SKI Rapport 99:35

Beskrivningar och modeller av säkerhetsfunktioner - en förstudie

Lars Harms-Ringdahl

Institutet för Riskhantering och Säkerhetsanalys AB
Bergsprängargränd 2, 116 35 Stockholm
(Internet: www.irisk.se)

September 1999

Denna rapport har gjorts på uppdrag av Statens kärnkraftinspektion, SKI.
Slutsatser och åsikter som framförs i rapporten är författarens egna
och behöver inte nödvändigtvis sammanfalla med SKIs.

SKI Rapport 99:35

Beskrivningar och modeller av säkerhetsfunktioner - en förstudie

Lars Harms-Ringdahl, Institutet för Riskhantering och Säkerhetsanalys AB

Innehållsförteckning

Sammanfattning **1**

1 Inledning **3**

2 Exempel från olika områden **5**

2.1 Om barriärer och djupförsvar 5

2.2 Nordiskt arbete med reaktorsäkerhet 8

2.3 Ett MTO-perspektiv 11

2.4 Från andra branscher 13

2.5 Standard om funktionell säkerhet 15

3 Summering av insamlat material **16**

3.1 Termer och principer 16

3.2 Metodik orienterad mot procedurer 18

3.3 Problem och behov 20

4 Struktur och modell **23**

4.1 Strukturering av säkerhetsfunktioner 23

4.2 Modell av säkerhetsfunktioner 26

5 Diskussion **29**

5.1 Frågeställningar och perspektiv 29

5.2 Om värdet av generaliserade säkerhetsfunktioner 30

5.3 Summering och slutsatser 33

6 Referenser **34**

Sammanfattning

Beskrivningar och modeller av säkerhetsfunktioner - en förstudie

SKI Rapport 99:35

Lars Harms-Ringdahl, Institutet för Riskhantering och Säkerhetsanalys AB, Bergsprängargränd 2, 116 35 Stockholm, Internet: www.irisk.se

En förstudie inriktad på frågor förknippade med säkerhetsfunktioner och barriärer har genomförts. En säkerhetsfunktion definieras här som en teknisk eller organisatorisk funktion med syfte att minska sannolikhet och/eller konsekvens förknippad med en riskkälla. I studien ingår en begränsad översikt av praxis och teorier relaterade till säkerhet inom kärnkraftsektorn och vid industriella tillämpningar. Genomgången grundar sig på litteraturstudier och intervjuer.

Begrepp med anknytning till "barriär" och "säkerhetsfunktion" från olika tillämpningar har sammanställts. Exempelvis har "barriär" dels en fysiskt/tekniskt baserad definition, dels en som inkluderar mänskliga, tekniska och organisatoriska element. Likaså har termen "säkerhetsfunktion" varierande innebörder.

Litteraturgenomgången har gett färre teoretiska och analytiska studier om barriärer och säkerhetsfunktioner än förväntat. Det gäller särskilt sådana funktioner som inkluderar kombinationer av tekniska, mänskliga och organisatoriska element.

I rapporten föreslås en strukturering och systematik för beskrivning av säkerhetsfunktioner. Dessa inkluderar ett antal karakteristika, såsom abstraktionsnivå, systemnivå, kategori, syfte, säkerhetsegenskaper och säkerhetsfunktionens delar. Ett förslag till en generaliserad modell av säkerhetsfunktioner har tagits fram som underlag för diskussion. Modellen utgår bland annat från att säkerhetsfunktioner indelas i ett antal "säkerhetsfunktionselement".

En slutsats är det finns en utvecklingspotential för teorier och metodik för hantering av säkerhetsarbete och procedurer. Säkerhetsfunktioner kan vara ett användbart begrepp i en sådan utveckling, och olika för- och nackdelar med detta diskuteras i rapporten. Om ett utvecklingsarbete ska bedrivas är det lämpligt att detta görs som en kombination av teori och fallstudier.

Abstract

Descriptions and models of safety functions - a prestudy

Beskrivningar och modeller av säkerhetsfunktioner - en förstudie
SKI Report 99:35

Lars Harms-Ringdahl, Institute for Risk Management and Safety Analysis, Bergsprängargränd 2, S- 116 35 Stockholm, Sweden, Internet: www.irisk.se

A study has been made with the focus on different theories and applications concerning “safety functions“ and "barriers". In this report, a safety function is defined as a technical or organisational function with the aim to reduce probability and/or consequences associated with a hazard.

The study contains a limited review of praxis and theories related to safety, with a focus on applications from nuclear and industrial safety. The study is based on a literature review and interviews. A summary has been made of definitions and terminology, which shows a large variation. E.g. "barrier" can have a precise physical and technical meaning, or it can include human, technical and organisational elements.

Only a few theoretical models describing safety functions have been found. One section of the report summarises problems related to safety issues and procedures. They concern errors in procedure design and user compliance.

A proposal for describing and structuring safety functions has been made. Dimensions in a description could be degree of abstraction, systems level, the different parts of the function, etc. A model for safety functions has been proposed, which includes the division of a safety function in a number connected "safety function elements".

One conclusion is that there is a potential for improving theories and tools for safety work and procedures. Safety function could be a useful concept in such a development, and advantages and disadvantages with this is discussed. If further work should be done, it is recommended that this is made as a combination of theoretical analysis and case studies.

1 Inledning

Några utgångspunkter
I system där en olycka kan få stora konsekvenser ställs höga krav på säkerheten. Det finns variationer mellan olika branscher, när det gäller utformning och bedömning av säkerhetssystem och säkerhetsarbete. Det är intressant att lära från olika tillämpningsområden, eftersom olika synsätt kan komplettera varandra och väcka intressanta frågeställningar.

En jämförelse gjordes för några år sedan av hur myndigheter ser på riskhanteringen inom sina områden (Harms-Ringdahl och Ohlsson, 1993). Jämförelsen visade att många frågeställningar var likartade, och att utveckling av metodik för säkerhetsfrågor pågick vid de flesta myndigheterna. Samtidigt var utbytet av erfarenheter över myndighetsgränserna tämligen svagt.

I denna studie har en utgångspunkt varit att studera begrepp, som *barriär, säkerhetsfunktion, skydd* etc., som används inom olika sektorer. Beroende på tillämpningen kan dock innebörden vara olika även om en och samma term används. Det kan gälla både betydelse och bakomliggande teorier, om det skulle finnas sådana.

Syfte
Syftet med denna förstudie var att undersöka fördelar och nackdelar med att utgå från principer för säkerhetsfunktioner utifrån ett generellt perspektiv. Mer preciserade mål var att:

a. Göra en strukturerad sammanställning av säkerhetsfunktioner, allmänt och med exempel av olika karaktär och från olika områden.
b. Utveckla en eller flera modeller för att beskriva karakteristika för säkerhetsfunktioner.
c. Bedöma användbarheten av ett generaliserat säkerhetsfunktionsbegrepp, och ange olika tillämpningar där det kan vara av värde att gå vidare.

Om terminologin
I studien används många termer, där innebörden kan skifta mellan olika tillämpningsområden. En stor del av litteraturen har varit på engelska, och en översättning av många facktermer har gjorts till svenska för att göra rapporten mer lättläst. Detta kan samtidigt innebära vissa betydelseförskjutningar, vilket läsaren bör vara uppmärksam på.

Ett grundbegrepp är säkerhetsfunktion (SF) vilket används med en bred betydelse. En provisorisk definition i rapporten är: *En säkerhetsfunktion är en teknisk eller organisatorisk funktion med syfte att minska sannolikhet och/eller konsekvens förknippad med en viss riskkälla.*

En annan term som har visat sig användas med varierande betydelse är *procedur*. För att undvika missförstånd vid läsningen, anges betydelsen av procedur redan här: *Sammanfattningen av en följd av handlingsmoment som tillsammans bildar en viss handling (särskilt av juridisk eller teknisk art), med särskild tanke på det vid handlingen osv. följda schemat eller tillämpade tillvägagångssättet.* Detta är en något nedkortad definition från Svenska akademins ordbok.

Arbetssätt

Denna förstudie har varit inriktad på att ge en övergripande beskrivning av området "säkerhetsfunktioner". I huvudsak har arbetet grundat sig på en litteraturgenomgång. Ett begränsat urval har gjorts, vilket i hög grad baserats på rekommendationer av kollegor. Exempel har främst hämtats från kärnkraftsområdet, kemiindustrin och automation av tekniska system. Vid litteraturgenomgången har intressanta aspekter varit principer och metodik för att uppnå säkerhet, och den terminologi som använts.

Några litteratursökningar har gjorts bl.a. i IAEAs (International Atomic Energy Agency) litteraturdatabas och på internet. Sökningarna gav ett tämligen litet tillskott till den redan identifierade litteraturen.

Intervjuer och diskussioner med inspektörer, forskare, och konsulter har varit en väsentlig del av studien. Dessa har haft en bra överblick av området, vilket i viss mån kompenserar begränsningarna i litteraturgenomgången.

Om rapporten

I kapitel 2 refereras de viktigaste delarna av litteraturgenomgången. Målgruppen för denna studie är bredare än bara personer inom kärnkraftsområdet. En del beskrivningar har därför inkluderats, trots att de kanske är självklara inom denna bransch. Kapitlet har disponerats utifrån det insamlade materialet.

Den läsare som vill hoppa över detta basmaterial kan gå direkt till kapitel 3, där det finns en summering av resultaten från datainsamlingen. Kapitel 4 ger förslag till strukturering och modeller för säkerhetsfunktioner. Diskussionskapitlet 5 behandlar några olika frågeställningar.

Denna förstudie har genomförts med stöd av medel från Statens kärnkraftinspektion. Rådet för arbetslivsforskning stödjer ett forskningsprojekt med inriktning på säkerhetsfunktioner inom arbetsmiljöområdet. Kompletterande resultat från detta projekt har inkluderats i denna rapport. Ett tack riktas till de personer som bidragit med synpunkter och information i studien. Det gäller bland annat Håkan Andersson (KSU), Anne Christianson Edland (SKI), Christer Karlsson (SKI), Carl Rollenhagen (SwedPower), Gerd Svensson (SKI), Ola Svenson (Stockholms universitet) och Björn Wahlström (VTT, Finland).

2 Exempel från olika områden

2.1 Om barriärer och djupförsvar

Detta avsnitt summerar övergripande terminologi och principer från kärnkrafts-området.

Några definitioner
Enligt Kärnenergiordlista (TNC, 1990):

- ***Barriär*** *är en naturlig eller konstruerad anordning som fördröjer eller förhindrar spridning av radioaktiva nuklider. En konstruerad barriär är en anordning som har tillverkats eller förändrats av människan.*

Enligt en föreskrift från SKI (1998):

- ***Barriär*** *är en fysisk inneslutning av radioaktiva ämnen.*
- ***Fysiskt skydd*** *är tekniska, administrativa och organisatoriska åtgärder som syftar till att skydda en anläggning mot sabotage etc* (nedkortad beskrivning)
- ***Säkert läge*** *är kall avställning eller annat driftläge som minimerar risken för en radiologisk olycka.*

Även INSAG (1988) anger barriärer som fysiska för att innesluta radioaktivitet. Enligt denna källa:

- ***Säkerhetsfunktion*** *är verkan av ett eller flera säkerhetssystem. Säkerhetssystem kan vara snabbstopp, reaktorisolering eller härdnödkylning.*
- ***Säkerhetssystem*** *är ett system avsett att vidmakthålla säkerheten vid onormala händelser i en kärnteknisk anläggning.*

Ordet säkerhetsfunktion används också i en bredare betydelse. Beard (1996) har granskat termen “safety function” inom kärnkraftsområdet. Beard fann inte något ställe där termen är formellt definierad, men den används i många olika sammanhang.

