Technická správa

Predprevádzková bezpečnostná správa

Kapitola 06.05.01.02 Hodnotenie projektu SKR

Stavba: Dostavba 3. a 4. blok JE Mochovce, stavenisko: Jadrová časť
Construction: 3&4 Unit NPP Mochovce Completion, site: Nuclear Island

Stavebník: Slovenské elektrárne, a.s., Bratislava, 3. a 4. blok JE Mochovce
Constructor: Slovenské elektrárne, a.s., Bratislava, 3&4 Unit NPP Mochovce

		LC				
SE Rev	*Date / Dátum*	*IS*	*Supervision Outcome / Stav schválenia*	*Supervised by / Overil*	*Checked by / Kontroloval*	*Approved by / Schválil*

SLOVENSKÉ ELEKTRÁRNE	*Language / Jazyk*	S	*Safety Class / Bezpečnostná trieda*	N	*SEC. INDEX / INDEX utajenia*	*Company use/P*
	Submited to Client to / Predložené odberateľovi na:	*Approval / Schválenie*	X	*Information Only / Len na informáciu*		
		The SE a.s. approval refers to the contract clauses only. All design responsibilities are charged to the Contractor / Schválenie SE a.s. sa vzťahuje iba na zmluvné náležitosti. Za vypracovanie projektu nesie dodávateľ plnú zodpovednosť.				

EPS No / Číslo EPS: PNM34360053	*Revision index / Index revízie: 07*	*Size / Veľkosť*	*Activity Code / Aktivita*	*Type / Subtype Typ / Podtyp*	*Discipline / Profesia*	*Plant Unit / Blok elektrárne*
File name / Názov súboru:	*SE doc. Code / SE číslo dokumentu: PNM34374359*	*A4*	*6.01*	*RS*	*Z*	*8*
** P N M 3 4 3 7 4 3 5 9 0 7 **		*Sheet / List*	*Of / z*		*Plant System / Systém elektrárne*	*Component / Komponent*
		1	*18*			

SE Contract No. / Číslo zmluvy SE:	**4600003952**		**VUJE Contract No. / číslo zmluvy VUJE:**	**1719/00/09**	
Part name / Označenie časti:	**PNM3437435907_S_C00_V**		**Issued on / Vydané dňa:**	**25.07.2019**	
Kód citlivosti[1] / Sensitivity code[1]	**3**	**Name / Meno**	**Organization / Organizácia**	**Dept. / Útvar**	**Date / Dátum**	**Signature / Podpis**
Author / Vypracoval:		[redacted]	VUJE, a.s.	0530	25.07.2019	[redacted]
Co-author / Spolupracoval:						
						[redacted]
Checked by / Kontroloval:		[redacted]	VUJE a.s.	0520	25.07.2019	
Verified by / Overil:		[redacted]	VUJE a.s.	0720	25.07.2019	[redacted]
Approved by / Schválil:		[redacted]	VUJE a.s.	1703	25.07.2019	[redacted]

Revision record / Záznam o revízii

Identification / **Identifikácia** (part/page/chapter/ member/section) (časť/strana/kapitola/ článok/odstavec)	**Brief description of modification /** **Stručná charakteristika úpravy** (description of modification and manner of implementation) (popis úpravy a spôsobu zapracovanie)	**Reason of modification /** **Dôvod úpravy** (author company, number of comments or other stimulation, name of author, comment document No.) (firma autora a číslo pripomienky, resp. iný podnet, meno autora, č. dokumentu pripomienok)
• Celý dokument	• Zapracovanie pripomienok ÚJD podľa Aarhuského výboru	• V súlade s dokumentom PNM34482979
•	•	•
•	•	•
•	•	•
•	•	•
•	•	•
•	•	•
•	•	•
•	•	•
•	•	•
•	•	•
•	•	•
•	•	•
•	•	•

List of document part
Zoznam častí dokumentu

Por. č. No.	Názov dokumentu Document name	Ev. č. súboru časti dokumentu / File ref. No. of document part	Číslo revízie / Revision No.
1.	• Titulný list	• PNM3437435907_S_C00_V	• 07
2.	• Textová časť	• PNM3437435907_S_C01_V	• 07
3.	•	•	•
4.	•	•	•
5.	•	•	•
6.	•	•	•
7.	•	•	•
8.	•	•	•
9.	•	•	•
10.	•	•	•
11.	•	•	•

OBSAH

ÚVOD

Kapitola 6.5.1.2 je vypracovaná v súlade s legislatívnymi dokumentmi ÚJD SR a IAEA, pozrite literatúru [II.13], [II.1], [II.2], [II.5].

Kapitola PpBS 6.5.1.2 je vypracovaná v súlade s bezpečnostným návodom ÚJD SR BNS I.1.2/2008 [II.1], pričom bolo prihliadnuté k novému platnému návodu BNS I.1.2/2014 [II.16] (v primeranom rozsahu).

