

KONSTRUKTION AV SYSTEM I KÄRNKRAFTVERK

1	ALLMÄNT	3
2	KRAV GÄLLANDE KONSTRUKTION AV SYSTEM	3
2.1	Konstruktionsmetoder	3
2.2	Allmänna krav på konstruktion	3
2.3	Krav gällande planeringsorganisation	5
2.4	Krav på konstruktion av säkerhetssystem	5
2.5	Beaktande av fel vid konstruktion	6
2.5.1	Tillförlitlighetstekniska konstruktionsprinciper	6
2.5.2	Uppfyllnad av felkriterier	6
2.5.3	Separation av system som är viktiga för säkerheten	6
2.6	Sannolikhetsbaserad konstruktion	7
2.7	Övriga ärenden som skall tas i beaktande vid konstruktion	7
3	RAPPORTERING TILL STRÅLSÄKERHETSCENTRALEN	7
3.1	Konstruktionsskeden och dithörande handlingar	7
3.2	Preliminär säkerhetsanalysrapport	8
3.3	Slutlig säkerhetsanalysrapport	8
3.4	Systemändringar i kärnkraftverk som tagits i drift	10
3.4.1	Allmänna krav på handlingar	10
3.4.2	Principplan	10
3.4.3	Material för systemets förhandsgranskning	10
4	REFERENSER	10

Detta direktiv är i kraft från och med den 1.12.2002 tills vidare. Direktivet upphäver direktiv YVL 2.3 av den 14.8.1975.

Helsingfors 2003

ISBN 951-712-631-X (pdf)
ISBN 951-712-632-8 (html)

Befogenhetsgrunder

Strålsäkerhetscentralen ger detaljerade direktiv gällande säkerheten vid användning av kärnenergi, skydds- och beredskapsarrangemang samt tillsyn över kärnämnen med stöd av följande lagar och föreskrifter:

- kärnenergilagen (990/1987) 55 § 2 mom. 3 punkten
- statsrådets beslut om allmänna föreskrifter om säkerheten vid kärnkraftverk (395/1991) 29 §
- statsrådets beslut om allmänna föreskrifter om skyddsarrangemang vid kärnkraftverk (396/1991) 13 §
- statsrådets beslut om allmänna föreskrifter om beredskapsarrangemang vid kärnkraftverk (397/1991) 11 §
- statsrådets beslut om allmänna säkerhetsföreskrifter för en anläggning för slutförvar av driftavfall från kärnkraftverk (398/1991) 8 §
- statsrådets beslut om säkerheten vid slutförvaring av använt kärnbränsle (478/1999) 30 §.

Tillämpningsregler

Publiceringen av YVL-direktivet ändrar inte i sig de beslut som Strålsäkerhetscentralen tagit före publiceringen av direktivet. Först efter att ha hört alla berörda parter ger Strålsäkerhetscentralen ett separat beslut om hur det nya eller förnyade YVL-direktivet skall tillämpas på kärnkraftverk som är i drift eller under uppförande, samt på den verksamhet drifttillståndets ägare bedriver. På nya kärnkraftverk tillämpas reglerna direkt.

Då Strålsäkerhetscentralen överväger hur den skall tillämpa de nya kraven på säkerhet som presenterats i YVL-direktivet på kärnanläggningen som är i drift eller under uppförande tar den i beaktande följande princip i statsrådets beslut (395/1991) 27 §: *För att ytterligare förbättra säkerheten skall sådana åtgärder vidtas som kan anses vara motiverade med beaktande av drifterfarenheterna och säkerhetsforskningen samt utvecklingen inom vetenskap och teknik.*

Om man vill avvika från de krav som ställs i YVL-direktivet måste man åt Strålsäkerhetscentralen presentera ett annat godtagbart förfarings sätt eller lösning, med vilka säkerhetsnivån som presenterats i YVL-direktivet uppnås.

1 Allmänt

Avsikten med detta direktiv är att ge instruktioner för konstruktion och övervakning av kärnkraftverkets system, särskilt säkerhetsklassificerade system. I detta direktiv preciseras de allmänna kraven på konstruktion som givits i direktiv YVL 1.0. Preciseringar ges också i andra YVL-direktiv. Med system avses en funktionell eller strukturell helhet. System kan vidare indelas i strukturer och komponenter.