Säkerhetsprinciper
Som ett överordnat begrepp använder INSAG (1988) ordet ***säkerhetsprincip***. En sammanställning finns i Tabell 2.1 över tolv fundamentala säkerhetsprinciper, vilka har uppdelats i 3 huvudgrupper:
- riskhantering (3 st)
- djupförsvar (3 st)
- generella tekniska principer (6 st)

INSAG (1988) anger också ett antal "***specifika säkerhetsprinciper***". I en figur summerar man 50 principer i två dimensioner: "Livscykeldimensionen" och "Säkerhetsdimensionen".

Tabell 2.1 Sammanfattning av generella säkerhetsprinciper enligt INSAG (1988)

Huvudgrupp	**Säkerhetsprincip**
Riskhantering	Säkerhetskultur Ansvar hos driftorganisationen Myndighetsövervakning och oberoende granskning
Djupförsvar	Djupförsvar Olycksförebyggande Minskning av olyckas konsekvenser
Tekniska principer	Beprövad konstruktionspraxis Kvalitetssäkring Mänskliga och organisatoriska faktorer Säkerhetsgranskning och verifiering Strålskydd Driftserfarenhet och säkerhetsforskning

Djupförsvar

I en senare rapport har INSAG (1996) utvecklat beskrivningen av principerna för djupförsvar. Ett sådant innebär att det finns flera oberoende barriärer mot oönskade händelser och konsekvenser. Ett system ska klara fel i en eller flera barriärer utan att det direkt leder till en olycka.

Strategin med djupförsvar är att förebygga olycksfall och, om detta misslyckas, begränsa konsekvenser och förhindra att händelseförloppet utvecklas mot ännu allvarligare förhållanden. Man gör vanligen en indelning i **fem *olika nivåer för djupförsvar***. Skulle en nivå fela, ska underliggande nivå ta över. Nivåerna är:

Nivå 1 Förebyggande av driftstörningar och fel

Nivå 2 Kontroll över driftstörningar och detektering av fel

Nivå 3 Kontroll över förhållanden som kan uppkomma vid konstruktionsstyrande haverier

Nivå 4 Kontroll över och begränsning av förhållanden som kan uppkomma vid svåra haverier

Nivå 5 Lindrande av konsekvenser vid utsläpp av radioaktiva ämnen till omgivningen

Barriärer inom kärnkraftsanläggningar

För kärnkraftsreaktorer under drift består barriärerna vanligtvis av själva bränslet, bränslekapslingen, reaktorns tryckbärande primärsystem och av reaktorinneslutningen, enligt de allmänna råden till Statens kärnkraftinspektions föreskrifter om säkerhet i vissa kärntekniska anläggningar (SKI, 1998). En annan beskrivning[1] har lagt till en femte barriär, som är reaktorbyggnaden.

[1] Internet http://www.kvf.se/eltillv/kkraft.html

Brister i barriärer och djupförsvar

Många slag av brister och problem i barriärer och djupförsvar kan uppkomma. En indelning efter allvarlighetsgrad har gjorts i tre kategorier (SKI, 1998). Det åligger tillståndsinnehavaren att bedöma och klassificera en brist i en barriär eller i djupförsvaret i någon av de tre kategorierna.

- *Kategori 1*: *Konstaterad allvarlig brist i en eller flera barriärer eller i djupförsvaret samt grundad misstanke om att säkerheten är allvarligt hotad.* Innan anläggningen tas i normaldrift krävs godkännande av SKI. Beskrivning ges av förhållanden som tillhör kategorin.
- *Kategori 2*: *Konstaterad brist i en barriär eller i djupförsvaret av mindre allvarligt slag än det som hänförs till kategori 1 samt grundad misstanke om att säkerheten är hotad.* Anläggningen får fortsätta att vara i drift, dock med vissa begränsningar.
- *Kategori 3*: *Tillfällig brist i djupförsvaret som uppkommer då sådan händelse eller förhållande åtgärdas och som utan åtgärder skulle kunna leda till ett allvarligare tillstånd, och som är dokumenterad i de säkerhetstekniska driftförutsättningarna enligt 5 kap.1§.* Anläggningen får fortsätta att vara i drift, dock med vissa begränsningar.

2.2 Nordiskt arbete med reaktorsäkerhet

Bakgrund

Wahlström och Gunsell (1998) har gjort en övergripande beskrivning och värdering av arbete med reaktorsäkerhet framför allt inom Norden. Beskrivningar och synpunkter från den sammanställningen återges här, eftersom den verkar ge en bra överblick av tänkande och praxis inom kärnkraftssäkerhetsområdet.

Projektets mål var att övergripande analysera säkerhetsarbetet för att identifiera områden där det finns brister, samt att bedöma effektiviteten av säkerhetsarbetet. Några huvudfrågor var:

- Täcker säkerhetsarbetet alla väsentliga frågor som påverkar säkerheten?
- Används resurserna på ett balanserat sätt och är utvecklingen av säkerhetsarbetet rätt prioriterad?
- Är arbetet effektivt?

Termer, principer etc

Säkerhetsarbete

Med *säkerhetsarbete* menas alla de aktiviteter, både hos myndighet och kraftbolag, som dels avser att förhindra olyckor vid kärnkraftverk och dels lindra konsekvenserna om en olycka inträffar. Exempel på aktiviteter är:

- analys av inträffade händelser,
- konstruktionsanalys
- kvalitetskontroll
- periodiska test
- systematisk erfarenhetsåterföring
- säkerhetsanalys
- säkerhetsgranskningar
- urval och utbildning av personal
- återkommande inspektion osv.

Enkelfelskriteriet och redundans

En övergripande princip gäller enkelfelskriteriet. Den innebär att inget enskilt fel i utrustning eller enskilt handhavandefel får leda till otillåten situation (kan vara olycka, nedsättning av säkerhetsfunktion etc.) För att klara detta finns olika principiella lösningar:

- Redundans innebär att man bygger in övertalighet, t.ex. att en viss funktion dubbleras
- Förreglingar och automation kan ge skydd mot felmanövrering
- Separation innebär att säkerhetssystem ska vara funktionellt och fysiskt separerade
- Diversitet innebär att system ska vara oberoende också till sin principiella lösning, så att ett visst konstruktionsfel inte ska slå ut flera system samtidigt.

Enkelfels-, separations- och diversitetsprinciperna är nära relaterade till varandra. De två senare är "starkare" genom att de minskar möjligheterna att ett visst fel slår ut flera "oberoende" system samtidigt.

Barriärer
"I begreppet inbegrips dels ett hot och dels en åtgärd som bryter den kausala kopplingen mellan en händelse och ett utfall."

- En *fysisk barriär* byggs in i konstruktionen, t.ex. bränslets kapsling, tryckhållande komponenter och inneslutningen.
- En *teknisk barriär* kan åstadkommas genom att man initierar automatiska styråtgärder om ett hot realiseras, t.ex. att kyla härden vid haveri
- *Administrativa barriärer* kan utgående från olika hot byggas in i rutiner och procedurer, t.ex. genom säkerhetstekniska föreskrifter.

Wahlström och Gunsell (1998) talar också om *sekundära barriärer*. Ett sekundärt hot kan uppkomma om en bestämd barriär (primär) inte fungerar när den behövs. För att hantera detta bygger man då in en "sekundär barriär", t.ex. i de administrativa systemen.

Andra exempel på säkerhetskrav

- Marginaler: Säkerhetsmarginaler har att göra med t.ex. hållfasthet relativt belastning. Besläktade begrepp är konservatism i antaganden och robusthet.
- Rådrumsregeln: Vid ett tillbud ska personalen ha viss tid på sig (i Sverige och Finland 30 minuter), innan de måste vidta en åtgärd. Det som sker innan ska vara automatiserat.
- Låg sannolikhet: Probabilistiska säkerhetsmål ställs. Skyddssystemen förväntas vara så effektiva att frekvensen för en härdskada kan begränsas till högst en gång per 100 000 reaktorår. Högst en härdskada av tio ska få leda till utsläpp av radioaktivitet.

Modeller

Olika aspekter

Wahlström och Gunsell (1998) diskuterar olika modeller av säkerhetsarbete. Några intressanta aspekter som tas upp är:

- *Hierarki*: samhälle, kraftbolag (myndighet), avdelning, kontor, grupp och individ
- "Aggregationsdimensionen": helhet, system, delsystem och komponenter
- *Aktivitet* kan definieras som objekt med attributen: namn, mål eller funktion, plats i organisationen, input och output, resurser, styrning och effektivitetsmått.
- *Barriär* med attributen: hot, funktionskrav, metoder att verifiera barriärens funktion och funktionella krav.
- "*Abstraktionsdimensionen*": funktionellt ändamål, abstrakt funktion, generaliserad funktion, funktionell lösning och konstruktion.

En besläktad studie Strandell (1997) tar likaså upp modeller och begrepp. Syftet med den studien var att hitta en metod, med vilken man kan konstruera översiktliga modeller av säkerhetsarbetet på kärnkraftverk. Artikeln tar upp flera aspekter på modellering och representation av verkligheten.

Abstraktioner

Avsikten med abstraktioner är att isolera och framhäva de aspekter som är viktiga för ett visst ändamål, samt att ignorera de aspekter som är oväsentliga i sammanhanget. Det är viktigt att kunna beskriva ett system för processkontroll oberoende av hur motsvarande implementering på systemplanet är gjord. Man kan behöva använda sig

olika abstraktionsnivåer och Strandell (1997) återger (efter Jens Rasmussen) en abstraktionsmodell med fem nivåer:

1. Fysisk form (hur anläggningen på komponentnivå är konstruerad)
2. Fysisk funktion (de fysiska systemen)
3. Funktionell struktur (själva processen, ibland matematiska modeller)
4. Abstrakt funktion (mer abstrakt modellering av processen)
5. Funktionell betydelse (svarar på frågan varför)

Några slutsatser

Wahlström och Gunsell (1998) kommer fram till ett antal slutsatser i sin studie, och flera är väsentliga för denna rapport. Det gäller särskilt:

Praxis och modeller

IAEA har summerat god praxis, men reglerna tillämpas mycket olika i IAEAs medlemsländer. Programmen OSART, ASSET och ASCOT är i princip systematiska värderingar som görs mot en modell av god praxis. Modellen är dock underförstådd och formulerad i en frågelista.

Svårighet med värderingar och validering

Dessa metoder har aldrig blivit validerade i en strikt vetenskaplig mening, och ingen teoretisk modell har stått som grund för frågelistorna. Den främsta nyttan är att värderingarna har hjälpt till att få till stånd ett erfarenhetsutbyte mellan personer engagerade i det praktiska säkerhetsarbetet. Det är många kopplingar mellan aktiviteterna i säkerhetsarbetet, vilket gör det svårt att reda ut kausala samband och att ge klara rekommendationer.

