkelt kan utnyttjas för att beskriva de olika riskscenarier som kan inträffa. Resultatet när man använder ett händelseträd är en beskrivning av ett antal riskscenarier som kan inträffa om den så kallade initierande händelsen inträffar. Detta resultat motsvarar den operationella definitionen av risk om den initierande händelsen är tillräckligt vagt definierad för att täcka in alla möjliga riskscenarier inom det område som man är intresserad av att beskriva risken. Om man exempelvis är intresserad av brandrisken i en byggnad kan man definiera den initierande händelsen som ”Brand uppstår i byggnaden”.

Resultaten från de övriga metoderna är uppsättningar med riskscenarier, ofta med tillhörande sannolikhetsskattningar och konsekvensskattningar. Det bör dock noteras att dessa riskscenarier ofta bara innebär att en eller kanske två komponenter i det aktuella systemet avviker från det som betraktas som det normala. Mer komplexa fel är svåra att identifiera med dessa tekniker.

Beskrivning av systemet
Samtliga metoder, utom möjligtvis grovanalysen, utgår från en förhållandevis detaljerad beskrivning av systemet, eller så framgår systembeskrivningen implicit av själva analysmetoden, vilket är fallet med exempelvis händelseträdsmetoden.

Hantering av riskscenariorymden
Felträdsanalys, händelseträdsanalys och grovanalys har ingen begränsning av riskscenariorymden, begränsningen bestäms av den aktuella analysen. När det gäller de övriga metoderna kan man säga att de har en tendens till att vara begränsade till förändringar av de komponenter som ingår i det tekniska system som man är intresserad av. Detta är dock vanligtvis inget problem eftersom fokus i dessa analyser ofta är på själva det tekniska systemet.

När det gäller uppdelningen av riskscenariorymden är det inte säkert att en fullständig uppdelning genomförs bara för att man använder någon av dessa metoder. Man kan dock säga att samtliga metoder, utom möjligtvis grovanalys, är uppbyggda på ett sätt som minskar risken för en ofullständig uppdelning. Exempelvis bör man vid genomförandet av en händelseträdsanalys undersöka om det finns ytterligare ”grenar” som skulle behöva läggas till för att kunna representera alla möjliga riskscenarier.

Detaljeringsgraden i uppdelningen av riskscenariorymden när man använder någon av de aktuella metoderna kan vara mycket stor. För komplexa system, exempelvis en kärnreaktor, kan uppdelningen vara mycket omfattande. Den uppdelning som genomförs är vanligtvis disjunkt.

Hantering av konsekvenser
Metoderna innebär ingen begränsning av vilka konsekvenser som kan studeras, men de ger heller vanligtvis ingen handledning rörande vilka konsekvens-dimensioner som skall studeras eller hur olika riskscenarier skall värderas.

Hantering av osäkerhet
Felträdsanalys och händelseträdsanalys är specifikt utformade för att kunna beräkna sannolikheten för olika riskscenarier. De övriga metoderna använder oftast en kvalitativ skattning av sannolikheten för ett specifikt riskscenario, förutom Hazop där normalt inga sannolikhetsskattningar ingår.

Simulering av riskscenarier
Ingen av metoderna använder sig av simulering när det gäller att generera riskscenarier. Ofta används dock simuleringsmodeller i kombination med exempelvis händelseträd för att beräkna konsekvenserna av olika riskscenarier.

3.2.3 Hierarkisk Holografisk Modellering (HHM)

Kort beskrivning av metoden
Hierarkisk Holografisk Modellering [11, 22] skiljer sig från de seminariebaserade scenariometoderna på så sätt att den har ett tydligare systemfokus i sin uppbyggnad. Den skiljer sig också från de traditionella metoderna eftersom den i många fall kan uppfattas som en meta-metod för risk- och sårbarhetsanalys, d.v.s.

den innebär att ett antal traditionella metoder för risk- och sårbarhetsanalys *tillämpas* som en del av HHM-metoden.

HHM-metoden är tänkt att användas för analys av risker i komplexa sociotekniska system som kan betraktas från många perspektiv. Just det faktum att HHM använder många olika perspektiv och olika tillvägagångssätt vid analysen är ett av dess karaktäristiska drag. Ett exempel som illustrerar vad som avses med olika perspektiv är en analys av risker och sårbarheter i ett vattendistributionssystem som presenteras i [11]. I den analysen används perspektiven: fysisk, omfattning, temporal, underhåll, institutionell, organisatorisk, ledning, resursfördelning. Det fysiska perspektivet har med vattendistributionssystemets fysiska komponenter, exempelvis rör och pumpar, att göra. Omfattningsperspektivet har att göra med att systemet sträcker sig genom flera regioner och därmed kan påverka flera olika kommuner och till och med hela regioner. I och med att systemet är så stort kan man exempelvis välja att betrakta konsekvenser av avbrott för de olika regionerna separat eller se det från en nationell nivå. Perspektivet som kallas temporal har att göra med att man i analysen skiftar tidsperspektiv när man gör analysen, exempelvis kan man betrakta konsekvenser på 3 - 5 års sikt eller på 10 – 20 års sikt, o.s.v.

Meningen med att använda ett antal olika perspektiv i analysen är att man strävar efter en bättre belysning av de sammansatta problem som den här typen av analyser ofta fokuserar på.

Syfte
HHM-metoden förefaller ha ett mycket brett användningsområde. Det huvudsakliga syftet med att applicera metoden i det här sammanhanget är dock att utreda riskerna i komplexa sociotekniska system samt att eventuellt också genomföra utvärderingar av olika alternativ för riskreduktion.

Resultat
Resultatet då man använder HHM är en uppdelning av riskscenariorymden i ett antal riskscenarier som härrör från ett antal olika perspektiv, alltså är de inte disjunkta. Resultatet kan också bestå av utvärderingar av olika alternativ för riskreducerande åtgärder för det aktuella systemet.

Beskrivning av systemet
Det framgår inte i vilken utsträckning som en systemmodell skapas när problemen analyseras med HHM. Det förefaller dock sannolikt att en förhållandevis detaljerad systemmodell uppdelad i hierarkier används i analysen. Utifrån den modellen sker sedan identifieringen av riskscenarier som har att göra med de olika perspektiven som identifierats.

Hantering av riskscenariorymden
Metoden som sådan sätter inga begränsningar på riskscenariorymden. Storleken på den har istället med vilka perspektiv som man väljer att använda i analysen att göra. Det är också svårt att avgöra om metoden ger något stöd för att undvika en icke fullständig uppdelning av riskscenariorymden. Det troligaste är att detta är upp till den som gör analysen att kontrollera.

När det gäller hur detaljerad uppdelningen av riskscenariorymden är så uppmuntrar metoden till en förhållandevis noggrann uppdelning genom att man utgår från ett antal typer av riskscenarier och för varje typ successivt identifierar mer detaljerade riskscenarier. De olika typerna av riskscenarier, exempelvis sådana som innebär en brand och sådana som innebär en storm, kan inträffa samtidigt och detta innebär att de riskscenarier som tas fram med HHM-metoden inte är disjunkta. Detta beskrivs som en av HHM-metodens styrkor eftersom det aktuella systemets sårbarhet analyseras med avseende på många typer av riskscenarier, men det kan också betraktas som en svaghet på grund av de skäl som diskuterades i avsnitt 3.1.

Hantering av konsekvenser
HHM har inga fastlagda konsekvensattribut utan dessa tas fram för de individuella analyserna. Däremot har HHM stöd för rangordning av riskscenarier genom användning av multiattributiv nyttoteori (se exempelvis [23]).

Hantering av osäkerhet
När man använder HHM finns det möjlighet att betrakta en uppsättning riskscenarier och även att skatta deras respektive sannolikheter, exempelvis genom användning av händelseträd eller beslutsträd.

3.2.4 Simuleringsmodeller

En del metoder som används i arbetet med att göra en risk- och sårbarhetsanalys är simuleringsmodeller. Dessa modeller är användbara för att beskriva den dynamiska utvecklingen i ett system, d.v.s. ett eller flera scenarier, givet att systemet befinner sig i ett visst utgångsläge och/eller givet att systemets tillstånd ändras på något sätt under scenarierna.

Man kan skilja på deterministiska och probabilistiska simuleringsmodeller. De deterministiska modellerna ger alltid samma resultat givet att systemets tillstånd vid början av simuleringen är detsamma, medan de probabilistiska modellernas kan skilja sig åt beroende på att vissa tillståndsförändringar under simuleringen är probabilistiska (se avsnitt 2.6).

En simuleringsmodell kan vara uppbyggd på så sätt att den beräknar en stor mängd riskscenarier för ett system och att den därför kan kallas för en riskanalysmetod eller sårbarhetsanalysmetod (eftersom den ”genererar” riskscenariorymden). Ett exempel på detta är den nätverksanalysmodell som beskrivs i rapporten ”Analys av

sårbarhet i teknisk infrastruktur med nätverksmodeller" [24]. De flesta simuleringsmodeller fungerar dock inte på det sättet utan är oftast deterministiska och genererar bara resultat som beskriver systemets dynamiska utveckling under ett scenario. Exempel på sådana metoder är FDS (Fire Dynamic Simulator) [25], vilket är en simuleringsmodell för brand- och brandgasspridning och FLACS (Flame Acceleration Simulator) [26] som används för att simulera explosioner. Dessa två simuleringsmodeller är i det aktuella sammanhanget ganska begränsade när det gäller användbarhet, framförallt eftersom de bara behandlar en mindre del av de system som vanligtvis är av intresse då man gör en risk- och sårbarhetsanalys för komplexa sociotekniska system.

Det finns dock simuleringsmodeller som kan vara mycket tillämpbara då en risk- och sårbarhetsanalys skall genomföras för ett system vars riskscenariorymd är så stor att det är praktiskt omöjligt att beskriva den. I det fallet är det mycket lättare att beskriva de regler som gäller för systemets dynamiska utveckling (tillståndsförändringar) och därefter låta en dator beräkna hur systemet kommer att utvecklas givet ett visst utgångstillstånd. En typ av modeller som kan vara användbara vid studier av ett systems sårbarhet är så kallade Input/Output-modeller. I denna typ av modell används differentialekvationer för att beskriva hur olika element i ett system är beroende av varandra och modellen kan användas för att beräkna den dynamiska utvecklingen av systemet efter en störning. Haimes har använt den metoden när han analyserat en del av den amerikanska ekonomins sårbarhet för olika typer av störningar samt olika infrastruktursystems beroenden av varandra [27-29].

Sammanfattningsvis kan simuleringsmodeller vara mycket användbara i risk- och sårbarhetsanalyser, men vanligtvis används de som ett komplement till andra metoder. Exempelvis skulle man kunna använda sig av händelseträdsmetodik för att göra en riskanalys, och för att beräkna en specifik sannolikhet eller konsekvens utnyttjar man sig av en simuleringsmodell.

3.2.5 Indexmetoder

En grupp metoder som ibland förekommer i det aktuella sammanhanget kallas *indexmetoder* [20]. Resultatet då man använder den typen av metoder är någon typ av index som representerar risken i det aktuella systemet, d.v.s. indexet kan användas för att uttala sig om risknivån i en specifik anläggning är högre eller lägre än i en annan anläggning.

Denna typ av metoder kommer inte att behandlas detaljerat i denna rapport eftersom de inte, enligt definitionerna av risk och sårbarhet i kapitel 2, kan användas för att analysera risker eller sårbarheter. För att göra det krävs att användningen av en metod resulterar i en uppsättning riskscenarier, deras sannolikhet och konsekvenser, vilket indexmetoderna inte kan användas till.

3.3 Utvärdering och jämförelse av metoder för risk- och sårbarhetsanalys

I ovanstående avsnitt har ett antal metoder beskrivits med hjälp av de teoretiska utgångspunkter som presenterades i föregående kapitel. Här följer nu en utvärdering av hur lämpliga metoderna är för olika typer av syften och vad deras styrkor och svagheter är.

3.3.1 Riskanalys

Om syftet med en analys är att genomföra en riskanalys, d.v.s. att svara på frågorna: ”Vad kan hända?”, ”Hur troligt är det?” och ”Vad blir konsekvenserna”, är det sannolikt så att de lämpligaste metoderna någon av de traditionella riskanalysmetoderna. För tekniska system, exempelvis en kemisk process, är förmodligen metoder såsom Hazop, FMEA, felträd och händelseträd de bästa teknikerna att använda. Om man förutom de tekniska komponenterna i processen även vill ta hänsyn till operatörers agerande kan någon metod från området Human Reliability Analysis (HRA) användas. Inom detta område finns modeller för att skatta sannolikheten att en operatör gör fel givet vissa förutsättningar och dessa skattningar kan användas i kombination med de traditionella riskanalysmetoderna.

Det är dock troligt att den typ av system som analyseras inte alltid är så förhållandevis enkelt att avgränsa som en process i en industri. Det kan till exempel röra sig om ett företags, en kommuns eller en regions risker. I det fallet kan visserligen tekniker som grovanalys, felträd och händelseträd vara användbara, men metoder som är specialiserade på analys av rent tekniska system blir svåra att tillämpa.

Täckningsgradsproblemet

För att göra en bra riskanalys av ett så komplext system som exempelvis en kommun måste konsekvenserna definieras tydligt och en beskrivning av hur systemet ser ut måste finnas tillgänglig. Därefter kan en analys av möjliga sätt som systemet kan drabbas av oönskade konsekvenser genomföras. En grovanalys är användbar för detta och även Hierarkisk Holografisk Modellering (HHM) kan vara bra. Det viktiga när man gör en riskanalys för ett system är att inte riskscenariorymden reduceras utan att man har fog för det, d.v.s. att man väljer att bortse från vissa riskscenarier utan att analysera deras konsekvenser eller sannolikheter. Detta kallas här för ”täckningsgradsproblemet”, d.v.s. hur ser man i analysen till att riskscenariorymden är fullständig i bemärkelsen att alla riskscenarier som kan inträffa finns representerade?

Genom en tydlig systemdefinition som man sedan systematiskt går igenom och analyserar ”fel” i kan man hantera denna problematik. Just i detta avseende finns en skillnad mellan de metoder som beskrivits som systembaserade och scenariobaserade. I och med att systembaserade metoder fokuserar på att först skapa en systemmodell för att sedan analysera riskscenarier kan systemmodellen

utnyttjas för att hantera täckningsgradsproblemet. Vid en analys av riskscenarier kan man då gå igenom alla elementen i systemmodellen och undersöka vad som skulle hända om något ”gick fel” i just det elementet. En sådan systematisk genomgång ger upphov till en rad olika initierande händelser (se kapitel 2). Ett alternativ till att gå igenom systemets samtliga element är att försöka identifiera ett antal händelser som kan påverka systemet och sedan utvärdera vad som händer med de olika elementen om händelsen inträffar. När dessa händelser identifieras är det mycket viktigt att inte riskscenarier utelämnas. Ett sätt att systematiskt hantera detta problem är att gruppera händelserna tydligt, exempelvis som ”Storm”, ”Översvämning”, ”Brand”, o.s.v. och sedan ha med typ av händelse som heter ”Övriga händelser”. Meningen med att ha med denna typ av händelse är att påminna den som gör analysen att kontinuerligt arbeta med att försöka utvärdera om någon annan typ av händelse än de som man identifierat kan inträffa i systemet. När man använder denna typ av angreppssätt är det viktigt att notera att de olika riskscenarierna som blir resultatet om de olika typerna av händelser inträffa förmodligen inte är disjunkta, d.v.s. de kan inträffa samtidigt. Exempelvis kan en storm inträffa samtidigt som en brand. Denna typ av kombinationer av händelser som identifierats är en viktig del av kartläggningen av olika riskscenarier och gruppen ”Övriga händelser” tjänar som en påminnelse om att hela tiden försöka identifiera nya typer av händelser eller kombinera de gamla typerna.

Sannolikhetsskattningar
Ett annat problem som måste hanteras av riskanalysmetoder är hur sannolikhetsskattningar för olika riskscenarier skall genomföras. Det finns åtminstone tre sätt att göra detta på. Ett sätt som man kan använda om man har tillgång till information från systemet eller liknande system, där det framgår hur ofta de olika riskscenarierna uppkommit, är att använda den informationen för skattningar av sannolikheten/frekvensen för de olika riskscenarierna. Själva skattningarna är i det här fallet förmodligen inte speciellt svåra att genomföra, problemet handlar snarare om att bedöma hur representativa de system som man har information om är för det aktuella system som är av intresse. Om man däremot bara har information om hur ofta *komponenterna* i systemet fungerar på fel sätt måste man använda logiska modeller, exempelvis felträd och händelseträd för att skatta sannolikheterna för olika riskscenarier som kan inträffa i systemet. Det sista sättet att skatta sannolikheterna för olika riskscenarier är att använda expertbedömningar.

De två sätt att skatta sannolikheter för olika riskscenarier som innebär att information från liknande system används, eller att logiska modeller används, förutsätter att det finns en systemmodell att utgå ifrån. I det första fallet måste man ha systemmodellen för att avgöra om den information som finns är relevant för det aktuella systemet och i det andra fallet måste man ha systemmodellen för att kunna ta fram de olika riskscenarierna. Endast i det sista fallet, d.v.s. då man enbart använder expertskattningar, kan analysen genomföras utan en systemmodell. Detta

är förmodligen något felaktigt eftersom personerna som jobbar med analysen troligtvis använder någon typ av systemmodell för att resonera om problemet, men den behöver inte uttryckas explicit.

Oavsett vilken metod som används för att skatta hur sannolika olika riskscenarier är bör man dokumentera den information som ligger till grund för en specifik skattning. Den som gör analysen bör också beskriva varför den aktuella informationen är lämplig att använda i det aktuella fallet, och om expertskattningar används bör experterna motivera sina skattningar genom att beskriva hur de kommit fram till dem.

Konsekvensskattningar
Skattningar av konsekvenserna av olika riskscenarier är kopplat till vilka typer av konsekvenser som tas med i en analys och beror normalt inte på vilken metod för riskanalys som används.

Samma krav som på sannolikhetsskattningar kan ställas på konsekvensskattningar, d.v.s. att informationen som ligger till grund för skattningen dokumenteras.

Olika metoders lämplighet
För att svara på de tre frågorna som beskrivits i inledningen på det här avsnittet bedöms de klassiska riskanalysmetoderna vara de mest lämpliga. Anledningarna till det är att de har ett tydligt systemfokus, vilket medför lägre risk att utelämna relevanta riskscenarier, samt att de också kan användas för att beräkna sannolikheter/frekvenser för olika riskscenarier. Dessa metoder har dock begränsningar när det gäller att analysera riskerna i mer komplexa system, vilket kommer att tas upp närmare i nästa avsnitt. Framförallt handlar metodernas begränsningar om att det kan vara praktiskt svårt att använda dem för sådana system eftersom analyserna blir mycket omfattande samt att vissa typer av riskscenarier är svåra att identifiera med den typen av metoder. De riskscenarier som är svåra att identifiera med denna typ av metoder är de som involverar flera olika element som inte fungerar som de skall, eller riskscenarier där operatörer eller andra agenter genomför handlingar som påverkar ett riskscenario.

Då systemet som studeras är mer komplext kan olika seminariebaserade scenariometoder fungera bra, men det förutsätter att man vid analysen är uppmärksam på framförallt täckningsgradsproblemet som togs upp ovan och att man är mycket noga med att dokumentera informationen som ligger till grund för sannolikhetsskattningar (se ovan). Därför bör de seminariebaserade metoderna (MVA, IBERO och ROSA) kompletteras med ett tydligare systemfokus där större vikt läggs vid att skapa en systemmodell med vilken man sedan systematiskt kan försöka identifiera olika händelser och riskscenarier som kan skada systemet. Det är förmodligen ingen nackdel om metoder såsom händelseträdsanalys och

felträdsanalys utnyttjas i detta arbete, även om det inte alltid behöver innebära en kvantifiering av sannolikheter.

3.3.2 Sårbarhetsanalys

Sårbarhet kan, precis som påpekades i avsnitt 2.5, uppfattas antingen som ett systems oförmåga att motstå en specifik påfrestning eller som ett tillstånd eller ett förhållande som gör att de negativa konsekvenserna i ett system blir stora om en specifik påfrestning inträffar. Om man använder den första tolkningen, d.v.s. som ett systems oförmåga att motstå en påfrestning kan man använda den i kapitel 2 föreslagna definitionen av sårbarhet (se avsnitt 2.5) som grund för en diskussion om vilka metoder som är lämpliga för att analysera det.

Om man däremot ser sårbarhet som ett tillstånd eller ett förhållande i ett system blir det något mer problematiskt att diskutera hur en bra metod för att analysera sådana sårbarheter skall vara uppbyggd. Det förefaller dock rimligt att för att identifiera sårbarheter i ett system måste först en analys av systemets oförmåga att motstå en specifik påfrestning genomföras (d.v.s. sårbarhet enligt den första tolkningen). Anledningen är att om man inte har genomfört en sådan analys vet man inte vad som kan hända och inte heller vad konsekvenserna blir eller hur troliga de är för den specifika påfrestningen. Om man inte vet det blir det svårt att identifiera ett tillstånd som gör att konsekvenserna blir stora om en specifik påfrestning inträffar. En analys av den första typen av sårbarhet (ett systems oförmåga) är alltså en förutsättning för att kunna identifiera den andra typen av sårbarhet (ett tillstånd). Det förefaller också rimligt att om en analys av ett systems oförmåga att motstå en specifik påfrestning är väl utredd borde den som gjort analysen ha en god uppfattning om eventuella sårbarheter i systemet. I det här avsnittet förutsätts att det är sårbarhet enligt definitionen i kapitel 2 som är av intresse.

Täckningsgradsproblemet

På samma sätt som när det gäller en metod för riskanalys måste en metod för sårbarhetsanalys kunna hantera det så kallade täckningsgradsproblemet, d.v.s. hur kan man vara säker på att man inte missat några riskscenarier i analysen? Detta är ett problem som de seminariebaserade scenariometoderna kan ha svårt att hantera. Av den dokumentation som finns att tillgå rörande de tre metoderna IBERO, MVA och ROSA förefaller det som om detta problem inte får speciellt stort utrymme. Faktum är att man kan få intrycket när man läser dokumentationerna att en påfrestning kan ge upphov till endast ett enda riskscenario. Visserligen kan man göra en grov uppdelning av riskscenariorymden och representera alla möjliga riskscenarier med bara ett enda, men detta är förmodligen alltför grovt för att det skall kunna betraktas som en bra representation av verkligheten (se avsnitt 3.1.8).

