SKI Rapport 2007:33

Forskning

Analys av mänsklig tillförlitlighet

HRA-begreppets tillämpbarhet vid revisionsavställning

Aino Obenius

Augusti 2007

ISSN 1104-1374
ISRN SKI-R-07/33-SE

SKI

SKI-perspektiv

Bakgrund

Analyser av mänsklig tillförlitlighet, Human Reliability Analysis (HRA) har använts under en längre tid i kärnkraftverkens probabilistiska säkerhetsanalyser. SKI har nyligen genomfört en utredning om befintliga metoder inom området HRA (litteraturstudie) och hur dessa metoder används av tillståndshavarna för de svenska kärnkraftverken med syfte att öka SKI:s kompetens och kunskaperna inom området (HRA – En översikt av användning metoder och tillsyn, SKI Utredningsrapport, ref 2006/576, 2007-05-02). Det kan också nämnas upplysningsvis att forskning inom HRA och dess metodik bedrivs t.ex. vid Institutet för Energiteknik (Institutt for energiteknik), OECD Halden Reactor Project.

HRA analyser genomförs för olika drifttillstånd och fokus har ofta varit på att analysera kontrollrumsoperatörernas samspel med tekniken, organisationen och förekommande arbetsförutsättningar, samt att på så sätt identifiera de risker som finns och åtgärda dessa. Vikten av att tillståndshavarna även genomföra HRA studier (som en del i PSA) avseende avställda reaktorer då t.ex. underhåll, bränslebyten och tester utförs har tidigt påpekats av SKI och tillståndshavarna för kärnkraftverken har genomfört sådana analyser.

Föreliggande SKI rapport är ett examensarbete som utförts av Aino Obenius vid Uppsala Universitet inom Civilingenjörsprogrammet System i teknik och samhälle. Syftet med examensarbetet är att beskriva de metoder och grundläggande modeller om mänsklig tillförlitlighet som används vid analys av avställningsperioden vid svenska kärnkraftverk. Examensarbetet har utförts på eget initiativ av författaren.

SKI:s syfte

SKI:s syfte är att stödja kompetensutvecklingen inom området HRA, vilket bedöms vara speciellt viktigt, eftersom det finns behov av att fördjupa kunskaperna inom området, samt vidareutveckla metodiken avseende samspelet Människa Teknik Organisation (MTO) och de faktorer som påverkar den mänskliga tillförlitligheten.

Resultat

Examensarbetet har gett en fördjupad kunskap om hur HRA genomförs i praktiken inom området avställd drift, samt diskuterar behoven av fortsatt utveckling av metodiken i ett MTO perspektiv.

Behov av ytterligare forskning

Rapporten innehåller förslag på fortsatt forskning.

Projektinformation

Handläggare av forskningsuppdraget har från SKI:s sida varit Per-Olof Sandén. Diarienumret för projektet är SKI 2007/141 och projektnumret är 200703016.

Förord

Projektet har genomförts inom ramen för ett examensarbete för civiliningenjörsprogrammet System i teknik och samhälle vid Uppsala universitet. Författaren vill rikta ett särskilt tack till handledaren Lena Kecklund, MTO Psykologi AB samt ämnesgranskaren Anders Jansson, IT-institutionen och avdelningen för Människa-datorinteraktion vid Uppsala universitet.

Tack också till representanter vid kärnkraftverken som hjälpt till med datainsamling och synpunkter på HRA. Tack till Anna Roos, som under tiden för detta arbete genomfört en kartläggning av metoder för och användning av HRA för SKI, och som varit en hjälp för att reda ut begreppen inom HRA. I övrigt vill jag tacka alla som jag varit i kontakt med och som framfört sina synpunkter och tankar om PSA och HRA för avställning.

Aino Obenius
Stockholm
Den 7 augusti 2007

SKI Rapport 2007:33

Forskning

Analys av mänsklig tillförlitlighet

HRA-begreppets tillämpbarhet vid revisionsavställning

Aino Obenius

MTO Psykologi AB
Hornsbruksgatan 28
117 34 Stockholm

Examensarbete 20 p.
Civilingenjörsprogrammet System i teknik och samhälle
Uppsala Universitet

Augusti 2007

Sammanfattning

Ett sätt att arbeta förebyggande med kärnkraftssäkerhet är att genomföra probabilistiska säkerhetsanalyser (PSA). Syftet med en sådan analys är att identifiera möjliga fel som kan inträffa och som i förlängningen kan leda till allvarliga konsekvenser i form av en härdskada. Analys av de kända olyckorna vid kärnkraftverken i Three Mile Island 1979 och Chernobyl 1986 bidrog till att bredda synen på kärnkraftsäkerhet. Ett systemperspektiv där Människa, Teknik och Organisation (MTO) i samverkan påverkar säkerheten växte fram. För att ta hänsyn till människans påverkan på det tekniska systemet används inom PSA analyser av mänsklig tillförlitlighet, Human Reliability Analysis (HRA).

PSA för avställningsperioden är under utförande för de svenska kärnkraftverken. Syftet med examensarbetet är att beskriva de metoder och grundläggande modeller för mänsklig tillförlitlighet som används vid analys av avställningsperioden. Följande frågeställningar behandlas:

1. Hur kan avställningsperioden karaktäriseras och definieras?
2. Vad är viktigt att ta hänsyn till vid analys av mänskliga ingrepp under avställningsperioden?
3. Hur kan mänskligt beteende i en riskanalys för avställning modelleras?
4. Mot bakgrund av tillgängligt empiriskt material, hur har punkterna ovan hanterats i genomförda analyser av ingrepp under avställning?
5. Hur påverkar resultatet av ovanstående frågor hur metod för avställningsanalys kan och/eller behöver utvecklas?

Metoden för projektet har främst varit litteraturstudier av tillgänglig teori för modellering av mänskligt beteende och riskanalys av avställningsperioden. För att identifiera hur mänskligt beteende modelleras i genomförda analyser, har avställningsanalyser för de svenska kraftverken granskats för de fyra första stegen i Kirwans (1994, 2005) HRA-process; Problemdefinition, Uppgiftsanalys, Identifiering av mänskliga felhandlingar och Representation.

Studien avser analys av planerade avställningar för genomförande av underhåll, bränslebyte tester och inspektion, så kallad revision. Avställningsperioden karaktäriseras av planerade underhållsaktiviteter utförda i roterande 3-skift, 24 timmar om dygnet, samt att en stor andel utomstående entreprenörer utför arbeten på verket. Arbetsförhållandena karaktäriseras av stress p.g.a. hög värme, strålning och fysiskt krävande eller monotona arbetsuppgifter. Fel och misstag under detta drifttillstånd kan ha stora konsekvenser både i det direkta arbetet samt som orsak till latenta fel som påverkar systemet i den kommande produktionen.

Människans påverkan på det tekniska systemet är av stor betydelse vid analys av avställning. Detta bör även påverka avställningsanalysens utgångspunkt och genomförande, för att möjliggöra en så realistisk analys som möjligt. Vid analys av mänskliga ingrepp under avställningsperioden bör ett holistiskt perspektiv användas. Ett sätt att ta hänsyn till människans förmåga och variabilitet i prestation är viktigt.

Modeller för mänskligt beteende i en riskanalys utgår idag normalt från ett *normativt* synsätt, om hur ett system och de människor som arbetar med systemet *borde* uppföra sig, alternativt från ett *deskriptivt* synsätt, d.v.s. att istället utgå från hur systemet och de som arbetar med det *faktiskt* beter sig, enligt en linjär orsak-verkan modell. Teoretiker menar att en sådan modell bara bör användas för slutna och/eller små system eller i väl avgränsade användningssituationer. Vicente (1999) förespråkar istället ett *formativt* synsätt, en modell som specificerar de *villkor* och *krav* som måste uppfyllas för att systemet ska bete sig på ett önskvärt sätt. Övergripande mål om säkerhet, produktivitet och hälsa bryts i den modellen ned med hjälp av analyser på olika konceptuella nivåer.

Ytterligare kritik riktas mot HRA och modellering av mänskligt beteende av bl.a. Hollnagel (2005), som menar att praktiskt taget alla HRA-metoder delar antagandet att det är meningsfullt att använda begreppet ”human error”, vilket medför att det är meningsfullt att utveckla sätt att värdera sannolikheter för mänskligt felhandlande. Hollnagel anser i stället att förutsägelserna borde handla om hur det sammankopplade systemet kan förlora kontrollen över situationen, snarare än om människan kommer att göra ett isolerat fel. En olycksmodell som beskriver detta är den för ”Funktionell resonans” (Hollnagel, 2007). Grundantagandet är då att olyckor är resultat av oväntade kombinationer (resonans eller genklang) av normal variabilitet i systemets prestation. Olyckor bör förebyggas genom att övervaka och dämpa denna variabilitet och en bibehållen säkerhet kräver en konstant förmåga att förutse och förekomma framtida händelser. En riskanalys bör då söka efter ”Effectiveness-Thorougness Trade-Off” (ETTO), d.v.s. en lämplig avvägning mellan effektivitet och noggrannhet och var denna avvägning kan gå fel.

Genomförda analyser av mänsklig tillförlitlighet för avställningsperioden har vid granskningen visat sig bygga på det normativa och det deskriptiva synsättet och en linjär orsak-verkan modell. Fokus för HRA inom ramen för PSA är kvantifiering av frekvensen av mänskliga handlingar som inledande händelser. Teori och praktik för modellering av mänskligt beteende i komplexa, sociotekniska system stämmer alltså inte överens. En grundläggande orsak till detta kan vara, att modeller som funktionell resonans, ännu inte har fått genomslag bland praktiserande analytiker, dels beroende på att det saknas beprövade metoder, dels för att genomförda analyser av avställning utgår från PSA, som därmed formar vilken typ av resultat som önskas från HRA, d.v.s. sannolikheter för mänskligt felhandlande.

Klart är att metoder för avställningsanalys behöver utvärderas och utvecklas vidare. Utgångspunkten för analys skulle, i stället för PSA, vara en holistisk analys med avseende på hur Mänskliga, Tekniska och Organisatoriska faktorer påverkar anläggningens säkerhet. För att uppnå detta skulle fortsatta aktiviteter kunna vara en fördjupad genomgång av befintliga avställningsanalyser, utveckling av kravspecifikation för avställningsanalyser, validering av HRA-processens arbetsgång samt utveckling av praktiskt tillämpbara metoder för analys av mänsklig prestation och variabilitet i sociotekniska system.

Summary

Probabilistic Safety Analysis (PSA) is performed for Swedish nuclear power plants in order to make predictions and improvements of system safety. The analysis of the Three Mile Island (1979) and Chernobyl (1986) accidents contributed to broaden the approach to nuclear power plant safety. A system perspective focusing on the interaction between aspects of Man, Technology and Organization (MTO) emerged in addition to the development of Human Factors knowledge. To take the human influence on the technical system into consideration when performing PSAs, a Human Reliability Analysis (HRA) is performed.

PSA is performed for different stages and plant operating states, and the current state of Swedish analyses is Low power and Shutdown (LP&SD), also called Shutdown PSA (SPSA). The purpose of this master's thesis is to describe methods and basic models used when analysing human reliability for the LP&SD state. The following questions are at issue:

1. How can the LP&SD state be characterised and defined?
2. What is important to take into consideration when performing a LP&SD HRA?
3. How can human behaviour be modelled for a LP&SD risk analysis?
4. According to available empirical material, how are the questions above treated in performed analysis of human operation during LP&SD?
5. How does the result of the questions above affect the way methods for analysis of LP&SD could and/or should be developed?

The procedure of this project has mainly consisted of literature studies of available theory for modelling of human behaviour and risk analysis of the LP&SD state. To identify how human behaviour has been modelled in performed analyses, human reliability analysis of SPSA:s performed in Sweden have been studied according to the four first steps of Kirwan's (1994, 2005) HRA-process: Problem definition, Task analysis, Human error analysis and Representation.

This study regards analysis of planned outages when maintenance, fuel change, tests and inspections are performed. The outage period is characterised by planned maintenance activities performed in rotating 3-shifts, around the clock, as well as many of the persons performing work tasks on the plant being external contractors. The working conditions are characterised by stress due to heat, radiation and physically demanding or monotonous work tasks. Errors and mistakes during this plant operating state may have severe consequences, both on the immediate work, as well as on the future power production.

The human influence on the technical system is of great importance when analysing the LP&SD condition. This should also affect the basis and performance of the analysis, to make as a realistic analysis as possible. When analysing human operation during LP&SD, a holistic perspective should be used. A way to take the human abilities and performance variability into consideration is important.

Human behaviour models in currently performed risk analyses are usually based on a *normative* approach, describing how a system and the people working with it *should* behave, alternatively on a *descriptive* approach, describing how a system and people *actually* behave, according to a linear cause and effects model. Human factors theorists say that such a model only should be used for closed and/or small systems or in clearly defined fields of application. Vicente (1999) advocates a *formative* approach, using a model which specifies the conditions and requirements to be fulfilled for the system to behave as desired. Overall aims of safety, productivity and health are decomposed using analysis on different conceptual levels.

Further criticism has been levelled against HRA and human behaviour modelling e.g. by Hollnagel (2005), who says that practically all methods for human reliability analysis share the assumption that the notion of "human error" is meaningful, which would result in that estimation of human error probabilities is a meaningful aim. Instead of this, Hollnagel considers it to be better if the predictions dealed with how the joint system can loose control of the situation, rather than with if the person will make an isolated error. An accident model for the joint system is the one for Functional resonance (Hollnagel, 2007). The basic assumption for this model is that accidents result from unexpected combinations (resonance) of normal system performance variability. Accidents should be prevented through supervision and moderation of this variability and a constant ability to foresee and prevent future events is necessary for safety retention. A safety assessment should seek the "Effectiveness-Thorougness Trade-Off" (ETTO), i.e. on the proper fit between work effectiveness and thoroughness and in which situations this fit may fail.

The study of performed analysis of human reliability for the LP&SD condition shows, that the normative and/or descriptive approach and the linear cause-effect model are used. The main objective of HRAs performed within SPSAs is the quantification of human interaction and error frequency. Modelling of human behaviour in complex, sociotechnical systems differs in theory and practice. A reason may be that models as the one for functional resonance, not yet are applicable for practising analysts, due to a lack of well tried methods and the fact that analysis of the LP&SD condition is performed in the PSA concept, which defines the type of results sought from the HRA, i.e. probabilities for human error.

LP&SD analysis methods need to be further evaluated, validated and developed. The basis for the analysis should, instead of PSA, be a holistic analysis according to how Man, Technology and Organization affect the system and plant safety. To achieve this, further activities could be to perform an in-depth study of existing analysis of the LP&SD condition, to develop specifications of requirement for LP&SD analysis, to further validate the HRA work process as well as to further develop practically applicable methods for human performance and variability analysis in sociotechnical systems.

Innehållsförteckning

1. Inledning

1.1 Bakgrund

Ett sätt att arbeta förebyggande med kärnkraftssäkerhet är att genomföra probabilistiska säkerhetsanalyser (PSA). Syftet med en sådan analys är att identifiera möjliga fel som kan inträffa och som i förlängningen kan leda till allvarliga konsekvenser i form av en härdskada. Analys av de kända olyckorna vid kärnkraftverken i Three Mile Island 1979 och Chernobyl 1986 bidrog till att bredda synen på kärnkraftsäkerhet. Ett systemperspektiv där Människa, Teknik och Organisation (MTO) i samverkan påverkar säkerheten växte fram. För att ta hänsyn till människans påverkan på det tekniska systemet används inom PSA analyser av mänsklig tillförlitlighet, Human Reliability Analysis (HRA).

PSA genomförs i steg där olika konsekvenser och driftförutsättningar avgränsar analysen. En del innebär att analysera den period under året då ett driftstopp planerats för att genomföra underhåll och tekniska förändringar. Denna avställningsperiod karaktäriseras av andra förhållanden jämfört med normal effektdrift och ställer därför andra krav på säkerheten och bedömning av mänsklig samverkan. Bland annat har avställningsperioden kallats för ”ett enda stort manuellt ingrepp”. Detta bör säkerhetsanalysen ta hänsyn till. Denna typ av analyser är av särskilt intresse därför att analyser med ursprungligen teknisk utgångspunkt (d.v.s. PSA) används för att värdera en situation där mänskliga ingrepp har stor betydelse. Det är tillförlitlighetsanalyser av mänskliga ingrepp vid avställning som är utgångspunkten för detta examensarbete.

1.2 Syfte och frågeställningar

Syftet med examensarbetet är att beskriva de metoder och grundläggande modeller för mänsklig tillförlitlighet som används vid analys av avställningsperioden. Målet är att kunna identifiera vad som är viktigt att ta hänsyn till vid analys av avställningsperioden baserat på tillgänglig teori och erfarenhet och sedan granska hur detta görs i praktiken. För att kunna göra detta ska följande frågeställningar besvaras:

6. Hur kan avställningsperioden karaktäriseras och definieras?
7. Vad är viktigt att ta hänsyn till vid analys av mänskliga ingrepp under avställningsperioden?
8. Hur kan mänskligt beteende i en riskanalys för avställning modelleras?
9. Mot bakgrund av tillgängligt empiriskt material, hur har punkterna ovan hanterats i genomförda analyser av ingrepp under avställning?
10. Hur påverkar resultatet av ovanstående frågor hur metod för avställningsanalys kan och/eller behöver utvecklas?

Ambitionen med detta examensarbete är att koppla modellering av mänskligt beteende med säkerhetsanalys för att identifiera vilka antaganden en analys av avställningsperioden bör grundas på.

Resultatet ska ge ökad förståelse för betydelsen av analys av mänskligt beteende för

avställningsperioden ur ett säkerhetsperspektiv.

1.3 Läsanvisning

Detta arbete bygger på en genomgång av den teoretiska grunden för mänskligt beteende och säkerhetsanalys. I denna rapport ges i kapitel 2 en bakgrund till säkerhetsanalys i allmänhet och probabilistisk säkerhetsanalys i synnerhet. Detta för att introducera viktiga begrepp och arbetssätt inom säkerhetsanalys för kärnkraftbranschen. Den insatte läsaren kan hoppa över avsnittet. Därefter ges en historik till mänsklig tillförlitlighetsanalys (HRA) samt en problematisering av varför utveckling av dessa analyser behövs. Detta sker med en beskrivning av hur analys av mänsklig tillförlitlighet hänger ihop med PSA samt hur detta påverkar tillförlitlighetsanalysen.

I kapitel 3 behandlas den första frågeställningen om hur avställningsperioden kan karaktäriseras och definieras med hjälp av en beskrivning av vad perioden innebär samt en jämförelse med det andra huvudsakliga drifttillståndet effektdrift. Tanken med avsnittet är också att skapa en förståelse för varför avställning kan ställa andra krav på analysmetoder än traditionella analyser av normal effektdrift.

Det fjärde kapitlet utgör genomgången av den teoretiska grunden för analyser av mänsklig tillförlitlighet. Syftet med detta avsnitt är att redovisa olika angreppssätt och modeller för mänskligt beteende från dels ett individuellt, personperspektiv och dels från ett holistiskt, systemperspektiv. Kapitel 5 ger ett angreppssätt för hur arbetssättet för analys av mänsklig tillförlitlighet kan beskrivas. Två specifika metoder, som representerar olika tankesätt och utvecklingssteg för HRA, beskrivs också kort då de båda använts i de granskade analyserna och utgör exempel på hur olika modeller för mänskligt beteende kan omvandlas i praktiska metoder.

Metodavsnittet i kapitel 6 beskriver hur själva granskningen av tre analyser genomförda vid de svenska kraftverken har gått till. Därefter följer kapitel 7 med resultatet av granskningen uppställt enligt den angivna arbetsprocessen för mänsklig tillförlitlighetsanalys tillsammans med sammanfattande tabeller. Genom att jämföra teori och praktik med de förutsättningar som avställningsperioden ger skall styrkor, svagheter och använd modell för mänskligt beteende i gällande analyser identifieras. Målet är att resultatet kan leda till rekommendationer om vidare forskning och utveckling av området.

1.4 Avgränsningar

Detta är ett examensarbete för civilingenjörsprogrammet System i teknik och samhälle och motsvarar 20 akademiska poäng, d.v.s. 20 veckors arbete.

Riskanalyser och analyser för mänsklig tillförlitlighet är ett mycket brett område. Detta arbete är inriktat på analyser som syftar till att bedöma sannolikheten för mänsklig tillförlitlighet under den begränsade period som kallas för avställning och specifikt den årliga planerade avställningen kallad revision. Det är de grundläggande antagandena och förutsättningar för dessa analyser som står i fokus.

Analyserna för mänsklig tillförlitlighet är vidare en del av omfattande probabilistiska säkerhetsanalyser (PSA). PSA genomförs både för drifttillstånden effektdrift och

avställning, samt i tre olika nivåer. De tillgängliga analyserna täcker den första nivån, där frekvensen för härdskada beräknas. Analyserna täcker inte in risken för att en sådan olycka skulle kunna leda till radioaktiva utsläpp utanför den inneslutning som härden är inbyggd i eller ut till omgivningen (nivå 2 och 3). Analyserna täcker vidare endast fel som kan uppkomma under en planerad avställning, d.v.s. den så kallade revisionsperioden, och inte de olyckssekvenser som kan uppstå under en oplanerad avställning, som ju i sig beror på en inträffad incident under effektdrift.

Detta arbete har inte som ambition att i detalj beskriva eller jämföra olika teoretiska, generella HRA-metoder. Det är i stället de teorier om mänskligt beteende som ingår i metoder och hur de används för avställning i de granskade analyserna som är av intresse. För en jämförelse av befintliga HRA-metoder hänvisas i stället till den av U.S. Nuclear Regulatory Commission publicerade rapporten *Evaluation of Human Reliability Analysis Methods against Good Practices* (NUREG-1842) samt till utredningsrapporten för SKI, *Riskanalyser ur ett MTO-perspektiv,* som slutförts under perioden för detta examensarbete (Roos, 2007).

Arbetet i denna undersökning har bland annat gått ut på att granska utvalda genomförda och pågående avställningsanalyser. Urvalet består av en pågående eller avslutad analys för vart och ett av de tre svenska kraftverken (Forsmark, Oskarshamn och Ringhals) i form av metodbeskrivningar och rapporter för den genomförda analysen. De olika analyserna benämns Avställningsanalys A, B och C (ej kopplat till uppräkningen av verken ovan). Märk också att syftet med denna rapport varken är att jämföra eller värdera de olika verkens analyser, utan de utgör exempel på hur HRA-metodiken tillämpas. Omfattningen av examensarbetet och genomgången av analyser har även medfört att endast de fyra första stegen i processen har granskats (se kapitel 5.2 samt 7.1 – 7.4).

1.5 Begrepp

Ett antal grundläggande begrepp för kärnkraftssäkerhet förekommer i rapporten. En förklaring och definition av de begrepp som inte beskrivs närmare i den löpande texten följer här.

Barriär: fysisk inneslutning av radioaktiva ämnen (SKIFS 2004:1)

Anm. Begreppet barriär används även för andra tekniska, administrativa och mänskliga aktiviteter som syftar till att förebygga och förhindra eller, efter en inträffad händelse, lindra konsekvensen av tekniska fel eller mänskliga handlingar som får oönskade konsekvenser. Exempel på en administrativ barriär är en instruktion som styr hur och i vilken ordning uppgiften skall utföras.

Barriär-analys: En typ av systematisk analys som genomförs:

a) för att identifiera de barriärer som kan förhindra eller begränsa ett händelseförlopp,
b) av de organisatoriska, administrativa och tekniska åtgärder som skulle ha kunnat stoppa en händelsesekvens (MTO),

c) för att identifiera de komponenter vars felfunktion kan förhindra barriärskyddande funktioner (inom PSA).

CCF: Common Cause Failures;
Fel som uppträder i två eller flera system eller komponenter på grund av en specifik, gemensam, händelse eller orsak.

Djupförsvar: Tillämpning av flera överlappande nivåer av teknisk utrustning, operationella åtgärder och administrativa rutiner för att skydda anläggningens barriärer och vidmakthålla dess effektivitet, samt för att skydda omgivningen om barriärerna inte skulle fungera som avsett. (SKIFS 2004:1)

Drift: Alla aktiviteter som utförs för att kunna använda en anläggning som förutsatts. Driftövervakning, underhåll, bränslebyte, kontroller och andra aktiviteter ingår i begreppet drift.