Exempel på problem

- Informationshanteringen är ett reellt problem för hela branschen. Stora mängder ska hanteras, och det är svårt att för varje behov hitta relevant information.
- Det är speciellt svårt med analyser av händelser med mänskligt felhandlande och organisatoriska brister. MTO[2]-utredningar har visat sig svåra och kvaliteten i utredningarna har varierat. Fortsatt forskning för att förbättra metodiken är nödvändig, eftersom erfarenheterna dock är övervägande positiva.
- Krav på högre effektivitet innebär att man åstadkommer samma resultat med mindre resurser. Exempelvis pressar man en organisation genom att ge mindre resurser utan att ändra målen. I längden blir situationen ohållbar och man går mot ett syndrom: *systemen optimeras tills något går sönder* (Starbuck och Frances, 1988).

En jämförelse

Generellt sett är det små skillnader mellan Finland och Sverige. Den största skillnaden är kopplad till förhållandet att Sverige har haft en inhemsk leverantör, och Finland har haft utländska leverantörer. Det har lett till en större vilja i Finland att dokumentera kraven man ställt gentemot leverantörer.

[2] Förkortning för Människa, Teknik, Organisation

2.3 Ett MTO-perspektiv

En forskargrupp vid Stockholms universitet har gjort ett antal studier med utgångspunkt från "säkerhetsbarriärfunktioner" (safety barrier function) och ett MTO-perspektiv. MTO står som förkortning för Människa, Teknik och Organisation. Det finns flera rapporter som på ett kompletterande sätt beskriver dessa modeller. Rapporterna är på engelska, varför den engelska terminologin i viss utsträckning behållits.

Analys av olyckor (AEB-modellen)

Svenson (1991 och 1994) har beskrivit en modell för olyckor och de barriärer som skulle kunnat förhindra olyckan. Modellen kallas "Accident Evolution and Barrier function" (AEB), och den ska ge en grafisk representation av ett olycksförlopp. En analys av en inträffad incident föreslås göras i sju steg. Syftet med en AEB-analys är att identifiera felande eller icke existerande barriärfunktioner i ett olycksförlopp, samt att vara ett stöd för att finna kompletterande barriärer.

Modellen innehåller tre huvudkomponenter:

a Fel av olika slag. Dessa kan vara förknippade med tekniska system respektive med organisation eller mänskliga handlingar
b Kedjan av fel i utvecklingen mot en olycka
c Barriärfunktion

Analys av barriärfunktioner

En metod för analys av aktiviteter, innan ett olycksfall inträffat, har beskrivits (Jacobsson Kecklund m.fl. 1994, och av Kecklund m.fl. 1995). En av utgångspunkterna är barriärfunktioner, och metoden kallas "Safety barrier function analysis". Metoden har exemplifierats genom analys av bränslebyte vid en kärnkraftreaktor. Metoden består av tre huvudsteg, som är modellering, klassificering och bedömning.

Modellering

Det första steget innebar att man gjorde en modell av händelser och barriärfunktioner (Event and Barrier Function Model, EBFM) i sekvensen för bränslebyte. I en modell ingår:

a Aktiviteter, som är åtgärder av människa eller maskin
b Fel av olika slag, som är kopplade till respektive aktivitet
c Barriärfunktioner

Klassificering

Barriärfunktionerna "verkställs" av barriärsystem (barrier function systems). I en klassificering delades barriärerna in i fyra huvudgrupper:

1 Mänsklig/organisatorisk barriärfunktion (planering, administrativa kontroller etc)
2 Teknisk barriärfunktion
3 Mänsklig barriärfunktion (som exempelvis utförs av en operatör)
4 Mänskliga och tekniska barriärfunktioner (baseras på både människor och tekniska barriärsystem)

Bedömning
Bedömningen görs därefter i form av en klassificering. Operatörer vid anläggningen skattar hur säker eller osäker varje barriär är. Operatörerna anger ett värde mellan 1 (mycket osäker) och 10 (mycket säker).

Exempel
Vid en av analyserna (studie 1) erhölls 9 aktiviter, samt 17 fel och lika många barriärfunktioner. Det vill säga att för varje felmöjlighet angavs en tillhörande barriärfunktion.

Kommentarer
AEB-perspektivet innebär att förklaringar som "grundorsaken" till en viss olycka inte blir meningsfull. Detta har inte minst en pedagogisk betydelse, eftersom det ibland kan vara svårt att få förståelse för att en olycka har många bidragande förklaringar.

Barriär-begreppet ges här ett bredare innehåll och inkluderar fysiska, tekniska, mänskliga och organisatoriska delar. Detta synsätt finns också på många andra håll (exempelvis Rollenhagen, 1995). Enligt Rollenhagen (personlig kommunikation) bör man ha en begränsad betydelse av begreppet barriär - att den fångar upp avvikelser eller lindrar konsekvenser vid en olycka. Ordet stödfunktion bör användas för funktioner som förebygger att avvikelser uppkommer.

2.4 Från andra branscher

Inledning

Principer och praxis för hur man hanterar risker och ska uppnå säkerhet varierar starkt mellan och inom branscher. För att illustrera olika varianter på principer tar detta avsnitt upp tre exempel; energiprincipen, arbetsmiljö- och kemiområdet.

Barriärer enligt "energitänkandet"

En tidig användning av begreppet barriär utgår från fysiska beskrivningar och från energier. Barriär är något som skyddar människor eller andra objekt från ett oönskat energiflöde. Man kan göra en uppdelning i barriärer som skyddar mot oönskat energiflöde "säkerhetsbarriärer", respektive i sådana som ska skydda mot skador från önskade energiflöden "kontrollbarriärer". En barriär kan vara fysisk, men även utgöras av procedurer, utbildning och träning etc. Detta har utvecklats utförligt i beskrivningar av metoden MORT (Johnson, 1980, Knox och Eicher, 1983).

Utifrån ett energitänkande finns det mer eller mindre uppenbara åtgärdsstrategier. Ett exempel finns i Tabell 2.3 (efter Harms-Ringdahl, 1987).

Tabell 2.3 Åtgärdsstrategier enligt energimodellen (efter Harms-Ringdahl, 1987)

KONTROLL AV ENERGI	BARRIÄRER	MÄNNISKAN
Eliminera energin	Skilj människan från energiflödet	Skydd på människan
Begränsa mängden	a) I rum	Minska konsekvenserna - om olycksfall inträffat
Säkrare alternativ lösning	b) I tid	
Förhindra att extrem energi byggs upp	Skydd på energikällan	
Förhindra att energin frigörs		
Kontrollerad reduktion av energin		

Från arbetsmiljöområdet

EU har gett ut ett direktiv om åtgärder för att främja förbättringar av arbetstagarnas säkerhet och hälsa i arbetet (EEG, 1989). Arbetsplatsdirektivet innehåller minimikrav och ska tillämpas på nästan alla typer av verksamhet. Där finns också en lista för prioriteringar av åtgärder.

De vanliga generella principerna finns med. Det gäller exempelvis, att arbetsgivaren är skyldig att svara för att arbetstagarens säkerhet och hälsa tryggas i alla avseenden som är förbundna med arbetet. Arbetsgivaren ska vidta tillräckliga åtgärder ..... samt iordningställande av erforderlig organisation och nödvändiga resurser.

Direktivet anger ett antal *principer för förebyggande* arbete:

a) Undvika risker
b) Utvärdera risker, som inte kan undvikas
c) Bekämpa riskerna vid källan
d) Anpassa arbetet till den enskilde ..... med avsikt att framför allt reducera monotont arbete .....
e) Ta hänsyn till den tekniska utvecklingen

f) Ersätta ämnen med ämnen som inte är farliga eller mindre farliga.
g) Prioritera gemensamma skyddsåtgärder framför individinriktade skyddsåtgärder.

Arbetsgivaren ska utvärdera riskerna för arbetstagarnas säkerhet och hälsa, bland annat vid val av arbetsutrustning, de kemiska ämnen och preparat som används samt arbetsplatsernas utformning. Som en följd av denna utvärdering ska vid behov förebyggande åtgärder garantera en förbättring av skyddsnivån.

Från kemibranschen
En generell bild av säkerhetsprinciper i kemibranschen har beskrivits av den amerikanska branschorganisationen (CCPS, 1993). Denna ger riktlinjer för dels generella säkerhetsaspekter, dels sådana förknippade med kontrollsystemen för process- och säkerhetsfunktionerna.

Ett grundläggande begrepp är skyddsbarriär (Protection layer), vilket emellertid inte direkt definieras. Det exemplifieras med 8 nivåer. Dessa är ordnade efter hur de aktiveras vid en eskalerande olycka.
1. Processutformning
2. Grundläggande kontroll, processlarm, och operatörens övervakning
3. Kritiska larm, operatörens övervakning och manuella ingripanden
4. Automatiskt säkerhetsinriktat förreglingssystem
5. Fysiskt skydd (säkerhetsventiler)
6. Fysiskt skydd (inneslutning)
7. Anläggningens hantering av nödsituation
8. Samhällets hantering av nödsituation

Automatiska styrsystem och kontrollsystem är väsentliga för säkerheten, och CCPS skiljer på *processkontrollsystemet* och *säkerhetssystemet*. För den senare finns en lista som beskriver en designfilosofi utifrån tio punkter:
1. Säkerhetssystemet separeras från processkontrollsystemet.
2. Delar och delsystem ska ha visad tillförlitlighet, i samma tillämpning som den aktuella.
3. Utformningen ska göras felsäker.
4. Systemet ska ha inbyggd feldiagnostik, och det ska finnas stöd för åtgärder vid felsituationer.
5. En övergripande brytare oberoende av programmerbar logik ska finnas. Vid krav på sekventiell nedkoppling krävs andra åtgärder.
6. Förbikoppling av givare etc får bara göras med beaktande av särskilda regler.
7. Signaler från andra delar av processkontrollsystemet får inte kunna försvaga säkerhetsfunktionerna.
8. Obevakade terminaler ska inte kunna ändra inställningen av kontrollfunktionerna i säkerhetssystemet.
9. Grundinställningarna för säkerhetssystemet (master records of safety system) ska lagras säkert. Det ska gå att enkelt jämföra grundinställningarna med aktuella arbetsinställningarna.
10. Upprätthålla systemets integritet genom företagsledningens uthålliga engagemang. Innebär periodisk test, olika rutiner etc.

2.5 Standard om funktionell säkerhet

En generell standard
Det finns en stor mängd internationella standarder som är relaterade till säkerhet. Ett generellt förslag (IEC, 1997) till standard har titeln "*Functional safety: safety related systems*" (IEC nummer 1508). Inriktningen är säkerhet i tekniska system förknippade med elektriska styrsystem.

Standarden är tänkt att täcka alla säkerhetsrelaterade system oberoende av tillämpningen, och några angivna exempel är process- och tillverkningsindustri, transporter och medicinsk utrustning. Standarden är i huvudsak inriktad på personsäkerhet.

