Meranie a regulácia v Jadrových Elektrárňach

doc. Ing. Róbert Hinca, PhD.

Sylaby 1

- **Bezpečnostné a riadiace systémy.** Základné definície. Základná terminológia pre systémy riadenia a regulácie, ochrany a blokády.
- **Základy merania teplotechnických a jadrovofyzikálnych meraní.** Fyzikálne princípy, merací kanál, detektory, sondy, vstupné prevodníky.
- Teoretické základy v oblasti automatizácie a regulácie. **Regulačná technika.** Vlastnosti regulátorov. Analógové systémy. Digitálne systémy. Hybridné systémy.
- **Hlavné blokové regulátory, ochrany a blokády.** Fyzikálne princípy, prístrojová technika, technológia, hlavné charakteristiky.

Sylaby 2

- **In-core, ex-core merania parametrov reaktora.** Výpočty vývinu tepla v aktívnej zóne. Nerovnomernosť, bezpečnostné rezervy.
- **Limity a bezpečnostné medze** vo vzťahu k riadiacim systémom.
- **Zabezpečovacie a ochranné systémy.** Technologické ochrany.
- **Havarijné informačné, monitorovacie a riadiace systémy.** Núdzová dozorňa. Informačné systémy a bloková dozorňa.
- Počítačová podpora riadiaceho personálu.
- Radiačný monitorovací systém.
- Kalibrácia a overovanie meradiel. Určené meradlá. Chyby a neistoty merania.

Bezpečnostné a riadiace systémy

- **V legislatívnom systéme SR sú požiadavky na bezpečnostné a riadiace systémy definujú hlavne vo vyhláškach UJD SR, IAEA Guides a normách STN.**
  - **vyhláška ÚJD SR č. 430/2011 o požiadavkách na jadrovú bezpečnosť**
  - **IAEA SSG-39/2016: Design of Instrumentation and Control Systems for Nuclear Power Plants**
  - **STN EN 60987:2015 -** ***Jadrové elektrárne. Prístrojové vybavenie a riadenie dôležité pre bezpečnosť. Požiadavky na návrh hardvéru pre systémy založené na počítačoch***

iné relevantné normy

- STN IEC 61502:2006 - Jadrové elektrárne. Tlakovodné reaktory. Monitorovanie vibrácie vnútroreaktorových prvkov
- STN IEC 61504:2006 - Jadrové elektrárne. Prístrojové vybavenie a riadenie systémov dôležitých pre bezpečnosť. Radiačná kontrola elektrárne
- STN IEC 60960:2000 - Funkčné kritériá návrhu systému oznamovania bezpečnostných parametrov pre jadrové elektrárne

Bezpečnostné a riadiace systémy

- Pod pojmom **riadiaci systém** sa rozumie systém zabezpečujúci riadenie technologického zariadenia jadrového zariadenia v nominálnych a prechodových režimoch; jeho cieľom je previesť technologické zariadenie z jedného bezpečného stavu do druhého.
- **Bezpečnostným systémom** sa rozumie systém zaisťujúci bezpečné **odstavenie** jadrového reaktora alebo **odvod tepla** z aktívnej zóny reaktora alebo **obmedzenie následkov** abnormálnej prevádzky a projektových havárií.

Základné bezpečnostné funkcie

podľa Terminologický slovník UJD SR: 2016

a) **regulácia reaktivity,**
b) **odvod tepla,**
c) **zadržanie rádioaktívnych látok vnútri fyzických bariér,**
d) **reguláciu a obmedzenie množstva a druhu rádioaktívnych látok uvoľnených do životného prostredia.**

Fundamental safety functions

Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1:2016

Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states:

