

Technická správa

Predprevádzková bezpečnostná správa

Kapitola 06.05.05.07 Systém riadenia procesov -
PCS (SAS1, SAS2, PAS)

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	
			Language / Jazyk	S	Safety Class / Bezpečnostná trieda	nie	SEC. INDEX / INDEX utajenia	Company use/P	
			Submitted to Client to / Predložené odberateľovi na:	Approval / Schválenie	x	Information Only / Len na informáciu			
EPS No / Číslo EPS: PNM34361068			Revision index / Index revízie: 06		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: PNM34361068		A4	6.01	RS	Z	8	
 * P N M 3 4 3 6 1 0 6 8 0 6 *				Sheet / List	Of / z		Plant System / Systém elektrárne	Component / Komponent	
				1	27				

SE Contract No. / Číslo zmluvy SE: 4600003952				VUJE Contract No. / číslo zmluvy VUJE: 1719/00/09			
Part name / Označenie časti: PNM3436106806_S_C00_V				Issued on / Vydané dňa: 05.08.2019			
Kód citlivosti ¹⁾ / Sensitivity code ¹⁾	3	Name / Meno	Organization / Organizácia	Dept. / Útvar	Date / Dátum	Signature / Podpis	
Author / Vypracoval:			VUJE a.s.	0530	05.08.2019		
Co-author / Spolupracoval:							
Checked by / Kontroloval:			VUJE a.s.	0520	05.08.2019		
Verified by / Overil:			VUJE a.s.	0720	05.08.2019		
Approved by / Schválil:			VUJE a.s.	1703	05.08.2019		

Tento dokument je vlastníctvom Slovenských elektrární, a.s.. Tento dokument, ako aj informácie z neho, môžu byť použité, kopírované, rozmnožované alebo zverejňované iba so súhlasom Slovenských elektrární, a.s.. Uvedené riešenie je obchodným tajomstvom VUJE, a.s..

This document is property of Slovenské elektrárne, a.s. This document as well as information it contains can only be used, copied, reproduced or published with consent of Slovenské elektrárne, a.s. The solution presented is trade secret of VUJE, a.s.

Revision record / Záznam o revízii

Identification / Identifikácia (part/page/chapter/ member/section) (časť/strana/kapitola/ článok/odstavce)	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	• PNM3436106806_S_C00_V	• 06
2.	• Textová časť	• PNM3436106806_S_C01_V	• 06
3.	•	•	•
4.	•	•	•
5.	•	•	•
6.	•	•	•
7.	•	•	•
8.	•	•	•
9.	•	•	•
10.	•	•	•
11.	•	•	•

OBSAH

ÚVOD.....	5
ZOZNAM SKRATIEK.....	6
6.5.5.7 SYSTÉM RIADENIA PROCESOV - PCS (SAS1, SAS2, PAS)	7
6.5.5.7.1 POPIS SYSTÉMU PCS.....	7
6.5.5.7.1.1 Účel systému.....	7
6.5.5.7.1.2 Popis konštrukcie a funkčnosti.....	7
6.5.5.7.1.2.1 Bezpečnostné funkcie	8
6.5.5.7.1.2.2 Bezpečnostná a seizmická kategorizácia	8
6.5.5.7.1.2.3 Popis systému	8
6.5.5.7.1.2.4 Systémové funkcie	11
6.5.5.7.1.2.5 Elektrické napájanie	11
6.5.5.7.1.3 Činnosť obsluhy.....	12
6.5.5.7.1.4 Popis prevádzkových stavov.....	12
6.5.5.7.1.4.1 Normálne prevádzkové stavy bloku	12
6.5.5.7.1.4.2 Abnormálne prevádzkové stavy bloku	12
6.5.5.7.1.4.3 Normálne prevádzkové stavy PCS systému	13
6.5.5.7.1.4.4 Abnormálne prevádzkové stavy PCS.....	13
6.5.5.7.1.5 Detailné prvky projektu.....	14
6.5.5.7.1.5.1 Dispozičné riešenie	14
6.5.5.7.2 TECHNICKÉ HODNOTENIE SYSTÉMU	14
6.5.5.7.2.1 Požiadavky na vybrané zariadenia	14
6.5.5.7.2.2 Seizmická odolnosť	15
6.5.5.7.2.3 Princípy bezpečného projektovania	15
6.5.5.7.2.3.1 Kritérium jednoduchšej poruchy.....	15
6.5.5.7.2.4 Kritérium poruchy so spoločnou príčinou	16
6.5.5.7.2.4.1 Diverzita	16
6.5.5.7.2.4.2 Nezávislosť.....	16
6.5.5.7.2.5 Kritérium bezpečnej poruchy.....	16
6.5.5.7.2.6 Analýza spoľahlivosti.....	17
6.5.5.7.2.7 Preukázanie kvalifikácie systému	17
6.5.5.7.3 BEZPEČNOSTNÉ ZHODNOTENIE.....	18
LITERATÚRA	22
ZOZNAM OBRÁZKOV.....	26
ZOZNAM TABULIEK	27