Att standarden har en hög ambitionsnivå framgår av en illustration med titeln "Världens säkerhetsparaply", och under paraplyet ryms:
- Specifikationsfel
- Konstruktions- och tillverkningsfel
- Installationsfel
- Fel vid drift och underhåll
- Fel vid ändringar

Om terminologin
Flera specialtermer ingår i standarden, varav några av de viktigaste återges nedan:
- ***Utrustning under kontroll*** (UUK) är den anordning för vilken man vill ha tillräckligt hög säkerhet.
- ***Funktionell säkerhet*** är förmågan hos ett säkerhetsrelaterat system att genomföra de nödvändiga åtgärderna för att uppnå eller bibehålla ett säkert tillstånd hos UUK.
- ***Säkerhetsintegritet*** (safety integrity) är sannolikheten att ett säkerhetsrelaterat system genomför erforderliga säkerhetsfunktioner under alla angivna omständigheter inom en given tidsperiod. Fyra nivåer definieras, vilka grundas på sannolikhetsmått.

Ett ***säkerhetsrelaterat system***:
- fullgör den önskade säkerhetsfunktionen för att uppnå eller bibehålla ett säkert tillstånd hos UUK,
- är avsett att uppnå, själv eller ihop med andra säkerhetsrelaterade system, nödvändig nivå på säkerhetsintegriteten. (En person kan vara del av ett säkerhetsrelaterat system.)

En term som inte definierades var "*säkerhetsfunktion*" även om den användes mycket. Ordet "*barriär*" verkade inte användas överhuvud taget.

3 Summering av insamlat material

3.1 Termer och principer

Inledning

Detta avsnitt summerar termer och principer med inriktning på att erhålla säkerhet i existerande system. Innehållet är inriktat på egenskaper i ett färdigt och fungerande tekniskt system, där det finns människor och olika slag av organisatoriska rutiner.

Termer och principer

Det finns ett stort antal termer som används, ibland med varierande betydelse. Tabell 3.1 innehåller begrepp relaterade till säkerhetsfunktioner. Det finns en kärnkraftsspecifik definition med en teknisk inriktning. Det finns också ett bredare användningsområde, som inkluderar fysiska, tekniska, mänskliga och organisatoriska funktioner.

Tabell 3.1 Definitioner av säkerhetsfunktion

Term / Princip	Definition eller förklaring	Referens
Säkerhetsfunktion i kärnkraftverk	Verkan av ett eller flera säkerhetssystem. Säkerhetssystem kan vara snabbstopp, reaktorisolering eller härdnödkylning.	INSAG, 1988
Säkerhetsfunktion, allmänt	För att kontrollera processen och bibehålla den i säkert tillstånd, innesluta och minska konsekvenser vid olycka.	Från Beard, 1996
	Används ofta utan definition	Bl.a. Beard, 1996
	Teknisk eller organisatorisk funktion med syfte att minska sannolikhet och/eller konsekvens förknippad med en viss risk.	Denna rapport, kapitel 1
Säkerhetsbarriär-funktion	En funktion som kan stoppa utvecklingen mot en olycka, genom att nästa steg i olyckskedjan ej inträffar.	Svenson, 1991
	Teknisk, organisatorisk eller mänsklig aktivitet placerad i en olyckssekvens för att skydda systemet mot fel.	Jacobsson Kecklund m.fl. 1994

Tabell 3.2 anger ett antal begrepp relaterade till barriärer. Barriär har genomgående en inriktning mot anordningar och åtgärder. Det finns dels några definitioner enbart inriktade mot tekniska anordningar, dels några mot tekniska, mänskliga och organisatoriska system.

En sammanställning av mer generella eller systemorienterade begrepp finns i Tabell 3.3. Där finns också två alternativa förslag till definitioner av riskhantering. Den första utgår från ett hierarkiskt tänkande där utgångspunkten är att genomföra företagets policy. Den andra är mer generell, och den implicerar bland annat att det finns en riskhantering även om det inte finns en säkerhetspolicy.

Tabell 3.2 Definitioner av barriärer etc.

Term / Princip	Definition eller förklaring	Referens
Barriär i kärnkraftverk	En naturlig eller konstruerad anordning som fördröjer eller förhindrar spridning av radioaktiva nuklider.	TNC, 1990 (Kärnenergi-ordlista)
	En fysisk inneslutning av radioaktiva ämnen.	SKI, 1998, & INSAG, 1988
Barriär, allmänt	En åtgärd som bryter den kausala kopplingen mellan en händelse och ett farligt utfall. En barriär kan vara fysisk, teknisk eller administrativ.	Wahlström & Gunsell, 1998
	Användning utan definition är vanligt.	-
Sekundär barriär	Ett sekundärt hot kan uppkomma om en bestämd barriär (primär) inte fungerar när den behövs. För att hantera detta bygger man då in en "sekundär barriär", t.ex. i de administrativa systemen.	Wahlström & Gunsell, 1998
Barriärsystem	Fysiskt, tekniskt, eller organisatoriskt system som realiserar barriärfunktionen.	Svenson, 1991
Skyddsbarriär (kemiindustri)	Definieras genom exempel, såsom processutformning, processlarm etc.	CCPS, 1993

Tabell 3.3 Definitioner av generella eller överordnade begrepp

Term / Princip	Definition eller förklaring	Referens
Djupförsvar	Flera oberoende barriärer mot oönskade händelser och konsekvenser. (T.ex. fem olika nivåer)	INSAG, 1996
System av skyddsbarriär	Kombination av skyddsbarriärer (kemiindustri)	CCPS, 1993
Säkerhetssystem	System avsett att vidmakthålla säkerheten vid onormala händelser i en kärnteknisk anläggning.	INSAG, 1988
Säkerhetsarbete	Aktiviteter, både hos myndighet och kraftbolag, som ska förhindra olyckor vid kärnkraftverk och lindra konsekvenserna om en olycka inträffar.	Wahlström & Gunsell, 1998
Riskhantering, formell	Systematisk tillämpning av ledningspolicy och procedurer för att analysera, bedöma och reducera risker.	SEK, 1998
Riskhantering, allmän	Organisatoriska aktiviteter och rutiner som är avsedda att hantera de risker och möjliga skador som företaget kan vålla eller drabbas av.	Harms-Ringdahl, 1995 (förslag)

Kommentarer

Tabellerna ger en sammanställning av säkerhetsfunktioner och anknytande begrepp från olika områden, vilket är ett delmålen för denna studie. Säkerhetsfunktion har definierats inom det kärntekniska området, men någon generell publicerad definition har inte framkommit. Däremot finns det flera olika begrepp med anknytning till barriärer, säkerhetssystem etc.

3.2 Metodik orienterad mot procedurer

Inledning
Föregående avsnitt summerade termer och principer med inriktning på existerande tekniska anläggningar. De flesta har ett fokus på hur det tekniska systemet ska fungera säkert. Både från litteraturgenomgången och intervjuer framstod organisatoriska förhållanden och procedurer som ett minst lika viktigt område. Detta avsnitt fokuserar därför på säkerhetsfunktioner och metodik med anknytning till detta område. I Avsnitt 3.3 återkommer detta tema, men då i ett mer probleminriktat sammanhang.

Procedur används med betydelsen: *Sammanfattningen av en följd av handlingsmoment som tillsammans bildar en viss handling med särskild tanke på det vid handlingen följda schemat eller tillämpade tillvägagångssättet.* (Nedkortad definition från Svenska akademins ordbok.) En procedur kan vara noggrant strukturerad och vara avsedd att följa en skriven instruktion mycket strikt. En annan procedur kan vara relativt ostruktuerad, och exempelvis vara inriktad på att uppnå ett visst resultat eller att lösa ett problem vid felsökning.

Procedurer är väsentliga för det praktiska genomförandet av säkerhetsfunktioner. En viktig del av säkerhetsarbetet är hur man ska "konstruera" respektive "granska" procedurer. Det gäller särskilt hur man säkerställer att procedurerna fungerar även vid ovana eller störda förhållanden. En frågeställning är, om det finns lämplig metodik till stöd för de personer som ska utforma procedurer för underhåll, ändringar, nödsituationer etc.

Organisationer och utveckling av procedurer
Det finns en mängd råd och en omfattande litteratur, om hur man ska bygga upp organisationer för att få god säkerhet. En del av dessa kan vara bra, medan annat kanske fungerar sämre för en specifik situationen eller organisation. Oftast bygger modellerna på hierarkiska system, vilket ofta innebär att man ska börja med policy och företagsledningens engagemang. Välkända exempel är beskrivningar av "säkerhetskultur" och "kvalitetssystem".

Vid de flesta intervjuerna har en fråga gällt om man känner till någon existerande metodik för att stödja utveckling av procedurer och instruktioner. De konkreta handledningar som nämndes gällde handfasta råd, vilket kunde vara utformning av text eller hur skärmbilder ska utformas. I några fall trodde man att det fanns metodik etc. hos kraftbolagen. Vid dessa finns ett omfattande material, som används i den praktiska verksamheten och inte är offentligt. Utformning och analys av instruktioner är ett specialistarbete, och det sköts ofta av drift- och utbildningssektioner.

Det kan således finnas material som behandlar detta på ett bra sätt, men som inte identifierats i denna begränsade teoretiskt orienterade studie. Å andra sidan, även om det skulle finnas bra material, verkar det inte ha kommit till mer generell användning i Sverige.

Kvalitetssystem
Kvalitetssystem har en hög status inom många områden, från administration, sjukvård, industri, transporter osv. Genom kvalitetssystem förväntar man sig att få bättre och mer väldokumenterade arbetssätt och procedurer. Kvalitetssäkring (quality assurance) är en av de tolv fundamentala säkerhetsprinciperna. (INSAG, 1988).

För kärnkraftsområdet har IAEA (1996) publicerat normer och riktlinjer för kvalitetssystem. Det var därför intressant att studera vilka råd som ges för hur "procedurer" ska utformas. I sektionen "*Arbetsinstruktioner*" (IAEA, 1996, sid. 45) beskrivs instruktioner för "personer som arbetar".

Det är där en fokusering på själva dokumentet, dvs. instruktionen. Under syfte anges dokumentets syfte, inte själva uppdragets. Det finns flera rubriker som är viktiga för säkerheten, mest direkt gäller det "Precautions". Det saknades dock många säkerhetsmässiga aspekter på arbetsuppgiftens genomförande. Det är därmed inte självklart att kvalitetssystem i sig själva, säkerställer att utformningen av procedurer blir bra ur ett säkerhetsperspektiv.

Metodik för utformning av procedurer
I en artikel av Marsden (1996) återfinns en metodik för utformning av procedurer, vilken är den enda som identifierats i den här studien. Marsden föreslår en formell arbetsgång för att utveckla procedurer i ett antal steg:
- Analys av uppgiften
- Gör preliminär procedurbeskrivning
- Kvalitetsgranska
- Godkänn proceduren
- Granska och följ upp effektiviteten

Analysen innebär att man gör ett flödesdiagram över proceduren. Man konstruerar sedan en "felanalysmatris", med kolumnerna: - Arbetsmoment -Felmöjlighet - Systemkonsekvener -Korrektion av fel etc.

Marsden räknar "*korrektion av fel*" som en barriär. Metodbeskrivningen är kort och det är svårbedömt hur väl den kan fungera. Metoden verkar inriktad på mänskliga fel, och mycket av texten är illustrationer av vilka fel som kan göras. Marsden verkar tänka sig procedurer på ganska låg nivå. Erfarenheterna verkar intressanta.