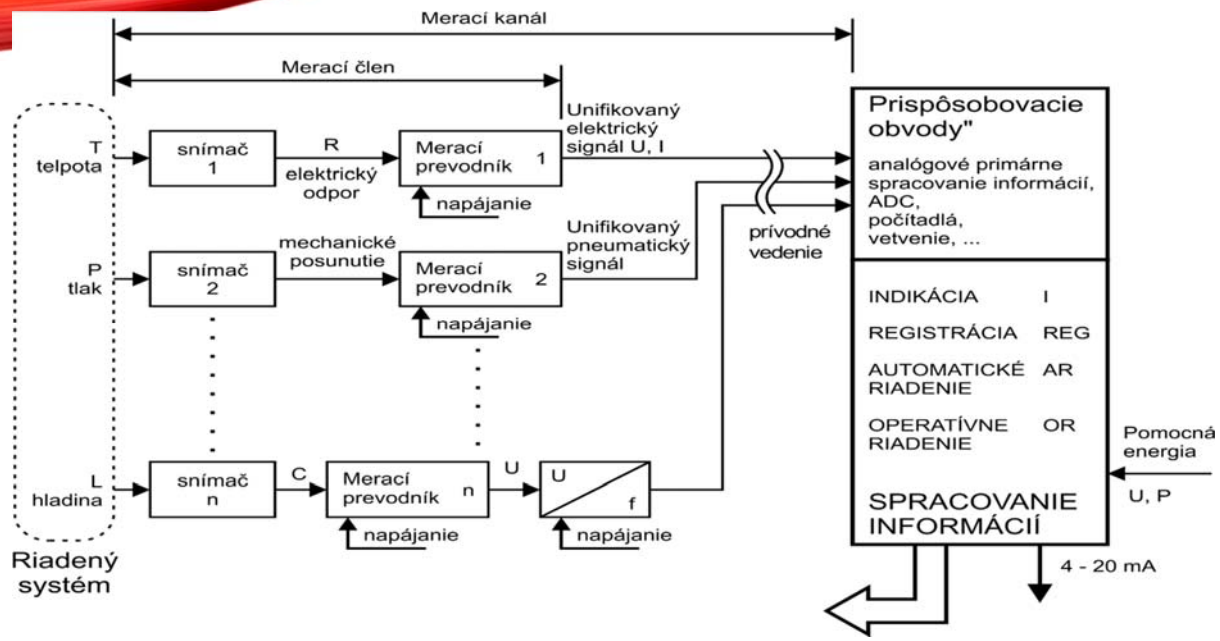
- (i) **control of reactivity**,
- (ii) **removal of heat** from the reactor and from the fuel store and
- (iii) **confinement of radioactive material**, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

