SKI Rapport 02:31

Forskning

Metodutveckling - PSA Tillsynshandbok

Jämförelse med en modern PSA-studie

Urban Boström
Gunnar Jung
Yngve Flodin

Mars 2003

ISSN 1104–1374
ISRN SKI-R-02/31-SE

SKI-perspektiv

Bakgrund
SKI:s föreskrift SKIFS 1998:1 ställer krav på att Probabilistiska säkerhetsanalyser (PSA) ska genomföras och redovisas för samtliga kärnkraftsanläggningar. Som stöd för granskning av PSA har SKI tagit fram en Tillsynshandbok i ett första koncept.

SKI:s syfte
SKI:s syfte med detta forskningsprojekt är att tillämpa Tillsynshandboken i en granskning och utvärdera användbarheten och fånga in nya synpunkter, bl.a. förslag på ytterligare faktorer som kan ha stor betydelse för att kunna bedöma om PSA nivå-1, nivå-2 och s.k. rumshändelsestudier kan anses uppfylla ställda krav.

Resultat
Rapporten ger en oberoende granskares syn på Oskarshamn PSA nivå-1 studien, dessutom ger den erfarenheter tillbaka till SKI från praktisk tillämpning av Tillsynshandboken för PSA.

Eventuell fortsatt verksamhet inom området
Detta projekt är ett av två som ska ge erfarenheter som beaktas i nästa utgåva av Tillsynshandboken för PSA. Se även SKI Rapport 01:49, 02:40

Effekt på SKI:s verksamhet
Resultatet från detta forskningsprojekt har utmynnat dels i observationer som föranlett SKI att ställa krav på att OKG Aktiebolag reviderar PSA-studien, dels observationer som förbättrar SKI:s Tillsynshandbok PSA och förenklar SKI:s framtida granskningar av PSA.

Projektinformation
SKI:s projekthandläggare: Ralph Nyman
Projektnummer: 01141, 2001-06-26
Dossié-diarienummer: 14.2-01141

SKI Rapport 02:31

Forskning

Metodutveckling - PSA Tillsynshandbok

Jämförelse med en modern PSA-studie

Urban Boström
Gunnar Jung
Yngve Flodin

SwedPower AB
Säkerhetsanalys
Box 527
162 16 Stockholm

Mars 2003

Dokumenttyp	Dokumentnummer	Utskriftsdatum	Rev	Rev.datum	Uppdragsnummer
RAPPORT	**T-SEKA 02/36**				1447000

Författare	Granskad		
Urban Boström, Gunnar Jung	Yngve Flodin		
Godkänd	**Godkännandedatum**	**Antal textsidor**	**Antal bilagor**
Hans Öberg	2002-07-04	43	-
Delges			
SKI			

Metodutveckling – PSA Tillsynshandbok, jämförelse med en modern PSA-studie

Sammanfattning

Sammanfattningsvis är de viktigaste slutsatserna:

- Tillsynshandboken (TH) är ej avsedd för detaljgranskning, utan för helhetsbedömning av PSA-program
- TH ger en bild av en ”ideal”, komplett PSA-studie. Vid en jämförande granskning av en delanalys kan därför upplevas avsevärda skillnader i ambitionsnivå
- TH beskrivningar och bedömningskriterier synes oftast väl genomarbetade. Avsnitten om resultatpresentation och analys av PSA-resultat är mycket välskrivna
- Ambitionsnivån för aktuell PSA-studie (Oskarhamn 2 nivå 1) synes ha varit hög vad avser tillämpningsområden m m. Brister finns dock, bl a konstateras i rapporten att:
    - Fördjupad resultatutvärdering saknas.
    - Delanalyserna är genomförda med mycket varierande grader av konservatism.
    - CCI-analysen har formen av ett första steg i en fullständig analys. Grovt ansatta screeningvärden har använts för frekvenser. Det är inte ingående utrett om händelserna överhuvudtaget leder till en CCI.
    - Osäkerhetsanalys saknas.
    - Kriterier för känslighetsanalysen saknas.
    - Använda brand- och översvämningsmodeller är alltför ”kantiga” för analys av äldre, med moderna mått dåligt separerade anläggningar.

Ovanstående får sammantaget anses innebära stora begränsningar i analysens användbarhet som beslutsunderlag inom angivna tillämpningsområden.

Arbetet är utfört på uppdrag av kärnkraftinspektionen inom deras FOU-budget, följer av SKI anvisade skrivregler och har numrerats SKI Rapport 02:31.

INNEHÅLLSFÖRTECKNING

1. 1. SAMMANFATTNING

1.1 BAKGRUND

Så här sammanfattar SKI syftet med PSA Tillsynshandbok:

”Denna tillsynshandbok skall utgöra ett stöd i SKI:s tillsyn av den PSA-verksamhet som tillståndshavarna bedriver. Begreppet PSA-verksamhet skall ses i vid mening, och inkluderar underliggande organisation och arbetsformer hos tillståndshavarna, uppläggning och utformning av PSA:n, samt dess användningsområden och tillämpning. Vidare beskrivs SKI:s rutiner för inspektion och granskning inom PSA-området.
Utgångspunkten är kraven och de allmänna råden i SKI:s föreskrift om säkerhet i vissa kärntekniska anläggningar. Tillsynshandboken presenterar bedömningskriterier och allmänna beskrivningar som skall ligga till grund för SKI:s bedömning av om en tillståndshavare uppfyller ställda krav. Bedömningskriterierna skall dock inte ses som krav.
Tillsynshandboken är tillämpbar på alla typer av inledande händelser och alla drifttillstånd. Det bör noteras att den inte gör den traditionella uppdelningen av PSA i inre och yttre händelser, effektdrift och avställning, eller nivå 1 och nivå 2 PSA. Anledningen till detta är dels att tillsynshandboken härigenom fått en mera logisk struktur, dels att uppläggningen betonar PSA:s integrerade karaktär vad gäller skapandet av en anläggnings riskbild.
Tillsynshandboken har utformats efter de krav som ställs vid PSA-analys av kärnkraftverk, eftersom detta är den mest omfattande tillämpningen. Den gäller dock, i tillämpliga delar, även vid analys av andra kärntekniska anläggningar.”

Syftet med föreliggande forskningsuppdrag har varit att som ett delmoment i arbetet med fastställandet av PSA-handboken jämföra (delar av) dess bedömningskriterier till omfattning och innehåll med en modern PSA-studie, och identifiera de viktigaste skillnaderna.

Stor vikt har också lagts vid analysen av själva felträdsmodellen, något som varit mindre vanligt förekommande vid tidigare av SKI beställda externa granskningar av PSA-studier.

Resultaten som presenteras nedan är dock ej resultatet av någon fullständig granskning av aktuell PSA-analys.

1.2 GENOMFÖRANDE

Mot bakgrund av diskussioner med SKI, SwedPower erfarenheter från genomförda PSA-projekt mm, valdes följande principiella upplägg för uppdraget:

1) *Övergripande jämförelse* vad gäller innehåll och transparens
   - ambitionsnivå i vald PSA-analys, både vad gäller projektbeskrivningens målsättningar och faktiskt redovisad analys, i jämförelse med PSA-handbokens nivåer.

2) *Mer detaljerad jämförelse* av följande:
   - hantering av feldata för utvalda komponenter
   - antaganden beträffande rumshändelser
   - CCIer, frekvenser, är dessa realistiskt beräknade?, identifiering / kategorisering

- kreditering av icke säkerhetsklassade system
- händelseträdsmodellering
- resultatpresentationen, kan dokumentationen förstås av en icke PSA-expert?

3) *Felträdsmodellen*, speciellt
   - kreditering av batterier under längre tider
   - modellering av reglerfunktioner
   - modellering av beroenden för rumshändelser
   - kontroll av kvalitetssäkringen av information i modellen, t ex av hur pappersdokumentation översatts till den logiska felträdsmodellen

1.3 RESULTAT

Tyngdpunkten i granskningen har legat på granskningen av anläggningsmodellen. Detta återspeglar sig också i denna rapport. Kommentarerna domineras av frågor med anknytning till modellering, men också kring antaganden och förutsättningar kring densamma.

SKI säger i ingressen till Tillsynshandboken att bedömningskriterierna inte ska ses som krav, och konstaterar att den inte gör den traditionella uppdelningen av PSA (för att bl a betona PSA:s integrerade karaktär). Vid granskning mot Tillsynshandboken måste detta beaktas. En enskild PSA-studie kan inte förväntas uppfylla alla ”krav”. Anläggningens hela PSA-program måste i så fall beaktas.

På en övergripande nivå synes studien vara i nivå med andra på senare tid genomförda PSA-analyser. I relation till den nivå som beskrivs i Tillsynshandbok PSA saknas dock, inte oväntat, en del.

1.4 SLUTSATSER

Sammanfattningsvis är de viktigaste slutsatserna:

- Tillsynshandboken (TH) är ej avsedd för detaljgranskning av delanalyser, utan mer för en helhetsbedömning av ett PSA-program

- TH ger en bild av en ”idealt” genomförd, komplett PSA-studie. Vid en jämförande granskning av en delanalys kan därför upplevas en avsevärd skillnad i ambitionsnivå

- TH beskrivningar och bedömningskriterier synes oftast väl genomarbetade. Avsnitten om resultatpresentation och analys av PSA-resultat är mycket välskrivna

- Ambitionsnivån för aktuell PSA-studie synes ha varit hög vad avser tillämpningsområden m m. Brister finns dock, bl a konstateras i rapporten att:

  - Fördjupad resultatutvärdering saknas.

  - Delanalyserna är genomförda med mycket varierande grader av konservatism.

- CCI-analysen har formen av ett första steg i en fullständig analys. Grovt ansatta screeningvärden har använts för frekvenser. Det är inte ingående utrett om händelserna överhuvudtaget leder till en CCI.

- Osäkerhetsanalys saknas.

- Kriterier för känslighetsanalysen saknas.

- Använda brand- och översvämningsmodeller är alltför ”kantiga” för analys av äldre, med dagens mått dåligt separerade anläggningar.

- Ovanstående får sammantaget anses innebära stora begränsningar i analysens användbarhet som beslutsunderlag inom angivna tillämpningsområden.

SUMMARY

1.5 BACKGROUND

This is the way the SKI summarises the preliminary edition of its regulatory handbook for PSA:

” This regulatory handbook is intended to be a support in the inspection and control of the PSA activities of the licensees. The term *PSA activities* shall be interpreted in its widest sense, and includes both the underlying organisation and working procedures of the licensee, the layout and contents of the PSA, and its areas of application. Furthermore, the regulatory handbook describes SKI procedures for inspection and review of PSA:s and PSA activities.
The starting point are the requirements included in SKI:s Regulations Concerning Safety in Certain Nuclear Facilities. The regulatory handbook presents criteria to be used in the assessment of the fulfilment of requirements. However, the criteria shall not be seen as strict requirements.
The regulatory handbook is applicable to all types of initiating events and all operating conditions. It should be noted that it does not make the traditional subdivision of PSA into internal and external events, level 1 and level 2 PSA, or power operation and shut-down. The reason for this is that this has given the regulatory handbook a more logical structure, and that this approach underlines the integrated character of PSA when it comes to creating the plan risk profile.
The regulatory handbook has been structured following the requirements on a PSA for a nuclear power plant, as this is the most demanding application. However, it is applicable also to the analysis of other nuclear installations.*”*

The purpose of the comparative review presented in this report has been to, as part of a quality review establish the PSA Handbook, compare (parts of) the handbook and its criteria with a recent PSA analysis, and to identify major discrepancies.

Considerable weight has also been allocated to a review of the plant model (Risk Spectrum event trees and fault trees).

The results presented in the report are not based on a complete review of the PSA in question (or of the complete PSA Handbook).

1.6 METHODOLOGY

Following discussions between the SKI and SwedPower, and also based on the experience of the SwedPower reviewers, the following issues were chosen to be the main parts of the project:

1) General comparison according to content and transparancy
- Levels of ambition in PSA Handbook, PSA method description and actual PSA report.

2) Detailed comparison of:
- Selected component failure data
- Assumptions regarding room events
- CCI frequencies, realism, identification, categorisation
- Taking credit for non-safety classified systems
- Event tree modelling
- Presentation of results

3) *Fault tree model*, specifically
- Time frame for crediting of battery capacity
- Modelling of regulators
- Modelling of dependencies for room events
- general quality, like how the paper documentation and the logic fault tree model correspond

1.7 RESULTS

The main focus of the review has been on the plant model. The comments and conclusions are dominated by issues concerning modelling.

As of part 1.5, the criteria for the review as presented in the PSA Handbook are not to be seen as strict requirements. The layout of the Handbook does not follow the traditional PSA with its subdivision of into internal and external events, level 1 and level 2 PSA, or power operation and shut-down. The reason for this is that this has given the regulatory handbook a more logical structure, and that this approach underlines the integrated character of PSA when it comes to creating the plan risk profile. When the Handbook is used as the reference for a review of a PSA this has to be taken into consideration. One partial analysis of a PSA program can not be expected to meet all requirements of the PSA Handbook.

On a general level, the PSA in question in many ways seem to be on a satisfactory level with modern PSA standard. As expected though, in relation to the level of ambition as described in the Handbook, some areas could be improved.

1.8 CONCLUSIONS

The main conclusions can be summarised as:

- The PSA Handbook (PSAHB) is not intended to be used for detailed review of analyses, but for an overall judgement of a complete PSA program

- The PSAHB pictures an ”ideal” version of a complete PSA. During a comparative review, as the one described in this report, considerable discrepancies show up concerning level of ambition etc.

- The PSAHB, and in particular its chapters on presentation and analysis of results are well written and worth considering for any PSA analyst.

- The specific PSA analysis studied shows a high level of ambition, but as

    - A thorough analysis of the results is missing.

    - Some of the analyses are overly conservative.

    - The CCI-analysis is presented only in a ”first screening” status.

    - No uncertainty analysis is presented.

    - The criteria for the sensitivity analysis are not shown.

    - The models used for internal fire- and flooding analyses are too conservative to be applied for older, poorly separated plants.

- The above shortcomings put severe limitations regarding the use for decision making for the intended applications

2. ÖVERGRIPANDE JÄMFÖRELSE MELLAN TILLSYNSHANDBOK OCH PSA

2.1 AMBITIONSNIVÅ

SKI syfte med PSA Tillsynshandbok framgår av avsnitt 1.1 – Bakgrund i föreliggande rapport.

En smidig granskning med hjälp av Tillsynshandboken skulle förutsätta ett mer eller mindre ”standardiserat” utseende för en PSA-analys vad avser innehåll. En del av de egenskaper som efterfrågas i dokumentet måste dock tillåtas finnas på annan plats än inom ramen för själva PSA-analysen. Man kanske väljer att genomföra / redovisa analysen i olika steg som inte behöver överensstämma med Tillsynshandbokens upplägg. Delar av informationen kanske man väljer att lägga utanför själva PSA-studien (då är det naturligtvis viktigt att tydliga hänvisningar finns angivna).