För säkerställandet av säkerheten vid kärnkraftverk är det centralt att driftstörningar och olyckor förebyggs (SRb 395/1991, 13 §, förebyggande). Detta innebär att anläggningens system, strukturer och komponenter planeras så att de störningar som orsakas av skador och felfunktioner i dem förblir så lindriga som möjligt och inte leder till olyckssituationer. Dessutom skall kärnkraftverket utrustas med system som snabbt upptäcker störnings- och olyckssituationer och hjälper att få dem under kontroll innan situationen förvärras (SRb 395/1991, 13 §, bemästrande av driftstörningar och olyckstillbud), och med system som hjälper att lindra och begränsa följderna av olyckssituationer (SRb 393/1991, 13 §, lindrande av följder).

Bemästrandet av driftstörningar och olycksituationer samt lindrandet av följderna grundar sig på upprätthållandet av säkerhetsfunktionerna. I direktiv YVL 1.0 definieras säkerhetssystem som ett system som utför en säkerhetsfunktion. Säkerhetsfunktionen är en med tanke på säkerheten viktig funktion, vars syfte är att förebygga uppkomsten eller framskridandet av störningar och olyckor eller lindra följderna av olyckan. Förutom säkerhetssystemen kan också andra system i kärnkraftverket ha betydelse för säkerheten. Likaså kan ett säkerhetssystem ha andra uppgifter utöver säkerhetsfunktionerna.

Det centrala vid inriktningen av Strålsäkerhetscentralens tillsynsåtgärder är vilken betydelse för säkerheten systemets funktion har. Säkerhetsklassificeringen av kärnkraftverkets system, strukturer och komponenter inverkar på deras övervakning. Säkerhetsklassificering av kärnkraftverk behandlas i direktiv YVL 2.1.

2 Krav gällande konstruktion av system

2.1 Konstruktionsmetoder

Vid konstruktion av system skall såväl deterministiska som sannolikhetsbaserade metoder användas.

Med deterministiska konstruktionsmetoder avses sådana metoder där man med grund i naturvetenskapliga teorier och empiriska uppgifter planerar en anordning eller ett system att fungera så, att den utför en fysikalisk funktion på önskat sätt och tekniskt ändamålsenligt. Man känner tillräckligt noggrant till avhängigheten mellan orsak och verkan för att kunna planera systemens och anordningarnas funktion samt med tillräcklig noggrannhet förutse hur de kommer att fungera, även i situationer som avviker från det normala.

Utgångspunkten för den deterministiska metoden är systemens planerade driftsituationer. Särskilt i säkerhetssystemens deterministiska konstruktion tar man, i enlighet med direktiv YVL 1.0, även i beaktande primära händelser som bedömts osannolika där ifrågavarande säkerhetsfunktion behövs. Säkerhetssystemets funktionella krav definieras på basis av följderna till dessa primära händelser och lindringsbehoven av dem. Sannolikheten av primära händelser och följdverkningarnas allvar tas i beaktande när de deterministiska kriterierna för godkännande definieras i enlighet med direktiv YVL 2.2.

Med sannolikhetsbaserade analyser (PSA) bedömer man olika säkerhetsfunktioners tillförlitlighet och balansen i konstruktionen dem emellan. Anläggningen skall planeras på ett sådant sätt att de beräkningsmässiga riskerna fördelas så att ingen enskild anordning, system, fenomen eller annan faktor dominerar risken och så att andelen svårkontrollerbara risker är så liten som möjligt. En anläggning som planerats på detta sätt är balanserad angående konstruktion.

2.2 Allmänna krav på konstruktion

De lösningar och metoder som man valt i konstruktion skall grunda sig på beprövad teknik

och tillförlitliga provresultat. Vid val av lösningar skall utvecklingen inom teknik utnyttjas (SRb 395/1991, 27 §). Brukbarheten av nya innovativa lösningar skall motiveras med omsorgsfulla, heltäckande undersökningar och prov innan de tas i bruk. Vid val av basteknologier skall man i planeringen ta i beaktande livscykeln för teknologi och anordningar samt förutse eventuella begränsningar som de för med sig. I planeringslösningarna bör man sträva efter att bli så oberoende av en enskild teknologi som möjligt och redan på förhand förbereda sig inför kommande byten av anordningar och möjligheten av teknologiska omvälvningar, för att behärskat och i god tid kunna planera de nödvändiga ändringarna i anläggningen.

Vid planeringen bör man sträva efter en så hög säkerhetsnivå som praktiskt möjligt (SAHARA-principen), se direktiv YVL 1.0, punkt 3.

Vid konstruktion av ett enskilt system skall särskild uppmärksamhet fästas vid ändamålsenligheten av systemets funktion och eventuella skadliga sidoeffekter, samt de krav som andra system ställer och den avhängighet och växelverkan som råder mellan systemen. Avhängighet och växelverkan som minskar systemens och anordningarnas tillförlitlighet skall undvikas.

