SK99ST007
December 1996

MDT 621.311.25: 621.039: 681.362

SLOVENSKÁ TECHNICKÁ NORMA

STN IEC 1226 (40 2101)

STN	Jadrové elektrárne **Systémy kontroly a riadenia dôležité pre bezpečnosť** Klasifikácia	STN IEC 1226 40 2101

ICS: 27.120.10

Nuclear power plants - Instrumentation and control systems important for safety Classification

Centrales nucléaires - Systemes d'instrumentation et de contrôle-commande importants pour la sureté - Classification

Kernkraftwerken - Leittechnischen Einrichtungen des Sicherheitssystems Klassifikation

Táto norma obsahuje IEC 1226: 1993.

This standard includes IEC 1226: 1993

Národný predhovor

Citované normy

IEC 780 zavedená v STN IEC 780 Overenie spôsobilosti elektrických častí bezpečnostného systému jadrových elektrární (35 6609)

IEC 812 zavedená v STN IEC 812 Metódy analýzy spoľahlivosti systému. Postup analýzy spôsobu a dôsledku porúch (FMEA) (01 0675)

IEC 863 zavedená v STN IEC 863 Prezentácia predpovedí bezporuchovosti, udržovateľnosti a pohotovosti (01 0621)

IEC 880 zavedená v STN IEC 880 Programové prostriedky počítačov bezpečnostných systémov jadrových elektrární (35 6587)

IEC 964 dosiaľ nezavedená

IEC 980 zavedená v STN IEC 980 Odporúčané spôsoby overovania seizmickej spôsobilosti elektrického zariadenia bezpečnostného systému jadrových elektrární (35 6614)

IEC 987 dosiaľ nezavedená

Deskriptory podľa tezauru BSI ROOT

Kód deskriptora/ znenie deskriptora: KDN.G/ jadrové elektrárne, LIG.DN/ klasifikácia, AF/ kontrola, YS/ riadenie výroby, GPG/ nukleárna bezpečnosť

Vypracovanie normy

Spracovateľ: Výskumný ústav jadrových elektrární Trnava a.s., IČO 31450474, RNDr. Ján Štefánik

Pracovník Slovenského ústavu technickej normalizácie: Ing. Rudolf Nemčič

30 - 16

Jadrové elektrárne
Systémy kontroly a riadenia dôležité pre bezpečnosť
Klasifikácia

IEC 1226
Prvé vydanie
1993

Obsah

Strana

Predhovor

1 Medzinárodná elektrotechnická komisia (IEC) je celosvetovou organizáciou pre normalizáciu zahŕňajúcu všetky národné elektrotechnické komisie (národné komitéty IEC) Cieľom IEC je podporovať medzinárodnú spoluprácu vo všetkých otázkach týkajúcich sa normalizácie v oblasti elektrotechniky a elektroniky. Na tento cieľ okrem iných činností vydáva IEC medzinárodné normy.

Ich prípravou sú poverené technické komisie; každý národný komitét IEC činný v tejto oblasti sa môže zúčastniť na týchto prípravných prácach. Medzinárodné vládne a mimovládne organizácie spolupracujúce s IEC sa takisto zúčastňujú na tejto príprave IEC tesne spolupracuje s Medzinárodnou organizáciou pre normalizáciu (ISO) podľa podmienok stanovených zmluvou medzi týmito dvoma organizáciami.

2 Oficiálne rozhodnutia alebo dohody IEC týkajúce sa technických otázok spracovaných technickými komisiami, v ktorých sú zastúpené všetky zainteresované národné komitéty, vyjadrujú v najväčšej možnej miere medzinárodnú zhodu v názore na predmet, ktorého sa týkajú.

3 Majú formu medzinárodných odporúčaní a sú v tomto zmysle prijaté národnými komitétmi.

4 Na podporu medzinárodného zjednotenia IEC vyjadruje želanie, aby všetky národné komitéty prijali text odporúčaní IEC do svojich národných noriem v rozsahu, v ktorom im to ich národné podmienky dovoľujú. Akékoľvek rozdiely medzi odporúčaním IEC a zodpovedajúcou národnou normou by mali byť pokiaľ možno v národnej norme zreteľne vyznačené.

Túto normu pripravila subkomisia 45A: Reaktorová prístrojová technika technickej komisie IEC č. 45: Jadrová prístrojová technika.

Text tejto normy je vypracovaný na základe nasledujúcich dokumentov:

Šesťmesačné pravidlo	Správa o hlasovaní
45A (CO) 128	45A (CO) 133

Úplné informácie o schválení tejto normy sú v správe o hlasovaní v predchádzajúcej tabuľke.

Príloha A je informatívna.

Úvod

Táto medzinárodná norma vychádza z odporúčania Medzinárodnej atómovej agentúry vytvoriť kategorizáciu funkcií, systémov a zariadení (FSZ) systémov kontroly a riadenia jadrových elektrární podľa ich dôležitosti pre bezpečnosť. Cieľom tejto normy je klasifikovať funkcie, systémy a zariadenia, dôležité pre bezpečnosť do troch všeobecných kategórií a navrhnúť požiadavky, adekvátne dôležitosti pre bezpečnosť každej z týchto klasifikačných kategórií. Bezpečnostná kategória FSZ je daná ich príspevkom k zmierneniu následkov postulovaných iniciačných udalostí (PIU). Metóda kategorizácie by bola v ideálnom prípade založená na kvantitatívnom posúdení rizika, pretože prístup, ktorý využíva semikvantitívne alebo kvalitatívne kritériá, je z hľadiska interpretácie otvorený. Kvantitatívne posúdenie rizika sa využíva v jadrových elektrárňach vo svete stále viac; ak sú tieto výsledky k dispozícii, mali by sa použiť ako základ na kategorizáciu. Pretože výsledky pravdepodobnostných analýz často nie sú k dispozícii, súčasne vzniká potreba metódy kategorizácie, ktorá nie je závislá na týchto analýzach .

Táto norma poskytuje metódu kategorizácie založenú na kvalitatívnych kritériách, ktorá nevyžaduje použitie výsledkov hodnotenia rizika. Predpokladá sa že v budúcnosti bude opätovne vydaná a že bude zahŕňať kvalitatívne aj kvantitatívne kritériá. Tieto kvalitatívne kritériá sa musia používať veľmi starostlivo, aby sa zaistilo, že kategorizácie sa budú zhodovať s výsledkami kategorizácie založenej na posúdení rizika. Kvantitatívne kritériá by mohli mať prednosť, ak sú k dispozícii numerické výsledky posúdenia rizika. Jednou z možností ich zavedenia je použitie kvantitatívne vyjadrených mier dôležitosti, ktoré sú odvodené z výsledkov pravdepodobnostného hodnotenia rizika vykonaného ako súčasť návrhu alebo posúdenia procesu.

Miery dôležitosti sú spoločným vyjadrením výpočtov Fussella-Veselyho, výpočtov redukcie rizika a výpočtov dosiahnutia rizika a môžu sa použiť na relatívne porovnanie dôležitosti pre bezpečnosť rôznych systémov a podsystémov.

Použitie kategorizácie

Medzinárodná agentúra pre atómovú energiu (IAEA) odporučila, aby sa systémy kontroly a riadenia (SKR) jadrových elektrární (JE) zatriedili do kategórií podľa ich dôležitosti pre bezpečnosť. Zatriedenie funkcií, im prislúchajúcich systémov a častí zariadení (FSZ) sa môže vykonať

podľa stanovenej dôležitosti každej funkcie, systému, alebo časti zariadenia pri zaisťovaní bezpečnosti jadrovej elektrárne. Bezpečnosť jadrovej elektrárne zaisťuje prevencia alebo zmiernenie následkov havárií tak, aby sa neprekročili limity frekvencie alebo hodnoty uvoľňovaného rádioaktívneho materiálu do prostredia alebo dávky prevádzkovému personálu.

Správna klasifikácia FSZ upriamuje pozornosť projektantov elektrárne, operátorov a dozorných orgánov na špecifikácie, návrh, kvalifikáciu, zaistenie kvality, riadenie kvality (QA a QC), výrobu, inštaláciu, údržbu a testovanie FSZ zaisťujúcich bezpečnosť.

Táto norma zavádza kritériá a metódy používané pri zatrieďovaní FSZ SKR jadrovej elektrárne do troch kategórií A, B a C, ktoré sú závislé od dôležitosti pre bezpečnosť, a neklasifikovanej kategórie, ktorá nemá priamu bezpečnostnú úlohu. Načrtnuté sú v nej všeobecné požiadavky pre každú kategóriu a špecifikované zásadné technické požiadavky pre záležitosti zaistenia kvality (QA), spoľahlivosti, testovania a údržby.