Ambitionsnivån i Tillsynshandboken ger generellt uttryck för en annan och högre sådan än den som i dagens läge tycks vara inriktningen från industrin.

Den studerade PSA-studien (Oskarshamn 2 PSA) följer naturligt nog en mall från dess huvudleverantör. Den standardisering av arbetssättet som framkommer av denna och andra analyser genomförda av aktuell leverantör kan vara till fördel, t ex ur ”effektivitetssynpunkt”. Man måste dock vara vaksam på att anpassa analysen efter de stationsspecifika förutsättningarna. Vad gäller O2-studiens upplägg relativt Handbokens kriterier kan följande avvikelser ur denna synpunkt konstateras:

- ambitionsnivå sedd till angivna användningsområden visar relativt god överensstämmelse
- man har använt alltför stora konservatismer i analyserna av bl a CCI, HRA samt brand och översvämning
- resultatpresentation / tolkningar är mager, den kvantitativa delen är helt dominerande.

Övriga slutsatser från jämförelsen redovisas nedan. Först anges Tillsynshandbokens skrivningar, därefter vad som anges i Oskarshamn 2 PSA-dokumentation, och slutligen SwedPower kommentarer.

Tillsynshandboken, Allmänt:

I avsnitt 5.3 av Tillsynshandboken anges att SKI:s granskning fokuseras på studiens kvalitet, dess användbarhet inom uttalade och förväntade användningsområden, samt tolkningar av studiens resultat. Granskningen omfattar såväl PSA:ns tekniska innehåll som dess uppläggning och resultat. De viktigaste aspekterna vid en PSA-granskning har sammanfattats i tabellform, se nedan.

Tabell-1 Summering av de viktigaste aspekterna i en PSA-granskning

Tekniskt innehåll	Dokumentationskvalitet	Resultat
• Uppfyllande av tillståndshavarens kravspecifikation för arbetet • Uppfyllande av i studien angivna mål och användbarhet inom angivna användningsområden • Täckningsgrad (system, inledande händelser, fenomen, etc.) • Överensstämmelse med praxis (state of the art) inom analysområdet • Rimlig modellering av komponenter, system, och säkerhetsfunktioner (rimlighet i studiens detaljeringsgrad, beskrivning och modellering av anläggningen och av missödessekvenser) • Bakgrundsanalyser (systemkrav, fenomen, tillgängliga tider etc.) • Tillräcklig grad av samordning mellan olika delar och delanalyser i PSA:n (detaljeringsnivå, val av data och modeller) • Identifiering av kritiska förutsättningar, samt värdering av deras resultatpåverkan • Behandling av erfarenheter för system och av RO • Grad av realism i kvantitativa data och användning av relevanta drifterfarenheter • Lämplighet för framtida uppdateringar • Användbarhet generellt m.a.p. LPSA (Living PSA)	• Överordnad dokumentationsstruktur • Grad av samordning mellan olika delar och delanalyser i PSA:n (innehåll, struktur, uppläggning, format, detaljeringsnivå) • Presenterad informations kvalitet och detaljeringsnivå (begriplighet, fullständighet etc.) • Kvalitet och användbarhet i presenterade tabeller och figurer • Användning och deklaration av referenser och bakgrunds-information • Växelverkan med andra dokument (FSAR, m.m.) • Lämplighet för framtida uppdateringar	• Resultatpresentation, inklusive osäkerhets- och känslighetsanalyser samt presentation av slutsatser och kvalitativa resonemang kring dessa • Robusthet (värdering av härdskadenivå, resultat från känslighetsanalyser och medvetna konservatismer) • Acceptanskriterier • Användning av osäkerhetsanalys samt värdering av osäkerheter • Användning av känslighetsanalys • Känslighetsanalys av viktiga förutsättningar och begränsningar • Jämförbarhet (t.ex. mellan resultat från analys av rumshändelser och processrelaterade inre händelser)

Detta är alltså riktlinjer för SKI:s egen granskning av redovisade PSA-analyser. De flesta av dessa punkter torde vara relevanta granskningsområden även för tillståndshavarens egen granskning av PSA.

Tillsynshandboken, kap. *7 Tillämpning av PSA*

Detta kapitel behandlar de krav som bör ställas på tillämpningar av PSA i olika sammanhang. Ordet *tillämpning* har här en vid betydelse och avser alla situationer där PSA-resultat eller -modeller används för att generera beslutsunderlag i frågor med kan ha säkerhetsmässig betydelse. Det kan röra sig både om resultatanalys i samband med att en PSA färdigställs för första gången och senare analyser som utnyttjar en existerande PSA.

Eftersom utgångspunkten i båda fallen är en färdig PSA, diskuteras först PSA:s möjliga användningsområden och presentationen av resultat i en PSA. Därefter diskuteras generella frågor som berör PSA-tillämpning, såsom beslutskriterier och jämförelse av PSA-resultat.

Följande delavsnitt ingår i kapitlet:

Användare och användningsområden	*Behandlas även i bilaga 2.1*
Resultatpresentation	*Behandlas även i bilaga 2.2*
Beslutskriterier	*Behandlas även i bilaga 2.3*

Jämförbarhet *Behandlas även i bilaga 2.4*

7.1 Användare och användningsområden

De krav som bör ställas på en PSA grundas ytterst på det sätt på vilket man vill använda PSA:n och dess resultat. Det är därför naturligt att inledningsvis diskutera vilka användningsområden som kan vara relevanta för en PSA. En sådan diskussion bör i sin tur utgå från användarna av en PSA och deras behov.

Specificeringen av användningsområden är således en viktig utgångspunkt för genomförandet av en PSA, eftersom dessa områden direkt eller indirekt kommer att ställa krav på PSA:ns förutsättningar och uppläggning samt på utformning och innehåll i PSA:ns resultatpresentation. En följdfråga är vilka typer av resultat som krävs inom dessa användningsområden; detta behandlas i avsnitt 7.2, ” Resultatpresentation”.
En fördjupad beskrivning ges i bilaga 2.1.

SKI:s krav och bedömningskriterier

Användare och användningsområden bör beskrivas i PSA:n, och det skall framgå att beskrivningen baseras på en analys.

Om en PSA används inom ett område som ej ursprungligen specificerats, bör detta påpekas och det bör visas att användningen ger relevanta resultat.

Förväntad framtida användning av en PSA bör beaktas; exempelvis bör en PSA nivå 1 alltid utföras på ett sätt som tillåter en framtida utvidgning till nivå 2.

En PSA bör, förutom att kunna användas av tillståndshavarnas säkerhetsavdelningar, även fungera som en redovisning till SKI (samhället) som visar att anläggningen är tillräckligt säker. Dessutom bör andra intressenter med god kunskap om kärnkraftverk, men som inte är PSA-experter, kunna överblicka och förstå PSA:n och dess resultat.

PSA:n bör användas inom följande områden:
Identifiering av relativa svagheter i anläggningen, d.v.s. identifiera och prioritering av säkerhetshöjande åtgärder som skall genomföras i anläggningen
Utvärdering av planerade eller genomförda anläggningsändringar
Utvärdering av inträffade händelser
Utvärdering av planerade eller genomförda ändringar i STF eller FSAR
Värdering av anläggningens risknivå mot säkerhetsmål
Utvärdering av dispenser från SKIFS 1998:01

Dessutom bör användning inom följande områden vara möjlig (eventuellt efter viss anpassning):
Optimering av test- och provintervall
Tidsberoende riskuppföljning
Trendindikatorer

Härutöver kan tillståndshavaren själv ha specificerat ytterligare användningsområden. Om så har skett, bör det visas att studien är utformad på ett sätt som tillåter användning även inom dessa områden.

Krav på redovisning till SKI av PSA-tillämpningar styrs av SKIFS 1998:1.

Ändringar i anläggningen och ändringar i eller tillfälliga avsteg från de säkerhetstekniska driftförutsättningarna skall anmälas till SKI. Om SKI baserat på anmälan väljer att ta in underlaget i ett ärende skall detta inkludera PSA-analyser i de fall detta är tillämpligt
(4 kap. 6 § och 4 kap. 1 §).

O2 PSA - 2.1.1 Kap. 1 – Introduktion till PSA O2, reg.nr. RELCON 95131/1 rev. 3 samt Sammanfattningsrapport OKG 2/A3/0001.134, 1999-04-23

Som målsättning anges här (kap. 1.3) bl a att man via beräkningar av härdskadefrekvenser ska kunna dra slutsatser rörande anläggningens säkerhetsnivå. Beroenden och värdering av förbättringsåtgärder ska kunna identifieras, och krav på anläggningen verifieras.

Som användningsområden anges
- Säkerhetsvärdering (beroenden ska identifieras / värderas)
- värdering av anläggningsändringar (identifiering / värdering av förbättringar)
- riskuppföljning (verifiering av probabilistiska krav)
- optimering av provningsintervall
- bestämning av reparationskriterier

Dessa verkar vara i rimlig överensstämmelse med Tillsynshandboken enligt ovan.

PSA-O2 ska dessutom vara grunden för en nivå 2 analys och en ned-/uppgångsanalys. Det anges dock inte vad detta praktiskt innebär för arbetet med nivå-1 studien.

Det anges ej explicit vilka de tänkta användarna av studien är (kraftverksledning, konstruktörer, PSA-experter, säkerhetsavdelningar, ….?

En fråga i Tillsynshandbokens ACCESS-databas är om PSA:n och dess resultat kan överblickas och förstås av intressenter med god kunskap om kärnkraftverk, men som inte är PSA-experter?
Allmänt kan sägas att det är svårt att anpassa en PSA så att en icke PSA-expert på egen hand kan överblicka och förstå PSA:n. En viss nivå på PSA-kunskap krävs. Det är ofta lämpligt att avsluta en PSA-studie med ett seminarium (kanske också en kurs) som presenterar metodik och resultat. När man identifierat användarna bör man se över tydligheten i dokumentationen. Frågeställningen är mycket viktig bl a för att öka acceptansen av PSA-metodiken. (Det allra bästa sättet att inge förtroende för en PSA är förstås att anläggningspersonalen är i hög grad involverad under arbetets gång!)

Vissa delar av aktuell analys är relativt lättlästa, andra delar kanske behöver förtydligas (t ex en anvisning om hur man tolkar diagrammen i Kap. 7.2, Resultat för resp. konsekvens).

Ytterligare en fråga i ACCESS-databasen behandlar användbarheten inom angivna användningsområden. Modellen / verktyget (Risk Spectrum) är i det stora hela användbart för angivna områden. Viss reservation måste göras för hur tidskrävande vissa beräkningar visat sig vara med de senaste komplexa modellerna. Också andra generiska brister, t ex avsaknaden av osäkerhetsanalys kan påverka användbarheten negativt. Varierande grad av konservatismer / icke-konservatismer kan dessutom snedvrida resultatbilden och försämra resultatens användbarhet som underlag för olika former av beslutsfattande.

Tillsynshandboken – Kap. 6.3 PSA-dokumentationens status och dokumentkontroll

PSA-dokument är komplexa, eftersom de består både av skriven dokumentation och av en datorbaserad anläggningsmodell.
I tillsynshandbokens beskrivning av PSA:ns olika delmoment (kapitel 8) uttrycks krav på dokumentationen av analysen, liksom i kapitel 3-7 av tillsynshandboken. Dessa krav upprepas inte i detta avsnitt. I stället är avsikten att summera generella krav på dokumentationen av delanalyserna.
En fördjupad beskrivning ges i bilaga 1.3.

SKI:s krav och bedömningskriterier

Tillståndshavaren skall ta fullt ansvar för PSA-rapporten.

PSA:n bör innehålla all relevant information. Analysen och dess beskrivning skall vara begripliga för studiens målgrupp.

All väsentlig information i PSA:n skall vara dokumenterad och möjlig att få fram. Baserat på redovisad information och referenser bör det dessutom i princip vara möjligt att reproducera samtliga resultat i en studie och genomföra värdering av hela PSA-projektets kvalitet.
Not: Detta innebär att om en bedömning eller värdering i PSA:n baseras på någon form av analys, bör denna antingen redovisas i sin helhet, eller vara lokaliserbar genom att en fullständig referens ges. Detta gäller exempelvis bakomliggande analyser, använda modeller, antaganden och förutsättningar samt använda data.

Om en referens ges till ett större dokument (t.ex. FSAR eller annan PSA) bör den vara specifik, d.v.s. identifiera relevant avsnitt.

PSA-dokumentationens bör behandlas som anläggningsteknisk dokumentation (liknande FSAR och STF).

Tillståndshavaren bör utse personer ansvariga för dokument och datorfiler.

Tillståndshavaren bör tillse att dokumentationen kontrolleras och underhålls i ett granskningsbart skick.

O2 PSA - 2.1.1 Kap. 1 – Introduktion till PSA O2, reg.nr. RELCON 95131/1 rev. 3

Dokumentationen ska uppfylla kraven på spårbarhet, fullständighet och förståelse.

Under kap. 1.7 Granskning sägs att ”Avseende PSA-modellens korrekthet har granskningen genomförts mot blockdiagram, kravmatris, FMEA samt genom att granska rimligheten i erhållna resultat”.

SwP kommentar:

Granskning av resultat avslöjar normalt endast modelleringsfel som ger ett för högt resultat. Om icke-konservativa antaganden, data, modeller etc. används så avslöjas det knappast enbart med en granskning av numeriska resultat och cut-set-listor.

Kontroll av referenser mm till huvudrapporten har ej ingått i omfattningen av detta uppdrag.

2.2 TEKNISKT INNEHÅLL

2.2.1 RUMSHÄNDELSER, ANTAGANDEN MM

Tillsynshandboken Bilaga 3.1.6 Rumshändelser

Identifiering av rumshändelser

Rumshändelser kan karaktäriseras av att de genom någon fysikalisk mekanism påverkar utrustningen i ett rum.
Fysikaliska mekanismer som kan komma i fråga är:
Brand (hetta, rökgaser)
Översvämning (vatten, ånga)
Fysisk åverkan (detonation/deflagration, missiler, jetstrålar)
Kemisk miljö (gaser, damm)
Joniserande strålning

Rumshändelsen inträffar utanför den ordinarie processen, och kan direkt eller indirekt påverka anläggningens säkerhetssystem. Rumshändelsen medför också att nya beroenden mellan komponenter skapas – rumsberoenden. Med rumsberoenden avses det sätt på vilket en komponent (funktion) direkt eller indirekt är beroende av utrustning i olika delar av anläggningen. En stor del av rumshändelseanalysen går ut på att fastställa detta beroende. Identifiering av viktiga rumshändelser kräver därför att komponenters (funktioners) rumsberoende kartlagts på ett tillräckligt detaljerat sätt.