ÚVOD

Kapitola POSAR 6.5.5.7 je vypracovaná v súlade so: Zákonom ÚJD SR č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (Atómový zákon), Vyhláškou ÚJD č. 31/2012 Z. z, BNS I.1.2/2008 a, IAEA Safety Standards Series No. GS-G-4.1.

Kapitola PpBS 6.5.5.7 je vypracovaná v súlade s bezpečnostným návodom ÚJD SR BNS I.1.2/2008 [II.1], pričom bolo prihladené k novému platnému návodu BNS I.1.2/2014 [II.18] (v primeranom rozsahu).

Pri vypracovaní predmetnej kapitoly PpBS boli súčasne zohľadnené aj pripomienky k PBS uvedené v rozhodnutí ÚJD SR č. 267/2008 [II.19].

Dokumenty spoločnosti Siemens AG pre vypracovanie tejto bezpečnostnej správy uvádzajú ako zdroj Vyhlášku ÚJD SR č. 50/2006 Z.z.

Dokumenty spoločnosti Siemens AG pre vypracovanie tejto bezpečnostnej správy uvádzajú ako zdroj Vyhlášku ÚJD SR č. 56/2006 Z.z.

Kapitola sa zaoberá technickým popisom a posúdením bezpečnosti Technologického riadiaceho systému PCS.

ZOZNAM SKRATIEK

AP	Automatizačný Procesor
CCF	Porucha so Spoločnou Príčinou
CP	Komunikačný Procesor
CPS	Centrálna Čerpacia Stanica
CPU	Centrálna Jednotka Spracovania
ECR	Núdzová Dozorňa
EEPS	Systém Núdzového Napájania (vlastnej spotreby)
EMC	Elektromagnetická Kompatibilita
ESFAS	Systém Aktivácie Technických Prostriedkov Zaistenia Bezpečnosti
FDPS	Systém požiarnej detekcie a ochrany
FUM	modul funkcie
HMI	rozhranie človek - stroj
HW	hardvér
IAEA	Medzinárodná agentúra pre atómovú energiu
IEC	Medzinárodná elektrotechnická komisia
I&C	Systém Kontroly a Riadenia
MCR	Bloková Dozorňa
NPP	Jadrová Elektrárň
PACS	Systém Prioritného Riadenia Pohonov
PAS	Systém Automatizácie Procesov
PCS	Počítačový Riadiaci Systém Elektrárne
PICS	Technologický Informačný Riadiaci Systém
POSAR	Predprevádzková bezpečnostná správa
RCS	Systém Riadenia Výkonu Reaktora
RLS	Systém Obmedzenia Výkonu Reaktora
RPS	Systém Ochrany Reaktora
RRCS	Systém Riadenia Regulačných Kaziet Reaktora
RTS	Systém Rýchleho Odstavenia Reaktora
SAS	Bezpečnostný Automatizačný Systém
SCALANCE	Ethernetový spínač
SICS	Bezpečnostný Informačný a Riadiaci Systém
SKR	Systém Kontroly a Riadenia
SJZ	Systém Jednotného Značenia
STD	Sprievodná technická dokumentácia
STN	Slovenská Technická Norma
TCS	Systém Riadenia Turbíny
TPS	Ochranný Systém Turbíny
ÚJD SR	Úrad Jadrového Dozoru Slovenskej Republiky