Kategória, ku ktorej je FSZ pridelená, určuje všeobecné a špecifické technické požiadavky. Všeobecné požiadavky pre každé FSZ sú založené na poskytnutí primeranej úrovne zaistenia, že toto FSZ dosiahne požadovanú výkonnosť a spoľahlivosť, ak bude volané na výkon funkcie. Týka sa to aspektov funkčnosti, spoľahlivosti, výkonnosti, odolnosti voči prostrediu a zaistenia kvality (QA). Preukázaná úroveň zaistenia týchto aspektov musí byť v zhode s dôležitosťou FSZ pre bezpečnosť.

a) Funkčnosť zabezpečujú úplné a vyčerpávajúce špecifikácie požiadaviek a aplikácia noriem a kódov.

b) Spoľahlivosť zabezpečuje výber primeraných komponentov, štruktúr, úrovne redundancie a diverzity v spojení s fyzickou separáciou a/alebo pomocou bariér, elektrickou izoláciou a periodickým testovaním počas prevádzky.

c) Zaistenie výkonnosti sa dosahuje špecifikáciou požiadaviek na vlastnosti, aplikáciou procedúr riadenia kvality (QC), overovaním a vyhodnocovaním počas návrhu a výroby, predprevádzkovými testami individuálneho a integrovaného FSZ a testami počas prevádzky.

d) Odolnosť voči prostrediu zaisťuje kvalifikačný program, ktorý zabezpečuje, že efekty starnutia a podmienky prostredia v čase, keď sa vyžaduje prevádzka zariadenia, nedegradujú jeho výkonnosť pod požadovanú úroveň.

e) Funkčnosť, výkonnosť, odolnosť voči prostrediu a spoľahlivosť v každej etape prác od tvorby koncepcie cez návrh, výrobu, testy, inštaláciu, prebierku a uvedenie do prevádzky zabezpečuje kontrola podľa príslušných programov zaistenia kvality (QA) a riadenia kvality (QC) vykonávaná v každej etape prác.

POZNÁMKA - Príručka bezpečnosti 50-SG-D8 vydaná IAEA v časti 3.1.1 odporúča, aby boli FSZ SKR vzťahujúce sa na bezpečnosť zaradené do kategórií podľa ich dôležitosti pre bezpečnosť. Kategorizácia si vyžaduje zvažovanie faktorov citovaných v ďalej zavedených kategóriách buď priamo, alebo zavedením dôležitosti funkcií, ktoré systémy SKR vykonávajú:

1 pravdepodobnosť a miera nebezpečnosti dôsledkov postulovanej iniciačnej udalosti (PIU), ak SKR zlyhá;

2 časový úsek, ktorý je k dispozícii od vzniku PIU k požadovanému začiatku bezpečnostnej funkcie;

3 časový úsek, v ktorom sa vyžaduje práca SKR, ak sa už vyvolala bezpečnostná funkcia;

4 časový sled a spoľahlivosť, s ktorou sa môžu vykonať alternatívne akcie;

5 časový sled a spoľahlivosť, s ktorou sa môže odstrániť každá porucha v SKR;

6 potenciál samotného SKR stať sa príčinou PIU, opatrenia v bezpečnostných systémoch alebo systémoch so vzťahom k bezpečnosti pre tieto PIU, kombinácie dôsledkov a pravdepodobnosť takýchto PIU.

1 Predmet normy

Táto norma zavádza metódu klasifikácie informačných a riadiacich funkcií jadrových elektrární, SKR a zariadení, ktoré tieto funkcie prevádzajú do kategórií určujúcich dôležitosť týchto FSZ pre bezpečnosť. Výsledná klasifikácia potom určuje príslušné kritériá návrhu.

Kritériá návrhu sú prostriedkom zabezpečovania kvality, ktorým sa zaistí adekvátnosť každého FSZ v relácii jeho dôležitosti pre bezpečnosť. V tejto norme sú to kritériá funkčnosti, spoľahlivosti, výkonnosti, odolnosti voči prostrediu a zaistenie kvality (QA).

Táto norma sa používa pre všetky informačné a riadiace funkcie, SKR a zariadenia, ktoré tieto funkcie vykonávajú. Funkcie, systémy a zariadenia, o ktoré ide, predstavujú automatizované ochrany, otvorené alebo uzavreté riadiace slučky a informačné systémy pre prevádzkový personál. Udržiavajú parametre jadrovej elektrárne v bezpečných prevádzkových medziach, vykonávajú automatické zásahy alebo umožňujú ručné zásahy, ktoré zmierňujú havarijné stavy, zabraňujú úniku rádioaktivity do okolia elektrárne alebo aj ďalej za hranice elektrárne alebo ho minimalizujú. FSZ, ktoré tieto bezpečnostné funkcie plnia, chránia zdravie a bezpečnosť operátorov jadrovej elektrárne a obyvateľstva.

Táto norma dopĺňa, ale nenahrádza bezpečnostné pokyny a praktické kódexy publikované IAEA. Pridržiava sa všeobecných princípov uvedených v IAEA Safety Code 50-C-D (Vyd.1) a Safety Guides 50-SG-D3, 50-SG-D8 a 50-SG-D11, stanovuje štruktúrne metódy aplikácie týchto kódexov a noriem na FSZ SKR jadrových elektrární.

2 Súvisiace normy

Nasledujúce normatívne dokumenty obsahujú ustanovenia, ktoré prostredníctvom odkazu v tomto texte vytvárajú ustanovenia tejto normy. V čase publikácie boli uvedené vydania platné.

Všetky normatívne dokumenty sú predmetom revízie a ich používatelia pri dohodách vychádzajúcich z týchto noriem by mali zistiť možnosť použiť najnovšie vydanie uvedených dokumentov. Členovia IEC a ISO udržiavajú zoznamy platných medzinárodných noriem.

IEC 780: 1984 Overenie spôsobilosti elektrických častí bezpečnostného systému jadrových elektrární

IEC 812: 1985 Metódy analýzy spoľahlivosti systému. Postup analýzy spôsobu a dôsledku porúch (FMEA)

IEC 863: 1986 Prezentácia predpovedí bezporuchovosti, udržovateľnosti a pohotovosti

IEC 880: 1986 Programové prostriedky počítačov bezpečnostných systémov jadrových elektrární

IEC 964: 1989 Navrhovanie dozorní pre jadrové elektrárne

IEC 980: 1989 Odporúčané spôsoby overovania seizmickej spôsobilosti elektrického zariadenia bezpečnostného systému jadrových elektrární

IEC 987: 1989 Počítačové systémy dôležité pre bezpečnosť jadrových elektrární

IAEA Code 50-C-D (Rev.1): 1988 Projekt z hľadiska bezpečnosti jadrových elektrární

IAEA Code 50-C-QA (Rev.1): 1988 Zabezpečenie kvality pre bezpečnosť jadrových elektrární

IAEA Safety Guide 50-SG-D1: 1979 Bezpečnostná funkcia a klasifikácia komponentov BWR, PWR, PTR

IAEA Safety Guide 50-SG-D3: 1980 Ochranný systém a jeho charakteristiky v JE

IAEA Safety Guide 50-SG-D8: 1984 Inštrumentácia a riadenie JE

IAEA Safety Guide 50-SG-D11: 1986 Základné princípy bezpečnosti projektu JE

3 Definície

V tejto norme sa používajú nasledujúce definície uvedené v abecednom poriadku. Sú zhodné, alebo identické s definíciami použitými v iných súčasných smerniciach a normách IEC alebo pokynoch a kódexoch IAEA, ak sú označené *.

kodex/code: sústava požiadaviek, ktoré sú v súhlase s požiadavkami zákonov krajiny, v ktorej platia

praktické kodexy: množina odporúčaní, s ktorými sa nevyžaduje súhlas; odchýlky od nich by v zmysle zákona neboli nedbalosťou. Predstavujú dobrú alebo najlepšiu priemyselnú prax

diverzita: existencia dvoch alebo viacerých spôsobov, resp. prostriedkov na dosiahnutie stanoveného cieľa; používa sa ako ochrana proti spoločným príčinám porúch. Môže byť dosiahnutá vytvorením fyzikálne alebo funkčne odlišných systémov, ktoré dosahujú stanovený cieľ rôznym spôsobom