Kategorisering av rumshändelser

Kategorisering av rumshändelser utförs normalt inte då säkerhetspåverkan av olika rumshändelser starkt varierar. Bortfall av ett rum utgör därför normalt en separat inledande händelse. Möjligheten att förenkla analysen genom att gruppera inledande händelser är därför starkt begränsad.

Gruppering av rum skall dock genomföras i vissa fall, såsom:
Bildande av uppsamlande utrymmen inom “Översvämningsanalys”
Bildandet av miljöpåverkad zon inom “Ångfrigörelseanalysen”
Bildandet av brandceller (omfattar normalt flera rum)
Vid känslighetsanalys av brandspridning

Frekvens för rumshändelser

Brand: Version 1 av X-Boken [8] omfattar en komplett redovisning av frekvenser för s.k. begynnande brand inom anläggningen. Frekvenserna är beräknade per anläggning, och inom varje anläggning per anläggningsdel (byggnad). Skattningen är gjord på basis av ett statistiskt material som för ändamålet insamlats från svenska och finska (TVO) kärnkraftverk. För PSA-ändamål måste brandfrekvensen per byggnad ytterligare splittras upp på enskilda rum eller brandceller. En sådan metod är Berry´s metod [9] där man med hjälp av checklistor bestämma den relativa sannolikheten för branduppkomst för varje rum i de aktuella byggnaderna.

Översvämning: För att kunna hantera utflödesfall (översvämningsanalyser) måste utflödesfrekvenser och relevanta utflödeskategorier bestämmas för olika utrymmen i anläggningen. I rapport [10] presenteras en skattning av frekvenser för “stora” läckage dels per anläggning och system, dels per system och objekttyp.

SwedPower kommentarer:
Tillsynshandboken ger enligt ovan få råd eller rekommendationer för utvärdering av rumshändelser.

I O2-PSA har två rumshändelser analyserats, översvämning respektive brand, men det framgår ej närmare hur man identifierat behovet av att analysera just dessa två och utelämnat övriga rumshändelser.

Den fysikaliska mekanism som påverkar utrustning vid översvämning är vattendränkning. Påverkan via ånga ingår ej eftersom utflöden från hetvatten eller ångsystem inte är analyserade. Vid brand anges ej specifikt om påverkan sker från själva branden, hög temperatur eller rökgaser.

För analysen av rumshändelser har komponenters / funktioners rumsberoenden kartlagts och kopplats till anläggningens respektive rumsnummer. Varje rumshändelse betraktas som en egen inledande händelse och har utvärderats med händelseträd TT, turbinsnabbstopp med dumpförbud. Utvärdering sker "rumsvis" och utrustning i rummet som är känslig för respektive händelse betraktas som utslagen. För brand har utvärdering genomförts även för hel brandcell och för översvämning har utvärdering även gjorts med hel "översvämningscell".

För beräkning av frekvens för inledande händelse brand har X-bok använts i kombination med Berry's metod för fördelning av byggnadens frekvens på rum. Frekvens för översvämning har hämtats från NUREG/CR- 2300 och byggnadens översvämningsfrekvens har fördelats på ett antal rum med kallvattensystem.

Vid jämförelse av O2 rumshändelseanalys mot tillsynshandbokens råd noteras sammanfattningsvis följande

- process för identifiering av rumshändelser saknas
- utvärdering av utflöden från hetvatten- och ångsystem saknas
- utflödesfrekvenser hämtas lämpligen från "Skattning av utflödesfrekvenser i nordiska kärnkraftverk”, SKI Rapport 99.01.

2.2.2 FELDATA

Tillsynshandboken Kap 8.7 Analys av erfarenhetsdata

Dataanalysen har beröringspunkter med flertalet övriga delmoment i PSA:n. Normalt utförs dock endast delar av analysen som separata aktiviteter. Detta beror på att ansättningen av relevanta data ingår som en integrerad del i vissa delanalyser; främst gäller detta analyserna av inledande händelser, manuella ingrepp och beroenden (CCF).

Detta delavsnitt omfattar därför i första hand generella aspekter på dataanalys och användning av erfarenhetsdata. En fördjupad beskrivning ges i bilaga 3.6.

Dataanalys inom specifika delanalyser diskuteras i följande bilagor:
Bilaga 3.1: Data för inledande händelser
Bilaga 3.3: Data för komponentfel
Bilaga 3.3: Data för test och underhåll
Bilaga 3.4: Data för manuella ingrepp
Bilaga 3.5: CCF-data

PSA:n bör fortlöpande uppdateras med aktuella data. En kartläggning av tillgängliga och relevanta datakällor bör göras som en del av PSA:ns dataanalys. Där så är möjligt bör använda data baserade på den analyserade anläggningens drift. I andra hand (för mera sällsynta händelser/feltyper) kan även data för andra anläggningar av samma typ användas. I vissa fall kan det vara befogat att använda generiska data; detta gäller händelser eller feltyper som kan antas vara oberoende av specifik anläggning.

En genomgång av under analysperioden inträffade rapportervärda omständigheter bör ingå i PSA, eftersom det är endast i dessa som inträffade avvikelser från konstruerad säkerhetsnivå analyseras. Genomgången kan ge viktiga uppslag till känslighetsanalyser.

Ingenjörsmässiga antaganden skall om möjligt undvikas. Om de ändå används skall de vara väl underbyggda.

Förenklande konservativa ansatser är normalt acceptabla endast om riskpåverkan är liten.

Data för osäkerhetsanalys bör ej bestämmas i en gemensam aktivitet (osäkerhetsanalys), utan parallellt med att grunddata inom olika delområden bestäms. Osäkerhetsanalysen bör således inte vara en separat aktivitet, utan endast kvantifiera redan fastlagda data.

Alla data som använts i en PSA bör lagras i databas och listas i appendix, tillsammans med referenser och eventuella kommentarer till valet av data, ingenjörsmässiga bedömningar etc.

Tillsynshandboken Bilaga 3.6.5 Användning av erfarenhetsdata

En anläggningsspecifik PSA:n skall inte bara korrekt modellera anläggningens tekniska system och dessas inbördes växelverkan och beroenden, utan även beakta den analyserade anläggningens drifterfarenheter.

Där så är möjligt skall använda data baseras på den analyserade anläggningens drift. I andra hand (för mera sällsynta händelser/feltyper) kan även data för andra anläggningar av samma typ användas. Viktiga exempel på anläggningsspecifika data är de data som presenteras i I-boken och T-boken.

I vissa fall kan det vara befogat att använda generiska data; detta gäller händelser eller feltyper som kan antas vara oberoende av specifik anläggning. Exempel är frekvenser för vissa yttre händelser och felsannolikhet för mindre standardkomponenter (dvärgbrytare, reläer etc.). Vid användning av generiska data skall dock om möjligt alltid en rimlighetskontroll göras genom avstämning mot egna drifterfarenheter.

Det är viktigt att i PSA-arbetet även ha en överblick över relevanta internationella data som används i aktuella utländska PSA samt internationell praxis med avseende på dataanalys.
Som framgår av ovanstående kan inte sättet att utnyttja erfarenhetsdata specificeras strikt, utan blir delvis en bedömningsfråga. Därför skall PSA:n inkludera en beskrivning av de analysprinciper som följts.

Exempel på områden där anläggnings- eller erfarenhetsdata skall användas är:
Frekvens för inledande händelser
Frekvenser för vanligt förekommande inledande händelser
Transientfrekvenser
CCI-frekvenser
Feldata för aktiva komponenter
Tider för förebyggande och avhjälpande underhåll
Frekvens för tester och förebyggande underhåll
En mera kvalitativ användning av anläggnings- eller erfarenhetsdata inkluderar:
Anpassning av anläggningsspecifika (såväl som generiska) rörbrottsfrekvenser för inre som yttre rörbrott
Utvärdering av system- eller komponentspecifika erfarenheter

Under analystiden inträffade rapportervärda omständigheter (RO), snabbstopp (SS), viktigare komponentfel (AO), underhåll (AU och FU), beroendefel (CCF), och fel som inkluderar manuella felgrepp (MTO)

Not: En genomgång av rapportervärda omständigheter (RO) bör ingå i PSA, eftersom det är endast i dessa som inträffade avvikelser från konstruerad säkerhetsnivå analyseras. Eftersom det är den konstruerade säkerhetsnivån som modelleras i PSA:n, kan genomgången bl.a. ge viktiga uppslag till känslighetsanalyser.

Ofta baseras systemanalyser i hög grad på ett formellt underlag, d.v.s. kretsscheman etc. Som en komplettering, bör en summering av drifterfarenheter för systemen redovisas i systemanalyserna, och vid behov även tillåtas påverka modelleringen.

Utnyttjade dispenser, t.ex. från STF skall beaktas (hindertider, reparationstider, övriga lärdomar)

Aktiveringsdata för säkerhetsrelaterad utrustning

Identifiering av reparerbara och icke reparerbara komponenter (i recoverysituationer)
Specificering av avställningsperioden, d.v.s. beskrivning av dess uppläggning och tidplanering. Detta möjliggör specificering av faser med likartade driftförhållanden och systemkrav.

SwedPower kommentarer:

Spårbarheten på indata som bygger på ingenjörsmässig bedömning är överlag dålig. Underhåll i App. E6 är klart och redigt. Dock förekommer några skiljaktigheter mellan RiskSpectrum-fil och App. E6.

Varför presentera sådana feldata som 354DR___EX5_____C? (CCF för exakt 5 drivdon) Värdet 3,8E-16 säger endast att man skapat en CCF-händelse och att man antagligen har glömt bort något mycket viktigt.

Händelsen !516-SS(2/3)-AS__H (1E-10) (Utebliven SS till 314 och HC-pumpar) har genom ett antagande strukits från listan av händelser som kan påverka otillgängligheten.

Obefogat stopp 351-pump är ej modellerat. Systemet nyttjas även för spädmatning varför obefogat stopp inte behöver vara försumbart. Även om T-boken version 4 ej innehåller "obefogat stopp kolvpump" så kan sådana stopp ske i realiteten.

För utebliven öppning för samtliga backventiler i snabbstoppsledningarna gäller att "failure rate" är lika med T4-19.1 dividerat med 2. Hur verifieras faktorn 2?

MVSS-funktionen kan i teorin utebli om t.ex. värmningen av MVSS bortfaller och temperaturen sjunker tillräckligt mycket. Varifrån kommer data till parametern 362MVSS (1E-3) till händelsen "Utebliven värmning MVSS"?
Är sannolikheten verkligen noll för låg temperatur som leder till att MVSS fryser?
Detta antagande gör parametern 32MVSS ointressant då värmning icke behövs i modellen.

För underhåll används STF-kriterierna. Det är konservativt, men är det en realistisk uppfattning för alla komponenter?

2.2.3 CCI:ER

Tillsynshandboken Kap 8.2 Inledande händelser

En inledande händelse kan definieras och beskrivas som en händelse, utrustningsfel eller störning som kommer att kräva automatisk eller operatörsinitierad övergång för att föra verket till ett säkert och stabilt läge. Detta ställer krav på säkerhetsfunktioner för att kontrollera reaktivitet, härdens säkra kylning, etc. I avsaknad av någon säkerhetsfunktion kan ett oönskat sluttillstånd existera.

En speciell typ av inledande händelser är s.k. Common Cause Initiators (CCI). En CCI innebär bortfall av hjälpsystem eller av andra funktioner som dels medför transient eller behov av avställning, dels medför bortfall eller degradering i ett eller flera av de säkerhetssystem som förväntas fungera efter händelsen. Exempel är processhändelser med funktionella beroenden, rumshändelser och externa händelser. För de två sistnämnda täcks detta problem in som en inherent del i metodiken att analysera dessa händelse, medan processhändelser kräver att funktionella beroenden studeras noga.

Omfattningen av studien som helhet påverkar även omfattningen av analysen av inledande händelser, och de typer av händelser som kommer att innefattas i kartläggningen av inledande händelser.

Analysen av inledande händelser omfattar tre steg:
Identifiering: att granska anläggningens konstruktion och drifterfarenheter för att identifiera händelser eller transienter som kan leda till ett oönskat sluttillstånd.

Kategorisering: att bestämma anläggningsspecifika villkor som skapas av inledande händelser och att gruppera händelser som har likartade effekter.
Kvantifiering: att bestämma frekvenser för inledande händelser.

En fördjupad beskrivning ges i bilaga 3.1.

SKI:s krav och bedömningskriterier

Alla inledande händelser inom studiens omfattning och som med ej försumbar frekvens antingen utgör primärmissöden, eller som har potential att utvecklas till missöden, bör identifieras och analyseras.

Not: Gränsen för försumbar frekvens kan inte definieras exakt, inte minst p.g.a. den stora osäkerheten vid skattningen av frekvens för sällsynta händelser med allvarlig konsekvens. Praxis i Sverige för PSA nivå 1 har varit att inkludera händelser med frekvens över $1*10^{-7}$/år.

Inledande händelseanalysen bör utföras för alla händelser som innefattas i studiens definition av omfattning (utsläppskategorier, driftmoder, händelsetyper, etc.).
Enligt definition av studiens omfattning skall alla typer av inledande händelser identifieras. Detta innebär t.ex. händelser som:
Processhändelser: Händelser som ligger inom processen, s.k. inre händelser.
Rumshändelser: Yttre händelser som inträffar utanför processen, inom anläggningen.
Yttre händelser: Yttre händelser som inträffar utanför processen, utanför anläggningen.
Analysen bör, genom en systematisk analys, försöka att generera en fullständig uppsättning inledande händelsegrupper och försöka bevisa att alla tänkbara händelser täcks in.
Yttre händelser bör värderas m.a.p. konsekvens och att probabilistiska måltal uppfylls.

Common cause initiators (CCI) kräver en noggrann analys för att försäkra att dessa händelser identifieras. Anläggningsmodellen utgör ett viktigt verktyg för kartläggning och identifiering, och skall användas. Komponenters (funktioners) rumsberoende skall kartläggas på ett tillräckligt detaljerat sätt för att identifiering av viktiga rumshändelser och CCI:er skall kunna ske.

Tillsynshandboken bilaga 3.1.8 CCI-händelser

En speciell typ av inledande händelser är Common Cause Initiators. CCI är bortfall av hjälpsystem eller av andra funktioner som dels medför transient eller behov av avställning, dels medför bortfall eller degradering i ett eller flera av de säkerhetssystem som förväntas fungera efter händelsen.

