Riskanalysmetoder

Fredrik Nystedt

Department of Fire Safety Engineering
Lund University, Sweden

Brandteknik
Lunds tekniska högskola
Lunds universitet

Rapport 7011, Lund 2000

Förord

Kompendiet utgör den teoretiska grunden till föreläsningarna om riskanalysmetoder i kursen Riskhantering 1 för BI3, HT99 och har tagits fram av Sycon Energikonsult AB på uppdrag av Brandteknik, LTH. Kompendiet är en sammanställning av befintlig litteratur med följande publikationer som viktiga referenser.

- Riskanalysmetoder, Hans T. Karlsson, Avd. för Kemisk teknologi, Lunds universitet, 1997.

- Risk Management 2000, Gustav Hamilton, Studentlitteratur, Lund, 1996.

- Värdering av risk, Räddningsverket, Rapport P21-182/97, Karlstad, 1997.

- Riskhantering och fysisk planering, Räddningsverket, Rapport P21-175/97, Karlstad, 1997.

- Riskinventering Öresund, O. Harrami & M. Kylefors, LUCRAM, Lunds universitet, 1999.

- Vådautsläpp av brandfarliga och giftiga gaser och vätskor, Försvarets forskningsanstalt, FOA-R—97-00490-990-SE, Umeå, 1997.

- Internt arbetsmaterial från Øresund Safety Advisers AB.

Innehållsförteckning

1. Introduktion

Med en risk menar vi faran för att en slumpmässig händelse negativt skall påverka möjligheten att nå ett uppställt mål. Matematiskt kan risken uttryckas som en produkt av sannolikheten för och konsekvensen av den skada som risken kan ge upphov till. Det finns en klar skillnad mellan en ”risk” och ett ”hot”. Vi lever med ett stort antal potentiella risker runt om oss, men endast ett fåtal utgör i varje ögonblick ett egentligt hot. Så länge vi går på trottoaren utgör trafiken på körbanan en risk, men blir först ett hot i det ögonblick som vi korsar gatan. Av alla risker är det därför hoten vi i första hand bör gardera oss emot. Huvudmoment som behandlas i detta kapitel är:

- Varför genomförs en riskanalys?
- Riskbegreppet – omfattning och innebörd
- Vad består en riskanalys av?
- Vilka metoder finns?

Riskbegreppet

Riskbegreppet är oerhört komplext och täcker in ett mycket stort antal olika samhällssektorer. Risker finns av alla möjliga slag, det kan vara politiska risker, inbrottsrisker, ekonomiska risker, miljörisker, olycksrisker etc. De risktyper som är mest dramatiska och skrämmande är de risker som hotar mänsklig överlevnad på kort eller lång sikt, t.ex. krig, svält, olyckor, och allvarlig miljöförstöring.

Med risker menas här risker för olyckor som kan skada människor, miljö och egendom, och som kan leda eller som skulle kunna till en räddningstjänstinsats. Exempel kan vara brand, explosion, trafikolyckor, kemikalieolyckor, naturolyckor etc.

Risker är i de flesta fall förknippade med något negativt, men ökad medvetenhet om risker kan också leda till positiva resultat genom ökat säkerhetstänkande och ökad förmåga att hantera olika situationer.

Risker, riskkällor och skadeförlopp

Man brukar särskilja begreppen risk och riskälla. En riskkälla är ett hot som kan leda till en olycka. Hotet är alltid den inneboende naturen hos kemikalier, viss processutrustning och apparatur, liksom handlanden och händelser. En lagringstank med eter är således en stor riskkälla, vilken kan leda till brand eller explosion. De huvudsakliga riskkällorna inom kemisk processindustri utgörs av de som kan leda till en eller flera av de tre följande konsekvenser:

- Brand
- Explosion
- Giftutsläpp

där giftutsläpp avser utsläpp av kemikalier som kan orsaka skador på människa och miljö. Man brukar ofta benämna de ovanstående faktorerna som de huvudsakliga riskkällorna inom kemisk processindustri.

Risk definieras som en storhet. Definitionen på risken för en olycka kan göras med följande ekvation:

$$R_0 = P_0 \times K_0$$

där P_0 är sannolikheten för olyckan och K_0 dess konsekvens. Man kan antingen räkna på risken för en olycka under en hel livslängd eller risken för att olyckan inträffar en gång. För konsekvenser med materiella skador, får risken för olyckan (R_0) enheten kr/år respektive kr. För dödsfall som konsekvens, blir enheten antal döda/år, respektive antal döda.

En olycka eller katastrof kan inträffa om en viss typ av avvikelse uppstår i en process. Vägen från denna avvikelse, sk utlösande händelse, till olycka är i regel lång och går via ett antal händelser i en viss sekvens, dvs ett sk skadeförlopp. Orsakerna till olyckor eller katastrofer inom kemisk processindustri har kartlagts i ett stort antal undersökningar. Resultatet av sådana undersökningar beror väsentligen av underlaget för undersökningen, samt hur stora olyckor som beaktas. Tabell 1 visar ett exempel baserat på utbetalning av försäkringar.

Tabell 1 Orsaker till olyckor inom kemisk industri

Orsak till olycka eller tillbud	Andel %
Bristande kunskap om kemikaliers egenskaper	4
Bristande kunskap om processkemin och processtekniken	11
Dålig dimensionering och layout av processutrustning	21
Dåligt underhåll	31
Operatörsfel	7
Annat	26

Procentandelen anger således andelen kapital som åtgått för att täcka förluster orsakade enligt de olika kategorierna. Som framgår utgör direkta brister i kunskaper avseende kemi och kemiteknik en relativt liten andel (15 %). Av större betydelse är brister i underhållsarbetet. Således leder bristande underhållsarbete till oönskade feltillstånd pga för tidigt slitage och korrosion av material och maskindelar. Med dålig dimensionering avses främst avvikelser från god praxis vad gäller ingenjörskonst. Detta kan vara antingen avsiktligt eller oavsiktligt. Det är vidare märkbart att en stor andel olyckor, tillhörande gruppen annat, inte kunnat klarläggas i detalj. Detta är ej sällan förekommande vid större olyckor eller katastrofer.

Inom processriskanalysen arbetar man med att modellera skadeförlopp. Detta sker med utgångspunkt från sk logiska processflödesscheman och statistiska teorier. Sådant modelleringsarbete faller under disciplinen tillförlitlighetsanalys. Utlösande händelser i ett skadeförlopp kan vara av mycket olika natur. I följande punkter ges de olika kategorierna som är av intresse:

- Felfunktioner kan inträffa i utrustningsdelar såsom pumpar, kompressorer, ventiler, omrörare och instrument. Orsaken till en felfunktion kan vara a) rent mekaniskt eller termiskt slitage; b) av slumpmässig natur pga störningar och vibration. Fel kan förr eller senare uppstå utan att det nödvändigtvis beror på slitage; c) installations- eller konstruktionsfel.

- Vid materialfel pga korrosion, erosion eller tryckpåkänningar, kan läckage i behållare, ledningar, kopplingar, axeltätningar etc uppstå.

- Mänskliga felhandlanden vid projektering, konstruktion, drift och underhåll är en typ av utlösande händelse. Denna är i regel svår att beakta.

- Yttre händelser, såsom blixtnedslag och oväder kan också vara en utlösande händelse.

De skadehändelser och konsekvenser som uppstår efter en utlösande händelse kan i princip vara vad som helst, inklusive den typ av fel som karaktäriseras som utlösande händelser. Således kan en skadehändelse vara a) förändringar i processparametrar såsom tryck, temperatur, koncentration, flöde och fassammansättning; b) läckage, utflöde och spridning av gaser och vätskor; c) mänskligt felhandlande; d) brand och explosion.

Följande slutkonsekvenser är tänkbara:

- Skada på processanläggningen.
- Skada på kringliggande anläggningar.
- Produktionsbortfall.
- Hälsoeffekter.
- Dödsfall.
- Skada på miljö och ekosystem.

Slutkonsekvenser kan således alltid hänföras till en eller flera av följande tre huvudkategorier; förlust av pengar, skada av miljö samt skada av hälsa, inklusive permanenta effekter och dödsfall. Således motiveras processriskanalysen inte enbart av miljöfrågor och risk för "liv och lem"'. En säker och tillförlitlig produktion är givetvis också av intresse. Åtgärder mot skadeförlopp kan sammanfattas enligt följande:

- Installation av säkerhetssystem i form av a) dubblering av kritiska system och processfunktioner, samt införande av b) säkerhetsventiler, facklor, etc. Dubblering av processutrustning är kostsamt, men kan erbjuda möjligheter till mycket driftsäkra system. Säkerhetsventiler och facklor hanterar oönskade övertryck och bryter ett skadeförlopp. Med facklor bränns överskott av brännbara gaser i en process.

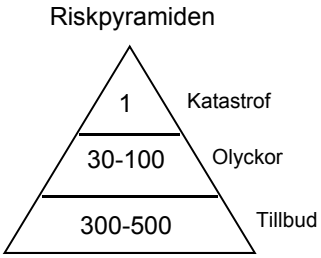
- Skyddsanordningar såsom skärmväggar och invallningar kan konstrueras för att skydda mot konsekvenser i form av explosioner. Till denna kategori av åtgärder kan också hänföras sprinklersystem och personlig skyddsutrustning

- Som sista åtgärd gäller att förbereda för skyddsåtgärder som larm, samt räddnings- och evakueringsinsatser.

De ovanstående faktorerna utnyttjas för att bryta ett skadeförlopp. Det gäller dock att undvika utlösande händelser.

Riskmått

Man vet att förlopp med en stor konsekvens inträffar mer sällan än förlopp med liten konsekvens. Detta har illustrerats i Figur 1 med den klassiska ”riskpyramiden”.



Figur 1 *Samband mellan frekvens och omfattning av konsekvens*

Man brukar dela in konsekvenser efter storlek som tillbud, olyckor och katastrofer. För varje katastrof inträffar således 30-100 olyckor och 300-500 tillbud.