För att hantera detta problem skulle de seminariebaserade metoderna behöva innefatta en systematisk genomgång av ett antal potentiella riskscenarier för en specifik påfrestning. Detta skulle exempelvis kunna innebära att systematiskt

utvärdera vad som händer om de olika aktörerna misslyckas eller fördröjs när de genomför sina uppgifter. Ett annat exempel på hur man kan utvärdera varianter av den typ av riskscenario som man jobbar med är att öka/minska någon viktig tillståndsvariabel som har med själva påfrestningen att göra. Vad händer exempelvis om vattenflödena i ett riskscenario som involverar översvämning skulle vara dubbelt så höga? Detta är ett sätt att systematiskt göra en mer detaljerad beskrivning av riskscenariorymden som påminner mycket om de traditionella riskanalysmetoderna, framförallt Hazop där man just använder ledord av typen ”mer, högre”, ”mindre, lägre” för att undersöka vad en tillståndsförändring av ett systemelement får för effekt på systemet. Detta förutsätter en beskrivning av systemets olika element, vilket även skulle kunna åstadkommas med en seminariebaserad scenariometod. Exempelvis innehåller MVA-metoden en inventeringsfas som kan användas för att beskriva delar av systemet.

Det är sannolikt omöjligt att veta exakt vad som händer i ett system efter en påfrestning. För att beskriva detta lämpar sig händelseträd mycket bra. Genom att den aktuella påfrestningen är den initierande händelsen i händelseträdet kan man använda fortsättningen av trädet för att illustrera olika möjliga riskscenarier i systemet som kan bli resultatet av påfrestningen.

Sannolikhetsskattningar
Att bedöma sannolikheter för olika riskscenarier givet en specifik påfrestning verkar inte vara något som ingår i MVA-metoden, IBERO eller ROSA. Detta hänger förmodligen samman med att det bara är ett eller ett begränsat antal riskscenarier till följd av en påfrestning som studeras och att det därför inte finns någon anledning att bedöma sannolikheter.

När det gäller sannolikhetsskattningar bör det observeras att det är betingade sannolikheter som skattningarna gäller, d.v.s. betingade på att en specifik påfrestning uppstått. Det handlar alltså inte om att bedöma sannolikheten att den specifika påfrestningen uppstår. Att bedöma sannolikheten för de olika riskscenarierna givet att påfrestningen inträffat är relevant för att bedöma sårbarheten i ett system. Utan sådana skattningar ger inte resultatet av sårbarhetsanalysen en rättvisande bild av systemets sårbarhet, speciellt inte om ett flertal riskscenarier har identifierats. Sannolikhetsbedömningar för riskscenarierna kan enkelt hanteras med hjälp av ett händelseträd som dessutom kan fungera som en bra illustration av vilka riskscenarier som kan inträffa i systemet. Dessutom kan felträdsmetodik användas för att skatta olika sannolikheter som ingår i en händelseträdsanalys. På samma sätt som när det gäller sannolikhetsskattningar för en riskanalys bör den information som ligger till grund för en sannolikhetsskattning som används i en sårbarhetsanalys dokumenteras (se avsnitt 3.3.1).

Konsekvensskattningar
De konsekvensskattningar som genomförs för de olika riskscenarierna i en sårbarhetsanalys skiljer sig inte från dem som genomförs i en riskanalys. Inte heller när det gäller konsekvensskattningar i en sårbarhetsanalys skiljer sig metoderna speciellt mycket åt. IBERO är den enda metoden som explicit ger uttryck för vilka konsekvensdimensioner som skall användas.

Samma krav som ställs på sannolikhetsskattningar kan också ställas på konsekvensskattningar, d.v.s. att informationen som ligger till grund för skattningen dokumenteras.

Olika metoders lämplighet
Att bedöma metodernas lämplighet när det gäller att genomföra en sårbarhetsanalys är svårt. Framförallt eftersom slutresultatet av analysen i hög grad beror på vilka personer som deltagit i analysen och vilken information som de haft tillgång till. Det finns dock några olika aspekter som skiljer metoderna åt och som förefaller relevanta för metodernas möjligheter att analysera ett systems sårbarhet enligt definitionen i kapitel 2 (se avsnitt 2.5).

De seminariebaserade scenariometoderna (MVA, ROSA och IBERO) bygger samtliga på gruppdiskussioner rörande hur systemet i fråga kan hantera en viss påfrestning. Metoderna är konstruerade för att inbjuda till diskussioner om risker och sårbarheter och syftena som kan uppfyllas med hjälp av metoderna är mycket bredare än för de traditionella riskanalysmetoderna (felträd, etc.). Styrkan hos dessa metoder när det gäller risk- och sårbarhetsanalys ligger i att de uppmuntrar till en kreativ process där identifieringen av olika möjliga händelser och riskscenarier blir effektiv. En av nackdelarna är dock att de ger litet stöd när det gäller uppdelningen av riskscenariorymden. Också när det gäller sannolikhetsbedömningar för de olika riskscenarierna är stödet från metoderna inte speciellt starkt.

De traditionella riskanalysmetoderna (felträd, händelseträd, etc.) har ett betydligt starkare stöd för uppdelning av riskscenariorymden samt för beräkning av sannolikheter för olika riskscenarier. Nackdelen med dessa metoder i det här sammanhanget har att göra med att de förutsätter en tydlig systemmodell och förhållandevis detaljerad kunskap om systemets dynamiska uppträdande. När det gäller risk- och sårbarhetsanalys för komplexa sociotekniska system kan detta vara svårt att uppfylla.

Eftersom båda dessa typer av analysmetoder har för- och nackdelar vid användning inom det aktuella området skulle troligtvis en kombination av dem vara fördelaktig. En metod som kombinerar den förhållandevis detaljerade genomgången av riskscenarier, som de seminariebaserade scenariometoderna innebär, med den systematiska uppdelningen av riskscenariorymden som kännetecknar de

traditionella metoderna skulle förmodligen vara mycket lämplig för analys av ett systems sårbarhet.

3.3.3 Värdering av risk- och sårbarhetsreducerande åtgärder

Om en analys skall användas för värdering (prioriteringar) av riskreducerande åtgärder bör det kunna ställas högre krav på metoden än om den bara skall resultera i att ett antal riskscenarier och deras tillhörande sannolikheter och konsekvenser identifieras. Det bör också diskuteras om det är lämpligt att använda en sårbarhetsanalys som grund för ett investeringsbeslut. Kanske är det så att det borde krävas att en sådan analys kompletteras med en analys av hur ofta den/de påfrestningar som undersökts i analysen inträffar. En sådan komplettering skulle innebära att sårbarhetsanalysen blev en riskanalys och därmed potentiellt mer lämplig att använda som grund för ett investeringsbeslut.

Ingen av de metoder som studerats ger någon detaljerad vägledning för hur man skall hantera en analys av olika åtgärder. Visserligen står det i dokumentationen till en del av metoderna att man skall ta fram åtgärdsförslag och värdera dessa, men det står inget om hur detta skall genomföras. Det finns alltså ett behov av att precisera detta lite bättre. Två krav som kan vara rimliga att ställa på en sådan metod är att:

- En värdering av risk- och sårbarhetsreducerande åtgärder bör innehålla en beskrivning av hur de föreslagna åtgärder påverkar det aktuella systemet, då detta inte alltid är självklart. Notera också att med ”systemet” avses den modell av verkligheten som används för analys av risk och sårbarhet. Att beskriva hur en åtgärd påverkar systemet handlar alltså inte om en allmän beskrivning av vad som händer i verkligheten om åtgärden införs utan om att beskriva hur den systemmodell som man använder för att analysera verkligheten förändras.

- Det bör finnas en beskrivning av hur samtliga förslag på riskreducerande åtgärder som föreslås påverkar riskscenariorymden. Detta innebär att för varje åtgärd som föreslås måste man identifiera vilka riskscenarier som påverkas av den aktuella åtgärden och vilken påverkan blir. En investering i risk- och sårbarhetsreducerande åtgärder skall reducera sannolikheten och/eller konsekvenserna för något/några riskscenarier. Därför är det mycket viktigt att det framgår i en värdering vilka de riskscenarier som påverkas är.

Beroende på hur den risk- och sårbarhetsanalys som ligger till grund för investeringsbeslutet ser ut kan redovisningen av de två kraven se lite olika ut. Om analysen som utgör grunden är utförd på ett sådant sätt att definitionerna av sårbarhet eller risk som presenteras i kapitel 2 använts bör även dessa definitioner utnyttjas vid en värdering av olika investeringsalternativ. Detta innebär att om de

riskscenarier som utgör risken/sårbarheten i systemet är beskrivna med sannolikheter/frekvenser bör även investeringsanalysen innehålla en kvantitativ bedömning av hur dessa påverkas. Om en sådan kvantitativ beskrivning inte finns bör en kvalitativ bedömning av hur sannolikheter/frekvenser påverkas presenteras.

3.3.4 Förmågebedömning

Ingen av de traditionella riskanalysmetoderna fokuserar på att ge stöd för bedömning av en agents (vanligtvis en organisation av något slag) förmåga att hantera en specifik störning. I dokumentationerna till de seminariebaserade scenariometoderna tas bedömning av förmåga upp, men det presenteras inte någon djupare genomgång av hur en sådan bedömning skall eller bör gå till. Detta är upp till användaren av metoderna att avgöra.

Vid bedömning av en aktörs förmåga är det viktigt att vara konkret med vad som menas med förmåga och framförallt hur förmåga skall mätas. För det första måste man klargöra vilken uppgift som förmågan att utföra skall bedömas för. Uppgift är det begrepp som används för att beteckna ”det som skall göras”. Genom att fundera över hur förmåga skall mätas kan man identifiera de faktorer som avgör hur bra eller dåligt en specifik uppgift utförs. Vanliga attribut är troligtvis tid och kvalité. Ett exempel kan vara att man vill bedöma en aktörs förmåga att ta prover på ett antal människor och få fram provsvar. I det fallet kan tiden vara en viktig faktor, d.v.s. hur snabbt får man fram provsvaren för ett visst antal människor och kvalité kan ha att göra med om man har dragit rätt slutsatser rörande proven.

Med utgångspunkt i de olika uppgifterna som en aktör kan ha och de olika faktorer som beskriver hur väl aktören lyckas med uppgifterna kan man med hjälp av definitionen av sårbarhet (se kapitel 2) diskutera vad förmåga är. Förmåga kan definieras som ”…möjlighet att utföra ngt, som enbart beror av inre egenskaper…”[11] och i det här sammanhanget innebär förmåga möjligheten att utföra en specifik uppgift *givet vissa omständigheter*. Att förmågan att utföra en viss uppgift är betingad av omständigheterna i vilka uppgiften utförs är rimligt eftersom omständigheterna i högsta grad kan påverka agenters förmåga att utföra uppgifter. Exempelvis är det troligtvis stor skillnad på en agents förmåga att kommunicera med andra agenter om de fasta och mobila telefonförbindelserna fungerar eller ej.

Utifrån detta resonemang kan man dra slutsatsen att en bedömning av en aktörs förmåga måste involvera *åtminstone* tre element:

[11] Hämtat från Nationalencyklopedins webbplats www.ne.se 2007-04-04, uppslagsord: ”förmåga”.

- En beskrivning av vilken aktör och vilken uppgift som avses med förmågebedömningen[12].
- En beskrivning av vilka faktorer som påverkar aktörens möjligheter att utföra uppgiften och vilka faktorer som avgör hur bra aktören lyckas med att utföra uppgiften.
- En beskrivning av under vilka omständigheter som förmågebedömningen gäller.

Utifrån dessa tre element och definitionen av sårbarhet kan sedan förmåga definieras som svaret på frågorna ”Vad kan hända givet att aktören skall utföra den aktuella uppgiften under de givna omständigheterna?”, ”Hur sannolikt är det?” och ”Vad blir konsekvenserna mätt med hjälp av de faktorer som avgör hur bra aktören lyckats med den aktuella uppgiften?”. Utifrån svaret på dessa frågor kan man sedan göra en *värdering* av förmågan och då kan slutsatserna bli av typen ”bra”, ”mindre bra”, etc.

Vilka omständigheter som skall tas med vid bedömningen bestäms av den påfrestning som analyseras. En specifik påfrestning på systemet kan resultera i olika omständigheter för aktören att genomföra sina uppgifter i beroende på vilket riskscenario som inträffar. En specifik påfrestning för systemet kan även resultera i att den aktuella agenten måste utföra olika uppgifter beroende på vilket riskscenario som inträffar.

Ett exempel på förmågebedömning är räddningstjänstens förmåga att släcka bränder. Faktorer som avgör räddningstjänstens möjligheter att utföra uppgiften kan vara hur länge branden pågått när larmet når räddningstjänsten, framkompligheten på vägarna, om alla resurserna i form av släckbilar är tillgängliga, etc. Med utgångspunkt i dessa faktorer kan räddningstjänstens förmåga att släcka bränder, då larmet når räddningtjänsten utan förseningar, då vägarna inte är blockerade och alla resurser är tillgängliga bedömas genom att beskriva ett antal riskscenarier som kan inträffa. Exempel på en sådan riskscenariobeskrivning är att branden inträffar i en byggnad utan automatiskt brandlarm på ett visst avstånd från brandstationen och att tiden det tar att släcka branden då är 35 minuter från brandstart. Ett annat riskscenario är att branden inträffar i en byggnad på samma avstånd från brandstationen, men med där byggnaden har ett automatiskt brandlarm och då tar det bara 20 minuter innan branden är släckt.

Exemplet illustrerar vilken aktör förmågebedömningen gäller för, d.v.s. Räddningstjänsten, vilken uppgift det är fråga om, d.v.s. släcka bränder, vilka faktorer som påverkar möjligheten att utföra uppgiften, d.v.s. vägarnas

[12] Förmågebedömningen kan gärna kompletteras med en beskrivning av vad uppgiften i praktiken innebär.

tillgänglighet etc., samt vilka riskscenarier som kan bli resultatet då aktören genomför uppgiften under de givna förutsättningarna. I samband med scenariobeskrivningarna ges också en beskrivning av konsekvenserna i termer av de attribut som konsekvenserna skall mätas, vilket i exemplet ovan var tiden från brandstart tills branden släckts.

3.4 Olika typer av system

Utöver att de olika metoderna för risk- och sårbarhetsanalys skiljer sig åt, inriktar de sig även på olika system (se föregående avsnitt). Dessa kan delas in i ett antal olika *systemtyper*. Det bör noteras att ”system” i det här sammanhanget syftar på en modell av verkligheten, vilket diskuteras mer utförligt i kapitel 2.

Indelningen i de olika typerna av system är gjord utifrån ett komplexitetsperspektiv, d.v.s. grad av komplexitet. Med komplexitet avses här storleken på systemens riskscenariorymder, mängden tillståndsvariabler samt beroenden mellan dessa. Det bör noteras att komplexiteten avser systemmodellen som representerar verkligheten och inte verkligheten i sig. Ett tekniskt system i det här sammanhanget är alltså en systemmodell som enbart innehåller element som är tekniska komponenter, eller andra artefakter.

3.4.1 Tekniskt system

De metoder för risk- och sårbarhetsanalys (framförallt riskanalys) som kan betraktas som traditionella eller etablerade, exempelvis felträdsanalys, händelseträdsanalys och FMEA, används ofta för system som kan beskrivas som *tekniska* system. Detta innebär att elementen i systemet till stor del är artefakter, d.v.s. föremål fabricerade av människor, och att människor inte finns med i systemet. Exempel på ett område där denna typ av system förekommer är riskanalyser för processindustrin. En analys av ett tekniskt system kan exempelvis handla om hur ofta man kan förvänta sig utsläpp från en kemisk industri. Det system som modelleras kan då bestå av rör, pumpar, ventiler, tankar, o.s.v. och riskscenariorymden består då av olika kombinationer av fel i komponenterna som eventuellt leder till utsläpp av något ämne.

Den verkliga motsvarigheten till dessa system är inte renodlat tekniska eftersom operatörer har en stor påverkan på hur sådana system fungerar. Detta är dock inte väsentligt för att avgöra om systemet (d.v.s. modellen av verkligheten) är teknisk eller socioteknisk. För att göra det är det bara relevant att undersöka vilka typer av element som förekommer i systemet (modellen) och om inga människor förekommer utan bara tekniska komponenter är det ett tekniskt system. En helt annan frågeställning har att göra om det är *lämpligt* att modellera verkligheten som ett tekniskt system (se avsnitt 3.1.8).

Riskanalyser för tekniska system utgår ofta från en beskrivning av systemet, exempelvis en ritning som visar hur rör, ventiler, pumpar, etc. är sammankopplade.

Utifrån denna systembeskrivning kan man sedan identifiera olika riskscenarier som ofta bygger på tillståndsförändringar i systemets olika komponenter, exempelvis ”Pump 1 slutar fungera”. Analyserna är *systembaserade* i bemärkelsen att en beskrivning av systemets element och elementens inbördes relationer är centralt för att analysera de olika riskscenarierna. Detta innebär dock inte att en fullständig beskrivning av systemet måste finnas då analysen inleds. Exempelvis kan en FMEA inledas med kunskap om något delsystem i en komplicerad process och med utgångspunkt i detta delsystem identifieras andra delsystem som är relevanta för det ”totala systemets” funktion. En systembaserad analys innebär snarare att en kartläggning av systemets tillståndsrymd fyller en central funktion för att kunna identifiera olika riskscenarier. Ett *scenariobaserat* angreppssätt fokuserar å andra sidan på att ta fram olika möjliga scenarier i stället för på att kartlägga systemets delar och deras möjliga tillstånd.

Det som karaktäriserar risk- och sårbarhetsanalyser för tekniska system är att:

- Analysen vanligtvis är systemorienterad, d.v.s. man utgår från systemets tillståndsrymd när man beskriver riskscenariorymden.
- Konsekvenserna som är av intresse är relaterade till funktionen hos det tekniska systemet, eller till det tekniska systemets påverkan på omgivningen.
- Människor inte finns med i systemet.

3.4.2 Tekniskt system med operatörer (enklare sociotekniskt system)

Eftersom människor kan reagera på en stor mängd olika aspekter i sin omgivning tenderar komplexiteten i en analys att öka om man förutom det tekniska systemet också explicit beaktar operatörer och deras handlande. Dessutom har människan ett minne som innebär att tidigare erfarenheter och även tidigare delar av ett riskscenario kan ha betydelse för människans agerande vid en viss tidpunkt. Förutom detta kan människor normalt påverka mycket mer i ett system än vad exempelvis en pump kan göra. Sammantaget gör detta att det kan vara svårt att göra en adekvat beskrivning av tillståndsrymden.

Inom området Human Reliability Aanalysis (HRA) skiljer man mellan första och andra generationens modeller för mänskligt felhandlande. Den första generationens modeller är fokuserade på att ta fram sannolikheter för att mänskliga felhandlingar uppstår givet en viss uppgift medan den andra generationens modeller mer betonar att det är kontexten i vilken handlingarna utförs som är viktig för att avgöra sannolikheten att en uppgift utförs korrekt, inte själva uppgiften i sig. Med den terminologi som används här kan man säga att den andra generationens modeller innebär en utökning av tillståndsrymden eftersom man där måste beskriva kontexten i vilken människor utför olika handlingar. Exempelvis karaktäriserar man kontexten som en människa befinner sig i metoden Cognitive Reliability and Error Analysis Method (CREAM) genom att beskriva vilken grad av kontroll som operatörern har över situationen [30]. Graden av kontroll beskrivs med hjälp av en

fyrgradig skala och den kan bestämmas genom att studera ett antal faktorer som beror av kontexten som kallas Common Performance Conditions (CPC). Om man alltså vill använda den här modellen för att beskriva hur sannolika olika scenarier är (om operatören gör fel eller ej) måste tillståndsrymden utökas så att alla CPC finns med i modellen.

Det som karaktäriserar risk- och sårbarhetsanalyser för tekniska system med operatörer är att:

- Analysen vanligtvis är systemorienterad, d.v.s. man utgår från systemets tillståndsrymd när man beskriver riskscenariorymden.
- Konsekvenserna som är av intresse är relaterade till funktionen hos det tekniska systemet, eller till det tekniska systemets påverkan på omgivningen.
- Människor finns med i systemet. Analysen är fokuserad på deras förmåga att hantera ett eller flera tekniska system.

3.4.3 Sociotekniskt system utan responsorganisationer

Operatörers beteende och antalet sätt de kan påverka systemet begränsas av träning, standardiserade arbetsrutiner och professionell disciplin. Detta underlättar analysen av tekniska system med operatörer betydligt jämfört med om man skulle analysera mänskligt beteende i allmänhet [31]. Då analyser av tekniska system med operatörer genomförs är man också ofta primärt intresserad av det tekniska systemets funktion, vilket gör att beteende som inte påverkar det tekniska systemet är mindre intressant.

Om man däremot är intresserad av ett system där det finns en stor variation i vad människor kan (och förväntas) göra, där dessa människor kan vara högst olika, och där man dessutom primärt är intresserad av vad dessa människor gör eller råkar ut för, innebär detta en analyssituation som är betydligt mer komplex. Ett exempel på en sådan situation är då man är intresserad av en kommun eller en regions förmåga att stå emot någon typ av påfrestning och där konsekvenserna som är intressanta bland annat rör medborgarna, exempelvis antal döda personer till följd av påfrestningen.

I en sådan analys är det i princip omöjligt att modellera enskilda människor eftersom tillståndsrymden blir mycket stor för ett sådant system. Det finns dock undantag, exempelvis vissa epidemiologiska modeller. I stället för att modellera enskilda människor kan man ha tillståndsvariabler som på något sätt är en sammanslagning av många människors tillstånd. Ett exempel på en sådan tillståndsvariabel är ”antalet döda människor” då man analyserar farligt gods transporter genom samhällen.