Identifiering och kategorisering av CCI:er

CCI-kartläggning kan delas in i tre delar,
Processhändelser med funktionella beroenden
Rumshändelser
Externa händelser

För de två sistnämnda täcks detta problem in som en inherent del i metodiken att analyseras dessa händelse som beskrivits tidigare. Detta avsnitt koncentreras därför på processhändelser och problematiken kring funktionella beroenden.

MLD tekniken (Master Logic Diagram) baseras på att systematiskt variera fundamentala mekanismer i huvudprocessen. Tekniken identifierar dock inte CCI:er primärt; det är nödvändigt att separat genomföra en systematisk sökning efter CCI:er.

Felträdsmodellen kan och skall användas som grund för identifiering av CCI:er. Metodiken kan liknas vid en felmods- och effektanalys (FMEA) som leder till att relevanta CCI:er identifieras genom:
att identifiera alla kopplingar mellan säkerhetssystemens tillgänglighet och driftpåverkan,
att visa funktionella beroenden mellan å ena sidan drift- och säkerhetssystem och å andra sidan servicefunktioner som kan påverka dessa system, och
att för varje CCI klarställa på vilket sätt den medför transient samt vid vilken tidpunkt detta sker.

En händelse som kan leda till en CCI utvärderas vidare i en enkel kvantitativ värdering för att bestämma om händelsen är tillräckligt viktig för att utvärderas fullständig i händelseträdsmodellen.

Följande huvudområden för identifiering kan nämnas:

Förlust av processkontroll. En analys av processkontroll inkluderar både mätning och kontroll av processparametrar. En mängd parametrar, effekt, nivå, tryck, flöde, temperatur, fukt etc. används för att styra och kontrollera anläggningen. Förlust av någon parameter kan innebära avställning och funktionell degradering av något eller några säkerhetssystem.
Felaktig nivåmätning
Obefogade isoleringar

Förlust av kraftförsörjning. Alla händelser i elsystemen som kan medföra avställning och funktionell degradering av något eller några säkerhetssystem skall identifieras.
Yttre nätbortfall
Förlust av specifika likströms- eller växelströmsskenor

Förlust av hjälpsystem. Fel i hjälpsystem, som t.ex. kylning eller manöver, kan medföra degradering av säkerhetsfunktioner och behov av avställning.
Förlust av instrumentluft
Förlust av kylvatten
Förlust av sekundära kylsystem
Förlust av tryckluft

Komponentfel i säkerhetssystem. Komponentfel i säkerhetssystem som medför degradering av säkerhetsfunktionen och behov av avställning.

Interfacing LOCA (ILOCA). Detta innebär oavsiktlig trycksättning av lågtryckskretsar med reaktortryck; t.ex. trycksättning av 321 lågtryckskrets. Eftersom konsekvenserna av en ILOCA kan vara mycket allvarlig ut risksynpunkt bör ett avsnitt finnas som behandlar detta.
Hantering av översvämning efter yttre LOCA,YLOCA. Här finns en koppling till översvämningsanalysen, som måste beskrivas. Korrekt hantering är att analysen görs i översvämnings-PSA:n, med samma metoder och antaganden som gäller för övriga utvalda rum.

Frekvens för CCI:er

Identifierade CCI kan frekvensmässigt redan vara inkluderade i existerande kategorier av inledande händelser. En klarare definition av dessa kan krävas. Frekvensmässigt blir påverkan i detta fall normalt liten, eftersom CCI-frekvenserna normalt utgör en bråkdel av de mera generella transientkategoriernas totala frekvens.

Frekvensbestämningen för identifierade CCI kan, p.g.a. begränsat erfarenhetsunderlag vara svår att göra men är mycket viktig eftersom CCI kan ge signifikanta riskbidrag. Att utnyttja ingenjörsmässiga bedömningar är normalt inte acceptabelt.

SwedPower kommentarer:

Analysen av CCI redovisas i kap. 3, kap. 4 samt kap 6.4.

Den kan indelas i
1 Processkontroll
2. Elsystem
3. Hjälpsystem

Frekvenserna verkar i flertalet fall framtagna med hjälp av s k ingenjörsmässig bedömning. Denna bedömning ger samma frekvens för de flesta hjälpsystem, vilket starkt kan ifrågasättas.

1. Processkontroll

I processkontrollen har man endast funnit CCI p g a brott på impulsledningar. Hur leder brott i 541 impulsledningar en ledning till CCI ? Varifrån kommer frekvensen 1E-4?

Spårbarheten på indata som bygger på ingenjörsmässig bedömning är överlag dålig.

2 Elsystem

Bortfall av i stort sett samtliga skenor antas leda till CCI. På samma gång finns för dessa skenor underhåll som enligt App. 6 kan pågå i dygns- (vecko-) skalan. Bortfall borde antingen leda till CCI eller otillgänglighet under drift. Eftersom el-CCI:er har stor inverkan på totalresultatet bör detta utredas närmare.

3. Hjälpsystem

För hjälpsystemen har samtliga inledande händelser frekvensen 1E-3 utom 711 som har en 10-potens lägre värde. (Enligt ABB rapport PAC 97-025 (koncept)). Hjälpsystemen har en underordnad betydelse för totalresultatet men de tillhuggna frekvenserna borde förklaras tydligare.

Leder bortfall av samtliga hjälpsystem till omedelbar CCI eller kan man undvika CCI m h a recovery? Om detta är möjligt (för 733 t ex) borde inte frekvenserna vara så likartade.

Sammanfattningsvis:

CCI-analysen har formen av ett första steg i en fullständig analys. Man har grovt ansatt konservativa värden på de händelser som möjligtvis kan leda till CCI. När detta har skett och resultaten har evaluerats borde steg två inletts. Fall med försumbar inverkan lämnas därhän. För de fall som har en märkbar påverkan fortsätter arbetet. Utred om de verkligen leder till CCI och om så är fallet gör en bättre uppskattning av frekvensen. Tyvärr har detta steg två icke inletts utan resultaten från screeninganalysen presenteras utan att det ens kommenteras i resultatkapitlet. Slutsatsen är att man genomfört en CCI-analys vars resultat är av begränsat värde.

2.2.4 EJ SÄKERHETSKLASSADE SYSTEM

SwedPower kommentarer:

Vi har ej hittat något i Tillsynshandboken kring detta. Generellt gäller dock att PSA ska vara så realistisk som möjligt och därför ska alla relevanta system/funktioner beaktas i analysen.

Matarvattensystemet (312) förstärker spädmatningsfunktionen men icke med samma dignitet som de säkerhetsklassade 323 och 327 som har RI-faktorer som är ca 250 och 25 gånger större.

För resteffektkylningen har man tillgodoräknat sig RAMA-systemen. Dessa system blev installerade och validerade för svåra haverier. När man tillgodoräknar sig RAMA systemen

sänks HS3 (HS p g a bortfall av resteffektkylningen) med ca en faktor 100. Systemen är säkerhetsklassade men är systemen/instruktionerna anpassade för detta driftsätt/förfarande?

2.2.5 HÄNDELSETRÄDSMODELLERING

Tillsynshandboken Kap 8.3 Sekvensanalys

Sekvensanalysen bedrivs i grunden med samma syfte och delvis med samma verktyg och metoder i nivå 1 och nivå 2 PSA. Den skall, utgående från ett initialtillstånd (inledande händelse eller stationstillstånd) verifiera och modellera anläggningens respons och händelsens fortsatta utveckling. Den skall vidare karakterisera de olika sluttillstånd som denna utveckling kan resultera i. Det faktiska genomförande av de olika delanalyser som ingår i sekvensanalysen skiljer sig dock avsevärt mellan nivå 1 och nivå 2 PSA.

I sekvensanalysen modelleras anläggningens respons på analyserade inledande händelser. Denna respons blir normalt olika för varje i PSA:n modellerad inledande händelse. Sekvensanalysen beaktar den direkta eller indirekta inverkan som den inledande händelsen har på säkerhetssystem eller hjälpsystem, tidsmässiga aspekter i utvecklingen av ett missöde och de kapacitetskrav som ställs på inblandade aktiva system.
Sekvensanalysen växelverkar med flertalet andra delanalyser i PSA:n, såsom analysen av inledande händelser, systemanalys, analysen av manuella ingrepp m.m., vilket medför att höga krav ställs på planering, genomförande och dokumentation av analysen.
En fördjupad beskrivning ges i bilaga 3.2.

SKI:s krav och bedömningskriterier

Säkerhetsfunktioner för alla inledande händelser, drifttillstånd och sluttillstånd som ingår i analysen skall definieras i PSA:n.

Säkerhetssystem, hjälpsystem och mänsklig växelverkan som aktivt eller passivt bidrar till att säkerhetsfunktioner etableras och upprätthålls skall identifieras.

Systemkrav bör vara realistiska. Detta gäller både kapacitetskrav och tidsmässiga randvillkor för systemet. Kraven skall baseras på FSAR eller verifierande beräkningar av mer realistiska krav

Not: Konservativa ansatser kan accepteras som del i en sållning (screening) eller om riskpåverkan är ringa.

Sekvensanalysen skall på ett korrekt och realistiskt sätt beaktar den direkta eller indirekta inverkan som den inledande händelsen har på säkerhetssystem eller hjälpsystem.

Not: Exempel är följdbrott i konsekvenslindrande system vid LOCA, systempåverkan vid CCI, och fysisk anläggningspåverkan vid rumshändelser eller yttre händelser.

Rimlig kredit bör tas för återställning av felande system (recovery).

Sluttillstånd bör definieras baserat på syftet med analysen. Även förutsättningarna för sluttillstånd utan härdskada bör beskrivas.

Sekvenser utan härdskada/utsläpp bör analyseras till en tidpunkt då ett säkert tillstånd etablerats. Kriterierna för ”säkert tillstånd” skall beskrivas och motiveras
Nivå 1-modellen bör utformas så, att en relevant uppsättning stationstillstånd (PDS, plant damage states) kan fås i nivå 2-analysen.

Generellt gäller att om delar av en PSA genomförs separat, tidsmässigt eller av annan projektgrupp, bör sekvensanalysen planeras så, att den täcker in även separat genomförda delar. Detta kan gälla t.ex. PSA för rumshändelser eller nivå 2 PSA.

För sekvensanalysen i nivå 2 PSA gäller följande specifika krav:
Alla händelser som i PSA nivå 1-studien ger ett inte försumbart bidrag till härdskadefrekvensen bör följas upp med avseende på hur de påverkar reaktorinneslutningen.

Not: Även sekvenser som ger ett försumbart bidrag till härdskadefrekvensen kan ge ett signifikant bidrag till frekvensen för stora utsläpp

Boolesk koppling bör finnas mellan nivå 1 och nivå 2 PSA.

För att analysera inneslutningens funktion efter ett härdsmälteförlopp bör händelseträdsteknik utnyttjas.

Alla fysikaliska fenomen som kan uppträda i samband med svåra haverier och hota inneslutningens integritet bör beaktas.

Verifierad och kvalitetssäkrad beräkningskod samt indata skall användas i haveri- och utsläppsanalyser.

I analysen bör det upprättas en adekvat uppsättning av konsekvenser och sluttillstånd för inneslutningens händelseträd, som beskriver olika händelsesekvensers karaktäristik avseende utsläppsstorlek, tidsintervall m.m.

Varje sluttillstånd bör innehålla en riskbedömning, en karakterisering av utsläppens storlek, tidsperiod och sammansättning samt eventuella andra aspekter som kan vara viktiga för att bedöma utsläppens konsekvenser.

Minst en deterministisk utsläppsberäkning bör genomföras för en representativ sekvens i varje utsläppskategori.

En känslighetsanalys av resultaten bör göras och är särskilt väsentlig för de fenomen vars konsekvensuppskattningar och uppkomstsannolikheter innehåller stora osäkerheter. För att möjliggöra detta fordras även modellering av fenomen som bedöms ge försumbart bidrag till riskbilden.

Tillsynshandboken Bilaga 3.2.6 Händelseträdsanalys

Varje händelseträdsmodell skall på ett realistisk sätt och i tillräcklig detalj modellera händelseutvecklingen givet en inledande händelse. Detta innebär en informationsinsamling enligt tidigare avsnitt, samt utveckling av en logik som beskriver denna händelseutveckling.
PSA:n bör även inkludera funktionsblockdiagram. Dessa beskriver kraven för en lyckad sekvens och inkluderar samtliga de funktioner som måste ingå för att ett säkert tillstånd skall uppnås. Diagrammen underlättar överblicken och användningen av händelseträden, särskilt för personer utan PSA-bakgrund.

En summering av systemfunktionskraven bör presenteras i en kravmatris. Matrisen ger en översikt över systemkraven och innehåller referenser till underlag som ligger till grund för händelseträdens utformning.

Tidsmässiga randvillkor för aktivering av system och operartörsingrepp är viktiga indata till analysen av mänskligt felhandlande. Det är därför av vikt att dessa tider redovisas explicit i anslutning till varje händelseträd.

Dokumentationen av en sekvensanalys skall omfatta all relevant information kring händelseutvecklingen givet en inledande händelse, och kan dokumenteras exempelvis enligt följande:
Förutsättningar för sekvensanalysen
Inledande händelse, inklusive sekundära effekter
Tillgängliga säkerhetsfunktioner och säkerhetssystem
Redovisning av systemkrav
Funktionsblockdiagram för den inledande händelsen
Grafiska händelseträd

Definition av sluttillstånd

Sluttillstånden i en sekvens kan i en nivå 1 PSA antingen vara härdskada eller ett mer eller mindre stabilt tillstånd. För båda dessa fall finns det normalt anledning att definiera flera sluttillstånd:
Definition av sluttillstånd med härdskada
Sluttillstånd (härdsmälta, övertryckning etc.) skall definieras.
Definition av sluttillstånd utan härdskada

Även framgångsrika sluttillstånd behöver beskrivas. Således behöver villkoren för framgång beskrivas, t.ex. hur länge tillståndet är stabilt eller vilka ytterligare åtgärder som behöver vidtas i ett längre perspektiv.

Tillsynshandboken Bilaga 3.2.8 Växelverkan med andra analysmoment

Sekvensanalysen växelverkar med flertalet övriga analysmoment i PSA:n. De viktigaste är:

Analysen av inledande händelser
Denna ger förutsättningarna för sekvensanalysen. Varje definierad inledande händelse består normalt av ett antal olika händelser som har liknande anläggningspåverkan. Det är störningens fortsatta förlopp, under beaktande av denna specifika påverkan, som skall bestämmas och modelleras i sekvensanalysen.

Systemanalys
I systemanalysen sker den detaljerade modelleringen av systemfunktionen. Analysen av inledande händelser och sekvensanalysen bestämmer gemensamt de olika systemdriftfall som behöver modelleras. I systemanalysen identifieras sedan de fel i komponenter, hjälpfunktioner, m.m. som kan medföra att systemet felar under dessa driftfall.