Zariadenia I&C

IAEA SSG-39/2016

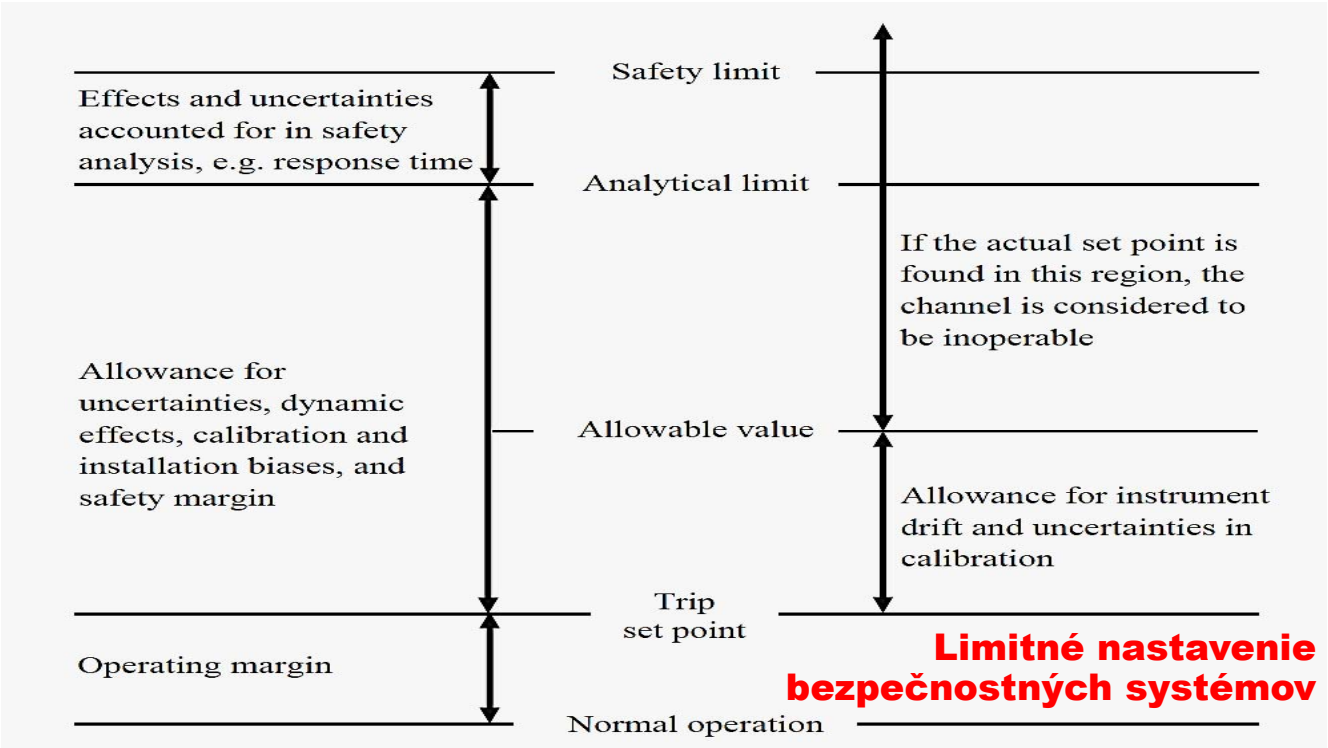
- senzory, detekčné jednotky
- riadenie akčných prvkov
- prístrojové vybavenie kontroly a riadenia zariadení JE
- operátorské stanice, interfejs
- informačné a komunikačné systémy
- softvér, bezpečnosť a spoľahlivosť softvéru
- programovateľné moduly prístrojov (FPGA)
- industriálne digitálne prístroje špeciálneho určenia

Informačný podsystém riadiaceho systému



Examples of I&C systems important to safety

- Reactor protection systems;
- Reactor control systems and reactivity control systems and their monitoring systems;
- Systems for monitoring and controlling reactor cooling;
- Systems for monitoring and controlling emergency power supplies;
- Systems for monitoring and controlling containment isolation;
- Instrumentation for accident monitoring;
- Systems for monitoring of effluents;
- I&C systems for fuel handling.



Limitné nastavenie bezpečnostných systémov

Požiadavky na projekt bezpečnostných a riadiacich systémov

Pod **kritériom jednoduchej poruchy** sa rozumie schopnosť komponentu alebo systému zvládnuť jednu náhodnú poruchu, ktorá môže mať za následok stratu schopnosti komponentu alebo systému plniť jeho bezpečnostné funkcie, na ktoré je určený; následné poruchy v dôsledku tejto jednoduchej poruchy sa považujú za jej súčasť.

Pod **kritériom bezpečnej poruchy** schopnosť komponentu alebo systému prejsť pri svojom zlyhaní do bezpečného stavu bez nutnosti iniciovania akejkoľvek činnosti.

Požiadavky na projekt
Princíp redundancie, Princíp nezávislosti

Princíp redundancie

Zabezpečuje zvýšenie spoľahlivosti využitím **viac než minimálneho počtu súborov** zariadenia k splneniu bezpečnostnej funkcie. Redundantný systém je schopný plniť svoju funkciu aj v prípade, že sa v systéme objaví náhodná jednoduchá porucha.

Princíp nezávislosti

Aplikáciou tohto princípu chceme dosiahnuť, aby porucha jedného systému (prvku) nezapríčinila poruchu iného systému. Využitie princípu sa v projekte systémov odzrkadlí vo **funkčnom** (rôzne sledované parametre) a/alebo **fyzickom** (separácia vzdialenosťou, bariérami) oddelení jednotlivých systémov.