Även om systemet aktiveras felaktigt eller vid behovet får det inte utsätta säkerhetsfunktionerna för fara eller orsaka nya primära händelser. De, med tanke på säkerheten ogynnsamma, sidoeffekter och följdverkningar som startandet eventuellt orsakar skall vara mycket små.

Kärnkraftverkets system skall planeras så att förlusten av en säkerhetsfunktion av vilken som helst inre eller yttre orsak skall vara mycket osannolik. Skador i ett delsystem får inte orsaka skador i andra delsystem i samma system och inte förlust av en funktion i det övriga systemet som deltar i samma säkerhetsfunktion.

Vid planeringen skall man ta i beaktande alla åldringsfenomen i normal drift, bland annat de som orsakats av miljöförhållanden. Säkerhetssystemet skall förbli funktionsdugligt i de miljöförhållanden dit det placerats som följd av en primär händelse.

När man definierar konstruktionsförutsättningarna skall man ta i beaktande primära händelser och deras följdverkningar, anläggningens inre händelser (som översvämning och elds-

våda) och yttre fenomen (som exceptionella väderleksförhållanden och jordbävningar) samt yttre händelser orsakade av människor (som flygkrasch och industriolycka). *Dessutom skall beaktas de enligt bedömning möjliga kombinationerna av inverkan av rådande omständigheter och naturfenomen i olycksituationer som har uppstått av inre orsaker i kraftverket* (SRb 395/1991, 20 §).

Vid planeringen skall man ta i beaktande slumpmässiga fel i anordningarna, risken av gemensamma fel och felfunktioner orsakade av människor, samt följdverkningarna av förväntade driftstörningar och olyckor. Systemets styråtgärder och de komponenter som behövs för dem skall planeras så att möjligheten till mänskliga fel är mycket liten när systemet är i användning.

Vid konstruktion av system skall man använda beprövade metoder som befunnits goda samt relevanta myndighetsföreskrifter, direktiv och standarder. Systemets säkerhetsklass skall definieras i enlighet med direktiv YVL 2.1. När systemet konstrueras skall man följa de kvalitetskrav som hör till säkerhetsklassen.

För säkerställande av systemets funktionsduglighet skall det konstrueras så att man kan utföra funktionstester på det så nära som möjligt de planerade driftsituationerna och parametrarna. De delar som är viktiga med tanke på systemets funktionsduglighet skall kunna granskas.

När man planerar systemets strukturer, material, placering och monteringar skall man ta i beaktande strålskyddets ALARA-princip och beredskapen inför underhåll och granskningar.

De delar i anläggningen som är viktiga med tanke på kärnsäkerheten skall placeras separat från de delar som enbart tjänar anläggningens normala drift. Dessutom skall de delsystem som är viktiga ur säkerhetssynvinkel placeras i egna utrymmen, fysiskt separata från varandra.

Systemets funktion och dess inverkan på hur anläggningen fungerar kan bero på anläggningens driftläge. Därför är det vid konstruktion av system nödvändigt att granska anläggningens alla normala driftsituationer, såsom effektdrift, uppkörning och avställning samt lägen vid driftstopp, och driftstörningar och olyckor som förekommer i dessa sammanhang.

2.3 Krav gällande planeringsorganisation

I 4 § SRb 395/1991 uppges att *kärnkraftverk skall planeras, uppföras och drivas inom ramen för en välutvecklad säkerhetskultur som grundar sig på att den högsta ledningen för respektive organisationer har en inställning som betonar säkerheten och att personalen är motiverad att utföra sitt arbete på ett ansvarsfullt sätt.* Från organisationen som ansvarar för konstruktionen förutsätter detta välordnade arbetsförhållanden och en öppen arbetsatmosfär samt främjande av vaksamhet och initiativförmåga för att upptäcka och eliminera faktorer som kan äventyra säkerheten.

I 5 § SRb 395/1991 förutsätts det att *högt utvecklade kvalitetssäkringsprogram skall tillämpas vid aktiviteter som gäller konstruktion, uppförande och drift av kärnkraftverk och som inverkar på säkerheten.* I direktiv YVL 1.4 ställs krav på konstruktions kvalitetskontroll och planeringsorganisationens kvalitetssystem.

Kärnkraftverkets planeringsorganisation skall ha tillräcklig erfarenhet av motsvarande uppgifter och den kunskap som behövs för att på ett övergripande sätt ta i beaktande anläggningens funktion, konstruktion och egenskaper.