Metoder för granskning av organisatoriska aktiviteter
Det finns åtskilliga metoder som är avsedda att granska organisationer och rutiner. En del kan användas också som en del i en olycksutredning. En översikt från industriella tillämpningar finns i en rapport av Harms-Ringdahl (1996). Exempel på metoder som kan vara relevanta är MORT (Johnson, 1980), SMORT (Kjellén och Tinmannsvik, 1989) och CRIOP (Ingstad och Bodsberg, 1990).

En bred litteraturöversikt (Hale m.fl., 1997) har tagit upp hur system för riskhantering (safety management system) kan granskas och teoretiskt beskrivas. Författarna föreslår också en generell modell för beskrivning av sådana system, vilken kan tillämpas på olika systemnivåer.
Från kärnkraftsområdet finns det flera metoder. Exempel är OSART, ASSET och ASCOT. Programmen är i princip en systematisk värdering som görs mot en modell

av god praxis. Modellen är dock underförstådd, och metodiken har inte validerats i en strikt vetenskaplig mening (Wahlström och Gunsell, 1998).

En fransk studie (Abramovici och Bourrier, 1998) har tagit upp fyra metoder inriktade på organisationens betydelse för användning i probabilistiska riskanalyser. Författarna har sökt efter bakomliggande modeller till metoderna och hur man förklarar organisationens inflytande. De menar att några sådana modeller inte verkar använts, utan de efterlyser en "översiktlig teori om organisatorisk tillförlitlighet, som kan belysa såväl organisatoriska fel som framgångar". Metoderna är:

SHERPA	Systematic Human Reduction and Prediction Approach (Embrey, 1986)
IMAS	Influence Modelling and Assessment Systems (Embrey, 1992)
SAM	Systems, Actions and Management (Pate-Cornell et al, 1996)
WPAM	Work Process Analysis Model (Dvoudian et al, 1994)

Kommentarer
Jämfört med tekniskt inriktade modeller och principer, verkar det finnas svårigheter med att finna en vetenskapligt verifierad metodik för att bedöma säkerhetsegenskaper hos procedurer. Dessutom verkar det saknas praktiskt och säkerhetsmässigt orienterad systematik för hur procedurer ska utformas.

3.3 Problem och behov

Inledning
Detta avsnitt är en summering av problem och behov baserad på litteraturgenomgången, och intervjuer. Denna summering kan ses som argument för förbättrat säkerhetsarbete och vara en del i underlaget vid värdering och utformning av modeller för säkerhetsfunktioner. I de flesta exemplen rör det sig om synpunkter från enstaka källor, och man bör se summeringen nedan som ett diskussionsunderlag.

De flesta problem som kommit upp har varit relaterade till procedurer av olika slag. I avsnitt 3.2 återges resultat från litteraturgenomgången om metodik förknippad med procedurer. Beskrivningen nedan är mer problemorienterad. Andra problemområden som tagits upp har varit förknippade med ändringar av yttre förhållanden och med datorstyrning.

Studie om fel vid procedurer
En artikel om procedurer (Marsden, 1996) återger en granskning av 700 incidenter vid kärnkraftsanläggningar. Enligt denna studie var fel med procedurer inblandade i mer än 69% av fallen. En liknande granskning av 180 fall i USA 1985 gav 65% relaterat till procedurer.

Marsden anger utformningen av procedurer som ett väsentligt problem. Han summerar detta: *"Procedurer utformade av tekniskt kvalificerade personer, som arbe-tar för sig själva, befinns ofta vara ofullständiga, felaktiga eller allmänt orealis-tiska. Kritisk information kan döljas i dokumentation som är olämpligt utformad"*.

Problem med procedurer

Problem med procedurer kan vara av många slag, och nedan ges några exempel:

Genomförande

- Fel och misstag uppkommer, när en operatör eller ett arbetslag försöker följa en procedur (Detta är mycket utförligt behandlat i litteraturen, och det finns stor metodarsenal.)
- Procedurer avbryts (trots att de kanske från början antagits skulle göras i en följd).
- Instruktionen (procedurbeskrivningen) ses som en formalitet, och genomförandet följer exempelvis i stället tidigare praxis (som kan vara mer eller mindre bra).
- Det är svårt att alltid verifiera att en procedur genomförts korrekt.

Beskrivning av procedur och utformning av instruktion

- Felaktigt "konstruerad" procedur.
- Instruktionen ofullständig, väsentliga element saknas.
- En instruktion går inte att följa, t.ex. om det finns en tidsgräns inom vilken proceduren ska vara klar, samtidigt som alltför många steg ska genomföras.
- Kompetensen otillräcklig när instruktionen skrivs, t.ex. saknas kunskap om tekniska förutsättningar. ("Beskrivningar behöver skrivas av sunda ingenjörer.")
- Vissa antaganden om systemtillstånd, personal etc. har gjorts, utan att detta klart framgår av instruktionen.
- Svårt att verifiera att en procedur konstruerats korrekt.
- Systemorienterat stödmaterial för att hjälpa dem som konstruerar procedurer och tar fram instruktioner verkar inte användas i större utsträckning. Ej heller har något sådant material identifierats med ett undantag (Marsden, 1996, referats i avsnitt 3.2).

I många fall hör problemen både till genomförandet och utformningen, exempelvis:

- Åtskilliga tillbud har förekommit när säkerhetsprocedurer ej fungerat
- Interaktionen med andra procedurer kan innebära störningar
- Procedurer har vuxit fram - i en del fall stämmer inte instruktioner och dokumentationen med hur aktiviteterna genomförs i verkligheten.

Problem med automation

Automatiska styrsystem och datorisering är ett tekniskt område med många exempel på att problem inträffat. Någon genomgång av dessa görs inte här. Det finns utförliga normer och standarder (se avsnitten 2.4 och 2.5), men dessa kommer knappast att lösa alla problem.

Problem med ändringar

Inom näringslivet sker kontinuerligt förändringar av teknik och organisation för att öka effektivitet och lönsamhet. Högre effektivitet innebär att man åstadkommer samma resultat med mindre resurser. Det kan vara att man försöker pressa en organisation genom att ge mindre resurser utan att ändra målen. I längden blir situationen ohållbar och man går mot ett syndrom, där man optimerar systemen tills något går sönder (Starbuck och Frances, 1988).

I många sammanhang har det tagits upp farhågor om att ändringar kan öka riskerna för olyckor (t.ex. Hovden, 1998). Några exempel från kärnkraftssektorn som tagits upp vid intervjuer är:

- Generationsskiften av teknik, särskilt styrsystem där datorbaserade system tar över.
- Generationsskifte av människor

En av flera bidragande förklaringar till att riskerna kan öka, är att "informella" säkerhetshöjande åtgärder försvinner. Det kan vara att operatörerna känner till viktiga problem, och att de korrigerar mer eller mindre medvetet för dessa. Samtidigt som problemen inte beaktas i instruktionerna. Denna "tysta kunskap" kan försvinna, exempelvis vid nyanställning eller inhyrd personal, och leda till problem av många slag. Vid datorisering av procedurer kan liknande bortfall av "tyst kunskap" uppkomma.

Ett annat exempel som tagits upp är förändringar av ägarbilden och ett mer ekonomistiskt tänkande. En farhåga har varit att detta kommer att medför en försämrad samförståndsanda mellan kärnkraftsindustri och tillsynsmyndighet. En bedömning är att detta kan leda till behov av en striktare hantering av säkerhetsfrågor, från båda sidor.

Behov

Diskussioner och litteraturgenomgången har indikerat ett antal problem inom området procedurer och säkerhetsarbete. Dessa skulle istället kunna omformuleras som behov. Det har också framkommit direkt formulerade behov. En summering av behov anges nedan. Denna är argument för ett behov av ytterligare utvecklingsarbete, vilket anknyter till diskussionen i Kapitel 5.

Allmänna krav

- Krav på högre effektivitet i kärnkraftverkens administration innebär, att man måste åstadkomma samma resultat med mindre resurser.
- Denna typ av ökande krav finns även inom arbetslivet generellt.

Procedurer och instruktioner

För granskning och utformning av procedurer har åtskilliga punkter nämnts vid intervjuerna, och några exempel på behov är:

- Teorier och modeller för hantering av "procedurer".
- Riktlinjer och bra verktyg för hur man tar fram bra procedurer för:

- mål och specifikationer
- design
- praktisk utformning
- verifiering.

- Systematiskt sätt att inkludera "tyst kunskap" i procedurer, så att inte nya risker introduceras vid ändringar.
- Mer systematiskt sätt att tillvarata observerade fel i procedurer. T.ex. när man vid en granskning upptäcker något som borde upptäckts i en tidigare granskningsinstans, är detta en viktig iakttagelse.

4 Struktur och modell

4.1 Strukturering av säkerhetsfunktioner

Inledning
Detta och efterföljande avsnitt tar upp idéer om strukturering och generell modellering. Det är ännu inte en färdig modell, utan syftet är att den ska utgöra ett underlag för fortsatta diskussioner. Förslaget inkluderar en strukturering av olika begrepp och en indelning i olika nivåer. Indelningarna kan möjligen förefalla självklara, men det är väsentligt att en terminologi förstås lika av alla berörda.

Tänkandet bakom modellen innebär att säkerhet och säkerhetsfunktioner ställs i centrum. Begreppet säkerhetsfunktion (SF) får här ha en bred betydelse. Definitionen är: *En säkerhetsfunktion är en teknisk eller organisatorisk funktion med syfte att minska sannolikhet och/eller konsekvens förknippad med en viss riskkälla.*

Uppdelningen har gjorts i några olika dimensioner:
1. Abstraktionsnivå
2. Systemnivå
3. Säkerhetsfunktionens delar
4. Typ av system

Abstraktionsnivå
En väsentlig del i en modell är att klargöra vilken abstraktionsnivå som beskrivs. Avsikten med abstraktioner är att isolera och framhäva de aspekter som är viktiga för ett visst ändamål, samt att ignorera de aspekter som är oväsentliga i sammanhanget. Det är viktigt att kunna beskriva ett system för processkontroll oberoende av hur motsvarande implementering på systemplanet är gjord (Wahlström och Gunsell, 1998, och Strandell, 1997). Ett referat på detta tema finns i avsnitt 2.2.