Požiadavky na projekt
Princíp rôznorodosti, rozmanitosti, rozličnosti

Zvyšuje spoľahlivosť systému redukciou výskytu určitej jednoduchej poruchy.
Rôznorodosť môžeme dosiahnuť rôznym prístrojovým vybavením redundantných systémov (rozličnosť vybavenia), ale aj sledovaním rôznych premenných veličín na detekciu poruchy (funkčná rozličnosť).

Požiadavky na projekt
Konzervatívny prístup

Konzervatívnym prístupom k zaisteniu jadrovej bezpečnosti sa rozumie prístup vedúci k pesimistickým výsledkom vo vzťahu k určeným kritériám prijateľnosti.
Pri projektovaní systémov sa využívajú prvky, technické riešenia a princípy, ktoré sú **dostatočne overené** predchádzajúcimi skúsenosťami z prevádzky, alebo testami, vedeckými výskumami, skúškami prototypov apod.

Požiadavky na projekt
Princíp testovateľnosti

Princíp testovateľnosti

Testovaním systémov docielime predovšetkým podstatné zníženie pravdepodobnosti zlyhania systému pri výzve k činnosti. Použitím modernej elektroniky môžeme dosiahnuť samotestovateľnosť systémov, v ktorých krátkymi impulzami s vysokou frekvenciou neustále testujeme ich funkčnosť. Samotestovateľný systém sám upozorní na svoju poruchu aj v prípade, keď jeho činnosť nie je potrebná.

Požiadavky na projekt
Princíp rozličnej priority, Princíp samoochranného projektu

Princíp rozličnej priority

Bezpečnostné systémy majú prednosť všetkými ostatnými systémami a ich činnosť nemôže byť prerušená ani operátorom.

Princíp samoochranného projektu

Bezpečnosť celého JEZ i jeho bezpečnostných zariadení je založená na prirodzených spätných väzbách a procesoch. Konkrétne pri projekte reaktora hovoríme o inherentnej bezpečnosti. Pri výskyte poruchy sa JEZ prevedie do bezpečného stavu bez požiadavky iniciovať akékoľvek činnosti.

Požiadavky na projekt
Ochrana pred vonkajšími vplyvmi

Tento princíp zahŕňa ochranu pred vplyvmi od **udalostí** mimo daného zariadenia (letiace predmety, tlakové vlny, záplavy) a ochranu pred neodborným či vedomým zlomyseľným zásahom ľudí (**sabotáže**). K dosiahnutiu ochrany využívame prostriedky:

- nedostupnosť pre zásah nepovolaným osobám
- rozmiestnenie v ťažko dostupných miestach
- decentralizácia zariadenia
- obmedzenie informovanosti o niektorých dôležitých zariadeniach okruhom zainteresovaných
- umiestnenie v chránených objektoch

Požiadavky na projekt
analýzy odozvy JE na vonkajšie postulované iniciačné udalosti

A. **nepriaznivé prírodné podmienky**
   1. extrémne zaťaženie vetrom,
   2. extrémne vonkajšie teploty,
   3. extrémne zrážky a lokálne záplavy,
   4. extrémne teploty chladiacej vody a námraza,
   5. zemetrasenie,

B. **náraz lietadla**,

C. **vplyv ľudskej činnosti** a priemyselných aktivít vrátane výbuchov v blízkosti jadrového zariadenia.

Požiadavky na projekt
Princíp ochrany do hĺbky

Ochranou do hĺbky sa rozumie systém viacnásobných ***fyzických bariér*** brániacich šíreniu ionizujúceho žiarenia a rádioaktívnych látok do pracovného prostredia alebo životného prostredia s opakovaným ***použitím technických a organizačných*** opatrení slúžiacich na ochranu a zachovanie účinnosti týchto bariér, ale aj na ochranu osôb a životného prostredia.

Z hľadiska koncepcie ochrany do hĺbky musí projekt jadrového zariadenia s vysokou pravdepodobnosťou zabrániť
a) ohrozeniu celistvosti fyzických bariér okrem činnosti poistných zariadení,
b) zlyhaniu fyzických bariér v prípade potreby ich činnosti,
c) zlyhaniu bariéry následkom zlyhania inej fyzickej bariéry.