Ansvarsfördelningen inom planeringsorganisationen skall vara klar. Särskilt då man planerar en omfattande helhet skall konstruktion under hela projektet framskrida så, att man genom olika planeringsgruppers utbyte av information och växelverkan i planeringen når bästa möjliga resultatet med tanke på säkerheten.

I konstruktionprocessen skall ingå synen som skall definieras i planeringsorganisationens kvalitetsplan.

Den tekniska ändamålsenligheten av den nya anläggningens konstruktion skall påvisas i säkerhetsanalysrapporten. I rapporten skall också ingå en utredning om hur planeringsorganisationen uppfyller de krav som ställts på den ovan. Tillståndssökanden skall, på basis av säkerhetsbedömningar som denne själv utför baserat på tillräckligt djup sakkunskap, vara övertygad om att konstruktion kan godkännas.

Vid kärnkraftverk som tagits i drift skall man med tanke på ändringar i omfattande systemhelheter eller system göra upp en principplan som innehåller det som presenterats i den preliminära säkerhetsanalysrapporten. Dessut-

om skall principplanen visa att en kompetent organisation har utfört planeringen och att det nödvändiga utbytet av information i planeringen har ägt rum. Tillståndshavaren skall med hjälp av granskningar bedöma om principplanen kan godtas, innan man börjar med den detaljerade systemkonstruktion. Man skall fortsätta med granskningarna under konstruktionprocessen. När det gäller planer som har en betydande inverkan på kärnsäkerheten, omfattande planer och planer som kräver specialkunnande skall tillståndshavaren överväga att låta en från den egna organisationen oberoende, utomstående bedömare utföra säkerhetsbedömningen. De personer och organisationer som utför konstruktionsgranskningar och oberoende säkerhetsbedömningar skall åtminstone ha den kompetens som planeringsuppgiften förutsätter och som i praktiken visat sig vara god. Efter att bedömningarna har utförts skall tillståndssökanden, på basis av säkerhetsbedömningar som denne själv utför baserat på tillräckligt djup sakkunskap, vara övertygad om att konstruktionen kan godkännas.

2.4 Krav på konstruktion av säkerhetssystem

Vid utförande av säkerhetsfunktioner skall man i första hand utnyttja system och anordningar som inte kräver någon yttre drivkraft för att utföra och styra sin funktion (SRb 395/1991, 18 §). Sådana system är t.ex. i nödkylningssystem använda tryckvattenbehållare som är trycksatta med komprimerad gas och reaktorinneslutningens yttre luftkylning som fungerar med naturlig cirkulation.

I andra hand kan man använda system där den egentliga funktionen eller dess styrning, eller båda två, kräver yttre drivkraft. Exempel på system vars egentliga funktion utnyttjar naturlagarna och vars styrning kräver yttre drivkraft är bortförsel av resteffekt från primärkretsen via naturlig cirkulation och reaktorns snabbstoppsystem som fungerar med tyngdkraft. Exempel på system där både den egentliga funktionen och dess styrning kräver yttre drivkraft är kylsystem som använder pumpar. När system som behöver yttre drivkraft för styrning och funktion förlorar sin drivkraft skall de ställa sig i ett ur säkerhetssynpunkt gynnsamt läge då detta går att definiera.

Målet med deterministisk konstruktion är att säkerställa att säkerhetsfunktionerna utförs i alla situationer som konstruktionen grundar sig på. Dessa situationer kan vara situationer anknutna till normal drift, förväntade driftstörningar, antagna olyckor eller allvarliga olyckor. Säkerhetssystemet kan ha en eller flera uppgifter gällande hindrandet av primära händelser eller begränsandet av deras framskridande och lindringen av följderna.

Systemets förmåga att utföra sina säkerhetsfunktioner skall påvisas med hjälp av resultat från konservativa analyser. Vid behov skall man med hjälp av tester påvisa systemets funktion och den tillräckliga exaktheten av analyser som behandlar den. Analyserna behandlas i direktiv YVL 2.2.

2.5 Beaktande av fel vid konstruktion

2.5.1 Tillförlitlighetstekniska konstruktionsprinciper

Det förutsätts att alla system, och särskilt säkerhetssystemen, fungerar tillförlitligt. Därför skall systemens funktion säkras i situationer där fel uppstår. Detta uppnås genom att tillämpa principerna av redundans, diversifiering och separation (SRb 395/1991, 18 §). Beaktande av fel vid konstruktion har behandlats i direktiv YVL 2.7. Beaktande av fel vid tryckkontroll av primär- och sekundärkrets i kärnkraftverk behandlas i direktiv YVL 2.4.