Analysen av manuella ingrepp
I sekvensanalysen kommer en stor del av de potentiellt viktiga ingreppen att identifieras. Detta gäller i första hand ingrepp som ingår i aktivering av system. Identifierade ingrepp analyseras i detalj i analysen av manuella ingrepp. Det är således av stor vikt att relevanta ingrepp verkligen identifieras i sekvensanalysen.

Kvantifiering
I kvantifieringen utgör händelseträden den överordnade logiska modellen. De inkluderar logiska kopplingar till de detaljerade systemfelträden och randvillkor, bl.a. i form av de speciella förhållanden som gäller för varje inledande händelse.

Koordinering av PSA nivå 1 och nivå 2
Det finns ett behov av att koordinera delanalyser i PSA nivå 1 och nivå 2. Detta gäller t.ex. system som krediteras i båda analyserna, systemkrav, detaljeringsgrad, använda databaser och samordning av randvillkor. Analyserna i PSA nivå 1 och nivå 2 skall vara konsistenta, d.v.s. likartade med avseende på allmän modelleringsfilosofi, detaljeringsgrad m.m. Samordning krävs främst för systemanalyser, analys av manuella ingrepp och data

SwedPower kommentarer

SKI krav vad gäller sekvensanalys och händelseträdsmodellering är i stort sett uppfyllda.

Händelseträden är beskrivna i studiens kapitel 4 i form av blockdiagram. I kapitlet definieras även konsekvenser, systemkrav samt att funktioner som krediteras i händelseträden beskrivs. Varje inledande händelse har ett separat händelseträd i modellen men flera inledande händelser utnyttjar samma typhändelseträd.

Konsekvenser

Följande konsekvenser definieras i händelseträden:

OK	Stationen har klarat av den uppkomna situationen.
HS1	Härdskada kategori 1. Utebliven reaktivitetskontroll, ej underkritisk reaktor.
HS2	Härdskada kategori 2. Utebliven spädmatning av reaktortank.
HS3	Härdskada kategori 3. Utebliven resteffektkylning
ÖT1	Övertryckning kategori 1. Överskridande av HTG
ÖT2	Övertryckning kategori 2. Snabb övertryckning av RT.
TB	Att jämföra med ”OK”. Stationen har klarat av den uppkomna situationen. Dock har tvångsnedblåsning genomförts.

Konsekvenserna ÖT1 och TB anges som ekonomiska konsekvenser. För ÖT2 anges att konsekvensen innebär ej härdskada utan leder sannolikt till tryckavlastning via tanklocksfläns.

Några konsekvenser borde definieras något tydligare i studien.

- Beträffande kriterier för "säkert tillstånd" noteras att resteffektkylning i vissa sekvenser är OK även om ingen resteffekt avges varken till hav eller atmosfär utan endast ackumuleras i inneslutningen. Ingen närmare förklaring ges till vilka ytterligare åtgärder som behöver vidtagas i ett längre tidsperspektiv (> 20 timmar). I kap 2.3.2 anges "att med säkert läge avses bortförsel av resteffekt från inneslutning"

- Sluttillstånden eller konsekvenserna ÖT1 och ÖT2 inträffar enligt beskrivning när HTG för primärsystem överskrids. I modellen används som det verkar en annan definition eftersom ÖT2 ej erhålls trots att HTG per definition överskrids innan 314 ventiler (som tillgodoräknas för tryckavsäkring) öppnar. Sluttillstånden efter ÖT1 och ÖT2 behöver förtydligas och eventuellt analyseras vidare speciellt med tanke nivå 2 analys.

Systemkrav

Systemkrav framgår av bilaga 1 i kap 4. Systemkraven har i de flesta fall hämtats via systembeskrivning och STF-basis och är därmed konservativa vilket även gäller för systemkrav där referenser saknas. För vissa funktioner som tryckavsäkring och spädmatning har MAAP beräkningar angivits som referens och därmed kan kraven förväntas vara mer realistiska. Vid en översiktlig genomgång av systemkrav noterades att förtydligande för vissa systemkrav är önskvärd. Det gäller bland annat

- systemkraven efter en situation lyckat /misslyckat hydrauliskt snabbstopp. Rimligen borde hårdare krav ställas på tryckavsäkring i en situation med misslyckat snabbstopp (men lyckat skruvstopp) än vid lyckat. Detsamma gäller för krav på spädmatnings- och resteffektkylfunktioner. En översyn och ökad diversifiering av systemkrav i modellen kan därför vara motiverad i vissa fall.

Sekvensanalys

Blockdiagram är framtagna för respektive typhändelseträd för att underlätta granskning inom sekvensanalysen. Följande notering lämnas

- Blockdiagrammen verkar ej helt uppdaterade med händelseträden i modellen speciellt vad gäller spädmatningsfunktioner.

- Beträffande den indirekta påverkan som den inledande händelsen kan ha på säkerhetssystem så verkar inte detta fullt ut beaktat i analysen. Bland annat beaktas inte dynamiska effekter som jetstrålar och missiler han ha på vek säkerhetsrelaterad utrustning vid inre och yttre LOCA.

- Effekter av störningar som inträffar i system efter inledande händelse borde omnämnas och beaktas i större omfattning. Vid tillexempel fel på reglering i matarvattensystem 312 anges att detta kan medföra toppfyllning och övertryckning i reaktortank (ÖT1). Att överfyllningen vid uteblivet manuellt ingrepp även kan medföra följande följdeffekter omnämns ej.

- vatten hamnar i ångledningar mot turbin med eventuella vattenslag och problem vid efterföljande skalventilstängning i huvudångledning beaktas ej
- toppfyllning med 312 skulle kunna medföra tömning av 733-tank på vatten så att spädmatning med 327 inte längre kan tillgodoräknas som tänkt i modellen
- etablering av resteffektkylning via 314/322 kan ej ske som tänkt då vattenavbördning inte efterfrågas i modellen efter toppfyllning.
- att både 312 och 327 kan börja arbeta parallellt med on-off reglering i stället för som avsetts med reglering mot nivåbörvärde

- Generellt gäller i studien att ingen kredit tas för manuell återställning av felande system (recovery)

2.3 RESULTATPRESENTATION

Tillsynshandboken: Kap 7.2 Resultatpresentation

Sättet att presentera en PSA:s resultat sätter gränser för deras användning och tolkning, och påverkar därmed förutsättningarna för en PSA-baserad beslutsprocess. Det måste i detta sammanhang betonas att ordet ”resultat” inte endast refererar till PSA:ns kvantitativa resultat, utan inkluderar även annat som behövs för att kunna förstå och tolka en PSA, d.v.s.

Beskrivning av antaganden och förutsättningar
Beskrivning av använda modeller och data
Kvalitativa resultat

Vad gäller vilka specifika krav som ställs på resultatpresentationen, så finns det en stark koppling till PSA:ns avsedda användningsområden, vilket diskuteras i avsnitt 7.1.
En fördjupad beskrivning ges i bilaga 2.2.

SKI:s krav och bedömningskriterier

Resultatpresentation i en PSA bör utgå från den information analysens målgrupper behöver för att rätt kunna utnyttja resultaten.
Vid val av data, parametrar och förutsättningar bör realism eftersträvas. Målet bör vara att uppnå jämförbarhet mellan de olika riskbidrag som uppskattas i PSA:n, d.v.s. både från olika kategorier av inledande händelser och från olika drifttillstånd.
Not: Om en realistisk ansats av olika skäl ej är möjligt, bör en motivering ges och resultatpåverkan uppskattas, exempelvis med känslighetsanalys.

PSA-analyser är en iterativ process, vilket bör återspeglas i resultatpresentationen. I samband med presentation och värdering av PSA-resultat gäller därför följande:
Resultatpresentationen bör beröra både absoluta och relativa kvantitativa resultat, d.v.s. den skall lyfta fram och diskutera risktoppar och tolka resultaten i termer av styrkor och svagheter i anläggningen.
Osäkerhets- och känslighetsanalysen bör utnyttjas aktivt i resultatanalysen både för att ge perspektiv på resultaten och för att bedöma PSA-modellens robusthet.
Förutsättningar och begränsningar skall presenteras och deras resultatpåverkan värderas. Denna lista är en viktig utgångspunkt för känslighetsanalysen.
PSA:n bör innehålla en diskussion som beskriver och värderar modellernas inneboende osäkerheter (data, metoder, förutsättningar, fullständighet, realism, konservatism, etc.), deras natur och storlek.
Slutsatser och rekommendationer skall formuleras. Dessa skall inte enbart beröra de föreliggande resultaten, utan också specifikt diskutera modifierings- och utvecklingsbehov för att förbättra de framtida möjligheterna att

använda PSA:n. Förslag till och värdering av anläggningsändringar som förbättrar säkerheten bör ingå i slutsatserna.

Minimikrav på resultatutformningen i en PSA presenteras i tabell 7-1; tabellen är uppdelad i kvantitativa och kvalitativa resultat.

Tabell -2 Minimikrav på resultatpresentation i en PSA

Kvantitativa resultat
Absolutnivå för risk
Presentation av de viktigaste bidragen till totalrisken
Listor över minimala cutsets (med tillräckligt upplösning). Listor presenteras på olika nivåer (per inledande händelse, per sluttillstånd, per sekvens)
Viktighetsmått på system- och komponentnivå (möjliggör identifiering av potentiellt stora riskbidrag)
Presentation av osäkerheter
Kvalitativa resultat
Tolkning av resultaten utgående från anläggningens utformning (t.ex. inverkan från otillräcklig subseparation)
Viktiga slutsatser (kvalitativt uttryckt)
Beskrivning och värdering av viktiga förutsättningar och begränsningar
Presentation av svaga (eller viktiga) punkter m.a.p. system, komponenter, mänsklig växelverkan m.m.
Identifiering och värdering av svagheter, kunskapsluckor eller osäkerheter med stor resultatpåverkan
Värdering av inverkan från faktorer som kan påverka eller försvåra prioritering av åtgärder (t.ex. med känslighetsanalyser)

Tillsynshandboken Bilaga 2.2 Resultatpresentation

Kvantifiering

Kvantifiering av felträden sker med ett PSA- eller felträdsprogram, och resulterar i listor över dominerande minimala cutsets. I kvantifieringen och resultatpresentationen ingår också känslighets- och osäkerhetsanalyser.

Kvantifieringar skall göras, redovisas och analyseras för tre nivåer:
anläggning
sekvenser
system (alla driftfall enligt händelseträden kvantifieras)

För alla dessa nivåer bör följande ingå:
lista över minimala cutsets
beskrivning av dominerande minimala cutsets
viktighetsmått för bashändelser
känslighetsanalys av bashändelser med höga riskökning- och riskminskningsfaktorer (RRW / RAW)

Listorna över minimala cutsets är den centrala delen av studiens resultat och utgör grunden för en stor del av den vidare användningen av studien. Listorna presenteras antingen på papper eller i form av datafiler.

Känslighetsanalys

Känslighetsanalysen består i att dels, baserat på analysens kvantitativa resultat, presentera viktighetsmått för bashändelser, system och säkerhetsfunktioner, dels att systematiskt värdera analysens förutsättningar.

Följande viktighetsmått bör presenteras för varje sekvens- eller konsekvensutvärdering.:
Fussel-Vesely
Riskminskningsfaktor, Risk Reduction Worth (RRW)
Riskökningsfaktor, Risk Achievement Worth (RAW)

Viktighetsmått ger användbar och lättillgänglig, men begränsad information, som bör kompletteras via systematiska känslighetsanalyser. De speglar alltid en situation med givna förutsättningar och en given anläggningsmodell. Således kan en i grunden konservativ modellering av en systemfunktion (t.ex. systemkrav 2

av 4 stråk i stället för 1 av 4 stråk) ha stor inverkan på beräknad risknivå, utan att resultera i en hög riskminskningsfaktor för funktionen. På motsvarande sätt kan en ickekonservativ modellering av en systemfunktion mycket väl ha en låg riskökningsfaktor för funktionen. Detta slag av påverkan från konservativa eller ickekonservativa systemkrav och modelleringar kan endast studeras genom ommodellering och omkvantifiering av studien.

I känslighetsanalysen ingår även att pröva studiens förutsättningar och begränsningar. Detta innebär att exempelvis alternativa modelleringssätt analyseras, liksom inverkan från olika val av systemfunktionskrav och tillgängliga tider. Känslighetsanalys kan även vara ett sätt att bedöma rimligheten i införda förenklingar.

Osäkerhetsanalys

Osäkerheter måste alltid beaktas vid analys av händelser som inträffar slumpmässigt i tiden, och blir extra viktigt om händelserna dessutom är sällsynta. Identifiering av osäkerheter och behandlingen av dem är därför av grundläggande betydelse både vid presentation av PSA-resultat och vid jämförelse mellan resultat från olika delanalyser.

I varje PSA måste två fundamentalt olika typer av osäkerheter beaktas:
Osäkerhet om händelser som inträffar stokastiskt i tiden /
Statistisk osäkerhet
d.v.s. osäkerhet som kommer sig av att frekvensen för ett fenomen (fel i komponent, inträffandet av viss inledande händelse, etc.) beskrivs både av ett läges- och ett spridningsmått. Denna osäkerhet kan ej elimineras med ökad kunskap; däremot kan precisionen i skattningen förbättras och osäkerhetsintervallet minskas.

Värdering av inverkan från analysförutsättningar

PSA-resultatens användbarhet och jämförbarhet påverkas starkt av valet av förutsättningar för analysen. En viktig grund för allt arbete med en analys eller med dess resultat är därför att ha kontroll över förutsättningarna, d.v.s. att veta vilka de är och vilken inverkan de har på analysens resultat. Man brukar kunna hitta tre slag av förutsättningar i en analys:
Förutsättningar som ges av analyspraxis, d.v.s. som beror på att analysen brukar utföras på ett visst sätt, t.ex. med ett visst val av analysmodell eller detaljeringsnivå. Exempel är användning av alfafaktormodellen för modellering av beroendefel.

Redovisade förutsättningar, d.v.s. som beror på ett medvetet val hos analysgruppen, och som redovisas som en del av analysen. Exempel är begränsningarna att inte modellera beroenden mellan olika säkerhetssystem eller spridning av brand mellan brandceller.

Oredovisade (ibland okända) förutsättningar, d.v.s. förutsättningar som inte redovisas i analysen, ibland därför att de inte är kända för analysgruppen. Orsaken till detta är ofta otillräcklig kartläggning.

Eftersom en PSA:s slutsatser och resultat endast gäller inom ramen för de uttalade och outtalade förutsättningar som utgör dess grund, är det av stor vikt att i PSA:n identifiera, dokumentera och värdera de förutsättningar som gällt i analysen. Ett generellt krav är därför att förutsättningar skall vara klart angivna.

