Strålsäkerhetsmyndigheten
Swedish Radiation Safety Authority

PROMEMORIA

2012-10-16

Dok nr: SSM 2010/1557-12

Samråd: Anders Hallman

Författare: Lovisa Wallin

Fastställd: Lars Skånberg

Jämförelse mellan svenskt och internationellt regelverk avseende konstruktion och utförande av kärnkraftreaktorer samt genomgång av implementerade säkerhetsförbättringar inom europeiska kärnkraftreaktorer

Utredning avseende den långsiktiga säkerhetsutvecklingen i den svenska kärnkraften och åtgärder med anledning av olyckan i Fukushima

Delprojekt 1 - Analys och förbättringar av säkerheten i äldre reaktorer baserat på nya kunskaper och säkerhetsutveckling

Etapp 1 och 2

Föreliggande PM avser att beskriva hur de säkerhetskrav som ställs i SSMFS 2008:17 avseende konstruktion och utförande av kärnkraftsreaktorer förhåller sig till internationella regelverk och säkerhetsstandarder. Därutöver redovisas en sammanställning av de säkerhetförbättringar som genomförts i Finland, Frankrike, Schweiz och Tyskland, bland annat till följd av krav från myndigheterna för att möjliggöra längre drifttider.

Strålsäkerhetsmyndigheten
Swedish Radiation Safety Authority

SE-171 16 Stockholm
Solna strandväg 96

Tel:+46 8 799 40 00
Fax:+46 8 799 40 10

E-post: registrator@ssm.se
Webb: stralsakerhetsmyndigheten.se

Sammanfattning

Jämförelse av internationella regelverk

De svenska kraven avseende konstruktion och utförande av kärnkraftsreaktorer har i detta PM jämförts med internationella krav och standarder. Resultatet av denna jämförelse tyder inte på några väsentliga skillnader avdeende omfattning (dvs ”vad” man ställer krav om) mellan de svenska kraven och de internationella kraven och standarderna och inte heller några väsentliga skillnader avseende den säkerhet som en konstruktion och ett utförande i enlighet med kraven bidrar till. Däremot skiljer sig detaljeringsgraden och utformandet (dvs ”hur” man ställer kraven) väsentligt mellan de olika länderna och organisationerna. Gemensamt för de internationella regelverken och standarderna är att de är betydligt mer preciserade än de svenska kraven. Utredningen finner att en viss ökning av detaljeringsnivå av de svenska kraven bör kunna ge tydligare krav, mer i harmoni med internationella krav och standarder. Tydligare krav kan även vara effektivare och i praktiken innebära ökad säkerhet genom att förutsägbarhet och därmed även rättstrygghet hos regelverket ökar samtidigt som tolkningsutrymmet minskar. Om alla parter vet vad som förväntas och vad som gäller så underlättas implementeringen och uppyllandet av kraven samt även granskningen av uppfyllandet och implementeringen. Resursmässigt skulle därmed tydligare krav kunna medföra att tidsödande granskningsprocesser som inkluderar uttolkande av krav kan minimeras. Som inspiration för en sådan utveckling bör detaljeringsnivån som återfinns inom det kanadensiska regelverket, inom de brittiska guiderna samt inom IAEA:s säkerhetsstandarder kunna användas eftersom dessa länder och denna organisation i likhet med Sverige använder sig av målinriktade krav.

Jämförelsen av de internationella kraven identifierar även ett fåtal områden där antingen de svenska kraven inte omfattar området fullt ut eller är så övergripande uttryckt att det är svårt att avgöra om de verkligen motsvarar de internationella kraven. Dessa områden är följande:

- åldring och förlängning av drifttillstånd,
- kärnkraftverkets förläggningsplats,
- uppförande och idrifttagning av ett kärnkraftverk,
- mänskliga faktorer (inkl. säkerhetskultur),
- säkerhetsforskning och drifterfarenheter,
- säkerhetsanalys och riskanalys (probabilistisk säkerhetsanalys),
- verifikation av säkerhet (via tillämpandet av s.k. ”safey cases”),
- brandskydd,
- elektriska system,
- instrumentering och kontrollutrustning (inkl. datorbaserade system),
- anläggningens layout,
- gränssnittet mellan kärnsäkerhet och fysiskt skydd,

- oberoendet inom djupförsvaret,
- evakueringszon och skyddszon, samt
- förbättring av marginaler

Utredningen rekommenderar att dessa områden beaktas inom pågående översyn av det svenska regelverket för kärnkraftreaktorer och att behov av kravförtydliganden avseende dessa områden utvärderas.

En stor skillnad mellan det svenska regelverket och de studerade ländernas samt organisationernas (IAEA och WENRA) krav har även visats vara att samtliga har väl utvecklade råd om tillämpning vilket det framstår som om det saknas i det svenska regelverket. Välutvecklade råd om tillämpning bör kunna skapa en mer ändamålsenliga kravbild genom att ge upphov till enhetliga tolkningar av kraven, underlätta implementering samt ge en effektivare granskning. De flesta länder samt IAEA har strukturmässigt även valt att hålla råd om tillämning i separata dokument. Det framstår vid jämförelsen som om en sådan struktur skulle kunna underlätta en kontinuerlig utveckling av råden i enlighet med senaste kunskaper och erfarenheter, samt ge större möjligheter att beroende på område skapa bästa möjliga utformning för råden. Det bör dock uppmärksammas att en sådan uppdelning inte följer svensk föreskrifstruktur.

Vid genomgången av de internationella regelverken framkommer även att Sverige tydligast har valt att på en hög och övergripande nivå dela upp kraven som reglerar konstruktion och utförandet av kärnkraftsreaktorer i olika kravdokument (exempelvis regleras kärnkraftsanläggningar och vissa delar av tillhörande verksamheter i olika kravdokument).

Denna uppdelning bedöms kunna ge en något komplex bild av kraven eftersom vissa kravdokumenten delvis överlappar varandra. Sådana överlapp syns inte lika tydligt i övriga studerade länders kravdoument och därmed kan det finnas anledning att se över denna struktur. Framför allt vid upprättande av krav för nya kärnkraftsreaktorer.

Jämförelse av säkerhetsförbättringar inom europeiska kärnkraftsreaktorer

De säkerhetsförbättringar som implementerats i utländska reaktorer till grund för längre drifttider och som har studerats i detta PM är ofta likartade för de olika länderna eller för de olika reaktortyperna och grundar sig på nya kunskaper erhållna via drift- eller andra erfarenhet, analys, forskning och utveckling, samt utveckling av IAEA:s säkerhetsstandarder och utveckling av industristandarder. Då den ursprungliga konstruktionen varierar hos de olika reaktorerna som beaktats ser man väsentliga skillnader både i omfattning och i antalet identifierade säkerhetsförbättringar. Det konstateras att fysisk separation, redundans och diversifiering (för att uppnå oberoende) är områden som generellt förstärkts inom de äldre reaktorerna medan förutsättningarna avseende dessa områden varit bättre hos de nyare anläggningarna och därmed har det inte krävts lika omfattande åtgärder för dessa. Av resultatet från genomgången framstår det som om Sverige ligger i

framkant vad gäller omfattning och delvis även framdrift. Detta eftersom Sverige varit mycket tidiga med att implementera omfattande säkerhetsförbättringar i anläggningarna såsom exempelvis implementeringen av de haveribegränsande funktionerna. Utredningen konstaterar att övriga länder generellt och tydligare, än vad som är gjort i Sverige, har lyft upp sitt säkerhetsförbättringsarbetat med följande områden:

- anläggningens möjlighet att hantera naturfenomen och andra händelser som kan uppkomma inom och utanför anläggningen (jordbävning, översvämning, brand, störningar i elkraftnätet inkl. ”station blackout”, etc.)
- oberoende kylning av härden i ett långtidsförlopp,
- åldring,
- möjlighet att vid ett beroende fel i primärpumparnas elmatning förse huvudcirkulationspumparnas (RCP) tätningar med vatten, samt
- bränslebassängernas kylning och integritet

Till följd av stresstesterna har emellertid de områden och säkerhetsförbättringar som tas upp av de andra länderna och som inte tydligt framgår av de svenska kraven och/eller de svenska övergångsbesluten för SSM 2008:17, kunnat belysas och inarbetas i de svenska åtgärdsplaneran för stresstesterna. Utöver de svagheter och säkerhetsförbättringsbehov som identifierats inom stresstesterna har det vid denna genomgång inte varit möjligt att identifiera några ytterligare säkerhetsförbättringsområden som inte omfattas av de befintliga svenska kraven.

Utredningen rekommenderar att man ser över de svenska föreskrifterna för att utveckla relevanta krav utifrån de behov som återspeglas i form av identifierade brister i resultatet från de europeiska stresstesterna samt i form av åtgärder inom de svenska åtgärdsplanerna till följd av stresstesterna. Vid denna översyn bör resultatet från genomgången av säkerhetsförbättringar som presenteras i denna rapport behandlas och därmed bör de områden som anges i punktform ovan speciellt beaktas.

Innehåll

1 Bakgrund

Regeringen beslutade den 8 april 2010 (M2010/2046/Mk) att ge Strålsäkerhetsmyndigheten (SSM) i uppdrag att senast den 31 oktober 2012 redovisa följande:

1. En samlad utvärdering av hur kärnkraftreaktorerna uppfyller de säkerhetskrav som myndigheten föreskrivit i SSMFS 2008:17 och hur myndigheten bedömer att detta moderniseringsarbete har påverkat reaktorsäkerheten.
2. En analys av förutsättningarna för att driva reaktorerna under längre tider (över 50 år) samt vilka ytterligare krav på säkerhetsförbättringar som följer av sådana långa drifttider och utvecklingen inom teknik och vetenskap.
3. En bedömning av vilka huvudsakliga förhållanden som kommer att vara avgörande för om en reaktor kan drivas vidare under långa tider med bibehållen säkerhet.
4. En analys av den svenska tillsynsmodellen inom reaktorsäkerhetsområdet utifrån internationella standarder.
5. Internationella erfarenheter av säkerhetsförbättringar av reaktorer som grund för beslut om långa drifttider.

Den 12 maj 2011 utvidgade regeringen uppdraget genom en komplettering (M2011/1946/Ke) med anledning av olyckan vid Fukushima Dai-ichi kärnkraftverk i Japan.

För att kunna fullfölja regeringsuppdraget skapades tre delprojekt inom SSM enligt följande:

1. Analys och förbättringar av säkerheten i äldre reaktorer baserat på nya kunskaper och säkerhetsutveckling
2. Drift längre än ursprungligt analyserad/konstruerad drifttid med särskild fokus på bevakning av åldringsaspekter och åldringshantering vid långtidsdrift
3. Myndighetens tillsyn av att säkerheten upprätthålls och utvecklas inom reaktorsäkerhetsområdet vid långtidsdrift

Föreliggande PM utgör ett underlag till delprojekt 1, *Analys och förbättringar av säkerheten i äldre reaktorer baserat på nya kunskaper och säkerhetsutveckling*, och avser att beskriva hur de säkerhetskrav som ställs i SSMFS 2008:17 avseende konstruktion och utförande av kärnkraftsreaktorer förhåller sig till internationella regelverk och säkerhetsstandarder. Därutöver avser PM:et att redovisas en jämförelse mellan de säkerhetsförbättringar som krävts av de svenska reaktorerna som grund för längre drifttider och de säkerhetsförbättringar som krävts av myndigheterna i Finland, Frankrike, Schweiz och Tyskland. Dessa två delar utgör etapp 1 respektive etapp 2 till delprojekt 1, och i föreliggande PM används etappbeteckningarna i de

enskilda styckesrubrikerna för att tydliggöra huruvida det är säkerhetskrav eller säkerhetsförbättringar som behandlas.

2 Omfattning och syfte

2.1 Etapp 1

Etapp 1 omfattar en förnyad avstämning av kraven i SSMFS 2008:17 mot de krav som gäller för moderna reaktorer s.k. generation III+ som nu planeras eller byggs i olika delar av världen. I etapp 1 ingår därför att göra en inledande kartläggning av vilka centrala krav som systermyndigheter ställer i de länder som nu uppför eller planerar uppföra moderna reaktorer s.k. generation III+. Utgångspunkten är att få en direkt jämförelse mellan dessa krav och de säkerhetskrav som ställs i SSMFS 2008:17. I detta ingår även att studera struktur och utformning av respektive lands regelvek samt jämföra denna mot det svenska.

Etapp 1 innefattar även en jämförelse av SSMFS 2008:17 mot resultat som framkommit inom WENRA:s Reactor Harmonization Working Group avseende ”Referens Levels” (RL) respektive ”Safety Objectives for new NPPs”. I detta har ingått att bedöma om det utgående från RL finns skäl att öka föreskrifternas detaljeringsgrad eller revidera hur kraven är uttryckta. Därutöver görs en genomgång av WENRAs Safety objektives för att bedöma om dessa på ett eller annat sätt bör utgöra krav på befintliga och/eller nya reaktorer.

2.1.1 Avgränsningar

Den analys och de karläggningar som omfattas av denna utredning har endast beaktat regelverk avseende konstruktion och utformning för kärnkraftsreaktorer utifrån ett kärnkraftssäkerhetsperspektiv (eng. nuclear safety) och har därmed ej beaktat eventuella aspekter avseende fysiskt skydd (eng. security) samt övriga krav relaterade till kärnkraftsreaktorer och dess verksamhet, såsom strålskydd, avfall och icke-spridningsasspekter.

Då kraven för konstruktion och utförande av kärnkraftsreaktorer ofta är uppdelad i flera olika dokument samt fördelade på olika kravnivåer har denna utredning, vid kartläggning av centrala krav, begränsats till att fokusera på ett fåtal övergripande kravdokument.

Flertalet länder samt IAEA tillämpar i dag en kravstruktur där de specifika kraven kompletteras med råd om tillämpning. Dessa råd har i denna utredning endast övergripande studerats för att kunna skapa en bild av respektive lands kravstruktur och någon djupare analys av rådens innehåll har inte utförts inom ramen för denna utredning.

Följande kravdokument för respektive land samt för IAEA har, om inget annat anges, studerats i denna utredning.

Sverige	*Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om konstruktion och utförande av kärnkraftsreaktorer*, SSMFS 2008:17
Finland	*Statsrådets förordning om säkerheten vid kärnkraftverk*, 27.11.2008/733
Storbritannien	*Safety Assessment Principles for Nuclear Facilities*, 2006 Edition, Revision 1
Kanada	*Design of New Nuclear Power Plants*, RD–337, November 2008, Regulatory Document
USA	*General Design Criteria for Nuclear Power Plants*, NRC Regulations Title 10, Code of Federal Regulations, Part 50 Domestic Licensing of Production and Utilization Facilities, Appendix A
IAEA	*Safety of Nuclear Power Plants Design*, IAEA Safety Standards, No. SSR-2/1, Specific Safety Requirements

Ursprungligen ingick även att studera Frankrikes kärnkraftskrav men eftersom relevanta krav inte varit möjliga att identifiera inom det franska systemet trots att resurs av fransk nationalitet anlitats för detta ändamål, har Frankrikes kärnkraftskrav utgått.

2.2 Etapp 2

Etapp 2 omfattar en systematisk kartläggning av de säkerhetsförbättringar som gjorts i utländska reaktorer bland annat till följd av krav från myndigheterna för att möjlliggöra längre drifttider. Denna kartläggning har inriktats på de säkerhetsförbättringar som genomförts i Finland [32], Frankrike [33], Schweiz [34] och Tyskland [35], och som redovisats i respektive lands nationalrapport till det 5:e granskningsmötet inom Kärnsäkerhetskonventionen (Convention on Nuclear Safety, CNS) i april 2011.

2.2.1 Avgränsningar

Den analys och de karläggningar som omfattas av denna utredning har endast beaktat säkerhetsförbättringar för kärnkraftsreaktorer utifrån ett kärnkraftssäkerhetsperspektiv (eng. nuclear safety) och har därmed ej beaktat eventuella aspekter avseende fysiskt skydd (eng. security).

USA har inte ingått i denna kartläggning eftersom den amerikanska myndigheten inte specifikt krävt omfattande säkerhetsförbättringar som grund för långtidsdrift (i samband med förnyat drifttillstånd, omlicensiering har dock myndigheten traditionellt sett haft möjlighet att kräva vissa typer av säkerhetsförbättringar). Likaså omfattas inte Storbritannien eftersom de säkerhetsförbättringar som implementerats i de äldre reaktorerna i Storbritannien i stor utsträckning bedömts vara direkt knutna till gasskylda reaktorer och därmed inte bedömts tillämpningsbara för de svenska lättvattenreaktorerna.

3 Genomförande

3.1 Etapp 1

Etapp 1 har delats upp i två delar där den första delen omfattar jämförelse av SSMFS 2008:17 mot andra länders samt IAEA:s krav och andra delen omfattar en jämförelse av SSMFS 2008:17 mot resultat som framkommit inom WENRA:s Reactor Harmonization Working Group avseende ”Referens Levels” (RL) respektive ”Safety Objectives for new NPPs”.

3.1.1 Jämförelse av SSMFS 2008:17 mot andra länders samt IAEA:s krav

En förnyad avstämning av kraven i SSMFS 2008:17 mot de krav som gäller för konstruktion och utförande av moderna kärnkraftsreaktorer i olika länder har genomförts. De länder och organisationer som studerats är Finland, Storbritannien, Kanada och USA samt IAEA. I samtliga studerade länder pågår nybyggnation kärnkraftverk eller myndighetsgranskning av ansökan om nybyggnation av kärnkraftverk. Urvalet av länder baseras även på tillgängligheten av kravdokumenten, där samtliga studerade länder tillhandahåller kravdokumenten via tillsynsmyndighetens hemsida på svenska eller engelska.

Under 2011 genomfördes en inventering och sammanställning av myndighetskrav i Finland, Frankrike, Storbritannien och USA. Arbetet gjordes med hjälp av externt stöd (myndighetsstöd) och inventering återges i [1]. Detta arbete har utgjort ett underlag för analysen samt ett underlag för kravsammanställningen i bilaga 1.

Utvärderingen av struktur och utformning av respektive lands regelverk samt jämförelsen av denna mot det svenska regelverket, baseras på en övergripande litteraturstudie där varje lands lag och kravdokument relaterad till kärnkraft studerats.

Utgångspunkten för kravinventeringen har varit att få en direkt jämförelse mellan de säkerhetskrav som ställs i SSMFS 2008:17 och de krav som ställs i de utvalda länderna samt inom IAEA:s säkerhetsstandarder. I bilaga 1 till detta PM sammanställs de internationella kraven och för varje paragraf i SSMFS 2008:17 listas motsvarande krav för respektive land samt för IAEA. Därutöver har relevanta krav som identifierats inom de studerade länderna och vars motsvarighet saknas inom SSMFS 2008:17 listats. Bilaga 1 är inte heltäckande utan tar endast upp relevanta krav och guider som identifierats i de krav- och rådgivande dokument som studerats för respektive land samt IAEA. Bilaga 1 är uppdelad i 25 kravområden som till stora delar motsvarar enskilda paragrafer i SSMFS 2008:17 men kan i vissa fall motsvara fler än en paragraf och har därutöver kompletterats med områden som inte behandlas inom SSMFS 2008:17. Kravområden inom bilaga 1 är följande:

1. Krav på säkerhetsfunktionerna
2. Krav avseende djupförsvarets utformande
3. Krav avseende rådrum vid manuella åtgärder
4. Krav avseende reaktorinneslutningen

5. Krav avseende instrumentering för att övervaka de parametrar som är väsentliga för hanteringen av alla händelser och olyckor
6. Krav avseende kylning av reaktorhärden
7. Krav avseende stabilt sluttillstånd och kylning av en smält härd
8. Krav avseende enkelfel
9. Krav avseende motverkandet av uppkomst av fel med gemensam orsak
10. Krav avseende fysisk och funktionell separation
11. Krav avseende tålighet mot händelser och förhållanden som kan uppkomma utanför eller inne i kärnkraftsanläggningen och som kan leda till en radiologisk olycka (inklusive rörbrott)
12. Krav avseende planerat underhåll under drift samt reparation under drift
13. Krav avseende åldring
14. Krav avseende miljötålighet och miljöpåverkan
15. Krav avseende drift och kontrollrum
16. Krav avseende reservövervakningsplats
17. Krav avseende klassning och kvalificering
18. Krav avseende händelseklassning och analys av händelser
19. Krav avseende bränsle och reaktorhärd
20. Krav avseende undantag
21. Krav avseende mänskliga faktorer
22. Krav avseende förläggningsplats samt uppförande och idrifttagning av ett kärnkraftverk
23. Krav avseende drifterfarenheter
24. Krav avseende säkerhetsforskning
25. Övrigt

Genom att studera dessa områden har en uppfattning om vilka områden som beaktats av respektive land samt i vilken utsträckning de enskilda områdena behandlats (speciellt med avseende på detaljeringsnivå) kunnat ges.

3.1.2 Jämförelse av SSMFS 2008:17 mot WENRA ”Referens Levels” (RL) respektive ”Safety Objectives for new NPPs”.

Etapp 1 har utöver ovanstående även innefattat en jämförelse av föreskrifterna i SSMFS 2008:17 mot resultat som framkommit inom WENRA:s arbetsgrupp för harminering av kärnkraftsreaktorer (WENRA Reactor Harmonization Working Group), speciellt avseende WENRA:s referensnivåer (Referens Levels, RL) respektive WENRA:s säkerhetsmål för nya kärnkraftverk (Safety Objectives for new nuclear power plants). I detta ingår att bedöma om det utgående från WENRA:s referensnivåer finns skäl att öka de svenska föreskrifternas detaljeringsgrad eller revidera hur kraven är uttryckta. Därutöver görs en genomgång av WENRA:s säkerhetsmål för nya kärnkraftverk för att bedöma om dessa på ett eller annat sätt bör utgöra krav för befintliga och/eller nya reaktorer.

Genomgången av WENRA:s referensnivåer och säkerhetsmål för nya kärnkraftverk utgår i första hand från WENRA:s uppdaterade lista över referensnivåer från 2008 [40] samt WENRA:s rapporteringar, *Safety*

Objectives for New Power Reactors från 2009 [36], och *Safety of new NPP designs 1/2012* (utkast) från 2012 [38].

3.2 Etapp 2

Under 2011 genomfördes en kartläggning med hjälp av externt stöd (myndighetsstöd) som inriktades på de säkerhetsförbättringar som genomförts i Finland, Frankrike, Schweiz och Tyskland bland annat till följd av krav från myndigheterna för att möjliggöra längre drifttider. Samtliga beaktade länder har lättvattenreaktorer som motsvara de svenska kärnkraftsanläggningarna och likt Sverige, byggdes under 1970- och 1980-talet [1].

Utgångspunkten för kartläggningen har varit att få en direkt jämförelse mellan de säkerhetsförbättringar som genomförts i Sverige och de säkerhetsförbättringar som genomförts i de utvalda länderna.

Som underlag till denna kartläggning användes respektive lands nationalrapport till det 5:e granskningsmötet inom Kärnsäkerhetskonventionen (Convention on Nuclear Safety, CNS) i april 2011, [32], [33], [34] och [35].

Den information som återges i detta PM är hämtad från kartläggningen i [1] och endast i ett fåtal fall har underlag hämtats direkt från respektive lands nationalrapport.

4 Analys

4.1 Etapp 1

4.1.1 Jämförelse av SSMFS 2008:17 mot andra länders samt IAEA:s krav

4.1.1.1 Kravens struktur och omfattning

Strukturen för krav gällande konstruktion och utförande av kärnkraftsreaktorer varierar mellan olika länder och måste ställas i relation till de befogenheter som respektive lands tillsynsmyndighet har samt ländernas politiska system och deras förvaltningsstruktur. Likaså variera den innehållsmässiga omfattning hos kraven inom olika länder och utformandet av kraven bör på liknande sätt som för strukturen ställas i relation till ländernas politiska system och deras förvaltningsstruktur samt även beaktas utifrån de kulturella skillnader som råder mellan olika länder.

Vid kartläggning av innehållet hos de centrala krav som finns avseende konstruktion och utförande av kärnkraftsreaktorer internationellt har föreliggande utredning begränsats till att fokusera på ett fåtal övergripande kravdokument i ett begränsat antal kärnkaraftsländer samt de krav som utfärdas av IAEA i enlighet med avsnitt 2.1.1. De länder som studerats i följande avsnitt är Finland, Storbritannien, Kanada, och USA. En övergripande sammanfattning av dessa krav finns i bilaga 1. Därutöver har den inventering och sammanställning av myndighetskrav i Finland,

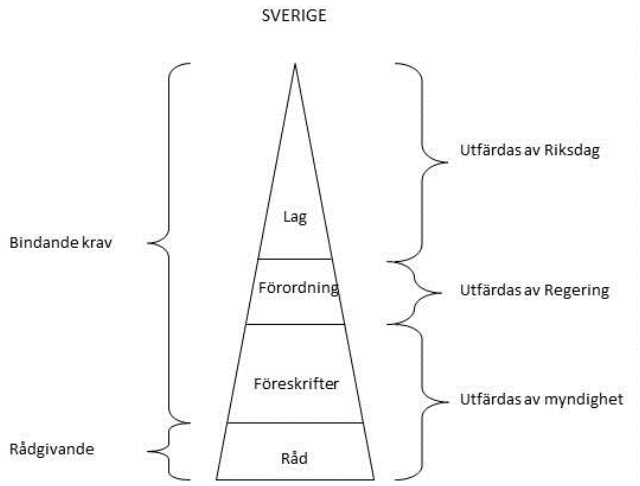
Frankrike, Storbritannien och USA som genomfördes under 2011 med hjälp av externt stöd (myndighetsstöd) och som återges i [1] utgjort ett underlag för denna analys. Dock har de fransk/tyska guiderna som behandlas inom [1] och som är framtagna i ett samarbete mellan franska Institut de Protection et de Sûreté Nucléaire (IPSN) och tyska Gesellschaft für Anlagen- und Reaktorsicherheit (GRS), endast övergripande studerats eftersom dessa inte tillhör ett specifikt lands regelverk och dess status inom de aktuella länderna inte har kunnat fastställas.

De studerade länderna samt IAEA tillämpar en kravstruktur där de specifika kraven kompletteras med råd om tillämpning. Dessa råd har i denna utredning endast övergripande studerats för att kunna skapa en bild av respektive lands kravstruktur och någon djupare analys av rådens innehåll och karaktär har inte utförts inom ramen för denna utredning.

I samtliga länder och inom IAEA med undantag för USA har kraven inom regelverket kontinuerligt reviderats och uppdaterats.

4.1.1.1.1 Sverige

De svenska kraven gällande konstruktion och utförande av kärnkraftsreaktorer framgår av den svenska lagen (1984:3) om kärnteknisk verksamhet [3], den svenska förordningen (1984:14) om kärnteknisk verksamhet [4] samt av Strålsäkerhetsmyndighetens föreskrifter.



Figur 1 - De svenska kraven gällande konstruktion och utförande av kärnkraftsreaktorer

Av Strålsäkerhetsmyndighetens föreskrifter är det framför allt *Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om konstruktion och utförande av kärnkraftsreaktorer* SSMFS 2008:17 [2] som berör det aktuella området. SSMFS 2008:17 kompletterar *Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om säkerhet i kärntekniska anläggningar* SSMFS 2008:1 [5] som definierar generella krav för alla kärntekniska anläggningar, med kärnkraftsreaktorspecifika krav och innehåller därför endast kärnkraftreaktorspecifika krav. Därutöver finns även en specifik föreskriftssamling avseende mekaniska anordningar, *Strålsäkerhetsmyndighetens föreskrifter om mekaniska anordningar i vissa*

kärntekniska anläggningar SSMFS 2008:13 [7] som likaså har stark beröring till detta område.

Till Strålsäkerhetsmyndighetens föreskrifter finns allmänna råd om tillämpning. Dessa råd varierar i omfattning beroende på vilket krav som avses och råden kan i vissa fall vara detaljerade samtidigt som de inte nödvändigtvis är heltäckande för den paragraf som behandlas. Råden[1] är inte bindande för vare sig myndigheter eller enskilda tillståndshavare utan avser endast att utgöra ett stöd vid tillämpning av kraven.

De svenska kraven är målinriktade och definierar en övergripande säkerhetsnivå som ska uppfyllas. Kraven uttrycks på formen ”ska” och ger i ett fåtal fall utrymme för anpassningar genom formuleringarna ”tillräcklig” och ”rimlig”. Enligt 28 § SSMFS 2008:17 ges Strålsäkerhetsmyndigheten möjligheten att ge undantag från föreskrifterna om särskilda skäl föreligger och om ett sådant undantag kan ges utan att syftet med föreskrifterna åsidosätts. När föreskrifterna trädde i kraft 2005 gavs även, med hänvisning till föreskrifternas övergångsbestämmelser, tillfälliga undantag för uppfyllandet av kraven och åtgärdsplaner upprättades för att samtliga reaktorer skulle inom vad som bedömdes som en rimlig tid, åtgärda de brister som identifierats och sedermera uppfylla kraven.

När det gäller innehållet i SSMFS 2008:17 [2] är detta uppdelat på ett antal huvudområden:

1. Tillämpningsområde och definitioner
2. Konstruktionsprinciper för djupförsvaret
3. Tålighet mot felfunktioner samt andra inre och yttre händelser[2]
4. Miljötålighet och miljöpåverkan
5. Bestämmelser om kontrollrum
6. Säkerhetsklassning
7. Händelseklassning
8. Bestämmelser om reaktorhärden
9. Undantag

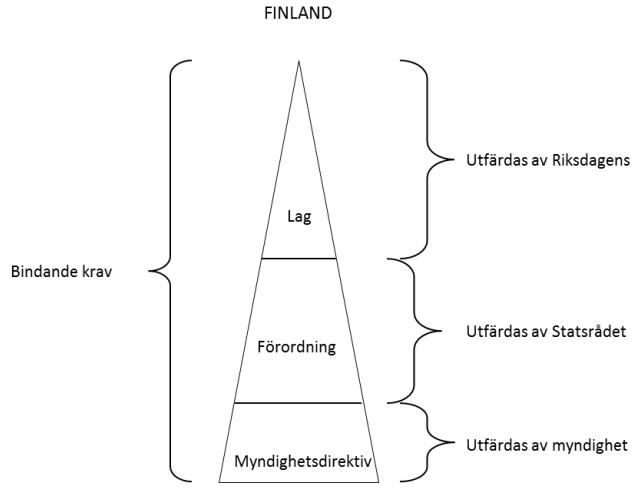
4.1.1.1.2 Finland

Regelverket i Finland avseende konstruktion och utförande av kärnkraftsreaktorer består dels av kärnenergilagen, statsrådets förordningar samt myndighetsdirektiv, där framför allt Statsrådets förordning om säkerheten vid kärnkraftverk (733/2008) [11] samt Kärnkraftverksdirektiven YVL, som är relevanta för detta område.

---

[1] 1 § Författningssamlingsförordningen (1976:725) definierar allmänna råd som sådana generella rekommendationer om tillämpningen av en författning som anger hur någon kan eller bör handla i ett visst hänseende.

[2] Inre händelser avser alla tänkbara fel eller situationer som kan uppstå inom anläggningen och som kan påverka anläggningens säkerhet.
Ytter händelser avser händelser som kan uppkomma utanför anläggningen och kan påverka anläggningens säkerhet. Yttre händelser innefattar bland annat naturfenomen, kemiska och bilogiska utsläpp i närregion, explosioner i närregion, flygplanskrascher samt händelser på det yttre elkraftnätet.



Figur 2 - De finska kraven gällande konstruktion och utförande av kärnkraftsreaktorer

Lagen som reglerar kärntekniska anläggningar i Finland [10] är på en hög nivå och liknar i detaljeringsnivå den svenska lagen om kärnteknisk verksamhet [3].

Den finska förordningen om säkerheten vid kärnkraftverk [11] har stora likheter med SSMFS 2008:17. Kraven är målinriktade och definierar en övergripande säkerhetsnivå som ska uppfyllas. Likaså är formuleringarna utformade på liknande sätt som de som återges i SSMFS 2008:17.

Förordningen är uppdelad i kapitel efter huvudområde:

1. Allmän säkerhet
2. Begränsning av strålexponering och utsläpp av radioaktiva ämnen
3. Kärnsäkerhet
4. Uppförande och idrifttagning av ett kärnkraftverk
5. Kärnkraftverkets drift
6. Organisation och personal
7. Ikraftträdande och övergångsbestämmelser

Den finska förordningen om säkerheten vid kärnkraftverk är förhållandevis strukturmässigt heltäckande avseende konstruktionen och utförande av kärnkraftsreaktorer. Kravens innehållsmässiga omfattning motsvarar i mångt och mycket den svenska kravbilden, med undantag för att den finska förordningen omfattar tydligare krav avseende åldring, kärnkraftverkets förläggningsplats, uppförande och idrifttagning av ett kärnkraftverk, mänskliga faktorer (inkl. säkerhetskultur), säkerhetsforskning och drifterfarenheter.

Den finska tillsynsmyndigheten utfärdar myndighetsdirektiv som går under beteckningen Kärnkraftverksdirektiven, YVL. Dessa myndighetsdirektiv påminner i detaljeringsgrad om de råd om tillämpning som ges ut av tillsynsmyndigheten i USA (Regulatory Guidens), men dess juridiska status framstår som något diffus. På tillsynsmyndighetens svenska hemsida används begrepp som ”krav” och ”regler” i samband med kärnkraftverksdirektiven vilket indikerar att de i juridisk mening skulle motsvara de föreskrifter som ges ut av tillsynsmyndigheten i Sverige. I en VTT-rapport från 2001 [41] som behandlar kärnkraftverksdirektiven,

publicerad på tillsynsmyndighetens hemsida, anges dock i motsatts till detta att kärnkraftverksdirektiven inte är bindande utan endast rådgivande. Likaså används begreppet ”guide” på engelska för att beskriva kärnkraftsverksdirektiven. Det konstateras även att kärnkraftsverksdirektivens formuleringar medför att det framstår som om det finns ett större utrymme för anpassningar än motsvarande svenska föreskrifter. Likaså ges till skillnad från undantagsförfarandet som anges enligt 28 § SSMFS 2008:17, en större möjlighet att avvika från kraven i och med att det generellt anges att den som vill avvika från de krav som ställs i kärnkraftverksdirektiven måste kunna presentera ett alternativt och godtagbart förfaringssätt eller lösning med vilken samma säkerhetsnivå som krävs i respektive kärnkraftverksdirektiv uppnås.

För befintliga kärnkraftsreaktorer som är i drift eller under uppförande beslutar tillsynsmyndigheten om hur de nya kärnkraftverksdirektiven skall tillämpas på anläggningarna och på den verksamheten som bedrivs av de som innehar driftstillstånd. För nya kärnkraftsreaktorer ska kärnkraftverksdirektiven tillämpas omedelbart.

Kärnkraftverksdirektiven har de senaste åren genomgått en större helomfattande revidering av struktur och den reviderade strukturen för kärnkraftverksdirektiven avses att fastställas under 2013.

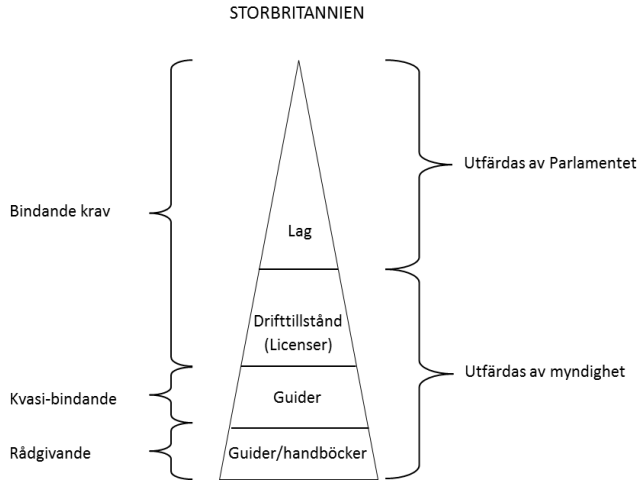
Kärnkraftverksdirektiven är uppdelade på huvudområden:

1. Allmänna direktiv
2. System
3. Tryckapparater
4. Byggnadsteknik
5. Andra konstruktioner och apparater
6. Kärnmaterial
7. Strålskydd
8. Kärnavfallsunderhåll

Till varje huvudområde finns ett antal ämnesområdesspecifika krav. Av dessa kan som exempel nämnas YVL 1.0 – Säkerhetsprinciper för planering av kärnkraftverk [11], YVL 1.10 – Kriterier gällande kärnkraftverkets förläggningsplats [13], och YVL 2.0 – Konstruktion av system i kärnkraftverk [14]. I jämförelse med de svenska kraven bedöms kraven som återges i kärnkraftverksdirektiven vara betydligt mer detaljerade och specifika samt även delvis mer långtgående. Exempel på områden som regleras utförligare i de finska kärnkraftsverksdirektivens än i de svenska föreskrifterna är elektriska system, brandskydd och MTO.

4.1.1.1.3 Storbritannien

Regelverket i Storbritannien avseende konstruktion och utförande av kärnkraftsreaktorer består av kärntekniklagen, respektive tillståndshavares drifttillstånd (licens) samt de mer detaljerade råden om tillämpning på två olika hierarkiska nivåer.



Figur 3 - De brittiska kraven gällande konstruktion och utförande av kärnkraftsreaktorer

Lagen som reglerar kärntekniska anläggningar i Storbritannien [15] är på en hög nivå och liknar i detaljeringsnivå den svenska lagen [3] tillsammans med förordningen [4] om kärntekniska verksamheter.

Den brittiska tillsynsmyndigheten har enligt lagen befogenhet att ställa de krav på respektive tillståndshavare som man anser nödvändiga för att respektive tillståndshavare och dess anläggning(ar) ska uppfylla lagen. Detta görs via specifika beslut och drifttillstånd (licenser). Trots den allmänt hållna nivån på lagen finns det inte i Storbritannien några bindande allmänna kravdokument på motsvarande nivå som de svenska föreskrifteran för kärnkraftsreaktorer. Den brittiska myndigheten har i stället valt att utfärda kvasi-bindande råd om tillämpning, s.k. guider. Dessa guider är mer detaljerade än lagen och definierar de säkerhetsnivåer som ska uppfyllas och tillämpas. I praktiken tillämpas dessa guider på liknande sätt som de svenska föreskrifterna eftersom de är starkt vägledande vid myndighetens beslut. När det gäller konstruktion och utförande av kärnkraftsreaktorer är det framförallt guiden *Safety Assessment Principles for Nuclear Facilities (SAP)* [16] som bör beaktas. Denna guide togs fram som en del av förberedelserna för nybyggnation av kärnkraft i Storbritannien och är starkt vägledande för tillsynsmyndighetens beslut relaterade till kärntekniska anläggningar, speciellt vid tillståndsprövningsprocessen för nya kärnkraftreaktorer. Syftet vid framtagandet var framförallt att ge myndighetens handläggare ett stöd för att kunna göra konsekventa och systematiska bedömningar avseende kärnsäkerhet. Därutöver har SAP även kunnat utgöra ett stöd för enskilda tillståndshavare vid tillämpning.

SAP [16] innehåller målinriktade säkerhetsprinciper och definierar i likhet med SSMFS 2008:17 en övergripande säkerhetsnivå för kärnkraftreaktorer. I likhet med vad som gäller för de finska kärnkraftverksdirektiven, måste den som vill avvika från guiden kunna presentera ett alternativt och godtagbart förfaringssätt eller lösning med vilken samma säkerhetsnivå som krävs i guiden uppnås.

SAP [16] är strukturerad efter ett antal huvudområden.

1. Allmänna Principer

2. Ledningssystem
3. Myndighetens utgångspunkter vid säkerhetsvärderingar
4. Myndighetens utgångspunkter vid säkerhetsvärderingar vid val av förläggningsplats
5. Principer för konstruktion och utförande
6. Strålskydd
7. Riskanalys
8. Marginaler och gränsvärden
9. Beredskap
10. Avfallshantering
11. Rivning
12. Sanering av mark

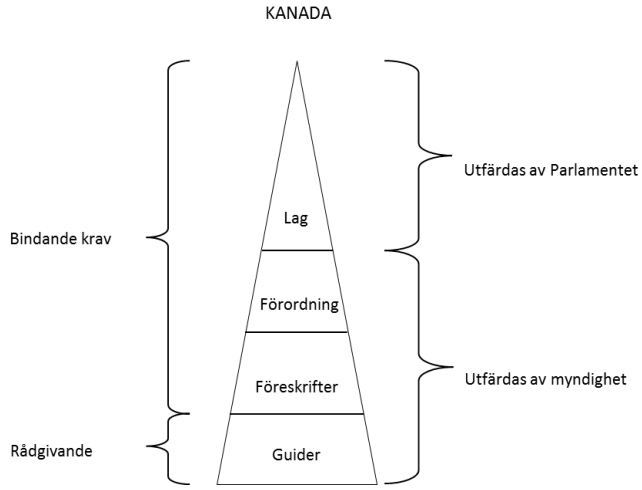
Inom varje huvudområde definieras ett antal övergripande principer, som bygger på IAEA Safety Fundamentals [42]. Dessa kan närmast liknas vid enskilda paragrafer inom det svenska regelverket och har i denna utredning beaktats motsvarande. Till de övergripande principerna finns ett antal vägledande råd. Dessa är ofta mer specifika och kan i mångt och mycket liknas vid de allmänna råd som ges till enskilda paragrafer inom det svenska regelverket men har i visa fall utformats på ett sådant sätt att de mer liknar enskilda paragrafer inom SSMFS 2008:17. Denna utredning har dock beaktat dessa vägledande råd motsvarande de svenska föreskrifterna och delar därför även upp de *övergripande principerna* och de *vägledande råden* i bilaga 1.

Den brittiska guiden är förhållandevis strukturmässigt heltäckande avseende konstruktionen och utförande av kärnkraftsreaktorer. Liksom den finska kravbilden motsvarar den innehållsmässiga omfattningen i den brittiska lagen tillsammans med guiden SAP, i mångt och mycket den svenska kravbilden men är utförligare, tydligare och mer specifik. Exempel på områden som behandlas tydligare eller alternativt inte har beaktas inom de svenska kraven är riskanalyser (probabilistisk säkerhetsanalys), förläggningsplats, uppförande och drifttagning av kärnkraftsreaktorer, åldring, verifikation av säkerhet (via tillämpandet av s.k. ”safey cases”), datorbaserade system, drifterfarenheter och mänskliga faktorer.

Utöver den ovannämnda guiden SAP utfärdar den brittiska myndigheten även detaljerade guider och handböcker på en lägre hierarkisk nivå, som ett stöd för myndighetens inspektörer och dessa dokument har på motsvarande sätt som SAP ingen bindande juridisk status och har inte studerats inom denna utredning.

4.1.1.1.4 Kanada

Regelverket i Kanada avseende konstruktion och utförande av kärnkraftsreaktorer består av kärntekniklagen, myndighetens förordningar (eng. Regulations), myndighetens föreskrifter (eng. Regulatory documents) samt de mer detaljerade råden om tillämpning (eng. Guidance document).



Figur 4 - De kanadensiska kraven gällande konstruktion och utförande av kärnkraftsreaktorer

Lagen som reglerar kärntekniska anläggningar i Kanada [17] är på en hög nivå och liknar i detaljeringsnivå den svenska lagen om kärnteknisk verksamhet [3]. Myndighetens förordningar (eng. Regulations) är likaså på en hög nivå. När det gäller kärnkraftsreaktorer är det framför allt regleringen *Class I Nuclear Facilities Regulations* [18] som är tillämpningsbar. I relation till det svenska regelverket motsvarar kravnivån i den kanadensiska lagen tillsammans med förordningen avseende kärntekniska anläggningar innehållsmässigt den svenska lagen [3] tillsammans med förordningen [4] avseende kärnteknisk verksamhet.

Den kanadensiska myndighetens föreskrifter innehåller målinriktade krav och definierar, i likhet med SSMFS 2008:17, en övergripande säkerhetsnivå för kärnkraftsreaktorer. När det gäller konstruktion och utförande av kärnkraftsreaktorer är det framförallt föreskrifterna i *Design of New Nuclear Power* [19] som bör beaktas. I detaljeringsnivå och upplägg liknar denna föreskrift den brittiska myndighetens guide SAP [16]. Säkerhetsanalysområdet, åldring samt förläggningsplats berörs dock endast övergripande i föreskriften eftersom att det för dessa områden finns separata föreskrifter i *Plants Safety Analysis for Nuclear Power Plants* [20], *Aging Management for Nuclear Power Plants* [21], *Life Extension of Nuclear Power Plants* [22] respektive *Site Evaluation for New Nuclear Power Plants* [23] som kravställer just dessa områden.

Föreskrifterna i [19] är strukturerade efter ett antal huvudområden:

1. Allmänna säkerhetsmål och begrepp
2. Säkerhetsstyrning under konstruktionsfas
3. Allmänna säkerhetsprinciper
4. Allmänna principer inom konstruktion och utförande
5. Systemspecifika krav
6. Säkerhetsanalys
7. Skydd av miljö
8. Alternativa tillvägagångssätt

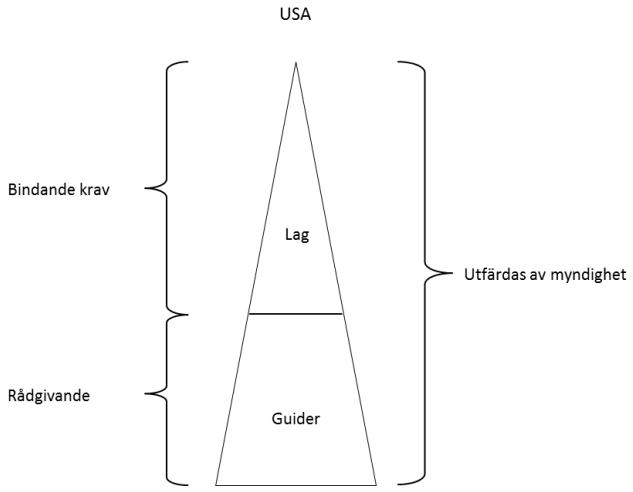
Den kanadensiska föreskriftsamlingen [19] är förhållandevis strukturmässigt heltäckande avseende konstruktionen och utförande av kärnkraftsreaktorer. För vissa områden har dock den kanadensiska myndigheten valt att utöver det som nämns i de övergripande föreskrifterna utfärda mer detaljerade krav vilket görs i specifika kravdokument i likhet med SSMFS 2008:13[7]. Detta gäller områden som säkerhetsanalys [20], åldring [21] och förlängning av drifttillstånd [22] samt förläggningsplats[23]. Samtliga områden berörs endast övergripande i motsvarande svenska föreskrifter.

Liksom den finska och brittiska kravbilden motsvarar den innehållsmässiga omfattningen i den kanadensiska lagen tillsammans med föreskrifterna i [19], i mångt och mycket den svenska kravbilden men är utförligare, tydligare och mer specifik. Exempel på områden som behandlas tydligare eller alternativt inte har beaktas inom den svenska kraven är säkerhetsanalys, åldring och förlängning av drifttillstånd, kärnkraftverkets förläggningsplats, uppförande och idrifttagning av ett kärnkraftverk, mänskliga faktorer (inkl. säkerhetskultur), säkerhetsforskning och drifterfarenheter.

Den kanadensiska myndigheten ger även ut detaljerade råd om tillämpning, s.k. guider. Guiderna avser att utgöra ett stöda för tillståndshavare och tillståndsansökanden avseende tolkning och tillämpning av de gällande kraven.

4.1.1.1.5 USA

Regelverket i USA avseende konstruktion och utförande av kärnkraftsreaktorer består av kärntekniklagen, respektive tillståndshavares drifttillstånd (licens) samt mer detaljerade råd om tillämpning.



Figur 5 - De amerikanska kraven gällande konstruktion och utförande av kärnkraftsreaktorer

Den amerikanska lagen som reglerar kärntekniska anläggningar och kärntekniska verksamhet [24] är mycket detaljerad och oerhört omfattande. Lagen i sig är inte målinriktad utan innehåller preciserade krav som anger hur saker och ting ska utföras. Dess likhet går inte att finna i något av de övriga studerade länderna.

När det gäller kärnkraftsreaktorer är det framför allt *Title 10 - Code of Federal Regulations, Chapter 1, Part 50 - Domestic Licensing of production and utilization facilities* [25] som är av intresse. Detta avsnitt omfattar 113 delavsnitt samt 18 bilagor, där varje delavsnitt och bilaga kan bestå av flera A4 sidor kravtext. Till följd av den otroligt omfattande lagen har denna utredning begränsats till att endast studera bilaga *Appendix A - General Design Criteria for Nuclear Power Plants (GDC)* [26]. Denna bilaga definierar en mängd kriterier som ska gälla vid konstruktion och utförande av kärnkraftreaktorer och har ursprungligen varit och är fortfarande till viss mån, vägledande för Sverige och andra kärnkraftländers krav. Detaljeringsnivån i GDC är dock betydligt högre än motsvarande svenska föreskrifter.

Kriterierna i GDC [26] är strukturerade efter ett antal huvudområden:

1. Allmänna krav
2. Skydd av säkerhetsbarriärer
3. Säkerhets- och reaktivitetskontrollsystem
4. Vattenbärandesystem
5. Inneslutning
6. Bränsle och reaktivitetskontroll

De amerikanska kraven och framför allt GDC framstår vid första anblick som heltäckande men då kraven inte utvecklats sedan de ursprunglige utfärdades saknas bland annat moderna krav såsom krav gällande svåra haverier, konstruktionsprinciper för djupförsvar (inkl. diversifiering) och säkerhetsfunktioner (inkl. rådrum).

Trots den exceptionella omfattningen hos det amerikanska regelverket har inga krav som sträcker sig utanför de svenska kravens innehållsmässiga omfattning kunnat identifieras. Däremot är samtliga krav betydligt mer utförliga och preciserade. Speciellt inom områden som brandskydd och elektriska system där de svenska kraven är anmärkningsvärt kortfattad.

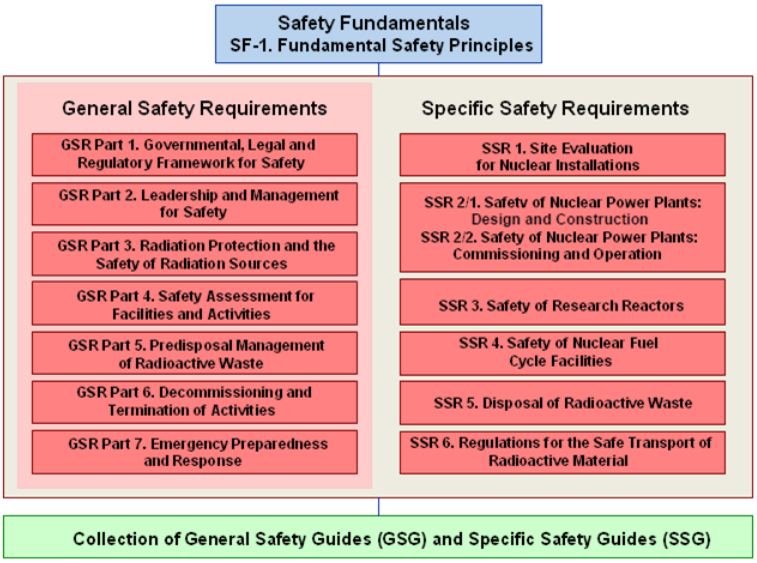
Utöver de mycket omfattande kravtexterna ger även den amerikanska myndigheten ut råd om tillämpning. Sådana råd kan dels rikta sig till myndighetens inspektörer och utredare såsom *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition* och dels till tillståndshavare och tillståndsansökanden såsom *NRC Regulatory Guides - Power Reactors (Division 1)* [28]. Råden avser att ge vägledning avseende tolkning och tillämpning av lagen och revideras vid behov. Råden har likt de amerikanska kraven varit vägledande för kärnteknisk verksamhet i många kärnkraftsländer och är till följd av den behovsanpassade revideringen fortfarande vägledande för stora delar av kärnkraftsindustrin runt om i världen.

4.1.1.1.6 IAEA

Säkerhetsstandarderna inom IAEA är uppbyggt i tre nivåer:

1. Övergripande säkerhetsprinciper
   (Safety Fundamentals)

2. Övergripande och specifika säkerhetskrav
   (General Safety Requirements respektive *Specific Requirements)*
3. Övergripande och specifika råd
   (General Safety Guides respektive *Specific Safety Guides)*



Figur 6 - Strukturen för IAEA:s säkerhetsstandarder

IAEA:s säkerhetsstandarder bygger på internationell konsensus avseende acceptabel strålsäkerhetsnivå och utvecklas i samarbete med internationell expertis. Översyn av befintliga säkerhetsstandarder sker med jämna intervall och vid behov utvecklas nya säkerhetsstandarder. Säkerhetsstandarderna riktar sig främst till tillsynsmyndigheter hos IAEA:s medlemsstater, men är även tillämpningsbara för övriga intressenter såsom industri samt forskningsinstitut och universitet.

När det gäller konstruktion och utförande av kärnkraftsreaktorer är det framför allt de specifika säkerhetskraven *Safety of Nuclear Power Plants Design, No. SSR-2/1* [29], *Site Evaluation for Nuclear Installations Safety Requirements, No SSR-1/1* [30], och *Safety of Nuclear Power Plants: Commissioning and Operation Specific Safety Requirements, No SSR -1/3* [31] som är av intresse. Utöver kraven ger IAEA även ut detaljerade råd om tillämpning, s.k. guider. Guiderna avser att utgöra ett stöda avseende tolkning och tillämpning av säkerhetskraven och är ofta mycket preciserade. Föreliggande utredning har begränsats till att endast övergripande studera dessa guider.

IAEA:s säkerhetsstandarder innehåller målinriktade krav och definierar, i likhet med SSMFS 2008:17, en övergripande säkerhetsnivå för kärnkraftsreaktorer. På en övergripande nivån motsvarar de svenska kraven innehållsmässigt väl kraven i IAEA:s säkerhetsstandarder. Dock är IAEA:s standarder i många fall mer utvecklade, tydliga och specifika samt omfattar tydligare krav avseende åldring, kärnkraftverkets förläggningsplats, uppförande och idrifttagning av ett kärnkraftverk, mänskliga faktorer (inkl. säkerhetskultur), säkerhetsforskning och drifterfarenheter.

4.1.1.1.7 Likheter och olikheter mellan de studerade länderna samt IAEA

Tillsynsmyndigheterna i Finland och Kanada har i likhet med tillsynsmyndigheten i Sverige rätt att utfärda mer detaljerade bindande krav än de som finns i lagen och förordningarna. Tillsynsmyndigheten i USA utfärdar kärntekniklagen för civil verksamhet inom USA vilken innehåller förhållandevis detaljerade krav. När det gäller Storbritannien är lagen utformad så att tillsynsmyndigheten har befogenhet att ställa de krav på respektive tillståndshavare som man anser nödvändiga för att respektive tillståndshavare och dess anläggning(ar) ska uppfylla lagen. Det finns dock inga bindande generella krav på motsvarande nivå som de svenska föreskrifterna för kärnkraftsreaktorer.

Med undantag för USA, har samtliga länders regelverk samt IAEA:s säkerhetsstandarder haft en kontinuerlig utveckling och genomgått en omfattande strukturella och innehållsmässiga revidering sedan de ursprungliga kraven utfärdades. I vilken utsträckning gamla anläggningar ska uppfylla moderna krav skiljer sig emellertid åt mellan länderna men de flesta länder har valt att ge tillsynsmyndigheten möjlighet att avgöra detta i enskilda fall. I USA har ändringarna av kraven i jämförels med övriga studerade länder varit marginella och för äldre anläggningar ges i större utsträckning undantag än i övriga länder.

Vid en övergripande genomgång av respektive lands regelverk avseende konstruktion och utförande av kärnkraftsreaktorer ser man tydligt att de svenska kravns textmässiga omfattning skiljer sig från övriga länder då de svenska kravdokumenten är betydligt mer kortfattade än övriga länders kravdokument. Sverige är även det land där man tydligast valt att på en allmänt hållen och övergripande nivå dela upp kraven som reglerar kärnkraftsreaktorer i olika kravdokument. Detta medför att vissa skillnader i omfattning mellan Sveriges och de övriga ländernas (studerade) kravdokument kan härledas till att vissa krav inom den svenska kravstrukturen återfinns i andra föreskrifter än de som ingår i SSMFS 2008:17 [2]. Exempelvis omfattar föreskrifterna SSMFS 2008:1 [5] och SSMFS 2008:13 [7] samt Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om kompetens hos driftpersonal vid reaktoranläggningar SSMFS 2008:32 [8] krav avseende konstruktion och utförande av kärnkraftverk. Det bör även tilläggas att förläggningsplats framförallt regleras av Miljöbalk (1998:808) [9]. Vidare noteras att denna uppdelning som finns i Sverige där flera olika kravdokument behandlar kärnkraftsanläggningarnas utförande och konstruktion samt dess tillhörande verksamheter, ger en något komplex bild av kraven eftersom denna struktur innebär ett visst överlapp mellan de olika kravdokumenten.

Genom att studera kraven i de olika länderna utifrån de kravområden som återges i bilaga 1 har en uppfattning om vilka områden som beaktats av respektive land samt i vilken utsträckning de enskilda områdena behandlats (speciellt med avseende på detaljeringsnivå) kunnat ges. Av denna jämförelse framgår tydligt att det är ett brett spann på fokusområden hos de enskilda länderna. Sverige är dock förhållandevis unik när det kommer till detaljeringsnivå hos kravbilden. Detta eftersom kravens detaljeringsnivå ofta

är mycket låg samtidigt som de allmänna råden som återges till de enskilda paragraferna ofta är begränsade i omfattning samt ej heltäckande.