Det som karaktäriserar sociotekniska system utan responsorganisationer är att:

- Konsekvenserna som är av intresse är ofta relaterade till människorna i systemet, och/eller till miljön.
- Människorna i systemet behöver inte vara operatörer av något tekniskt system.

3.4.4 Socioteknisk system med responsorganisationer

Med begreppet ”responsorganisationer” avses någon typ av organisation som har som uppgift att agera då något går fel i ett system. Ett exempel på en responsorganisation är räddningstjänstens operativa avdelning som åker ut för att släcka bränder.

Skillnaden i förhållande till systemtypen ”Socioteknisk system utan respons-organisationer” är att i den här typen av system modelleras aktörer som har till uppgift att lindra konsekvenserna av en oönskad händelse explicit. Skillnaden mellan en operatör, som också kan sägas ha till uppgift att lindra konsekvenserna av en oönskad händelse, och en aktör som tillhör gruppen responsorganisationer är att operatören även är involverad i den normala verksamheten i systemet och normalt bara kan påverka den del av systemet som motsvarar ett specifikt tekniskt system medan aktören vanligtvis kan påverka en betydligt större del av systemet.

Den här typen av system analyseras ofta med scenariobaserade metoder där konsekvenserna av ett eller flera riskscenarier bedöms genom diskussioner med flera olika aktörer.

Det som karaktäriserar sociotekniska system med responsorganisationer är att:

- Konsekvenserna som är av intresse är ofta relaterade till människorna i systemet, eller till miljön.
- Människorna i systemet behöver inte vara operatörer av något tekniskt system.
- Olika agenter som har som mål att lindra konsekvenserna av en händelse finns uttryckligen med i systemet.

3.4.5 Systemtypernas påverkan på risk- och sårbarhetsanalyser

Beskrivningarna av systemtyperna ger en möjlighet att diskutera vilka metoder för risk- och sårbarhetsanalys som är mest lämpliga att använda för de olika typerna. Detta kan sedan utgöra en utgångspunkt för diskussioner om problem som måste hanteras i risk- och sårbarhetsanalyser och krav som kan ställas på dessa. Det går förmodligen inte alltid att avgöra precis i vilken kategori som en specifik analys hamnar, men det är inte heller meningen. Systemtyperna kan ändå användas som en utgångspunkt för diskussioner om utmaningar som måste hanteras i en risk- och sårbarhetsanalys och förhoppningsvis kan de också leda till en utveckling av nya metoder som bättre svarar upp mot dessa utmaningar.

På sätt och vis representerar de olika systemtyperna olika grad av oenighet när det gäller hur risk- och sårbarhetsanalyser skall genomföras och vad som är en bra sådan. Det är troligtvis lättare att komma fram till vad som är en bra risk- och sårbarhetsanalys för ett tekniskt system än för ett sociotekniskt system med responsorganisationer. Metoderna som används för att analysera tekniska system är förhållandevis etablerade och har funnits under en lång tid. Analyser av tekniska system med operatörer har stora likheter med de analyser som genomförs för renodlat tekniska system. Även analyser av sociotekniska system utan responsorganisationer, kan genomföras med metoder som påminner mycket om de som används för att analysera tekniska system, exempelvis kvantitativ riskanalysmetodik (QRA) för analys av kemikalieutsläpp från processindustrier. I sådana analyser används exempelvis händelseträd och felträd och konsekvenserna som är av intresse rör hur många människor i omgivningen som drabbas av ett eventuellt utsläpp från en specifik fabrik. Detta innebär att människor som bor runt omkring anläggningen är en del av systemet och att påverkan på dem är av central betydelse för analysen. Analyser som genomförs för den sista systemtypen, d.v.s. Sociotekniskt system med responsorganisationer, påminner vanligtvis inte så mycket om de analyser som genomförs för tekniska system. För denna systemtyp är det troligtvis så att analyserna genomförs med ett större inslag av scenariobaserade metoder.

Två anledningar till att det är stor skillnad att genomföra en risk- och sårbarhetsanalys för ett tekniskt system och ett sociotekniskt system med responsorganisationer är förekomsten av en större mängd *beroenden och agenter* i den senare typen av system.

Beroenden innebär att tillståndet för en tillståndsvariabel påverkas av en eller flera andra tillståndsvariabler, vilket gör det svårt att förutsäga hur ett system utvecklas dynamiskt efter en specifik påfrestning. Ett förhållandevis litet antal beroenden är vanligtvis inga problem att hantera i risk- och sårbarhetsanalyser och det görs också i de traditionella metoderna. Exempelvis finns det i ett seriekopplat produktionssystem (alla komponenter måste fungera för att systemet skall fungera) beroenden mellan de olika komponenterna som innebär att om en komponent som är placerad före den aktuella komponenten i produktionssystemet går sönder så kommer inte heller den aktuella komponenten att kunna producera något. Detta är ett förhållandevis enkelt uppbyggt system och det är lätt att beskriva vad som händer om en sådan störning skulle ske. Om det däremot finns återkopplingar (feedback) i systemet som innebär att funktionen hos en komponent är beroende av en eller flera andra komponenter i systemet som i sin tur är beroende av den aktuella komponenten blir det svårare. Teoretiskt går sådana situationer att hantera genom exempelvis simuleringar där beroenden mellan olika tillståndsvariabler beskrivs med differentialekvationer. Ett exempel på en sådan metod är den Input-Output modell för att modellera störningar på komplexa infrastruktursystem som utvecklats av Haimes [27, 32, 33]. Att använda dessa metoder i praktiken, när man

förutom att analysera ett systems sårbarhet också är intresserad av att finna sätt att reducera sårbarheten, kan vara problematiskt eftersom de metoderna vanligtvis inte är speciellt detaljerade.

En agent innebär i det här sammanhanget ett element i systemet som har förmåga att interagera med sin omgivning, som har mål, minne, en uppsättning förmågor, mm. (se nästa kapitel för en mer detaljerad beskrivning). Vanligtvis avses en person eller en organisation. Då agenter förekommer i de system som analyseras ökar antalet beroenden och andra tillståndsvariabler som måste tas med i analysen. Dessutom utgör agenternas minne en aspekt som gör det svårt att skapa en representativ systemmodell eftersom en agents minne kan påverka hur denne agerar i en viss situation. Detta medför att scenariorymden och riskscenariorymden växer, vilket kan utgöra ett praktiskt problem vid analyser. Även om man kan beskriva beroenden mellan olika tillståndsvariabler (inklusive agenternas) med mycket små fel i förhållande till verkligheten, gör den stora mängden beroenden att felen till slut kan växa sig stora vilket gör det svårt att förutsäga hur systemet kommer att uppföra sig.

Beroenden och agenter diskuteras i nästa kapitel som avslutas med tre förslag på hur risk- och sårbarhetsanalyser kan genomföras för komplexa sociotekniska system.

4 Beroenden och komplexa adaptiva system

Fler beroenden i ett system innebär att scenariorymden och även riskscenariorymden blir större och det blir mer arbetskrävande att genomföra en analys. Det här kapitlet beskriver hur beroenden uppfattas från ett systemperspektiv och hur beroenden kan kartläggas. Vidare innehåller kapitlet också en kort presentation av vad som menas med ett *komplext adaptivt system* (KAS). KAS, och framförallt den terminologi som används då man studerar sådana system, är användbar även vid analys av olika systems förmåga att motstå påfrestningar. Kapitlet innehåller också ett antal exempel på verkliga påfrestningar för att illustrera en del av de begrepp och fenomen som diskuteras.

I kapitel 2 definieras system som en samling element som på något sätt bildar en helhet. Elementen är antingen *artefakter*, *agenter* eller *naturföremål*. Agenter har förmågan att interagera med sin omgivning inklusive andra agenter. Agenter kan reagera på saker som sker i dess omgivning och utföra mer eller minde målmedvetna handlingar. Vanligtvis har agenter en *geografisk position*, d.v.s. var agenten befinner sig; en *uppsättning förmågor*, d.v.s. hur agenten kan påverka världen runtomkring; och *minne*, d.v.s. de intryck som agent minns från sitt förflutna [34]. I det här sammanhanget kan en agent vara en person, men det kan även vara ett företag eller en statlig myndighet. När begreppet agent används i den här rapporten avses vanligtvis en organisation som har någon typ av funktion relevant för krishantering. Artefakter är föremål som skapats av människan, vilka agenter kan använda. Dessa föremål kan också ha förmågor och geografisk position, men de har vanligtvis inte egna mål. I detta sammanhang kan artefakter exempelvis vara resurser i form av reservkraftverk, fordon, sandsäckar, etc. Man kan även tänka sig en tredje klass av element, naturföremål, d.v.s. föremål som inte skapats av människan.

4.1 System och beroenden

Beroenden innebär i det här sammanhanget att tillståndet i en del av ett system påverkas av tillståndet i en annan del av systemet. Vanligtvis används begreppet för att indikera att störningar i en del av ett system fortplantar sig till andra delar. Det förekommer också att begreppet används för att indikera att vissa villkor måste vara uppfyllda för att exempelvis en organisation skall kunna utföra en viss krishanteringsuppgift, exempelvis att organisationen är beroende av en viss resurs för att utföra uppgiften. Beroenden är inte begränsade till organisationer utan kan även gälla tekniska system, exempelvis är telekommunikationssystem beroende av ström för att fungera.

I det här kapitlet kommer beroenden *mellan olika system* att diskuteras, vilket även kan betraktas som beroenden mellan *två element* i ett större system (beroende på hur man definierar systemavgränsningarna). Exempelvis kan elsystemet i en kommun betraktas som ett system och fjärrvärmesystemet som ett annat och man

kan diskutera beroenden mellan dessa, men det är också möjligt att definiera det system som man analyserar som att det innehåller både elsystemet och fjärrvärmesystemet.

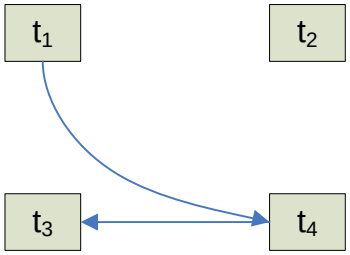
När begreppet beroenden används i det här kapitlet innebär det att ett elements tillstånd, d.v.s. den uppsättning tillståndsvariabler som beskriver det aktuella elementet (se kapitel 2), påverkar ett annat elements tillstånd. Beroenden kan exempelvis medföra att det *beroende* systemet inte fungerar som det är tänkt, alternativt har en nedsatt funktionsförmåga, om det system vilket det är *beroende av* inte fungerar, eller har en nedsatt funktionsförmåga. Att ett element är beroende av ett annat element innebär alltså att en eller flera tillståndsvariabler i elementen beror av varandra.

För att beskriva en tillståndsförändring i ett system används en pilsymbol, → (se avsnitt 2.6). Antag att ett system består av fyra tillståndsvariabler (t_1, t_2, t_3, t_4) och att dessa variabler kan anta värdena 1 eller 0. (0, 0, 1, 1) → (0, 0, 1, 0) betyder att om systemet befinner sig i det första tillståndet, d.v.s. två nollor och två ettor, ändras det till det andra tillståndet, d.v.s. tre nollor och en etta. Ett beroende mellan variablerna t_1 och t_4 kan illustreras med följande tillståndsförändringar:

(0, 0, 1, 1) → (0, 0, 1, 0)
(1, 0, 1, 1) → (1, 0, 1, 1)

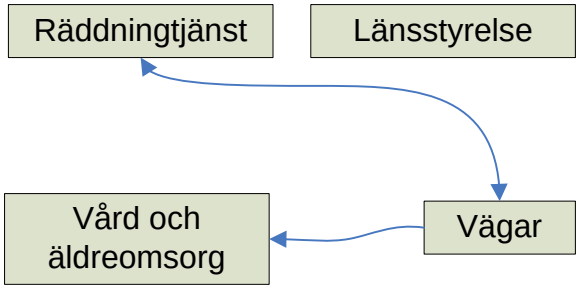
Enda skillnaden i tillstånden som systemet utgår från i de två tillståndsförändringarna är att t_1 i den första tillståndsförändringen har värdet 0 och i den andra har värdet 1. Denna skillnad gör dock att variabeln t_4 efter den första transformationen har värdet 0 och efter den andra transformationen har den värdet 1, alltså finns ett beroende mellan variablerna t_1 och t_4.

Beroenden i ett system kan illustreras med hjälp av ett diagram över de *omedelbara beroendena* mellan olika element eller tillståndsvariabler. Ett omedelbart beroende mellan tillståndsvariablerna t_1 och t_4 innebär att om t_1 ändras, och alla andra tillståndsvariabler i systemet hålls konstanta, så kommer t_4 också att ändras, alltså precis det som illustrerades ovan. Figur 8 illustrerar ett exempel på ett diagram över de omedelbara beroendena i ett system bestående av fyra tillståndsvariabler. Av diagrammet framgår att variabeln t_2 är oberoende av de andra variablerna, d.v.s. en förändring av någon av variablerna t_1, t_3 eller t_4 (alla andra variabler antas vara konstanta) resulterar inte i någon förändring av t_2. En förändring av t_2 resulterar inte heller i någon förändring av de andra variablerna.



Figur 8 *Illustration av omedelbara beroenden mellan fyra tillståndsvariabler.*

I praktiken är det troligare att ett diagram med de omedelbara beroendena konstrueras med hjälp av elementen, d.v.s. agenterna och artefakterna, i stället för med de olika tillståndsvariablerna. Ett exempel på detta illustreras i Figur 9 där omedelbara beroenden mellan fyra element, tre agenter och en artefakt, illustreras. Ett beroende mellan två element, exempelvis Räddningstjänst och Vägar, innebär att det finns en eller flera tillståndsvariabler som är associerade med elementet Räddningstjänsten och som påverkar en eller flera tillståndsvariabler som är associerade med Vägar.



Figur 9 *Illustration av omedelbara beroenden mellan fyra element i ett system.*

Förutom att illustrera de omedelbara beroendena mellan olika element eller tillståndsvariabler kan man också illustrera *slutliga beroenden*, vilket innebär att även alla beroenden som fortplantas via en/ett mellanliggande element eller tillståndsvariabel skall illustreras. I Figur 9 skulle detta innebära en extra pil mellan Räddningstjänst och Vård och äldreomsorg.

4.1.1 Olika typer av beroende

Man kan skilja på olika typer av beroenden [35]: fysiska beroenden, informationsberoenden (kallas även cyberberoenden), geografiska beroenden och logiska beroenden. Beroendena kan existera mellan olika element i ett system där ett element kan vara vad som i dagligt tal beskrivs som ett ”teknisk system”, exempelvis ett elsystem.

Fysiska beroenden innebär att det ena elementets funktion är materiellt beroende av det andra elementet. Exempelvis kan ett värmekraftverk vara beroende av pellets för att fungera. Om pellets levereras via någon typ av transportsystem kan kraftverket sägas vara fysiskt beroende av ett fungerande transportsystem.

Informationsberoenden innebär att ett element behöver information för att kunna fungera. Detta kan exempelvis röra sig om järnvägstransportsystemet där man är beroende av att veta var tåg befinner sig.

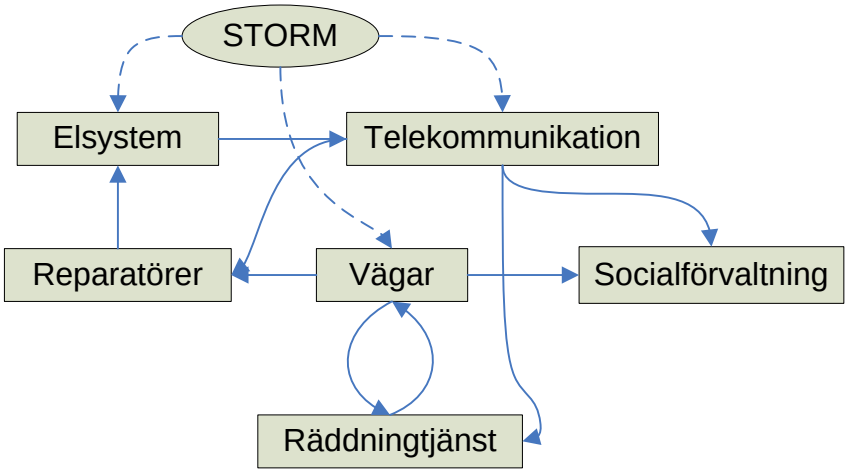
Geografiskt beroende syftar på att delar av två system kan vara geografiskt placerade nära varandra, vilket exemplifieras av branden i Akallatunneln den 29 Maj 2002 [36]. Akallatunneln innehåller komponenter från ett antal olika tekniska infrastruktursystem såsom vattenrör, fjärrvärmerör, Elkablar (11 kV, 33 kV och 110 kV), kablar för tele- och datakommunikation samt för styrfunktioner och övervakning. Branden började på samma plats som en tidigare brand i tunneln (11 Mars 2001) och allt pekar på att orsaken till branden var en skarv i en 33 kV-kabel. Branden pågick i ca 7 timmar och orsakade strömavbrott för 20 000 kunder och 30 000 arbetsplatser. I detta fall fanns ett geografiskt beroende mellan alla de tekniska system som var placerade i samma tunnel.

Logiskt beroende innebär att funktionen hos ett system påverkas av funktionen i ett annat system via en mekanism som varken kan klassas som fysiskt beroende, informationsberoende, eller geografiskt beroende.

Illustration av några beroenden vid stormen Gudrun
Den 8 januari 2005 drabbades södra Sverige av stormen Gudrun. Stormen illustrerar hur beroende samhället är av el och telekommunikation. I takt med att stormen drog fram över landet slogs strömmen ut för omkring 730 000 elkunder, och 250 000 kunder i det fasta telefonnätet drabbades av avbrott [37]. Ledningen av reparationsarbetet försvårades av att fast och mobil telekommunikation i stora delar av det aktuella området var utslagen, samt att de träd som hade blåst ner på vägar och i terrängen gjorde reparationsarbetet svårare [37, 38] (s16, s1). Framkomlighetssvårigheterna påverkade också socialförvaltningens och räddningstjänstens insatser och räddningstjänsten fick avdela stora resurser till att försöka röja vägar i det stormdrabbade området.

Dessa beroenden illustreras i Figur 10, vilken visar att vägarna har en central roll eftersom reparatörer, räddningstjänst och socialförvaltningen är beroende av dem för att utföra sina uppgifter. Vidare gör vägarnas negativa påverkan på reparationsarbetet att elsystemet inte kommer igång så snabbt som det annars skulle ha gjort, vilket i sin tur leder till att telekommunikationen påverkas och försämrar socialförvaltningens och räddningstjänstens förmåga att utföra sina uppgifter. Stormen är inte en del av systemet utan en påfrestning på systemet som

åstadkommer en förändring av systemets tillstånd och därför illustreras den med en oval form och dess påverkan på systemet illustreras med streckade pilar.



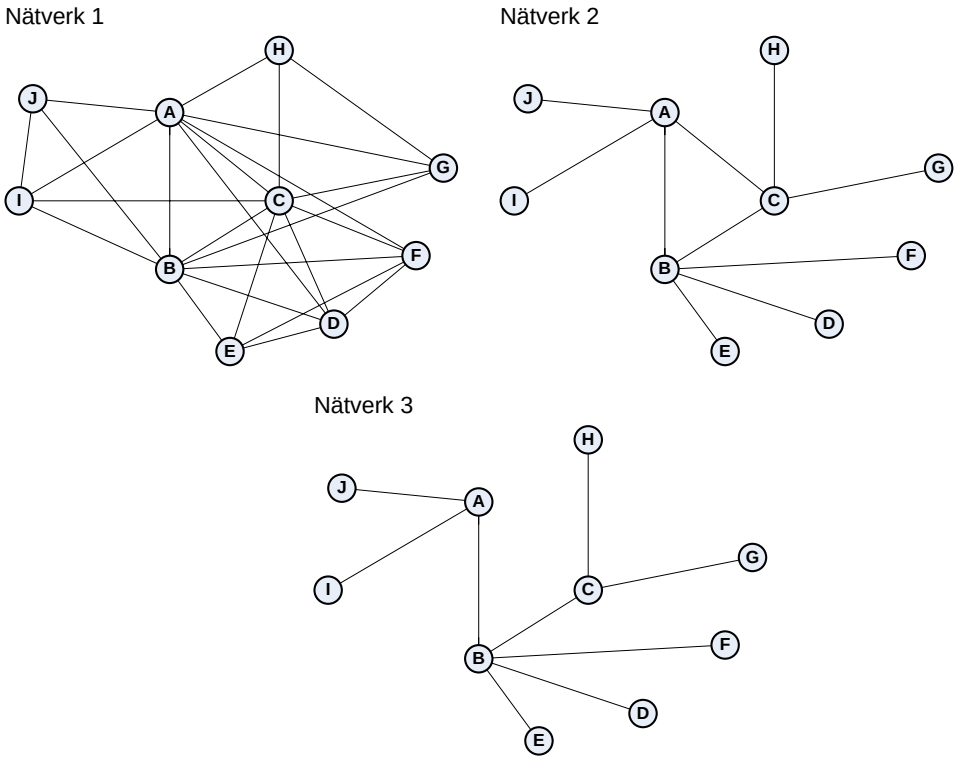
Figur 10 *Illustration av några beroenden under stormen Gudrun.*

En viktig aspekt av risk och sårbarhet i olika system är förekomsten av komplexa interaktioner [39]. Att ett system har många delar utgör inget problem i en risk- och sårbarhetsanalys så länge delarna interagerar linjärt med varandra. Linjära interaktioner exemplifieras bäst med en produktionslinje där alla moment utförs sekventiellt, d.v.s. efter varandra. Om problem uppstår med någon del i ett sådant system är det lätt att förstå vad som kommer att hända längre ner i produktionslinjen. Det kommer inte att finnas något material att jobba med, och uppåt i produktionslinjen kommer material att börja ansamlas om inte produktionen stoppas. Om däremot vissa delar av produktionslinjen har flera funktioner blir problemet med att förstå konsekvenserna av ett stopp någonstans i systemet inte lika enkelt. I exemplet med stormen Gudrun utgjorde vägarna en resurs för flera aktörer (räddningstjänst, reparatörer, socialförvaltningen) och när framkomligheten på vägarna reducerades påverkades alltså fler än bara en aktör. Detta är ett exempel på mer komplexa interaktioner. Att framkomliga vägar var en viktig förutsättning för många som var involverade i krishanteringsarbetet var kanske väntat, men de effekter som detta gav upphov till i och med att många aktörer påverkades kan mycket väl vara oväntade. Det finns sannolikt en hel del, ur ett krishanteringsperspektiv, viktiga beroenden som inte är kända idag eller som bara ett begränsat antal människor eller organisationer känner till. En organisation kan exempelvis ha kunskap om vad som påverkar dess förmåga att fungera, men kanske inte om vilka som i sin tur är beroende av dem. Detta är något som olika myndigheter uppmärksammat som ett problem i arbetet med risk- och sårbarhetsanalyser [40] (s. 84). Även om organisationer har kunskap om det har man ändå vanligtvis bara *lokal information*, d.v.s. bara kunskap om dess absoluta närhet, inte den *globala information* som ofta behövs för att kunna bedöma

effekterna av störningar i ett större sammanhang (system). Global och lokal information kan illustreras bättre genom att använda *nätverk*, vilket nästa avsnitt handlar om.

