SKI Rapport 2008:49

Forskning

En studie av olyckstredningsmetoders utveckling: En sammanställning över "State-of-the-Art"

Erik Hollnagel
Josephine Speziali

Januari 2008

ISSN 1104-1374
ISRN SKI-R-08/49-SE

SKI

SKI-perspektiv

Bakgrund

Inom svensk kärnkraftindustri har man i stort sett arbetat med en och samma metod för olycksutredning sedan 90-talet. Metoden kallas MTO (Människa-Teknik-Organisation och är baserad på INPOs Human Performance Enhancement System (HPES). För att få en samlad bild av hur metoden står sig i jämförelse med andra metoder och om det fanns anledning att få industrin att pröva nya metoder för att bättre kunna komma åt bakomliggande orsaker och förhindra att händelser upprepas såg SKI ett behov av en översyn och värdering inom området.

Syfte

Projektets syfte var att kartlägga de huvudsakliga olycksutredningsmetoder som utvecklats sedan början av 1990-talet och att ta fram en välgrundad samling av principer eller kriterier som kunde användas för att karakterisera de utvalda metoderna.

Resultat

De olika metoderna kategoriserades efter dimensionerna koppling (från lös till tät koppling av komponenter) och interaktioner (överskådlighet). Detta ledde till fyra grupper där kärnkraftindustrin är en verksamhet som kan hänföras till det komplexa, tätt kopplade systemet och således behöver använda metoder som är anpassade därefter. Exempel på sådana metoder är FRAM (Functional Resonance Accident Model) och STAMP (Systems-Theoretic Accident Modeling and Process).

Majoriteten av de händelser som inträffar och utreds i kärnkraftindustrin skulle dock kunna hänföras till att ha något mindre tät koppling av komponenter och ha mer överskådliga interaktioner. Metoder som passar för den typen av verksamhet är bl.a. CREAM (Cognitive Reliability and Error Analysis) och MTO. Det finns också många händelser som kan utredas med ännu enklare metoder.

För att få vägledning i sitt val av metod kan ett antal frågor ställas, till exempel:

1. Liknade olyckan något som inträffat förut, eller var den ny och okänd? (Referens här bör vara både det specifika verket och hela industrin.)
2. Var organisationen redo att reagera på olyckan, i den betydelsen att det fanns etablerade procedurer och riktlinjer tillgängliga?
3. Kunde situationen snabbt fås under kontroll eller var utvecklingen utdragen?
4. Var olyckan och materiell påverkan begränsat till ett klart avgränsat subsystem (teknologiskt eller organisatoriskt) eller involverade det flera subsystem, eller hela verket?
5. Var konsekvenserna i stort sett förväntade/bekanta eller var de ovanliga eller sällsynta?
6. Var konsekvenserna i proportion till den initierande händelsen eller var de oväntat stora?

Medan det kan vara bekvämt, eller till och med nödvändigt, för en organisation att anamma en specifik metod som standard, ska detta alltid göras medvetet och med en öppenhet att revidera valet när omständigheterna kräver det.

SKI har genom studien fått ökad kunskap om olika metoder och dess användningsområde. Slutsatsen är att ingen specifik metod är den generellt bästa, i den mening att den kan användas för att utreda alla typer av förhållanden. MTO metoden fungerar bra för de händelser som är lite mer komplexa men för enklare händelser kan, av resursskäl, en enklare metod användas. Det viktiga är man är medveten om sina val och vad det innebär för resultatet och att man använder den metod som bäst passar händelsen så att bakomliggande orsaker kan identifieras. Inga händelser förhindras dock genom att de utreds och en förutsättning för det är att det finns en organisation och ett system som tar hand om resultatet från genomförda utredningar och att rätt åtgärder vidtas.

Behov av ytterligare forskning

SKI har i dagsläget inte planerat för någon ytterligare forskning inom området. Däremot följer vi den forskning som bedrivs inom området.

Projektinformation

SKI:s handläggare för projektet har varit Pia Jacobsson.

SKI-referens: SKI 2007/1819, SSM 2008/177
Projektnummer: 200703011

SKI Rapport 2008:49

Forskning

En studie av olyckstredningsmetoders utveckling: En sammanställning över "State-of-the-Art"

Erik Hollnagel
Josephine Speziali

Ecole des Mines de Paris
rue Claude Daunesse
F-06904 Sophia Antipolis Cedex
France

Januari 2008

Sammanfattning

Projektets syfte var att kartlägga de huvudsakliga olycksutredningsmetoder som utvecklats sedan början av 1990-talet. Motivationen är den ökande frekvensen av olyckor som sätter sig upp mot förklaringar i enkla termer, så som orsak-verkanskedjor eller mänskliga fel. Medan komplexiteten hos sociotekniska system är stadigt ökande i alla industriella domäner, kärnkraftsindustrin inräknad, uppdateras olycksutredningsmetoderna bara när deras oförmåga att redogöra för nya typer av olyckor och incidenter blir ofrånkomlig. Olycksutredningsmetoder släpar därför vanligen efter ungefär tjugo år, eller mer, i förhållande till de sociotekniska systemen.

Först identifierades en samling av metoder utifrån den erkända vetenskapliga litteraturen och stora forsknings- och utvecklingsprogram, metoder som begränsar sig till endast riskanalys, tekniska funktionsstörningar, mänsklig tillförlitlighet och säkerhetsstyrning. Detta ursprungliga urval på 21 metoder reducerades sedan till sju metoder för att enbart innehålla egentliga olycksutredningsmetoder och undvika överlappande, eller i stor utsträckning lika metoder.

Det andra steget var att ta fram en samling metoder för att karakterisera metoderna. Utgångspunkten var Perrows (1984) beskrivning av normala olyckor i sociotekniska system. Vilken använder dimensionerna koppling (från lös till tät koppling av komponenter) och interaktioner (från linjära till komplexa). Av praktiska skäl ändrades den andra dimensionen till överskådlighet, eller hur enkelt det är att beskriva systemet, där subkriterierna är detaljnivå, tillgänglighet av en uttalad modell och systemdynamiken. Med detta som grund karakteriserades de sju utvalda metoderna efter vilka system, eller förhållanden, de kan redogöra för. Detta ledde till följande fyra grupper:

1. Metoder lämpade för överskådliga system med löst kopplade komponenter
2. Metoder lämpade för överskådliga system med tätt kopplade komponenter
3. Metoder lämpade för oöverskådliga system med löst kopplade komponenter
4. Metoder lämpade för oöverskådliga system med tätt kopplade komponenter

Antalet metoder i dessa grupper var fyra, tre, noll respektive två.

Ställd inför behovet att utreda en olycka är det nödvändigt att den valda metoden är lämplig för systemet och situationen. Kärnkraftverk anses vara system som vars komponenter är tätt kopplade och som är mer eller mindre oöverskådliga och kräver därför olycksmodeller och olycksutredningsmetoder som klarar av att redogöra för dessa egenskaper. Om en olycka berör hela kärnkraftsverkets verksamhet, måste metoderna passa för system som är tätt kopplade och oöverskådliga, eller möjligen löst kopplade och överskådliga. Rapporten tillhandahåller ett förslag på hur dessa egenskaper kan bestämmas.

Slutsatsen är att ingen specifik metod är den generellt bästa, i den mening att den kan användas för alla förhållanden. Medan det kan vara bekvämt, eller till och med nödvändigt för en organisation att anta en specifik metod som sin standard ska detta alltid göras medvetet och med en öppenhet att ompröva valet när omständigheterna så kräver. Vi måste förvänta oss att de metoder som utvecklas idag om fem eller tio år kommer att vara delvis förlegade, inte för att metoderna har förändrats utan för att de sociotekniska systemens natur förändras, och således även olyckornas natur.

Summary

The objective of this project was to survey the main accident investigation methods that have been developed since the early or mid-1990s. The motivation was the increasing frequency of accidents that defy explanations in simple terms, for instance cause-effect chains or "human error". Whereas the complexity of socio-technical systems is steadily growing across all industrial domains, including nuclear power production, accident investigation methods are only updated when their inability to account for novel types of accidents and incidents becomes inescapable. Accident investigation methods therefore typically lag behind the socio-technological developments by 20 years or more.

The project first compiled a set of methods from the recognised scientific literature and in major major research & development programs, excluding methods limited to risk assessment, technological malfunctions, human reliability, and safety management methods. An initial set of 21 methods was further reduced to seven by retaining only *prima facie* accident investigation methods and avoiding overlapping or highly similar methods.

The second step was to develop a set of criteria used to characterise the methods. The starting point was Perrow's (1984) description of *normal accidents* in socio-technical systems, which used the dimensions of *coupling*, going from loose to tight, and *interactions*, going from linear to complex. For practical reasons, the second dimension was changed to that of *tractability* or how easy it is to describe the system, where the sub-criteria are the level of detail, the availability of an articulated model, and the system dynamics. On this basis the seven selected methods were characterised in terms of the systems – or conditions – they could account for, leading to the following four groups:

1. Methods suitable for systems that are loosely coupled and tractable
2. Methods suitable for systems that are tightly coupled and tractable
3. Methods suitable for systems that are loosely coupled and intractable
4. Methods suitable for systems that are tightly coupled and intractable

The number of methods in each group were four, three, zero, and two, respectively.

Faced with the need to investigate an accident it is essential that the chosen method is appropriate for the system and the situation. Nuclear power plants considered as systems are tightly coupled and more or less intractable and therefore require accident models and accident investigation methods that are capable of accounting for these features. If an accident concerns the NPP operation as a whole, the methods must be suitable for systems that are tightly coupled and intractable. If an accident only concerns the operation of a subsystem or a component, the methods must be suitable for systems that are tightly coupled and tractable, or possible loosely coupled and tractable. The report provides a proposal for how these characteristics can be determined.

The conclusion is that no specific method is the overall best in the sense that it can be used for all conditions. While it may be convenient, or even necessary, for an organisation to adopt a specific method as its standard, this should always be done knowingly and with a willingness to reconsider the choice when the conditions so demand it. In five or ten years we must expect that the methods developed today will have been partly obsolete, not because the methods change but because the nature of socio-technical systems, and therefore the nature of accidents, do.

Innehållsförteckning

1 Syfte

Komplexiteten hos sociotekniska system har under årtionden varit ständigt ökande, något som märkts inom alla industriella domäner, kärnkraft inkluderat. En påtaglig konsekvens av detta är att många av de incidenter och olyckor som förekommer sätter sig upp mot enkla förklaringar som exempelvis orsak-verkankedjor eller mänskliga fel. För att förklara vad som hänt krävs mer genomarbetade tillvägagångssätt, d.v.s. mer sofistikerade modeller och kraftfullare metoder. Olycksmodeller tillhandahåller principer som kan användas för att förklara hur en olycka sker. De är ett bekvämt sätt att referera till den samling av axiom, antaganden, övertygelser och fakta om olyckor som utgör basen för att förstå och förklara specifika händelser. En metod för olycksutredning beskriver, eller till och med föreskriver, hur en utredning ska utföras för att den ska kunna få fram en förklaring till olyckan. Denna beskrivning är vanligtvis en steg för steg beskrivning. Syftet med metoderna är att försäkra sig om att modellens begrepp tillämpas på ett konsekvent och likartat sätt, för att på så vis minska möjligheten för subjektiva tolkningar och variationer. Resultatet av en olycksutredning bör inte bero på personlig erfarenhet och insikt utan ska vila på generaliserad allmän kunskap och vedertaget sunt förnuft.

Utvecklingen av nya metoder och tillvägagångssätt har ofta drivits framåt när etablerade metoder inte räckt till för att förklara nya typer av olyckor och incidenter. En annan drivkraft har varit brist på effektivitet, d.v.s. när rekommendationer och åtgärder baserade på en metod inte gett önskad effekt och förbättring. Nya teoretiska insikter, även om de sällan varit oberoende av ovanstående, har varit en tredje drivkraft.

Syftet med det här projektet är att granska och ge en översikt av de huvudsakliga metoder för olycksutredning som utvecklats sedan början av 90-talet. Arbetet har bestått av två lika viktiga delar. En del var att sammanställa en lista över metoder som motsvarade valkriterierna och att från denna lista välja de metoder som skulle studeras närmare. Den andra delen var att ta fram en välgrundad samling av principer eller kriterier som kunde användas för att karakterisera de utvalda metoderna. Den här granskningen har inte haft till syfte att rekommendera en specifik metod som generellt är den ”bästa” metoden, utan snarare att tillhandahålla en analys av och sammanställning över metoder. Vilken kan tjäna som beslutsunderlag vid val av metod för olycksanalys i specifika fall.

1.1 Olycksutredning och olycksanalys

Trots att projektet fokuserat på metoder för olycksutredning stod det snart klart att de flesta metoder, så väl etablerade som nyare, inriktar sig på olycksanalys snarare än olycksutredning. Skillnaden mellan en metod för utredning och en metod för analys är en skillnad i räckvidd. En olycksutredning omfattar allt från den initiala planeringen av hur olyckan ska utredas, fördelning samt schemaläggande av resurser, insamling av data och information, analys av detta, rekommendationer utifrån analysen, implementering av rekommendationerna och slutligen utvärdering av den effekt dessa fått. En olycksanalys fokuserar på hur en förståelse för vad som skett kan skapas utifrån tillgänglig data och information. En olycksanalys är alltså bara en del av en olycksutredning. Analysen bestämmer dock indirekt hur datainsamlingen utförs, särskilt

om analysmetoden används regelbundet inom organisationen. Vilka rekommendationer som ges begränsas även det i viss mån av vilken analysmetod som väljs (Hollnagel, 2008). Att användandet av en specifik metod för olycksanalys alltså skapar konsekvenser i andra delar av olycksutredningen är inte något som metoderna för olycksanalys normalt sett tar hänsyn till. Eftersom viljan att förstå varför en olycka ägt rum helt uppenbart är den huvudsakliga anledningen att en olycka studeras lägger de flesta metoderna sin tyngdpunkt där och lite, eller ingen, uppmärksamhet ägnas åt de andra delarna av utredningen. Sammantaget gör detta att den här rapporten inte enbart kommer att behandla utredningsmetoder utan även analysmetoder.

2 Bakgrund

En tidigare SKI-rapport (Harms-Ringdahl, 1996) sammanfattade femton olika metoder för riskanalys. Av dessa ansågs följande vara direkt applicerbara i olycksutredningar:

- Avvikelseanalys
- Human Error Analytical Taxonomy (HEAT)
- Management Oversight and Risk Tree (MORT)
- Safety Management and Organization Review Technique (SMORT)

Medan följande två ansågs som potentiellt applicerbara:

- CRisis Intervention in Offshore Production (CRIOP)
- International Safety Rating system (ISRS)

Sammanfattningen av de fyra första metoderna återfinns i Appendix 1 i denna rapport.

2.1 Förändring av risk- och säkerhetsbegreppen

De flesta av de metoder för riskanalys och olycksutredning som idag används inom kärnkraftsindustrin, och många andra industrier, har sitt ursprung i 1960-talet. Detta var en period då metoder för teknisk- eller ingenjörsanalys utvecklades som ett svar på den ökande komplexiteten hos teknologiska system. Exempel **på sådana metoder** är;

1. felträd, som utvecklades 1961 för att utvärdera avfyrningsystemet för Minuteman ICBM, (se Leveson, 1995),
2. Hazard and Operability Analysis (HAZOP) som utvecklades av Imperial Industries i England i början av 1960-talet(CISHC, 1977),
3. Failure Mode and Effects Analysis (FMEA) som ursprungligen utvecklades av den amerikanska militären 1949 men som senare ersatts av Failure Mode,
4. Effects and Criticality Analysis (FMECA) (MIL-STD-1629A, 1980).

En annan period med snabb tillväxt av metoder var början av 1980-talet. Detta skedde huvudsakligen som en svarsreaktion på olyckan vid kärnkraftverket på Three Mile Island i Harrisburg 1979. Olyckan ledde till erkännandet av att mänskliga faktorer och -fel[1] spelade en signifikant roll för säkerheten i den typen av system. Således blev det

[1] På engelska benämnt som *human factors* och *human errors*

nödvändigt att metoder för riskanalyser och olycksutredningar inkluderar mer än bara det teknologiska systemet. Viljan att inkludera den mänskliga faktorn utökades senare till att även täcka in organisationer och organisatoriska faktorer. Något som uppkomsten av ”säkerhetskultur” är ett bra exempel på. Den allvarliga Tjernobylolyckan 1986 manade på utvecklingen ytterligare.