2.5.2 Uppfyllnad av felkriterier

Vid planering av system används termerna enkelfel och gemensamma fel. Med *enkelfel* avses fel som hindrar en enskild komponent från att utföra sina funktioner samt följdverkningarna av felet. Fel som uppkommer som följdverkningar av primära händelser räknas inte som enkelfel. Med *gemensamma fel* avses fel som uppstår i likadana komponenter eller konstruktioner som följd av samma enskilda händelse eller orsak.

I direktiv YVL 2.7 presenteras de säkerhetsfunktioner som skall utföras fastän det förekommer ett enkelfel i systemet som utför säkerhetsfunktionen, eller i dess delsystem. I enlighet med direktiv YVL 2.7 skall det tas i beaktande att man vid konstruktion av de system som utför de viktigaste säkerhetsfunktionerna utöver enskilda fel utgår ifrån att vilken komponent som

helst samtidigt kan vara funktionsoduglig på grund av underhåll eller reparation.

Redundansprincipen går ut på att man förbereder sig på fel genom att låta samma funktion utföras av fler än ett delsystem. Delsystemen kan vara sinsemellan lika eller olika. En säkerhetsfunktion kan behöva fler än ett delsystem. Vid beaktande av fel i delsystem följer man de krav som ställs i direktiv YVL 2.7.

Genom att öka antalet likadana parallella delsystem kan man förbättra systemets totala tillförlitlighet, som dock begränsas av eventuella gemensamma fel. Orsaken till det gemensamma felet kan vara ett fel i anordningens konstruktion, tillverkning, användning eller underhåll, någon yttre händelse eller annan orsak som inverkar på flera delsystem samtidigt.

För att förebygga inverkningarna av gemensamma fel, och på så sätt öka systemets tillförlitlighet, skall man vid säkerställandet av säkerhetsfunktionerna i mån av möjlighet använda system, delsystem och komponenter som grundar sig på olika funktionsprinciper (diversifieringsprincipen, SRb 395/1991, 18 §). Exempel på diversifieringar i funktionsprinciper är styrventiler som fungerar med elektricitet eller pneumatik och nödkylningssystem som fungerar passivt eller som är försedda med pumpar. Då diversifieringsprincipen tillämpas skall man sörja för att systemets ökade komplexitet inte omintetgör den ökning i tillförlitligheten som diversifieringsprincipen ger. I direktiv YVL 2.7 har man räknat upp de viktigaste säkerhetsfunktionerna, i säkerställandet av vilka olikhetsprincipen åtminstone skall användas. I samma direktiv beskrivs också hur enkelfel skall tas i beaktande när man tillämpar diversifieringsprincipen.

2.5.3 Separation av system som är viktiga för säkerheten

System som endast utför säkerhetsfunktioner skall avskiljas strukturellt från anläggningsdelar som tjänar den normala driften. System och delsystem som utför samma säkerhetsfunktion skall avskiljas från varandra oberoende av om de är lika eller olika. Genom att separera dem försäkras man sig om att sannolikheten för gemensamma fel som orsakas av yttre inverkan är mycket liten (separationsprincipen). Exempel

på sådana yttre inverkningar är bl.a. översvämningar, eldsvådor, missiler, flygkrascher och sällsynta naturfenomen.

Separata delsystem kan dock konstrueras så att de i avvikande situationer kan korskopplas genom driftåtgärder. Detta förutsätter att korskopplingen förbättrar och inte försämrar systemhelhetens tillförlitlighet och att obefogad korskoppling har förhindrats på ett tillförlitligt sätt.

I direktiv YVL 4.3 ges detaljerade konstruktionskrav för den utrymmesplanering och separation som görs med tanke på brand.

I direktiv YVL 5.2 och YVL 5.5 ges konstruktionskrav för separation av el- och automations-system.

2.6 Sannolikhetsbaserad konstruktion

Med tillförlitlighetstekniska metoder skall man påvisa att anläggningen till sin konstruktion är balanserad ur tillförlitlighetssynvinkel på det sätt som beskrivits i kapitel 2.1. Särskilt skall det påvisas att man i konstruktionen funnit rätt balans mellan

- olika säkerhetsfunktioner
- olika system som utför samma funktion
- huvudsystem och stödsystem
- olika delsystem i samma system.

De olika riskerna (mätt på basis av frekvens och allvar av härdskador och/eller miljöutsläpp) som beror på olika primära händelser skall fördela sig mellan de primära händelserna på ett sådant sätt, att inga händelsekedjor, system, delsystem, konstruktioner eller komponenter ensam orsakar en oproportionerligt stor andel av den totala risken.