Tre vanliga sätt att kombinera information om sannolikhet och konsekvens för förlust eller skada diskuteras i Chemical Process Quantitative Risk Analysis (Center for Chemical Process Safety, 1989):

Riskindex

Riskindex som är en siffra/tabeller som ger en enkel presentation. Kan användas som ett relativt eller ett absolut mått. Begränsning i att de inte utgör ett absolut kriterium för att acceptera eller förkasta en risk, saknar nyansering och kommunicerar inte samma information som individ- och samhällsriskmåtten. Exempel på vanliga index: *The Fatal Accident Rate* (FAR) (se Tabell 2) beskriver antal dödsfall per 10^8 exponeringstimmar. Indexet är direkt proportionerlig till den genomsnittliga individrisken.

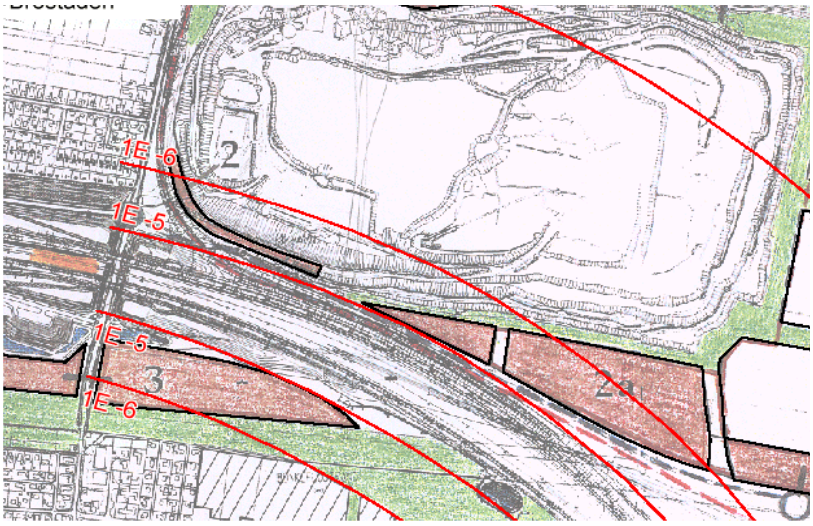
Tabell 2 *Antal dödsoffer enligt FAR. Siffrorna återspeglar antalet dödsoffer för 1000 personers totala arbetstid under ett helt liv.*

Aktivitet	Index
Kemisk industri	3.5
Stålindustri	8
Jordbruk	10
Fiske	35
Kolgruvor	40
Banarbete/järnväg	45
Byggnadsindustri	67

The Individual Hazard Index (IHI) är i princip FAR fast för en särskild fara. *The Average Rate of Death* (ARD) uttrycker det förväntade genomsnittliga antalet dödsfall per tidsenhet till följd av alla möjliga händelser (kallas också Accident Fatality Number). *The Equivalent Social Cost Index* är en modifierad variant av ARD där hänsyn tas till samhällets motvilja mot stora olyckor. *The Mortality Index or Number* baseras på det observerade genomsnittliga förhållandet mellan dödsfall och massa lagrat material och används för att karaktärisera potential fara för giftiga, lagrade ämnen.Detta är egentligen ett faroindex då ingen hänsyn tas till sannolikheten. *The Economic Index* är ett mått på ekonomisk förlust och kan användas för rangordna olika riskreducerande åtgärder eller jämföras mot ett specifikt ekonomiskt riskmål.

Individrisk

Måtten för individrisk beskriver risken för en individ som kan befinna sig var som helst inom riskområdet/det av händelser påverkade området. Individrisken beskrivs ofta med riskkonturer (se Figur 2) som visar den förväntade frekvensen för en händelse som orsakar en viss nivå av skada i ett specifikt område oberoende om det finns någon i området eller inte. Ett flertal varianter av individrisk används också: *Maximal individuell risk* beskriver den maximala individrisken inom den population som exponeras för risken (oftast, men inte nödvändigtvis, närmast riskkällan). *Genomsnittlig individuell risk (I)* för den exponerade populationen kan vara lämplig om risken är relativt likformigt distribuerad över populationen (annars missvisande). *Genomsnittlig individuell risk (II)* för en i förväg definierad population där ingen hänsyn tas till om populationen verkligen är exponerad för risken. Om den valda populationen är för stor kommer den genomsnittliga individrisken att undervärderas. *Genomsnittlig individuell (III) risk* kan också uttryckas för en exponeringstid eller arbetstid.



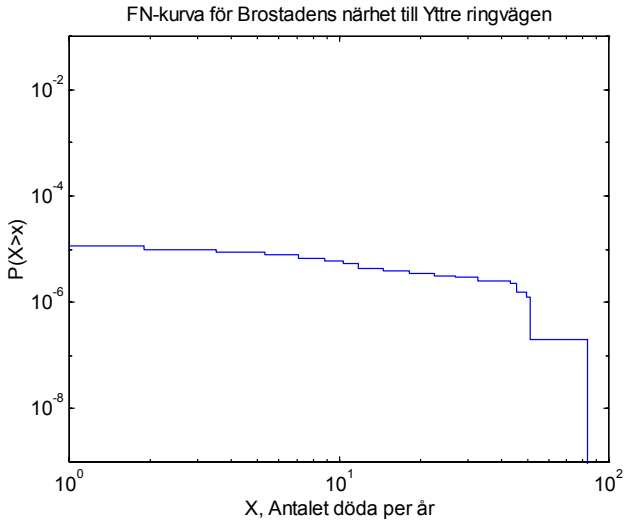
Figur 2 *Exempel på riskkonturer markerade på en karta som underlag för stadsplanering*

Samhällsrisk

Risken för en grupp människor inom riskområdet benämns samhällsrisk. Samhällsrisk beskrivs ofta med en *FN-kurva* som visar frekvensen (ackumulerad) för olyckor mot antal omkomna (fatala händelser) men kan också beskrivas som *förväntat antal omkomna per år* (PLL – Potential Loss of Lives). Exempel på FN-kurva visas i Figur 3.

Skillnaden mellan individ- och samhällsrisk kan beskrivas med att individrisken för en population inom riskområdet inte påverkas av populationens storlek medan samhällsrisken är direkt beroende av antal människor i populationen, vilket utvecklas i nedanstående exempel.

I ett kontorshus i närheten av en kemisk industri vistas 400 människor dagtid och en vakt på natten. Om sannolikheten för olycka är lika stor hela dygnet så utsätts varje individ för en risk som är oberoende av antalet personer närvarande. Den individuella risken är den samma för alla 400 dagtid och för den ensamma vakten på natten. Samhällsrisken är dock avsevärt högre dagtid då 400 personer är närvarande än på natten då endast en person är i huset.



Figur 3 *Exempel på FN-kurva för utsläpp av giftig gas intill ett bostadsområde*

Riskperception, acceptanskriterier och värdering

I våra dagars samhälle är sannolikheten för ett dödsfall endast i undantagsfall större än en på l 000. Risker på denna nivå och högre bedöms så allvarliga att samhället ingriper och satsar avsevärda resurser för att begränsa dem När sannolikheten blir en på l0 000, vilket gäller t ex bilolyckor, är samhället benäget att ingripa endast i begränsad omfattning. Risken en på 100 000 medför i regel bara måttliga eller små åtgärder från samhällets sida. Enligt uppgift torde den schweiziska industrin vara beredd att acceptera risker som är mindre än en på 10 000 000. Vid en sannolikhet under införs inga åtgärder i förebyggande syfte.

Människor reagerar dock inte på riskers siffermässiga värde utan mer på antalet, hur de själva upplever risken. Risker som hänger samman med en ny okänd teknik överdrivs ofta, under det att gamla kända risker inte sällan underskattas. Vi kan sålunda acceptera risken för en bilolycka men knappast risken för ett haveri i ett kärnkraftverk, trots att antalet dödsoffer i trafiken, hur man än räknar, vida överträffar antalet döda i inträffade kärnkraftolyckor. I en tid då vi utsätts för nya tekniker nästan dagligen bör man hålla detta i minnet. Med bristande erfarenhet av en ny företeelse följer en större eller mindre osäkerhet. Risken kan också uppfattas som en möjlighet. Det kinesiska språket har samma uttryck för risk som chans.

När det gäller om en risk skall anses vara acceptabel eller tolerabel säger Räddningsverket bla:

- Det finns ingen generellt accepterad nivå.
- Att olyckor legat på en viss nivå under en längre tid innebär inte att de är acceptabla.
- Det är inte acceptabelt att flera hundra människor kan omkomma i en olycka.

En viss verksamhet kan bedömas acceptabel å allmänhetens vägnar och de oönskade risker som verksamheten medför anses då vara tolerabla. Acceptanskriterier är nödvändiga för att göra det möjligt att använda ett riskbaserat angreppssätt och uppmuntra konstruktörer till detta. Genom att den säkerhetsnivå som samhället

finner acceptabel preciseras och kvantifieras skapas ett medvetande om vilka risker olika verksamheter är förknippade med.

Värdering av risker görs utifrån ett antal principer beroende på bla utifrån vilket syfte man har med riskjämförelsen:

- Rimlighetsprincipen innebär att en risk som med rimliga medel kan elimineras eller reduceras alltid ska åtgärdas.
- Proportionalitetsprincipen innebär att de totala riskerna för en verksamhet ska vara i proportion med nyttan av densamma.
- Fördelningsprincipen innebär att enskilda och grupper inte ska vara utsatta för oproportionerligt stora risker i förhållande till de fördelar som verksamheten innebär för dem.
- Principen om undvikande av katastrofer innebär att risker inte ska resultera i konsekvenser som tillgängliga beredskapsresurser inte kan hantera.