Sedan mitten av 1990-talet har tillväxten fortsatt, men sällan varit innovativ. Denna ökning har skett i respons till det av såväl teoretiker som praktiker, identifierade behovet av en nyorientering av synen på säkerhet. Detta för att kunna utveckla metoder och tillvägagångssätt som är effektivare vid användning och vilar på välgrundade begrepp och föreställningar.

Några av de viktigaste förändringarna och landvinningarna sedan mitten av 1990-talet är:

- ökat fokus på organisatoriska faktorer, en utveckling sporrad av James Reasons bok om organisatoriska olyckor (1997),
- mjukvarans ökade betydelse (tex. begreppet ”Safeware”, Leveson, 1996),
- det förändrade synsättet på kausalitet, från sekventiella- till systemiska modeller (Hollnagel, 2004),
- det tillhörande skiftet i synen på mänskliga fel, från det ”gamla” synsättet till det ”nya” (Dekker, 2006),
- skiftet inom träning, från träning av specifika färdigheter till träning i generell kommunikation och samarbete (Helmreich et al, 1999),
- skiftet från reaktiv till proaktiv, så som beskriven av resilience engineering (Hollnagel, Woods och Leveson, 2006).

Under samma period, sedan mitten av 1990-talet, har den ökande komplexiteten hos sociotekniska system nödvändiggjort utvecklandet av mer kraftfulla olycksutredningsmetoder och analytiska principer. Denna komplexitet, som så träffande diagnostiserats av Perrow (1984), har tyvärr ofta manifesterat sig i form av allvarliga olyckor och visar inga tecken på att avta. Några av de mer välkända exemplen är JCO-olyckan i Tokai-Mura, Japan (1999), olyckan med rymdfärjan Columbia (2003) och flygkollisionen över Überlingen (2002). Utöver dessa finns tusentals små och stora olyckor i praktiskt taget varje industriell domän. Denna utveckling är inte isolerad till en specifik industriell domän, så som kärnkraftsindustrin, utan har ägt rum i många olika industrier och servicefunktioner.

En konsekvens av detta har lett till insikten att olycksutredning och riskanalys är var sin sida av samma mynt såtillvida att de betraktar samma händelse eller fenomen antingen efter att de ägt rum (retrospektiv) eller innan de äger rum (prospektiv). I det prospektiva fallet finns förstås möjligheten att en händelse aldrig kommer att äga rum, att försäkra sig om att så är fallet är själva anledningen till att riskanalyser genomförs. Beroendet mellan olycksutredning och riskanalys har framhävts både av den så kallade andra generationens metoder för Human Reliability Assessment (HRA), särskilt då ATHEANA (Cooper et al., 1996), CREAM (Hollnagel, 1998) och MERMOS (Le Bot et al., 1999) och är även ett centralt antagande inom Resilience Engineering (Hollnagel, Woods & Leveson, 2006).

3 Behovet av och syftet med olycksutredningar

För att kunna försäkra sig om en godtagbar säkerhetsnivå inom kärnkraftsindustrin, så väl som vilken annan komplex industriprocess som helst, är det nödvändigt att lära sig av erfarenheter. Kunskap om vad som inträffat tidigare i en industriell verksamhet, så som ett kärnkraftverk, och särskilt kunskap om varför något gått fel, är nödvändigt för att kunna dra de rätta slutsatserna utifrån tidigare händelser. Sådan kunskap kan antingen fungera för att förhindra en upprepning av samma händelse, för att förhindra förekomsten av liknande händelser, eller för att skydda sig ifrån specifika typer av negativa utfall.

Inom utredning och analys av inträffade händelser är det vanligt att skilja mellan utfall av olika svårighetsgrad. Typiska kategorier är; *olyckor*, *incidenter* och *nära misstag* (Renborg et al., 2007). Traditionen att skilja mellan olika typer av utfall inrättades av Heinrich (1929) som betonade skillnaden mellan *olyckan* och *åverkan (*eller *utfallet)*[2]. Heinrich menar att det är vilseledande att enbart beakta olyckor som leder till större åverkan eftersom det enligt hans egna undersökningar är en 29 till 1 ratio mellan mindre och större åverkan. Han introducerade därför kategorin *nära olyckor*[3], åsyftande de händelser som inte hade någon åverkan alls fast de haft potentiell kraft att ha det (Ibid, sid 4). Från 1980-talet och framåt blev det vanligt att tala om nära misstag, definierade som situationer ”där en olycka kunde ha hänt om ett effektivt och i tid lägligt återhämtande uteblivit” (van der Schaaf & Kanse, 2004), och om incidenter som något mitt emellan olyckor och nära misstag. (Definitionerna har, beroende av vilken domän de används inom, refererat till hur allvarligt utfallet är, t.ex. om människoliv spillts eller ej.) Detta projekt har tittat enbart på olyckor, och inte på incidenter och nära misstag. Det är möjligt, och även troligt, att samma tillvägagångssätt kan användas för att karakterisera hur andra typer av utfall utreds, men att argumentera för detta ligger utanför ramarna för det här projektet.

Syftet med en olycksutredning är, självklart, att förstå varför olyckan ägde rum. Detta tar sig ofta uttryck i ett sökande efter den möjliga orsaken eller orsakerna till olyckan. Sedan slutet av 1970-talet eller början av 1980-talet har det varit vanligt att både söka efter tydligt igenkännbara orsaker (motsvarande Aristoteles verkande orsak[4]) och att peka på mänskliga fel som huvudsaklig orsak till olyckor (se exempelvis Hollnagel, 1998). Vad gäller denna senare tendens är det viktigt att komma ihåg att finnandet av orsaker är en psykologisk snarare än logisk process. Särskilt då, (översatt från Woods et. al., 1994, sid xvii)

---

2 Av Heinrich (1929) benämnt som *accident*, *incident* och *outcome*.

3 Av Heinrich (1929) benämnt som *near-accidents.*

4 Aristoteles föreslog att skillnad görs mellan fyra olika typer av orsaker: (1) den materiella orsaken är det från vilket något är gjort, d.v.s. delarna i ett system, (2) den formella orsaken talar om för oss vad något är, de fundamentala principerna eller generella lagarna, (3) den verkande orsaken är det från vilken förändringen eller slutet av förändringen först börjar, motsvarande det rådande orsak-verkanbegreppet och (4) ändamålsorsaken, eller syftet, är det som någonting existerar eller utförs för, vilket inkluderar både målinriktade och bidragande handlingar och aktiviteter.

”... mänskliga fel inte är en väldefinierad kategori av mänskliga prestationer. Att tillskriva fel till en persons-, grupps- eller organisations handlingar är i grunden en social och psykologisk process och inte en objektiv och teknisk process.”

Få ifrågasätter behovet av att lära sig av erfarenheter, ett lärande som kan ske på många olika sätt och spänner från det noggranna till det ytliga. Att lära sig av erfarenheter innefattar mer än att samla in data från olyckor, incidenter och nära misstag eller att skapa en företagsomspännande databas. Vissa organisationer verkar ändå tro att detta är tillräckligt, troligen på grund av att de förväxlar data med erfarenhet. Men medan data är relativt enkelt att lägga på hög och går att samla in mer eller mindre på rutin så kräver erfarenhet en ansenlig investering i möda och tid mer eller mindre fortlöpande. Olycksutredning är en viktig del av att lära sig från erfarenheter. Några av de grundläggande frågorna som en utredning måste hantera är vad som rapporteras, och när; hur händelser analyseras; hur resultat används och meddelas samt vilka effekterna är på säkerheten och det dagliga arbetet.

En olycksutredning sker alltid enligt en metod eller procedur. Det finns flera olika metoder tillgängliga, både mellan och inom olika domäner och dessa kan variera med avseende på hur välformulerade och hur välgrundade de är. Vikten av en bra metod ska inte underskattas. Den valda metoden kommer att leda utredningen till att titta närmare på vissa saker och inte på andra. En grundorsaksanalys kommer till exempel ha en tendens att söka efter en bestämd orsak medan en ”Swiss cheese”- eller epidemiologisk analys kommer tendera att söka efter latenta förhållanden. Det är helt enkelt inte möjligt att börja en utredning med ett helt öppet sinne, på samma sätt som det är omöjligt att passivt ”se” vad som finns där. Olycksutredningar , så väl som sökningar i allmänhet, verkar följa en What-You-Look-For-Is-What-You-Find[5]-princip (WYLFIWYF) Hollnagel, 2008). Eftersom valet av utredningsmetod alltid kommer att påverka utredningens resultat är det viktigt att utredare inte bara känner till metoderna de använder, i den mening att de är skickliga användare, utan även att de känns vid de explicita och implicita antaganden som de olika metoderna gör.

4 Den ökande komplexiteten hos sociotekniska system

Den huvudsakliga anledningen för att utveckla en ny metod för olycksutredning är, som beskrivits ovan, att en större olycka som utmanar de befintliga metoderna ägt rum. Skälet till att detta sker är helt enkelt att sociotekniska system, drivna av en kombination av teknologisk innovation, kommersiella avväganden och användarkrav, utvecklas kontinuerligt och i rask takt. I kontrast till detta utvecklas metoder för riskanalys och säkerhetsstyrning i en mycket lugnare takt, om de överhuvudtaget utvecklas, vilket innebär att de sällan kan representera eller adressera den faktiska komplexiteten hos industriella system. I den mån metoder utvecklas är det ofta som en försenad reflektion över ”nya” typer av olyckor. Resultatet av detta är exempelvis ett fokus på en specifik, framträdande faktor hos en händelse (t.ex. överträdelser, efter Tjernobylolyckan), eller att metoderna blir mer omfattande genom försök att samla den kollektiva erfarenheten och förändringar i synsätt (t.ex. den andra generationens HRA-metoder).

Olycksförebyggande-, riskreducerande- och säkerhetsökande åtgärder måste självfallet hänvisa till den etablerade förståelsen eller det som är allmänt accepterat som stat-of-

---

5 *Det du söker efter är vad du finner*

the-art. Om något, trots dessa försiktighetsåtgärder, inträffar är det alltså något som inte kunde ha hanterats av de metoder och modeller som använts, d.v.s. något som går bortom den etablerade förståelsen. Sådana händelser utmanar de existerande metoderna och kan därför inte adekvat förklaras med hjälp av dem.

En viktig karakterisering, för att inte säga förklaring, av denna utveckling gavs av den amerikanska sociologen Charles Perrow i en bok kallad *Normal Accidents* (Perrow, 1984). Denna boks grundtes är att (det västerländska) samhället, som det såg ut då, och i synnerhet de teknologiska miljöer som utgjorde det samhällets grund, hade blivit så komplexa att olyckor tvunget måste inträffa. Olyckor var alltså en oundviklig del av att använda och arbeta med komplexa system, och således normala snarare än sällsynta förekomster. Sedan Perrow publicerade sina analyser har varken de sociotekniska systemen eller de problem som följer dem blivit mindre komplexa.

Perrow baserade sitt resonemang på en genomgång av en stor mängd data från olika typer av olyckor och katastrofer. Områden som inkluderades i studien var kärnkraftverk, oljeraffinaderier, flygplan och flygbolag, marina verksamheter, jordbundna system (så som dammar, gruvor och sjöar), samt slutligen exotiska system (så som rymduppdrag, vapen och DNA). Listan är väldig, detta trots att stora olyckor så som Challenger, Tjernobyl och Zebrűgge inte finns med eftersom de inträffade först efter att boken givits ut.

Perrow föreslår två deskriptiva dimensioner för att karakterisera olika typer av olyckor: interaktionens komplexitet och komponenternas koppling. Med avseende på interaktionens komplexitet så kännetecknas ett komplext system, i motsats till ett linjärt system, av följande:

- Indirekta eller inferentiella informationskällor.
- Begränsad isolering av icke-fungerande komponenter.
- Begränsad utbytbarhet hos utrustning och material.
- Begränsad förståelse för vissa processer (associerade med kemiska omvandlingsprocesser).
- Många kontrollparametrar med potentiell interaktion.
- Många beröringspunkter mellan komponenter som inte befinner sig i en produktionssekvens.
- Specialisering hos personalen begränsar medvetenhet av beroendeförhållanden
- Platsbrist mellan utrustning.
- Okända eller oavsiktliga återkopplingsloopar.

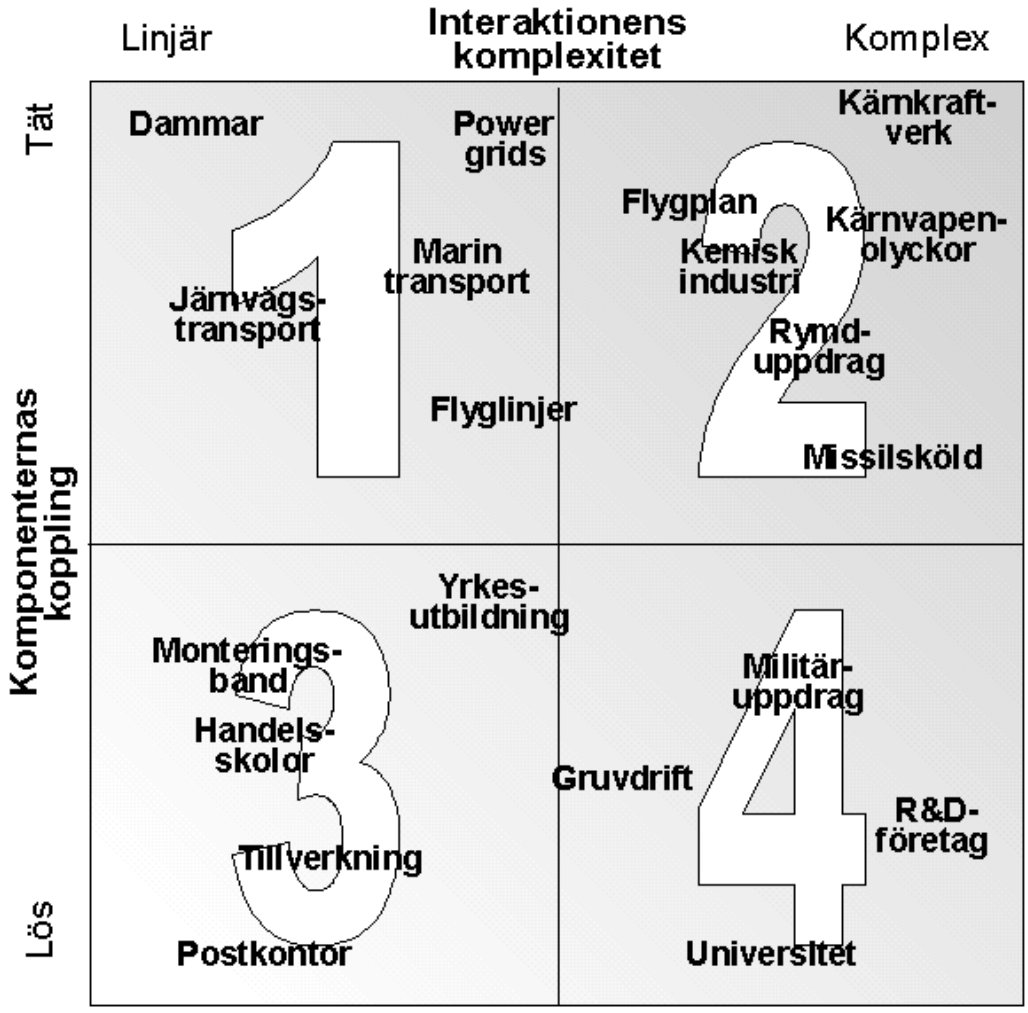
Enligt Perrow så är komplexa system svåra att förstå samt instabila på så vis att området inom vilka gränser driften är säker (*the normal performance envelope*) är ganska litet. Vidare hävdar han att anledningen till att vi har komplexa system helt enkelt är att vi inte vet hur vi kan åstadkomma samma saker med linjära system. Och när de komplexa systemen en gång skapats behåller vi dem eftersom vi har gjort oss själva beroende av det de producerar.