POZNÁMKA - Táto definícia je širšia ako táto definícia v IAEA 50-C-D, ktorá je:
existencia redundantných komponentov alebo systémov na realizáciu stanovenej funkcie, pričom takéto komponenty alebo systémy majú jeden alebo viac rôznych spoločných atribútov. Príkladmi takýchto atribútov sú rôzne prevádzkové podmienky, rôzna veľkosť zariadení, rôzni výrobcovia, rôzne výrobné princípy a typy zariadení, ktoré používajú rôzne fyzikálne metódy.

zariadenie *: jedna alebo viac častí systému; súčasťou zariadenia je jednotlivo definovateľný (a zvyčajne odstrániteľný) element alebo časť systému

funkcia: špecifický cieľ, ktorý má byť dosiahnutý; môže sa špecifikovať alebo popísať bez ohľadu na fyzikálne prostriedky, ktorými sa to dosiahne

funkčnosť: kvalitatívne označenie rozsahu a oboru funkcií, ktoré môže vykonať systém alebo časť zariadenia. Systém, ktorý môže vykonávať mnohé komplexné funkcie, má vysokú funkčnosť; systém, ktorý môže vykonávať len málo jednoduchých funkcií, má nízku funkčnosť

FSZ: funkcie, príslušné systémy a zariadenia; funkcie sa vykonávajú na dosiahnutie nejakého cieľa. Príslušné systémy a zariadenia sú súhrnom komponentov, ktoré slúžia na realizáciu týchto funkcií

pokyny: publikácia IAEA, ktorá odporúča praktické návody pre projektantov, konštruktérov, operátorov alebo inšpektorov jadrových elektrární a ktorá môže viesť k vytvoreniu IEC alebo inej národnej alebo medzinárodnej normy

KR FSZ dôležité pre bezpečnosť: SKR FSZ obsahujúce:

a) tie SKR FSZ, ktorých chybná funkcia alebo porucha by mohli viesť k neprípustnému ožiareniu personálu elektrárne alebo obyvateľstva;

b) tie SKR FSZ, ktoré zabraňujú, aby očakávané prevádzkové udalosti viedli k nejakým vážnym sekvenciám;

c) tie SKR FSZ, ktoré zmierňujú následky chybnej funkcie alebo poruchy štruktúry, systémov alebo komponentov

môže: v tejto norme sa slovom môže označuje, že súhlas s odporučením je voľbou

bezpečnosť JE: zabránenie neplánovaného a nekontrolovaného uvoľnenia rádioaktívneho materiálu, ktoré by mohlo ublížiť zdraviu prevádzkového personálu JE alebo obyvateľstva

jadrová bezpečnosť: schopnosť jadrovej elektrárne predchádzať jadrovým nehodám, t. j. neplánovaným alebo nekontrolovateľným kritickým parametrom s veľkosťou, ktorá spôsobuje poškodenia, alebo zamedziť ich

on-line: stav systému vykonávajúceho stanovené funkcie podľa požiadaviek návrhu JE

výkonnosť: efektívnosť výkonu istej funkcie (napr. časovej odozvy, presnosti, citlivosti na zmeny parametrov)

postulovaná iniciačná udalosť (PIU) *: udalosť vedúca k očakávaným prevádzkovým poruchám a havarijným podmienkam, ich pravdepodobným následným poruchám a pravdepodobným kombináciám[1] týchto porúch

redundancia *: zabezpečenie viac než minimálneho počtu elementov alebo systémov (rovnakých alebo rôznych) tak, že výpadok jedného nemá za následok stratu požadovanej funkcie ako celku

bezpečnostná funkcia *: špecifická funkcia, ktorá musí byť zavedená na zaistenie bezpečnosti

bezpečnostné systémy *: systémy dôležité pre bezpečnosť zaisťujúce za každých okolností bezpečné odstavenie reaktora, odvod tepla z aktívnej zóny a/alebo obmedzujúce následky PIU a závažných sekvencií

SKR FSZ so vzťahom k bezpečnosti: tie SKR FSZ dôležité pre bezpečnosť, ktoré nie sú systémami bezpečnosti

je..., požaduje sa, je nevyhnutné, je požadované, dovoľuje sa iba, je dovolené iba: požiadavka, ktorá sa musí splniť

odporúča sa, je odporúčané, malo by..., je obvyklé: požiadavka, ktorá sa síce nemusí splniť, ale jej splnenie sa dôrazne odporúča

závažná sekvencia: pravdepodobná séria alebo množina udalostí, ktorá by mohla mať neakceptovateľné dôsledky, napr.:

- neakceptovateľný únik rádioaktivity do priestorov elektrárne alebo do širokého okolia. Môže ísť o masívny nekontrolovaný únik s frekvenciou, ktorá je mimo projektových limitov JE, únik s frekvenciou, ktorá je v projektových medziach, ale s prekročenou veľkosťou úniku a/alebo s prekročenou frekvenciou únikov;

- neakceptovateľné poškodenie paliva. Môže to byť poškodenie obalu paliva, ktoré by viedlo k neakceptovateľnému zvýšeniu aktivity primárneho okruhu alebo poškodeniu štruktúry paliva znemožňujúcemu jeho chladenie

kritérium jednotlivej chyby *: zostava zariadenia vyhovuje kritériu jednotlivej poruchy, ak zariadenie môže plniť svoj účel aj napriek tomu, že jednotlivá náhodná porucha sa vyskytne kdekoľvek v zostave. Následné poruchy, ktoré sú dôsledkom jednotlivej náhodnej poruchy, sa považujú za súčasť tejto poruchy

norma: množina povinných požiadaviek; súlad s nimi síce nie je právnou požiadavkou, ale nesúlad s nimi bez platného zdôvodnenia by bol nedbalosťou

---

[1] Začiatočnou príčinou postulovaných iniciačných udalostí môžu byť poruchy zariadení, a/alebo chyby operátora (v elektrárni ako aj vonkajšie), prírodné udalosti a externé, človekom vyvolané udalosti. Špecifikáciu postulovaných iniciačných udalostí musí akceptovať nadriadený dozorný orgán jadrových elektrární. Ďalšie podrobnosti sú uvedené v IAEA Code 50-C-D a IAEA Safety Guide 50-SG-D8.

sub-FSZ: FSZ sa môže rozdeliť do niekoľkých sub-FSZ, ktoré sa môžu zvažovať samostatne, ale spoločne pôsobia na dosiahnutie celkového cieľa FSZ

subsystém *: časť nejakého systému s charakteristikami systému

systém *: množina navzájom poprepájaných prvkov vytvorená na dosiahnutie zadaného cieľa vykonaním stanovenej funkcie

typová skúška: určenie alebo preverenie schopnosti konkrétneho typu zariadenia splniť špecifikované požiadavky pri vystavení jeho reprezentatívnej časti alebo určitého počtu častí množine fyzikálnych, chemických vplyvov, prostredia a prevádzky.

4 Skratky

ALARA	v najmenšej dosiahnuteľnej veľkosti
FAT	test vo výrobnom závode
FMEA	analýza módov porúch a účinkov
FSZ	funkcia (funkcie) a nadväzné systémy a zariadenia, ktoré ju (ich) implementujú
IAEA	medzinárodná agentúra pre atómovú energiu
SKR	systém kontroly a riadenia
JE	jadrová elektráreň
PIU	postulovaná iniciačná udalosť
PRA	pravdepodobnostné hodnotenie rizika
QA	zaistenie kvality
QC	riadenie kvality
SAT	akceptačný test na mieste

5 Požiadavky

FSZ SKR jadrovej elektrárne musia byť zadelené do kategórií podľa dôležitosti pre bezpečnosť. Kritériá zodpovedajúce týmto kategóriám sa musia použiť pri návrhu, výrobe, montáži, preberacích skúškach a údržbe počas prevádzky.

5.1 Pozadie

Princíp ochrany do hĺbky je pevne zavedenou bezpečnostnou návrhovou zásadou jadrových elektrární. Základná idea spočíva v tom, že by malo byť niekoľko vrstiev alebo úrovní ochrany zamedzujúcich vznik nebezpečných podmienok; prvoradé je predchádzať nebezpečným podmienkam, nie žiadať zmierňovanie následkov; prevenciu treba vždy preferovať. Pretože pre bezpečnosť JE sa vyžaduje prevádzka veľkého počtu zariadení a princípom ochrany do hĺbky sa tento počet zvyšuje, je dôležité, aby bola známa závažnosť každého FSZ pre bezpečnosť.

Klasifikácia systémov JE podľa dôležitosti pre bezpečnosť uvádza IAEA Safety Guide 50-SG-D1; uvádza aj príklady klasifikácie hlavných systémov niekoľkých typov JE.