Effektdrift: Den del av säsongen då kärnkraftsanläggningen producerar och levererar elektricitet.

Human Factors: De områden där kunskap om mänskliga funktioner och förutsättningar behöver beaktas för att säkra en livslång säkerhet och effektivitet i ett system eller en organisation. (RSSB, 2006) Till detta räknas ex. frågor om ergonomi och gränssnitt, men även om organisation och säkerhetskultur.

Incident: En mindre händelse med mindre allvarliga konsekvenser.

Kognitiv: Avser intellektuella funktioner såsom tänkande, varseblivning, minne m.m. Kognitionsvetenskap studerar hur information representeras och bearbetas i den mänskliga hjärnan och hur detta kan modelleras (NE).

MTO: Systemperspektiv med fokus på samverkan mellan Mänskliga, Tekniska och Organisatoriska faktorer, ett helhetsperspektiv på säkerhet.

Olycka: Inom kärnkraft definieras en radiologisk *olycka* som en uppkommen brist i en barriär eller annat förhållande som medför spridning av radioaktiva ämnen, eller som ger upphov till stråldoser, utöver vad som är tillåtet vid normaldrift (SKIFS 2004:1).

System: Begreppet system avser en avgränsning av ett studieobjekt. I denna rapport specificeras om det är det tekniska systemet som avses, eller om det är det *sociotekniska systemet*, d.v.s. ett system bestående av både det tekniska systemet och samspelet med omgivande miljö/organisation och människor.

Transient: Sammanfattande benämning för händelser som leder till obalans mellan tillförd och bortförd värmeeffekt i reaktorn.

2. Kärnkraft och säkerhetsanalys

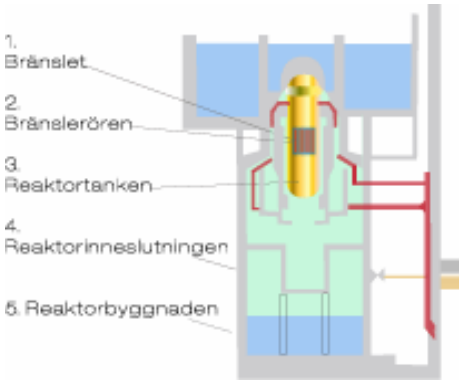
2.1 Kärnkraft i Sverige

Nästan hälften av Sveriges totala elproduktion kommer från kärnkraften. Sveriges första reaktor, R1, startades 1954 i ett bergrum i centrala Stockholm. Det var en forskningsreaktor med en maximal effekt på en megawatt. Idag finns det tio kraftproducerande reaktorer på tre platser i Sverige med en sammanlagd kapacitet på ca 9234 megawatt (antal reaktorer per plats inom parentes); Forsmark (3), Oskarshamn (3) och Ringhals (4). Sju av dessa är kokvattenreaktorer medan tre av Ringhals reaktorer är av tryckvattentyp. Kärnkraftverket i Barsebäck stängde sina reaktorer 1999 och 2005. (Om inget annat anges är denna och följande information i detta kapitel hämtad från; www.ski.se 2006-12-13)

En gång per år stängs de svenska kärnkraftverken av från tillståndet då el produceras, *effektdrift*, för bränslebyte och underhåll under en planerad så kallad *revisionsavställning*. Revisionen pågår i ungefär tre veckor och då byts den del av bränslet i reaktorhärden som är förbrukat ut, vilket utgör ungefär en femtedel av den totala mängden bränsle i drift. Under revisionen görs också underhållsarbeten då reparationer och kontroller samt införande av förbättrade tekniska lösningar kan ske. Många av dessa arbeten kan inte göras när reaktorn är igång eftersom strålningsnivån då är för hög. Efter avslutad revision kontrolleras att alla säkerhetssystem fungerar som de ska genom att en mängd prover utförs, t.ex. för att försäkra sig om att reaktorinneslutningen är tät. Slutligen startas reaktorn igen.

Även andra orsaker kan leda till en *avställning*. Incidenter, mindre händelser då något sker men konsekvenserna inte är så allvarliga, och större fel, olyckor, kan leda till så kallade snabbstopp. Även detta medför att rektorn stängs av, för att möjliggöra kontroller av vad som gått fel, åtgärder av detta och återgång till effektdrift på ett säkert sätt. Analys av denna typ av avställning ligger dock utanför ramen för denna rapport.

Ansvaret för säkerheten ligger enligt kärntekniklagen helt på den som har tillstånd att driva en kärnteknisk anläggning. Statens kärnkraftsinspektion (SKI) anger i föreskrifter vad detta ansvar innebär och kontrollerar att tillståndshavaren tar sitt ansvar. En viktig säkerhetsaspekt utgörs av barriärtänkandet, där fysiska och administrativa funktioner skall begränsa eller förhindra en olycka. Figur 1 exemplifierar detta med hjälp av de huvudsakliga fysiska barriärerna för ett kärnkraftverk.



Figur 1. De fem fysiska säkerhetsbarriärerna

Enligt SKI:s författningssamling ”*skall säkerheten fortlöpande analyseras och bedömas på ett systematiskt sätt*” (SKIFS 2004:1, 2 kap 10§). Detta skall ske med både deterministiska och probabilistiska metoder. Kontrollen av dessa analyser utförs med avseende på att ”*tillämpliga säkerhetsaspekter är beaktade, och att tillämpliga säkerhetskrav på anläggningens konstruktion, funktion, organisation och verksamhet är uppfyllda*” (SKIFS 2004:1, 4 kap 3§). I följande kapitel beskrivs grunderna för vad säkerhetsanalys och de olika metoderna för detta innebär.

2.2 Säkerhetsanalys

Säkerhetsanalys, även kallat riskanalys, är en systematisk procedur att analysera tekniska system för att identifiera och utvärdera risker, faror och kännetecken för säkerheten i systemet. Enligt en standard som presenteras av International Electrotechnical Commission innebär riskanalys att systematiskt använda tillgänglig information för att identifiera risker och faror samt för att beräkna denna risk för individer eller populationer, egendom eller miljö. (Harms-Ringdahl, 2001)

Risk kan definieras på olika sätt. Den definition av begreppet som används inom de analyser som denna studie omfattar är (Harms-Ringdahl 2001, s. 36):

$$risk = frekvensen\ för\ att\ en\ händelse\ inträffar \times konsekvensen\ för\ en\ specifik\ farlig\ händelse$$

I formeln är orden *frekvens* (hur ofta händelsen väntas inträffa) och *konsekvens* (hur händelsen påverkar systemet och/eller dess omgivning) de viktiga begreppen.

En riskanalys kan beroende på syfte utföras på olika sätt och ge olika typer av resultat. En *kvalitativ* riskanalys går ut på att värdera om systemet möter de krav som ställs enligt lagar, regler och standards, samt om hänsyn tas till ergonomi och andra designkriterier som påverkar säkerheten, positivt eller negativt. Resultatet blir en beskrivning av hur olyckor kan ske och hur de kan förebyggas med hjälp av bättre verktyg, gränssnitt och rutiner. I en *kvantitativ* riskanalys beräknas sannolikheten att en viss olycka sker och en skala av möjliga konsekvenser värderas. Det kvantitativa värdet kan sedan användas för att avgöra om risken är acceptabel för det aktuella systemet. Detta ger alltså sannolikhetstal som kan lyfta fram riskfyllda system och dessutom användas för en direkt jämförelse mellan analyser och system. (Harms-Ringdahl, 2001) Båda dessa typer av riskanalys är av intresse för denna rapport, då de används för att beskriva och avgränsa de analyser som granskas.

Den grundläggande orsaken till att genomföra säkerhetsanalyser är alltså att förebygga olyckor. I förlängningen innebär det också ekonomiska fördelar, då det oftast kostar mindre (i monetära termer) att utföra analyser och genomföra de förbättringar som analysen rekommenderar, än att hantera de kostnader som en allvarlig olycka kan medföra. (Harms-Ringdahl, 2001) Säkerhetsanalyser är extra viktiga i branscher där konsekvenserna av en olycka kan innebära stora kostnader för människorna, samhället och företaget. Kärnkraftsbranschen är en urtyp för detta.

2.2.1 Deterministisk säkerhetsanalys

Säkerhetsanalyser kan vara deterministiska eller probabilistiska. Deterministiska analyser används vanligen då grunden för en viss design värderas, t.ex. om den klarar vissa typer av olyckor eller för att beräkna kraven på systemets kapacitet under olika drifttillstånd. (Knochenhauer, 1996) Enligt SKI:s föreskrifter skall kapaciteten hos en anläggnings barriärer och djupförsvar att förebygga radiologiska olyckor, och lindra konsekvenserna om olyckor ändå skulle ske, analyseras med deterministiska metoder innan en anläggning uppförs och tas i drift (SKIFS 2004:1). Med andra ord används en deterministisk analys vid utvärdering av förutsättningarna för en konstruktion eller en analys (Hallman, Knochenhauer, Nyman, 2003).

Den deterministiska säkerhetsanalysen försöker förutse störningar som kan inträffa. I analysen hanteras varje barriär var för sig så att de ska klara dessa möjliga störningar. (www.ski.se 2006-11-29) De genomförda deterministiska analyserna har gett grund för konstruerade barriärer i djupförsvaret. De utgör även avgränsningen för en probabilistisk analys och dess säkerhetskriterier.

2.2.2 Probabilistisk säkerhetsanalys

Den probabilistiska säkerhetsanalysen (PSA) gör det möjligt att utvärdera både hur allvarligt ett tillstånd är samt att identifiera och prioritera möjliga förbättringar (Knochenhauer, 1996). Analysen används för att jämföra barriärer och värdera deras styrka. (Hallman et. al., 2003)

PSA är en sannolikhetsbaserad analys och ett sätt att betrakta ett kärnkraftverks barriärer och hur de fungerar i samband med olika störningar och missöden i en och samma analys. Därför anses sådana analyser ge en helhetsbild och möjlighet att fånga upp fel som påverkar varandra, så kallade Common Cause Failures (CCF). (www.ski.se 2006-11-29)

Enligt SKI:s författning ska en kärnkraftsanläggning, förutom en deterministisk analys, analyseras med probabilistiska metoder för att ge en så allsidig bild som möjligt av säkerheten. (SKIFS 2004:1, 4 kap 1§) I nästa kapitel följer en närmare beskrivning av de viktiga beståndsdelarna i PSA. De är av betydelse för förståelsen av denna rapport, då samtliga de granskade analyserna av mänsklig tillförlitlighet ingår i en PSA, vilket medför att analysernas omfattning och fokus påverkas av den övergripande analysens.

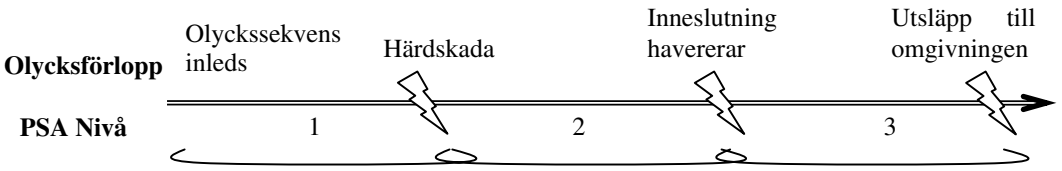
2.3 PSA

Enligt ovanstående kapitel ställer den granskande myndigheten SKI krav på att säkerheten vid de svenska kärnkraftsanläggningarna analyseras med probabilistiska metoder. Probabilistiska säkerhetsanalyser har utförts för svenska kärnkraftverk sedan mitten av 1970-talet och de probabilistiska analyserna har ökat i användning sedan 1980-talet och utgör idag en etablerad metod för att analysera säkerheten (Knochenhauer, 1996). En PSA syftar till att identifiera felkombinationer som innebär att samtliga säkerhetsbarriärer slås ut. Resultatet uttrycks som frekvensen för härdskador eller radioaktiva utsläpp. (Hallman et. al., 2003)

PSA klassificeras enligt nivå och drifttillstånd. Inom kärnkraft delas analysen in i tre nivåer

och omfattningen ökar beroende på vilken slutlig risk som beaktas. (Hallman et. al., 2003) Detta illustreras i figur 2.

- *Nivå 1*: Frekvensen för härdskada beräknas. Detta innebär att tänkbara missödessekvenser identifieras samt att sannolikheten för att de inträffar beräknas. I resultatet ingår också en uppskattning av den totala frekvensen för härdskador.
- *Nivå 2*: Frekvensen för radioaktiva utsläpp utanför reaktorinneslutningen utgör riskmått. Dessutom ingår en analys av härdsmältningsförloppet och hur inneslutningen klarar detta, vilket resulterar i beräkningen av storleken och frekvensen för radioaktiva utsläpp.
- *Nivå 3*: Frekvensen för omgivningskonsekvenser av radioaktiva utsläpp beräknas. I analysen ingår dessutom hur radioaktiva ämnen sprids i omgivningen samt en uppskattning av strålningsdoser till befolkningen.



Figur 2. Omfattning och nivåindelning för PSA

En PSA av nivå 1 och nivå 2 för samma kraftverk kommer att leda till delvis olika slutsatser eftersom omfattningen är olika, d.v.s. olika definition av sluttillståndet (frekvensen för härdskada eller radioaktiva utsläpp) ger utslag på olika komponenters riskbidrag. Det beror på att det vanligen inte är samma händelsesekvens som har störst betydelse exempelvis för frekvensen för härdskada (nivå 1) som för frekvensen för radioaktiva utsläpp (nivå 2 och 3). (Knochenhauer, 1996)

Den andra parametern i klassificeringen av probabilistiska säkerhetsanalyser är de drifttillstånd som analysen omfattar, *effektdrift* och *avställning*. En PSA för avställning kallas också SPSA från den engelska benämningen Shutdown Probabilistic Safety Analysis. Begreppet avställning kan delas upp ytterligare i varm avställning, kall avställning, nedgång från och uppgång till effektdrift. (Knochenhauer, 1996) De olika stegen karaktäriseras av att kärnkraftsanläggningens egenskaper varierar med exempelvis härdens temperatur och strålningsnivå. De granskade analyserna i denna rapport ingår alla i en avställningsanalys (SPSA) för nivå 1, varför arbetsgången och viktiga begrepp för en PSA på denna nivå beskrivs närmare.

2.3.1 PSA nivå 1

Syftet med en PSA nivå 1 är att skatta säkerhetsnivån genom att identifiera vad som kan utgöra risker för härdskada, identifiera vilken typ av händelser som kan leda till en härdskada samt att identifiera tekniska system, objekt, komponenter och mänsklig växelverkan som är viktiga för säkerheten. Resultaten skall bland annat tillämpas för att identifiera förbättringsområden samt att använda resultaten vid ändringar av anläggningen och för driftrelaterade frågor. (Hellström, 2004)

Metodiken för PSA kan beskrivas med fyra grundbegrepp (Hallman et. al., 2003), som även är av betydelse för arbetsgången och innehållet i analysen av mänsklig tillförlitlighet. Figur 3 visar även hur begreppen hänger ihop i analysprocessen.

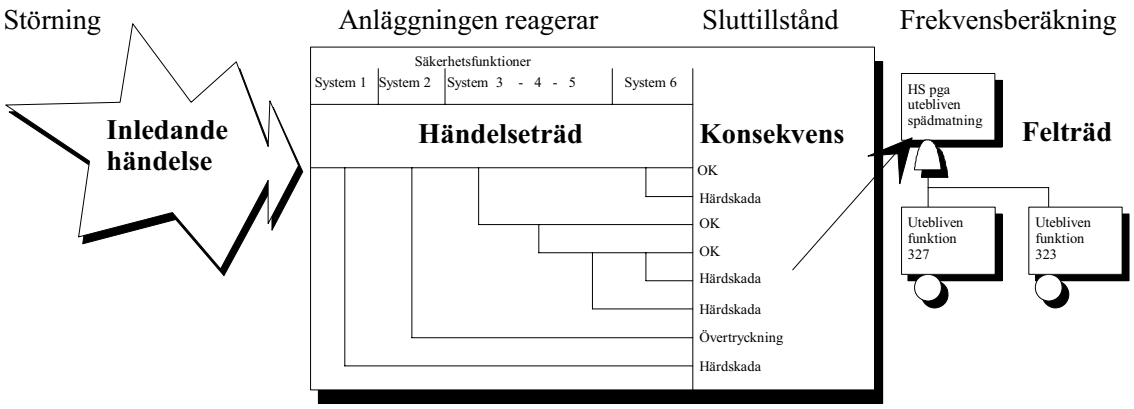
Den *inledande händelsen* kallas det missöde eller den störning som ses som startpunkten för en olyckssekvens. Händelsen är av sådan omfattning att den kräver att anläggningen stängs av och ställer därmed krav på säkerhetssystemens funktion för att kontrollera reaktivitet, säkerställa härdens kylning, etc. Analysen av inledande händelser omfattar tre steg:

- *Identifiering* av händelser som kan leda till ett oönskat sluttillstånd. Detta sker genom granskning av anläggningens konstruktion och drifterfarenheter samt av annat relevant underlag, exempelvis internationella guider eller PSA för liknande anläggningar.
- *Kategorisering*; i detta steg bestäms de anläggningsspecifika effekter som fås efter de olika inledande händelserna, och händelserna grupperas på ett sådant sätt att inledande händelser med likartad anläggningspåverkan grupperas tillsammans.
- *Kvantifiering*; frekvenser för inledande händelser bestäms.

Det andra begreppet, *händelseträd*, beskriver anläggningens reaktion på en störning. I händelseträden beskrivs alternativa möjligheter att uppfylla säkerhetsfunktioner. Analysen skall identifiera samtliga möjliga händelsekedjor (sekvenser) efter en störning. I händelseträdet visas vilka händelser eller handlingar som måste lyckas för att målet för systemet skall uppnås. Motsatt kan man då säga att det redovisas vilka händelser som måste misslyckas för att ett haveri skall inträffa.

Begreppet *konsekvens* beskriver sluttillståndet för varje sekvens. Sluttillståndet för PSA nivå 1 är antingen ett stabilt läge (OK) eller en härdskada (HS).

Felträd är ett sätt att modellera de olika sekvenser man identifierat och används för att avbilda systemfunktioner. I felträden visas både säkerhetssystemens uppbyggnad och deras möjliga felfunktioner. Resultatet blir en logisk modell som används för att beräkna frekvensen för de sekvenser som konstaterats medföra allvarliga konsekvenser. Utgångspunkten för felträdet är den oönskade händelsen, här benämnd topphändelse. Trädet byggs på nedåt, bakåt i händelsekedjan med de händelser som kan påverka utfallet. De händelser som kommer längst ner i modellen är då de identifierade inledande händelserna med sina felfrekvenser. Utöver detta ingår möjliga sätt att påverka händelseförloppet och återställa systemet (även kallat *recovery*).



Figur 3. Översiktsbild över PSA-metodik

Efter slutsatserna dragna i felträdsanalysen (d.v.s. de beräknade frekvenserna för att ett fel inträffar) görs en analys av resultatet som ofta inkluderar osäkerhets- och känslighetsanalyser (Knochenhauer, 1996). Avsikten är i första hand att utvärdera osäkerheter i PSA-modellen. Osäkerhetsanalysen ger svar på hur känsligt analysresultatet är för osäkerheter i parameterdata. Känslighetsanalysen genomförs med avsikt att värdera osäkerheter i exempelvis systemkrav, d.v.s. hur känsligt systemet är för olika typer av händelser. (Hellström, 2004)

I en fullständig probabilistisk säkerhetsanalys ingår alltså att, utöver de möjliga tekniska felfunktionerna, identifiera vilka mänskliga handlingar som kan leda till negativa konsekvenser. Detta kallas för analys av mänsklig tillförlitlighet eller Human Reliability Analysis (HRA).

2.4 Utvecklingen av HRA

Analys av mänsklig tillförlitlighet är ett relativt sett ungt forskningsområde. Den första probabilistiska studien för ett kärnkraftverk genomfördes på 1960-talet. Föregångare var kvantitativa bedömningar av mänsklig påverkan på militära system där en ökad komplexitet i de tekniska systemen ledde till styrningsproblem. Ett behov uppstod att studera ergonomi, tillförlitlighet, styrbarhet och upprätthållande av det tekniska systemets syften och egenskaper. En viktig drivkraft för utvecklingen av analyserna var att praktiskt kunna tillämpa denna kunskap. (Pyy, 2000)

År 1975 publicerades en stor probabilistisk säkerhetsanalys, inklusive en mänsklig tillförlitlighetsanalys kallad WASH-1400. Syftet med rapporten var att göra en realistisk uppskattning av kärnkraftens risker för att kunna jämföra dem med redan existerande risker som samhället och dess individer utsätts för. Resultatet skulle vidare kunna användas för att hjälpa samhället att besluta om framtida satsningar på kärnkraft. Rapporten bidrog med en insikt om den stora betydelsen av fel vid mänskligt handlande. Den tog dock inte hänsyn till anläggningsspecifika egenskaper, utan bestod av en studie av två reaktorer och drog generella slutsatser från dem. (NUREG-75/014)

Hollnagel (2005) beskriver hur utvecklingen av HRA starkt påverkades av olyckan vid

Three Mile Island år 1979. Ett stort antal HRA-metoder växte fram under 1980-talet. En av de metoder som har fått störst genomslag, THERP (Technique for Human Error Rate Prediction) publicerades år 1983. Teorier och metoder ur denna används som grund även i dagens analyser. Utvecklingen och forskningen var under denna tid mest inriktad på olika tekniker för *kvantifiering* av mänsklig tillförlitlighet, men har under 1990-talet gradvis skiftat tyngdpunkt till att fokusera mer på *identifiering* av möjliga mänskliga felhandlingar (Kirwan, 2005).

Den utveckling av HRA som Kirwan beskriver med mer fokus på identifiering av mänskliga felhandlingar inom HRA har lett till metoder som kommit att kallas andra generationens HRA. En sådan metod är Hollnagels metod Cognitive Reliability and Error Analysis Method (CREAM), som tillsammans med THERP beskrivs närmare i kapitel 5.3.

Denna bakgrund har syftat till att skapa förståelse för och ge en introduktion till det sammanhang som analys av mänsklig tillförlitlighet vid avställning genomförs i inom kärnkraftsbranschen, d.v.s. inom ramen för en probabilistisk säkerhetsanalys. I kommande kapitel sker en fördjupning i vad en avställning innebär, hur mänskligt beteende kan modelleras och analyseras inom ramen för en avställningsanalys samt hur detta beskrivs i tillgängliga metoder för HRA. Nedan följer det avsnitt som bemöter det första av syftets frågeställningar, hur avställningsperioden kan karaktäriseras och definieras.

3. Beskrivning och analys av revisionsavställning

3.1 Avställningsperiodens karaktär

Ett kärnkraftverk ställs av för revision en gång per år, ett tillfälle då gammalt bränsle byts ut och underhåll utförs. Då en avställd reaktor kostar mycket i form av uteblivna intäkter från elproduktion, är detta en period då stora vinster kan göras av en effektiv organisation för att nå optimalt utnyttjande av resurser i form av personal och utrustning. (Kecklund, 1998b)

En avställning för bränslebyte kan bestå av följande arbetsuppgifter (YVL 1.13, 1995):

- byte av kärnbränsle
- interna inspektioner och provning av system, komponenter och strukturer varav många aktiviteter endast kan utföras när komponenter är driftsatta (d.v.s. man kan bara testa om något fungerar när funktionen används)
- reparation av felfungerande komponenter och strukturer
- periodiskt underhåll av komponenter och strukturer
- anläggningsändringar
- myndighetsinspektion

Revisionen för kärnkraftverken förläggs under perioden april-september och pågår vanligen under ca tre veckor. Perioden karaktäriseras av planerade underhållsaktiviteter utförda i roterande 3-skift, 24 timmar om dygnet, samt att en stor andel utomstående entreprenörer utför arbeten på verket. Arbetsförhållandena karaktäriseras av stress p.g.a. hög värme, strålning och fysiskt krävande eller monotona arbetsuppgifter. Fel och misstag under detta drifttillstånd kan ha stora konsekvenser både i det direkta arbetet samt som orsak till latenta fel som påverkar systemet i den kommande produktionen. (Kecklund, 1998b) Som en jämförelse kan nämnas att arbetet under normal drift i huvudsak består av transport av använt bränsle och underhåll av utrustning samt att arbetet sker på dagtid.