I direktiv YVL 2.8 presenteras de sannolikhetsbaserade konstruktionsmålen och numeriska säkerhetsmålen.

Tillförlitlighetstekniska metoder kan också användas när man jämför olika konstruktionalternativ. Exempel på detta är optimering av antalet parallella delsystem och kapaciteten för varje enskilt delsystem med tanke på säkerheten och användbarheten, samt en sådan planering av delsystemens korskopplingsmöjligheter som förbättrar tillförlitligheten hos systemhelhetens funktion.

2.7 Övriga ärenden som skall tas i beaktande vid konstruktion

När ett system kopplar sig till ett annat system skall systemens gränssytor definieras och kopplingarna mellan system konstrueras så att förbindelsen mellan systemen inte äventyrar säkerheten hos systemet som utför säkerhetsfunktionen. Dessutom skall gränssytor för säkerhetssystemet och dess nödvändiga stödsystem i mån av möjlighet planeras så att skador i gränssytor inte äventyrar säkerheten för systemets egen, eller någon annan, säkerhetsfunktion och så att skadorna inte framskrider över gränssytan.

Säkerhetsfunktionens tillförlitlighet grundar sig på de system som utför den egentliga funktionen, men också på de nödvändiga stödsystemens tillförlitlighet. Tillförlitligheten hos huvudsystemen som deltar i säkerhetsfunktionen och stödsystemen som tjänar dem skall vara i balans sinsemellan. När man analyserar hjälp- och stödsystemens tillförlitlighetsnivå kan man ta i beaktande möjligheterna att reparera systemet i situationer där säkerhetsfunktionen behövs, förutsatt att man i konstruktionen förberett sig på reparationer (miljöförhållanden, t.ex. temperatur, fuktighet, strålning).

3 Rapportering till Strålsäkerhetscentralen

3.1 Konstruktionsskeden och dithörande handlingar

När ett nytt kärnkraftverk konstrueras skall följande information om systemen lämnas in:

- Systemens eller systemhelheternas konstruktionsförutsättningar, tekniska baslösningar och placering i anläggningen ges i den preliminära säkerhetsanalysrapporten. På basis av den preliminära säkerhetsanalysrapporten skall man kunna forma en helhetsbild av de tekniska grundprinciperna för varje system som inverkar på säkerheten och hur systemen är förbundna till anläggningshelheten. Dessutom skall man få en bild av lösningarna gällande systemens förverkligande. Uppgifter om alla säkerhetsfunktioner och anläggningens huvudproces-

ser ges i den omfattning som är nödvändig för att det skall gå att bedöma anläggningens funktion i störnings- och olyckssituationer.

- I den preliminära säkerhetsanalysrapporten skall det också påvisas att konstruktionen har organiserats i enlighet med punkt 2.3.
- I den slutliga säkerhetsanalysrapporten ges detaljerade tekniska lösningar för varje system. Lösningarna innehåller bl.a. systemens planerade funktionsvärden, nödvändiga mätningar och styrningar, analys av system o.s.v. På basis av innehållet i den slutliga säkerhetsanalysen, och dithörande ämnesrelaterade rapporter, skall man kunna bedöma om förverkligandet av systemhelheten och systemets funktion kan godkännas.
- I granskningsmaterialet för varje enskild komponent som hör till systemet ges detaljerade tekniska definitioner för utvalda komponenter. På basis av dem skall man kunna bedöma om komponenterna kan godkännas för sina planerade uppgifter.

3.2 Preliminär säkerhetsanalysrapport

Den preliminära säkerhetsanalysrapporten för system som hör till säkerhetsklasserna 1, 2 och 3, samt i nödvändig omfattning säkerhetsklass 4, skall innehålla följande utredningar:

- systemets konstruktionsprinciper och -förutsättningar
- systemets funktioner, funktionsprinciper och viktigaste planeringsvärden
- beskrivning av systemets betydelse vid utförande av egentlig säkerhetsfunktion, om systemet är stödsystem för systemet som utför säkerhetsfunktionen
- separationsprinciperna (placering i avdelningar, skydd) för systemet och dess komponenter och den preliminära utplaceringen i anläggningen i enlighet med punkt 3.3 i direktiv YVL 4.3.
- krav och beroenden som orsakas av övriga system, inklusive hjälp- och stödsystem
- tillförlitlighetsmål för den säkerhetsfunktion i utförandet av vilken systemet deltar
- utredning om de analyser och prov som utförts eller utförs för att visa att systemet fungerar
- preliminär säkerhetsanalys som utarbetats av planeraren

- tillståndshavarens egen säkerhetsbedömning som gjorts i enlighet med punkt 2.3.