Bezpečnostné návody Safety Guides 50-SG-D3 a 50-SG-D8 uvádzajú rozdiely medzi bezpečnostnými systémami. Sú to systémy, ktoré zaisťujú bezpečné odstavenie reaktora a odvod tepla z aktívnej zóny, obmedzujú dôsledky očakávaných prevádzkových porúch alebo havarijných podmienok, a systémy SKR so vzťahom k bezpečnosti, ktoré sú dôležité pre bezpečnosť, ale nie sú súčasťou bezpečnostných systémov. Z hľadiska dôležitosti pre bezpečnosť a príslušných požiadaviek sa budú časti bezpečnostných systémov a systémov so vzťahom k bezpečnosti líšiť, preto je primerané zadeliť ich do rôznych bezpečnostných kategórií. Niektoré SKR môžu mať závažný vplyv na bezpečnosť, a preto si vyžadujú patričnú pozornosť. Iné systémy

majú strednú, malú alebo žiadnu závažnosť pre bezpečnosť. Budú mať preto nižšie nároky na zaistenie výkonnosti a bezpečnostné zdôvodnenie, teda aj rozdielne technické požiadavky.

Táto norma rozširuje stratégiu klasifikácie prezentovanú v IAEA Safety Guide 50-SG-D1, uvádza kritériá a metódy, ktoré treba použiť pri zatrieďovaní FSZ SKR jadrovej elektrárne do jednej z troch kategórií A, B a C v závislosti od dôležitosti zariadenia pre bezpečnosť alebo do neklasifikovanej kategórie pre FSZ, ktoré nemajú bezpečnostnú úlohu.

5.2 Popis kategórií

5.2.1 Kategória A

Kategória A zahŕňa FSZ s významnou úlohou pri zaisťovaní a udržiavaní bezpečnosti jadrovej elektrárne. Tieto FSZ zabraňujú, aby PIU viedli k bezpečnostne závažným sekvenciám udalosti, alebo zmierňujú ich následky. Kategória A FSZ sa môže uviesť do činnosti automaticky alebo ručnými zásahmi, ak sú takéto zásahy v možnostiach operátora. Do kategórie A patria aj FSZ, ktorých poruchy by mohli priamo zapríčiniť závažnú sekvenciu udalostí. Kategória A má vysoké požiadavky na pohotovosť. Môže byť obmedzená vo funkčnosti, aby jej pohotovosť bola dôveryhodne garantovaná.

5.2.2 Kategória B

Kategória B obsahuje FSZ dopĺňajúce kategóriu A FSZ pri dosahovaní a údržbe bezpečnosti jadrovej elektrárne. Prevádzka FSZ kategórie B môže zamedziť potrebe iniciovať FSZ kategórie A. FSZ kategórie B môže zlepšiť alebo doplniť výkon FSZ kategórie A pri zmiernení dôsledkov PIU, aby poškodenie elektrárne alebo zariadenia, resp. úniky aktivity neboli žiadne alebo minimálne. Kategória B zahŕňa FSZ, ktorých porucha by mohla iniciovať alebo zvýšiť drsnosť PIU. Z dôvodu prítomnosti FSZ kategórie A na konečnú prevenciu alebo zmiernenie následkov PIU nie sú bezpečnostné požiadavky na FSZ kategórie B také vysoké ako pri kategórii A. V prípade potreby to umožňuje vyššiu funkčnosť FSZ kategórie B ako FSZ kategórie A, ak ide o metódy detekcie a aktivácie alebo ich následné činnosti.

5.2.3 Kategória C

Kategória C obsahuje FSZ s pomocnou alebo nepriamou úlohou pri dosahovaní a údržbe bezpečnosti jadrovej elektrárne. Kategória C zahŕňa FSZ s určitou dôležitosťou pre bezpečnosť, ale nie kategórie A alebo B. FSZ kategórie C môžu byť súčasťou celkovej reakcie na haváriu, ale nie sú priamo zapojené do zmierňovania jej fyzikálnych následkov.

5.3 Zásady klasifikácie

FSZ SKR sa musia posudzovať podľa dôsledkov ich zlyhaní, ako je porucha činnosti alebo chybná činnosť. Pri tomto posudzovaní sa musí zvažovať aj údržba a testovanie. PIU musia byť zvažované pri projektovom návrhu JE. Úvahy musia zahŕňať analýzy závažných sekvencií udalostí, aby sa určili funkcie, ktoré bude treba realizovať pomocou FSZ SKR.

Úvahy o funkciách, ktoré majú FSZ SKR realizovať, musia vyústiť do zadelenia každej FSZ do jednej z troch kategórií A, B alebo C alebo medzi neklasifikované FSZ. FSZ sa začleňuje medzi neklasifikované, ak nie je dôležitá pre bezpečnosť.

Prítomnosť nižších kategórií FSZ (B, C, resp. neklasifikovaných) nesmie viesť k odstráneniu alebo vynechaniu vyššej kategórie (A, B alebo C).

Národné aplikácie princípov a kritérií tejto normy môžu prideľovať kategóriám A, B, C rôzne nomenklatúry. Tieto národné aplikácie musia byť v súlade s princípmi, kritériami a nadväznými požiadavkami tejto normy. Musia zahŕňať aj ustanovenia a príslušnú sprievodnú dokumentáciu k definovaným kategóriám.

FSZ SKR, ktoré spadajú podľa IAEA Safety Guide 50-SG-D8 medzi bezpečnostné systémy, budú všeobecne pridelené do kategórie A. FSZ SKR označené v uvedenom návode IAEA ako systémy so vzťahom k bezpečnosti budú zadelené do kategórie A, B alebo C.

6 Kritériá priradenia

Ďalej sa uvádzajú kritériá, ktoré sa musia použiť pri zadeľovaní FSZ do kategórií A, B a C.

Ak FSZ nespĺňa žiadne z týchto kritérií, musí byť zadelená medzi neklasifikované.

V prípadoch viacnásobného priradenia musí konečné priradenie každej FSZ a sub-FSZ nutných na dosiahnutie cieľov FSZ zodpovedať najvyššej použiteľnej kategórii.

6.1 Kategória A

FSZ SKR musia byť zaradené do kategórie A, ak spĺňajú niektoré z nasledujúcich kritérií:

a) vyžadujú sa na zmiernenie dôsledkov PIU, na zabránenie, aby PIU viedlo k závažnej sekvencii udalostí;

b) v prípade poruchy FSZ, ak sa žiada na činnosť ako odozva na PIU, môže dôjsť k závažnej sekvencii udalostí;

c) chybu alebo poruchu v FSZ by nemohla zmierniť iná FSZ kategórie A a viedla by priamo k závažnej sekvencii udalostí;

d) vyžaduje sa poskytnutie informácie alebo schopnosti ovládania, ktoré umožnia stanovené ručné zásahy nutné na zmiernenie dôsledkov PIU na zabránenie závažnej sekvencie udalostí.

Pri kategorizácii FSZ vo vzťahu k bodu d) sa musia vziať do úvahy faktory, ako je disponibilita redundantných zdrojov informácií, dostatok času na operátorské posúdenie alternatívnych zdrojov informácií a to či sú ručné zásahy jediným prostriedkom na zmiernenie sekvencie závažných udalostí.

Ak sa ručný zásah vyžaduje na zaistenie bezpečnosti JE, príslušné FSZ-SKR, ktoré tento zásah umožňuje, je nutné zaradiť do kategórie A.

6.2 Kategória B

FSZ SKR musí byť zaradená do kategórie B, ak spĺňa niektoré z nasledujúcich kritérií a nie je inak zaradená do kategórie A:

a) riadi parametre procesu elektrárne tak, aby boli v rozmedzí limitov predpokladaných bezpečnostnou analýzou;

b) poruchy FSZ (kategórie B) by mali za následok požiadavku na činnosť FSZ kategórie A na zamedzenie závažnej sekvencii udalostí;

c) slúži na prevenciu alebo zmiernenie malých únikov rádioaktivity alebo malých poškodení paliva v rozsahu danom projektom JE, ale menšej dôležitosti, ako sú závažné sekvencie udalostí[1)];

d) slúži na výstrahu personálu blokovej dozorne, že porucha je v FSZ kategórie A;

[1)] Definícia malých rádioaktívnych únikov alebo malého poškodenia paliva musí byť v súlade s národnou praxou. Malým únikom rádioaktivity môže byť dôsledok úniku primárneho chladiva pri nepoškodenom palive. Malé poškodenie paliva môže predstavovať poškodenie obalu paliva v malom množstve v podmienkach bez úniku chladiva alebo bez straty schopnosti dostatočného chladenia aktívnej zóny.

e) slúži na kontinuálne monitorovanie pohotovosti FSZ kategórie A plniť ich bezpečnostnú úlohu;

f) slúži na značné zníženie frekvencie PIU v súlade s nárokmi bezpečnostnej analýzy.