Förutsättningarna för avställningsperioden, det vill säga att en mängd underhåll ska genomföras och bränsle bytas ut, förändrar alltså anläggningens karaktär, men även typen av möjliga olyckssekvenser. Under revision är reaktorinneslutningen öppen under längre perioder eftersom både människor och utrustning behöver passera. Om en incident skulle inträffa så att reaktorn förlorar sitt skyddande vatten i denna situation skulle det inte finnas någon barriär som kan hålla tätt för det radioaktiva utsläppet vid en härdskada. (Bennemo, 2005)

Ökad stress och arbetsbelastning medför ökad risk för mänskliga felhandlingar. För att kunna bedöma den övergripande risken är ett holistiskt perspektiv viktigt vid värdering av mänskliga felhandlingar (Kecklund 1998b). I NUREG/CR-6883 ges en överblick över vad som skiljer drifttillstånden effektdrift och avställning åt. I tabell 1 återges detta, med de utvalda skillnader som kan ha betydelse för modellering av mänskligt beteende för en avställningsanalys.

Tabell 1. Jämförelse av förhållanden under perioderna effektdrift och avställning. (NUREG /CR-6883)

Full effektdrift	**Avställning**	**Kommentarer**
Väl inövade, väl definierade inledande händelser.	Olika typer av inledande händelser kan inträffa.	Det kan exempelvis inträffa olyckor med kylmedelsförlust (s.k. LOCA) som kan föranledas av aktiviteter under avställningsperioden.
Fler säkerhetssystem är tillgängliga.	Olika/varierande säkerhetssystem är tillgängliga.	System kan avaktiveras för att möjliggöra genomförande av unerhåll.
Transienter är till naturen konsekventa och operatörerna mer tränade i att hantera uppkomna situationer.	Transienter är mindre konsekventa; operatörer i kontrollrum och andra har inte lika mycket träning från simulatorövningar för avställningssituationens förhållanden.	I Sverige har man börjat öva mer även på förhållanden för avställningssituationen. (Förf. kommentar)
Få variationer mellan utrustningens konfigurationer (inställningar) och förutsättningar för manövrerbarhet finns.	Fler varianter finns av utrustningens konfigurationer och förutsättningar för manövrerbarhet.	Under avställning är det mycket mer krävande att hålla reda på gällande förutsättningar. Olika verksamheter, ex. hantering av använt bränsle, är viktiga händelser.
Fel i hårdvara (rent tekniska fel) utgör den mest troliga orsaken till inledande händelser.	Mänskliga felhandlingar kan vara en troligare bidragande orsak till inledande händelser.	Mer personal, fler aktiviteter, fler ofullständiga eller sällan använda instruktioner karaktäriserar avställningsperioden.
Färre aktiviteter utförs.	Ett stort antal aktiviteter utförs samtidigt såsom tester, underhåll och reparationer.	Högre grad av komplexitet kan gälla under avställningssituationen.
Förväntade/förutbestämda inställningar/konfiguration för utrustning norm.	Olika/varierande konfigurationer för utrustning ofta normen.	Mindre frekvent utförda aktiviteter under avställning gör att variationen ökar.
Förutsägbar arbetsbelastning under normala omständigheter under full effektdrift.	Varierande, kanske oväntad, förändring i arbetsbelastning under normala avställningsperioder (t. ex. den årliga revisionen).	
De flesta aktiviteter är formellt inövade (ex. enligt ett rullande schema) och enligt en tydlig rutin/procedur.	Många av procedurerna man följer består av arbetsorder (d.v.s. beställningar på ex. ett specifikt underhåll som skall utföras), är mer skräddarsydda, mer skiftande, och har i många fall inte testats.	Instruktioner måste specificera ordningsföljden för uppgifter som skall utföras, exempelvis när och vilka ventiler som skall öppnas och stängas innan svetsningspersonal kan ges tillträde till sitt arbete. Hur tillfälliga lösningar eller modifikationer skapas för att möjliggöra vissa arbeten, inklusive vilka system som måste finnas tillgängliga, beskrivs i den arbetsorder som styr arbetet. Detta är dock inte något man vanligen övar så mycket på, till skillnad från ex. rutiner för nedgång och uppstart av anläggningen.

3.2 Analys av avställning

SPSA (Shutdown PSA) är beteckningen på PSA för avställningsperioden vid kärnkraftverk. Det internationella samarbetsorganet International Atomic Energy Agency (IAEA) ger i en rapport rekommendationer för hur en sådan analys bör genomföras. (IAEA, 2000) De anger bl.a. att en SPSA bör ha sin utgångspunkt i PSA för effektdrift för att ge en heltäckande bild av anläggningens riskbild.

SKI har vidare i en tillsynshandbok (Hallman et al, 2003) identifierat de verksamheter som kräver analys av risk för frigörelse av radioaktivitet. De delar då upp avställningsperioden i tre drifttillstånd:

- nedgång till avställd reaktor,
- avställd reaktor (benämns även kall avställning), samt
- uppgång för avställd reaktor,

där de två första punkterna vanligen sammanfaller under benämningen revision.

Historiskt sett har de risker som kopplas till det årliga underhållet och bränslebytet inte analyserats i lika stor utsträckning eller på samma sätt som riskerna kopplade till effektdrift. Länge var uppfattningen den, att en avställd reaktor i vilken den nukleära fissionen upphört, inte kunde orsaka några allvarliga strålningskonsekvenser till omgivningen. I mitten av 1980-talet gjordes studier för franska tryckvattenreaktorer som dock visade att risken för allvarlig bränsleskada under avställning var av samma storleksordning som under effektdrift. Sedan dess har flera studier tillsammans med rapporter om inträffade incidenter bekräftat detta. (Bennemo, 2005)

Avställningsanalyser genomfördes inledningsvis i Sverige som relativt enkla, kvalitativa utvärderingar av risk och de barriärer som förhindrar oönskade incidenter. Med dessa analyser var det möjligt att peka ut scenarier som kunde äventyra säkerheten om tillgängliga barriärer kom till korta eller var urkopplade. ”Barriärmetoden” kunde dock inte användas för att analysera *sannolikheten* för dessa risker. (Bennemo 2005)

Flera faktorer bidrar till risken för härdskada under avställning, exempelvis otillgängliga säkerhetsrelaterade system, mänskliga handlingar före och efter en inledande händelse och otillgängliga, passiva, fysiska barriärer. Numera görs analyser med hjälp av PSA även för avställning med en metodologi som så mycket som möjligt liknar den för effektdrift. (Bennemo 2005) Eftersom risker under effektdrift främst kopplas till tekniska fel och risker under avställning främst kopplas till mänsklig påverkan är indata till de olika analyserna väldigt olika. PSA för avställning genomförs på nivå 1 och 2, d.v.s. för risken för härdskada samt för hur mycket radioaktivitet som skulle komma ut i den omgivande miljön vid en inträffad härdskada. De flesta genomförda analyser täcker nivå 1.

Enligt ovanstående beskrivning av avställningsperioden är människans påverkan på systemet betydande, vilket också medför att analysen av mänsklig tillförlitlighet anses vara en viktig del i en SPSA. IAEA (2000) anger vad som är speciellt viktigt att ta i beaktande, vilket denna rapports andra frågeställning efterlyser. Främst gäller det att iaktta försiktighet i de kvantifieringar av mänskliga handlingar som görs, genom s.k. konservativt tänkande (d.v.s. använda en ”försiktighetsmarginal” för att inte underskatta den mänskliga påverkan). För att kunna hantera den komplexa analysen av mänsklig interaktion med det tekniska

systemet under avställning anses det vara mycket viktigt att HRA:n utförs på ett strukturerat och logiskt sätt och att HRA-specialister medverkar redan från början vid modellering av hur olyckssekvenser utvecklas. IAEA anger även att målet, oavsett vilken HRA-modell man väljer, bör vara att generera felsannolikheter som är konsistenta både med varandra och med övriga delar av PSA:n, d.v.s. de kvantitativa värden som analysen producerar måste följa den modell och den struktur som används för PSA, för att kunna ingå i denna övergripande analys.

En vanligt förekommande tillämpning är att inkludera en ”screening cycle” i HRA-processen. I denna screening läggs tyngdpunkten först på att uppnå en så komplett identifiering av mänskliga interaktioner med systemet som möjligt, samt att preliminärt använda konservativa värden för screeningen. Utvärdering av modellerna görs sedan för att ta reda på för vilka mänskliga interaktioner som en mer detaljerad analys är nödvändig och användbar, d.v.s. vilka handlingar som har störst effekt på systemets säkerhet. På detta sätt kan den största ansträngningen för att genomföra en detaljerad analys begränsas till de viktigaste interaktionerna.

Genomförande av en analys av mänsklig tillförlitlighet kräver intervjuer med personal av olika kategorier och positioner som är inblandade i planering och utförande av avställning, d.v.s. personal som arbetar med planering samt med styrning (operatörer) och underhåll av anläggningen. Detta är framför allt viktigt för att återge den aktuella anläggningens design och driftegenskaper under avställningsperioden, för att genomföra en anläggningsspecifik analys. Det är också viktigt för att få förståelse för de utförda arbetsuppgifterna samt och under vilka omständigheter de utförs. Planering, förberedelse och genomförande av intervjuer och möten gör detta till en tidsödande process både med hänseende till mantimmar och till kalendertid.

Den amerikanska tillsynsmyndigheten Nuclear Regulatory Commission (NRC) har gett ut ”Good practices for implementing Human Reliability Analysis” (NUREG-1792) med syfte att stödja utförande och granskning av mänskliga tillförlitlighetsanalyser. Nämnas bör dock att rekommendationerna utgår från en analys av drifttillståndet effektdrift. Specifika rekommendationer för olika utförandesteg av en HRA återges i kapitel 5.

Grunden för genomförandet av en analys av mänsklig tillförlitlighet för avställningsperioden, d.v.s. en HRA inom ramen för en PSA, består av modeller och antaganden för hur människor fungerar och agerar i olika situationer. De modeller för mänskligt beteende som används i dagens avställningsanalyser, samt nya teorier för hur detta kan modelleras, beskrivs i följande kapitel.

4. Modellering av mänskligt beteende

4.1 Inledning

Detta kapitel innehåller den grundläggande teorin av intresse för detta examensarbete och bemöter syftets tredje frågeställning, hur mänskligt beteende i en riskanalys för avställning kan modelleras. Modeller för mänskligt beteende, i samband med riskanalys, försöker beskriva människans grundläggande funktioner och förutsättningar för att hantera en riskfylld situation. Utgångspunkten är då människan, enskilt eller i grupp. Vid analys av risker och olyckor har en utveckling av modeller med ett holistiskt perspektiv skett – analys av det sociotekniska systemet, d.v.s. människan och tekniken i samspel och som en helhet. Utgångspunkten är då det sammanlagda systemet. Genom att studera dessa modeller för de två dimensionerna kan en identifiering ske av vilka antaganden om mänskligt beteende de granskade analyserna grundar sig på.

Som bakgrund till dessa modeller ges först en introduktion till de vetenskapsområden som utvecklats för att behandla dessa dimensioner i praktiken, MTO och Human Factors.

4.1.1 Human Factors och MTO

Human factors är ett etablerat forskningsområde, som i grunden handlar om ergonomi och förståelse för människans förutsättningar för att skapa miljöer och arbetsverktyg som uppfyller dessa krav (exempelvis gränssnitt för operatörer). En definition av begreppet human factors i samband med risk är (RSSB, 2006):

> *Alla områden där ”människokunskap” behöver beaktas för att säkra en livslång säkerhet och effektivitet i ett system eller en organisation.*

Human factors kan delas upp i två utgångspunkter, där det ena har människan eller den enskilda *personen* och dess förutsättningar i fokus, medan den andra utgår från helheten, det vill säga *systemet*. Dessa båda dimensioner interagerar med syfte att skapa säkerhet. Människan agerar i systemet och förutsättningar för detta måste ges. Olycksutredningar och säkerhetsanalyser måste därför hantera båda nivåerna samt interaktionen dem emellan.

MTO är ett systemperspektiv som fokuserar på samverkansytor mellan *Mänskliga, Tekniska* och *Organisatoriska* faktorer. (Kecklund, 1998a) MTO betonar ett helhetsperspektiv på säkerhet i en verksamhet och relationerna mellan olika delsystem snarare än enskilda delsystem var för sig. Övergripande kan MTO-området även definieras som ett perspektiv på säkerhet vars syfte är att studera hur människans fysiska, psykologiska och sociala förutsättningar samspelar med olika teknologier och organisationsformer samt att, utifrån denna kunskap, verka för ökad säkerhet (Rollenhagen, 1995)

Ovan nämndes att analys av avställningsperioden kräver ett holistiskt perspektiv. MTO står för ett sådant helhetsperspektiv, och används i denna uppsats som ett samlande begrepp för en analys med människan, tekniken och organisationen i fokus.

För både MTO och Human factors gäller alltså att man genom att studera samspelet mellan människan och systemet kan skapa bättre förutsättningar för säkerhet. Redovisningen av

den tillgängliga och för denna rapport betydelsefulla teorin utgår från dessa två dimensioner.

4.2 Personnivå – människokunskap

Problem som kan uppstå i samband med att människor interagerar med tekniska system bygger på grundläggande kunskaper om perception och kognition, något som har studerats länge inom beteendevetenskaperna. Det handlar om medvetna och automatiserade handlingar, lång- och korttidsminne, mönsterigenkänning med mera. Inga detaljer om sådan teori presenteras här, utgångspunkten är i stället Kecklunds (2007) indelning i fem stycken mänskliga behov och processer, där en del av ovanstående funktioner ingår. Därefter beskrivs teori för hur fel kan uppstå, med grund i Reasons (1990) indelning i *slips, mistakes* och *violations*.

4.2.1 Mänskliga behov och processer

Beskrivningen av följande fem processer fungerar som utgångspunkt för att kunna förstå vad som påverkar mänskligt beteende och hur detta kan påverka utfallet av olika beslut och människans prestation. Samtlig information i detta kapitel är hämtad från Kecklund (2007).

De s*ociala processerna* handlar om människors grundläggande behov av att ha kontakt och samverka med andra människor. Människor påverkar varandra, andras värderingar och attityder har därmed betydelse för det egna beteendet. Detta beteende påverkas av omgivande miljö, kultur och normer och kan även kopplas till begreppet *säkerhetskultur*, som är ett svårdefinierat begrepp, formulerat av ACSNI Human Factors Study Group (1993) som en produkt av värderingar hos individ och grupp, attityder, kompetens och beteendemönster som avgör engagemanget för, samt sättet och förmågan att skapa och upprätthålla program för organisationens säkerhet och välmående.

Biologiska processer beskriver människans förmåga till och behov av *aktivite*t för att få stimulans från omgivningen. För att vara aktiv krävs vila och *återhämtning* för att återställa systemet efter en period av ansträngning. Detta innebär att grundläggande behov som sömn (eller från det andra perspektivet, vakenhet) och mat har betydelse för människans prestation, för att återställa och skapa energi som kan användas till ny aktivitet. Även stress, som kan uppstå vid nya eller pressade situationer, kan påverka prestationen både i positiv och i negativ riktning. I en pressad situation kan måttlig stress innebära skärpt uppmärksamhet för att hantera situationen. Om tiden upplevs som för kort för att identifiera och utföra de uppgifter som krävs för att lösa situationen finns en risk att man inte beaktar alla möjliga handlingsalternativ vilket medför att beslutsfattande och handlingar kan bli ineffektiva. För lite aktivering kan innebära förnekande eller undvikande, t. ex. att man inte söker efter tecken på fara eller förnekar tecken på uppenbar fara.

När vi utför en handling vill vi ha någon form av *återkoppling* eller reaktion på det vi gör, en bekräftelse på att vi gör rätt. Återkoppling är nödvändigt för att kunna ändra ett beteende som inte fått avsedd effekt. På samma sätt är återkoppling på bedömningar och beslut viktigt så att beslutsfattaren har möjlighet att ändra beslutet.

En viktig egenskap hos människan handlar om a*npassning*. Människor är anpassningsbara och flexibla, kan lösa nya problem och hantera nya och oväntade situationer. Människor anpassar också situationen till de resurser och förutsättningar som de har för tillfället. Ett sådant exempel är att man vid tidspress kan vara mindre noggrann. Detta visar att anpassningsprocesserna är ändamålsenliga för att klara av en situation, men att de också kan leda till fel, exempelvis om den minskade noggrannheten gör att steg i arbetsuppgiften som är viktiga för säkerheten hoppas över eller utförs i fel ordning.

Den sista processen gäller *informationsbehandling*. Denna process har varit av central betydelse när det gäller utveckling av teorier inom human factors. Människor omges ständigt av en stor mängd information, som vi tar till oss (varseblivning) och bearbetar och ger mening. Ett urval sker av de sinnesintryck som tas in från omgivningen så att endast en liten del uppmärksammas och tas in i medvetandet. Baserat på dessa intryck gör människan bedömningar och fattar beslut om åtgärder. Därefter utförs de beslutade handlingarna. Möjligheten att ta till sig information och fatta beslut varierar beroende på situationen (även här kan stress påverka), men är också beroende av personens egen erfarenhet och kunskap. Under stress och tidspress kan människor hantera en mindre mängd information och ta hänsyn till färre faktorer än vid lugna förhållanden, liksom att vana användare kan hantera mer information jämfört med ovana. Hela processen påverkas också av individens attityd och motivation, men också av vilken energinivå individen har (om personen är pigg eller utmattad när informationen ska behandlas).

Dessa processer kan tillsammans användas för att beskriva ett antal mänskliga egenskaper som är av betydelse för interaktionen med ett (tekniskt) system. Människan är:

- anpassningsbar
- flexibel
- kan improvisera
- ”reglerbar”
- kan kompensera
- kan lösa nya problem, samt
- hantera nya och oväntade situationer.

Trots dessa egenskaper utför människor felhandlingar. Hur detta kan beskrivas och kategoriseras ur ett person-perspektiv beskrivs nedan.

4.2.2 Typer av fel

Rasmussen fann (Rasmussen, 1986; Rasmussen, Pejtersen & Goodstein, 1994) att de vanligaste modellerna för människans informationshantering (se t.ex. Newell, 1990) inte var tillräckliga som förklaringsmodeller när de analyserade felsökningsprotokoll från operatörer som arbetade med uppgifter där de fick använda hela sin skicklighet och sitt yrkeskunnande för att lösa problemen. Detta ledde till utvecklingen av SRK-modellen för mänskligt beteende. Ett utmärkande drag för SRK-modellen är att den har som utgångspunkt att människans kognitiva system är opportunistiskt, d.v.s. det utnyttjar den kognitiva kapaciteten på ett optimalt sätt och använder därför problemlösningsstrategier som är så enkla som möjligt och som förbrukar så lite kognitiv kraft som möjligt. Operatörerna uppvisade användning av kognitivt krävande analysstrategier endast om

situationen krävde detta. I andra fall användes enklare och mer lättillgängliga lösningar. SRK-modellen utgår från att operatörer analyserar och löser problem på tre olika nivåer – Skill, Rule och Knowledge. Detta ger stöd för idéerna om att människan i högsta grad är anpassningsbar, en effekt som inte är särskilt väl representerad i andra, mer kända modeller över mänsklig informationshantering (se t.ex. Newell, 1990).

Anpassningsbara processer kan dock, som nämnts ovan, gå fel. Reason (1990) beskriver typer av fel med avseende på relationen till ***kognitiva processer*** med grund i Rasmussens SRK-modell för mänskligt beteende. Det handlar om oavsiktliga handlingar i form av misstag (*slips* och *lapses*). Personen har haft rätt intention, men handlingen utförs inte som planerat. Det kan också innebära ett oavsiktligt igångsättande eller urkopplande av utrustning, att fel objekt för åtgärd valts eller att misslyckas med att följa en instruktion eller rutin. Det handlar alltså om fel vid själva *utförandet* av en uppgift och kan exempelvis kopplas till uppmärksamhet, då vanan att utföra en uppgift på ett visst sätt medför att man missar en förändring i förutsättningarna.

Den andra typen av misstag är en avsiktlig handling (*mistake*) som kan kopplas till *beslutet* att utföra en handling på ett visst sätt. Dessa misstag inträffar då personen missuppfattat situationen och där intentionen är felaktig, och utförs enligt den felaktiga planen. Ett exempel relevant för avställningssituationen kan vara att en felaktig diagnos av ett fel i en komponent gjorts, vilket resulterar i en lagning som inte är relevant för det felaktiga tillståndet, d.v.s. det verkliga felet åtgärdas inte.

Den sista typen är avsiktliga felhandlingar eller *regelbrott* som innebär en medveten överträdelse av en regel eller åsidosättande av säkerheten (*violation*). Det behöver inte betyda att handlingen sker med ont uppsåt, tvärtom finns oftast ”goda” anledningar, som för att hoppa över någon hindrande organisatorisk barriär. Fel inträffar när situationer inte är anpassade till eller överskrider människans kapacitet eller när människan använder anpassningsprocesser på ett sätt som inte passar i situationen.

Ett annat sätt att klassificera fel, som är mycket etablerat inom analys av mänsklig tillförlitlighet och som har ett ***tekniskt perspektiv*** och syftar på den effekt felet har på systemet, är Swain och Guttmanns klassificering i HRA-metoden THERP (se kapitel 5.3.1) (NUREG/CR-1278, 1983) och kan kopplas till utförandetypen av fel ovan (*slips* och *lapses*):

- ”Error of Omission”: utelämnande fel eller avsaknad av handling, att helt *missa att utföra* (*lapses*) handlingar för att upprätthålla anläggningens försvar (t.ex. misslyckas med att starta nödutrustning).
- ”Error of Commission”: Handlingar utöver det som krävs av situationen, som orsakar eller förstärker en onormal händelse, d.v.s. att *utföra fel* åtgärd (*slips*), åtgärder i fel ordning eller för tidigt eller för sent.

Det andra perspektivet för att beskriva hur risker och olyckor uppstår utgår alltså, i motsats till den enskilda människan eller gruppen av människor och våra egenskaper, från helheten, systemet.

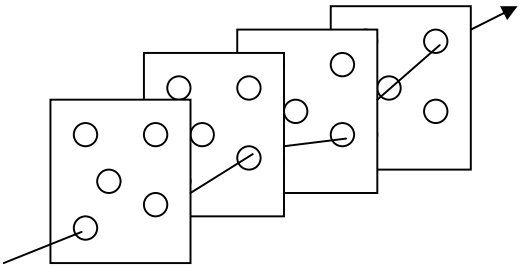
4.3 Systemnivå - modellering av risker och olyckor

Sättet att beskriva olyckor och risker på har förändrats och utvecklats över tid. Man kan skilja på linjära och icke-linjära modeller. De bygger på i grunden olika sätt att se på orsaken till att en olycka inträffar, något som beskrivs för respektive modell nedan.

4.3.1 Linjära modeller

Grunden för den första typiska olycksmodellen bygger på linjära modeller där olycksförloppet ses som sekventiellt. En enkel, linjär orsak-verkan modell, den så kallade Dominomodellen presenterades av Heinrich år 1930 (Hollnagel, Woods, Leveson, 2006). Grundantagandet för modellen är att en skada är resultatet av en *serie* händelser eller omständigheter, där den sista händelsen är själva olyckan i sig. Olyckan anses ha en identifierbar *grundorsak* antingen beroende på att en teknisk komponent havererar eller på en människas (riskabla) handlande. Detta innebär att det mänskliga felhandlandet hanteras på ”komponentnivå”. Att förebygga olyckor handlar då om att hitta dessa möjliga orsaker och eliminera möjligheten för dem att inträffa. Systemets säkerhet förbättras genom att bryta den linjära sekvensen, antingen genom att ta bort en ”dominobricka” eller genom att öka avståndet mellan brickorna och öka organisationens förutsättningar att hantera olycksförloppet. Syftet med en riskanalys enligt detta synsätt blir att finna sannolikheten att någonting går sönder (eller felfungerar) på komponentnivå, vilket är den modell som PSA:ns händelseträd bygger på, d.v.s. sannolikheten för ett haveri beroende på logiska och bestämda/fixerade kombinationer.