Det är möjligt att jämföra risker på flera rationella sätt trots att dessa kan vara väldigt olika och direkt motstridiga. De flesta modeller för riskvärdering utgår ifrån ett fåtal kvantifierbara faktorer som sedan utvärderas. Sociala värderingar är svåra att kvantifiera och lämnas därför oftast utanför värderingen. Vidare kan resultaten av utvärderingarna som ofta är endimensionella och därmed inte ger en bild av den komplexitet som oftast råder i sakfrågan ifrågasättas. Det finns åtta dimensioner som var och en för sig är för komplicerade för att karakteriseras endimensionellt. Dessa är:

- Negativa konsekvensers karaktär kan variera beroende på vilken metod som används för att värdera konsekvenserna. Karaktären av risken påverkas också av hur konsekvenserna av en verksamhet/riskkälla (tex sannolikheten för att dödsfall, skadade, sjukdomar, och kortsiktig respektive långsiktig påverkan på miljön) värderas sinsemellan.

- Frivilligheten (kan enkelt sett anses bestå av aspekterna uppoffring och kontroll) är svår att värdera i risksammanhang eftersom det är en subjektiv uppfattning hur stor uppoffring som krävs för att undvika en risk och vilken grad av kontroll man som enskild har över en risk.

- Individuell och kollektiv syn på risk skiljer sig och det behövs oftast en sammanvägning (kan göras på många olika sätt) av dessa synsätt. T ex beskriver det förväntade antal dödsfall den kollektiva risken medan individrisken lämpligast beskrivs med sannolikheten att omkomma till följd av exponering.

- Katastrofer och sannolikhet – samtidigt som de flesta riskanalytiker anser att konsekvenser ska värderas i proportion till sannolikheten visar flera psykosociala studier att de flesta människor inte uppfattar risk på detta sätt. Det finns förespråkare för att stora olyckor/katastrofer ska ges proportionerligt liten vikt medan det är mer vanligt att det anses att dessa olyckor ska ges stor vikt trots att de är mycket osannolika.

- Tidsfaktorn är viktig vid beslut om risker. Hur påverkar beslut idag de framtida generationerna? Kan man skjuta fram beslut och hoppas på teknologiska framsteg eller kommer det ske en teknisk regression? Det är svårt att förutspå politiska förändringar och förändringar i värderingar (vi vet tex att vår syn på hälsorisker har förändrats drastiskt under det senaste seklet).

- Beslut under osäkerhet. Det råder oftast brist på information vid riskbeslut. En indelning av bristen på information kan göras enligt följande: *known knowns* (rationell kunskap/saker du kan förutsäga), *unknown knowns* (underförstådd kunskap/saker som du inte vet att du vet), *known unknowns* (saker som du vet att du inte kan förutsäga) och *unknown unknowns* (saker som du ännu inte vet att du inte vet). Till denna indelning brukar man lägga till en klass som kallas *knowabel unknowns* eller *rouge set* (dessa kan göras förutsägbara genom att testa dem men kostnaden är för stor – t ex om en missil kommer igenom ett radarsystem).

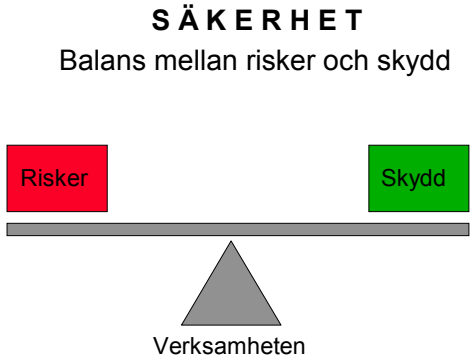
- Nya och gamla risker. Oftast ställs högre krav på nya teknologier jämfört med gamla eftersom det anses finnas tillräcklig erfarenhet av äldre teknologier och de risker som är förknippade med dessa (vilket inte alltid behöver vara fallet t ex kan kemikalier ha hälso- och miljöpåverkan på mycket lång sikt). Ytterligare en anledning till att nya teknologier och risker till följd av dessa bedöms hårdare är att det inte är önskvärt med en allt för stor ökning av den totala risknivån.

- Kunskapstillgängligheten har visat sig vara viktig för hur gemene man uppfattar risker. Om informationen om en risk är svårtillgänglig (stödjer sig på teknisk kunskap inom högt specialiserade områden eller att spridningen av information är bristfällig) tolkas det som en osäkerhetsfaktor i samband med värdering av risken.

Riskanalysen

Riskanalysen kartlägger en verksamhets riskmiljö. Med verksamhet menas företag, kommun, offentlig förvaltning, etc. Den övergipande målsättningen med en riskanalys är att få fram ett underlag för risk managerns beslutsprocess i form av trovärdig information om hot och risker.

- Riskanalysen skall sålunda identifiera hot och risker.
- Riskanalysen skapar därmed förutsättningar för att programmet för skydd och säkerhet blir korrekt och fullständigt.
- Riskanalysen skall ge underlag för ett kostnadseffektivt val av förebyggande åtgärder, så att reduktionen av skadekostnaden alltid blir större än kostnaden för själva åtgärden (se Figur 4).



Figur 4 *Säkerhet innebär en god balans mellan risker och skydd*

Riskanalysen inleds lämpligen med en tillbakablick för att få kunskap om de skador och förluster som verksamheten drabbats av tidigare. Studera därför den statistik som bör finnas över skador och förluster under den senaste femårsperioden. Redan denna granskning ger en översiktlig bild av riskmiljön men också hur den har påverkat verksamheten. Fortsätt därefter med en analys av dagens risker. Denna analys skall primärt identifiera de risker som finns för att sedan övergå i en värdering av dem. Identifieringen tar fram vilka risker som finns, under det att värderingen skall klara ut hur stora och frekventa de är. Riskanalys/riskvärdering är den process, formell eller intuitiv, genom vilken framtida förväntade förluster eller enskilda största förlust beräknas i monetära, kvantitativa eller kvalitativa termer eller som acceptabla/ oacceptabla

Mål och syfte

Förutom att utförandet av en riskanalys kan betyda lägre risk för person- och miljöskador kan det många gånger vara direkt ekonomiskt föredelaktigt att utföra en riskanalys. Denna pekar ju på egenskaper hos det studerade systemet som innebär risk för skadehändelser och därmed kanske också risk för ekonomisk förlust pga skadad egendom. Genom sk kostnads-nytta analys kan kostnaden för att minska risken ställas i relation till minskningen av den ekonomiska förlusten. Härmed erhålls ett mått på om de riskreducerande åtgärderna är lönsamma eller ej. Utöver egendomskostnader kan även andra kostnader uppstå vid en olycka:

- Produktionsavbrott kan i vissa fall innebära stora kostnader. Förutom direkt kostnad för förlorad produktion kan ett längre produktionsavbrott innebära risk för att man tappar enskilda order eller kunder.
- En olycka ger upphov till mycket improduktiv tid i samband med undersökningar och utredningar, rekrytering etc.
- Direkta kostnader för miljöskador kan komma i form av saneringskostnader. Indirekta kostnader kan uppkomma i form av försämrade omvärldsrelationer.
- Övriga kostnader kan uppkomma i form av ökade försäkringskostnader, skadestånd mm.

Riskanalysen syftar till att optimera riskkostnaden. Riskkostnaden är en kalkylerad kostnad för skador och skyddsåtgärder i vid bemärkelse. Den utgör summa av försäkringspremier, kostnad för skadeförebyggande åtgärder, skadekostnader och RM-administration. De lösningar för ökad säkerhet och trygghet som riskanalysen resulterar i skall baseras på en medveten avvägning mellan risk och totalekonomi (se Figur 5). Riskanalysen används även som ett verktyg för en kommun vid upprättande av räddningstjänstplan mm.

Figur 5 Avvägning mellan skydds- och skadekostnad

Vem ställer krav?

I många verksamheter föreligger det krav från olika myndigheter att genomföra en riskanalys. Exempel på myndigheter som kan ställa sådana krav är:

- Spängämnesinspektionen
- Arbetarskyddsstyrelsen
- Statens Räddningsverk
- Statens Naturvårdsverk
- Koncessionsnämnd
- Byggnadsnämnd
- Yrkesinspektion
- Räddningsnämnd
- Länsstyrelsen

Några lagar med relativt brett tillämpningsområde som berör riskanalys är:

- Lagen och förordningen om brandfarliga och explosiva varor (LBE och LFE).
- Arbetsmiljölagen, Arbetsmiljöförordningen och Arbetarskyddsstyrelsens Författningssamling.
- Räddningstjänstlagen (RäL) och -förordningen (RäF). *Speciellt §43 RäL. Anläggningar där verksamheten innebär att fara för olyckshändelse skall orsaka allvarliga skador på människor eller i miljön.*
- Miljöbalken

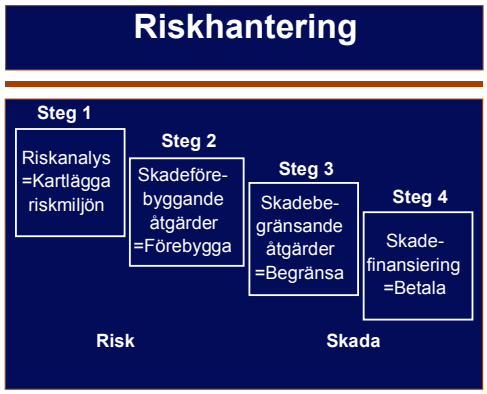
Även om det inte föreligger något krav på att utföra en riskanalys kan det i många fall ändå vara tillrådigt att utföra en. Det kan t ex gälla att bedöma riskerna för personalen eller riskerna för ekonomiska förluster pga egendomsskada, produktionsbortfall eller kvalitetsförsämringar.

Omfattning

Tag som ett exempel en verksamhet som innefattar kemikaliehantering. En analys av de risker som gäller själva kemikaliehanteringen bygger förutom på egenskaperna hos de ämnen som hanteras och hanteringsförhållandena, även på uppgifter om;

- Stör- och skadehändelser (vad kan hända, var hur och i vilken omfattning)
- Spridningsförhållanden (omgivningsdata)
- Skadeobjekt (vad kan påverkas)
- Skadeförebyggande, -begränsande åtgärder (hur minskas sannolikheter och konsekvenser)

Riskanalysarbetet innebär att ta fram och granska dessa underlagsuppgifter, att beskriva de skadefall som kan inträffa och som innebär risk för olyckor samt att uppskatta sannolikheter för och konsekvenser av dessa. Riskanalysen är en del av riskhanteringsprocessen som syftar till att kartlägga riskmiljön, förebygga, begränsa och finansiera skadorna (Figur 6).