4.1.2 Nätverk

För att illustrera beroenden mellan olika delar av ett system kan man använda sig av nätverk. Nätverk kan dock användas för andra ändamål än att kartlägga beroenden och därför är det mer passande att använda begreppet *relationer* när man diskuterar nätverk. Beroenden kan sägas vara en typ av relation mellan två delar i ett system. I Figur 10 illustrerades några av de beroenden som var relevanta under stormen Gudrun i ett riktat nätverk. I ett sådant nätverk har relationerna en riktning, d.v.s. de går från en nod till en annan. I ett oriktat nätverk kan man bara se om en relation finns mellan två noder, den har ingen riktning. De relationer som sammanbinder noderna kallas länkar. Noder kan, beroende på vilket system man studerar, exempelvis vara personer, komponenter i ett tekniskt system eller organisationer. I Figur 11 illustreras tre oriktade nätverk bestående av 10 noder.



Figur 11 Illustration av tre nätverk.

När det gäller sårbarhetsanalyser är man ofta intresserad av att undersöka ett systems funktion då någon typ av påfrestning på systemet inträffar. Antag att de

nätverk som illustreras i Figur 11 representerar någon typ av tekniskt system där det är önskvärt att de olika noderna är sammankopplade. Sårbarheten i systemet kan analyseras genom att undersöka vad som händer då man slår ut en eller flera noder, vilket i ett elsystem skulle kunna vara olika fördelningsstationer. Om man studerade ett vägnät skulle det kunna vara vägkorsningar. I figuren syns att Nätverk 1 har många länkar i förhållande till noder och intuitivt verkar inte detta nätverk speciellt sårbart för utslagning av någon nod. Oavsett vilken nod man slår ut kommer de kvarvarande att vara i kontakt med varandra. Om man däremot betraktar Nätverk 2 ser man att nätverket är betydligt mer sårbart för utslagning av noder än det första. I nätverk 2 finns en ”kärna” av tre noder (A, B och C) som sammanbinder nätverket och om man skulle slå ut någon av dem skulle minst två noder förlora kontakten med det övriga nätverket. Detta skulle i ett elnät innebära att abonnenter som är kopplade till de noder som förlorar kontakten med nätverket förlorar sin ström. I ett vägnät innebär det att vissa delar inte kan nås av exempelvis räddningstjänsten.

I Nätverk 2 var noderna A, B och C ungefär lika viktiga för sårbarheten (hur många noder som förlorar kontakten med nätverket), men i Nätverk 3 är nod B viktigare än både A och C. Om någon av nod A eller C slås ut kommer nätverket att delas upp i tre bitar (en med sju noder och två med en nod), om däremot nod B slås ut kommer nätverket att delas upp i fem mindre bitar (två med tre noder och tre med en nod).

För att kunna göra analyser av sårbarhet i ett system med hjälp av nätverk måste man först kartlägga systemet. På senare tid har det skett en dramatisk ökning av antalet kartläggningar, och analyser, av olika typer av system med nätverksstruktur. Alltifrån tekniska nätverk, såsom elnätverk och tunnelbanenätverk, till biologiska och sociala nätverk har kartlagts. I takt med denna utveckling har det blivit allt tydligare att även om de olika nätverken representerar olika typer av system har de ibland stora likheter när det gäller uppbyggnad, inte minst när det gäller deras egenskaper avseende sårbarhet.

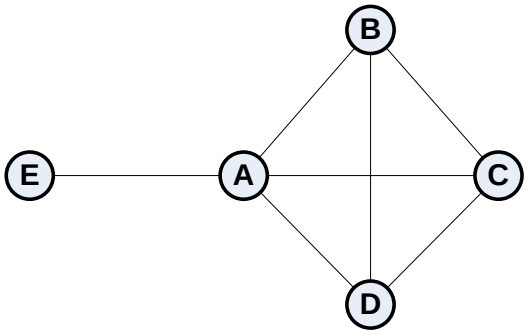
I mitten av 1900-talet lade två matematiker, Paul Erdős och Alfréd Réniy grunden till en modell av nätverk (grafer) som kallas slumpmässiga grafer. Modellen går ut på att man tar ett antal noder och sedan kopplar ihop noderna slumpmässigt med hjälp av ett visst antal länkar. Denna modell av hur ett nätverk bildas har en del egenskaper som är av intresse om man är intresserad av sårbarhet. Framförallt blir det intressant då man studerar hur sammanhängande grupper av noder, eller *kluster*, bildas i den här typen av nätverk. När man har få länkar i förhållande till noder kommer det inte att finnas några stora kluster. De flesta noder kommer att vara isolerade från varandra och de kluster som finns kommer vanligtvis att bestå av endast två noder. När fler länkar slumpmässigt läggs till kommer fler kluster att uppstå, en del kommer att vara lite större, men de flesta kommer fortfarande att vara relativt små. Då man lagt till ett visst antal länkar kommer intressanta saker att

börja hända med nätverket, plötsligt uppstår ett stort kluster som binder ihop en stor del av noderna i nätverket. Detta fenomen kallas fasövergång inom fysiken. Nätverk och fasövergångar är relevanta för studier av samhällets sårbarhet och det illustreras på ett bra sätt om man tänker sig att noderna i ett nätverk representerar människor och länkarna representerar kontakter vid vilka sjukdomar kan spridas mellan två personer. I detta fall vill man inte att någon större sammanhängande grupp av noder skall bildas eftersom det skulle innebära att en majoritet av befolkningen skulle smittas (om sjukdomen är mycket smittsam).

Ett problem med Erdős och Réniys modell när det gäller att modellera verkliga nätverk är att den förutsäger att det är lika troligt att nod A:s granne, nod B, har en länk till nod A:s andra granne, nod C, som att nod B har en länk till vilken annan nod som helst i nätverket. Om man tänker sig ett socialt nätverk där noderna är personer och där länkarna symboliserar vänskap inser man att den slumpmässiga grafmodellen inte är en bra modell för den typen av relationer. Personliga relationer är inte slumpmässiga och i ett sådant socialt nätverk är det mycket troligare att person A:s vän, person B, är vän med person A:s andra vän, person C, än att han eller hon är vän med någon slumpmässigt vald person i världen. Även i andra typer av nätverk än sociala nätverk uppträder sådana tydliga *kluster* av noder.

För att mäta gruppering bland noder som är nära varandra introducerade Watts och Strogatz [41] ett mått som kallas *klustringskoefficient*. Klustringskoefficienten beräknas för en nod genom att räkna antalet av dess grannar som också är kopplade till varandra och sedan dividera detta tal med antalet *möjliga* kopplingar mellan grannarna. Om en nod är isolerad, d.v.s. inte har några länkar till andra noder, eller om den bara har en länk har den klusterkoefficienten 0.

För att beräkna klustringskoefficienten för nod A i nätverket som illustreras i Figur 12 räknar man först hur många länkar som finns mellan nod A:s grannar, d.v.s. 3 (B-C, C-D, B-D). Sedan räknar man ut hur många länkar som skulle kunna ha funnits mellan grannarna, d.v.s. 6 (B-C, C-D, B-D, samt E-B, E-C, E-D). Nod A:s klustringskoefficient är alltså 0,5 och på samma sätt kan man räkna ut de övriga nodernas klustringskoefficienter. Nod B, nod C och nod D har alla klustringskoefficienten 1 och nod E har klustringskoefficienten 0.



Figur 12 Illustration av ett enkelt nätverk.

Klustringskoefficienten går också att mäta för ett helt nätverk och då använder man sig av medelvärdet av alla noders klustringskoefficienter. Nätverket i Figur 12 har klustringskoefficienten 0,7. Eftersom klustringskoefficienten för en nod kan variera mellan 0 och 1 kommer även klustringskoefficienten för ett nätverk att kunna variera mellan 0 och 1.

Genom att mäta klustringskoefficienten för ett antal verkliga nätverk kunde Watts och Strogatz konstatera att hög grad av klustring inte var en egenskap som bara fanns i sociala nätverk, den fanns i allt från tekniska till biologiska nätverk. Den typ av nätverk som Watts och Strogatz hittade kallade de för ”Small worlds” och det är en typ av nätverk där klustringskoefficienten är relativt hög, men där det samtidigt är förhållandevis korta avstånd mellan de olika noderna. Avståndet mellan två noder mäter man genom att räkna hur många länkar man måste följa för att komma från den ena till den andra noden. Avståndet mellan nod E och Nod C i Figur 12 är 2. Det som var förvånande med Watts och Strogatz upptäckt var inte att det fanns nätverk med korta avstånd (i förhållande till antalet noder), eller att det fanns nätverk med hög grad av klustring, utan att båda egenskaperna kunde finnas i samma nätverk. I uppsatsen som Watts och Strogatz publicerade i tidskriften *Nature* visar de att ”små världar” finns i nätverk som representerar elnätet i nordvästra USA (ett teknisk nätverk), i den lilla masken *Caenorhabditis Elegans* neurala nätverk (ett biologiskt nätverk) samt i ett nätverk av Hollywoodskådespelare där länkar mellan skådespelarna representerar att de spelat i samma film (ett socialt nätverk). För att kunna generera nätverk som har liknande egenskaper som de nätverk man hittade i verkligheten skapade Watts och Strogatz en modell som går ut på att man börjar med ett nätverk i vilket alla noder är sammankopplade med sina närmaste grannar, d.v.s. en hög klustringskoefficient. Sedan går man igenom alla länkar i nätverket och med en viss sannolikhet p kopplar man om dem slumpmässigt i nätverket. Med hjälp av denna modell kan man skapa nätverk som antingen är helt regelbundna gitter (alla noder är kopplade till sina närmsta grannar) om $p = 0$, eller slumpmässiga nätverk om $p = 1$. Om sannolikheten att koppla om en länk ligger någonstans mellan 0 och 1 kan man

skapa modeller av små världar, d.v.s. nätverk som har hög klustring, men samtidigt korta avstånd mellan noderna.

Watts och Strogatz modell för nätverk gör att man kan generera nätverk som liknar de som har hög klustringskoefficient och korta avstånd, men det finns ytterligare en egenskap som uppkommer i många verkliga nätverk som den modellen inte kan generera – vissa noder i verkliga nätverk har extremt många länkar i förhållande till de andra noderna.

1999 publicerade Albert-László Barabásis forskargrupp en uppsats i tidskriften *Nature* som heter *Internet: Diameter of the World Wide Web* [42]. I uppsatsen redovisar gruppen sina resultat från undersökningar av Internet, eller World Wide Web. Gruppen samlade in information om hur sidor på Internet länkar till varandra, vilket kan illustreras som ett (riktat) nätverk. I sin analys av materialet fann de att fördelningen av antalet ingående och utgående länkar från webbsidor följer en så kallad ”power law”, d.v.s. en liten del av webbsidorna har en majoritet av länkarna. Vid en senare analys av 203 miljoner webbsidor visade det sig att dessa centrala webbsidor, eller *hubbar*, var ungefär tre stycken och att nära en miljon andra webbsidor refererade till var och en av dessa. 90% av webbsidorna i undersökningen hade 10 eller färre länkar som refererade till dem [43](s.58). En sådan skev fördelning av antalet länkar i ett nätverk får man varken med den traditionella slumpmässiga grafmodellen, eller med ”small world”-modellen. Uppenbarligen var det en annan process än en rent slumpmässig som genererade dessa nätverk.

Barabási och hans grupp föreslog en ny modell för hur nätverk bildas som kan generera så kallade *skalfria* nätverk, d.v.s. den typ av nätverk där ett fåtal noder har majoriteten av länkarna [44]. Den modellen bygger på att nätverk växer och att när nya noder läggs till nätverket är det större sannolikhet att dessa noder kopplas ihop med noder som redan har många länkar än med dem som har få länkar. Denna process, som gör att den nod som redan har många länkar har större sannolikhet att få fler, leder till den typ av fördelning som observerades för internetlänkarna.

Det visar sig att många verkliga nätverk är skalfria. Exempel på det är nätverket av skådespelare i Hollywood (ett fåtal skådespelare har spelat mot väldigt många andra) [43](s73), det sexuella nätverket mellan folk i åldrarna 18 till 74 år i Sverige (ett fåtal personer har haft den största delen av de sexuella kontakterna) [45] och det nordamerikanska elnätet [46].

När sårbarhet studeras i nätverk brukar måttet på sårbarhet som används ha att göra med hur ”sammankopplat” nätverket är, exempelvis nätverkets *diameter* vilken definieras som den längsta av alla kortaste vägar mellan nätverkets nodpar. För att simulera påfrestningar på ett nätverk och mäta sårbarheten använder man sig vanligtvis av *slumpmässiga attacker* eller *riktade attacker* på noder eller länkar.

Detta motsvarar ett antal riskscenarier enligt den operationella definitionen av sårbarhet, se kapitel 2. Allt eftersom man simulerar attacker mot ett nätverk mäter man hur sammankopplingen av nätverket ökar eller minskar. Sårbarheten i nätverket kan sedan analyseras genom att studera hur stor del av nätverket som måste förstöras för att åstadkomma en viss reduktion i nätverkets sammankoppling, eller hur stor påverkan på nätverkets sammankoppling ett visst riskscenario har.

Slumpmässiga attacker kan användas för att slå ut antingen noder eller länkar i ett nätverk. Dessa attacker efterliknar ”vardagsfel” i ett nätverk, d.v.s. det finns ingen tanke bakom attackerna utan de inträffar slumpmässigt. Riktade attacker däremot är tänkta att simulera en attack där någon avsiktligen attackerar delar av nätverket som är viktigt för den totala funktionen hos nätverket. I exempelvis ett elnät kan slumpmässiga attacker mot noder representera slumpmässiga fel i olika fördelningsstationer och riktade attacker mot noder är riktade mot de punkter i elnätet som gör störst skada.

Vid undersökningar av hur sårbara olika nätverk är för riktade och slumpmässiga attacker har det visat sig att beroende på nätverkens struktur kan de uppvisa betydande olikheter i deras förmåga att motstå attacker [47]. De skalfria nätverken (många verkliga nätverk) är mycket robusta mot slumpmässiga fel, d.v.s. nätverkets funktion påverkas inte speciellt mycket då noder attackeras slumpmässigt. När man däremot attackerar de skalfria nätverken med riktade attacker mot de noder som har de flesta länkar, d.v.s. hubbarna, är nätverken mycket sårbara.

Även andra, mer sofistikerade, attackstrategier har använts för att undersöka nätverks sårbarhet. Holme m.fl. [48] visar en analys av ett antal nätverk där man använder 8 olika attackstrategier, fyra för att attackera noder och fyra för att attackera länkar. Av de fyra strategierna för att attackera länkar respektive noder är två baserade på mått som beräknats från ursprungsnätverket, d.v.s. så som det såg ut innan man började attackera det och två som baseras på att man kontinuerligt räknar om måtten. De två måtten som används är *intermeditet* och *grad*. Intermeditet är ett mått på hur många kortaste vägar mellan noder i nätverket som passerar den aktuella noden eller länken. Grad är ett mått på hur många länkar en nod har kopplade till sig och för länkar är det ett mått på hur många länkar de noder som länken sammanbinder har kopplade till sig. En slutsats som man drar från analysen är att de attackstrategier som går ut på att kontinuerligt räkna om måtten är mer effektiva för att förstöra nätverket än de som bygger på mått beräknade på det ursprungliga nätverket.

Det har publicerats en hel del undersökningar där man analyserat olika sätt att avgöra hur sårbart olika nätverk (både verkliga och fiktiva) är för olika typer av attacker. Ett av användningsområdena som i högsta grad är relevant för samhällets risk- och sårbarhetsanalyser är analyser av elnätverk [46, 49]. Sådana analyser har

även genomförts i Sverige [50, 51]. Analys av smittspridning har också genomförts med hjälp av nätverksteori. Angreppssättet påminner mycket om det som används för att se hur sårbart ett nätverk är, skillnaden när man analyserar smittspridning är att det är önskvärt att få nätverket att falla sönder (noderna representerar personer och länkarna potentiella spridningsvägar).

4.1.3 Betydelsen av sociala nätverk för krishantering

Teknisk infrastruktur är relativt lätt (förutsatt att det finns korrekta ritningar/kartor tillgängliga) att kartlägga i form av nätverk, betydligt svårare är det att kartlägga sociala nätverk. Sociala nätverk, d.v.s. relationer mellan människor, kan dock vara mycket viktiga för sårbarheten i en kommun, region eller företag. Det här avsnittet diskuterar hur två exempel på sociala nätverk kan påverka krishantering.

Ett exempel på hur sociala nätverk mellan olika organisationer kan bidra till att mildra effekterna av en olycka som skulle kunna ha utvecklats till en mycket allvarlig kris är en brand som uppstod hos biltillverkaren Toyota. Redogörelsen är hämtad från [52-54].

Den 1 februari 1997 brann en fabrik som tillhörde Toyotas underleverantör av så kallade proportioneringsventiler (eng. proportioning valves), eller P-ventiler. Innan branden hade man producerat omkring 32 000 ventiler per dag och de användes i nästan alla fordon tillverkade av Toyota. Två aspekter som gjorde branden till en potentiell katastrof av gigantiska mått var att Toyota bara hade en enda leverantör av P-ventiler, företaget Aisin Seiki, och att man bara hade motsvarande 2 dagars produktion med ventiler i lager. Eftersom ventilerna är nödvändiga komponenter i samtliga fordon innebar detta att all produktion hos Toyota samt hos större delen av deras underleverantörer riskerade att stoppas för en mycket lång tid framöver. Med en planerad produktion av ungefär 15 000 bilar per dag stod det snart klart för de inblandade att branden hade potential att orsaka enorm skada.

I branden förstördes samtliga av de verktyg som användes för att göra ventilerna, och Aisin och Toyota insåg att de inte skulle klara att hantera krisen själva utan skulle behöva hjälp från andra företag. Redan innan branden slocknat organiserade man ett krishanteringscenter och gick ut med en förfrågan om hjälp till företag i Toyota-gruppen och underleverantörer. Man fick snabbt svar, och det visade sig att 62 företag kunde hjälpa till med att försöka producera ventiler och ytterligare 150 företag blev engagerade i arbetet eftersom de 62 som skulle producera behövde nya verktyg för att göra ventilerna. Av de företag som hjälpte till med produktionen hade bara ett fåtal erfarenhet av att producera ventiler. De flesta hade ingen erfarenhet alls av sådan tillverkning och vissa, exempelvis symaskinstillverkaren Brother Industries, hade aldrig tillverkat bildelar. Utsikterna för att produktionen av ventiler skulle kunna komma igång snabbt såg ganska mörka ut, underleverantörerna saknade lämpliga verktyg, de flesta hade aldrig tillverkat ventiler, och de var dessutom ovana vid kriser av den omfattning som de stod inför.

Förutom dessa svårigheter blev Aisins krishanteringscenter snabbt överbelastat med problem och kunde i princip inte hjälpa de olika underleverantörerna med produktionen av ventiler.

Förvånande nog lyckades Toyota och deras underleverantörer komma igång med produktionen bara tre dagar efter branden, och en vecka efter branden var produktionsvolymerna i fabrikerna normala.

Analysen av branden hos Aisin visar på att sociala relationer kan vara mycket betydelsefulla för krishantering. Watts [53] påpekar att det förvånande med krisen inte var att alla underleverantörer av allt från symaskiner till faxmaskiner *ville* hjälpa till utan att de *kunde* göra det. Med ungefär 200 företag inblandade i arbetet med att producera ventiler, utan någon betydande central ledning, är det inte svårt att föreställa sig att det mycket väl kunde ha slutat i kaos. Det gjorde det dock inte. I efterhand konstaterades att en avgörande faktor för den lyckosamma utgången av branden var att personer ofta flyttade runt mellan företagen och att det fanns ett väl utvecklat kontaktnät mellan personer på de olika företagen, eller som före detta Toyota anställde Masakazu Ishikawa, numera vice VD för Somic Ishikawa Inc. uttryckte det:

> "Suppliers never asked Toyota or Aisin what they would be paid for rushing out the valves, says Somic's Mr. Ishikawa. 'We trusted them.'" [54]

Toyotabranden visar på vikten av förtroende mellan personer i olika organisationer, vilket ger möjligheter till effektivare kommunikation och flexibilitet. Krackhardt och Stern [55] noterar att för att få en organisation att anpassa sig och bemöta en kris krävs mer samarbete inom organisationen än normalt. Om man antar att förtroende mellan personer förbättrar samarbetsförmågan är det önskvärt att personer *inom* olika organisationsdelar, men framförallt *mellan* olika delar har förtroende för varandra. Författarna noterar också att eftersom en vänskapsrelation ofta inkluderar att man har förtroende för personen i fråga är det önskvärt att folk i olika delar av en organisation, eller olika organisationer som skall samarbeta i händelse av en kris, känner varandra.