6.5.5.7 SYSTÉM RIADENIA PROCESOV - PCS (SAS1, SAS2, PAS)

6.5.5.7.1 POPIS SYSTÉMU PCS

6.5.5.7.1.1 Účel systému

Hlavné úlohy PCS spočívajú v získavaní nameraných hodnôt a informácií ohľadne stavu technológie, vo vykonávaní funkcií otvorenej a uzavretej slučky a v riadení technologických akčných členov najmä počas normálnej prevádzky, keďže je priradený do prvej línie ochrany do hĺbky. Avšak, ak je systém vhodný, jeho použitie môže byť rozšírené takisto pre vyššie línie ochrany do hĺbky.

PCS je projektovaný so SAS a PAS, aby poskytol možnosť riadiť technologické procesy elektrárne počas nábehu, prevádzky na výkone, zmene zaťaženia s vysokou bezpečnosťou a dostupnosťou a s minimálnymi nákladmi na prevádzkový personál.

Rozdelenie medzi SAS a PAS je kvôli rôznej bezpečnostnej kategorizácii funkcií, ktoré vykonávajú. PAS nevykonáva bezpečnostné funkcie, zatiaľ čo SAS vykonáva bezpečnostné funkcie. Teda SAS je rozdelený do dvoch podsystémov SAS1 a SAS2

Pre veľmi málo prípadov neriadených pomocou ESFAS, keď sú požadované bezpečnostné funkcie, sú použité moduly prioritnej logiky (PACS). Počas normálnej prevádzky PCS je klasifikácia BT II dostatočná nato, aby boli splnené jeho funkcie

Systémy, ktorých automatizácia je založená na PCS, sú napr. RCS, PICS, SICS, regulátory primárneho a sekundárneho okruhu, systém regulácie a ochrany turbogenerátorov. Kvôli ich dôležitosti sú popísané a hodnotené v samostatných kapitolách.

6.5.5.7.1.2 Popis konštrukcie a funkčnosti

Systém riadenia technologického procesu je rozdelený na tri hlavné úrovne:

- úroveň riadenia bloku
- úroveň riadenia skupiny
- úroveň individuálneho riadenia.

Riadenie skupiny sa používa vždy, keď prvky ovládania podriadenej podskupiny musí byť riadené automatickými príkazmi. Riadenie každej skupiny riadi dve až štyri podskupiny, ktoré spoločne riadia celý technologický systém. Riadenie skupiny je možné zapnúť a vypnúť v pracovnom okne na displeji bloku v PICS. Keď bolo riadenie skupiny zapnuté, je možné navoliť program pre nábeh alebo odstavenie. Riadenie skupiny potom zapne ovládanie príslušnej podskupiny pre jej nábeh alebo odstavenie v súlade s príslušnými kritériami.

Pomocou týchto kritérií a možností predvoľby je možné robiť rozhodnutia:

- koľko riadení podskupín musí nabehnúť alebo sa musí odstaviť a kedy
- ovládanie, ktorej podskupiny musí nabehnúť ako prvé.

Ak sa ovládanie podskupiny zastaví z dôvodu poruchy, ovládanie skupiny sa prepne na podskupinu v rezerve.

Rozloženie procesno-technických funkcií a hierarchická štruktúra sa odráža v usporiadaní hardvéru PAS/SAS.

Toto znázorňuje princíp konfigurácie SKR, vrátane SAS a PAS pre projekt MO34 (použiteľný aj pre druhý blok).

SAS a PAS sú realizované pomocou automatizačného systému. Oba SAS a PAS sú poskytnuté v divíziách 1,2,3 a N aj pre jadrový ostrov a pre konvenčný ostrov [I.8].

SAS je ďalej rozdelený na dva podsystémy za účelom oddelenia riadenia funkcií kategórie B (SAS1) od riadenia funkcií kategórie C (SAS2).