Utvecklingen av detta synsätt är Reasons komplexa, linjära orsak-verkan modell (även kallad ”Swiss cheese model”) från 1990. (Hollnagel et. al., 2006) Enligt denna modell är olyckor resultatet av en kombination av *aktiva* operatörsfel (osäkra handlingar) och *latenta* förutsättningar såsom försvagade barriärer och försvar (representerat av hålen i ostskivorna, se figur 4). Denna modell är mer komplex, men fokus är ändå på strukturer och komponenter och deras funktioner, snarare än det sammanlagda systemets funktion. Olyckor bör enligt modellen förebyggas genom att barriärer och försvarsfunktioner förstärks och säkerheten tryggas genom att mätningar och stickprov görs av indikatorer på systemets prestation. Faran i systemet är alltså en degradering i komponenternas funktion (organisatoriska, mänskliga eller tekniska), vilket medför att en riskanalys söker efter tendenser och sannolikheter för ett försvagat försvar, i enskilda komponenter eller i kombinationer.



Figur 4. Swiss cheese-modellen

”Swiss cheese-modellen” är den i dag rådande modellen för analys av olyckor, samt för riskanalys, och det finns etablerade metoder som bygger på detta tänkande. Även om det inte längre är det *enda* linjära skeendet som utgör den kausala strukturen, är en olycka fortfarande resultatet av en relativt enkel och ren kombination av händelser och en barriärs misslyckande är kopplat till att en enskild funktion inte fungerat. Nästa kapitel beskriver det nya tankesättet, där den sammanlagda kontexten och systemets helhet utgör grunden.

4.3.2 Icke-linjära modeller

Den komplexa linjära modellen har inte i tillräcklig utsträckning kunnat förklara alla typer av olyckor och därför finns ett behov av alternativa förklaringsmodeller. Exempelvis Perrow har i *Normal accidents* (1999) påpekat att olyckor kan ses som beroende på en kombination eller sammanhopning av omständigheter eller händelser. Detta tillfälliga *sammanträffande* av två eller fler händelsers egenskaper som påverkar varandra kan då bättre beskriva uppkomsten av en olycka. I detta sammanhang är begreppet *komplexa system* centralt. Det komplexa systemets prestation varierar, både på grund av den omgivande miljöns samt de ingående delsystemens *variabilitet*. (Hollnagel et. al., 2006)

Hollnagel (2007) preciserar vidare det komplexa systemets egenskaper. Han menar att det är naturligt att arbetssituationen i ett komplext system alltid är otillräckligt specificerat och därmed delvis oförutsägbara. Därför kan få, om några, uppgifter utföras framgångsrikt om inte instruktioner och verktyg kan anpassas till situationen. *Variabilitet i prestation är både normalt och nödvändigt.* På grund av detta kan inte problem lösas genom att eliminera denna föränderlighet, eftersom detta även eliminerar grunden för att kunna utföra ett effektivt arbete. Utmaningen är i stället att förstå föränderlighetens natur (*varför*: orsaken till förändringen, *när*: övervakning av förändringen, *hur*: möjliga konsekvenser av förändringen) och hur den kan *begränsas* när den kan bli farlig. Detta leder också till att människor och teknik inte borde beskrivas som två interagerande, enskilda komponenter, utan som att det utgör ett sammanfogat (kognitivt) system.

En olycksmodell som försöker beskriva detta är modellen för ”Funktionell resonans” (Hollnagel, 2007). Grundantagandet är då att olyckor är resultat av oväntade kombinationer (resonans eller genklang) av normal variabilitet i systemets prestation. Olyckor bör förebyggas genom att övervaka och dämpa denna variabilitet och en bibehållen säkerhet kräver en konstant förmåga att förutse och förekomma framtida händelser. En riskanalys

bör då söka efter ”Effectiveness-Thorougness Trade-Off” (ETTO), d.v.s. en lämplig avvägning mellan effektivitet och noggrannhet och var denna avvägning kan gå fel. Om effektivitet får dominera kan handlingar bli dåligt förberedda eller felaktiga, medan en alltför hög dominans av noggrannhet i arbetet kan medföra för lite tid att utföra handlingarna. Avvägningen handlar också om tillgänglig tid kontra behövd tid för att utföra en handling.

4.3.3 Typer av fel

Inom analys av mänsklig tillförlitlighet kategoriseras typer av mänskliga fel, med det tekniska systemet och kunskapen om hur människan gör fel (se kapitel 4.1.2) som utgångspunkt. IAEA (2000) gör en indelning i tre kategorier av mänskliga handlingar med utgångspunkt i hur systemet påverkas av den mänskliga handlingen och när i olyckssekvensen handlingen utförs:

Kategori A – Pre-initiator
Handlingar som sker *före* en onormal händelse och påverkar systemets tillgänglighet negativt, d.v.s. latenta fel exempelvis på grund av testning och underhåll av systemet. Handlingarna kan orsaka fel hos en komponent eller en grupp av komponenter eller efterlämna utrustning i ej manövrerbart tillstånd. Om detta inte upptäcks, blir komponenten eller komponentgruppen otillgängliga när de behövs efter en inledande händelse. Extra viktiga att analysera är de interaktioner som har potential att resultera i samtidig otillgänglighet av flera olika säkerhetssystem.

Kategori B – Initiator
Handlingar som kan *orsaka* en inledande händelse, d.v.s. som utlöser en olycka eller en incident. Dessa handlingar bidrar till frekvensen av inledande händelser i PSA-analysen. Det handlar alltså om en aktiv mänsklig handling som anses orsaka en olycka eller incident.

Kategori C – Post-initiator
Handlingar som utförs *efter* en olycka, under ett haveriförlopp och både kan förvärra eller förbättra situationen. Dessa handlingar kallas även återställande handlingar (så kallad ”recovery”), som utförs som reaktion på den onormala händelsen med syfte att mildra konsekvensen av olyckan eller incidenten. Inom denna kategori kan även de feltyper som presenterades för person-perspektivet i kapitel 4.1.2, att utföra fel åtgärd (”Error of Commission”) samt att missa att utföra en handling (”Error of Omission”) användas för att specificera felet.

Efter en inledande händelse kan operatören behöva utföra handlingar för att säkra att anläggningen reagerar på ett säkert sätt. Denna typ av mänskliga interaktioner är enlig IAEA (2000) extra viktiga under avställningsperioden beroende på att kärnkraftsanläggningen då har en lägre automatiseringsnivå. Sådana handlingar har tenderat till att bli den dominerande bidragande orsaken till frekvensen för härdskada i de flesta hittills genomförda avställningsanalyser (SPSA). Det anses därför troligt att det är viktigt att göra en realistisk utvärdering av deras felsannolikhet för att kunna göra en realistisk värdering av härdskadefrekvensen.

Det finns en rad svårigheter med att genomföra en mänsklig tillförlitlighetsanalys för SPSA för typ C-handlingar. Existerande metoder har generellt sett utvecklats för förutsättningarna

vid effektdrift då operatörerna nödgas utföra handlingar som vanligtvis är nedtecknade i instruktioner och väl inövade, inom tidsramar som typiskt varar mindre än 60 minuter. Även i de fall då det finns vägledning för procedurer tillgänglig för de handlingar som en operatör måste utföra vid inledande händelser under avställning, är informationen vanligen mindre detaljerad än i en instruktion för effektdrift. Operatörerna har även vanligen mindre övning av de situationer som kan uppstå under avställning, tidsfönstret för operatörens åtgärd är generellt sett mycket längre än för olyckor som initieras vid effektdrift. (IAEA, 2000)

4.4 Kritik och utveckling av modeller för mänsklig tillförlitlighet

Mänskligt felhandlande, eller ”human error”, är i sig ett komplicerat och omdebatterat begrepp. Vanligtvis anses det vara ett symptom på eller resultat av flera underliggande fel i det mänskliga, tekniska och organisatoriska delsystemet eller i interaktionen mellan dessa delsystem. (Kecklund 1998b, s. 8) Det finns en bred kritik mot detta begrepp, framför allt från den beteendevetenskapliga sidan, då poängen inte anses vara att den mänskliga handlingen i sig orsakar en olycka, utan snarare kan ses som startpunkten för en djupare undersökning av hur ett system bestående av människor, organisationer och teknologier både fungerar och havererar.

En alternativ syn på hur risker och faror i ett tekniskt system kan förebyggas står Vicente (1999) för. Vicente menar att de antaganden som utgör grunden för PSA, och som gör det möjligt att beräkna såväl kvantitativa som kvalitativa risker, i grunden bygger på en *normativ* modell om hur ett system och de människor som arbetar med systemet *borde* uppföra sig. Ett sådant bestämmande synsätt måste utgå från starka, väl avgränsade antaganden om vad som kan hända med systemet och med dem som arbetar med det i konkreta situationer. Vicente menar att en sådan modell bara bör användas för slutna och/eller små system eller i väl avgränsade användningssituationer. I öppna och/eller stora system (som kärnkraftverk är) är ett sådant synsätt bedrägligt eftersom de oväntade och ovanliga systemhändelserna inte går att beräkna på ett meningsfullt sätt. Den beräknade risken blir enbart en sammanfattning av vad man redan vet. Vicente är dock ingen anhängare av ett rent *deskriptivt* synsätt, d.v.s. att istället utgå från hur systemet och de som arbetar med det *faktiskt* beter sig. Detta synsätt kan förvisso ge visst stöd för insikter om vilka risker som finns eftersom man som utgångspunkt väljer den faktiska användningen av systemet.

En väl etablerad insikt (Vicente, 1999; Perrow, 1999) är att alla öppna och stora system ganska snart börjar användas på andra sätt än vad som föreskrivits av systemarkitekter och systemingenjörer. Men när det gäller det förebyggande arbetet kan även ett deskriptivt synsätt vara bedrägligt enligt Vicente (1999). Han nämner som exempel de intervjuer som gjordes med operatörerna vid Three Mile Island efter tillbudet där år 1979. Analyserna visade att operatörernas uppfattning om hur systemet fungerade inte stämde med hur det faktiskt fungerade i verkligheten. Vicente förespråkar istället ett *formativt* synsätt, en modell som specificerar de *villkor* och *krav* som måste uppfyllas för att systemet ska bete sig på ett önskvärt sätt. Övergripande mål om säkerhet, produktivitet och hälsa bryts i den modellen ned med hjälp av analyser på olika konceptuella nivåer. En viktig skillnad mellan denna modell och andra modeller är, att analys av specifika uppgifter (så kallad uppgiftsanalys, det andra steget i HRA-processen, se kapitel 5) måste föregås av en

holistisk domänanalys för att ta reda på vilka olika delar av systemet som operatörerna behöver känna till för att riskfritt kunna utföra konkreta arbetsuppgifter.

Det är även i detta sammanhang som kritik mot hela HRA-processen har sin utgångspunkt. Hollnagel (2005) menar att praktiskt taget alla HRA-metoder delar antagandet att det är meningsfullt att använda begreppet ”human error” vilket medför att det är meningsfullt att utveckla sätt att värdera sannolikheter för mänskligt felhandlande. Han refererar vidare till Woods et. al. som säger att (Hollnagel 2005, s. 159)

> ”*Attributing error to the actions of some person, team, or organization is fundamentally a social and psychological process and not an objective, technical one*.”

I sin kritik mot tillgängliga HRA-metoder nöjer Hollnagel (2005) sig med att definiera mänskligt felhandlande som en identifierbar mänsklig handling som *i efterhand* ses som orsaken till ett oönskat utfall. Han menar dock att förutsägelser om systemfel borde koncentreras på att utveckla effektiva sätt att beskriva hur prestationen hos sammankopplade system (joint human-machine system) beror på det totala systemets förutsättningar snarare än att fokusera på potentialen för mänskligt felhandlande. Det vill säga, förutsägelserna borde handla om hur det sammankopplade systemet kan förlora kontrollen över situationen, snarare än om människan kommer att göra ett isolerat fel. (Hollnagel, 2005)

Hollnagel använder två ytterligheter för att beskriva förändringen i perspektivet för human factors. Det gamla, *teknologisk optimism*, innebär att systemen anses kunna fungera tack vare att de är väldesignade, noggrant underhållna, att instruktioner är kompletta och korrekta samt att människor beter sig som de förväntas och utbildas att göra. Människor är, kontroversiellt uttryckt, en belastning, och variabilitet ett hot. Designens syfte är att begränsa variabilitet så att effektivitet uppnås. Det nya, kallat ett kognitivt systemperspektiv eller *teknologisk realism*, innebär i stället att saker går rätt tack vare människors egenskaper och möjlighet att lära sig att övervinna brister i design och tekniska funktionsfel, att vi kan anpassa vår prestation för att möta systemets krav, att vi kan tolka och tillämpa instruktioner för att matcha förutsättningarna samt att vi har förmågan att upptäcka och rätta fel som uppstår. Människor är då, motsatt till en belastning, en tillgång som är oumbärlig för moderna tekniska systems korrekta funktion.

Ett resultat av denna kritik är den tidigare beskrivna modellen för *funktionell resonans* beskriven ovan, som är under utveckling och behöver testas i praktiken för att utveckla specifika metoder.

Med teorin om mänskliga egenskaper och hur detta kan modelleras för analys av avställning beskrivs i följande kapitel de arbetssätt och metoder som idag är i bruk för mänsklig tillförlitlighetsanalys.

5. Metod för mänsklig tillförlitlighetsanalys

5.1 Inledning

I begreppet Human Reliability Analysis (HRA), analys av mänsklig tillförlitlighet, är det ordet *tillförlitlighet* som står i fokus. Begreppet definieras generellt enligt (Harms-Ringdahl 2001, s. 17):

> *Sannolikheten att ett objekt utför en begärd funktion under rådande förhållanden under en angiven tidsperiod.*

Analys av mänsklig tillförlitlighet är ett tvärvetenskapligt kunskapsområde som kombinerar (1) ingenjörsvetenskap och tillförlitlighet å ena sidan, samt (2) psykologi och ergonomi å andra sidan. Den förra kräver sannolikheter för mänskligt felhandlande (human error) som passar in i det logiska och matematiska ramverket för probabilistisk säkerhetsanalys (PSA) där kvantifiering av förväntade frekvenser för olyckor ger ett riskmått som kan jämföras med den på förhand definierade acceptabla nivån. Psykologi och ergonomi uppmanar till mer detaljerade och teoretiskt giltiga modeller för komplexiteten i mänsklig styrning och prestation, samt behovet att beakta mänsklig prestation i dess rätta kontext. (Kirwan, 2005)

HRA kan användas oberoende av den kvantifierande probabilistiska säkerhetsanalysen, men sammanhanget i detta arbete bygger på kopplingen mellan analyserna och HRA:n måste inkorporeras i PSA:n för att risken ska kunna värderas på ett korrekt sätt. (Kirwan, 2005)

Kirwan (1994, 2005) har utarbetat en tiostegs process för utförandet av en mänsklig tillförlitlighetsanalys. De övergripande målen för analysen kan dock sammanfattas i tre punkter:

- *Identifiering av mänskligt felhandlande*: Vad kan gå fel?
- *Kvantifiering av mänskligt felhandlande*: Hur ofta gör en människa fel?
- *Reducering av mänskligt felhandlande*: Hur kan man hindra att en människa gör fel eller minska konsekvensen för systemet av ett sådant handlande?

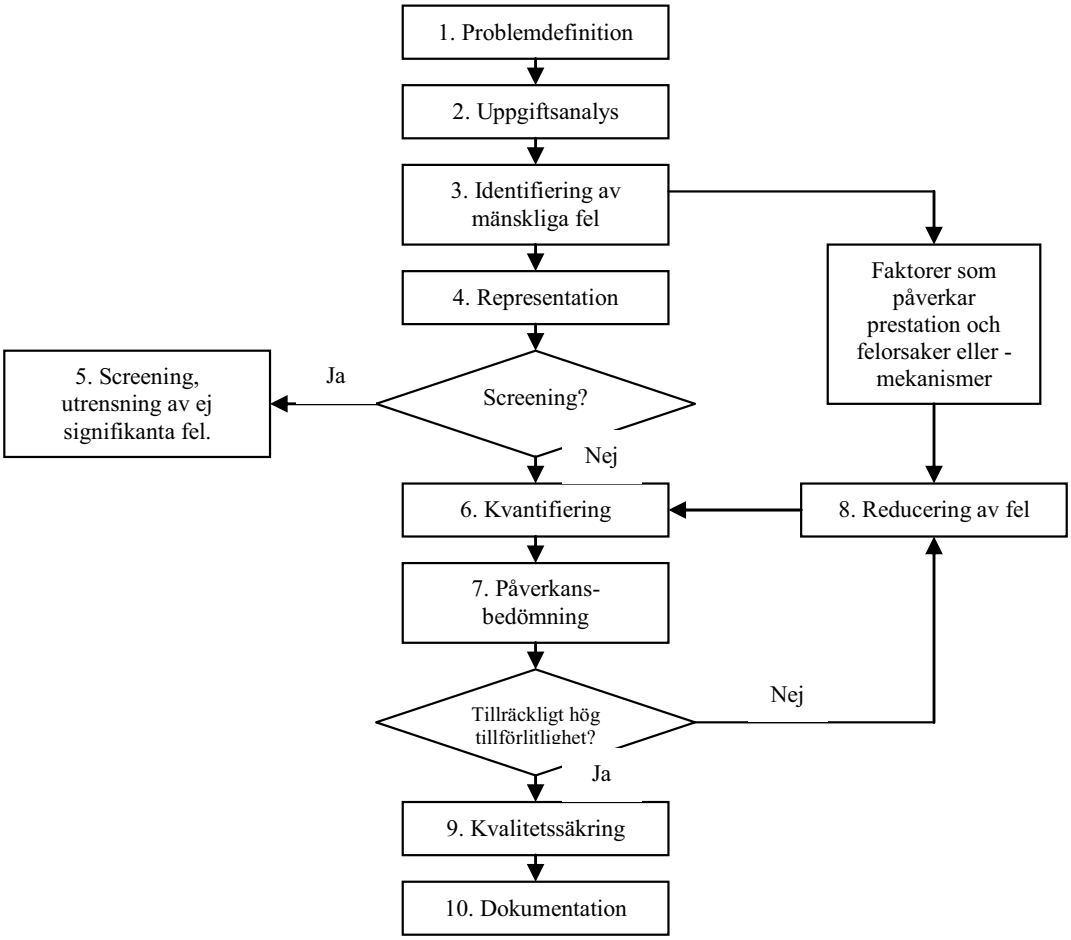
En mängd metoder har utvecklats för denna typ av analyser, men bara ett fåtal har fått fäste bland dem som utför verkliga analyser inom olika industrier. I kapitel 5.3 ges två exempel på explicita metoder för analys av mänskligt felhandlande som används inom de granskade avställningsanalyserna. I följande kapitel ges först en beskrivning av Kirwans process för mänsklig tillförlitlighetsanalys. De fyra första stegen används sedan vid granskningen av genomförda avställningsanalyser.

5.2 HRA-processen

Det generella syftet med analyser av mänsklig tillförlitlighet är att förutse mänskliga felhandlanden i en specifik uppgift samt att överväga vad som kan gå fel. (Harms-Ringdahl 2001) För att kunna använda resultatet från HRA i PSA ligger fokus på kvantifiering. Syftet blir då att beräkna sannolikheten för att en uppgift utförs på ett framgångsrikt sätt (eller att

man misslyckas).

Enligt Kirwan, som har sammanfattat processen för mänsklig tillförlitlighetsanalys, består den av tio steg (1994, 2005), se figur 4 nedan. Processen beskriver de aktiviteter som en komplett analys av mänsklig tillförlitlighet innebär. Den specifika metoden för varje aktivitet kan variera, och de flesta befintliga HRA-metoder som finns tillgängliga täcker ett antal eller alla steg i processen.



Figur 4. HRA-processen (Kirwan, 1994)

Som framgår av figuren är HRA-processen iterativ, d.v.s. en pågående utvärdering av stegen i processen gör att den förfinas med avseende på urvalet av felhandlingar och kvantifieringen av dem.

Noteras bör dock, att det finns andra tolkningar av vad en HRA-process innehåller. Det nyligen publicerade NRC-dokumentet som jämför ett antal HRA-metoder med tidigare uppsatta kriterier och ”good practice” (NUREG-1842, 2006) beskriver processen då den ingår i en PSA. Processen börjar då med att sätta samman en HRA-grupp, fortsätter med hur mänskliga felhandlingar skall identifieras och modellera dem inom PSA:n, hur en screening och kvantifiering av en nominell felsannolikhet skall genomföras, hur återställande aktiviteter (”recovery”) skall modelleras för att avslutas med dokumentation

av processen. Detta är snarlikt med processen i figuren ovan, men uppdelat i färre steg. ”Good practice” (NUREG-1792, 2005) för genomförande av en analys anges även vara att den bör utföras av en grupp med olika typer av kompetenser samt i interaktion med PSA-analytiker för varje olycksscenario och steg i analysen.

Roos (2007) har genomfört intervjuer med representanter för de svenska kärnkraftverken och har efter deras beskrivning sammanfattat arbetsgången för en HRA enligt processen *initiering*, *genomförande*, *granskning* och *åtgärder*. I initieringsfasen ingår beslutet om att det finns ett behov för en HRA, samt den interna process för beställande av ett sådant arbete, vilket vanligtvis sker av dem som arbetar med PSA. Genomförandet sker med hjälp av externa leverantörer med deltagande av personal från drift och underhåll, beroende på vilket arbete som analyseras. Slutligen sker en granskning av den genomförda analysen för att sedan redovisa resultatens rekommendationer till den aktuella anläggningen som tar ställning till vilka åtgärder som skall genomföras.

Huvuddelar i HRA är:

- identifiering av de mänskliga interaktioner som behöver tas i beaktande;
- sållning (screening) av vilka interaktioner som kan ge störst bidrag till risken;
- uppgiftsanalys för att identifiera de faktorer som primärt påverkar prestationen;
- kvantifiering, inklusive tilldelning av sannolikheter, utvärdering av osäkerheter och känslighetsanalys; samt
- om nödvändigt, identifiering av effektiva åtgärder för att reducera negativa effekter på säkerheten från mänskligt handlande, samt att förbättra utsikterna för framgång.

Nedan följer en beskrivning av processen för mänsklig tillförlitlighet som, om inget annat anges, bygger på Kirwans beskrivning (1994, 2005).

5.2.1 Problemdefinition

Enlig Kirwan innebär detta steg att bestämma problemet och dess inramning i termer av systemets mål och övergripande former av mänskligt orsakade avvikelser från dessa mål, d.v.s. att bestämma syftet med analysen.

Problemet kan definieras beroende på om problemet beaktas för sig eller som en integrerad del av en större riskanalys. Det är det andra sammanhanget som är av intresse för denna rapport, då analysen av mänsklig tillförlitlighet är en del av PSA-processen och de beaktade problemen väljs ut beroende på hur stor inverkan de, enligt PSA:n, bedöms ha för säkerheten. I dessa fall finns det fem typer av interaktioner mellan människa och system som analysen bör ta hänsyn till:

1. Fel vid underhåll eller provning som påverkar säkerhetssystemets tillgänglighet (latent fel).
2. Fel vid styrningen av anläggningen utförd av operatörer, som påbörjar en olycksekvens, d.v.s. en inledande händelse .
3. Avhjälpande ingrepp med vilken operatören kan avbryta incidenten, efter den inledande händelsen.
4. Att ställa fel diagnos och därmed utföra fel avhjälpande handling (”Error of Commission”) genom vilken operatören kan förlänga eller till och med förvärra

incidenten.
5. Reparationer vid nödläge, d.v.s. åtgärder med vilken operatören kan återställa initialt otillgänglig utrustning och system.

Detta kan kopplas till IAEA:s (2000) kategorisering av feltyper enligt kapitel 4.3.3. Interaktion 1 och 2 kan då kopplas samman med felkategori A (före en inledande händelse) respektive B (inledande händelse), medan de sista tre interaktionerna alla är olika typer av felkategori C (efter en inledande händelse).

Denna fas innebär även att identifiera vilka tillgängliga resurser som finns för analysen, d.v.s. vilken dess omfattning är, vilka beröringspunkter som finns med andra analyser (i detta fall PSA), samt om det är en ny, grundläggande analys eller en uppdatering av en tidigare genomförd HRA/PSA.

Då det är PSA som driver analysen av mänsklig tillförlitlighet bör följande aspekter beaktas:

- Vad är målkriteriet för PSA?
- Vilket är syftet med analysen: Skall åtgärder för riskreducering genomföras eller sker endast identifiering av risker?
- Är det HRA- eller PSA-analytiker som definierar omfattningen (vilka situationer/inledande händelser som ska beaktas)?