Av det studerade kravdokumenten är den finska förordningen [11] mest lik de svenska föreskrifterna [5] men till skillnad från de svenska föreskrifterna kompletteras den finska förordningen med utförligare krav i de s.k. kärnkraftverksdirektiven. Kärnkraftverksdirektiven är emellertid ”öppnare” än de svenska föreskrifterna eftersom det generellt ges möjlighet till avsteg om man kan visa att intentionen med kravet och att säkerhetsnivå upprätthålls. Detta medför att det i vissa fall i kärnkraftverksdirektiven framstå som om kraven snarare ska ses som råd om tillämpning än som strikta krav.

Det amerikanska regelverket ligger längst ifrån den svenska avseende struktur, detaljeringsnivå och textmässiga omfattning. Det kan dock noteras att det amerikanska regelverket förefaller som förhållandevis unik i dessa avseenden och har till skillnad från övriga länder inte genomgått någon struktur- och innehållsmässig modernisering sedan det ursprungliga instiftandet. Detta medför att det inte vid genomgången identifierats några direkta moderna krav som inte finns i det svenska regelverket.

När det gäller den sammanvägda detaljeringsnivå för kraven relaterade till konstruktion och utförande av kärnkraftsreaktorer i de olika länderna så verkar det som om Storbritannien tillsammans med Kanada har mest likheter med Sverige. Både Storbritannien och Kanada tillämpar målinriktade krav, som i likhet med de svenska kraven definierar en övergripande säkerhetsnivå för kärnkraftreaktorer. Det som skiljer Sverige från de båda övriga länderna är att man i dessa valt att ge ut mer detaljerade råd om tillämpning än de som återfinns i de svenska allmänna råden om tillämpning.

Därutöver är kraven hos dessa länder mer utförliga, tydliga och specifika. Detta gäller framför allt följande områden:

- Åldring och förlängning av drifttillstånd,
- kärnkraftverkets förläggningsplats,
- uppförande och idrifttagning av ett kärnkraftverk,
- mänskliga faktorer (inkl. säkerhetskultur), samt
- säkerhetsforskning och drifterfarenheter.

Därutöver återfinns även tydligare krav gällande:

- säkerhetsanalys och riskanalys (probabilistisk säkerhetsanalys),
- verifikation av säkerhet (via tillämpandet av s.k. ”safey cases”),
- brandskydd,
- elektriska system, samt
- instrumentering och kontrollutrustning (inkl. datorbaserade system).

Den övergripande skillnaden som finns i tydlighet och precisering mellan det svenska regelverket och övriga studerade länder samt IAEA, diskuteras vidare i avsnitt 4.1.3.

Beträffande råd om tillämpning konstateras att alla studerade länderna samt IAEA använder sig av råd om tillämpning för att antingen vägleda myndighetens inspektörer och utredare, och/eller tillståndshavare och

tillståndsansökanden. Den textmässiga omfattningen av dessa skiljer sig betydligt. I Sverige finns i dag s.k. allmänna råd om tillämpning till respektive föreskriftsamling. Dessa råd är i många fall mindre utvecklande än de som finns i övriga studerade länder samt att dess omfattning variera betydligt. Med varierande omfattning avses här det faktum att för vissa paragrafer i SSMFS 2008:17 är de allmänna råden om tillämpning mycket preciserade avseende specifika delar av kravet medan andra delar av kravet helt utelämnas. Övriga länders råd är mer harmoniserade både avseende omfattning och detaljeringsnivå. Det kan även noteras att för USA är det just via råden om tillämpning som den amerikanska myndigheten har getts möjlighet att införa en modern syn på kärnsäkerhetsarbete och att det är via dessa råd som inspiration till moderna krav bör kunna hämtas.

4.1.2 Jämförelse av SSMFS 2008:17 mot WENRA ”Referens Levels” (RL) respektive ”Safety Objectives for new NPPs”.

WENRA:s referensnivåer (eng. WENRA Reference Levels) och säkerhetsmål för nya kärnkraftsverk (eng. WENRA safety objectives for new nuclear power plants), har utvecklats av en arbetsgrupp inom WENRA (Reactor Harmonization Working Group, RHWG) genom en systematisk översyn av befintliga säkerhtersprinciper för kärnkraftsverk.

Avsikten med WENRA:s referensnivåer och övergripande säkerhetsmål är att skapa en förståelse för eventuella skillnader mellan WENRA:s medlemsländers krav avseende kärnkraftsäkerhet samt att möjliggöra en harmonisering av säkerhetsarbetet och kärnsäkerhetskraven inom medlemsländerna. Säkerhetsmålen avser även att frambringa en högre säkerhetsnivå hos nya kärnkraftreaktorer än vad som är möjligt att åstadkomma i befintliga anläggningar.

Referensnivåerna var ursprungligen framtagna för befintliga kärnkraftverk men har senare bedömts kunna utgöra en grund för utvecklandet av krav för nya kärnkraftverk.

Säkerhetsmålen som utvecklades efter att de ursprungliga referensnivåerna var fastställda riktas i första hand mot nya kärnkraftverk men har på liknande sätt som för referensnivåerna omvärderats och bedöms nu även kunna användas för att identifiera behov av säkerhetsförbättringar för befintliga anläggningar.

4.1.2.1 WENRA:s referensnivåer

WENRA:s referensnivåer fastställdes ursprungligen i *WENRA Harmonization of Reactor Safety in WENRA Countries* från 2006 [39] och uppdaterades därefter i *WENRA Reactor Safety Reference Levels* från 2008 [40]. Till följd av olyckan i kärnkraftverket i Fukushima Dai-ichi beslutade WENRA i april 2012 att man ska se över referensnivåerna för att inarbeta erfarenheter från kärnkraftolyckan samt resultatet från de europeiska stresstesterna som genomfördes 2011-2012 och det extraordinära granskningsmötet för kärnsäkerhetskonventionen som genomfördes i augusti 2012. Förslag till ändringar av referensnivåerna avses att presenteras vid WENRA-mötet november 2013.

Avsikten med referensnivåerna var att utifrån IAEA:s säkerhetsstandarder utveckla och definiera de mest grundläggande säkerhetskraven utifrån 18 övergripande säkerhetsaspekter. Dessa skulle sedan kunna utgöra grund för medlemsländernas säkerhetsarbete och skapa en hög nivå av säkerhets hos alla kärnkraftverk inom WENRA:s medlemsländer.

I Sverige har WENRA:s referensnivåer legat till grund för de uppdateringar av föreskrifterna inom SSMFS 2008:1 som skett och pågående föreskriftöversyn avser att på liknande sätt beakta referensnivåerna och inarbeta dessa i de svenska kraven.

WENRA:s referensnivåer delas upp i 18 huvudområden och för varje område återges specificerade mål och vägledning till hur målet ska uppfyllas. Nedan återges de 18 huvudområdena:

1. Säkerhetsprogram
2. Driftorganisation
3. Ledningssystem
4. Utbildning och behörighet för kärnkraftspersonal
5. Ursprungliga konstruktionsförutsättningar för befintliga reaktorer
6. Utvidgade konstruktionsförutsättningar för befintliga reaktorer
7. Säkerhetsklassificering av strukturer, system och komponenter
8. Säkerhetstekniska driftförutsättningar
9. Åldringsprogram
10. Erfarenhetsåterföringsprogram
11. Underhåll, inspektion, provning och tester
12. Störningsinstruktioner och handbok för svåra haverier
13. Innehåll och uppdatering av säkerhetsredovisningen
14. Probabilistisk säkerhetsanalys (PSA)
15. Återkommande helhetsbedömning av anläggningens säkerhet (PSR)
16. Anläggningsändringar
17. Haveribereskap inom anläggningen
18. Brandskydd

Motsvarande områden återfinns i det svenska regelverket men omfattningen hos de svenska kraven varierar och för ett fåtal områden uppfyller inte den svenska kravbilen referensnivåerna fullt ut[3].

Den stora generella skillnaden mellan de svenska kraven och referensnivåerna är detaljeringsgraden och referensnivåerna är betydligt mer preciserade än motsvarande svenska krav. Skillnaden medför att

[3] Uppfyllandet av WENRA:s referensnivåer behandlas vidare i etapp 3 av denna utredning.

referensnivåerna kan uppfattas som tydligare än de svenska kraven och ger mindre utrymme för tolkning. Detta gäller framför allt områdena åldring, probabilistisk säkerhetsanalys och brandskydd, där de befintliga svenska kraven är på en så övergripande nivå att är svårt att bedöma huruvida referensnivån verkligen uppfylls. Precisering av krav behandlas vidare i avsnitt 4.1.3 i detta PM.

4.1.2.2 WENRA:s säkerhetsmål

Grunderna för WENRA:s säkerhetsmål beskrivs i RHWG:s rapport, *Safety Objectives for New Power Reactors* [36], från December 2009. Av detta PM framgår att IAEA:s övergripande säkerhetsprinciper, *Fundamental Safety Principles* (SF-1) [37], som gavs ut 2006 har legat till grund för definitionen av säkerhetsmålen. Utöver IAEA:s övergripande säkerhetsprinciper har arbetet även beaktat Kärnsäkerhetskonventionen, IAEA:s övriga standarder gällande konstruktion och drift av kärnkraftverk, befintliga nationella regelverk avseende kärnkraftsäkerhet, en genomgång av gällande bästa praxis avseende kärnkraftsäkerhet inom OECD/NEA och EU, samt identifierade framtida utmaningar för kärnsäkerhetsmyndigheter.

Säkerhetsmålen delas upp sju områden O1 – O7, vilka återges i Tabell 1 nedan. Då säkerhetsmålen är kvalitativa och på en hög nivå har en områdesvis vägledning till säkerhetsmålen tagits fram samt exempel på åtgärder som bör vidtas för att uppfylla respektive säkerhetsmål. Dessa återges likaså i Tabell 1 nedan.

WENRA:s Säkerhetsmål	**Område**	**Beskrivning**	**Vägledning**	**Exempel på åtgärder**
O1	Normal drift (H1), Föväntade händelser (H2), samt förebyggande av olyckor.	Reducera frekvensen för H2-händelser genom att öka anläggningens förmåga att hantera uppkomna fel inom normal drift.	Det ska vara möjligt att visa att alla drifterfarenheter har tagits tillvara för att identifiera eventuella säkerhetsproblem som kan vara relevanta för planerade nya reaktorer	Materialval och tillverkning anpassas för att minska frekvensen för fel.
				Bättre metoder för att identifiera åldringseffekter samt implementering av utvecklade åldringsprogram för att hantera åldring redan från utformning och konstruktion.
		Förebygga olyckor genom att förhindra att uppkomna H2-händelser inom anläggningen kan förvärras.		Stora inbyggda marginaler ska finnas för att minska frekvensen för H2-händelser.
			Det ska vara möjligt att bekräfta att tillräckliga åtgärder har vidtagits för att belysa sådana säkerhetsproblem.	Bättre identifiering av fel som kan leda till händelser inom och utanför anläggningen genom att beakta drifterfarenheter och PSA.
				Större fokus på MTO och förbättra gränssnittet mellan människa och teknik genom erfarenhetsåterföring och beaktandet av tester och på så vis undvika mänskligt felhandande.
			Marginaler vid alla driftförhållanden ska vara stärkta.	Anpassa utformning och konstruktion för att förbättra möjligheter att under drift

WENRA:s Säkerhetsmål	Område	Beskrivning		Vägledning	Exempel på åtgärder	
					inspektera, testa och övervaka åldring.	
					Öka kapaciteten hos driftsystem för att undvika onödig initiering av säkerhetssystem.	
					Förbättra operatörerna möjlighet att övervaka situationer genom att utveckla gränssnittet mellan människa och teknik.	
O2	Ej förväntade händelser (H3) och Osannolika händelser (H4)	Säkerställa att H3- och H4-händelser inte leder till otillåtna radiologiska konsekvenser för omgivningen, dvs sådana händelser ska ej leda till behov av jodprofylax, utökat skydd eller evakuering.		Härdskadefrekvensen ska vara lägre än 10-5/år.	Systematisk inventering av alla inledande händelser för alla driftlägen.	
				Det radiologiska utsläppet ska understiga nivåer som kräver intag av jodprofylax, utökat skydd och evakuering i enlighet med artikel 50.2 i direktiv 96/29/Euratom från den 13 maj 1996.	Systematisk inventering av alla inledande händelser som inte relaterar till reaktorhärd men som rör avfall, använt bränsle, etc.	
					Systematisk inventering av fel med gemensam orsak	
		Reducering så långt det är rimligt och möjligt av:	• härdskadefrekvensen med beaktandet av alla typer av händelser och fel samt kombinationer av alla händelser		Användande av PSA vid utfromning och konstruktion för att:	• kontrollera att härdskadefrekvensen har minskat
						• identifiera behov av ytterligare åtgärder/ modifieringar
						• identifiera behov av att diversifiera säkerhetssystem som komplement till redundans
			• utsläpp av radioaktivitet från alla typer av källor		Minska risken för mänskligt felhandande genom att:	• tillämpa automatisk eller passiva säkerhetssystem
						• säkerställa att tillräckligt rådrum finns
		För att minska konsekvenser av externa- och antagonistiska händelser bör det säkerställa att val av förläggningsplats samt reaktorns utformning och konstruktion har utvärderats i tillräcklig utsträckning				• förbättra gränssnittet mellan människa och teknik
					Minska risk för igensättning av filter genom val av material	
O3	Mycket osannolika händelser (H5)	Minska potentiella radioaktiva utsläpp till	• olyckor som förväntas leda till härdsmälta	För att kunna anse att en händelse har eliminerats krävs att det går att med hög	Med beaktande av möjliga felfoder för inneslutningen under	• minska belastningen på inneslutningen under svåra

WENRA:s Säkerhetsmål	Område	Beskrivning		Vägledning	Exempel på åtgärder	
		omgivningen i samband med härdsmälta i ett långtidsförlopp genom att tillämpa följande kriterier:	och ett tidigt omfattande utsläpp ska inte kunna inträffa.	tillförlitlighet visa att sannoliketen är extremt låg. Det är inte tillräckligt att tillämpa standardiserade probabilistiska gränsvärden. Även om sannolikheten är låg ska rimliga säkerhetsåtgärder implementeras för att minska sannolikheten ytterligare. Det ska även visas att tillräcklig kunskap finns avseende alla förhållanden som kan förväntas uppstå i samband med svåra olyckor (såsom ångexplosioner, vägasproblematik, etc). Därutöver ska osäkerheter relaterade till data och analysmetoder kvantifieras.	härdsmältascenarier bör följande genomföras:	haverier och eller öka inneslutningens motståndskraft till belastningar
			• vid olyckor som leder till härdsmälta och som inte kan förhindras ska det säkerställas att endast begränsade skyddsåtgärder krävs inom en rimlig tid för befolkning (ingen permanent evakuering av området, ingen evakuering utanför anläggningens närområde, begränsat utökat skydd, samt inga långtidsrestriktioner för kost och spannmål) samt att en rimlig tid att genomföra dessa finns.	På samma sätt som för O2 ska de nivåer som definieras av artikel 50.2 i direktiv 96/29/Euratom från den 13 maj 1996, beaktas och målet för utformningen och konstruktionen av reaktorn ska vara att minimera antalet skyddsåtgärder som krävs med beaktandet av plats och tid, samt att beakta alla osäkerhetser som		• förbättra tätheten hos inneslutningen under svåra haverier i långtidsförlopp
						• förhindra genomsmältning av inneslutningens bottenplatta
						• systematisk inventering och eliminering av potentiella förhållanden som kan leda till bypass av inneslutning
					Använda PSA för att verifiera att säkerhetsmålen har uppnåtts samt för att identifiera behov av förbättringar.	
					Använda förbättrade material:	• hos ånggeneratorer för att minska risken för tubbrott under härdsmältascenarier
						• hos reaktorns interndelar samt för konstruktioner under reaktortanken för att bättre kunna hantera härdsmältascenarier

WENRA:s Säkerhetsmål	Område	Beskrivning		Vägledning	Exempel på åtgärder	
				följer av tillämpade metoder.		
O4	Oberoende mellan alla nivåerna inom djupförsvaret.	Öka oberoendet mellan olika nivåer inom djupförsvaret genom att implementera diversifieringsprinciper (detta går utöver de krav på robusthet hos de enskilda nivåerna vilket tas upp i de föregående tre säkerhetsmålen) för att så lång det är rimligt och möjligt åstadkomma en förstärkning av djupförsvaret.			Inför dedikerade system för svåra haverier för att säkerställa oberoendet hos fjärde nivån inom djupförsvaret.	
O5	Gränssnitt mellan kärnkraftsäkerhet (safety) och fysiskt skydd (security)	Säkerställ att säkerhetsåtgärder och åtgärder avseende fysiskt skydd är utformade, konstruerade och implementerade med beaktade av båda aspekterna. Synergier mellan förstärkningar av säkerhet och fysiskt skydd ska främjas.			Anläggningens ska kunna hantera en flygplanskrasch med ett stort civilt flygplan	
O6	Strålskydd och avfallshantering	Reducera följande, så lång det är rimligt och möjligt och för alla driftlägen, genom utformning och konstruktion av anläggning, under rivning och avställning:	• individuell och kollektiv dos till personal	Avseende dosgränser för individer ska tillåtna värden understiga gällande gränsvärden som återges i direktiv 96/29/Euratom från den 13 maj 1996. Avseende kollektiva dosgränser gäller att varje tillståndhavare ska kunna motivera valda gränsvärden utifrån drifterfarenheter från befintliga anläggningar samt med beaktande av optimering.	Förbättra bränslets kapsling för att undvika utsläpp av fissionsprodukter	
			• radioaktivt och icke radioaktivt utsläpp till omgivning		Genom val av material och förbättrande av kemi kan produktion och uppbyggnad av radioaktiva nuklider minskas så att:	• onödig aktivering minskar • kontamination av anläggningsens system till följd av aktiverade korrosionsprodukter minskar • ytdekontaminationen av komponenter blir enklare att genomföra
			• radioaktivt och icke radioaktivt utsläpp till omgivning		Förbättra tillgängligheten hos system och komponenter som i dagsläget är eller förväntas bli de främsta orsakerna till personaldos.	

WENRA:s Säkerhetsmål	Område	Beskrivning		Vägledning	Exempel på åtgärder	
				Avseende utsläpp till omgivning har inga kvantitativa gränsvärden angivits, men varje tillståndhavare ska kunna motivera valda gränsvärden utifrån drifterfarenheter från befintliga anläggningar samt med beaktande av optimering.	Implementering av snabbmonterad och återanvändningsbara isolering	
					Minska antalet svetsar för att minska behovet av inspektioner i utrymmen med hög aktivitet samt minska uppbyggnad av aktivitet i systemen (i ojämnheter och krökar)	
					Optimera anläggningens layout med avseende på strålskyddsaspekter genom att:	• införa lämpliga strålskyddsbarriärer för utrymmen där personal förväntas dagligen vistas eller där personal förväntas vistas under en olycka
				Avseende kvantitet och aktivitet av radioaktivt avfall har inga kvantitativa gränsvärden angivits, men varje tillståndhavare ska kunna motivera valda gränsvärden utifrån drifterfarenheter från befintliga anläggningar samt med beaktande av optimering.		• beakta tillträdesbehov och tillträdesregler för personal
						• förbättra tillträdesmöjligheten till komponenter
					Mer systematisk tillämpning av fjärrstyrd utrustning för reperationer och inspektioner	
					Minska användandet av farliga ämnen	
					Minska produktion och uppbyggnad av radioaktiva nuklider genom val av material och förbättrad kemi	
					Tillämpa bästa möjliga teknik för att behandla, rena samt hantera vätskor och gaser	
					Ge möjlighet att invänta avklingning av kortlivade nuklider.	
					Filtrera och rena med lämplig metod för att minska utsläpp	
					Förbättra anläggningens layout för att:	• skapa tillräckligt utrymme för att förvara och hantera radioaktivt avfall
						• skapa tillräckligt utrymme för att bevaka användandet och förvaring av radioaktivt material
						• underlätta dekontamination av

WENRA:s Säkerhetsmål	Område	Beskrivning		Vägledning	Exempel på åtgärder	
						komponenter
					Verifiera under konstruktions- och utformningsfasen att det finns möjlighet att slutförvara den förväntade mängden radioaktivt avfall	
O7	Ledarskap och styrning av säkerhetsarbete	Säkerställa effektivt ledning och styrning från konstruktions- och utformningsstadiet. Detta medför att tillståndshavare ska:	• etablera ett effektivt ledarskap och en effektiv styrning under hela nybyggnationsprojektet samt att tillräcklig teknisk och finansiell kunskap och kompetens finns för att kunna ta ett säkerhetsansvar.			
			• säkerställa att personal inom alla organisationer som involveras i arbetet som rör förläggningsplatsen (markarbeten, etc), konstruktion och utformning, uppförande, drifttagning, drift, rivning för nya reaktorer innehar tillräcklig			

WENRA:s Säkerhetsmål	Område	Beskrivning		Vägledning	Exempel på åtgärder
			kännedom om de kärnsäkerhetsaspekter som rör deras arbete och deras roll, för att tillförsäkra en hög säkerhet.		

Tabell 1 – WENRA:s säkerhetsmål samt vägledning vid implementering och exempel på åtgärder

4.1.2.2.1 WENRA:s förtydliganden från 2012

I WENRA:s utkast till rapport från 2012 [38], har WENRA valt att ge ytterligare förtydliganden i sju punkter avseende djupförsvarets utformande, hantering av fel med gemensam orsak (multipla fel), hantering av svåra haverier, eliminering av olyckor som kan leda till stora tidiga utsläpp, hantering av yttre händelser[4] och flygplanskrascher. Av dessa förtydliganden framgår:

1. Avseende djupförsvarets utformande konstateras att samtliga nivåer enlig tabellen nedan ska beaktas.

[4] Ytter händelser avser händelser som kan uppkomma utanför anläggningen och kan påverka anläggningens säkerhet. Yttre händelser innefattar bland annat naturfenomen, kemiska och bilogiska utsläpp i närregion, explosioner i närregion, flygplanskrascher samt händelser på det yttre elkraftnätet.

Djupförsvarets nivåer	Syfte	Omfattning	Radiologiska konsekvenser
Nivå 1	Motverka förväntade händelser och fel	Konservativa antaganden och kvalitet inom utformning, konstruktion och drift, samt stor tillförlitlighet hos övervakning och kontroll av de viktigaste parametrarna för att säkerställa att de hålls inom definierade driftgränser.	Myndighetsens accepterade utsläppsgränser vid normal drift
Nivå 2	Hantera förväntade händelser och fel	Funktioner och system för att hantera och begränsa händelser och fel	
Nivå 3 3a	Hantera ej förväntade och osannolika händelser för att minimera potentiella utsläpp och förhindra härdsmälta	Reaktorskyddssystemet, säkerhetssystem och störningsinstruktioner	Inga eller begränsade radiologiska konsekvenser för omgivning
Nivå 3 3b		Övriga skyddsfunktioner och störningsinstruktioner	
Nivå 4	Hantera mycket osannolika händelser för att minimera utsläpp till omgivning	Kompletterande säkerhetsfunktioner och strategi för att hantera härdsmältascenarier	Behov av begränsade manuella åtgärder inom en rimlig tid och från en rimlig plats
Nivå 5	Motåtgärder för att hantera radiologiska konsekvenser till följd av betydande utsläpp av radioaktivt material	Haveriberedskap utanför anläggning Gränsvärden	Radiologiska omgivningskonsekvenser och nödvändiga motåtgärder

Tabell 2 – Djupförsvarets olika nivåer enligt WENRA

2. Avseende oberoende mellan djupförsvarets olika nivåer konstateras att det bör eftersträvas ett oberoende mellan nivå 2, 3 och 4 samt att 3a och 3b ska så långt det är rimligt och möjligt vara oberoende.

   Ett oberoende mellan de haveribegränsande funktionerna och övriga säkerhetsfunktioner som tillämpas inom de övriga djupförsvarsnivåerna ska eftersträvas. Oberoendet ska demonstreras via lämplig kombination av deterministiska och probabilistiska analyser samt ingenjörsmässiga bedömningar.

   För varje postulerad inledande händelser ska samtliga systemet och funktioner som behövs för att hantera situationen identifieras och det ska visas via säkerhetsanalys att krediterade funktioner och system inom varje nivå av djupförsvaret är tillräckligt oberoende från övriga nivåer inom djupförsvaret.

   Alla system och funktioner som krediteras ska uppfylla samtliga krav som gäller för respektive nivå av djupförsvaret som de tillhör.

   Tillräcklig uppmärksamhet ska riktas mot utformning och konstruktion av instrumentering och kontrollutrustning samt säkerhetsfunktionernas stödfunktioner, och oberoendet ska beaktas.

   Ytterligare förtydliganden ges i bilaga 2 till [38].

3. Avseende hantering av fel med gemensam orsak (multipla fel) ska följande situationer beaktas inom utformning och konstruktion:

- Ett postulerat fel med gemensam orsak eller degradering av samtliga stråk inom ett säkerhetssystem, vilket medför att en krävd säkerhetsfunktion inte kan utföra sin funktion för att motverka eller hantera en förväntad händelse eller en postulerad inledande händelse.
- Ett postulerat fel med gemensam orsak inom ett säkerhetssystem eller ett säkerhetsrelaterat system, vilket behövs för att säkerställa funktionen hos de fundamentala säkerhetsfunktionerna vid normal drift.

Utöver detta ska alla rimliga och möjliga åtgärder vidtas för att förhindra uppkomst av fel med gemensam orsak, såsom exempelvis åtgärder som avser att stärka fysisk separation mellan redundanta delar inom säkerhetssystem, säkerhetsrelaterade system och dess tillhörande stödfunktioner.

För djupförsvarsnivån 3b gäller till skillnad från 3a, att vissa anpassningar kan göras och probabilistiska antaganden samt att realistiska metoder och metodik kan i viss mån tillämpas.

Ytterligare förtydliganden ges i Appendix 3 till [38].

4. Avseende hantering av svåra haverier konstateras att inneslutningens funktion är en av de mest centrala funktionerna och därmed ska väsentliga skyddsfunktioner såsom filtrerad ventilering, vätgashantering och tryckbegränsande funktioner implementeras. Därutöver ska angivna värden i tabellen nedan gälla.

Åtgärder	**Evakueringszon (< 3 km)**	**Skyddszon (< 20 km)**	**Övrigt**
Permanent utflyttning	Nej	Nej	Nej
Evakuering	Ja	Nej	Nej
Utökat skydd	Ja	Ja	Nej
Jodprofylax	Ja	Ja	Nej
Restriktioner för jordbruk	Ja (> 1 år)	Ja (> 1 år)	Nej
Restriktioner för natur och miljö	Ja (> 1 år)	Ja (> 1 år)	Ja (> 1 år)

Tabell 3 – Omgivningspåverkan till följd av svåra haverier enligt WENRA

Begreppen evakueringszon och skyddszon saknar direkt motsvariget inom den svenska beredskapsstrategin där man i stället talar om den inre beredskapszonen och zon för strålningsmätning. Den förstnämnds av dessa kan närmast ses som en kombination av evakueringszon och skyddszon.

5. Avseende eliminering av olyckor som kan leda till stora tidiga utsläpp konstateras att för att det ska vara möjligt att anta att en händelse eller situation inte kan inträffa så måste följande beaktas:

   – Det ska vara fysiskt omöjligt att en sådan händelse eller situation inträffar.

   – Sådana olyckor ska visas med hög tillförlitlighet vara mycket osannolika (i enlighet med IAEA SSR-2.1). Det är dock inte tillräckligt att tillämpa standardiserade probabilistiska gränsvärden.

   För att identifiera potentiella händelser och situationer som kan leda till stora tidiga utsläpp ska deterministiska och probabilistiska metoder och/eller ingenjörsmässiga bedömningar tillämpas. Speciell uppmärksamhet ska riktas mot situationer och händelser som beaktas inom de lägre djupförvarsnivåerna och som skulle kunna eskalera och leda till olyckor.

   Situationer och händelser enligt figuren nedan ska beaktas.

Figur 7 – Översiktlig bild av situationer och händelser som ska beaktas inom anläggningens säkerhetsdemonstration

6. Avseende hantering av yttre händelser[5] ska säkerhetsanalyser visa att hot från yttre händelser antingen har eliminerats eller minimerats så långt det är rimligt och möjligt. Detta göras genom att visa att säkerhetsystem och

[5] Ytter händelser avser händelser som kan uppkomma utanför anläggningen och kan påverka anläggningens säkerhet. Yttre händelser innefattar bland annat naturfenomen, kemiska och bilogiska utsläpp i närregion, explosioner i närregion, flygplanskrascher samt händelser på det yttre elkraftnätet. I detta fall avses även antagonistiska händelser. Karaktäriserande för denna typ av händelse är att anläggningen oftast här mycket liten möjlighet att påverka den inledande händelsen.

säkerhetsfunktioner är kvalificerade för att klara situationer som kan uppkomma i samband med yttre händelser. Likaså ska val av förläggningsplats och anläggningens layout väljas utifrån beaktandet av yttre händelser, speciellt för anläggningar med flera reaktorer.

Yttre händelser som kan förväntas inträffa samt ej förväntade händelser och osannolika händelser ska inte leda till tidiga och/eller stora utsläpp. Därutöver ska mycket osannolika händelser beaktas och analyseras.

Samtliga möjliga yttre händelser som kan förväntas påverka anläggningens säkerhet och ska beaktas. Likaså ska potentiella kombinationer av yttre händelser beaktas samt eventuella tröskeleffekter.

7. Avseende flygplanskrascher konstateras att en sådan händelse inte ska kunna leda till härdsmälta och endast orsaka begränsade utsläpp i enlighet med säkerhetsmål O2. Alla strukturer, funktioner och system som behövs för att ta reaktorn till ett säkert läge ska utformas och konstrueras för att klara förhållanden som kan uppstå till följd av denna händelse. Utöver detta ska direkta och indirekta effekter och följdfel beaktas. Byggnader som innehåller kärnbränsle ska utformas och konstrueras så att de klara en flygplanskrasch.

4.1.2.2.2 Jämförelse mellan WENRA:s säkerhetsmål och de svenska kraven

Vid jämförelse mellan WENRA:s säkerhetsmål och det svenska regelverket konstateras att stora delar av säkerhetsmålen uttrycks i de svenska kraven. Säkerhetsmålen går dock något längre avseende precisering. Ett antal skillnader noteras vid jämförelsen:

1. WENRA föreslår ett värde för en härdskadefrekvens som är satt till 10^{-5}/år inom vägledningen till säkerhetsmålen. SSM har idag inte något kriterium för acceptabel härdskadefrekvens, vilket är ett medvetet val. SSM:s inställning är att ett sådant kriterium inte heller i framtiden ska vara del av föreskrifterna. Dock finns ett svenskt kriterium för utsläppsfrekvens som regeringen använder för att precisera den tillförlitlighet som de svenska haverifiltren ska ha.
2. WENRA:s säkerhetsmål tar upp krav på förläggningsplats. I det svenska regelverket är kraven på förläggningsplatsen inte lika utförliga och definieras till störst del av miljöbalken vilken har ett annat fokus än det som ges i säkerhetsmålen. Med beaktande av olyckan i Fukushima Dai-ichi som demonstrerade vikten av val av förläggningsplatsens, framstår det som om det vid nybyggnation av kärnkraftverk är rimligt att utveckla kraven avseende förläggningsplatsens utformande och det bedöms även rimligt att man för befintliga kärnkraftverk ser över relevant svensk krav med avsikt att skapa en harmonisering med internationell standard och identifiera behov av ytterligare säkerhetsförbättringar.
3. Flera av WENRA:s säkerhetsmål tar upp krav gällande anläggningens layout. Motsvarande krav återfinns inte tydligt i de svenska kraven men bedöms vara väsentligt vid om- och nybyggnation för att minska personaldoser, möjliggöra framtida säkerhetsförbättringar och skapa förutsättningar för utförligare

inspektioner och provning samt möjliggöra ett effektivare underhåll. Vid modifieringar av befintliga anläggningar bedöms denna aspekt vara relevant och det framstår som rimligt att föreslå att en översyn av kraven på anläggningslayout sker för att tydligare harmonisera denna med internationell standard.

4. Kraven på oberoende inom djupförsvaret som återges i WENRA:s säkerhetsmål utrycks i de svenska kraven men inte lika specificerat. I avsnitt 4.1.3 till detta PM behandlas precisering inom regelverk vidare.
5. WENRA:s säkerhetsmål avseende gränssnittet mellan kärnsäkerhet och fysiskt skydd är inte lika tydligt i de svenska kraven. I takt med att modern mjukvarubaserad utrustning implementeras i befintliga anläggningar aktualiseras behovet av en utvecklad strategi och hantering av detta område och det bedöms som rimligt att föreslå att en översyn av kraven för detta område sker.
6. Vägledningen för WENRA:s säkerhetsmål anger att man bör arbeta för att öka marginaler. De svenska föreskrifterna anger att man kontinuerlit ska utveckla säkerheten och implementera säkerhetsförbättringar. Detta bedöms medföra att intentionen med vägledningen till säkerhetsmålet är uppfylld inom de svenska kraven även om man inte utryckligen refererar till marginaler.
7. Vägledningen till WENRA:s säkerhetsmål tar upp hantering av åldringseffekter. Detta område behandlas begränsat i de svenska kraven men kommer att förstärkas till följd av bland annat de utredningar som gjorts inom ramen för delprojekt 2 i regeringsupdraget som denna rapport är en del av (se vidare avsnitt 1).
8. Vägledningen och framförallt förtydligandet av WENRA:s säkerhetsmål tar upp begreppen evakueringszon och skyddszon. Dessa begrepp saknar direkta motsvarigheter i den svenska beredskapsstrategin där man endast talar om inre beredspakszon och zon för strålningsmätning. Den inre beredskapszonen motsvarar närmast en kombination av de två begreppen, evakueringszon och skyddszon. Det framstår som rimligt att man från svensk sida ser över eventuella behovet av att uppdatera strategin för beredskap utifrån säkerhetsmålen och utreder betydelse och säkerhetsnytt med den föreslagna zonindelningen.
9. WENRA:s säkerhetsmål tar upp yttre händelser[6] och specifikt flygplanskrascher av stora flygplan ur både ett olycks- och ett fysiskt skyddsperspektiv. I de svenska kraven skiljer man tydligt på antagonistiska händelser samt olyckor och naturfenomen vilket

[6] Ytter händelser avser händelser som kan uppkomma utanför anläggningen och kan påverka anläggningens säkerhet. Yttre händelser innefattar bland annat naturfenomen, kemiska och bilogiska utsläpp i närregion, explosioner i närregion, flygplanskrascher samt händelser på det yttre elkraftnätet.

medför att vissa skillnader mellan de svenska kraven och säkerhetsmålen kan identifieras. Denna skillnad bedöms dock inte medföra några väsentliga skillnader i praktiken och det framstår därmed inte heller som om det finns behov av uppdateringar av de svenska kraven till följd av dessa skillnader.

De skillnader som identifierats mellan det svenska regelverket och WENRA:s säkerhetsmål med tillhörande vägledningen och förtydliganden, beror till mångt och mycket på att de svenska kraven inte är lika preciserade. En utförligare diskussion avseende preciserad kravbild återges i efterföljande avsnitt, avsnitt 4.1.3 till detta PM.

4.1.3 Diskussion avseende precisering av krav

Vid jämförelser mellan svenska krav och internationella krav samt säkerhetsstandarder[7] avseende konstruktion och utformning konstateras att strukturen hos de svenska kärnkraftsäkerhetskraven, vilka består av en övergripande lag och förordning, målinriktade myndighetsföreskrifter samt mer detaljerade allmänna råd om tillämpning av föreskrifterna, återfinns likande struktur i flera länder och bedöms av denna utredning vara en ändamålsenlig struktur. Dock framkommer vid jämförelsen tydligt att de svenska kravens utformning med avseende på detaljeringsnivå är förhållandevis unik. I följande avsnitt avser att diskuter skillnaderna i detaljeringsnivån hos krav och råd om tillämpning för att kunna dra slutsatser om eventuella behov av ändringar hos den svenska kravbilen.

Syftet med en mer detaljerad kravbild är att öka tydlighet, förutsägbarhet och därmed rättstrygghet genom att minska tolkningsutrymmet och därmed underlätta tillsynen samt tillståndshavarnas uppfyllnad av kraven. De stora nackdelarna med en alltför detaljerad kravbild är å andra sidan att det kan skapa en viss passivitet och ett tunnelseende hos berörda samt minska möjligheterna att i varje enskilt fall åstadkomma en bästa möjliga lösning. Det gäller således att få fram en lämplig nivå som eliminerar brister och problem i dagens regelverk och samtidigt inte skapar nya problem.

Vid jämförelsen av kraven gällande utformning och konstruktion för kärnkraftverk framkom att de mål för säkerheten som definieras i de svenska kraven motsvarar väl de krav som återfinns i övriga studerade länders regelver samt IAEA:s säkerhetsstandarder och WENRA:s referensnivåer och säkerhetsmål. Den stora skillnaden är dock att samtliga studerade internationella krav och standarder förtydligar målen och definierar mer preciserade krav relaterade till dessa mål. I vissa länder och inom IAEA:s säkerhetsstandarder samt WENRA:s säkerhetsmål ges även ytterligare förtydliganden via råd om tillämpning.

Utredningen finner att en utökad precisering till en lämplig detaljnivå ofta ger bättre stöd vid tillsyn då det minskar utrymmet för individuell tolknings i enskilda fall. Det bedöms även underlätta tillståndshavarnas arbete med att

[7] Internationella säkerhetsstandarder omfattar här IAEA:s säkerhetsstandarder samt WENRAS:s referensnivåer och säkerhetsmål.

säkerställa att deras verksamhet uppfyller kraven. Utredningen noterar att erfarenheter från myndighetens tillsyn indikerar att tolkningsutrymmet inom den svenska kravbilden avseende konstruktion och utformning har skapat stora skillnader avseende kravens tillämpning och tolkning hos berörda tillståndshavare samt även delvis skapat olika tolkningar inom den egna myndigheten. Dessa tolkningsskillnader bedöms kunna resultera i en kontraproduktiv påverkan på säkerhetsarbetet eftersom det kräver större resurser både hos tillståndshavarna som genomförare och hos myndigheten som granskare, då individuella tolkningen ska tas fram och granskas separat för varje enskilt fall.

Precisering till ”lämplig detaljnivå” kan framstå som en något diffus beskrivning. Det är även svårt att bedöma på vilken hierarkisk nivå som är lämplig för denna precisering. Vid studier av olika länders kravbild finner man dock att i exempelvis USA som är ett land där kraven är exceptionellt detaljerade, har vissa juridiska problem kunnat uppstå när det gäller uppdateringar eller revideringar av kraven för befintliga reaktorer. I USA:s fall har detta medfört att kravbilen inte genomgått någon fullständig revidering sedan det ursprungliga utfärdandet och kan därför uppfattas som något föråldrad. Som resultat av detta har den amerikanska myndigheten valt att arbeta förhållandevis intensivt med utvecklingen av råd om tillämpning och det är i dessa råd om tillämpning som man kan finna moderna säkerhetskrav och som nutidens kunskaper och erfarenheter har påvisat behovet av. Det är emellertid en väsentlig skillnad att dessa moderna säkerhetskrav återges som råd om tillämpning och inte som rena krav eftersom de då inte blir tvingande.

I Finland där detaljeringsnivån hos kraven i likhet med USA är hög har myndighen skapat en generell kommentar till de krav som återges i de så kallade Kärnkraftverksdirektiven. Denna allmänna kommentar anger att den som vill avvika från de krav som ställs i kärnkraftverksdirektiven måste kunna presentera ett alternativt och godtagbart förfaringssätt eller lösning med vilken samma säkerhetsnivå som krävs i respektive kärnkraftverksdirektiv uppnås. Kommentaren medför att det inom de finska myndighetsdirektiven ges större utrymme för anpassningar än vad som går att finna i motsvarande svenska föreskrifter samt att kärnkraftverksdirektiven i vissa sammanhang har liknats vid råd om tillämpning.

Vid studier av Kanadas kravbild, IAEA:s upplägg för säkerhetsstandarderna samt WENRA:s säkerhetsmål och referensnivåer, finner man att kraven är målinriktade och, i jämförelse med Sverige, kan man säga att detaljeringsnivå för dessa är medel. Medel i detta sammanhang innebär att kraven är något mer detaljerade än de svenska föreskrifterna men samtidigt uppfattas de inte som för snäva. Dock har både Kanada och IAEA valt att ta fram välutvecklade råd om tillämpning vars detaljeringsnivå är betydligt mer utförlig än de svenska råden om tillämpning och återges i separata dokument.

Det sista landet som studerats är Storbritannien. För Storbritannien saknas definierade krav men om man studerar myndighetens råd om tillämpning så finner man att dessa har en detaljeringsnivå som kan jämföras med den man finner i Kanada eller inom IAEA:s säkerhetsstandarder.

Utifrån ovan konstateras att det framstår som om de målinriktade krav som finns inom det svenska regelverket är ändamålsenliga och väl motsvarar internationella krav och säkerhetsstandarder[8]. En viss ökning av detaljeringsnivå hos de svenska kraven bedöms dock kunna ge en tydligare kravbild mer i harmoni med internationella krav och standarder, samt underlätta tillsynen samt tillståndshavarnas uppfyllnad av kraven. Med beaktande av USA och Finland framstår det som om man bör vara noggrann med att inte skapa för detaljerade krav utan snarare hålla sig på en detaljeringsnivå som motsvarar Kanadas, Storbritanniens och IAEA:s. Som ett exempel på där den detaljerade kravnivån bedöms som mer änamålsenlig, kan krav gällande fel med gemensam orsak nämnas (se vidare Bilaga 1 sid 135 ”*Krav avseende motverkandet av uppkomst av fel med gemensam orsak*”). I detta fall har det mycket övergripande svenska kravet genererat stora tolkningsskillnader mellan myndighet och tillståndshavare samt även tillståndshavare emellan, vilket har försvårat tillsyn och tillämpning av kravet. Ett annat exempel där en ökad precisering bedöms kunna ge ett tydligare krav gäller tålighet mot naturfenomen och andra händelser som uppkomma inom och utanför anläggningen (se Bilaga 1 sid 147 ”*Krav avseende tålighet mot händelser och förhållanden som kan uppkomma utanför eller inne i kärnkraftsanläggningen och som kan leda till en radiologisk olycka (inklusive rörbrott)*”. I detta fall framgår det inte tydligt av det svenska kravet att exempelvis tröskeleffekter och kombinationer av händelser ska beaktas. Något som tydligare framgår av övriga länders krav.

Den stora skillnaden mellan det svenska regelverket och de studerade ländernas och organisationernas regelverk är att samtliga till skillnad från Sverige, har väl utvecklade råd om tillämpning. De svenska råden för konstruktion och utformning är mycket varierade i omfattning och karaktär samt ofta förhållandevis kortfattade. Vid jämförelse framstår det som om tydligare och mer utvecklade råd om tillämning är något som saknas i det svenska regelverket. Detta eftersom välutvecklade råd om tillämpning bedöms kunna skapa en mer ändamålsenlig kravbild genom att ge upphov till enhetliga tolkningar av kraven, underlätta implementering samt ge en effektivare granskning.

De flesta länder och IAEA har strukturmässigt även valt att hålla råd om tillämning i separata dokument för att på ett enklare sätt kunna uppdatera dem i enlighet med senaste kunskaper och erfarenheter. Inom området konstruktion och utförande framstår det vid jämförelsen som om denna struktur är tydligare och enklare att hantera. Befintliga svenska allmänna råd om tillämpning är mycket varierande i omfattning och karaktär och då de strukturmässigt är placerade i föreskriftsamlingarna kan de uppfattas som svårare att uppdatera och därmed mindre utvecklingsbara. Därutöver framstår det som om denna uppdelning skulle kunna ge möjligheter att beroende på område skapa bästa möjliga utformning för råden om tillämpning. Det bör dock uppmärksammas att en sådan uppdelning inte följer svenska föreskriftstruktur.

---

[8] Internationella säkerhetsstandarder omfattar här IAEA:s säkerhetsstandarder samt WENRAS:s referensnivåer och säkerhetsmål.

4.2 Etapp 2

4.2.1 Jämförelse mellan säkerhetsförbättringar av kärnkraftsreaktorer i Sverige och internationellt

Detta avsnitt avser att behandla de säkerhetsförbättringar som genomförts i Finland, Frankrike, Schweiz och Tyskland bland annat till följd av krav från myndigheterna för att möjliggöra längre drifttider och jämföra dessa med de säkerhetsförbättringar som krävts av de svenska tillståndshavarna i form av regeringsbeslut samt av myndighetskrav och beslut. Analysen utgår i första hand från den kartläggning som genomförts av externt stöd (myndighetsstöd) 2011 [1] men har i vissa fall hämtat information direkt ifrån respektive lands nationalrapport, [32], [33], [34] och [35].

4.2.1.1 Sverige

Omfattande säkerhetsförbättringar har genomförts i samtliga svenska kärnkraftverk. Säkerhetsförbättringarna har initierats via regeringsbeslut eller till följd av nya föreskrifter och grundar sig på ny kunskap erhållen via drift- eller andra erfarenhet, analys, forskning och utveckling, samt utveckling av IAEA:s säkerhetsstandarder och industristandarder.

En grundlig genomgång av de svenska säkerhetsförbättringarna ges i etapp 3 till denna utredning. Av denna framgår att säkerhetsförbättringarna i svenska anläggningar bland annat har innefattat säkerhetsförbättringar avseende:

- fysisk och funktionell separation inom anläggningar,
- diversifiering av säkerhetsfunktioner,
- olycks- och haverihantering,
- skydd mot dynamiska och lokala effekter till följd av rörbrott
- skydd vid naturfenomen och andra händelser som kan inträffa inne i eller utanför anläggningen,
- drift,
- underhåll samt
- miljötålighet och miljöpåverkan.

4.2.1.2 Finland

Omfattande säkerhetsförbättringar har genomförts i de finska kärnkraftsreaktorerna, särskilt i samband med effekthöjningarna.

I nedanstående tabell redovisas de säkerhetsförbättringar som har identifierats och till stora delar har implementerats i de finska kärnkraftverken.

Anläggning	**Säkerhetsförbättringar avseende följande områden**	**Beskrivning**
Loviisa	Primärsystemets integritet	Ersättning av bränsleknippen i härdens periferi med motsvarande dummy i rostfritt stål för minimering av neutronbestrålningen och försprödningen av reaktortanken
		Värmebehandling av en av reaktortankens svetsar
	Brandskydd	Installation av vätgasantändare i inneslutningen. Senare även ändring av systemet med vätgasantändare samt installation av

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning
		vätgasrekombinatorer
		Installation av ytterligare ett hjälpmatarvattensystem för att hantera händelsen av samtidigt bortfall av matarvattensystemet och ordinarie hjälpmatarvattensystemet i samband med brand i turbinhall
		Uppförande av en separat byggnad för ett diversifierat resteffektkylningssystem
		Införande av ett sprinklersystem för huvudtransformatorn (för skydd av den angränsande turbinhallen)
		Uppgradering av brandskyddssystemen inklusive uppförande av en ny brandpumpstation innehållande dieselsäkrade brandpumpar och separat brandvattentankar
	Oberoende	Införande av ett oberoende sprinklersystem för reaktorinneslutningen
	Skydd vid LOCA	Ökning av ytan för sumparnas silar i inneslutningen
		Införande av ny mätutrustning för primärläckage
	Övervakning	Ändring av instrumenterings och kontrollutrustningens logik gällande skador i ånggeneratorer
	Manuell tryckavlastning av primärsystemet	Införande av ventiler för manuell tryckavlastning av primärsystemet (genomfört i samband med byte av tryckhållarens säkerhetsventiler)
	Hantering av svåra haverier	Ändringar baserade på experiment som avser att förbättra möjligheterna att upprätthålla reaktortankens integritet samt skapa kylning av en härdsmälta via extern kylning av reaktortank
		Införande av ny instrumentering och kontrollutrustning för hantering av svåra haverier
		Införande av nya dedikerat elektriskt system
		Byggande av ett separerat kontrollrum gemensamt för Loviisa 1 & 2, för hantering av svåra olyckor
	Åldring	Effekthöjning till 1500 MWth (inkluderar moderniseringsåtgärder för att förlänga drifttiden till 50 år, vilket motsvarar 20 år utöver den ursprungliga drifttiden).
	Reservövervakningsplats	Ny reservövervakningsplats (planeras)
	Instrumentering och kontrollutrustning	Ny instrumentering och kontrollutrusning (2014)
	Simulator	Byggande av en simulator för utbildning av kontrollrumspersonalen (planeras)
Olkiluoto	Hantering av svåra haverier	Installation av filtrerad tryckavlastning av inneslutning
		Möjlighet att flöda nedre drywell från kondensationsbassängen för att skydda inneslutningens bottenplatta och genomföringar i samband med härdsmälta
		Införande av skydd för vissa genomföringar i inneslutningens nedre drywell
		Införande av ett system för vattenfyllnad av inneslutningen

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning
		Installation av instrumentering och kontrollutrustning för svåra haverier
		Införande av instruktioner för svåra haverier
	Brandskydd	Införande av ett sprinklersystem för transformatorerna
		Förbättring av brandskyddet för säkerhetsrelaterade elkablar
	Bränslets utformning	Övergång från 8x8 bränsle till 10x10 bränsle (det senare har 40% lägre linjär värmebelastning)
	Skydd vid inre och yttre händelser	Förbättrat jordbävningsskydd
		Förbättrat skydd mot isbildning i huvudkylvattenintagen
		Förbättrat skydd mot snöstorm för dieselgeneratorernas luftintag
	Turbinövervakning	Nytt datorbaserat instrumenterings och kontrollutrusningssystem för turbinen
	Diversifiering	Analysera möjligheter att installera ett nytt resteffektkylsystem oberoende av havsvatten
		Diversifiering av reaktorns tryckavlastningssystem genom installation av två tillkommande avlastningsventiler
		Diversifiering av nivåmätning i reaktortanken (planeras)
		Förbättrat skydd mot felfunktion på syrstavar genom bl .a. automatisering av borsystemet, samt ökning av borsystemets kapacitet
	Reservövervakningsplats	Ny reservövervakningsplats (planeras)
	Instrumentering och kontrollutrustning	Ny instrumentering och kontrollutrusning (planeras)
	Robusthet	Utökat skydd vid obefogad öppning av turbinens by-pass ventiler
		Ökning av resteffektkylsystemets kapacitet

Tabell 4- Säkerhetsförbättringar i finska kärnkraftverk

4.2.1.3 Frankrike

Säkerhetsförbättringar har införts i de franska kärnkraftsreaktorerna i samband med återkommande säkerhetsutvärdering (PSR).

I nedanstående tabell redovisas de säkerhetsförbättringar som har identifierats och till stora delar har implementerats i de franska kärnkraftverken.

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning
900 MWe reaktorerna	Svåra haverier	Förbättrad hantering av risker kopplade till explosiva gaser (detektering av vätgas, miljötålig utrustning)
		Förbättrat skydd vid svåra haverier (t.ex. övervakning av härdsmälta vid genomsmältning av reaktortanken)
	Recirkulationsmöjligheter	Ändringar hos inneslutningssumparna (refererar till den s.k. silhändelsen i Barsebäck, år 1992)
	Primärsystemets integritet	Förbättrad hantering av höga tryck i reaktortanken vid kallt tillstånd och överfyllnad av ånggeneratorerna
	Brott på primärsystemet (LOCA)	Utökad tillförlitlighet av recirkulation vid brott på primärsystemet
	Inneslutningens integritet	Utökad täthet av reaktorinneslutningen
	Brandskydd	Utökande av det förebyggande och avhjälpande brandskyddet
	Inre och yttre händelser	Förstärkning av anläggningarnas skydd vid svåra väderförhållanden (projektiler i samband med kraftig vind, bortfall av värmesänka, extrema temperaturer, översvämning).
		Förnyad bedömning av risken för yttre översvämning med mer konservativa antaganden samt införande av förbättringsåtgärder för att öka skyddet mot yttre översvämning (inkluderar fysiska åtgärder såsom isolering/tätning av byggnadsdelar under marknivå samt administrativa åtgärder såsom etablering av lokal/nationell räddningsorganisation)
		Analys av potentiella generiska åtgärder avseende reaktorernas ventilationssystem, sekundär värmesänka, huvudgenerator, turbinkondensor och tillåtna termiska utsläpp från verken för att öka skyddet av anläggningarna vid extremt höga lufttemperaturer
		Förbättrat tålighet hos vissa komponenter och strukturer för att minimera effekter av jordbävning
	Bränslebassängernas integritet	Förbättrat skydd mot snabb dränering av bränslebassängerna
	Fysisk separation	Utökad fysisk separation inom säkerhetsrelaterade byggnader
	Långtidsförlopp	Ändringar av pumpar tillhörande högtrycksinsprutningssystemet (SI) och i sprinklersystemet för reaktorinneslutningen för att förbättra deras uttålighet med avseende på vibrationer

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning
	Strålskydd	Förbättrande av strålskyddet genom att införa exempelvis avtagbar isolering, biologiskt skydd, rening av primärsystemet före avställningar
	Instrumentering och kontrollutrustning	Modernisering av reaktorskyddssystemet
		Modernisering av instrumentering och kontrollutrustning för turbin
	Härdens kylbarhet	Förbättrad kapacitet hos högtrycksinsprutningssystemet (SI)
1300 MWe reaktorerna	Härdens kylbarhet	Förbättrad beräkning och monitering av vattennivån i reaktortanken i samband med händelser och olyckor
	Manövrering av säkerhetssystem	Förbättrad möjlighet att från det centrala kontrollrummet manuellt manövrera pumparna i högtrycksinsprutningssystemet (SI) och i sprinklersystemet för reaktorinneslutningen, när deras elmatning sker via dieselgeneratorerna
	Recirkulationsmöjligheter	Ändringar hos inneslutningssumparna (refererar till den s.k. silhändelsen i Barsebäck, år 1992)
	Primärsystemets integritet	Förbättrad möjlighet att vid beroende fel i primärpumparnas elmatning förse huvudcirkulationspumparnas (RCP) tätningar med vatten
	Långtidsförlopp	Ändringar av pumpar tillhörande högtrycksinsprutningssystemet (SI) och i sprinklersystemet för reaktorinneslutningen för att förbättra deras uttålighet med avseende på vibrationer
	Fysisk separation	Utökad fysisk separation inom säkerhetsrelaterade byggnader
	Inre och yttre händelser	Analys av potentiella generiska åtgärder avseende reaktorernas ventilationssystem, sekundär värmesänka, huvudgenerator, turbinkondensor och tillåtna termiska utsläpp från verken för att öka skyddet av anläggningarna vid extremt höga lufttemperaturer
		Förnyad bedömning av risken för yttre översvämning med mer konservativa antaganden samt införande av förbättringsåtgärder för att öka skyddet mot yttre översvämning (inkluderar fysiska åtgärder såsom isolering/tätning av byggnadsdelar under marknivå samt administrativa åtgärder såsom etablering av lokal/nationell räddningsorganisation)
	Instrumentering och kontrollutrustning	Ändringar i instrumentering- och kontrollutrustning för dränageledningen i kemi- och volymkontrollsystemet (CVCS)

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning
	Skydd vid brott på primärsystemet	Ändringar i logiken för instrumentering och kontrollutrustningsystemet för hjälpmatarvattensystemet i händelse av tubbrott i en ånggenerator.
1300 MWe reaktorerna	Svåra haverier	Miljötålighet och miljökvalificering av vissa komponenter
	Inre och yttre händelser	Förbättrad tillförlitlighet av startfunktionen för huvudcirkulationspumparna vid inre och yttre händelser
		Förnyad bedömning av risken för yttre översvämning med mer konservativa antaganden samt införande av förbättringsåtgärder för att öka skyddet mot yttre översvämning (inkluderar fysiska åtgärder såsom isolering/tätning av byggnadsdelar under marknivå samt administrativa åtgärder såsom etablering av lokal/nationell räddningsorganisation)
		Analys av potentiella generiska åtgärder avseende reaktorernas ventilationssystem, sekundär värmesänka, huvudgenerator, turbinkondensor och tillåtna termiska utsläpp från verken för att öka skyddet av anläggningarna vid extremt höga lufttemperaturer
		Kvalificering av kylsystemet för styrstavarnas styrsystem med avseende på jordbävning
	Långtidsförlopp	Ändringar av pumpar tillhörande högtrycksinsprutningssystemet (SI) och i sprinklersystemet för reaktorinneslutningen för att förbättra deras uttålighet med avseende på vibrationer
	Recirkulationsmöjligheter	Ändringar hos inneslutningssumparna (refererar till den s.k. silhändelsen i Barsebäck, år 1992)
	Anläggningens robusthet	Minska sannolikheten för härdskada genom att genomföra åtgärder som identifierats inom den probabilistiska säkerhetsanalysen

Tabell 5- Säkerhetsförbättringar av franska kärnkraftreaktorer

4.2.1.4 Schweiz

Säkerhetsförbättringar har införts i de schweiziska kärnkraftsreaktorerna via myndighetsbeslut eller till följd av ny kunskap erhållen via drift- eller andra erfarenhet, analys, forskning och utveckling.

I nedanstående tabell redovisas de säkerhetsförbättringar som har identifierats och till stora delar har implementerats i de schweiziska kärnkraftverken.