Projekt musí zohľadniť skutočnosť, že existencia viacnásobnej úrovne ochrany do hĺbky nie je dostatočným zabezpečením pokračovania prevádzky jadrového zariadenia, **ak je nefunkčná jedna úroveň ochrany**. Môže byť definované dovolené trvanie **nepohotovosti** bariér pre rôzne prevádzkové režimy.

Požiadavky na projekt
Princíp ochrany do hĺbky

V projekte jadrového zariadenia musí byť ochrana do hĺbky zahrnutá:

a) použiť **konzervatívny prístup** s cieľom obmedziť vznik prevádzkových udalostí,

b) riešiť **viacnásobné fyzické bariéry** proti úniku rádioaktívnych látok

c) poskytovať **viacnásobné prostriedky** na splnenie bezpečnostných funkcií,

d) obsahovať okrem vnútorných bezpečnostných charakteristík aj návrh **spoľahlivých technických prostriedkov** na zaistenie bezpečnosti,

e) obsahovať **preventívne opatrenia** proti vzniku prevádzkových udalostí, na ich **zdolávanie** a na **zmiernenie** ich následkov pomocou systémov, konštrukcií a komponentov a aj prevádzkových predpisov,

f) zabezpečovať doplnenie riadenia jadrového zariadenia **automatickým zapracovaním** bezpečnostných systémov a **ručnými zásahmi** vybraných a odborne spôsobilých zamestnancov.

Päť úrovní ochrany do hĺbky

1. prvej úrovne ochrany je **predchádzanie** stavom abnormálnej prevádzky a poruchám systémov,
2. druhej úrovne ochrany je **zisťovanie** a obmedzovanie rozvoja stavov abnormálnej prevádzky tak, aby sa zabránilo ich vystupňovaniu do havarijných podmienok,
3. tretej úrovne ochrany je **riadenie projektových havárií** tak, aby sa dosiahli stabilné a prijateľné podmienky po takýchto udalostiach,
4. štvrtej úrovne ochrany je riadenie havárií v podmienkach rozšíreného projektu, **zabránenie ich ďalšiemu rozvoju a udržiavanie únikov** rádioaktívnych látok na najnižšej možnej úrovni; v prípade havárií v podmienkach rozšíreného projektu s tavením jadrového paliva **zmiernenie** ich následkov,
5. piatej úrovne ochrany je **zmiernenie rádiologických následkov významných únikov** rádioaktívnych látok alebo ionizujúceho žiarenia, ktoré vznikli v dôsledku havarijných podmienok.

Úlohy bezpečnostného systému

(1) Projekt musí zabezpečiť, aby bezpečnostné systémy mali výstup pre aktiváciu systému odstavenia jadrového reaktora a ďalej tieto systémy musia

a) uviesť sa **automaticky** do činnosti s cieľom zabezpečiť neprekročenie projektových parametrov pri výskyte iniciačných udalostí,

b) byť schopné uviesť jadrový reaktor do **podkritického stavu** pri všetkých prevádzkových stavoch a udržať ho v podkritickom stave aj v situácii s najvyššou úrovňou reaktivity aktívnej zóny,

c) byť schopné **zabrániť samovoľnému vzniku kritického stavu**; táto požiadavka musí byť splnená aj za predpokladaných činností zvyšujúcich reaktivitu pri uvedení jadrového reaktora do podkritického stavu, a to **aj pri jednoduchej poruche** týchto systémov,

úlohy bezpečnostného systému

d) pozostávať najmenej z dvoch **nezávislých systémov** založených na **rôznych princípoch** a schopných vykonávať funkciu aj pri jednoduchej poruche,

e) byť projektované tak, že jeden zo systémov podľa písmena d) musí byť schopný uviesť jadrový reaktor čo najrýchlejšie do podkritického stavu s rezervou zápornej reaktivity,

f) byť projektované tak, že jeden zo systémov podľa písmena d) musí byť schopný uviesť jadrový reaktor do podkritického stavu a udržať ho v tomto stave aj v situácii s najvyššou úrovňou reaktivity aktívnej zóny,

g) umožniť riadenie reaktivity alebo úpravu rozloženia neutrónového toku za prevádzky tak, aby bola neustále zachovaná **rezerva zápornej reaktivity** na uvedenie jadrového reaktora do podkritického stavu.