En indelning i 5 olika abstraktionsnivåer föreslås här. Innebörden framgår av exempel i listan nedan, och i några av följande figurer. Nivåerna har ännu inte givits en strikt definition.
1 Teori (bild av sammanhang)
2 Generell funktion (t.ex. ändamål)
3 Principiell funktion (t.ex. inneslutning av radioaktivitet)
4 Funktionell lösning (t.ex. övertemperaturskydd)
5 Utformning, konkret (t.ex. reaktortank, säkerhetsrelä, operatörs åtgärd)

Systemnivå
Det är också angeläget att klargöra vilken systemnivå som behandlas. Ett förslag till indelning är:
a Generellt system
b Specifik anläggning (t.ex. en viss självständig anläggning, en konsultbyrå)
c Delsystem (produktionsanläggning, säkerhetsarbete, kvalitetsarbete)
d Subsystem (t.ex. uppvärmningsugn, reaktortank, inspektion, kvalitetsrevision)
e Komponent (t.ex. relä, ventil, viss åtgärd)

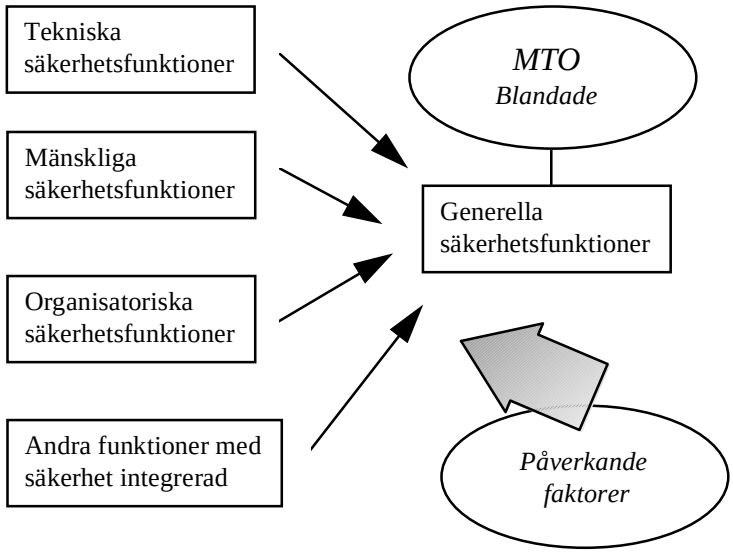
System inkluderar både teknik och människor, samt deras samverkan. Nivåerna c, d och e kan innehålla såväl renodlat tekniska som mänskliga delar, liksom en kombination av dessa.

Som Wahlström och Gunsell (1998) påpekar finns det en "fraktal struktur" på säkerhetsarbetet, eftersom varje del innehåller komponenter i liknande struktur, såsom planering, analys, erfarenhetsåterföring osv. Detta kan i vissa situationer innebära en komplikation vid en uppdelning på nivåer.

Säkerhetsfunktionens delar
Säkerhetsfunktioner kan beskrivas på alla abstraktionsnivåer och kan vara av många slag. MTO-perspektivet är väsentligt, och en uppdelning har gjorts i mänskliga, tekniska och organisatoriska säkerhetsfunktioner, vilket illustreras i Figur 4.1. Det finns också behov att särskilja andra funktioner, vars syfte primärt inte är säkerhet men som ändå påverkar denna.

Påverkande faktorer finns både i den anläggning som studeras, liksom i omvärlden. Dessa faktorer kan påverka hur funktioner utformas och fungerar i praktiken. Några exempel på sådana faktorer är attityder i samhället och hos ägare, ekonomiska förhållanden, attityder hos personal och ledning i anläggningen. Det finns ett behov att i senare skede klarare beskriva vad som bör inkluderas i "påverkande faktor".

Figur 4.1 Säkerhetsfunktionens delar



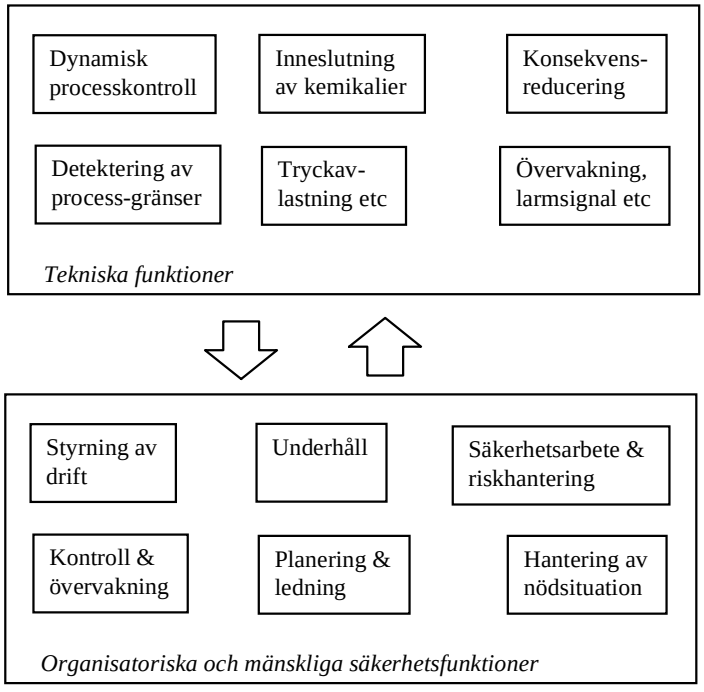
Typ av system
Både själva säkerhetsfunktionen och objektet, dvs det som ska göras säkert, kan vara olika typer av system. Några exempel är:

- Sammansatt system (flera delsystem, som kan vara av olika typ)
- Tekniska system
- Programvara
- Man-maskin-system
- Organisatoriska aktiviteter

Organisatoriska aktiviteter är ett brett område, och man kan behöva pröva olika sätt att inkludera detta i säkerhetsfunktioner.

Exempel
För att illustrera ovanstående strukturering kan man utgå från en liten kemisk anläggning. De principiella säkerhetsfunktionerna för den specifika anläggningen visas i Figur 4.2. Enligt strukturingen hamnar man här på *Abstraktionsnivå 3* och *Systemnivå c*. En indelning har gjorts i tekniska, respektive organisatoriska-/mänskliga säkerhetsfunktioner.

Figur 4.2 Blockschema över säkerhetsfunktioner vid kemisk anläggning

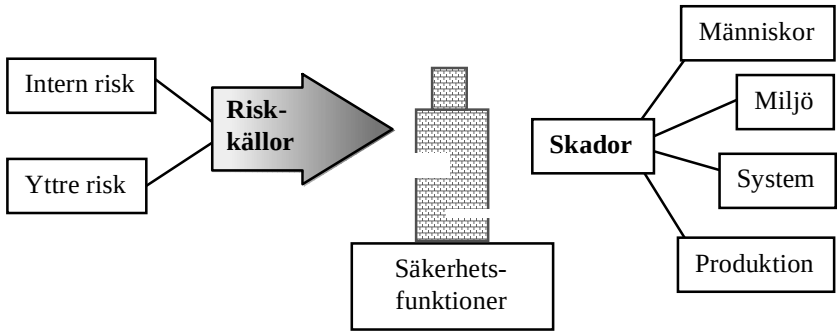


4.2 Modell av säkerhetsfunktioner

Inledning
Detta avsnitt är en är skiss över hur man skulle kunna modellera och teoretiskt beskriva säkerhetsfunktioner. Resonemangen nedan är tänkta att gälla olika abstraktionsnivåer, olika systemnivåer och inkludera ett MTO-perspektiv.

Figur 4.3 visar de övergripande säkerhetsfunktionerna för en anläggning. Ändamålet med dessa är att förhindra att inre eller yttre risker leder till skada på män-niskor, miljö, på produktionssystemet och anläggningen, samt att produktionen skulle hindras.

Figur 4.3 Övergripande bild av säkerhetsfunktionernas roll



Säkerhetsfunktionens egenskaper
En viss SF karakteriseras av ett antal egenskaper. En utgångspunkt är den struktu-rering som skissats i avsnitt 4.1. Ett förslag är:
- *Abstraktionsnivå* (enligt ovan)
- *Systemnivå* (enligt ovan)
- *Typ av system* (enligt ovan)
- *Syfte* (dels generellt, dels säkerhetsrelaterat)
- *Säkerhetsegenskaper*

Säkerhetsegenskaper hos SF
Ett antal egenskaper ur säkerhetsperspektiv kan summeras för varje SF. Dessa blir av olika karaktär, beroende på om det exempelvis gäller en teknisk kontinuerligt inkopplad funktion, eller en serie åtgärder som ska vidtas i en nödsituation. Egen-skaperna kan ha anknytning till olika teman, som exempelvis nedan:

a) Konsekvens vid fel
- Allvarlighet vid fel (ev. kategorisering)
- Berörda delsystem (hur många delsystem som berörs etc)

b) Robusthet
- Robusthet mot avvikelser och tolerans för fel. (Det kan gälla om tekniska fel eller avbrott i en procedur leder till allvarliga konsekvenser.)
- Beroende av andra SF (Oberoende, ensidigt eller ömsesidigt beroende)

c) Verifierbarhet

- Effektens eller slutresultatets verifierbarhet
- Om en SF är korrekt relativt önskade mål, och att inga väsentliga luckor finns
- Om fel skulle uppkomma, bör dessa bli synliga och ej dolda.
- Det ska vara verifierbart att en säkerhetsprocedur följts korrekt.
- Om felupptäcktsmekanismer för SF, t.ex. en procedur, är klarlagda.

I en generell standard (IEC, 1997) finns förslag till relaterade termer för att karakterisera säkerhetsegenskaper. (Se vidare avsnitt 2.5).

- *Funktionell säkerhet* är förmågan hos ett säkerhetsrelaterat system att genomföra de nödvändiga åtgärderna.
- *Säkerhetsintegritet* är sannolikheten att ett säkerhetsrelaterat system genomför erforderliga säkerhetsfunktioner.

"*Effektivitet*" var ett begrepp som användes i början av studien, och det var tänkt som ett generellt kvalitetsmått. Ingenstans i den studerade litteraturen eller i intervjuer har detta begrepp använts i denna betydelse. Det som närmast liknar detta begrepp skulle kunna vara *Funktionell säkerhet* och *Säkerhetsintegritet*. I denna förstudie fanns det därför inte anledning att introducera och definiera ett specifikt effektivitetsmått.

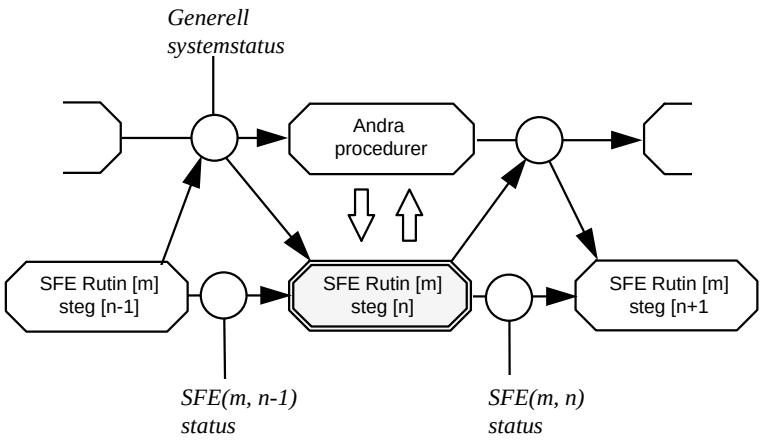
I exemplen ovan är de flesta egenskaperna kvalitativa, men några kan vara kvantifierbara i synnerhet säkerhetsintegritet.

Modell av SF

Man kan tänka sig att bryta ner en säkerhetsfunktion i flera "*Säkerhetsfunktionselement"* - SFE . Det kan gälla ett system med en säkerhetsfunktion som innebär ett tidsförlopp med ett antal steg för att uppnå ett säkerhetsrelaterat syfte. Det skulle kunna vara ett datorstyrt automatiskt system eller en operatör som följer en procedur.