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning
Beznau	Kontrollrummets utformning	Införande av datorbaserade stödsystem för operatörerna i det centrala kontrollrummet
	Brott på primärutrymmet	Byte av ånggeneratorer
	Svåra haverier	Installation av ett system för filtrerad tryckavlastning av inneslutningen
	Fysisk separation	Installation av ett eller två separerade avställning- och resteffektkylsystem (inklusive tillhörande dieselaggregat) i vattentäta utrymmen
	Diversifiering	Installation av ett nytt separerat hjälpmatarvattensystem med dedikerade hjälpdiesel i vattentäta utrymmen
	Robusthet	Uppdatering av vissa säkerhetsrelaterade ventiler
	Instrumentering och kontrollutrustning	Införande av ett nytt datorbaserat reaktorskyddsystem
	Inre och yttre händelser	Förnyade analyser avseende flygplanstörtning
		Förbättringar av automatiseringen för att minska behovet av operatörshandlande de 30 första minuterna vid en konstruktionsstyrande händelse, och de första 10 timmarna vid en yttre händelse
		Införande av ett jordbävningssäkrat nöddieselaggregat som ska ersätta ursprunglig vattenkraftsbaserad hjälpkraft
		Förnyade probabilistisk säkerhetsanalys avseende jordbävning och efterföljande säkerhetshöjande åtgärder
Mühleberg	Inre och yttre händelser	Förbättringar av automatiseringen för att minska behovet av operatörshandlande de 30 första minuterna vid en konstruktionsstyrande händelse, och de första 10 timmarna vid en yttre händelse
		Förnyade analyser avseende flygplanstörtning
		Hantering och förhindrande av vätgasexplosioner i anläggningen
		Förnyade probabilistisk säkerhetsanalys avseende jordbävning och efterföljande säkerhetshöjande åtgärder
	Robusthet	Uppdatering av vissa säkerhetsrelaterade ventiler
	Recirkulationsmöjligheter	Förbättring av silar till härdnödkylsystemen
	Kontrollrummets utformning	Införande av datorbaserade stödsystem för operatörerna i det centrala kontrollrummet
	Svåra haverier	Förbättring av instrumenteringen för svåra olyckor

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning
		Installation av ett system för filtrerad tryckavlastning av inneslutningen
	Reaktortankens interndelar	Förstärkning av moderatortanken och införande av alternativ vattenkemi för att motverka sprickbildning på grund av spänningskorrosion
	Primärsystemets integritet	Byte av ledningarna i huvudcirkulationssystem
	Fysisk separation	Installation av ett eller två separerade avställning- och resteffektkylsystem (inklusive tillhörande dieselaggregat) i vattentäta utrymmen
Gösgen	Inre och yttre händelser	Förbättringar av automatiseringen för att minska behovet av operatörshandlande de 30 första minuterna vid en konstruktionsstyrande händelse, och de första 10 timmarna vid en yttre händelse
		Förnyade probabilistisk säkerhetsanalys avseende jordbävning och efterföljande säkerhetshöjande åtgärder
		Förbättrat skydd mot jordbävning (speciellt byggnadsstrukturer)
		Förbättrat åskskydd
		Förnyade analyser avseende flygplanstörtning
	Robusthet	Förbättra möjligheten till "feed and bleed" i samband med olyckor
		Uppdatering av vissa säkerhetsrelaterade ventiler
	Åldring	Ett åldringshanteringsprogram har införts
	Instrumentering och kontrollutrustning	Utbyte av all kontrollutrustning
	Kontrollrummets utformning	Införande av datorbaserade stödsystem för operatörerna i det centrala kontrollrummet
	Svåra haverier	Installation av ett system för filtrerad tryckavlastning av inneslutningen
		Förbättrad instrumenteringen vid svåra olyckor
Leibstadt	Härdens integritet	Installation av ett separerat nödkylsystem för avställd reaktor
	Inre och yttre händelser	Förbättringar av automatiseringen för att minska behovet av operatörshandlande de 30 första minuterna vid en konstruktionsstyrande händelse, och de första 10 timmarna vid en yttre händelse
		Förnyade analyser avseende flygplanstörtning

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning
		Hantering och förhindrande av vätgasexplosioner i anläggningen
		Förbättrat åskskydd
		Förnyade probabilistisk säkerhetsanalys avseende jordbävning och efterföljande säkerhetshöjande åtgärder
	Recirkulationsmöjligheter	Förbättring av silar till härdnödkylsystemen
	Diversifiering	Förbättrat skydd mot felfunktion hos styrstavar
	Robusthet	Uppdatering av vissa säkerhetsrelaterade ventiler
	Kontrollrummets utformning	Införande av datorbaserade stödsystem för operatörerna i det centrala kontrollrummet
	Svåra haverier	Installation av ett system för filtrerad tryckavlastning av inneslutningen

Tabell 6- Säkerhetsförbättringar av schweiziska kärnkraftverk

4.2.1.5 Tyskland

Säkerhetsförbättringar har införts i de tyska kärnkraftsreaktorerna till följd av kunskaper erhållna genom framför allt utförandet av nya säkerhetsanalyser.

I nedanstående tabell redovisas de säkerhetsförbättringar som har identifierats och till stora delar har implementerats i de tyska kärnkraftverken.

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning
PWR (Gen 1)	Yttre elkraftnät	Installation av extra kraftmatning från yttre nät
	Redundans	Installation av nytt reservdieselaggregat
		Installation av extra hög- och lågtryckshärdnödkylsystem
		Förstärkning av härdnödkylsystem samt installation av extra insprutningsledningar
		Modifieringar av säkerhetskritiska komponenter för att bättre motstå konstruktionsstyrande händelser
		Installation av extra hjälpmatarvattensystem
	Robusthet	Förbättra säkerhetssystems möjlighet att hantera olyckor
		Förbättrat gränssnitt mellan högtrycks- och lågtrycksdelarna i härdnödkylsystemen

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning
	Recirkulationsmöjligheter	Modifiering av silarna i inneslutningens sump (som följd av silhändelsen i Barsebäck, år 1992).
	Fysisk separation	Förbättrad fysisk separation genom installation av nya system i separata byggnader
	Brandskydd	Installation av nya brandskyddsystem samt modernisering av befintliga brandskyddsystem
		Modifieringar av anläggningarna för att förebygga rökgasspridning i säkerhetsrelaterade byggnader i samband med brand i anläggning eller på anläggningsplatsen (erfarenheter från branden i Krümmel, år 2007)
		Förbättringar avseende brandspjäll och brandseparation
		Installation av nya brandspjäll
	Brott på primärsystem	Förbättrat material i ånggeneratorer
	Inre och yttre händelser	Moderniseringar för att öka anläggningens motståndskraft och hantering av inre och yttre händelser
	Oberoende	Hantering av ”station blackout” via batterimatad högtrycksinsprutningssystemet (SI)
	Svåra haverier	Införa inert atmosfär i inneslutningen under drift
		Införande av system för filtrerad tryckavlastning av inneslutningen
		Övervakning av inneslutningens atmosfär
PWR (Gen 2)	Yttre kraftnät	Installation av extra kraftmatning från yttre nät
	Redundans	Förstärkning av härdnödkylsystem samt installation av extra insprutningsledningar
		Installation av ett extra hjälpmatarvattensystem
	Robusthet	Modifieringar av säkerhetskritiska komponenter för att bättre motstå konstruktionsstyrande händelser
		Förbättra säkerhetssystemens möjlighet att hantera olyckor
		Förbättrat gränssnitt mellan högtrycks- och lågtrycksdelarna i härdnödkylsystemen
	Recirkulationsmöjligheter	Modifiering av silarna i inneslutningens sump som följd av silhändelsen i Barsebäck, år 1992.
	Brandskydd	Modifieringar av anläggningarna för att förhindra rökgasspridning i säkerhetsrelaterade byggnader i samband med brand i anläggning eller på anläggningsplatsen (erfarenheter från branden i Krümmel, år 2007)

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning
		Förbättringar avseende brandspjäll och brandseparation
	Svåra haverier	Införa inert atmosfär i inneslutningen under drift
		Införande av system för filtrerad tryckavlastning av inneslutningen
		Övervakning av inneslutningens atmosfär
	Inre och yttre händelser	Moderniseringar för att öka anläggningens motståndskraft och hantering av inre och yttre händelser
	Oberoende	Hantering av ”station blackout” via batterimatad högtrycksinsprutningssystemet (SI)
PWR (Gen 3)	Robusthet	Förbättrat gränssnitt mellan högtrycks- och lågtrycksdelarna i härdnödkylsystemen
	Svåra haverier	Införande av system för filtrerad tryckavlastning av inneslutningen
		Övervakning av inneslutningens atmosfär
	Brandskydd	Modifieringar av anläggningarna för att förhindra rökgasspridning i säkerhetsrelaterade byggnader i samband med brand i anläggning eller på anläggningsplatsen (erfarenheter från branden i Krümmel, år 2007)
	Inre och yttre händelser	Moderniseringar för att öka anläggningens motståndskraft och hantering av inre och yttre händelser
	Recirkulationsmöjligheter	Modifiering av silarna i inneslutningens sump som följd av silhändelsen i Barsebäck, år 1992.
	Oberoende	Hantering av ”station blackout” via batterimatad högtrycksinsprutningssystemet (SI)
PWR (Gen 4)	Robusthet	Förbättrat gränssnitt mellan högtrycks- och lågtrycksdelarna i härdnödkylsystemen
	Svåra haverier	Införa inert atmosfär i inneslutningen under drift
		Införande av system för filtrerad tryckavlastning av inneslutningen
		Övervakning av inneslutningens atmosfär
	Recirkulationsmöjligheter	Modifiering av silarna i inneslutningens sump som följd av silhändelsen i Barsebäck, år 1992.
	Brandskydd	Modifieringar av anläggningarna för att förhindra rökgasspridning i säkerhetsrelaterade byggnader i samband med brand i anläggning eller på anläggningsplatsen (erfarenheter från branden i Krümmel, år 2007)

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning
	Inre och yttre händelser	Moderniseringar för att öka anläggningens motståndskraft och hantering av inre och yttre händelser
	Oberoende	Hantering av ”station blackout” via batterimatad högtrycksinsprutningssystemet (SI)
BWR 69	Yttre kraftnät	Installation av extra kraftmatning från yttre nät
	Redundans	Installation av nytt reservdieselaggregat
		Installation av extra ventiler för isolering av inneslutningen
		Tekniska förbättringar av för säkerheten viktiga komponenter för att motstå konstruktionsstyrande haverier
	Robusthet	Förbättra säkerhetssystems möjlighet att hantera olyckor
		Förbättrat gränssnitt mellan högtrycks- och lågtrycksdelarna i härdnödkylsystemen
	Diversifiering	Införande av oberoende härdnödkylsystem
		Diversifierade styrventiler för säkerhets- och avblåsningsventiler
		Diversifierade tryckavlastningsventiler
	Fysisk separation	Fysisk separation genom installation av nya system i separata byggnader
	Brandskydd	Modifieringar av anläggningarna för att förhindra rökgasspridning i säkerhetsrelaterade byggnader i samband med brand i anläggning eller på anläggningsplatsen (erfarenheter från branden i Krümmel, år 2007)
		Installation av nya brandskyddspjäll
	Primärsystemets integritet	Byte av rörledningar för ångsystem, matarvattensystem och nukleära driftsystem till material med förbättrade egenskaper
	Svåra haverier	Införa inert atmosfär i inneslutningen under drift
		Förbättring av utrustning för minimering av skador
		Införande av system för filtrerad tryckavlastning av inneslutningen
		Framtagning av instruktioner för svåra olyckor
		Övervakning av inneslutningens atmosfär
	Inneslutningens integritet	Bortförsel av vatten från tryckbärande system med möjlighet till omkoppling utanför inneslutningen.

Anläggning	Säkerhetsförbättringar avseende följande områden	Beskrivning
	Inre och yttre händelser	Moderniseringar för att öka anläggningens motståndskraft och hantering av inre och yttre händelser
	Oberoende	Hantering av ”station blackout” via batterimatad högtrycksinsprutningssystemet (SI)
BWR 72	Redundans	Installation av extra reservdieselaggregat
	Robusthet	Förbättrat gränssnitt mellan högtrycks- och lågtrycksdelarna i härdnödkylsystemen
	Diversifiering	Införande av oberoende härdnödkylsystem
		Diversifierade tryckavlastningsventiler
	Svåra haverier	Införa inert atmosfär i inneslutningen under drift
		Införande av system för filtrerad tryckavlastning av inneslutningen
		Framtagning av instruktioner för svåra olyckor
		Övervakning av inneslutningens atmosfär
	Brandskydd	Modifieringar av anläggningarna för att förhindra rökgasspridning i säkerhetsrelaterade byggnader i samband med brand i anläggning eller på anläggningsplatsen (erfarenheter från branden i Krümmel, år 2007)
	Inre och yttre händelser	Moderniseringar för att öka anläggningens motståndskraft och hantering av inre och yttre händelser
	Oberoende	Hantering av ”station blackout” via batterimatad högtrycksinsprutningssystemet (SI)

Tabell 7- Säkerhetsförbättringar av tyska kärnkraftsreaktorer

4.2.1.6 Likheter och olikheter mellan Sverige och de studerade länderna

Vid jämförelse av de olika ländernas identifierade säkerhetsförbättringar ser man tydligt att flertalet av de identifierade säkerhetsförbättringarna är gemensamma för de olika länderna respektive reaktortyperna. Då ursprungliga konstruktionen varierar hos de olika studerade reaktorerna ser man väsentliga skillnader både i omfattning och i antalet identifierade säkerhetsförbättringar. Det konstateras att fysisk separation, redundans och diversifiering (för att skapa oberoende) är något som förstärkts generellt inom de äldre reaktorerna medan förutsättningarna avseende dessa områden varit bättre hos de nyare anläggningarna och därmed inte krävt lika omfattande åtgärder. Vidare konstateras att det kan vara svårt att utifrån de korta beskrivningar som återges i nationalrapporterna få en klar uppfattning av omfattningen hos respektive lands säkerhetsförbättring. Detta medför att en jämförelse endast är möjlig på en övergripande nivå.

När det gäller skillnader mellan Sverige och övriga studerade länder framstår det som om implementering av oberoende härdnödkylsystem är något som Schweiz och Tyskland har kommit betydligt längre än Sverige med. Likaså framstår det som om man framför allt i Schweiz, men även i övriga länder, har kunnat identifiera fler säkerhetsförbättringar än vad Sverige har gjort gällande naturfenomen och andra olyckor utanför och innanför anläggningsplatsen (såsom åtgärder för att stärka skyddet vid jordbävning, explosioner och översvämning). Det noteras dock att vikten av ett oberoende härdnödkylsystem belystes inom de svenska stresstestesterna samt att flertalet av de åtgärder som övriga länder identifierat avseende naturfenomen och andra händelser inom och yttre anläggningarna även identifierats inom de svenska stresstestesterna och kommer att hanteras i enlighet med åtgärdsplanerna för stresstesterna.

Med utgångspunkt från de övergripande beskrivningar som återges i ländernas nationalrapporter till kärnsäkerhetskonventionen samt beaktande av de svenska åtgärdsplanerna för stresstesterna har det inte varit möjligt att via denna genomgång identifiera några väsentliga säkerhetsförbättringar som man hittills inte behandlat i Sverige.

5 Resultat och slutsatser

5.1 Etapp 1

5.1.1 Resultat och slutsatser avseende kravstruktur och kravens omfattning

5.1.1.1 Svenska krav i relation till andra länders krav

Strukturen för krav gällande konstruktion och utförande av kärnkraftsreaktorer varierar mellan olika länder och måste ställas i relation till de befogenheter som respektive lands tillsynsmyndighet har samt ländernas politiska system och deras förvaltningsstruktur. Likaså variera den innehållsmässiga omfattning hos kraven inom olika länder och utformandet av kraven bör på liknande sätt som för strukturen ställas i relation till ländernas politiska system och deras förvaltningsstruktur samt även beaktas utifrån de kulturella skillnader som råder mellan olika länder.

Av den övergripande genomgång av respektive lands regelverk avseende konstruktion och utförande av kärnkraftsreaktorer som genomförts inom ramen för denna utredning framgår att de svenska kravens textmässiga omfattning skiljer sig från övriga länder då de svenska kraven är betydligt mer kortfattade än övriga länders kravdokument, samt att detaljeringsnivå inom de svenska kraven är betydligt lägre och de svenska kraven är mindre tydliga och specifika. Vid en jämförelse framstår det emellertid som om de målinriktade krav som finns inom det svenska regelverket är ändamålsenliga och uppfyller internationella krav och säkerhetsstandarder även om utformandet av kraven skiljer sig. Det noteras dock att tydligare krav kan vara effektivare och i praktiken innebära ökad säkerhet genom att

förutsägbarhet och därmed även rättstrygghet hos regelverket ökar samtidigt som tolkningsutrymmet minskar. Om alla parter vet vad som förväntas och vad som gäller så underlättas implementeringen och uppyllandet av kraven samt även granskningen av uppfyllandet och implementeringen. Resursmässigt skulle tydligare krav kunna medföra att tidsödande granskningsprocesser som inkluderar uttolkande av krav kan minimeras. Vidare bedöms en viss ökning av detaljeringsnivå hos de svenska kraven kunna ge en tydligare kravbild, mer i harmoni med internationella krav och standarder. Som inspiration för en sådan utveckling bör detaljeringsnivån som återfinns inom det kanadensiska regelverket, inom de brittiska guiderna samt inom IAEA:s säkerhetsstandarder, kunna användas eftersom dessa länder och denna organisation i likhet med Sverige använder sig av en målinriktad kravbild.

Genomgången visar även att Sverige är det land där man tydligast valt att på en hög och övergripande nivå dela upp kraven som reglerar kärnkraftsreaktorer i olika kravdokument (exempelvis regleras kärnkraftsanläggningar och vissa delar av dess tillhörande verksamheter i olika kravdokument). Denna uppdelning kan ge en något komplex bild av kraven eftersom vissa kravdokumenten även delvis överlappar varandra. Sådana överlapp syns inte lika tydligt i övriga studerade länder.

När det gäller uppfyllnad av moderna krav visar genomgången att det finns en väsentlig skillnad när det gäller i vilken utsträckning som gamla anläggningar ska uppfylla moderna krav. De flesta studerade länder har dock i likhet med Sverige valt att ge tillsynsmyndigheten möjlighet att avgöra detta i enskilda fall, vilket bedöms som rimligt då anläggningarnas ursprungliga konstruktion varierar.

Alla studerade länderna samt IAEA använder sig av råd om tillämpning för att antingen vägleda myndighetens inspektörer och utredare, och/eller tillståndshavare och tillståndsansökanden. Genomgången visar att de studerade ländernas råd om tillämpning är mer harmoniserade både avseende omfattning och detaljeringsnivå, än de svenska råden om tillämpning. Vid jämförelse framstår det som om tydligare och mer utvecklade råd om tillämning är något som saknas i det svenska regelverket. Detta eftersom välutvecklade råd om tillämpning bedöms kunna skapa en mer ändamålsenlig kravbild genom att forma enhetliga tolkningar av kraven, underlätta implementering samt ge en effektivare granskning. Vidare konstateras att de flesta länder och IAEA har valt att strukturmässigt hålla råd om tillämning i separata dokument för att på ett enklare sätt kunna uppdatera dem i enlighet med senaste kunskaper och erfarenheter. Inom området konstruktion och utförande framstår det vid jämförelsen som om denna struktur är tydligare och effektivare samt enklare att hantera, eftersom denna uppdelning ger större möjligheter att beroende på område skapa bästa möjliga utformning för råden om tillämpning.

När det gäller det specifika innehållet i kraven har utredningen funnit att i förhållande till de svenska kraven så kravställs vissa områden betydligt mer utförligt i de övriga studerade länderna samt inom IAEA. Detta gäller framför allt områdena:

- åldring och förlängning av drifttillstånd,
- kärnkraftverkets förläggningsplats,
- uppförande och idrifttagning av ett kärnkraftverk,
- mänskliga faktorer (inkl. säkerhetskultur), samt
- säkerhetsforskning och drifterfarenheter.

Därutöver återfinns även tydligare krav gällande:

- säkerhetsanalys och riskanalys (probabilistisk säkerhetsanalys),
- verifikation av säkerhet (via tillämpandet av s.k. ”safey cases”),
- brandskydd,
- elektriska system, samt
- instrumentering och kontrollutrustning (inkl. datorbaserade system).

5.1.1.2 Svenska krav i relation till WENRA:s referensnivåer

WENRA:s referensnivåer har legat till grund för de ändringar av föreskrifterna inom SSMFS 2008:1 som genomförts under 2011 och pågående föreskriftöversyn avser att på liknande sätt beakta referensnivåerna och inarbeta dessa i den svenska kraven. Detta har medfört att de 18 huvudområden som utgör grunden för referensnivåerna är tydligt spårbara i det svenska regelverket även om omfattningen av kraven kan variera.

Den huvudsakliga skillnaden mellan de svenska kraven och referensnivåerna är detaljeringsgraden. WENRA:s referensnivåer är betydligt mer preciserade än motsvarande svenska krav. Skillnaden medför att referensnivåerna kan uppfattas som tydligare än de svenska kraven och ger mindre utrymme för tolkning. Detta gäller framför allt områdena åldring, probabilistisk säkerhetsanalys och brandskydd, där de befintliga svenska kraven är på en så övergripande nivå att är svårt att bedöma huruvida referensnivån verkligen uppfylls.

5.1.1.3 Svenska krav i relation till WENRA:s säkerhetsmål

Vid jämförelse mellan WENRA:s säkerhetsmål och det svenska regelverket konstateras att stora delar av säkerhetsmålen uttrycks i de svenska kraven. Säkerhetsmålen går dock något längre avseende precisering. Ett antal skillnader noteras vid jämförelsen:

1. WENRA föreslår ett värde för en härdskadefrekvens som är satt till 10^{-5}/år inom vägledningen till säkerhetsmålen. SSM har idag inte något kriterium för acceptabel härdskadefrekvens, vilket är ett medvetet val. SSM:s inställning är att ett sådant kriterium inte heller i framtiden ska vara del av föreskrifterna. Dock finns ett svenskt kriterium för utsläppsfrekvens som regeringen använder för att precisera den tillförlitlighet som de svenska haverifiltren ska ha.
2. WENRA:s säkerhetsmål tar upp krav på förläggningsplats. I det svenska regelverket är kraven på förläggningsplatsen inte lika utförliga och definieras till störst del av miljöbalken vilken har ett annat fokus än det som ges i säkerhetsmålen. Med beaktande av olyckan i Fukushima Dai-ichi som demonstrerade vikten av val av förläggningsplatsens, framstår det som om det vid nybyggnation av

kärnkraftverk är rimligt att utveckla kraven avseende förläggningsplatsens utformande och det bedöms även rimligt att man för befintliga kärnkraftverk ser över relevant svensk krav med avsikt att skapa en harmonisering med internationell standard och identifiera behov av ytterligare säkerhetsförbättringar.

3. Flera av WENRA:s säkerhetsmål tar upp krav gällande anläggningens layout. Motsvarande krav återfinns inte tydligt i de svenska kraven men bedöms vara väsentligt vid om- och nybyggnation för att minska personaldoser, möjliggöra framtida säkerhetsförbättringar och skapa förutsättningar för utförligare inspektioner och provning samt möjliggöra ett effektivare underhåll. Vid modifieringar av befintliga anläggningar bedöms denna aspekt vara relevant och det framstår som rimligt att föreslå att en översyn av kraven på anläggningslayout sker för att tydligare harmonisera denna med internationell standard.
4. Kraven på oberoende inom djupförsvaret som återges i WENRA:s säkerhetsmål utrycks i de svenska kraven men inte lika specificerat. I avsnitt 4.1.3 till detta PM behandlas precisering inom regelverk vidare.
5. WENRA:s säkerhetsmål avseende gränssnittet mellan kärnsäkerhet och fysiskt skydd är inte lika tydligt i de svenska kraven. I takt med att modern mjukvarubaserad utrustning implementeras i befintliga anläggningar aktualiseras behovet av en utvecklad strategi och hantering av detta område och det bedöms som rimligt att föreslå att en översyn av kraven för detta område sker.
6. Vägledningen för WENRA:s säkerhetsmål anger att man bör arbeta för att öka marginaler. De svenska föreskrifterna anger att man kontinuerlit ska utveckla säkerheten och implementera säkerhetsförbättringar. Detta bedöms medföra att intentionen med vägledningen till säkerhetsmålet är uppfylld inom de svenska kraven även om man inte utryckligen refererar till marginaler.
7. Vägledningen till WENRA:s säkerhetsmål tar upp hantering av åldringseffekter. Detta område behandlas begränsat i de svenska kraven men kommer att förstärkas till följd av bland annat de utredningar som gjorts inom ramen för delprojekt 2 i regeringsupdraget som denna rapport är en del av (se vidare avsnitt 1).
8. Vägledningen och framförallt förtydligandet av WENRA:s säkerhetsmål tar upp begreppen evakueringszon och skyddszon. Dessa begrepp saknar direkta motsvarigheter i den svenska beredskapsstrategin där man endast talar om inre beredspakszon och zon för strålningsmätning. Den inre beredskapszonen motsvarar närmast en kombination av de två begreppen, evakueringszon och skyddszon. Det framstår som rimligt att man från svensk sida ser över eventuella behovet av att uppdatera strategin för beredskap utifrån säkerhetsmålen och utreder betydelse och säkerhetsnytt med den föreslagna zonindelningen.

9. WENRA:s säkerhetsmål tar upp yttre händelser[9] och specifikt flygplanskrascher av stora flygplan ur både ett olycks- och ett fysiskt skyddsperspektiv. I de svenska kraven skiljer man tydligt på antagonistiska händelser samt olyckor och naturfenomen vilket medför att vissa skillnader mellan de svenska kraven och säkerhetsmålen kan identifieras. Denna skillnad bedöms dock inte medföra några väsentliga skillnader i praktiken och det framstår därmed inte heller som om det finns behov av uppdateringar av de svenska kraven till följd av dessa skillnader.

5.2 Etapp 2

Säkerhetsförbättringar grundade på ny kunskaper erhållna via drift- eller andra erfarenhet, analys, forskning och utveckling, samt utveckling av IAEA:s säkerhetsstandarder och utveckling av industristandarder, har implementerats i flertalet europeiska reaktorer och utgör ofta ett krav vid ansökan om förnyade drifttillstånd. Hur säkerhetsförbättringarna initieras och under vilka tidsramar säkerhetsförbättringarna ska implementeras varierar dock kraftigt mellan länderna men det framstår som om Sverige ligger i framkant vad gäller omfattning och delvis även framdrift. Detta eftersom Sverige varit mycket tidiga med att implementera omfattande ändringar såsom exempelvis de haveribegränsande funktionerna.

Flertalet av de identifierade säkerhetsförbättringar som studerats inom denna genomgång har varit gemensamma för de olika länderna respektive reaktortyperna. Då ursprungliga konstruktionen varierar hos de olika reaktorerna ser man dock väsentliga skillnader både i omfattning och i antalet identifierade säkerhetsförbättringar. Det konstateras att fysisk separation, redundans och diversifiering (för att skapa oberoende) är något som förstärkts generellt inom de äldre reaktorerna medan förutsättningarna avseende dessa områden varit bättre hos de nyare anläggningarna och därmed har det inte krävts lika omfattande säkerhetsförbättringar av dessa anläggningar.

På grund av att informationen som funnits tillgänglig avseende ländernas implementerade säkerhetsförbättringar varit begränsad och på en mycket övergripande nivå har det varit svårt att identifiera säkerhetsförbättringar som inte tidigare identifierats inom Sverige. Det konstateras dock att länderna generellt tydligare har lyft upp sitt arbete med anläggningens möjlighet att hantera naturfenomen och andra händelser som kan uppkomma inom och utanför anläggningen (jordbävning, översvämning, brand, störningar i elkraftnätet inkl. ”station blackout”, etc.), än vad man hittills gjort i Sverige. Vidare identifieras genomgången relevanta säkerhetsförbättringar såsom gällande oberoende kylning av härden i ett långtidsförlopp, åldring, möjlighet att vid beroende fel i primärpumparnas

[9] Ytter händelser avser händelser som kan uppkomma utanför anläggningen och kan påverka anläggningens säkerhet. Yttre händelser innefattar bland annat naturfenomen, kemiska och bilogiska utsläpp i närregion, explosioner i närregion, flygplanskrascher samt händelser på det yttre elkraftnätet.

elmatning förse huvudcirkulationspumparnas (RCP) tätningar med vatten, samt bränslebassängernas kylning och integritet, hos de studerade europeiska länderna.

Till följd av stresstesterna har emellertid de säkerhetsförbättringar som tas upp av de andra länderna kunnat belysas och inarbetas i de svenska åtgärdsplaneran för stresstesterna. Det bedöms dock som rimligt att man ser över de svenska föreskrifterna för att utveckla relevanta krav utifrån de behov som återspeglas i form av identifierade brister i resultatet från stresstesterna samt i form av åtgärder inom de svenska åtgärdsplanerna till följd av stresstesterna. En sådan översyn bör speciellt beakta de säkerhetsförbättringar som identifierats i denna utredning och som anges i stycket ovan.

6 Referenser

[1] Den långsiktiga säkerhetsutvecklingen i den svenska kärnkraften, Delprojekt 1 – Utredning av säkerhetsförbättringar, Del av Etapp 1 och Etapp 2, Jean-Pierre Bento, JPB Consulting AB, September 2011
[2] Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om konstruktion och utförande av kärnkraftsreaktorer, SSMFS 2008:17
[3] Lag (1984:3) om kärnteknisk verksamhet, Svensk författningssamling 1984:3
[4] Förordning (1984:14) om kärnteknisk verksamhet, Svensk författningssamling 1984:14
[5] Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om säkerhet i kärntekniska anläggningar, SSMFS 2008:1
[6] Föreskrifter om ändring i Strålsäkerhetsmyndighetens föreskrifter (SSMFS 2008:1) om säkerhet i kärntekniska anläggningar, SSMFS 2011:3
[7] Strålsäkerhetsmyndighetens föreskrifter om mekaniska anordningar i vissa kärntekniska anläggningar, SSMFS 2008:13
[8] Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om kompetens hos driftpersonal vid reaktoranläggningar, SSMFS 2008:32
[9] Miljöbalk (1998:808), Ikraftträdande 1999-01-01
[10] Kärnenergilagen (990/1987)
[11] Statsrådets förordning om säkerheten vid kärnkraftverk, 27.11.2008/733
[12] Säkerhetsprinciper för planering av kärnkraftverk, YVL 1.0, 12.1.1996
[13] Kriterier gällande kärnkraftverkets förläggningsplats, YVL 1.10, 11.7.2000
[14] Konstruktion av system i kärnkraftverk, YVL 2.0, 1.7.2002
[15] Nuclear Installations Act 1.965, CHAPTER 57
[16] Safety Assessment Principles for Nuclear Facilities, 2006 Edition, Revision 1
[17] Nuclear Safety and Control Act, S.C. 1997, c. 9

[18] Class I Nuclear Facilities Regulations, SOR/2000-204
[19] Design of New Nuclear Power Plants, RD-337, November 2008
[20] Safety Analysis for Nuclear Power Plants, RD-310, February 2008
[21] Aging Management for Nuclear Power Plants, RD-334, June 2011
[22] Life Extension of Nuclear Power Plants, RD-360, February 2008
[23] Site Evaluation for New Nuclear Power Plants, RD-346, November 2008
[24] Title 10 - Code of Federal Regulations, Chapter 1
[25] Title 10 - Code of Federal Regulations, Chapter 1, Part 50 - Domestic Licensing of production and utilization facilities
[26] Title 10 - Code of Federal Regulations, Chapter 1, Part 50 - Domestic Licensing of production and utilization facilities, Appendix A - General Design Criteria for Nuclear Power Plants
[27] Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, NUREG-0800, June 1987
[28] NRC Regulatory Guides - Power Reactors (Division 1)
[29] IAEA Specific Safety Requirements - Safety of Nuclear Power Plants Design, No. SSR-2/1, February 20, 2012
[30] IAEA Specific Safety Requirements - Site Evaluation for Nuclear Installations Safety Requirements, No SSR-1/1, December 18, 2003
[31] IAEA Specific Safety Requirements - Safety of Nuclear Power Plants: Commissioning and Operation Specific Safety Requirements No SSR -1/3, July 14, 2011
[32] Finnish report on nuclear safety - Finnish 5th national report as referred to in Article 5 of the Convention on Nuclear Safety, STUK-B 120 / AUGUST 2010
[33] France – Convention on Nuclear Safety – Fith National Report for the 2011 Peer Review Meeting, July 2010
[34] Implementation of the obligation of the Convention on Nuclear Safety – The fifth Swiss report in accordance with Article 5, July 2010
[35] Convention on Nuclear Safety – Report by the Government of the Federal Republic of Germany for the Fifth Review Meeting in April 2011, 04 August 2010
[36] Safety Objectives for New Power Reactors - Study by WENRA Reactor Harmonization Working Group, December 2009
[37] IAEA Safety Fundamentals, Fundamental Safety Principles, Series No. SF-1, November 07
[38] Safety of new NPP designs 1/2012 - Study by WENRA Reactor Harmonization Working Group, May 2012, DRAFT
[39] Harmonization of Reactor Safety in WENRA Countries - Report by WENRA Reactor Harmonization Working Group, January 2006
[40] WENRA Reactor Safety Reference Levels, January 2008
[41] Views on the Finnish nuclear regulatory guides, Björn Wahlström, Risto Sairanen, VTT Automation - VTT Energy
[42] IAEA Fundamental Safety Principles, No. SF-1, November 07 2006

Bilaga 1

Svenska respektive internationella krav avseende anläggningars utformanden (med fokus på säkerhetsförbättringar)

I nedanstående bilaga redovisas relevanta krav och råd (guider) avseende anläggningars utformanden hämtade från Sverige, Finland, Storbritannien, Kanada, USA samt IAEA. Då kraven för konstruktion och utförande av kärnkraftsreaktorer ofta är uppdelad i flera olika dokument samt fördelade på olika kravnivåer har denna bilaga begränsats till att fokusera på endast ett fåtal övergripande kravdokument. De flesta länder tillämpar i dag en kravstruktur där de specifika kraven kompletteras med råd om tillämpning. Där så bedömts relevant, har i denna bilaga de redovisade kraven kompletterats med specifika råd.

Följande kravdokument för respektive land har, om inget annat anges, studerats och redovisas i denna bilaga.

Sverige
Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om konstruktion och utförande av kärnkraftsreaktorer, SSMFS 2008:17

Finland
Statsrådets förordning om säkerheten vid kärnkraftverk 27.11.2008/733

Storbritannien
Safety Assessment Principles for Nuclear Facilities, 2006 Edition, Revision 1

Kanada
Design of New Nuclear Power Plants, RD–337, November 2008, Regulatory Document

USA
NRC Regulations Title 10, Code of Federal Regulations Part 50 Domestic Licensing of Production and Utilization Facilities, Appendix A to Part 50 - General Design Criteria for Nuclear Power Plants

IAEA
IAEA Safety Standards, Safety of Nuclear Power Plants Design, Specific Safety Requirements, No. SSR-2/1

Krav på säkerhetsfunktionerna

Sverige

Krav

3 § Kärnkraftsreaktorn ska vara konstruerad så att säkerhetsfunktionerna reaktivitetskontroll, primärsystemets integritetsskydd, härdnödkylning, resteffektkylning och inneslutningsfunktionen kan upprätthållas, i den omfattning som behövs beroende på driftläget, vid alla händelser till och med händelseklassen osannolika händelser.

Konstruktionen ska beakta händelser i händelseklassen mycket osannolika händelser i enlighet med 4-9 samt 18-20 §§.

Finland

Krav

14 § Säkerhetsfunktioner och tryggande av dem

Vid tryggande av säkerhetsfunktioner ska i första hand utnyttjas naturliga säkerhetsegenskaper som kan uppnås med goda planeringslösningar. I synnerhet ska samverkan av de fysikaliska återkopplingsfenomenen i kärnreaktorn vara sådan att den motverkar en ökning av reaktoreffekten.

Om naturliga säkerhetsegenskaper inte kan utnyttjas för att trygga en säkerhetsfunktion, ska sådana system och anordningar utnyttjas som inte kräver någon yttre drivkraft och som, om drivkraften går förlorad, ställer sig i ett ur säkerhetssynpunkt gynnsamt läge.

För att olyckor ska kunna hindras och deras följder lindras ska kärnkraftverket ha system för att stänga av reaktorn och kvarhålla den i subkritiskt tillstånd samt system för avlägsnande av den resteffektvärme som bildas i reaktorn och säkerställande av att radioaktiva ämnen stannar inom anläggningen.

Vid planeringen av ifrågavarande system ska principer som säkerställer att säkerhetsfunktionen träder i funktion också vid felsituationer följas. Sådana principer är mångfalds-, åtskillnads- och olikhetsprincipen.

De viktigaste system som behövs för övergång i kontrollerat läge och kvarhållandet av det ska kunna utföra sina funktioner även om en enskild komponent i vilket system som helst blir funktionsoduglig och även om vilken som helst annan komponent i samma system eller en komponent i ett stöd- eller hjälpsystem som är nödvändigt med tanke på dess funktion samtidigt är ur bruk på grund av behövliga reparationer eller underhåll.

De effekter som en gemensam felorsak i säkerhetssystemen har på anläggningens säkerhet ska vara ringa.

Kärnkraftverket ska ha matarsystem för yttre och inre eleffekt. Säkerhetsfunktionerna ska kunna genomföras med användning av vilketdera som helst av dessa elmatarsystem.

I syfte att kunna ha kontroll över och följa upp allvarliga reaktorolyckor ska planeras system, konstruktioner och anordningar som är oberoende av de system som är konstruerade för driftsituationer och antagna olyckor. De system som behövs för säkerställande av tätheten hos reaktorinneslutningen i samband med en allvarlig reaktorolycka ska vara kapabla att utföra sina säkerhetsfunktioner också i händelse av att det uppstår ett fel i en enskild anordning. Anläggningen ska planeras så att den kan ställas i ett säkert läge efter en allvarlig reaktorolycka.

YVL B.1 §421

YVL B.1 §433-434

YVL B.1 §436-438

Storbritannien

Övergripande principer

EKP.4 Safety function
The safety function(s) to be delivered within the facility should be identified by a structured analysis.

EKP.5 Safety measures
Safety measures should be identified to deliver the required safety function(s).

ESS.1 Requirement for safety systems
All nuclear facilities should be provided with safety systems that reduce the frequency or limit the consequences of fault sequences, and that achieve and maintain a defined safe state.

ESS.2 Determination of safety system requirements
The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and required reliabilities should be determined.

ERC.1 Design and operation of reactors
The design and operation of the reactor should ensure the fundamental safety functions are delivered with an appropriate degree of confidence for permitted operating modes of the reactor.

Vägledande råd

145 The identification of safety functions should be based on an analysis of normal operation and all significant fault sequences arising from possible initiating faults determined by fault analysis (see *paragraph 496 ff.*).

146 Safety should be secured by characteristics as near as possible to the top of the list below:

(f) Passive safety measures that do not rely on control systems, active safety systems or human intervention.
(g) Automatically initiated active engineered safety measures.
(h) Active engineered safety measures that need to be manually brought into service in response to the fault.
(i) Administrative safety measures (see paragraph 376 f.).
(j) Mitigation safety measures (eg filtration or scrubbing).

Note: The hierarchy above should not be interpreted to mean that the provision of an item towards the top of the list precludes provision of other items where they can contribute to defence in depth.

147 The availability and reliability of the safety measures should be commensurate with the significance of the radiological hazards to be controlled. There should also be measures in place to mitigate the consequences of any accident where radioactivity is released from its intended containment, but these should not be regarded as a substitute for fault prevention but as further defence in depth.

166 Engineered structures, systems and components should be designed to deliver their required safety functions with adequate reliability, according to the magnitude and frequency of the radiological hazard, to provide confidence in the robustness of the overall design.

167 Ideally, the structures, systems and components important to safety should be fail-safe, ie they should have no unsafe failure modes.

168 The design should incorporate redundancy to avoid the effects of random failure, and diversity and segregation to avoid the effects of common cause failure. Examples of diversity are different operating conditions, different working principles or different design teams, different sizes of equipment, different manufacturers, different components, and types of equipment that use different physical methods. The design should also be tolerant of random failure occurring anywhere within the safety systems provided to secure each safety function.

169 The application of the principles in this section may vary according to whether the structures, systems and components form part of a safety system (which acts in response to a plant fault, to prevent or mitigate a radiological consequence) or a safety-related system (a plant system other than a safety system, on which safety may depend).

170 It should be demonstrated that the required level of reliability for their intended safety function has been achieved.

336 A reactor should be provided with safety systems that can shut it down safely in normal operating and fault conditions and maintain it in the shutdown condition. There should be a margin of reactivity that allows for systematic changes and uncertainties in nuclear characteristics, variations in plant state and other processes or mechanisms that might affect the reactivity of the core, even for the most reactive conditions of the core.

337 The design basis (Principles FA.4 (paragraph 512 f.) and FA.9 (paragraph 525 f.)) and probabilistic safety (Principle FA.14 (paragraph 540

f.)) analyses (or other suitable analyses) should determine the safety system provisions, functions and required reliabilities.

440 For example, if the action is to initiate a coolant flow then the flow should be measured directly and not inferred from measurement of power to actuation devices such as pumps, valves etc.

Kanada

Krav

RD–337, 6.2 Safety Functions
The NPP design provides adequate means to:

1. Maintain the plant in a normal operational state;
2. Ensure the proper short-term response immediately following a PIE; and
3. Facilitate the management of the plant in and following any DBA, and in accident conditions beyond DBAs.

The following fundamental safety functions are available in normal operation, and during and following AOOs and DBAs:

1. Control of reactivity;
2. Removal of heat from the core;
3. Confinement of radioactive material;
4. Control of operational discharges and hazardous substances, as well as limitation of accidental releases; and
5. Monitoring of safety critical parameters to guide operator actions.

The above functions also facilitate response to BDBAs to the extent practicable.

SSCs necessary to fulfill safety functions following a PIE are identified. This approach identifies the need for such functions as reactor shutdown, emergency core cooling, containment, emergency heat removal, and power systems, etc.

USA

Krav

10 CFR 50 Appendix A, Criterion 1, Quality standards and records.
Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A quality assurance program shall

be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

10 CFR 50 Appendix A, Criterion 2, Design bases for protection against natural phenomena.
Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect: (1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena and (3) the importance of the safety functions to be performed.

10 CFR 50 Appendix A, Criterion 5, Sharing of structures, systems, and components.
Structures, systems, and components important to safety shall not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and cooldown of the remaining units.

10 CFR 50 Appendix A, Criterion 17, Electric power systems.
An onsite electric power system and an offsite electric power system shall be provided to permit functioning of structures, systems, and components important to safety. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents.

The onsite electric power supplies, including the batteries, and the onsite electric distribution system, shall have sufficient independence, redundancy, and testability to perform their safety functions assuming a single failure.

Electric power from the transmission network to the onsite electric distribution system shall be supplied by two physically independent circuits (not necessarily on separate rights of way) designed and located so as to minimize to the extent practical the likelihood of their simultaneous failure under operating and postulated accident and environmental conditions. A switchyard common to both circuits is acceptable. Each of these circuits shall be designed to be available in sufficient time following a loss of all onsite alternating current power supplies and the other offsite electric power

circuit, to assure that specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded. One of these circuits shall be designed to be available within a few seconds following a loss-of-coolant accident to assure that core cooling, containment integrity, and other vital safety functions are maintained.

10 CFR 50 Appendix A, Criterion 21, Protection system reliability and testability.
The protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

10 CFR 50 Appendix A, Criterion 29 Protection against anticipated operational occurrences.

The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.

10 CFR 50 Appendix A, Criterion 38 Containment heat removal.

A system to remove heat from the reactor containment shall be provided. The system safety function shall be to reduce rapidly, consistent with the functioning of other associated systems, the containment pressure and temperature following any loss-of-coolant accident and maintain them at acceptably low levels.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 4: Fundamental safety functions
Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states: (i) control of reactivity, (ii) removal of heat from the reactor and from the fuel store and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

IAEA Safety Standard, No. SSR-2/1, Requirement 20: Design extension conditions
A set of design extension conditions shall be derived on the basis of

engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences if they do occur.

IAEA Safety Standard, No. SSR-2/1, 4.1.
A systematic approach shall be taken to identifying those items important to safety that are necessary to fulfil the fundamental safety functions and to identifying the inherent features that are contributing to fulfilling, or that are affecting, the fundamental safety functions for all plant states.

IAEA Safety Standard, No. SSR-2/1, Requirement 6: Design for a nuclear power plant
The design for a nuclear power plant shall ensure that the plant and items important to safety have the appropriate characteristics to ensure that safety functions can be performed with the necessary reliability, that the plant can be operated safely within the operational limits and conditions for the full duration of its design life and can be safely decommissioned, and that impacts on the environment are minimized.

IAEA Safety Standard, No. SSR-2/1, 4.11
The design:

(f) Shall provide multiple means for ensuring that each of the fundamental safety functions is performed, thereby ensuring the effectiveness of the barriers and mitigating the consequences of any failure or deviation from normal operation.

IAEA Safety Standard, No. SSR-2/1, 5.1
Plant states shall typically cover:

(a) Normal operation;
(b) Anticipated operational occurrences, which are expected to occur over the operating lifetime of the plant;
(c) Design basis accidents;
(d) Design extension conditions, including accidents with significant degradation of the reactor core.

IAEA Safety Standard, No. SSR-2/1, 5.7
An analysis of the postulated initiating events for the plant shall be made to establish the preventive measures and protective measures that are necessary to ensure that the required safety functions will be performed.

IAEA Safety Standard, No. SSR-2/1, 5.23
Methods to ensure a robust design shall be applied, and proven engineering practices shall be adhered to in the design of a nuclear power plant to ensure that the fundamental safety functions are achieved for all operational states and for all accident conditions.

Krav avseende djupförsvarets utformande

Sverige

Krav

4 § Vid utformningen av reaktorns djupförsvar ska följande konstruktionsprinciper tillämpas i den omfattning som är möjlig och rimlig:

a) Enkelhet och tålighet i uppbyggnaden av säkerhetssystemen.
b) Redundans, inklusive diversifiering samt fysisk och funktionell separation i uppbyggnaden av säkerhetsfunktionerna.
c) Automatisk styrning eller passiv funktion vid nödvändiga aktiveringar och driftomläggningar av säkerhetsfunktionerna.
d) Fel i säkerhetsklassad utrustning leder till ett för säkerheten acceptabelt läge.
e) Fel i driftklassad utrustning får inte påverka funktionen hos utrustning med säkerhetsfunktion.
f) Vid delning av säkerhetssystem mellan reaktorer får ett fel i en av reaktorerna inte påverka möjligheten att genomföra avställning och resteffektkylning av andra reaktorer.

Finland

Krav

12 § Förebyggande av olyckor och lindring av följderna av olyckor
… För att driftstörningar och olyckor skulle kunna förebyggas och deras följder lindras ska principen om funktionellt djupförsvar följas på det sätt som anges i denna paragraf.

Vid planeringen, byggandet och driften av ett kärnkraftverk ska beprövad eller i övrigt omsorgsfullt undersökt, högklassig teknik användas. Vid organisering av verksamheten inom tillståndshavarens organisation ska målet vara att säkerställa att störningar och olyckor kan förebyggas på ett tillförlitligt sätt (förebyggande).

Kärnkraftverket ska ha system med hjälp av vilka man snabbt och tillförlitligt upptäcker driftstörningar och olyckssituationer samt förhindrar att situationen förvärras. Olyckor som leder till stora utsläpp av radioaktiva ämnen ska vara ytterst osannolika (bemästrande av driftstörningar och olyckstillbud).

Beredskap att lindra följderna av en olycka ska upprätthållas med effektiva tekniska och administrativa arrangemang. Motåtgärder i syfte att få en olycka under kontroll och förebygga strålskador ska planeras på förhand (lindrande av följder).

13 § Tekniska hinder för spridning av radioaktiva ämnen
För att hindra spridningen av radioaktiva ämnen ska principen om strukturellt djupförsvar följas på det sätt som anges i denna paragraf.

Spridning av radioaktiva ämnen från en kärnreaktors bränsle till omgivningen ska förhindras med på varandra följande hinder, vilka är

bränslet och dess inkapsling, kärnreaktorns kylkrets (primärkretsen) och reaktorinneslutningen.

Bränsle, reaktor, reaktorns primärkrets och tryckvattenreaktorns sekundärkrets, deras vattenkemi, inkapsling samt säkerhetsfunktioner ska planeras så att följande säkerhetsmål nås:

1) För tryggande av bränslets integritet ska
   - sannolikheten för att en bränsleskada uppstår vara liten i normal drift och vid förväntade driftstörningar,
   - antalet bränsleskador vid antagna olyckor vara litet och kylningen av bränslet inte få äventyras, och
   - möjligheten av att en kriticitetsolycka inträffar vara ytterst liten.
2) För tryggande av primär- och sekundärkretsens integritet ska
   - ett kärnkraftverks primärkrets planeras och byggas så att den uppfyller höga kvalitetskrav så att sannolikheten för skadliga fel i konstruktioner och mekanismer som hotar deras integritet är ytterst liten och att möjliga fel kan upptäckas på ett tillförlitligt sätt genom besiktningar,
   - ett kärnkraftverks primärkrets med tillräcklig marginal tåla de påfrestningar den utsätts för under normala driftsförhållanden, under förväntade driftstörningar, vid antagna olyckor och vid spridning av antagna olyckor,
   - ett kärnkraftverks primärkrets och de system som är direkt kopplade till den samt de delar i en tryckvattenreaktors sekundärkrets som är viktiga med tanke på säkerheten skyddas på ett tillförlitligt sätt mot förväntade driftsstörningar och alla olyckssituationer för att hindra skador på grund av övertryck, och
   - anläggningen förses med tillräckliga övervakningssystem för att upptäcka läckage.
3) För tryggande av reaktorinneslutningens integritet ska
   - reaktorinneslutningen planeras så att den bibehåller sin täthet vid förväntade driftsstörningar samt med stor säkerhet också i alla olyckssituationer,
   - vid planering av reaktorinneslutningen beaktas sådana tryck-, stråL- och värmebelastningar, brinnande gaser, flygande föremål samt kortvariga fenomen av hög energi som uppstår till följd av en olycka, och
   - möjligheten att reaktortryckkärlet skadas vid en allvarlig reaktorolycka så att reaktorinneslutningens integritet äventyras vara ytterst liten.

Kärnkraftverket ska förses med system som garanterar att den härdsmälta som uppstår vid en allvarlig reaktorolycka stabiliseras och kyls ned. En direkt kontakt mellan härdsmälta och den bärande konstruktionen i reaktorinneslutningen ska hindras på ett tillförlitligt sätt.

14 § Säkerhetsfunktioner och tryggande av dem
Vid tryggande av säkerhetsfunktioner ska i första hand utnyttjas naturliga säkerhetsegenskaper som kan uppnås med goda planeringslösningar. I

synnerhet ska samverkan av de fysikaliska återkopplingsfenomenen i kärnreaktorn vara sådan att den motverkar en ökning av reaktoreffekten.

Om naturliga säkerhetsegenskaper inte kan utnyttjas för att trygga en säkerhetsfunktion, ska sådana system och anordningar utnyttjas som inte kräver någon yttre drivkraft och som, om drivkraften går förlorad, ställer sig i ett ur säkerhetssynpunkt gynnsamt läge.

För att olyckor ska kunna hindras och deras följder lindras ska kärnkraftverket ha system för att stänga av reaktorn och kvarhålla den i subkritiskt tillstånd samt system för avlägsnande av den resteffektvärme som bildas i reaktorn och säkerställande av att radioaktiva ämnen stannar inom anläggningen.

Vid planeringen av ifrågavarande system ska principer som säkerställer att säkerhetsfunktionen träder i funktion också vid felsituationer följas. Sådana principer är mångfalds-, åtskillnads- och olikhetsprincipen.

De viktigaste system som behövs för övergång i kontrollerat läge och kvarhållandet av det ska kunna utföra sina funktioner även om en enskild komponent i vilket system som helst blir funktionsoduglig och även om vilken som helst annan komponent i samma system eller en komponent i ett stöd- eller hjälpsystem som är nödvändigt med tanke på dess funktion samtidigt är ur bruk på grund av behövliga reparationer eller underhåll.

De effekter som en gemensam felorsak i säkerhetssystemen har på anläggningens säkerhet ska vara ringa.

Kärnkraftverket ska ha matarsystem för yttre och inre eleffekt. Säkerhetsfunktionerna ska kunna genomföras med användning av vilketdera som helst av dessa elmatarsystem.

I syfte att kunna ha kontroll över och följa upp allvarliga reaktorolyckor ska planeras system, konstruktioner och anordningar som är oberoende av de system som är konstruerade för driftsituationer och antagna olyckor. De system som behövs för säkerställande av tätheten hos reaktorinneslutningen i samband med en allvarlig reaktorolycka ska vara kapabla att utföra sina säkerhetsfunktioner också i händelse av att det uppstår ett fel i en enskild anordning. Anläggningen ska planeras så att den kan ställas i ett säkert läge efter en allvarlig reaktorolycka.

YVL B.1 §423 – 426

YVL B.1 §430

YVL B.1 §432

YVL B.1 §443

YVL B.1 §457-459

YVL B.1 Appendix A §101-102

YVL B.1 Appendix B §144-145

YVL B.1 Appendix D §123

YVL B.1 403

YVL B.1 Appendix B §114-115

YVL B.1 Appendix D §106

Storbritannien

Övergripande principer

FP.6 Prevention of accidents
All reasonably practicable steps must be taken to prevent and mitigate nuclear or radiation accidents.

EKP.1 Inherent safety
The underpinning safety aim for any nuclear facility should be an inherently safe design, consistent with the operational purposes of the facility.

EKP.3 Defence in depth
A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several levels of protection.

EKP.5 Safety measures
Safety measures should be identified to deliver the required safety function(s).

EDR.1 Failure to safety
Due account should be taken of the need for structures, systems and components important to safety to be designed to be inherently safe or to fail in a safe manner and potential failure modes should be identified, using a formal analysis where appropriate.

EDR.2 Redundancy, diversity and segregation
Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.

ERL.1 Form of claims
The reliability claimed for any structure, system or component important to safety should take into account its novelty, the experience relevant to its proposed environment, and the uncertainties in operating and fault conditions, physical data and design methods.

ERL.2 Measures to achieve reliability
The measures whereby the claimed reliability of systems and components will be achieved in practice should be stated.

ERL.3 Engineered safety features
Where reliable and rapid protective action is required, automatically initiated engineered safety features should be provided.

ERL.4 Margins of conservatism
Where multiple safety-related systems and/or other means are claimed to reduce the frequency of a fault sequence, the reduction in frequency should have a margin of conservatism with allowance for uncertainties.

ESS.1 Requirement for safety systems
All nuclear facilities should be provided with safety systems that reduce the frequency or limit the consequences of fault sequences, and that achieve and maintain a defined safe state.

ESS.2 Determination of safety system requirements
The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and required reliabilities should be determined.

ESS.7 Diversity in the detection of fault sequences
The protection system should employ diversity in the detection of fault sequences, preferably by the use of different variables, and in the initiation of the safety system action to terminate the sequences.

ESS.8 Automatic initiation
A safety system should be automatically initiated and normally no human intervention should be necessary following the start of a requirement for protective action.

ESS.10 Definition of capability
The capability of a safety system, and of each of its constituent sub-systems and components, should be defined.

ESS.11 Demonstration of adequacy
The adequacy of the system design as the means of achieving the specified function and reliability should be demonstrated for each system.

ESS.12 Prevention of service infringement
Adequate provisions should be made to prevent the infringement of any service requirement of a safety system, its sub-systems and components.

ESS.16 No dependency on external sources of energy
Where practicable, following a safety system action, maintaining a safe facility state should not depend on an external source of energy.

ESS.17 Fault identification and assurance of safe state
Foreseeable faults within a safety system that could cause any single plant variable, or combination of variables, to change to significantly less safe values should be identified and, as necessary, avoidance measures or appropriate protective features provided.

ESS.18 Failure independence
No fault, internal or external hazard should disable a safety system.

ESS.19 Dedication to a single task
A safety system should be dedicated to the single task of performing its safety function.

ESS.20 Avoidance of connections to other systems
Connections between any part of a safety system (other than the safety system support features) and a system external to the plant should be avoided.

ESS.21 Reliability
The design of a safety system should avoid complexity, apply a fail-safe

approach and incorporate the means of revealing internal faults from the time of their occurrence.

ESS.22 Avoidance of spurious operation
A safety system should avoid spurious operation at a frequency that might directly or indirectly degrade safety.

ESS.23 Allowance for unavailability of equipment
In determining the safety system provisions, allowance should be made for the unavailability of equipment.

ERC.2 Shutdown systems
At least two diverse systems should be provided for shutting down a civil reactor.

EES.4 Sharing with other plants
Where essential services are shared with other plants on a multi-facility site, the effect of the sharing should be taken into account in assessing the adequacy of the supply.

EES.5 Cross-connections to other services
The capacity of the essential services to meet the demands of the supported safety functional requirement(s) should not be undermined by making cross-connections to services provided for non-safety functions.

EHF.2 Allocation of safety actions
When designing systems, the allocation of safety actions between humans and technology should be substantiated and dependence on human action to maintain a safe state should be minimised.

EHF.3 Identification of actions impacting safety
A systematic approach should be taken to identifying human actions that can impact on safety.

EHF.5 Task analysis
Analysis should be carried out of tasks important to safety to determine demands on personnel in terms of perception, decision making and action.

Vägledande råd

124 Interactions between facilities, between facilities and shared services and between shared services, where events in one may adversely affect others, should be explicitly considered in determining the potential for escalation of the risks for the site. This requires an analysis of events that can have physical effects outside the boundaries or limits for the particular

a) faults, internal hazards or external hazards that affect more than one facility and shared service at the same time;
b) domino effects that can progress directly from one facility to another or via shared services;
c) interactions between shared services that affect several facilities.