System i klass EYT (icke klassificerad kärntekniskt) skall beskrivas i den omfattning som är nödvändig för att uppskatta anläggningens totala funktion.

I systemets konstruktionsförutsättningar skall man framföra vilka direktiv och standarder som används vid konstruktion av systemet. Likaså skall man framföra den preliminära säkerhetsklassificeringen för systemet och dess komponenter samt systemets miljöförhållanden och vilka krav de ställer på konstruktionen.

I direktiv YVL 5.5 ges instruktioner om analyser, prov, typtester och utarbetande av en plan för godkännande av automationssystem. I direktiv YVL 7.11 ges instruktioner om konstruktion och godkännande av anläggningens strålningsmätningssystem. I direktiv YVL 4.3 ställs krav på kärnkraftverkens brandskyddsarrangemang.

Ur den preliminära säkerhetsanalysrapporten skall det framgå hur systemet uppfyller de säkerhetskrav som ställs på det.

3.3 Slutlig säkerhetsanalysrapport

Den slutliga säkerhetsanalysrapporten för system som hör till säkerhetsklasserna 1, 2 och 3, samt i nödvändig omfattning säkerhetsklass 4, skall innehålla följande utredningar:

- systemets detaljerade konstruktionsförutsättningar
- systemets detaljerade funktionsbeskrivning
- utredning om placering, ur vilken framgår hur man i utplaceringen tagit i beaktande specialkraven för placering av systemets konstruktioner och komponenter (komponenternas fysiska separation, placeringskraven för tryckanordningar, zonindelning av strålningsövervakning och luftkonditionering, uppsamling och övervakning av läckage, beredskap att underhålla och kontrollera anordningar, tillgänglighet i drift- och olyckssituationer, ergonomi, ALARA-principen)
- inverkning på kärnkraftverkets andra system och beroende av hjälp- och stödsystem, samt förhindring av felspridning
- sannolikhetsbaserad granskning av systemets betydelse för anläggningens säkerhet med hjälp av viktighetsmått (se direktiv YVL 2.8)

- utredning om de analyser, prov och typtester med vilka systemets lämplighet för sitt tänkta syfte påvisas, och resultaten av dessa godkännanden
- konstruktörs säkerhetsbedömning om hur systemet uppfyller de säkerhetskrav som ställts på det
- tillståndshavarens egen säkerhetsbedömning som gjorts i enlighet med punkt 2.3
- krav på systemets säkerhetstekniska föreskrifter
- övriga nödvändiga utredningar.

Av konstruktionsförutsättningarna skall i regel följande ärenden framföras:

- systemets syfte, dithörande säkerhetsfunktioner samt de konstruktionsmål som ställs på systemet angående säkerheten
- krav som ställts på systemets konstruktionsförutsättningar i YVL-direktiv, standarder, normer o.s.v., bl.a. felkriterium, genomförande av diversifieringsprincipen och krav gällande fysisk separation
- systemets miljöförhållanden och vilka krav de ställer på konstruktionen
- utredning om hur olyckor utanför systemet och andra faktorer som inverkar störande på dess funktionsförmåga har tagits i beaktande vid konstruktionen (översvämningar, brand, jordbävningar, häftiga väderleksförhållanden, naturfenomenens inverkan, missiler, explosioner och övriga yttre hot)
- säkerhetsklassificering av systemet och dess komponenter
- systemets tillförlitlighetsmål och dess betydelse med tanke på säkerhetsfunktionens tillförlitlighet och hårdskadefrekvensen
- i systemets planerade driftsituationer förekommande, och som grund för systemets dimensionering använda, parametrar (t.ex. tryck, volymflöde, temperatur, kyleffekt, sammansättning och strålningsnivå av strömmande ämne) och på basis av dem ställda krav på funktionsvärden och konstruktionsmaterial hos systemets komponenter
- beräkningar och motiveringar som hör ihop med systemets funktionella konstruktion eller referenser till separata utredningar, ämnesrelaterade rapporter, analyser och andra handlingar där dessa ärenden framförs.

System i klass EYT (icke klassificerad kärntekniskt) skall beskrivas i den omfattning som är nödvändig för att uppskatta anläggningens totala funktion.

Systemets funktion i de situationer som granskats vid anläggningens konstruktion i enlighet med punkt 2.2 skall framgå ur systemets funktionsbeskrivning. Med funktionsbeskrivningen skall man påvisa ändamålsenligheten av systemets funktion och att de eventuella skadliga sidoeffekterna är ringa.