Om man översätter resonemanget ovan till krishantering i svenska kommuner/regioner skulle man kunna komma fram till att förtroende mellan personer som jobbar på olika avdelningar inom en kommun, men också mellan olika organisationer som kan vara aktuella för krishanteringsarbetet (exempelvis polis, länsstyrelse, etc.), är viktigt för hur dessa organisationer kommer att kunna samarbeta vid en kris.

Toyotabranden illustrerar ytterligare en aspekt av kriser som är av intresse för den här rapporten. När man läser om branden och det jobb som genomfördes för att återställa produktionen är det lätt att förbryllas över att styrningen och koordineringen av insatsen inte var centraliserad och att Toyota inte hade någon

välutvecklad beredskapsplan för denna typ av händelse. Visserligen sattes ett krishanteringscenter upp på Aisin redan första dagen, men efter att detta center skickat ut ett ”nödrop” till olika firmor tillsammans med ritningar på samtliga ventiler som behövde produceras blev man så överbelastad att alla företag som hjälpte till i produktionen fick klara sig själva utan central styrning:

> “Finally, in the first few days of the crisis, Aisin was in a state of chaos and was difficult to contact. Indeed, so confused were conditions at Aisin that during the evening of the first day of the fire, Taiho Kogyo's director of production control was wrongly informed that master cylinders, not P-valves, were the main problem for Aisin. Within days, Aisin installed 250 additional fixed phones and 300 mobile phones in an attempt to accommodate skyrocketing inquiries. The magnitude of incoming calls, however, overwhelmed Aisin's capacity to respond.
>
> Because Aisin lacked sufficient resources to provide direct assistance to every firm at once, collaborating firms had to figure out by themselves how to program their machining centers for P-valve production and find or make appropriate drills.”
>
> “Although Aisin supported these efforts as much as it could by setting up a 'drill center' to coordinate drill purchases and by organizing meetings to discuss technical problems and solutions, firms had to rely largely on their own capabilities to begin P-valve production.”[52]

Arbetet med att producera ventilerna utvecklades alltså som en följd av de individuella firmornas (människornas) handlingar som fattades baserat på *lokal information*, d.v.s. de kände inte till vad som skedde hos majoriteten av de övriga inblandade firmorna. Detta är ett exempel på *självorganisation* i ett *komplext system*, vilket i det här fallet ledde till *emergenta* (eng. emergent) egenskaper, d.v.s. egenskaper hos systemet som var mer eller mindre oförutsedda och inte kan förstås bara genom att studera de individuella komponenterna (i det här fallet de enskilda firmorna).

Komplexa system, självorganisation och emergenta egenskaper diskuteras senare i rapporten, men först presenteras ett exempel på hur sociala nätverk kan bidra till att förvärra en kris i stället för att hjälpa till att lösa den.

Det kanske mest aktuella exemplet på hur sociala nätverk kan bidra till eskaleringen av en krissituation utgörs av risken för en global pandemi, d.v.s. en världsomfattande epidemi. Tidigare i rapporten har det påpekats att de skalfria nätverken, d.v.s. de som har ett fåtal noder med en stor andel av nätverkets totala länkar, är mycket robusta mot slumpmässiga fel (se avsnitt 4.1.2). Trots att en stor del av noderna slagits ut är den resterande delen fortfarande ihopkopplad. I det fall nätverket utgörs av ett elnät vill man att det skall fortsätta att vara ihopkopplat,

men om nätet i stället är ett nät som representerar smittspridning mellan personer så vill man att nätet så snabbt som möjligt skall brytas upp i mindre delar. Därför vore det illa om ett nätverk som representerade möjliga smittspridningsvägar hade en skalfri struktur i stället för exempelvis en slumpmässig.

När det gäller sexuellt överförbara sjukdomar, exempelvis HIV/AIDS, är strukturen av så kallade sexuella nätverk av intresse, d.v.s. nätverk som visar vilka personer som har haft en sexuell relation. 2001 publicerades en uppsats av en gupp svenska och amerikanska forskare i tidskriften *Nature* [45]. I uppsatsen visar man resultaten av en analys av 2 810 svenskars sexuella kontakter. Fördelningen av sexuella kontakter hade en skalfri fördelning. Resultatet bekräftades senare i en liknande amerikansk undersökning och om det som dessa resultat indikerar stämmer för befolkningen i stort kan det mycket väl vara en orsak till varför AIDS blivit en epidemi som inte dött ut [43] (s.138).

Eftersom influensavirus kan spridas mellan människor utan att de behöver ha kroppslig kontakt (exempelvis via luften) blir antalet potentiella spridningsvägar mellan människor betydligt större än när det gäller sexuellt överförbara sjukdomar. Det är inte helt orimligt att tänka sig att ett nätverk för spridning av en influensaepidemi har en skalfri struktur. Om det skulle vara så behöver det dock nödvändigtvis inte vara dåligt för samhällets förmåga att skydda sig mot en epidemi. Om man bara kunde vaccinera de människor som står för en stor del av de potentiella smittspridningsvägarna (de som har många kontakter med andra människor) skulle nätverket mycket snabbt brytas upp och smittspridningen avstanna. Svårigheten med denna strategi är möjligtvis att hitta de personer som utgör ”hubbarna” i ett smittspridningsnätverk.

De två exemplen (Toyotabranden och smittspridning) visar att sociala nätverk kan spela en betydande roll för utvecklingen av en krissituation och det finns anledning att belysa det i risk- och sårbarhetsanalyser. Att kartlägga sociala relationer kan vara svårare än att kartlägga relationer i ett tekniskt system. Inom FRIVA-projektet har ett datorstöd för att kartlägga sociala relationer i och mellan organisationer tagits fram och även använts för att kartlägga relationer som uppstod vid utsläppet av svavelsyra i Helsingborg år 2005 [56].

4.1.4 Moduler

I en krissituation kommer organisationer att ställas inför en mängd olika uppgifter som skall utföras och flödet av information och mängden beslut som skall fattas kan vara mycket stor. Risken för att en central del i organisationen överbelastas är uppenbar, vilket exemplifieras av Toyotabranden (som beskrivits ovan) där krishanteringscentret förlorade sin funktion och de olika underleverantörerna i princip fick klara sig själva. I en centraliserad organisation är detta inte förvånande, krissituationen ställer krav på att många uppgifter skall lösas samtidigt och det

innebär också att om en central del i organisationen skall vara med och lösa samtliga uppgifter blir arbetsbördan snart mycket stor.

Ledtrådar till hur en eller flera organisationer kan hantera en stor mängd komplexa uppgifter samtidigt kan finnas inom andra områden där komplexa system hanterar en uppsjö olika uppgifter på en gång. Ett exempel på ett sådant system är människokroppen där komplexa uppgifter såsom att reglera hjärtrytmen, fördela näring till celler, reparera skador, o.s.v. sköts samtidigt och oftast utan problem. Lösningen på problemet att hantera ett stort antal komplexa uppgifter samtidigt kan vara så kallade *moduler* [43](s.230).

I en cell finns en stor mängd proteiner som interagerar med varandra och utför därigenom en mängd olika funktioner i cellerna, exempelvis att bygga upp och underhålla cellerna samt att upprätthålla kommunikation mellan dem. När man studerat nätverket (proteiner är noderna i nätverket och interaktioner mellan två proteiner är länkar) har man funnit att även om det är ett sammankopplat nätverk[13] finns det olika grupperingar av proteiner, *moduler*, som har specifika uppgifter [57]. Indelningen i moduler kan vara en förklaring till varför komplexa system kan hantera ett stort antal uppgifter samtidigt. Att arbetsuppdelning kan leda till positiva effekter är givetvis ingenting nytt, men sättet på vilket modulerna i komplexa system i naturen är organiserade kan ge ledtrådar till hur man skulle kunna utforma krishanteringsorganisationer för att göra dem både flexibla och förmögna att hantera stora mängder av komplexa problem samtidigt. I proteinnätverket som analyseras i [57] är indelningen i moduler tydlig, och till varje modul hör ofta ett protein som är en så kallad *hub*, d.v.s. ett protein som deltar i betydligt fler interaktioner än de flesta andra proteiner. En intressant aspekt av indelningen i moduler är att hubbarna i nätverket *mycket sällan har direktkontakt med varandra*, d.v.s. de interagerar ofta *via* andra proteiner. Precis samma typ av fenomen har man sett då man analyserat Internets struktur [58].

En positiv effekt av att organisera ett nätverk med hjälp av moduler är att nätverkets robusthet mot störningar ökar. Både Internets struktur och proteinnätverken är skalfria nätverk, vilka är mycket sårbara för attacker riktade mot de noder som har många länkar, *hubbarna*. Genom att organisera ett skalfritt nätverk i form av moduler minskar sårbarheten för denna typ av attacker. Anledningen är att eftersom en hub i ett modulbaserat nätverk troligtvis inte har en länk till en annan hub kommer utslagningen av en hub inte att fortplantas i nätverket så snabbt som den hade gjort om andelen sådana kopplingar var större. Störningen isoleras alltså till en modul och fortplantas förhoppningsvis inte till resten av nätverket [57].

Moduler verkar spela en stor roll för huruvida ett fel i ett komplext system kan fortplanta sig till andra delar av systemet. Det är värt att notera att modultänkandet

[13] Det finns en väg genom nätverket mellan samtliga noder.

på intet sätt är något nytt när det gäller att hantera en stor mängd uppgifter samtidigt. Fordonstillverkare har exempelvis länge praktiserat modulbaserade produktionssystem [59], vilka gör det möjligt att bedriva utveckling av olika delsystem på samma gång utan att produktionssystemet blir kaotiskt som följd av ändringar i ett system som påverkar ett annat system, som påverkar ett tredje, o.s.v. Det är troligt att robusta system kan skapas genom att bygga dem i form av moduler inom vilka man kan isolera fel som uppkommer och på så vis undvika fel som eskalerar. Även om Perrow [60] inte använder begreppet moduler är det lätt att se kopplingen mellan hans resonemang om hur robusta system bör byggas. Han hävdar att man bör bygga in decentraliserade autonoma grupper vars beroende av varandra skall vara få och kunna övervakas. I nätverkstermer kan detta tolkas som grupper av noder som är tätt sammanlänkade för att kunna lösa specifika uppgifter och deras beroende av resten av systemet är endast via ett fåtal länkar vars funktion kontinuerligt kan övervakas.

Moduler är inte bara relevanta för system som skall vara robusta mot störningar, de är även relevanta för den organisation som byggs upp för att hantera en kris. Kontexten i vilken en sådan organisation skall fungera är med största sannolikhet högst osäker och ställer höga krav på flexibilitet och förmåga att lösa många uppgifter samtidigt. Moduler kan även i denna typ av system vara ett viktigt begrepp. De organisationer som deltar i arbetet med att försöka kontrollera en kris har vanligtvis en beredskapsplan för hur man skall organisera sig. I sådana planer finns redan klara ”moduler”, d.v.s. uppdelningar av den formella organisationen i exempelvis en hierarkisk form. Vid studier av verkliga kriser (stormen Gudrun och kemikalieutsläppet i Helsingborg) har det visat sig att det finns tendenser till något som kan liknas vid en ”modul-organisation”, men som inte helt följer de formella gränserna mellan olika organisationer.

Moduler är intressanta ur ett sårbarhetsperspektiv framförallt eftersom de skulle kunna användas i komplexa system för att reducera sårbarheten på det sätt som Perrow menar (se ovan), men också eftersom konceptet skulle kunna användas i ett förberedande skede då olika organisationer som vid någon speciell typ av kris kan bli mycket beroende av varandra skulle kunna förbereda en sorts modulorganisation.

4.2 Komplexa adaptiva system

I kapitel 3 diskuterades anledningar till varför det kan vara svårt att göra risk- och sårbarhetsanalyser på vissa typer av system, framförallt då systemet innefattar en stor mängd agenter och beroenden mellan många tillståndsvariabler. Anledningen till mycket av problemen är att tillståndsrymden och riskscenariorymden blir mycket stora då dessa system skall beskrivas samt att det kan vara svårt att beskriva den dynamiska utvecklingen av ett sådant system. Därför är det av intresse att om möjligt kunna reducera tillståndsrymden, alternativt hantera

problematiken på ett annat sätt så att sårbarhetsanalyser för denna typ av system kan genomföras.

Ett första steg i att försöka hantera denna typ av problem är att försöka finna en terminologi för att beskriva systemen och de fenomen som är intressanta. En sådan användbar terminologi finns inom området *komplexa adaptiva system*.

4.2.1 Att beskriva komplexa adaptiva system

Det här avsnittet bygger i stora delar på det ramverk för komplexa adaptiva system som återfinns i [34] och i viss mån i [61]. Avsnittet syftar till att diskutera några viktiga begrepp inom området komplexa adaptiva system som kan vara viktiga för risk- och sårbarhetsanalyser av sociotekniska system.

Tidigare i kapitlet har *system* definierats som en uppsättning element, där vissa av dessa representerar agenter, artefakter och naturföremål. Agenter har förmågan att interagera med sin omgivning, de kan reagera på saker som sker och kan utföra mer eller minde målmedvetna handlingar. De har vanligtvis en *geografisk position*, samt en *uppsättning förmågor*, och *minne*. Artefakter är föremål eller objekt som agenter kan använda, de kan ha en uppsättning förmågor, men de har vanligtvis inte egna mål (se inledningen på kapitlet). Naturföremål påminner om artefakter, men de har, till skillnad från dessa, inte konstruerats av människan. I den fortsatta diskussionen används bara begreppet artefakter eftersom skillnaden mellan naturföremål och artefakter ofta inte spelar så stor roll i det här sammanhanget, det är deras egenskaper som är viktiga.

Precis som när det gäller begreppet *risk* finns ingen definition av ett *komplext system* som är allmänt vedertagen. Definitioner som förekommer är:

> *"Rough Definition of Complex Systems*. A complex system is a system with a large number of elements, building blocks or *agents*, capable of exchanging stimuli with one another and with their environment." [62]

> *"Roughly, by a complex system I mean one made up of a large number of parts that have many interactions. …in such system the whole is more than the sum of the parts in the weak but important pragmatic sense that, given the properties of the parts and the laws of their interaction, it is not a trivial matter to infer the properties of the whole."* [61]

I krishanteringssammanhang när fokus är på att analysera beroenden och dess effekter kan man använda en förhållandevis grov definition av komplexitet. När ordet komplext system används avses ett system som består av *många olika delar* och där delarna *interagerar* med varandra, ofta på ett icke-linjärt vis. I sådana system är det ofta svårt att förutsäga den framtida utvecklingen, även om man känner till systemets tillstånd vid en viss tidpunkt. Detta är problematiskt ur ett

sårbarhetsanalysperspektiv eftersom man där önskar beskriva olika möjliga scenarier till följd av en viss störning på systemet.

Ett komplext system behöver inte innehålla några agenter utan kan bestå av enbart artefakter. De system som är av intresse i krishanteringssammanhang innehåller dock vanligtvis någon eller några typer av agenter. I och med att dessa agenter kan ha inflytande på hur systemet beter sig blir de också en del av det system som man bör analysera (se diskussionen om olika typer av system i slutet av förra kapitlet).

En ofta viktig aspekt i ett system som innehåller agenter är att de försöker att *adaptera*, eller anpassa sig, i förhållande till sin omgivning (vilken bland annat innefattar de övriga agenterna). Adaptionen sker genom att agenter ändrar sina *strategier*. En strategi är ett sätt på vilka en agent agerar i förhållande till omgivningen för att uppnå sina mål. Beroende på hur agentens omgivning ser ut kan en och samma strategi resultera i att agenten utför olika handlingar, d.v.s. faktiska handlingar och strategier behöver inte vara samma sak. För att en agent skall kunna anpassa sin strategi till sin omgivning måste den ha något sätt att avgöra om en viss strategi är bra eller dålig, den måste ha ett *mått för hur framgångsrika olika strategier är*.

Agenterna i ett system kan vanligtvis delas in i olika *samlingar*, eller *populationer*, *av agenter*. Exempelvis kan man i en krissituation dela in personer (agenter) i olika samlingar efter vilken organisation de tillhör, eller så kan man dela in organisationer (agenter) i de tre populationerna privata, offentliga och övriga. Inom en samling agenter kan man skilja mellan olika *typer*. Typerna kan exempelvis ha att göra med hur pass väl en person (agent) kan klara sig på egen hand i händelse av ett avbrott i någon typ av teknisk infrastruktur.

Med hjälp av de delar som beskrivits ovan kan man definiera ett *komplext adaptivt system* som ett komplext system som innehåller agenter som *försöker* anpassa sig till sin omgivning. Att agenterna *försöker* anpassa sig till sin omgivning bör betonas eftersom deras försök inte nödvändigtvis leder till en förbättring utan kan leda till en försämring. Det viktiga är att agenternas *intentioner* är att förbättra situationen enligt någon typ av mått för framgång. Sociotekniska system som är intressanta ur ett krishanteringsperspektiv har i regel agenter som kan anpassa sig till sin omgivning och därmed påverka konsekvenserna av en påfrestning. Detta innebär att just agenters förmåga att anpassa sig under en kris är intressant att bedöma i sårbarhetsanalyser och som ett hjälpmedel för att göra det kan en del begrepp som presenterats i ett ramverk för att beskriva komplexa adaptiva system användas (översatt och modifierat från [34]):

- *Agent* – Ett element i ett system som har mål, strategier och förmågor att påverka artefakter och andra agenter.

- *Artefakt* – En materiell resurs som har en geografisk position och kan reagera på agenters handlingar.
- *Strategi* – Ett betingat handlingsmönster som indikerar vad som skall göras under vissa omständigheter.
- *Population* – En samling av agenter.
- *Typ* – Alla agenter i en population som har någon egenskap gemensamt, alternativ alla relationer mellan agenter och/eller mellan artefakter som har något gemensamt.
- *Selektion* – Processen som leder till en ökning eller minskning av antalet agenter eller strategier av en viss typ.
- *Mått för framgång* – Ett mått som används av en agent för att avgöra hur framgångsrik en viss strategi är.

Begreppen *beroenden*, *nätverk*, *moduler* och *självorganisation* kan inkluderas i ramverket för komplexa adaptiva system:

Beroenden är en form av relation mellan agenter och/eller mellan artefakter. Relationen innebär att en eller flera tillståndsvariabler som är associerade med den agent/artefakt som är i beroendeställning påverkas om en eller flera tillståndsvariabler som är associerade med den aktör/artefakt som är källan till beroendet skulle ändras på något sätt. Beroenden kan delas upp i de typer som diskuterades i början av kapitlet (se avsnitt 4.1.1).

Nätverk är en representation av någon typ av relation mellan agenter och/eller mellan artefakter.

Moduler (se avsnitt 4.1.4) är en population av agenter eller artefakter som bildar en grupp i ett nätverk av någon typ av relation. En modul har vanligtvis någon specifik funktion, exempelvis att stödja ledningsarbetet för en specifik organisation under en kris. Under en kris är det förmodligen inte ovanligt att moduler bildas av agenter som tillhör skilda organisationer (populationer).

Självorganisation och emergenta egenskaper kan i det här sammanhanget betraktas som att enskilda agenter eller artefakter anpassar sig till sin omgivning genom enbart lokal information om det totala systemet och på så vis uppkommer någon typ av egenskap hos systemet som inte enkelt kan härledas från kunskap om de enskilda agenterna/artefakterna. Självorganisation kan förekomma utan att några speciella systemegenskaper uppkommer, men detta är inte speciellt intressant i det aktuella sammanhanget.

Ramverket för analys av komplexa adaptiva system är ett verktyg som kan användas vid studier av samhällets sårbarhet och krishantering. Det bör dock understrykas att ramverket inte ger några konkreta förslag på hur detta skall gå till, det är något som måste preciseras beroende på vilket fenomen som vill studeras.

Två sådana typer av fenomen som kan vara intressant att studera är självorganisation och emergenta systemegenskaper.

4.2.2 Självorganisation och emergenta systemegenskaper

I en krissituation kan det uppkomma egenskaper hos de olika systemen som är inblandade som är mer eller mindre oväntade och som man inte kan förutsäga bara med kunskap om systemets delar. Ett bra exempel på detta kommer från jordbävningskatastrofen i Whittier Narrows, Kalifornien, 1987. I jordbävningen slogs strömmen till trafikljusen ut, vilket resulterade i att trafiken i praktiken blev stillastående. I denna kaotiska situation övergav vissa trafikanter sina bilar vid sidan av vägen och ställde sig och dirigerade trafiken i närmaste korsning. Andra trafikanter som såg detta gjorde samma sak när de nådde nästa korsning, o.s.v. Genom att trafikanterna, *utan extern påverkan (ingen gav order)*, valde att koordinera det lokala flödet av trafik i en korsning ledde detta till att det globala flödet (flödet i hela vägtrafiksystemet) avsevärt förbättrades [63] (s. 32). Detta är ett exempel på vad som menas med emergenta (eng. emergent) systemegenskaper.

Emergenta systemegenskaper innebär egenskaper som är oväntade eller svåra att förutse. Sådana egenskaper hos system kan uppstå genom förhållandevis enkla ”regler” för interaktion mellan element på en lägre systemnivå. När en person står i korsningen efter jordbävningen och dirigerar bilar vet han/hon inget om systemets *globala egenskaper*, d.v.s. hur flyter trafiken i hela systemet, utan han/hon kan bara utgå från den *lokala* information som är tillgänglig. De regler som personen använder för att dirigera bilisterna är förmodligen inte speciellt avancerade utan av typen: när trafiken verkar röra sig bort från korsningen på en av gatorna dirigeras bilar från de övriga gatorna till den gatan.