136 An ‘inherently safe’ design is one that avoids radiological hazards rather than controlling them. It prevents a specific harm occurring by using an approach, design or arrangement that ensures that the harm cannot happen,

for example a criticality safe vessel. Inherent safety is not the same as ‘passive safety’. Where inherently safe design is not achievable, the design should be fault tolerant.

139 Any failure, process perturbation or mal-operation in a facility should produce a change in plant state towards a safer condition, or produce no significant response. If the change is to a less safe condition, then systems should have long time constants so that key parameters deviate only slowly from their desired values.

140 International consensus is that the appropriate strategy for achieving the overall safety objective is through the application of the concept of defence in depth. This should provide a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails.

141 The levels of protection should prevent faults, or if prevention fails should ensure detection, limit the potential consequences and prevent escalation.

142 The concept of defence in depth should be applied so that:

a) deviations from normal operation and failures of structures, systems and components important to safety are prevented;
b) any deviations from normal operation are allowed for by safety margins that enable detection and action that prevents escalation;
c) inherent safety features of the facility, fail-safe design and safety measures are provided to prevent fault conditions that occur from progressing to accidents;
d) additional measures are provided to mitigate the consequences of severe accidents.

Table 1 Objective of each level of protection and essential means of achieving them

Level	Objective	Essential means
Level 1	Prevention of abnormal operation and failures by design	Conservative design, construction, maintenance and operation in accordance with appropriate safety margins, engineering practices and quality levels
Level 2	Prevention and control of abnormal operation and detection of failures	Control, indication, alarm systems or other systems and operating procedures to prevent or minimise damage from failures
Level 3	Control of faults within the	Engineered safety features, multiple barriers and

	design basis	accident or fault control procedures
Level 4	Control of severe plant conditions in which the design basis may be exceeded, including the prevention of fault progression and mitigation of the consequences of severe accidents	Additional measures and procedures to prevent or mitigate fault progression and for accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive substances	Emergency control and on- and off-site emergency response

143 Defence in depth is generally applied in five levels. The methodology ensures that if one level fails, it will be compensated for, or corrected by, the subsequent level. The aims for each level of protection are described in detail in IAEA Safety Standard NS-R-19, on which Table 1 is based. It should be noted that Table 1 deals with the application of defence in depth in the design of a facility, and does not deal with other important contributions such as human performance or equipment reliability. These topics are addressed in other sections of the SAPs.

144 An important aspect of the implementation of defence in depth is the provision of multiple, and as far as possible independent, barriers to the release of radioactive substances to the environment, and to ensure the confinement of radioactive substances at specified locations. The number of barriers will depend on the magnitude of the radiological hazard and the consequences of failure.

146 Safety should be secured by characteristics as near as possible to the top of the list below:

a) Passive safety measures that do not rely on control systems, active safety systems or human intervention.
b) Automatically initiated active engineered safety measures.
c) Active engineered safety measures that need to be manually brought into service in response to the fault.
d) Administrative safety measures (see paragraph 376 f.).
e) Mitigation safety measures (eg filtration or scrubbing).

Note: The hierarchy above should not be interpreted to mean that the provision of an item towards the top of the list precludes provision of other items where they can contribute to defence in depth.

166 Engineered structures, systems and components should be designed to deliver their required safety functions with adequate reliability, according to

the magnitude and frequency of the radiological hazard, to provide confidence in the robustness of the overall design.

168 The design should incorporate redundancy to avoid the effects of random failure, and diversity and segregation to avoid the effects of common cause failure. Examples of diversity are different operating conditions, different working principles or different design teams, different sizes of equipment, different manufacturers, different components, and types of equipment that use different physical methods. The design should also be tolerant of random failure occurring anywhere within the safety systems provided to secure each safety function.

167 The design should incorporate redundancy to avoid the effects of random failure, and diversity and segregation to avoid the effects of common cause failure. Examples of diversity are different operating conditions, different working principles or different design teams, different sizes of equipment, different manufacturers, different components, and types of equipment that use different physical methods. The design should also be tolerant of random failure occurring anywhere within the safety systems provided to secure each safety function.

180 For requirements that are less demanding or on a longer timescale, operator actions or administrative control may be acceptable to complement the engineered systems. The objective should be to minimise the dependence on human action to maintain a safe state.

336 A reactor should be provided with safety systems that can shut it down safely in normal operating and fault conditions and maintain it in the shutdown condition. There should be a margin of reactivity that allows for systematic changes and uncertainties in nuclear characteristics, variations in plant state and other processes or mechanisms that might affect the reactivity of the core, even for the most reactive conditions of the core.

347 Infringement of any service would include removal or degradation of support services such as power supplies, instrument air, environment etc.

348 Where prevention, or acceptably low likelihood, of infringement cannot be demonstrated, features should be incorporated to ensure a fail-safe outcome.

351 This principle is aimed at ensuring that the plant remains safe following the occurrence of foreseeable safety system faults. This includes, but is not limited to, the placement of the safety system in a fail-safe state, where practicable and achievable, following the detection of safety system faults.

352 Safety systems should be physically separate, independent, isolated from other systems, including safety-related systems, and share no equipment or services. There should be adequate segregation between independent parts of the safety system (including pipework and cabling) and also between a safety system and other facility equipment that, in the event of a fault, might jeopardise the safe working of the safety system.

353 Where it is necessary for other functions to be encompassed, the whole system should be classified as a safety system and the safety function should not be jeopardised by the other functions.

354 If connections external to the plant cannot be avoided, for electrical, electronic or computer-based safety systems they should be restricted in function to that of monitoring only, and should incorporate adequate isolation features so that no fault associated with that equipment or its connections would jeopardise the function of the safety system.

355 Where this principle cannot be achieved because of the use of complex hardware, the elements of a safety demonstration should be determined. The demonstration should include:

a) a comprehensive examination of all the relevant scientific and technical issues;
b) a review of precedents set under comparable circumstances in the past;
c) an independent third-party assessment in addition to the normal checks and conventional design;
d) periodic review of further developments in technical information, precedent and best practice.

356 The nature of some systems may be such that it is not possible to reveal all faults until the time of a test, eg in the case of fluid or mechanical systems. In such cases, in-service or periodic testing will be the sole means available to support reliability claims for the equipment, see Principle EMT.6 *(paragraph 189 f.)*.

372 It should be shown that the safety requirements for all facilities are met for all operational states (including maintenance) and fault conditions.

373 Where such cross-connections are necessary, provisions should be made to isolate the essential services from these other services so that the essential services can meet their safety functional requirements.

Kanada

Krav

RD–337, 4.3.1 Defence-in-depth
The concept of defence-in-depth is applied to all organizational, behavioural, and design-related safety and security activities to ensure that they are subject to overlapping provisions. With the defence-in-depth approach, if a failure were to occur it will be detected and compensation made, or it would be corrected.

This concept is applied throughout the design process and operation of the plant to provide a series of levels of defence aimed at preventing accidents, and ensuring appropriate protection in the event that prevention fails.

The design provides all five levels of defence during normal operation; however, some relaxations may be specified for certain shutdown states.

These levels are introduced in general terms below, and are discussed in greater detail in subsection 6.1.

Level One
The aim of the first level of defence is to prevent deviations from normal operation, and to prevent failures of systems, structures, and components (SSCs).

Level Two
The aim of the second level of defence is to detect and intercept deviations from normal operation in order to prevent AOOs from escalating to accident conditions, and to return the plant to a state of normal operation.

Level Three
The aim of the third level of defence is to minimize the consequences of accidents by providing inherent safety features, fail-safe design, additional equipment, and mitigating procedures.

Level Four
The aim of the fourth level of defence is to ensure that radioactive releases caused by severe accidents are kept as low as practicable.

Level Five
The aim of the fifth level of defence is to mitigate the radiological consequences of potential releases of radioactive materials that may result from accident conditions.

RD–337, 4.3.2 Consideration of Physical Barriers
An important aspect of implementing defence-in-depth in the NPP design is the provision of a series of physical barriers to confine radioactive material at specified locations.

RD–337, 5.4 Proven Engineering Practices
The design authority identifies the modern standards and codes that will be used for the plant design, and evaluates those standards and codes for applicability, adequacy, and sufficiency to the design of SSCs important to safety.

Where needed, codes and standards may be supplemented or modified to ensure that the final quality of the design is commensurate with the necessary safety functions.

SSCs important to safety are of proven designs, and are designed according to the standards and codes identified for the NPP.

Where a new SSC design, feature, or engineering practice is introduced, adequate safety is proven by a combination of supporting research and development programs, and by examination of relevant experience from similar applications. An adequate qualification program is established to verify that the new design meets all applicable safety expectations. New designs are tested before being brought into service, and are then monitored in service to verify that the expected behaviour is achieved.

The design authority establishes an adequate qualification program to verify that the new design meets all applicable safety design requirements.

In the selection of equipment, due attention is given to spurious operation and to unsafe failure modes (e.g., failure to trip when necessary). Where the design has to accommodate an SSC failure, preference is given to equipment that exhibits known and predictable modes of failure, and that facilitates repair or replacement.

RD–337, 6.1 Application of Defence-in-depth
Defence-in-depth is achieved at the design phase through application of design provisions specific to the five levels of defence.

Level One
Achievement of defence-in-depth level one calls for conservative design and high-quality construction to provide confidence that plant failures and deviations from normal operations are minimized and accidents are prevented.

This entails careful attention to selection of appropriate design codes and materials, design procedures, equipment qualification, control of component fabrication and plant construction, and use of operational experience.

Level Two
Defence-in-depth level two is achieved by controlling plant behaviour during and following a PIE using both inherent and engineered design features to minimize or exclude uncontrolled transients to the extent possible.

Level Three
Achievement of defence-in-depth level three calls for provision of inherent safety features, fail safe design, engineered design features, and procedures that minimize the consequences of DBAs. These provisions are capable of leading the plant first to a controlled state, and then to a safe shutdown state, and maintaining at least one barrier for the confinement of radioactive material. Automatic activation of the engineered design features minimizes the need for operator actions in the early phase of a DBA.

Level Four
Defence-in-depth level four is achieved by providing equipment and procedures to manage accidents and mitigate their consequences as far as practicable.

Most importantly, adequate protection is provided for the confinement function by way of a robust containment design. This includes the use of complementary design features to prevent accident progression and to mitigate the consequences of selected severe accidents. The confinement function is further protected by severe accident management procedures.

Level Five
The design provides an adequately equipped emergency support centre, and plans for on-site and off-site emergency response.

RD–337, 6.1.1 Consideration of Physical Barriers
To ensure maintenance of the overall safety concept of defence-in-depth, the design provides multiple physical barriers to the uncontrolled release of radioactive materials to the environment. Such barriers include the fuel

matrix, the fuel cladding, the reactor coolant pressure boundary, and the containment. In addition, the design provides for an exclusion zone.

To the extent practicable, the design therefore prevents:

1. Challenges to the integrity of physical barriers;
2. Failure of a barrier when challenged; and
3. Failure of a barrier as a consequence of failure of another barrier.

The design also allows for the fact that the existence of multiple levels of defence is not a sufficient basis for continued power operation in the absence of one defence level.

RD–337, 6.3 Accident Prevention and Plant Safety Characteristics
The design applies the principles of defence-in-depth to minimize sensitivity to PIEs. Following a PIE, the plant is rendered safe by:

1. Inherent safety features;
2. Passive safety features, or action of control systems;
3. Action of safety systems; or
4. Specified procedural actions.

RD–337, 7.22.1 Design Principles
The design is such that the NPP and any other on-site facilities with potential to release large amounts of radioactive material or energy are protected against malevolent acts.

Threats from credible malevolent acts are referred to as DBTs. More severe but unlikely threats are referred to as beyond design basis threats (BDBTs). Both types of threats are considered in the design.

Threats identified as DBTs have credible attributes and characteristics of a potential insider or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage against which a physical protection system is designed and evaluated.

BDBTs are threats too unlikely to warrant incorporation into the design basis, but for which the consequences are assessed in order to establish means of mitigation to the extent practicable.

Consistent with the concept of defence-in-depth, the design provides multiple barriers for protection against malevolent acts, including physical protection systems, engineered safety provisions, and measures for post-event management, as appropriate. The failure of a preceding barrier should not compromise the integrity and effectiveness of subsequent barriers.

RD–337, 7.6.1 Common-cause Failures
Failure of a number of devices or components to perform their functions may occur as a result of a single specific event or cause. Common-cause failures may also occur when multiple components of the same type fail at the same time. This may be caused by such occurrences as a change in ambient conditions, saturation of signals, repeated maintenance error or design deficiency.

The potential for common-cause failures of items important to safety is considered in determining where to apply the principles of diversity,

separation, and independence to achieve the necessary reliability. Such failures may simultaneously affect a number of different items important to safety. The event or cause may be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human-induced event, or an unintended cascading effect from any other operation or failure within the plant.

The design provides sufficient physical separation between redundant divisions of safety support systems and process systems. This applies to equipment and to routing of the following items:

1. Electrical cables for power and control of equipment;
2. Piping for service water for the cooling of fuel and process equipment; and
3. Tubing and piping for compressed air or hydraulic drives for control equipment.

Where physical separation is not possible, safety support system equipment may share physical space. In such cases, the reasons for the lack of separation and justification for the space sharing arrangement is explained in the design documentation.

Where space sharing is necessary, services for safety and for other important process systems are arranged in a manner that incorporates the following considerations:

1. A safety system designed to act as backup is not located in the same space as the primary safety system; and
2. If a safety system and a process system must share space, then the associated safety functions are also provided by another safety system to counter the possibility of failures in the process system.

The design provides effective protection against common-cause events where sufficient physical separation among individual services or groups of services does not exist. The design authority assesses the effectiveness of specified physical separation or protective measures against common-cause events.

Diversity is applied to redundant systems or components that perform the same safety function by incorporating different attributes into the systems or components. Such attributes include different principles of operation, different physical variables, different conditions of operation, or production by different manufacturers.

It is important that any diversity used actually achieves the desired increase in reliability. For example, to reduce the potential for common-cause failures, the application of diversity is examined for any similarity in materials, components, and manufacturing processes, or subtle similarities in operating principles or common support features. If diverse components or systems are used, there should be a reasonable assurance that such additions are of overall benefit, taking into account associated disadvantages such as the extra complication in operational, maintenance, and test procedures, or the consequent use of equipment of lower reliability.

RD–337, 7.6.2 Single Failure Criterion
All safety groups function in the presence of a single failure. The single failure criterion requires that each safety group perform all safety functions required for a PIE in the presence of any single component failure, and:

1. All failures caused by that single failure;
2. All identifiable but non-detectable failures, including those in the non-tested components; and
3. All failures and spurious system actions that cause (or are caused by) the PIE.

Each safety group is able to perform the required safety functions under the worst permissible systems configuration, taking into account such considerations as maintenance, testing, inspection and repair, and equipment outage.

Analysis of all possible single failures, and all associated consequential failures, is conducted for each element of each safety group until all safety groups have been considered.

Unintended actions and failure of passive components are considered as two of the modes of failure of a safety group.

The single failure is assumed to occur prior to the PIE, or at any time during the mission time for which the safety group is required to function following the PIE. Passive components may be exempt from this expectation.

Exemptions for passive components apply only to those components that are designed and manufactured to high standards of quality, that are adequately inspected and maintained in service, and that remain unaffected by the PIE. Design documentation includes analytical justification of such exemptions, taking loads and environmental conditions into account, as well as the total period of time after the PIE for which the functioning of the component is necessary.

Check valves are active components if they must change state following a PIE.

Exceptions to the single failure criterion are infrequent, and clearly justified.

RD–337, 7.6.3 Fail-safe Design
The principle of fail-safe design is applied to the design of SSCs important to safety. To the greatest extent practicable, application of this principle enables plant systems to pass into a safe state if a system or component fails, with no necessity for any action to be taken.

RD–337, 7.6.5 Shared Systems
In cases where a system performs both process functions and safety functions, the following design considerations apply:

1. The process and safety functions are not required or credited at the same time;
2. If the process function is operating, and a PIE in that system is postulated, it can be shown that all essential safety functions of the system that are required to mitigate the PIE are unaffected;

3. The system is designed to the standards of the function of higher importance with respect to safety;
4. If the process function is used intermittently, then the availability of the safety function after each use, and its continued ability to meet expectations, can be demonstrated by testing; and
5. The expectations for instrumentation sharing are met.

Shared Instrumentation for Safety Systems
Instrumentation is not typically shared between safety systems.

Where justified, there may be sharing between a safety system and a non-safety system (such as a process or control system).

Reliability and effectiveness of a safety system will not be impaired by normal operation, by partial or complete failure in other systems, or by any cross-link generated by the proposed sharing.

The design includes provisions to ensure that the sharing of instruments does not result in an increased frequency in demand on the safety system during operation.

The design provides for periodic testing of the entire channel of instrumentation logic, from sensing device to actuating device.

If the design includes sharing of instrumentation between a safety system and a non-safety system, then the following expectations apply:

1. Sharing is limited to the sensing devices and their pre-amplifiers or amplifiers as needed to get the signal to the point of processing;
2. The signal from each sensing device is electrically isolated so that failures cannot be propagated from one system to the other; and
3. Isolation devices between systems of different safety importance are always associated with the system classified as being of greater importance to safety.

Sharing of SSCs between Reactors
SSCs important to safety are typically not shared between two or more reactors.

In exceptional cases when SSCs are shared between two or more reactors, such sharing excludes safety systems and turbine generator buildings that contain high-pressure steam and feedwater systems.

If sharing of SSCs between reactors is arranged, then the following expectations apply:

1. All safety requirements are met for all reactors during normal operation, AOOs, and DBAs; and
2. In the event of an accident involving one of the reactors, orderly shutdown, cool down, and removal of residual heat is achievable for the other reactor(s).

When an NPP is under construction adjacent to an operating plant, and sharing of SSCs between reactors has been justified, the availability of the SSCs and their capacity to meet all safety requirements for the operating units is assessed during the construction phase.

USA

Krav

10 CFR 50 Appendix A, Criterion 22, Protection system independence.
The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

10 CFR 50 Appendix A, Criterion 24, Separation of protection and control systems.
The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

10 CFR 50 Appendix A, Criterion 26, Reactivity control system redundancy and capability.
Two independent reactivity control systems of different design principles shall be provided. One of the systems shall use control rods, preferably including a positive means for inserting the rods, and shall be capable of reliably controlling reactivity changes to assure that under conditions of normal operation, including anticipated operational occurrences, and with appropriate margin for malfunctions such as stuck rods, specified acceptable fuel design limits are not exceeded. The second reactivity control system shall be capable of reliably controlling the rate of reactivity changes resulting from planned, normal power changes (including xenon burnout) to assure acceptable fuel design limits are not exceeded. One of the systems shall be capable of holding the reactor core subcritical under cold conditions.

10 CFR 50 Appendix A, Criterion 34, Residual heat removal.
A system to remove residual heat shall be provided. The system safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified acceptable fuel design limits and the design conditions of the reactor coolant pressure boundary are not exceeded.

Suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

10 CFR 50 Appendix A, Criterion 35, Emergency core cooling.
A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts.

Suitable redundancy in components and features, and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

10 CFR 50 Appendix A, Criterion 38, Containment heat removal.
A system to remove heat from the reactor containment shall be provided. The system safety function shall be to reduce rapidly, consistent with the functioning of other associated systems, the containment pressure and temperature following any loss-of-coolant accident and maintain them at acceptably low levels.

10 CFR 50 Appendix A, Criterion 44, Cooling water.
A system to transfer heat from structures, systems, and components important to safety, to an ultimate heat sink shall be provided. The system safety function shall be to transfer the combined heat load of these structures, systems, and components under normal operating and accident conditions.

Suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

10 CFR 50 Appendix A, Criterion 23, Protection system failure modes.
The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.

10 CFR 50 Appendix A, Criterion 24, Separation of protection and control systems.
The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

10 CFR 50 Appendix A, Criterion 5, Sharing of SSC.
SSC important to safety shall not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and cooldown of the remaining units.

§50.62 (c) Requirements.
Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system.

Each boiling water reactor must have an alternate rod injection (ARI) system that is diverse (from the reactor trip system) from sensor output to the final actuation device. The ARI system must have redundant scram air header exhaust valves. The ARI must be designed to perform its function in a reliable manner and be independent (from the existing reactor trip system) from sensor output to the final actuation device.

Each boiling water reactor must have a standby liquid control system (SLCS) with the capability of injecting into the reactor pressure vessel a borated water solution at such a flow rate, level of boron concentration and boron-10 isotope enrichment, and accounting for reactor pressure vessel volume, that the resulting reactivity control is at least equivalent to that resulting from injection of 86 gallons per minute of 13 weight percent sodium pentaborate decahydrate solution at the natural boron-10 isotope abundance into a 251-inch inside diameter reactor pressure vessel for a given core design. The SLCS and its injection location must be designed to perform its function in a reliable manner. The SLCS initiation must be automatic and must be designed to perform its function in a reliable manner for plants granted a construction permit after July 26, 1984, and for plants granted a construction permit prior to July 26, 1984, that have already been designed and built to include this feature.

Each boiling water reactor must have equipment to trip the reactor coolant recirculating pumps automatically under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 7: Application of defence in depth
The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable.

IAEA Safety Standard, No. SSR-2/1, Requirement 21: Physical separation and independence of safety systems
Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.

IAEA Safety Standard, No. SSR-2/1, Requirement 22: Safety classification
All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance.

IAEA Safety Standard, No. SSR-2/1, Requirement 24: Common cause failures
The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.

IAEA Safety Standard, No. SSR-2/1, Requirement 26: Fail-safe design
The concept of fail-safe design shall be incorporated, as appropriate, into the design of systems and components important to safety.

IAEA Safety Standard, No. SSR-2/1, Requirement 33: Sharing of safety systems between multiple units of a nuclear power plant
Safety systems shall not be shared between multiple units unless this contributes to enhanced safety.

IAEA Safety Standard, No. SSR-2/1, Requirement 39: Prevention of unauthorized access to, or interference with, items important to safety.
Unauthorized access to, or interference with, items important to safety, including computer hardware and software, shall be prevented.

IAEA Safety Standard, No. SSR-2/1, Requirement 40: Prevention of harmful interactions of systems important to Safety
The potential for harmful interactions of systems important to safety at the nuclear power plant that might be required to operate simultaneously shall be evaluated, and effects of any harmful interactions shall be prevented.

IAEA Safety Standard, No. SSR-2/1, Requirement 41: Interactions between the electrical power grid and the Plant
The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply.

IAEA Safety Standard, No. SSR-2/1, Requirement 42: Safety analysis of the plant design
A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed.

IAEA Safety Standard, No. SSR-2/1, 2.12
The primary means of preventing accidents in a nuclear power plant and

mitigating the consequences of accidents if they do occur is the application of the concept of defence in depth [1, 5, 6]. This concept is applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states. This is to ensure that all safety related activities are subject to independent layers of provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. Application of the concept of defence in depth throughout design and operation provides protection against anticipated operational occurrences and accidents, including those resulting from equipment failure or human induced events within the plant, and against consequences of events that originate outside the plant.

IAEA Safety Standard, No. SSR-2/1, 2.13
Application of the concept of defence in depth in the design of a nuclear power plant provides several levels of defence (inherent features, equipment and procedures) aimed at preventing harmful effects of radiation on people and the environment, and ensuring adequate protection from harmful effects and mitigation of the consequences in the event that prevention fails. The independent effectiveness of each of the different levels of defence is an essential element of defence in depth at the plant and this is achieved by incorporating measures to avoid the failure of one level of defence causing the failure of other levels. There are five levels of defence:

(a) The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety. This leads to requirements that the plant be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices. To meet these objectives, careful attention is paid to the selection of appropriate design codes and materials, and to the quality control of the manufacture of components and construction of the plant, as well as to its commissioning. Design options that reduce the potential for internal hazards contribute to the prevention of accidents at this level of defence. Attention is also paid to the processes and procedures involved in design, manufacture, construction and in-service inspection, maintenance and testing, to the ease of access for these activities, and to the way the plant is operated and to how operating experience is utilized. This process is supported by a detailed analysis that determines the requirements for operation and maintenance of the plant and the requirements for quality management for operational and maintenance practices.
(b) The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions. This is in recognition of the fact that postulated initiating events are likely to occur over the operating lifetime of a nuclear power plant, despite the care taken to prevent them. This second level of defence necessitates the provision of specific systems and features in the design, the confirmation of their

effectiveness through safety analysis, and the establishment of operating procedures to prevent such initiating events, or else to minimize their consequences, and to return the plant to a safe state.

(c) For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding level and that an accident could develop. In the design of the plant, such accidents are postulated to occur. This leads to the requirement that inherent and/or engineered safety features, safety systems and procedures be provided that are capable of preventing damage to the reactor core or significant off-site releases and returning the plant to a safe state.

(d) The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. The most important objective for this level is to ensure the confinement function, thus ensuring that radioactive releases are kept as low as reasonably achievable.

(e) The purpose of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accident conditions. This requires the provision of an adequately equipped emergency control centre and emergency plans and emergency procedures for on-site and off-site emergency response.

IAEA Safety Standard, No. SSR-2/1, 2.14
A relevant aspect of the implementation of defence in depth for a nuclear power plant is the provision in the design of a series of physical barriers, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations. The number of barriers that will be necessary will depend upon the initial source term in terms of amount and isotopic composition of radionuclides, the effectiveness of the individual barriers, the possible internal and external hazards, and the potential consequences of failures.

IAEA Safety Standard, No. SSR-2/1, 4.9
The defence in depth concept shall be applied to provide several levels of defence that are aimed at preventing consequences of accidents that could lead to harmful effects on people and the environment, and ensuring that appropriate measures are taken for the protection of people and the environment and for the mitigation of consequences in the event that prevention fails.

IAEA Safety Standard, No. SSR-2/1, 4.10
The design shall take due account of the fact that the existence of multiple levels of defence is not a basis for continued operation in the absence of one level of defence. All levels of defence in depth shall be kept available at all times and any relaxations shall be justified for specific modes of operation.

IAEA Safety Standard, No. SSR-2/1, 4.11
The design:

(a) Shall provide for multiple physical barriers to the release of radioactive material to the environment;
(b) Shall be conservative, and the construction shall be of high quality, so as to provide assurance that failures and deviations from normal operation are minimized, that accidents are prevented as far as is practicable and that a small deviation in a plant parameter does not lead to a cliff edge effect;
(c) Shall provide for the control of plant behaviour by means of inherent and engineered features, such that failures and deviations from normal operation requiring actuation of safety systems are minimized or excluded by design, to the extent possible;
(d) Shall provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures and deviations from normal operation that exceed the capability of control systems can be controlled with a high level of confidence, and the need for operator actions in the early phase of these failures or deviations from normal operation is minimized;
(e) Shall provide for systems, structures and components and procedures to control the course of and, as far as practicable, to limit the consequences of failures and deviations from normal operation that exceed the capability of safety systems;
(f) Shall provide multiple means for ensuring that each of the fundamental safety functions is performed, thereby ensuring the effectiveness of the barriers and mitigating the consequences of any failure or deviation from normal operation.

IAEA Safety Standard, No. SSR-2/1, 4.12
To ensure that the concept of defence in depth is maintained, the design shall prevent, as far as is practicable:

(a) Challenges to the integrity of physical barriers;
(b) Failure of one or more barriers;
(c) Failure of a barrier as a consequence of the failure of another barrier;
(d) The possibility of harmful consequences of errors in operation and maintenance.

IAEA Safety Standard, No. SSR-2/1, 4.13
The design shall be such as to ensure, as far as is practicable, that the first, or at most the second, level of defence is capable of preventing an escalation to accident conditions for all failures or deviations from normal operation that are likely to occur over the operating lifetime of the nuclear power plant.

IAEA Safety Standard, No. SSR-2/1, 5.8
The expected behaviour of the plant in any postulated initiating event shall be such that the following conditions can be achieved, in order of priority:

(1) A postulated initiating event would produce no safety significant effects or would produce only a change towards safe plant conditions by means of inherent characteristics of the plant.
(2) Following a postulated initiating event, the plant would be rendered safe by means of passive safety features or by the action of systems

that are operating continuously in the state necessary to control the postulated initiating event.

(3) Following a postulated initiating event, the plant would be rendered safe by the actuation of safety systems that need to be brought into operation in response to the postulated initiating event.

(4) Following a postulated initiating event, the plant would be rendered safe by following specified procedures.

IAEA Safety Standard, No. SSR-2/1, 5.23
Methods to ensure a robust design shall be applied, and proven engineering practices shall be adhered to in the design of a nuclear power plant to ensure that the fundamental safety functions are achieved for all operational states and for all accident conditions.

IAEA Safety Standard, No. SSR-2/1, 5.33
Safety system equipment (including cables and raceways) shall be readily identifiable in the plant for each redundant element of a safety system.

IAEA Safety Standard, No. SSR-2/1, 5.35
The design shall be such as to ensure that any interference between items important to safety will be prevented, and in particular that any failure of items important to safety in a system in a lower safety class will not propagate to a system in a higher safety class.

IAEA Safety Standard, No. SSR-2/1, 5.36
Equipment that performs multiple functions shall be classified in a safety class that is consistent with the most important function performed by the equipment.

IAEA Safety Standard, No. SSR-2/1, 5.41
Systems and components important to safety shall be designed for fail-safe behaviour, as appropriate, so that their failure or the failure of a support feature does not prevent the performance of the intended safety function.

IAEA Safety Standard, No. SSR-2/1, 5.43
It shall not be permissible for a failure of a support service system to be capable of simultaneously affecting redundant parts of a safety system or a system fulfilling diverse safety functions and compromising the capability of these systems to fulfil their safety functions.

IAEA Safety Standard, No. SSR-2/1, 5.63
Safety system support features and safety related items shall be permitted to be shared between several units of a nuclear power plant if this contributes to safety. Such sharing shall not be permitted if it would increase either the likelihood or the consequences of an accident at any unit of the plant.

IAEA Safety Standard, No. SSR-2/1, 6.32.
The protection system shall be designed:

(a) To be capable of overriding unsafe actions of the control system;
(b) With fail-safe characteristics to achieve safe plant conditions in the event of failure of the protection system.

IAEA Safety Standard, No. SSR-2/1, 6.34
Design techniques [for instrumentation and control systems] such as testability, including a self-checking capability where necessary, fail-safe characteristics, functional diversity and diversity in component design and in concepts of operation shall be used to the extent practicable to prevent loss of a safety function.

IAEA Safety Standard, No. SSR-2/1, 6.36
When a safety system, or part of a safety system [within the instrumentation and control systems], has to be taken out of service for testing, adequate provision shall be made for the clear indication of any protection system bypasses that are necessary for the duration of the testing or maintenance activities.

Krav avseende rådrum vid manuella åtgärder

Sverige

Krav

4 § Vid utformningen av reaktorns djupförsvar ska följande konstruktionsprinciper tillämpas i den omfattning som är möjlig och rimlig:
… Manuella åtgärder vid nödvändiga aktiveringar och driftomläggningar av reaktorns säkerhetsfunktioner får tillämpas endast om personalen ges tillräcklig tid - rådrum - för att genomföra åtgärderna på ett säkert sätt.

Finland

Krav

19 § Övervakning och styrning av kärnkraftverk
I kärnkraftverkets kontrollrum ska finnas anordningar som ger uppgifter om kärnreaktorns tillstånd och visar eventuella avvikelser från det normala. I kärnkraftverk ska finnas automatiska system som ser till att säkerhetsfunktionerna blir påkopplade vid behov samt som styr och övervakar deras funktion vid driftstörningar och olyckor.

De automatiska systemen ska ha förmåga att hålla kraftverket under kontroll så pass länge att reaktoroperatörerna får tillräckligt med betänketid för att vidta rätta åtgärder.

I kärnkraftverk ska finnas en av kontrollrummet oberoende reservkontrollcentral och nödvändiga lokala styrsystem som gör det möjligt att stänga av och kyla ned kärnreaktorn samt att avlägsna resteffekten i bränslet i reaktorn och i det använda bränsle som upplagras i anläggningen.

Storbritannien

Övergripande principer

ESS.9 Time for human intervention
Where human intervention is necessary following the start of a requirement for protective action, then the time before such intervention is required should be demonstrated to be sufficient.

Vägledande råd

180 For requirements that are less demanding or on a longer timescale, operator actions or administrative control may be acceptable to complement the engineered systems. The objective should be to minimise the dependence on human action to maintain a safe state.

344 The practice on UK civil nuclear power reactor facilities is that no human intervention should be necessary for approximately 30 minutes following the start of a requirement for protective action. It would be expected that this practice continues to be met.

Kanada

Krav

RD–337, 7.3.3 Design Basis Accidents
The set of design basis accidents sets the boundary conditions according to which SSCs important to safety are designed.

The design is such that releases to the public following a DBA will not exceed the dose acceptance criteria.

In order to prevent progression to a more severe condition that may threaten the next barrier, the design includes provision to automatically initiate the necessary safety systems where prompt and reliable action is required in response to a PIE.

Provision is also made to support timely detection of, and manual response to, conditions where prompt action is not necessary. This includes such responses as manual initiation of systems or other operator actions.

The design takes into account operator actions that may be necessary to diagnose the state of the plant and to put it into a stable long-term shutdown condition in a timely manner. Such operator actions are facilitated by the provision of adequate instrumentation to monitor plant status, and controls for manual operation of equipment.

Any equipment necessary for manual response and recovery processes is placed at the most suitable location to allow safe and timely worker access when needed.

RD–337, 8.4.3 Monitoring and Operator Action
Once automatic shutdown is initiated, it is impossible for an operator to prevent its actuation.

The need for manual shutdown actuation is minimized.

The means for monitoring shutdown status and manual actuation is provided in the main control room.

RD–337, 8.10.4 Equipment Requirements for Accident Conditions
If operator action is required for actuation of any safety system or safety support system equipment, all of the following expectations apply:

1. There are clear, well-defined, validated, and readily available operating procedures that identify the necessary actions;
2. There is instrumentation in the control rooms to provide clear and unambiguous indication of the necessity for operator action;
3. Following indication of the necessity for operator action inside the MCR, there is at least 15 minutes available before the operator action is required; and
4. Following indication of the necessity for operator action outside the MCR, there is a minimum of 30 minutes available before the operator action is required.

Alternative action times may be used if justified, making due allowance for the complexity of the action to be taken, and for the time needed for such activities as the diagnosing the event and accessing to the remote station.

For automatically initiated safety systems and control logic actions, the design facilitates backup manual initiation from inside the appropriate control room.

USA

Guide

RG 1.62 "Manual Initiation of Protective Actions".
This RG provides an acceptable method for establishing the design criteria for existing I&C systems and for establishing the design criteria for digital and advanced analog systems for the manual initiation of protective actions.

RG 1.152 "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants":
"The design techniques of functional diversity, design diversity, diversity in operation, and diversity within the four echelons of defense in depth (provided by the reactor protection, engineered safety features actuation, control, and monitoring I&C systems) can be applied as defense against common-cause failures. Manual operator actuations of safety and nonsafety systems are acceptable, provided that the necessary diverse controls and indications are available to perform the required function under the associated event conditions and within the acceptable time".

Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition — Human Factors Engineering (NUREG-0800, Chapter 18).

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 61: Protection system
A protection system shall be provided at the nuclear power plant that has the capability to detect unsafe plant conditions and to initiate safety actions automatically to actuate the safety systems necessary for achieving and maintaining safe plant conditions.

IAEA Safety Standard, No. SSR-2/1, 4.11
The design:

(g) Shall provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures and deviations from normal operation that exceed the capability of control systems can be controlled with a high level of confidence, and the need for operator actions in the early phase of these failures or deviations from normal operation is minimized;

IAEA Safety Standard, No. SSR-2/1, 5.11
Where prompt and reliable action would be necessary in response to a postulated initiating event, provision shall be made in the design for automatic safety actions for the necessary actuation of safety systems, to prevent progression to more severe plant conditions.

IAEA Safety Standard, No. SSR-2/1, 5.12
Where prompt action in response to a postulated initiating event would not be necessary, it is permissible for reliance to be placed on the manual initiation of systems or on other operator actions. For such cases, the time interval between detection of the abnormal event or accident and the required action shall be sufficiently long, and adequate procedures (such as administrative, operational and emergency procedures) shall be specified to ensure the performance of such actions. An assessment shall be made of the potential for an operator to worsen an event sequence through erroneous operation of equipment or incorrect diagnosis of the necessary recovery process.

IAEA Safety Standard, No. SSR-2/1, 5.13
The operator actions that would be necessary to diagnose the state of the plant following a postulated initiating event and to put it into a stable long term shutdown condition in a timely manner shall be facilitated by the provision of adequate instrumentation to monitor the status of the plant, and adequate controls for the manual operation of equipment.

IAEA Safety Standard, No. SSR-2/1, 5.58
The design shall be such as to promote the success of operator actions with due regard for the time available for action, the conditions to be expected and the psychological demands being made on the operator.

IAEA Safety Standard, No. SSR-2/1, 5.59
The need for intervention by the operator on a short time scale shall be kept to a minimum, and it shall be demonstrated that the operator has sufficient time to make a decision and sufficient time to act.

IAEA Safety Standard, No. SSR-2/1, 6.33
The design [Protection system]:

(b) Shall automate various safety actions to actuate safety systems so that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or accident conditions;

Krav avseende reaktorinneslutningen

Sverige

Krav

5 § Kärnkraftsreaktorns inneslutning ska vara konstruerad med beaktande av fenomen och belastningar som kan uppstå vid händelser i händelseklassen mycket osannolika händelser i den utsträckning som behövs för att begränsa utsläpp av radioaktiva ämnen till omgivningen.

Finland

Krav

13 § Tekniska hinder för spridning av radioaktiva ämnen
… För tryggande av reaktorinneslutningens integritet ska:

- reaktorinneslutningen planeras så att den bibehåller sin täthet vid förväntade driftsstörningar samt med stor säkerhet också i alla olyckssituationer,
- vid planering av reaktorinneslutningen beaktas sådana tryck-, strål- och värmebelastningar, brinnande gaser, flygande föremål samt kortvariga fenomen av hög energi som uppstår till följd av en olycka, och
- möjligheten att reaktortryckkärlet skadas vid en allvarlig reaktorolycka så att reaktorinneslutningens integritet äventyras, vara ytterst liten.

YVL B.1 §427-428

Storbritannien

Övergripande principer

EMC.23 Ductile behaviour
For metal pressure vessels and circuits, particularly ferritic steel items, the operating regime should ensure that they display ductile behaviour when significantly stressed.

ECE.6 Loadings
For safety-related structures, load development and a schedule of load combinations within the design basis together with their frequency should be

used as the basis for the design against operating, testing and fault conditions.

ECE.7 Foundations
The foundations should be designed to support the structural loadings specified for normal operation and fault conditions.

ECE.12 Structural analysis and model testing
Structural analysis or model testing should be carried out to support the design and should demonstrate that the structure can fulfil its safety functional requirements over the lifetime of the facility.

ECE.14 Sensitivity studies
Studies should be carried out to determine the sensitivity of analytical results to the assumptions made, the data used, and the methods of calculation.

ECE.15 Validation of methods
Where analyses have been carried out on civil structures to derive static and dynamic structural loadings for the design, the methods used should be adequately validated.

ECE.21 Proof pressure tests
Pre-stressed concrete pressure vessels and containment structures should be subjected to a proof pressure test, which may be repeated during the life of the facility.

ECE.22 Leak tightness
Civil engineering structures that retain or prevent leakage should be tested against the leak tightness requirements prior to operation to demonstrate that the design intent has been met.

EKP.5 Safety measures
Safety measures should be identified to deliver the required safety function(s).

ECV.2 Minimisation of releases
Nuclear containment and associated systems should be designed to minimise radioactive releases to the environment in normal operation, fault and accident conditions.

ECV.3 Means of confinement
The primary means of confining radioactive substance should be by the provision of passive sealed containment systems and intrinsic safety features, in preference to the use of active dynamic systems and components.

ECV.5 Provision of containment barriers
Where the radiological challenge dictates, waste storage vessels, process vessels, piping, ducting and drains (including those that may serve as routes for escape or leakage from containment) and other plant items that act as containment for nuclear matter, should be provided with further containment barrier(s) that have sufficient capacity to deal safely with the leakage resulting from any design basis fault.

Pressure systems

EPS.1 Removable closures
The failure of a removable closure to a pressurised component or system that could lead to a major release of radioactivity should be prevented.

EPS.2 Flow limitation
Flow limiting devices should be provided to piping systems that are connected to or form branches from a main pressure circuit, to minimise the consequences of postulated breaches.

EPS.3 Pressure relief
Adequate pressure relief systems should be provided for pressurised systems and provision should be made for periodic testing.

EPS.4 Overpressure protection
Overpressure protection should be consistent with any pressure-temperature limits of operation.

EPS.5 Discharge routes
Pressure discharge routes should be provided with suitable means to ensure that any release of radioactivity from the facility to the environment is minimised.

Integrity of metal components and structures: highest reliability components and structures

EMC.1 Safety case and assessment
The safety case should be especially robust and the corresponding assessment suitably demanding, in order that an engineering judgement can be made for two key requirements:

a) the metal component or structure should be as defect-free as possible;
b) the metal component or structure should be tolerant of defects.

EMC.2 Use of scientific and technical issues
The safety case and its assessment should include a comprehensive examination of relevant scientific and technical issues, taking account of precedent when available.

EMC.3 Evidence
Evidence should be provided to demonstrate that the necessary level of integrity has been achieved for the most demanding situations.

EMC.4 Procedural control
Design, manufacture and installation activities should be subject to procedural control.

EMC.5 Defects
It should be demonstrated that safety-related components and structures are both free from significant defects and are tolerant of defects.

EMC.6 Defects
During manufacture and throughout the operational life the existence of defects of concern should be able to be established by appropriate means.

EMC.7 Loadings
For safety-related components and structures, the schedule of design

loadings (including combinations of loadings), together with conservative estimates of their frequency of occurrence should be used as the basis for design against normal operating, plant transient, testing, fault and internal or external hazard conditions.

EMC.8 Requirements for examination
Geometry and access arrangements should have regard to the requirements for examination.

EMC.9 Product form
The choice of product form of metal components or their constituent parts should have regard to enabling examination and to minimising the number and length of welds in the component.

EMC.10 Weld positions
The positioning of welds should have regard to high-stress locations and adverse environments.

EMC.11 Failure modes
Failure modes should be gradual and predictable.

EMC.12 Brittle behaviour
Designs in which components of a metal pressure boundary could exhibit brittle behaviour should be avoided.

Vägledande råd

147 The availability and reliability of the safety measures should be commensurate with the significance of the radiological hazards to be controlled. There should also be measures in place to mitigate the consequences of any accident where radioactivity is released from its intended containment, but these should not be regarded as a substitute for fault prevention but as further defence in depth.

300 Where appropriate, drainage systems should be provided to confirm the continuing containment integrity of the structures or to detect, locate, collect, quantify and where possible allow repair of leakages.

423 The safety functionality should be clearly identified for operational states and fault and accident conditions. Where appropriate, containment should be designed to protect the facility from external hazards and to withstand internal hazards.

424 Where appropriate, containment design should:

a) define the containment boundaries with means of isolating the boundary;
b) establish a set of design safety limits for the containment systems and for individual structures and components within each system;
c) define the requirements for the performance of the containment in the event of a severe accident as a result of internal or external hazards, including its structural integrity and stability;
d) include provision for making the facility safe following any incident involving the release of radioactive substances within or from a

containment, including equipment to allow decontamination and post-incident re-entry to be safely carried out;

e) minimise the size and number of service penetrations in the containment boundary, which should be adequately sealed to reduce the possibility of nuclear matter escaping from containment via routes installed for other purposes;
f) avoid the use of ducts that need to be sealed by isolating valves under accident conditions. Where isolating valves and devices are provided for the isolation of containment penetrations, their performance should be consistent with the required containment duties and should not prejudice adequate containment performance;
g) provide discharge routes, including pressure relief systems, with treatment system(s) to minimise radioactive releases to acceptable levels. There should be appropriate treatment or containment of the fluid or the radioactive material contained within it, before or after its released from the system;
h) allow the removal and reinstatement of shielding;
i) define the performance requirements of containment systems to support maintenance activities;
j) demonstrate that the loss of electrical supplies, air supplies and other services does not lead to a loss of containment nor the delivery of its safety function;
k) demonstrate the control methods and timescales for re-establishing the containment conditions where access to the containment is temporarily open (eg during maintenance work);
l) incorporate measures to minimise the likelihood of unplanned criticality wherever significant amount of fissile materials may be present.

425 Should the pressure relief system operate, the performance of the containment should not be degraded.

426 When considering secondary containment, the design should include appropriate means of isolation. It should also incorporate, where appropriate, redundant storage provisions with sufficient capacity and associated services to ensure prolonged safe storage of the maximum anticipated volume of material requiring relocation, allowing for any volume increase due to the method of transfer (eg from the use of ejectors).

427 Where access is necessary it should be designed to ensure that at all times the containment will perform its safety function.

428 There should be no requirement for access to the containment to ensure the safety of the facility in either the short or long term following an accident.

Kanada

Krav

RD–337, 7.3.4 Beyond Design Basis Accidents
The design authority identifies credible BDBAs, based on operational experience, engineering judgment, and the results of analysis and research. This includes events leading to significant core degradation (severe accidents), particularly those events that challenge containment.

Complementary design features are then considered with the goal of preventing identified BDBA scenarios, and mitigating their consequences if they do occur.

Complementary design features include design or procedural considerations, or both, and are based on a combination of phenomenological models, engineering judgments, and probabilistic methods.

The design identifies the rules and practices that have been applied to the complementary design features. These rules and practices do not necessarily need to incorporate the same degree of conservatism as those applied to the design basis.

The design identifies a radiological and combustible gas accident source term for use in the specification of the complementary design features for BDBAs. This source term is referred to as the reference source term, and is based on a set of representative core damage accidents established by the design authority.

In the case of multi-unit plants, the use of available support from other units is relied upon only if it can be established that the safe operation of the other units is not compromised.

To the extent practicable, the design provides biological shielding of appropriate composition and thickness to protect operational personnel during BDBAs, including severe accidents.

Severe Accidents
The design should be balanced such that no particular design feature or event makes a dominant contribution to the frequency of severe accidents, taking uncertainties into account.

Early in the design process, the various potential barriers to core degradation are identified, and features that can be incorporated to halt core degradation at those barriers are considered.

The design also identifies the equipment to be used in the management of severe accidents. A reasonable level of confidence that this equipment will perform as intended in the case of a severe accident is demonstrated by environmental, fire, and seismic assessments.

Particular attention is placed on the prevention of potential containment bypass in accidents involving significant core degradation.

Consideration is given to the plant’s full design capabilities, including the possible use of safety, non-safety, and temporary systems, beyond their originally intended function. This applies to any system that can be shown with a reasonable degree of assurance to be able to function in the environmental conditions expected during a severe accident.

Containment maintains its role as a leak-tight barrier for a period that allows sufficient time for the implementation of off-site emergency procedures following the onset of core damage. Containment also prevents uncontrolled releases of radioactivity after this period.

The design authority establishes initial severe accident management guidelines, taking into account the plant design features and the understanding of accident progression and associated phenomena.

The design considers prevention of recriticality following severe accidents.

RD–337, 8.6.2 Strength of the Containment Structure
The strength of the containment structure provides sufficient margins of safety based on potential internal overpressures, underpressures, temperatures, dynamic effects such as missile generation, and reaction-forces anticipated to result in the event of DBAs. Application of strength margins applies to access openings, penetrations, and isolation valves, and to the containment heat removal system.

The margins reflect:

1. Effects of other potential energy sources, such as possible chemical reactions and radiolytic reactions;
2. Limited experience and experimental data available for defining accident phenomena and containment responses; and
3. Conservatism of the calculation model and input parameters.

The positive and negative design pressures within each part of the containment boundary include the highest and lowest pressures that could be generated in the respective parts as a result of any DBA.

The containment structure protects systems and equipment important to safety in order to preserve safety functions for the plant.

The design supports maintenance of full functionality following a DBE of all parts of the containment system credited in the safety analysis.

The seismic design of the concrete containment structure has an elastic response when subjected to seismic ground motions. The special detailing of reinforcement allows the structure to possess ductility and energy-absorbing capacity which permits inelastic deformation without failure.

RD–337, 8.6 Containment

RD–337, 8.6.1 General Requirements
Each nuclear power reactor is installed within a containment structure to minimize the release of radioactive materials to the environment during normal operation, AOOs, and DBAs. Containment also assists in mitigating the consequences of BDBAs.

The containment system is designed for all AOOs and DBAs, and also considers BDBAs, including severe accident conditions.

The containment is a safety system and includes complementary design features, both of which are subject to the respective design expectations provided in this regulatory document.

The design includes a clearly defined continuous leak-tight containment envelope, the boundaries of which are defined for all conditions that could exist in the operation or maintenance of the reactor, or following an accident.

All piping that is part of the main or backup reactor coolant systems is entirely within the main containment structure, or in a containment extension.

The containment design incorporates systems to assist in controlling internal pressure and the release of radioactive material to the environment following an accident.

The containment includes at least the following subsystems:

1. The containment structure and related components;
2. Equipment required to isolate the containment envelope and maintain its completeness and continuity following an accident;
3. Equipment required to reduce the pressure and temperature of the containment and reduce the concentration of free radioactive material within the containment envelope; and
4. Equipment required for limiting the release of radioactive material from the containment envelope following an accident.

When the containment design includes the use of compressed air or non-condensable gas systems in response to a DBA, the autonomy of the compressed air system is demonstrated. In the event of a loss of compressed air, containment isolation valves fail in their safe state.

The design authority identifies where and when the containment boundary is credited for providing shielding for people and equipment.

RD–337, 8.6.2 Strength of the Containment Structure
The strength of the containment structure provides sufficient margins of safety based on potential internal overpressures, underpressures, temperatures, dynamic effects such as missile generation, and reaction-forces anticipated to result in the event of DBAs. Application of strength margins applies to access openings, penetrations, and isolation valves, and to the containment heat removal system.

The margins reflect:

1. Effects of other potential energy sources, such as possible chemical reactions and radiolytic reactions;
2. Limited experience and experimental data available for defining accident phenomena and containment responses; and
3. Conservatism of the calculation model and input parameters.

The positive and negative design pressures within each part of the containment boundary include the highest and lowest pressures that could be generated in the respective parts as a result of any DBA.

The containment structure protects systems and equipment important to safety in order to preserve safety functions for the plant.

The design supports maintenance of full functionality following a DBE of all parts of the containment system credited in the safety analysis.

The seismic design of the concrete containment structure has an elastic response when subjected to seismic ground motions. The special detailing of reinforcement allows the structure to possess ductility and energy-absorbing capacity which permits inelastic deformation without failure.

RD–337, 8.6.3 Capability for Pressure Tests
The containment structure is subject to pressure testing at a specified pressure to demonstrate structural integrity. Testing is conducted before plant operation commences and throughout the plant's lifetime.

RD–337, 8.6.4 Leakage
Leakage Rate Limits
The safety leakage rate limit assures that:

1. Normal operation release limits are met; and
2. AOOs and DBAs will not result in exceeding dose acceptance criteria.

The design leakage rate limit is:

1. Below the safety leakage rate limit;
2. As low as is practicably attainable; and
3. Consistent with state-of-the-art design practices.

Test Acceptance Leakage Rate Limits
A test acceptance leakage rate provides the maximum rate acceptable under actual measurement tests. Test acceptance leakage rate limits are established for the entire containment system, and for individual components that can contribute significantly to leakage.

Leak Rate Testing
The containment structure and the equipment and components affecting the leak tightness of the containment system are designed to allow leak rate testing:

1. For commissioning, at the containment design pressure; and
2. Over the service lifetime of the reactor, either at the containment design pressure or at reduced pressures that permit estimation of the leakage rate at the containment design pressure.

To the extent practicable, penetrations are to be designed to allow individual testing of each penetration.

The design is expected to provide for ready and reliable detection of any significant breach of the containment envelope.

RD–337, 8.6.5 Containment Penetrations
The number of penetrations through the containment will be kept to a minimum.

All containment penetrations are subject to the same design expectations as the containment structure itself, and are to be protected from reaction forces stemming from pipe movement or accidental loads, such as those due to missiles, jet forces, and pipe whip.

All penetrations are designed to allow for periodic inspection.

If resilient seals such as elastomeric seals, electrical cable penetrations, or expansion bellows are used with penetrations, they have the capacity for leak testing at the containment design pressure. To demonstrate continued integrity over the lifetime of the plant, this capacity supports testing that is independent of determining the leak rate of the containment as a whole.

RD–337, 8.6.6 Containment Isolation
Each line of the reactor coolant pressure boundary that penetrates the containment, or that is connected directly to the containment atmosphere, is to be automatically and reliably sealable. This provision is essential to maintaining the leak tightness of the containment in the event of an accident, and preventing radioactive releases to the environment that exceed prescribed limits.

Automatic isolation valves are positioned to provide the greatest safety upon loss of actuating power.

Piping systems that penetrate the containment system have isolation devices with redundancy, reliability, and performance capabilities that reflect the importance of isolating the various types of piping systems. Alternative types of isolation may be used where justification is provided.

Where manual isolation valves are used, they have locking or continuous monitoring capability.

Reactor Coolant System Auxiliaries that Penetrate Containment
Each auxiliary line that is connected to the reactor coolant pressure boundary, and that penetrates the containment structure, includes two isolation valves in series. The valves are normally arranged with one inside and one outside the containment structure.

Where the valves provide isolation of the heat transport system during normal operation, both valves are normally in the closed position.

Systems directly connected to the reactor coolant system that may be open during normal operation are subject to the same isolation expectations as the normally closed system, with the exception that manual isolating valves inside the containment structure will not be used. At least one of the two isolation valves is either automatic or powered, and operable from the main and secondary control rooms.

For any piping outside of containment that could contain radioactivity from the reactor core, the following expectations apply:

1. Design parameters are the same as those for a piping extension to containment, and are subject to the requirements for metal penetrations of containment;
2. All piping and components that are open to the containment atmosphere are designed for a pressure greater than the containment design pressure;
3. The piping and components are housed in a confinement structure that prevents leakage of radioactivity to the environment and to adjacent structures; and

4. This housing includes detection capability for leakage of radioactivity and the capability to return the radioactivity to the flow path.

Systems Connected to Containment Atmosphere
Each line that connects directly to the containment atmosphere, that penetrates the containment structure and is not part of a closed system, is to be provided with two isolation barriers that meet the following expectations:

1. Two automatic isolation valves in series for lines that may be open to the containment atmosphere;
2. Two closed isolation valves in series for lines that are normally closed to the containment atmosphere; and
3. The line up to and including the second valve is part of the containment envelope.

Closed Systems
All closed piping service systems have at least one single isolation valve on each line penetrating the containment, with the valve being located outside of, but as close as practicable to, the containment structure.

Where failure of a closed loop is assumed to be a PIE or the result of a PIE, the isolations for reactor coolant system auxiliaries apply.

Closed piping service systems inside or outside the containment structure that form part of the containment envelope need no further isolation if:

1. They meet the applicable service piping standards and codes; and
2. They can be continuously monitored for leaks.

RD–337, 8.6.7 Containment Air Locks
Personnel access to the containment is through airlocks that are equipped with doors that are interlocked to ensure that at least one of the doors is closed during normal operation, AOOs, and DBAs.

Where provision is made for entry of personnel for surveillance or maintenance purposes during normal operation, the design specifies provisions for personnel safety, including emergency egress. This expectation also applies to equipment air locks.

RD–337, 8.6.8 Internal Structures of the Containment
The design provides for ample flow routes between separate compartments inside the containment. The openings between compartments are to be large enough to prevent significant pressure differentials that may cause damage to load bearing and safety systems during AOOs and DBAs.

The design of internal structures considers any hydrogen control strategy, and assists in the effectiveness of that strategy.

RD–337, 8.6.9 Containment Pressure and Energy Management
The design enables heat removal and pressure reduction in the reactor containment in all plant states. Systems designed for this purpose are considered part of the containment system, and are capable of:

1. Minimizing the pressure-assisted release of fission products to the environment;

2. Preserving containment integrity; and
3. Preserving required leak tightness.

RD–337, 8.6.10 Control and Cleanup of the Containment Atmosphere
The design provides systems to control the release of fission products, hydrogen, oxygen, and other substances into the reactor containment as necessary, to:

1. Reduce the amount of fission products that might be released to the environment during an accident; and
2. Prevent deflagration or detonation that could jeopardize the integrity or leak tightness of the containment.

The design also:

1. Supports isolation of all sources of compressed air and other non-condensable gases into the containment atmosphere following an accident;
2. Ensures that, in the case of ingress of non-condensable gas resulting from a PIE, containment pressure will not exceed the design limit; and
3. Provides isolation of compressed air sources to prevent any bypass of containment.

RD–337, 8.6.11 Coverings, Coatings, and Materials
The coverings and coatings for components and structures within the containment are carefully selected, and their methods of application specified to ensure fulfillment of their safety functions. The primary objective of this expectation is to minimize interference with other safety functions or accident mitigation systems in the event of deterioration of coverings and coatings. In addition, the choice of materials inside containment takes into account the impact on post-accident containment conditions, including fission product behaviour, acidity, equipment fouling, radiolysis, fires, and other factors that may affect containment performance and integrity, and fission product release.

RD–337, 8.6.12 Severe Accidents
Following onset of core damage, the containment boundary should be capable of contributing to the reduction of radioactivity releases to allow sufficient time for the implementation of off-site emergency procedures. This expectation applies to a representative set of severe accidents.

Damage to the containment structure is limited to prevent uncontrolled releases of radioactivity, and to maintain the integrity of structures that support internal components.