6.3 Kategória C

FSZ SKR musí byť zaradená do kategórie C, ak spĺňa niektoré z nasledujúcich kritérií a nie je inak zaradená do kategórie A alebo B:

a) slúži na zníženie očakávanej frekvencie PIU;

b) slúži na zníženie požiadaviek na činnosť alebo zvýšenie výkonnosti FSZ kategórie A;

c) slúži na dozorovanie alebo registráciu podmienok FSZ určujúcich ich bezpečnostný status (pripravený na prevádzku, v prevádzke, vypadnutý, neschopný prevádzky), najmä tých, ktorých porucha by mohla spôsobiť PIU;

d) slúži na monitorovanie interných nebezpečí a vykonanie následných činností v rozsahu danom projektom JE (napr. požiar, zatopenie);

e) slúži na zaistenie bezpečnosti personálu počas, alebo po udalostiach, ktoré spôsobia, alebo majú za následok uvoľnenie rádioaktivity do priestorov elektrárne alebo riziko radiačného ožiarenia;

f) slúži na varovanie personálu o závažnom uvoľnení rádioaktivity do priestorov jadrovej elektrárne alebo o nebezpečenstve radiačného ožiarenia;

g) slúži na monitorovanie a uskutočnenie zmierňovacích činností pri závažných prírodných udalostiach, ako je zemetrasenie a tornádo;

h) slúži na vnútornú kontrolu vstupov na jadrovej elektrárni.

7 Postup klasifikácie

Náčrt postupu je uvedený na obrázku 1.

7.1 Stanovenie navrhovaných zásad

Hlavným vstupom procesu kategorizácie FSZ je povaha JE a typ reaktora (napr. PWR, BWR, alebo iný typ), príslušné postulované iniciačné udalosti (PIU), hlavné kritériá návrhu redundancie mechanických a elektrických systémov a zariadení. Ďalším hlavným vstupom je určenie hlavných zmierňovacích FSZ a ich podporných FSZ pre každú PIU.

Zaradenie FSZ do kategórií je závislé od ich úlohy pri prevencii a zmierňovaní dôsledkov PIU. Proces kategorizácie si vyžaduje zvažovanie úlohy FSZ pri prevencii a zmierňovaní dôsledkov PIU vo všetkých prevádzkových stavoch a podmienkach elektrárne (napr. spúšťanie, normálna prevádzka, výmena paliva), pretože niektoré FSZ môžu mať významnú úlohu iba v niektorých prevádzkových režimoch a po PIU, ako sú prírodné udalosti (katastrofy, zemetrasenie, zatopenie, tornádo, blesk), vnútorné príčiny havarijných situácií (napr. požiar, vnútorné zatopenie, letiace predmety), únik rádioaktivity zo susednej JE, únik chemických látok z iných staníc alebo priemyselných podnikov.

7.2 Identifikácia a kategorizácia FSZ

Už v začiatočnom štádiu návrhu JE musia byť stanovené funkcie s bezpečnostnou úlohou. Proces stanovenia týchto funkcií a ich priradenia k FSZ SKR alebo operátorom by mal prebie-

hať podľa IEC 964. Po tomto začiatočnom stanovení FSZ sa im musí pridelíť kategória podľa kritérií v 6.

V začiatočnom štádiu procesu návrhu nebude možné detailne stanoviť všetky FSZ, pretože charakteristiky JE ešte nebudú plne definované. Proces stanovenia a kategorizácie FSZ musí preto pokračovať počas celej fázy návrhu. V prípadoch, kde je zaradenie FSZ do kategórie neisté, by sa mala pridať vysvetľujúca poznámka.

Musia sa preskúmať funkcie každého SKR s cieľom stanoviť sub-FSZ v každom FSZ a priradiť každé sub-FSZ do príslušnej kategórie.

Pretože jednotlivé FSZ môžu zahŕňať z hľadiska realizácie niekoľko aspektov a špecifikácií požiadaviek, môže proces priraďovania viesť v niektorých FSZ k zaradeniu do niekoľkých kategórií. V prípade viacnásobného priradenia musí byť konečné zaradenia každého FSZ a sub-FSZ nutných na dosiahnutie cieľov FSZ do najvyššej použiteľnej kategórie.

Ak sú redundancie, diverzity a ďalšie technické požiadavky na FSZ stanovené presnejšie, napríklad bezpečnostné analýzy a prevádzkové predpisy, musí byť kategorizácia zjemnená a revidovaná na odvodenie konečného zoznamu. Tento zoznam sa musí zahrnúť do dokumentácie vyžadovanej na získanie a udržanie licencie na prevádzku JE.

8 Stanovenie požiadaviek

Kritériá návrhu sú požiadavky, ktorých prostredníctvom sa zaisťuje adekvátnosť FSZ z hľadiska ich dôležitosti na bezpečnosť elektrárne. Tieto kritériá sa týkajú zaistenia funkčnosti, výkonnosti, spoľahlivosti, odolnosti voči podmienkam prostredia, zaistenia kvality (QA) a riadenia kvality (QC).

Na zaistenie, aby FSZ pracovali v súlade s funkčnými špecifikáciami, je potrebný súlad s príslušnými normami a kodexami počas návrhu kvalifikácie zariadení. Aby prežilo očakávané prevádzkové udalosti, je potrebné zaistiť kvalitu (QA) a riadenie kvality (QC) počas projektu výroby, inštalácie a prevádzky. Kodexy, pokyny a normy uvedené v bode 2 tejto normy sú normatívnymi odkazmi, a preto sú aj ustanoveniami tejto normy.

Ak je to možné, malo by sa použiť FSZ s dobre dokumentovanou overenou históriou spoľahlivej prevádzky v jadrovom alebo inom priemysle.

8.1 Požiadavky na zaistenie funkčnosti

8.1.1 Základné požiadavky

Základnou požiadavkou na zaistenie funkčnosti je existencia jasných, vyčerpávajúcich a jednoznačných funkčných požiadaviek a projektových špecifikácií, s ktorými musí byť FSZ overované počas výroby, inštalácie a prevádzky, a ktoré musia slúžiť ako referenčné pre zmeny a modifikácie počas prevádzky.

8.1.2 Špecifické požiadavky

a) Kategória A

Návrh musí byť v súlade s požiadavkami uznávaných kodexov, pokynov a noriem primeraných na vysokú úroveň zaistenia funkčnosti požadovanej od FSZ kategórie A.

Návrh sa musí ľahko overiť, musí sa dodržať jednoduchosť. Musí to vylúčiť funkciu nižšej kategórie z FSZ. (Napríklad softvér bezpečnostného systému by nemal vykonávať špeciálne zo-

brazovacie výpočty a preklady komunikačných protokolov.) Ak sú použité počítače, nutné je splniť požiadavky noriem IEC 880 a IEC 987.

b) Kategória B

Proces návrhu musí prebiehať podľa uznávaných kodexov, pokynov a noriem (ako je proces návrhu uvedený v IEC 964 pre blokovú dozorňu), alebo sa môžu použiť systémy a zariadenia s dokumentovanou históriou uspokojivej prevádzky v podobných aplikáciách.

c) Kategória C

Návrh by mal preveriť, že zariadenia a systémy boli navrhnuté alebo testované na poskytovanie stanovených funkcií v plnom rozsahu prevádzkových podmienok vrátane najhorších očakávaných prevádzkových podmienok alebo udalostí, pri ktorých sa funkcia vyžaduje.

8.2 Požiadavky na zaistenie spoľahlivosti

8.2.1 Základné požiadavky

Spoľahlivosť vyžadovaná od FSZ v kategóriách A, B alebo C musí byť stanovená buď pomocou kvantitatívneho pravdepodobnostného ohodnotenia JE, kvalitatívneho pravdepodobnostného ohodnotenia JE, alebo kvalitatívnym inžinierskym posúdením a začlenená do špecifikácií. Táto analýza musí byť zhotovená štruktúrovaným spôsobom overenými postupmi a musí byť zdokumentovaná.

Hoci požiadavky na spoľahlivosť FSZ rôznych kategórií môžu byť rovnaké, úroveň zaistenia, že dosiahnu špecifikovanú spoľahlivosť, bude rôzna pre rôzne kategórie. Kategória A si vyžaduje najväčšie zaistenie. Základné požiadavky na zaistenie vysokej spoľahlivosti sú spojené s primeranou redundanciou, diverzitou, priestorovým, geografickým, fyzikálnym a elektrickým oddelením a/alebo rozdelením.