Andra aspekter som är av betydelse för detta steg i HRA-processen är vilka mål som finns för det tillgängliga systemet, både på rent teknisk nivå, samt högre, organisatorisk nivå. I slutet av problemdefinieringsfasen bör det aktuella problemet vara uttryckligen definierat i relation till det aktuella systemet. Dessutom bör en lista över vilka scenarion som är aktuella för analysen identifieras samt, för varje scenario, en övergripande lista över de uppgifter som behöver utföras för att uppnå system- och säkerhetsmål. Detta ger grunden för nästa steg, uppgiftsanalysen. (Kirwan, 2005)

Kirwans beskrivning av detta steg innebär att processen för analysen följer en sekventiell struktur. Detta steg bestämmer alltså hur mänskligt beteende i interaktion med systemet modelleras.

5.2.2 Uppgiftsanalys

Syftet med uppgiftsanalysen är att definiera den data, utrustning, beteende, planer och gränssnitt som används av operatören för att nå systemmålen samt att identifiera faktorer som påverkar mänsklig prestation inom dessa uppgifter. För att identifiera vad som kan gå fel måste man klargöra hur en uppgift utförs och resultatet av en uppgiftsanalys blir en modell över hur en uppgift utförs på korrekt sätt.

Det finns olika metoder för att genomföra en uppgiftsanalys. Sekventiell uppgiftsanalys beskriver operatörens handlingar i den kronologiska ordning de inträffar. Hierarkisk uppgiftsanalys (HTA) beaktar uppgifter i termer av de hierarkiska mål operatören försöker uppnå i en hierarkisk ”karta”. Detta innebär att ett identifierat övergripande mål delas upp i de steg som måste utföras för att nå detta mål, de olika stegen kan behövas utföras i en viss ordning, men det finns även exempel där ordningen inte är avgörande för att målet skall

uppfyllas. Tabulär uppgiftsanalys (TTA) modelleras i tabellform med målet att undersöka ergonomiska aspekter, där operatörens prestation beror på den tillgängliga informationen och operatörens kunskap, förväntningar och uppfattning om situationen.

Uppgiftsanalysen kan också ske på olika detaljnivå, beroende på det övergripande syftet med riskanalysen. Metoder för att upprätta en uppgiftsanalys är genom: observationer; intervjuer med operatörer, underhållspersonal, kontrollant/inspektörer, avdelningschef och systemdesigner; analys av rutiner och instruktioner; olycksanalyser; strukturerad genomgång av arbetsproceduren (där operatören går igenom proceduren med analytikern); och granskning av systemdokumentation (flödesscheman, processbeskrivningar m.m.). Det är kombinationen av dessa informationskällor som är viktigt, då det kan skilja sig mellan teori (instruktion) och praktiskt utförande av uppgiften, något som också är viktigt att identifiera.

5.2.3 Identifiering av mänskliga felhandlingar

Identifiering av mänskliga fel är kärnan i en analys av mänsklig tillförlitlighet. Målet är att identifiera de mänskliga handlingar som påverkar systemets prestation negativ samt hur inträffade fel kan avhjälpas. Detta steg är avgörande för analysens resultat, eftersom utelämnande av betydelsefulla felhandlingar i detta steg innebär att felet inte syns i analysen som därmed riskerar att underskatta människans negativa påverkan på systemet.

I detta steg används de olika feltyper som beskrevs i kapitel 4 som ett sätt att välja ut fel samt kategorisera felhandlingar. Uppgiftsanalysen kan användas för att identifiera de steg som är viktiga för att systemets säkerhet upprätthålls, därefter identifieras hur det är möjligt att göra fel eller avhjälpa ett fel för den aktuella uppgiften.

NUREG-1792 (2005) ger specifika råd och ”good practices” för analys av händelser före och efter en inledande händelse (typ A och typ C), men hanterar inte specifikt det mänskliga bidraget till inledande händelser (typ B-fel) p.g.a. att praxis inom PSA idag är att inte specifikt modellera detta, utan frekvensen för inledande händelser anses skapas genom att data om händelser utlösta av teknik *eller* av mänskliga handlingar sammanfogas. (Notera dock att rekommendationerna främst gäller analys av effektdrift.)

Identifiering av mänskliga felhandlingar *före* en inledande händelse (typ A), preciseras enligt NUREG-1792 som mänskliga handlingar som kan leda till att utrustning lämnas otillgänglig och bör enligt ”good practice” genom en granskning av tillgänglig utrustning, procedurer och handlingar som krediteras i PSA skall granskas. För identifiering av felhandlingar *efter* en inledande händelse (typ C) bör instruktioner för och träning av denna typ av händelser granskas, exempelvis de instruktioner som finns för onormala drifttillstånd (s.k. Emergency Operating Procedures).

Att identifiera fel på detta sätt bygger på synen på mänskliga fel som att mänskligt beteende i sig innehåller misstag. Utan misstag förlorar vi dock ett viktigt system för återkoppling på vårt beteende, något som är grundläggande för lärande. Enligt beskrivningen av mänskliga behov och processer i kapitel 4.2.1 utgör även återkoppling på bedömningar och beslut en möjlighet för beslutsfattaren att ändra på beslutet eller åtgärden (Kecklund, 2007). Detta sätt att beskriva hur fel uppstår är enligt tidigare ett av de mest kritiserade problemen inom HRA, men ingår trots detta i Kirwans beskrivning av arbetsgången för mänsklig

tillförlitlighetsanalys.

5.2.4 Representation

Efter att ha definierat vad operatörerna bör göra för att uppnå systemmålen m.h.a. uppgiftsanalysen samt att ha identifierat vad som kan gå fel är nästa steg att representera denna information på ett sätt som möjliggör den kvantitativa värderingen av de mänskliga handlingarnas påverkan på systemet. Vid en PSA-driven analys handlar det om att sätta in enskilda handlingar i det sammanhang och den modell som beskriver möjliga tekniska fel, vanligtvis i fel- och händelseträd (se kapitel 2.3.1). Dessa modeller innebär att den sammanlagda risken för alla olika ”felvägar” kan bestämmas, oavsett om mänskligt handlande är inblandat eller inte, samt vilka av dessa felvägar som bidrar mest till systemets risker. Alla fel och återställningsmöjligheter integreras i en logisk struktur som kan kvantifieras. (Kirwan 2005)

”Good practice” (NUREG-1792) för detta steg i processen anges i form av råd för hur de identifierade mänskliga handlingarna bör inkorporeras i PSA-modellen, d.v.s. i felträdet. Det är också viktigt att definiera felen så att de är specifika för den aktuella anläggningen samt för den specifika händelsesekvensen.

I detta sammanhang är det också viktigt att ta hänsyn till hur olika fel och system kan påverka varandra, via så kallade *beroenden*, samt de möjligheter till att *återställa* felet som finns. Att identifiera dessa möjligheter är nödvändigt för att få ett rättvisande kvantitativt värde, eftersom ett beroende kan öka sannolikheten för att ett fel leder till en allvarlig konsekvens, medan möjligheten till avhjälpande handlingar kan minska denna sannolikhet.

5.2.5 Screening (vid behov)

En screeninganalys identifierar vilka sekvenser eller felhändelser som tyngdpunkten skall läggas på vid en kvantifiering. Målet är att skilja ut de uppgifter som ger stort bidrag till systemets risknivå.

Detta delsteg är viktigt och nödvändigt vid en PSA-driven HRA för kärnkraftverk, då det komplexa systemets art gör det väldigt resurskrävande att utföra analyser vilket medför att förenklingar och fokus på de mest riskbidragande delarna är nödvändig (se även kapitel 3.2). En sållning leder till att endast de viktigaste mänskliga interaktionerna analyseras i detalj. (IAEA, 2000)

De flesta metoder för screening medför dock en fara för att viktiga fel och interaktioner sorteras bort. En tumregel oavsett nivå på analysen eller metod för screening bör vara att hålla kvar alla felhandlingar där minsta osäkerhet om dess påverkan finns. ”Good practices” (NUREG-1792) anger även att handlingar som påverkar redundanta och multipla system och utrustningar inte bör sållas bort. Denna process bör även itereras för specifika tillämpningar (vid en detaljanalys) samt vid uppdateringar av tidigare genomförda analyser.

5.2.6 Kvantifiering

Alla kvantifieringstekniker för mänskligt felhandlande medför en beräkning av den så kallade Human Error Probability (HEP). Detta är det kvantitativa bidraget till PSA-

analysen, d.v.s. det värde som sätts in i felträdsmodellen och som anger sannolikheten för att den aktuella uppgiften utförs på fel sätt. Sannolikheten beräknas enligt formeln:

$$HEP = \frac{antal\ gånger\ ett\ fel\ har\ inträffat}{antal\ möjliga\ gånger\ för\ felet\ att\ inträffa}$$

Trots att ett antal kvantifieringstekniker för HRA har utvecklats genom åren, finns idag ingen allmänt accepterad metod med en fast teoretisk bas. Tre ansatser för kvantifiering kan särskiljas (NEA, 2004):

1. Nedbrytning av uppgifter till en nivå för vilken det finns referensdata tillgängligt som kan justeras till uppgiftens detaljer;
2. Tidsberoende metoder, antagande att mänskliga felsannolikheter är en funktion av den tillgängliga tiden för att reagera på en händelse;
3. Metoder baserade på expertbedömningar, som använder sig av experters kunskap och erfarenhet av de analyserade situationerna.

Den största svårigheten med detta steg i processen är att hitta tillförlitliga data att grunda kvantifieringen på. Den ideala källan för data på mänskligt felhandlande skulle vara från faktiska erfarenheter av hur ofta en uppgift går fel inom den aktuella industrin, men tillgången till sådana data är begränsad. Ett alternativ kan vara att skapa sådana data med hjälp av simuleringar. En simulering kan dock aldrig ersätta vekliga erfarenhetsdata, eftersom man i en simulator inte kan skapa en helt autentisk miljö, med den stress och påfrestning som en verklig situation skapar, samt att simuleringen i sig är en begränsad version av verklighetens alla möjliga variationer av händelser och utfall. Det sätt som annars dominerar är nyttjandet av kunskapen och erfarenheten hos de personer som arbetat med olika uppgifter i det aktuella systemet, så kallade *expertbedömningar*.

De flesta kvantifieringsmetoder som används försöker på ett ungefärligt sätt ta med effekten av påverkansfaktorer (PSF), faktorer som påverkar en persons förmåga att utföra en handling. Exempel på vanligt förekommande faktorer är stress, arbetsmiljö, tid på dygnet (trötthet) och hur fullständiga instruktioner som finns tillgängliga för uppgiften. Genom att identifiera påverkansfaktorer identifieras också faktorer som kan förändras för att förbättra prestationen. Detta är ett sätt att ta med den omgivande miljöns, eller kontextens, inverkan på systemets och människans tillförlitlighet, vilket påverkar sannolikheten för att göra fel och därmed systemets säkerhet. Detta är dock ett omdiskuterat begrepp. Det anses vila på en förenklad syn på mänskligt beteende, som litar på definierade klasser av allmänna situationer vars tillämpning för specifika fall kan bli problematiskt. (NEA, 2004)

5.2.7 Påverkansbedömning

När sannolikheter för mänskligt felhandlande har kvantifierats kan systemets risk eller tillförlitlighet beräknas och jämföras med en acceptabel nivå för att se om det finns behov att genomföra förbättringar. Om så är fallet är det i första hand nödvändigt att bestämma om mänskligt felhandlande var en betydande bidragande orsak till systemets otillräckliga prestation. Detta innebär en analys av betydelsen av varje delhändelse för att topphändelsen (olyckan) i felträdsmodellen inträffar. Detta sker vanligen med hjälp av någon mjukvara.

Om slutsatsen blir att mänskligt handlande har en betydande negativ effekt på systemets säkerhet bör möjliga metoder att reducera dessa fel undersökas. I annat fall kan risknivån sänkas med tekniska förändringar. Vid förslag på åtgärder bör dock det nya systemets sammansättning och påverkan på den övergripande riskbilden beaktas. Detta steg innebär alltså en iterativ process där de vidtagna åtgärdernas effekt bör värderas enligt ovanstående metod.

5.2.8 Reducering av fel

Detta steg innebär att hantera resultaten av analysen och att identifiera och implementera möjliga åtgärder. Målet är att hitta sätt att stödja möjligheten till avhjälpande av fel, samt sätt att förbättra mänsklig prestation för att nå systemmålen så att en acceptabel nivå för systemets prestation kan nås.

Kirwan (2005) rekommenderar ett antal sätt att reducera felmöjligheter med betydande effekt på systemets risknivå:

- Förändringar i hård- eller mjukvara: skapa funktioner som spärrar möjligheten att göra fel, exempelvis genom att automatisera en uppgift.
- Öka systemets tolerans: gör systemet hård- och mjukvara mer flexibelt eller självjusterande så att en högre grad av variabilitet i operatörens agerande tillåts och systemets mål ändå kan uppnås.
- Förbättra möjligheter till återställande: öka möjligheten att upptäcka och rätta fel genom ökad återkoppling, genomgång av instruktioner och rutiner, granskning och automatisk övervakning av prestationen.
- Reducering av felets källa: genom förbättrade instruktioner, träning och design av gränssnitt eller utrustning.

5.2.9 Kvalitetssäkring och dokumentation

Kvalitetssäkring handlar om att säkerställa att analysen når de avsedda målen samt att säkerställa att resultaten uppnår krav på validitet och reliabilitet, både avseende kvalitativa och kvantitativa resultat. Kvaliteten av analysen innebär också att uppnå målet att se till så att det förbättrade systemet på ett tillfredsställande sätt möter systemets prestationskrav, samt fortsätter att göra det i framtiden.

Dokumentationen är viktig för att analysens genomförande och resultat ska kunna förmedlas och granskas. En väl dokumenterad analys innebär att en upprepning av analysen skall kunna ske med samma resultat. Därför är det viktigt att de antaganden, metoder, verktyg och hjälpmedel, bedömningar samt dataunderlag som analysen bygger på är väl dokumenterade. (NUREG-1792)

5.3 HRA i PSA

Förutsättningen för de granskade analyserna av mänsklig tillförlitlighet är att de är en del av en mer omfattande probabilistisk säkerhetsanalys. Den internationella samarbetsorganisationen OECD:s Nuclear Energy Agency (NEA) diskuterar i rapporten *Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants* (2004) relationen mellan de båda analyserna.

Mänsklig prestation kan ha väsentligt inflytande på tillförlitlighets- och säkerhetsnivån för komplexa tekniska system. Därför utgör HRA en viktig del av PSA, med syfte att få en förståelse för olyckssekvenser och mänskliga interaktioners bidrag till den allmänna risken. Huvudsyftena med HRA i förhållande till PSA är (NEA, 2004):

- att se till att de avgörande mänskliga interaktionerna *identifieras*, analyseras och införlivas i säkerhetsanalysen på ett systematiskt och spårbart sätt
- att *kvantifiera* sannolikheten för att handlingarna lyckas och misslyckas
- att ge insikt om hur förutsättningarna för mänsklig prestation kan höjas. Detta kan exempelvis innebära förbättringar av gränssnitt mellan människa och maskin, förbättrade instruktioner och träning, bättre anpassning mellan uppgiftskrav och mänsklig förmåga, ökade möjligheter för framgångsrika avhjälpande ingrepp, samt minimering av påverkan av beroenden mellan mänskliga felhandlingar.

I NEA:s rapport identifieras huvudsakliga svagheter i gällande HRA-metoder inom den industriella användningen av PSA. För det första menar man att metoderna är begränsade i sin representation av den kognitiva aspekten av mänsklig prestation speciellt kopplat till fel vid diagnos av ett uppstått problem (d.v.s. att förstå problemet och identifiera lämpliga åtgärder) samt beslutsfel. Det handlar både om vilka faktorer som driver de olika kognitiva processerna i specifika situationer samt hur deras påverkan på säkerheten kvantifieras. Det andra problemet med dagens analysmetoder anses vara att det förekommer signifikanta skillnader i de kvantitativa resultaten gjorda av olika analytiker, både vid användande av samma och olika metoder. Vidare utrycker rapporten att det råder en delvis överdriven tillit till expertbedömningar. Detta beror i sin tur på en brist på tillgänglig data grundat på erfarenheter av aktuella händelser som kan ligga till grund för kvantifiering. Att i tillräcklig utsträckning identifiera möjliga fel, samt att explicit representera och kvantifiera handlingar med potentiellt negativa effekter på anläggningens förhållanden, specifikt med avseende på handlingar som orsakar (d.v.s. inleder) eller förstärker en onormal händelse (så kallad *error of commission*), anges också som en brist. Dagens analyser tar vidare bara begränsad hänsyn till beroenden mellan handlingar och ingen explicit hänsyn till påverkan av organisations- och ledningsaspekter tas (även om de inkluderas i vissa så kallade påverkansfaktorer, PSF).

Dessa problem är av betydelse, eftersom den högre variabiliteten, eller osäkerheten, associerad med mänskliga handlingar, särskilt för de handlingar som utförs efter en inledande händelse, är betydligt högre jämfört med vad som är typiskt för hårdvarufel. (NEA, 2004)

Analyser av mänsklig tillförlitlighet har dock inte bara brister, utan gör enligt NEA:s rapport även nytta. Som resultat av genomförda HRA har det varit möjligt att identifiera betydande brister relaterade till mänsklig prestation. Det har bland annat resulterat i förändringar i form av nya och ändrade arbetsrutiner och instruktioner, reviderad träning och utbildning, installation av ny hårdvara och supportsystem för operatörer eller automatiserade funktioner, samt modifiering av system och deras fysiska uppbyggnad.

Utvecklingen av HRA drivs idag av behovet av nya tillämpningar av PSA och av medvetenhet om begränsningarna i nuvarande tillvägagångssätt. Följande behov identifieras av NEA (2004):

- Stora skillnader i implementering av frekvent använda metoder förekommer. Utveckling av PSA behövs för att täcka avställningssituationen. Användning av PSA för att stödja planering uppmanar till ett behov av betydande och anläggningsspecifika modeller för underhåll och testning av det tekniska systemet.
- Förvånande få försök till validering av HRA-metoder har gjorts. (Ett forskningsprojekt i Halden startades dock år 2006 i NEA:s regi med syfte att utvärdera olika metoder genom att utveckla en förståelse för nuvarande HRA-metoders exakthet, styrkor och svagheter baserat på empiriska erfarenheter. Förf. anm.)
- Förbättrad behandling av beslutsbaserade fel betonas i utvecklingen av HRA-metoder.
- Systematisk behandling av ”errors of commission” (EoC, se kapitel 4.2.2) och beroenden mellan handlingar kräver att hänsyn tas till föregående operatörsfel, inklusive deras detaljerade orsaker. Kunskap om den fulla kontexten av en handling, både vad gäller anläggningens tillstånd, men även vad gäller utvecklingen av operatörens kognitiva tillstånd, är nödvändigt. Detta skulle utöka komplexiteten av analysen väldigt mycket, men problemet skulle kunna hanteras bättre med hjälp av dynamiska, simulatorbaserade, ansatser som skulle kunna stödja hanterandet av EoC i ett längre perspektiv.
- Utveckling av hur organisations- och ledningsaspekter skall hanteras inom PSA behövs. En huvudfråga är om detta är något som bör integreras i PSA eller inte.

5.4 Exempel på HRA-metoder

I detta kapitel ges exempel på två utarbetade metoder för genomförande av en analys av mänsklig tillförlitlighet. Delar av dessa metoder används och nämns i granskade analyser. De representerar dessutom två olika typer av modellering av mänskligt felhandlande, där THERP är den mest etablerade och använda HRA-metoden med en ingenjörsmässig utgångspunkt för händelsers konsekvens och påverkan på det tekniska systemet, medan CREAM representerar en nyare syn för den andra generationens HRA, med utgångspunkt i kognitiva och psykologiska aspekter för hur fel uppstår och påverkar säkerheten.

5.4.1 Technique for Human Error Rate Prediction (THERP)

Detta är en metod som täcker hela arbetssekvensen för analys och kvantifiering av sannolikheter för mänskligt felhandlande, d.v.s. identifiering, modellering och kvantifiering samt reducering av risker. Metoden i sin helhet är mycket omfattande och resurskrävande och består av följande delsteg (Harms-Ringdahl, 2001):

1. Identifiering av systemfunktioner som är känsliga för mänskligt felhandlande
2. Analys av de arbetsuppgifter som relaterar till de känsliga funktionerna
3. Värdering av felsannolikheter
4. Värdering av mänskliga felhandlingars påverkan
5. När analysen tillämpas på designstadiet, ingår att tillvarata resultaten för ändringar av systemet. Dessa ändringar behöver sedan utvärderas vidare.

Handboken innehåller även tabeller med skattningar av felsannolikheter för olika feltyper.

Dessa sannolikheter kan påverkas med hjälp av påverkansfaktorer, d.v.s. analytikern gör anpassningar av värdena i ljuset av gränssnittets kvalitet mellan människa och maskin, den individuella operatörens erfarenhet, etc. Metoden innehåller också en modell för hur beroenden mellan handlingar kan hanteras, hur tillgänglig tid att utföra ingrepp på påverkar den sammanlagda risken samt för återställande handlingar.

5.4.2 Cognitive Reliability and Error Analysis Method (CREAM)

En grundläggande beståndsdel i modellen är att en person försöker upprätthålla kontroll över en situation. De utförda handlingarna bestäms mer av den egentliga situationen än av inre psykologiska mekanismer för misslyckande, handlingar och kontext hänger alltid ihop. En åtskillnad har gjorts mellan fyra kontrollmoder (Harms-Ringdahl, 2001):

- *Blandad kontroll (Scrambled control)*; valet av nästa handling är i praktiken oförutsägbart, oftast beroende på att situationen är obekant och förändras på oväntade sätt, när det egna tänkandet paralyseras och medvetenheten om den aktuella situationen är helt förlorad.
- *Opportunistisk kontroll*; nästa handling bestäms av den gällande situationen/kontexten snarare än av varaktiga intentioner. Personen utför mycket begränsad planering, eventuellt beroende på att sammanhanget eller kontexten inte förstås fullt ut eller för att tiden är för begränsad. Handlandet styrs vanligen av väl kända rutiner eller vanan för att utföra uppgiften eller av ett till synes styrande gränssnitt.
- *Taktisk kontroll*; detta baseras på planering och följer en mer eller mindre känd procedur eller rutin. Planeringen är dock begränsad till sin omfattning och regelmässigheten i handlingen styrs mer av liknande förutsättningar än av ett ”naturligt” agerande för den aktuella situationen.
- *Strategisk kontroll*; innebär att personen beaktar den globala kontexten och högre stående mål, d.v.s. handlingen grundar sig på ett längre tidsperspektiv. Detta ger en mer robust och effektiv prestation, men är beroende av personens kunskap och färdighet, d.v.s. av personens kompetens att utföra uppgiften.

Händelseförlopp beskrivs med hjälp av *fenotyp*, en händelses konsekvens, och *genotyp*, effektens bakomliggande orsaker. Konsekvensen av en händelse antas alltid ha orsakats av flera bakomliggande orsaker tillsammans, klassificerade enligt mänsklig, teknisk eller organisatorisk (MTO) påverkan.

I korthet baseras CREAM på principen att sannolikheten för mänskligt felhandlande beror på situation och kontext. Mänskliga felhandlingar kan inte analyseras som isolerade händelser. Sannolikheten att ett fel leder till en olycka beror på systemets funktion och tillstånd samt att förutsägelser om framtida olyckor och fel baseras på analys av och förståelse för tidigare incidenter.

Detta avslutar den teoretiska delen av denna rapport. I följande kapitel beskrivs den metod som använts för att analysera hur kunskap om avställningsperiodens karaktär och modellering av mänskligt beteende har använts i ett antal genomförda analyser av ingrepp under avställning. Därefter följer redovisningen av resultaten av granskningen.

6. Metod för granskning av genomförda avställningsanalyser

Syftet med att granska i Sverige genomförda analyser av avställning är att, mot bakgrund av ovan redovisat material, undersöka hur denna teori praktiskt har använts och tillämpats. Detta är en ansats till att koppla befintlig teori med det praktiska utförandet, för att identifiera eventuella skillnader och ge en grund för vidare utveckling av metoder för analys av mänsklig tillförlitlighet, speciellt för revisionsavställning.

Granskningen har genomförts i tre delar för de fyra första stegen i Kirwans HRA-process. Att dessa steg valts ut beror dels på att en avgränsning varit nödvändig med avseende på tillgänglig tid, samt att dessa har en stark koppling till hur mänskligt beteende modelleras i analysen.