Pri vypracovaní predmetnej kapitoly PpBS boli súčasne zohľadnené aj pripomienky k PBS uvedené v rozhodnutí ÚJD SR č. 267/2008 [II.17].

Kapitola sa zaoberá technickým a bezpečnostným vyhodnotením celkovej architektúry SKR.

ZOZNAM SKRATIEK

AO	automatické odstavenie
BREAKER	výkonový vypínač rýchleho odstavenia reaktora
CCF	porucha zo spoločnej príčiny
DBA	projektová havária
DiD	ochrana do hĺbky
DRTS	diverzitný systém rýchleho odstavenia reaktora
ECCS	havarijný systém chladenia zóny
ECR	núdzová dozorňa
EMC	elektromagnetická kompatibilita
ERC	havarijné riadiace stredisko
ESFAS	systém aktivácie technických prostriedkov zaistenia bezpečnosti
EUR	požiadavky európskych prevádzkovateľov
EXCORE	systém merania neutrónového toku
HMI	rozhranie človek-stroj
HP	vysokotlakový
HRK	havarijná a regulačná kazeta
IAEA	Medzinárodná Agentúra pre Atómovú Energiu
I&C	meranie a regulácia
IEC	Medzinárodná Elektrotechnická Komisia
INCORE	systém vnútroreaktorovej kontroly
I.O.	primárny okruh
II.O.	sekundárny okruh
MCR	bloková dozorňa
MO34	jadrová elektráreň Mochovce 3. a 4. blok
NPP	jadrová elektráreň
PAMS	pohavarijný monitorovací systém
POSAR	Predprevádzková bezpečnostná správa
PROFIBUS	informačná/riadiaca zbernica technologického procesu
PSA	pravdepodobnostná bezpečnostná analýza
PV	podpäťové vypínanie
QDS	systém kvalifikovaných displejov
RRCS	systém riadenia regulačných kaziet reaktora

RCS	systém riadenia výkonu reaktora
RLS	limitačný systém reaktora
RPP	panel ochrany reaktora (bezpečnostný panel)
RPS	systém ochrany reaktora
RTS	systém rýchleho odstavenia reaktora
RTB	vypínač rýchleho odstavenia reaktora
SMS	systém monitorovania seizmicity
TCS	systém regulácie turbíny
TG	turbogenerátor
ÚJD SR	Úrad Jadrového Dozoru Slovenskej Republiky

6.5.1.2 HODNOTENIE PROJEKTU SKR

6.5.1.2.1 TECHNICKÉ HODNOTENIE

6.5.1.2.1.1 Aplikácia konceptu ochrany do hĺbky

6.5.1.2.1.1.1 Zaradenie SKR do úrovní ochrany do hĺbky

SKR MO34 boli priradené k rôznym úrovniam ochrany do hĺbky (DiD) ako je to definované Vyhláškou ÚJD SR č. 50/2006 Z.z. (resp. Vyhláškou ÚJD SR č. 430/2011 Z.z.).

- Systémy SKR normálnej prevádzky v 1. línii sú tie systémy, ktoré zabraňujú prechodu reaktora do oblasti nebezpečných prevádzkových stavov, a ktoré udržujú reaktor v bezpečnej prevádzkovej oblasti. Tento cieľ môže byť dosiahnutý použitím prevádzkových regulátorov, prevádzkových ochrán a blokád, ovládacích a ukazovacích prístrojov, signalizácie a varovných hlásení.

  V architektúre MO34 sú k tejto línii priradené: Prevádzkové systémy.

- Systémy preventívnej ochrany v 2. línii ochrany do hĺbky majú za cieľ znížiť frekvenciu pôsobenia systémov ochrany včasným zistením abnormálnej prevádzky a zregulovaním bloku do normálnej prevádzky podobným spôsobom ako je to u ochrany reaktora, ale menej drsným spôsobom s ohľadom na proces. Do tejto línie patria preventívne ochranné systémy.

- Bezpečnostné systémy (ochranné systémy) v 3. línii ochrany do hĺbky majú za účel riadiť projektovú haváriu (DBA), aby sa dosiahli stabilné a akceptovateľné pohavarijné podmienky takisto v prípade malej pravdepodobnosti zlyhania bezpečnostného systému kvôli poruchám zo spoločnej príčiny.

  Hlavnou vlastnosťou všetkých týchto systémov je vydanie signálu rýchleho odstavenia reaktora.

  Systém aktivácie technických prostriedkov zaistenia bezpečnosti

  Výstupný výkon a perióda reaktora sú vypočítané systémom merania neutrónového toku.).

  Seismický monitorovací systém (SMS) vybavuje bezpečnostné systémy signálmi rýchleho odstavenia (binárne signály), keď sú prekročené príslušné prahové úrovne zrýchlenia pre horizontálne a vertikálne seizmické zrýchlenia.

- Systémy 4. línie majú za úlohu monitorovať a manuálne riadiť nadprojektové havárie.