Figur 6 *Riskhanteringsprocessens fyra steg*

2. Tillförlitlighetsberäkningar

Behovet av tillförlitlighetsanalys föreligger därför att apparatur och utrustning i processer kan haverera eller gå sönder. Teorier för tillförlitlighet omfattar två problemområden. Det första området är analys och beskrivning av fel och orsaker till fel hos enskilda komponenter i en process. Man använder både kvalitativa beskrivningar och kvantifieringar med hjälp av sk feldata. Det andra området är analys av hur ett komponentfel påverkar driften av den process i vilken komponenten ingår. Speciellt vill man se hur ett visst fel fortplantar sig i en process. Denna analys av ett system kan vara kvalitativ såväl som kvantitativ.

Det grundläggande och centrala begrepp man utnyttjar är den sk tillförlitligheten, betecknad R(t) efter engelskans ”reliability”. Som framgår är R(t) en tidsberoende storhet. Man definierar tillförlitligheten för ett system som:

- Sannolikheten att systemet ej havererar under en drifttid av t (timmar, år, etc)

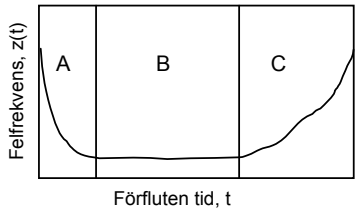
Med system kan avses en enskild komponent eller en hel process. Tillförlitligheten är således ett sannolikhetsmått och beskriver exempelvis inte hur ofta, eller hur lång tid, ett system befinner sig i feltillstånd. Med feltillstånd avses att systemet ej uppfyller kraven för normaldrift. Tillförlitligheten antar värden i intervallet $0 < R(t) < 1$. Gränserna gäller för utopiska system där $R(t) = 0$ för ett system som helt säkert kommer att hamna i feltillstånd och $R(t) = 1$ för ett system som aldrig kommer att hamna i ett feltillstånd. Ett användbart begrepp är komplementet till tillförlitligheten, vilket är otillförlitligheten, definierad som:

$$Q(t) = 1 - R(t) \qquad \textit{Ekvation 1}$$

som således beskriver sannolikheten för att ett system havererar när det varit i drift under tiden t.

Felfrekvenser

Det klassiska exemplet att beskriva felfrekvensen kvalitativt på ett generellt sätt är den sk ”badkarskurvan:’, vilken visas i Figur 7. Det framgår av dess karakteristiska utseende hur kurvan har fått sitt namn. Kurvan illustrerar ett flertal tänkbara felmekanismer för en tilltänkt komponent.



Figur 7 Felfrekvens enligt badkarskurvan

Under fas A, dvs strax efter uppstart minskar felen kraftigt och snabbt i frekvens. Detta kan hänföras till ett flertal faktorer som intrimning, eliminering av konstruktionsfel, samt upplärning av operatören. Under fas B sker felen med någorlunda konstant felfrekvens. Haverier kan exempelvis uppstå genom statistiska störningar utifrån såsom vibrationer och tryckstötar. Efter en viss drifttid (fas C) ökar

och sedan accelererar felen i frekvens. Detta beror på slitage och exponering för exempelvis korrosiv miljö och damm.

Då en fungerande komponent går mot ett feltillstånd sker detta slumpmässigt och irreversibelt. Under dessa förutsättningar kan man beskriva antalet felfungerande komponenter enligt följande:

$$\frac{dn}{dt} = -z\,x\,n \qquad \textit{Ekvation 2}$$

där z är ”hastighetskonstanten” för sönderfallet och n är antalet komponenter. Under antagandet att vi har ett statistiskt sett stort antal komponenter från början, kan vi skriva tillförlitligheten, baserat på den rena definitionen enligt följande:

$$R(t) = \frac{n}{n_0} \qquad \textit{Ekvation 3}$$

Derivering av detta samband med avseende på tiden ger:

$$\frac{dn}{dt} = n_0\,x\frac{dR(t)}{dt} \qquad \textit{Ekvation 4}$$

Eliminering av n genom insättning av de senare två ekvationerna i Ekvation 2, ger följande samband efter separering:

$$-z(t)dt = \frac{dR(t)}{R(t)} \qquad \textit{Ekvation 5}$$

Denna kan nu integreras. Man startar från tiden t = 0 där det alltid gäller att R(t) = 1 och integrerar till en godtycklig tidpunkt:

$$-\int_0^t z(t)dt = \int_1^{R(t)} \frac{dR(t)}{R(t)} = \ln\left[R(t)\right] - \ln\left[1\right] \qquad \textit{Ekvation 6}$$

Från detta samband kan tillförlitligheten lösas:

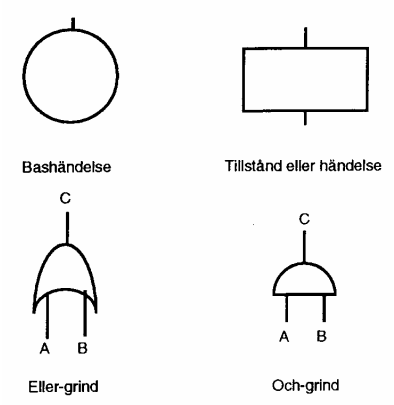
$$R(t) = \exp\left[-\int_0^t z(t)dt\right] \qquad \textit{Ekvation 7}$$

Denna ekvation är generell och gäller för alla typer av utseenden av felfrekvensen. Det är viktigt att notera att den tidsberoende felfrekvensen beskriver ett momentanvärde vid en viss tidpunkt t, medan tillförlitligheten är ett medelvärde för intervallet [0,t].

Logiska diagram

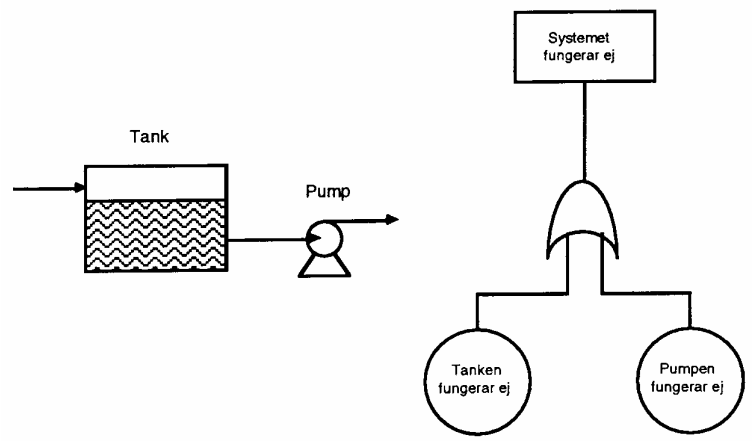
Ett felträd utgörs av logiska diagram som byggs upp av ett antal symboler, vilka visas i Figur 8. En händelse eller tillstånd är något som inträffar till följd av att en eller flera händelser inträffat tidigare. En händelse har en ingående koppling och en utgående koppling. Om symbolen avser det studerade tillståndet för processen, har den endast en ingående koppling och ingen utgående. Man brukar benämna detta topphändelse.

En bashändelse har en utgående koppling men ingen ingående. En bashändelse kan vara en utlösande händelse eller en händelse som inte är en konsekvens av något tidigare inträffat.



Figur 8 *De fyra nödvändiga symbolerna för logiska diagram*

Grindar används för att koppla samman händelser och tillstånd. En grind har alltid en utgående koppling och minst två ingående. För en eller-grind gäller att det utgående inträffar om minst en av de ingående har inträffat. Således är en av de ingående tillräckligt. För en och-grind gäller att det utgående inträffar om alla ingående inträffar. Strukturen i ett logiskt diagram skall illustreras med ett mycket enkelt exempel, omfattande en pump och en tank i serie. Vi bortser från rörledningarna och förutsätter att endast pumpen och tanken kan gå sönder. Vi definierar avsett tillstånd som: ”systemet fungerar ej”. Systemfunktionen är trivial: ”systemet fungerar endast om både pump och tank fungerar”. Det logiska diagrammet visas i Figur 9, som illustrerar användandet av en eller-grind. Det räcker således att den ena eller den andra bashändelsen inträffar för att topphändelsen skall inträffa.



Figur 9 *Logiskt diagram för en pump och tank i serie*

Konstruering av mer komplicerade logiska diagram kräver lång erfarenhet. För ett givet processflödesschema kan logiska diagram i regel konstrueras på fler än ett sätt. Det finns få generella konstruktionsmetoder som är idiotsäkra. En grundläggande konstruktionsregel föreslås dock att man alltid skall börja i toppen med det avsedda tillståndet för processen och arbeta sig nedåt mot bashändelserna.

Räkneregler

Räknereglerna för grindar utnyttjas vid kvantifieringen av det logiska diagrammet med hjälp av feldata. Räknereglerna är också av användning för att upptäcka vissa fel i diagrammet.