System kan också beskrivas utifrån komponenternas koppling, vilken kan variera mellan att vara tät och lös. Med koppling menas att subsystem och/eller komponenter är kopplade eller funktionellt beroende av varandra. Tätt kopplade system känns på följande egenskaper:

- Buffert och redundans är en del av designen och alltså avsiktligt.
- Förseningar i processen är inte möjliga.

- Händelseförloppet är konstant.
- Utbytbarhet hos tillgångar, utrustning och personal är begränsad och innefattad i designen.
- Det tillåtna spelrummet vad gäller tillgångar, utrustning och personal är litet.
- Det finns bara ett sätt att nå målet.
- Tätt kopplade system är svåra att kontrollera då en händelse i en del av systemet snabbt sprider sig till andra delar.

Perrow använde dessa två dimensioner (interaktionens komplexitet och komponenternas koppling) för att illustrera skillnader mellan olika typer av system, jämför figur 1.



Figur 1. Koppling-interaktionsdiagrammet (Perrow, 1984)

Med olyckspotential i åtanke är den allra värsta kombinationen självklart det komplexa, tätt kopplade systemet. Perrows främsta exempel på ett sådant system är kärnkraftverket, med Harrisburgolyckan som fallstudie. Andra system som tillhör samma kategori är exempelvis flygplan och kemisk industri. Det är troligtvis inte en slump att de system som Perrow beskriver i sin bok alla kännetecknas av att de har en tät koppling mellan sina komponenter och enbart skiljer sig åt i grad av komplexitet hos interaktionen. De flesta systemen som beskrivs ligger i den andra kvadranten.

Perrows tes, så som visad i figur 1, är relevant för olycksutredningsmetoder eftersom förklaringen till olyckan måste kunna redogöra för interaktionens natur och hur tätt eller löst kopplade komponenterna i systemet är. Om vi, för att skapa ett förtydligande exempel, refererar till de fyra kvadranterna i figur 1 så står det klart att systemen i den tredje kvadranten skiljer sig avsevärt från systemen i den andra kvadranten. En metod som är lämplig för att förklara en olycka i ett system ur tredje kvadranten (t.ex. en personskada vid ett monteringsband) kommer knappast att vara tillräcklig för att förklara en olycka i ett system ur andra kvadranten (t.ex. en INES-händelse på ett kärnkraftverk). (Även om det omvända förhållandet inte nödvändigtvis råder kan det vara ineffektivt att använda mer komplexa och kraftfulla metoder för att utreda olyckor i enkla system.) Diagrammet utgör alltså en extern referensram för olycksmetoder, som ett komplement till de mer traditionella krav, så som konsekvens, tillförlitlighet, användbarhet, etc.

5 En första sammanställning av metoder

Även om helt nya metoder är relativt sällsynta så finns det ett stadigt inflöde av metoder på ”marknaden”. De flesta av dessa är dock variationer av de grundläggande angreppssätten, antingen för att tillgodose behoven i en viss domän eller applikation, eller som ett resultat av undersökningar, forskningsprojekt etc.

Det är praktiskt taget omöjligt att lista alla de metoder som introducerats under de senaste 10-15 åren. Istället har en sammanställning av metoder som blivit erkända i den allmänna vetenskapliga litteraturen och i de stora forsknings- och utvecklingsorganisationerna gjorts. För att skapa sammanställningen har ett antal rapporter och undersökningar så som CCPS (1992), DOE (1999) och Sklet (2002) använts. De metoder som redan beskrivits av Harms-Ringdahl (1996) (Avvikelseanalys, HEAT, MORT och SMORT) har inte inkluderats i sammanfattningen. **(**Som tidigare nämnts återfinns sammanfattningen av dem i Appendix 1.**)** Metoder som i huvudsak är tänkta för riskanalys (t.ex. Bayesianska nätverk kombinerade med felträd, teknologiska funktionsstörningar (t.ex. Sneak Path Analysis), mänsklig tillförlitlighet (t.ex. ATHEANA) eller metoder för säkerhetsstyrning (t.ex. TRIPOD).

Den första sammanställningen av metoder, med ovanstående urvalskriterier tillämpade, resulterade i en lista med 21 metoder för olycksutredning eller olycksanalys. Dessa metoder beskrivs kortfattat i Tabell 1, nedan.

Tabell 1: En första sammanställning av metoder för olycksutredning

Akronym	Metodnamn	Kort beskrivning	Referens
AEB	Accident Evolution and Barrier Analysis	AEB-modellen tillhandahåller en metod för analys av händelser och olyckor som modellerar utvecklingen mot en händelse/olycka som en serie av interaktioner mellan människan och tekniska system.	Svensson (2001)
BA	Barrier Analysis	BA används för att identifiera faror associerade med en olycka och de barriärer som skulle ha varit på plats för att förhindra den. En barriär är ett medel, vilket som helst, använd för att kontrollera, förhindra eller dämpa möjligheten för faran att nå sitt mål.	Dianous & Fiévez (2006)

Akronym	Metodnamn	Kort beskrivning	Referens
CA	Change Analysis	Den här tekniken används för att undersöka en olycka genom att analysera skillnaden mellan vad som skedde före, eller förväntades ske och den faktiska sekvensen av händelser. Utredaren som genomför förändringsanalysen identifierar specifika skillnader mellan den olycksfria situationen och olycksscenariot. Dessa skillnader utvärderas sedan för att avgöra huruvida de bidrog till olyckan.	DOE (1999)
CREAM	Cognitive Reliability and Error Analysis	CREAM kan användas både prospektivt och retrospektivt. Den retrospektiva användningen (olycksanalys) baseras på en distinktion mellan det som kan observeras (fenotyper) och det som måste tolkas ut (genotyper). De genotyper som används i CREAM är fördelade på tre kategorier: individuella, teknologiska och organisatoriska.	Hollnagel (1998)
ECFC	Events and Causal Factors Charting	EFCF är ett sätt att visualisera en olyckas kronologiska ordning och metoden används i huvudsak för att samla och organisera bevisning för att avbilda sekvensen av händelser i en olycka.	DOE (1999)
ECFCA	Events and Causal Factors Charting and Analysis	ECFCA kan användas för att bestämma de kausala faktorerna hos en olycka. Denna process är ett viktigt förstasteg för att senare kunna bestämma grundorsakerna till en olycka. ECFCA kräver deduktiv bevisföring för att bestämma vilka händelser och/eller villkor som bidrog till olyckan.	DOE (1999)
FRAM	Functional Resonance Accident Model	En metod för olycksutredning så väl som riskanalys, baserad på beskrivningen av systemfunktioner. Icke-linjär spridning av händelser beskrivs i termer av funktionell resonans.	Hollnagel (2004)
HERA	Human Error in ATM	HERA är en metod för att identifiera och kvantifiera den mänskliga faktorns påverkan i en incident-/olycksutredning, säkerhetsstyrning och bedömning av potentiella, nya typer av fel som kan uppstå till följd av ny teknik. Mänskliga fel ses som en potentiellt svag länk i ATM-systemet och åtgärder måste därför vidtas för att förhindra fel och deras effekter, samt för att maximera andra mänskliga kvaliteter så som upptäckande av fel och återhämtande av situationer**.** HERA grundar sig på antagandet att mänskliga fel är den största bidragande faktorn till olyckor och incidenter.	Isaac et al. (2002)

Akronym	Metodnamn	Kort beskrivning	Referens
HFACS	Human Factors Analysis and Classification System	HFACS identifierar de mänskliga orsakerna till en olycka och tillhandahåller ett verktyg som inte enbart underlättar utredningsprocessen utan även stödjer uppsättande av mål för träning och förebyggande åtgärder. HFACS tar fyra olika nivåer (vilka återknyter till the Swiss cheese model) av mänskliga fel beaktande . Dessa nivåer inkluderar icke-säkra handlingar (operatörens fel), förutsättningar för icke-säkra handlingar (så som sömnighet och bristfällig kommunikation), icke-säker ledning (exempelvis att para samman och låta två oerfarna flygare utföra ett svårt uppdrag) samt organisatorisk påverkan (så som brist på flygtid på grund av budgetrestriktioner).	FAA/NTIS (2000)
HFIT	Human Factors Investigating Tool	HFIT utvecklades från en teoretisk utgångspunkt med referenser till existerande verktyg och modeller. Det samlar in fyra typer av information om den mänskliga faktorn; a) fel som uppträder direkt innan incidenten, b) återhämtningsmekanismer, i nära misstag-fallen, c) tankeprocesserna som lett fram till felet samt d) de underliggande orsakerna.	Gordon, Flin & Mearns (2005)
HINT - J-HPES	HINT - J-HPES	HINT är en utveckling av J-HPES, den japanska versionen av INPOs Human Performance Enhancement System, se nedan. Den övergripande principen är att använda grundorsaksanalys av små händelser för att identifiera trender och använda som en bas för att förhindra olyckor. Metoden består av ett antal steg (liknande stegen i SAFER, vilken beskrivs senare). Dessa är; Steg 1: Förstå händelsen. Steg 2: Samla in och klassificera data. Steg 3: Orsaksanalys, med hjälp av grundorsaksanalys. Steg 4: Förslag till motåtgärder.	Takano et al. (1994)
HPES	Human Performance Enhancement System	En metod sponsrad av INPO som nyttjar en hel familj av tekniker för att utreda händelser, med särskilt fokus på att bestämma aspekter av den mänskliga prestationen. HPES metodologin innefattar flera verktyg, så som uppgiftsanalys, CA, BA, orsak-verkananalys samt ECFC. Vidare har ett flertal liknande metodologier utvecklas utifrån HPES och där det varit nödvändigt anpassats för att passa individuella organisationers specifika krav.	INPO (1989)
MTO	Människa-Teknik-Organisation	Grunden för MTO-analysen är att mänskliga-, tekniska- och organisatoriska faktorer ska få lika stort fokus i en olycksutredning. Metoden är baserad på HPES.	Rollenhagen (1995), Bento (1992)
PEAT	Procedural Event Analysis Tool	Syftet med PEAT är att hjälpa flygbolag att utveckla effektiva åtgärder för att förhindra förekomsten av framtida liknande fel. PEAT-processen bygger på ett icke-straffande angreppsätt för att identifiera de för en besättnings besluts huvudsakligen bidragande faktorerna. Genom att använda den här processen kan flygbolagets säkerhetsansvarige komma med rekommendationer inriktade mot att kontrollera de bidragande faktorernas effekt. PEAT innehåller databaslagring, analys och rapporteringsmöjlighet.	Moodi & Kimball (2004)

Akronym	Metodnamn	Kort beskrivning	Referens
RCA	Root cause analysis	RCA (grundorsaksanalys) identifierar underliggande bristfälligheter i ett säkerhetsstyrningssystem vilka, om de åtgärdas, skulle förhindra samma och liknande olyckor från att hända igen. RCA är en systematisk process som använder den fakta och resultat från analysen för att bestämma de viktigaste anledningarna till en olycka.	T.ex. IAEA (1999)
SAFER	SAFER 2007	SAFER är en allmän metod för olycksutredning utvecklad av TEPCO (J) bestående av 8 steg. Steg 1: Förstå Human Factors Engineering, Steg 2: Skapa ett flödesschema över händelserna: arrangera information för att förstå en händelsers detaljer och för att ha som utgångspunkt för kommunikation och spridande av information, Steg 3: Fånga upp problematiska sidor, Steg 4: Skapa ett kausalt diagram över bakgrundsfaktorer (Background Factors Causality Diagram), Steg 5: Skapa åtgärder som kapar de kausala kopplingarna mellan bakgrundsfaktorerna (enl. diagrammet eller flödesschemat), Steg 6: Rangordna åtgärderna, Steg 7: Implementera åtgärderna, Steg 8: Utvärdera resultatet.	Yoshizawa (1999)
SCAT	Systematic Cause Analysis Technique	SCAT har utvecklats av The International Loss Control Institute (ILCI) för att stödja utredningen av arbetsincidenter. ILCIs ”Loss Causation Model” utgör ramverket för SCAT-systemet. Resultatet av en olycka är förluster, t.ex. skada på personer, egendom, produkter eller miljö. En incident (i det här fallet åsyftas kontakten mellan energikällan och ”offret”) är händelsen som föregår förlusten. Den omedelbara orsaken till olyckan är de omständigheter som föregick kontakten. Dessa kan normalt ses eller anas. De kallas ofta för icke-säkra handlingar eller -förhållanden men i ILCI-modellen används termerna undermåliga handlingar (eller undermåligt utövande) samt undermåliga förhållanden.	Bird & Germain (1985)
STAMP	Systems-Theoretic Accident Modeling and Process	STAMP grundar sig på hypotesen att systemteori är ett användbart sätt att analysera olyckor, särskilt då systemolyckor. Olyckor uppstår när externa störningar, komponenthaveri eller dysfunktionell växelverkan mellan systemkomponenter inte hanteras korrekt av kontrollsystemet. Säkerhet betraktas som ett kontrollproblem och styrs av en kontrollstruktur som är inbäddad i ett adaptivt socioteknisk system. För att förstå varför en olycka ägt rum krävs ett fastställande av varför kontrollstrukturen var ineffektiv. För att förhindra framtida olyckor krävs att kontrollstrukturen designas så att den stärker de nödvändiga restriktionerna. System anses vara relaterade komponenter som hålls i en dynamisk jämvikt av återkopplingsloopar.	Leveson (2004)

Akronym	Metodnamn	Kort beskrivning	Referens
STEP	Sequentially Timed Events Plotting	STEP föreslår en systematik process för olycksutredning baserad på en multi-linjär sekvens av händelser, samt att olycksfenomenet betraktas som en process. Att betrakta en olycka som en process innebär att en olycka betraktas som något som börjar med den händelse som startade omvandlingen från den beskrivna processen till olycksprocessen. En olycka slutar med den senast skadliga händelsen som hänger samman med den olycksprocessen.	Hendrick & Benner (1987)
Swiss cheese	Reason's Swiss Cheese model	Schweizerostmodellen av olycksorsaker är en modell använd inom riskanalys och riskhantering i mänskliga system. Det liknar systemet vid multipla skivor med schweizerost, stående på högkant efter varandra. Modellen föreslogs ursprungligen av den brittiske psykologen James T. Reason 1990 och har sedan dess erhållit en omfattande acceptans och användning inom sjukvård, flygsäkerhetsindustri och räddningstjänst.	Reason (1990, 1997)
TRACEr	Technique for Retrospective Analysis of Cognitive errors	TRACEr tillhandahåller en teknik för att identifiera mänskliga fel och har specialiserats för användning inom flygtrafikledningsdomänen. Den bygger på felmodeller (error models) från andra fält och integrerar Wickens (1992) modell över informationsbehandling i flygledning. TRACEr visualiseras med hjälp av en serie av diagram över beslutsflöden. Metoden markerar ett skifte bort från de kunskapsbaserade felen, som återfinns i andra verktyg, mot att bättre reflektera den visuella och auditiva naturen hos flygledning.	Shorrock & Kirwan (1999, 2002)

Det står klart, även från den kortfattade beskrivningen ovan, att många metoder är besläktade, i den mån att de hänvisar till samma huvudprinciper. Detta exemplifieras av de olika metoder som fokuserar på barriärer, eller de metoder som studerar grundorsaker. Det är därför nödvändigt att göra ett mindre urval av metoder som förtjänar en närmare betraktelse. För att kunna göra detta är det nödvändigt att först överväga på vilka kriterier ett sådant urval kan göras.

6 Kriterier för jämförelse av metoder för olycksutredning

Vid kartläggning av metoder är det vanligt att föreslå någon form av urvalskriterier enligt vilka den ”bästa” metoden, eller metoderna, kan hittas. Detta sker för olycksutredningsmetoder såväl som andra typer av metoder (se t.ex. Swain, 1989 eller Kirwan 1994). Syftet med det här projektet har dock inte varit att finna en ”bästa” metod utan att tillhandahålla ett beslutsunderlag för att välja en metod som passar det givna syftet, med andra ord ett sorts beslutsstöd.

I en studie utförd på uppdrag av the Occupational Safety and Health Administration (OSHA) i USA, klassade Benner (1985) 14 olika olycksmodeller och 17 olika olycksutredningsmetoder som användes av statliga organ. Han började med en samling bedömningskriterier och ett klassificeringsschema utvecklat från användarinformation, förordningar, tillämpningar och arbetsprodukter.