  Patria sem prostriedky pre styk s operátorm potrebné na vykonávanie monitorovania a manuálneho riadenia pre nasledovné účely:

  - Sledovanie bezpečnostného stavu zariadení bloku vo všetkých stavoch elektrárne
  - Vykonanie ručných zásahov na zariadeniach
  - Možnosť normálnej prevádzky elektrárne v prípade výpadku počítačového informačného a riadiaceho systému
  - Bezpečné odstavenie a udržiavanie bloku v prípade výpadku počítačového informačného a riadiaceho systému.

- 5. línia ochrany je na obmedzenie následkov súvisiacich s radiáciou.

6.5.1.2.1.1.2 Poruchy so spoločnou príčinou medzi líniami ochrany do hĺbky

Porucha so spoločnou príčinou pri systémoch kontroly a riadenia medzi rôznymi líniami ochrany do hĺbky je spôsobená hlavne softvérovými chybami. Aby sa minimalizoval výskyt softvérovej chyby, sú všetky

bezpečnostné platformy, vystavené správnemu procesu verifikácie a validácie, ako je to zdokumentované v príslušných kapitolách POSAR pre jednotlivé systémy (pozrite si kapitoly 6.5.2, 6.5.3).

Avšak, proces verifikácie a validácie vylučuje hlavne softvérové chyby. Aby sa zvýšila robustnosť architektúry systémov kontroly a riadenia MO34 a jeho odolnosť voči CCF, sú medzi rôzne línie ochrany do hĺbky zavedené princípy diverzity a nezávislosti. Princípom diverzity je garantované, že poruchy CCF medzi jednotlivými líniami ochrany do hĺbky sú eliminované. Jednotlivé línie ochrany do hĺbky sú funkčne, fyzicky a elektricky i dátovo nezávislé.

6.5.1.2.1.1.2.1 Diverzita línií ochrany do hĺbky

Diverzita je podstatná pre koncept ochrany do hĺbky, keďže prispieva k nárastu úspešných zásahov príslušných systémov v zainteresovanej línii ochrany do hĺbky. Implementácia softvérovej diverzity je obmedzená iba na línie 1 až 4 ochrany do hĺbky, ktoré sú jedinými bariérami priamo zúčastnenými v ochrane fyzických bariér.

Použitie rôznych platforiem pri rôznych úrovniach ochrany do hĺbky v skutočnosti vytvára dostatočnú diverzitu, aby sa minimalizoval účinok porúch so spoločnou príčinou.

Ako je znázornené takisto v kapitole 6.5.1.1 sú systémy kontroly a riadenia zhotovené na rôznych platformách a technológiách.

6.5.1.2.1.1.2.2 Nezávislosť línií ochrany do hĺbky

Fyzická, funkčná a dátová separácia v architektúre MO34 je zaistená:

- medzi redundanciami (divíziami) bezpečnostných systémov:
    - rôzne redundancie (rovnakého systému) sú nainštalované v rôznych miestnostiach, s oddelenými káblovými trasami
    - výmena dát medzi rôznymi redundanciami (rovnakého systému) nie je dovolená
    - sú použité prepäťové bariéry (napr. oddeľovacie relé, galvanické oddelenie), aby zabránili interferenciám medzi redundanciami.
- Medzi systémami rôznych bezpečnostných kategórií:
    - systémy rôznych bezpečnostných kategórií sú fyzicky nainštalované v oddelených skriniach
    - separácia dát je garantovaná (použitím rôznych technických riešení napr. káble z optických vlákien, oddelenie optickým členom, kvalifikované relé, atď.).
    - systémy rôznych bezpečnostných kategórií sú funkčne nezávislé.
- medzi systémom a jeho diverzitou:
    - systém a jeho diverzita sú inštalované v rôznych skriniach, s oddelenými káblovými trasami
    - výmena dát medzi systémom a jeho diverzitou nie je dovolená
    - sú použité rôzne technické riešenia, napr. prepäťové bariéry, oddeľovacie relé alebo galvanické oddelenie, aby sa zabránilo interferencii medzi systémom a jeho diverzitou.

Z týchto dôvodov je nezávislosť medzi rôznymi líniami ochrany do hĺbky zaistená.

6.5.1.2.1.2 Návrh spoľahlivosti

Okrem vyššie vysvetlených vlastností diverzity a nezávislosti sú všetky platformy implementované v projekte MO34 navrhnuté s mnohými vlastnosťami, ktoré zvyšujú ich spoľahlivosť a dostupnosť (podľa ich bezpečnostnej klasifikácie).

6.5.1.2.1.2.1 Kritérium jednoduchej poruchy

Redundancia komponentov je požadovaná iba pre systémy zaradené do tried A a B v súlade s medzinárodným štandardom IEC 61226.

Pri systémoch zaradených do 4. línie ochrany do hĺbky sa kritérium jednoduchej poruchy aplikuje iba na SICS (kde sa týka pôsobenia akčných členov A alebo B podľa STN IEC 61226) a na PAMS kategórie 1 a kategórie 2.