Eller-grind

Rent allmänt gäller att ingående feldata måste vara av en typ, dvs antingen enbart sannolikheter eller enbart felfrekvenser. Utgående feldata blir av samma typ som ingående. För felfrekvenser blir utgående felfrekvens summan av ingående felfrekvenser. För två ingående kopplingar (A och B) blir för utgående koppling (C):

$$z_C = z_A + z_B \qquad \textit{Ekvation 8}$$

För det generella fallet med n stycken ingående kopplingar blir den utgående felfrekvensen:

$$z_{ut} = z_1 + z_2 + \ldots + z_n \qquad \textit{Ekvation 9}$$

Dessa samband är triviala. För sannolikheter blir sambandet något mer komplicerat. För två ingående kopplingar gäller alltid:

$$P_C = P_A + P_B - P_A \times P_B \qquad \textit{Ekvation 10}$$

Och-grind

Som huvudregel finns två tänkbara representationer av feldata. Enligt den första är alla kopplingar representerade med sannolikheter. Sannolikheten för den utgående blir då alltid produkten av alla ingående sannolikheter. För fallet med två ingående (A och B), blir utgående:

$$P_C = P_A \times P_B \qquad \textit{Ekvation 11}$$

eller generellt för n stycken ingående:

$$P_{ut} = P_1 \times P_2 \times \ldots \times P_n \qquad \textit{Ekvation 12}$$

Enligt fall två representeras en ingående av en felfrekvens och de övriga med sannolikheter. I det fallet fås den utgående som en felfrekvens. För det förenklade fallet blir:

$$z_C = z_A \times P_B \qquad \textit{Ekvation 13}$$

Eller generellt för n stycken ingående kopplingar:

$$z_{ut} = z_1 \times P_2 \times \ldots \times P_n \qquad \textit{Ekvation 14}$$

Om feldata ej representerats som indikerats av räknereglerna bör man överväga om det logiska diagrammet är rätt uppställt.

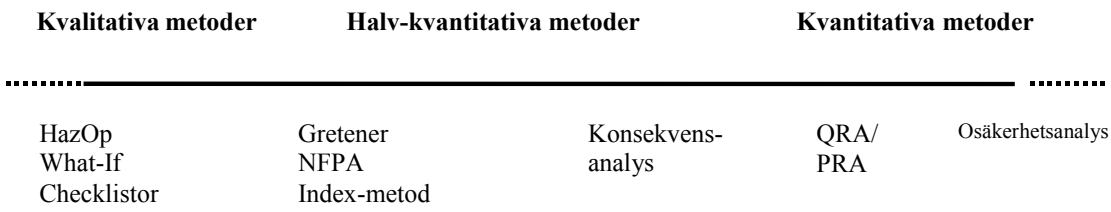
3. Riskanalysmetoder

Det finns ett flertal olika metoder för riskanalys med olika omfattnings- och detaljeringsgrad. Vissa metoder lämpar sig bäst för övergripande analyser, kanske första gången ett objekt eller system analyseras emedan andra är bäst lämpade för detaljerade studier av ett begränsat system. Hur skall man utvärdera olika metoder för riskanalys? Innan frågan besvaras är det viktigt att titta på de faktorer som måste tas hänsyn till:

- Vald metod måste vara användbar. Resultatet av riskanalysen måste uttryckas i termer som kan förstås och tolkas av ledningen.
- Vald metod måste vara praktisk. Värdet av en riskanalys måste vara större än kostnaden att genomföra den.
- Vald metod måste vara trovärdig. Osäkerheten i riskanalysens resultat måste vara inom acceptabla gränsvärden.

Översikt

I avsnittet ges en översiktlig beskrivning av några analysmetoder. Riskanalysmetoder kan delas in olika grupper beroende på deras grad av kvantifierbarhet, vilket illustreras i Figur 10 nedan.



Figur 10 Redovisning av olika riskanalysmetoder

Kvalitativa metoder

Till de enklare metoderna sett ur ett kvantitativt begrepp hör t.ex. grovanalysmetoder, HazOp och liknande. Dessa är vanligen speciellt anpassade för olika verksamheter t.ex. kemisk processindustri. Resultatet är ofta i form av beskrivningar av skeenden vid olika förutsättningar. Metoderna används främst för att identifiera riskerna. Visserligen är metoderna enkla till sin struktur och ger resultat som skulle kunna anses vara otydliga men man ska inte förledas att tro att de är dåliga för den sakens skull.

Halv-kvantitativa metoder

Nästa steg i raden av metoder för riskanalyser är de s.k. graderingsmetoderna eller indexmetoderna. De är något mer detaljerade i sin uppbyggnad och innehåller inslag av mått på konsekvenser av den oönskade händelsen samt sannolikheten för densamma. Dessa mått behöver inte utgöras av direkta siffermått utan kan beskriva storleksordningar. Den stora nyttan med denna typ av metoder är att de ger ett underlag för att kunna jämföra olika alternativ förenade med olika risk. De ger alltså

en rangordning på alternativen uttryckt i risk. Exempel på sådana metoder är SIA 81, också känt som Gretenersystemet, NFPA 101M och Räddningsverkets riskmatris.

Kvantitativa metoder

Den sista gruppen av metoder är där som risken beskrivs i kvantitativa termer t.ex. i sannolikheten för den oönskade konsekvensen eller i förväntat antal döda per år till följd av en viss verksamhet. Till denna grupp räknas också de konsekvensanalyser som inte innehåller något om sannolikheter. Dessa metoder brukar beskrivas som deterministiska eftersom de ger ett enstaka värde som resultat. Detta kan vara fallet t.ex. när utrymningssäkerheten i en lokal utvärderas. Mer vanligt är dock att sannolikheten och konsekvensen kombineras till ett riskmått. Man talar då ofta om s.k. probabilistiska metoder eftersom de just innehåller en beskrivning av konsekvenserna med olika sannolikheter. Alla riskanalyser kräver någon form av beskrivning av den oönskade händelsen.

Det finns i dag vedertagna former för att genomföra s.k. kvantitativa riskanalyser (QRA - Quantitative Risk Analysis) för scenarier som beskrivs med hjälp av händelseträd. Dessa kan ta hänsyn till att t.ex. olika tekniska system inte fungerar, med given sannolikhet. Vill man lägga riktigt mycket tid på en analys kan en QRA dessutom genomföras sammantaget med en osäkerhetsanalys. Resultatet blir både mycket detaljerat samt mycket omfattande. Det är därför viktigt att en avvägning görs mellan detaljeringsgrad och mängd information som behövs för att fatta beslut om åtgärder.

Checklistor

Checklistor baseras på tidigare gjorda erfarenheter och används för att identifiera kända typer av riskkällor och för att kontrollera att vedertagna standardförhållanden tillämpas. Den eller de som upprättar checklistorna måste således ha goda kunskaper om och stor erfarenhet av den aktuella anläggningen eller processen.

Checklistorna kan vara mycket detaljerade och anpassade till den specifika anläggningen eller processen, men även mer allmänt formulerade checklistor förekommer. I första fallet förekommer ofta specificerade krav på utrustningens tekniska utformning och på lämpliga driftsbetingelser. I det senare fallet kan frågor beträffande egenskaperna hos hanterade ämnen, förekomsten av riskhöjande hanteringsmetoder, effekter av yttre störningar och fel i stödfunktioner som el, tryckluft, kylvatten, behov av och kondition hos skyddsutrustning mm förekomma.

Checklistor kan förekomma i samband med

- Planläggning/utformning
- Konstruktion/uppbyggnad
- Inspektion/uppstart
- Drift
- Slutlig avstängning

En checklista är enkel att använda och kan ge resultat relativt snabbt. Checklistan erbjuder som regel en av de mest tids- och kostnadseffektiva metoderna för säkerhetsgranskning i samband med välbeprövad teknik där god praxis erbjuder tillfredsställande säkerhet.

Grovanalys

Grovanalys eller preliminär riskanalys används för att identifiera riskkällor utan hänsyn till detaljer i tekniska system. Ofta är avsikten att med metoden ge en grov bild av vilka system som kan medföra mer allvarliga risker. För dessa högrisksystem kan det vara motiverat att komplettera riskanalysen med en mer detaljerad analysmetodik.

Grovanalys tillämpas ofta tidigt i planeringsarbetet när enbart huvuddragen i processen eller anläggningen är kända men kan även med fördel användas som en första analys av riskkällorna i befintliga system. Metoden ger en kvalitativ lista över riskkällorna i anläggningen utan numeriska uppskattningar eller prioriteringar. Genom att låta personer med erfarenhet av liknande förhållanden intuitivt gradera riskkällornas sannolikheter och konsekvenser efter en tre- eller femgradig skala (se Tabell 3) samt sammanställa dessa uppskattningar erhålls dock en erfarenhetsbaserad värdering av riskerna.

Tabell 3 Exempel på frekvens- och konsekvensklasser för skadehändelser

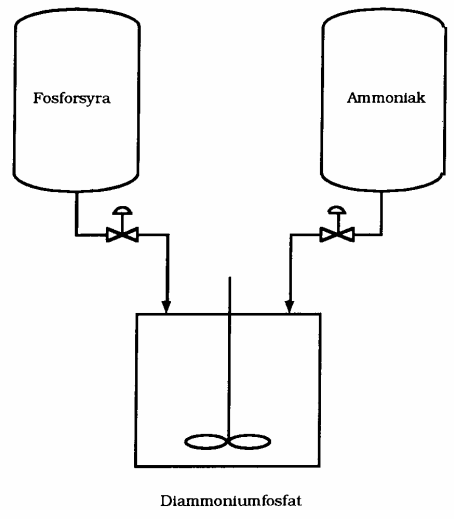
Klass	Frekvens	Konsekvens
1	Osannolik (< 1 gång per 1000 år)	Försumbar (ingen eller ringa skador)
2	(1 gång per 100-1000 år)	Farlig (mindre person- och egendomsskador)
3	Sannolik (1 gång per 10-100 år)	Allvarlig (betydande person- och egendomsskador)
4	(1 gång per }-10 år)	
5	Mycket sannolik (> 1 gång per år)	

En preliminär riskanalys sker enligt följande arbetsgång:

1. Avgränsa processen eller processteget
2. Identifiera och lista möjliga skadehändelser
3. Identifiera möjliga orsaker till dessa skadehändelser
4. Identifiera konsekvenserna av skadehändelserna
5. Värdera sannolikheten för skadehändelserna enligt en graderad skala (se Tabell 3)
6. Värdera konsekvenserna enligt en graderad skala (se Tabell 3)
7. Ge förslag till åtgärder

Exempel

En process för framställning av diammoniumfosfat från fosforsyra och gasformig ammoniak har förenklats såsom framgår av figuren. Genomför en preliminär riskanalys för diammoniumfosfatprocessen.