Pri návrhu a následných modifikáciách treba uvažovať pre všetky FSZ prostriedky na detekciu chýb a opravy.

Hodnotenia spoľahlivosti a disponibility musia vziať do úvahy čas opráv, testov a údržby a potenciál pre poruchy, ktoré sa odhalia samy, ako aj poruchy, ktoré sa samy neodhalia. Predpoklady založené na spoľahlivostných analýzach s rešpektovaním údržby, testovania a opráv musia byť overené počas prevádzky. Ak sú nejasnosti, treba urobiť korekcie.

8.2.2. Špecifické požiadavky

a) Kategória A

FSZ kategórie A musia mať takú redundanciu, že splnenie kritéria jednotlivej poruchy je považované za minimum.

Musí sa použiť oddelenie a/alebo rozdelenie, aby sa zaistilo, že jednotlivé vnútorné havárie nebudú môcť zneschopniť redundantné vetvy FSZ. Použitie kritéria jednotlivej poruchy musí byť podľa IAEA Code 50-C-D (Rev.1) paragraf 329 až 336.

Požiadavky na spoľahlivosť FSZ SKR kategórie A musia byť stanovené, ako je uvedené v 8.2.1. Musia byť stanovené požiadavky spoľahlivosti pre funkcie nutné na dosiahnutie akceptovateľne nízkeho rizika závažných sekvencií udalostí; z nich sa potom určia požiadavky na spoľahlivosť FSZ SKR. Spoľahlivosti FSZ SKR nutné na dosiahnutie požadovanej funkcie sa musia potom posúdiť a porovnať so špecifikáciami. Prípadné nezrovnalosti sa musia vyriešiť.

Posúdenie spoľahlivosti sa musí týkať aj efektov spoločnej príčiny porúch vrátane porúch hardvéru, softvéru a ľudských chýb počas prevádzky, údržby, zmien a opráv. Techniky používané

na posúdenie týchto efektov siahajú od kvalitatívnych technických posudkov až po detailné kvantitatívne analýzy, ktoré môžu byť závislé na kvalitatívnych odhadoch. Vybratý druh analýzy musí byť konzistentný s požiadavkami na spoľahlivosť a dôslednejšími technikami.

Ak sa pri zvažovaní účinkov spoločnej príčiny porúch, ako sú poruchy softvéru, ľudské chyby, preukáže dosiahnutie limitov spoľahlivosti redundantných FSZ, možno bude potrebná diverzita pre FSZ.

Príslušné funkcie si môžu vyžadovať dve alebo viac-FSZ, ktoré sú navzájom diverzitné.[1)]

Analýza módov porúch a účinkov pre FSZ kategórie A musí byť podľa IEC 812. Detailnosť analýzy musí byť na úrovni zhodnej s úrovňou integrácie návrhu na úrovni komponentov pre jednoduché FSZ s málo komponentmi a na úrovni modulov pre vysokointegrované FSZ.

Ak má FSZ zabudovanú autodiagnostiku, s ktorou sa počíta v bezpečnostnej analýze, analýza módu porúch a účinkov musí byť zameraná na posúdenie miery pokrytia porúch objavených samotestovaním. Ak táto analýza ukazuje, že niektoré poruchy nemusia byť detegované a objavené operátorom pomocou samodiagnostiky FSZ, musia sa vyvinúť testy na ich objavenie. Intervaly na overovacie testy musia byť stanovené podľa frekvencie výskytu nedetegovaných porúch a spoľahlivosti požadovanej od FSZ. Ak nie sú k dispozícii spoľahlivostné údaje, interval testov sa musí zvoliť porovnaním s ďalšími podobnými FSZ. Po získaní skúseností sa musí testovací interval prehodnotiť.

b) Kategória B

Musí byť stanovená požadovaná spoľahlivosť FSZ a porovnaná s výpočtovou spoľahlivosťou podľa návrhu. Je žiadúce, aby FSZ tejto kategórie malo redundanciu, ale nie je to podstatné, ak FSZ dosiahne požadovanú spoľahlivosť bez nej. Ak nie je redundancia, FSZ musí byť systematicky zhodnotené na určenie jednotlivých porúch, ktoré môžu brániť jeho prevádzke. Musí sa analyzovať pravdepodobnosť bezpečnostných dôsledkov týchto porúch. Ak sa dôsledky jednotlivých porúch neakceptujú z dôvodu veľkosti alebo frekvencie ich vplyvu na bezpečnosť, musí byť zavedená redundancia.

Použité komponenty musia mať preukázanú vysokú kvalitu a spoľahlivosť; musia byť zabudované prostriedky zaisťujúce rýchlu detekciu porúch a opravy.

c) Kategória C

FSZ tejto kategórie všeobecne nepotrebujú redundanciu, ale môže sa využiť na dosiahnutie stanovenej spoľahlivosti.

Pre prípady FSZ kategórie C, kde je nutná redundancia na dosiahnutie požadovanej disponibility, by sa mala využiť spoľahlivosť a redundancia ako pre kategóriu B.

8.3 Požiadavky na zaistenie výkonnosti

8.3.1. Základné požiadavky

Základné požiadavky zaistenia výkonnosti sú:

a) požiadavky na výkonnosť musia byť špecifikované;

b) musí byť zavedený program zaistenia kvality (QA) podľa IAEA Code 50-C-QA. Musí vyžadovať špecifikácie výkonnosti, treba definovať a overiť testovanie;

[1)] Pre samostatný systém, ktorý obsahuje softvér vyvinutý v súlade s najvyššími kritériami kvality (IEC 880 a IEC 987) sa môže nárokovať spoľahlivosť 10^{-4} porúch/požiadavka ako primeraný limit, ak sa berú do úvahy všetky potenciálne zdroje porúch v dôsledku špecifikácie, návrhu, výroby, inštalácie, prevádzkového prostredia a praxe údržby. Táto hodnota zahŕňa riziko spoločnej príčiny porúch v redundantných kanáloch systému a platí pre celý systém - od snímačov cez spracovanie signálov až po výstup k akčnému zariadeniu. Nároky na lepšie spoľahlivosti nie sú vylúčené, ale v takých prípadoch je potrebné zvláštne podporné doloženie, ktoré berie do úvahy všetky uvedené faktory.

c) komponenty, moduly, subsystémy a FSZ sa musia testovať podľa plánu zaistenia kvality, aby sa preukázali ich uspokojivé vlastnosti počas výroby, montáže, inštalácie a v súlade s kategóriou, do ktorej patria.
Testy sa musia vykonať na komponentoch, moduloch a subsystémoch pre uistenie, že pri zabezpečovaní kvality pri výrobe budú FSZ pracovať v súlade so špecifikovanými požiadavkami. Kombinované testy inštalovaného FSZ SKR spolu s mechanickými a fluidnými systémami sa musia uskutočniť na JE pred jej prevádzkou v režime vyžadujúcom disponibilitu bezpečnostných funkcií (poskytovaných FSZ).
Zámer testov na mieste je ten istý pre všetky kategórie, hoci kontrola kvality a požiadavky na dokumentovanie sa menia v súlade s kategóriou, ako je to uvedené v 8.5;

d) počas prevádzky sa musí robiť on-line a/alebo periodické testovanie na preukázanie, že sa udržiava výkonnosť systému.
Na detekciu porúch zariadenia sa musí navrhnúť testovanie; každý zistený nedostatok sa musí následne korigovať nejakou zmenovou riadiacou procedúrou. O tejto korekcii sa musí viesť vhodný záznam;

e) ak sa používa počítačové zariadenie, musí sa použiť program zaistenia kvality cyklu životnosti softvéru primeraný kategórii FSZ.

8.3.2 Špecifické požiadavky

a) Kategória A

Musia sa urobiť typové skúšky dokazujúce, že zariadenia rovnakej konštrukcie ako zariadenie inštalované v jadrovej elektrárni budú pracovať podľa požiadaviek v návrhu, ak sú pod vplyvom očakávaného prevádzkového prostredia.

Musia sa urobiť funkčné testy komponentov, modulov, subsystémov a, ak je to možné tak aj celého FSZ.

Tieto testy musia byť osvedčené v licencii alebo jej reprezentatívnej náhrade.

Ak sa použilo počítačové zariadenie, systém treba podrobiť formálnemu overovaniu a vyhodnoteniu podľa IEC 880 a IEC 987.

Funkčné testy sa môžu vykonať vo výrobnom závode alebo v elektrárni. Testy vykonané v závode a v elektrárni sa musia koordinovať na dosiahnutie ich plného pokrytia.