Pri bezpečnostných systémoch zahrnutých do 3. línie ochrany do hĺbky je kritérium jednoduchej poruchy splnené.

6.5.1.2.1.2.2 Kritérium poruchy so spoločnou príčinou

Kritérium poruchy so spoločnou príčinou podľa štandardu STN IEC 61226 sa aplikuje iba na tie systémy kategorizované ako A, t.j. systémy priradené do 3. línie ochrany do hĺbky.

6.5.1.2.1.2.2.1 Diverzita

Diverzita je použiteľná iba pre bezpečnostné systémy.

6.5.1.2.1.2.2.2 Nezávislosť

Požadovaná fyzická, funkčná a dátová separácia je garantovaná nasledovne:

Funkčné oddelenie neumožňuje interakcie medzi zariadeniami a komponentmi z jednotlivých redundancií systému (t.j. prepäťové bariéry, káble z optických vlákien, galvanické oddelenie) a interakcie medzi zariadeniami a komponentmi redundantných systémov rôznych bezpečnostných kategórií.

Fyzické oddelenie je garantované skutočnosťou, že systémy sú inštalované v rôznych miestnostiach s oddelenými káblovými trasami. Fyzické oddelenie redukuje poruchu so spoločnou príčinou (CCF) pri projektových postulovaných (požiare, explózia, záplava, pád lietadla, teplota, vlhkosť, atď...).

Dátová separácia je garantovaná prenosom dát v jednom smere zo systému vyššej bezpečnostnej triedy do systémov nižšej bezpečnostnej triedy. Pravidlo, že porucha v systéme nižšej dôležitosti nemôže mať dopad na funkčnosť systému s vyššou dôležitosťou je dodržané.

6.5.1.2.1.2.2.3 Ochrana voči interným a externým nebezpečenstvám

Účelom je obmedziť následky nebezpečenstiev (napr. požiaru, záplavy, iného ohrozenia prostredia). Platformy systémov A sú kvalifikované a vhodné z hľadiska odolnosti voči elektromagnetickej interferencii a zemetraseniu. Okrem havárií požadujúcich iniciáciu ochranných zásahov, sú iniciačné udalosti takisto postulované pre ochranný systém. Tieto postulované udalosti (PIE) môžu vyústiť do aktívnej alebo pasívnej poruchy systému. Časť systému, ktorá zostane prevádzkovaná je viac menej ešte postačujúca na účely riadenia havárie.

6.5.1.2.1.2.2.4 CCF spôsobené softvérovými chybami

Softvérové komponenty, ktoré sú nezávislé od konkrétneho nasadenia (operačný systém, prostredie reálneho času, funkčné bloky) sú verifikované v súlade s príslušnými štandardmi (IEC 60 880, DIN ISO 9000-3) a odskúšané typovými testami.

Proces vývoja softvéru a systém vyčerpávajúceho testovania sú kombinované, aby zaistili softvér takej vysokej úrovne kvality, že privodené poruchy softvéru (softvérové chyby a modely postulovaných iniciačných dát) nie sú očakávané.

Na zníženie možnosti aktivácie latentných chýb softvéru) sú použité nasledujúce systémové opatrenia ako sú predpísané štandardom IEC 60880:

- nemenné cyklické spracovanie (pevné cykly) bezpečnostných funkcií
- nemennosť záťaže spracovania a komunikačnej záťaže
- nepoužívanie vonkajších prerušení spôsobených technologickým procesom.

V prípade málo pravdepodobnej poruchy bezpečnostného systému z dôvodu spoločnej príčiny sú dostupné diverzitné systémy podľa paragrafu 6.5.1.2.1.2.2.1.

Podobný prístup bol zavedený pri vývoji platformy pre systém merania neutrónového toku. Softvér bol v skutočnosti vyvinutý tiež podľa požiadaviek medzinárodného štandardu IEC 60880 pre jadrový softvér. Softvér je zhotovený takým spôsobom, že široké autonómne monitorovanie je schopné poskytnúť veľmi vysokú úroveň potenciálnych chýb.

SMS predpokladá bezpečnostný plán podľa štandardu IEC 61508, ktorý je použitý ako plán zaistenia kvality podľa požiadaviek zo štandardu IEC 60880. Verifikácia softvéru je plánovaná pomocou celkového plánu verifikácie a validácie zariadenia a dodatočných základných plánov skúšok pre špecifické položky. Počas vývoja zapisovača silného pohybu MRSK2002 boli všetky požiadavky na verifikáciu softvéru sledovateľné. Väčšina verifikácie softvéru je urobená v rámci typového testu pre kompletné zariadenie (integrovaný softvér a hardvér).

6.5.1.2.1.2.3 Kritérium „bezpečnej poruchy"

Kritérium jednoduchej poruchy vyžaduje, aby v prípade poruchy, nastavení systému nespôsobí falošné zapracovanie a nepriaznivý prechodový proces v technológii.