Figur 11 *Beskrivning av process för framställning av diammoniumfosfat*

Lösning

Information framtagen enligt den föreslagna arbetsgången kan sammanställas i ett formulär enligt det exempel som visas i Tabell 4. Den allvarligaste riskkällan utgörs av utströmning av ammoniak enligt sammanställningen.

Tabell 4 *Exempel på preliminär riskanalys för diammoniumfosfatprocess. (a) och (b) står för frekvens- resp konsekvensklass enligt Tabell 3.*

Skadehändelse	Orsak	Konsekvens	(a)	(b)	Åtgärd
Sprängning av ammoniaktank	Stumfyllning	Stort utflöde	1	3	Tryckavlastning, sektionering
Kopplingsläckage på gasledning	Fel på packning	Litet utflöde	3	2	Detektering, underhåll
Överdosering av ammoniak	Utrustningsfel	Utflöde	3	2	Analys, underhåll
Överdosering av ammoniak	Operatörsfel	Utflöde	4	1	Rutiner, utbildning
Brott på syraledning	Korrosion	Stort utflöde	2	2	Underhåll
Läckage i koppling på syraledning	Åldrad packning	Litet utflöde	3	1	Sprutskydd

”What if”-analys

Syftet med ”What if”-metoden är att identifiera riskkällor genom att värdera följderna av oplanerade händelser i det studerade systemet. Metoden innebär en analys av tänkbara avvikelser från planerad funktion och drift av systemet genom att ställa frågor av typen: ”Vad händer om…”. Frågorna formuleras utifrån tidigare erfarenheter och tillämpningen utgår ifrån ritningar, flödes- och instrumentscheman.

”What-if”-metoden kan användas i samband med utveckling, planläggning/ utformning, före uppstart eller på ett system i drift. Det är särskilt vanligt att metoden tillämpas för att värdera riskförhållandena i samband med en planerad förändring av en process eller utrustning. Resultatet utgörs av tabeller där möjliga skadeförlopp och följdverkningar anges tillsammans med eventuella förslag på riskreducerande åtgärder. Resultaten är kvalitativa och några inbördes jämförelser eller kvantitativa värderingarna av riskerna görs inte.

Följande arbetsgång tillämpas:

1. Ställ frågan: Vad händer om …. ?
2. Uppskatta sannolikheten för detta (låg, medel eller hög).
3. Identifiera konsekvensen.
4. Föreslå åtgärd.
5. Ställ ny fråga.

Exempel
Gör en riskanalys på diammoniumprocessen genom att ställa frågan:
Vad händer om? Exemplifiera endast med ett fåtal frågor.

Lösning
Knepet med den aktuella riskanalysmetoden är ju givetvis att komma på vilka frågor som skall ställas. Således krävs lång erfarenhet och insikt om processen. En analys kan exempelvis börja som följer:

Vad händer om:	Fel råvara levereras i stället för fosforsyra?
Sannolikhet:	Låg.
Konsekvens:	Oklar.
Åtgärd:	Utred vidare.
Vad händer om:	Fosforsyrans koncentration är för låg?
Sannolikhet:	Medel.
Konsekvens:	Ammoniaken förbrukas ej utan tillförs delvis arbetsluften.
Åtgärd:	Rutinmässig koncentrationsbestämning vid leverans före processtart.

osv…

Metoden är enkel men förutsätter fantasi. Det är lätt att förbise något väsentligt problem och den bör därför användas i form av successiva delanalyser av den totala riskmiljön.

HazOp - analys

Namnet står för ”Hazard and operability studies” och har utvecklats för att identifiera dels riskkällor och dels andra förhållanden i en process som även om de inte innebär skaderisker, kan försämra anläggningens förmåga att uppfylla de produktionsmål som uppställts. Metoden leder alltså längre än till enbart en analys av riskförhållanden.

HazOp-analysen innebär att en grupp bestående av personer med kompetens från flera olika områden utför en form av styrd ”brainstorming”. Man söker efter möjliga avvikelser från planerade driftförhållanden m h a systembeskrivningar, checklistor och ett speciellt system av s k ledord. Totalt finns sju ledord såsom framgår av Tabell 5.

Arbetsgången kan sammanfattas med följande tio punkter:

1. Välj en analyspunkt i processen.
2. Definiera normaltillstånd eller avsedd funktion i punkten.
3. Välj en processparameter i punkten.
4. Härled avvikelse genom att kombinera processparametern med ett ledord
5. Ta reda på möjliga orsaker till avvikelsen.
6. Uppskatta konsekvenserna.

7. Föreslå åtgärder.
8. Härled ny avvikelse (gå till 4).
9. Välj ny processparameter (gå till 3).
10. Välj ny analyspunkt (gå till 1).

Metoden är betydligt mer arbetskrävande än de som beskrivits tidigare. Den är mest kostnadseffektiv då den tillämpas på nya system, när utformningen nästan är fastställd och dokumenterad, eller på befintliga system, när mer omfattande förändringar planeras vad gäller processer eller utrustning. Metoden kan även med framgång tillämpas på befintliga system utan att förändringar planeras

Tabell 5 Ledord för HazOp

	Ledord	Betydelse
1	Nej, inte, inget	Avsedd funktion uteblir helt
2	Mer, högre	Kvantitativ ökning
3	Mindre, lägre	Kvantitativ minskning
4	Dessutom	Kvalitativ ökning
5	De av, delvis	Kvalitativ minskning
6	Motsatt	Omkastad funktion
7	I stället för	Funktion ersätts av annan

Exempel
Illustrera hur man kombinerar ledorden i Tabell 5 för att härleda en avvikelse i en process. Processparametern är flöde av (blandningen) A genom ett rör.

Lösning
För ledorden i Tabell 5 fås de respektive avvikelserna i processen som:

1. Inget flöde av A genom röret.
2. Flödet av A överstiger dimensionering.
3. Flödet av A understiger dimensionering.
4. Flödet består av A och något annat.
5. Endast vissa av komponenterna i A transporteras.
6. Flödet går i fel riktning.
7. Flödet består av andra komponenter än A.

Det är också viktigt att påpeka att en kombination av en processparameter och ett ledord inte alltid existerar, dvs det blir inte alltid en avvikelse för varje ledord. Genomgången av checklistan eller arbetsgången kan leda till ett flertal alternativ:

- Avvikelsen är irrelevant då den saknar möjlig orsak.
- Avvikelsen är möjlig men den får inga konsekvenser som är relevanta med hänsyn till analysens syfte.
- Avvikelsen innebär en risk då den kan leda till skadehändelser med allvarliga konsekvenser.
- Det behövs mer information för att ett tillräckligt detaljerat svar skall kunna ges.

Framkommer förslag till åtgärder för att eliminera identifierade riskkällor antecknas dessa och sammanställs i analysgruppens dokumentationsrapport.

FMECA

FMECA står för Felfunktions-, effekt- och konsekvensanalys (eng Failure Mode, Effect and Criticality Analysis) och innebär en tabellering av:

- Utrustningsdelar i systemet
- Delarnas avsedda funktion
- Delarnas möjliga felfunktion
- Varje felfunktions effekt på systemet
- En uppskattning av hur kritiska effekterna är vad gäller risken för skador

Felfunktionen anger hur utrustningsdelarna avviker från avsedd funktion (öppen, stängd, igång, stopp, läckage etc). Effekterna är systemets svar på det händelseförlopp som felfunktionerna orsakar.

FMECA kan användas vid planläggning/utformning, konstruktion/uppbyggnad samt vid drift. Metoden är inte effektiv när det gäller att identifiera kombinationer av felfunktioner vilka tillsammans leder till skadehändelser. I sådana fall kan en händelseträds- eller felträdsanalys vara lämpligare.

FMEA (Felfunktion- effektanalys) är ekvivalent med FMECA men utan uppskattning och rangordning av konsekvenser. Dock används ofta begreppen synonymt.

Mänsklig tillförlitlighetsanalys

Tillförlitliga operatörsåtgärder är en avgörande förutsättning för säkerheten hos en anläggning. Det är därför viktigt att kunna konstatera att operatörerna har rimliga möjligheter att identifiera, åtgärda och verifiera aktuellt processtillstånd. Analysen innebär en systematisk utvärdering av förhållanden som påverkar tillförlitligheten i operatörers, underhållspersonals och teknikers arbetsuppgifter. Sådana förhållanden är av både teknisk, kunskapsmässig och organisatorisk natur. Analysen identifierar beslut eller åtgärder som kan medföra ökad sannolikhet för att skadeförlopp utlöses eller utvecklas vidare. Orsaken till sådana beslut eller åtgärder kartläggs.