Základná štruktúra SAS a PAS má redundantné automatizačné procesory (AP) a neredundantné funkčné moduly (FUM), ktoré môžu byť poskytnuté v redundantnej konfigurácii (aby sa zvýšila spoľahlivosť systému) v prípade veľmi kritických aplikácií. Popis je uvedený v ďalšom.

6.5.5.7.1.2.1 Bezpečnostné funkcie

PCS je zaradený do 1. línie ochrany do hĺbky, aby vybavil operátorov so všetkými informáciami a radiáciami prostriedkami potrebnými na prevádzku a monitorovanie elektrárne.

PCS sa zúčastňuje na riadení reaktivity a odstránenia tepla z aktívnej zóny.

6.5.5.7.1.2.2 Bezpečnostná a seizmická kategorizácia

Bezpečnostná kategorizácia klasifikácia je stanovená vo Vyhláške ÚJD č. 50/2006. Seizmická klasifikácia je stanovená v IAEA Safety Standards Series NS-G-1.6 Seismic Design and Qualification for Nuclear Power Plants [II.13].

Zariadenia systému PCS sú navrhnuté, skonštruované, dodané a inštalované v zmysle vyhlášky ÚJD SR č. 50/2006 [II.17] a v súlade s dokumentom „Zoznam vybraných zariadení pre 3. blok MO34 a spoločné zariadenia 3. a 4. bloku - textová časť“ [I.40] a príslušnými Plánmi kvality vybraných zariadení pre dané zariadenia systému PCS, vydanými na základe zákona č. 541/2004 Z.z. [II.21], resp. v dobe odovzdania platnej vyhlášky ÚJD SR č. 56/2006 [II.22].

Po uplynutí platnosti prechodného ustanovenia uvedenom vo vyhláške ÚJD SR č. 430/2011 Z.z. (viď [II.3], §7 "Prechodné ustanovenie", t.j. 31.12.2014) je v platnosti §3 „Kategorizácia vybraných zariadení do bezpečnostných tried" predmetnej vyhlášky (t.j. ÚJD SR č. 430/2011 Z.z. [II.3]).

Na základe vyhlášky ÚJD SR č. 430/2011 Z.z. [II.3], §3, resp. Príloha č.1 a Príloha č.3, pre vybrané zariadenia systému PCS nie sú žiadne dodatočné požiadavky v porovnaní s vyhláškou ÚJD SR č. 50/2006 [II.17].

Z uvedeného a s odvolaním na obsah a konštatovania kap. 6.5.5.7.1.2.1 vyššie vyplýva, že zariadenia PCS požiadavky platnej vyhlášky ÚJD SR č. 430/2011 Z.z. [II.3] (t.j. po uplynutí prechodného ustanovenia, viď §7 „Prechodné ustanovenie“ platné do 31.12.2014), spĺňajú.

Funkčné kritérium EMC celého PCS je A alebo B, v závislosti na vykonávanej funkcii.

Systém spĺňa normálne prevádzkové podmienky v miestnostiach SKR, kde sú umiestnené komponenty PAS a SAS, sú uvedené v [I.27]

6.5.5.7.1.2.3 Popis systému

PCS je tvorený štyrmi časťami podľa divízií (1,2,3,N). Každá z týchto častí je zložená z PAS, SAS1 a SAS2.

Štruktúra SAS

System SAS obsahuje: - automatizačné procesory AP(A) a AP(B)

- redundantné komunikačné procesory,
- priemyselné stočené dvojlinky
- priemyselný Ethernet prepínač
- . SAS zbernicu
- pár komunikačných procesorov CP.

Aby sa takisto garantovala nezávislosť, zbernica SAS nemá žiadne fyzikálne prepojenie na žiadne iné zbernicové systémy alebo na akékoľvek iné komponenty s výnimkou príslušných automatizačných systémov SAS.

Preto ako bolo už vysvetlené, zbernica SAS nemá žiadne priame prepojenie s blokovou zbernicou alebo sieťou ostrovnej zbernice a žiadny komponent nižšej bezpečnostnej triedy nie je pripojený na zbernicu SAS, signály kategórie B sú plne oddelené od nižšie kategorizovaných signálov, ako aj signály kategórie C sú plne oddelené od nekategorizovaných signálov.