6.5.1.2.1.3 Havarijná odozva systémov kontroly a riadenia

Ako je predpokladané v PSA sú všetky Postulované Iniciačné Udalosti pokryté systémami patriacimi do 3. línie ochrany do hĺbky.

Postulované Iniciačné Udalosti

Poruchy reaktivity a zmeny rozloženia výkonu
Nekontrolované vyťahovanie skupiny kaziet HRK pri spúšťaní
Nekontrolované vyťahovanie skupiny kaziet HRK na výkone
Neriadený pohyb kaziet HRK
Chybné pripojenie odstavenej cirkulačnej slučky
Vystrelenie kazety z aktívnej zóny

Znižovanie koncentrácie bóru v primárnom chladive v dôsledku chybnej funkcie systému doplňovania a bórovej regulácie
Zníženie prietoku primárneho chladiva
Chybné uzatvorenie jednej hlavnej uzatváracej armatúry v cirkulačnej slučke
Zadretie rotora jedného hlavného cirkulačného čerpadla
Zlomenie hriadeľa na jednom hlavnom cirkulačnom čerpadle
Rôzne kombinácie výpadkov hlavných cirkulačných čerpadiel
Zvýšenie množstva chladiva v primárnom okruhu
Chybné uvedenie HP ECCS reaktora do činnosti počas prevádzky na výkone
Chybná činnosť normálneho systému doplňovania
Zvýšenie odvodu tepla II.O.
Porucha v systéme napájacej vody, ktorá znižuje teplotu napájacej vody
Porucha v systéme napájacej vody, ktorá zvyšuje prietok napájacej vody
Porucha regulácie tlaku v II.O., ktorá vedie k zvýšeniu prietoku pary z SG
Chybné otvorenie SV SG alebo prepúšťacej stanice do atmosféry SDA
Spektrum roztrhnutí parných potrubí vo vnútri alebo mimo ochrannej obálky
Zníženie odvodu tepla II.O.
Porucha systému kontroly a riadenia, ktorá vedie k zníženiu prietoku pary z SG
Strata vonkajšieho elektrického zaťaženia, porucha v systéme napájacej vody
Zatvorenie rýchlouzatváracích ventilov turbíny, prietok napájacej vody je zvýšený
Zatvorenie armatúr na parovodoch
Strata vákua v kondenzátore
Výpadok hlavných napájacích čerpadiel
Strata vnútorných a vonkajších zdrojov elektrického napájania

6.5.1.2.2 BEZPEČNOSTNÉ HODNOTENIE

Bezpečnostné hodnotenie systémov kontroly a riadenia implementovaných na JE MO34 je založené na Bezpečnostnom Návode NS-G-1.3 IAEA [II.15]. Tento návod poskytuje kritériá na hodnotenie v dostatočnom rozsahu.

Implementácia konceptu ochrany do hĺbky

Koncept ochrany do hĺbky je správne implementovaný v architektúre MO34. Ako je uvedené v paragrafe 6.5.1.2.1.1, použitie rôznych platforiem na rôznych úrovniach ochrany do hĺbky vytvára vskutku dostatočnú diverzitu, aby sa minimalizoval účinok porúch so spoločnou príčinou. Navyše je týmto zaistená fyzické, funkčné oddelenie a oddelenie dát medzi redundanciami toho istého bezpečnostného systému, medzi systémami rôznych kategórií a medzi systémom a jeho diverzitou, takisto je zaistená nezávislosť medzi rôznymi líniami ochrany do hĺbky. Preto architektúra I&C, t.j. organizácia systémov kontroly a riadenia odráža politiku ochrany do hĺbky stanovenú v [III-3] a dosahuje požadovanú nezávislosť medzi rôznymi stanovenými líniami ochrany do hĺbky.

Postulované Iniciačné Udalosti (PIE)

Výzvy na všetkých úrovniach ochrany do hĺbky, ktoré sa môžu vyskytnúť, budú rozpoznané pri projektovaní elektrárne a budú zabezpečené navrhované opatrenia, aby zaistili, že požadované bezpečnostné funkcie sú splnené a ciele bezpečnosti môžu byť splnené. Systémy kontroly a riadenia sú vybavené tak, aby snímali začiatok výzvy od PIE a iniciovali zásahy, keď sú potrebné, na splnenie požadovaných bezpečnostných funkcií, a tak zaistili, že medze identifikované v úvodnom projekte nie sú prekročené.

Splnenie technologických požiadaviek a kritériá pre iniciáciu bezpečnostných funkcií boli verifikované deterministickými bezpečnostnými analýzami projektových havárií a nadprojektových havárií.

Projektové požiadavky:

Spoľahlivosť systémov

Pravdepodobnosť poruchy systémov a zariadení kategórie A vykonávať ich funkciu je menšia než 10^{-4} na požiadavku, ako je zdokumentovaná v príslušnej kapitole 6.5.3 a 6.5.2.