Detta resulterade i en uppsättning på tio kriterier som användes för att klassificera olycksmodellerna (se Tabell 2). De flesta av dem berör kvaliteten hos analysens resultat (realistiskt, definitiv, tillräckligt, grundlig, disciplinerande, konsistent, vägledande samt förståelig eller synlig) snarare än modellen som sådan, även om detta i viss mån även reflekterar modellens egenskaper. Två av Benners kriterier är mer direkt relaterade till olycksmodellens natur, nämligen att den ska vara funktionell och icke-kausal.

Tabell 2: Benners (1985) kriterier för klassificering av olycksmodeller

Kriterium	**Definition**
Realistisk	En utredning ska resultera i en realistisk beskrivning av de händelser som i verkligheten ägt rum.
Definitiv	En utredningsprocess ska tillhandahålla kriterier för att identifiera och definiera den data som krävs för att beskriva vad som hänt.
Tillräcklig	Resultaten ska vara tillräckliga för de som initialiserade utredningen och andra individer som kräver resultat från utredningen.
Grundlig	En utredningsprocess ska vara grundlig så att det inte råder något tvivel om vad som hände, inga oväntade luckor eller hål i förklaringen och inga otydligheter vad gäller förståelsen ska uppstå hos rapportens läsare.
Disciplinerande	En utredningsprocess ska tillhandahålla ett ordnat, systematiskt ramverk och en uppsättning instruktioner för att styra utredarnas uppgifter så att ansträngningarna läggs på de viktiga uppgifterna och för att undvika upprepning av uppgifter och utförande av irrelevanta uppgifter.
Konsistent	Modellen måste vara teoretiskt konsistent med begreppen i det aktuella organets säkerhetsprogram.
Vägledande	Utredningsprocessen ska tillhandahålla resultat som inte kräver ytterligare datainsamling innan de nödvändiga kontrollerna kan identifieras och förändringar göras.
Funktionell	En utredningsprocess ska vara funktionell för att göra arbetet effektivt, t.ex. genom att hjälpa utredaren att avgöra vilka händelser som var en del av olycksprocessen och vilka som inte var det.
Icke-kausal	En utredning ska utföras i ett icke-kausalt ramverk och resultera i en objektiv beskrivning av händelserna i olycksprocessen. Att tillskriva orsaker eller skuld ska endast göras separerat från utredningen, och efter att förståelsen för olycksprocessen är fullbordad, om detta krav ska vara uppfyllt.
Förståelig eller synlig	Resultatet ska vara lätt att förstå.

Benners ursprungliga antagande var att alla olycksutredningsprogram drivs av olycksmodeller och att metoderna därför kan värderas utifrån allmänna kriterier. Men hans analyser ledde honom till slutsatsen att så inte var fallet. Istället identifierades tre olika typer av relation mellan olycksmodeller och utredningsmetodik. I det första fallet kom olycksmodellen före olycksutredningsmetoden och den förra bestämde således den senare. I det andra fallet var situationen den omvända, nämligen den att utredningsmetoden bestämde olycksmodellen. Slutligen, i det tredje fallet, var det en utvald (formellt antagen inom organisationen, eller traditionell) analys metod som skulle bestämma både olycksmodellen och utredningsmetoden, utan att modellen eller

utredningsmetodiken påverkat varandra. Med denna slutsats i åtanke utvecklade Benner senare separata kriterier för att utvärdera olycksutredningsmetoder. Dessa kriterier återfinns i tabell 3.

Tabell 3: Benners (1985) kriterier för klassificering av metoder för olycksutredning

Kriterium	**Definition**
Uppmuntran	Metoden måste uppmuntra harmoniskt deltagande.
Oberoende	Metoden måste ge oklanderligt resultat.
Initiativ	Metoden måste stödja personliga initiativ.
Upptäckt	Metoden måste stödja varseblivning av problem i tid.
Kompetens	Metoden måste öka den anställdes kompetens.
Standarder	Metoden måste kunna uppvisa bestämda åtgärder.
Upprätthållande	Metoden måste upprätthålla accepterade förväntningar och beteendenormer.
Delstater	Metoden måste uppmuntra delstaterna att ta ansvar.
Exakthet	Metoden måste vara behjälplig i att testa resultatets exakthet.
Sluten cirkel	Metoden måste vara kompatibel med undersökningar (eller säkerhetsanalyser) av potentiella olyckor.

Det är intressant att notera att även här gäller kriterierna aspekter vid användandet av metoderna (t.ex. uppmuntran och initiativ) snarare än aspekter hos metoderna som just metoder (tillförlitlighet, eller oberoende av användarens kunskaper).

(Det kan vara av intresse att notera att de tre, enligt Benners kriterier, bästa olycksmodellerna var: the Event Process model, the Energy Flow Process model samt the Fault Tree model. Samt att de tre bästa olycksutredningsmetoderna var: Event Analysis, the MORT system samt Fault Tree Analysis. Benner avslutade sin granskning genom att rekommendera både att ”signifikanta ändringar av olycksutredningsprogrammen borde övervägas i de organ och organisationer som använde de lågt rankade olycksmodellerna eller utredningsmetodologierna” samt att ”det fanns ett tvingande behov för mer uttömmande forskning kring val av olycksmodeller och olycksutredningsmetodologier”. Sklet (2002) har använt samma kriterier för att studera 15 olika metoder men karakteriserar dem enbart i en avslutande tabell utan att ranka dem.

Ett annat angreppssätt återfinns i en genomgång av olycksmodeller och klassificering av fel (Hollnagel, 1998), som föreslår följande sex kriterier (tabell 4):

Tabell 4. Hollnagels (1998) kriterier för att klassificera olycksmodeller och -metoder.

Kriterium	**Definition**
Analytisk förmåga	Analytisk förmåga är förmågan hos varje angreppssätt att stödja en retrospektiv analys av händelser som involverar mänskliga felhandlingar. Resultatet från en retrospektiv analys bör vara en beskrivning av de kännetecknen av mänsklig kognition som återfinns bland de antagna orsakerna.
Förutsägande förmåga	Förutsägande förmåga är förmågan hos varje angreppssätt att förutse de troliga typerna av felhandlingar (fenotyper) för en specifik situation. Om möjligt bör förutsägelsen även innefatta omfattningen och allvaret av den felhandlingen.
Teoretisk förankring	Teoretiskt innehåll, i vilken utsträckning som modeller skapade inom de olika angreppssätten har sin grund i en tydligt identifierbar modell av mänskliga handlingar.
Relation till befintliga taxonomier	Relationen till och/eller beroende av existerande klassificeringsscheman, i vilken utsträckning var och en av angreppssätten är länkade med användbara system för att klassificera de felhandlingar som äger rum i en verklig processverksamhet.
Användbarhet	Användbarheten hos varje angreppssätt, d.v.s. hur enkelt angreppssättet kan omsättas i en praktiskt användbar metod eller göras operationell.
Kostnadseffektivitet	Den relativa kostnaderna och fördelarna som är associerade med de olika angreppssätten.

De ovanstående kriterierna är mer direkt riktade mot metodens kvaliteter, både i avseende på dess teoretiska grund och på dess effektivitet. I viss mån tar kriterierna hänsyn till såväl olycksmodellen (analytisk förmåga, prospektiv förmåga, teknisk grund samt relation till befintliga taxonomier) som utredningsmetoden (användbarhet samt kostnadseffektivitet).

Utöver kriterier för att skilja mellan metoder, för att på så vis kunna göra ett grundat metodval i en specifik situation, finns mer praktiska kriterier som är gemensamma för alla metoder:

- **Tillförlitlighet –** huruvida metoden kommer att ge samma resultat om den tillämpas igen (eller på ett liknande fall), och till vilken grad metoden är oberoende av användaren och hans/hennes kunskaper och erfarenheter.
- **Granskningsbarhet –** huruvida det är möjligt att spåra analysens gång och återskapa de val, beslut eller kategoriseringar som gjorts under analysen. (Detta motsvarar Benners kriterium om att en utredningsprocess ska vara grundlig.)
- **Inlärningstid** – hur lång tid det tar att lära sig att använda metoden och att bli en skicklig användare. Även om den tid som läggs på detta är en engångsinvestering används det ibland som ett argument mot att anamma nya metoder.
- **Resursåtgång** – eller hur svårt/lätt det är att använda metoden. Bland huvudresurserna återfinns behov av personal (arbetstimmar), tid, information och dokumentationsbehov.
- **Giltighet** – huruvida de resultat metoden tillhandahåller är riktiga. Detta är en väldigt omstridd fråga i och med att det inte finns något enkelt sätt att bestämma resultatets riktighet. Det är väldigt ovanligt att samma olycka utreds på mer än

ett sätt och även när detta sker finns det inget oberoende kriterium att värdera resultaten med.

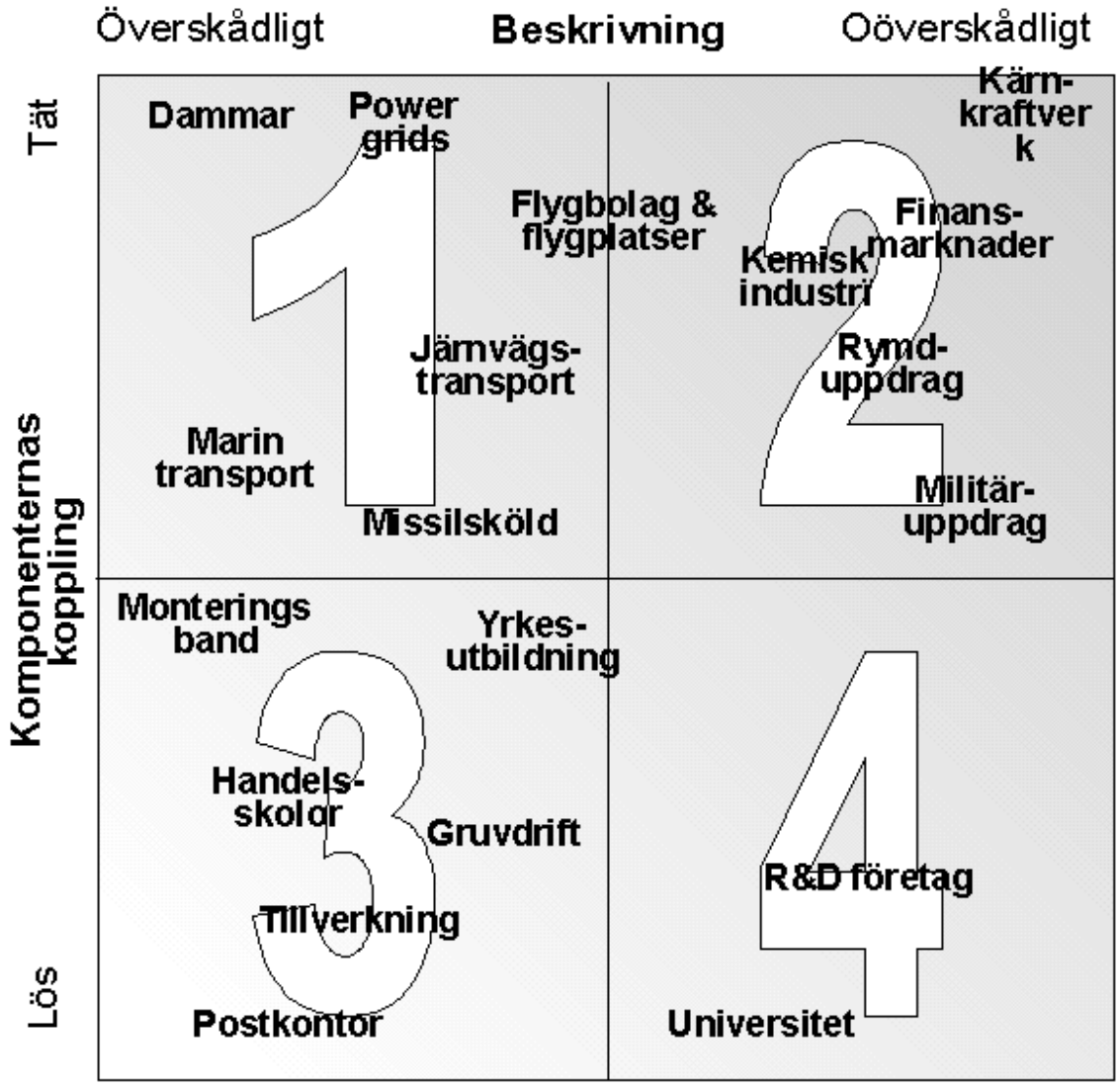
Anledningen till att jämföra och bedöma olika metoder är för att kunna välja den metod som är bäst lämpad för att lösa ett visst problem. Även om kriterium så som hastighet, resursåtgång och utbredning inom industrin inte är obetydliga måste det primära målet vara huruvida en utredningsmetod kan göra vad den ska göra: nämligen att skapa en adekvat förklaring till varför en negativ händelse (olycka eller incident) har ägt rum. En utredningsmetod är ett verktyg, och det är helt klart avgörande att det verktyget är välanpassat för den uppgift det ska användas till. Även om de flesta verktyg kan användas för olika syften (en skiftnyckel kan exempelvis användas som hammare) är det helt klart mycket bättre och mer effektivt om verktyget passar sin uppgift perfekt. Detta gäller för så väl fysiska verktyg som metoder. Således är det viktigt att kunna karakterisera metoderna med avseende på hur väl de passar för den uppgift de ska lösa, vilket i praktiken innebär hur väl de kan representera och förklara komplexiteten hos den aktuella situationen.

Få av de kriterier som nämnts ovan behandlar alls denna kvalitet, med undantag från Benners funktionell och icke-kausal. Perrows (1984) beskrivning av komplexiteten hos sociotekniska system (figur 1) utgör en bra startpunkt. Perrow föreslog två dimensioner: komponenternas koppling (från lös till tät) samt interaktionens komplexitet (från linjär till komplex). Medan begreppet ”komponenternas koppling” är relativt rättframt måste begreppet om ”interaktionens komplexitet” användas mer försiktigt. Detta eftersom det antingen kan syfta på den ontologiska eller epistemologiska komplexiteten[6] (Pringle, 1951). Av praktiska skäl är det att föredra att välja ett nytt begrepp, nämligen hur enkelt det är att beskriva systemet, där extremvärdena är överskådliga respektive oöverskådliga system. Ett system eller en process är överskådlig om de principer enligt vilka det fungerar är kända, om beskrivningarna av det är enkla, med få detaljer och viktigast: om systemet inte ändrar sig medan det beskrivs. Omvänt gäller att ett system eller en process är oöverskådlig om de principer enligt vilka det fungerar endast till viss del är kända eller till och med okända, om beskrivningarna av det är genomarbetade med många detaljer, samt om systemet kan komma att förändras innan beskrivningen av det är slutförd. Ett bra exempel på ett överskådligt system är ett postkontor, eller snarare ett postkontors normala funktioner, eller funktionen hos en värmepump för hemmabruk. På samma sätt är ett strömavbrott på ett kärnkraftverk eller aktiviteterna på ett sjukhus akutavdelning bra exempel på ett oöverskådligt system. I det senare fallet är aktiviteterna inte standardiserade och ändras så snabbt att det inte är möjligt att någonsin skapa en detaljerad och fullständig beskrivning av systemet.

Denna modifiering av terminologin gör att vi kan föreslå en ny version av Perrows diagram, se figur 2. (Observera att detta även innebär att vissa av de exempel Perrow använde måste flyttas och att andra (t.ex. kärnvapenolyckor) har tagits bort, samt att ytterligare andra (finansmarknader) har introducerats. Dessa förändringar är dock illustrativa snarare än uttömmande.).

---

6 Epistemologisk komplexitet kan definieras som det antal parametrar som behövs för att helt och hållet definiera ett system i tid och rum. Ontologisk komplexitet har ingen vetenskapligt upptäckbar mening och det är inte möjligt att referera till ett systems komplexitet oberoende av hur det ses eller beskrivs.