Rozhrania SAS s inými systémami

Rozhranie so SICS

Výmena signálov medzi SAS a SICS sa vykonáva cez pevne nadržované prepojenia. Moduly FUM sú použité na rozhranie s ovládacími, ukazovacími zariadeniami a zariadeniami výstražnej a havarijnej signalizácie na SICS.

Rozhranie s PICS

Výmena signálov medzi SAS a PICS je realizovaná cez optickú zbernicu bloku. Jednotka spracovania PU na PICS, ktorý je pripojený k zbernici bloku spracováva a rozdeľuje údaje medzi PICS a SAS.

Rozhranie s PAS

Ak sú signály zo SAS vyžadované v PAS, výmena signálu je vykonaná cez optickú zbernicu bloku. V prípade potreby by mohla byť realizovaná cez nadržované prepojenia.

Ak sú signály z PAS vyžadované v SAS, prenos signálu je vykonávaný cez pevne nadržované spojenie medzi modulmi FUM v PAS a FUM modulmi v SAS.

Rozhranie s PACS

Výmena signálov medzi SAS a PACS sa vykonáva cez priame optické prepojenie medzi automatickými procesormi SAS a PACS.

Rozhranie s RPS

Prenos signálu je vykonávaný pevne nadržovanými prepojeniami medzi modulmi RPS a FUM modulmi v SAS.

Rozhranie s RLS

Prenos signálu je vykonávaný pevne nadržovanými prepojeniami medzi modulmi RLS a FUM modulmi v SAS.

Rozhranie s TCS/TPS

Výmena signálov medzi PICS a TCS/TPS je vo všeobecnosti realizovaná cez optickú blokovú zbernicu a gateway (CM104). Signály z ochrán a ďalšie dôležité signály z TCS/TPS do SAS budú pevne nadráťované.

Rozhranie s meraniami, akčnými členmi a rozvádzačmi (úroveň 0)

Prepojenie ku komponentom poľa na úrovni 0 (napr. pohony, binárne spínače, prevodníky) je pevne nadráťované a vedené z FUM modulov cez svorky v skrini do ranžirovacej skrine a odtiaľ na zariadenie poľa.

Štruktúra PAS

System SAS obsahuje: - redundantné automatizačné procesory AP(A) a AP(B)

- redundantné komunikačné procesory,
- - priemyselné stočené dvojlinky
- oddelujúci priemyselný Ethernet prepínač

Rozhrania PAS s inými systémami**Rozhranie so SICS**

Výmena signálov medzi PAS a SICS sa vykonáva cez pevne zapojené prepojenia. FUM moduly slúžia k prepojeniu s ovládacími, signalizačnými zariadeniami a zariadeniami výstražnej a havarijnej signalizácie na SICS.

Rozhranie s PICS

Výmena signálov medzi PAS a PICS je pomocou zbernice bloku z optických vlákien. PU na PICS, ktorý je pripojený k zbernici bloku spracováva a rozdeľuje údaje medzi PICS a PAS.

Rozhranie so SAS

Výmena signálov medzi PAS a SAS sa vykonáva pomocou zbernice bloku z optických vlákien. Tieto signály môžu byť v prípade potreby pevne zapojené.

Rozhranie s PACS

Výmena signálov medzi PAS a PACS sa vykonáva cez priame optické spojenie medzi PAS automatizačnými procesormi a PACS.

Rozhranie s RPS

Môže byť požadovaný prenos signálu medzi RPS a PAS (v prípade, že signál už nie je požadovaný v SAS). V takom prípade sa prenos signálu vykonáva cez pevne zapojené spojenie medzi modulmi RPS a FUM modulmi PAS.

Rozhranie s RLS

Môže byť požadovaný prenos signálu medzi RLS a PAS. V takom prípade sa prenos signálu vykonáva cez pevne nadráťované spojenie medzi modulmi RLS a FUM modulmi PAS.