úlohy bezpečnostného systému

(2) Projekt musí zahŕňať aj výskyt možných postulovaných iniciačných udalostí v stavoch **nízkeho výkonu alebo odstavenia reaktora**, keď môže byť znížená pohotovosť bezpečnostných systémov alebo riadiacich systémov.

(3) Projekt musí zabezpečiť **kvalifikované prístrojové vybavenie** vrátane záznamových zariadení na zaistenie nevyhnutných **informácií** pre monitorovanie zmien stavu prostredia jadrového zariadenia, stavu jeho bezpečnostných systémov na automatické odstavenie reaktora a zmiernenie následkov havárií, ako aj ostatných systémov dôležitých pre bezpečnosť počas havarijných podmienok a po nich, v prípade vybraných ťažkých havárií len v primeranej miere. Tento systém musí poskytovať vybraným zamestnancom potrebné informácie o priebehu havárie a uvoľnení rádioaktívnych látok.

úlohy bezpečnostného systému

(4) Projekt musí zahŕňať primerané prístrojové vybavenie použiteľné v prostredí **ťažkých havárií** podľa návodov na ich riadenie.

(5) Potrebné informácie z meraní podľa predchádzajúceho odseku musia byť zobrazované na **blokovej** dozorni, **núdzovej** dozorni, ale aj na **havarijnom riadiacom stredisku** takým spôsobom, ktorý umožňuje zhodnotenie aktuálneho stavu jadrového zariadenia a jeho základných bezpečnostných funkcií v podmienkach ťažkých havárií.

(6) Aktivácia a manipulácia s bezpečnostnými systémami musí byť automatizovaná alebo vykonávaná pasívnym spôsobom tak, že **zásah obslužného personálu nie je potrebný počas najmenej 30 minút** po iniciačnej udalosti. Akékoľvek zásahy obslužného personálu požadované projektom počas prvých 30 minút po iniciačnej udalosti musia byť opodstatnené a odôvodnené.

Vyhláška ÚJD SR č. 430/2011

osobitné požiadavky na bezpečnostné a riadiace systémy

(1) Bezpečnostné systémy sa musia projektovať s najvyššou dosiahnuteľnou funkčnou **spoľahlivosťou, zálohovaním a nezávislosťou jednotlivých kanálov** tak, aby jednoduchá porucha

- nespôsobila stratu ochrannej funkcie systému,
- neznížila počet nezávislých meracích a informačných kanálov týchto systémov na jeden.

Vyhláška ÚJD SR č. 430/2011
osobitné požiadavky na bezpečnostné a riadiace systémy

(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.

Vyhláška ÚJD SR č. 430/2011
osobitné požiadavky na bezpečnostné a riadiace systémy

(3) Bezpečnostný systém sa musí navrhnúť tak, aby účinnosť systému ochrany nemohla byť zrušená nesprávnym zásahom, správne zásahy však nesmie obmedzovať (**fail safe**).

Fail-Safe.

Osobitné požiadavky na bezpečnostné a riadiace systémy

(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 riadiaci systém alebo bezpečnostný systém závisí od spoľahlivosti počítačového systému, musia sa stanoviť a uplatniť špecifické kritériá kvality a postupy na vývoj, dodávku a skúšanie technického, a predovšetkým **programového vybavenia** počítačového systému počas životnosti riadiaceho systému a bezpečnostného systému.

Osobitné požiadavky na bezpečnostné a riadiace systémy

(6) Úroveň požadovanej **<u>spoľahlivosti počítačového systému</u>** musí byť primeraná jeho bezpečnostnej dôležitosti. Úroveň spoľahlivosti sa musí dosiahnuť komplexnou stratégiou, ktorá používa vzájomne sa doplňujúce prostriedky v každej fáze vývoja procesu, so zohľadnením efektívnej metódy analýz a testovania, ale aj stratégie verifikácie a validácie s cieľom potvrdiť požiadavky na projekt.