Jordbävningsexemplet visar också på *självorganisation*, vilket är ett begrepp som använts inom många olika discipliner och som har olika definitioner. I krishanteringssammanhang kan begreppet användas för ett system som vid en kris uppvisar någon typ av ordnat beteende, d.v.s. inte slumpmässigt, och som på så vis påverkar krisens förlopp utan att det finns en central ledningsfunktion för det ordnade beteendet. När trafiken efter jordbävningen i Whittier Narrows stod still var det ingen som beordrade personerna i bilarna att stiga ur och börja dirigera trafiken, de gjorde det på eget initiativ. Självorganisation är ofta en önskvärd egenskap i ett krishanteringssystem, men svår att åstadkomma i praktiken [63] (s.271). I de 11 jordbävningarna mellan 1985 och 1995 som forskaren Louise Comfort analyserar i sin bok ”Shared Risk: Complex Systems in Seismic Response” [63] observerar hon delar av krishanteringssystem som uppvisar självorganisation, exempelvis frivilligorganisationer och privatpersoner, men i inget av fallen har dessa fenomen en framträdande roll.

Det verkar rimligt att självorganisation är en önskvärd egenskap i ett krishanteringssystem, framförallt eftersom det kan minska belastningen på vissa

funktioner i den formella krishanteringsorganisationen. Om man har ett system där exempelvis frivilligorganisationer måste styras i detalj förutsätter detta att man har kapaciteten att göra det, annars riskerar andra funktioner inom krishanteringsorganisationen att drabbas av överbelastning. Man kan också frigöra resurser som följd av självorganisation. I exemplet ovan från jordbävningen i Whittier Narrows skulle polisen kunnat utföra uppgiften med att dirigera trafiken, men i och med att bilisterna gjorde det kunde polisens resurser användas för annat. Även i exemplet med Toyotabranden (se avsnitt 4.2.1) var det självorganisation bland underleverantörerna som var en avgörande orsak till att konsekvenserna på grund av krisen blev begränsade.

Även i Sverige har tendenser till självorganisation i samband med kriser kunnat observeras. I samband med stormen Gudrun observerades en del fenomen som passar in på beskrivningen av fenomenet, exempelvis röjningsarbetet av vägar som till viss del sköttes av personer utan central koordinering.

En annan tendens till självorganisation som framkommit under studier av framförallt stormen Gudrun (2005) och Svavelsyraolyckan i Helsingborg (2005) har att göra med uppbyggnaden av det så kallade *krishanteringsnätverket*. Krishanteringsnätverket kan i det här sammanhanget betraktas som ett socialt nätverk där noderna i nätverket är personer som på något sätt är involverade i att hantera någon typ av påfrestning på samhället. Sådana nätverk finns i stora delar ”fördefinierade”, d.v.s. man vet redan på förhand vilka som skall ingå i nätverken och i viss mån vilka funktioner de skall ha. Detta är vad beredskapsplanering bland annat handlar om. Vid studier av stormen Gudrun och Svavelsyrautsläppet i Helsingborg framgår det att inte bara personer som fanns med i beredskapsplanerna spelar en roll i nätverken, även personer som inte tillhör någon myndighet har engagerats [56]. Vid närmare studie av dessa individer framgår det att deras engagemang kan ses som en typ av självorganisation inom krishanteringsnätverket. Antingen har en person som redan är engagerad i olyckan kontaktat en person eller organisation som normalt inte har något med olyckshantering att göra, eller så har en sådan person kontaktat någon inom krishanteringsorganisationen och på så vis blivit engagerad i arbetet. Båda typerna av kontakter har initierats utan att personerna uttryckligen blivit beordrade av någon att göra det, vilket kan ses som en typ av självorganisation.

Självorganisation har många fördelar när det gäller krishantering, men det finns givetvis även nackdelar. En sådan nackdel är möjligheten att olika aktörer genom självorganisation skapar en situation där konsekvenserna för systemet som helhet blir värre än det hade varit om någon hade koordinerat aktörernas agerande och beordrat dem till en viss typ av handlande. Ett exempel på en sådan situation skulle kunna uppkomma då två, eller flera, aktörer är i behov av en gemensam resurs och den lokala information som var och en av aktörerna har tillgänglig indikerar att resursen skulle vara mest användbar hos agenten själv. Den här situationen skulle

kunna leda till en suboptimering av resursutnyttjandet om det är så att resursen, ur ett globalt perspektiv, bäst behövdes hos en agent som inte får resursen på grund av att en annan agent anser sig behöva den.

4.2.3 Plötsliga förändringar i komplexa adaptiva system

En egenskap som många komplexa adaptiva system har är att en liten ändring av systemets förutsättningar kan få stora förändringar i systemets tillstånd. I vår vardag förväntar vi oss vanligtvis inte den här typen av effekter. Inget dramatiskt bör hända om vi ökar inomhustemperaturen några grader, om vi missar bussen kan vi ta nästa buss, ytterligare en arbetsuppgift får ingen större effekt på vår arbetssituation, o.s.v. Risken är stor att vi förväntar oss samma beteende hos betydligt mer komplexa system än de som vi stöter på i vår vardag.

Stormen Gudrun utgör ett exempel på en påfrestning där många som deltog i krishanteringsarbetet troligtvis är nöjda med insatsen. Det är dock inte säkert att insatsen hade blivit lika framgångsrik om stormen inträffat då det varit kallare [64]. Om det hade varit kallare under stormen hade det akuta hjälpbehovet kunnat bli avsevärt större, dessutom hade vägarna kunnat bli mer svårframkomliga och tidskrävande att röja. Det är inte alls säkert att den totala effekten av en inte alltför dramatisk temperatursänkning i samband med stormen bara hade haft marginell effekt på insatsens genomförande. På grund av beroenden och interaktioner skulle en sådan temperatursänkning mycket väl kunnat få katastrofala följder för insatsen och påfrestningen skulle ha kunnat bli betydligt större än den blev vid stormen Gudrun. Det kan därför vara olämpligt att betrakta utgången av stormen som ett bevis för att ”vi kan hantera effekterna av en allvarlig storm”. Konsekvenserna av Gudrun kunde hanteras relativt väl, men vad hade de sammanlagda effekterna av Gudrun plus en för årstiden låg temperatur inneburit? Det är omöjligt att säga, men vad som kan konstateras är att effekter i komplexa system vanligtvis inte är linjära, d.v.s. en liten ökning av exempelvis temperaturen ger inte nödvändigtvis en ”linjär” förändring av systemet. Ett bra exempel på ett sådant system är vatten. Vid rumstemperatur är vatten flytande och inget dramatiskt kommer att hända om man sänker temperaturen på vattnet. När man däremot sänker temperaturen under 0ºC sker som alla vet dramatiska saker och vattnet övergår från att ha varit flytande till fast form. Vattnet har nu helt andra egenskaper, trots att det består av samma vattenmolekyler som när det var flytande. På fysikers språk har vattnet genomgått en *fasomvandling*. På samma sätt som vattnets egenskaper uppkommer genom interaktioner mellan vattenmolekyler uppkommer egenskaperna hos ett system för att hantera kriser genom interaktioner mellan olika agenter och artefakter. På samma sätt som vatten kan övergå från en fas till en annan bara genom en liten ändring av temperaturen, kan andra komplexa system övergå från en ”fas” till en annan. Det är inte osannolikt att ett system för krishantering kan uppvisa liknande dramatiska ”fasövergångar” som vatten. Kanske hade lite lägre temperatur under stormen Gudrun räckt för att samhället, inklusive de organisationer som arbetade med krishanteringen, skulle ha upplevt en dramatiskt annorlunda situation.

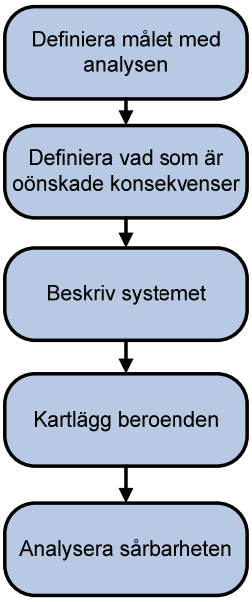
Att de system som är intressanta då man gör risk- och sårbarhetsanalyser uppvisar tendenser som liknar en hastig fasomvandling gör det svårt att genomföra bra analyser. I sådana fall är det viktigt att försöka identifiera de ”gränser” för när en sådan fasomvandling skulle kunna ske och om möjligt inkludera riskscenarier på ”båda sidor om gränsen” i sin analys. Det kan också bli aktuellt att i högre grad använda sig av simulering för att finna dessa gränser.

4.3 Analys av sårbarhet med fokus på beroenden

I detta kapitel har det presenterats en del exempel på hur man kan betrakta olika kriser ur ett systemperspektiv där beroenden mellan olika element i systemet har en framträdande roll. Frågan är nu hur denna typ av kunskap kan användas, tillsammans med definitionerna av risk, sårbarhet, scenario, mm. i kapitel 2 och med de befintliga metoderna som presenterats i kapitel 3, för att föreslå hur sårbarhetsanalyser kan genomföras för komplexa sociotekniska system.

Till att börja med är det viktigt att poängtera att fokus i detta avsnitt är på sårbarhetsanalys och inte på riskanalys. Visserligen är dessa två analysformer nära besläktade och när det gäller den operationella definitionen av sårbarhet (se kapitel 2) skiljer den sig inte speciellt mycket.

Utgångspunkten för analysen är att någonting är skyddsvärt och att det existerar någon typ av hot mot det skyddsvärda. Det skyddsvärda i det här sammanhanget kommer att vara en del i det system som sårbarhetsanalysen genomförs för och hotet(en) kan orsaka ett antal riskscenarier som resulterar i oönskade konsekvenser för systemet. Här följer en beskrivning av ett möjligt tillvägagångssätt för en sådan analys, vilket också illustreras i Figur 13.



Figur 13 *Illustration av olika steg i arbetet med att göra en analys av sårbarhet i ett system med fokus på beroenden.*

Steg 1 - Definiera målet med analysen
Det första som måste göras oavsett vilken metod som används för en sårbarhetsanalys är att klargöra vad som är målet med analysen. Är den exempelvis tänkt att användas för att analysera sårbarheten, enligt definitionen i kapitel 2, i ett visst system på grund av brand, eller på grund av utsläpp av farligt gods? Skall analysen ligga till grund för någon typ av beslut, eller vill man använda analysen för att identifiera svaga delar i systemet? Beroende på vilka målsättningar man har och vilka resurser som står till för fogande kommer analysen att utformas på olika sätt.

I detta skede är det också viktigt att klargöra hur man skall uppfylla målet med hjälp av analysen, vilket bland annat har att göra med vilken metod som skall användas.

Steg 2 - Definiera vad som är oönskade konsekvenser
Vad som utgör *oönskade konsekvenser* för systemet har troligtvis diskuterats redan under steg 1 då målet med analysen klargjorts. I detta steg kan dock dessa konsekvenser behöva klargöras ytterligare och framförallt måste man klargöra hur konsekvenserna skall mätas och värderas. Detta är viktigt även om sårbarhetsanalysen inte är kvantitativ. För att definiera de oönskade konsekvenserna kan det vara nyttigt att fundera över syftet med det aktuella systemet, eller delsystemet. Detta kan ge uppslag till hur oönskade konsekvenser för systemet bör definieras. Om syftet med ett system är att förse invånarna i en

kommun med något (exempelvis el) kan oönskade konsekvenser definieras som händelser där syftet inte uppnås, exempelvis att alla invånare inte har tillgång till el.

Ibland kan det vara nödvändigt att mäta oönskade konsekvenser med hjälp av flera attribut, exempelvis antal invånare som är sjuka på grund av katastrofen, antal invånare som är döda på grund av katastrofen, o.s.v. Det kan också bli nödvändigt att definiera attributen på så vis att de inte bara gäller en specifik tidpunkt under ett scenario, exempelvis antal sjuka. I en sårbarhetsanalys skall ett antal möjliga *riskscenarier* (se definition i kapitel 2) identifieras och meningen med konsekvensattributen är att man för varje riskscenario skall kunna bestämma konsekvenserna med hjälp av det aktuella attributet, vilket inte går att göra om attributet definieras som ”antal hushåll utan elförsörjning”. Antal hushåll utan elförsörjning är en tillståndsvariabel i systemet som kan ha olika värde vid olika tidpunkter i scenarierna. Därför måste konsekvensattributet exempelvis definieras som ”maximalt antal hushåll utan strömförsörjning upp till en månad efter riskscenariots början”, se diskussionen angående konsekvenser i avsnitt 2.3.

Steg 3 - Beskriv systemet
Att beskriva systemet innebär att man preciserar vad som ingår i det system som sårbarhetsanalysen gäller, samt i vilka tillstånd systemet kan befinna sig. Att beskriva systemet är viktigt för den fortsatta analysen och det kan hända att bara själva definitionen av systemet ger insikter rörande sårbarheten.

Ett system består av ett antal *element* som har något gemensamt, och i detta sammanhang kan man skilja på två typer av element i systemet: *artefakter* och *agenter*. Exemplen tidigare i det här kapitlet visar att människor och organisationer som agerar under en kris kan ha stor påverkan på krisens händelseförlopp. Därför är det viktigt att i en sårbarhetsanalys ta med agenterna, d.v.s. de organisationer[14] som kan tänkas påverka det aktuella systemets möjlighet att hantera påfrestningar. I en kommun kan exempelvis olika förvaltningar vara agenter, eller kanske till och med olika avdelningar inom förvaltningarna. Om sårbarhetsanalysen genomförs för kommunen kan andra viktiga aktörer vara länsstyrelse, olika myndigheter, företag, frivilligorganisationer, mm. I det första steget är det önskvärt att försöka identifiera så många aktörer som möjligt för att senare i analysen eventuellt ta bort dem om de inte bedöms ha någon signifikant påverkan på systemet.

I samband med att agenterna i systemet definieras bör man också kartlägga vilka *uppgifter* som de har, eller kan ha. En uppgift är något som agenterna kan utföra och vanligtvis handlar det om en påverkan på resten av systemet. En agent kan ha många olika uppgifter, men det är bara de som är viktiga för att bedöma sårbarheten i systemet på grund av det aktuella hotet som behöver tas med i en

[14] Vanligtvis syftar agent på en organisation, men det kan också syfta på en enskild människa (se tidigare i kapitlet).

analys. Eftersom det kan vara svårt och tidskrävande att kartlägga alla uppgifter som en aktör kan ha är det en bra utgångspunkt att börja kartlägga de uppgifter som kan betraktas som *samhällsviktiga*. Samhällsviktiga uppgifter skall i det här sammanhanget betraktas som sådana uppgifter som *om de inte utförs orsakar att en kris uppkommer*, eller sådana uppgifter som *om de genomförs minskar konsekvenserna av en kris*. Denna definition överensstämmer med Krisberedskapsmyndighetens definition av vad som utgör *samhällsviktig verksamhet* [65].

Artefakterna i systemet, d.v.s. element som inte själva har mål att agera efter, kan utgöras av olika tekniska infrastrukturer, föremål, fordon, etc. Det är inte ovanligt att en specifik agent i systemet förfogar över en viss artefakt och den enda som använder artefakten är agenten själv. Ett exempel på detta är räddningstjänstens släckbilar. Andra artefakter används av ett antal agenter, exempelvis olika tekniska infrastrukturer såsom vägar och elsystem och därför delas gruppen artefakter in i grupperna *teknisk infrastruktur* och *resurser*.

Det är användbart att anamma Simons [61] beskrivning av ett system, eller del av system, som bestående av en inre och yttre miljö (”inner environment” och ”outer environment”). Den inre miljön hos ett system är de delar som systemet är uppbyggt av och den yttre miljön är den omgivning i vilket systemet verkar. Begreppen inre och yttre miljö kan användas på flera olika ”nivåer” och ibland är den yttre miljön för ett system den inre miljön för ett annat. Om man exempelvis är intresserad av att studera hur en person beter sig i vissa situationer kan människokroppen vara den inre miljön och personens omgivning den yttre miljön. Är man däremot intresserad av att studera en organisation kan personerna tillhöra den inre miljön (de som ingår i organisationen) eller den yttre miljön (de som inte tillhör organisationen). Indelningen i yttre och inre miljö är mycket lämpligt när det gäller att analysera funktionen hos komplexa system eftersom man ofta kan förutsäga ett systems beteende bara baserat på kunskap om systemets *mål och dess yttre miljö* [61]. Exempelvis är det troligt att personer vid en brand i en byggnad försöker rädda sina barn även om det skulle innebära att de utsätter sig själva för stora risker. För att beskriva beteendet hos en person vid utrymning behöver man inte veta hur det inre systemet ser ut, d.v.s. hur kroppen är uppbyggd o.s.v., det räcker med att veta hur personen reagerar på sin omgivning. Tanken med att kartlägga ett sociotekniskt system som man vill genomföra en sårbarhetsanalys för är att det genom att kartlägga de olika artefakterna och agenterna, deras mål, strategier samt förmåga att påverka sin omgivning går att få kunskap om systemets beteende vid en påfrestning utan att ha kunskap om agenternas eller artefakternas inre miljö.

Att kartlägga vilka agenter och artefakter som är relevanta för ett sociotekniskt systems krishanteringsförmåga kan inledas genom att *studera dokument* som redogör för det aktuella systemets organisation. Genom en sådan studie kan

personen/personerna som genomför analysen få en inledande överblick över de olika agenterna i systemet. Studier av dokument gör också att den som genomför analysen får inledande kunskap om det system som studeras, vilket kan underlätta när intervjuer med personer i relevanta organisationer senare genomförs. Det absolut viktigaste under denna del av informationsinsamlingen är att sträva efter att försöka *identifiera* alla relevanta agenter och artefakter. För att kunna veta vad en relevant agent eller artefakt är måste man i denna del av analysen försöka avgöra om agenterna/artefakterna har någon betydelse för konsekvenserna i systemet på grund av det hot för vilket man analyserar sårbarheten.

Steg 4 - Kartlägg beroenden
En viktig aspekt hos agenterna är deras förmågor att påverka sin omvärld och vad de är beroende av för att kunna göra det. Förmåga att påverka omvärlden och beroenden kan kartläggas genom nätverk, där noderna representerar agenter och länkar representerar beroenden mellan agenter. Även beroenden av artefakter kan kartläggas genom att använda ett nätverk.

I praktiken genomförs detta steg genom intervjuer med nyckelpersoner inom de olika organisationerna som identifierats i steg 3. Detta kan exempelvis vara personer i ledande ställning på olika förvaltningar i en kommun, eller personer med speciell kunskap om krishantering som är relevant för analysen, exempelvis beredskapssamordnare. Målet med intervjuerna är att ytterligare förbättra kunskapen om det aktuella systemet som helhet, samt få detaljerad kunskap om just den organisation som personen i fråga tillhör. Intervjuerna bör fokusera på organisationens (agentens) mål, strategier, resurser, samt förmåga att påverka sin omgivning. Exempel på mer konkreta frågeställningar är:

- Vilka uppgifter kan organisationen ha vid en kris?
- Vilka uppgifter utför organisation vid normal verksamhet?
- Vilka uppgifter som kan betraktas som samhällsviktiga har organisationen?
- Vilka resurser (artefakter), som kan vara viktiga för krishantering, disponerar organisationen?
- Vilken kunskap som kan vara användbar vid krishantering disponerar organisationen? Var finns kunskapen?
- Vilka resurser är organisationen beroende av för att kunna utföra sina uppgifter?
- Vilka andra agenter eller artefakter är beroende av att den aktuella organisationen genomför sina uppgifter?
- Hur påverkas organisationens förmåga att genomföra sina uppgifter om vissa resurser inte finns tillgängliga?
- Vilka mål har organisationen med sin verksamhet, både i normalfallet och i en krissituation?
- Finns det vissa mål som är viktigare än andra?

- Hur uppfyller organisationen målen (vilka strategier tillämpar man), både vid normal verksamhet och vid eventuella störningar?
- Hur får organisationen information om sin omgivning (exempelvis via privat organisation, myndighet eller media)?

Genom de inledande intervjuerna i steg 4 kommer förmodligen ytterligare organisationer som ingår i det system som är av intresse att kunna identifieras. Det innebär att personer som har kunskap om dessa organisationer intervjuas på samma sätt och om nya organisationer eller agenter identifieras fortsätter intervjuerna med dessa. Hela processen kan liknas vid att rulla en snöboll som hela tiden växer och växer (tekniken kallas snowballing på engelska [66]). Till slut kommer inga fler agenter eller artefakter som tillhör systemet att kunna identifieras och då är identifieringsprocessen slut. Resultatet blir ett antal agenter och artefakter som tillhör det aktuella systemet samt kunskap om beroenden inom systemet, men också mellan systemet och dess yttre miljö.

Steg 5 - Analysera sårbarheten
Att analysera sårbarhet i ett system kan genomföras på ett stort antal sätt med varierande noggrannhet. Utgångspunkten i det här avsnittet är att sårbarhet definieras på det sätt som diskuterades i kapitel 2. Beskrivningen av analysfasen är uppdelad i tre delar där olika tillvägagångssätt för analys av sårbarheten i ett komplext socioteknisk system diskuteras. Det som skiljer delarna åt är mängden information som måste finnas tillgänglig, tidsåtgången för analysen, samt hur noggrant de olika riskscenarierna som kan inträffa beskrivs. I avsnitt 4.3.1 beskrivs det tillvägagångssätt som troligtvis kräver minst information och tid och i avsnitt 4.3.3 beskrivs det som kräver mest information och tid.

4.3.1 Grov analys av olika typer av fel

Den enklaste typ av analys som kan genomföras då materialet rörande det aktuella systemet samlats in är att göra en i huvudsak kvalitativ analys av sårbarheten i systemet. Detta innebär exempelvis att varken sannolikheter för olika riskscenarier eller beroenden mellan olika element i systemet behöver kvantifieras. Ibland kan det dock vara önskvärt att kvantifiera konsekvenserna av ett visst scenario.

Analyser av det här slaget kan med fördel genomföras i form av en seminarieövning där ett flertal personer från de berörda aktörerna deltar. Målet med analysen är att producera en uppsättning riskscenarier som kan tänkas inträffa om en specifik störning drabbar systemet, d.v.s. en uppdelning av *riskscenariorymden* (se kapitel 2). Som en inledande metod för att göra en grov klassificering av scenarier kan man beakta olika typer av ”fel” i det system som man studerar. Den första typen av fel som är förhållandevis enkel att skydda sig mot och därför en av de första typerna som bör studeras är *enskilda fel*. Komplexa system kan vara sårbara för enskilda fel om det finns delar i systemet, agenter eller artefakter, som många andra agenter och artefakter är beroende av. Det primära skyddet mot

enskilda fel är redundans. Ett exempel på ett redundant system är då man har två reservkraftgeneratorer i ett tekniskt system. Om en av generatorerna av någon anledning inte fungerar kan den andra försörja systemet med ström.