Rozhranie s TCS/TPS

Výmena signálov medzi PAS a TCS/TPS sa vo všeobecnosti robí cez blokovú zbernicu z optických vlákien a gateway (CM104). Signály z ochrán a ďalšie dôležité signály budú pevne nadráťované.

Rozhranie so snímačmi, pohonmi a rozvádzačmi (úroveň 0)

Výmena signálov medzi PAS a zariadeniami na úrovni 0 sa vykonáva cez pevne zapojené spojenie medzi zariadením Úrovne 0 a FUM modulmi PAS.

Rozhranie s FDPS

Z FDPS je vydávaný signál cez „suchý“ (beznapäťový) kontakt v FDPS, ktorý preruší silové napájanie požiarnej klapy cez napájacie obvody alebo cez pomocné obvody.

6.5.5.7.1.2.4 Systémové funkcie

SAS a PAS získavajú namerané hodnoty a informácie o stave technológie, vykonávajú funkcie riadenia v otvorenej a v uzavretej slučke a ovládajú technologické akčné členy.

SAS a PAS sú naprojektované tak, aby pracovali počas normálnych prevádzkových podmienok, ale môžu byť použité pri všetkých podmienkach elektrárne, ak sú dostupné.

6.5.5.7.1.2.5 Elektrické napájanie

Koncept elektrickej časti a systémov pomocného napájania MO34 je popísaný v kapitole 06.06 - Elektrické napájanie [I.37].

V kapitole sú stanovené:

- Spoločné a základné princípy riešení systémov pomocného napájania JE
- Požiadavky zákazníka na elektrické napájanie (popis údajov a hodnôt)
- Popis schémy systému pomocného napájania JE - Zdroje a siete systému pomocného napájania a ich funkcií/prevádzkových režimov

Koncept riešenia napájania SKR je popísaný v „[I.17].

Požiadavky na napájanie a údaje o elektrickom zaťažení skrine napájania SKR sú popísané v dokumente [I.18].

Napájanie skriň PAS/SAS

Systémy SAS/PAS sú napájané z príslušného systému zaisteného elektrického napájania (EEPS) ako akčné členy riadené pomocou nich.

Napájanie prevádzkového SKR na úrovni 0

Polná inštrumentácia a skrine PAS/SAS, ktoré sú k nim pripojené, patria k rovnakému systému napájania.

Polná inštrumentácia pripojená a napájaná z príslušných analógových alebo binárnych vstupných modulov PAS/SAS nainštalovaných v priestoroch elektronických zariadení, v ktorých je vždy zachované oddelenie po systémoch. Výstupy sú chránené proti skratu, prepätiu a proti preťaženiu.

Miestne riadiace pracoviská

Napájanie spotrebičov SKR na tejto úrovni je zabezpečené z miestneho napájacieho prívodu 230 V AC..

6.5.5.7.1.3 Činnosť obsluhy

Činnosť obsluhy PCS počas normálnej prevádzky pozostáva z pozorovania údajov, prehliadok a periodického testovania v termínoch určených príslušným prevádzkovým predpisom. Okrem týchto činností je zariadenie prevádzkované bez obsluhy.

Počas projektových havárií a abnormálnych prevádzkových podmienok prevádzkový vykonáva činnosti na PCS, ak je dostupný, vrátane pozorovania signalizácie bezpečnostných panelov a potvrdzovania alarmov.

Každý komponent riadiaceho systému má na doske svoj vlastný diagnostický softvér. Tento je neoddeliteľnou štandardnou súčasťou systémového softvéru a nepotrebuje žiadnu prídavnú konfiguráciu/programovanie. Zistené poruchy vždy vedú k predvídateľným, definovaným stavom príslušného komponentu a v prípade redundancie k prepnutiu na pohotovostný komponent. Závady sú automaticky označené a archivované ako signalizácia SKR v prevádzkovom a monitorovacom systéme PICS.

Poruchy týkajúce sa modulov v skrini sú tiež signalizované miestne prostredníctvom poruchovej kontrolky na prednom paneli modulu. Pre rýchle privedenie obslužného personálu na miesto poruchy je rozsvietená kontrolka na príslušnej skrini.