The ability of the containment system to withstand loads associated with severe accidents is demonstrated in design documentation, and includes the following considerations:

1. Various heat sources, including residual heat, metal-water reactions, combustion of gases, and standing flames;
2. Pressure control;
3. Control of combustible gases;

4. Sources of non-condensable gases;
5. Control of radioactive material leakage;
6. Effectiveness of isolation devices;
7. Functionality and leak tightness of air locks and containment penetrations; and
8. Effects of the accident on the integrity and functionality of internal structures.

USA

Krav

10 CFR 50 Appendix A, Criterion 16 Containment design.
Reactor containment and associated systems shall be provided to establish an essentially leak-tight barrier against the uncontrolled release of radioactivity to the environment and to assure that the containment design conditions important to safety are not exceeded for as long as postulated accident conditions require.

10 CFR 50 Appendix A, Criterion 50 Containment design basis.
The reactor containment structure, including access openings, penetrations, and the containment heat removal system shall be designed so that the containment structure and its internal compartments can accommodate, without exceeding the design leakage rate and with sufficient margin, the calculated pressure and temperature conditions resulting from any loss-of-coolant accident. This margin shall reflect consideration of (1) the effects of potential energy sources which have not been included in the determination of the peak conditions, such as energy in steam generators and as required by § 50.44 energy from metal-water and other chemical reactions that may result from degradation but not total failure of emergency core cooling functioning, (2) the limited experience and experimental data available for defining accident phenomena and containment responses, and (3) the conservatism of the calculational model and input parameters.

10 CFR 50 Appendix A, Criterion 51 Fracture prevention of containment pressure boundary.
The reactor containment boundary shall be designed with sufficient margin to assure that under operating, maintenance, testing, and postulated accident conditions (1) its ferritic materials behave in a nonbrittle manner and (2) the probability of rapidly propagating fracture is minimized. The design shall reflect consideration of service temperatures and other conditions of the containment boundary material during operation, maintenance, testing, and postulated accident conditions, and the uncertainties in determining (1) material properties, (2) residual, steady state, and transient stresses, and (3) size of flaws.

10 CFR 50 Appendix A, Criterion 52 Capability for containment leakage rate testing.
The reactor containment and other equipment which may be subjected to containment test conditions shall be designed so that periodic integrated leakage rate testing can be conducted at containment design pressure.

10 CFR 50 Appendix A, Criterion 53 Provisions for containment testing and inspection.
The reactor containment shall be designed to permit (1) appropriate periodic inspection of all important areas, such as penetrations, (2) an appropriate surveillance program, and (3) periodic testing at containment design pressure of the leaktightness of penetrations which have resilient seals and expansion bellows.

10 CFR 50 Appendix A, Criterion 54 Piping systems penetrating containment.
Piping systems penetrating primary reactor containment shall be provided with leak detection, isolation, and containment capabilities having redundancy, reliability, and performance capabilities which reflect the importance to safety of isolating these piping systems. Such piping systems shall be designed with a capability to test periodically the operability of the isolation valves and associated apparatus and to determine if valve leakage is within acceptable limits.

10 CFR 50 Appendix A, Criterion 55 Reactor coolant pressure boundary penetrating containment.
Each line that is part of the reactor coolant pressure boundary and that penetrates primary reactor containment shall be provided with containment isolation valves as follows, unless it can be demonstrated that the containment isolation provisions for a specific class of lines, such as instrument lines, are acceptable on some other defined basis:

One locked closed isolation valve inside and one locked closed isolation valve outside containment; or

One automatic isolation valve inside and one locked closed isolation valve outside containment; or

One locked closed isolation valve inside and one automatic isolation valve outside containment. A simple check valve may not be used as the automatic isolation valve outside containment; or

One automatic isolation valve inside and one automatic isolation valve outside containment. A simple check valve may not be used as the automatic isolation valve outside containment.

Isolation valves outside containment shall be located as close to containment as practical and upon loss of actuating power, automatic isolation valves shall be designed to take the position that provides greater safety.

Other appropriate requirements to minimize the probability or consequences of an accidental rupture of these lines or of lines connected to them shall be provided as necessary to assure adequate safety. Determination of the appropriateness of these requirements, such as higher quality in design, fabrication, and testing, additional provisions for inservice inspection, protection against more severe natural phenomena, and additional isolation valves and containment, shall include consideration of the population density, use characteristics, and physical characteristics of the site environs.

10 CFR 50 Appendix A, Criterion 56 Primary containment isolation.
Each line that connects directly to the containment atmosphere and penetrates primary reactor containment shall be provided with containment isolation valves as follows, unless it can be demonstrated that the containment isolation provisions for a specific class of lines, such as instrument lines, are acceptable on some other defined basis:

One locked closed isolation valve inside and one locked closed isolation valve outside containment; or

One automatic isolation valve inside and one locked closed isolation valve outside containment; or

One locked closed isolation valve inside and one automatic isolation valve outside containment. A simple check valve may not be used as the automatic isolation valve outside containment; or

One automatic isolation valve inside and one automatic isolation valve outside containment. A simple check valve may not be used as the automatic isolation valve outside containment.

Isolation valves outside containment shall be located as close to the containment as practical and upon loss of actuating power, automatic isolation valves shall be designed to take the position that provides greater safety.

10 CFR 50 Appendix A, Criterion 57 Closed system isolation valves.
Each line that penetrates primary reactor containment and is neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere shall have at least one containment isolation valve which shall be either automatic, or locked closed, or capable of remote manual operation. This valve shall be outside containment and located as close to the containment as practical. A simple check valve may not be used as the automatic isolation valve.

10 CFR 50.44 “Combustible Gas Control for Nuclear Power Reactors”.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 54: Containment system for the reactor
A containment system shall be provided to ensure, or to contribute to, the fulfilment of the following safety functions at the nuclear power plant: (i) confinement of radioactive substances in operational states and in accident conditions, (ii) protection of the reactor against natural external events and human induced events and (iii) radiation shielding in operational states and in accident conditions.

IAEA Safety Standard, No. SSR-2/1, Requirement 55: Control of radioactive releases from the containment
The design of the containment shall be such as to ensure that any release of radioactive material from the nuclear power plant to the environment is as

low as reasonably achievable, is below the authorized limits on discharges in operational states and is below acceptable limits in accident conditions.

IAEA Safety Standard, No. SSR-2/1, Requirement 56: Isolation of the containment
Each line that penetrates the containment at a nuclear power plant as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of an accident in which the leaktightness of the containment is essential to preventing radioactive releases to the environment that exceed acceptable limits.

IAEA Safety Standard, No. SSR-2/1, Requirement 58: Control of containment conditions
Provision shall be made to control the pressure and temperature in the containment at a nuclear power plant and to control any buildup of fission products or other gaseous, liquid or solid substances that might be released inside the containment and that could affect the operation of systems important to safety.

IAEA Safety Standard, No. SSR-2/1, 5.27
An analysis of design extension conditions for the plant shall be performed[8]. The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions not considered design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to maintain the integrity of the containment. These additional safety features for design extension conditions, or this extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions in which there is a significant amount of radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core). The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that significant radioactive releases would be practically eliminated (see footnote 1). The effectiveness of provisions to ensure the functionality of the containment could be analysed on the basis of the best estimate approach.

IAEA Safety Standard, No. SSR-2/1, 5.30
In particular, the containment and its safety features shall be able to withstand extreme scenarios that include, among other things, melting of the reactor core. These scenarios shall be selected using engineering judgement and input from probabilistic safety assessments.

IAEA Safety Standard, No. SSR-2/1, 6.20
The containment structure and the systems and components affecting the leaktightness of the containment system shall be designed and constructed so that the leak rate can be tested after all penetrations through the containment have been installed and, if necessary, during the operating lifetime of the plant, so that the leak rate can be tested at the containment design pressure.

IAEA Safety Standard, No. SSR-2/1, 6.21
The number of penetrations through the containment shall be kept to a practical minimum and all penetrations shall meet the same design requirements as the containment structure itself. The penetrations shall be protected against reaction forces caused by pipe movement or accidental loads such as those due to missiles caused by external or internal events, jet forces and pipe whip.

IAEA Safety Standard, No. SSR-2/1, 6.27
The design shall provide for sufficient flow routes between separate compartments inside the containment. The cross-sections of openings between compartments shall be of such dimensions as to ensure that the pressure differentials occurring during pressure equalization in accident conditions do not result in unacceptable damage to the pressure bearing structure or to systems that are important in mitigating the effects of accident conditions.

IAEA Safety Standard, No. SSR-2/1, 6.28
The capability to remove heat from the containment shall be ensured, in order to reduce the pressure and temperature in the containment, and to maintain them at acceptably low levels after any accidental release of high energy fluids. The systems performing the function of removal of heat from the containment shall have sufficient reliability and redundancy to ensure that this function can be fulfilled.

IAEA Safety Standard, No. SSR-2/1, 6.29
Design features to control fission products, hydrogen, oxygen and other substances that might be released into the containment shall be provided as necessary:

(a) To reduce the amounts of fission products that could be released to the environment in accident conditions;
(b) To control the concentrations of hydrogen, oxygen and other substances in the containment atmosphere in accident conditions so as to prevent deflagration or detonation loads that could challenge the integrity of the containment.

IAEA Safety Standard, No. SSR-2/1, 6.30
Coverings, thermal insulations and coatings for components and structures within the containment system shall be carefully selected and methods for their application shall be specified to ensure the fulfilment of their safety functions and to minimize interference with other safety functions in the event of deterioration of the coverings, thermal insulations and coatings.

Krav avseende instrumentering för att övervaka de parametrar som är väsentliga för hanteringen av alla händelser och olyckor

Sverige

Krav

6 § Instrumentering ska finnas som ger möjlighet att övervaka de parametrar som är väsentliga för hanteringen av alla händelser till och med händelseklassen mycket osannolika händelser.

Finland

Krav

12 § Förebyggande av olyckor och lindring av följderna av olyckor
Kärnkraftverket ska ha system med hjälp av vilka man snabbt och tillförlitligt upptäcker driftstörningar och olyckssituationer samt förhindrar att situationen förvärras. Olyckor som leder till stora utsläpp av radioaktiva ämnen ska vara ytterst osannolika (bemästrande av driftstörningar och olyckstillbud).

19 § Övervakning och styrning av kärnkraftverk
I kärnkraftverkets kontrollrum ska finnas anordningar som ger uppgifter om kärnreaktorns tillstånd och visar eventuella avvikelser från det normala. I kärnkraftverk ska finnas automatiska system som ser till att säkerhetsfunktionerna blir påkopplade vid behov samt som styr och övervakar deras funktion vid driftstörningar och olyckor.

De automatiska systemen ska ha förmåga att hålla kraftverket under kontroll så pass länge att reaktoroperatörerna får tillräckligt med betänketid för att vidta rätta åtgärder.

27 § Strålningsmätningar och övervakning av utsläpp av radioaktiva ämnen
Strålningsnivåerna i kärnkraftverkets lokaler samt aktivitetskoncentrationerna i inneluften och de gaser och vätskor som ingår i systemen ska mätas samt utsläppen av radioaktiva ämnen från kraftverket övervakas och deras halter i omgivningen observeras.

YVL B.1 Appendix B §117

YVL B.1 Appendix B §139-140

YVL B.1 Appendix B §143

Storbritannien

Övergripande principer

ESS.3 Monitoring of plant safety
Adequate provisions should be made to enable the monitoring of the plant state in relation to safety and to enable the taking of any necessary safety actions.

ESS.4 Adequacy of initiating variables
Variables used to initiate a safety system action should be identified and shown to be sufficient for the purpose of protecting the facility.

ESS.5 Plant interfaces
The interfaces required between a safety system and the plant to detect a

fault sequence and bring about a safe facility state should be engineered by means that have a direct, known, timely and unambiguous relationship with plant behaviour.

ESS.6 Adequacy of variables
Where it is not possible to use a directly related variable to detect a fault sequence, the variable chosen should have a known relationship with the fault sequence.

ESS.7 Diversity in the detection of fault sequences
The protection system should employ diversity in the detection of fault sequences, preferably by the use of different variables, and in the initiation of the safety system action to terminate the sequences.

ESS.8 Automatic initiation
A safety system should be automatically initiated and normally no human intervention should be necessary following the start of a requirement for protective action.

ECV.6 Monitoring devices
Suitable monitoring devices with alarms and provisions for sampling should be provided to detect and assess changes in the stored radioactive substances or changes in the radioactivity of the materials within the containment.

ECV.7 Leakage monitoring
Appropriate sampling and monitoring systems and other provisions should be provided outside the containment to detect, locate, quantify and monitor leakages of nuclear matter from the containment boundaries under normal and accident conditions.

ESR.8 Minimisation of provisions
Where provisions are required for the import or export of nuclear matter into or from the facility containments, the number of such provisions should be minimised.

Vägledande råd

338 Monitoring provisions should be classified as safety or safety-related systems as appropriate and should be made:

a) in a central control location; and
b) at emergency locations (preferably a single point) that will remain habitable during foreseeable facility emergencies.

339 The limiting conditions for these variables for which the safety system has been qualified should be specified. The safety system should be designed to respond so that these limiting conditions are not transgressed.

340 For example, if the action is to initiate a coolant flow then the flow should be measured directly and not inferred from measurement of power to actuation devices such as pumps, valves etc.

341 The physical and temporal coupling should be as close as possible. Any mechanism for the transmission of misleading information should be analysed and appropriate corrective measures adopted.

343 The design should be such that facility personnel cannot negate correct safety system action at any time, but they can initiate safety system functions and perform necessary actions to deal with circumstances that might prejudice safety.

Kanada

Krav

RD–337, 7.3.3 Design Basis Accidents
The set of design basis accidents sets the boundary conditions according to which SSCs important to safety are designed.

The design is such that releases to the public following a DBA will not exceed the dose acceptance criteria.

In order to prevent progression to a more severe condition that may threaten the next barrier, the design includes provision to automatically initiate the necessary safety systems where prompt and reliable action is required in response to a PIE.

Provision is also made to support timely detection of, and manual response to, conditions where prompt action is not necessary. This includes such responses as manual initiation of systems or other operator actions.

The design takes into account operator actions that may be necessary to diagnose the state of the plant and to put it into a stable long-term shutdown condition in a timely manner. Such operator actions are facilitated by the provision of adequate instrumentation to monitor plant status, and controls for manual operation of equipment.

Any equipment necessary for manual response and recovery processes is placed at the most suitable location to allow safe and timely worker access when needed.

RD–337, 7.6.5 Shared Systems
…Shared Instrumentation for Safety Systems
Instrumentation is not typically shared between safety systems.

Where justified, there may be sharing between a safety system and a non-safety system (such as a process or control system).

Reliability and effectiveness of a safety system will not be impaired by normal operation, by partial or complete failure in other systems, or by any cross-link generated by the proposed sharing.

The design includes provisions to ensure that the sharing of instruments does not result in an increased frequency in demand on the safety system during operation.

The design provides for periodic testing of the entire channel of instrumentation logic, from sensing device to actuating device.

If the design includes sharing of instrumentation between a safety system and a non-safety system, then the following expectations apply:

1. Sharing is limited to the sensing devices and their pre-amplifiers or amplifiers as needed to get the signal to the point of processing;
2. The signal from each sensing device is electrically isolated so that failures cannot be propagated from one system to the other; and
3. Isolation devices between systems of different safety importance are always associated with the system classified as being of greater importance to safety.

RD–337, 7.9 Instrumentation and Control

RD–337, 7.9.1 General Considerations

The design includes provision of instrumentation to monitor plant variables and systems over the respective ranges for normal operation, AOOs, DBAs, and BDBAs, in order to ensure that adequate information can be obtained on plant status.

This includes instrumentation for measuring variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems, and containment, as well as instrumentation for obtaining any information on the plant that is necessary for its reliable and safe operation.

The design is such that the safety systems and any necessary support systems can be reliably and independently operated, either automatically or manually, when necessary.

The design also includes the capability to trend and automatically record measurement of any derived parameters that are important to safety.

Instrumentation is adequate for measuring plant parameters for emergency response purposes.

The design includes reliable controls to maintain variables within specified operational ranges.

The design minimizes the likelihood of operator action defeating the effectiveness of safety and control systems in normal operation and AOOs, without negating correct operator actions following a DBA.

System control interlocks are designed to minimize the likelihood of inadvertent manual or automatic override, and to provide for situations when it is necessary to override interlocks to use equipment in a non-standard way.

Various safety actions are automated so that operator action is not necessary within a justified period of time from the onset of AOOs or DBAs. In addition, appropriate information is available to the operator to confirm the safety action.

RD–337, 7.9.2 Use of Computer-based Systems or Equipment

Appropriate standards and codes for the development, testing, and maintenance of computer hardware and software are applied to the design of systems or equipment important to safety that are controlled by computer. These standards and codes are implemented throughout the life cycle of the system or equipment, particularly during the software development cycle.

A top-down software development process is used to facilitate verification and validation activities. This approach includes verification at each step of the development process to demonstrate that the respective product is correct, and validation to demonstrate that the resulting computer-based system or equipment meets its functional and performance requirements.

If software provided by a third-party vendor is used in systems or equipment important to safety, then the software—and any subsequent release of the software—is developed, inspected, and tested in accordance with standards of a category commensurate with the safety function provided by the given system or equipment.

The software development process, including control, testing, and commissioning of design changes, as well as the results of independent assessment of that process, is reviewable and systematically documented in the design documentation.

Where a function important to safety is computer-based, the following expectations apply:

1. Functions not essential to safety are separate from and shown not to impact the safety function;
2. The safety function is normally executed in processors separate from software that implements other functions, such as control, monitoring, and display;
3. The expectations associated with diversity apply to computer-based systems that perform similar safety functions—the choice of diversity type is justified;
4. The design incorporates fail-safe and fault tolerance features, and the additional complexity ensuing from these features results in an overall gain in safety;
5. The design provides protection against physical attack, intentional and non-intentional intrusion, fraud, viruses, and other malicious threats; and
6. The design provides for effective detection, location, and diagnosis of failures in order to facilitate timely repair or replacement of equipment or software.

RD–337, 7.9.3 Post-accident Instrumentation
Instrumentation and recording equipment is such that essential information is available to support plant procedures during and following accidents by:

1. Indicating plant status;
2. Identifying the locations of radioactive material;
3. Supporting estimation of quantities of radioactive material;
4. Recording vital plant parameters; and
5. Facilitating decisions in accident management.

RD–337, 8.4.1 Reactor Trip Parameters
The design authority specifies derived acceptance criteria for reactor trip parameter effectiveness for all AOOs and DBAs, and performs a safety analysis to demonstrate the effectiveness of the means of shutdown.

For each credited means of shutdown, the design specifies a direct trip parameter to initiate reactor shutdown for all AOOs and DBAs in time to meet the respective derived acceptance criteria. Where a direct trip parameter does not exist for a given credited means, there are two diverse trip parameters specified for that means.

For all AOOs and DBAs, there are at least two diverse trip parameters unless it can be shown that failure to trip will not lead to unacceptable consequences.

There is no gap in trip coverage for any operating condition (i.e., power, temperature, etc.) within the OLCs. This is ensured by providing additional trip parameters if necessary. A different level of effectiveness may be acceptable for the additional trip parameters.

The extent of trip coverage provided by all available parameters is documented for the entire spectrum of failures for each set of PIEs.

An assessment of the accuracy and the potential failure modes of the trip parameters is provided in the design documentation.

RD–337, 8.10.4 Equipment Requirements for Accident Conditions
If operator action is required for actuation of any safety system or safety support system equipment, all of the following expectations apply:

1. There are clear, well-defined, validated, and readily available operating procedures that identify the necessary actions;
2. There is instrumentation in the control rooms to provide clear and unambiguous indication of the necessity for operator action;
3. Following indication of the necessity for operator action inside the MCR, there is at least 15 minutes available before the operator action is required; and
4. Following indication of the necessity for operator action outside the MCR, there is a minimum of 30 minutes available before the operator action is required.

Alternative action times may be used if justified, making due allowance for the complexity of the action to be taken, and for the time needed for such activities as the diagnosing the event and accessing to the remote station.

For automatically initiated safety systems and control logic actions, the design facilitates backup manual initiation from inside the appropriate control room.

USA

Krav

10 CFR 50 Appendix A, Criterion 13 Instrumentation and control.
Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure

boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

10 CFR 50.44 (4) Monitoring. (i) Equipment must be provided for monitoring oxygen in containments that use an inerted atmosphere for combustible gas control. Equipment for monitoring oxygen must be functional, reliable, and capable of continuously measuring the concentration of oxygen in the containment atmosphere following a significant beyond design-basis accident for combustible gas control and accident management, including emergency planning.

10 CFR 50.44 (4) Monitoring. (ii) Equipment must be provided for monitoring hydrogen in the containment. Equipment for monitoring hydrogen must be functional, reliable, and capable of continuously measuring the concentration of hydrogen in the containment atmosphere following a significant beyond design-basis accident for accident management, including emergency planning.

10 CFR Part 20, "Standards for Protection Against Radiation" §IV(a)(4) of Appendix S, "Earthquake Engineering Criteria for Nuclear Power Plants," to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," requires that suitable instrumentation must be provided so that the seismic response of nuclear power plant features important to safety can be evaluated promptly after an earthquake. §IV(a)(3) of Appendix S to 10 CFR Part 50 requires shutdown of the nuclear power plant if vibratory ground motion exceeding that of the operating basis earthquake ground motion (OBE) occurs.

Guide

RG 1.97 Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 59: Provision of instrumentation
Instrumentation shall be provided for determining the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems and the containment at the nuclear power plant, for obtaining essential information on the plant that is necessary for its safe and reliable operation, for determining the status of the plant in accident conditions and for making decisions for the purposes of accident management.

IAEA Safety Standard, No. SSR-2/1, Requirement 62: Reliability and testability of instrumentation and control Systems
Instrumentation and control systems for items important to safety at the

nuclear power plant shall be designed for high functional reliability and periodic testability commensurate with the safety function(s) to be performed.

IAEA Safety Standard, No. SSR-2/1, Requirement 71: Process sampling systems and post-accident sampling systems
Process sampling systems and post-accident sampling systems shall be provided for determining, in a timely manner, the concentration of specified radionuclides in fluid process systems, and in gas and liquid samples taken from systems or from the environment, in all operational states and in accident conditions at the nuclear power plant.

IAEA Safety Standard, No. SSR-2/1, Requirement 82: Means of radiation monitoring
Equipment shall be provided at the nuclear power plant to ensure that there is adequate radiation monitoring in operational states and design basis accident conditions and, as far as is practicable, in design extension conditions.

IAEA Safety Standard, No. SSR-2/1, 4.2.
Means of monitoring the status of the plant shall be provided for ensuring that the required safety functions are fulfilled.

IAEA Safety Standard, No. SSR-2/1, 5.13
The operator actions that would be necessary to diagnose the state of the plant following a postulated initiating event and to put it into a stable long term shutdown condition in a timely manner shall be facilitated by the provision of adequate instrumentation to monitor the status of the plant, and adequate controls for the manual operation of equipment.

IAEA Safety Standard, No. SSR-2/1, 6.12
Instrumentation shall be provided and tests shall be specified for ensuring that the means of shutdown are always in the state stipulated for a given plant state.

IAEA Safety Standard, No. SSR-2/1, 6.31
Instrumentation and recording equipment shall be provided to ensure that essential information is available for monitoring the status of essential equipment and the course of accidents, for predicting the locations of release and the amount of radioactive material that could be released from the locations that are so intended in the design, and for post-accident analysis.

Krav avseende kylning av reaktorhärden

Sverige

Krav

7 § Reaktorhärden ska kunna kylas genom strilning eller tillräcklig vattentäckning vid samtliga typer och storlekar av kylmedelsförlust som kan följa av brott i anslutningar till reaktortryckkärlet.

Finland

Krav

13 § Tekniska hinder för spridning av radioaktiva ämnen
… För tryggande av bränslets integritet ska

- sannolikheten för att en bränsleskada uppstår vara liten i normal drift och vid förväntade driftstörningar,
- antalet bränsleskador vid antagna olyckor vara litet och kylningen av bränslet inte få äventyras, och
- möjligheten av att en kriticitetsolycka inträffar vara ytterst liten.

YVL B.1 Appendix A §109

YVL B.1 Appendix A §111

Storbritannien

Övergripande principer

ESR.8 Monitoring of radioactive substances
Instrumentation should be provided to enable monitoring of the locations and quantities of radioactive substances that may escape from their engineered environment.

Vägledande råd

462 In the case of liquid heat transport systems, there should be a margin against failure of the operating heat transfer regime under anticipated normal and fault conditions and procedures. The minimum value of this margin should be stated and justified with reference to the uncertainties in the data and in the calculational methods employed.

Kanada

Krav

RD–337, 8.2 Reactor Coolant System
The design provides the reactor coolant system and its associated components and auxiliary systems with sufficient margin to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in normal operation, AOOs, or DBAs.

The design ensures that the operation of pressure relief devices will not lead to unacceptable releases of radioactive material from the plant, even in DBAs. The reactor coolant system is fitted with isolation devices to limit any loss of radioactive coolant outside containment.

The material used in the fabrication of the component parts is selected so as to minimize activation of the material.

Plant states in which components of the pressure boundary could exhibit brittle behaviour should be avoided.

The design reflects consideration of all conditions of the boundary material in normal operation (including maintenance and testing), AOOs, and DBAs, as well as expected end-of-life properties affected by ageing mechanisms, the rate of deterioration, and the initial state of the components.

The design of the moving components contained inside the reactor coolant pressure boundary, such as pump impellers and valve parts, minimizes the likelihood of failure and associated consequential damage to other items of the reactor coolant system. This applies to normal operation, AOOs, and DBAs, with allowance for deterioration that may occur in service.

The design provides a system capable of detecting and monitoring leakage from the reactor coolant system.

RD–337, 8.2.2 Inventory
Taking volumetric changes and leakage into account, the design provides control of coolant inventory and pressure to ensure that specified design limits are not exceeded in normal operation. This expectation extends to the provision of adequate capacity (flow rate and storage volumes) in the systems performing this function.

The inventory in the reactor coolant system and its associated systems are sufficient to support cool down from hot operating conditions to zero power cold conditions without the need for transfer from any other systems.

RD–337, 8.2.4 Removal of Residual Heat from Reactor Core
The design provides a means (i.e., backup) of removing residual heat from the reactor for all conditions of the RCS. The backup is independent of the configuration in use.

The means of removing residual heat meets reliability requirements on the assumptions of a single failure and the loss of off-site power, by incorporating suitable redundancy, diversity, and independence. Interconnections and isolation capabilities have a degree of reliability that is commensurate with system design requirements.

Heat removal is at a rate that prevents the specified design limits of the fuel and the reactor coolant pressure boundary from being exceeded.

If a residual heat removal system is required when the RCS is hot and pressurized, it can be initiated at the normal operating conditions of the RCS.

RD–337, 8.7 Heat Transfer to an Ultimate Heat Sink
The design includes systems for transferring residual heat from SSCs important to safety to an ultimate heat sink. This function is subject to very high levels of reliability during normal operation, AOOs, and DBAs. All systems that contribute to the transport of heat by conveying heat, providing power, or supplying fluids to the heat transport systems, are therefore designed in accordance with the importance of their contribution to the function of heat transfer as a whole.

Natural phenomena and human-induced events are taken into account in the design of heat transfer systems, and in the choice of diversity and

redundancy, both in the ultimate heat sinks and in the storage systems from which fluids for heat transfer are supplied.

The design extends the capability to transfer residual heat from the core to an ultimate heat sink so that, in the event of a severe accident:

1. Acceptable conditions can be maintained in SSCs;
2. Radioactive materials can be confined; and
3. Releases to the environment can be limited.

RD–337, 8.8 Emergency Heat Removal System
The design includes an emergency heat removal system (EHRS) which provides for removal of residual heat in order to meet fuel design limits and reactor coolant boundary condition limits.

If the design of the plant is such that the EHRS is required to mitigate the consequences of a DBA, then the EHRS is designed as a safety system.

Correct operation of the EHRS equipment following an accident is not dependent on power supplies from the electrical grid or from the turbine generators associated with any reactor unit that is located on the same site as the reactor involved in the accident.

Where water is required for the EHRS, it comes from a source that is independent of normal supplies.

The design supports maintenance and reliability testing without a reduction in system effectiveness below that required by the OLCs.

As far as practicable, inadvertent operation of the EHRS, or of part of the EHRS, will not have a detrimental effect on plant safety.

If the fire water supply or system components are interconnected to the EHRS, operation of one does not impair operation of the other.

USA

Krav

10 CFR 50 Appendix A, Criterion 33 Reactor coolant makeup.
A system to supply reactor coolant makeup for protection against small breaks in the reactor coolant pressure boundary shall be provided. The system safety function shall be to assure that specified acceptable fuel design limits are not exceeded as a result of reactor coolant loss due to leakage from the reactor coolant pressure boundary and rupture of small piping or other small components which are part of the boundary. The system shall be designed to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished using the piping, pumps, and valves used to maintain coolant inventory during normal reactor operation.

10 CFR 50 Appendix A, Criterion 35 Emergency core cooling.
A system to provide abundant emergency core cooling shall be provided.

The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts.

Suitable redundancy in components and features, and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 52: Emergency cooling of the reactor core
Means of cooling the reactor core shall be provided to restore and maintain cooling of the fuel under accident conditions at the nuclear power plant even if the integrity of the pressure boundary of the primary coolant system is not maintained.

IAEA Safety Standard, No. SSR-2/1, 6.18
The means provided for cooling of the reactor core shall be such as to ensure that:

(a) The limiting parameters for the cladding or for integrity of the fuel (such as temperature) will not be exceeded;
(b) Possible chemical reactions are kept to an acceptable level;
(c) The effectiveness of the means of cooling of the reactor core compensates for possible changes in the fuel and in the internal geometry of the reactor core;
(d) Cooling of the reactor core will be ensured for a sufficient time.

IAEA Safety Standard, No. SSR-2/1, 6.19
Design features (such as leak detection systems, appropriate interconnections and capabilities for isolation) and suitable redundancy and diversity shall be provided to fulfil the requirements of para. 6.18 with adequate reliability for each postulated initiating event.

Krav avseende stabilt sluttillstånd och kylning av en smält härd

Sverige

Krav

8 § Det ska vara möjligt vid alla händelser, till och med händelseklassen mycket osannolika händelser, att uppnå ett stabilt sluttillstånd med

vattentäckt härd/härdsmälta och etablerad resteffektkylning. En smält härd ska kunna kylas i ett långtidsförlopp.

Finland

Krav

13 § Tekniska hinder för spridning av radioaktiva ämnen
[…] Kärnkraftverket ska förses med system som garanterar att den härdsmälta som uppstår vid en allvarlig reaktorolycka stabiliseras och kyls ned. En direkt kontakt mellan härdsmälta och den bärande konstruktionen i reaktorinneslutningen ska hindras på ett tillförlitligt sätt.

14 § Säkerhetsfunktioner och tryggande av dem
[…] För att olyckor ska kunna hindras och deras följder lindras ska kärnkraftverket ha system för att stänga av reaktorn och kvarhålla den i subkritiskt tillstånd samt system för avlägsnande av den resteffektvärme som bildas i reaktorn och säkerställande av att radioaktiva ämnen stannar inom anläggningen. …

[…] Anläggningen ska planeras så att den kan ställas i ett säkert läge efter en allvarlig reaktorolycka.

Storbritannien

Övergripande principer

ERC.2 Shutdown systems
At least two diverse systems should be provided for shutting down a civil reactor.

Vägledande råd

336 A reactor should be provided with safety systems that can shut it down safely in normal operating and fault conditions and maintain it in the shutdown condition. There should be a margin of reactivity that allows for systematic changes and uncertainties in nuclear characteristics, variations in plant state and other processes or mechanisms that might affect the reactivity of the core, even for the most reactive conditions of the core.

443 No single moveable fissile assembly, moderator or absorber when added to or removed from the core should increase the reactivity by an amount greater than the shutdown margin, with an appropriate allowance for uncertainty. The uncontrolled movement of reactivity control devices should be prevented.

444 Where a shutdown system is also used for the control of reactivity, a suitable and sufficient shutdown margin should be maintained at all times.

445 Reactor shutdown and subsequent hold-down should not be inhibited by mechanical failure, distortion, erosion, corrosion etc of plant components, or by the physical behaviour of the reactor coolant, under normal operation or design basis fault conditions.

Kanada

Krav

RD–337, 7.11 Guaranteed Shutdown State
The design authority defines the guaranteed shutdown state (GSS) that will support safe maintenance activities of the NPP.

The design provides two independent means of preventing recriticality from any pathway or mechanism during the GSS.

The shutdown margin for GSS is such that the core will remain subcritical for any credible changes in the core configuration and reactivity addition. Where possible, this is achieved without operator intervention.

RD–337, 8.4 Means of Shutdown
The design provides means of reactor shutdown capable of reducing reactor power to a low value, and maintaining that power for the required duration, when the reactor power control system and the inherent characteristics are insufficient or incapable of maintaining reactor power within the requirements of the OLCs.

The design includes two separate, independent, and diverse means of shutting down the reactor.

At least one means of shutdown is independently capable of quickly rendering the nuclear reactor subcritical from normal operation, in AOOs, and in DBAs by an adequate margin, on the assumption of a single failure. For this means of shutdown, a transient recriticality may be permitted in exceptional circumstances if the specified fuel and component limits are not exceeded.

At least one means of shutdown is independently capable of rendering the reactor subcritical from normal operation, in AOOs, and in DBAs, and maintaining the reactor subcritical by an adequate margin and with high reliability for even the most reactive conditions of the core.

Redundancy is provided in the fast-acting means of shutdown if, in the event that the credited means of reactivity control fails during any AOO or DBA, inherent core characteristics are unable to maintain the reactor within specified limits.

RD–337, 8.10.1 Main Control Room
The design provides for a main control room (MCR) from which the plant can be safely operated, and from which measures can be taken to maintain the plant in a safe state or to bring it back into such a state after the onset of AOOs, DBAs, and, to the extent practicable, following BDBAs.

While resetting the means of shutdown, the maximum degree of positive reactivity and the maximum rate of increase are within the capacity of the reactor control system.

To improve reliability, stored energy should be used in shutdown actuation.

The effectiveness of the means of shutdown (i.e., speed of action and shutdown margin) is such that specified limits are not exceeded, and the possibility of recriticality or reactivity excursion following a PIE is minimized.

USA

Krav

10 CFR 50 Appendix A, Criterion 27 Combined reactivity control systems capability.
The reactivity control systems shall be designed to have a combined capability, in conjunction with poison addition by the emergency core cooling system, of reliably controlling reactivity changes to assure that under postulated accident conditions and with appropriate margin for stuck rods the capability to cool the core is maintained.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 46: Reactor shutdown
Means shall be provided to ensure that there is a capability to shut down the reactor of the nuclear power plant in operational states and in accident conditions, and that the shutdown condition can be maintained even for the most reactive conditions of the reactor core.

IAEA Safety Standard, No. SSR-2/1, Requirement 53: Heat transfer to an ultimate heat sink
Systems shall be provided to transfer residual heat from items important to safety at the nuclear power plant to an ultimate heat sink. This function shall be carried out with very high levels of reliability for all plant states.

IAEA Safety Standard, No. SSR-2/1, Requirement 51: Removal of residual heat from the reactor core
Means shall be provided for the removal of residual heat from the reactor core in the shutdown state of the nuclear power plant such that the design limits for fuel, the reactor coolant pressure boundary and structures important to safety are not exceeded.

IAEA Safety Standard, No. SSR-2/1, 5.13
The operator actions that would be necessary to diagnose the state of the plant following a postulated initiating event and to put it into a stable long term shutdown condition in a timely manner shall be facilitated by the provision of adequate instrumentation to monitor the status of the plant, and adequate controls for the manual operation of equipment.

IAEA Safety Standard, No. SSR-2/1, 6.7
The effectiveness, speed of action and shutdown margin of the means of

shutdown of the reactor shall be such that the specified design limits for fuel are not exceeded.

IAEA Safety Standard, No. SSR-2/1, 6.8
In judging the adequacy of the means of shutdown of the reactor, consideration shall be given to failures arising anywhere in the plant that could render part of the means of shutdown inoperative (such as failure of a control rod to insert) or that could result in a common cause failure.

IAEA Safety Standard, No. SSR-2/1, 6.9
The means for shutting down the reactor shall consist of at least two diverse and independent systems.

IAEA Safety Standard, No. SSR-2/1, 6.10
At least one of the two different shutdown systems shall be capable, on its own, of maintaining the reactor subcritical by an adequate margin and with high reliability, even for the most reactive conditions of the reactor core.

IAEA Safety Standard, No. SSR-2/1, 6.11
The means of shutdown shall be adequate to prevent any foreseeable increase in reactivity leading to unintentional criticality during the shutdown, or during refuelling operations or other routine or non-routine operations in the shutdown state.

IAEA Safety Standard, No. SSR-2/1, 6.12
Instrumentation shall be provided and tests shall be specified for ensuring that the means of shutdown are always in the state stipulated for a given plant state.

Krav avseende enkelfel

Sverige

Krav

9 § Säkerhetsfunktionerna enligt 3 § ska vara tåliga mot enkelfel vid alla händelser till och med händelseklassen osannolika händelser. Vid händelser i händelseklassen mycket osannolika händelser ska de aktiva komponenter som tillhör de konsekvenslindrande systemen vara tåliga mot enkelfel.

Finland

Krav

14 § Säkerhetsfunktioner och tryggande av dem

… De viktigaste system som behövs för övergång i kontrollerat läge och kvarhållandet av det ska kunna utföra sina funktioner även om en enskild komponent i vilket system som helst blir funktionsoduglig och även om vilken som helst annan komponent i samma system eller en komponent i ett

stöd- eller hjälpsystem som är nödvändigt med tanke på dess funktion samtidigt är ur bruk på grund av behövliga reparationer eller underhåll…

YVL B.1 §431

Storbritannien

Övergripande principer

EDR.2 Redundancy, diversity and segregation
Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.

EDR.4 Single failure criterion
During any normally permissible state of plant availability no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.

ESS.18 Failure independence
No fault, internal or external hazard should disable a safety system.

ESS.24 Minimum operational equipment requirements
The minimum amount of operational safety system equipment for which any specified facility operation will be permitted should be defined and shown to meet the single failure criterion.

Guide

168 The design should incorporate redundancy to avoid the effects of random failure […]. The design should also be tolerant of random failure occurring anywhere within the safety systems provided to secure each safety function.

175 Consequential failures resulting from the assumed single failure should be considered as an integral part of the single failure. Further discussion of the single failure criterion is given in IAEA Safety Standard NS-G-1.2.[4]

Kanada

Krav

RD–337, 7.6.2 Single Failure Criterion
All safety groups function in the presence of a single failure. The single failure criterion requires that each safety group perform all safety functions required for a PIE in the presence of any single component failure, and:

1. All failures caused by that single failure;
2. All identifiable but non-detectable failures, including those in the non-tested components; and
3. All failures and spurious system actions that cause (or are caused by) the PIE.

Each safety group is able to perform the required safety functions under the worst permissible systems configuration, taking into account such considerations as maintenance, testing, inspection and repair, and equipment outage.

Analysis of all possible single failures, and all associated consequential failures, is conducted for each element of each safety group until all safety groups have been considered.

Unintended actions and failure of passive components are considered as two of the modes of failure of a safety group.

The single failure is assumed to occur prior to the PIE, or at any time during the mission time for which the safety group is required to function following the PIE. Passive components may be exempt from this expectation.

Exemptions for passive components apply only to those components that are designed and manufactured to high standards of quality, that are adequately inspected and maintained in service, and that remain unaffected by the PIE. Design documentation includes analytical justification of such exemptions, taking loads and environmental conditions into account, as well as the total period of time after the PIE for which the functioning of the component is necessary.

Check valves are active components if they must change state following a PIE.

Exceptions to the single failure criterion are infrequent, and clearly justified.

USA

Krav

10 CFR 50 Appendix A, Criterion 21 Protection system reliability and testability.
The protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

Guide

RG 1.53 "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems".

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 25: Single failure criterion
The single failure criterion shall be applied to each safety group incorporated in the plant design[10].

IAEA Safety Standard, No. SSR-2/1, 5.39
Spurious action shall be considered to be one mode of failure when applying the concept to a safety group or safety system.

IAEA Safety Standard, No. SSR-2/1, 5.40
The design shall take due account of the failure of a passive component, unless it has been justified in the single failure analysis with a high level of confidence that a failure of that component is very unlikely and that its function would remain unaffected by the postulated initiating event.

Krav avseende motverkandet av uppkomst av fel med gemensam orsak

Sverige

Krav

10 § Vid konstruktion, tillverkning, installation, idrifttagning, drift och underhåll av säkerhetssystem ska rimliga tekniska och administrativa åtgärder vidtas för att motverka uppkomst av fel med gemensam orsak.

Finland

Krav

14 § Säkerhetsfunktioner och tryggande av dem
… De effekter som en gemensam felorsak i säkerhetssystemen har på anläggningens säkerhet ska vara ringa…

YVL B.1 §469

Storbritannien

Övergripande principer

EDR.2 Redundancy, diversity and segregation
Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.

EDR.3 Common cause failure
Common cause failure (CCF) should be explicitly addressed where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability.

ERC.2 Shutdown systems
At least two diverse systems should be provided for shutting down a civil reactor.

Vägledande råd

168 The design should incorporate redundancy to avoid the effects of random failure, and diversity and segregation to avoid the effects of common cause failure. Examples of diversity are different operating conditions, different working principles or different design teams, different sizes of equipment, different manufacturers, different components, and types of equipment that use different physical methods. The design should also be tolerant of random failure occurring anywhere within the safety systems provided to secure each safety function.

171 CCF claims should be substantiated.

172 In general, claims for CCF should not be better than one failure per 100 000 demands. The figure of one failure per 100 000 demands represents a judgement by NII of the best limit that could reasonably be supported for a simple system by currently available data and methods of analysis. A worse figure may need to be used (say 1 per 10 000 or 1 per 1000) according to the complexity and novelty of the system, the nature of threat and the capability of the equipment.

173 Nevertheless, it is conceivable that the continuing accumulation of good data and advances in its analysis could lead, in exceptional circumstances, to a situation where a strong case could be made by the dutyholder for better figures. Such a case would not then be ruled out of consideration.

174 Where required reliabilities cannot be achieved due to CCF considerations, the required safety function should be achieved taking account of the concepts of diversity and segregation, and by providing at least two independent safety measures.

181 Usually, safety-related systems tend to be more complex than safety systems and are typically designed to less rigorous standards. Hence special attention should be devoted to potential common cause failures, due pessimism in assigned reliability values, availability, and measures to ensure that its safety significance will continue to be recognised throughout its life. This is particularly important where claims are made on combinations of more than one safety-related system.

Kanada

Krav

RD–337, 7.6.1 Common-cause Failures
Failure of a number of devices or components to perform their functions may occur as a result of a single specific event or cause. Common-cause failures may also occur when multiple components of the same type fail at the same time. This may be caused by such occurrences as a change in

ambient conditions, saturation of signals, repeated maintenance error or design deficiency.

The potential for common-cause failures of items important to safety is considered in determining where to apply the principles of diversity, separation, and independence to achieve the necessary reliability. Such failures may simultaneously affect a number of different items important to safety. The event or cause may be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human-induced event, or an unintended cascading effect from any other operation or failure within the plant.

The design provides sufficient physical separation between redundant divisions of safety support systems and process systems. This applies to equipment and to routing of the following items:

1. Electrical cables for power and control of equipment;
2. Piping for service water for the cooling of fuel and process equipment; and
3. Tubing and piping for compressed air or hydraulic drives for control equipment.

Where physical separation is not possible, safety support system equipment may share physical space. In such cases, the reasons for the lack of separation and justification for the space sharing arrangement is explained in the design documentation.

Where space sharing is necessary, services for safety and for other important process systems are arranged in a manner that incorporates the following considerations:

3. A safety system designed to act as backup is not located in the same space as the primary safety system; and
4. If a safety system and a process system must share space, then the associated safety functions are also provided by another safety system to counter the possibility of failures in the process system.

The design provides effective protection against common-cause events where sufficient physical separation among individual services or groups of services does not exist. The design authority assesses the effectiveness of specified physical separation or protective measures against common-cause events.

Diversity is applied to redundant systems or components that perform the same safety function by incorporating different attributes into the systems or components. Such attributes include different principles of operation, different physical variables, different conditions of operation, or production by different manufacturers.

It is important that any diversity used actually achieves the desired increase in reliability. For example, to reduce the potential for common-cause failures, the application of diversity is examined for any similarity in materials, components, and manufacturing processes, or subtle similarities in operating principles or common support features. If diverse components or

systems are used, there should be a reasonable assurance that such additions are of overall benefit, taking into account associated disadvantages such as the extra complication in operational, maintenance, and test procedures, or the consequent use of equipment of lower reliability.

RD–337, 9.3 Hazards Analysis
Hazards analysis is the process of collecting and evaluating information about the NPP to identify the associated hazards and determine those that are significant and must be addressed. A hazards analysis demonstrates the ability of the design to effectively respond to credible common-cause events.

As discussed in Section 9.1, the first step of the hazards analysis is to identify PIEs. For each common-cause PIE, the hazards analysis then identifies:

1. Applicable acceptance criteria (i.e., the success path criteria);
2. The hazardous materials in the plant and at the plant site;
3. All qualified mitigating SSCs credited during and following the event—all non-qualified safety or safety support systems are assumed to fail, except in cases where their continued operation would result in more severe consequences;
4. Operator actions and operating procedures for the event; and
5. Plant or operating procedure parameters for which the event is limiting.

The hazards analysis confirms that:

1. The plant design incorporates sufficient diversity and separation to cope with credible common-cause events;
2. Credited SSCs are qualified to survive and function during and following credible common-cause events, as applicable; and
3. The following criteria are met
    a) the plant can be brought to a safe shutdown state,
    b) the integrity of the fuel in the reactor core can be maintained,
    c) the integrity of the reactor coolant pressure boundary and containment can be maintained, and
    d) safety-critical parameters can be monitored by the operator.

The hazards analysis report includes the findings of the analysis and the basis for those findings. This report also:

1. Includes a general description of the physical characteristics of the plant that outlines the prevention and protection systems to be provided;
2. Includes the list of safe shutdown equipment;
3. Defines and describes the characteristics associated with hazards for all areas that contain hazardous materials;
4. Describes the performance criteria for detection systems, alarm systems, and mitigation systems, including requirements such as seismic or environmental qualification;

5. Describes the control and operating room areas and the protection systems provided for these areas, including additional facilities for maintenance and operating personnel;
6. Describes the operator actions and operating procedures of importance to the given analysis;
7. Identifies the plant parameters for which the event is limiting;
8. Explains the inspection, testing, and maintenance parameters needed to protect system integrity; and
9. Defines the emergency planning and coordination requirements for effective mitigation, including any necessary measures to compensate for the failure or inoperability of any active or passive protection system or feature.

USA

Krav

10 CFR 50 Appendix A, Criterion 22 Protection system independence.
The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

10 CFR 50 Appendix A, Criterion 24 Separation of Protection and Control Systems.
The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

10 CFR 50 Appendix A, Criterion 26 Reactivity control system redundancy and capability.
Two independent reactivity control systems of different design principles shall be provided. One of the systems shall use control rods, preferably including a positive means for inserting the rods, and shall be capable of reliably controlling reactivity changes to assure that under conditions of normal operation, including anticipated operational occurrences, and with appropriate margin for malfunctions such as stuck rods, specified acceptable fuel design limits are not exceeded. The second reactivity control system shall be capable of reliably controlling the rate of reactivity changes resulting from planned, normal power changes (including xenon burnout) to assure acceptable fuel design limits are not exceeded. One of the systems shall be capable of holding the reactor core subcritical under cold conditions.

10 CFR 50 Appendix A, Criterion 29 Protection Against Anticipated Operational Occurrences.
The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 21: Physical separation and independence of safety systems
Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.

IAEA Safety Standard, No. SSR-2/1, Requirement 24: Common cause failures
The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.

IAEA Safety Standard, No. SSR-2/1, 5.39
Spurious action shall be considered to be one mode of failure when applying the concept to a safety group or safety system.

IAEA Safety Standard, No. SSR-2/1, 5.40
The design shall take due account of the failure of a passive component, unless it has been justified in the single failure analysis with a high level of confidence that a failure of that component is very unlikely and that its function would remain unaffected by the postulated initiating event.

IAEA Safety Standard, No. SSR-2/1, 6.8
In judging the adequacy of the means of shutdown of the reactor, consideration shall be given to failures arising anywhere in the plant that could render part of the means of shutdown inoperative (such as failure of a control rod to insert) or that could result in a common cause failure.

IAEA Safety Standard, No. SSR-2/1, 6.37
For computer based equipment in safety systems or safety related systems:

(a) Common cause failures deriving from software shall be taken into consideration;
(b) Protection shall be provided against accidental disruption of, or deliberate interference with, system operation.

Krav avseende fysisk och funktionell separation

Sverige

Krav

11 § För att motverka samtidig utslagning av redundanta delar av säkerhetssystem, ska kärnkraftsreaktorn vara konstruerad så att de redundanta delarna och dess stödfunktioner har en tillräcklig fysisk och funktionell separation.

Graden av separation ska bestämmas med utgångspunkt från konsekvenserna i anläggningen av de inledande händelser som medför att säkerhetssystemet behöver tas i bruk.

Finland

Krav

14 § Säkerhetsfunktioner och tryggande av dem
Vid tryggande av säkerhetsfunktioner ska i första hand utnyttjas naturliga säkerhetsegenskaper som kan uppnås med goda planeringslösningar. I synnerhet ska samverkan av de fysikaliska återkopplingsfenomenen i kärnreaktorn vara sådan att den motverkar en ökning av reaktoreffekten.

De viktigaste system som behövs för övergång i kontrollerat läge och kvarhållandet av det ska kunna utföra sina funktioner även om en enskild komponent i vilket system som helst blir funktionsoduglig och även om vilken som helst annan komponent i samma system eller en komponent i ett stöd- eller hjälpsystem som är nödvändigt med tanke på dess funktion samtidigt är ur bruk på grund av behövliga reparationer eller underhåll.

Om naturliga säkerhetsegenskaper inte kan utnyttjas för att trygga en säkerhetsfunktion, ska sådana system och anordningar utnyttjas som inte kräver någon yttre drivkraft och som, om drivkraften går förlorad, ställer sig i ett ur säkerhetssynpunkt gynnsamt läge. …

… Vid planeringen av ifrågavarande system ska principer som säkerställer att säkerhetsfunktionen träder i funktion också vid felsituationer följas. Sådana principer är mångfalds-, åtskillnads- och olikhetsprincipen. …

... De effekter som en gemensam felorsak i säkerhetssystemen har på anläggningens säkerhet ska vara ringa.

Kärnkraftverket ska ha matarsystem för yttre och inre eleffekt. Säkerhetsfunktionerna ska kunna genomföras med användning av vilketdera som helst av dessa elmatarsystem…

YVL B.1 §411

YVL B.1 §413-414

YVL B.1 §445-447

Storbritannien

Övergripande principer

EDR.2 Redundancy, diversity and segregation
Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.

ESS.19 Dedication to a single task
A safety system should be dedicated to the single task of performing its safety function.

ESS.20 Avoidance of connections to other systems
Connections between any part of a safety system (other than the safety system support features) and a system external to the plant should be avoided.

Vägledande råd

352 Safety systems should be physically separate, independent, isolated from other systems, including safety-related systems, and share no equipment or services. There should be adequate segregation between independent parts of the safety system (including pipework and cabling) and also between a safety system and other facility equipment that, in the event of a fault, might jeopardise the safe working of the safety system.

354 If connections external to the plant cannot be avoided, for electrical, electronic or computer-based safety systems they should be restricted in function to that of monitoring only, and should incorporate adequate isolation features so that no fault associated with that equipment or its connections would jeopardise the function of the safety system.

Kanada

Krav

RD–337, 7.6.1 Common-cause Failures
Failure of a number of devices or components to perform their functions may occur as a result of a single specific event or cause. Common-cause failures may also occur when multiple components of the same type fail at the same time. This may be caused by such occurrences as a change in ambient conditions, saturation of signals, repeated maintenance error or design deficiency.

The potential for common-cause failures of items important to safety is considered in determining where to apply the principles of diversity, separation, and independence to achieve the necessary reliability. Such failures may simultaneously affect a number of different items important to safety. The event or cause may be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human-induced event, or an unintended cascading effect from any other operation or failure within the plant.

The design provides sufficient physical separation between redundant divisions of safety support systems and process systems. This applies to equipment and to routing of the following items:

4. Electrical cables for power and control of equipment;
5. Piping for service water for the cooling of fuel and process equipment; and
6. Tubing and piping for compressed air or hydraulic drives for control equipment.

Where physical separation is not possible, safety support system equipment may share physical space. In such cases, the reasons for the lack of separation and justification for the space sharing arrangement is explained in the design documentation.

Where space sharing is necessary, services for safety and for other important process systems are arranged in a manner that incorporates the following considerations:

5. A safety system designed to act as backup is not located in the same space as the primary safety system; and
6. If a safety system and a process system must share space, then the associated safety functions are also provided by another safety system to counter the possibility of failures in the process system.

The design provides effective protection against common-cause events where sufficient physical separation among individual services or groups of services does not exist. The design authority assesses the effectiveness of specified physical separation or protective measures against common-cause events.

Diversity is applied to redundant systems or components that perform the same safety function by incorporating different attributes into the systems or components. Such attributes include different principles of operation, different physical variables, different conditions of operation, or production by different manufacturers.

It is important that any diversity used actually achieves the desired increase in reliability. For example, to reduce the potential for common-cause failures, the application of diversity is examined for any similarity in materials, components, and manufacturing processes, or subtle similarities in operating principles or common support features. If diverse components or systems are used, there should be a reasonable assurance that such additions are of overall benefit, taking into account associated disadvantages such as the extra complication in operational, maintenance, and test procedures, or the consequent use of equipment of lower reliability.

RD–337, 7.12 Fire Safety
The design of the NPP, including that of external buildings and SSCs integral to plant operation, includes provisions for fire safety.

RD–337, 7.12.1 General Provisions
Suitable incorporation of operational procedures, redundant SSCs, physical

barriers, spatial separation, fire protection systems, and design for fail-safe operation achieves the following general objectives:

1. Prevents the initiation of fires;
2. Limits the propagation and effects of fires that do occur by
    a) quickly detecting and suppressing fires to limit damage, and
    b) confining the spread of fires and fire by-products that have not been extinguished;
3. Prevents loss of redundancy in safety and safety support systems;
4. Provides assurance of safe shutdown;
5. Ensures that monitoring of critical safety parameters remains available;
6. Prevents exposure, uncontrolled release, or unacceptable dispersion of hazardous substances, nuclear material, or radioactive material, due to fires;
7. Prevents the detrimental effects of event mitigation efforts, both inside and outside of containment; and
8. Ensures structural sufficiency and stability in the event of fire.

Buildings or structures are constructed using non-combustible or fire retardant and heat resistant material.

Fire is considered an internal hazard. The essential safety functions are therefore available during a fire.

Fire suppression systems are designed and located such that rupture, or spurious or inadvertent operation, will not significantly impair the capability of SSCs important to safety.

RD–337, 9.3 Hazards Analysis
Hazards analysis is the process of collecting and evaluating information about the NPP to identify the associated hazards and determine those that are significant and must be addressed. A hazards analysis demonstrates the ability of the design to effectively respond to credible common-cause events.

As discussed in Section 9.1, the first step of the hazards analysis is to identify PIEs. For each common-cause PIE, the hazards analysis then identifies:

1. Applicable acceptance criteria (i.e., the success path criteria);
2. The hazardous materials in the plant and at the plant site;
3. All qualified mitigating SSCs credited during and following the event—all non-qualified safety or safety support systems are assumed to fail, except in cases where their continued operation would result in more severe consequences;
4. Operator actions and operating procedures for the event; and
5. Plant or operating procedure parameters for which the event is limiting.

The hazards analysis confirms that:

1. The plant design incorporates sufficient diversity and separation to cope with credible common-cause events;

2. Credited SSCs are qualified to survive and function during and following credible common-cause events, as applicable; and
3. The following criteria are met
    a) the plant can be brought to a safe shutdown state,
    b) the integrity of the fuel in the reactor core can be maintained,
    c) the integrity of the reactor coolant pressure boundary and containment can be maintained, and
    d) safety-critical parameters can be monitored by the operator.

The hazards analysis report includes the findings of the analysis and the basis for those findings. This report also:

1. Includes a general description of the physical characteristics of the plant that outlines the prevention and protection systems to be provided;
2. Includes the list of safe shutdown equipment;
3. Defines and describes the characteristics associated with hazards for all areas that contain hazardous materials;
4. Describes the performance criteria for detection systems, alarm systems, and mitigation systems, including requirements such as seismic or environmental qualification;
5. Describes the control and operating room areas and the protection systems provided for these areas, including additional facilities for maintenance and operating personnel;
6. Describes the operator actions and operating procedures of importance to the given analysis;
7. Identifies the plant parameters for which the event is limiting;
8. Explains the inspection, testing, and maintenance parameters needed to protect system integrity; and
9. Defines the emergency planning and coordination requirements for effective mitigation, including any necessary measures to compensate for the failure or inoperability of any active or passive protection system or feature.