Osobitné požiadavky na bezpečnostné a riadiace systémy

(7) **Verifikácia a validácia** užívateľského **softvéru** bezpečnostného počítačového systému musia byť zabezpečené osobou nezávislou od jeho dodávateľa.

(8) Pre bezpečnostné systémy musí byť **vykonaná analýza poruchových stavov** a dôsledkov porúch, aby sa zistila zraniteľnosť systému pri poruchách komponentov a posúdila sa vhodnosť projektovej stratégie na detekciu porúch alebo na zmiernenie ich následkov.

osobitné požiadavky na bezpečnostné a riadiace systémy

(9) Úroveň spoľahlivosti predpokladaná v analýze bezpečnosti pre systémy na báze počítača musí zahŕňať špecifikovaný **konzervativizmus**, ktorý vyváži komplikovanosť použitej technológie a obťažnosť vykonávaných analýz bezpečnosti.

(10) 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 a aj projektových zmien týchto systémov.

osobitné požiadavky na bezpečnostné a riadiace systémy

(11) Počítačový systém bezpečnostného systému alebo riadiaceho systému s vplyvom na jadrovú bezpečnosť musí byť **kvalifikovaný.**

(12) Bezpečnostné systémy založené na počítačových systémoch musia spĺňať tieto podmienky:

- požaduje sa vysoká **kvalita** použitého hardvéru a softvéru,
- celý vývojový proces zahŕňajúci kontrolu, testovanie, uvedenie do prevádzky a zmeny projektu musí byť systematicky **dokumentovaný** a revidovaný,
- ak nie je možné preukázať spoľahlivosť systému s vysokou mierou dôveryhodnosti, musí byť zabezpečená **diverzita** plnenia funkcií ochrany.

osobitné požiadavky na bezpečnostné a riadiace systémy

(13) 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.

osobitné požiadavky na bezpečnostné a riadiace systémy

(14) **<u>Bezpečnostné a riadiace systémy musia byť oddelené</u>**, prípadne ak oddelenie nie je možné dosiahnuť, ich funkčne nevyhnutné a účelné prepojenie sa musí obmedziť tak, aby porucha riadiacich systémov neovplyvnila bezpečnostné funkcie.

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

osobitné požiadavky na bezpečnostné a riadiace systémy

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

(17) Bezpečnostný systém na báze počítača musí mať **potvrdenie o zabezpečení jeho spoľahlivosti** vykonané odborníkmi nezávislými od jeho projektanta a dodávateľa, pričom ak nemôže byť s predpokladanou mierou spoľahlivosti preukázaná vyžadovaná integrita systému, je nutné použiť iné prostriedky na zabezpečenie splnenia bezpečnostných funkcií.

osobitné požiadavky na bezpečnostné a riadiace systémy

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

(19) Riadiace systémy sa musia projektovať tak, aby **poskytovali** požadované signály o odchýlkach dôležitých prevádzkových parametrov a procesov od prípustných medzí.

(20) 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.

osobitné požiadavky na bezpečnostné a riadiace systémy

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

(22) Ukazovacie, signalizačné a ovládacie prístroje sa musia projektovať a rozmiestňovať tak, aby **zamestnanci** mali neustále **dostatok informácií** o prevádzke a mohli v prípade potreby operatívne zasiahnuť.

osobitné požiadavky na bezpečnostné a riadiace systémy

(23) Meracie, ukazovacie, signalizačné a zapisovacie prístroje sa musia projektovať tak, aby v prípade udalostí **poskytovali**

- údaje o okamžitom stave,
- základné informácie o priebehu udalostí a ich záznam,
- údaje umožňujúce charakterizovať šírenie rádioaktívnych látok a ionizujúceho žiarenia do pracovného prostredia a do životného prostredia.