Ak nie je možné preukázať, že sa všetky špecifikované funkcie môžu pri testoch dosiahnuť, musí sa vypracovať zvláštne osvedčenie.

Testovanie v elektrárni musí preukázať, ako je to len možné, že stanovené bezpečnostné funkcie inštalovaných systémov a zariadení sa môžu dosiahnuť s požadovanou výkonnosťou. Toto testovanie musí vziať do úvahy zmeny prevádzkových parametrov. To je akceptačný test na mieste, ktorý musí byť osvedčený licenciou alebo jej reprezentatívnou náhradou.

Ak sa použilo počítačové zariadenie, musí byť implementovaný program zaistenia kvality softvéru v súlade s IEC 880.

On-line a/alebo periodické testy musia preukázať schopnosť vykonávať všetky požadované bezpečnostné funkcie. Periodické testy musia zahŕňať potvrdenie funkčnej kapacity všetkých sub-FSZ potrebných na testovanie FSZ.

Perióda testov pre časti kategórie A sa bude pohybovať v rozmedzí mesiac až rok v závislosti od zložitosti a stupňa dynamickosti prevádzky a autotestovania implementovaného v návrhu.

Testovanie si môže vyžiadať potlačenie výstupných signálov alebo vytvorenie prekleňovacích by-passov. Ak je zariadenie by-passu súčasťou príslušného FSZ, jeho integrita sa musí osvedčiť, aby sa preukázalo, že sa nemôže použiť spôsobom, ktorý by mohol brániť FSZ pri plnení

stanovených bezpečnostných funkcií. Napríklad ich použitie môže byť fyzicky obmedzené na jednotlivú vetvu redundantného FSZ v tom istom čase.

Pre niektoré FSZ by mal návrh zahŕňať redundanciu, ktorá umožní testovanie počas prevádzky elektrárne. Mali by to byť FSZ, v ktorých nie je možné bez periodických testov preukázať dostatočnú spoľahlivosť alebo efektívnosť, ktoré by nebolo možné testovať s elektrárňou prevádzkovanou v režime, v ktorom sa vyžaduje FSZ , aby FSZ bola disponibilná, a ktoré nemajú samotestovanie, ktoré môže zistiť všetky poruchy.

Nie je nevyhnutné zabudovať redundanciu pre celé FSZ, ale len pre tie časti, ktoré musia byť testované so systémom v prevádzke.

b) Kategória B

Musia sa vykonať typové skúšky na preukázanie, že zariadenia podobnej konštrukcie ako zariadenie inštalované v JE bude pracovať tak, ako sa požaduje v návrhu, ak je pod vplyvom očakávaných prevádzkových podmienok prostredia (ako je uvedené v 8.4.2b) za predpokladu, že boli vykonané analýzy na preukázanie, že rozdiely v zariadeniach neurobia výsledky testov neplatnými.

Pred prevádzkou sa musia urobiť funkčné skúšky na dokázanie, že všetky stanovené funkcie sa môžu uskutočniť systémami so zariadeniami podobnej konštrukcie, ako je zariadenie inštalované v JE. Niektoré alebo všetky tieto skúšky môžu byť vykonané v JE.

Softvér použitého počítačového zariadenia musí byť vyvinutý systematickým štruktúrovaným spôsobom v súlade s intenciami IEC 880. Avšak plná aplikácia najprísnejších požiadaviek IEC 880 sa nevyžaduje.[1)]

Testovanie v JE (SAT) má v najvyššej možnej miere preukázať, že všetky stanovené bezpečnostné funkcie inštalovaného zariadenia sú dosiahnuteľné. Testy riadiacich zariadení musia preukázať schopnosť správne reagovať na prechodné stavy a zmeny požiadaviek.

Testovanie displejov a signalizačných zariadení musí zahŕňať testy s privedením signálov na príslušné vstupy na preukázanie vyhovujúcich vlastností.

On-line a/alebo periodické testovanie výkonnosti musí zahŕňať potvrdenie funkčnej kapacity sub-FSZ.

Perióda testovania má byť vybratá tak, aby vyhodnotená kategória poruchy alebo pravdepodobnosť zlyhania pri požiadavke na činnosť bola v súlade s požiadavkami na spoľahlivosť podľa bezpečnostnej analýzy.

c) Kategória C

Licencia môže akceptovať testy od výrobcu ako adekvátne na preukázanie, že sa dosiahnu stanovené vlastnosti. Ak je to nutné, urobia sa špecifické typové a funkčné skúšky, ale zvyčajne sa nevyžadujú.

Akceptačné testy by sa mali urobiť v JE, aby sa preukázalo, že FSZ dosiahnu stanovenú funkčnosť a výkonnosť. Periodické testovanie výkonnosti môže byť obmedzené na prekontrolovania počas výmeny paliva alebo podobných odstávok.

Ako vodítko musí byť takéto testovanie vykonané v intervale najviac jeden až dva roky. Pri redundanciách musia byť zahrnuté individuálne kontroly funkčnej kapacity všetkých redundantných FSZ alebo sub-FSZ. Testy on-line sú prostriedkami na splnenie týchto požiadaviek.

[1)] Budúce dodatky k IEC 880 budú obsahovať špecifické požiadavky na softvér systémov kategórie B.

8.4 Požiadavky na zaistenie odolnosti voči prostrediu

8.4.1 Základné požiadavky

Nutné je poskytnúť uistenie, že FSZ nezlyhajú v dôsledku podmienok prostredia, ktorému môžu byť vystavené počas PIU a po nej. Toto uistenie môže poskytnúť formálna kvalifikácia zariadenia alebo iné techniky.

8.4.2. Špecifické požiadavky

a) Kategória A

Prijaté opatrenia na zaistenie, že FSZ kategórie A bude pokračovať v prevádzke pri všetkých očakávaných prevádzkových podmienkach, musia zahŕňať formálnu kvalifikáciu zariadenia podľa IEC 780 na podmienky prostredia a IEC 980 na podmienky zemetrasenia.

Výsledky testov sa musia zaznamenať a udržiavať medzi celoživotnými záznamami jadrovej elektrárne. Všetky poruchy počas kvalifikačných testov sa musia preskúmať a musia sa zdokumentovať príčiny a nápravné opatrenia.

Kvalifikácia zariadení kategórie A sa môže dosiahnuť použitím jednej metódy alebo kombináciou niekoľkých rôznych metód: testami, analýzou, ich kombináciou alebo na základe dostupných prevádzkových skúseností.

b) Kategória B

Zariadenia kategórie B si môžu vyžadovať formálnu kvalifikáciu. Musia byť stanovené najhoršie očakávané podmienky prostredia, v ktorých musí zariadenie pracovať a špecifikované požiadavky. Návrh zariadení by sa mal systematicky kontrolovať, aby sa vyhovelo týmto špecifikáciám.

Ak ide o nové zariadenie, alebo sa vyžaduje prevádzka komerčného zariadenia v podmienkach, na ktoré nebolo navrhované (napr. zemetrasenie alebo extrémne podmienky prostredia), musí byť zavedená množina pravidiel, ktoré musí návrh rešpektovať, alebo podľa ktorých má byť posúdený. Tieto pravidlá musia byť založené na skúsenostiach získaných so špeciálnymi požiadavkami návrhu zariadenia kategórie A.

c) Kategória C

Zariadenia kategórie C sa môžu akceptovať na úrovni normálneho komerčného návrhového štandardu, ak si ich úloha nevyžaduje špeciálnu kvalifikáciu, napr. na seizmickú odolnosť, na požiadavky protipožiarnej ochrany, na zabránenie prepätí a elektrických šumov, čím by zariadenia kategórie C mohli ovplyvniť FSZ kategórie A alebo B.

Nároky na prevádzku v abnormálnych podmienkach prostredia musia byť doložené zdokumentovanými dôkazmi.

8.5 Požiadavky na zaistenie kvality/riadenie kvality (QA/QC)

8.5.1 Základné požiadavky

Cieľmi riadenia kvality je riadenie konfigurácie, zmien a postupností. Návrh musí byť dostatočne detailne zdokumentovaný, aby podporil fázy výroby, inštalácie, preberacích skúšok a prevádzky JE. Primeranú pozornosť treba venovať dokumentácii umožňujúcej budúce modifikácie návrhu.

Špeciálne QA/QC a testovanie by sa malo vykonať počas vývoja úmerne k relatívnej novosti alebo zložitosti nového návrhu, resp. modifikácie. Tieto činnosti vývoja by sa mali primerane zdokumentovať v súlade s dôležitosťou FSZ pre bezpečnosť.