USA

Krav

10 CFR 50 Appendix A, Criterion 22 Protection system independence.
The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

10 CFR 50 Appendix A, Criterion 24 Separation of Protection and Control Systems.

The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

10 CFR 50 Appendix A, Criterion 26 Reactivity control system redundancy and capability.
Two independent reactivity control systems of different design principles shall be provided. One of the systems shall use control rods, preferably including a positive means for inserting the rods, and shall be capable of reliably controlling reactivity changes to assure that under conditions of normal operation, including anticipated operational occurrences, and with appropriate margin for malfunctions such as stuck rods, specified acceptable fuel design limits are not exceeded. The second reactivity control system shall be capable of reliably controlling the rate of reactivity changes resulting from planned, normal power changes (including xenon burnout) to assure acceptable fuel design limits are not exceeded. One of the systems shall be capable of holding the reactor core subcritical under cold conditions.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 21: Physical separation and independence of safety systems
Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.

IAEA Safety Standard, No. SSR-2/1, Requirement 24: Common cause failures
The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.

IAEA Safety Standard, No. SSR-2/1, Requirement 40: Prevention of harmful interactions of systems important to safety
The potential for harmful interactions of systems important to safety at the nuclear power plant that might be required to operate simultaneously shall be evaluated, and effects of any harmful interactions shall be prevented.

IAEA Safety Standard, No. SSR-2/1, Requirement 41: Interactions between the electrical power grid and the
Plant The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid,

including anticipated variations in the voltage and frequency of the grid supply.

IAEA Safety Standard, No. SSR-2/1, Requirement 64: Separation of protection systems and control systems
Interference between protection systems and control systems at the nuclear power plant shall be prevented by means of separation, by avoiding interconnections or by suitable functional independence.

IAEA Safety Standard, No. SSR-2/1, Requirement 66: Supplementary control room
Instrumentation and control equipment shall be kept available, preferably at a single location (a supplementary control room) that is physically, electrically and functionally separate from the control room at the nuclear power plant. The supplementary control room shall be so equipped that the reactor can be placed and maintained in a shutdown state, residual heat can be removed, and essential plant variables can be monitored if there is a loss of ability to perform these essential safety functions in the control room.

IAEA Safety Standard, No. SSR-2/1, 5.43
It shall not be permissible for a failure of a support service system to be capable of simultaneously affecting redundant parts of a safety system or a system fulfilling diverse safety functions and compromising the capability of these systems to fulfil their safety functions.

IAEA Safety Standard, No. SSR-2/1, 5.70
If two fluid systems important to safety are interconnected and are operating at different pressures, either the systems shall both be designed to withstand the higher pressure, or provision shall be made to prevent the design pressure of the system operating at the lower pressure from being exceeded.

IAEA Safety Standard, No. SSR-2/1, 6.38
If signals are used in common by both a protection system and any control system, separation (such as by adequate decoupling) shall be ensured and the signal system shall be classified as part of the protection system.

IAEA Safety Standard, No. SSR-2/1, 5.69
In the analysis of the potential for harmful interactions of systems important to safety, due account shall be taken of physical interconnections and of the possible effects of one system’s operation, maloperation or malfunction on local environmental conditions of other essential systems, to ensure that changes in environmental conditions do not affect the reliability of systems or components in functioning as intended.

Krav avseende tålighet mot händelser och förhållanden som kan uppkomma utanför eller inne i kärnkraftsanläggningen och som kan leda till en radiologisk olycka (inklusive rörbrott)

Sverige

Krav

12 § Kärnkraftsreaktorn ska vara tålig mot globala och lokala belastningar och andra effekter som kan uppstå vid ett rörbrott.

Konsekvenserna av ett rörbrott som inledande händelse, ska analyseras och värderas med avseende på hur sådana effekter påverkar barriärer och de säkerhetsfunktioner som tillgodoräknas vid rörbrottet.

13 § Lokala dynamiska effekter behöver inte beaktas i de delar av anläggningen där rörsystemen har givits en sådan utformning, sådana driftbetingelser och miljöförhållanden att förutsättningarna för skador i rörsystemen, till följd av kända och identifierbara degraderingsmekanismer, har reducerats så långt som möjligt och där åtgärder har vidtagits så att skador som trots detta kan uppkomma leder till detekterbara läckage innan brott inträffar.

Ytterligare bestämmelser om konstruktion, tillverkning och kontroll av rörsystem finns i Strålsäkerhetsmyndighetens föreskrifter (SSMFS 2008:13) om mekaniska anordningar i vissa kärntekniska anläggningar.

14 § Kärnkraftsreaktorn ska vara dimensionerad för att motstå naturfenomen och andra händelser som uppkommer utanför eller inne i anläggningen och som kan leda till en radiologisk olycka. För sådana naturfenomen och händelser ska dimensionerande värden vara fastställda. Naturfenomen och händelser med så snabbt förlopp att skyddsåtgärder inte hinner vidtas då de inträffar, ska dessutom händelseklassas. För varje slag av naturfenomen som kan leda till en radiologisk olycka ska det finnas en fastlagd handlingslinje för de situationer då de dimensionerande värdena riskerar att överskridas.

Finland

Krav

17 § Skydd mot yttre händelser[10]
Vid planeringen av ett kärnkraftverk ska sådana yttre händelser beaktas som kan hota genomförandet av säkerhetsfunktioner. System, konstruktioner och anordningar ska planeras, placeras och skyddas så att effekterna av yttre händelser på kraftverkets säkerhet blir små. Som yttre händelser ska beaktas åtminstone exceptionella väderförhållanden, seismiska fenomen och andra faktorer som beror på omgivningen eller mänskliga aktiviteter. Vid planeringen ska också möjligheten av lagstridig verksamhet i syfte att skada anläggningen samt av en kollision med ett stort trafikflygplan beaktas.

[10] Ytter händelser avser händelser som kan uppkomma utanför anläggningen och kan påverka anläggningens säkerhet. Yttre händelser innefattar bland annat naturfenomen, kemiska och bilogiska utsläpp i närregion, explosioner i närregion, flygplanskrascher samt händelser på det yttre elkraftnätet.

18 § Skydd mot inre händelser[11]
Vid planeringen av ett kärnkraftverk ska sådana inre händelser beaktas som kan hota genomförandet av säkerhetsfunktioner. System, konstruktioner och anordningar ska planeras, placeras och skyddas så att sannolikheten för inre händelser blir liten och deras effekter på kraftverkets säkerhet blir små. Som inre händelser ska beaktas åtminstone eldsvådor, översvämningar och explosioner samt att rörledningar, cisterner och anordningar går sönder och att tunga föremål faller ned.

YVL B.1 §411

Storbritannien

Övergripande principer

FA.5 Initiating faults
The safety case should list all initiating faults that are included within the design basis analysis of the facility.

EMT.8 Effect of internal/external events
Structures, systems and components important to safety should be inspected and/or re-validated after any internal or external event that might have challenged their design basis.

EHA.1 Identification
External and internal hazards that could affect the safety of the facility should be identified and treated as events that can give rise to possible initiating faults.

EHA.2 Data sources
For each type of external hazard either site specific or, if this is not appropriate, best available relevant data should be used to determine the relationship between event magnitudes and their frequencies.

EHA.3 Design basis events
For each internal or external hazard, which cannot be excluded on the basis of either low frequency or insignificant consequence, a design basis event should be derived.

EHA.4 Frequency of exceedance
The design basis event for an internal and external hazard should conservatively have a predicted frequency of exceedance in accordance with the fault analysis requirements (FA.5).

EHA.5 Operating conditions
Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition.

[11] Inre händelser avser alla tänkbara fel eller situationer som kan uppstå inom anläggningen och som kan påverka anläggningens säkerhet.

EHA.6 Analysis
Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects.

EHA.7 ‘Cliff-edge’ effects
A small change in DBA parameters should not lead to a disproportionate increase in radiological consequences.

EHA.8 Aircraft impact
The total predicted frequency of aircraft crash, including helicopters and other airborne vehicles, on or near any facility housing structures, systems and components important to safety should be determined.

EHA.9 Earthquakes
The seismology and geology of the area around the site and the geology of the site should be evaluated to derive a design basis earthquake (DBE).

EHA.10 Electromagnetic interference
The design of facility should include protective measures against the effects of electromagnetic interference.

EHA.11 Extreme weather
Nuclear facilities should withstand extreme weather conditions that meet the design basis event criteria.

EHA.12 Flooding
Nuclear facilities should withstand flooding conditions that meet the design basis event criteria.

EHA.13 Fire, explosion, missiles, toxic gases etc – use and storage of hazardous materials
The on-site use, storage or generation of hazardous materials should be minimised, and controlled and located so that any accident to, or release of, the materials will not jeopardise the establishing of safe conditions on the facility.

EHA.14 Fire, explosion, missiles, toxic gases etc – sources of harm
Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.

EHA.15 Fire, explosion, missiles, toxic gases etc – effect of water
The design of the facility should prevent water from adversely affecting structures, systems and components important to safety.

EHA.16 Fire, explosion, missiles, toxic gases etc – fire detection and fighting
Fire detection and fire-fighting systems of a capacity and capability commensurate with the credible worst-case scenarios should be provided.

EHA.17 Fire, explosion, missiles, toxic gases etc – use of materials
Non-combustible or fire-retardant and heat-resistant materials should be used throughout the facility.

EPS.1 Removable closures
The failure of a removable closure to a pressurised component or system that could lead to a major release of radioactivity should be prevented.

EPS.2 Flow limitation
Flow limiting devices should be provided to piping systems that are connected to or form branches from a main pressure circuit, to minimise the consequences of postulated breaches.

EPS.3 Pressure relief
Adequate pressure relief systems should be provided for pressurised systems and provision should be made for periodic testing.

EPS.4 Overpressure protection
Overpressure protection should be consistent with any pressure-temperature limits of operation.

EPS.5 Discharge routes
Pressure discharge routes should be provided with suitable means to ensure that any release of radioactivity from the facility to the environment is minimised.

ECE.23 Inspection of sea and river flood defences
Provision should be made for the routine inspection of sea and river flood defences to determine their continued fitness for purpose.

ESS.18 Failure independence
No fault, internal or external hazard should disable a safety system.

EMC.7 Loadings
For safety-related components and structures, the schedule of design loadings (including combinations of loadings), together with conservative estimates of their frequency of occurrence should be used as the basis for design against normal operating, plant transient, testing, fault and internal or external hazard conditions.

EMC.13 Materials
Materials employed in manufacture and installation should be shown to be suitable for the purpose of enabling an adequate design to be manufactured, operated, examined and maintained throughout the life of the facility.

EMC.14 Techniques and procedures
Manufacture and installation should use proven techniques and approved procedures to minimise the occurrence of defects that might affect the required integrity of components or structures.

EMC.15 Control of materials
Materials identification, storage and issue should be closely controlled.

EMC.16 Contamination
The potential for contamination of materials during manufacture and installation should be controlled to ensure the integrity of components and structures is not compromised.

EMC.17 Examination during manufacture
Provision should be made for examination during manufacture and

installation to demonstrate the required standard of workmanship has been achieved.

EMC.18 Third-party inspection
Manufacture and installation operations should be subject to appropriate third-party independent inspection to check that processes and procedures are being carried out as required.

EMC.19 Non-conformities
Where non-conformities with the procedures are judged to have a detrimental effect on integrity or significant defects are found and remedial work is necessary, the remedial work should be carried out to an approved procedure and should be subject to the same requirements as the original.

EMC.20 Records
Detailed records of manufacturing, installation and testing activities should be made and be retained in such a way as to allow review at any time during subsequent operation.

EMC.24 Operation
Facility operations should be monitored and recorded to demonstrate compliance with the operating limits and to allow review against the safe operating envelope defined in the safety case.

EMC.25 Leakage
Means should be available to detect, locate, monitor and manage leakage that could indicate the potential for an unsafe condition to develop or give rise to a significant radiological effect.

EMC.26 Forewarning of failure
Detailed assessment should be carried out where monitoring is claimed to provide forewarning of significant failure.

EMC.28 Margins
An adequate margin should exist between the nature of defects of concern and the capability of the examination to detect and characterise a defect.

EMC.34 Defect sizes
Where high reliability is required for components and structures and where otherwise appropriate, the sizes of crack-like defects of structural concern should be calculated using verified and validated fracture mechanics methods with verified application.

Vägledande råd

208 External hazards are those natural or man-made hazards to a site and facilities that originate externally to both the site and its processes, ie the dutyholder may have very little or no control over the initiating event. External hazards include earthquake, aircraft impact, extreme weather, electromagnetic interference (off-site cause) and flooding as a result of extreme weather/climate change (this list is not exhaustive). Terrorist or other malicious acts are assessed as external hazards. The dutyholder should demonstrate that an effective process has been applied to identify all types of external hazard relevant to a particular site.

209 Internal hazards are those hazards to plant and structures that originate within the site boundary but are, for example, external to the process in the case of nuclear chemical plant, or external to the primary circuit in the case of power reactors. That is, the dutyholder has control over the initiating event in some form. Internal hazards include internal flooding, fire, toxic gas release, dropped loads and explosion/missiles.

210 This sub-section starts with general principles, followed by principles for specific internal and external hazards.

211 This identification should include consequential events and, as appropriate, combinations of consequential events from a common initiating event.

212 Any generic type of hazard with a total frequency that is demonstrably below once in ten million years may be excluded. Any generic type of hazard, the impact of which has no effect on the safety of the facility, can also be excluded. This screening should retain all hazards for which the frequency of realisation and the potential impact might make a significant contribution to the overall risks from the facility.

213 The potential of a hazard to affect the safety of a facility may take account of factors such as the source of the hazard in relation to the facility and the design characteristics of the facility.

214 Some hazards may not be amenable to the derivation of a design basis event. Such hazards may include fire and lightning, but are addressed through appropriate application of codes and standards.

215 Consideration may also be given to arguments presented to derive the design basis event from a higher frequency of exceedance if the facility cannot give rise to high, unmitigated doses.

216 Where the radiological consequences arising from an external hazard are low, it may be appropriate for a facility to be designed to hazard loads using normal industrial standards.

217 To achieve the above two principles the analysis should take into account that:

a) certain internal or external hazards may not be independent of each other and may occur simultaneously or in a combination that it is reasonable to expect;
b) an internal or external hazard may occur simultaneously with a facility fault, or when plant is out for maintenance;
c) there is a significant potential for internal or external hazards to act as initiators of common cause failure, including loss of off-site power and other services;
d) many internal and external hazards have the potential to threaten more than one level of defence in depth at once;
e) internal hazards (eg fire) can arise as a consequence of faults internal or external to the site and should be included, therefore, in the relevant fault sequences; and

f) the severity of the effects of the internal or external hazard experienced by the facility may be affected by facility layout, interaction, and building size and shape.

218 The calculation of crash frequency should include the most recent crash statistics, flight paths and flight movements for all types of aircraft and take into account foreseeable changes in these factors if they affect the risk. (Malicious acts are dealt with separately).

219 Should the total predicted frequency of aircraft crash be shown to be lower than that typically defined as a design basis event, and greater than that which can be automatically excluded, efforts should be made to understand and minimise the potential impact consequences on structures, systems and components important to safety. The external hazard associated with the impacts should include the possibility of fires and/or explosions from aircraft fuel.

220 The studies should:

a) establish information on historical and instrumentally recorded earthquakes that have occurred in the region;
b) be proportionate to the radiological hazard posed by the site, while covering those aspects that could affect the estimation of the seismic hazard at the site; and
c) enable buildings, structures and plant in the nuclear facility to be designed to withstand safely the ground motions involved, if needed.

221 An operating basis earthquake (OBE) should also be determined. No structure, system or component important to safety should be impaired by the repeated occurrence of ground motions at the OBE level. Where the appropriate response to an OBE is a facility shutdown, the facility should not be restarted until inspection has shown that it is safe to do so.

222 In determining the effect of a seismic event on any facility, the simultaneous effect of that event on any other facility or installation in the vicinity, and on the safety of any system or service that may have a bearing on safety, should also be taken into account.

223 An assessment should be made to determine whether any source of electromagnetic interference either on-site or off-site could cause malfunction in or damage to safety-related equipment or instrumentation.

224 Types of extreme weather should include abnormal wind loadings, windblown debris, precipitation, accumulated ice and snow deposits, lightning, extremes of high and low temperature, humidity and drought.

225 The design basis event should take account of reasonable combinations of extreme weather conditions that may be expected to occur, and of the effect of failure of any non-nuclear hazardous installations off-site and other nuclear facilities, on- or off-site, during such conditions.

226 The reasonably foreseeable effects of climate change over the lifetime of the facility should be taken into account.

227 The area around the site should be evaluated to determine the potential for flooding due to external hazards eg precipitation, high tides, storm

surges, barometric effects, overflowing of rivers and upstream structures, coastal erosion, seiches and tsunamis.

228 The design basis flood should take account, as appropriate, of the combined effects of high tide, wind effects, wave actions, duration of the flood and flow conditions.

229 The potential for generation of hazardous materials (including toxic, corrosive and flammable) through normal or abnormal processes should be considered.

230 This identification should take into account:

a) projects and planned future developments on and off the site;
b) the adequacy of protection of the nuclear facility from the effects of any incident in an installation, means of transport, pipeline, power supplies, water supplies etc either inside or outside the nuclear site.
c) sources could be either on or off the site;

231 The design of the facility should include adequate provision for the collection and discharge of water reaching the site from any design basis external event or internal flooding hazard or, if this is not achievable, the structures, systems and components important to safety should be adequately protected against the effects of water.

232 The systems should be designed and located so that any damage they may sustain or their spurious operation does not affect the safety of the facility.

233 A fire hazard analysis should be made of the facility to:

a) analyse the potential for fire initiation and growth and the possible consequences on safety systems and other structures, systems and components important to safety;
b) determine the need for segregation of plant and the location and required fire resistance of boundaries to limit the spread of fire; and
c) determine the capacity and capability of the detection and fire-fighting systems to be provided.

234 In such situations:

a) adequate redundancy and where appropriate, diversity of closure method should be provided; and
b) provision should be made to ensure closures cannot be removed when it is unsafe to do so.

235 The flow limiting devices should be as close to the main circuit as practicable. There should be redundancy and diversity of such devices. Closure times of valves and the flow conditions under which they can close should be consistent with the protection they are claimed to provide. Dynamic loadings due to valve closure should be considered.

236 Basic characteristics of pressure relief are the pressure at which the relief actuates and the flow capacity of the relief route. The differences between the pressures for first actuation, full relief flow and termination of relief need to be considered. If the pressure relief system is a combination of

relief valves and an active protection system to terminate generation of energy or mass input (eg reactor trip), the case for the system as a whole needs to be made.

237 In some circumstances the safe operating pressure of a system may vary with temperature (eg a ferritic reactor vessel moving from cold shutdown to normal operation). The overpressure protection system should provide protection for all operating temperatures. This may require the provision of programmable safety relief valves that can be reset as the pressure vessel temperature changes.

301 This provision should cover such aspects as erosion and degradation of materials and structures that protect the site. Provision should be made for non-routine inspection following extreme weather or other indications of degradation.

422 The potential for a fire can have a major impact on the design of the ventilation and containment system, influencing for example the position, number and type of fire dampers. Where fire dampers are provided, their position and operation should not compromise the containment function, and their effect on the ventilation system should be considered. In addition to the principles in this sub-section, other impacts of fire may need to be considered, and reference should be made to the principles on protection against fire (paragraph 228 ff.).

Kanada

Krav

RD–337, 6.6 Facility Layout
The design takes into account the interfaces between the safety and security provisions of the NPP and other aspects of the facility layout, such as:

1. Access routes for normal operational actions and maintenance;
2. Access control to minimize radiation exposures;
3. Actions taken in response to internal or external events;
4. Egress routes;
5. Movement of hazardous substances, nuclear materials, and radioactive materials;
6. Movement of authorized and unauthorized personnel; and
7. Interaction of building and support functions.

It is likely that some design requirements associated with these factors will conflict with others in the determination of facility layout requirements. The design therefore reflects an assessment of options, demonstrating that an optimized configuration has been sought for the facility layout.

RD–337, 7.4 Postulated Initiating Events Considered in the Design
Postulated initiating events can lead to AOO or accident conditions, and include credible failures or malfunctions of SSCs, as well as operator errors, common-cause internal hazards, and external hazards.

RD–337, 7.4.1 Internal Hazards
SSCs important to safety are designed and located in a manner that minimizes the probability and effects of fires and explosions caused by external or internal events.

The plant design takes into account the potential for internal hazards, such as flooding, missile generation, pipe whip, jet impact, fire, smoke, and combustion by-products, or release of fluid from failed systems or from other installations on the site. Appropriate preventive and mitigation measures are provided to ensure that nuclear safety is not compromised.

The design considers the possible interaction of external and internal events, such as external events initiating internal fires or floods that may lead to the generation of missiles.

Where two fluid systems operating at different pressures are interconnected, failure of the interconnection is considered. Either both withstand the higher pressure, or provision is made so that the pressure of the system operating at the lower pressure will not be exceeded.

RD–337, 7.4.2 External Hazards
The design considers all natural and human-induced external events that may be linked with significant radiological risk. The subset of external events that the plant is designed to withstand is selected, and design basis events are determined from this subset.

Various interactions between the plant and the environment, such as population in the surrounding area, meteorology, hydrology, geology and seismology are identified during the site evaluation and environmental assessment processes. These interactions are taken into account in determining the design basis for the NPP.

Applicable natural external hazards include such events as earthquakes, droughts, floods, high winds, tornadoes, tsunami, and extreme meteorological conditions. Human-induced external events include those that are identified in the site evaluation, such as potential aircraft crashes, ship collisions, and terrorist activities.

RD–337, 7.4.3 Combinations of Events
Combinations of randomly occurring individual events that could credibly lead to AOOs, DBAs, or BDBAs are considered in the design. Such combinations are identified early in the design phase, and are confirmed using a systematic approach.

Events that may result from other events, such as a flood following an earthquake, are considered to be part of the original PIE.

RD–337, 7.12 Fire Safety
The design of the NPP, including that of external buildings and SSCs integral to plant operation, includes provisions for fire safety.

RD–337, 7.12.1 General Provisions
Suitable incorporation of operational procedures, redundant SSCs, physical barriers, spatial separation, fire protection systems, and design for fail-safe operation achieves the following general objectives:

1. Prevents the initiation of fires;
2. Limits the propagation and effects of fires that do occur by
    a) quickly detecting and suppressing fires to limit damage, and
    b) confining the spread of fires and fire by-products that have not been extinguished;
3. Prevents loss of redundancy in safety and safety support systems;
4. Provides assurance of safe shutdown;
5. Ensures that monitoring of critical safety parameters remains available;
6. Prevents exposure, uncontrolled release, or unacceptable dispersion of hazardous substances, nuclear material, or radioactive material, due to fires;
7. Prevents the detrimental effects of event mitigation efforts, both inside and outside of containment; and
8. Ensures structural sufficiency and stability in the event of fire.

Buildings or structures are constructed using non-combustible or fire retardant and heat resistant material.

Fire is considered an internal hazard. The essential safety functions are therefore available during a fire.

Fire suppression systems are designed and located such that rupture, or spurious or inadvertent operation, will not significantly impair the capability of SSCs important to safety.

RD–337, 7.13.1 Seismic Design and Classification
The design authority identifies SSCs important to safety that are credited to withstand a design basis earthquake (DBE), and ensures that they are qualified accordingly. This applies to:

1. SSCs whose failure could directly or indirectly cause an accident leading to core damage;
2. SSCs restricting the release of radioactive material to the environment;
3. SSCs that assure the subcriticality of stored nuclear material; and
4. SSCs such as radioactive waste tanks containing radioactive material that, if released, would exceed regulatory dose limits.

The design of these SSCs also meets the DBE criteria to maintain all essential attributes, such as pressure boundary integrity, leak-tightness, operability, and proper position in the event of a DBE.

The design provides that no substantive damage to these SSCs will be caused by the failure of any other SSC under DBE conditions.

Seismic fragility levels should be evaluated for SSCs important to safety by analysis or, where possible, by testing.

RD–337, 7.7 Pressure-retaining SSCs
All pressure-retaining SSCs are protected against overpressure conditions, and are classified, designed, fabricated, erected, inspected, and tested in accordance with established standards.

All pressure-retaining SSCs of the reactor coolant system and auxiliaries are designed with an appropriate safety margin to ensure that the pressure boundary will not be breached, and that fuel design limits will not be exceeded in normal operation, AOOs, or DBA conditions.

The design minimizes the likelihood of flaws in pressure boundaries. This includes timely detection of flaws in pressure boundaries important to safety in a manner that supports leak-before-break detection capability.

Unless otherwise justified, all pressure boundary SSCs are designed to withstand static and dynamic loads anticipated in normal operation, AOOs, and DBAs.

SSC design includes protection against postulated pipe ruptures, unless otherwise justified.

The operation of pressure relief devices does not lead to unacceptable releases of radioactive material from the plant.

Adequate isolation is provided at the interfaces between the reactor coolant system (RCS) and connecting systems operating at lower pressures to prevent the overpressure of such systems and possible loss of coolant accidents. Consideration is given to the characteristics and importance of the isolation and its reliability targets. Isolation devices are either closed or close automatically on demand. The response time and speed of closure are in accordance with the acceptance criteria defined for postulated initiating events.

All pressure boundary piping and vessels are separated from electrical and control systems to the greatest extent practicable.

Pressure-retaining components whose failure will affect nuclear safety are designed to permit inspection of their pressure boundaries throughout the design life. If full inspection is not achievable, then it is augmented by indirect methods such as a program of surveillance of reference components. Leak detection is an acceptable method when the SSC is leak-before-break qualified.

RD–337, 7.15 Civil Structures

RD–337, 7.15.1 Design
The NPP design specifies the required performance for the safety functions of the civil structures under normal operation and accident conditions.

Civil structures important to safety are designed and located so as to minimize the probabilities and effects of internal hazards such as fire, explosion, smoke, flooding, missile generation, pipe whip, jet impact, or release of fluid due to pipe breaks.

External events such as earthquakes, floods, high winds, tornadoes, tsunamis, and extreme meteorological conditions are considered in the design of civil structures.

Settlement analysis and evaluation of soil capacity includes consideration of the effects of fluctuating ground water on the foundations, and identification and evaluation of potential liquefiable soil strata and slope failure.

Civil structures are designed to meet the serviceability, strength, and stability requirements for all possible load combinations under normal operation, AOO, and DBA conditions, and in the event of external hazards. The serviceability considerations include, without being limited to, deflection, vibration, permanent deformation, cracking, and settlement.

The design specifications also define all loads and load combinations, with due consideration given to concurrence probability and loading time history.

Environmental effects are considered in the design of civil structures and the selection of construction materials. The choice of construction material is commensurate with the designed service life and potential life extension of the plant.

The plant safety assessment includes structural analyses for all civil structures important to safety.

RD–337, 8.6.5 Containment Penetrations
The number of penetrations through the containment will be kept to a minimum.

All containment penetrations are subject to the same design expectations as the containment structure itself, and are to be protected from reaction forces stemming from pipe movement or accidental loads, such as those due to missiles, jet forces, and pipe whip.

All penetrations are designed to allow for periodic inspection.

If resilient seals such as elastomeric seals, electrical cable penetrations, or expansion bellows are used with penetrations, they have the capacity for leak testing at the containment design pressure. To demonstrate continued integrity over the lifetime of the plant, this capacity supports testing that is independent of determining the leak rate of the containment as a whole.

RD–337, 9.3 Hazards Analysis
Hazards analysis is the process of collecting and evaluating information about the NPP to identify the associated hazards and determine those that are significant and must be addressed. A hazards analysis demonstrates the ability of the design to effectively respond to credible common-cause events.

As discussed in Section 9.1, the first step of the hazards analysis is to identify PIEs. For each common-cause PIE, the hazards analysis then identifies:

1. Applicable acceptance criteria (i.e., the success path criteria);
2. The hazardous materials in the plant and at the plant site;
3. All qualified mitigating SSCs credited during and following the event—all non-qualified safety or safety support systems are assumed to fail, except in cases where their continued operation would result in more severe consequences;
4. Operator actions and operating procedures for the event; and
5. Plant or operating procedure parameters for which the event is limiting.

The hazards analysis confirms that:

1. The plant design incorporates sufficient diversity and separation to cope with credible common-cause events;
2. Credited SSCs are qualified to survive and function during and following credible common-cause events, as applicable; and
3. The following criteria are met
    a) the plant can be brought to a safe shutdown state,
    b) the integrity of the fuel in the reactor core can be maintained,
    c) the integrity of the reactor coolant pressure boundary and containment can be maintained, and
    d) safety-critical parameters can be monitored by the operator.

The hazards analysis report includes the findings of the analysis and the basis for those findings. This report also:

1. Includes a general description of the physical characteristics of the plant that outlines the prevention and protection systems to be provided;
2. Includes the list of safe shutdown equipment;
3. Defines and describes the characteristics associated with hazards for all areas that contain hazardous materials;
4. Describes the performance criteria for detection systems, alarm systems, and mitigation systems, including requirements such as seismic or environmental qualification;
5. Describes the control and operating room areas and the protection systems provided for these areas, including additional facilities for maintenance and operating personnel;
6. Describes the operator actions and operating procedures of importance to the given analysis;
7. Identifies the plant parameters for which the event is limiting;
8. Explains the inspection, testing, and maintenance parameters needed to protect system integrity; and
9. Defines the emergency planning and coordination requirements for effective mitigation, including any necessary measures to compensate for the failure or inoperability of any active or passive protection system or feature.

USA

Krav

10 CFR 50 Appendix A, Criterion 4, Environmental and dynamic effects design bases.
SSC important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These SSC shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit. However, dynamic effects

associated with postulated pipe ruptures in nuclear power units may be excluded from the design basis when analyses reviewed and approved by the Commission demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping.

10 CFR 50 Appendix A, Criterion 50, Containment design basis. The reactor containment structure, including access openings, penetrations, and the containment heat removal system shall be designed so that the containment structure and its internal compartments can accommodate, without exceeding the design leakage rate and with sufficient margin, the calculated pressure and temperature conditions resulting from any loss-of-coolant accident. This margin shall reflect consideration of (1) the effects of potential energy sources which have not been included in the determination of the peak conditions, such as energy in steam generators and as required by § 50.44 energy from metal-water and other chemical reactions that may result from degradation but not total failure of emergency core cooling functioning, (2) the limited experience and experimental data available for defining accident phenomena and containment responses, and (3) the conservatism of the calculational model and input parameters.

10 CFR 50 Appendix A, Criterion 2, Design bases for protection against natural phenomena.
SSC important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. The design bases for these SSC shall reflect: (1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena and (3) the importance of the safety functions to be performed.

10 CFR 50 Appendix A, Criterion 3, Fire protection.
SSC important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Non combustible and heat resistant materials shall be used wherever practical throughout the unit, particularly in locations such as the containment and control room. Fire detection and fighting systems of appropriate capacity and capability shall be provided and designed to minimize the adverse effects of fires on SSC important to safety. Fire fighting systems shall be designed to assure that their rupture or inadvertent operation does not significantly impair the safety capability of these SSC.

10 CFR 50.48 Fire Protection

10 CFR 50.63 Loss of all alternating current power

50.150 Aircraft Impact Assessment
(1) Assessment. Each applicant listed in paragraph (a)(3) shall perform a design-specific assessment of the effects on the facility of the impact of a large, commercial aircraft. Using realistic analyses, the applicant shall

identify and incorporate into the design those design features and functional capabilities to show that, with reduced use of operator actions:

(i) The reactor core remains cooled, or the containment remains intact; and

(ii) Spent fuel cooling or spent fuel pool integrity is maintained.

Guide

RG1.59 ""Design Basis Floods for Nuclear Power Plants"

RG1.76 "Design Basis Tornado for Nuclear Power Plants"

RG1.102 "Flood Protection for Nuclear Power Plants".

Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition — Design of Structures, Components, Equipment, and Systems (NUREG-0800, Chapter 3) SRP 3.5.1.6 Aircraft Hazards.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 16: Postulated initiating events
The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design.

IAEA Safety Standard, No. SSR-2/1, Requirement 17: Internal and external hazards
All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered for determination of the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant.

IAEA Safety Standard, No. SSR-2/1, 5.6
The postulated initiating events shall include all foreseeable failures of structures, systems and components of the plant, as well as operating errors and possible failures arising from internal and external hazards, whether in full power, low power or shutdown states.

IAEA Safety Standard, No. SSR-2/1, 5.16
The design shall take due account of internal hazards such as fire, explosion, flooding, missile generation, collapse of structures and falling objects, pipe whip, jet impact and release of fluid from failed systems or from other installations on the site. Appropriate features for prevention and mitigation shall be provided to ensure that safety is not compromised.

IAEA Safety Standard, No. SSR-2/1, 5.17
The design shall include due consideration of those natural and human induced external events (i.e. events of origin external to the plant) that have been identified in the site evaluation process. Natural external events shall be addressed, including meteorological, hydrological, geological and seismic events. Human induced external events arising from nearby industries and transport routes shall be addressed. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and fire fighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available.

IAEA Safety Standard, No. SSR-2/1, 5.18
Items important to safety shall be designed and located to minimize, consistent with other safety requirements, the likelihood of external events and their possible harmful consequences.

IAEA Safety Standard, No. SSR-2/1, 5.19
Features shall be provided to minimize any interactions between buildings containing items important to safety (including power cabling and control cabling) and any other plant structure as a result of external events considered in the design.

IAEA Safety Standard, No. SSR-2/1, 5.20
The design shall be such as to ensure that items important to safety are capable of withstanding the effects of external events considered in the design, and if not, other features such as passive barriers shall be provided to protect the plant and to ensure that the required safety function will be performed.

IAEA Safety Standard, No. SSR-2/1, 5.21
The seismic design of the plant shall provide for a sufficient safety margin to protect against seismic events and to avoid cliff edge effects (see footnote 5).

IAEA Safety Standard, No. SSR-2/1, 5.22
For multiple unit plant sites, the design shall take due account of the potential for specific hazards giving rise to simultaneous impacts on several units on the site.

IAEA Safety Standard, No. SSR-2/1, 5.32
Where the results of engineering judgement, deterministic safety assessments and probabilistic safety assessments indicate that combinations of events could lead to anticipated operational occurrences or to accident conditions, such combinations of events shall be considered to be design basis accidents or shall be included as part of design extension conditions, depending mainly on their likelihood of occurrence. Certain events might be consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered to be part of the original postulated initiating event.

Guide

Modifications to Nuclear Power Plants Safety Guide, Series No. NS-G-2.3, October 23, 2001.

Krav avseende underhåll samt planerat underhåll under drift och reparation under drift

Sverige

Krav

15 § Utrustning som har krav på driftklarhet får ställas av för planerat underhåll under drift, om kärnkraftsreaktorn är konstruerad så att de berörda säkerhetssystemen tål enkelfel i samband med åtgärderna, och den tillämpade diversifieringen och separationen av den berörda säkerhetsfunktionen kan upprätthållas.

16 § Utrustning som har krav på driftklarhet får ställas av för reparation och provning under drift, om kärnkraftsreaktorn är konstruerad så att säkerhetsfunktionerna enligt 3 § tål enkelfel i samband med åtgärderna. Sådan reparation och provning får tillämpas, även om en säkerhetsfunktion inte tål enkelfel under ingreppet, under förutsättning att en säkerhetsanalys visar att det riskbidrag som på så sätt uppkommer är mycket litet.

Finland

Krav

14 § Säkerhetsfunktioner och tryggande av dem
… De viktigaste system som behövs för övergång i kontrollerat läge och kvarhållandet av det ska kunna utföra sina funktioner även om en enskild komponent i vilket system som helst blir funktionsoduglig och även om vilken som helst annan komponent i samma system eller en komponent i ett stöd- eller hjälpsystem som är nödvändigt med tanke på dess funktion samtidigt är ur bruk på grund av behövliga reparationer eller underhåll.

23 § Driftverksamhet
… För underhåll och reparation av anordningarna ska det finnas skriftliga föreskrifter och anvisningar i anslutning därtill. …

26 § Övervakning av skick samt underhåll
Kärnkraftverk ska ha ett program för övervakning av kraftverkets skick och underhåll av kraftverket för att säkerställa systemens, konstruktionernas och anordningarnas integritet och tillförlitliga funktion. I programmet anges inspektioner, provningar, underhåll och byten samt andra förfaranden för övervakning av anläggningens skick och verkningar av dess driftsmiljö.

YVL B.1 §408

YVL B.1 Appendix D §108

Storbritannien

Övergripande principer

ECM.1 Commission testing
Before operating any facility or process that may affect safety it should be subject to commissioning tests to demonstrate that, as built, the design intent claimed in the safety case has been achieved.

EMT.1 Identification of requirements
Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.

EMT.2 Frequency
Structures, systems and components important to safety should receive regular and systematic examination, inspection, maintenance and testing.

EMT.3 Type-testing
Structures, systems and components important to safety should be type tested before they are installed to conditions equal to, at least, the most severe expected in all modes of normal operational service.

EMT.4 Validity of equipment qualification
The validity of equipment qualification for structures, systems and components important to safety should not be unacceptably degraded by any modification or by the carrying out of any maintenance, inspection or testing activity.

EMT.5 Procedures
Commissioning and in-service inspection and test procedures should be adopted that ensure initial and continuing quality and reliability.

EMT.6 Reliability claims
Provision should be made for testing, maintaining, monitoring and inspecting structures, systems and components important to safety in service or at intervals throughout plant life commensurate with the reliability required of each item.

EMT.7 Functional testing
In-service functional testing of systems, structures and components important to safety should prove the complete system and the safety-related function of each component.

EMC.27 Examination
Provision should be made for examination that is reliably capable of demonstrating that the component or structure is manufactured to the required standard and is fit for purpose at all times during service.

EMC.28 Margins
An adequate margin should exist between the nature of defects of concern and the capability of the examination to detect and characterise a defect.

EMC.29 Redundancy and diversity
Examination of components and structures should be sufficiently redundant and diverse.

EMC.30 Control
Personnel, equipment and procedures should be qualified to an extent

consistent with the overall safety case and the contribution of examination to the structural integrity aspect of the safety case.

EMC.31 Repairs and modifications
In-service repairs and modifications should be carefully controlled through a formal procedure for change.

ESS.24 Minimum operational equipment requirements
The minimum amount of operational safety system equipment for which any specified facility operation will be permitted should be defined and shown to meet the single failure criterion.

ESS.25 Safety system vetoes
The vetoing or the taking out of service of any safety system function should be avoided.

Vägledande råd

182 The commissioning tests should endeavour to identify any errors made during the design, manufacture, or construction/installation stages.

183 Commissioning should be more than a demonstration that the plant will work. It should also include safety tests as a key step in assuring safety. This is the intent of Licence Condition 21 (see the HSE website). The tests should be designed to demonstrate that the plant and associated safety systems provide the intended degree of protection against faults, including human errors.

184 The safety case should identify those commissioning tests and inspections required to:

a) confirm the facility's design safety assumptions and predicted performance, in particular that of the safety provisions; and
b) characterise the facility as a basis for evaluating its behaviour during its operational life. The safety analysis should be reviewed in the light of the results of the commissioning programme and of any modifications made to the design or intended operating procedures since the commencement of construction.

185 The tests should be divided into stages to complete as much inactive testing before the introduction of radioactive substance. Inactive testing should demonstrate that the facility has been constructed, manufactured, and installed correctly. Where any deviations from the documentation are found, the licensee should demonstrate that this does not compromise the safety analysis in the safety case.

186 Inactive testing should also be used to confirm the operational features of the facility and be used to develop the operating instructions, which should then be confirmed during active commissioning. Before active commissioning can begin, the necessary arrangements to satisfy Principles MS.2 (paragraph 51 f.) and SC.6 (paragraph 95 f.), especially in relation to operating limits and conditions, together with accident management and emergency preparedness, should be in place.

187 Appropriate and sufficient locations should be provided within the plant where process materials, plant items, construction materials and other items arising from plant breakdown, maintenance or refurbishment can be temporarily stored so that their level of contamination, chemical and physical properties, ease of decontamination and repair can be assessed.

188 For components of particular concern and where it is not possible to confirm the ability to operate under the most onerous design conditions, reference data from commissioning or rig testing should be established for comparison against in-service test results.

189 Such inspection should be of sufficient extent and frequency to give adequate confidence that degradation will be detected before loss of the safety function

190 In especially difficult circumstances where this cannot be done, either additional design measures should be incorporated to compensate for the deficiency, or it should be demonstrated that the adequate long-term performance would be achieved without such measures.

191 Where test equipment, or other engineered means, is claimed as part of in-service or periodic testing, maintenance, monitoring and inspection provisions, the extent to which they reveal failures affecting safety functions should be justified. The test equipment, or other engineered means, should be tested at intervals sufficient to uphold the reliability claims of the equipment within which it is claimed to reveal faults.

192 Maintenance, inspection and testing are a part of normal operation and it should be possible to carry out these tests without any loss of any safety function.

193 Where complete functional testing is claimed not to be reasonably practicable, an equivalent means of functional proving should be demonstrated.

271 This principle applies to both pre-service and in-service inspection and so does not preclude ongoing confirmation by in-service inspection.

272 The nuclear safety classification should be taken into account when determining the appropriate extent of the redundancy, diversity and qualification requirements.

273 For physical changes to plant, the principles of design, manufacture and installation should be used. Changes to defined limits of operation, monitoring, examination, testing and maintenance should be dealt with as modifications. Incidental consequences of a change should be considered for their significance, not just the direct purpose of the change.

358 Where such action is proposed, each need should be justified and the adequacy of its implementation demonstrated. In a safety system comprising several redundant or diverse sub-systems no single action should affect more than one sub-system.

Kanada

Krav

RD–337, 7.6.4 Allowance for Equipment Outages
The design includes provisions for adequate redundancy, reliability, and effectiveness, to allow for online maintenance and online testing of systems important to safety, except where these activities are not possible due to access control restrictions.

The design considers the time allowed for each equipment outage and the respective response actions.*Guide*

USA

Krav

10 CFR 50.65(a)(4) requires that licensees perform assessments before maintenance activities are performed on SSCs covered by the Maintenance Rule and manage the increase in risk that may result from the proposed activities.

10 CFR 50 Appendix A, Criterion 21, Protection system reliability and testability.
The protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

10 CFR 50 Appendix A, Criterion 37, Testing of emergency core cooling system.
The emergency core cooling system shall be designed to permit appropriate periodic pressure and functional testing to assure (1) the structural and leaktight integrity of its components, (2) the operability and performance of the active components of the system, and (3) the operability of the system as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the system into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.

10 CFR 50 Appendix A, Criterion 40, Testing of containment heat removal system.
The containment heat removal system shall be designed to permit appropriate periodic pressure and functional testing to assure (1) the structural and leaktight integrity of its components, (2) the operability and performance of the active components of the system, and (3) the operability

of the system as a whole, and under conditions as close to the design as practical the performance of the full operational sequence that brings the system into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.

10 CFR 50 Appendix A, Criterion 43, Testing of containment atmosphere cleanup systems.
The containment atmosphere cleanup systems shall be designed to permit appropriate periodic pressure and functional testing to assure (1) the structural and leaktight integrity of its components, (2) the operability and performance of the active components of the systems such as fans, filters, dampers, pumps, and valves and (3) the operability of the systems as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the systems into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of associated systems.

10 CFR 50 Appendix A, Criterion 46, Testing of cooling water system.
The cooling water system shall be designed to permit appropriate periodic pressure and functional testing to assure (1) the structural and leaktight integrity of its components, (2) the operability and the performance of the active components of the system, and (3) the operability of the system as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the system into operation for reactor shutdown and for loss-of-coolant accidents, including operation of applicable portions of the protection system and the transfer between normal and emergency power sources.

10 CFR 50 Appendix A, Criterion 52, Capability for containment leakage rate testing.
The reactor containment and other equipment which may be subjected to containment test conditions shall be designed so that periodic integrated leakage rate testing can be conducted at containment design pressure.

10 CFR 50 Appendix A, Criterion 53, Provisions for containment testing and inspection.
The reactor containment shall be designed to permit (1) appropriate periodic inspection of all important areas, such as penetrations, (2) an appropriate surveillance program, and (3) periodic testing at containment design pressure of the leaktightness of penetrations which have resilient seals and expansion bellows.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, 5.46
Where items important to safety are planned to be calibrated, tested or maintained during power operation, the respective systems shall be designed

for performing such tasks with no significant reduction in the reliability of performance of the safety functions. Provisions for calibration, testing, maintenance, repair, replacement or inspection of items important to safety during shutdown shall be included in the design so that such tasks can be performed with no significant reduction in the reliability of performance of the safety functions.

IAEA Safety Standard, No. SSR-2/1, 5.47
If an item important to safety cannot be designed to be capable of being tested, inspected or monitored to the extent desirable, a robust technical justification shall be provided that incorporates the following approach:

(a) Other proven alternative and/or indirect methods such as surveillance testing of reference items or use of verified and validated calculational methods shall be specified.
(b) Conservative safety margins shall be applied or other appropriate precautions shall be taken to compensate for possible unanticipated failures.

Guider

Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants Safety Guide, Series No. NS-G-2.6, October 29, 2002.

Krav avseende åldring

Sverige

-

Finland

Krav

5 § Hantering av åldrande
I planeringen och uppförandet av ett kärnkraftverk ska beaktas att de system, konstruktioner och anordningar som är av betydelse för säkerheten föråldras. Genom uppföljning av systemens, konstruktionernas och anordningarnas skick säkerställs att dessa förblir funktionsdugliga och uppfyller de krav som planeringen baseras på.

Ersättandet av dem med ny eller liknande teknik samt ändringarna och reparationerna ska göras systematiskt.

Storbritannien

Övergripande principer

EAD.1 Safe working life
The safe working life of structures, systems and components that are important to safety should be evaluated and defined at the design stage.

EAD.2 Lifetime margins
Adequate margins should exist throughout the life of a facility to allow for the effects of materials ageing and degradation processes on structures, systems and components that are important to safety.

EAD.3 Periodic measurement of material properties
Where material properties could change with time and affect safety, provision should be made for periodic measurement of the properties.

EAD.4 Periodic measurement of parameters
Where parameters relevant to the design of plant could change with time and affect safety, provision should be made for their periodic measurement.

EAD.5 Obsolescence
A process for reviewing the obsolescence of structures, systems and components important to safety should be in place.

Vägledande råd

194 Particular attention should be given to the evaluation of those components that are judged to be difficult or impracticable to replace.

195 There should be an adequate margin between the intended operational life and the predicted safe working life of such structures, systems and components.

196 The design process and periodic reviews should allow for any uncertainties in determining the initial state of components and the rate of ageing and degradation.

197 Programmes for monitoring, inspection, sampling, surveillance and testing, to detect and monitor ageing and degradation processes, should be used to verify assumptions and assess whether the margins will be adequate for the remaining life of the structure, system or component.

198 Appropriate testing of material aged under representative conditions should be undertaken and the results reviewed against the safety case expectations for such changes.

199 The effects of and interactions between the mechanical, thermal, chemical, physical, biological and radiation environment on materials properties, materials ageing and degradation processes should be considered.

200 Timely mitigation of ageing and its effects should be undertaken to ensure that the required safety margins are maintained.

201 The properties should be obtained from fully representative samples of material especially when the component or structure forms a principal means of ensuring nuclear safety.

202 This principle is more likely to be applicable to systems and components rather than the main structural elements of a facility. The process should

identify threats from obsolescence and ensure that an adequate supply of spare parts is available until a solution to any obsolescence issues can be found. The solution will depend on the particular circumstances, but may involve providing alternative components or items of equipment that can carry out the same safety duty, or it may involve redesigning the plant to remove the need for the obsolescent system or components.

452 The design of the core and its components should take account of any identified safety-related factors, including:

a) irradiation;
b) chemical and physical processes;
c) static and dynamic mechanical loads;
d) thermal distortion;
e) thermally-induced stress; and
f) variations in manufacture.

Kanada

Krav

RD–337, 7.17 Ageing and Wear
The design considers the effects of ageing and wear on SSCs. For SSCs important to safety, this consideration includes:

1. An assessment of design margins, taking into account all known ageing and wear mechanisms and potential degradation in normal operation, including the effects of testing and maintenance processes; and
2. Provisions for monitoring, testing, sampling, and inspecting SSCs to assess ageing mechanisms, verify predictions, and identify unanticipated behaviours or degradation that may occur during operation as a result of ageing and wear.

RD-334: Aging Management for Nuclear Power Plants

USA

-

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 3: Safety of the plant design throughout the lifetime of the plant
The operating organization shall establish a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant.

IAEA Safety Standard, No. SSR-2/1, Requirement 14: Design basis for items important to safety
The design basis for items important to safety shall specify the necessary capability, reliability and functionality for the relevant operational states, for accident conditions and for conditions arising from internal and external hazards, to meet the specific acceptance criteria over the lifetime of the nuclear power plant.

IAEA Safety Standard, No. SSR-2/1, Requirement 30: Qualification of items important to safety
A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing.

IAEA Safety Standard, No. SSR-2/1, Requirement 31: Ageing management
The design life of items important to safety at a nuclear power plant shall be determined. Appropriate margins shall be provided in the design to take due account of relevant mechanisms of ageing, neutron embrittlement and wear out and of the potential for age related degradation, to ensure the capability of items important to safety to perform their necessary safety functions throughout their design life.

IAEA Safety Standard, No. SSR-2/1, 5.49
The qualification programme for items important to safety shall include the consideration of ageing effects caused by environmental factors (such as conditions of vibration, irradiation, humidity or temperature) over the expected service life of the items important to safety. When the items important to safety are subject to natural external events and are required to perform a safety function during or following such an event, the qualification programme shall replicate as far as is practicable the conditions imposed on the items important to safety by the natural event, either by test or by analysis or by a combination of both.

IAEA Safety Standard, No. SSR-2/1, 5.51
The design for a nuclear power plant shall take due account of ageing and wear out effects in all operational states for which a component is credited, including testing, maintenance, maintenance outages, plant states during a postulated initiating event and plant states following a postulated initiating event.

IAEA Safety Standard, No. SSR-2/1, 5.52
Provision shall be made for monitoring, testing, sampling and inspection to assess ageing mechanisms predicted at the design stage and to help identify unanticipated behaviour of the plant or degradation that might occur in service.

Krav avseende miljötålighet och miljöpåverkan

Sverige

Krav

17 § Kärnkraftsreaktorns barriärer samt utrustning som tillhör reaktorns säkerhetssystem ska vara utformade så att de tål de miljöbetingelser som barriärerna och utrustningarna kan utsättas för i de situationer då deras funktion tillgodoräknas i reaktorns säkerhetsanalys.

Utrustning i kärnkraftsreaktorn får inte ge upphov till en sådan miljöpåverkan att reaktorns säkerhetsfunktioner nedsätts.

Finland

Krav

4 § Säkerhetsklassificering
… Ur säkerhetssynpunkt viktiga system, konstruktioner och anordningar ska planeras, tillverkas och monteras samt användas så att deras kvalitetsnivå samt de bedömningar, kontroller och provningar, inklusive miljömässig funktionsduglighet, som behövs för att fastställa kvalitetsnivån

YVL B.1 §405

YVL B.1 §455

YVL B.1 Appendix B §112

Storbritannien

Övergripande principer

EMT.3 Type-testing
Structures, systems and components important to safety should be type tested before they are installed to conditions equal to, at least, the most severe expected in all modes of normal operational service.

Vägledande råd

188 For components of particular concern and where it is not possible to confirm the ability to operate under the most onerous design conditions, reference data from commissioning or rig testing should be established for comparison against in-service test results.

199 The effects of and interactions between the mechanical, thermal, chemical, physical, biological and radiation environment on materials properties, materials ageing and degradation processes should be considered.

Kanada

Krav

RD–337, 7.8 Equipment Environmental Qualification
The design provides an equipment environmental qualification program.

Development and implementation of this program ensures that the following functions are carried out in post-accident conditions:

1. The reactor is safely shut down and kept in a safe shutdown state during and following AOOs and DBAs;
2. Residual heat is removed from the reactor after shutdown, and also during and following AOOs and DBAs;
3. Potential for release of radioactive material from the plant is limited, and the resulting dose to the public from AOOs and DBAs is kept within prescribed limits; and
4. Post-accident conditions are monitored to indicate whether the above functions are being carried out.

The environmental conditions to be accounted for include those expected during normal operation, and those arising from AOOs and DBAs. Operational data and applicable design assist analysis tools, such as the probabilistic safety assessment, are used to determine the envelope of environmental conditions.

Equipment qualification also includes consideration of any unusual environmental conditions that can reasonably be anticipated, and that could arise during normal operation or AOOs (such as periodic testing of the containment leak rate).

Equipment credited to operate during BDBA and severe accident states is assessed for its capacity to perform its intended function under the expected environmental conditions. A justifiable extrapolation of equipment behaviour may be used to provide assurance of operability, and is typically based on design specifications, environmental qualification testing, or other considerations.

RD–337, 7.12.3 Environmental Protection and Nuclear Safety
The design minimizes the release and dispersion of hazardous substances or radioactive material to the environment, and minimizes the impact of any releases or dispersions, including those resulting from fire.

RD–337, 7.15.1 Design
… Environmental effects are considered in the design of civil structures and the selection of construction materials. The choice of construction material is commensurate with the designed service life and potential life extension of the plant.

RD–337, 9.3 Hazards Analysis
…The hazards analysis report includes the findings of the analysis and the basis for those findings. This report also:

4. Describes the performance criteria for detection systems, alarm systems, and mitigation systems, including requirements such as seismic or environmental qualification;

USA

Krav

10 CFR 50 Appendix A, Criterion 4, Environmental and dynamic effects design bases.
Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit. However, dynamic effects associated with postulated pipe ruptures in nuclear power units may be excluded from the design basis when analyses reviewed and approved by the Commission demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping.

10 CFR 50.44 (5)(B)
It shall be demonstrated that systems and components necessary to establish and maintain safe shutdown and to maintain containment integrity will be capable of performing their functions during and after exposure to the environmental conditions created by the burning of hydrogen, including local detonations, unless such detonations can be shown unlikely to occur.

10 CFR 50.44 (5) (C) (3) Equipment Survivability.
Containments that do not rely upon an inerted atmosphere to control combustible gases must be able to establish and maintain safe shutdown and containment structural integrity with systems and components capable of performing their functions during and after exposure to the environmental conditions created by the burning of hydrogen. Environmental conditions caused by local detonations of hydrogen must also be included, unless such detonations can be shown unlikely to occur. The amount of hydrogen to be considered must be equivalent to that generated from a fuel clad-coolant reaction involving 100 percent of the fuel cladding surrounding the active fuel region.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 29: Calibration, testing, maintenance, repair, replacement, inspection and monitoring of items important to safety
Items important to safety for a nuclear power plant shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored as required to ensure their capability of performing their functions and to maintain their integrity in all conditions specified in their design basis.

IAEA Safety Standard, No. SSR-2/1, Requirement 30: Qualification of items important to safety
A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant

are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing.

IAEA Safety Standard, No. SSR-2/1, 5.48
The environmental conditions considered in the qualification programme for items important to safety at a nuclear power plant shall include the variations in ambient environmental conditions that are anticipated in the design basis for the plant.

IAEA Safety Standard, No. SSR-2/1, 5.49
The qualification programme for items important to safety shall include the consideration of ageing effects caused by environmental factors (such as conditions of vibration, irradiation, humidity or temperature) over the expected service life of the items important to safety. When the items important to safety are subject to natural external events and are required to perform a safety function during or following such an event, the qualification programme shall replicate as far as is practicable the conditions imposed on the items important to safety by the natural event, either by test or by analysis or by a combination of both.

IAEA Safety Standard, No. SSR-2/1, 5.50
Any environmental conditions that could reasonably be anticipated and that could arise in specific operational states, such as in periodic testing of the containment leak rate, shall be included in the qualification programme.

Guide

The Operating Organization for Nuclear Power Plants Safety Guide, Series No. NS-G-2.4, December 07, 2001.

Krav avseende drift och kontrollrum

Sverige

Krav

18 § Kärnkraftsreaktorn ska normalt kunna styras och övervakas från det centrala kontrollrummet i alla förekommande driftlägen och åtgärder kunna vidtas från det centrala kontrollrummet för att bringa reaktorn i säkert läge, och behålla reaktorn i detta läge, vid alla händelser till och med händelseklassen osannolika händelser.

19 § Händelser som kan utgöra hot mot fortsatt verksamhet i det centrala kontrollrummet ska identifieras och en fastlagd handlingslinje finnas för hur dessa hot ska hanteras med bibehållande av reaktorsäkerheten.

Finland

Krav

12 § Förebyggande av olyckor och lindring av följderna av olyckor
Kärnkraftverket ska ha system med hjälp av vilka man snabbt och

tillförlitligt upptäcker driftstörningar och olyckssituationer samt förhindrar att situationen förvärras. Olyckor som leder till stora utsläpp av radioaktiva ämnen ska vara ytterst osannolika (bemästrande av driftstörningar och olyckstillbud).

14 § Säkerhetsfunktioner och tryggande av dem
[…] För att olyckor ska kunna hindras och deras följder lindras ska kärnkraftverket ha system för att stänga av reaktorn och kvarhålla den i subkritiskt tillstånd samt system för avlägsnande av den resteffektvärme som bildas i reaktorn och säkerställande av att radioaktiva ämnen stannar inom anläggningen. …

[…] Anläggningen ska planeras så att den kan ställas i ett säkert läge efter en allvarlig reaktorolycka.

19 § Övervakning och styrning av kärnkraftverk
I kärnkraftverkets kontrollrum ska finnas anordningar som ger uppgifter om kärnreaktorns tillstånd och visar eventuella avvikelser från det normala. I kärnkraftverk ska finnas automatiska system som ser till att säkerhetsfunktionerna blir påkopplade vid behov samt som styr och övervakar deras funktion vid driftstörningar och olyckor.

De automatiska systemen ska ha förmåga att hålla kraftverket under kontroll så pass länge att reaktoroperatörerna får tillräckligt med betänketid för att vidta rätta åtgärder.