Tillförlitligheten av mänskligt handlande utgör dock en av de svåraste sakerna att uppskatta. Det finns några tumregelsmetoder för uppskattning av sannolikheten för felhandlande när ett larm signalerar. En mer avancerad metod har utvecklats för att skatta sannolikheten för operatörsfel vid olika situationer. Metoden som kallas TESEO (Technica Empirica Stima Errori Operati) baseras på faktorer som bestäms av typ av aktivitet, stressituation, operatörens förutsättningar, situationens allvarlighetsgrad och den ergonomiska situationen. Faktorerna uppskattas med hjälp av Tabell 6. Sannolikheten för operatörsfel beräknas med hjälp av faktorerna enligt följande ekvation:

$$P = \prod_{i=1}^{5} K_i \qquad \textit{Ekvation 15}$$

Tabell 6 Faktorer för skattning av mänsklig tillförlitlighet enligt TESEO

Typ av aktivitet	**K_1**
- Enkel, rutinbetonad	0.001
- Rutinbetonad, men kräver uppmärksamhet	0.01
- Ej rutinbetonad	0.1
Momentan stressfaktor (rutinbetonad aktivitet)	**K_2**
Tillgänglig tid (s)	
- 2	10
- 10	1
- 20	0.5
Momentan stressfaktor (ej rutinbetonad aktivitet)	**K_2**
Tillgänglig tid	
- 3	10
- 30	1
- 60	0.1
Operatörens förutsättningar för aktuell aktivitet	**K_3**
- Noga utvald, expert, väl utbildad	0.5
- Genomsnittlig kunskap och utbildning	1
- Liten kunskap, dålig utbildning	3
Situationens allvarlighetsgrad	**K_4**
- Allvarligt nödläge	3
- Hotande nödläge	2
- Normal situation	1
Ergonomisk situation	**K_5**
Bild av arbetsmiljö resp anläggningsstatus	
- Mycket bra	0.7
- Bra	1
- Varierande	3
- Varierande respektive dålig	7
- Dålig	10

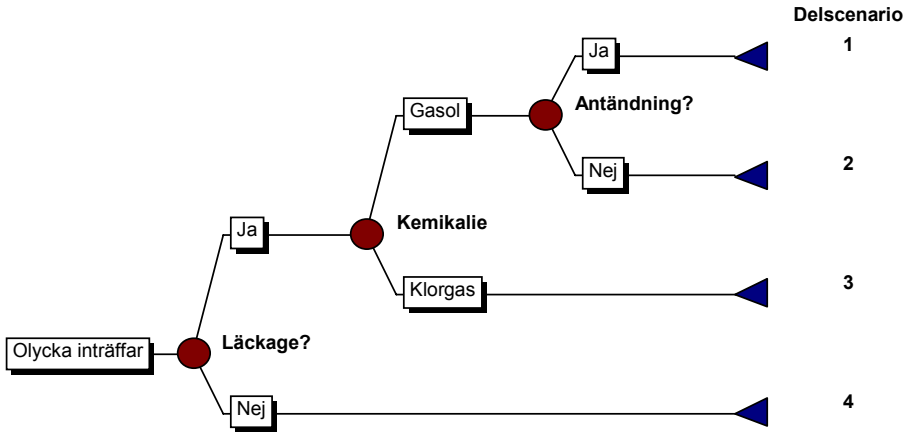
Händelseträdsanalys

Händelseträdsanalys används för att bestämma vilka skadehändelser som kan ske i ett system förorsakade av en specifik utlösande händelse som t ex en felfunktion i en stödfunktion, en utrustningsdel eller en mänsklig felhandling. Tillämpningen baseras med fördel på resultaten från en FMECA-analys.

Händelseträdsanalysen behandlar operatörernas handlande och utrustningens respons på den utlösande händelsen för att avgöra dess möjliga konsekvenser. Metoden är väl lämpad för system som har säkerhetssystem och nödlägesrutiner avsedda att förhindra utvecklingen av skadeförlopp. Ett händelseträd utgår från en initierande skadehändelse, tex farligtgodsolycka sker eller brand uppkommer. Beroende av vad som händer på vägen så formas att antal delscenarier. Genom att beräkna sannolikhet och konsekvens för resp delscenario kan ett antal riskmått tas fram. Metoden visas i följande exempel:

Exempel
Beskriv möjliga utfall vid en olycka med ett fordon som transporterar farligtgods. De kemikalier som transporteras på vägsträckan är gasol och klorgas. Beräkna sannolikheten för varje delscenario.

Lösning
Händelseträdet kan se ut enligt Figur 12 nedan:



Figur 12 Händelseträd för farligtgodsolycka

Från statistik och annan litteratur hittas sannolikheter för de olika händelserna. $P_{Läckage}$ = 0.20, P_{Gasol} = 0.90, $P_{Antändning}$ = 0.30. För varje händelse skall summan av alternativens sannolikheter vara lika med 1, dvs P_{Gasol} + $P_{Klorgas}$ = 1.00 Sannolikheterna för de olika delscenarierna beräknas då till.

P_1 = 0.20 x 0.90 x 0.30 = 0.054
P_2 = 0.20 x 0.90 x 0.70 = 0.126
P_3 = 0.20 x 0.10 = 0.02
P_4 = 0.80

Om sannolikheterna för samtliga delscenarier summeras skall summan alltid bli 1.00.

Felträdsanalys

Felträdsanalysen används för att identifiera de kombinationer av felhandlingar och felfunktioner som kan leda till någon viss skadehändelse. Denna s k topphändelse är utgångspunkten för analysen. Topphändelsens sannolikhet belyses genom att villkoren för att den skall utlösas av närmast underliggande händelse anges. Lösningen till felträdet består av en tabell med de kombinationer av händelser och tillstånd som fordras för att den aktuella topphändelsen skall inträffa.

Felträdsanalysens styrka som ett kvalitativt redskap är dess förmåga att åskådliggöra skadeförloppet genom att bryta ner det i sina beståndsdelar och förklara deras inbördes förhållanden. Denna och andra trädmetoder blir mycket svårtolkade samt tids- och kostnadskrävande för stora och komplicerade system. För att en omfattande felträdsanalys skall vara motiverad gäller det att de potentiella skadeverkningarna skall vara allvarliga samtidigt som sannolikheterna för skadorna är svåra att uppskatta.

En felträdsanalys är en riskanalys baserad på ett logiskt diagram. Det logiska diagrammet, felträdet, beskriver förutsättningarna för en avvikelse i en process. Själva avvikelsen är vanligen en allvarlig konsekvens eller slutkonsekvens, exempelvis ”reaktorn skenar”. Karakteristiskt är att avvikelsen utgör en topphändelse i felträdet.

Utlösande händelser som kan leda fram till avvikelsen utgör bashändelser i felträdet. En felträdsanalys kan omfatta tre delmoment:

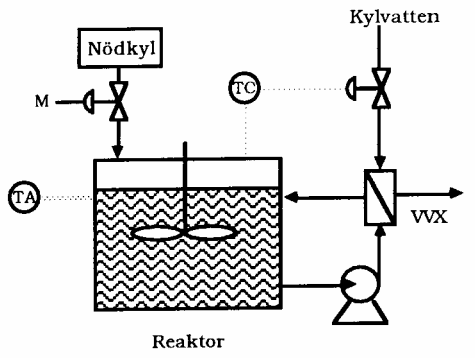
- Framtagning av logiskt diagram (felträd) för beskrivning av tänkbara skadeförlopp.
- Identifiering av sk ”Minimal Cut Sets” (MCS) som beskriver vilka kombinationer av bashändelser som leder till topphändelsen.
- Genomförandet av felfrekvens- och tillförlitlighetsberäkningar.

Felträd

Första delsteget vid konstruktion av ett felträd är att definiera topphändelsen, dvs en allvarlig slutkonsekvens som identifieras. Baserat på processflödesschemat listas vilka delsystem och apparater som är kritiska. Slutligen listas alla tänkbara utlösande händelser som kommer att utgöra bashändelser i felträdet. Bashändelserna berör oftast de nämnda kritiska delsystemen och apparaterna. Om felfrekvensberäkningar skall genomföras måste feldata fastställas för bashändelserna. Konstrueringen av felträdet genomförs enklast genom att starta med topphändelsen och arbeta sig nedåt mot bashändelserna.

Exempel

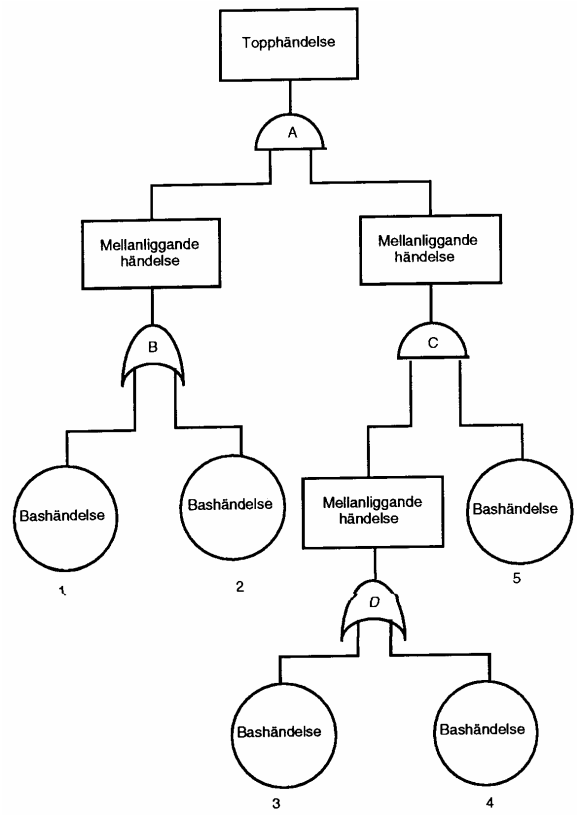
En process består av en satsvis arbetande reaktor i vilken en starkt exoterm reaktion genomförs (se Figur 13). Temperaturen regleras genom att recirkulera reaktionsblandningen med konstant hastighet genom en extern värmeväxlare. Kylvattenflödet styrs så att reaktortemperaturen hålls konstant. En manuellt reglerad nödkylning kan aktiveras om temperaturen blir för hög; larmet TA påkallar operatören. Konstruera ett felträd för topphändelsen att reaktorn skenar.



Figur 13 Process för en starkt exoterm reaktion

Lösning

Topphändelsen utgörs av slutkonsekvensen ”reaktorn skenar”. Genom erfarenhet har man konstaterat att följande system är kritiska: recirkulationspumpen, temperaturregleringen, nödkylningssystemet, temperaturlarmet och operatören. System som tanken och rörledningar anses vara säkra. Det kan också konstateras att system som temperaturregleringen kan brytas ned till delsystem såsom ventil, instrument, värmeväxlare etc.