En värdering av inverkan från viktigare förutsättningar bör ingå i PSA:n, bl.a. med referens till relevant bakgrundsmaterial, och utgör en viktig utgångspunkt för val av fall för känslighetsanalys. Vissa förutsättningar kan visas ha liten riskpåverkan, och är därmed berättigade förenklingar av analysen. I andra fall är riskpåverkan betydande, kanske till och med dominerade.

Värderingen av förutsättningar och begränsningar bör inkludera bedömning av resultatpåverkan från:

Kända eller identifierade förutsättningar och begränsningar (förenklingar, konservatismer, icke-konservatismer, etc.)
Underförstådda mekanismer
Förenklade eller trunkerade analyser
Kända eller identifierade förutsättningar och begränsningar

Konservatismer kan vara starkt arbetsbesparande, och är ofta befogade. Det är t.ex. normalt inte nödvändigt att analysera ett driftsystem med liten säkerhetsmässig betydelse lika detaljerat som ett vitalt säkerhetssystem. Målet med PSA:n måste dock vara att så långt möjligt ge en realistisk riskbild för anläggningen - denna realism får ej onödigtvis försvagas genom att parametrar eller funktioner med stor riskpåverkan modelleras konservativt. Det är viktigt att konservativa antaganden värderas. Det bör t.ex. framgå klart varför en konservatism används och på vilket sätt den påverkar riskbilden.

Ickekonservatismer kan vara omedvetna, eller ligga i en förenkling eller begränsning av studien. Förenklingar är ofta både nödvändiga och motiverade. Det bör dock noteras explicit om de är ickekonservativa. Ofta pekar dessa områden ut kandidater för en utbyggnad av studien mot större realism.
Underförstådda mekanismer

Underförstådda mekanismer är grundläggande antaganden om former för växelverkan eller utveckling av sekvenser. Även förutsättningar av detta slag måste identifieras, dokumenteras och utvärderas. Det följande är några exempel på underförstådda mekanismer:
Endast rörslag beaktat som dynamiska effekter efter LOCA
Sannolikhet och förlopp för sekundär storstörning, d.v.s. bortfall av yttre nät som en följd av anläggningstransient.
Beroendemekanism i CCF-analys av högredundanta system
Antagande om att rätt isolering fås efter rörbrott
Försummande av CCF mellan system
Antagande om fungerande selektivitet i samband med brandanalys

Förenklade eller trunkerade analyser

Till följd av analyspraxis eller begränsade resurser redovisas ofta förenklade eller trunkerade analyser. En identifiering, redovisning och bedömning av riskpåverkan måste göras. Ofta pekar dessa områden på kandidater för en utbyggnad av studien mot större realism. Det följande är några exempel på förenklade/trunkerade analyser:
Översvämningsfrekvensen fördelas jämnt över modellerade rum.
CCI-frekvenser baserat på ingenjörsmässiga bedömningar
Konservativ krediteringar av återinkoppling av felande system (recoveries)
Förenklade spridningsantaganden i analys av rumshändelser

Tabell 11-5 visar ett exempel på hur viktiga förutsättningar i en PSA kan summeras. Det är av värde att utarbeta en presentation av detta slag inom en PSA.

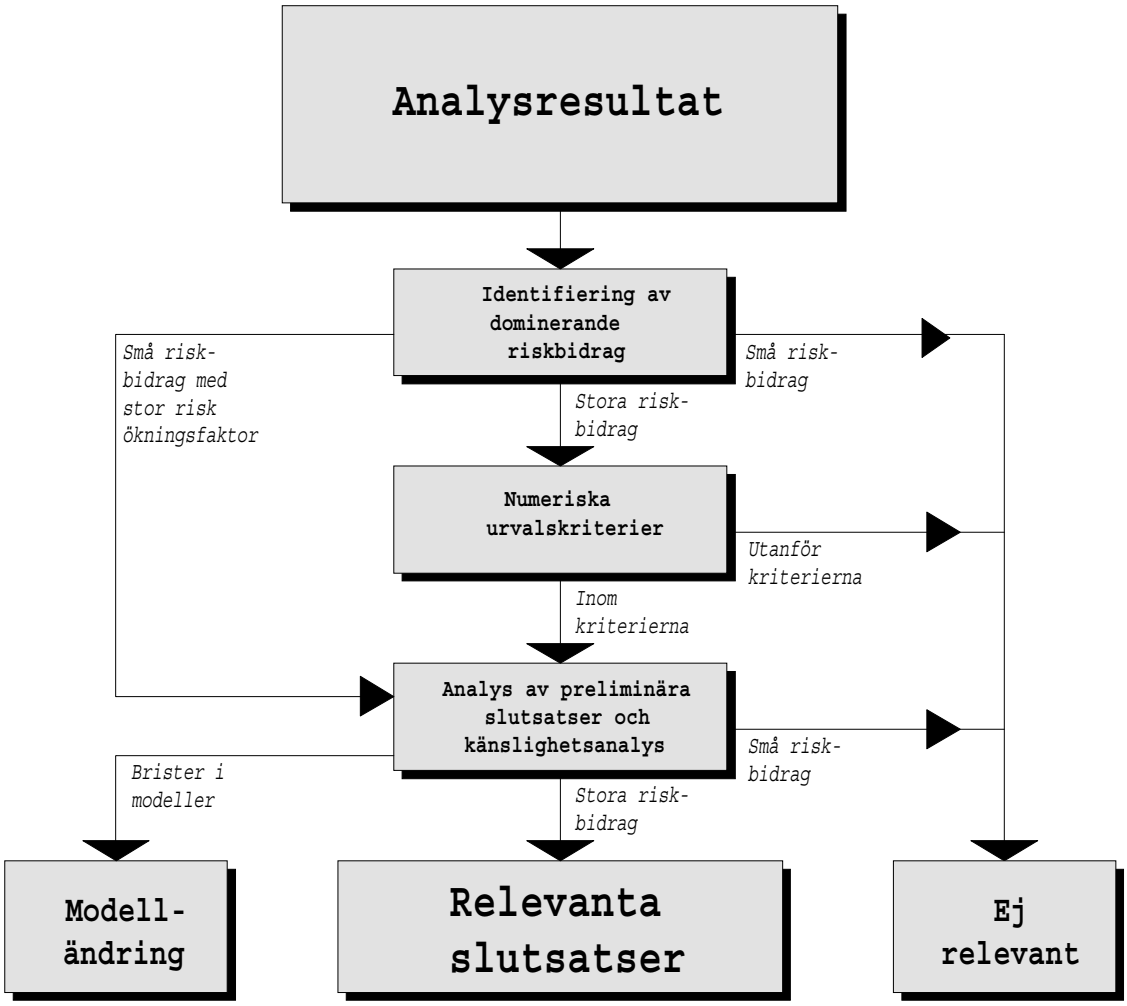
Tabell -3 Översikt över förutsättningar i en PSA (exempel)

Analyssteg	**Kvalitativa förutsättningar**	**Kvantitativa förutsättningar**
Inledande händelser	Urval av inledande händelser Fördelningsmodell för LOCA-frekvenser Omfattning av CCI-analys Brand och översvämning/ urval av fall Inkluderade yttre händelser	Beräkning av LOCA-frekvenser Val av Te-frekvens Val av CCI-frekvens Skattning av frekvens för sällsynta transienter
⇓ Anläggnings-påverkan	Påverkan från brand/översvämning Dynamiska effekter efter rörbrott Modellering av husturbindrift	
⇓ Sekvensanalys	Användning av FSAR-krav Krediterade system Spridning vid brand och översvämning Funktionstid för system Modellering av återkomst av yttre nät	
⇓ Systemmodeller	Modellering av otillgänglighet p.g.a. test och underhåll Modellering av testintroducerade fel	Val av komponentfeldata Val av data för test och underhåll
⇓ Manuella ingrepp	Endast ingrepp som ingår i ÖSI modelleras Omfattning av analysen Val av HRA-modell	Val av data för manuella ingrepp
⇓ Kvantifiering		Cut-off-nivå för kvantifiering
⇓ Konsekvens	Definition av HS1 (även lokala bränsleskador ingår) Förutsättningar för klassning av stationstillstånd	Verifierande beräkningar vid fastställande av sluttillstånd

Arbetsgång vid analys av PSA-resultat

Ett systematiskt angreppssätt är nödvändigt vid analys av PSA-resultat. Orsaken är att det annars kan vara svårt att få en jämn bedömningsgrund. Det är viktigt att analysen inte enbart inriktas på att generera slutsatser som berör den analyserade anläggningen (ändringar i system eller procedurer), utan även identifierar behov av ändringar i PSA:n i sig. Ett exempel på en generell arbetsgång vid resultatanalys beskrivs i figur 1.

Arbetsgången inkluderar analys av preliminära slutsatser och genomförande av känslighetsanalyser m.a.p. inverkan från val av data och modeller, samt inverkan från kända osäkerheter. Slutsatser kan vara av två slag, svagheter i anläggningen som kräver ändringar i system eller procedurer, eller svagheter i analysen i sig, som för sin lösning kan kräva utveckling av analysen.



Figur -1 Arbetsgång i resultatanalys (exempel)

Beslutskriterier

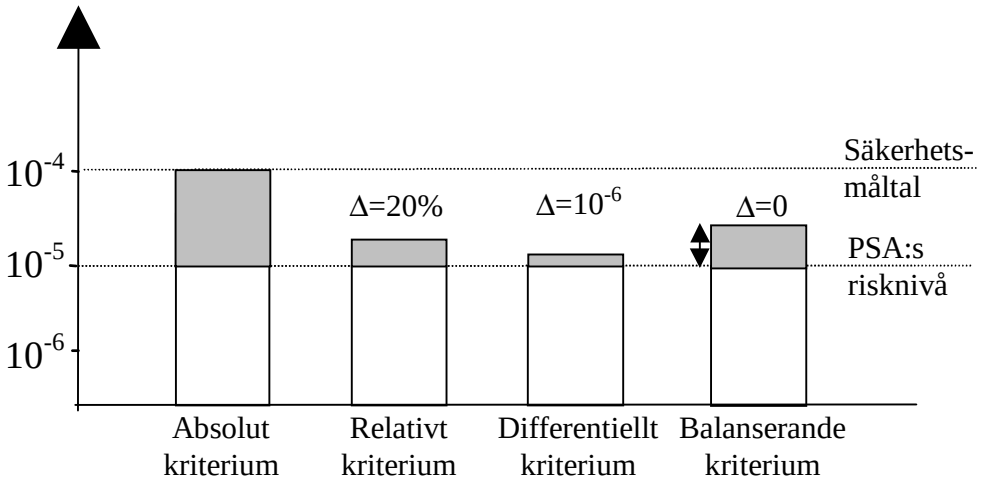
I en PSA:s resultatanalys krävs alltid någon form av beslutskriterier. Dessa kan vara både kvantitativa och kvalitativa och har till syfte både att systematisera resultatanalysen och att möjliggöra identifiering av potentiella säkerhetsproblem. Några vanliga typer av kriterier illustreras översiktligt i figur 2 (angivna frekvenser är exempel):

Absoluta kriterier, d.v.s. PSA:ns risknivå (härdskadefrekvens eller frekvens för stora utsläpp) jämförs med ett säkerhetsmåltal.

Relativa kriterier, d.v.s. fokus ligger på relativa avvikelser från en basrisknivå

Differentiella kriterier, d.v.s. en högsta tillåten absolut avvikelse från referensnivån definieras

Balanserande kriterier (Trade-off Criteria), d.v.s. avvikelser från basrisknivån (ökad risk) skall balanseras så att basrisknivån åter uppnås



Figur -2 Översiktlig beskrivning av några beslutskriterier

I tabell 4 ges några exempel på typer av beslutskriterier som kan användas i analys av PSA-resultat.

Tabell -4 Typer av resultatanvändning

Absoluta kvantitativa kriterier	**Relativa kvantitativa kriterier**	**Kvalitativa kriterier**
Maximal total härdskadefrekvens Maximalt frekvens för utsläpp till omgivningen av >0.1% av härdinventariet Maximalt frekvens för enskild sekvens Maximal sannolikhet för fel i säkerhetsfunktion *Not: Appliceras separat för varje modellerad inledande händelse*	Enskild sekvens andel av total härdskadefrekvens *Not: Detta kan vara svårt att applicera per inledande händelse, eftersom man då påverkas starkt av definitionen av dessa.* Sjunkande trend Kan appliceras inom ett LPSA-program (living PSA), där en och samma analys uppdateras kontinuerligt. *Not: Vid större revisioner av analysmodellen blir kriteriet svårt att applicera.*	Dominerande parametrar eller bashändelser för totalrisk Stora osäkerheter i skattningen av totalrisk Möjliga åtgärders effektivitet i relation till identifierade problems allvarlighet Egna drift- och underhållserfarenheter Omvärldsanalys (State of the art) Kostnadseffektivitet Känt problemområde

Jämförbarhet

Utgångspunkt

I begreppet *probabilistisk analys* finns underförstått att PSA-modellen byggts upp på ett sätt som i största möjliga mån är realistiskt både kvalitativt och kvantitativt, d.v.s. som bygger på anläggningsspecifika faktorer och drifterfarenheter. Detta gäller t.ex. frekvens för inledande händelser, systemkrediteringar och systemkrav, feldata för komponenter, val av parametrar i CCF-modell, modellering av mänsklig växelverkan samt modellering av förebyggande och avhjälpande underhåll.

Målet är en riskuppskattning som i princip skall kunna tolkas i absoluts termer (om än med vissa förbehåll), exempelvis genom att jämföras med ett säkerhetsmåltal eller genom inbördes jämförelser av riskbidraget från olika inledande händelser eller drifttillstånd. Notera att detta, och vad som sägs nedan, gäller riskjämförelser för en och samma anläggning (ej jämförelse mellan olika anläggningar).

Jämförbarhet mellan resultat från två eller flera olika delanalyser i en PSA innebär att relevanta jämförelser kan göras mellan analysernas kvantitativa resultat, vilket i förlängningen möjliggör väl underbyggda prioriteringar av säkerhetshöjande insatser. Frågan om jämförbarhet blir därmed ett av de viktigaste problemen vid användning av PSA-resultat.

Kritiska faktorer

Kritiska faktorer m.a.p. jämförbarhet är sådana som antingen underlättar eller försvårar en resultatjämförelse. Frågan hänger till stor del samman med identifieringen av grundläggande skillnader mellan olika analyser - varje identifierad skillnad kan också försvåra en jämförelse, medan en hög grad av överensstämmelse underlättar jämförelse.