Projekt sa takisto stáva robustným použitím zásad redundancie, diverzity, fyzického, funkčného oddelenia a separácie dát v systémoch patriacich do 3. línie ochrany do hĺbky. Takéto opatrenia umožňujú zvýšiť spoľahlivosť I&C funkcií a robustnosť celkovej architektúry, spĺňajúcej kritérium jednoduchej poruchy.

Kritérium jednoduchej poruchy

Toto projektové riešenie zaisťuje súlad jednotlivého systému s kritériom jednoduchej poruchy. Bezpečnostné systémy sú projektované ako redundantné systémy, ktoré zaisťujú, že:

- jednoduchá porucha nespôsobí zlyhanie funkcie systému počas prevádzky, údržby a opravy.
- jednoduchá porucha nespôsobí nesprávnu aktiváciu počas prevádzky, údržby a opravy.

Všetky ostatné systémy v architektúre MO34, na ktoré sa jednoduchá porucha aplikuje, zaisťujú správnu implementáciu konceptu redundancie a nezávislosti.

Avšak, kritérium jednoduchej poruchy je aplikované takisto na systémy kategorizované podľa IEC 61226 v architektúre MO34 ako kategória C.

Diverzita

Diverzita v systémoch kontroly a riadenia je princíp monitorovania rôznych parametrov použitím rôznych technológií, rôznych logík alebo algoritmov alebo rozličných prostriedkov pôsobenia, aby bolo poskytnutých niekoľko spôsobov detekovania a reagovania na významnú udalosť. Diverzita je splnená pri systémoch kategórie A . Diverzita nie je vykonávaná automatickou cestou.

Kvalifikácia

Systémy dôležité pre bezpečnosť sú schopné vykonávania ich bezpečnostných funkcií, keď je to požadované pri normálnej prevádzke, externých udalostiach a očakávaných prevádzkových podmienkach a pri podmienkach projektových havárií a po nich.

Úspešná kvalifikácia každého hardvérového a softvérového komponentu je dokladovaná certifikátom alebo hodnotiacou správou, vrátane príslušnej konfigurácie a identifikácie. Komponenty hardvéru a softvéru TXS použité v aplikáciách bezpečnostných systémov kontroly a riadenia projektu JE Mochovce pre bloky 3 a 4 sú popísané spolu s príslušnými skúšobnými certifikátmi v prehľade dát špecifických pre Mochovce v dokumente [I.29].

Spoľahlivosť softvéru

Spoľahlivosť softvéru je založená na kvalitatívnom hodnotení berúc do úvahy zložitosť projektu, kvalitu verifikácie, validácie a testovania procesu vývoja cez široký rozsah vstupných podmienok a spätnú väzbu prevádzkových skúseností.

Platformy sú vyvinuté tak, aby sledovali požiadavky predpísané Medzinárodným Štandardom IEC 60880 a boli podrobené prísnemu a zdokumentovanému procesu verifikácie a validácie a plánu kvality. Softvéry implementujú všetky potrebné nástroje autodiagnostiky potrebné na identifikáciu výskytu poruchy na jednotlivom systéme.

Rozhranie človek-stroj

Pre systémy dôležité pre bezpečnosť sú potrebné efektívne rozhrania človek-stroj, aby vybavili operátora presnými, kompletnými a aktuálnymi informáciami o stave elektrárne a umožnili správnu prevádzku systémov riadených pomocou systémov kontroly a riadenia.

Kedykoľvek je detekovaná porucha, je operátor okamžite informovaný. HMI elektrárne v tejto kapitole nie je hodnotený (pozrite si kapitolu 05.06), ale je taký, že operátor:

- spozná okamžite indikáciu poruchy a rozlíši ju z iných prevádzkových indikácií;
- rozhodne sa či prijať manuálny zásah, aby uviedol elektráreň do bezpečného stavu;
- identifikuje systémy, ktoré sa týkajú príslušného personálu údržby.

Všetky tieto zásahy prispievajú k robustnosti architektúry a implementácie samotného princípu ochrany do hĺbky, najmä na úrovni 1 ochrany do hĺbky. Pri ostatných úrovniach je automatizácia taká, že všetky rozhodnutia operátora sú redukované. Ak nastane havária, operátor je vedený podľa samotných nástrojov HMI v procese na vykonanie rozhodnutia.

Testovanie

Testovanie počas prevádzky poskytuje zaistenie toho, že systémy dôležité pre bezpečnosť zostanú prevádzkovateľné a schopné vykonávania ich bezpečnostných úloh. Frekvencia testov je stanovená na základe požiadaviek na dostupnosť a spoľahlivosť systému. Testovanie systémov dôležitých pre bezpečnosť je na JE EMO34 možná počas prevádzky a takisto počas odstávok.

Komunikačné linky

Komunikačné linky spĺňajú súhrnné špecifikácie požiadaviek na výkonnosť pri všetkých požadovaných podmienkach pre elektráreň.