I praktiken kan en sådan analys genomföras med hjälp av kartläggningen av systemets element (agenter och artefakter). Genom att successivt gå igenom de olika elementen och fråga sig ”Vad händer med de andra elementen om det här elementet inte fungerar?” kan man snabbt få en uppfattning om vilka element i systemet som har en stor potential att orsaka negativa konsekvenser i systemet. Den här typen av analys liknar en så kallad What if-analys som brukar användas inom processindustrin. Analysen innebär inte att man behöver definiera något specifikt hot utan riskscenariorymden kan sägas bestå av alla de möjliga scenarier som medför att något av elementen i systemet inte fungerar, oavsett vad det var som orsakade det. Resultatet från analysen blir ett antal riskscenarier där påfrestningen på systemet består i att olika element slutar fungera som de ska. För vart och ett av dessa scenarier skall det också finnas en beskrivning av konsekvenserna.

En annan typ av fel som kan vara svårare att upptäcka och skydda sig mot är så kallade *”common cause failures”*. När det gäller komplexa system är detta en typ av påverkan som kommer från systemets omgivning, men som får flera delar i systemet att sluta fungera. Genom *diversifiering*, d.v.s. att alla komponenter i systemet inte är av samma typ, kan ett visst skydd erhållas mot den här typen av fel. Att inte bara förlita sig på en typ av tekniskt system för någon viktig krishanteringsfunktion, exempelvis genom att ha möjlighet att använda två eller flera olika typer av system för kommunikation, är ett exempel på diversifiering. Genom att kartlägga ett system och analysera dess komponenter kan externa orsaker (utanför systemet) som kan skada flera komponenter samtidigt identifieras.

En tredje typ av fel som kan vara allvarlig i komplexa system med starka kopplingar (beroenden) är *kaskadfel*. Ett kaskadfel är ett fel som innebär att någon komponent i systemet slutar fungera, eller får nedsatt funktion, och som en konsekvens av detta sker en ”lastomfördelning” i systemet. Denna omfördelning resulterar i att en eller flera andra komponenter får bära en större last än vad de klarar av, vilket innebär att de kollapsar. Detta leder på nytt till en lastomfördelning, vilket i sin tur kan leda till att ytterligare komponenter slås ut, o.s.v. Genom att öka skillnaden mellan belastningen som en komponent klarar och den som den normalt utsätts för kan risken för kaskadfel minskas. Det går också att bygga system enligt ”modul-konceptet” (se avsnitt 4.1.4) för att minska sannolikheten för fel som sprids utanför den del av systemet som felet uppstod i. Kaskadfel är svåra analysera bara med hjälp av kvalitativa metoder, men det går i alla fall att föra en diskussion om dem och möjligtvis kan man också resonera sig fram till hur ett fel kan fortplanta sig i det aktuella systemet.

Om ett system har kända svagheter kan dessa utnyttjas av någon som vill skada systemet. Detta är en annan typ av påfrestning på systemet än de övriga typerna av fel. Antagonistiska ”fel” är inte oberoende och därför fungerar skyddsstrategin med att introducera redundans i systemet inte lika effektivt som mot oberoende fel. Antagonistiska attacker kan resultera i ett ”common cause failure”, eller ett kaskadfel. När dessa fel är ett resultat av en antagonistisk handling är det troligare att systemets svagheter utnyttjas och att attacken mot systemet kommer vid en tidpunkt som är lämplig från antagonistens synpunkt, men olämplig från systemets synpunkt, exempelvis då belastningen på systemet redan är stor. Att skydda sig mot antagonistiska hot är svårare än att skydda sig mot övriga typer av fel och det blir givetvis inte lättare av att de tekniska och sociala system som samhället vill skydda blir allt mer starkt kopplade till varandra. Ett sätt att minska möjligheten för konsekvenserna av antagonistiska handlingar att sprida sig i ett system är genom uppdelning i moduler som sinsemellan har relativt få kopplingar och som dessutom kan vara övervakade. I system med skalfria egenskaper (se avsnitt 4.1.2) är det speciellt viktigt att förse hubbarna (de noder eller systemdelar som har många länkar till andra delar) med ett adekvat skydd.

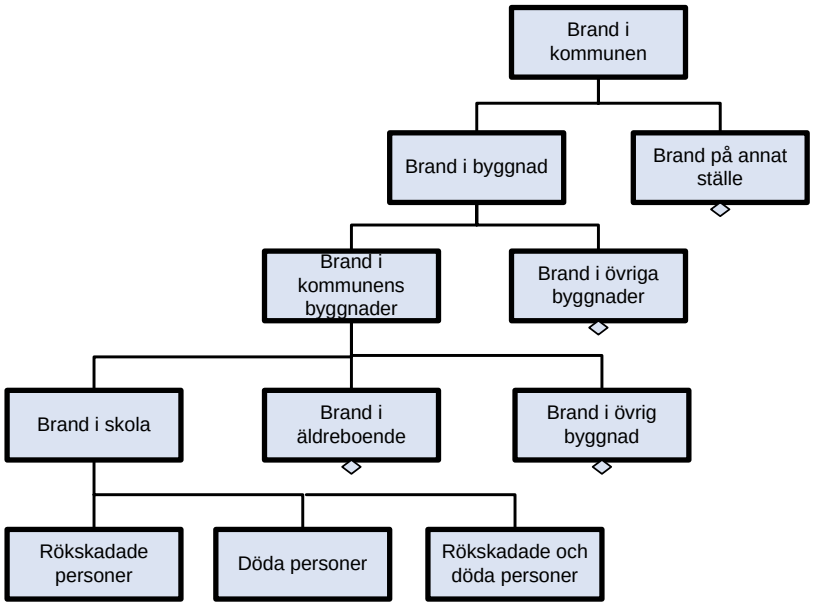
En annan viktig sak när det gäller antagonistiska påfrestningar är att bara för att hotet inte realiserats när systemet befinner sig i ett ”normalt” tillstånd innebär det inte att hotet inte existerar. Eftersom personer som vill skada ett system sannolikt vill göra så stor skada som möjligt är det inte otänkbart att de väntar tills dess att påfrestningen på systemet är större än normalt, eller möjligheten att göra skada är större. Ett bra exempel på detta är de allierades desinformationskampanj mot de tyska spionerna inför invasionen i Normandie under andra världskriget. De allierade kände till en stor mängd tyska spioner långt innan invasionen, men valde att inte göra något åt dem eftersom påfrestningarna på det tyska ”systemet” inte var tillräckligt stora och skadan som de skulle kunna åstadkomma inte var tillräckligt stor. När däremot invasionen skulle genomföras var möjligheten att göra stor skada stor. När de allierade läckte falsk information om var landstigningen skulle ske till samtliga tyska spioner som man kände till blev effekten mycket lik ett ”common cause failure”, d.v.s. flera komponenter i systemet (flera spioner) drabbades av fel (lämnade vidare felaktig information) på grund av samma externa orsak (de allierade) [34].

Kartläggningen av systemet, d.v.s. agenterna, artefakterna, uppgifterna, beroendena, mm., kan användas då man tillämpar metoden Anticipatory Failure Determination (AFD) [67], vilken är en metod som är lämplig då man gör en sårbarhetsanalys med avseende på antagonistiska hot. I korthet går AFD ut på att i stället för att fundera över vilka möjliga skadliga händelser som kan orsakas av antagonister fundera över hur man bäst kan skada systemet. Detta sätt att vända på frågeställningen kan göra det lättare att hitta svagheter i systemet, speciellt då man har en bra systembeskrivning samt en klar definition av vad som menas med oönskade konsekvenser.

Resultatet från en grov analys av olika typer av fel blir en beskrivning av vilka aktörer som ingår i systemet, exempelvis olika organisationer eller delar av organisationer, och vilka artefakter som ingår, exempelvis fysiska resurser. Vidare resulterar analysen i en systematisk genomgång av alla dessa element med syftet att identifiera riskscenarier som kan uppstå på grund av att något händer med elementen. Exempel på ett sådant riskscenario kan vara att en organisation av någon anledning inte kan utföra en specifik uppgift. Riskscenariot skall också kompletteras med någon typ av konsekvensbedömning för scenariot, d.v.s. vad får det för konsekvenser för systemet att det specifika elementet inte fungerar som det var tänkt? Om det är möjligt är det också bra om en sannolikhetsbedömning för riskscenarierna genomförs, men detta är inte nödvändigt i en grov analys.

4.3.2 Kvalitativ analys av sårbarhet

Ett vanligt sätt att dela upp riskscenariorymden är att använda hierarkisk indelning i ett scenarioträd där riskscenariorymden delas upp och blir mer specifik ju längre ner i hierarkin man kommer. Ett exempel på ett sådant scenarioträd illustreras i Figur 14 där påfrestningen som analyseras är en brand i en kommun. En snedställd fyrkant under en scenariobeskrivning betyder att scenariot skulle kunna ha utvecklats mer. Helst skall uppsättningen av scenarier vara disjunkta (se kapitel 2), d.v.s. de skall inte kunna sammanfalla. Om ”brand i byggnad” och ”brand på annat ställe” i exemplet nedan (Figur 14) definieras som att branden någon gång under förloppet involverar en byggnad respektive att branden någon gång under förloppet involverar något annat än en byggnad gäller inte detta. En brand kan ju börja på ett annat ställe än i en byggnad och sedan sprida sig till en byggnad. Om ”brand i byggnad” i stället innebär att branden börjar i byggnaden och ”brand på annat ställe” innebär att den börjar någon annanstans är uppdelningen av riskscenariorymden disjunkt (en brand kan inte både börja i en byggnad och samtidigt inte göra det).



Figur 14 Illustration av ett hierarkiskt scenarioträd.

Med hjälp av ett scenarioträd kan påfrestningen på systemet, exempelvis ”brand i kommunen”, delas upp i ett antal beskrivningar av tidiga skeden i olika riskscenarier (ett riskscenario är inte fullständigt förrän systemet nått ett *sluttillstånd*, se kapitel 2). För vart och ett av dessa beskrivningar skall sedan systemets möjliga sluttillstånd bedömas. Detta innebär att konsekvenserna, såsom de definieras i steg 2 skall bedömas för de olika riskscenarierna som blir resultatet av påfrestningarna. När man gör detta måste man försöka reducera antalet bedömningar som är nödvändiga genom att ”slå ihop riskscenarier”, annars riskerar man att arbetsbelastningen blir för hög. Att slå ihop riskscenarier innebär att man bedömer att konsekvenserna för systemet blir lika oavsett vilket av två riskscenarier som inträffar och därför betraktas de två scenarierna som ett när konsekvenserna för systemet bedöms. Exempelvis kanske det inte spelar någon roll för konsekvenserna för systemet om en brand uppkommer i en skola, i ett äldreboende eller övrig byggnad och i så fall kan dessa scenarier i Figur 14 slås ihop då konsekvensbedömningen för systemet genomförs. Det är mycket viktigt att alla sådana sammanslagningar inklusive alla scenarioträd dokumenteras på ett adekvat sätt. I dokumentationen bör motiveringar till varför sammanslagningarna är rimliga finnas.

Resultatet från den här typen av analys blir en indelning av riskscenariorymden där kravet på indelningen är (precis som i kapitel 2) att den skall vara fullständig, uppräknelig och disjunkt. Detta kan åstadkommas genom att se till att samtliga riskscenarier som kan inträffa i systemet och som involverar det specifika hotet, exempelvis brand, täcks in av scenariobeskrivningarna. Vidare måste man också

vara uppmärksam på ”överlappningar” mellan scenarier (se början av detta avsnitt). Om man lyckas med detta kommer resultatet att vara en uppsättning riskscenarier för systemet som kan uppkomma om den aktuella påfrestningen på systemet inträffar, d.v.s. hotet realiseras. För vart och ett av dessa riskscenarier skall konsekvenserna för det aktuella systemet bedömas samt sannolikheten att det aktuella riskscenariot inträffar, givet påfrestningen. I den här typen av analys räcker det med en kvalitativ beskrivning av konsekvenserna respektive sannolikheterna.

En kvalitativ analys av sårbarhet kan enkelt kombineras med den typ av analys som tidigare benämns seminariebaserade scenariometoder, exempelvis IBERO, ROSA och MVA (se kapitel 3). I praktiken kan detta åstadkommas genom att vara noga med att genomföra en beskrivning av systemet innan identifieringen av olika riskscenarier inleds (se början av detta avsnitt 4.3) och att vara noggrann med att dokumentera riskscenariorymden, d.v.s. samtliga riskscenarier som kan inträffa i systemet på grund av den aktuella påfrestningen. På grund av resursbegränsningar kan man troligtvis inte beskriva alla typer av riskscenarier lika detaljerat, men det är heller inget krav för att kunna använda metoden. Figur 13 är ett bra exempel på hur det kan gå till. Där framgår att de riskscenarier som kan inträffa antingen innebär att branden inträffar i en byggnad, eller på något annat ställe. Riskscenarier som inträffar i byggnader har beskrivits mer i detalj än bränder på andra ställen. Samma teknik kan användas när olika aktörers förmåga att genomföra olika uppgifter under en kris tas med i analysen, d.v.s. vissa riskscenarier innebär att aktören lyckas med den aktuella uppgiften (exempelvis ordna reservkraft till äldreboenden), medan andra innebär att aktören misslyckas. Båda dessa typer av riskscenarier behöver dock inte analyseras vidare. Det är dock viktigt att göra en (grov) bedömning av konsekvenserna för de riskscenarier som inte beskrivs mer detaljerat.

4.3.3 Kvantitativ analys av sårbarhet

Eftersom den operationella definitionen av sårbarhet är mycket lik den operationella definitionen av risk kan många av de metoder som normalt används för riskanalys även användas för sårbarhetsanalys. Skillnaden är att tillämpningen av metoderna är betingade på att en viss påfrestning drabbat systemet, se kapitel 2. Det finns några viktiga detaljer när det gäller tillämpningen av kvantitativ sårbarhetsanalys som kan vara lämpliga att nämna här.

Innan man genomför en kvantitativ sårbarhetsanalys skall man fråga sig om det är nödvändigt och om det inte räcker med en kvalitativ analys. Om man bör göra en kvantitativ analys beror på målsättningen och syftet med sårbarhetsanalysen, d.v.s. steg 1 ovan. Exempel på syften som vanligtvis kräver en kvantitativ analys är om man önskar att göra jämförelser av sårbarhet mellan olika system eller olika utformningar av samma system. Om syftet kan uppfyllas med hjälp av en kvalitativ analys (möjligtvis med några kvantitativa inslag, vilket diskuterades i föregående

avsnitt) är det vanligtvis bäst att använda en sådan eftersom den typen av analys troligtvis kräver mindre resurser och ställer lägre krav på dynamisk modellering av det aktuella systemet.

Målet med den kvantitativa analysen är att producera en uppsättning riskscenarier som är betingade på en viss påfrestning. För varje riskscenario skall också en sannolikhet, vilken är betingad på att den aktuella påfrestningen inträffat, beräknas. Dessutom skall konsekvenserna för varje riskscenario redovisas. En sådan uppsättning av riskscenarier, sannolikheter och konsekvenser är en approximation av den aktuella sårbarheten, men för att kunna göra jämförelser av olika systems sårbarhet eller för att presentera sårbarheten på ett enkelt sätt måste uppsättningen förenklas. Vanliga mått som används i riskanalyser och som även kan vara användbara för sårbarhetsanalyser är FN-kurvor och individriskkonturer (se exempelvis ”Handbok för riskanalys” [20]), men troligare är att mått som den maximala konsekvensen på grund av en specifik påfrestning och medelvärdet av konsekvenserna på grund av störningen (mätt i någon lämplig konsekvensenhet) är mer användbara för presentation av resultatet från en sårbarhetsanalys.

Det är även möjligt att presentera resultatet av en sårbarhetsanalys som en graf som visar hur ett konsekvensmått ökar som följd av att systemet påfrestas mer och mer. Detta är vad som ofta används för att presentera resultatet när nätverk används för sårbarhetsanalys, se rapporten ”Analys av sårbarhet i teknisk infrastruktur med nätverksmodeller” [24].

Förutom att beräkna mått för ett systems sårbarhet på grund av en viss påfrestning kan man även använda sårbarhetsanalysen för att identifiera scenarier som leder till största möjliga konsekvenser för systemet. Dessa scenarier kan man sedan försöka förebygga genom diverse åtgärder för att minska systemets sårbarhet. Det är också möjligt att genom kvantitativ sårbarhetsanalys identifiera viktiga element i det aktuella systemet, d.v.s. element (agenter eller artefakter) som om de inte fungerar som det är tänkt medför den största ökningen av konsekvenserna på grund av en specifik påfrestning på det aktuella systemet.

Det förmodligen enklaste sättet att genomföra en kvantitativ analys av sårbarhet är att utgå från den teknik som beskrevs i föregående avsnitt, men i stället för att bara genomföra kvantitativa skattningar av konsekvenser och sannolikheter för de olika riskscenarierna så genomförs kvantitativa sådana. Detta innebär att resultatet av en sådan analys blir en uppsättning riskscenarier samt skattningar av deras sannolikheter och konsekvenser, d.v.s. den operationella definition av sårbarhet som föreslagits i rapporten (se avsnitt 2.5).

5 Slutsatser och diskussion

I avsnitt 1.3 redovisas ett antal syften med den här rapporten. I detta kapitel presenteras slutsatser som är relaterade till syftena.

5.1 En operationell definition av sårbarhet

Det finns många definitioner av begreppen risk och sårbarhet, men förhållandevis få av dessa definitioner ger någon vägledning rörande hur risken eller sårbarheten i ett specifikt system kan analyseras. En definition som ger sådan vägledning kallas för en operationell definition och en sådan definition har i rapporten föreslagits för ett systems sårbarhet (se avsnitt 2.5).

Den definition av ett systems sårbarhet som föreslagits i rapporten innebär att sårbarhet uppfattas som svaret på de tre frågorna:

- Vad kan hända, givet en specifik påfrestning?
- Hur sannolikt är det, givet påfrestningen?
- Vad blir konsekvenserna?

Svaren på frågorna kan vara flera, d.v.s. den första frågan ”Vad kan hända, givet en specifik påfrestning?” kan besvaras på flera sätt. Vart och ett av dessa svar motsvaras av ett riskscenario, d.v.s. en händelseutveckling i systemet som är en avvikelse från det normala.

Den kanske viktigaste aspekten av sårbarhetsdefinitionen är att den är *betingad* av att en specifik påfrestning på systemet har inträffat. Man kan alltså inte diskutera ett systems sårbarhet i allmänhet utan man måste specificera vilken påfrestning som avses. Detta har att göra med att ett system kan vara robust mot en typ av påfrestning, exempelvis stormar, men sårbart för en annan, exempelvis översvämningar.

5.2 Metoder för risk- och sårbarhetsanalys

Att ha en klar definition av hur risk och sårbarhet definieras är en förutsättning för att kunna göra en analys av risken eller sårbarheten i ett specifikt system. Med utgångspunkt i den operationella definition av sårbarhet som presenteras i rapporten och den definition av risk som presenterats tidigare [3] går det att diskutera vad en risk- och sårbarhetsanalys egentligen innebär.

5.2.1 Vad är en risk- och sårbarhetsanalys?

I rapporten används begreppet risk- och sårbarhetsanalys något slarvigt för att beteckna en riskanalys *och/eller* en sårbarhetsanalys. Anledningen är att enligt de definitioner av risk och av sårbarhet som används är en riskanalys och en

sårbarhetsanalys mycket nära besläktade och i de sammanhang som begreppen används här behövs det oftast inte göras skillnad på dem.

I lagstiftningen och diverse handböcker förekommer dock begreppet risk- och sårbarhetsanalys och det kan vara bra att klargöra vad en sådan analys skulle kunna innebära med utgångspunkt i de definitioner som används i den här rapporten.

För att göra det måste ett antal olika innebörder av begreppen risk och sårbarhet användas. Begreppen risk och sårbarhet kan betraktas från två perspektiv där det första perspektivet innebär att man betraktar risk och sårbarhet som en egenskap hos ett system. I det fallet kan man exempelvis analysera *brandrisken i ett system*, eller ett *systems sårbarhet för stormar*. Resultatet från sådana analyser innebär att man identifierar vad som kan hända i systemet, hur sannolikt det är och vad konsekvenserna bli. När det gäller sårbarhet är frågorna betingade av den specifika påfrestningen. Detta är en analys enligt den operationella definition av sårbarhet som föreslagits i rapporten.

Det andra perspektivet innebär att man betraktar risk och sårbarhet som en eller flera förhållanden eller omständigheter i det aktuella systemet som gör att de negativa konsekvenserna på grund av vissa händelser blir stora. I det här fallet kan man tala om *en sårbarhet*, eller *en risk*. En sårbarhet eller en risk kan exempelvis vara att stålpelarna i en byggnad är oskyddade mot brand. Detta utgör *en risk* eller *en sårbarhet* eftersom om en brand uppstår kommer de negativa konsekvenserna att bli stora.

Mot bakgrund av dessa olika sätt att betrakta begreppet risk och sårbarhet kan en *risk- och sårbarhetsanalys* exempelvis innebära följande:

- En riskanalys med målet att analysera systemets risk (enligt det första perspektivet ovan) där man försöker att identifiera sårbarheter i system (enligt det andra perspektivet).
- En grov riskanalys med målet att analysera systemets risk (enligt det första perspektivet ovan), samt en sårbarhetsanalys (enligt det andra perspektivet) som är mer detaljerad för några av de riskscenarier som man identifierat i den inledande riskanalysen.

Mot bakgrund av att begreppet *risk- och sårbarhetsanalys* kan tolkas på olika sätt (fler sätt än de två som redovisats ovan är möjliga), kan det vara klokt att redogöra för den tolkning som använts då en analys genomförs.