Det första steget har inneburit en återkoppling till tidigare beskrivning av Kirwans metod för genomförande av det aktuella steget i HRA-processen (koppling till kapitel 5). Dessutom beskrivs vad som är viktigt att ta hänsyn till, med avseende på mänsklig tillförlitlighet och avställningssituationens karaktär (enligt kapitel 3).

I det andra steget beskrivs, i så stor utsträckning som möjligt, hur var och en av de aktuella avställningsanalyserna hanterar det aktuella steget i HRA-processen. Detta är i huvudsak baserat på en studie av respektive kraftverks genomförda analys, men även med ett visst inslag av informella, ostrukturerade intervjuer med personer som genomfört analys av mänsklig tillförlitlighet för revisionsavställning. För en av analyserna har endast metodbeskrivning för analysens genomförande varit tillgänglig, och inte någon rapport för det avslutade analysarbetet.

Slutligen sammanfattas resultaten i en tabell med aktuella frågeställningar samt i löpande text med de slutsatser som är möjliga att dra i förhållande till teori och det redovisade resultatet.

7. Granskning av avställningsanalyser med hjälp av HRA-processen

7.1 Problemdefinition

7.1.1 Definition och koppling till avställningsperioden

För detta steg är det av intresse att identifiera hur avställningssituationen och därmed problemet definieras. Detta påverkar vilka typer av mänskliga fel, samt i vilka system och av vilken personal som man kan förväntas hitta fel. Omfattningen av analysen bestäms också i detta steg. Redan här kan man avgöra vilken modell för mänskligt handlande som ligger till grund för analysen, men detta påverkar även metoden för övriga delsteg. Därför sker diskussion av modellering mer specifikt i kapitel 8.

Som en påminnelse kan nämnas att avställningsperioden exempelvis karaktäriseras av att olika säkerhetssystem är tillgängliga jämfört med effektdrift, att systemens gränser är mer ”flytande” då varierande och ett större antal system är avstängda för reparation och underhåll. Detta påverkar även utrustningens konfiguration och förutsättningarna för att manövrera och styra olika system. Anläggningens säkerhet påverkas även av att en lägre grad av redundans råder. Av stor betydelse är att det är en stor andel mänskliga ingrepp i anläggningen.

I detta steg skall alltså följande granskas:

- Vad är syftet och målet med analysen?
- I vilken omfattning genomförs analysen?
    - Vilka typer av felhandlingar analyseras (se även kap. 7.3)?
- Hur beskrivs det aktuella systemet för avställning?

7.1.2 Redovisning av avställningsanalyser

Avställningsanalys A

Denna avställningsanalys genomförs inom ramen för en probabilistisk säkerhetsanalys för nivå 1, riskmåttet och konsekvensen som utreds är alltså händelser som kan leda till en härdskada.

Det mest intressanta med denna analys är att den, förutom att beräkna felsannolikheter för de från PSA identifierade inledande händelserna, har som mål att göra en *kvalitativ* analys av den administrativa styrningen av avställningsperioden under revision. Mer specifikt har analysen av mänskligt felhandlande som syfte:

1. Att analysera den administrativa styrningen av en revisonsavställning.
2. Att genomföra en screeninganalys av manuella inledande händelser, barriäringrepp och recoveryåtgärder.
3. Att genomföra en detaljanalys av utvalda manuella ingrepp.

Mer specifikt har analysen av den administrativa styrningen tre syften bestående av att (a) analysera några nyckelgruppers förutsättningar för att ta fram och använda den administrativa styrningen samt ge förslag på förbättringar, att (b) ge delar av den bakgrundsinformation som behövs för att bedöma utvalda screeningingrepp (det vill säga de HRA-arbeten som är en del av PSA-modellen) samt att (c) ingå i den urvalsmängd som ligger till grund för val av detaljanalyser. Med administrativ styrning avses dokument som ger förutsättningar för arbeten i anläggningen, dokument som anger när, var och under vilka förutsättningar arbetes ska utföras och tas fram för varje revision. Ansatsen är att kvaliteten på den administrativa styrningen är starkt kopplad till hur bra förutsättningarna är för de aktuella nyckelgrupperna att utföra sitt arbete (exempelvis för planering och styrning av arbetet under revisionsperioden). Den kvalitativa analysen avser att leda till eventuella bättringsförslag för den administrativa styrningen av revisionsperioden.

Den kvantitativa analysen sker inom ramen för PSA, med en screeninganalys för att välja ut de känsligaste händelserna för vidare, detaljerad analys.

Den aktuella rapporten hänvisar till tidigare versioner, vilket innebär att analysen är en uppdatering. I denna analys är det inte bara de inledande händelser som identifieras i PSA:n som beaktas, utan även händelser som identifierats i den administrativa analysen ingår enligt delsyfte (3) ovan.

Hur definieras då avställningssituationen? Avställningsperioden har delats in i åtta faser som bestäms av tillgängligheten på system och behov av systemfunktioner under avställningen, samt hur lång tid anläggningen befinner sig i respektive fas. Vidare beskrivs skillnaderna mot effektdrift som att insatser av personal kan orsaka störningar, vissa systems tillgänglighet påverkas samt att resteffekten är lägre, vilket innebär att eventuellt andra system än vid effektdrift kan användas samt att tid för återställning är längre (t. ex. reparation av utrustning).

Den övergripande målsättningen med analysen är att kartlägga och analysera de händelser som kan inträffa under avställning samt att kvantifiera frekvensen för olika konsekvenser orsakat av fel vid avställning.

Avställningsanalys B

Det specifika syftet är att analysera mänskliga felhandlingar under kall avställning inom ramen för en probabilistisk riskanalys för nivå 1. Analysen kompletterar en tidigare genomförd förstudie för ned- och uppgång samt kall avställd reaktor, som huvudsakligen bestod av en *kvalitativ* analys av ett begränsat antal ingrepp, samt en mer *kvantitativ* analys av kall avställning för andra anläggningar vid kraftverket. Denna analys av kall avställning har vidare utgått från de händelser som identifierats i ett särskilt projekt där säkerhet under revisionsavställning varit studieobjekt och en inventering av inledande händelser under kall avställning gjorts.

Omfattningen för analysen har styrts av ovanstående projekt, vilket medfört att det främst är felhandlingar som kan ge upphov till en inledande händelse (typ B enligt IAEA:s notation) som kvantifierats. Kvantifiering har även skett för misslyckade korrigerande åtgärder *före* en inledande händelse. Analysen fokuserar inte på den administrativa styrningen av avställningsperioden, men inkluderar planeringsfel bland analyserade

felhandlingar. Även återställande handlingar efter den inledande händelsen (ingrepp av typ C) har analyserats *kvalitativt* för ett antal händelser.

Ett antal mål med uppdateringar av PSA-studierna för kraftverkets anläggningar har identifierats, vari det bland annat står att ”state-of-the-art” metodik skall tillämpas för HRA (exempelvis genom att beakta rekommendationer från NRC:s ”Good practices”, NUREG-1792, 2005). Däremot följer kvantifieringarna äldre konventioner (första generationens HRA-metodik), ”*eftersom den bedöms vara mest kostnadseffektiv relativt alla osäkerheter som ändå finns vid kvantifieringar*”. Vid behov skall även kvantifieringar kompletteras med detaljanalyser som fokuserar på kvalitativa beskrivningar av påverkansfaktorer för att kunna ta fram åtgärdsförslag. Detta har ännu inte utförts inom ramen för denna analys.

Ytterligare en avgränsning för analysen är att endast arbeten som utförs under normala revisioner ingår, vilket innebär att speciella arbeten som exempelvis anläggningsändringar av engångskaraktär och udda underhållsarbeten inte ingår. I analysen ingår inte heller så kallade kortstopp, där anläggningen tas ner till kall avställning av andra skäl än för att genomföra den årliga revisionen med bränslebyte.

Avställningssituationen beskrivs med gynnsamma omständigheter avseende risken för härdskada såsom låg effekt, lågt tryck och låg temperatur. Mindre gynnsamma omständigheter är att många arbeten pågår ute i anläggningen samt att färre barriärer innebär reducerad styrka i djupförsvaret. Vidare specificeras, i en annan del av metodbeskrivningen, att många arbeten pågår samtidigt ute i anläggningen och i kontrollrummet, att många larm kan vara aktiverade samtidigt, vilket gör att aktiverat larm inte bedöms vara en lika stark signal under kall avställning som under effektdrift.

De manuella ingreppen analyseras som en del av en screeninganalys varav ett antal ingrepp väljs ut till detaljanalys.

Avställningsanalys C

Denna analys följer till sin arbetsgång den av Kirwan beskrivna processen. Enligt den allmänna beskrivningen av problemidentifieringsfasen är detta den enda av de studerade analyserna som ingår i en PSA som täcker både nivå 1 och 2 för avställning. Omfattningen ökar dessutom då både ned- och uppgång ingår. Detta beskrivs i olika drifttillstånd bestående av varm avställning, kall avställning, statisk avställning, bränslebyte och oladdad härd då inget bränsle finns i reaktortanken vid uppgången till varm avställning. Analysen integreras med tidigare gjorda PSA för effektdrift och drifttillstånden till och från varm avställning.

Syftet med analysen anges vara att identifiera både kvalitativa och kvantitativa styrkor och svagheter för anläggningen under avställning. PSA ligger till grund för analysen och fungerar som det huvudsakliga filtret för urval och identifiering av de händelser och mänskliga handlingar som analyseras. Analysen kallas inte bara en HRA, utan för en HFA, som står för Human Factors Analysis och då inkluderar den kvalitativa delen via MTO-analys. Påverkan från administrativa faktorer och tillämpad styrning övervägs i begränsad omfattning om det kan relateras till de kritiska sekvenser och mänskliga handlingar som är utvalda för analys, i omfattningen ingår alltså inte en komplett analys av den administrativa styrningen.

Analysen har för avsikt att behandla följande typer av felhandlingar:

- Mänskliga fel som orsakar/leder till en inledande händelse inkluderat att ingen återställning sker före den inledande händelsen.
- Mänskliga fel vid återställande åtgärder under en olyckssekvens.
- Felaktiga mänskliga handlingar som leder till komponenters otillgänglighet. Exempel på sådana handlingar anges som att en komponent som ska stå i stand-by felaktigt tas ur drift för underhåll.

Data för detta steg i processen hämtas från analysen av inledande händelser och från ett studiebesök gjort av HRA-teamet på kärnkraftverket under den årliga revisionen. Baserat på information från dessa källor väljs kritiska arbetsuppgifter ut för den kvalitativa analysen.

Ett antal avgränsningar räknas upp enligt:

- Endast mänskliga handlingar som kan hänföras till den årliga revisionsperioden analyseras.
- Errors of Commission i olyckssekvenser hanteras inte.
- Sabotage inkluderas inte i analysen
- Återställande av tekniska fel tas endast med i beräkningen när det finns tillräcklig tid för reparation före en oönskad konsekvens inträffar. Som ett första antagande inkluderas inte reparation som en återställande handling.
- Beroenden mellan olika handlingar hanteras bara om beroendet ökar sannolikheten för handlande.

Ingen egentlig *analys* av administrativ styrning genomförs. En beskrivning med syfte att ge generell input till kvantifieringen av mänskliga handlingar i SPSA:n görs genom att information om viktiga administrativa faktorer samt ledningsfrågor samlas in under workshops med verkets personal. En screening tillämpas och endast de viktigaste administrativa faktorerna inkluderas i vidare analys.

De speciella förhållandena under avställning beskrivs på följande sätt. Under avställningsperioden byter operatörer kontinuerligt konfigurationen för reaktorns kylsystem för att möjliggöra underhåll, provning eller andra aktiviteter relaterade till perioden. Den ökade nivån för underhåll och provning medför också färre tillgängliga säkerhets- och stödsystem och därtill hörande provningsutrustning. Vidare beskrivs avställning som en period då automatiska kontroll- och säkerhetsfunktioner kan vara tagna ur funktion, de flesta meddelanden i kontrollrummet markerar larm, få tekniska specifikationer är tillämpbara och konfigurationsspecifika rutiner och instruktioner för nödlägen är otillgängliga. Det påpekas dock att en del av dessa brister har åtgärdats under de senaste åren, bland annat har instruktioner för nödlägen skapats.

7.1.3 Sammanfattning

I tabell 2 ges en sammanställning av ett antal viktiga punkter för problemdefinitionsfasen. Samtliga avställningsanalyser som granskats ingår i en probabilistisk säkerhetsanalys

(PSA) för nivå 1, d.v.s. det är de händelser som kan leda till en allvarlig konsekvens i form av härdskada som analyseras. Enda undantaget är avställningsanalys C som även analyserar nivå 2 (beräkning av frekvensen för radioaktiva utsläpp utanför inneslutningen, efter en härdskada). Även när det gäller de olika drifttillstånden för avställning avviker analys C, då den avser täcka kall avställning såväl som upp- och nedgång till avställd reaktor, medan de övriga analyserna endast behandlar drifttillståndet kall avställning. Detta anger alltså omfattningen för hela PSA-analyserna. Ett annat sätt att beskriva detta är att analyserna för mänsklig tillförlitlighet är PSA-drivna.

Att analyserna ingår i en större PSA, medför att målet är att identifiera risker samt att *kvantifiera* dessa, för att producera indata till PSA-modellen (d.v.s. beräkna sannolikheter som via felträdet tas med i den allmänna riskbedömningen för det analyserade felet). Trots detta märks dock skillnader i upplägg och, enligt ovan, omfattning på analysen. Detta kan delvis bero på att analyserna är anpassade till den anläggning som analyseras, men skillnaden kan även bero på att det inte finns några formella krav på vad en mänsklig tillförlitlighetsanalys skall innehålla.

Avställningsanalys A utmärker sig genom att innehålla en *analys* av den administrativa styrningen av revisionsperioden. De övriga analyserna *beskriver* till viss del den administrativa styrningen. Övrig kvalitativ analys består av att identifiera

I problemdefinitionen ingår en beskrivning av avställningsperiodens förhållanden, som överensstämmer med den bild som gavs i kapitel 3 (jämför exempelvis tabell 1 med tabell 2 nedan), även om inte varje analys beskriver samtliga punkter. Beskrivningarna kan mer ses som en bakgrund och problemformulering i ganska allmänna ordalag. (Det är även möjligt att avställningsperioden beskrivs närmare i andra delar av den sammanlagda analysen, men här kommenteras endast HRA-delen.)

Tabell 2. Sammanfattning av problemidentifieringsfasen

HRA-processen (Kirwan, 1994)		**A.**	**B.**	**C.**
Delprocess	**Frågeställning**			
1. Problemdefinition	Omfattning på PSA	PSA nivå 1, kall avställning.	PSA nivå 1, kall avställning.	PSA nivå 1 och 2, kall avställning samt ned- och uppgång.
	Målkriterium för HRA Kvalitativ/kvantitativ analys?	Kvalitativ analys av administrativ styrning av avställning. Kvantitativ analys av mänskliga inledande händelser till PSA. Övergripande mål: - att kartlägga och analysera de händelser som kan inträffa under avställning - att kvantifiera frekvensen för olika konsekvenser orsakat av fel vid avställning.	Viss kvalitativ beskrivning (planeringsfel ingår). Kvalitativ analys av typ C ingrepp. Kvantitativ analys av mänskliga inledande händelser till PSA. Kompletteras vid behov av detaljanalyser som fokuserar på kvalitativa beskrivningar av påverkansfaktorer för att ta fram åtgärdsförslag (ingår ej i denna analys).	Viss kvalitativ beskrivning. Kvantitativ analys av mänskliga inledande händelser till PSA. Påverkan från administrativa faktorer och tillämpad styrning övervägs om det kan relateras till de kritiska sekvenser och mänskliga handlingar som är utvalda för analys.
	Beskrivning av avställning	Åtta faser beroende av - tillgängligheten på system - behov av systemfunktioner under avställningen - tid i respektive fas Skillnad mot effektdrift: - insatser av personal kan orsaka störningar - vissa systems tillgänglighet påverkas - lägre resteffekt => andra system än vid effektdrift kan användas => tid för återställning längre	Endast arbeten under normal avställning ingår. Gynnsamma omständigheter avseende risken för härdskada: - låg effekt - lågt tryck - låg temperatur Mindre gynnsamma omständigheter: - många arbeten i anläggningen - färre barriärer - många larm kan vara aktiverade samtidigt	- Operatören byter kontinuerligt konfigurationen för reaktorns kylsystem för att möjliggöra underhåll, provning eller andra aktiviteter - Färre tillgängliga säkerhets- och stödsystem - Automatiska kontroll- och säkerhetsfunktioner kan vara tagna ur funktion - många larmindikeringar i kontrollrummet - få tekniska specifikationer är tillämpbara - instruktioner för nödläge vid olika konfigurationer saknas delvis

7.2 Uppgiftsanalys

7.2.1 Definition och koppling till avställningsperioden

En uppgiftsanalys går ut på att explicit definiera den information, utrustning, beteenden, metoder och gränssnitt som används av operatörer för att uppnå systemets syften, samt för att identifiera faktorer som påverkar mänsklig prestation inom dessa uppgifter, de så kallade påverkansfaktorerna (PSF) identifieras.

Avställningsperioden medför att ett stort antal uppgifter utförs och därmed kan påverka systemets säkerhet. Dessutom kan uppgifterna vara av sådan art, att de inte utförs så ofta (exempelvis sker en del underhåll med vissa tidsintervall, t.ex. vart tredje år) vilket innebär att operatörer och underhållspersonal är mindre vana vid uppgiften.

Generellt anges i analyserna att de inhämtar information om de olika händelserna från instruktioner och andra skrivna beskrivningar om de arbetsuppgifter som utförs. En annan viktig källa för information är operatörer och underhållspersonal som arbetar på kraftverken, som besitter kunskap och erfarenhet om olika situationer och systemets beteende. Dessa expertbedömningar gör även analysen mer anläggningsspecifik, det vill säga mer giltig för den aktuella anläggningen. Att beakta är dock den kritik som tidigare nämnts mot att ha för stor tilltro till expertbedömningar.

För denna del av granskningen undersöks:

- Hur analyseras eller beskrivs aktuella arbetsuppgifter?

7.2.2 Redovisning av avställningsanalyser

Avställningsanalys A

Analys av administrativ styrning:
Analysen av den administrativa styrningen förbereds genom en beskrivning av revisionsavställningen i löpande text. Utöver detta finns även flöden över arbetsgången, bestående av ett hierarkiskt schema över händelsesekvenser.

Förutsättningarna för grupperna analyseras genom att ett antal områden värderas med hjälp av frågemallar med påståenden om de olika områdena i förhållanden till krav på hur de bör hanteras i organisationen, som besvaras med bestämda intervall (stämmer fullständigt – stämmer inte alls) i fem steg:

1. Säkerhetsanalys
2. Säkerhetsgranskning/verifiering
3. Kvalitetsrelaterade aktiviteter
4. Ledning
5. Erfarenhetsåterföring
6. Human resource management
7. Personella resurser
8. Tidsmässiga resurser
9. Finansiella resurser
10. Metodresurser
11. Andra resurser
12. Integritet
13. Kompetens och erfarenhet
14. Tidsmässighet
15. Effektivitet
16. Transparens
17. Formalism
18. Kommunikationsförmåga
19. Fullständighet
20. Lärande
21. Fysiska arbetsförhållanden
22. Trötthet/vaksamhet
23. Samarbetsklimat
24. Arbetets komplexitet
25. Säkerhetskultur

1. – 6. Övergripande värderingsområden
7. – 11. Resursrelaterade värderingsområden
12. – 25. Övriga värderingsområden

Med hjälp av denna värdering fås ett medelvärde för varje område som jämförs med ett uppsatt mål. En sådan bedömning har gjorts för ett antal administrativa och styrande tjänster för revision. De olika värderingsområden har valts ut med hjälp av metoden CREAM, som bakomliggande orsaker för hur väl uppgifter under revision kan utföras.

Screening av manuella inledande händelser
För att erhålla en fullständig bild av hur sekvenserna som leder till härdskada modellerats måste enligt analysen hänsyn tas till samverkan mellan inledande händelse, barriäringrepp, möjligheter till återställande handlingar samt tekniska redundanta system. Detta är sammankopplat med PSA-modellens uppbyggnad och analysen av den.
De manuella inledande händelserna har delats upp i:

- manuellt initierad LOCA (Loss Of Coolant Accident), förlust av kylmedel
- manuellt initierad förlust av resteffektkylning
- manuellt initierad övertryckning
- manuellt initierad tappad last vid tunga lyft i reaktorhall
- manuellt initierad kall kriticitet

Kartläggningen av de olika händelserna utförs främst genom att utnyttja flödesscheman, systembeskrivningar och tidigare utförda riskanalyser. Tillsammans med ämnesområdesexperter (personer med ett antal års erfarenhet för uppgiften) identifieras sedan komponenter eller system som är av betydelse för den aktuella händelsen samt vilka typer av fel som kan leda till allvarliga konsekvenser.

Kartläggning av barriäringrepp
Med manuella barriärer avses manuellt aktiverade system som förhindrar att en händelse utvecklas till en inledande händelse, och där syftet med aktiveringen primärt är att utgöra denna barriär.

Kartläggning av barriäringrepp sker genom att utgå från oönskade konsekvenser och att från intervjuer, instruktioner och systembeskrivningar identifiera metoder som förhindrar den oönskade konsekvensen beroende på hur den uppkommer.

Kartläggning av återställande handlingar
Kartläggning av återställande handlingar (recovery) genomförs genom att beakta samtliga fall då en inledande händelse förorsakats av manuellt felhandlande. Recoverys för sekvenser orsakade av mekaniska fel beaktas i allmänhet inte, förutom om ”långa” tider finns tillgängliga (mer än 6 timmar) innan den oönskade händelsen inträffar.

Avställningsanalys B

Analys av operatörsingripanden och mänskligt felhandlande baseras på händelseträds- och systemanalyser där man kartlägger möjliga operatörsingripanden och mänsklig växelverkan som bidrar till risk. Relevanta ingripanden och felhandlanden modelleras och kvantifieras som en del av händelse- och felträdsanalysen. Detta är alltså en del av PSA-analysen, varav själva kvantifieringen kallas HRA.

Ur PSA-modellens synpunkt är ett ingrepp den helhet av handlingar eller åtgärder som personalen genomför i syfte att påverka processen för ett visst syfte. PSA-modellens ingrepp är ett slags ”super-ingrepp” som består av ett eller flera specifika ingrepp vilka analyseras och kvantifieras i HRA.

Ingreppen i HRA delas upp i tre klasser;

1. *Enkla ingrepp*, där en handling antingen lyckas eller leder till ett felhandlande d.v.s. sannolikheten att göra fel = p,
2. *ingrepp med återkopplingsmöjlighet*, där ett inledande handlande kan misslyckas med sannolikheten p1, men då det finns en chans för en återställande handling (återkoppling), som kan misslyckas om alla efterföljande barriärer felfungerar med sannolikheten p2, d.v.s. den sammanlagda sannolikheten att det leder till ett oönskat tillstånd eller händelse = p1*p2, samt
3. *växelverkan*, där personen eller gruppen måste lyckas i flera steg för att nå ett lyckat resultat och det dessutom kan finnas en möjlighet till återkoppling under vissa förutsättningar (ex. typ C ingrepp). Sannolikheten att det blir fel är då
   $P(fel) = p_1 + (1 - p_1) \times p_2 + (1 - p_1) \times (1 - p_2) \times p_3 \times p_4$

I en kvalitativ analys av operatörsingrepp av typ C beskrivs användning av instruktioner, rollfördelning och utbildning.

Identifiering av ingrepp sker m.h.a. sekvensanalyser: händelsesekvenser har diskuterats med operatörerna för att få deras bedömning om möjliga och prioriterade ingrepp.

I de tillgängliga rapporterna görs inte någon schematisk uppgiftsanalys, däremot finns en händelsebeskrivning av de inledande händelser som valts ut för analys.

Avställningsanalys C

De kritiska arbetsuppgifter som ingår i sekvenser som kan resultera i härdskada väljs ut för uppgiftsanalys. En kvalitativ analys genomförs som en detaljerad beskrivning av deluppgifter, baserat på instruktioner och drifterfarenheter.

En hierarkisk uppgiftsanalys (HTA) används, uppgifterna grupperas i kategorier och typiska/representativa arbetsuppgifter för avställningssituationen analyseras.