Figur 2. Modifierad version av Perrows diagram

Enligt den här principen bör karakteriseringen av metoder för olycksutredning ske i termer gällande de system, eller villkor, de kan förklara. Benners (1995) funderingar till trots så beror detta på den underliggande olycksmodellen. Till exempel kan en enkel linjär olycksmodell (så som dominomodellen (Heinrich, 1931)) användas för att förklara vissa typer av olyckor men inte andra. Dominomodellen är passande för system (och alltså även för olyckor) vars komponenter är löst kopplade och som är överskådliga. Anledningen till detta är helt enkelt att de flesta systemen var av den typen när modellen utvecklades. Kärnkraftsverk, som system, har tätt kopplade komponenter och mer eller mindre oöverskådliga. De kräver därför olycksmodeller och metoder för olycksutredning som kan redogöra för dessa egenskaper. Det är därför rimligt att karakterisera utredningsmetoder utifrån vilka användningsområden de kan redogöra för. Detta avgör inte huruvida en metod är ”bättre” än någon annan men det gör det möjligt att välja en metod som lämpar sig för ett specifikt syfte och/eller system och på så vis utelämnas de metoder som inte är förmögna att uppfylla de krav som ställs på en utredning.

7 Val av metoder för olycksutredning

Genom att följa de principer som beskrivits ovan är det möjligt att definiera fyra kategorier av metoder för olycksutredning. Dessa fyra kategorier motsvarar de fyra kvadranterna i figur 2. De 21 metoder som listats i tabell 1 reducerades för att enbart innehålla egentliga olycksutredningsmetoder och undvika överlappande metoder. Som en följd av detta beskrivs följande metoder inte närmare; CA (Change Analysis), ECFC (Events and Causal Factors Charting), ECFCA (Events and Causal Factors Charting Analysis), HFACS (Human Factors Analysis and Classification System), HFIT (Human Factors Investigating Tool), HPES (Human Performance Enhancement System), PEAT (Procedural Event Analysis Tool), SAFER 2007, SCAT (Systematic Cause Analysis Technique), STEP (Sequentially Timed Events Plotting) samt TRACEr (Technique for Retrospective Analysis of Cognitive Errors).

Nedan beskrivs metoderna indelade efter vilken av de fyra kvadranterna i figur 2 de tillhör. Varje metod beskrivs med avseende på följande egenskaper:

- **Referenser** – Den viktigaste referensen, eller källan till information, som beskriver metoden.
- **Relaterade metoder** – Andra metoder av samma typ, eller som använder sig av samma principer.
- **Huvudprincip** – Den huvudsakliga analytiska princip på vilken metoden är baserad.
- **Förfarande** – Huvudstegen vid tillämpning av metoden.
- **Typ av resultat** – Det huvudsakliga resultat som metoden producerar.
- **Operationell kraft och metodologisk styrka** – Hur enkelt det är att använda metoden i praktiken och hur mycket metoden beror av användarens kunskap och erfarenhet.
- **Teoretisk grund** – Hur välgrundade begreppen och kategorierna är, särskilt då vilken olycksmodell metoden antar.
- **Praktiskt värde** – Exempelvis hur väl metoden stödjer **skapandet av** effektiva rekommendationer.

7.1 Metoder lämpade för överskådliga system med löst kopplade komponenter

Även idag är, med avseende på frekvens och antal, överskådliga system med löst kopplade komponenter de vanligast förekommande systemen. Även om kärnkraftverk helt uppenbart inte återfinns bland dessa, och trots att bara ett fåtal andra säkerhetskritiska industrier gör det, verkar många av de mest använda utredningsmetoderna icke desto mindre vara bäst lämpade för, eller till och med anta att, systemen de beskriver är överskådliga system med löst kopplade komponenter. I praktiken innebär detta att det är möjligt att ha både en mer eller mindre komplett beskrivning av systemet och att redogöra för händelser (t.ex. brister och funktionsstörningar) var för sig eller del för del. Dessa antaganden skapar metoder som är lätta, eller enkla att tillämpa men det betyder även att sådana metoder är oförmögna att redogöra för komplexa fenomen, och således kan de heller inte producera praktiskt användbara resultat vid analys av olyckor i den typen av system.

Det finns flera underkategorier bland de metoder som är lämpade för överskådliga system med löst kopplade komponenter. Nedan kommer fyra underkategorier att beskrivas: 1) Metoder som fokuserar på identifierande av bristande barriärer, 2) Metoder som fokuserar på mänskliga fel, 3) Metoder som fokuserar på isolerade grundorsaker samt 4) Metoder som fokuserar på kombinerade grundorsaker.

Exempel på metoder som fokuserar på barriärer och/eller försvar och som förklarar olyckor som ett resultat av bristande eller otillräckliga barriärer.

Namn	Accident Evolution and Barrier Analysis (AEB)
Referens	Svensson, O. (2001). Accident and Incident Analysis Bases on the Accident Evolution and Barrier Function (AEB) Model. Cognition, Technology & Work, 3 (1), 42-45.
Relaterade metoder	Metoder för barriäranalys fokuserar generellt sett på de barriärer som borde ha hindrat, men inte hindrade förekomsten av en negativ händelse och/eller ett oönskat utfall. Barriäranalys används för att identifiera faror associerade med en olycka och de barriärer som skulle ha varit på plats för att förhindra den. En barriär är någon metod, vilken som helst, använd för att kontrollera, förhindra eller dämpa möjligheten för faran att nå sitt mål. Barriäranalyser adresserar: barriärer som var på plats och hur de uppförde sig, barriärer som inte var på plats men som var nödvändiga, barriärer som om de hade varit närvarande eller förstärkta hade kunnat förhindra att samma, eller liknande, olyckor från att inträffa i framtiden.
Huvudprincip	AEB-modellen tillhandahåller en metod för analys av händelser och olyckor som modellerar utvecklingen mot en händelse/olycka som en serie av interaktioner mellan människan och tekniska system. Dessa interaktioner består av brister, funktionsstörningar eller fel som kan ha lett till eller resulterat i en olycka. Metoden tvingar användaren att integrera mänskliga och tekniska system simultant vid utförandet av en olycksanalys.
Förfarande	Metodens utgångspunkt är dess enkla flödeschemateknik. Flödesschemat består till en början av tomma lådor i två parallella kolumner, en för de mänskliga systemen och en för de tekniska. Under analysens gång identifieras dessa lådor som de brister, funktionsstörningar eller fel som utgör olycksutvecklingen. Oftast följer sekvensen av lådor innehållande fel den kronologiska ordningen hos händelserna. Mellan varje par av på varandra följande lådor innehållande fel finns en möjlighet att hejda utvecklingen mot en incident/olycka. En AEB-analys består av två huvudfaser. Den första fasen är att modellera olycksutvecklingen i ett flödesschema. AEB modellerar enbart fel och är inte en händelsesekvensmetod. Den andra fasen består av barriärfunktionsanalysen. I den här fasen identifieras barriärfunktionerna (ineffektiva och/eller icke-existerande). Samma barriärfunktion kan utföras av olika barriärfunktionssystem. I överensstämmelse med detta kan varje barriärfunktionssystem utföra olika barriärfunktioner.
Typ av resultat	Ett viktigt syfte med AEB-analysen är att identifiera brustna barriärfunktioner, anledningen till varför det inte fanns någon barriärfunktion eller varför de existerande barriärfunktionerna fallerade, och att föreslå förbättringar.
Operationell kraft och metodologisk styrka	Metoden är enkel att använda tack vare sin diagrammatiska representation. Men då den enbart representerar vad som gick fel, snarare än hela sekvensen av händelser, begränsas dess förmåga att stödja rekommendationer och beslut om försiktighetsåtgärder och skydd. I praktiken kan den bara ge rekommendationer om att stärka (bristande) barriärer.
Teoretisk grund	Antagandet om linjär kausalitet utgör den teoretiska grunden på vilken AEB vilar. Metoden baseras på en enkel linjär olycksmodell och den grafiska representationen motsvarar ett felträd, men utan kombinationerna. Metoden erkänner samverkan mellan människa och teknik.
Praktiskt värde	Metoden har en begränsad praktisk tillämpning.

Exempel på metoder som fokuserar på mänskliga fel som den huvudsakliga bidragaren till negativa händelser.

Namn	Human Error in European Air Traffic Management (HERA)
Referens	Isaac, A., Shorrock, S. & Kirwan, B. (2002) Human error in European air traffic management: The HERA project. Reliability Engineering and System Safety, 75 (2), 257-272. Additional documentation is available from: http://www.eurocontrol.int/humanfactors/public/standard_page/hera.html
Relaterade metoder	Technique for Retrospective Analysis of Cognitive Errors (TRACEr)
Huvudprincip	HERA är en metod för att identifiera och kvantifiera den mänskliga faktorns påverkan i en incident-/olycksutredning, säkerhetsstyrning och bedömning av potentiella, nya typer av fel som kan uppstå till följd av ny teknik. Mänskliga fel ses som en potentiellt svag länk i ATM-systemet och åtgärder måste därför vidtas för att förhindra fel och deras effekter, samt för att maximera andra mänskliga kvaliteter så som upptäckande av fel och återhämtande av situationer. HERA grundar sig på antagandet att mänskliga fel är den största bidragande faktorn till olyckor och incidenter.
Förfarande	1. Definiera typen av fel. 2. Definiera det felaktiga, regelbrytande eller överträdande beteendet med hjälp av ett flödesschema. 3. Identifiera detaljerna hos felet med hjälp av ett flödesschema. 4. Identifiera felmekanismerna och tillhörande felaktig informationsbehandling med hjälp av flödesscheman. 5. Identifiera uppgifterna med hjälp av tabeller. 6. Identifiera utrustning och information med hjälp av tabeller. 7. Identifiera alla kontextuella förhållanden med hjälp av ett flödesschema och tabeller.
Typ av resultat	Identifiering av mänskliga fel och överträdelser. Kvantitativ data på den relativa frekvensen av olika typer av fel och arbetsförhållanden.
Operationell kraft och metodologisk styrka	HERA backas upp med instruerande manualer, kurser och viss mjukvara. Om metodens antaganden accepteras är det därför en av de mer mogna metoderna för olycksanalys. I praktiken finns dock viss tveksamhet angående de exakta definitionerna, och användandet, av de kategorier som används inom HERA, så som exempelvis överträdelser, misstag, etc.
Teoretisk grund	HERA grundar sig på antaganden om linjär kausalitet och mänskliga fel. Som namnet antyder letar metoden enbart efter exempel på mänskliga fel som orsaker. Den underliggande teorin baserar sig på olika typer av modeller av mänsklig informationsbehandling, så som den beskrivs av bland annat Reason (1997). Metoden antar att den primära orsaken till negativa händelser är mänskliga fel varför den tittar efter sådana hellre än överväger den möjliga effekten av prestandapåverkande förhållanden (performance shaping conditions).
Praktiskt värde	HERA används omfattande av europeiska flygtrafiktjänstorganisationer med varierande grad av framgång. Eurocontrol har kompletterat utvecklingen av HERA med relaterade metoder så som HERA-JANUS, HERA-Observe, HERA-PREDICT och HERA-SMART. Analysresultaten har samlats i en databas för att stödja riskanalys av framtida ATM-system. Det är osäkert huruvida angreppssättet kan överföras till kärnkraftsdomänen utan en komplett revision av det klassificeringssystem som används.

Exempel på metoder som fokuserar på grundorsaker

Namn	Root cause analysis (RCA)
Referens	Wilson, P. et al. (1993). Root cause analysis – A tool for total quality management. Milwaukee, WI: Quality Press. Enligt engelskspråkiga Wikipedia förekommer termen ”root cause” (grundorsak) för första gången 1905 (i en artikel i The Lancet). Termen är vida använd i den allmänna litteraturen och även fast det inte finns någon speciell RCA-teori eller modell, bortsett från några företags broschyrer. Grundorsak är ett filosofiskt snarare än vetenskapligt begrepp.
Relaterade metoder	TapRooT®
Huvudprincip	En grundorsaksanalys identifierar underliggande bristfälligheter i ett säkerhetsstyrningssystem vilka, om de åtgärdas, skulle förhindra samma och liknande olyckor från att hända igen. RCA är en systematisk process som använder den fakta och resultat från analysen för att bestämma de viktigaste anledningarna till en olycka.
Förfarande	1. Fastställ händelsesekvensen 2. Fastställ de kausala faktorerna 3. Analysera varje kausal faktors grundorsaker 4. Analysera varje grundorsaks generiska orsaker 5. Ta fram och värdera korrigerande åtgärder 6. Rapportera och implementera korrigerande åtgärder
Typ av resultat	Specifika grundorsaker som kan vara föremål för specifika stödjande eller korrigerande åtgärder.
Operationell kraft och metodologisk styrka	Användandet av grundorsaksanalys är vida spritt och stöds av omfattande träningsmaterial och praktiskt guidning (handböcker, prioriteringsdiagram etc.). Det anses var en väldigt effektiv metod och eftersom angreppssättet är ett enkelt baklänges spårande av orsaker är den ganska robust. Enkelheten hos metoden betyder emellertid också att sökandet är väldigt begränsad och således blir resultatet begränsat till de kategorier som definieras av metoden.
Teoretisk grund	En grundorsak definieras som en eller flera kausala faktorer vilka, om de åtgärdas, skulle förhindra att olyckan upprepas. En grundorsaksanalys definieras som: en metod som identifierar kausala faktorer som, om de åtgärdas, skulle förhindra att olyckan upprepas. Grundorsaksanalysen representerar därför filosofin om en enskild orsak. D.v.s. tron att det finns en enskild orsak för alla utfall, som om den förhindrades, även skulle förhindra själva utfallet. I den här kontexten är grundorsaken den orsak som dominerar över alla andra bidragande faktorer. Denna typ av resonemang bygger på användandet av icke reellt antagna villkorsbisatser. Problemet är att det logiskt sett inte går att anta att det efterföljande inte kommer att inträffa bara för att det föregående inte gjorde det. Med andra ord: man kan inte dra slutsatsen att om grundorsaken är borttagen så kommer inte effekterna att ske. Anledningen till detta är helt enkelt att det kan finnas flera andra sätt som samma effekter kan uppstå på.
Praktiskt värde	Grundorsaksanalys används inom många industrier, t.ex. sjukvård och kvalitetshantering (T.ex. Ishikawas fiskbensdiagram.).

Exempel på metoder som kombinerar multipla faktorer för att förklara olyckor

Namn	HINT - J-HPES
Referens	Takano, K., Sawayanagi, K . & Kabetani, T. (1994). System for analysing and evaluating human-related nuclear power plant incidents. Journal of Nuclear Science Technology, 31, 894-913. INPO (1989). Human performance enhancement system: Coordinator manual (INPO 86-016, Rev- 02). Atlanta, GA: Institute of Neuclear Power Operations.
Relaterade metoder	The Human Performance Enhancement System (HPES), ursprungligen utvecklad av the Institute of Nuclear Power Operations 1987. Använder en hel familj av tekniker för att utreda händelser, med särskilt fokus på att bestämma aspekter av den mänskliga prestationen. HPES metodologin innefattar flera verktyg, så som uppgiftsanalys, CA, BA, orsak och verkansanalys samt ECFC. Vidare har ett flertal liknande metodologier utvecklas utifrån HPES och där det varit nödvändigt anpassats för att passa individuella organisationers specifika krav.
Huvudprincip	HINT är en vidareutveckling av J-HPES, den japanska versionen av HPES. Den övergripande principen är att använda grundorsaksanalys av små händelser för att identifiera trender och använda dessa som en utgångspunkt för att förhindra olyckor. Samma principer återfinns i SAFER, även om den senare metoden har en större omfattning och således kan vara applicerbar även på olyckor i system med tätt kopplade komponenter.
Förfarande	Metoden består av följande steg: 1. Förstå händelsen 2. Samla in och klassificera data 3. Orsaksanalys, med hjälp av grundorsaksanalys 4. Förslag till motåtgärder
Typ av resultat	Metoden fokuserar på smärre mänskliga fel för att tillhandahålla en trendanalys av dessa för att möjliggöra förebyggande av allvarliga olyckor.
Operationell kraft och metodologisk styrka	Metodens steg beskrivs på en relativt hög nivå och kan alltså lättast appliceras av människor med en avsevärd mängd erfarenhet av både domänen och mänskliga faktorer. Metoden inriktar sig på olycksutredning snarare än olycksanalys men är mindre direkt och explicit i steg 1, 2 och 4 än i steg 3.
Teoretisk grund	Metoden är en variant av en grundorsaksanalys, utökad genom att ta hänsyn till mänskliga och organisatoriska faktorer.
Praktiskt värde	Metoden understöds av the Central Institute for Electric Power Industry (CRIEPI) i Japan. Den presenteras som en felförebyggande metod för industri och affärsverksamhet i allmänhet, men den verkliga tillämpningsnivån är okänd.