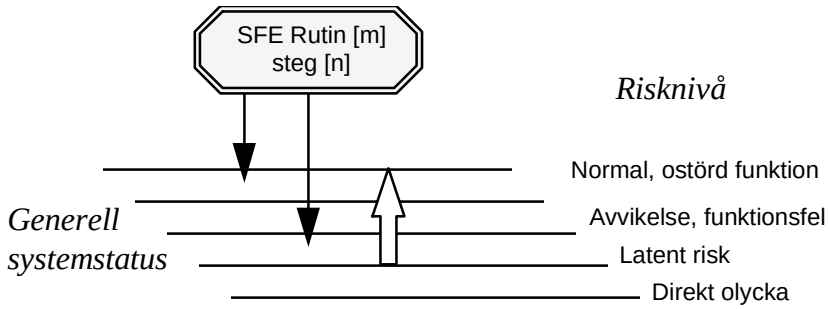
En SFE och dess kopplingar till omvärlden symboliseras i Figur 4.4. I centrum står *"Steg n*" i "*Rutin m*", som kallas ***SFE(m, n)***. "*Rutin m*" kan vara en delprocedur i en större procedur, en sekvens i ett datorprogram etc.

Figur 4.4 Modell av säkerhetsfunktionselement (SFE) och dess kopplingar till systemet i ett tidsförlopp



Denna SFE har föregåtts av ***SFE(m,n-1)***, som satt Rutin m i läget "***SFE(m,n-1)-status***". Detta kan innebära att ett visst dokument har fyllts i, att ett datorprogram har parametrar ställda på ett visst sätt, att manöverdon har ställts i ett specifikt läge etc. *SFE(m,n-1)-status* är en delmängd av den "generella systemstatusen". Denna i sin tur är tänkt att representera alla väsentliga parametrar i det totala systemet.

Figur 4.5 Ett säkerhetsfunktionselement SFE (m,n) och kopplingar till systemets risknivå



När SFE(m,n) gås genom kan systemets risknivå påverkas, vilket är illustrerat i Figur 4.5. Kategoriseringen av risknivån är schematisk, och en förbättrad systematik behövs. SFE(m,n) kan leda till att exempelvis ett antal avvikelser uppkommer, som även kan innebära en latent risk om en barriär sätts ur funktion. Alternativt kan risknivån minska (breda pilen), vilket kan vara det direkta syftet med ett element.

5 Diskussion

5.1 Frågeställningar och perspektiv

Om detta kapitel

Detta diskussionskapitel är inriktat på att belysa frågeställningar med anknytning till säkerhetsfunktioner. Dessa gäller tekniska system i allmänhet, och inte enbart kärnkraftsinstallationer. På flera ställen är därför diskussionen generell och principiell, vilket möjligen samtidigt gör den abstrakt och svårbegriplig. Det var dock en av utgångspunkterna just att pröva ett generellt angreppssätt.

Kapitlen 2 och 3 har summerat resultat från litteraturgenomgången och intervjuer. En av målsättningarna med projektet var att göra en strukturerad sammanställning av säkerhetsfunktioner från olika områden. Detta finns i avsnitt 3.1 och mer utvecklat i avsnitt 4.1. I avsnittet 4.2 finns en modell för att beskriva säkerhetsfunktioner, liksom exempel på olika karakteristika. Avsnitt 5.2 diskuterar för- och nackdelar med principer om generaliserade säkerhetsfunktioner, samt vad som kan ingå i ett eventuellt fortsatt utvecklingsarbete.

Modeller för beskrivning

En väsentlig del i denna studie var att finna modeller och teorier för att beskriva säkerhetsegenskaper. En sådan beskrivning skulle behöva vara bred och bland annat inkludera ett MTO-perspektiv. Det kunde gälla ett specifikt system, eller hur väl ett säkerhetssystem ger önskad säkerhet. Det vore också önskvärt att finna modeller som kunde vara operativa i någon bemärkelse, exempelvis vara till stöd vid:
a) Specifikation av säkerhetskarakteristika
b) Utformning av säkerhetsrutiner
c) Utvärdering av säkerhetsarbete

Wahlström och Gunsell (1998) tar upp flera intressanta aspekter på modeller av säkerhetsarbete och problem med detta (se avsnitt 2.2). En del av dessa har utnyttjats i modellskisserna i avsnitt 4.4. Författarna tar även upp brist på generella modeller, såsom att metoder för granskning av säkerhetsarbete inte har blivit validerade i en strikt vetenskaplig mening, och att ingen teoretisk modell har stått som grund för utformningen. Liknande slutsatser har även dragits i en annan studie (Abramovici och Bourrier, 1998). I övrigt har inte diskussioner om generella teorier observerats i den studerade litteraturen.

I det material som presenterats i Kapitel 2, finns flera exempel på generella modeller. Dessa modeller verkar dock inte vara baserade på en generell teori, utan de har mer speglat en god praxis. Några exempel är:

- Generella säkerhetsprinciper enligt INSAG (1988)
- Principerna för djupförsvar enligt INSAG (1996)
- "Skyddsbarriärer" med flera nivåer från kemibranschen enligt CCPS (1993).

I Kapitel 2.3 finns ett referat av två modeller med ett utpräglat MTO-perspektiv. *AEB- modellen* visar olyckor och de barriärer som skulle kunnat förhindra olyckan (t.ex. Svenson, 1994). En annan studie (t.ex. Kecklund m.fl., 1995) beskriver en modell av händelser och barriärfunktioner (Event and Barrier Function Model, EBFM) i sekvensen för bränslebyte.

Både AEB- och EBFM-modellen är orienterade mot analytiska förklaringar av olycksförlopp. De utgår båda i sina beskrivningar från konkreta renodlade frågeställningar. Båda verkar också utgå från specifika felhändelser, för vilka det finns en unik barriär.

Svenson (1994) pekar på en del svagheter i AEB-modellen (vilket även gäller EBFM). Exempelvis ger modellen ett drastiskt reducerat perspektiv på de samverkande komplexa systemen (mänskliga, organisatoriska och tekniska).

En reflektion är att konsekvenserna vid fel inte nämnts i artiklarna om EBFM. Detta borde vara väsentligt vid bedömningen av vilka krav som ska ställas. Man har inte heller så tydligt belyst relationen mellan olika barriärer, respektive om andra barriärer kan påverka samma fel. Modellerna verkar därför inte vara utformade för att vara utgångspunkter för en generell analysmetodik, men de är mycket intressanta som delar i en metodutveckling.

5.2 Om värdet av generaliserade säkerhetsfunktioner

Om utgångspunkterna

Denna förstudie har bl.a. varit inriktad på att undersöka för- och nackdelar med generaliserade säkerhetsfunktioner, och hur användbart detta skulle kunna vara. Några direkta svar från litteraturen eller vid intervjuer har inte kommit på dessa teman. Den ursprungliga idén till hur värderingen skulle göras utgick från att ett preliminärt förslag skulle behandlas vid ett seminarium. På grundval av diskussionen skulle sedan en sammanställning göras.

Av flera skäl har inte ett sådant seminarium genomförts, och den summering som anges här behöver kompletteras. Det främsta skälet är att personer med olika erfarenheter och intressen kan prioritera och värdera med skilda utgångspunkter. Därmed skulle en sådan värdering få en större giltighet.

Om begreppet säkerhetsfunktion

I denna rapport har en grundläggande definition varit: *En säkerhetsfunktion är en teknisk eller organisatorisk funktion med syfte att minska sannolikhet och/eller konsekvens förknippad med en viss riskkälla.*

Vid utformningen av rapporten har en del ändringar gjorts. I stället för "riskkälla" stod ursprungligen "risk", vilket är mångtydigt och därmed ej så praktiskt. I den ursprungliga målformuleringen stod "generaliserat säkerhetsfunktionsbegrepp", vilket blir en tautologi med den nuvarande generella definitionen. Underförstått i definitionen är att sannolikhet gäller en olycka och att konsekvens gäller skadans storlek eller allvarlighet.
I ett fortsatt utvecklingsarbete behöver flera principiella aspekter beaktas på definitionen:

- Främst gäller det när begreppet säkerhetsfunktion används på olika "*abstraktionsnivåer*" eller "*systemnivåer*". När passar begreppet "funktion" att användas, och när det ska det ersättas med något annat?
- På högre "*abstraktionsnivåer*" eller "*systemnivåer*" är funktionerna mer generella, och de blir en kombination av teknik och organisation.
- En säkerhetsfunktion kan vara inkluderat i ett system, utan att den riskkälla den ska hantera existerar.
- En säkerhetsfunktion kan existera utan att det funnits någon "avsikt" att den ska ge ett visst skydd. Ordet "avsikt" är därför inte lämpligt i definitionen.
- En väsentlig aspekt är hur man ska hantera det informella säkerhetsarbetet. Det är delvis beaktat i begreppet "säkerhetskultur", men inte hanterat i någon metodik. Dessa kan i en modell inkluderas som "påverkande faktor" eller som en kategori i en SF-struktur.

Inom kärnkraftsområdet används termen med en specifik innebörd (avsnitt 3.1), men det finns ingen principiell skillnad i betydelsen. Termen används i andra sammanhang, men då vanligen utan formell definition. Det har därmed inte framkommit några egentliga skäl att söka ett alternativt begrepp. Däremot finns det anledning att försöka förbättra definitionen.

OM FÖR- OCH NACKDELAR

Nedan summeras exempel på för- och nackdelar med användning av säkerhetsfunktioner. Tyngden hos dessa beror på situationen och tillämpningen.

Nackdelar

- Redan etablerade arbetssätt kan vara tillräckligt effektiva, och nyttan är kanske marginell eller åtminstone okänd.
- Kan ta resurser från ett vanligt arbetssätt.
- Finns inte exempel på tillämpningar.
- Abstrakta begrepp och ingen färdig teori.
- Kan bli svåra att pedagogiskt förklara.
- Finns ingen utvärdering av teori och erfarenheter.
- Kategorisering kan bli svår.

Fördelar

Stödjande

Användningen kan stödja:

- Ett analytiskt arbetssätt och beskrivningsmetodik som är användbar på olika systemnivåer.
- Utnyttjandet av erfarenheter från olika tillämpningsrådet, t.ex. kemisk industri och transportsektorn, om man arbetar med liknande beskrivningsmodeller.
- Specifikation av en viss SF, t.ex. tydliggöra användningsområde och behov av tillförlitlighet.
- Hanteringen av "gränssnitt" av olika slag, t.ex. mellan ansvarsområden. (Detta argument är grundat på erfarenhet från många olyckor, där beslut som varit kritiska för olycksförloppet tagits högt upp i företagshierarkin.)
- Förbättring av effektivitet och tillförlitlighet (se nedan).
- Stimulans till nytänkande (se nedan).

Effektivitet och tillförlitlighet
I system med stora risker och höga krav på säkerhet, är effektivitet och tillförlitlighet nyckelord i bedömningen och utformningen av säkerhetsarbete och säkerhetsanordningar. Från tekniska system finns en gedigen erfarenhet för att erhålla god tillförlitlighet och flera olika principer såsom redundans, diversifiering etc. (se avsnitt 2.2). Användning av generella SF skulle kunna stödja att sådana principer systematiskt tillämpas på ett bredare område.