En tabulär uppgiftsanalys (TTA) används för att dokumentera kontexten och förutsättningarna under vilka uppgifterna utförs. I detta sammanhang identifieras de påverkansfaktorer och det stöd som finns för uppgiften.

Den huvudsakliga datakällan utgörs av besök av anläggningen, workshop med utvalda i personalen samt instruktioner och arbetsordrar (ett specifikt dokument som för underhållspersonalen anger vad som skall åtgärdas i anläggningen) som ger det administrativa stödet för avställningsperioden.

7.2.3 Sammanfattning

I tabell 3 ges en sammanfattning av analysernas användning av uppgiftsanalyser. De olika analyserna använder olika metodik för beskrivning av de uppgifter som ingår i de händelser som analyseras. Endast analys C uppger att den avser att använda de av Kirwan beskrivna typerna av uppgiftsanalys.

Trots att arbetsuppgifter för avställningsperioden inte beskrivs med hjälp av en uppgiftsanalys, används i princip samma tillvägagångssätt för kartläggning av arbetet. Det handlar om att genomföra intervjuer med berörda personalgrupper (underhåll, instrument och kontroll, operatörer m.fl.) samt att använda de instruktioner som styr dessa gruppers arbete.

Det är också viktigt att identifiera vilka ingrepp, händelser eller arbetsuppgifter som är intressanta att kartlägga. Detta görs i de olika analyserna genom att dela in manuella händelser i olika kategorier. Indelningen sker enligt modellen för PSA, där handlingarna och uppgifterna beskrivs i förhållande till de typer av fel med allvarliga konsekvenser som ska analyseras. I avställningsanalys B görs även en indelning i typen av ingrepp, om de är enkla, har återkopplingsmöjlighet eller sker i växelverkan och i flera steg. En koppling sker även till IAEA:s klassificering av fel i typ A, B och C.

Detta föregår och leder till viss del till nästa steg i HRA-processen, identifiering av mänskliga fel.

Tabell 3. Sammanfattning av steget för uppgiftsanalys

HRA-processen (Kirwan, 1994)		**A.**	**B.**	**C.**
Delprocess	**Frågeställning**			
2. Uppgiftsanalys	Hur analyseras/beskrivs aktuella arbetsuppgifter? Möjliga metoder t. ex.: - HTA - Observationer - Intervjuer och granskning av dokument - Länkanalys - Verbala protokoll - Decision action diagrams - TTA	*Administrativ styrning* Hierarkiskt schema för händelsesekvenser Framtagande av värderingsområden *Screeninganalys av manuella inledande händelser* Processbeskrivningar, kartläggning m.h.a. flödesscheman, systembeskrivningar och tidigare utförda riskanalyser Observationer Intervjuer och granskning av dokument	Sekvensanalyser Intervjuer med operatörer Granskning av dokument	Uppgiftsanalyser i överensstämmelse med Kirwans rekommendationer utförs i forma av: Hierarkisk uppgiftsanalys (HTA) Tabulär upptiftsanalys (TTA) Urval av Påverkansfaktorer föregår analysen och identifieras för aktuella uppgifter i TTA. Analys sker med: Observationer Intervjuer och granskning av dokument

7.3 Identifiering av mänskliga felhandlingar

7.3.1 Definition och koppling till avställningsperioden

Steget innebär att identifiera (alla) signifikanta mänskliga felhandlingar som påverkar systemets prestation, samt sätt som de mänskliga felhandlingarna kan återställas på. För detta steg beskrivs också vilken typ av fel som eftersöks. Speciellt för avställningssituationen är, enligt tabell 1, att det finns fler olika typer av inledande händelser som kan inträffa än under effektdrift. Som tidigare nämnts är detta steg i processen mycket viktigt. Det är endast de fel som identifieras och analyseras som påverkar bidraget till den övergripande risken.

Vid diskussion med en erfaren analytiker belystes att det för avställning handlar om att hitta parallella händelsekedjor som påverkar varandra och bidrar till stora negativa konsekvenser. Frågan av intresse är då om det finns andra arbeten än det aktuella, som påverkar situationen? Alla händelser måste fångas, inte bara den sekvens som leder till ett fel. Omgivande händelser påverkar hur snabbt rätt ”tråd” hittas, sedan tar det tid att göra tillhörande kontroller innan du kan utföra en viss åtgärd. Vid avställning gäller dock att tidsfönstret är längre. Svårigheten ligger alltså i att hitta risker i anläggningen, då olika arbeten påverkar varandra (händelsekedjor påverkar varandra). En viktig förutsättning för att kunna identifiera dessa risker är en bra utredning av händelsekedjor. En HRA-analytiker som är påläst på händelseanalysen har större möjlighet att identifiera riskerna. En tydlig beskrivning av händelsen, dess förutsättningar och hur den styrs är viktigt. En svårighet är att hitta misstagen som görs, möjliga förväxlingar med liknande arbeten, misstag på grund av vana att utföra uppgiften eller förväxling med en annan situation. I genomförda analyser har situationer med parallella sekvenser som påverkar varandra hittats, vilket lett till restriktioner för hur dessa arbeten får genomföras.

En aspekt som grundar sig på människans förmåga är också om det finns någon situation (oavsett om det är samma förutsättningar som gäller) där du använder samma verktyg, men på ett annat sätt? Sådana situationer skulle kunna leda till att uppgiften utförs, men med fel system i åtanke.

För avställning används enligt samma analytiker samma analysmetoder som för effektdrift, men med andra frågeställningar. Det är människan som anses starta upp felet. Frågor som är viktiga blir då:

- När utförs arbetsuppgiften?
- Utförs arbetet på rätt plats?
- Utförs arbetet vid rätt tidpunkt?

Hur dessa frågeställningar påverkat aktuella analysers identifiering av fel är svårt att säga inom ramen för detta arbete, men belyser tankesättet vid en analys av mänskligt felhandlande.

De frågeställningar som använts vid denna del av granskningen är:

- Hur väljs möjliga inledande händelser ut?

- Hur klassificeras/beskrivs mänsklig påverkan (med hjälp av feltyper etc.)?

7.3.2 Redovisning av avställningsanalyser

Avställningsanalys A

Analys av administrativ styrning:
Identifiering av risker sker med utgångspunkt ur händelsesekvenserna för de aktuella nyckelgrupperna och med hjälp av en analys av felets tillstånd och effekt på systemet (s.k. FMEA, Failure Mode and Effects Analysis), med avseende på felaktigt administrativt underlag.

Efter att ha samlat information om hur revisionsperioden planeras och hanteras har en kvalitativ bedömning av nyckelgruppernas förutsättningar gjorts. De framtagna värderingsområdena har bedömts med hjälp av ett antal specifika påståenden som tagits fram utifrån beskrivningen av området. Ett medelvärde för värderingsområdet räknas sedan fram som klassificeras från ”mycket dåligt stöd” (1 medelvärdespoäng) till ”mycket bra stöd” (5 medelvärdespoäng). Värderingen görs subjektivt av dem som utför det specifika arbetet. Till stöd för bedömningen finns även bedömningsgrunder som får frångås så länge andemeningen för värderingsområdet behålls vid utvärderingen.

Med hjälp av värderingen kan områden som behöver förbättras med avseende på den administrativa styrningen identifieras. Resultaten som presenteras är subjektiva omdömen gjorda av HFA-teamet, där intervjuresultaten med representanter från nyckelgrupperna varit mycket viktiga indata.

Screening av manuella inledande händelser
Identifiering av inledande händelser för den totala avställningsanalysen (PSA) omfattar både händelser initierade av manuella ingrepp, tekniska fel samt yttre nätbortfall (d.v.s. elförsörjningen till kraftverket försvinner). Även tappad last vid tunga lyft i reaktorhall samt händelser som kan orsaka kall kriticitet undersöks. Dessa händelser inkluderas dock inte i PSA-modellen utan beaktas i samband med expertbedömningar och ingår i resultatkapitel och slutredovisning.

Enligt metodbeskrivningen skall manuella ingrepp som genomförs på ett felaktigt sätt (*Error of Commission*) eller inte genomförs alls (*Error of Omission*) analyseras, då de också kan leda till (*typ A*) – eller utgöra (*typ B*) – inledande händelser. Ett felaktigt utfört manuellt ingrepp kan även degradera något system som behövs i senare skeden av förloppet. Sådana ingrepp identifieras och kvantifieras. Vid behov hanteras även manuella ingrepp som nyttjas för återställande av systemet.

I samband med kartläggningen av de olika inledande händelserna (enligt steg 2, uppgiftsanalys) för de olika typerna av manuella inledande händelser, identifieras tillsammans med expertgruppen komponenter och tillhörande system som är viktiga för den aktuella händelsen samt vilka typer av fel som kan leda till allvarliga konsekvenser.

Som hjälp att göra bedömningarna för LOCA-sekvenser[1] finns riktlinjer som beskriver vilka explicita system och avgränsningar det gäller. Dessutom beskrivs sex stycken typfall där en närmare beskrivning av möjliga scenarion och antagna förutsättningar ges. Eftersom den aktuella rapporten bygger på en tidigare bedömning har experter i denna nyare version ombetts att gå igenom de gamla bedömningarna för de nuvarande omständigheterna för att bedöma om de fortfarande är giltiga.

De inledande händelser som har valts ut för detaljanalys är:

- Tunga lyft
- Reaktorhallsarbeten allmänt
- Drivdonsdemontage
- HC-pumpsdemontage
- Upptäckt i centrala kontrollrummet av läckage från reaktortank
- Förlust av resteffektkylning på grund av fel i system 754
- Kall trycksättning

Dessa inledande händelser utgör alltså topphändelser i ett felträd och tillvägagångssättet för analys bygger på det ”what-if” tänkande som modellen för felträd innebär. Topphändelsen utgör då den oönskade händelsen som sedan bryts ner för att identifiera underliggande delhändelser och möjliga barriärer. Identifiering av delhändelser görs genom att ställa frågan: ”Vad ska ske för att topphändelsen/delhändelsen inte ska inträffa?”. Efter att de barriärer, de funktioner som kan stoppa en inledande sekvens, identifierats, beaktas eventuella beroenden mellan händelser och barriärer i felträdet och slutligen bedöms vilka påverkansfaktorer som finns för den lägsta nivåns händelser.

Avställningsanalys B

Inledande händelser för denna analys är i huvudsak de som identifierats inom projektet för säkerhet under revisionsavställning. Utöver detta har en komplettering skett med hjälp av anläggningserfarenhet (d.v.s. expertbedömningar).

Kategorisering av inledande händelser har skett enligt följande:

- Reaktivitetsmissöde
- Läckage från reaktortank (LOCA)
- Läckage från reaktortank under härdnivå
- Läckage från reaktortank över härdnivå
- Bortfall av resteffektkylning
- Övertryckning av RCPB
- Tappad last (lyft)
- Tappad bränslepatron
- (Oavsiktlig friläggning av bränslepatron)

[1] LOCA: Loss Of Coolant Accident. Kylning av bränslet är viktigt även när reaktorn är avställd, p.g.a. den resteffekt som alstras.

- Friläggning av använd bränslepatron

Dessutom ingår i analysen:
Operatörsingrepp efter en inledande händelse (*typ C*-ingrepp)

Denna analys bygger på en indelning i felhandlingar av typ A-C (IAEA, 2000) med definitionerna (jämför med kapitel 4.2.3):

A) felhandling som genomförts *före* händelsen, utan att initiera densamma (kan dock vara den bakomliggande orsaken till händelsen)
B) felhandling som *initierar* händelsen, samt misslyckat försök att omedelbart stoppa händelseutvecklingen (motsvarande barriärfunktion: ”recovery *före* IH”)
C) Misslyckat försök att efter inträffad händelse förhindra/mildra dess konsekvenser (motsvarande barriärfunktion ”recovery *efter* IH”)

För att precisera bedömningen av de olika händelserna klassificeras ingreppen för typ A och B via en tabell med möjliga felhandlingar (utebliven handling, förväxling, för tidig handling, för sen handling, sekvensfel och för lite/mycket) för olika personalgrupper (planering, drift och underhåll). Noteras bör, att mänskligt felhandlande som kan leda till en inledande händelse inte analyseras i HRA för effektdrift, men beaktas explicit i PSA för avställningsfasen.

Identifiering av ingrepp av typ C, operatörsingripanden, har huvudsakligen skett i samband med sekvensanalyser. Händelsesekvenser har då diskuterats tillsammans med operatörerna för att få deras bedömning om möjliga och prioriterade ingrepp. På grund av den komplexa situation som råder för operatörsingripanden, då de beror på störningens förlopp på hur operatören upplever störningssituationen samt på störningens dynamik, görs det i analysen vissa förenklingar och begränsningar. Analysen begränsas huvudsakligen till instruktionsstyrda ingrepp och eventuellt till ingrepp som annars ingår i anläggningens praxis eller utbildningsprogram. Analysen syftar till att skatta sannolikheten att det i störningsinstruktionerna föreskrivna eller rutinformade ingreppet uteblir (error of omission). Aktiva operatörsfel (error of commission) lämnas utanför analysen.

I metodbeskrivningen anges även hur en detaljanalys skall gå till, men då detta ännu inte genomförts beskrivs inte detta närmare.

Avställningsanalys C

Baserat på uppgiftsanalysen identifieras möjliga mänskliga felhandlingar i de typiska uppgifterna samt de kontextuella förutsättningarna och påverkansfaktorerna. PSA-identifierade sekvenser är dock i grunden styrande för urvalet av händelsesekvenser, i form av urval av analyserade scenarion.

Med hjälp av deltagande experter för aktuella ämnesområden (ex. underhållspersonal, kontrollrumspersonal och personal för planering och administrativ styrning av revisionsperioden) väljer analysgruppen ut sådana felmöjligheter som kan bidra till negativa konsekvenser.

Felen grupperas i olika kategorier för att bilda felkategorier, som kan anses representera ett antal typer av handlingar som kan leda till fel. Varje kategori skall sedan analyseras och

kvantifieras. Ett exempel på en väntad sådan kategori är avställning och dränering av ett systemstråk före genomförande av underhåll, en kategori som kan representera avställning av dränering av flera liknande systemstråk.

Någon indelning i feltyper enligt IAEA:s kategorisering anges inte.

7.3.3 Sammanfattning

Det som framgår mest tydlig av ovanstående analyser är att de händelser som analyseras är identifierade i aktuell PSA. Till viss del kan det vid genomgången av de aktuella avställningsanalyserna kännas som att denna del i processen hamnar lite ”fel” i ordningen. Som en del av PSA har de intressanta inledande händelserna identifierats, detta steg begränsas då till att identifiera möjliga mänskliga fel för detta begränsade urval. Det bör dock sägas att även en HRA-expert vanligtvis deltar vid PSA:ns urval av inledande händelser. Denna konsekvens är alltså ”naturlig” i det avseendet att analyserna ingår i en PSA-analys och att analysen vore ohanterlig om ”alla möjliga fel” skulle identifieras. En avgränsning är alltså nödvändig. En slutsats av detta kan dock anses vara, att HRA-expertisens roll vid urval av handlingar och identifiering av dem som kan ha stor negativ påverkan på systemets säkerhet, bör definieras tydligt.

Vid analys av de inledande händelserna försöker man sedan finna de händelser då människan kan ha påverkat systemet så att en felsekvens inleds. I anslutning till detta följer två av analyserna den standard som IAEA anger av typer av fel, där man kan påverka systemet, före, under eller efter en inledande händelse, samt att denna påverkan kan ha positiv eller negativ verkan på händelsförloppet, det vill säga att man lyckas eller misslyckas med att avhjälpa felet.

Intressant att notera är, att avställningsanalys B anger att även mänskligt felhandlande som kan *leda* till en inledande händelse (typ B) analyseras för avställningsfasen, till skillnad mot analys av effektdrift och även de rekommendationer som ges i NUREG-1792 (som gäller för normaltillståndet effektdrift).

I samtliga analyser framgår även att medverkande av experter, d.v.s. operatörer, underhållspersonal m.fl. är viktigt vid identifieringen av möjliga felhandlingar. Identifieringen av felhandlingar följer ett normativt synsätt, med utgångspunkt i hur system och människor *borde* uppföra sig.

Att, som en analytiker påpekade, hitta parallella händelsekedjor som påverkar varandra och bidrar till stora negativa konsekvenser är alltså en viktig, men svår uppgift, vid analys av avställning.

Tabell 4. Sammanfattning av identifiering av mänskliga fel

HRA-processen (Kirwan, 1994)		**A.**	**B.**	**C.**
Delprocess	**Frågeställning**			
3. Identifiering av mänskliga felhandlingar	**Hur väljs möjliga inledande händelser (IH) ut?**	*Administrativ styrning:* Ur händelsesekvenser för nyckelgrupperna. *Manuella inledande händelser:* Kartläggning och identifiering av manuella IH m.h.a. flödesscheman, systembeskrivningar och tidigare utförda riskanalyser.	IH väljs ut via generell rapport om säkerhet vid revisionsavställning. Identifiering av ingrepp av typ C med hjälp av sekvensanalyser.	Urval av IH via PSA, identifiering av möjliga mänskliga felhandlingar ur uppgiftsanalysen.
	Hur klassificeras mänsklig påverkan? Hur sker modellering av mänsklig inverkan på systemet: human error? => Identifiering av feltyper: A-C	*Administrativ styrning:* Bedömning av värderingsområden. *Manuella inledande händelser:* Typ A-C (dock ej enligt den terminologin). Error of Omission och Error of Commission beskrivs i andra ordalag, båda skall ingå i analysen. Manuella ingrepp som utnyttjas för återställande handlingar.	Klassificering typ A-C samt tabell för möjliga felhandlingar för olika personalgrupper. Endast ingrepp och återkopplingar som är definierade i instruktioner beaktas i screeningfasen. Typ C: endast Error of Omission analyseras (För effektdrift analyseras endast typ A och C.)	Felen grupperas i olika feltyper för kvantifiering. (Anges ej specifikt om feltyp A-C enl. IAEA) Kontextuella förutsättningar och påverkansfaktorer identifieras.

7.4 Representation

7.4.1 Definition och koppling till avställningsperioden

Representation innebär att skapa en logisk modell för de mänskliga felhandlingarna och möjligheter till återställning så att deras påverkan på systemet kan bestämmas kvantitativt. Detta kräver vanligtvis en integration av mänskliga felhandlingar med tekniska hårdvarufel i ett fel- eller händelseträd.

För en analys av avställning är det kritiska steget att hitta eventuella beroenden mellan mänskliga handlingar. Detta blir mer komplicerat än för effektdrift, både på grund av att fler personer är i kontakt med anläggningen, men också för att de mänskliga ingreppen i sig är fler. Ett beroende kan exempelvis finnas om en person, inom samma tidsperiod, genomför ett antal olika åtgärder.

Punkter som ingår i granskningen är alltså:

- Hur hanteras och modelleras de mänskliga felhandlingarna?
- Hur modelleras beroenden?
- Hur modelleras återställande handlingar?

7.4.2 Redovisning av avställningsanalyser

Avställningsanalys A

De manuella inledande händelserna integreras med PSA-modellen och modelleras med hjälp av felträd.

Modellering av beroenden

Enligt en analytiker vid kraftverket är en av svårigheterna med avställningsanalys beroenden. Det är också dessa som kan påverka systemets säkerhet mycket, eftersom händelser eller aktiviteter som påverkar varandra kan förstärka (eller försvaga) effekten på systemet.

Alla händelser måste fångas, inte bara den sekvens som leder till ett fel. Omgivande händelser påverkar hur snabbt rätt ”tråd” hittas, sedan tar det tid att göra tillhörande kontroller innan en viss åtgärd kan genomföras. Vid avställning gäller dock att den tillgängliga tiden för att utföra en åtgärd (s.k. tidsfönster) är längre. Svårigheten ligger alltså i att hitta risker i anläggningen, då olika arbeten påverkar varandra (händelsekedjor påverkar varandra). En viktig förutsättning för att kunna identifiera dessa risker är en bra utredning av händelsekedjor. En HRA-analytiker som är påläst på händelseanalysen har större möjlighet att identifiera riskerna. En tydlig beskrivning av händelsen, dess förutsättningar, hur det är uppstyrt är viktigt. En svårighet är att hitta misstagen som görs, möjliga förväxlingar med liknande arbeten, misstag på grund av vana, förväxling med en annan situation etc.

Under screeningprocessen har modellering av beroenden skett med hjälp av THERP:s s.k.

kopplingsfaktorer, där beroendet klassificeras på en skala från ”inget beroende” till ”totalt berodende”.

Vid detaljanalys är ett steg att beakta beroenden i felträdet (mellan delhändelser, mellan barriärer samt mellan händelser på olika nivåer).

Modellering av återställande handlingar (recovery)
Recoverys modelleras som tidsberoende om det inte finns behov att utvärdera om funktionen snabbt måste återställas.

Modelleringen utgår från samtliga manuellt inledande händelser och de mekaniska inledande händelser där mer än 6 timmar finns tillgängliga innan härdskada uppstår. Även för detta används en modell från metoden THERP, en tidsdiagnoskurva och Annunciator Response Model.

Avställningsanalys B

Händelsebeskrivning samt analys bestående av en skriftlig beskrivning av möjliga händelseförlopp och felhandlingar sker för varje inledande händelse. Därefter följer en bedömning av om händelsen skall analyseras vidare (alltså kvantifieras).

Som stöd till modellering av ingrepp har en felträdsanalys utförts för relevanta säkerhetsfunktioner och operatörsingrepp.

Modellering av beroenden
Typ C-handlingar (efter en inledande händelse):
De olika ingrepp som krävs för hantering av situationen är starkt kopplade till varandra dels via berörda mänskliga resurser och dels via processkopplingar. För att någorlunda beakta dessa beroenden modelleras ett fåtal ingrepp som sedan representerar större funktioner med gemensamt syfte.

Analys av beroenden mellan operatörsingrepp:

- Analys av minimala snitt med förhöjda sannolikheter:
    - Syftar till att identifiera händelsesekvenser där flera än ett operatörsingrepp kan förekomma och att bedöma om det finns ett beroende mellan dessa operatörsingrepp som bör beaktas genom att justera sannolikheter.
    - PSA-modellen körs med förhöjda felsannolikhetsvärden för operatörsingreppsbashändelser (lägsta nivån i ett felträd) för att lyfta upp de minimala snitt som innehåller operatörsingreppen i listan med minimala snitt.

Modellering av återställande handlingar (recovery)
Recoverys beskrivs efter kvantifiering av möjliga felhandlingar. Bedömning sker av sannolikhet för misslyckade återställande handlingar (olika fall).

Avställningsanalys C

Grunden för analysen är den *normativa* beskrivningen av arbetet under de utvalda typuppgifterna under avställningsperioden så som de dokumenteras i instruktioner och manualer på anläggningen. Arbetsuppgifterna beskrivs i en hierarkisk uppgiftsstruktur, där

typfelen också beskrivs. För komplexa uppgiftssekvenser kan även representation i felträd användas.

Modellering av beroenden
För modellering och beräkning av beroenden används THERP:s ”Positive dependence model” (anger grad av beroende enligt skalan inget beroende – totalt beroende). (Endast positivt beroende beaktas alltså.)

Modellering av återställande handlingar (recovery)
Återställande handlingar i olyckssekvenser tas alltid i beaktande i de fall en inledande händelse orsakats av en felaktig mänsklig handling. Återställande för inledande händelser orsakade av tekniska fel beaktas endast då den tillgängliga tiden för att utföra den återställande handlingen anses vara tillräcklig. En generell gräns för ”tillräcklig tillgänglig tid” (i denna analys bedömd till 10 minuter) kan användas i analysen och kan om nödvändigt baseras på övergripande krav för den totala avställninsanalysen (SPSA).

För olika tidsintervall presenteras i tabeller från THERP:s modell för tidsdiagnoskurvan justerade sannolikheter för återställande handlingar som bedöms som enkla eller av normal svårighetsgrad (exempelvis så kan återställande ske med hjälp av ett litet antal åtgärder, eller att det finns tydliga larm som indikerar när och var ett fel inträffat) respektive för svåra återställande handlingar (en återställande handling klassas som svår om det exempelvis är svårt att bedöma vilka åtgärder som krävs, eller om åtgärderna i sig är svåra att utföra). Återställande handlingar som klassas som mycket svåra (exempelvis om multipla larm visas i samband med en mängd andra larm, vilket gör det svårt att identifiera det verkliga felet) beaktas inte i analysen.