Architektúra a technológia komunikačných liniek zaisťujú, že požiadavky na nezávislosť medzi systémami sú splnené. Okrem fyzickej separácie a elektrického oddelenia projekt zahrňuje opatrenia na zaistenie toho, že problémy s komunikačnými linkami nepoškodia moduly spracovania.

Komunikačné linky zahrňujú opatrenia na kontrolovanie prevádzky komunikačných zariadení a integrity prenášaných dát.

Redundancie komunikačných liniek sú vybavené tak, aby sa vyrovnali s poruchami.

Dodávatelia systémov a komunikačných liniek aplikujú zásady a princípy, ktoré sú už uplatnené v aplikáciách. Nezávislá V&V nepreukázala rozpory so štandardmi.

Komunikačné linky SKR sú podrobne popísané v jednotlivých kapitolách PpBS.

Systémy kontroly a riadenia kategórie A JE MO34 spĺňajú požiadavky štandardov STN IEC 61513, STN IEC 61226 a Špecifikácie požiadaviek pre systémy kontroly a riadenia tlakovodných reaktorov vlastníkov JE „EUR“.

LITERATÚRA

I Zdrojové dokumenty, ktoré sú vo vlastníctve SE, a.s.

[I.1] POSAR EMO 1, 2 arch. No. 254/97 Sign.5986 as of 12.12.1997 rev.01.00

[I.2] TP/6011 Systém SIS

[I.3] Špecifikácia RPS ;

[I.4] Zoznam vstupných signálov ESFAS;

[I.5] Zoznam výstupných signálov ESFAS;

[I.6] I&C Function Specification for Unit 3 ESFAS (Level 3);

[I.7] Design Concept for PICS Screens of RPS, RLS and PAMS/SAMS; 1

[I.8] Generická analýza vhodnosti : Platforma Teleperm XS ;

[I.9] Plán verifikácie a validácie pre hlavný SKR;

[I.10] Špecifikácia SKR;

[I.11] Popis systému SICS ;

[I.12] Prioritné riadenie pohonov;

[I.13] Design Concept for Reactor Protection Panel;

[I.14] Koncept prevádzky a bezpečnosti bezpečnostného SKR;

[I.15] Koncept signalizácie poruch a výstrah systémov založených na TXS;

[I.16] Revize a dopracováni Úvodního projektu pro MO34;

[I.17] Maintenance and periodic test concept;

[I.18] Koncept galvanického oddeľovania;

[I.19] SICS Panel Layout;

[I.20] Koncept napájania hlavného SKR;

[I.21] Koncept zberu , úpravy a rozvodu signálov a ošetrenie výstupných signálov bezpečnostného SKR;

[I.22] Support document for justification of CAS deviations to EMC concept;

[I.23] Evaluation of the uncertainty for RTS,DRTS and ESFAS signals for safety analysis;

[I.24] 3LP/1001 Limity a podmienky bezpečnej prevádzky;

[I.25] RPS. Spoľahlivostná analýza;

[I.26] Spoľahlivostná analýza kombinácie rôznych SKR;

[I.27] Plán kvality vybraného zariadenia pre systém reaktorovej ochrany , fáza projektovania;

[I.28] DPS3.11.01 Čistiaca stanica drenážnych vôd I.O. - Nádrže - Zoznam potrubných trás,

[I.29] I&C equipment qualification documents “QN101” for the safety I&C system components,

[I.30] EXCORE - Pravdepodobnostné hodnotenie spoľahlivosti a bezpečnosti dodaného systému - DPS 3.10.01

[I.31] 3TP/6001 Systém skupinového a individuálneho riadenia HRK RRCS a systém RTB,

II Legislatívne dokumenty (zákony, vyhlášky, normy, dokumenty MAAE, apod.)

[II.1] Rozsah a obsah bezpečnostnej správy, ÚJD SR, Bratislava, 11/2008

[II.2] Format and Content of the Safety Analysis Report for Nuclear Power Plants, IAEA Safety Standards Series No. GS-G-4.1, Vienna, 5/2004

[II.3] Vyhláška ÚJD SR č.430/2011 o požiadavkách na jadrovu bezpečnosť

[II.4] Vyhláška ÚJD SR č.431/2011 o systéme manažérstva kvality

[II.5] Vyhlášku ÚJD SR č. 58/2006 Z.z. ktorou sa ustanovujú podrobnosti o rozsahu, obsahu a spôsobe vyhotovenia dokumentácie jadrových zariadení potrebnej k jednotlivým rozhodnutiam

[II.6] IEC 61508-1-7 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1-7

[II.7] STN EN 61226 : 2009 Nuclear power plants - Instrumentation and control systems important to safety - Classification of instrumentation and control functions

[II.8] IEC 62340 Nuclear power plants-Instrumentation and control systems important to safety-Requirements for coping with common cause failure (CCF)

[II.9] STN IEC 61513 Jadrové elektrárne. Meranie a regulácia systémov dôležitých pre bezpečnosť. Všeobecné požiadavky na systémy