Följande utredningar skall i regel tillfogas funktionsbeskrivningen:

- systemets process- och instrumenteringsschema (PI-schema), ur vilken systemets gränser och förbindelser till andra system samt de processtekniska parametrar som är centrala för funktionen framgår
- utredning om styrning, reglering och instrumentering
- utredning om de principer på basis av vilka systemets drivenergi säkerställs
- förteckning över systemets komponenter och mätpunkter.

Systemets funktionsbeskrivning eller dithörande ämnesrelaterade rapporter skall vara så detaljerade att man på basis av informationen i dem kan analysera systemet.

Genom att analysera systemet visar man att de konstruktionsförutsättningar och -krav som gäller det har uppfyllts. Centrala analyser i säkerhetsanalysrapporten eller ämnesrelaterade rapporter är bl.a. analyser som behandlar systemets fysikaliska funktion, analys som behandlar enkelfel, feleffektanalys och viktighetsmått. Den inbördes viktighetsordningen mellan olika typer av analyser varierar från ett tekniskt område till ett annat.

Vid planering av automationssystem skall man följa de krav gällande kvalitetskontroll, analysering, prov och typtester som ges i direktiv YVL 5.5.

I säkerhetsbedömningen, som görs skilt för varje system, visar man att kraven som ställts i YVL-direktiven och andra konstruktionsförutsättningar har uppfyllts. Dessutom presenteras de tillförlitlighetstekniska bedömningar som gjorts i samband med konstruktion av systemet.

Separat material skall lämnas in angående

återkommande inspektioner och tester som utförs medan anläggningen är i drift och som berör systemet.

3.4 Systemändringar i kärnkraftverk som tagits i drift

3.4.1 Allmänna krav på handlingar

Förhandsgranskningen av system som ändras eller tillfogas medan kärnkraftverket är i drift skall göras på basis av material för förhandsgranskningen och en separat principplan angående ändringsarbetet. Den allmänna principen är att principplanerna och materialet för förhandsgranskningen av varje system som hör till klasserna 1,2 och 3, samt sådana system som STUK i mer detaljerade YVL-direktiv eller genom ett separat beslut kräver att granskas, skall skickas till STUK för godkännande. Materialet för förhandsgranskningen av system som hör till säkerhetsklass 4 skall skickas till STUK för kännedom.

Om systemändringen är så liten att den inte väsentligt ändrar systemets konstruktionsföresättningar, funktionsprincip eller uppgift behöver man inte skicka in en principplan om ändringen. Systemändringens betydelse för säkerheten inverkar på hur omfattande och detaljerat materialet för förhandsgranskningen skall vara.

I samband med ändringsarbetet skall man utan dröjsmål göra tillbörliga ändringar i den slutliga säkerhetsanalysrapporten. Krav gällande ändringar i handlingar ges i direktiv YVL 1.1. Ändringsarbeten behandlas också i direktiv YVL 1.8.

3.4.2 Principplan

Innehållet i systemets principplan skall i regel motsvara innehållet i den preliminära säkerhetsanalysrapporten. Dessutom skall följande utredningar ingå i principplanen:

- utredning om principerna för kvalitetskontroll, bl.a. om konstruktionsgranskningar och planeringsorganisationens kompetens

- utredning om utomstående oberoende säkerhetsgranskningar om sådana har utförts (de ersätter inte tillståndshavarens egen säkerhetsbedömning).

I samband med systemändringar skall man i principplanen också granska vilken inverkan ändringen har på hela anläggningens riskbedömning.

3.4.3 Material för systemets förhandsgranskning

Materialet för systemets förhandsgranskning skall i regel innehålla utredningar som motsvarar innehållet i den slutliga säkerhetsanalysrapporten. Dessutom skall materialet för systemets förhandsgranskning innehålla

- en kvalitetsplan där man beskriver de metoder som används inom kvalitetskontrollen för att konstruera och förverkliga system
- en utredning om utförda oberoende säkerhetsgranskningar och deras resultat, om sådana har behövts för att påvisa att systemet kan godkännas.

I enlighet med direktiv YVL 2.5 skall ett program om systemets provdrift skickas till STUK för godkännande.

4 Referenser

1. IAEA, SS No. 110, The Safety of Nuclear Installations, 1993.
2. IAEA, 50-C-D, Safety of Nuclear Power Plants: Design, 2000.
3. IAEA, 50-SG-Q10, Quality Assurance in Design, 1996.
4. INSAG-10, Defence in Depth in Nuclear Safety, 1996.
5. INSAG-12, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 rev.1, 1999.
6. IAEA, DS309, The Format and Content of Safety Analysis Reports for Nuclear Power Plants, DRAFT Safety Guide-Version 3.