7.4.3 Sammanfattning

Även för detta steg i HRA-processen är metodiken starkt kopplad till PSA. Modellen för mänskliga felhandlingar bygger, som tidigare nämnts, på ett normativt synsätt, d.v.s. med utgångspunkt i hur system och människor borde uppföra sig. Enligt avställningsanalys A är detta steg viktigt för att kunna identifiera möjliga beroenden och felsekvenser som påverkar varandra. Vid analys av beroende använder sig samtliga analyser av en modell ur den etablerade metoden THERP (se kapitel 5.2.1). Detta visar två aspekter av problematiken med HRA och modellering av mänskligt beteende som lyfts fram i denna rapport.

För det första visar detta att det är svårt att skapa praktiskt användbara modeller för mänskligt beteende, och kanske framför allt för beroenden mellan händelser

För det andra är detta ett exempel på att beprövade metoder har en stark ställning vid analyser genomförda vid (svenska) kärnkraftverk. Trots att THERP, som har sin utgångspunkt i ingenjörsvetenskapen, och inte så mycket i kognitiva och psykologiska teorier, är en gammal metod som har kritiserats mycket, ger den förslag på explicita tillvägagångssätt med resultat som är förhållandevis lätta att tolka och använda i en analys.

Tabell 5. Sammanfattning av representation

HRA-processen (Kirwan, 1994)		**A.**	**B.**	**C.**
Delprocess	**Frågeställning**			
4. Representation	**Hur modelleras identifierade mänskliga felhandlingar?**	Integreras i PSA-analysen och modelleras med hjälp av felträd.	Händelsebeskrivning för bedömning om vidare analys. Felträdsanalys	Normativ beskrivning grund Felträd
	Hur modelleras beroenden?	*Screening:* Modellering m.h.a. THERP:s kopplingsfaktorer. *Detaljanalys:* Beakta beroenden i felträdet	Typ C: Fåtal ingrepp modelleras som representerar större funktioner med gemensamt syfte.	THERP:s *positive* dependence model
	Hur modelleras återställande handlingar (recoverys)?	Recoverys modelleras tidsberoende (6h. tillgänglig tid innan härdskada) THERP:s tidsdiagnoskurva samt Annunciator Response Model.	THERP bassannolikhetskurva (justerad), tidsoberoende modell med indelning enligt svårighetsgrader	Varierande tidsintervall: THERP:s tidsdiagnoskurva

8. Diskussion

8.1 Inledning

8.1.1 Syfte och frågeställningar

Syftet med detta examensarbete är som tidigare nämnts att beskriva de metoder och grundläggande modeller för mänsklig tillförlitlighet som används vid analys av avställningsperioden. Målet har varit att besvara följande frågeställningar:

1. Hur kan avställningsperioden karaktäriseras och definieras?
2. Vad är viktigt att ta hänsyn till vid analys av avställning när det gäller mänskligt beteende?
3. Hur kan mänskligt beteende i en riskanalys för avställning modelleras?
4. Mot bakgrund av tillgängligt empiriskt material, hur har punkterna ovan hanterats i genomförda analyser av ingrepp under avställning?
5. Hur påverkar resultatet av ovanstående frågor hur metod för avställningsanalys kan och/eller behöver utvecklas?

I följande diskussion behandlas frågeställningarna var för sig för att mynna ut i förslag på fortsatt forskning i ämnet.

8.1.2 Vilka slutsatser kan dras baserat på undersökningens resultat?

Denna undersökning har, som tidigare nämnts, varit begränsad främst beroende på tillgänglig tid. Detta har i sin tur påverkat möjligheterna till insamling av material och genomförande av intervjuer. Förhoppningen är ändå att sammanställningen av teori för modellering av mänskligt beteende, en beskrivning av avställningsperiodens karaktär samt hur denna kunskap tillämpas i genomförda analyser av mänsklig tillförlitlighet vid svenska kärnkraftverk kan belysa frågeställningar och behovet av vidare forskning i området.

Trots ovanstående begränsning har det varit möjligt att utläsa hur mänskligt beteende modelleras i genomförda analyser, vilket gjort det möjligt att dra slutsatser om hur teori och empiri stämmer överens.

8.2 Hur har studien bidragit till att koppla teori och tillämpad metod för HRA?

8.2.1 Hur kan avställningsperioden karaktäriseras och definieras?

I kapitel 3 ges en beskrivning av avställningsperioden. Den karaktäriseras av en hög grad av mänsklig interaktion i form av testning, underhåll och reparationer. Under avställningsperioden byts även använt bränsle ut. Samtliga dessa aktiviteter medför att det tekniska systemets egenskaper påverkas, exempelvis då underhåll skall utföras på system som normalt sett är avstängda för mänskligt tillträde. Dessutom är inte alla säkerhetssystem

tillgängliga. Den totala bilden av systemets egenskaper förändras alltså flera gånger under en avställningsperiod, vilket ökar komplexiteten. Det finns ekonomiska incitament för att en revision bör genomföras så snabbt och effektivt som möjligt. Detta medför att kraven på personalen ökar, med högre arbetsbelastning och högre stressnivå.

Slutsatsen av detta är, att avställningsperioden skiljer sig mycket från förhållandet då normal effektdrift råder, framför allt med avseende på mänsklig interaktion med det tekniska systemet.

8.2.2 Vad är viktigt att ta hänsyn till vid analys av avställning när det gäller mänskligt beteende?

Enligt ovanstående slutsats är människans påverkan på det tekniska systemet av stor betydelse vid analys av avställning. Detta bör även påverka analysen utgångspunkt och genomförande, för att möjliggöra en så realistisk analys som möjligt.

Enligt noteringen i kapitel 7.1.3 är det för avställningsanalys av stor vikt att hitta parallella händelsekedjor som påverkar varandra och bidrar till stora negativa konsekvenser. Detta handlar om människans uppfattning av hur systemet fungerar och vilka ingrepp som kan göras, och när, utan att det påverkar säkerheten negativt. Med ett, enligt Vicente, formativt synsätt skulle det innebära att känna till vilka villkor och krav som gäller för att systemets säkerhet skall upprätthållas.

Den höga graden av komplexitet i systemet under avställningsperioden är viktig att ta hänsyn till vid analys av avställning. Enligt teorin bör ett holistiskt perspektiv användas vid analys av komplexa, sociotekniska system. Ett sätt att ta hänsyn till människans förmåga och variabilitet i prestation är viktigt.

Slutsatsen av detta resonemang är att utgångspunkten vid analys av avställning böra vara holistiska modeller som i så stor utsträckning som möjligt tar hänsyn till det sammanlagda bidraget från Mänskliga, Tekniska och Organisatoriska aspekter.

8.2.3 Hur kan mänskligt beteende i en riskanalys för avställning modelleras?

Dagens analyser bygger dock på en komplex, linjär orsak – verkan modell (”Swiss cheese). Granskningen av genomförda avställningsanalyser belyser att det är PSA som utgör förutsättningen för analysen.

Den problematik som uppstått inom ramen för detta examensarbete gäller främst hur mänskligt beteende i allmänhet och mänskligt felhandlande i synnerhet skall modelleras i samband med ett tekniskt, komplext system och riskanalys för avställning. En riskanalys är dock aldrig förutsättningslös, utan bygger på antaganden om det analyserade systemet och de förhållanden som råder, i detta fall att analysen genomförs inom ramen för PSA och för perioden avställning. Detta innebär att problemet måste identifieras och definieras, vilket medför att det är det första steget i Kirwans HRA-process, problemdefinition, som är avgörande för den resterande analysens steg och resultat.

I ovanstående genomgång av analyser syns detta genom att stegen efter problemdefinitionen präglas av ”Swiss cheese”-tänkandet, där fel identifieras som enskilda

händelser i en sekvens, med påverkan från mänskliga egenskaper och yttre omständigheter i form av påverkansfaktorer. Mänskligt handlande ses också som enskilda, isolerade händelser i olyckssekvensen.

I samband med PSA ter sig steget för problemdefinition i processen förutbestämt och bidrar till att hela analysen styrs mot ett sekventiellt tänkande. Frågan är då om det vid en ansats för att anamma en annan modell för hur mänskligt beteende och risk skall analyseras även krävs att arbetsprocessen ses över. Kirwans HRA-process är logisk och ”lätt” att jobba med, men får man ut den information och kunskap om systemet man vill ha? Det är inte något som detta arbete kan svara på, men som skulle kunna vara grund för vidare forskning.

Detta skulle med den redovisade teorin för detta arbete innebära att den modell som bäst beskriver hur fel och olyckor kan uppkomma i systemet är den för funktionell resonans. Målet med en riskanalys blir då att hitta de tillfällen, då avvägningen mellan effektivitet och noggrannhet (Effectiveness – Thoroughness Trade Off) kan gå fel.

Slutsatsen av detta är, att det i dag finns modeller för hur analys av hur fel uppstår som i högre grad har som ansats att ta hänsyn till det komplexa, sociotekniska systemets variabilitet än den sekventiella modell som ligger till grund för dagens HRA och PSA-metoder.

8.2.4 Mot bakgrund av tillgängligt empiriskt material, hur har punkterna ovan hanterats i genomförda analyser av ingrepp under avställning?

Om PSA utgör grunden för HRA påverkas alltså analysen av mänskligt felhandlande av de gränser som PSA sätter. Fokus för en PSA-analytiker är att identifiera inledande händelser och modeller för hur fel påverkar det tekniska systemet, samt att kvantifiera frekvensen för att en händelse inträffar. Ur detta perspektiv är analys av mänsklig tillförlitlighet bara en liten del, vilket kan anses vara en felaktig ståndpunkt när det gäller avställningssituationen[2].

I de granskade analyserna märks detta på sådant sätt, att det är den kvantitativa analysen av mänsklig tillförlitlighet som är det centrala. För avställningssituationen blir det, enligt tidigare resonemang om behovet av ett helhetsperspektiv, dock svårare att skilja på syftena med HRA och MTO. Avställningsperioden innebär, som vissa säger, ett enda stort manuellt ingrepp, och det kräver analys av vilka faktorer som påverkar arbetsförhållanden för att kunna göra realistiska bedömningar. Kanske är det då dags att i större utsträckning se de kvalitativa aspekterna som värdefulla resultat som, ju bättre och noggrannare de är undersökta, kan ge bättre skattningar till PSA. Med ett sådant synsätt blir MTO-analyser och analys av den administrativa styrningen värdefull indata till själva HRA (i bemärkelsen kvantitativ analys).

I befintliga HRA-analyser finns alltså olika mycket av det kvalitativa inslaget, framför allt läggs olika mycket resurser på en kvalitativ *analys*. En av de granskade analyserna sticker ut med en separat analys av den administrativa styrningen. För övriga analyser ingår en grundläggande situationsbeskrivning, men det är inte alltid tydligt hur det förberedande

[2] Det är inte helt sant att PSA-analytiker inte erkänner att mänsklig tillförlitlighet är viktigt. Inom avställningsanalyserna påpekas att HRA är en viktig del och att människans påverkan på systemet är stor. I analysen innebär detta dock att det är det den kvantitativa analysen som får mest utrymme.

arbetet inför kvantifiering har gått till, hur urval av påverkansfaktorer skett mm. För att det skall bli en kvalitativ *analys* krävs dock en värdering av denna situation och de förutsättningar som råder för att människan skall kunna hantera situationen (eller göra fel). En kvalitativ analys är nödvändig för att kunna göra en bra *kvantitativ* bedömning av risken att göra fel. I resultatet av en HRA faller det alltid ut kvalitativa värden som ”biprodukter”, då utgångspunkten vid beräkning av sannolikheter är möjliga händelsekedjor och vad som påverkar prestationen i olika situationer för att en realistisk skattning av felsannolikheten (främst vid expertbedömningar) skall kunna göras. En förberedande analys av administrativ styrning har stor genomslagskraft på hur värderingarna i de andra delarna av analysen görs. Om samma experter används för en analys av den administrativa styrningen och den *kvantitativa* analysen, har deras medvetenhet om kontexten och situationen för de olika ingreppen ökat via den *kvalitativa* analysen, vilket kan ge en bättre, mer verklighetsnära bedömning av de olika händelserna. En brist i HRA enligt NEA (se kapitel 2.4) är dock en alltför stor tilltro till expertbedömningar. De granskade analyserna bygger till stor del på just sådana expertbedömningar, vilket kan förklaras med den tidigare nämnda bristen på empiriska erfarenhetsdata.

Slutsatsen är, att HRA-betgreppet i genomförda analyser av ingrepp under avställning, innebär en kvantifieringsmetod för mänskliga handlingar och påverkan på det tekniska systemet. En breddning av begreppet HRA skulle i stället kunna göra det till en metod för att beskriva, analysera och utvärdera samspelet mellan Människa, Teknik och Organisation.

8.2.5 Hur påverkar resultatet av ovanstående frågor hur metod för avställningsanalys kan och/eller behöver utvecklas?

Teorin om hur olyckor och risker uppkommer behöver befästas i metoder som är möjliga att ta till sig och att tillämpa. Hur ska detta ske? Utvärdering av vad dagens metoder kan komma fram till, respektive vad nya metoder kan visa, krävs. NEA:s rapport belyser en del problem med HRA av idag, de flesta handlar om kvantifiering. Är kvantitativa metoder vettiga och möjliga för HRA, och speciellt, för HRA för avställning? Ur PSA-synpunkt ligger fokus just på de kvantitativa resultaten. Den största bristen anses dock vara tillgång på erfarenhetsdata. Ingen (eller mycket liten) explicit hänsyn tas heller till påverkan av organisations- och ledningsaspekter (utöver de påverkansfaktorer som används för att beskriva kontexten).

Frågan om hur en PSA påverkas av att människan har stor påverkan på det tekniska systemet skulle också kunna ställas. Ett möjligt svar är att osäkerheten i analysen ökar. Om en analys har hög grad av osäkerhet är det svårare att dra slutsatser och identifiera verkliga orsaker. Hur skulle då en metod påverkas av att utgå från människan i stället för tekniken? Om förutsättningen för en analys av avställning inte är en PSA, utan en holistisk utgångspunkt där ett MTO-synsätt och HRA bestämmer analysens omfattning. Detta vore att byta utgångspunkt och möjligheten till och nyttan av ett sådant arbetssätt behöver undersökas vidare.

Något som blivit tydligt under detta examensarbetes gång är, att det inte är en enkel uppgift att jämföra olika avställningsanalyser, än mindre analyser gjorda för olika kraftverk. Trots att utgångspunkten är PSA kan angreppssätten skilja sig mycket åt. Detta är inte nödvändigtvis något dåligt, det utgör tvärtom en grund för utveckling av analysmetoder. Däremot finns det en poäng med att skapa rekommendationer för vad som är viktigt att

analysera för just avställning. NUREG:s ”Good practice” gäller för effektdrift och en viktig del som visat sig saknas i dessa rekommendationer är viktiga aspekter vid analys av mänskliga handlingar som inledande händelser (typ B), något som dessutom anses vara mycket svårt att göra.

I ovanstående diskussion har ett antal punkter lyfts fram om skillnaden mellan vilken utgångspunkt teoretiker anser att en analys av mänsklig tillförlitlighet i komplexa system bör ha och hur det i praktiken ser ut för mänsklig tillförlitlighetsanalys för avställning. Enligt teorin behövs en utveckling av HRA för att bättre ge svar på hur säkerheten i systemet kan analyseras och förbättras. Mer forskning behövs, men också ytterligare incitament för att belysa den särskilda problematiken och eventuellt behov av ett förändrat synsätt för avställningsanalys. Ett sådant incitament utgörs av myndighetskrav, eftersom innehållet i säkerhetsanalyser till stor del definieras av de krav som gällande myndighet ställer. Detaljnivå på analysen samt vilka delmoment och prioriteringar (utgångspunkt från PSA eller HRA-MTO?) som är viktiga för avställning är frågeställningar som bör behandlas.

8.3 Förslag till fortsatt forskning

För att säkerställa och fördjupa ovanstående resonemang krävs vidare forskning. Följande punkter är exempel på möjliga utgångspunkter.

- *Fördjupad genomgång av befintliga avställningsanalyser*: Fler och mer strukturerade intervjuer samt en mer heltäckande genomgång av genomförda analyser av mänsklig tillförlitlighetsanalys hade behövts för att säkerställa och bekräfta resultat och arbetssätt vid genomförande av HRA.
- *Utveckling av praktiskt tillämpbara metoder*: De teoretiska tankarna för modellering av mänsklig tillförlitlighet i samverkan med och som en del av systemet kan anses vara bra, men hur ska man jobba med det i praktiken?
- *Validering av HRA-processens arbetsgång*: Vid en ansats för att anamma en annan modell för hur mänskligt beteende och risk skall analyseras krävs även att arbetsprocessen ses över. Dessutom har genomgången av genomförda analyser visat att arbetsprocessen i praktiken sker i färre, till PSA anpassade, steg. Detta kan även kopplas samman med behovet att verifiera de metoder som används, ett arbete som är påbörjat, bl. a. i Halden.
- *Utveckling av kravspecifikation för avställningsanalys*: Även frågan om hur denna typ av analyser bör (och behöver?) styras av myndighetskrav bör undersökas närmare.

Slutligen kan sägas, att analys av mänsklig tillförlitlighet i allmänhet och för avställningsperioden i synnerhet är ett mycket intressant och aktuellt ämne, men som också är mycket omfattande och i vissa fall svårt att greppa. Behov av fortsatt forskning finns!

9. Referenser

Tryckta källor

ACSNI Study Group on Human Factors. (1993). 3rd Report: *Organising for Safety*. HSE Books.

Bennemo, L. (2005). *Swedish authority demands shutdown analyses – Growing awareness of risks during nuclear plant's yearly outage,* SKIs forskningstidning Nucleus 3/2005, s. 38-41

Hallman, A., Knochenhauer, M., Nyman, R.(2003). *Tillsynshandbok PSA*, SKI Rapport 2003:48. Statens kärnkraftinspektion, Stockholm

Harms-Ringdahl, L. (2001). *Safety analysis, principles and practice in occupational safety*, 2nd edition, Taylor and Francis, London. ISBN 0-415-23655-X

Hellström, P. (2004). *Övergripande beskrivning av PSA nivå 1 och 2 och analys av yttre händelser*, Relcon AB. Med tillstånd från författaren.

Hollnagel, E. (2005). *Human Reliability Assessment in Context*, Nuclear Engineering and Technology, vol. 37 No. 2, april 2005, s. 159-166

Hollnagel, E. (2007). *Human Error: From 'Fallible Machines' to 'Coping with* Complexity'. Procedings; International Rail Accident Investigation Conference, 2007-02-28 – 2007-03-01, London.

Hollnagel, E., Woods, D. D., Leveson, N. (2006). *Resilience Engineering, Concepts and Precepts*. Ashgate Publishing Limited, Hampshire, England.

IAEA (2000). *Probabilistic safety assessments of nuclear power plants for low power and shutdown modes*, IAEA-TECDOC-1144, International Atomic Energy Agency, Wien

Kecklund, L. (1998a). *Samspelet Människa-Teknik-Organisation (MTO) och säkerhet i tekniska system*, Uppsats för Människan i komplexa system, doktorandkurs vid CMD 1990-1991

Kecklund, L. J. (1998b). *Studies of Safety and Critical Work Situations in Nuclear Power Plants: A Human Factors Perspective*, Akademitryck AB, Edsbruk. ISBN 91-7153-762-7

Kecklund, L. (2007). *Human Factors in Accident Investigations*. Procedings; International Rail Accident Investigation Conference, 2007-02-28 – 2007-03-01, London.

Kirwan, B. (1994). *A guide to practical human reliability assessment*, Taylor & Francis, London, ISBN 0-7484-0052-4

Kirwan, B. (2005). *Human reliability assessment*. Kapitel 32 i Wilson, J.R., Corlett, N., *Evaluation of human work,* 3rd ed. s. 833-875. Taylor and Francis Group, Boca Raton, Fla.

ISBN 0-415-26757-9

Knochenhauer, M. (1996). *Status and Use of PSA in Sweden*, SKI Rapport 96:40. Statens kärnkraftinspektion, Stockholm

NEA (2004). *Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants*, Committee on the Safety of Nuclear Installations, Technical Opinion Papers No. 4, OECD Nuclear Energy Agency, No. 5068. ISBN 92-64-021574

NUREG-75/014 (1975). WASH-1400. *Reactor Safety Study – An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*. U.S. Nuclear Regulatory Commission, Washington DC

NUREG-1792 (2005). *Good Practices for Implementing Human Reliability Analysis (HRA)*. Sandia National Laboratories, U.S. Nuclear Regulatory Commission, Washington

NUREG-1842 (2006). *Evaluation of Human Reliability Analysis Methods against Good Practices*. U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington DC

NUREG/CR-6883. (2005). *The SPAR-H Human Reliability Analysis Method*, U.S. Nuclear Regulatory Commission, Washington DC

Perrow, C. (1999). *Normal Accidents*. Princeton University Press, Princeton. ISBN 0-691-004129

Pyy, P. (2000). *Human reliability analysis methods for probabilistic safety assessment*. VTT Technical Research Centre of Finland Publications 422, Espoo

Reason, J. (1990). *Human error*. Cambridge University Press, Cambridge. ISBN 0-521-31419-4

Rollenhagen, C. (1995). *MTO – en introduktion*, Studentlitteratur, Lund. ISBN 91-44-60031-3

Roos, A. (2007). *HRA – En översikt av användning, metoder och tillsyn*. SKI utredningsrapport. Statens kärnkraftinspektion, Stockholm

SKIFS 2004:1, *Statens kärnkraftinspektions föreskrifter om säkerhet i kärntekniska anläggningar*. Statens kärnkraftsinspektion, Stockholm

RSSB (2006). *Understanding Human Factors, v1.0r.* UK

YVL 1.13 (1995). *Nuclear Power Plant Outages*. Finnish Radiation and Nuclear Safety Authority (STUK), Helsingfors. ISBN 951-712-257-8

Vicente, K.J. (1999). *Cognitive Work Analysis, Toward safe, productive, and healthy computer-based work*, Lawrence Erlbaum Associates, Mahwah, New Jersey. ISBN 0-8058-2397-2

Internet

www.ski.se (2006-11-29)
hem/om kärnkraft/kärnkraft/säkerhetsanalys
http://www.ski.se/extra/tools/parser/index.cgi?url=/html/parse/index.html&selected=3&mainurl=/page/1/21.html

www.ski.se (2006-12-13)
Information har hämtats från följande länkar:
hem/om kärnkraft/kärnkraft
http://www.ski.se/extra/tools/parser/index.cgi?url=/html/parse/index.html&selected=3&mainurl=/page/1/21.html

hem/om kärnkraft/kärnkraft/så fungerar ett kärnkraftverk
http://www.ski.se/extra/tools/parser/index.cgi?url=/html/parse/index.html&selected=3&mainurl=/page/1/45.html%3F14647

hem/om kärnkraft/kärnkraft/revision
http://www.ski.se/extra/tools/parser/index.cgi?url=/html/parse/index.html&selected=3&mainurl=/page/1/45.html%3F14647

Avställningsanalyser

FT-2005-619. (2005). *PSA Forsmark 1 / 2 och Forsmark 3; Bilagor till huvudrapporten 1.1.5; Metodbeskrivning för dataanalys (HRA för effektdrift)*

FT-2006-110. (2006). *PSA Forsmark 1 / 2 och Forsmark 3; Bilagor till huvudrapporten 1.3; Metodbeskrivning för analys nivå 1 kall avställning*

FT-2006-2057. (2006). *PSA Forsmark 1 och 2; Bilagor till huvudrapporten 6.7.3; Operatörsingrepp och mänskligt felhandlande (kall avställning)*

OKG 2004-03217. (2004). *Metodbeskrivning för analys av avställning*

OKG 96-08668. (1996). *Metodbeskrivning för avställningsanalys*

OKG 2005-14606. (2005). *Oskarshamn 1 – Kapitel 1.3.5 – PSA Nivå 1 – Redovisning av behandlade operatörsingrepp*

OKG 1/A3/0005.2 . (1999). *HFA-delen inom avställningsanalysen*

Rapport (1999). *Metodbeskrivning avställningsanalys Ringhals 1*

Rapport 2006107-R-002. (2006). *Ringhals 3 and 4 SPSA – Methodology for Human Factors Analysis*, Relcon Risk Management

www.ski.se

STATENS KÄRNKRAFTINSPEKTION
Swedish Nuclear Power Inspectorate

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