[II.10] IEC 61225 : 2005 Nuclear power plants - Instrumentation and control systems important to safety - Requirements for electrical supplies

[II.11] IEC 60987 : 2007 Nuclear power plants- Instrumentation and control important to safety - Hardware design requirements for computer -based systems

[II.12] IEC 60880 : 2006 Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions

[II.13] Zákon NR SR č. 541/2004 Z.z. o mierovom využívaní jadrovej energie (Atómový zákon) a o zmene a doplnení niektorých zákonov

[II.14] Format and Content of the Safety Analysis Report for Nuclear Power Plants, IAEA Safety Standards Series No. GS-G-4.1, Vienna, 5/2004

[II.15] IAEA Safety Standards Series - Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Guide no. NS-G-1.3

[II.16] BNS I.1.2/2014 Rozsah a obsah bezpečnostnej správy, ÚJD SR, Bratislava, 01/2014

[II.17] Rozhodnutie ÚJD SR č. 267/2008 Pripomienky k rozsahu a obsahu PBS pre MO34

[II.18] Vyhláška ÚJD SR č. 50/2006 Z. z., ktorou sa ustanovujú podrobnosti o požiadavkách na jadrovú bezpečnosť jadrových zariadení pri ich umiestňovaní, projektovaní, výstavbe, uvádzaní do prevádzky, prevádzke, vyraďovaní a pri uzatvorení úložiska, ako aj kritériá pre kategorizáciu vybraných zariadení do bezpečnostných tried

[II.19] Vyhláška ÚJD SR č. 56/2006 Z. z., ktorou sa ustanovujú podrobnosti o požiadavkách na dokumentáciu systému kvality držiteľa povolenia, ako aj podrobnosti o požiadavkách na kvalitu jadrových zariadení, podrobnosti o požiadavkách na kvalitu vybraných zariadení a podrobnosti o rozsahu ich schvaľovania

III Zdrojové dokumenty, ktoré sú spravidla vytvorené VUJE, a.s. (a nie sú v I. a II. skupine)

[III.1] Technologické zadanie pre ochranné systémy RTS, ESFAS a limitačný systém RLS, DMO/022/2901/T/F0/S

[III.2] Legislatíva, licencovanie a normatívne požiadavky vo vzťahu k dozorným orgánom, DMO/022/2902/T/F0/S

[III.3] Kategorizácia systémov SKR a požiadavky na kvalifikáciu,

[III.4] Priradenie systémov SKR do línií ochrany do hĺbky,

[III.5] Koncept fyzického, funkčného a dátového oddelenia,

[III.6] Koncept riadenia akčných orgánov,

[III.7] Koncept zberu a spracovania signálov,

[III.8] Koncept napájania vo všetkých úrovniach riadenia a ovládania,

[III.9] PNM34067032 Amendment No. 0012 EMC Concept

[III.10] Celková koncepcia a návrh štruktúry SKR,

[III.11] Systém ochrany reaktora,

[III.12] Systém zaistenia bezpečnosti (ESFAS),

[III.13] Výkonové vypínače AO (RTS) BREAKERe,

[III.14] Podporné T-H analýzy pre „Technologické zadanie pre ochranné systémy RTS, ESFAS a limitačný systém“ vypracované pre MO34.

[III.15] Kapitola 06.05.02 Systém automatických ochrán reaktora (RTS/DRTS, EXCORE, SMS, RTB)

[III.16] Kapitola 06.05.03 Systém zaistenia bezpečnosti ESFAS

[III.17] Kapitola 06.05.04.01 PAMS/QDS

[III.18] Kapitola 06.05.04.02 SAMS/QDS

[III.19] Kapitola 06.05.04.03 Systém monitorovania vodíka

[III.20] Kapitola 06.05.06.04 Prevádzková diagnostika I.O.

[III.21] Kapitola 06.05.06.05 Chemický monitorovací systém - CHDIS

[III.22] Kapitola 06.05.05.01 Počítačový informačný a riadiaci systém - PICS

[III.23] Kapitola 06.05.05.02 SICS

[III.24] Kapitola 06.05.05.03 Systém skupinového a individuálneho riadenia HRK - RRCS

[III.25] Kapitola 06.05.05.04 Automatický regulátor výkonu reaktora - RCS

[III.26] Kapitola 06.05.05.05 Limitačný systém reaktora - RLS

[III.27] Kapitola 06.05.05.06 Systém vnútroreaktorovej kontroly - Incore

[III.28] Kapitola 06.05.05.07 Systém riadenia procesov - PCS (SAS1, SAS2, PAS)

[III.29] Kapitola 06.05.06.01 Regulátory I.O.

[III.30] Kapitola 06.05.06.02 Regulátory II.O.

[III.31] Kapitola 06.05.06.03 Riadiaci a ochranný systém TG

[III.32] Kapitola 06.05.09 Havarijné podporné strediská - HRS