Figur 14 Felträd för topphändelsen "reaktorn skenar"

Som bashändelser kan man nu lista: 1) pump havererar, 2) temperaturreglering havererar, 3) operatören reagerar ej på larmet, 4) temperaturlarmet fungerar ej samt 5) nödkylningen fungerar ej. Felträdet visas i Figur 14. Utgående från topphändelsen kartlägger man vilka händelser eller tillstånd som leder till denna direkt utan andra mellanhändelser eller villkor. Man kan då konstatera att tillstånden ”hög temperatur i reaktorn” och ”ingen nödkylning av reaktorn” måste föreligga samtidigt. Alltså leder dessa tillstånd till topphändelsen via en och-grind. Sedan går man vidare och konstruerar felträdet vidare mot bashändelserna. Tillståndet hög temperatur i reaktorn orsakas av ”pumphaveri” respektive ”haveri av temperaturreglering”'. Dessa händelser är bashändelser. Vidare gäller att det räcker om en av dessa inträffar för att reaktortemperaturen skall bli hög. Således en eller-grind. Nödkylningen sker ej om operatören inte aktiverar nödkylningen eller om nödkylningen inte fungerar osv, se Figur 14.

Minimal Cut Sets

Vi vet att utlösande händelser (bashändelser) *kan* leda till en slutkonsekvens (topphändelse). Frågan som då uppstår är: när inträffar topphändelsen? Först kan man konstatera att följande två regler gäller:

- Om en bashändelse inträffar så behöver detta inte leda till att topphändelsen inträffar.
- För att topphändelsen skall inträffa krävs ej nödvändigtvis att alla bashändelser inträffar.

I regel är det så att topphändelsen kan inträffa genom ett flertal olika kombinationer av bashändelser. Hur detta fungerar kan man utreda med en teknik där man tar fram

olika sk ”Cut Sets”. Behovet av en dylik teknik inses lätt då antalet kombinationer av bashändelser blir mycket stort redan vid ett mindre antal föreliggande bashändelser. Att leta på måfå är i regel lönlöst. Det finns ytterligare användningsområden för Cut Sets. Med dessa kan den mest sannolika kombinationen av bashändelser som leder fram till topphändelsen fastläggas, utan att man känner felfrekvensdata för processen.

Ett ”Cut Set” (CS) definieras som en kombination av bashändelser som leder till topphändelsen. Ett ”Minimal Cut Set” (MCS) definieras som ett minimalt antal bashändelser som leder till topphändelsen. Med minimalt antal avses att alla bashändelser som ingår i ett MCS erfordras för att topphändelsen skall inträffa. I ett CS kan det ingå flera bashändelser än det minimala antalet. Följande arbetsgång och regler måste tillämpas:

1. Märk alla grindar i felträdet med unika bokstäver; dessa bokstäver representerar egentligen en symbol för den utgående kopplingen.

2. Märk alla bashändelser med unika siffror. Om samma bashändelse figurerar på fler än ett ställe i felträdet så skall samma siffra förekomma på alla dessa ställen.

3. Härled med Bolsk algebra ett uttryck som beskriver topphändelsen som en funktion av bashändelserna. Uttrycket härleds genom successiv eliminering av alla bokstäver utom topphändelsens. Man startar från toppen. Räkneregler krävs för och- respektive eller-grindar. Antag att ingående n stycken kopplingar till en grind beteckna med $B_1 \ldots B_n$ och själva grinden betecknas med A. Då gäller för en och-grind att:

   $$A = B_1 \, x \, B_2 \, x \, \ldots \, x \, B_n \qquad \textit{Ekvation 16}$$

   och för en eller-grind att

   $$A = B_1 + B_2 + \ldots + B_n \qquad \textit{Ekvation 17}$$

   Utveckla uttrycket fullt ut. Det kan exempelvis se ut som följer:

   $$A = 1 \, x \, 5 + 1 \, x \, 3 \, x \, 4 + 3 \, x \, 4 \, x \, 7 + 3 \, x \, 4 + \ldots$$

4. Det utvecklade uttrycket representerar nu summan av ett antal CS. Dessa innehåller MCS samt eventuellt några överflödiga CS. Lista alla CS, exempelvis CS1 = 1,5; CS2 = 1,3,4; CS3 = 3,4,7; CS4 = 3,4;…

5. Vi är bara intresserade av MCS, så alla ”överflödiga” CS kan elimineras med följande två regler:

   - Om en siffra förekommer fler än en gång i ett CS, så stryk alla överflödiga Tex CS = 1,1,2,3,5,5 → MCS = 1,2,3,5
   - Stryk alla överordnade CS. Tex av de två CS 1,2,3 och 1,2 är endast ett MCS, nämligen 1,2

Exempel
Ta fram alla MCS för felträdet i föregående exempel.

Lösning
Alla grindar och bashändelser är utmärkta med bokstäver och siffror såsom visas i Figur 14. Vi börjar med att ställa upp sambanden för alla fyra grindarna:

$$A = B \times C$$
$$B = 1 + 2$$
$$C = D \times 5$$
$$D = 3 + 4$$

Därefter elimineras alla bokstäverna utom A successivt; C = (3 + 4) x 5; B = 1 + 2; A = B x C = (1 + 2) x ((3 + 4) x 5) = 1 x 3 x 5 + 1 x 4 x 5 + 2 x 3 x 5 + 2 x 4 x 5. Fyra CS erhålls och tillämpningsreglerna visar att inget av dessa kan elimineras eller reduceras. Således har vi fyra MCS: MCS1 = 1,3,5; MCS2 = 2,3,5; MCS3 = 1,4,5; MCS4 = 2,4,5

De MCS som erhålls vid en analys av ett felträd utgör de kombinationer av (minimalt antal) bashändelser som kan leda till topphändelsen. Om inga felfrekvensdata föreligger kan en god riskbedömning göras med två regler som man i första hand bör fokusera sig mot.

Bedömningen baserar sig på en rankning med hjälp av följande två regler:

1. Antal bashändelser: Ju färre antal ingående bashändelse i ett MCS, desto större sannolikhet att topphändelsen inträffar.
2. Typ av bashändelser. Sannolikheten för topphändelsen ökar enligt följande serie:

    - Mänskligt fel
    - Fel i aktiv komponent (pump, instrument, etc)
    - Fel i passiv komponent (tank, etc)

I praktiken föreligger alltid gränsfall och kombinering av de två reglerna kräver alltid erfarenhet. För flera ingående bashändelser är det inte uppenbart hur regel två skall tillämpas. Om man har två bashändelser så minskar sannolikheten enligt följande serie av felkombinationer: 1 mänskligt & mänskligt; 2 mänskligt & aktivt; 3 mänskligt & passivt; 4 aktivt & aktivt; 5 aktivt & passivt; 6 passivt & passivt.

Exempel
Tolka innebörden av de MCS som framtagits i föregående exempel genom att ta fram de sannolikaste kombinationerna av bashändelser som leder till toppändelsen.

Lösning
Alla MCS innehåller tre bashändelser. Första regeln rankar således alla MCS lika. MCS1 och MCS2 innehåller vars ett mänskligt felhandlande och vars två fel på aktiva komponenter. Dessa är således sannolikast enligt regel två. Övriga MCS innehåller tre fel på tre aktiva komponenter varför dessa två bedöms som lika sannolika, men mindre sannolika än de två första.

Felfrekvens och tillförlitlighet

Kvantitativa beräkningar av ett felträd går i regel ut på att beräkna felfrekvensen för topphändelsen och därefter sannolikheten för att topphändelsen inträffar under en viss driftperiod, säg anläggningens livslängd. För beräkningarna erfordras feldata för bashändelserna. Följande regel gäller i allmänhet:

- Feldata för kontinuerliga komponenter anges som felfrekvenser.
- Feldata för intermittenta komponenter som sannolikheter.

Om förutsättningarna för regeln inte föreligger måste antingen feldata omvandlas enligt beräkningssamband, eller också är felträdet felkonstruerat. Topphändelsens felfrekvens kan antingen beräknas genom successiv eliminering av feldata. Man börjar med bashändelserna och går mot toppen. En approximativ metod kan också utnyttjas baserat på alla MCS. Felfrekvensen för ett MCS är alltid lika med produkten av feldata för alla bashändelser som ingår i just det MCS. Felfrekvensen för topphändelsen blir då summan av felfrekvenserna för alla n stycken MCS:

$$z_A \approx \sum_{i=1}^{n} z_{MCS_i} \qquad \textit{Ekvation 18}$$

där z_{MCS_i} är felfrekvensen för MCS_i.

När väl felfrekvensen för topphändelsen är känd (z_A) kan systemets tillförlitlighet för en drifttid av t år beräknas med:

$$R_S = \exp\left[-\int_0^t z_A dt\right] \qquad \textit{Ekvation 19}$$

Sannolikheten att topphändelsen inträffar under tidsperioden blir:

$$Q_S = 1 - \exp\left[-\int_0^t z_A dt\right] \qquad \textit{Ekvation 20}$$

Exempel
Beräkna felfrekvensen för topphändelsen i föregående exempel.

Lösning
Vi börjar med bashändelserna och beräknar feldata för hög temperatur i reaktorn. Bashändelserna 1 och 2 är felfrekvenser eftersom det rör sig om kontinuerliga komponenter. Enligt räkneregel för eller-grind blir:

$$z_B = z_1 + z_2$$

Sannolikheten för att operatören inte aktiverar nödkylningen blir:

$$P_D = P_3 + P_4 - P_3 \times P_4$$

Sannolikheten för att nödkylningen av reaktorn uteblir kan sen skrivas:

$$P_C = P_D + P_5 - P_D \, x \, P_5 = P_3 + P_4 + P_5 - P_3 \, x \, P_4 - P_3 - P_5 - P_4 - P_5 + P_3 - P_4 - P_5$$

Om produkterna är små kan dessa försummas:

$$P_C \approx P_3 + P_4 + P_5$$

Felfrekvensen för topphändelsen blir:

$$z_A \approx (z_1 + z_2) \text{ x } (P_3 + P_4 + P_5)$$

Alternativt kan man basera beräkningarna på alla MCS. För MCS1 blir $z_{MCS1} = z_1 \text{ x } P_3$ osv. Summan av felfrekvenserna för alla MCS ger sen samma resultat som ovan.