5.2.2 Inventering av metoder

I kapitel 3 presenteras en inventering av ett antal olika metoder för riskanalys och/eller sårbarhetsanalys. Majoriteten av de metoder som identifierats kan delas in i två grupper *scenariobaserade* och *systembaserade*.

Scenariobaserade metoder karaktäriseras av att de är fokuserade på att beskriva ett eller flera riskscenarier som kan inträffa i framtiden. Vanligtvis resulterar användningen av denna typ av metoder i ett antal relativt väl beskrivna riskscenarier. Exempel på metoder som tillhör den här gruppen är MVA-metoden, ROSA och IBERO.

De systembaserade metoderna fokuserar mera på att beskriva det aktuella systemet som analysen gäller för. Därefter används den systemmodell som byggts upp på ett systematiskt sätt för att identifiera olika riskscenarier som kan inträffa i systemet. Exempel på metoder som tillhör den här gruppen är felträdsanalys, händelseträdsanalys, Hazop och FMEA.

En mer detaljerad beskrivning av inventeringen finns i avsnitt 3.2.

5.2.3 Problem vid genomförandet av en risk- och sårbarhetsanalys

Det finns ett antal problem som måste hanteras då en risk- och sårbarhetsanalys genomförs för komplexa sociotekniska system. Mot bakgrund av den definition av risk och sårbarhet som används i rapporten har några av dessa bedömts vara extra viktiga:

Systemdefinition. För att kunna göra en analys av ett systems risk eller sårbarhet krävs att systemet definieras. En svårighet då systemdefinitionen inte sker uttryckligen i en risk- och sårbarhetsanalys är att det kan uppstå oklarheter rörande vad som faktiskt ingår i analysen. Detta kan i sin tur leda till svårigheter att avgöra om man i en analys lyckats hantera några av de andra problem som tas upp nedan, exempelvis täckningsgradsproblemet. För att hantera detta problem krävs en beskrivning av vad som är elementen i det aktuella systemet och vad som är systemets omgivning. En sådan beskrivning ger också en indikation på vilken detaljeringsgrad som används i analysen, d.v.s. hur noggrant beskrivet är systemet.

Hantering av osäkerhet i analysen. Oavsett om en analys är en riskanalys eller en sårbarhetsanalys måste problemet med att man inte på förhand kan veta vilket/vilka riskscenarier som kommer att inträffa i framtiden hanteras. Vid användning av de operationella definitionerna av risk och av sårbarhet som används i rapporten hanteras detta problem genom att en *uppsättning* riskscenarier identifieras för det aktuella systemet. Visserligen kan uppsättningen bestå av enbart ett enda riskscenario, men i så fall är det tveksamt om detta riskscenario verkligen representerar verkligheten på ett bra sätt, vilket hänger samman med nästa problem som beskrivs nedan. Det mest fundamentala i en riskanalys eller sårbarhetsanalys när det gäller hantering av osäkerhet är att man i analysen uttryckligen beaktar möjligheten att det faktiskt kan uppkomma olika typer av riskscenarier i ett system.

Täckningsgradsproblemet. En riskanalys eller sårbarhetsanalys där osäkerheten rörande vilket/vilka riskscenarier som kommer att inträffa i systemet beaktas på ett adekvat sätt måste även hantera det problem som kallas täckningsgradsproblemet. Detta problem innebär att alla de händelseutvecklingar med negativa utfall som kan inträffa i systemet enligt de avgränsningar som gjorts skall kunna representeras av något av de riskscenarier som har identifierats i analysen. Om en riskanalys exempelvis är gjord för brandrisken i en byggnad måste alla brandscenarier som kan inträffa i byggnaden kunna representeras av något riskscenario som ingår i analysen.

Detaljeringsgrad. En riskanalys eller sårbarhetsanalys kan få problem att uppfylla det syfte som den är avsedd att uppfylla om inte detaljeringsgraden i de riskscenarier som identifierats är tillräckligt hög. Ett exempel som illustrerar detta är en analys av brandriskerna i en byggnad där två riskscenarier identifierats: 1. en brand i byggnaden som orsakar personskador inträffar och 2. en brand i byggnaden som inte orsakar personskador inträffar. Dessa två riskscenarier representerar samtliga brandscenarier som kan inträffa i byggnaden (antingen så uppkommer personskador i en brand, eller så gör det inte det), men detaljeringsgraden i riskscenarierna är så låg att analysen knappast blir användbar.

Sannolikhetsskattningar. Något som kan orsaka problem i en riskanalys eller sårbarhetsanalys är sannolikhetsskattningar. Enligt de definitioner av risk och av sårbarhet som används i rapporten är sannolikheten att ett specifikt riskscenario inträffar en viktig del av begreppen risk och sårbarhet. Det är troligt att det saknas systematiskt insamlad information rörande hur ofta många av de riskscenarier som identifieras i riskanalyser och sårbarhetsanalyser för komplexa sociotekniska system har inträffat. Detta innebär att man i en analys får förlita sig på skattningar av experter, och/eller på logiska modeller (exempelvis felträd). Det bör dock noteras att sannolikhetsskattningar inte nödvändigtvis behöver vara uttryckta med sannolikheter mellan 0 och 1, de kan också uttryckas på en ordinal skala exempelvis genom beskrivningar av typen ”myckets sannolikt”, ”troligt”, ”mindre troligt”, o.s.v.

Beskriver riskscenarierna verkligheten på ett korrekt sätt. Det problem som förmodligen är det svåraste att hantera i riskanalyser och i sårbarhetsanalyser och som hänger ihop med några av de problem som beskrivits tidigare är hur man kan se till att de riskscenarierna som identifierats faktiskt beskriver verkligheten på ett korrekt sätt. Ofta uppstår detta problem i samband med att konsekvenserna av olika riskscenarier skall bedömas, d.v.s. det kan vara svårt att beskriva vad konsekvensen av ett specifikt riskscenario blir. Det är svårt att ge någon generell handledning för hur detta problem skall kunna hanteras, det beror till stor del på vilket typ av system som analyseras. Att ha personer som har god kunskap om systemet involverade i analysen är en bra utgångspunkt för att minska detta problem.

5.3 Att genomföra en risk- och sårbarhetsanalys för ett system

Det sista syftet med rapporten som presenteras i avsnitt 1.3 innebär att rapporten skall ge förslag på hur risk- och sårbarhetsanalyser kan genomföras för att undvika/minimera de potentiella problem som presenteras ovan. I rapporten presenteras förslag på tre olika typer av sårbarhetsanalyser (liknande förslag kan formuleras för riskanalyser). Dessa typer av analyser kan genomföras med kombinationer av de metoder för risk- och sårbarhetsanalys som har identifierats (se avsnitt 3.2).

Den första typen kallas *Grov analys av olika typer av fel* (se avsnitt 4.3.1) och skulle kunna utgöra ett första steg i en mer avancerad sårbarhetsanalys. Själva analysen går ut på att göra en systembeskrivning och systematiskt gå igenom systemets komponenter för att analysera vilka konsekvenserna blir för systemet som helhet om en komponent inte skulle fungera som det är tänkt (oavsett orsak till detta). Fokus i denna metod ligger på att skapa en lämplig systemmodell och därför blir de riskscenarier som identifieras förhållandevis grovt beskrivna. Notera också att den här metoden inte tar utgångspunkt i någon speciell *typ* av påfrestning, exempelvis storm eller terrorattentat. Påfrestningen på systemet är i stället av typen ”element X fungerar inte som det är tänkt”. Resultatet efter användning av metoden blir en systemmodell där systemet beskrivs och element såsom viktiga aktörer och resurser identifieras. Vidare blir resultatet också en beskrivning av ett antal riskscenarier som vart och ett innebär att ett element inte fungerar som det är tänkt. Ett exempel kan vara en kommun där ett riskscenario kan vara att ”Hemtjänsten kan inte leverera mat” och där konsekvenserna kan bli allt ifrån att personer avlider (beroende på hur lång tid matleveranserna inte fungerar) till att inga negativa konsekvenser uppstår.

Nästa analystyp kallas för *Kvalitativ analys av sårbarhet* (se avsnitt 4.3.2) och innebär att olika riskscenarier identifieras för systemet i fråga och att bedömningar av sannolikheter och konsekvenser sker kvalitativt. Den operationella definitionen av sårbarhet som presenteras i rapporten är användbar för denna typ av analys. Analysen innebär att fokus ligger på att beskriva de riskscenarier som kan uppkomma som en följd av en påfrestning och att hantera *täckningsgradsproblemet* (se ovan). Resultatet från en analys av den här typen blir en uppsättning riskscenarier och en kvalitativ beskrivning av deras respektive sannolikhet och konsekvens. Eftersom det är mycket svårt att uttala sig om hur väl genomförd en analys är bara genom att studera detta resultat är det även rimligt att det i analysen inkluderas beskrivningar av hur de olika potentiella problemen som identifierats ovan har hanterats. Detta ger i så fall en indikation på hur väl genomförd analysen är.

Den sista analystypen kallas för *Kvantitativ analys av sårbarhet* (se avsnitt 4.3.3) och innebär i princip samma sak som Kvalitativ analys av sårbarhet med skillnaden att sannolikheter och konsekvenser beskrivs med kvantitativa mått, vilket

möjliggör att sårbarhet kan beskrivas med enklare kvantitativa mått liknande FN-kurvor och individrisk som används i riskanalyser.

5.4 Fortsatt forskning

Den operationella definition av sårbarhet som presenteras i rapporten utgör en grund från vilken metoder för sårbarhetsanalys kan utformas. På så sätt görs resultaten som produceras av olika metoder för sårbarhetsanalys jämförbara, detsamma gäller den operationella definitionen av risk som diskuteras i rapporten och riskanalyser.

En utmaning för framtida forskning inom området är att konkretisera metoder för risk- och sårbarhetsanalys där systemet av intresse är ett komplext socioteknisk system, exempelvis en kommun, region eller en nation. I den här rapporten har några grova förslag på hur framförallt sårbarhetsanalyser kan genomföras för den typen av system presenterats, men det finns mycket mer att göra när det gäller utvecklingen av den typen av metoder.

En annan intressant utmaning för den typen av forskning är att beskriva hur analyser på olika ”nivåer”, exempelvis kommunal, regional och nationell nivå, hänger ihop. En kommun ingår i en region och en region ingår i en nation och därmed bör det också finnas en koppling mellan risk- och sårbarhetsanalyser på de olika nivåerna. Det systembaserade tankesättet som beskrivs i den här rapporten är sannolikt en fruktbar utgångspunkt för forstsatt forskning rörande hur kommunala risk- och sårbarhetsanalyser kan användas på den regionala nivån och hur de regionala analyserna kan ge underlag till en nationell analys.

Ett problem av stor praktisk betydelse som bör studeras mer är hur verkligheten kan beskrivas i termer av en systemmodell så att modellen inte blir alltför praktiskt svårhanterlig, d.v.s. kräver för mycket arbete att skapa och genomföra analyser med, men samtidigt inte blir så grov att den saknar praktiskt värde.

6 Referenser

1. Hallin, P.-O., Nilsson, J. och Olofsson, N., *Kommunal sårbarhetsanalys*, Krisberedskapsmyndigheten, Stockholm, 2004.
2. Kaplan, S., The words of risk analysis, *Risk Analysis*, Vol. 17, s. 407-417, 1997.
3. Kaplan, S. och Garrick, B. J., On the quantitative definition of risk, *Risk Analysis*, Vol. 1:1, s. 11-27, 1981.
4. Abrahamsson, M. och Magnusson, S. E., *Risk- och sårbarhetsanalyser: utgångspunkter för fortsatt arbete*, Krisberedskapsmyndigheten, Stockholm, 2004.
5. Malm, A., Softa, J., Andersson, J. J. och Lindström, K., *IT och sårbarhet - Kritiska beroendeförhållanden i den nationella IT-infrastrukturen*, Krisberedskapsmyndigheten, 2003.
6. Krisberedskapsmyndigheten, *Hot- och riskrapport 2004 - Gränsöverskridande sårbarhet*, KBM:s temaserie, 2004:6, Stockholm, 2004.
7. Krisberedskapsmyndigheten, *Hot- och riskrapport 2005*, KBM:s temaserie, 2005:11, Stockholm, 2005.
8. Krisberedskapsmyndigheten, *Uppföljning av myndigheternas arbete med risk- och sårbarhetsanalyser*, Dnr: 0152/2005, Stockholm, 2005.
9. Kaplan, S., Haimes, Y. Y. och Grarrick, B. J., Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk, *Risk Analysis*, Vol. 21:5, s. 807-819, 2001.
10. Ingelstam, L., *System - att tänka över samhälle och teknik*, Energimyndigheten, Eskilstuna, 2002.
11. Haimes, Y. Y., *Risk Modeling, Assessment, and Management*, John Wiley & Sons, New York, 1998.
12. Ashby, R. W., *An Introduction to Cybernetics*, Chapman & Hall, London, 1956.
13. Apostolakis, G., Probability and Risk Assessment - Subjectivistic Viewpoint and Some Suggestions, *Nuclear Safety*, Vol. 19:3, s. 305-315, 1978.
14. Dilley, M. och Boudreau, T. E., Coming to terms with vulnerability: a critique of the food security definition, *Food Policy*, Vol. 26:3, s. 229-247, 2001.
15. Buckle, P., Re-defining community and vulnerability in context of emergency management, *Australian Journal of Emergency Management*, Vol. 13:4, 1998.
16. Haimes, Y. Y., On the Definition of Vulnerabilities in Measuring Risks to Infrastructures, *Risk Analysis*, Vol. 26:2, s. 293-296, 2006.
17. Keeney, R. L., Raiffa, H., *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*, John Wiley & Sons, New York, 1976.

18. Länsstyrelsen i Stockholms län, *IBERO Steg för steg - Manual*, Stockholm, 2006.
19. Länsstyrelsen i Kronobergs län, *ROSA - en metod för risk- och sårbarhetsanalyser*, Växjö, 2003.
20. Räddningsverket, *Handbok för riskanalys*, Räddningsverket, Karlstad, 2003.
21. Johansson, H., *Decision Analysis in Fire Safety Engineering - Analysing Investments in Fire Safety*, Lund University, Lund, 2003.
22. Haimes, Y. Y., Kaplan, S. och Lambert, J. H., Risk filtering, ranking, and management framework using hierarchical holographic modeling, *Risk Analysis*, Vol. 22:2, s. 383-397, 2002.
23. Mattsson, B., *Riskhantering vid skydd mot olyckor - Problemlösning och beslutsfattande*, Räddningsverket, Karlstad, 2000.
24. Johansson, H., Jönsson, H. och Johansson, J., *Analys av sårbarhet i teknisk infrastruktur med nätverksmodeller*, Rapport 1011, LUCRAM, Lunds universitet, Lund, 2007.
25. McGrattan, K. och Forney, G., *Fire Dynamics Simulator (Version 4) User´s guide*, National Institute of Standards and Technology, Washington, 2006.
26. Bjerketvedt, D., Bakke, J. R. och Van Wingerden, K., Gas explosion handbook, *Journal of Hazardous Materials*, Vol. 52:1, s. 1-150, 1997.
27. Crowther, K. G. och Haimes, Y. Y., Application of the inoperability input-output model (IIM) for systemic risk assessment and management of interdependent infrastructures, *Systems Engineering*, Vol. 8:4, s. 323-341, 2005.
28. Santos, J. R. och Haimes, Y. Y., Modeling the Demand Reduction Input-Output (I-O) Inoperability Due to Terrorism of Interconnected Infrastructures, *Risk Analysis*, Vol. 24:6, s. 1437-1451, 2004.
29. Greenberg Michael, R., Lahr, M. och Mantell, N., Understanding the Economic Costs and Benefits of Catastrophes and Their Aftermath: A Review and Suggestions for the U.S. Federal Government, *Risk Analysis*, Vol. 27:1, s. 83-96, 2007.
30. Fujita, Y. och Hollnagel, E., Failures without errors: quantification of context in HRA, *Reliability Engineering & System Safety*, Vol. 83:2, s. 145-152, 2004.
31. Mosleh, A. och Chang, Y. H., Model-based human reliability analysis: prospects and requirements, *Reliability Engineering & System Safety*, Vol. 83:2, s. 241-254, 2004.
32. Lian, C. och Haimes, Y. Y., Managing the risk of terrorism to interdependent infrastructure systems through the dynamic inoperability input-output model, *Systems Engineering*, Vol. 9:3, s. 241-258, 2006.
33. Haimes, Y. Y., Jiang, P., Leontief-Based Model of Risk in Complex Interconnected Infrastructures, *Journal of Infrastructure systems*, Vol.:7, s. 1-12, 2001.

34. Axelrod, R. och Cohen, M. D., *Harnessing Complexity, Organizational Implications of a Scientific Frontier*, Basic Books, New York, 2000.
35. Rinaldi, S. M., Peerenboom, J.P. och Kelly, T.K., Identifying, understanding, and analyzing critical infrastructure interdependencies, *IEEE Control Systems Magazine*, Vol. 21:6, s. 11-25, 2001.
36. Birka Nät AB, *Kabelbrand i Akallatunneln den 29 Maj 2002 - Haveriutredningens slututlåtande*, Stockholm, 2002.
37. Krisberedskapsmyndigheten, *Krishantering i stormens spår - Sammanställning av myndigheternas erfarenheter*, Dnr: 0257/2005, Stockholm, 2005.
38. Räddningsverket, *Redovisning av erfarenheter av krishanteringsarbetet i samband med orkanen som drabbade södra Sverige i januari 2005, Diarienummer 600-1157-2005*, Karlstad, 2005.
39. Perrow, C., *Normal Accidents*, Princeton University Press, Princeton, 1999.
40. Abrahamsson, M. och Magnusson, S. E., *Användning av risk- och sårbarhetsanalyser i samhällets krishantering - delar av en bakgrundsstudie*, Rapport 1007, LUCRAM, Lunds universitet, Lund, 2004.
41. Watts, D. J. och Strogatz, S. H., Collective dynamics of 'small-world' networks, *Nature*, Vol. 393:6684, s. 440-442, 1998.
42. Albert, R., Jeong, H. och Barabási, A.-L., Internet: Diameter of the World Wide Web, *Nature*, Vol. 401:6749, s. 130-131, 1999.
43. Barabási, A.-L., *Linked : how everything is connected to everything else and what it means for business, science, and everyday life*, Plume, New York, 2003.
44. Barabási, A.-L. och Albert, R., Emergence of Scaling in Random Networks, *Science*, Vol. 286:5439, s. 509-512, 1999.
45. Liljeros, F., Edling, C. R., Amaral, L. A. N., Stanley, H. E. och Åberg, Y., The web of human sexual contacts, *Nature*, Vol. 411:6840, s. 907-908, 2001.
46. Chassin, D. P. och Posse, C., Evaluating North American electric grid reliability using Barabási-Albert network model, *Physica A: Statistical Mechanics and its Applications*, Vol. 355:2-4, s. 667-677, 2005.
47. Albert, R., Jeong, H. och Barabási, A.-L., Error and attack tolerance of complex networks, *Nature*, Vol. 406:6794, s. 378-382, 2000.
48. Holme, P., Kim, B. J., Yoon, C. N. och Han, S. K., Attack vulnerability of complex networks, *Physical Review E*, Vol. 65:056109, 2002.
49. Albert, R., Albert, I. och Nakarado, G. L., Structural vulnerability of the North American power grid, *Physical Review E*, Vol. 69:025103(R), 2004.
50. Holmgren, Å., *Vulnerability Analysis of Electric power Delivery Systems*, Royal Institute of Technology, Stockholm, 2004.

51. Johansson, J., Jönsson, H., Johansson, H., Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions, *Int. J. Emergency Management*, Vol. 4:1, s. 4-17, 2007.
52. Nishiguchi, T. och Beaudet, A., The Toyota Group and the Aisin Fire, *Sloan Management Review*,Vol. 40:1, s. 49-60, 1998.
53. Watts, D. J., *Six degrees - The science of a connected age*, Vintage, London, 2004.
54. Reitman, V., How Toyota Recovered from a Major Fire in Less Than a Week, *Wall Street Journal*, 8 maj, s. A-1, 1997.
55. Krackhardt, D. och Stern, R. N., Informal Networks and Organizational Crises: An Experimental Simulation, *Social Psychology Quarterly*, Vol. 51:2, s. 123-140, 1988.
56. Uhr, C. och Johansson, H., Mapping an emergency management network, *Int. J. Emergency Management*, Vol. 4:1, s. 104-118, 2007.
57. Maslov, S. och Sneppen, K., Specificity and stability in topology of protein networks, *Science*, Vol. 296:5569, s. 910-913, 2002.
58. Pastor-Satorras, R., Vázquez, A. och Vespignani, A., Dynamical and correlation properties of the Internet, *Physical Review Letters*, Vol. 87:258701, 2001.
59. Chappell, L., Nissan's Solution: Modules, *Automotive News*, Vol. 75:5919, s. 1-3, 2001.
60. Perrow, C., Organizing to Reduce the Vulnerabilities of Complexity, *Journal of contingencies and crisis management*, Vol. 7:3, s. 150-155, 1999.
61. Simon, H. A., *The Sciences of the Artificial*, MIT Press, Cambridge, 1996.
62. Ottino, J. M., Complex Systems, *AIChE Journal*, Vol. 49:2, s. 292-299, 2003.
63. Comfort, L. K., *Shared Risk: Complex Systems in Seismic Response*, Pergamon Press, Oxford, 1999.
64. Rothenborg, O., Problemlösare Svensson en av "Gudruns" tysta hjältar, *Dagens Nyheter*, 8 januari, 2006.
65. Krisberedskapsmyndigheten, *Samhällsviktigt! Ett första förslag till samhällsviktig verksamhet ur ett krisberedskapsperspektiv*, Dnr: 0253/2005, Stockholm, 2006.
66. Scott, J., *Social Network Analysis*, Sage Publications, London, 2000.
67. Kaplan, S., Visnepolchi, S., Zlotin, B., Zusman, A., *New Tools for Failure and Risk Analysis - Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring*, Ideation International Inc., Southfield, 1999.