Stimulans till nytänkande
Tekniska och organisatoriska förändringar kan ändra riskbilden och behov av säkerhetssystem (kort diskuterat i avsnitt 3.3). Teorier och diskussioner kring säkerhetsfunktioner, skulle kunna vara stimulans till ifrågasättande och nytänkande. En fördel med ett abstrakt arbetssätt är man kan framhäva de aspekter som är viktiga för ett visst ändamål, samt att ignorera de som är oväsentliga i sammanhanget.

En hopvägning
Hur de positiva och negativa argumenten ska vägas ihop är långt ifrån självklart. Författarens bedömning är att de positiva klart väger över - mot att det vore värdefullt med ett fortsatt utvecklingsarbete. Ett sådant får sedan visa om det kan ge meningsfulla resultat. Ett utvecklingsarbete behöver inte i och för sig bedrivas inom kärnkraftssektorn, principerna är allmängiltiga.

Några tillämpningsområden
Några exempel på områden där tillämpningar skulle kunna prövas är:
- Utredning av tillbud.
- Analys av säkerhetsfunktioner i ett tekniskt system.
- Bedömning av lämpligheten hos specifika säkerhetsfunktioner.
- Katalog över säkerhetsfunktioner och generiska egenskaper. Det kan vara på olika abstraktions- och systemnivåer, där särskilt procedurer kan vara intressanta.
- Stödmaterial för design, särskilt procedurer.
- Modellering för probabilistisk tillämpning.

Om fortsatt utvecklingsarbete
Litteraturgenomgången och intervjuerna pekar på en utvecklingspotential för säkerhetsarbete och ett behov av förbättringar, särskilt med anknytning till procedurer. Det verkar troligt att angreppssätt baserade på skisserade säkerhetsfunktioner eller liknande tankesätt skulle kunna ge väsentliga bidrag.

Ett fortsatt arbete bör lägga vikt vid några fallstudier, för att i högre grad kombinera praktiska och teoretiska ansatser än vad som varit möjligt i denna studie. För detta verkar de två första punkterna i exemplen på tillämpningar intressantast. De skulle kunna inledas som en utredning av ett specifikt fall, med avsikt att på sikt resultera i mer generella analysverktyg. Detta förstås under förutsättning att de praktiska resultaten och det teoretiska underlaget motiverar detta.

5.3 Summering och slutsatser

Om studien
Denna rapport är av karaktären förstudie, vilket innebär att många metoder och studier inte har inkluderats. Detta har i någon mån kompenserats genom att flera personer med en bra överblick av området intervjuats. Hur stort bortfallet kan vara är svårbedömt, men om viktiga fakta inte kommit fram, indikerar detta samtidigt att de "saknade resultaten" ej slagit genom.

Barriärer och säkerhetsfunktioner
Det finns många begrepp som används med anknytning till "barriär" och "säkerhetsfunktioner", och sammanställningar i denna rapport visar på olika användningar. Exempelvis är en definition av barriär strikt fysiskt/tekniskt orienterad och väl preciserad. Ett alternativ är att barriär har en bredare innebörd som inkluderar mänskliga, tekniska och organisatoriska element. Det finns ibland problem med terminologin, dels att betydelsen av ord kan variera mellan olika tillämpningar, dels att termer inte alls definieras.

Teorier och modeller
Det har framkommit avsevärt mindre teoretiserande kring barriärer och säkerhetsfunktioner än förväntat. Det gäller särskilt generella funktioner som inkluderar tekniska, mänskliga och organisatoriska element. Inom vissa teknik- och forskningsområden finns mycket teoretiska diskussioner, men de verkar begränsas av sina områdens avgränsningar.

I denna studie finns ett förslag till generaliserad modell av säkerhetsfunktioner, som bland annat utgår från "säkerhetsfunktionselement". En beskrivning finns också av tänkbara karakteristika hos säkerhetsfunktionerna.

Behov och utvecklingsarbete
För- och nackdelar med generaliserade säkerhetsfunktioner har ställts samman. Baserad på detta bedömer författaren att det vore värdefullt att pröva ett fortsatt utvecklingsarbete. Litteraturgenomgången och intervjuerna pekar på en utvecklingspotential för säkerhetsarbete och ett behov av förbättringar, särskilt med anknytning till procedurer. Det verkar troligt att angreppssätt baserade på skisserade säkerhetsfunktioner eller liknande tankesätt skulle kunna ge väsentliga bidrag.

Om ett utvecklingsarbete ska bedrivas, bör fallstudier vara väsentliga. Sex exempel på teman finns angivna i avsnitt 5.2, och särskilt intressanta vore inriktningar mot utredning av tillbud, och mot analys av säkerhetsfunktioner i ett tekniskt system.

6 Referenser

Abramovici, M. och Bourrier, M. Beyond the Black Box: Organisational factors in probabilistic risk assessment methods. *Society for Risk Analysis - Europe 1998 Annual Conference*, Paris, 13 s., 1998

Beard J.T. What Does "Safety Function" Mean? J. T. Beard Inc., Maryland, 1996. *Publicerad på http://www3.dp.doe.gov/CTG/authbase/sf_paper.htm.*

CCPS (Center for Chemical Process Safety). Guidelines for Safe Automation of Chemical Industries. American Institute of Chemical Engineers, New York, 424 s., 1993

DOE (Department of Energy). Improved Safety Function Definition in Safety Documentation for Nuclear Facilities. US Department of Energy, Wahington, DC, 1996. *Publicerad på http://www3.dp.doe.gov/CTG/resource/sils/96-04.htm*

Dvoudian, K., Wu, J. och Apostolakis, G. The Work Process Analysis Model (WPAM). *Reliability Engineering and System Safety.* Vol 53, s.107-125, 1994

EEG. Rådets direktiv av den 12 juni 1989 om åtgärder för att främja förbättringar av arbetstagarnas säkerhet och hälsa i arbetet. *Europeiska gemenskapernas officiella tidning* Nr L 183, 10.7.1989

Embrey D.E. SHERPA: A systematic human error reduction and prediction approach. *Proc. Advances in Human Factors in Nuclear Power Systems Meeting,* Knoxville, 1986.

Embrey D.E. Incorporating management and organisational factors into probabilistic safety assesment. *Reliability Engineering and Systems Safety*, Vol. 38, s.199-208, 1992

Hale A.R., Heming B.H.J., Carthey J. och Kirwan B. Modelling of safety management systems. *Safety Science,* Vol. 26, s. 121-140, 1997.

Harms-Ringdahl L. Säkerhetsanalys i skyddsarbetet. Folksam, 189 s., 1987

Harms-Ringdahl L. Riskhantering och ledningssystem för säkerhet, hälsa och miljö. Institutet för Riskhantering och Säkerhetsanalys, Stockholm, 166 s., 1995

Harms-Ringdahl L. Riskanalys i MTO-perspektiv - summering av metoder för industriell tillämpning. SKI Rapport 96:63. Statens kärnkraftinspektion, Stockholm, 27 s., 1996

Harms-Ringdahl L. och Ohlsson K. Om elva myndigheters perspektiv på olyckor och riskhantering. Institutet för Riskhantering och Säkerhetsanalys, Stockholm, 87 s., 1993

Hovden J. Sikkerhetsforskning - En utredning for NFR. Norges teknisk-naturvitenskapelige universitet, Trondheim, 1998.

IAEA. Human reliability analysis in probabilistic safety assessment for nuclear power plants. A safety practice. *Safety series* No. 50-P-10. International Atomic Energy Agency, Wien, 92 s., 1995

IAEA. Quality assurance for safety in nuclear power plants and other nuclear installations. *Code and Safety Guides* Q1-Q14. International Atomic Energy Agency, Wien, 350 s., 1996

IEC. Standard IEC 1508: Functional safety: safety related systems (Draft). IEC International Electrotechnical Commission, 350 s.**,** 1997

Ingstad, O. och Bodsberg, L. CRIOP: A scenario-method for evaluation of offshore control centers. SINTEF, Trondheim, 94 s., 1990

INSAG (International Nuclear Safety Advisory Group). Basic safety principles for Nuclear Power Plants, 75-INSAG-3, International Atomic Energy Agency, Wien, 73 s., 1988

INSAG (International Nuclear Safety Advisory Group). Defence in depth in nuclear safety, INSAG-10. International Atomic Energy Agency, Wien, 33 s., 1996

Jacobsson Kecklund L., Edland A., Wedin P., och Svenson O. Safety barrier function analysis of the refuelling process in a nuclear power plant. Ingår i: *Bradley, GE and Hendrick HW (eds.). Human factors in organizational design and management*. Amsterdam, North-Holland, s. 145-150, 1994

Johnson W.G. MORT Safety Assurance Systems. National Safety Council, Chicago, 525 s., 1980

Kecklund L., Edland A., Wedin P., och Svenson O. Comparison of safety barrier functions in the refueling process in a nuclear power plant before and after a technical and organizational change. Ingår i *L.Norros (Ed.) Fifth European Conference on Cognitive Science Approaches to Process Controll,* VTT, Espoo, Finland, 1995.

Kjellén, U. och Tinmannsvik, R. SMORT - Säkerhetsanalys av industriell organisation, Arbetarskyddsnämnden, Stockholm, 72 s., 1989

Knox, N.W. och Eicher, R.W. MORT User's Manual, ODE 76/45-4, SSDC-4, EG&G Idaho Inc, 1983

Marsden P. Procedures in the nuclear industry. Ingår i *Stanton N (red). Human Factors in Nuclear Safety*. Taylor & Francis, London, s. 99-116 (352 s.) 1996

Paté-Cornell , E. och Murphy, D. Human and management factors in probabilistic risk analysis: the SAM approach and observations from recent applications. *Reliability Engineering and System Safety*. Vol 53, s.115 -126, 1996

Rollenhagen C. MTO - en introduktion. Sambandet Människa, Teknik och Organisation. Utbildningshuset Studentlitteratur, Lund, 198 s., 1995

SEK. Tillförlitlighet - Ordlista. Svensk standard SS441 05 05. Svenska Elektriska Kommissionen, 79 s., 1998

SKI. Statens kärnkraftinspektions föreskrifter om säkerhet i vissa kärntekniska anläggningar. SKIFS 1998:1. Statens kärnkraftinspektion, Stockholm, 1998.

Starbuck W.H. och Frances J.M. Challenger: Fine-tuning the odds until something breaks. *Journal of Management Studies*, 25:4, s. 319-340, 1988

Strandell C. Kärnkraftsäkerhetens begrepp och deras relationer; en analysmodell av säkerhetsarbetets komponenter och innehåll. (NKS/-RAK-1(97) R2. VTT automation, Esbo, Finland, 80 s., 1997

Svenson O. The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Analysis* Vol. 11, No 3, s. 499-507, 1991

Svenson O. Incident analysis and the accident evolution and barrier function (AEB). *OECD/NEA Workshop on the Modification of Nuclear Power Plants Event Investigation and Operability Decisions*, Helsinki, 7 s., 1994

TNC, Tekniska nomenklaturcentralen. Kärnenergiordlista, TNC, 225 s., 1990

Wahlström B., och Gunsell L. Reaktorsäkerhet; En beskrivning och en värdering av säkerhetsarbetet i Norden. (NKS/RAK-1(97) R8. NKS-sekretariatet, Risö forsknings-center, Danmark, 175 s., 1998