8.5.2 Špecifické požiadavky

a) Kategória A

Požiadavky zaistenia kvality (QA) musia byť podľa IAEA Code 50-C-QA. Dokumentácia musí umožňovať sledovanie histórie časti zariadenia vrátane aspektov návrhu, výroby a prevádzky. Musí sa to týkať všetkých zariadení v návrhu až po úroveň modulov.

Konfigurácia sa musí kontrolovať smerom dole, až po najnižší sledovateľný element. Sledovateľnosť čísel dodávky, materiálov atď. musí siahať cez celé FSZ až po úroveň samostatných modulov.

Dokumentácia riadenia kvality (QC) musí umožniť skúmajúcemu spätné sledovanie hardvéru alebo softvéru až k špecifikáciám stanovujúcim požiadavky na jednotlivé komponenty, ktoré ich realizujú.

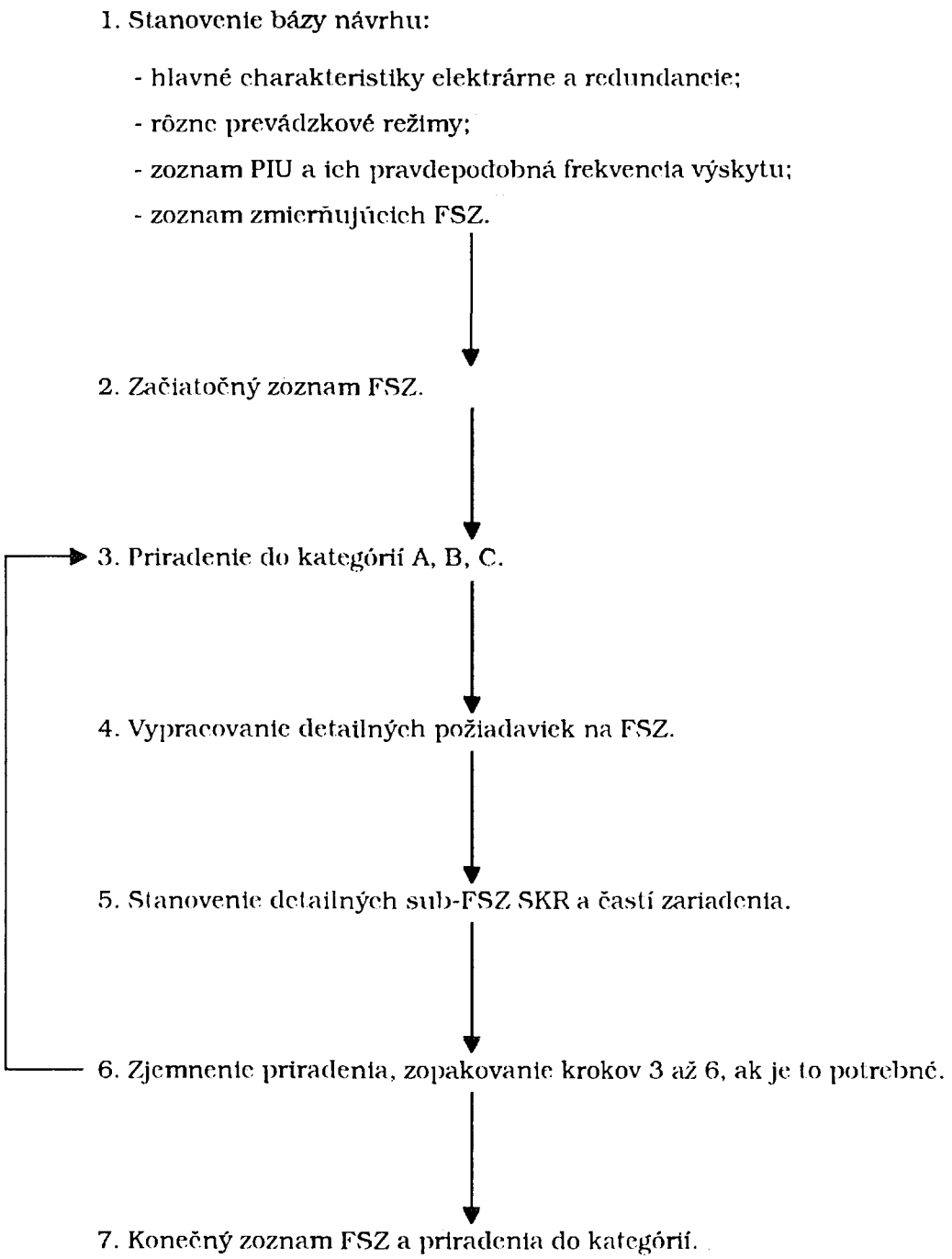
b) Kategória B

Úroveň zaistenia kvality (QA) použitá pre FSZ kategórie B môže byť nižšia ako pri kategórii A, hoci by mal byť program QA konzistentný s obdobnými programami kategórie A.

Požiadavky na dokumentáciu a sledovateľnosť nadväznosti musí byť na úrovni normálnej komerčnej praxe.

c) Kategória C

Pre FSZ kategórie C sa môže QA akceptovať na komerčnej úrovni so zodpovedajúcim QC.



Obrázok 1 - Metóda kategorizácie

Príloha A (informatívna)

Príklady kategórií

A.1 Kategória A

A.1.1 Typické funkcie

FSZ SKR zaradené do kategórie A sú nutné na:

a) odstavenie reaktora a udržiavanie podkritickosti;

b) odvod zvyškového tepla až po konečnú hranicu odvodu v prostredí;

c) izolácia kontainmentu;

d) informácie pre závažné činnosti operátora.

A.1.2 Typické systémy

a) systém ochrany reaktora;

b) systém zabezpečenia bloku a podporné systémy bezpečnostných systémov;

c) kľúčová inštrumentácia a zobrazovače umožňujúce predurčené činnosti operátora stanovené v prevádzkových predpisoch vyžadované na zaistenie bezpečnosti JE.

A.2 Kategória B

A.2.1 Typické funkcie

FSZ SKR kategórie B sú nutné na:

a) automatické riadenie podmienok v primárnom a sekundárnom okruhu elektrárne udržiavajúc parametre v limitoch predpokladaných bezpečnostnou analýzou a predchádzanie udalostiam, ktoré by mohli vyústiť do havárií;

b) monitorovacie a ovládacie výkony individuálnych systémov a časti zariadenia počas havárie a po nej na včasné varovanie o začiatku problémov a na udržanie únikov rádioaktivity v čo možno najmenšej miere (ALARA);

c) obmedzenie dôsledkov vnútorných nebezpečenstiev;

d) monitorovanie/ovládanie pri manipuláciách s palivom, kde by porucha mohla spôsobiť malé uvoľnenie rádioaktivity.

A.2.2 Typické systémy

a) systém automatickej regulácie JE alebo systém preventívnej ochrany;

b) systém spracovania dát v blokovej dozorni;

c) systém potlačenia požiaru;

d) bezpečnostné okruhy a blokády systémov manipulácie s palivom používané pri odstavenom reaktore.

A.3 Kategória C

A.3.1 Typické funkcie

FSZ SKR priradené do kategórie C môžu obsahovať:

a) všetko, čo slúži varovaniu pred vnútornými alebo vonkajšími nebezpečenstvami (požiar, zatopenie, explózia, seizmické udalosti atď.);

b) všetko, čo pri chybnej činnosti môže spôsobiť malé uvoľnenie rádioaktivity alebo viesť k radiačnému ohrozeniu prevádzkového personálu JE;

c) systémy kontroly vstupu, komunikačné systémy na varovanie pri závažných únikoch rádioaktivity do priestorov elektrárne alebo do okolitého prostredia na účely uskutočnenia havarijného plánu JE.

A.3.2 Typické systémy

a) varovný systém;

b) monitorovanie toku rádioaktívneho odpadu a blokády, radiačné monitorovanie priestoru (okolia);

c) systém kontroly vstupu;

d) systém komunikácie v núdzových podmienkach.

Upozornenie: Zmeny a doplnky ako aj správy o nových vydaných technických normách sú uverejňované vo Vestníku Úradu pre normalizáciu, metrológiu a skúšobníctvo SR

STN IEC 1226
Vydavateľ: Slovenský ústav technickej normalizácie - Vydavateľstvo
Karloveská 63, P. O. BOX 246, 840 00 Bratislava
Rok vydania 1996, strán 24, náklad 300 výtlačkov, č. publ. 11615
Vytlačila tlačiareň Sineal, Kazanská 2, 821 06 Bratislava
Cenová skupina 12