7.2 Metoder lämpade för överskådliga system med tätt kopplade komponenter

Den under 80- och 90-talen ökande frekvensen av icke-triviala olyckor tydliggjorde att flera av dessa inte kunde förklaras som ett resultat av sekvenser eller kedjor med händelser utan att det var nödvändigt att redogöra för hur kombinationer av multipla

händelsesekvenser, eller händelser och latenta tillstånd, kunde uppstå. Detta ledde till fram till förslaget av en typ av modeller som ofta klassificeras som epidemiologiska (Hollnagel, 2004). Prototypen för denna typ av modeller är the Swiss Cheese model, schweizerostmodellen.

Namn	The Swiss Cheese Model (SCM)
Referens	Reason, J.T. (1990). Human Error. Cambridge University
Relaterade metoder	TRIPOD-konceptet och dess metoder, vilka även på sätt och vis är schweizerost modellens ursprung. Idéen bakom TRIPOD är att organisatoriska brister är huvudfaktorer bland olycksorsaker. Dessa faktorer är mer ”latenta” och är, när de bidrar till en olycka, åtföljda av ett antal tekniska och mänskliga fel. Human Factors Analysis and Classification System (HFACS), använt av the Federal Aviation Agency i USA.
Huvudprincip	I schweizerostmodellen modelleras en organisations försvar mot olyckor som en serie barriärer, representerade som skivor av schweizerost. Hålen i ostskivorna representerar individuella svagheter i individuella delar av systemet, och de varierar hela tiden, i varje skiva, i storlek och position. Systemet som helhet producerar misslyckanden (t.ex. olyckor) när hålen i var och en av skivorna för ett ögonblick överlappar och då skapar en bana för olycksmöjligheter att använda som passage, genom hålen i de olika försvaren och på så vis skapa en olycka.
Förfarande	Grundmetoden för att använda schweizerostmodellen är att söka sig bakåt, från olyckan. Analysen letar efter två huvudfenomen: aktiva brister, vilka är osäkra handlingar utförda av människor (slips, lapses, fumbles, mistakes och procedural violations) samt latenta tillstånd, vilka uppstår från beslut fattade av designers, byggare, instruktionsförfattare och ledning. Latenta tillstånd kan innebära felprovocerande omständigheter på de lokala arbetsplatserna och de kan skapa långvariga hål eller svagheter hos försvaren. Till skillnad från aktiva brister, vilkas specifika form ofta är svår att förutse, kan latenta tillstånd identifieras och avhjälpas innan en negativ händelse äger rum. Att förstå detta leder till proaktiv snarare än reaktiv riskstyrning.
Typ av resultat	Identifiering, och klassificering, av aktiva brister och latenta tillstånd.
Operationell kraft och metodologisk styrka	Metoden är till en början enkel att använda, men i sin originalform saknar den detaljer om tillämpning. Detta har resulterat i diverse institutionaliserade versioner (t.ex. SHELL), men den kräver fortfarande en märkbar erfarenhetsnivå för att gå att använda effektivt. Metoden understöds av en ganska omfattande samling instruktionsmaterial, övningsböcker, webb-baserade instruktioner, etc.
Teoretisk grund	Metoden representerar en komplex, linjär modell. Den är ganska lik ett felträd, även om den vanliga grafiska representationen skiljer sig, och mindre detaljerad. Metoden fokuserar på mänskliga fel i kombination med latenta operationella omständigheter och skiljer mellan fel vid den skarpa, respektive trubbiga änden av en organisation.
Praktiskt värde	Modellen föreslogs ursprungligen av James Reason, och har sedan dess vunnit vida acceptans och användning inom sjukvård, flygsäkerhetsindustrin och räddningstjänst. Den har nyligen ifrågasatts av flera forskare.

Namn	Människa-Teknik-Organisation (MTO)
Referens	Rollenhagen, C. (1995)*, MTO – En introduktion: Sambandet Människa, Teknik och Organisation, Lund: Studentlitteratur. Bento, J-P. (1992). Människa, teknik och organisation. Kurs i MTO-analys för Socialstyrelsen, Studsvik, Nyköping: Kärnkraftssäkerhet och Utbildnings AB. Worledge, D. (1992). Role of human performance in emergency systems management. Annual Review of Energy and the Environment, 17, 285-300.
Relaterade metoder	Metoden är baserad på INPOs Human Performance Enhancement System (HPES).
Huvudprincip	Grunden för MTO-analysen är att mänskliga-, tekniska- och organisatoriska faktorer ska få lika stort fokus i en olycksutredning.
Förfarande	En MTO-utredning innehåller tre metoder: 1. Strukturerad analys, ett händelse- och orsaksdiagram. 2. Förändringsanalys, genom att beskriva hur händelserna avvikit från tidigare händelser, eller det vanliga förfarandet. 3. Barriärsanalys, som identifierar de teknologiska och administrativa barriärer som har fallerat eller saknades. Det första steget i en MTO-analys är att beskriva händelsesekvensen longitudinellt och att illustrera den i ett blockdiagram. Sedan ska möjliga teknologiska och mänskliga orsaker till händelser identifieras och ritas ut i diagrammet, vertikalt i förhållande till händelserna. Nästa steg är att göra en förändringsanalys för att göra en uppskattning av hur händelserna i olyckan skiljer sig från den normala situationen. Vidare analyseras vilka mänskliga-, tekniska- eller organisatoriska barriärer som fallerat eller saknades under olycksutvecklingen. Huvudfrågorna under analysen är: Vad kunde ha hindrat fortsättningen av olyckssekvensen? Vad kunde organisationen ha gjort (i det förgångna) för att förhindra olyckan? Det sista steget i MTO-analysen är att identifiera och presentera rekommendationer. Dessa ska vara så realistiska och specifika som möjligt och kan vara på mänsklig-, teknisk- eller organisatorisk nivå.
Typ av resultat	Detaljer och klarhet kring vilka faktorer som antingen ledde, eller bidrog, till olyckan.
Operationell kraft och metodologisk styrka	Användningen av metoden stöds av instruktionsmaterial och böcker. Den är relativt enkel att använda, men rekommenderas inte för nybörjare. Identifikationen av specifika orsaker och villkor beror mer på erfarenhet än på en väldefinierad mängd kategorier. Metoden inkluderar flera av de aspekter som utgör en olycksutredning, rekommendationer inkluderade.
Teoretisk grund	Metoden grundas på en komplex, linjär modell. Den vanliga representationen är dock mer i form av ett fiskbensdiagram än ett händelseträd. Metoden tenderar att ta hänsyn till kausala faktorer var för sig snarare än i en större kontext.
Praktiskt värde	Användandet av MTO-modellen är utbrett inom den svenska kärnkraftsindustrin. Principerna är också vida spridda inom andra domäner så som trafiksäkerhet och flygväsendet. MTO-metoderna har flera gemensamma nämnare med andra metoder (schweizerost modellen, HPES) men skiljer sig från de metoder som studerar enskilda-faktorer.
	*SKI-kommentar: Rollenhagen har 2003 utkommit med ”Att utreda olycksfall - teori och praktik”.

Namn	Cognitive Reliability and Error Assessment Method (CREAM)
Referens	Hollnagel, E. (1998). Cognitive reliability and error assessment method. Oxford: Elsevier Science Ltd.
Relaterade metoder	CREAM är en så kallad andra generations metod för Human Reliability Assessment (HRA), men skiljer sig från andra sådana metoder (ATHEANA, MERMOS) genom att vara utvecklad för både olycksutredning och riskanalys.
Huvudprincip	CREAM kan användas både prediktivt och retrospektivt. CREAM använder sig av Contextual Control Model (COCOM) som utgångspunkt för att definiera fyra olika kontrollsätt; strategiskt, taktiskt, opportunistiskt och slumpartat. Det antas att en lägre grad av kontroll motsvarar en mindre tillförlitlig prestanda. Kontrollnivån bestäms av Common Performance Conditions (CPC). Den retrospektiva användningen (olycksanalys) baseras på en distinktion mellan det som kan observeras (fenotyper) och det som måste tolkas ut (genotyper). De genotyper som används i CREAM är fördelade på tre kategorier: individuella, teknologiska och organisatoriska.
Förfarande	En CREAM analys består av följande steg: 1. Skapa en första, systematisk beskrivning av vad som verkligen hände 2. Karakterisera CPCerna 3. Skapa en beskrivning av signifikanta händelser i form av en tidslinje 4. Välj de intressant handlingarna 5. Identifiera, för varje handling, feltyp (detta görs iterativt) 6. För varje feltyp, hitta de relevanta kopplingarna mellan föregående och efterföljande handlingar (detta görs rekursivt) 7. Tillhandahåll en övergripande beskrivning samt dra slutsatser
Typ av resultat	En graf, eller ett nätverk av till olyckan föregående handlingar som tillsammans utgör en effektiv förklaring av olyckan. Grafen visar hur olika handlingar och villkor påverkat varandra i den givna situationen.
Operationell kraft och metodologisk styrka	CREAM-metoden finns tydligt beskriven, men är inte lätt att använda. Detta på grund av metodens icke-hierarkiska natur. Metoden producerar ett tydligt, granskningsbart spår vilket ökar dess tillförlitlighet. Stödet för metoden har nyligen utökats till att även innehålla en mjukvara med navigeringsverktyg, vilket gör metoden enklare att använda när den väl lärts in.
Teoretisk grund	Metoden söker inte efter specifika orsaker utan snarare efter operationella villkor som kan leda till förlust av kontrollen och därmed olyckor. Den grundar sig på Cognitive Systems Engineering. Likt övriga andra generationens HRA-metoder avvisar den synen på mänskligt fel som en meningsfull kausal kategori. Grunden för analysen är händelsen så som den ägde rum snarare än de på förhand bildade uppfattningarna om kausala faktorer.
Praktiskt värde	CREAM som metod går i princip även att tillämpa på olyckor i oöverskådliga system. Men dess tonvikt på överskådligheten hos inträffade händelser, om än inte systemet självt, gör att den primärt bör användas i överskådliga system. Användandet av CREAM som en specifik metod för trafikolyckor är utbrett i Norge och Sverige. Metoden går då under namnet DREAM, där D står för Driver (förare). Metodens proaktiva version har vid en rad tillfällen tillämpats för riskanalys, av bland annat nödrutiner inom kärnkraftsindustrin samt verksamhet på rymdstationer.

7.3 Metoder lämpade för oöverskådliga system med löst kopplade komponenter

Det finns inga utredningsmetoder för den här kategorin. Anledningen till detta går att finna i den historiska utvecklingen av olycksmodeller och utredningsmetoder.
I början, nämligen under 1930-talet, var de industriella systemen spårbara och dess komponenter löst kopplade.

Allteftersom teknologin och samhället utvecklades blev systemens komponenter tätare kopplade genom vertikal och horisontell integration. Och på samma gång blev de mindre överskådliga, detta då ny teknologi möjliggjorde snabbare förfaranden med mer omfattande automation. Det senare innebar i synnerhet att systemen blivit mer eller mindre självreglerande under normal drift, med minskad överskådlighet som resultat.

Eftersom även de olyckor som ägde rum ”följde” denna utveckling så utvecklades metoder för att adressera dessa nya problem. Samtidigt som få, om ens några, olyckor ägde rum i de oöverskådliga systemen med löst kopplade komponenter, varför heller inga metoder för att redogöra för sådana olyckor utvecklades. Huvudanledningen till detta är att sådana system är sociala snarare än teknologiska, så som exempelvis universitet, forskningsföretag och liknande.

7.4 Metoder lämpade för oöverskådliga system med tätt kopplade komponenter

Den ständigt ökande komplexiteten hos de sociotekniska systemen, och den följande minskningen av överskådligheten har lett till en fundamental förändring av hur risk- och säkerhetsfrågor angrips. Det mest iögonfallande exemplet på detta är utvecklandet av Resilience Engineering (Hollnagel, Woods & Leveson, 2006) som skiftar fokus, från brister och handlingar som gått fel, till användbarheten hos den normala variationen i utförandet. För olycksutredning innebär detta en strävan efter att förstå hur negativa händelser kan vara ett resultat av oväntade kombinationer av variationer i den normala prestandan, för att på så sätt överkomma behovet av att söka efter mänskliga fel eller grundorsaker.

Det här synsättet kallas ofta ett systemiskt synsätt. För närvarande finns endast två förslag på metoder som följer detta synsätt, STAMP och FRAM.

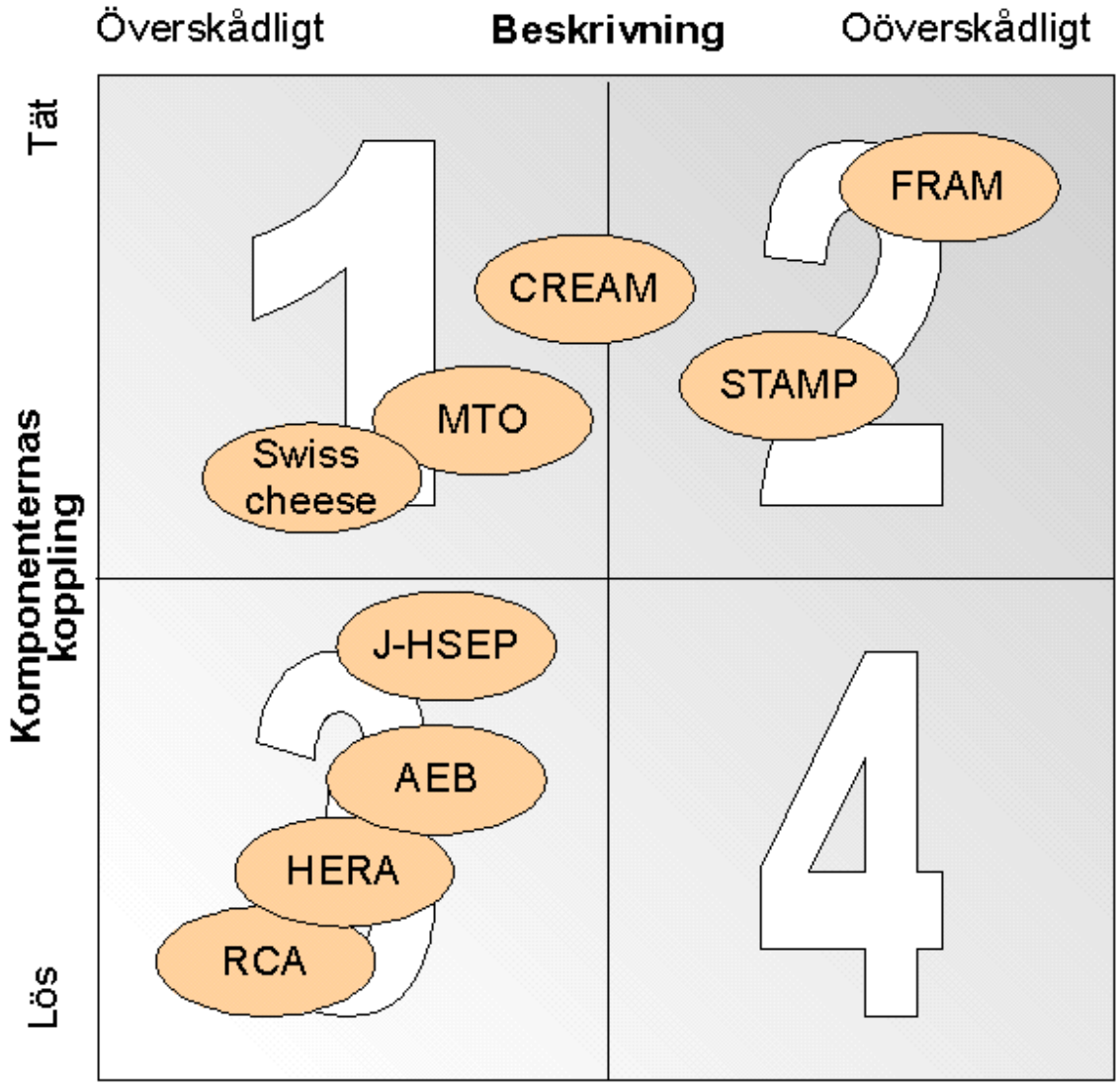
Namn	System-theoretic model of accidents (STAMP)
Referens	Leveson, N. G. (2004). A New Accident Model for Engineering Safer Systems, Science, 42 (4), 237-270
Relaterade metoder	Visst, men inte starkt, samband finns till kontrollteoretiska metoder så som Acci-kartor. Metoden har även viss likhet med Why-Because Analysismethod (WBA), se exempelvis http://www.rvs.uni-bielefeld.de/research/WBA