23 § Driftverksamhet
I kärnkraftverkets kontrollrum ska alltid finnas ett tillräckligt antal operatörer som har kännedom om kraftverkets och dess systems och anordningars tillstånd. Styrningen av och kontrollen över ett kärnkraftverk ska basera sig på skriftliga anvisningar som motsvarar verkets aktuella konstruktion och tillstånd. För underhåll och reparation av anordningarna ska det finnas skriftliga föreskrifter och anvisningar i anslutning därtill.

Med tanke på driftstörningar och olyckssituationer ska det finnas lämpliga anvisningar för identifiering och kontroll av situationerna.

Driftåtgärderna och sådana händelser som inverkar på säkerheten ska dokumenteras så att de kan analyseras i efterhand.

25 § Säkerhetstekniska driftsvillkor
I kärnkraftverkets säkerhetstekniska driftsvillkor ska sådana tekniska och administrativa krav anges genom vilka säkerställs att driften sker i enlighet med planeringsgrunderna och säkerhetsanalyserna. I de säkerhetstekniska driftsvillkoren ska dessutom de krav anges genom vilka man säkerställer funktionsdugligheten hos sådana system, konstruktioner och anordningar som är viktiga med tanke på säkerheten samt anges de begränsningar som ska tillämpas ifall det uppstår något fel i anordningarna. Kärnkraftverket ska drivas i enlighet med dessa villkor och begränsningar och iakttagandet av dem ska övervakas och avvikelser från dem rapporteras.

YVL B.1 Appendix B §111

YVL B.1 Appendix B §113

YVL B.1 Appendix B §149-151

YVL B.1 Appendix C §106

YVL B.1 Appendix E §111

Storbritannien

Övergripande principer

ESR.1 Provision in control rooms and other locations
Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate locations on the facility.

ESR.7 Communications systems
Adequate communications systems should be provided to enable information and instructions to be transmitted between locations and to provide external communications with auxiliary services and such other organisations as may be required.

EHF.1 Integration with design, assessment and management
A systematic approach to integrating human factors within the design, assessment and management of systems should be applied throughout the entire facility life-cycle.

EHF.2 Allocation of safety actions
When designing systems, the allocation of safety actions between humans and technology should be substantiated and dependence on human action to maintain a safe state should be minimised.

EHF.3 Identification of actions impacting safety
A systematic approach should be taken to identifying human actions that can impact on safety.

EHF.4 Identification of administrative controls
Administrative controls used to remain within the safe operating envelope should be systematically identified.

EHF.5 Task analysis
Analysis should be carried out of tasks important to safety to determine demands on personnel in terms of perception, decision making and action.

EHF.6 Workspaces
Workspaces in which plant operations and maintenance are conducted should be designed to support reliable task performance, by taking account of human perceptual and physical characteristics and the impact of environmental factors.

EHF.7 User interfaces
User interfaces, comprising controls, indications, recording instrumentation and alarms should be provided at appropriate locations and should be suitable and sufficient to support effective monitoring and control of the plant during all plant states.

EHF.10 Human reliability
Risk assessments should identify and analyse human actions or omissions that might impact on safety.

ESS.13 Confirmation to operating personnel
There should be a direct means of confirming to operating personnel:

a) that a demand for safety system action has arisen;
b) that the safety actuation systems have operated fully; and
c) whether any limiting condition for which the safety system has been qualified has been exceeded.

ESS.14 Prohibition of self-resetting of actions and alarms
Safety system actions and associated alarms should not be self-resetting, irrespective of the subsequent state of the initiating fault.

ESS.15 Alteration of configuration, operational logic or associated data
No means should be provided, or be readily available, by which the configuration of a safety system, its operational logic or the associated data (trip levels etc) may be altered, other than by specifically engineered and adequately secured maintenance/testing provisions used under strict administrative control.

ESS.16 No dependency on external sources of energy

Where practicable, following a safety system action, maintaining a safe facility state should not depend on an external source of energy.

ESS.27 Computer-based safety systems
Where the system reliability is significantly dependent upon the performance of computer software, the establishment of and compliance with appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by a demonstration of ‘production excellence’ and ‘confidence-building’ measures.

Vägledande råd

338 Monitoring provisions should be classified as safety or safety-related systems as appropriate and should be made:

a) in a central control location; and
b) at emergency locations (preferably a single point) that will remain habitable during foreseeable facility emergencies.

360 Production excellence’ requires a demonstration of excellence in all aspects of production, covering initial specification through to the finally commissioned system, comprising the following elements:

a) Thorough application of technical design practice consistent with current accepted standards for the development of software for computer-based safety systems.
b) Implementation of an adequate quality assurance programme and plan in accordance with appropriate quality assurance standards.

c) Application of a comprehensive testing programme formulated to check every system function, including:
    - prior to installation on site, the verification of all phases of the system production process and the validation of the integrated system against its requirements specification by persons not involved in the specification and design activities;
    - following installation on site, a demonstration that the safety system, in conjunction with the plant, performs to requirements, this demonstration being devised by persons other than the system specifiers, designers or manufacturers; and
    - a programme of dynamic testing, applied to the complete system that is capable of demonstrating that the system meets its reliability requirements.

361 Independent 'confidence-building' should provide an independent and thorough assessment of a safety system's fitness for purpose. This comprises the following elements:

a) Complete and preferably diverse checking of the finally validated production software by a team that is independent of the systems suppliers, including:
    - independent product checking providing a searching analysis of the product;
    - independent checking of the design and production process, including activities needed to confirm the realisation of the design intention; and
b) Independent assessment of the test programme, covering the full scope of test activities.

362 Should weaknesses be identified in the production process, compensating measures should be applied to address these. The type of compensating measures will depend on, and should be targeted at, the specific weaknesses found.

366 The provisions should encompass normal operation, abnormal operation and postulated fault conditions including, where reasonably practicable, severe accidents. The equipment should include indicating and recording instrumentation and controls as appropriate.

377 This principle includes defining the safety actions of personnel responsible for monitoring and controlling plant and responding to faults, and of personnel carrying out maintenance, testing and calibration activities. It also includes considering the impact on safety of engineers, analysts, managers and other staff who may not directly interact with plant and equipment.

378 The design of these controls should be such that the requirements for personnel action are clearly identified and unambiguous to those responsible for their implementation.

379 The analysis should address the actions identified using Principles EHF.3 and EHF.4, and should include consideration of physical, psychological and cognitive factors that could impact on human performance.

380 The analysis should demonstrate the feasibility of these actions within the available timescales and should inform the way they are designed and supported to achieve reliable task performance. It should be sufficiently detailed, and demonstrably employed, to provide a basis for developing user interfaces, procedures and job aids, as well as defining operator roles and responsibilities, staffing levels, personnel competence and training needs, communication networks and workspace design.

381 The workload of personnel required to fulfil safety-related actions should be analysed and demonstrated to be reasonably achievable. Wherever possible, this demonstration should form part of the inactive commissioning of the facility.

382 Shift systems should be designed to minimise the likelihood of human error.

383 This principle applies to central control rooms, local control stations on the plant and emergency locations that should remain habitable during foreseeable facility emergencies. It also applies to provisions for maintenance and testing.

384 The user interface provisions should encompass normal operation, abnormal operation and postulated fault conditions including, where reasonably practicable, severe accidents.

385 The user interface should:

a) enable the operator to determine plant states and the availability, and status, of plant equipment;
b) provide a conspicuous early warning of any safety-related changes in plant state;
c) provide the means of confirming safety system challenges and identifying, initiating and confirming necessary safety actions;
d) support effective diagnosis of plant deviations; and
e) enable the operator to determine and execute appropriate system actions, including actions to overcome failures of automated safety systems or to reset a safety system after its operation.

386 The user interface should be designed to ensure compatibility with human psychological and physical characteristics and to facilitate reliable human performance. Interfaces and equipment should be clearly labelled.

389 Assessments should include precursor errors, such as the introduction of unrevealed errors during maintenance, actions that contribute to initiating events, post-fault responses and long-term recovery actions.

390 The selection and application of probability data for human errors should be:

a) derived from operational experience data and/or through the application of recognised human reliability assessment techniques. Use of either approach should be justified and its relevance for the task and context demonstrated;
b) underpinned by task analysis and reflect the influence of human performance shaping factors, making due allowance for uncertainty.

391 Risk assessments should directly model dependent human errors committed by a single operator or different operators. The results of the risk assessments should be used in the fault analysis.

Kanada

Krav

RD–337, 4.3.3 Operational Limits and Conditions
Operational limits and conditions (OLCs) are the set of limits and conditions that can be monitored by or on behalf of the operator, and that can be controlled by the operator.

The OLCs are established to ensure that plants operate in accordance with design assumptions and intent (parameters and components), and include the limits within which the facility has been shown to be safe. The OLCs are documented in a manner that is readily accessible for control room personnel, with the roles and responsibilities clearly identified. Some OLCs may include combinations of automatic functions and actions by personnel.

Safe operation depends on personnel as well as equipment. OLCs therefore typically include:

1. Control system constraints and procedural constraints on important process variables;
2. Requirements for normal operation and AOOs, including shutdown states;
3. Actions to be taken and limitations to be observed by operating personnel;
4. Principal requirements for surveillance and corrective or compensatory actions; and

The limitations to be observed and the operational requirements to be met by SSCs in order that their intended functions, as assumed in the safety analysis, can be met.

The basis on which the OLCs are derived will be readily available in order to facilitate the ability of plant personnel to interpret, observe, and apply the OLCs.

RD–337, 7.21 Human Factors
The design includes a human factors engineering program plan.

Relevant and proven systematic analysis techniques are used to address human factors issues within the design process.

Human factors considerations:

1. Reduce the likelihood of human error as far reasonably achievable;
2. Provide means for identifying the occurrence of human error, and methods by which to recover from such error; and
3. Mitigate the consequences of error.

The human factors engineering program also facilitates the interface between the operating personnel and the plant by promoting attention to plant layout and procedures, maintenance, inspection, training, and the application of ergonomic principles to the design of working areas and working environments.

Appropriate and clear distinction between the functions assigned to operating personnel and those assigned to automatic systems is facilitated by systematic consideration of human factors and the human-machine interface. This consideration continues in an iterative way throughout the entire design process.

The human-machine interfaces in the main control room, the secondary control room, the emergency support centre, and in the plant, provide operators with necessary and appropriate information in a usable format that is compatible with the necessary decision and action times.

Human factors verification and validation plans are established for all appropriate stages of the design process to confirm that the design adequately accommodates all necessary operator actions.

To assist in the establishment of design criteria for information display and controls, each operator is considered to have dual roles—that of a systems manager, including responsibility for accident management, and that of an equipment operator. Verification and validation activities are comprehensive, such that the design conforms to human factors design principles and meets usability requirements.

The design identifies the type of information that facilitates an operator’s ability to readily:

1. Assess the general state of the plant, whether in normal operating, AOO, or DBA states;
2. Confirm that the designed automatic safety actions are being carried out; and
3. Determine the appropriate operator-initiated safety actions to be taken.

The design provides the type of information that enables an individual in an equipment operator role to identify the parameters associated with individual plant systems and equipment, and to confirm that the necessary safety actions can be initiated safely.

Design goals include promoting the success of operator action with due regard for the time available for response, the physical environment to be expected, and the associated psychological demands made on the operator.

The need for operator intervention on a short time scale is kept to a minimum. Where such intervention is necessary, the following conditions apply:

1. The information necessary for the operator to make the decision to act is presented simply and unambiguously;
2. The operator has sufficient time to make a decision and to act; and
3. Following an event, the physical environment is acceptable in the main control room or in the secondary control room, and in the access route to the secondary control room.

RD–337, 8.4.3 Monitoring and Operator Action
Once automatic shutdown is initiated, it is impossible for an operator to prevent its actuation.

The need for manual shutdown actuation is minimized.

The means for monitoring shutdown status and manual actuation is provided in the main control room.

RD–337, 8.10 Control Facilities

RD–337, 8.10.1 Main Control Room
The design provides for a main control room (MCR) from which the plant can be safely operated, and from which measures can be taken to maintain the plant in a safe state or to bring it back into such a state after the onset of AOOs, DBAs, and, to the extent practicable, following BDBAs.

The design identifies events both internal and external to the MCR that may pose a direct threat to its continued operation, and provides practicable measures to minimize the effects of these events.

The safety functions initiated by automatic control logic in response to an accident can also be initiated manually from the main and secondary control rooms.

The layout of the controls and instrumentation, and the mode and format used to present information, provide operating personnel with an adequate overall picture of the status and performance of the plant and provide the necessary information to support operator actions.

The design of the MCR is such that appropriate lighting levels and thermal environment are maintained, and noise levels are minimized to applicable standards and codes.

The design of the MCR takes ergonomic factors into account to provide both physical and visual accessibility to controls and displays, without adverse impact on health and comfort. This includes hardwired display panels as well as computerized displays, with the aim of making these displays as user friendly as possible.

Cabling for the instrumentation and control equipment in the MCR is arranged such that a fire in the secondary control room cannot disable the equipment in the MCR.

The design provides visual and, if appropriate, audible indications of plant states and processes that have deviated from normal operation and that could affect safety.

The design also allows for the display of information needed to monitor the effects of the automatic actions of all control, safety, and safety support system.

The MCR is to be provided with secure communication channels to the emergency support centre and to off-site emergency response organizations, and to allow for extended operating periods.

RD–337, 8.10.1.1 Safety Parameter Display System
The MCR contains a safety parameter display system that presents sufficient information on safety-critical parameters for the diagnosis and mitigation of DBAs and BDBAs, including severe accidents.

The safety parameter display system has the following capabilities:

1. Display safety critical parameters within the full range expected in normal operation and during accidents;
2. Track data trends;
3. Indicate when process or safety limits are being approached or exceeded; and
4. Display the status of safety systems.

The safety parameter display system is designed and installed such that the same information is made available in a secure manner to the emergency support centre.

The safety parameter display system is integrated and harmonized with the overall control room human-system interface design.

USA

Krav

10 CFR 50 Appendix A, Criterion 19, Control room.
A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident. Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

10 CFR 50.34 (4): Analysis and evaluation of ECCS cooling performance and the need for high point vents following postulated loss-of-coolant accidents must be performed in accordance with the requirements of § 50.46 and § 50.46a ...

10 CFR 50.34 (f)(2)
(iv) Provide a plant safety parameter display console that will display to operators a minimum set of parameters defining the safety status of the plant, capable of displaying a full range of important plant parameters and data trends on demand, and capable of indicating when process limits are being approached or exceeded. (I.D.2)

(v) Provide for automatic indication of the bypassed and operable status of safety systems. (I.D.3)

(ix) Provide a system for hydrogen control that can safely accommodate hydrogen generated by the equivalent of a 100% fuel-clad metal water reaction. Preliminary design information on the tentatively preferred system option of those being evaluated in paragraph (f)(1)(xii) of this section is sufficient at the construction permit stage. The hydrogen control system and associated systems shall provide, with reasonable assurance, that: (II.B.8)...

(C) Equipment necessary for achieving and maintaining safe shutdown of the plant and maintaining containment integrity will perform its safety function during and after being exposed to the environmental conditions attendant with the release of hydrogen generated by the equivalent of a 100% fuel-clad metal water reaction including the environmental conditions created by activation of the hydrogen control system.

(xi) Provide direct indication of relief and safety valve position (open or closed) in the control room. (II.D.3)

(xvii) Provide instrumentation to measure, record and readout in the control room: (A) containment pressure, (B) containment water level, (C) containment hydrogen concentration, (D) containment radiation intensity (high level), and (E) noble gas effluents at all potential, accident release points. Provide for continuous sampling of radioactive iodines and particulates in gaseous effluents from all potential accident release points, and for onsite capability to analyze and measure these samples. (II.F.1)

(xix) Provide instrumentation adequate for monitoring plant conditions following an accident that includes core damage. (II.F.3)

Guide

RG1.97 Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants.

RG 1.78 "Evaluating the Habitability of a Nuclear Power Plant Control Room During a Postulated Hazardous Chemical Release, including chlorine".

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 65: Control room
A control room shall be provided at the nuclear power plant from which the plant can be safely operated in all operational states, either automatically or manually, and from which measures can be taken to maintain the plant in a safe state or to bring it back into a safe state after anticipated operational occurrences and accident conditions.

IAEA Safety Standard, No. SSR-2/1, 5.53
The design for a nuclear power plant shall specify the minimum number of operating personnel required to perform all the simultaneous operations necessary to bring the plant into a safe state.

IAEA Safety Standard, No. SSR-2/1, 5.54
Operating personnel who have gained operating experience in similar plants shall, as far as is practicable, be actively involved in the design process conducted by the design organization, in order to ensure that consideration is given as early as possible in the process to the future operation and maintenance of equipment.

IAEA Safety Standard, No. SSR-2/1, 5.55
The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks, and shall limit the effects of operating errors on safety. The design process shall pay attention to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant.

IAEA Safety Standard, No. SSR-2/1, 5.56
The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, in accordance with the necessary decision times and action times. The information necessary for the operator to make a decision to act shall be simply and unambiguously presented.

IAEA Safety Standard, No. SSR-2/1, 5.57
The operator shall be provided with the necessary information:

(a) To assess the general state of the plant in any condition;
(b) To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions);
(c) To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended;
(d) To determine both the need for and the time for manual initiation of the specified safety actions.

IAEA Safety Standard, No. SSR-2/1, 5.58
The design shall be such as to promote the success of operator actions with due regard for the time available for action, the conditions to be expected and the psychological demands being made on the operator.

IAEA Safety Standard, No. SSR-2/1, 5.59
The need for intervention by the operator on a short time scale shall be kept to a minimum, and it shall be demonstrated that the operator has sufficient time to make a decision and sufficient time to act.

IAEA Safety Standard, No. SSR-2/1, 5.60
The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the control room or the supplementary control room and in locations on the access route to the supplementary control room do not compromise the protection and safety of the operating personnel.

IAEA Safety Standard, No. SSR-2/1, 5.61
The design of workplaces and the working environment of the operating personnel shall be in accordance with ergonomic concepts.

IAEA Safety Standard, No. SSR-2/1, 5.62
Verification and validation, including by the use of simulators, of features relating to human factors shall be included at appropriate stages to confirm that necessary actions by the operator have been identified and can be correctly performed.

IAEA Safety Standard, No. SSR-2/1, 6.39
Appropriate measures shall be taken, including the provision of barriers between the control room at the nuclear power plant and the external environment, and adequate information shall be provided for the protection of occupants of the control room against hazards such as high radiation levels resulting from accident conditions, release of radioactive material, fire, or explosive or toxic gases.

IAEA Safety Standard, No. SSR-2/1, 6.40
Special attention shall be paid to identifying those events, both internal and external to the control room, that could challenge its continued operation, and the design shall provide for reasonably practicable measures to minimize the consequences of such events.

Krav avseende reservövervakningsplats

Sverige

Krav

20 § För de händelser där ordinarie kontrollrum inte är tillgängligt ska det finnas en reservövervakningsplats med tillräcklig instrumentering och manövermöjligheter så att reaktorn kan föras till varmt avställt läge, resteffekt kylas bort och nödvändiga säkerhetsparametrar övervakas. Reservövervakningsplatsen ska vara fysiskt och funktionellt separerad från det centrala kontrollrummet. Övervakning från reservövervaknings-platsen ska vara möjlig även vid ett enkelfel i något av de system som är nödvändiga för reaktorns säkra avställning och kylning.

Vid förande av reaktorn till kallt avställt läge får andra lokala manöverplatser än reservövervakningsplatsen utnyttjas. Ledning och

övervakning av avställningen till kallt läge ska dock kunna ske från reservövervakningsplatsen.

Finland

Krav

19 § Övervakning och styrning av kärnkraftverk
I kärnkraftverk ska finnas en av kontrollrummet oberoende reservkontrollcentral och nödvändiga lokala styrsystem som gör det möjligt att stänga av och kyla ned kärnreaktorn samt att avlägsna resteffekten i bränslet i reaktorn och i det använda bränsle som upplagras i anläggningen.

YVL B.1 Appendix C §107-108

YVL B.1 Appendix C §120

Storbritannien

Övergripande principer

ESR.1 Provision in control rooms and other locations
Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate locations on the facility.

Vägledande råd

338 Monitoring provisions should be classified as safety or safety-related systems as appropriate and should be made:

a) in a central control location; and
b) at emergency locations (preferably a single point) that will remain habitable during foreseeable facility emergencies.

366 The provisions should encompass normal operation, abnormal operation and postulated fault conditions including, where reasonably practicable, severe accidents. The equipment should include indicating and recording instrumentation and controls as appropriate.

Kanada

Krav

RD–337, 8.10.2 Secondary Control Room
The design provides a secondary control room (SCR) that is physically and electrically separate from the MCR, and from which the plant can be placed and kept in a safe shutdown state when the ability to perform essential safety functions from the MCR is lost.

The design identifies all events that may pose a direct threat to the continued operation of the MCR and the SCR. The design of the MCR and the SCR are such that no event can simultaneously affect both control rooms to the extent that the essential safety functions cannot be performed.

For any PIE, at least one control room is habitable, and is accessible by means of a qualified route.

Instrumentation, control equipment, and displays are available in the SCR, so that the essential safety functions can be performed, essential plant variables can be monitored, and operator actions are supported.

Safety functions initiated by automatic control logic in response to an accident can also be initiated manually from both the MCR and the SCR.

The design of the SCR ensures that appropriate lighting levels and thermal environment are maintained, and noise levels align with applicable standards and codes.

Ergonomic factors apply to the design of the SCR to ensure physical and visual accessibility in relation to controls and displays, without adverse impact on health and comfort. These include hardwired display panels as well as computerized displays that are as user friendly as possible.

Cabling for the instrumentation and control equipment in the SCR is such that a fire in the main control room cannot disable the equipment in the SCR.

The SCR is equipped with a safety parameter display system similar to that in the MCR. As a minimum, this display system provides the information required to facilitate the management of the reactor when the MCR is uninhabitable.

The SCR is to be provided with secure communication channels to the emergency support centre and to off-site emergency response organizations.

The SCR allows for extended operating periods.

RD–337, 8.10.4 Equipment Requirements for Accident Conditions
If operator action is required for actuation of any safety system or safety support system equipment, all of the following expectations apply:

1. There are clear, well-defined, validated, and readily available operating procedures that identify the necessary actions;
2. There is instrumentation in the control rooms to provide clear and unambiguous indication of the necessity for operator action;
3. Following indication of the necessity for operator action inside the MCR, there is at least 15 minutes available before the operator action is required; and
4. Following indication of the necessity for operator action outside the MCR, there is a minimum of 30 minutes available before the operator action is required.

Alternative action times may be used if justified, making due allowance for the complexity of the action to be taken, and for the time needed for such activities as the diagnosing the event and accessing to the remote station.

For automatically initiated safety systems and control logic actions, the design facilitates backup manual initiation from inside the appropriate control room.

RD–337, 8.13.3 Monitoring
Equipment is provided to ensure that there is adequate radiation monitoring in normal operation, AOOs, and DBAs.

Stationary alarming dose rate meters are therefore provided:

1. For monitoring the local radiation dose rate at places routinely occupied by operating personnel;
2. Where the changes in radiation levels may be such that access may be limited for periods of time;
3. To indicate the general radiation level at appropriate locations in the event of DBAs and, as far as practicable, severe accidents; and
4. To give sufficient information in the control room or at the appropriate control position to enable plant personnel to initiate corrective actions when necessary.

Monitors are to be provided for measuring the activity of radioactive substances in the atmosphere:

1. For areas routinely occupied by personnel;
2. For areas where the levels of activity of airborne radioactive materials may, on occasion, be expected to necessitate protective measures; and
3. To give an indication in the control room, or in other appropriate locations, of when a high concentration of radionuclides is detected.

Facilities are provided for monitoring individual doses to and contamination of personnel.

Stationary equipment and laboratory facilities are to be provided to determine the concentration of selected radionuclides in fluid process systems as appropriate, and in gas and liquid samples taken from plant systems or the environment.

Stationary equipment is provided for monitoring the effluents prior to or during discharge to the environment.

USA

Krav

10 CFR 50 Appendix A, Criterion 19, Control room.
…Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 66: Supplementary control room
Instrumentation and control equipment shall be kept available, preferably at a single location (a supplementary control room) that is physically, electrically and functionally separate from the control room at the nuclear power plant. The supplementary control room shall be so equipped that the reactor can be placed and maintained in a shutdown state, residual heat can be removed, and essential plant variables can be monitored if there is a loss of ability to perform these essential safety functions in the control room.

IAEA Safety Standard, No. SSR-2/1, 5.60.
The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the control room or the supplementary control room and in locations on the access route to the supplementary control room do not compromise the protection and safety of the operating personnel.

IAEA Safety Standard, No. SSR-2/1, 6.41
The requirements of para. 6.39 for taking appropriate measures and providing adequate information for the protection of occupants against hazards also apply for the supplementary control room at the nuclear power plant.

IAEA Safety Standard, No. SSR-2/1, 6.78
Stationary dose rate meters shall be installed to indicate the general radiation levels at suitable plant locations in accident conditions. The stationary dose rate meters shall provide sufficient information in the control room or in the appropriate control position that operating personnel can initiate corrective action if necessary.

Krav avseende klassning och kvalificering

Sverige

Krav

21 § Kärnkraftsreaktorns byggnadsdelar, system, komponenter och anordningar ska indelas i säkerhetsklasser. De närmare kvalitets- och funktionskrav, som följer av denna säkerhetsklassning ska definieras och styras genom angivelse av underliggande klasser, bl.a. mekanisk kvalitetsklass, elektrisk funktionsklass samt klassning med avseende på seismik och miljötålighet.

Ytterligare bestämmelser om kvalitetsklassning finns i Strålsäkerhetsmyndigheten föreskrifter (SSMFS 2008:13) om mekaniska anord-ningar i vissa kärntekniska anläggningar.

Finland

Krav

4 § Säkerhetsklassificering
Ett kärnkraftverks säkerhetsfunktioner ska anges och de system, konstruktioner och anordningar som ansluter sig till dessa ska klassificeras utgående från deras betydelse för säkerheten.

Ur säkerhetssynpunkt viktiga system, konstruktioner och anordningar ska planeras, tillverkas och monteras samt användas så att deras kvalitetsnivå samt de bedömningar, kontroller och provningar, inklusive miljömässig funktionsduglighet, som behövs för att fastställa kvalitetsnivån är tillräckliga med beaktande av varje objekts betydelse för säkerheten.

YVL B.1 §312-313

Storbritannien

Övergripande principer

ECS.1 Safety categorisation
The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety.

ECS.2 Safety classification of structures, systems and components
Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regard to safety.

ECS.3 Standards
Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate standards.

ECS.4 Codes and standards
For structures, systems and components that are important to safety, for which there are no appropriate established codes or standards, an approach derived from existing codes or standards for similar equipment, in applications with similar safety significance, may be applied.

ECS.5 Use of experience, tests or analysis
In the absence of applicable or relevant codes and standards, the results of experience, tests, analysis, or a combination thereof, should be applied to demonstrate that the item will perform its safety function(s) to a level commensurate with its classification.

EQU.1 Qualification procedures
Qualification procedures should be in place to confirm that structures, systems and components that are important to safety will perform their required safety function(s) throughout their operational lives.

Vägledande råd

148 The effective implementation of defence in depth needs support from a number of general principles and related measures that assure the reliability and capability of the means of achieving the objectives. It is important that structures, systems and components, including software for instrumentation and control, are classified on the basis of their safety significance and are designed, manufactured, installed and then subsequently commissioned, operated and maintained to a level of quality commensurate with their classification.

149 A safety categorisation scheme could be determined on the following basis:

a) Category A – any function that plays a principal role in ensuring nuclear safety.
b) Category B – any function that makes a significant contribution to nuclear safety.
c) Category C – any other safety function.

150 The method for categorising safety functions should take into account:

a) the consequence of failing to deliver the safety function;
b) the extent to which the function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults;
c) the potential for a functional failure to initiate a fault or exacerbate the consequences of an existing fault;
d) the likelihood that the function will be called upon.

151 The categorisation of safety functions should take no account of any redundancy, diversity or independence within the design – these aspects relate to the structures, systems and components required to deliver the safety function.

152 The categorisation assigned to each safety function should be used to classify structures, systems and components required to deliver that function.

153 The method for classifying the safety significance of a structure, system or component should primarily be based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgement, with account taken of factors such as:

a) the category of safety function(s) to be performed by the item (see Principle ECS.1);
b) the consequences of failure to perform its function;
c) the probability that the item will be called upon to perform a safety function;
d) the time following any initiating fault at which, or the period throughout which, it will be called upon to operate.

154 A safety classification scheme could be determined on the following basis:

a) Class 1 – any structure, system or component that forms a principal means of fulfilling a Category A safety function.
b) Class 2 – any structure, system or component that makes a significant contribution to fulfilling a Category A safety function, or forms a principal means of ensuring a Category B safety function.
c) Class 3 – any other structure, system or component.

155 Appropriately designed interfaces should be provided between structures, systems and components of different classes to ensure that any failure in a lower class item will not propagate to an item of a higher class. Equipment providing the function to prevent the propagation of failures should be assigned to the higher class.

156 Auxiliary services that support components of a system important to safety should be considered part of that system and should be classified accordingly unless failure does not prejudice successful delivery of the safety function.

157 The standards should reflect the functional reliability requirements of structures, systems and components and be commensurate with their safety classification.

158 Appropriate national or international codes and standards should be adopted for Classes 1 and 2 of structures, systems and components. For Class 3, appropriate non-nuclear-specific codes and standards may be applied.

159 Codes and standards should be preferably nuclear-specific codes or standards leading to a conservative design commensurate with the importance of the safety function(s) being performed. The codes and standards should be evaluated to determine their applicability, adequacy and sufficiency and should be supplemented or modified as necessary to a level commensurate with the importance of the safety function(s) being performed.

160 Where a structure, system or component is required to deliver multiple safety functions, and these can be demonstrated to be delivered independently of one another, codes and standards should be used appropriate to the category of the safety function. Where independence cannot be demonstrated, codes and standards should be appropriate to the class of the structure, system or component (ie in accordance with the highest category of safety function to be delivered). Whenever different codes and standards are used for different aspects of the same structure, system or component, the compatibility between these should be demonstrated.

161 The combining of different codes and standards for a single aspect of a structure, system or component should be avoided or justified when used. Compatibility between these codes and standards should be demonstrated.

162 The qualification procedures should demonstrate a level of confidence commensurate with their safety classification.

163 Procedures for the qualification of equipment should address operational, environmental and fault conditions (including severe accidents where appropriate) specified in the design.

164 The procedures should include a physical demonstration that individual items can perform their safety function(s) under the required conditions, and within the time substantiated in the facility's safety case.

165 The procedures should ensure that adequate arrangements exist (Licence Condition 6, see the HSE website) for the recording and retrieval of lifetime data covering the item's construction, manufacture, testing, inspection and maintenance to demonstrate that any assumptions made in the safety case remain valid throughout operational life.

Kanada

Krav

RD–337, 7.1 Classification of SSCs
The design authority classifies SSCs in a consistent and clearly defined classification scheme. The SSCs are then designed, constructed, and maintained such that their quality and reliability is commensurate with this classification.

In addition, all SSCs are identified as either important or not important to safety. The criteria for determining safety importance are based on:

1. Safety function(s) to be performed;
2. Consequence of failure;
3. Probability that the SSC will be called upon to perform the safety function; and
4. The time following a PIE at which the SSC will be called upon to operate, and the expected duration of that operation.

SSCs important to safety include:

1. Safety systems;
2. Complementary design features;
3. Safety support systems; and
4. Other SSCs whose failure may lead to safety concerns (e.g., process and control systems).

The design provides appropriately designed interfaces between SSCs of different classes to minimize the risk of an SSC less important to safety from adversely affecting the function or reliability of an SSC of greater importance.

RD–337, 7.8 Equipment Environmental Qualification
The design provides an equipment environmental qualification program. Development and implementation of this program ensures that the following functions are carried out in post-accident conditions:

1. The reactor is safely shut down and kept in a safe shutdown state during and following AOOs and DBAs;

2. Residual heat is removed from the reactor after shutdown, and also during and following AOOs and DBAs;
3. Potential for release of radioactive material from the plant is limited, and the resulting dose to the public from AOOs and DBAs is kept within prescribed limits; and
4. Post-accident conditions are monitored to indicate whether the above functions are being carried out.

The environmental conditions to be accounted for include those expected during normal operation, and those arising from AOOs and DBAs. Operational data and applicable design assist analysis tools, such as the probabilistic safety assessment, are used to determine the envelope of environmental conditions.

Equipment qualification also includes consideration of any unusual environmental conditions that can reasonably be anticipated, and that could arise during normal operation or AOOs (such as periodic testing of the containment leak rate).

Equipment credited to operate during BDBA and severe accident states is assessed for its capacity to perform its intended function under the expected environmental conditions. A justifiable extrapolation of equipment behaviour may be used to provide assurance of operability, and is typically based on design specifications, environmental qualification testing, or other considerations.

RD–337, 7.13 Seismic Qualification
The seismic qualification of all SSCs aligns with the requirements of Canadian national—or equivalent—standards.

The design includes instrumentation for monitoring seismic activity at the site for the life of the plant.

RD–337, 7.13.1 Seismic Design and Classification
The design authority identifies SSCs important to safety that are credited to withstand a design basis earthquake (DBE), and ensures that they are qualified accordingly. This applies to:

1. SSCs whose failure could directly or indirectly cause an accident leading to core damage;
2. SSCs restricting the release of radioactive material to the environment;
3. SSCs that assure the subcriticality of stored nuclear material; and
4. SSCs such as radioactive waste tanks containing radioactive material that, if released, would exceed regulatory dose limits.

The design of these SSCs also meets the DBE criteria to maintain all essential attributes, such as pressure boundary integrity, leak-tightness, operability, and proper position in the event of a DBE.

The design provides that no substantive damage to these SSCs will be caused by the failure of any other SSC under DBE conditions.

Seismic fragility levels should be evaluated for SSCs important to safety by analysis or, where possible, by testing.

USA

Krav

10 CFR 50 Appendix A, Criterion 1, Quality standards and records.
Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.

10 CFR 50.69 Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors.

(2) The SSCs must be categorized by an Integrated Decision-Making Panel (IDP) staffed with expert, plant-knowledgeable members whose expertise includes, at a minimum, PRA, safety analysis, plant operation, design engineering, and system engineering.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 22: Safety classification
All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance.

IAEA Safety Standard, No. SSR-2/1, Requirement 23: Reliability of items important to safety
The reliability of items important to safety shall be commensurate with theirsafety significance.

IAEA Safety Standard, No. SSR-2/1, Requirement 30: Qualification of items important to safety
A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing.

IAEA Safety Standard, No. SSR-2/1, 5.34
The method for classifying the safety significance of items important to

safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, with due account taken of factors such as:

(a) The safety function(s) to be performed by the item;
(b) The consequences of failure to perform a safety function;
(c) The frequency with which the item will be called upon to perform a safetyfunction;
(d) The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

IAEA Safety Standard, No. SSR-2/1, 5.35
The design shall be such as to ensure that any interference between items important to safety will be prevented, and in particular that any failure of items important to safety in a system in a lower safety class will not propagate to a system in a higher safety class.

IAEA Safety Standard, No. SSR-2/1, 5.36
Equipment that performs multiple functions shall be classified in a safety class that is consistent with the most important function performed by the equipment.

IAEA Safety Standard, No. SSR-2/1, 5.37
The design of items important to safety shall be such as to ensure that the equipment can be qualified, procured, installed, commissioned, operated and maintained to be capable of withstanding, with sufficient reliability and effectiveness, all conditions specified in the design basis for the items.

IAEA Safety Standard, No. SSR-2/1, 5.48
The environmental conditions considered in the qualification programme for items important to safety at a nuclear power plant shall include the variations in ambient environmental conditions that are anticipated in the design basis for the plant.

IAEA Safety Standard, No. SSR-2/1, 5.49
The qualification programme for items important to safety shall include the consideration of ageing effects caused by environmental factors (such as conditions of vibration, irradiation, humidity or temperature) over the expected service life of the items important to safety. When the items important to safety are subject to natural external events and are required to perform a safety function during or following such an event, the qualification programme shall replicate as far as is practicable the conditions imposed on the items important to safety by the natural event, either by test or by analysis or by a combination of both.

IAEA Safety Standard, No. SSR-2/1, 5.50
Any environmental conditions that could reasonably be anticipated and that could arise in specific operational states, such as in periodic testing of the containment leak rate, shall be included in the qualification programme.

IAEA Safety Standard, No. SSR-2/1, 5.75
The deterministic safety analysis shall mainly provide:

(c) Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements;

Guide

Recruitment, Qualification and Training of Personnel for Nuclear Power Plants Safety Guide, Series No. NS-G-2.8, November 19, 2002.

Krav avseende händelseklassning och analys av händelser

Sverige

Krav

22 § För att analysera säkerheten ska de inledande händelser som ingår i den deterministiska säkerhetsanalysen, enligt 4 kap. 1 § Strålsäkerhetsmyndighetens föreskrifter (SSMFS 2008:1) om säkerhet i kärntekniska anläggningar, indelas i ett begränsat antal händelseklasser med specificerade analysförutsättningar och acceptanskriterier. Dessa händelseklasser ska täcka normala drifthändelser, förväntade händelser, ej förväntade händelser, osannolika händelser och mycket osannolika händelser. Vid analys av händelser som inte har beaktats i reaktorns konstruktion får anpassade analysförutsättningar och acceptanskriterier tillämpas.

Finland

Krav

2 § Definitioner
I denna förordning avses med

6) *antagen olycka* sådan avvikelse från normala driftslägen som kan antas inträffa mera sällan än en gång under en tid av hundra driftår och som kärnkraftverket förutsätts klara av utan allvarliga bränsleskador, även om enstaka anordningar i system som är viktiga med tanke på säkerheten skulle vara ur funktion på grund av underhållsarbeten eller fel; antagna olyckor delas in i två klasser utgående från initialhändelsens omfattning enligt följande:
    a) antagna olyckor av klass 1 är olyckor som kan antas inträffa mera sällan än en gång per hundra driftår, men minst en gång per tusen driftår,
    b) antagna olyckor av klass 2 är olyckor som kan antas inträffa mera sällan än en gång per tusen driftår,

3 § Bedömning och verifiering av säkerheten
Ett kärnkraftverks säkerhet ska bedömas i anslutning till ansökan om byggnadstillstånd och ansökan om driftstillstånd, i samband med ändringar i anläggningarna samt regelbundet under drifttiden.

Om det utgående från kärnkraftverkets planeringslösning inte är möjligt att direkt konstatera att säkerhetskraven uppfylls, ska uppfyllandet av dessa påvisas. Ett kärnkraftverks säkerhet och de tekniska lösningarna i dess säkerhetssystem ska motiveras med hjälp av experimentella och kalkylmässiga metoder. Sådana är störnings- och olycksanalyser, hållfasthetsanalyser, feleffektsanalyser samt sannolikhetsbaserade riskanalyser. Analyserna ska hållas à jour och vid behov preciseras med beaktande av drifterfarenheter, experimentella forskningsresultat, ändringar i anläggningarna och den utveckling som sker av beräkningsmetoderna.

De beräkningsmetoder som används för att visa att säkerhetskraven uppfylls ska vara tillförlitliga och validerade för sitt ändamål. De ska tillämpas så att de beräkningsmässiga slutresultat på vilka dimensioneringen av system baseras med stor säkerhet uppfyller kriterierna för godkännande. Vid fastställandet av säkerhetsmarginaler ska osäkerheten hos resultat bedömas och beaktas.

Storbritannien

Övergripande principer

FP.3 Optimisation of protection
Protection must be optimized to provide the highest level of safety that is reasonably practicable.

FP.4 Safety assessment
The dutyholder must demonstrate effective understanding of the hazards and their control for a nuclear site or facility through a comprehensive and systematic process of safety assessment.

FA.1 Design basis analysis, PSA and severe accident analysis
Fault analysis should be carried out comprising design basis analysis, suitable and sufficient PSA, and suitable and sufficient severe accident analysis.

FA.2 Identification of initiation faults
Fault analysis should identify all initiating faults having the potential to lead to any person receiving a significant dose of radiation, or to a significant quantity of radioactive material escaping from its designated place of residence or confinement.

FA.3 Fault sequences
Fault sequences should be developed from the initiating faults and their potential consequences analysed.

FA.4 Fault tolerance
BA should be carried out to provide a robust demonstration of the fault

tolerance of the engineering design and the effectiveness of the safety measures.

FA.5 Initiating faults
The safety case should list all initiating faults that are included within the design basis analysis of the facility.

FA.6 Fault sequences
For each initiating fault in the design basis, the relevant design basis fault sequences should be identified.

FA.8 Linking of initiating faults, fault sequences and safety measures
DBA should provide a clear and auditable linking of initiating faults, fault sequences and safety measures.

FA.9 Further use of DBA
DBA should provide an input into the safety classification and the engineering requirements for systems, structures and components performing a safety function; the limits and conditions for safe operation; and the identification of requirements for operator actions.

FA.10 Need for PSA
Suitable and sufficient PSA should be performed as part of the fault analysis and design development and analysis.

FA.11 Validity
PSA should reflect the current design and operation of the facility or site.

FA.12 Scope and extent
PSA should cover all significant sources of radioactivity and all relevant initiating faults identified at the facility or site.

FA.13 Adequate representation
The PSA model should provide an adequate representation of the site and its facilities.

FA.14 Use of PSA
PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities.

FA.15 Fault sequences
Fault sequences beyond the design basis that have the potential to lead to a severe accident should be analysed.

FA.16 Use of severe accident analysis
The severe accident analysis should be used in the consideration of further risk-reducing measures.

FA.17 Theoretical models
Theoretical models should adequately represent the facility and site.

FA.18 Calculation methods
Calculational methods used for the analyses should adequately represent the physical and chemical processes taking place.

FA.19 Use of data
The data used in the analysis of safety-related aspects of plant performance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means.

FA.20 Computer models
Computer models and datasets used in support of the analysis should be developed, maintained and applied in accordance with appropriate quality assurance procedures.

FA.21 Documentation
Documentation should be provided to facilitate review of the adequacy of the analytical models and data.

FA.22 Sensitivity studies
Studies should be carried out to determine the sensitivity of the fault analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation.

FA.23 Data collection
Data should be collected throughout the operating life of the facility to check or update the fault analysis.

FA.24 Update and review
The fault analysis should be updated where necessary, and reviewed periodically.

Vägledande råd

514 Initiating faults identified in Principle FA.2 should be considered for inclusion in this list, but the following need not be included:

a) faults in the facility that have an initiating frequency lower than about 1 x 10-5 pa;
b) failures of structures, systems or components for which appropriate specific arguments have been made;
c) natural hazards that conservatively have a predicted frequency of being exceeded of less than 1 in 10 000 years;
d) those faults leading to unmitigated consequences which do not exceed the BSL for the respective initiating fault frequency in Target 4 (paragraph 599 f.).

Note: The risks from initiating faults in d) should be shown to be as low as reasonably practicable by application of relevant good engineering practice supported by deterministic and probabilistic analysis as appropriate.

515 Initiating fault frequencies should be determined on a best-estimate basis with the exception of natural hazards where a conservative approach should be adopted.

545 This should include:

a) determination of the magnitude and characteristics of their radiological consequences, including societal effects; and
b) demonstration that there is no sudden escalation of consequences just beyond the design basis.

546 The analysis should consider failures that could occur in the physical barriers preventing release of radioactive material, or in the shielding against direct radiation.

547 A best estimate approach should normally be followed. However, where uncertainties are such that a realistic analysis cannot be performed with confidence, a conservative or bounding case approach should be adopted to avoid optimistic conclusions being drawn.

548 Where severe accident uncertainties are judged to have a significant effect on the assessed risk, research aimed at confirming the modelling assumptions should be performed.

Kanada

Krav

RD–337, 4.2.3 Safety Analyses
To demonstrate achievement of the safety objectives, a comprehensive hazard analysis, a deterministic safety analysis, and a probabilistic safety assessment are carried out. These analyses identify all sources of exposure, in order to evaluate potential radiation doses to workers at the plant and to the public, and to evaluate potential effects on the environment.

The safety analyses examine plant performance for:

1. Normal operation;
2. Anticipated operational occurrences;
3. Design basis accidents; and
4. Beyond design basis accidents (BDBAs), including event sequences that may lead to a severe accident.

Based on these analyses, the capability of the design to withstand postulated initiating events (PIEs) and accidents can be confirmed, the effectiveness of the items important to safety can be demonstrated, and requirements for emergency response can be established. The results of the safety analyses are fed back into the design.

The safety analyses are discussed in further detail in Section 9.0.

RD–337, 4.2.4 Accident Mitigation and Management
The design includes provisions to limit radiation exposure in normal operation and AOOs to ALARA levels, and to minimize the likelihood of an accident that could lead to the loss of normal control of the source of radiation. However, given that there is a remaining probability that an accident may occur, measures are taken to mitigate the radiological consequences of accidents.

This includes such measures as:

1. Consideration of inherent safety features;
2. Incorporation of engineered design features;
3. Establishment by the operating organization of on-site accident management procedures; and
4. Establishment of off-site intervention measures by appropriate authorities.

The design applies the principle that plant states that could result in high radiation doses or radioactive releases have a very low frequency of occurrence, and plant states with significant frequency of occurrence have only minimal, if any, potential radiological consequences.

RD–337, 5.6 Safety Assessment
Safety assessment is a systematic process applied throughout the design phase to ensure that the design meets all relevant safety requirements. This includes the requirements set by the operating organization and by regulatory authorities. The basis for the safety assessment is the data derived from the safety analysis, previous operational experience, results of supporting research, and proven engineering practices.

The safety assessment is part of the design process, with iteration between the design and analyses, and increases in scope and level of detail as the design process progresses.

Before the design is submitted, an independent peer review of the safety assessment is conducted by individuals or groups separate from those carrying out the design.

Safety assessment documentation identifies those aspects of operation, maintenance, and management that are important to safety. This documentation is maintained in a dynamic suite of documents to reflect changes in design as the plant evolves.

Safety assessment documentation is presented clearly and concisely, in a logical and understandable format, and will be made readily accessible to designers, operators, and the CNSC.

RD–337, 7.2 Plant Design Envelope
The design authority establishes the plant design envelope, which comprises the design basis and complementary design features.

The design basis specifies the capabilities that are necessary for the plant in normal operation, AOOs, and DBAs.

Conservative design measures and sound engineering practices are to be applied in the design basis for normal operation, AOOs, and DBAs. This provides a high degree of assurance that no significant damage will occur to the reactor core, and that radiation doses will remain within established limits.

Complementary design features address the performance of the plant in BDBAs, including selected severe accidents.

RD–337, 7.3 Plant States
Plant states are grouped into the following four categories:

1. Normal Operation—operation within specified OLCs, including start-up, power operation, shutting down, shutdown, maintenance, testing, and refuelling;
2. Anticipated Operational Occurrence—a deviation from normal operation that is expected to occur once or several times during the operating lifetime of the NPP but which, in view of the appropriate design provisions, does not cause any significant damage to items important to safety, nor lead to accident conditions;
3. Design Basis Accidents—accident conditions for which an NPP is designed according to established design criteria, and for which damage to the fuel and the release of radioactive material are kept within regulated limits; and
4. Beyond Design Basis Accidents—accident conditions less frequent and more severe than a design basis accident. A BDBA may or may not involve core degradation.

Acceptance criteria are assigned to each plant state, taking into account the expectation that frequent PIEs will have only minor or no radiological consequences, and events that may result in severe consequences are of extremely low probability.

RD–337, 7.3.1 Normal Operation
The design facilitates safe operation of the plant within a defined range of parameters, with an assumed availability of a minimum set of specified support features for safety systems.

The design minimizes the unavailability of safety systems. The design addresses the potential for accidents to occur when the availability of safety systems may be reduced, such as during shutdown, start-up, low power operation, refuelling, and maintenance.

The design establishes a set of requirements and limitations for safe normal operation, including:

1. Limits important to safety;
2. Constraints on control systems and procedures;
3. Plant maintenance, testing, and inspection requirements to ensure that SSCs function as intended, taking the ALARA principle into consideration; and
4. Clearly defined operating configurations, such as start-up, power production, shutdown, maintenance, testing, surveillance, and refuelling—these configurations include relevant operational restrictions in the event of safety system and safety support system outages.

These requirements and limitations, together with the results of safety analysis, form the basis for establishing the OLCs according to which the plant will be authorized to operate, as discussed in subsection 4.3.3 of this document.

RD–337, 7.3.2 Anticipated Operational Occurrences
The design includes provisions such that releases to the public following an AOO do not exceed the dose acceptance criteria.

The design also provides that, to the extent practicable, SSCs not involved in the initiation of an AOO will remain operable following the AOO.

The response of the plant to a wide range of AOOs allows safe operation or shutdown, if necessary, without the need to invoke provisions beyond defence-in-depth Level 1 or, at most, Level 2.

The facility layout is such that equipment is placed at the most suitable location to ensure its immediate availability when operator intervention is required, allowing for safe and timely access during an AOO.

RD–337, 7.3.3 Design Basis Accidents
The set of design basis accidents sets the boundary conditions according to which SSCs important to safety are designed.

The design is such that releases to the public following a DBA will not exceed the dose acceptance criteria.

In order to prevent progression to a more severe condition that may threaten the next barrier, the design includes provision to automatically initiate the necessary safety systems where prompt and reliable action is required in response to a PIE.

Provision is also made to support timely detection of, and manual response to, conditions where prompt action is not necessary. This includes such responses as manual initiation of systems or other operator actions.

The design takes into account operator actions that may be necessary to diagnose the state of the plant and to put it into a stable long-term shutdown condition in a timely manner. Such operator actions are facilitated by the provision of adequate instrumentation to monitor plant status, and controls for manual operation of equipment.

Any equipment necessary for manual response and recovery processes is placed at the most suitable location to allow safe and timely worker access when needed.

RD–337, 7.3.4 Beyond Design Basis Accidents
The design authority identifies credible BDBAs, based on operational experience, engineering judgment, and the results of analysis and research. This includes events leading to significant core degradation (severe accidents), particularly those events that challenge containment.

Complementary design features are then considered with the goal of preventing identified BDBA scenarios, and mitigating their consequences if they do occur.

Complementary design features include design or procedural considerations, or both, and are based on a combination of phenomenological models, engineering judgments, and probabilistic methods.

The design identifies the rules and practices that have been applied to the complementary design features. These rules and practices do not necessarily

need to incorporate the same degree of conservatism as those applied to the design basis.

The design identifies a radiological and combustible gas accident source term for use in the specification of the complementary design features for BDBAs. This source term is referred to as the reference source term, and is based on a set of representative core damage accidents established by the design authority.

In the case of multi-unit plants, the use of available support from other units is relied upon only if it can be established that the safe operation of the other units is not compromised.

To the extent practicable, the design provides biological shielding of appropriate composition and thickness to protect operational personnel during BDBAs, including severe accidents.

Severe Accidents

The design should be balanced such that no particular design feature or event makes a dominant contribution to the frequency of severe accidents, taking uncertainties into account.

Early in the design process, the various potential barriers to core degradation are identified, and features that can be incorporated to halt core degradation at those barriers are considered.

The design also identifies the equipment to be used in the management of severe accidents. A reasonable level of confidence that this equipment will perform as intended in the case of a severe accident is demonstrated by environmental, fire, and seismic assessments.

Particular attention is placed on the prevention of potential containment bypass in accidents involving significant core degradation.

Consideration is given to the plant’s full design capabilities, including the possible use of safety, non-safety, and temporary systems, beyond their originally intended function. This applies to any system that can be shown with a reasonable degree of assurance to be able to function in the environmental conditions expected during a severe accident.

Containment maintains its role as a leak-tight barrier for a period that allows sufficient time for the implementation of off-site emergency procedures following the onset of core damage. Containment also prevents uncontrolled releases of radioactivity after this period.

The design authority establishes initial severe accident management guidelines, taking into account the plant design features and the understanding of accident progression and associated phenomena.

The design considers prevention of recriticality following severe accidents.

RD–337, 7.4 Postulated Initiating Events Considered in the Design

Postulated initiating events can lead to AOO or accident conditions, and include credible failures or malfunctions of SSCs, as well as operator errors, common-cause internal hazards, and external hazards.

Safety Analysis for Nuclear Power Plants, RD–310, February 2008, Regulatory Document

USA

Krav

10 CFR 50.34: Content of Applications; Technical Information.

Guide

Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition — Transient and Accident Analysis (NUREG-0800, Chapter 15)

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 16: Postulated initiating events
The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design.

IAEA Safety Standard, No. SSR-2/1, Requirement 19: Design basis accidents
A set of accident conditions that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear power plant to withstand, without acceptable limits for radiation protection being exceeded.

IAEA Safety Standard, No. SSR-2/1, Requirement 20: Design extension conditions
A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences if they do occur.

IAEA Safety Standard, No. SSR-2/1, Requirement 42: Safety analysis of the plant design
A safety analysis of the design for the nuclear power plant shall be

conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed.

IAEA Safety Standard, No. SSR-2/1, 5.1
Plant states shall typically cover:

(a) Normal operation;
(b) Anticipated operational occurrences, which are expected to occur over the operating lifetime of the plant;
(c) Design basis accidents;
(d) Design extension conditions, including accidents with significant degradation of the reactor core.

IAEA Safety Standard, No. SSR-2/1, 5.2
Criteria shall be assigned to each plant state, such that frequently occurring plant states shall have no, or only minor, radiological consequences and plant states that could give rise to serious consequences shall have a very low frequency of occurrence.

IAEA Safety Standard, No. SSR-2/1, 5.5
The postulated initiating events shall be identified on the basis of engineering judgement and a combination of deterministic assessment and probabilistic assessment. A justification of the extent of usage of deterministic safety analysis and probabilistic safety analysis shall be provided, to show that all foreseeable events have been considered.

IAEA Safety Standard, No. SSR-2/1, 5.6
The postulated initiating events shall include all foreseeable failures of structures, systems and components of the plant, as well as operating errors and possible failures arising from internal and external hazards, whether in full power, low power or shutdown states.

IAEA Safety Standard, No. SSR-2/1, 5.9
The postulated initiating events used for developing the performance requirements for the items important to safety in the overall safety assessment and the detailed analysis of the plant shall be grouped into a specified number of representative event sequences that identify bounding cases and that provide the basis for the design and the operational limits for items important to safety.

IAEA Safety Standard, No. SSR-2/1, 5.10
A technically supported justification shall be provided for exclusion from the design of any initiating event that is identified in accordance with the comprehensive set of postulated initiating events.

IAEA Safety Standard, No. SSR-2/1, 5.24
Design basis accidents shall be used to define the design bases, including performance criteria, for safety systems and for other items important to safety that are necessary to control design basis accident conditions, with the objective of returning the plant to a safe state and mitigating the consequences of any accidents.

IAEA Safety Standard, No. SSR-2/1, 5.25
The design shall be such that for design basis accident conditions, key plant parameters do not exceed the specified design limits. A primary objective shall be to manage all design basis accidents so that they have no, or only minor, radiological impacts, on or off the site, and do not necessitate any off-siteintervention measures.

IAEA Safety Standard, No. SSR-2/1, 5.26
The design basis accidents shall be analysed in a conservative manner. This approach involves postulating certain failures in safety systems, specifying design criteria and using conservative assumptions, models and input parameters in the analysis.

IAEA Safety Standard, No. SSR-2/1, 5.27
An analysis of design extension conditions for the plant shall be performed[8]. The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions not considered design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to maintain the integrity of the containment. These additional safety features for design extension conditions, or this extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions in which there is a significant amount of radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core). The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that significant radioactive releases would be practically eliminated (see footnote 1). The effectiveness of provisions to ensure the functionality of the containment could be analysed on the basis of the best estimate approach.

IAEA Safety Standard, No. SSR-2/1, 5.29
The analysis undertaken shall include identification of the features that are designed for use in, or that are capable[9] of preventing or mitigating, events considered in the design extension conditions. These features:

(a) Shall be independent, to the extent practicable, of those used in more frequent accidents;
(b) Shall be capable of performing in the environmental conditions pertaining to these design extension conditions, including design extension conditions in severe accidents, where appropriate;
(c) Shall have a reliability commensurate with the function that they are required to fulfil.

IAEA Safety Standard, No. SSR-2/1, 5.71
On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed (see footnote 6). It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all

operational states, and is capable of meeting acceptable limits for accident conditions.

IAEA Safety Standard, No. SSR-2/1, 5.72
The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant.

IAEA Safety Standard, No. SSR-2/1, 5.73
The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant.

IAEA Safety Standard, No. SSR-2/1, 5.74
The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design.

IAEA Safety Standard, No. SSR-2/1, 5.75
The deterministic safety analysis shall mainly provide:

(a) Establishment and confirmation of the design bases for all items important to safety;
(b) Characterization of the postulated initiating events that are appropriate for the site and the design of the plant;
(c) Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements;
(d) Comparison of the results of the analysis with dose limits and acceptable limits, and with design limits;
(e) Demonstration that the management of anticipated operational occurrences and design basis accident conditions is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator;
(f) Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator.

Guide

Deterministic Safety Analysis for Nuclear Power Plants Specific Safety Guide, Series No. SSG-2, January 05, 2010.

Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants Specific Safety Guide, Series No. SSG-3, April 27, 2010.

Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants Specific Safety Guide, Series No. SSG-4, May 25, 2010.

Krav avseende bränsle och reaktorhärd

Sverige

Krav

23 § Reaktorhärden och anslutande system ska vara utformade så att

- konstruktionsgränserna för härden kan innehållas med tillräckliga marginaler vid alla händelser till och med händelseklassen förväntade händelser,
- effektpendlingar inte är möjliga, eller tillförlitligt kan upptäckas och dämpas innan kärnbränsleknippenas konstruktionsgränser överskrids.