Att PSA:n är fullständig är viktigt. En rättvisande riskbild förutsätter en fullständig analys, d.v.s. en analys som inkluderar alla driftfall och typer av inledande händelser som kan ge relevanta bidrag till anläggningens totalrisk. Dessutom måste inom varje drifttillstånd en fullständig kartläggning göras av de inledande händelser som kan förekomma och resultera i risk för härdskada eller frigörelse av radioaktivitet.

Det finns också ett stort antal faktorer i genomförandet av en analys som måste beaktas vid jämförelse mellan resultat från olika delanalyser. I många fall kan man här på ett relativt enkelt sätt undvika problem genom att välja faktorerna på ett sådant sätt att jämförelse förblir möjlig. Viktiga exempel är:

Samordning av delanalyser

Vid planering av olika delanalyser i en PSA måste gemensamma delar eller delar som kan behandlas med samma metodik identifieras. Detta gäller exempelvis systemkrav, detaljeringsgrad i modellering av system och säkerhetsfunktioner, analys av mänsklig växelverkan, val av CCF-modell och val av komponentfeldata.

Analysens detaljeringsgrad

Jämförelse förutsätter att analysernas detaljeringsgrad är ungefär densamma.
Val av modeller och resultatpåverkan från valda modeller

Val av modeller (för CCF-modellering, analys av mänskligt felhandlande, beräkning av brandbelastning, etc.) har alltid resultatpåverkan, d.v.s. det kvantitativa resultatet blir normalt inte detsamma om alternativa modeller för samma fenomen används. Likartade parametrar eller förlopp i de olika analyserna måste därför modelleras med samma metoder.

Val av data

Val av feldata är normalt betydligt mindre kontroversiellt än metodval, men kan vara problematiskt, särskilt för sällsynta händelser. Även här skall förstås likartade händelser i de olika analyserna modelleras med samma (eller likartade) data. Dessutom bör osäkerheten i data beaktas i resultatpresentationen.

Kända förutsättningar (konservatismer, förenklingar och begränsningar)

Valet av förutsättningar kan genom att begränsa analysens omfattning eller grad av realism också begränsa jämförbarheten. Därför bör alla kända förutsättningar i en analys värderas m.a.p. sin resultatpåverkan.

Okända förutsättningar (fullständighet och modellrelevans)

I vissa fall kan förutsättningar vara okända, vilket kan gälla t.ex. frågor rörande fullständighet eller relevans i valda modeller. Ett försök bör göras att bedöma om det kan finnas påverkan från okända förutsättningar av detta slag. Om så är fallet, kan känslighetsanalyser eller kvalitativa betraktelser ibland vara en väg att bedöma deras möjliga inverkan.

Utformning av resultat (val av riskmått och presentationsform)

Jämförbarheten påverkas självklart också av valet av riskmått (bör vara detsamma), samt av hur resultaten presenteras (skall vara på ett format som tillåter jämförelse).

Tillsynshandboken:
5.4 Värdering av PSA-resultat

När resultat från PSA-studier som överstiger härdskadefrekvensen $1*10^{-5}$/år redovisas för SKI eller om det vid SKI:s granskning har identifierats betydande icke-konservatismer begär SKI att tillståndshavaren redovisar sin värdering av resultatet. Tillståndshavarens värdering bör innehålla en redogörelse av hur väsentliga förutsättningar, konservatismer, möjliga icke-konservatismer m.m. påverkar resultatet. Vidare bör den innehålla en tydlig beskrivning av de bakomliggande orsaker som bidrar till de dominerande sekvenserna samt om åtgärdsplan. Denna redovisning utgör en viktig grund för SKI:s värdering. SKI har däremot inte fastställt krav för kärnkraftverkens drifttillstånd baserade på absoluta gränser för frekvensen för härdskada.

Tillståndshavarna har utarbetat egna säkerhetspolicyn där bl.a. mål för PSA-resultaten finns med. Målet för härdskada är $1*10^{-5}$/år. SKI anser att det angivna målet för härdskada är ett bra säkerhetsmål och att det bör uppfyllas.

Några kvantitativa gränser som man okritiskt tillämpar vid avvikelser från säkerhetsmålen har varken SKI eller tillståndshavarna. En bedömning av säkerheten och hantering av avvikelser från säkerhetsmål görs som en sammantagen bedömning där PSA-resultatet är ett bidrag. Övriga förhållanden är bl.a. om det föreligger direkta avvikelser från licensieringskraven. I en bedömning måste också beaktas hur osäkra PSA-resultaten är.

Denna bedömning innebär att SKI bestämmer hur lång tid det är acceptabelt att de förhållanden som föranlett avvikelsen från säkerhetsmålet kan få råda innan de åtgärdas. Vid stora avvikelser kan bedömningen bli den att reaktorn genast måste bringas till säkert läge.
SKI granskar de faktorer som har givit upphov till avvikelsen från säkerhetsmålen. Granskningen omfattar feldata, mänskliga ingrepp som har eller inte har krediterats, tekniska analyser mm. Granskningen omfattar dock endast de faktorer som bidrar till de dominerande sekvenserna. Denna granskning som därmed begränsas till en mycket liten del av studien kan vara noggrannare/mer kritisk än SKI:s normala granskningar av hela studier. Detta innebär att SKI vid granskningen kan komma att ifrågasätta befintliga data, förutsättningar mm som SKI vid tidigare granskningar, t.ex. av andra block, inte har haft några synpunkter på. Resultatet av granskningen blir en bedömning av orsakerna till avvikelsen och en av SKI bedömd härdskadefrekvens eller utsläppsfrekvens. Dessa frekvenser kan komma att skilja sig något både uppåt och nedåt jämfört med resultatet i PSA studien.

Följande värderingsgrunder utgör ett stöd vid beslut om hantering av avvikelser oavsett om avvikelser från licensieringskraven föreligger eller ej:
Vid härdskadefrekvenser > $1*10^{-3}$/år bör omedelbar nedgång till säkert läge ske. Härdskadefrekvenser > $1*10^{-3}$/år innebär att en mycket allvarlig svaghet har identifierats och sannolikt uppfylls inte heller viktiga deterministiska krav. Efter genomförande av temporära åtgärder kan fortsatt drift åter tillåtas till nästkommande revisionsperiod. Härdskadefrekvenser på denna nivå motsvaras av allvarlig brist i en barriär eller i djupförsvaret enligt SKIFS 1998:1 2 kap 2§ och bilaga 1 kategori 1, d.v.s. reaktorn skall bringas i säkert läge utan dröjsmål.
Vid härdskadefrekvenser mellan $1*10^{-3}$/år och $1*10^{-4}$/år är det normalt acceptabelt med fortsatt drift till nästkommande revisionsperiod. Efter införande av temporära åtgärder kan driften fortsätta ytterligare ett eller flera år beroende av de temporära åtgärdernas art. Denna nivå motsvaras av brist i en barriär eller i djupförsvaret enligt SKIFS 1998:1 2 kap 2§ och bilaga 1 kategori 2, d.v.s. reaktorn får fortsätta att vara i drift under den tid som åtgärder vidtas. “Tid som åtgärder vidtas” inbegriper förutom tid för genomförande av anläggningsändringar även tid för utredning, planering och förberedelser.
Vid härdskadefrekvenser mellan $1*10^{-4}$/år och $1*10^{-5}$/år skall en åtgärdsplan tas fram. Om det är omfattande åtgärder eller om det av andra skäl är lämpligt att genomförandet av åtgärderna dröjer i flera år kan detta vara acceptabelt. Detta motsvaras i SKIFS 1998:1 av uppdagade förhållanden av betydelse för säkerheten enligt 5 kap 6§.

Om resultatet från en PSA studie eller en inträffad händelse skulle avslöja signifikanta avvikelser från licencieringskraven kan en strängare bedömning göras än vad ovanstående värderingsgrunder gör gällande. 5-reaktorstoppet 1992 är ett exempel på när detta har tillämpats. Stoppet föranleddes av att silar i kondensationsbassängen snabbt sattes igen med nedblåst mineralullsisolering efter obefogad öppning av en säkerhetsventil,

Om man under genomförandet av en PSA eller i samband med någon annan verksamhet identifierar avvikelser mot licensieringskraven skall tillståndshavaren begära tillfälligt undantag från säkerhetsredovisningen eller anmäla ändring av säkerhetsredovisningen. Dessa blir då anmälningsärenden och eventuellt villkorsärenden. Villkorsärenden bedöms i enlighet med vad som anges under avsnitt 5.4 och 5.5. Noteras bör att värderingen

endast görs av det bidrag som orsakas av avvikelsen från licensieringskraven. Detta innebär att en avvikelser från licensieringskraven som inte bidrar till de dominerande sekvenserna påverkar inte bedömningen enligt detta avsnitt utan hanteras av andra rutiner.

SwedPower kommentarer:

Sammanfattningsvis så fokuserar Tillsynshandboken (Kap. 7.2 m fl enligt ovan) på ett i PSA-studier ofta eftersatt område, resultatpresentation och slutsatser. Beskrivningarna bl a av hur man bör arbeta både kvantitativt och kvalitativt med detta är läsvärda.

Oskarshamn 2 PSA: Kap. 7 – Resultatsammanställning, reg.nr. RELCON 95131/133 rev. 3

Kap. 7.1 – Inledning
- borde man inte ”standardisera” de olika kategorierna av konsekvenser? Definitionerna av HS 1, 2 resp. 3 skiljer sig t ex från Ringhals 1 PSA.

Kap. 7.2 – Resultat för resp. konsekvens
- det bör beskrivas hur man läser/tolkar diagramtypen, detta är inte självklart.

Kap. 7.3.1 – Rörbrott
- förekommer ingen kategori ”små rörbrott”?, bara A och S1? (S2 ingår i TI?)

Appendix F1 – Känslighetsanalys, reg.nr. RELCON 95131/131 rev. 3
- sammanfattande bedömning / tolkning av känslighetsanalyserna saknas.
- motiveringar till val av parametrar för känslighetsanalyser saknas.

Kap. S – Sammanfattningsrapport, reg.nr. OKG 2/A3/0001.134 utgåva 2
Kap. 2.1 – Inledande händelser
- slarvig definition av CCIer

Kap. 4.1 – Inledande händelser
- screeningvärden använda för CCI i supportsystem. Är dessa verkliga CCIer?

Kap. 8 – Slutsatser från PSA-O2
- kapitlet borde kunna utvecklas väsentligt!

I Tillsynshandbokens ACCESS-databas frågar man om analysen är rimligt realistisk, och om avsteg motiverats. Frågan kan inte enkelt besvaras. I brandanalysen har ett mer konservativt arbetssätt använts (i Sammanfattningsrapporten anges explicit att de beräknade frekvenserna i brand- och översvämningsanalyserna inte kan jämföras med övriga analyser). Delar i grundstudien kanske också är överdrivet konservativt modellerade, t ex att man inte generellt tar någon kredit för manuell aktivering av komponenter som ej automatiskt startar / ändrar läge.

Det är dock ofta nödvändigt att (initialt) ha det på detta sätt, det är inte kostnadseffektivt att gå på djupet i ett för tidigt skede av en PSA. Vid olika tillämpningar, och uttolkningar av resultaten från dessa, är det dock helt nödvändigt att nogsamt beakta hur olikheter / avvikelser vad avser realism kan ha påverkat utfallet.

I nästa fråga i ACCESS-databasen diskuteras hur resultatpresentationen bör lyfta fram både kvantitativa och kvalitativa resultat. OKG PSA Kap. 7 – Resultatsammanställning innehåller ingen diskussion / tolkning kring risktoppar, styrkor och svagheter. I kap Sammanfattning PSA O2 återfinns en lite djupare beskrivning av dominerande händelser per konsekvenskategori.

I avsnittet S.8 Slutsatser från PSA O2 görs ett försök att mycket kortfattat dra slutsatser. Kapitlet är dock mycket magert. Detta är i viss mån förståeligt då olika grader av konservatism och djup i modelleringen av olika händelser till stor del omöjliggör en rimlig kvalitativ och/eller kvantitativ jämförelse. För att utgöra ett användbart underlag för beslut i olika säkerhetsfrågor måste vissa av analyserna fördjupas.

Kap. 2 – Metodbeskrivning, reg.nr. RELCON 95131/2 rev. 2

Kap. 2.3.7 – Steg 6-Analyser
- Ingen osäkerhetsanalys genomförd i Fas 1 av PSA O2 eftersom modellens omfattning medför att denna typ av analys inte kan utföras på ett korrekt sätt med idag tillgängligt verktyg.

Kap. 2.7.2 – Riskuppföljning
- För händelser med högt riskbidrag analyseras riskökning- och riskminskningsfaktorer. Avsikten med detta är dels att erhålla kunskap om hur inträffade händelser skulle kunna propagera till värre tillstånd och dels erhålla kunskap om hur riskbidraget från inträffade händelser skulle kunna minskas.

3. OSKARSHAMN 2 PSA NIVÅ 1

3.1 ALLMÄNNA KOMMENTARER UTGÅENDE FRÅN GRANSKNING AV FELTRÄDSMODELLEN

3.1.1 HJÄLPKRAFTSYSTEM

Felträd för skenor i gasturbin- och dieselsäkrade växelspänningsnät har modellerats i olika varianter. Bland annat 0-2 timmars träd, som representerar utebliven matning från skenor de 2 första timmarna vid ett avställningsförlopp, och 2-20 timmars träd representerande utebliven spänning från skenor timme 2-20. I 0-2 timmars träd tillgodoräknas matning från förutom ordinarie 400kV nät även matning från 130kV, dieselgeneratorer och gasturbiner. I 2-20 timmars träd tillkommer matning från manuell inkoppling av återvändande 400kV nät om detta fallit bort initialt. Det förekommer även andra felträdsvarianter såsom T-träd med initialt tillgänglig matning liksom felträd för att undvika rundgång i felträdsmodellen.

Även för skenor i de batterisäkrade näten förekommer i olika varianter av felträd. Dels "normala felträd" där både batterier och matning från 0-2 timmars växelspänningsträd tillgodoräknas dels "UB-träd" där inte batterier tillgodoräknas utan endast matning från 2-20 växelspänningsträd. Systemfunktioner som endast behövs initialt i ett störningsförlopp är därför kopplade endast till 0-2 timmars träd medan funktioner som behövs även i långtidsförlopp kopplas både till 0-2 och 2-20 timmarträd (alternativt normala och UB-träd i batterinäten).