Huvudprincip	Det antagande som ligger till grund för STAMP är att systemteori är en bra utgångspunkt för att analysera olyckor. Olyckor uppstår när externa störningar, komponentfel eller dysfunktionell interaktion mellan systemkomponenter inte hanteras på ett lämpligt sätt av kontrollsystemet. Säkerhet betraktas som ett kontrollproblem och styrs av en kontrollstruktur som är inbäddad i ett adaptivt socioteknisk system. För att förstå varför en olycka ägt rum krävs ett fastställande av varför kontrollstrukturen var ineffektiv. För att förhindra framtida olyckor krävs att kontrollstrukturen designas så att den stärker de nödvändiga restriktionerna. System anses vara relaterade komponenter som hålls i en dynamisk jämvikt av återkopplingsloopar. STAMP gör anspråk på att vara en generell metod för förklaring av teleologiska system.
Förfarande	STAMP använder återkopplingskontrollsystem som en särskild kausal modell. Analysen fortgår enligt följande steg: 1. I teleologiska system upprätthåller olika subsystem restriktioner som förhindrar olyckor. 2. Om en olycka uppstått har dessa restriktioner brutits emot. 3. STAMP undersöker de involverade systemen, särskilt subsystem bestående av människor och organisation, för att identifiera saknade eller opassande huvuddrag (de som misslyckats med att upprätthålla restriktionerna). 4. Metoden fortsätter genom att analysera feedback- och kontrollförfaranden.
Typ av resultat	STAMPs grundkomponent är inte en händelse, utan en restriktion. Olyckor ses således som ett resultat av interaktioner mellan komponenter som bryter mot de restriktioner som skapar systemets säkerhet. Kontrollprocesserna som upprätthåller dessa restriktioner måste begränsa systemets beteende till de säkra förändringar och anpassningar som restriktionerna implicerar. Otillräcklig kontroll kan bero av saknade säkerhetsrestriktioner, otillräckligt kommunicerade restriktioner, eller från restriktioner som inte drivits igenom ordentligt på en lägre nivå.
Operationell kraft och metodologisk styrka	STAMP kan systematiskt blottlägga organisatoriska strukturer och rikta analysen för att ställa avslöjande frågor. Eftersom STAMP enbart är en analysmetod är den väldigt beroende av kvaliteten hos utredningsrapporten (data, information). På grund av komplexiteten hos den underliggande modellen (se nedan) kräver metoden en ansenlig ansträngning av användaren och i sitt nuvarande tillstånd är den enbart lämplig för erfarna användare. En metod för strukturerad presentation av resultaten finns ännu inte tillgänglig.
Teoretisk grund	STAMP använder en specifik kausal modell, nämligen ett återkopplingskontrollsystem. Grundprincipen är att en olycka sker ner de operationella restriktionerna bryts. Modellen tar hänsyn till både mjukvara, organisation, ledning, mänskligt beslutsfattande, och förflyttningen av system (över tid) till tillstånd med högre risk.
Praktiskt värde	STAMP har ännu inte använts i någon större utsträckning och metoden måste anses som att den fortfarande är under utveckling. För- och nackdelar med metoden har diskuterats i the RISK forum (http://catless.ncl.ac.uk/risks).

Namn	Functional Resonance Accident Model (FRAM)
Referens	Hollnagel, E. (2004). Barriers and accident prevention. Aldershot: Ashgate Nouvel, D., Travadel, S. & Hollnagel, E. (2007). Introduction of the concept of functional resonance in the analysis of a near-accident in aviation. Ispra, November 2007, 33rd ESReDA Seminar: Future challenges of accident investigation. Sawaragi, T., Horiguchi, Y. & Hina, A. (2006) Safety analysis of systemic accidents triggered by performance deviation. Bexco, Busan. South Korea, October 18-21, SICE-ICASE International Joint Conference 2006
Relaterade metoder	Det finns visst släktskap med variationsträd och variationsdiagram, även om dessa utvecklades för överskådliga system med löst kopplade komponenter.
Huvudprincip	En metod för olycksutredning såväl som riskanalys, baserad på beskrivningen av systemfunktioner. Icke-linjär spridning av händelser beskrivs i termer av funktionell resonans, utlöst av normal variation i utförandet.
Förfarande	1. Definiera syftet med modellerandet och beskriv situationen som ska analyseras. 2. Identifiera väsentliga funktioner: karakterisera varje funktion med avseende på sex grundparametrar (input, output, tid, kontroll, förhandskrav samt resurser). 3. Karakterisera den (kontextberoende) variationen genom att använda en checklista. Ta hänsyn till både den normala och den värsta tänkbara variationen. 4. Definiera den funktionella resonansen med utgångspunkt i de möjliga beroendena (kopplingarna) mellan funktionerna. 5. Identifiera barriärer för variationen (dämpande faktorer) och specificera behovet av övervakning över utförandet.
Typ av resultat	Analysen blottlägger beroenden mellan funktioner och uppgifter som normalt sett missas. Den identifierar även den information som behövs för utredningen. Det konkreta resultatet kan vara i form av en grafisk återgivning av hur olyckan utvecklades och/eller en detaljerad skriftlig beskrivning.
Operationell kraft och metodologisk styrka	Metoden är strukturellt enkel och täcker flera av en olycksutrednings faser. Den kräver dock en inlärningsperiod på grund av sin oortodoxa teoretiska grund (se nedan). Eftersom metoden inte innehåller en samling kausala kategorier (taxonomi), är det nödvändigt att användaren har en utbredd domänkunskap, såväl som kunskap om mänskliga och organisatoriska faktorer. FRAM stöds av the FRAM visualizer, en mjukvara.
Teoretisk grund	FRAM bygger på en teori om funktionell resonans. Detta gör att metoden kan redogöra för icke-linjära interaktioner och komma ifrån den klassiska orsak-verkan relationen. Grunden, för både olycksanalys och riskanalys, är en beskrivning av systemfunktioner (människa, teknik och organisation inkluderat), snarare än systemstrukturer eller komponenter. Metoden är därför, utan större ansträngning, skalbar.
Praktiskt värde	Användandet av FRAM är utbrett inom flera olika domäner (flygväsendet, flygledning, kritisk informationsinfrastruktur, räddningstjänst, offshore-verksamhet samt sjukvård).

8 Diskussion och slutsats

Ett sätt att summera karakteriseringen av de nio olycksutredningsmetoder som beskrivits i det föregående kapitlet är att placera ut dem på den modifierade versionen av Perrows diagram (figur 2). Resultatet av detta återfinns i figur 3. Detta visar att de flesta metoderna kan appliceras på överskådliga system, eller snarare: att dessa metoder gör antagandet att systemet är överskådligt. Omvänt går det att dra slutsatsen att dessa metoder inte ska användas för oöverskådliga system, eftersom de inte kommer att kunna skapa adekvata förklaringar beskrivning av händelsen. Flera av de vanligen använda metoderna, grundorsaksanalys, AEB och HERA inkluderade, kräver även att systemets komponenter är löst kopplade. Med andra ord är de oförmögna att redogöra för konsekvenserna av system med tätt kopplade komponenter, och således även oförmögna att förklara olyckor i system av den typen.



Figur 3. Karakterisering av metoder för olycksutredning

Det är förnuftigt att anta att vilken metod som helst skulle vara lämplig för den typ av problem som var vanliga under den tid då metoden utvecklades. Det finns faktiskt få anledningar till att utveckla en metod som är alltför komplex eller mer kraftfull än vad

som krävs. Som påpekat i början av den här rapporten utvecklas nya metoder vanligen därför att de befintliga metoderna vid någon tidpunkt stöter på problem för vilka de är ineffektiva eller otillräckliga. Detta, i sin tur, beror på att de sociotekniska systemen där olyckor sker fortsätter att utvecklas och blir mer och mer komplexa och tätare och tätare kopplade. Det oundvikliga resultatet är att även nya metoder efter ett tag förlorar i kraft eftersom problemens natur förändras, även om metoden var helt och hållet adekvat för de problem den skapades för från början.

De olika metodernas position i diagrammet i figur 3 visar en karakterisering av metoderna utförd med hjälp av de två dimensionerna; täthet hos komponenternas koppling samt systemets överskådlighet, och visar därför även indirekt på de sociotekniska systemens utveckling sedan 1930-talet. Utan att gå inpå detaljer kring den här utvecklingen, kan den tredje kvadranten sägas representera industriella system innan 1900-talets mitt, med andra ord innan informationsteknologi började användas i stor skala. Sedan dess har utvecklingen varit en utveckling i termer av tätare kopplade komponenter (en flytt upp mot och in i den första kvadranten) och en förlust av överskådligheten (en flytt rakt in i den andra kvadranten). Detta har i sin tur krävt utveckling av nya metoder, vilket visas i diagrammet.

En metods position reflekterar antagandena bakom metoden, särskilt det som har kallats olycksmodellen. Argumenten för var och en av metodernas position i diagrammet återfinns ovan. För att illustrera positionens signifikans, betrakta de två extremfallen, grundorsaksanalys (RCA) och FRAM.

- Grundorsaksanalys (RCA) antar att negativa utfall kan beskrivas som ett utfall av en eller flera sekvenser av händelser, eller som en kedja av orsaker och dess effekter. Utredningen blir därför ett spårande bakåt, från olyckan, för att försöka finna den/de effektiva orsakerna. Metoden kräver att systemet är överskådligt, eftersom det annars skulle vara omöjligt att genomföra denna bakåtspårning. Metoden kräver även att systemets komponenter är löst kopplade, eftersom det annars skulle vara omöjligt att känna sig säker på att åtgärdandet eller elimineringen av grundorsaken hindrar att olyckan återupprepas.
- Resonansolycksmodellen (FRAM) antar att negativa utfall är resultatet av oväntade kombinationer av normal variation hos systemfunktioner. Med andra ord, att det är de täta kopplingarna som leder till det negativa utfallet och inte sekvenser av orsaker och verkan. Eftersom en utredning dessutom söker efter funktioner snarare än strukturer, blir det mindre problematiskt om beskrivningen är oöverskådlig. Funktioner kan faktiskt komma och gå över tid, medan systemstrukturer måste vara mer permanenta. Funktioner associeras med den sociala organisationen av arbetet och kraven hos en specifik situation. Strukturer associeras med det fysiska systemet och utrustningen, vilken inte ändras från situation till situation.

Det här sättet att karakterisera på betyder inte att FRAM är en bättre metod än grundorsaksanalys. (Vilket även går att säga för vilken annan jämförelse av två modeller som helst.) Men det betyder att FRAM passar väl för vissa typer av problem och att grundorsaksanalys passar väl för andra. (Självklart innebär det också att det finns problem för vilka båda metoderna passar illa.).

För att kunna välja rätt metod för att utreda en olycka är det nödvändigt att först av allt karakterisera olyckan. Detta kan göras genom att besvara ett antal frågor, till exempel:

1. Liknade olyckan något som inträffat förut, eller var den ny och okänd? (Referens här bör vara både det specifika verket och hela industrin.)

2. Var organisationen redo att reagera på olyckan, i den betydelsen att det fanns etablerade procedurer och riktlinjer tillgängliga?
3. Kunde situationen snabbt fås under kontroll eller var utvecklingen utdragen?
4. Var olyckan och materiell påverkan begränsat till ett klart avgränsat subsystem (teknologiskt eller organisatoriskt) eller involverade det flera subsystem, eller hela verket?
5. Var konsekvenserna i stort sett förväntade/bekanta eller var de ovanliga eller sällsynta?
6. Var konsekvenserna i proportion till den initierande händelsen eller var de oväntat stora?

(När frågorna behandlas bör man självklart ha i åtanke att svaren beror på en initial och informell förståelse av vad som kan ha hänt. En erfaren olycksutredare bör kunna göra detta utan att påverkas av förhastade antaganden om orsakens natur.)

De första tre frågorna illustrerar frågor som relaterar till överskådlighetsdimensionen. Om frågorna besvaras jakande indikerar detta att systemet var överskådligt, åtminstone till en viss gräns. Det motsatta gäller om frågorna besvarades nekande.

Fråga 4-6 illustrerar frågor som relaterar till kopplingsdimensionen. Om frågorna besvaras jakande indikerar detta att systemets komponenter var av den löst kopplade typen. Även i det här fallet gäller det motsatta om frågorna besvarades nekande.

Avslutningsvis är det viktigt när man står inför behovet att utreda en olycka att den valda metoden är passande för systemet och situationen, med andra ord att metoden är kapabel att tillhandahålla en förklaring. Om olyckan gäller kärnkraftsverkets verksamhet som helhet så motsvarar problemet den andra kvadrantens karaktärsdrag. Om olyckan bara rör ett subsystems eller enskild komponents verksamhet, kan problemet motsvara karaktärsdragen hos den första, eller till och med tredje, kvadranten. Utredningsmetoden kan därför alltså variera. De sex frågorna ovan föreslår hur karaktärsdragen hos en olycka kan fastställas.

Som ett tillägg till detta kan även andra angelägenheter spela in, så som resurskrav, enkelhet att använda och överensstämmelse med andra metoder inom organisationen eller industrin. Medan det kan vara bekvämt, eller till och med nödvändigt, för en organisation att anamma en specifik metod som standard, ska detta alltid göras medvetet och med en öppenhet att revidera valet när omständigheterna kräver det. Sociotekniska system, processer och organisationer förändras och utvecklas fortlöpande, drivna av interna och externa krafter och krav. De metoder som finns tillgängliga för att hantera dessa system och för att utreda dem när något går snett, förändras dock med mycket långsammare hastighet. Dessutom är förändringar diskreta snarare än kontinuerliga. Den ofta upplevda konsekvensen av detta är att de tillgängliga metoderna släpar efter verkligheten, ofta så mycket som ett årtionde eller två. Diagrammet i figur 3 representerar därför enbart situationen i skrivande stund, d.v.s. ca 2008. Vi måste förvänta oss att metoderna i den andra kvadranten om fem eller tio år sakta kommer att ha förskjutits mot den tredje kvadranten, inte för att metoderna har förändrats utan för att systemen har. Nya och mer kraftfulla metoder kommer, förhoppningsvis, vid det här laget ha utvecklats för att anpassa sig till det här sakförhållandet.

9 Referenser

Benner, L. Jr., (1985). Rating accident models and investigation methodologies. *Journal of Safety Research*, 16, 105-126.

Bento, J.-P. (1992). *Människa, teknik och organisation. Kurs i MTO-analys för Socialstyrelsen*. Studsvik, Nyköping: Kärnkraftsäkerhet och Utbildnings AB.

Bird, F. E. Jr. & Germain, G. L. (1985). *Practical loss control leadership*. Georgia, USA: International Loss Control Institute.

CCPS (1992). *Guidelines for Investigating Chemical Process Incidents*. Center for Chemical Process Safety of the American Institute of Chemical Engineers.

CISHC (Chemical Industry and Safety Council), (1977). *A guide to hazard and operability studies*. London: Chemical Industries Association.

Cooper, S. E., Ramey-Smith, A. M., Wreathall, J., Parry, G. W., Bley, D. C., & Luckas, W. J. (1996). *A Technique for Human Error Analysis (ATHEANA)*. Washington, DC: Nuclear Regulatory Commission.

Dekker, S. (2006). *The field guide to understanding human error*. Aldershot, UK: Ashagte.

Dianous, V. D. & Fiévez, C. (2006). ARAMIS project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance. *Journal of Hazardous Materials*, *130*(3), 220-233.

DOE. (1999). *Conducting Accident Investigations: DOE Workbook* (Revision 2, May 1, 1999). Washington, DC: U.S. Department of Energy.

