BEHROUZ MEHRI/AFP/Getty Images

Projektovanie riadiacich, meracích, ukazovacích a signalizačných systémov pre jadrové zariadenia

Vo vyhláške č. 50/2006 vydanej Úradom jadrového dozoru Slovenskej republiky sa ustanovujú podrobnosti o požiadavkách na jadrovú bezpečnosť jadrových zariadení pri ich umiestňovaní, projektovaní, výstavbe, uvádzaní do prevádzky, prevádzke, vyraďovaní a pri uzatváraní úložiska, ako aj kritériá pre kategorizáciu vybraných zariadení do bezpečnostných tried.

V prílohe č. 3 tejto vyhlášky sú v bode L presne vymedzené požiadavky na projektovanie a ďalšie vlastnosti bezpečnostných, riadiacich, meracích, ukazovacích a signalizačných systémov používaných v súvislosti s jadrovými zariadeniami. Medzi najdôležitejšie zásady patria (citácia vyhlášky):

1. Bezpečnostné systémy sa musia projektovať s najvyššou dosiahnuteľnou funkčnou spoľahlivosťou, zálohovaním a nezávislosťou jednotlivých kanálov, aby jednoduchá porucha:

a) nespôsobila stratu ochrannej funkcie systému,

b) neznížila počet nezávislých meracích kanálov a informačných kanálov na jeden.

2. Bezpečnostný systém musí umožňovať periodické skúšky funkcie jednotlivých nezávislých informačných kanálov pri normálnej prevádzke a vyskúšanie ich spoločných obvodov pri odstavenom jadrovom zariadení. Tieto spoločné obvody sa musia projektovať tak, aby ich možné poruchy viedli nanajvýš k odstaveniu jadrového zariadenia, a nie k strate ich ochrannej funkcie.

3. Bezpečnostný systém sa musí navrhnúť tak, aby účinnosť systému ochrany nemohla byť zrušená nesprávnym zásahom vybraného zamestnanca, správne zásahy však nesmie obmedzovať.

4. Bezpečnostný systém sa musí navrhnúť tak, aby účinky podmienok pri normálnej prevádzke, abnormálnej prevádzke a pri projektových haváriách na záložné kanály systému nespôsobili stratu jeho funkčnosti; v opačnom prípade sa musí preukázať jeho spoľahlivosť na inom princípe.

5. Ak je riadiaci systém alebo bezpečnostný systém závislý od spoľahlivosti počítačového systému, musia sa ustanoviť a uplatniť špecifické kritériá kvality a postupy vývoja, dodávky a skúšania technického a predovšetkým programového vybavenia počítačového systému počas životnosti riadiaceho systému a bezpečnostného systému.

6. Úroveň požadovanej spoľahlivosti počítačového systému musí byť primeraná jeho bezpečnostnej dôležitosti. Úroveň spoľahlivosti sa musí dosiahnuť komplexnou stratégiou, pri ktorej sa používajú vzájomne sa doplňujúce prostriedky v každej fáze vývoja procesu

so zohľadnením efektívnej metódy analýz a testovania, ako aj stratégie validácie s cieľom potvrdenia požiadaviek na projekt.

7. Úroveň spoľahlivosti predpokladaná v analýze bezpečnosti pre systémy na báze počítača musí zahŕňať špecifikovaný konzervativizmus, ktorý vyváži komplikovanosť použitej technológie a ťažkosť vykonávaných analýz bezpečnosti.

8. Proces vývoja počítačového systému, bezpečnostného systému alebo riadiaceho systému sa musí dokumentovať a kontrolovať, pričom sa musí umožniť jeho spätné preskúmanie vrátane jeho skúšania a spúšťania, ako aj projektových zmien týchto systémov.

9. Počítačový systém bezpečnostného systému alebo riadiaceho systému s vplyvom na jadrovú bezpečnosť musí byť kvalifikovaný.

10. Ak nemožno preukázať existenciu dostatočného množstva údajov z prevádzkovej činnosti rovnakých systémov použitých v podobných prípadoch, musí sa prijať konzervatívna úroveň spoľahlivosti predpokladaná v analýze bezpečnosti počítačového systému.

11. Bezpečnostné systémy a riadiace systémy musia byť oddelené, aby porucha riadiacich systémov neovplyvnila bezpečnostné funkcie. Ak to nie je možné, funkčne nutné a účelné spojenie bezpečnostných a riadiacich systémov sa musí obmedziť natoľko, aby bezpečnostná funkcia nebola ovplyvnená.

12. Bezpečnostné systémy a riadiace systémy musia mať zabudované automatizované bezpečnostné zásahy tak, aby počas odôvodneného časového úseku od vzniku udalosti sa nevyžadoval zásah človeka, pričom musia byť k dispozícii informácie o automatizovaných bezpečnostných zásahoch, aby bolo možné monitorovať ich účinok.

13. Bezpečnostný systém sa musí navrhnúť tak, aby sa neprekročili projektové parametre ani pri chybnej funkcii riadiaceho systému. Činnosť bezpečnostného systému musí byť nadradená činnosti riadiaceho systému, ako aj činnosti človeka s možnosťou aktivovať bezpečnostný systém ručne.

14. Bezpečnostný systém na báze počítača musí mať potvrdenie o zabezpečení spoľahlivosti vykonané odborníkmi nezávislými od jeho projektanta a dodávateľa, pričom ak sa nemôže s predpokladanou mierou spoľahlivosti preukázať vyžadovaná integrita systému, treba použiť iné prostriedky na zabezpečenie splnenia bezpečnostných funkcií.

15. Bezpečnostný systém musí byť navrhnutý tak, aby rozoznával postulované iniciačné udalosti a uviedol do činnosti systémy určené na zmiernenie ich následkov.

16. Riadiace systémy sa musia projektovať tak, aby poskytovali požadované signály o odchýlkach dôležitých prevádzkových parametrov a procesov od prípustných medzí. Riadiace systémy musia byť vybavené prístrojmi, aby mohli sledovať, merať, registrovať a ovládať hodnoty a systémy dôležité z hľadiska jadrovej bezpečnosti pri normálnej a abnormálnej prevádzke.

17. Riadiace systémy musia priebežne v pravidelných intervaloch alebo podľa potreby zaznamenávať parametre, ktoré sú podľa analýz bezpečnosti dôležité z hľadiska jadrovej bezpečnosti.

18. Ukazovacie, signalizačné a ovládacie prístroje sa musia projektovať a rozmiestňovať tak, aby mali zamestnanci stále dostatok informácií o prevádzke a mohli v prípade potreby operatívne zasiahnuť.

19. Meracie, ukazovacie, signalizačné a zapisovacie prístroje sa musia projektovať tak, aby v prípade udalostí poskytovali:

a) údaje o okamžitom stave,

b) základné informácie o priebehu udalostí a ich záznam,

c) údaje umožňujúce charakterizovať šírenie rádioaktívnych látok a ionizujúceho žiarenia do pracovného prostredia a do životného prostredia.

-tog-