Denna uppdelning av matningar i olika tidsfönster är bra och ökar realismen i elmodellen. Risken för felmodellering ökar dock något dels p g a av fler felträdsvarianter men framförallt p g a att objektens koppling till respektive variant av felträd inte är beskrivna i studiens pappersdokumentationen och därför inte är enkelt granskningsbara. Kopplingen framgår endast av endast av felträdsmodellen. Några tveksamma modelleringar som noterats i elfelträd är bland annat

- Funktioner som behövs initialt efter en störning t ex skruvstopp är kopplat till felträd som utnyttjar matning från gasturbin (med ca 2 minuters starttid)
- 351 borsystem är kopplat till 0-2 timmars träd men tillgodoräknas med manuell start först efter 4-timmar.Även andra funktioner som kan behövas i långtidsförlopp t ex backspolning och tvångsnedblåsning är endast kopplade till 0-2 timmarsträd
- Funktioner som alltid behöver avbrottsfri matning t ex viloströmskopplade villkor i 516-kedjor är kopplade till UB-träd. I UB-träd beaktas dock inte att batterier behövs i samband med omkopplingar och rensningar då ordinarie matning kortvarigt är borta.
- För funktioner som behövs i långtidsförlopp t ex resteffektkylning efterfrågar modellen kraftmatning (till pumpar o s v) men inte matningar till kontrollutrustning.

En genomgång av hur funktioner och objekt är kopplade till olika varianter av felträd kan vara motiverad samt en komplettering av studien med tydligare dokumentation avseende hur detta är genomfört i modellen.

3.1.2 SIGNALMODELLERING

Signalmodellering i felträden är omfattande och detaljerad. God överensstämmelse noteras mellan modell och beskrivande avsnitt i kap 6.12 signalmodellering.

Några förenklingar i modelleringen har tillgripits i system 516. Det gäller bland annat SS-kedja, I-kedja och start 314 vilka ej är modellerade med olika delvillkor utan ersatta med bashändelser. Sannolikhet för utebliven SS-signal har uppskattats till 1E-10/behov och utebliven "start 314" är satt till 1E-8/behov. Utebliven I-isolersignal är modellerad som "ej obefogad" vilket t ex innebär att signal alltid erhålls vid behov. Den förenklade modelleringen kan innebära en viss ickekonservatism eftersom det i många andra studier har framgått att delvillkor och 2-av 3-kopplingar i kedjor kan ha en viss inverkan på resultat. I något fall har underlag i form av logikschemor saknats, bland annat för 516-SS4 och SS5-villkor. Det kan tyckas märkligt att man trots denna brist av underlag genomför analys och redovisar resultat utan att belysa inverkan.

3.1.3 SYSTEMANALYS

Funktionsbeskrivning för krediterade systemfunktioner är utförligt beskrivna i kap 4.1.4 och framgår till viss del även av studiens systemanalyser i kap 5. En jämförelse av modellen mot dessa beskrivningar har resulterat i att några funktioner bör ses över. Det gäller främst hur system och funktioner har tillgodoräknats och använts i modellen. T ex noteras följande

- Vid yttre brott i huvudångledningar tillgodoräknas motordonsstängning för 311V5-V8. Normalt är denna stängning alldeles för långsam, endast egenmediestängning bör tillgodoräknas. Detsamma gäller krediterad signal Y20 för stängningsfunktion. Det kan även vara så att fler ventiler än endast ventilen i drabbad 311- ledning måste stänga p g a by-passflöde via turbin.

- System 321/331 tillgodoräknas ej i modellen för resteffektkylning p g a att instruktion för inkoppling saknas (ÖSI). Vid utebliven resteffektkylning med 322/721/712 sker därför enligt modellen resteffektkylning via vattenfyllning av inneslutningen med RAMA-system 322O. Inte ens vid transient TP planerad nedgång då kylning med 321/331 systemet per definition är i drift tillgodoräknas denna kylväg. Transient TP svarar för dominerande bidrag för konsekvens HS3,utebliven resteffektkylning. Det finns därför anledning att se över instruktioner (ÖSI) så att resteffektkylning med 321/331 kan tillgodoräknas.

- I funktionshändelse (U-1), nedstyrning av 327 hjälpmatarvattenflöde utnyttjas samma felträd för **reglering** som i funktionshändelse U, spädmatning med system 327. Eftersom det i händelseträden först frågas om regleringen fungerar i funktion U så blir det fel att fråga en gång till om regleringen fungerar även i U-1 efter lyckad U. Risken för toppfyllning via 327 underskattas troligen därför i modellen och modelleringen bör ses över (*denna observation är besvarad av OKG strax före rapportens utgivning*).

- Även när det gäller samfunktionen mellan 312 matarvatten och 327 hjälpmatarvatten efter SS4 bör förtydliganden göras. Efter SS4 tar system 327över spädmatningen p g a högre nivåbörvärde. I händelseträden frågas dock ej efter 327 funktion(U) så länge som 312 (Q) fungerar. Det frågas ej heller om nedstyrning med 327 (U1) lyckas trots att systemet är i drift.

Mellan vissa funktionshändelser i händelseträden finns beroenden som kanske inte helt har beaktats eller kommenterats. Mellan t ex resteffektkylfunktioner W3 och W4 finns troligen beroenden på så vis att om manuell uppfyllning av bassängen med 322O (W3) misslyckas så är det ganska stor sannolikhet att även manuell sprinkling via 322O (W) också misslyckas. Likaså kan det finnas beroenden mellan 314funktioner så att om ventiler för tryckavsäkring inte öppnar så är det troligt att samma ventiler inte heller kommer att öppna vid tvångsnedblåsning.

3.1.4 SYSTEMFELTRÄD

Komponent och systemfelträden är systematiskt och strikt uppbyggda och stämmer bra mot systemvisa FMEA

De resurser som har lagt ned på modellering av olika systemfelträd kan synas något ojämn och bör bakgrund bör till detta bör förklaras. Det gäller bland annat system för reaktoravställning (354, 532 ,221och 222). Här har hundratals felträd modellerats för SS-grupper och styrstavar för att fånga upp oberoende fel, men det ändå är CCF som klart dominerar felsannolikheten för utebliven avställning. Signaler för att aktivera dessa avställningsfunktioner är emellertid inte modellerade med felträd utan endast med en bashändelse med bedömd felsannolikhet på 1E-10/behov. Förhållandet är detsamma i system 314.

Felträdsmodellerna speglar väl de verkliga funktionerna. Endast ett fåtal noteringar har gjorts beträffande utförandet av felträden, bland annat följande

- reglerventiler 323 V9 och V10 liksom minflödesventilerna 323V13 och V14 är enligt systembeskrivningar väsentliga för 323 funktion. Signalberoenden för dessa ventiler saknas dock till stor del i systemmodellerna

Övrigt

Några *generiska frågor* som ofta återkommer vid granskning av PSA även vid O2 PSA

- Tillgodoräknande av ordinarie 314 bassängblåsande ventiler för tryckavsäkring i vattenfas varierar mellan studier. Kvalificering av ventilerna för denna funktion saknas.
- Möjliga manuella ingrepp inom 30 minuter efter inledande händelse analyseras normalt ej.
- 314 trycknedtagning med 314 reglerventilstråk (så att 322 resteffektkylning kan etableras respektive 321 kan kopplas in vid 10 bar /180^{0}C) modelleras vanligen ej.
- Bortfall av rumskylning i elutrymmen är ej analyserade.
- Påverkan på signalkretsar vid brand är svårbedömd och ansatta felmoder varierar mellan olika studier
- Obefogad spänningssättning vid brand och sannolikhet för obefogade ventilmanövrar analyseras normalt ej

3.2 KONSERVATIV BRANDANALYS

O2 PSA Kapitel 6.7 Konservativ brandanalys . Rev 3 99-03-08

Brandanalysen redovisar konsekvens av brand rumsvis. Detta är ett effektivt sätt att relativt snabbt identifiera svagheter i separation och brandskydd mellan säkerhetssystem. Av resultatkapitel att döma så har också svagheter identifierats i händelse av helt utslaget rum.

Brandanalyser är omfattande och arbetskrävande. Analyserna måste förenklas genom ett inledande screeningförfarande för att begränsa arbetsinsatserna för att sedan, som steg två, noggrannare studera rum som ger större härdskadebidrag. I O2 har brandanalyserna endast genomförts i ett steg.

Brandanalyserna är genomförda med som det anges konservativa förutsättningar och antaganden. Närmare granskning av analysförutsättningar har medfört följande noteringar:

- felmoder som följd av brand är inte alltid konservativt valda, vilket dock påpekas i något fall i studien. T.ex. bortses helt från eventuellt uteblivna / felaktiga signaler i viloströmskopplade signalkretsar (som i system 516) vid brand

- rumsberoenden och logik för några väsentliga signaler för stationens säkerhetssystem (516) saknas i felträdsmodell.

- brandspridning mellan rum har inte närmare studerats samtidigt som brandskydd mellan rummen inte är redovisat

- alla rum är ej beaktade, endast rum med PSA-objekt ingår. Eventuell brandspridning från rum utan PSA-objekt till "PSA-rum" värderas således ej.

Trots att inte alltid konservatism använts i utvärderingarna har enligt resultatredovisningen ett antal rum identifierats med potential att ge höga HS-bidrag i händelse av en utvecklad brand i rummet.

Steg 2 i en brandanalys är att närmare studera rum, som ej blivet bortgallrade som ointressanta, med mer realistiska antaganden. Detta steg har ej genomförts i O2 analysen. Realistiska värden på härdskadesannolikhet givet brandhändelsen framgår därför ej.

Beräkningar har genomförts för konsekvenser HS1, HS2, HS3 och ÖT2. För utrymmen som uppvisar en härdskadesannolikhet > 1E-3 givet brand har konsekvenserna beskrivits kvalitativt. Något förvånande är att utvärderingen för t ex HS2 (utebliven spädmatning) genomförts utan att modellen varit komplett vad gäller väsentliga signaler för nivåmätning. Orsak till varför 516-signaler som SS4 och SS5 (låg och hög nivå i reaktorn) inte modellerats med rumsberoenden och logik anges vara att underlag saknas. Kvalitativa resultat kan därför i vissa fall ifrågasättas.

Flera rum i O2 uppvisar hög härdskadesannolikhet givet brand. HS-bidrag från brand är även höga jämfört med bidrag från LOCA och transienter. I studiens kap.8 resultattolkning, anges att orsaken till höga värden är att O2 inte tål den konservativa ansatsen i brandanalysen d v s att ett helt rum slås ut av brand. Detta eftersom separationen i anläggningen till stor del

bygger enbart på avståndsseparation mellan redundanta kretsar. Någon rekommendation till mer detaljerad brandanalys eller förbättringsförslag ges ej i analysen annat än att det är väsentligt att en efterföljande värdering av resultatet sker.

Inför en uppdatering av brandanalysen bör lämpligen följande beaktas:

- genomgående konservativa eller realistiska antaganden bör utnyttjas i den inledande screeningfasen för att med säkerhet inte missa några väsentliga beroenden och så att ointressanta rum ur brandsynpunkt kan gallras bort

- genomför, som steg 2, om möjligt en noggrannare analys med mer realistiska antagande i dominerande utrymmen. Beakta till exempel effekter av släckanordningar, i första hand fasta sådana, liksom avståndsseparation mellan redundanta funktioner för att få fram mer realistiska värden på HS-bidrag

- Komplettera felträdsmodellen med beroenden (spänning/signalberoenden) speciellt inom 516 vilket kan ha stor betydelse för resultat

- Inarbeta HS-bidrag från rumsanalyser i resultat för anläggnings totala HS-frekvens

- Om möjligt bör rumsanalyserna integreras i modellen på samma sätt som för övriga inledande händelser som LOCA och transienter. Härvid ökar möjligheterna att använda modellen vid utvärdering av t ex anläggningsändringar genom att även påverkan från brand kommer med.

3.3 ÖVERSVÄMNINGSANALYS

O2 PSA Kap 6.8 Konservativ översvämningsanalys. Rev 3 1999-03-22.

Huvudsyftet med översvämningsanalysen är enligt inledande kapitel 6.8.1 är att beskriva de konsekvenser som översvämningar har på anläggningen samt att beräkna och bedöma härdskadefrekvensen.

Granskningen har visat att analysen är grov och många konservativa antaganden tillämpas. De konsekvenser som översvämningar medför på anläggningen blir därför inte realistiska och HS-frekvensen blir troligen mycket osäker (och överskattad). Kapitel med resultatberäkning och redovisning har av denna anledning inte studerats eller kommenterats närmare. Synpunkter lämnas i stället på avsnitt i analysen som har koppling till omfattning och fullständighet liksom antaganden som kan innebära ickekonservatismer. (Se detaljkommentarer Ö1-14 i ACESS-databasen)

Översvämningsanalysen skulle vid en uppdatering troligen vinna på om följande beaktas:

- Redovisa fullständiga utflödesscenarier och koncentrera resultatredovisning på anläggningskonsekvenser av dessa, (istället för som nu på översvämning av enskilda rum).
- Sätt utflödesfrekvens på utflödeskällor i stället för att fördela anläggningens översvämningsfrekvens på rum
- Beakta i analysen även utflöden från hetvatten och ångsystem och inte enbart kallvattensystem.
- För att öka realismen i resultat: tillgodoräkna bland annat möjlighet att manuellt avbryta utflöden och eventuell miljökvalificering av objekt, samt beakta möjliga maximala vattennivåer i olika utrymmen.
- Beskriv översvämningsskydd som tillgodoräknas i analyserna samt översvämningssamband mellan olika utrymmen, gärna i form av en enkel skiss. Detta ökar förståelsen av översvämningsanalysen och resultat.

4. FÖR ARBETET TILLGÄNGLIGT UNDERLAG

Följande underlag har gjorts tillgängligt av SKI:

SKI-dokument:

SKI Rapport 99:48, Tillsynshandbok PSA (koncept 99-12-03) Del 1 - Huvudrapport
SKI Rapport 99:48, Tillsynshandbok PSA (koncept 99-12-03) Del 2 - Bilagor

Oskarshamn 2 PSA dokumentation:

RELCON-95131/134, Sammanfattning PSA O2, 1997-10-09
OKG Rapport 2/A3/0001.134, Sammanfattningsrapport, 1999-04-23
RELCON-95131/1, Introduktion till PSA O2, 1999-06-01
RELCON-95131/2, Metodbeskrivning, 1997-10-13
RELCON-95131/3, Analys av inledande händelser (med bilagor), 1999-06-01
RELCON-95131/133, Resultatsammanställning, 1999-03-23
RELCON-98168/143, Resultattolkning nivå 1, 1999-03-30
RELCON-95131/131, Känslighetsanalys, 1999-03-31
RELCON händelseträdsanalyser, kap. 4.01 – 4.66
RELCON Systemanalyser & FMEA, kap 5.01 – 5.47
RELCON kap. 6.x, Analys av diversifiering, separation och beroenden
RELCON-95131/133, Resultatsammanställning, 1999-03-23
RELCON appendix A – G

Oskarshamn 2 PSA felträdsmodell:
O2-a9850