FAA/NTIS (2000). *The Human Factors Analysis and Classification System – HFACS* (DOT/FAA/AM-00/7). Washington, DC: Federal Aviation Administration.

Gordon, R., Flin, R. & Mearns, K. (2005). Designing and evaluating a human factors investigation tool (HFIT) for accident analysis. *Safety Science*, *43*, 147–171.

Harms-Ringdahl, L. (1987). *Säkerhetsanalys i skyddsarbetet - En handledning*. Folksam, Stockholm.

Harms-Ringdahl, L. (1993). *Safety analysis - Principles and practice in occupational safety*. Elsevier, London.

Harms-Ringdahl, L. (1996). *Riskanalys i MTO perspektiv: Summering av metoder för industriell tillämpning* (SKI Raport 96:63). Stockholm, Sweden: SKI.

Heinrich, H. W. (1929). The foundation of a major injury. *The Travelers Standard*, 17(1), 1-10.

Heinrich, H. W. (1931). *Industrial accident prevention*: New York: McGraw-Hill.

Helmreich, R. L., Merritt, A. C. & Wilhelm, J. A. (1999). The evolution of Crew Resource Management training in commercial aviation. *International Journal of Aviation Psychology*, *9*(1), 19-32.

Hendrick, K. & Benner, L. Jr. (1987). *Investigating accidents with STEP*. Marcel Dekker.

Hollnagel, E. (1998). *Cognitive reliability and error analysis method*. Oxford, UK: Elsevier Science Ltd.

Hollnagel, E. (2004). *Barriers and accident prevention*. Aldershot, UK: Ashgate.

Hollnagel, E. (2008). *Investigation as an impediment to learning*. In Hollnagel, E., Nemeth, C. & Dekker, S. (Eds.) *Remaining sensitive to the possibility of failure* (Resilience engineering series). Aldershot, UK: Ashgate.

Hollnagel, E., Woods, D. D. & Leveson, N. G. (2006). *Resilience engineering: Concepts and precepts*. Aldershot, UK: Ashgate.

IAEA (1999). *Root cause analysis for fire events at nuclear power plants* (IAEA-TECDOC-1112). Vienna, Austria: IAEA.

INPO (1989). *Human performance enhancement system: Coordinator manual* (INPO 86-016, Rev. 02). Atlanta, GA: Institute of Nuclear Power Operations.

Isaac, A., Shorrock, S. & Kirwan, B. (2002) Human error in European air traffic management: The HERA project. *Reliability Engineering and System Safety*, *75*(2), 257-272.

Kirwan, B. (1994). *A guide to practical human reliability assessment*. London: Taylor & Francis.

Le Bot, P., Cara, F., & Bieder, C. (1999). *MERMOS, A second generation HRA method*. Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment", Washington, DC.

Leveson, N. G. (1995). *Safeware - system safety and computers*. Reading, MA: Addison-Wesley.

Leveson, N. G. (2004). A New Accident Model for Engineering Safer Systems. *Science*, *42*(4), 237-270.

MIL-STD-1629A (1980). *Procedures for performing a failure mode, effects and criticality analysis*. Washington, DC: Department of Defence.

Moodi, M. & Kimball, S. (2004). *Example application of procedural event analysis tool* (PEAT). Seattle, WA: Boeing Company.

Nouvel, D.; Travadel, S. & Hollnagel, E. (2007). *Introduction of the concept of functional resonance in the analysis of a near-accident in aviation*. Ispra, Italy, November 2007, 33rd ESReDA Seminar: Future challenges of accident investigation.

Perrow, C. (1984). *Normal accidents*: *Living with high risk technologies*. New York: Basic Books, Inc.

Pringle, J. W. S. (1951). On the parallel between learning and evolution. *Behaviour*, *3*, 175-215.

Reason, J. T. (1990). *Human Error*. Cambridge University Press.

Reason, J. T. (1997). *Managing the risk of organisational accidents.* Aldershot, UK: Ashgate.

Renborg, B., Jonsson, K., Broqvist, K. & Keski-Seppälä, S. (2007). *Hantering av händelser, nära misstag* (SKI 2007:16). Stockholm: SKI.

Rollenhagen, C. (1995). *MTO – En Introduktion: Sambandet Människa, Teknik och Organisation*. Lund, Sweden: Studentlitteratur.

Sawaragi, T.; Horiguchi, Y. & Hina, A. (2006). *Safety analysis of systemic accidents triggered by performance deviation*. Bexco, Busan, South Korea, October 18-21. SICE-ICASE International Joint Conference 2006.

Shorrock, S. T. & Kirwan, B. (1999). *The development of TRACEr - A technique for the retrospective analysis of cognitive errors in ATM*. Proceedings of the 2nd International Conference, 28-30 Oct. 1998, Oxford, UK. (Vol. 3, pp. 163-171).

Shorrock, S. T. & Kirwan, B. (2002). Development and application of a human error identification tool for air traffic control. *Applied Ergonomics*, *33*, 319–336.

Sklet, S. (2002). *Methods for accident investigation* (ROSS (NTNU) 200208). Trondheim, Norway: NTNU.

Svensson, O. (2001). Accident and Incident Analysis Based on the Accident Evolution and Barrier Function (AEB) Model. *Cognition, Technology & Work*, *3*(1), 42-52.

Swain, A. D. (1989). *Comparative evaluation methods for human reliability analysis*. Köln, Germany: Gessellschaft für Reaktorsicherheit.

Takano, K., Sawayanagi, K. & Kabetani, T. (1994). System for analysing and evaluating human-related nuclear power plant incidents. *Journal of Nuclear Science Technology*, *31*, 894-913.

van der Schaaf, T. & Kanse, L. (2004). Biases in incident reporting databases: an empirical study in the chemical process industry. *Safety Science*, 42, 57-67.

Weick, K. E., Sutcliffe, K. M. & Obstfeld, D. (1999). Organising for high reliability: processes of collective mindfulness. *Research in Organisational Behaviour*, *21*, 81–123.

Wickens, C. D. (1992). *Engineering psychology and human performance*. New York: Harper-Collins.

Wilson, P. et. al., (1993). *Root cause analysis – A tool for total quality management*. Milwaukee, WI: Quality Press.

Woods, D. D., Johannesen, L. J., Cook, R. I. & Sarter, N. B. (1994). *Behind human error: Cognitive systems, computers and hindsight*. Columbus, OH: CSERIAC.

Worledge, D. (1992). Role of human performance in emergency systems management. *Annual Review of Energy and the Environment*, *17*, 285-300.

Yoshizawa,Y. (1999). *Activities for on-site application performed in human factors group*. Proceedings of 3rd International Conference on Human Factors in Nuclear Power Operation (ICNPO-III), Mihama, Japan.

Appendix I

Namn:	Avvikelseanalys
Princip:	Olyckor och risker föregås av avvikelser från den planerade eller vanliga funktionen. Avvikelser kan gälla tekniska, mänskliga och organisatoriska funktioner. Kan man kontrollera sådana avvikelser, minskar sannolikheten för en olycka. Metoden syftar till att ge en identifiering av avvikelser som kan leda till skador, och att ta fram förslag till åtgärder. Objekt för en analys kan vara ett tekniskt system eller en aktivitet (procedur).
Referenser:	Harms-Ringdahl, L. (1987). Säkerhetsanalys i skyddsarbetet - En handledning. Folksam, Stockholm. Harms-Ringdahl, L. (1993). Safety analysis - Principles and practice in occupational safety. Elsevier, London.
Procedur / arbetsgång:	Arbetsgången inkluderar fyra steg: 1. Strukturera systemet (eller aktiviteten) i delar. 2. Identifiera avvikelser för en del i taget. Hjälp av checklista som anger tekniska, mänskliga och organisatoriska avvikelser. 3. Bedöm avvikelserna; exempelvis som acceptabel, respektive icke acceptabel (görs lämpligen aven arbetsgrupp eller expertpanel). 4. Föreslå åtgärder; en enkel åtgärdssystematik finns.
Typ av resultat:	Huvudresultatet är en helhetsbild av de förbättringar som en arbetsgrupp anser nödvändiga. Delresultat är: l) En strukturerad beskrivning av systemet 2) Lista på urval av möjliga avvikelser, 3) En bedömning av avvikelser och risker. 4) Lista på förslag till åtgärder.
Kommentarer:	Metoden är av generell karaktär, och den är närbesläktad andra metoder såsom FMEA och HAZOP. Den kan tillämpas dels på stora objekt för att ge en överblick, dels rör detaljerade analyser av delsystem. Man kan inkludera olika typer av risker, t.ex. "vanliga" olyckor, produktionsbortfall, kvalitetsproblem, miljöskador, och risk för ohälsa. Metoden är prövad i olika slags system och har fungerat väl. Metoden har ingått i utbildningar av yrkesinspektörer, skyddsingenjörer m.fl. och har då funnits fungera i många olika situationer. Någon specifik utvärdering har inte gjorts, när det gäller validitet eller reliabilitet. En analys med metoden kan ta från någon dag till flera veckors insats. En väsentlig del av arbetsinsatsen är ofta "struktureringen", d.v.s. den strukturerade och systematiska beskrivningen av objektet.

Namn:	HEAT - Human Error Analytical Taxonomy
Princip:	Metoden går ut på att utreda olycksfall och incidenter systematiskt och väl strukturerat för att identifiera faktorer som kan leda till mänskliga fel i en processanläggning. En taxonomi har utvecklats, där en indelning har gjorts j fyra huvudkategorier: *Human performance, Decision making, Socio-organizational conditions och External situation.*
Referenser:	Final report. "HEAT" project. Human Error Analytical Taxonomy. C.E.C. Contract N,STEP-CT 90~0089-DTEE. Milan, October 1994. Ruuhilehto, K och Lepistö, I. (1995). A manual for the HEAT human error analysis (på finska). VTT Tillverkningsteknik, Tammerfors.
Procedur / arbetsgång:	Utgångspunkten är ett olycksfall eller tillbud. Med hjälp av ett frågeschema gås hela taxonomin igenom. Fasta svarsalternativ används och det finns en handledning som ger detaljerat stöd. Datorstöd grundat på Excel har utvecklats. Det ena är för lagring av svaren och presentation av dessa. Det andra är för analys av insamlad data. Metoden är tänkt att kunna användas av företaget självt, t.ex. arbetsledare, företagsledning och skyddsingenjörer.
Typ av resultat:	Man får en strukturerad beskrivning av förhållanden som påverkar förekomsten av mänskliga misstag.
Kommentarer:	Jag har inte studerat originalrapporterna utan bygger sammanställningen på information i andra hand, Den finska versionen tror jag är mer genomarbetad, och den kan vara intressant att studera. Användningen av metoden höjer kvaliteten på olycksutredningar avsevärt när det gäller att behandla människans roll. Det ger en ökad förståelse och underlag för att argumentera för förbättringar.

Namn:	MORT - Management Oversight and Risk Tree
Princip:	Revisionsmetod. MORT kan beskrivas som ett logiskt diagram, som är en modell av ett idealt säkerhetsprogram. Det kan användas rör a) att utreda ett olycksfall, och b) för att analysera ett organisatoriskt program för säkerhet. MORI-trädet är ett problembeskrivande träd. Det är ganska likt ett felträd och använder samma symboler. Det ingår cirka 200 grundläggande problem i trädet. Men tillämpas det på olika områden kan antalet potentiella orsaker bli 1.500. Topphändelsen kan vara ett inträffat olycksfall. Detta beror på att en accepterad risk utlöses, eller på organisatoriska misstag och försummelser. För att en risk ska räknas som accepterad krävs att den analyserats och blivit godkänd av företagsledningen.
Referenser:	Johnson W. G. (1980). MORT Safety Assurance Systems. National Safety Council, Chicago. Know, N. W. och Eicher, R. W. (1976). MORT User's manual. For use with the Management Oversight and Risk Tree analytical diagram. EG&G Idaho Inc., Idaho.
Procedur / arbetsgång:	Vid analysen utgår man från MORT -diagrammet; först översiktligt och sedan mer detaljerat. De frågor man direkt finner svar på markeras på diagrammet. Olika färger används sedan för att koda svaren. Grönt och rött betyder då OK respektive “LTA" . Blått innebär att man inte fått svar på frågan. Irrelevanta frågor stryks. Analysen är klar när alla element är ifyllda. Vid analysen går man genom de olika elementen som finns i trädet, vilka är numrerade. Det finns en lista som kompletterar trädet. För varje element finns specifika frågor som analytikern ska ställa. Svaren bedöms som “Satisfactory" eller "Less Than Adequate" (LTA).
Typ av resultat:	Identifiering av problem i hanteringen av risker. Förmodligen blir det också förslag till åtgärder och en mer strukturerad syn på säkerhetsarbetet. En jämförelse mellan modellen och säkerhetsarbetet i företaget.
Kommentarer:	Metoden är klassisk och väl etablerad. Den har sina rötter hos amerikanska AEC (U.S. Atomic Energy Commission). I vilken utsträckning den används idag vet jag ej. Några försök har gjorts i Finland. MORT är omfattande, men de enskilda elementen är lätta att förstå. Johnson anger att en analys av ett olycksfall kan genomföras på några dagar. En finsk erfarenhet är att tidsbehovet för analytikern är två till åtta veckor vid granskning aven organisation. Metoderna innebär att många problem identifieras. Johnson (1980) nämner att vid fem utredningar med MORT av allvarliga olycksfall, identifierade man 197 problem, d.v.s.. 38 per fall. MORT utgår från en ideal organisationsmodell. Om företaget avviker mycket från denna, blir det fort många negativa svar, som analytikern kan få svårt att hantera om han inte har stor erfarenhet.

Namn:	SMORT - Safety Management and Organization Review Technique
Princip:	Revisionsmetod. SMORT utgår från en modell av ett idealt säkerhetsprogram, som har summerats som en checklista. Utifrån denna diskuteras det aktuella företagets säkerhetsarbete. Metoden kan användas för a) att utreda ett olycksfall, och b) för att analysera ett organisatoriskt program för säkerhet. Utgångspunkter är att företaget har en skyddspolicy. en plan för att genomföra den och en uppföljning av resultaten. Analysen görs på fyra nivåer; från ett händelseförlopp (t.ex. ett haveri) till högsta ledningsfunktionen.
Referenser:	Kjellen, U. och Tinmannsvik, R. (1989). SMORT - Säkerhetsanalys av industriell organisation, Arbetarskyddsnämnden, Stockholm.
Procedur / arbetsgång:	Man kan välja att göra analysen som en generell genomgång, eller att ta ett inträffat olycksfall som utgångspunkt. En analys görs på en "nivå" i taget. För varje nivå finns en checklista med frågor som ska diskuteras och besvaras med *Ja* eller *Nej.* De fyra nivåerna är: 1. Händelseförloppet analyseras för inträffade eller tänkbara olycksfall. 2. Förhållanden i produktionen som kan förklara varför problem ej upptäckts och rättats till. 3. Resurserna för att ta tillvara säkerheten vid utformning av nya anläggningar. 4. Informationssystemen inom företaget beträffande säkerheten, skyddspolicy och genomförandet av denna på företagsnivå.
Typ av resultat:	Summering av brister i säkerheten och förslag till åtgärder. En jämförelse mellan modellen och säkerhetsarbetet i företaget. (Arbetssättet innebär många kontakter med personer på olika befattningar, vilka ska ge kommentarer till protokoll etc. Man kan därmed förmoda att för många företag får man förbättring av attityderna till säkerhet.).
Kommentarer:	Genomgången med metoden kan ge ett stort antal idéer till åtgärder. SMORT utgår från en ideal organisationsmodell. Om företaget avviker mycket från denna, blir det fort många negativa svar, som analytikern kan få svårt att hantera om han inte har stor erfarenhet. Det finns en off-shore version av metoden.

www.ski.se

STATENS KÄRNKRAFTINSPEKTION
Swedish Nuclear Power Inspectorate

POST/POSTAL ADDRESS SE-106 58 Stockholm
BESÖK/OFFICE Klarabergsviadukten 90
TELEFON/TELEPHONE +46 (0)8 698 84 00
TELEFAX +46 (0)8 661 90 86
E-POST/E-MAIL ski@ski.se
WEBBPLATS/WEB SITE www.ski.se