24 § Reaktorhärden och anslutande kylsystem ska vara utformade så att nettoeffekten av härdens omedelbara reaktivitetsåterkoppling motverkar en reaktivitetsökning under effektdrift.

25 § Reaktorhärden och reaktivitetskontrollsystemen ska vara utformade på sådant sätt att reaktivitetstillskottet begränsas vid alla händelser till och med händelseklassen osannolika händelser, för att förhindra att

- konstruktionsgränserna för kärnbränsleknippenas kylbarhet överskrids,
- reaktortryckkärlets interna delar skadas så att härdens kylbarhet försämras,
- acceptansgränserna i konstruktionsförutsättningarna för de tryckbärande delarna i reaktorns primärsystem överskrids.

26 § En fastställd gräns ska finnas för högsta effektuttag från kärnbränsleknippena vid normal drift.

Vid det högsta effektuttaget enligt första stycket ska härden vara kylbar vid kylmedelsförlust. Gränsen för det högsta effektuttaget ska bestämmas så att

- överhettning och försprödning av bränslestavarnas kapsling samt väteproduktionen från knippena begränsas vid kylmedelsförlust,
- härdgeometrin inte förändras på sådant sätt vid kylmedelsförlust att kylningen förhindras,
- kärnbränsleknippenas resteffekt kan kylas bort.

27 § För varje bränslekonstruktion och utformning av härden ska det finnas fastställda driftgränser och parametrar som ska övervakas och följas upp vid driften av härden, i den utsträckning som behövs för att bestämmelserna i 23-26 §§ ska tillgodoses.

Analyserna av konstruktions- och driftgränser för reaktorhärden ska redovisas i kärnkraftsreaktorns säkerhetsredovisning enligt 4 kap. 2 § Strålsäkerhetsmyndighetens föreskrifter (SSMFS 2008:1) om säkerhet i kärntekniska anläggningar.

Finland

Krav

2 § Definitioner
I denna förordning avses med

6) *antagen olycka* sådan avvikelse från normala driftslägen som kan antas inträffa mera sällan än en gång under en tid av hundra driftår och som kärnkraftverket förutsätts klara av utan allvarliga bränsleskador, även om enstaka anordningar i system som är viktiga med tanke på säkerheten skulle vara ur funktion på grund av underhållsarbeten eller fel; antagna olyckor delas in i två klasser utgående från initialhändelsens omfattning enligt följande:
    c) antagna olyckor av klass 1 är olyckor som kan antas inträffa mera sällan än en gång per hundra driftår, men minst en gång per tusen driftår,
    d) antagna olyckor av klass 2 är olyckor som kan antas inträffa mera sällan än en gång per tusen driftår,
7) *spridning av antagna olyckor* situation som orsakas av en sällsynt yttre händelse[12] eller där en gemensam felorsak eller en invecklad kombination av flera fel uppträder i säkerhetssystemen i initialskedet av en driftstörning eller en antagen olycka av klass 1 och som kraftverket förutsätts klara av utan allvarliga bränsleskador,
8) *allvarlig reaktorolycka* situation där en betydande del av bränslet i reaktorn skadas,

13 § Tekniska hinder för spridning av radioaktiva ämnen
För att hindra spridningen av radioaktiva ämnen ska principen om strukturellt djupförsvar följas på det sätt som anges i denna paragraf.

Spridning av radioaktiva ämnen från en kärnreaktors bränsle till omgivningen ska förhindras med på varandra följande hinder, vilka är bränslet och dess inkapsling, kärnreaktorns kylkrets (primärkretsen) och reaktorinneslutningen.

Bränsle, reaktor, reaktorns primärkrets och tryckvattenreaktorns sekundärkrets, deras vattenkemi, inkapsling samt säkerhetsfunktioner ska planeras så att följande säkerhetsmål nås:

1) För tryggande av bränslets integritet ska
    – sannolikheten för att en bränsleskada uppstår vara liten i normal drift och vid förväntade driftstörningar,
    – antalet bränsleskador vid antagna olyckor vara litet och kylningen av bränslet inte få äventyras, och
    – möjligheten av att en kriticitetsolycka inträffar vara ytterst liten.

…

14 § Säkerhetsfunktioner och tryggande av dem
Vid tryggande av säkerhetsfunktioner ska i första hand utnyttjas naturliga säkerhetsegenskaper som kan uppnås med goda planeringslösningar. I

[12] Ytter händelser avser händelser som kan uppkomma utanför anläggningen och kan påverka anläggningens säkerhet. Yttre händelser innefattar bland annat naturfenomen, kemiska och bilogiska utsläpp i närregion, explosioner i närregion, flygplanskrascher samt händelser på det yttre elkraftnätet.

synnerhet ska samverkan av de fysikaliska återkopplingsfenomenen i kärnreaktorn vara sådan att den motverkar en ökning av reaktoreffekten. …

YVL B.1 §402

YVL B.1 Apendix B §135-136

Storbritannien

Övergripande principer

ERC.1 Design and operation of reactors
The design and operation of the reactor should ensure the fundamental safety functions are delivered with an appropriate degree of confidence for permitted operating modes of the reactor.

ERC.3 Stability in normal operation
The core should be stable in normal operation and should not undergo sudden changes of condition when operating parameters go outside their specified range.

ERC.4 Monitoring of safety-related parameters
The core should be designed so that safety-related parameters and conditions can be monitored in all operational and design basis fault conditions and appropriate recovery actions taken in the event of adverse conditions being detected.

Vägledande råd

439 The principles described in this sub-section apply to the reactor core as an assembly and to its main elements (eg the fuel, moderator, coolant, neutron absorbers, core restraints/supports and also breeder assemblies in fast reactors) individually when in the core. Specific principles for graphite cores are in the sub-section on Graphite components and structures (paragraph 303 ff.). The principles relate to the requirements to control reactivity, heat generation/removal and other aspects of the design so that components within the reactor can be kept within specified limits set to ensure an appropriate level of safety during operation and in design basis fault conditions.

440 The above principle covers normal operation, refuelling, testing and shutdown and design basis fault conditions. The fundamental safety functions are:

a) control of reactivity (including re-criticality following an event);
b) removal of heat from the core;
c) confinement or containment of radioactive substances.

441 There should be suitable and sufficient margins between the normal operational values of safety-related parameters and the values at which the physical barriers to release of fission products are challenged.

442 The requirements for loading and unloading of fuel and core components, refuelling programmes, core monitoring and the criteria and strategy for dealing with fuel failures should be specified.

443 No single moveable fissile assembly, moderator or absorber when added to or removed from the core should increase the reactivity by an amount greater than the shutdown margin, with an appropriate allowance for uncertainty. The uncontrolled movement of reactivity control devices should be prevented.

444 Where a shutdown system is also used for the control of reactivity, a suitable and sufficient shutdown margin should be maintained at all times.

445 Reactor shutdown and subsequent hold-down should not be inhibited by mechanical failure, distortion, erosion, corrosion etc of plant components, or by the physical behaviour of the reactor coolant, under normal operation or design basis fault conditions.

446 An increase in reactivity or reduction in coolant flow, caused by the unplanned:

a) movement within the core;
b) loss from the core; or
c) addition to the core;

of any component, object or substance should be prevented.

447 The geometry of the core should be maintained within limits that enable the passage of sufficient coolant to remove heat from all parts of the core. Where appropriate, means should be provided to prevent any obstruction of the coolant flow that could lead to damage to the core as a result of overheating. In particular the overheating of fuel should be prevented where this would give rise to:

a) fuel geometry changes that have an adverse effect on heat transport;
b) failure of the primary coolant circuit.

Note: Where these mechanisms cannot be prevented by design, protective measures should be available to maintain the plant in a safe condition.

448 The structural integrity limits for the core structure and its components (including the fuel) should ensure that their geometry will be suitably maintained.

449 Changes in temperature, coolant voiding, core geometry or the nuclear characteristics of components that could occur in normal operation or fault conditions should not cause uncontrollably large or rapid increases in reactivity.

450 Effects of changes in coolant condition or composition on the reactivity of the reactor core should be identified. The consequences of any adverse changes should be limited by the provision of protective systems or by reactor core design parameters.

451 There should be suitable and sufficient design margins to ensure that any reactivity changes do not lead to unacceptable consequences. Limits should be set for the maximum degree of positive reactivity.

452 The design of the core and its components should take account of any identified safety-related factors, including:

a) irradiation;
b) chemical and physical processes;
c) static and dynamic mechanical loads;
d) thermal distortion;
e) thermally-induced stress; and
f) variations in manufacture.

453 The core should be securely supported and positively located with respect to other components in the reactor to prevent gross unplanned movements of the structure of the core or adverse internal movements.

454 Core components should be mutually compatible and compatible with the remainder of the plant.

455 The incorrect location of any core components should be physically inhibited.

Kanada

Krav

RD–337, 7.11 Guaranteed Shutdown State
The design authority defines the guaranteed shutdown state (GSS) that will support safe maintenance activities of the NPP.

The design provides two independent means of preventing recriticality from any pathway or mechanism during the GSS.

The shutdown margin for GSS is such that the core will remain subcritical for any credible changes in the core configuration and reactivity addition. Where possible, this is achieved without operator intervention.

RD–337, 8.1 Reactor Core
The design provides protection against deformations to reactor structures that have the potential to adversely affect the behaviour of the core or associated systems.

The reactor core and associated structures and cooling systems:

1. Withstand static and dynamic loading, including thermal expansion and contraction;
2. Withstand vibration (such as flow-induced and acoustic vibration);
3. Ensure chemical compatibility;
4. Meet thermal material limits; and
5. Meet radiation damage limits.

The reactor core design facilitates the application of a guaranteed shutdown state as described in subsection 7.11.

The design of the core is such that:

1. The fission chain reaction is controlled during normal operation and AOOs; and
2. The maximum degree of positive reactivity and its maximum rate of increase by insertion in normal operation, AOOs, and DBAs are limited so that no resultant failure of the reactor pressure boundary will occur, cooling capability will be maintained, and no significant damage will occur to the reactor core.

The shutdown margin for all shutdown states is such that the core will remain subcritical for any credible changes in the core configuration and reactivity addition.

If operator intervention is required to keep the reactor in a shutdown state, the feasibility, timeliness, and effectiveness of such intervention is demonstrated.

RD–337, 8.1.1 Fuel Elements and Assemblies
Fuel assembly design includes all components in the assembly, such as the fuel matrix, cladding, spacers, support plates, movable rods inside the assembly, etc. The fuel assembly design also identifies all interfacing systems.

Fuel assemblies and the associated components are designed to withstand the anticipated irradiation and environmental conditions in the reactor core, and all processes of deterioration that can occur in normal operation and AOOs. At the design stage, consideration is given to long-term storage of irradiated fuel assemblies after discharge from the reactor.

Fuel design limits are established to include, as a minimum, limits on fuel power or temperature, limits on fuel burn-up, and limits on the leakage of fission products in the reactor cooling system. The design limits reflect the importance of preserving the cladding and fuel matrix, as these are the first barriers to fission product release.

The design accounts for all known degradation mechanisms, with allowance being made for uncertainties in data, calculations, and fuel fabrication.

Fuel assemblies are designed to permit adequate inspection of their structures and component parts prior to and following irradiation.

In DBAs, the fuel assembly and its component parts remain in position with no distortion that would prevent effective post-accident core cooling or interfere with the actions of reactivity control devices or mechanisms. The acceptance criteria for the fuel for DBAs are consistent with these expectations.

The expectations for reactor and fuel assembly design apply in the event of changes in fuel management strategy or in operating conditions over the lifetime of the plant.

Fuel design and design limits reflect a verified and auditable knowledge base. The fuel is qualified for operation, either through experience with the same type of fuel in other reactors, or through a program of experimental testing and analysis, to ensure that fuel assembly requirements are met.

RD–337, 8.1.2 Control System
The design provides the means for detecting levels and distributions of neutron flux. This applies to neutron flux in all regions of the core during normal operation (including after shutdown and during and after refuelling states), and during AOOs.

The reactor core control system detects and intercepts deviations from normal operation with the goal of preventing AOOs from escalating to accident conditions.

Adequate means are provided to maintain both bulk and spatial power distributions within a predetermined range.

The reactor control mechanisms limit the positive reactivity insertion rate to a level required to control reactivity changes and power manoeuvring.

The control system, combined with the inherent characteristics of the reactor and the selected operating limits and conditions, minimize the need for shutdown action.

The control system and the inherent reactor characteristics keep all critical reactor parameters within the specified limits for a wide range of AOOs.

USA

Krav

10 CFR 50 Appendix A, Criterion 10, Reactor design.
The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.

10 CFR 50 Appendix A, Criterion 12, Suppression of reactor power oscillations.
The reactor core and associated coolant, control, and protection systems shall be designed to assure that power oscillations which can result in conditions exceeding specified acceptable fuel design limits are not possible or can be reliably and readily detected and suppressed.

10 CFR 50 Appendix A, Criterion 11, Reactor inherent protection.
The reactor core and associated coolant systems shall be designed so that in the power operating range the net effect of the prompt inherent nuclear feedback characteristics tends to compensate for a rapid increase in reactivity.

10 CFR 50 Appendix A, Criterion 20, Protection system functions.
The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident

conditions and to initiate the operation of systems and components important to safety.

10 CFR 50 Appendix A, Criterion 25, Protection system requirements for reactivity control malfunctions. The protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods.

10 CFR 50 Appendix A, Criterion 27, Combined reactivity control systems capability.
The reactivity control systems shall be designed to have a combined capability, in conjunction with poison addition by the emergency core cooling system, of reliably controlling reactivity changes to assure that under postulated accident conditions and with appropriate margin for stuck rods the capability to cool the core is maintained.

10 CFR 50 Appendix A, Criterion 28, Reactivity limits.
The reactivity control systems shall be designed with appropriate limits on the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents can neither (1) result in damage to the reactor coolant pressure boundary greater than limited local yielding nor (2) sufficiently disturb the core, its support structures or other reactor pressure vessel internals to impair significantly the capability to cool the core. These postulated reactivity accidents shall include consideration of rod ejection (unless prevented by positive means), rod dropout, steam line rupture, changes in reactor coolant temperature and pressure, and cold water addition.

Guide

Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition (NUREG-0800).

SRP Section 4.2 describes all fuel damage criteria.

SRP Section 4.3 establishes fuel criteria for axial offset anomaly (AOA). The review of the nuclear design of the fuel assemblies, control systems, and reactor core is carried out to aid in confirming that fuel design limits will not be exceeded during normal operation or anticipated operational transients and that the effects of postulated reactivity accidents will not cause significant damage to the reactor coolant pressure boundary or impair the capability to cool the core and to assure conformance with the requirements of General Design Criteria (GDC) 10, 11, 12, 13, 20, 25, 26, 27, and 28.

For those criteria that involve DNBR or CPR limits, SRP Section 4.4 provides specific thermal-hydraulic criteria.

SRP Section 4.2 describes all fuel damage criteria. SRP Section 4.3 establishes fuel criteria for axial offset anomaly (AOA). For those criteria that involve DNBR or CPR limits, SRP Section 4.4 provides specific thermal-hydraulic criteria.

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 43: Performance of fuel elements and assemblies
Fuel elements and assemblies for the nuclear power plant shall be designed to maintain their structural integrity, and to withstand satisfactorily the anticipated radiation levels and other conditions in the reactor core, in combination with all the processes of deterioration that could occur in operational states.

IAEA Safety Standard, No. SSR-2/1, Requirement 44: Structural capability of the reactor core
The fuel elements and fuel assemblies and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions other than severe accidents, a geometry that allows for adequate cooling is maintained and the insertion of control rods is not impeded.

IAEA Safety Standard, No. SSR-2/1, Requirement 45: Control of the reactor core
Distributions of neutron flux that can arise in any state of the reactor core in the nuclear power plant, including states arising after shutdown and during or after refuelling, and states arising from anticipated operational occurrences and from accident conditions not involving degradation of the reactor core, shall be inherently stable. The demands made on the control system for maintaining the shapes, levels and stability of the neutron flux within specified design limits in all operational states shall be minimized.

IAEA Safety Standard, No. SSR-2/1, Requirement 46: Reactor shutdown
Means shall be provided to ensure that there is a capability to shut down the reactor of the nuclear power plant in operational states and in accident conditions, and that the shutdown condition can be maintained even for the most reactive conditions of the reactor core.

IAEA Safety Standard, No. SSR-2/1, 6.1
The processes of deterioration to be considered shall include those arising from: differential expansion and deformation; external pressure of the coolant; additional internal pressure due to fission products and the build-up of helium in fuel elements; irradiation of fuel and other materials in the fuel assembly; variations in pressure and temperature resulting from variations in power demand; chemical effects; static and dynamic loading, including flow induced vibrations and mechanical vibrations; and variations in performance in relation to heat transfer that could result from distortions or chemical effects. Allowance shall be made for uncertainties in data, in calculations and in manufacture.

IAEA Safety Standard, No. SSR-2/1, 6.2
Fuel design limits shall include limits on the permissible leakage of fission products from the fuel in anticipated operational occurrences so that the fuel remains suitable for continued use.

IAEA Safety Standard, No. SSR-2/1, 6.3
Fuel elements and fuel assemblies shall be capable of withstanding the loads and stresses associated with fuel handling.

IAEA Safety Standard, No. SSR-2/1, 6.4
Adequate means of detecting the neutron flux distributions in the reactor core and their changes shall be provided for the purpose of ensuring that there are no regions of the core in which the design limits could be exceeded.

IAEA Safety Standard, No. SSR-2/1, 6.5
In the design of reactivity control devices, due account shall be taken of wear out and of the effects of irradiation, such as burnup, changes in physical properties and production of gas.

IAEA Safety Standard, No. SSR-2/1, 6.6
The maximum degree of positive reactivity and its rate of increase by insertion in operational states and accident conditions not involving degradation of the reactor core shall be limited or compensated for to prevent any resultant failure of the pressure boundary of the reactor coolant systems, to maintain the capability for cooling and to prevent any significant damage to the reactor core.

IAEA Safety Standard, No. SSR-2/1, 6.7
The effectiveness, speed of action and shutdown margin of the means of shutdown of the reactor shall be such that the specified design limits for fuel are not exceeded.

IAEA Safety Standard, No. SSR-2/1, 6.8
In judging the adequacy of the means of shutdown of the reactor, consideration shall be given to failures arising anywhere in the plant that could render part of the means of shutdown inoperative (such as failure of a control rod to insert) or that could result in a common cause failure.

IAEA Safety Standard, No. SSR-2/1, 6.9
The means for shutting down the reactor shall consist of at least two diverse and independent systems.

IAEA Safety Standard, No. SSR-2/1, 6.10
At least one of the two different shutdown systems shall be capable, on its own, of maintaining the reactor subcritical by an adequate margin and with high reliability, even for the most reactive conditions of the reactor core.

IAEA Safety Standard, No. SSR-2/1, 6.11
The means of shutdown shall be adequate to prevent any foreseeable increase in reactivity leading to unintentional criticality during the shutdown, or during refuelling operations or other routine or non-routine operations in the shutdown state.

IAEA Safety Standard, No. SSR-2/1, 6.12
Instrumentation shall be provided and tests shall be specified for ensuring that the means of shutdown are always in the state stipulated for a given plant state.

Krav avseende undantag

Sverige

Krav

28 § Strålsäkerhetsmyndigheten får medge undantag från dessa föreskrifter om särskilda skäl föreligger och om det kan ske utan att syftet med föreskrifterna åsidosätts.

Finland

Den som vill avvika från de krav som ställs i direktivet måste för Strålsäkerhetscentralen presentera ett annat godtagbart förfaringssätt eller lösning, med vilka samma säkerhetsnivån som krävs i direktivet visas uppnås.

Storbritannien

-

Kanada

-

USA

Krav

10 CFR 50.12 Specific exemptions.
(a) The Commission may, upon application by any interested person or upon its own initiative, grant exemptions from the requirements of the regulations of this part, which are--

(1) Authorized by law, will not present an undue risk to the public health and safety, and are consistent with the common defense and security.
(2) The Commission will not consider granting an exemption unless special circumstances are present. Special circumstances are present whenever--
    (i) Application of the regulation in the particular circumstances conflicts with other rules or requirements of the Commission; or
    (ii) Application of the regulation in the particular circumstances would not serve the underlying purpose of the rule or is not necessary to achieve the underlying purpose of the rule; or
    (iii) Compliance would result in undue hardship or other costs that are significantly in excess of those contemplated when the

regulation was adopted, or that are significantly in excess of those incurred by others similarly situated; or

(iv) The exemption would result in benefit to the public health and safety that compensates for any decrease in safety that may result from the grant of the exemption; or

(v) The exemption would provide only temporary relief from the applicable regulation and the licensee or applicant has made good faith efforts to comply with the regulation; or

(vi) There is present any other material circumstance not considered when the regulation was adopted for which it would be in the public interest to grant an exemption. If such condition is relied on exclusively for satisfying paragraph (a)(2) of this section, the exemption may not be granted until the Executive Director for Operations has consulted with the Commission.

(b) Any person may request an exemption permitting the conduct of activities prior to the issuance of a construction permit prohibited by § 50.10. The Commission may grant such an exemption upon considering and balancing the following factors:

(a) Whether conduct of the proposed activities will give rise to a significant adverse impact on the environment and the nature and extent of such impact, if any;

(b) Whether redress of any adverse environment impact from conduct of the proposed activities can reasonably be effected should such redress be necessary;

(c) Whether conduct of the proposed activities would foreclose subsequent adoption of alternatives; and

(d) The effect of delay in conducting such activities on the public interest, including the power needs to be used by the proposed facility, the availability of alternative sources, if any, to meet those needs on a timely basis and delay costs to the applicant and to consumers.

Issuance of such an exemption shall not be deemed to constitute a commitment to issue a construction permit. During the period of any exemption granted pursuant to this paragraph (b), any activities conducted shall be carried out in such a manner as will minimize or reduce their environmental impact.

IAEA

-

Krav avseende mänskliga faktorer

Sverige

-

Finland

Krav

6 § Bemästrande av mänskliga faktorer
Vid planeringen, uppförandet, driften och underhållet av ett kärnkraftverk ska särskild uppmärksamhet fästas vid undvikande, upptäckt och korrigering av mänskliga fel.

Förekomsten av eventuella fel ska beaktas vid planeringen av både kärnkraftverket och dess drift och underhåll så att eventuella mänskliga fel och de avvikelser från anläggningens normala verksamhet som de orsakar inte äventyrar säkerheten vid anläggningen. Effekterna av mänskliga fel ska begränsas genom olika metoder vid säkerhetsplaneringen såsom djupförsvar, mångfald, olikhet och åtskiljning.

Storbritannien

Övergripande principer

EHF.1 Integration with design, assessment and management
A systematic approach to integrating human factors within the design, assessment and management of systems should be applied throughout the entire facility life-cycle.

EHF.2 Allocation of safety actions
When designing systems, the allocation of safety actions between humans and technology should be substantiated and dependence on human action to maintain a safe state should be minimised.

EHF.3 Identification of actions impacting safety
A systematic approach should be taken to identifying human actions that can impact on safety.

EHF.4 Identification of administrative controls
Administrative controls used to remain within the safe operating envelope should be systematically identified.

EHF.5 Task analysis
Analysis should be carried out of tasks important to safety to determine demands on personnel in terms of perception, decision making and action.

EHF.6 Workspaces
Workspaces in which plant operations and maintenance are conducted should be designed to support reliable task performance, by taking account of human perceptual and physical characteristics and the impact of environmental factors.

EHF.7 User interfaces
User interfaces, comprising controls, indications, recording instrumentation and alarms should be provided at appropriate locations and should be suitable and sufficient to support effective monitoring and control of the plant during all plant states.

EHF.8 Personnel competence
A systematic approach to the identification and delivery of personnel competence should be applied.

EHF.9 Procedures
Procedures should be produced to support reliable human performance during activities that could impact on safety.

EHF.10 Human reliability

Risk assessments should identify and analyse human actions or omissions that might impact on safety.

Vägledande råd

375 A nuclear facility is a complex socio-technological system that comprises both engineered and human components. The human contribution to nuclear safety can be positive or negative, and may be made during facility design, construction, commissioning, operation, maintenance and decommissioning. A systematic approach to understanding the factors that affect human performance, and minimising the potential for human error to contribute to faults, should therefore be applied throughout the entire facility life-cycle. Assessments of the way in which individual, team and organisational performance can impact upon nuclear safety should influence the design of the plant, equipment and administrative control systems. The allocation of safety actions to human or engineered components should take account of their differing capabilities and limitations. The assessments should demonstrate that interactions between human and engineered components are fully understood, and that human actions that might impact on nuclear safety are clearly identified and adequately supported.

377 This principle includes defining the safety actions of personnel responsible for monitoring and controlling plant and responding to faults, and of personnel carrying out maintenance, testing and calibration activities. It also includes considering the impact on safety of engineers, analysts, managers and other staff who may not directly interact with plant and equipment.

378 The design of these controls should be such that the requirements for personnel action are clearly identified and unambiguous to those responsible for their implementation.

379 The analysis should address the actions identified using Principles EHF.3 and EHF.4, and should include consideration of physical, psychological and cognitive factors that could impact on human performance.

380 The analysis should demonstrate the feasibility of these actions within the available timescales and should inform the way they are designed and supported to achieve reliable task performance. It should be sufficiently detailed, and demonstrably employed, to provide a basis for developing user interfaces, procedures and job aids, as well as defining operator roles and responsibilities, staffing levels, personnel competence and training needs, communication networks and workspace design.

381 The workload of personnel required to fulfil safety-related actions should be analysed and demonstrated to be reasonably achievable. Wherever possible, this demonstration should form part of the inactive commissioning of the facility.

382 Shift systems should be designed to minimise the likelihood of human error.

383 This principle applies to central control rooms, local control stations on the plant and emergency locations that should remain habitable during foreseeable facility emergencies. It also applies to provisions for maintenance and testing.

384 The user interface provisions should encompass normal operation, abnormal operation and postulated fault conditions including, where reasonably practicable, severe accidents.

385 The user interface should:

a) enable the operator to determine plant states and the availability, and status, of plant equipment;
b) provide a conspicuous early warning of any safety-related changes in plant state;
c) provide the means of confirming safety system challenges and identifying, initiating and confirming necessary safety actions;
d) support effective diagnosis of plant deviations; and
e) enable the operator to determine and execute appropriate system actions, including actions to overcome failures of automated safety systems or to reset a safety system after its operation.

386 The user interface should be designed to ensure compatibility with human psychological and physical characteristics and to facilitate reliable human performance. Interfaces and equipment should be clearly labelled.

387 The process for identifying and delivering competence should encompass the phases of: job analysis; identification of competence requirements; training needs analysis; training programme design and implementation; formal assessment of competence; and evaluation. The process should be applied to all those whose actions could impact on safety, including employees and other groups of staff such as contractors. Directors, managers and leaders should be included in this process. Appropriate supervision and monitoring should be maintained until individuals are demonstrably competent to perform their tasks.

388 Procedures should be accurate and designed and presented in a format that is compatible with the needs of the end user and suitable for the task that they are designed to support.

389 Assessments should include precursor errors, such as the introduction of unrevealed errors during maintenance, actions that contribute to initiating events, post-fault responses and long-term recovery actions.

390 The selection and application of probability data for human errors should be:

a) derived from operational experience data and/or through the application of recognised human reliability assessment techniques. Use of either approach should be justified and its relevance for the task and context demonstrated;
b) underpinned by task analysis and reflect the influence of human performance shaping factors, making due allowance for uncertainty.

391 Risk assessments should directly model dependent human errors committed by a single operator or different operators. The results of the risk assessments should be used in the fault analysis.

Kanada

Krav

RD–337, 7.21 Human Factors
The design includes a human factors engineering program plan.

Relevant and proven systematic analysis techniques are used to address human factors issues within the design process.

Human factors considerations:

1. Reduce the likelihood of human error as far reasonably achievable;
2. Provide means for identifying the occurrence of human error, and methods by which to recover from such error; and
3. Mitigate the consequences of error.

The human factors engineering program also facilitates the interface between the operating personnel and the plant by promoting attention to plant layout and procedures, maintenance, inspection, training, and the application of ergonomic principles to the design of working areas and working environments.

Appropriate and clear distinction between the functions assigned to operating personnel and those assigned to automatic systems is facilitated by systematic consideration of human factors and the human-machine interface. This consideration continues in an iterative way throughout the entire design process.

The human-machine interfaces in the main control room, the secondary control room, the emergency support centre, and in the plant, provide operators with necessary and appropriate information in a usable format that is compatible with the necessary decision and action times.

Human factors verification and validation plans are established for all appropriate stages of the design process to confirm that the design adequately accommodates all necessary operator actions.

To assist in the establishment of design criteria for information display and controls, each operator is considered to have dual roles—that of a systems manager, including responsibility for accident management, and that of an equipment operator. Verification and validation activities are comprehensive, such that the design conforms to human factors design principles and meets usability requirements.

The design identifies the type of information that facilitates an operator's ability to readily:

1. Assess the general state of the plant, whether in normal operating, AOO, or DBA states;
2. Confirm that the designed automatic safety actions are being carried out; and
3. Determine the appropriate operator-initiated safety actions to be taken.

The design provides the type of information that enables an individual in an equipment operator role to identify the parameters associated with individual plant systems and equipment, and to confirm that the necessary safety actions can be initiated safely.

Design goals include promoting the success of operator action with due regard for the time available for response, the physical environment to be expected, and the associated psychological demands made on the operator.

The need for operator intervention on a short time scale is kept to a minimum. Where such intervention is necessary, the following conditions apply:

1. The information necessary for the operator to make the decision to act is presented simply and unambiguously;
2. The operator has sufficient time to make a decision and to act; and
3. Following an event, the physical environment is acceptable in the main control room or in the secondary control room, and in the access route to the secondary control room.

USA

-

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, Requirement 32: Design for optimal operator performance
Systematic consideration of human factors, including the human–machine

interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process.

IAEA Safety Standard, No. SSR-2/1, 5.53
The design for a nuclear power plant shall specify the minimum number of operating personnel required to perform all the simultaneous operations necessary to bring the plant into a safe state.

IAEA Safety Standard, No. SSR-2/1, 5.54
Operating personnel who have gained operating experience in similar plants shall, as far as is practicable, be actively involved in the design process conducted by the design organization, in order to ensure that consideration is given as early as possible in the process to the future operation and maintenance of equipment.

IAEA Safety Standard, No. SSR-2/1, 5.55
The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks, and shall limit the effects of operating errors on safety. The design process shall pay attention to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant.

IAEA Safety Standard, No. SSR-2/1, 5.56
The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, in accordance with the necessary decision times and action times. The information necessary for the operator to make a decision to act shall be simply and unambiguously presented.

IAEA Safety Standard, No. SSR-2/1, 5.57
The operator shall be provided with the necessary information:

(a) To assess the general state of the plant in any condition;
(b) To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions);
(c) To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended;
(d) To determine both the need for and the time for manual initiation of the specified safety actions.

IAEA Safety Standard, No. SSR-2/1, 5.58
The design shall be such as to promote the success of operator actions with due regard for the time available for action, the conditions to be expected and the psychological demands being made on the operator.

IAEA Safety Standard, No. SSR-2/1, 5.59
The need for intervention by the operator on a short time scale shall be kept to a minimum, and it shall be demonstrated that the operator has sufficient time to make a decision and sufficient time to act.

IAEA Safety Standard, No. SSR-2/1, 5.60
The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the control room or the supplementary control room and in locations on the access route to the supplementary control room do not compromise the protection and safety of the operating personnel.

IAEA Safety Standard, No. SSR-2/1, 5.61
The design of workplaces and the working environment of the operating personnel shall be in accordance with ergonomic concepts.

IAEA Safety Standard, No. SSR-2/1, 5.62
Verification and validation, including by the use of simulators, of features relating to human factors shall be included at appropriate stages to confirm that necessary actions by the operator have been identified and can be correctly performed.

Guide

Recruitment, Qualification and Training of Personnel for Nuclear Power Plants Safety Guide, Series No. NS-G-2.8, November 19, 2002.

Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants Safety Guide, Series No. NS-G-2.2, December 19, 2000.

Krav avseende förläggningsplats samt uppförande och idrifttagning av ett kärnkraftverk

Sverige

-

Finland

Krav

11§ Kärnkraftverkets förläggningsplats
Vid valet av förläggningsplats för ett kärnkraftverk ska de lokala förhållandenas inverkan på säkerheten samt skydds- och beredskapsarrangemangen beaktas.

Förläggningsplatsen ska vara sådan att de olägenheter och hot som anläggningen medför för sin omgivning är mycket små och att anläggningens värmeavledning till omgivningen kan ordnas på ett tillförlitligt sätt.

21 § Uppförande
Den som innehar tillstånd att uppföra ett kärnkraftverk ska under konstruktionsprocessen se till att kraftverket uppförs och byggandet genomförs i enlighet med godkända planer och förfaranden.

Tillståndshavaren ska också se till att anläggningsleverantören och de underleverantörer som producerar tjänster och produkter som är viktiga med tanke på säkerheten förfar på ett sakligt sätt.

22 § Idrifttagning
Vid idrifttagningen av ett kärnkraftverk ska tillståndshavaren säkerställa att systemen, konstruktionerna och anordningarna samt kraftverket i dess helhet fungerar planenligt.

När kärnkraftverket tas i drift ska tillståndshavaren se till att det finns en ändamålsenlig organisation, tillräckligt med yrkeskunnig personal och relevanta anvisningar med tanke på den kommande driften av anläggningen.

Storbritannien

Övergripande principer

ST.1 Siting factors
Account should be taken of all relevant factors that might affect the protection of individuals and populations from radiological risk when assessing the siting of a new facility.

ST.2 Population characteristics
The safety case should demonstrate that the characteristics of the population off-site would allow for an effective off-site emergency response.

ST.3 Local physical data
The safety case should include information on local physical data relevant to the dispersion of released radioactivity and its potential effects on people.

ST.4 External hazards
Natural and man-made external hazards should be considered if they have the potential to adversely affect the siting decision.

ST.5 Effect on other hazardous installations
The safety case should take account of any hazardous installations that might be affected by an incident at the nuclear facility.

ST.6 Multi-facility sites
On multi-facility sites, the safety case should consider the site as a whole to establish that hazards from interactions between facilities have been taken into account.

ST.7 Through life siting issues
The safety case should be revised to take account of off-site changes that could affect safety on a nuclear site.

ECM.1 Commission testing
Before operating any facility or process that may affect safety it should be subject to commissioning tests to demonstrate that, as built, the design intent claimed in the safety case has been achieved.

Vägledande råd

103 Siting characteristics are relevant to various circumstances – new facilities or sites or modifications to them. The factors that should be considered in assessing sites cover three main aspects:

a) the location and characteristics of the population around the site and the physical factors affecting the dispersion of released radioactivity that might have implications for the radiological risk to people;
b) external hazards that might preclude the use of the site for its intended purpose;
c) the suitability of the site for the engineering and infrastructure requirements of the facility.

105 The acceptability of a site is regulated by HSE with respect to the direct radiation shine from normal operation and for all doses from accidents. The environment agencies, in liaison with HSE, regulate discharges from normal operations. Protection against direct radiation shine is covered by the radiological protection principles, see paragraph 476 ff.

106 In assessing an application for the use of a site, NII takes account of the practicability of emergency responses to mitigate the health implications for humans of exposure to radiation through the inhalation of radioactivity, radiation shine from radioactivity in the atmosphere or deposited on the ground or structures, and inadvertent ingestion of contaminated dust or soil. Consideration of other routes of exposure such as contaminated foodstuffs or water, and effects on the non-human environment or economic activity, are undertaken using advice from these bodies. NII consults these other bodies before granting a licence for the use of the site, under NIA, as amended by the Environment Act 1995 Schedule 2 paragraph 7.

107 For an application to use a site for a new nuclear power station, and for subsequent land-use in the vicinity, UK Government policy at the time of writing includes the consideration of demographics to constrain the number of people who might be affected in the event of an emergency. Although siting is usually considered with respect to a new facility on a new site, any new facility, either on an existing site or in its vicinity, or any significant extension to such a facility, should be checked to ensure that its presence does not invalidate any of the arguments used in granting the licence. NII, as part of HSE, is a statutory consultee for any planning application in the vicinity of a nuclear licensed site.

109 The factors of interest here include: the demography around the site; the need for effective accident management and emergency preparedness; and certain external hazards associated with the site.

110 Any foreseeable variations in these factors during the expected life-cycle of the site should be identified and taken into account. The factors should be included in the periodic reviews of safety cases for the facility.

111 For new nuclear power stations, the criteria defined in Government policy should be used in assessment.

112 Allowing for some natural growth in the size and distribution of the population around the site, it should be shown that:

a) it would be possible to invoke off-site countermeasures within an appropriate timescale consistent with the emergency plan (see the section on Accident management and emergency preparedness (paragraph 639 ff.));
b) there are no institutions with a high concentration of relatively immobile people; or if there is any such institution, the emergency planning authority (ie the local authority) confirms that appropriate arrangements have been made in its emergency plan.

113 The characteristics of the off-site population should not prejudice the extendibility of emergency response beyond the Detailed Emergency Planning Zone (DEPZ), on an appropriate timescale, to deal with a larger radiation emergency than that used to define the DEPZ.

114 Consideration should be given to aspects that might affect the movement of people and goods, including nuclear materials, into and out of the site, regarding any implications for safety during normal operation (see the sub-section on Control of nuclear matter (paragraph 392 ff.)).

115 These considerations should include all transport routes, including road, rail, sea, air and underground routes.

116 The safety case should identify data on aspects of local topography, hydrology, geology and hydrogeology relevant to radioactivity dispersion.

117 The safety case should identify data on aspects of meteorology relevant to radioactivity dispersion off-site, including any local variations from the regional.

118 To demonstrate the practicability of emergency response, the data should be used in assessment of potential dispersion and deposition of radioactivity from possible radiation emergencies, using well-established and researched models.

119 The safety case should provide information on local topography and transport routes and identify any implications for the movement of people arising from the new facility.

120 Consideration should be given to implications for the emergency response of local topography and transport routes, taking account of factors including the evacuation of people off-site, movement and protection of emergency personnel and emergency vehicles and goods travelling to and from the site.

121 If the external hazards over which the dutyholder has no control are judged to be too great to be accommodated through the design of plant, the use of a site may be precluded for its proposed purpose.

122 This principle covers possible situations where a non-nuclear hazardous installation off-site might be damaged by a nuclear or non-nuclear incident on the nuclear site. This may exacerbate the off-site effects of the nuclear site incident or increase the difficulty of remedial action on the nuclear site. It should cover transport facilities as well as fixed installations etc.

123 The assessment of interactions between facilities requires that:

a) all potential radiological hazards on the site should be identified;
b) all facilities on the site should be identified: for completeness, this must include facilities that do not contain radioactive or nuclear material;
c) all services on the site should be identified.

124 Interactions between facilities, between facilities and shared services and between shared services, where events in one may adversely affect others, should be explicitly considered in determining the potential for escalation of the risks for the site. This requires an analysis of events that can have physical effects outside the boundaries or limits for the particular facility or service. These may be:

a) faults, internal hazards or external hazards that affect more than one facility and shared service at the same time;
b) domino effects that can progress directly from one facility to another or via shared services;
c) interactions between shared services that affect several facilities.

125 In considering the risks from a site, and whether they are ALARP, consideration on a site-wide basis will be needed for certain internal or external hazards that have the potential to affect all the facilities and services on the site.

126 Where a site has been considered for analysis purposes as comprising several facilities, a specific consideration of overall site risks should be carried out, unless it can be shown that there are no common shared services or interactions between the facilities, between facilities and shared services and between shared services.

127 Where neighbouring sites, which may be under the control of different dutyholders, share common systems or have the potential for interactions, there should be co-operation between them in developing safety cases. Formal mechanisms should be established and demonstrated to be working to regulators. All relevant dutyholders should be able to demonstrate that they are undertaking liaison and acting upon agreed decisions with site owners and all external stakeholders.

128 The safety case needs to be reviewed to take account of the potential impact of local developments on the site.

129 Arrangements should be in place for the relevant planning authority(ies) to be consulted throughout the facility lifecycle on any proposed land-use developments off-site that might prejudice the effectiveness of the arrangements to protect individuals and populations. HSE makes similar arrangements to be consulted by planning authorities.

130 New information that could have an impact on activities on-site or off-site should be checked to establish the affect on safety. Suitable amendments should be made to the safety case and operation and emergency arrangements, as appropriate.

182 The commissioning tests should endeavour to identify any errors made during the design, manufacture, or construction/installation stages.

183 Commissioning should be more than a demonstration that the plant will work. It should also include safety tests as a key step in assuring safety. This is the intent of Licence Condition 21 (see the HSE website). The tests should be designed to demonstrate that the plant and associated safety systems provide the intended degree of protection against faults, including human errors.

184 The safety case should identify those commissioning tests and inspections required to:

a) confirm the facility's design safety assumptions and predicted performance, in particular that of the safety provisions; and
b) characterise the facility as a basis for evaluating its behaviour during its operational life. The safety analysis should be reviewed in the light of the results of the commissioning programme and of any modifications made to the design or intended operating procedures since the commencement of construction.

185 The tests should be divided into stages to complete as much inactive testing before the introduction of radioactive substance. Inactive testing should demonstrate that the facility has been constructed, manufactured, and installed correctly. Where any deviations from the documentation are found, the licensee should demonstrate that this does not compromise the safety analysis in the safety case.

186 Inactive testing should also be used to confirm the operational features of the facility and be used to develop the operating instructions, which should then be confirmed during active commissioning. Before active commissioning can begin, the necessary arrangements to satisfy Principles MS.2 (paragraph 51 f.) and SC.6 (paragraph 95 f.), especially in relation to operating limits and conditions, together with accident management and emergency preparedness, should be in place.

Kanada

Krav

RD–337, 7.16 Commissioning
All plant systems are designed such that, to the greatest extent practicable, tests of the equipment can be performed to confirm that design requirements have been achieved prior to the first criticality.

RD-346, Site Evaluation for New Nuclear Power Plants

USA

Krav

Of the NRC's existing regulations, the following are most relevant to the design, siting, construction, and operation of new commercial nuclear power facilities:

10 CFR Part 51, "Environmental Protection Regulations for Domestic Licensing and Related Regulatory Functions"

10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants"

IAEA

Krav

Site Evaluation for Nuclear Installations Safety Requirements, No. NS-R-3

Safety of Nuclear Power Plants: Commissioning and Operation Specific Safety Requirements, No. SSR-2/2

Guider

Commissioning for Nuclear Power Plants Safety Guide, Series No. NS-G-2.9, June 16, 2003.

External Human Induced Events in Site Evaluation for Nuclear Power Plants Safety Guide, Series No. NS-G-3.1, June 05, 2002.

Dispersion of Radioactive Material in Air and Water and Consideration of Population Distribution in Site Evaluation for Nuclear Power Plants Safety Guide, Series No. NS-G-3.2, April 02, 2002.

Geotechnical Aspects of Site Evaluation and Foundations for Nuclear Power Plants Safety Guide, Series No. NS-G-3.6, March 11, 2005.

Licensing Process for Nuclear Installations Specific Safety Guide, Series No. SSG-12, November 08, 2010.

Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations Specific Safety Guide, Series No. SSG-18, December 01, 2011.

Seismic Hazards in Site Evaluation for Nuclear Installations Specific Safety Guide, Series No. SSG-9, September 15, 2010.

Safety Aspects in Siting for Nuclear Installations, DS433 (DRAFT)

Construction of Nuclear Installations, DS441 (DRAFT)

Krav avseende drifterfarenheter

Sverige

Krav

-

Finland

Krav

24 § Drifterfarenheter och säkerhetsforskning
Drifterfarenheterna från kärnkraftverk ska samlas och resultaten av säkerhetsforskningen ska uppföljas och båda ska utvärderas i syfte att förbättra säkerheten. Sådana händelser under driften som är av betydelse med tanke på säkerheten ska undersökas för att deras grundläggande orsaker ska kunna klarläggas och korrigerande åtgärder ska kunna anges och vidtas. De tekniska förbättringar av säkerheten som uppdagas genom säkerhetsforskningen ska beaktas i den mån det är motiverat med tanke på de principer om vilka det föreskrivs i 7 a § i kärnenergilagen.

Storbritannien

Övergripande principer

MS.4 Learning from experience
Lessons should be learned from internal and external sources to continually improve leadership, organisational capability, safety decision making and safety performance.

Kanada

Krav

RD–337, 5.5 Operational Experience and Safety Research
The NPP design draws on operational experience that has been gained in the nuclear industry, and on the results of relevant research programs.

USA

-

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, 3.6
The formally designated entity shall ensure that the plant design meets the acceptance criteria for safety, reliability and quality in accordance with relevant national and international codes and standards, laws and regulations.

A series of tasks and functions shall be established and implemented to ensure the following:

(c) That the knowledge of the design that is needed for safe operation, maintenance (including adequate intervals for testing) and modification of the plant is available, that this knowledge is maintained up to date by the operating organization, and that due account is taken of past operating experience and validated research findings;

IAEA Safety Standard, No. SSR-2/1, 4.6
The design shall take due account of relevant available experience that has been gained in the design, construction and operation of other nuclear power plants, and of the results of relevant research programmes.

IAEA Safety Standard, No. SSR-2/1, 4.16
Where an unproven design or feature is introduced or where there is a departure from an established engineering practice, safety shall be demonstrated by means of appropriate supporting research programmes, performance tests with specific acceptance criteria or the examination of operating experience from other relevant applications. The new design or feature or new practice shall also be adequately tested to the extent practicable before being brought into service, and shall be monitored in service to verify that the behaviour of the plant is as expected.

IAEA Safety Standard, No. SSR-2/1, 4.19
In the provision for construction and operation, due account shall be taken of relevant experience that has been gained in the construction of other similar plants and their associated structures, systems and components. Where best practices from other relevant industries are adopted, such practices shall be shown to be appropriate to the specific nuclear application.

IAEA Safety Standard, No. SSR-2/1, 5.54
Operating personnel who have gained operating experience in similar plants shall, as far as is practicable, be actively involved in the design process conducted by the design organization, in order to ensure that consideration is given as early as possible in the process to the future operation and maintenance of equipment.

IAEA Safety Standard, No. NS-G-2.11, A System for the Feedback of Experience from Events in Nuclear Installations Safety Guide

Krav avseende säkerhetsforskning

Sverige

-

Finland

Krav

24 § Drifterfarenheter och säkerhetsforskning
Drifterfarenheterna från kärnkraftverk ska samlas och resultaten av säkerhetsforskningen ska uppföljas och båda ska utvärderas i syfte att förbättra säkerheten. Sådana händelser under driften som är av betydelse med tanke på säkerheten ska undersökas för att deras grundläggande orsaker ska kunna klarläggas och korrigerande åtgärder ska kunna anges och vidtas. De tekniska förbättringar av säkerheten som uppdagas genom säkerhetsforskningen ska beaktas i den mån det är motiverat med tanke på de principer om vilka det föreskrivs i 7 a § i kärnenergilagen.

Storbritannien

-

Kanada

Krav

RD–337, 5.5 Operational Experience and Safety Research
The NPP design draws on operational experience that has been gained in the nuclear industry, and on the results of relevant research programs.

USA

-

IAEA

Krav

IAEA Safety Standard, No. SSR-2/1, 3.6
The formally designated entity shall ensure that the plant design meets the acceptance criteria for safety, reliability and quality in accordance with relevant national and international codes and standards, laws and regulations. A series of tasks and functions shall be established and implemented to ensure the following:

(c) That the knowledge of the design that is needed for safe operation, maintenance (including adequate intervals for testing) and modification of the plant is available, that this knowledge is maintained up to date by the operating organization, and that due account is taken of past operating experience and validated research findings;

IAEA Safety Standard, No. SSR-2/1, 4.6
The design shall take due account of relevant available experience that has been gained in the design, construction and operation of other nuclear power plants, and of the results of relevant research programmes.

IAEA Safety Standard, No. SSR-2/1, 4.16
Where an unproven design or feature is introduced or where there is a departure from an established engineering practice, safety shall be demonstrated by means of appropriate supporting research programmes, performance tests with specific acceptance criteria or the examination of operating experience from other relevant applications. The new design or feature or new practice shall also be adequately tested to the extent practicable before being brought into service, and shall be monitored in service to verify that the behaviour of the plant is as expected.

Övrigt

Sverige

-

Finland

-

Storbritannien

Övergripande principer

Safety system functions
ESS.2 Determination of safety system requirements
The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and required reliabilities should be determined.

ESS.10 Definition of capability
The capability of a safety system, and of each of its constituent sub-systems and components, should be defined.

ESS.11 Demonstration of adequacy
The adequacy of the system design as the means of achieving the specified function and reliability should be demonstrated for each system.

ESS.12 Prevention of service infringement
Adequate provisions should be made to prevent the infringement of any service requirement of a safety system, its sub-systems and components.

ESS.13 Confirmation to operating personnel
There should be a direct means of confirming to operating personnel:

a) that a demand for safety system action has arisen;
b) that the safety actuation systems have operated fully; and
c) whether any limiting condition for which the safety system has been qualified has been exceeded.

ESS.16 No dependency on external sources of energy
Where practicable, following a safety system action, maintaining a safe facility state should not depend on an external source of energy.

ESS.17 Fault identification and assurance of safe state
Foreseeable faults within a safety system that could cause any single plant variable, or combination of variables, to change to significantly less safe values should be identified and, as necessary, avoidance measures or appropriate protective features provided.

ESS.18 Failure independence
No fault, internal or external hazard should disable a safety system.

ESS.19 Dedication to a single task
A safety system should be dedicated to the single task of performing its safety function.

ESS.20 Avoidance of connections to other systems
Connections between any part of a safety system (other than the safety system support features) and a system external to the plant should be avoided.

ESS.21 Reliability
The design of a safety system should avoid complexity, apply a fail-safe approach and incorporate the means of revealing internal faults from the time of their occurrence.

Vägledande råd

345 The capability should exceed by a clear margin the maximum service requirement(s) including the environmental envelope. The selected margin should make due allowance not only for uncertainties in plant characteristics, but also for the effects of foreseeable degradation mechanisms.

346 A ‘safety schedule’ (also known as a fault and protection schedule) should be provided that lists all postulated faults and hazards with unacceptable consequences. The schedule should include all initiating faults with their frequencies and consequences, the safety systems and beneficial safety-related systems involved for each initiating fault and the overall protection claim.

347 Infringement of any service would include removal or degradation of support services such as power supplies, instrument air, environment etc.

348 Where prevention, or acceptably low likelihood, of infringement cannot be demonstrated, features should be incorporated to ensure a fail-safe outcome.

350 For this principle an external source of energy means external to a safety system.

351 This principle is aimed at ensuring that the plant remains safe following the occurrence of foreseeable safety system faults. This includes, but is not limited to, the placement of the safety system in a fail-safe state, where practicable and achievable, following the detection of safety system faults.

352 Safety systems should be physically separate, independent, isolated from other systems, including safety-related systems, and share no equipment or services. There should be adequate segregation between independent parts of the safety system (including pipework and cabling) and also between a safety system and other facility equipment that, in the event of a fault, might jeopardise the safe working of the safety system.

353 Where it is necessary for other functions to be encompassed, the whole system should be classified as a safety system and the safety function should not be jeopardised by the other functions.

354 If connections external to the plant cannot be avoided, for electrical, electronic or computer-based safety systems they should be restricted in function to that of monitoring only, and should incorporate adequate isolation features so that no fault associated with that equipment or its connections would jeopardise the function of the safety system.

355 Where this principle cannot be achieved because of the use of complex hardware, the elements of a safety demonstration should be determined. The demonstration should include:

a) a comprehensive examination of all the relevant scientific and technical issues;
b) a review of precedents set under comparable circumstances in the past;
c) an independent third-party assessment in addition to the normal checks and conventional design;
d) periodic review of further developments in technical information, precedent and best practice.

356 The nature of some systems may be such that it is not possible to reveal all faults until the time of a test, eg in the case of fluid or mechanical systems. In such cases, in-service or periodic testing will be the sole means available to support reliability claims for the equipment, see Principle EMT.6 *(paragraph 189 f.)*.

Kanada

-

USA

Krav

§ 50.109 Backfitting.

(a)

(1) Backfitting is defined as the modification of or addition to systems, structures, components, or design of a facility; or the design approval or manufacturing license for a facility; or the procedures or organization required to design, construct or operate a facility; any of which may result from a new or amended provision in the Commission's regulations or the

imposition of a regulatory staff position interpreting the Commission's regulations that is either new or different from a previously applicable staff position after:

(i) The date of issuance of the construction permit for the facility for facilities having construction permits issued after October 21, 1985;

(ii) (ii) Six (6) months before the date of docketing of the operating license application for the facility for facilities having construction permits issued before October 21, 1985;

(iii) The date of issuance of the operating license for the facility for facilities having operating licenses;

(iv) The date of issuance of the design approval under subpart E of part 52 of this chapter;

(v) The date of issuance of a manufacturing license under subpart F of part 52 of this chapter;

(vi) The date of issuance of the first construction permit issued for a duplicate design under appendix N of this part; or

(vii) The date of issuance of a combined license under subpart C of part 52 of this chapter, provided that if the combined license references an early site permit, the provisions in § 52.39 of this chapter apply with respect to the site characteristics, design parameters, and terms and conditions specified in the early site permit. If the combined license references a standard design certification rule under subpart B of 10 CFR part 52, the provisions in § 52.63 of this chapter apply with respect to the design matters resolved in the standard design certification rule, provided however, that if any specific backfitting limitations are included in a referenced design certification rule, those limitations shall govern. If the combined license references a standard design approval under subpart E of 10 CFR part 52, the provisions in § 52.145 of this chapter apply with respect to the design matters resolved in the standard design approval. If the combined license uses a reactor manufactured under a manufacturing license under subpart F of 10 CFR part 52, the provisions of § 52.171 of this chapter apply with respect to matters resolved in the manufacturing license proceeding.

(2) Except as provided in paragraph (a)(4) of this section, the Commission shall require a systematic and documented analysis pursuant to paragraph (c) of this section for backfits which it seeks to impose.

(3) Except as provided in paragraph (a)(4) of this section, the Commission shall require the backfitting of a facility only when it determines, based on the analysis described in paragraph (c) of this section, that there is a substantial increase in the overall protection of the public health and safety or the common defense and security to be derived from the backfit and that the direct

and indirect costs of implementation for that facility are justified in view of this increased protection.

(4) The provisions of paragraphs (a)(2) and (a)(3) of this section are inapplicable and, therefore, backfit analysis is not required and the standards in paragraph (a)(3) of this section do not apply where the Commission or staff, as appropriate, finds and declares, with appropriated documented evaluation for its finding, either:

(i) That a modification is necessary to bring a facility into compliance with a license or the rules or orders of the Commission, or into conformance with written commitments by the licensee; or

(ii) That regulatory action is necessary to ensure that the facility provides adequate protection to the health and safety of the public and is in accord with the common defense and security; or

(iii) That the regulatory action involves defining or redefining what level of protection to the public health and safety or common defense and security should be regarded as adequate.

(5) The Commission shall always require the backfitting of a facility if it determines that such regulatory action is necessary to ensure that the facility provides adequate protection to the health and safety of the public and is in accord with the common defense and security.

(6) The documented evaluation required by paragraph (a)(4) of this section shall include a statement of the objectives of and reasons for the modification and the basis for invoking the exception. If immediately effective regulatory action is required, then the documented evaluation may follow rather than precede the regulatory action.

(7) If there are two or more ways to achieve compliance with a license or the rules or orders of the Commission, or with written licensee commitments, or there are two or more ways to reach a level of protection which is adequate, then ordinarily the applicant or licensee is free to choose the way which best suits its purposes. However, should it be necessary or appropriate for the Commission to prescribe a specific way to comply with its requirements or to achieve adequate protection, then cost may be a factor in selecting the way, provided that the objective of compliance or adequate protection is met.

(b) Paragraph (a)(3) of this section shall not apply to backfits imposed prior to October 21, 1985.

(c) In reaching the determination required by paragraph (a)(3) of this section, the Commission will consider how the backfit should be scheduled in light of other ongoing regulatory activities at the facility and, in addition, will consider information available concerning any of the following factors as may be appropriate and any other information relevant and material to the proposed backfit:

(1) Statement of the specific objectives that the proposed backfit is designed to achieve;
(2) General description of the activity that would be required by the licensee or applicant in order to complete the backfit;
(3) Potential change in the risk to the public from the accidental off-site release of radioactive material;
(4) Potential impact on radiological exposure of facility employees;
(5) Installation and continuing costs associated with the backfit, including the cost of facility downtime or the cost of construction delay;
(6) The potential safety impact of changes in plant or operational complexity, including the relationship to proposed and existing regulatory requirements;
(7) The estimated resource burden on the NRC associated with the proposed backfit and the availability of such resources;
(8) The potential impact of differences in facility type, design or age on the relevancy and practicality of the proposed backfit;
(9) Whether the proposed backfit is interim or final and, if interim, the justification for imposing the proposed backfit on an interim basis.

(d) No licensing action will be withheld during the pendency of backfit analyses required by the Commission's rules.
(e) The Executive Director for Operations shall be responsible for implementation of this section, and all analyses required by this section shall be approved by the Executive Director for Operations or his designee.

IAEA

Guide

Modifications to Nuclear Power Plants Safety Guide, Series No. NS-G-2.3, October 23, 2001.

Severe Accident Management Programmes for Nuclear Power Plants Safety Guide, Series No. NS-G-2.15, July 14, 2009.