Okrem toho je obsluha nasmerovaná k poruche na dohliadacom diagnostickom systéme pre všetky komponenty riadiaceho systému .

V prípade vzniku poruchy PCS obsluha vyvolá zásah údržby. Podmienky na prevádzku bloku sú špecifikované v Limitách a Podmienkach [1.25].

6.5.5.7.1.4 Popis prevádzkových stavov

6.5.5.7.1.4.1 Normálne prevádzkové stavy bloku

SAS

Počas normálnej prevádzky je SAS v normálnych prevádzkových podmienkach. Automatické funkcie, ako aj funkcie ručného ovládania a monitorovacie funkcie SAS cez PICS sú plne dostupné.

V prípade nefunkčnosti PICS počas normálnej prevádzky (kvôli vnútorným chybám v PICS) bude SICS prepnutý do aktívneho stavu, aby riadil a monitoroval elektrárňu na obmedzený čas v prevádzke so stavom na ustálenom výkone, ak nemôže byť dosiahnuté obnovenie funkcie PICS, aby uviedol blok a udržal ho v odstavenom stave. Automatické funkcie SAS sú od stavu PICS nezávislé. Funkcie manuálneho ovládania a monitorovania SAS potrebné v tomto prípade, ak existujú, sú priamo pripojené k SICS.

PAS

Počas normálnej prevádzky je PAS vystavený bežným prevádzkovým podmienkam. Automatické funkcie, ako aj manuálne ovládanie a monitorovacie funkcie PAS cez PICS sú plne k dispozícii.

V prípade nefunkčnosti PICS počas normálnej prevádzky (z dôvodu vnútornej chyby v PICS) sa SICS prepne do aktívneho stavu pre riadenie a monitorovanie bloku po obmedzenú dobu v stave ustálenej výkonovej prevádzky, a ak nie je možné dosiahnuť obnovenie PICS, pre odstavenie bloku a udržiavanie ho v odstavenom stave. Automatické funkcie PAS sú od stavu PICS nezávislé. Funkcie manuálneho ovládania a monitorovania PAS potrebné v tomto prípade, ak existujú, sú priamo pripojené k SICS.

6.5.5.7.1.4.2 Abnormálne prevádzkové stavy bloku

SAS

PCS, a teda aj SAS1, SAS2 sú v úvodnom projekte zaradené do prvej línie ochrany do hĺbky, čo znamená normálnu prevádzku, ale tieto môžu byť použité takisto v inej línii ochrany do hĺbky (ak je to vhodné). Pokiaľ sú hraničné podmienky počas abnormálnych podmienok a havarijných podmienok bloku identické s normálnymi prevádzkovými podmienkami, SAS môže byť stále v normálnom prevádzkovom stave systému.

Manuálne funkcie SAS, ktoré sú v tomto prípade potrebné, ak nejaké sú, sú dostupné cez SICS.

V prípade straty programovateľných regulátorov v SAS nebude regulácia k dispozícii. Regulácia bloku sa bude vykonávať pomocou SICS a PACS.

PAS

Počas všetkých abnormálnych podmienok prevádzky bloku je PAS v stave normálnej prevádzky systému. Pokiaľ je PICS prevádzkyschopné, k dispozícii sú všetky funkcie manuálneho a automatického ovládania a monitorovania PAS.

V prípade nefunkčnosti PICS pri abnormálnych podmienkach (prechodové javy) a haváriách, sa SICS prepne do aktívneho stavu na podporu zmiernenia dôsledkov po poruche. Manuálne funkcie PAS potrebné v tomto prípade, ak existujú, sú prístupné cez SICS. Automatické funkcie PAS potrebné v tomto prípade, ak existujú, sú od prevádzkyschopnosti PICS nezávislé.

V prípade výpadku programovateľných regulátorov nebude PAS k dispozícii. Riadenie bloku sa bude vykonávať prostredníctvom SICS a PACS.

6.5.5.7.1.4.3 Normálne prevádzkové stavy PCS systému

Počas normálnych prevádzkových podmienok SAS/PAS vykonáva navrhnuté aplikačné funkcie podľa funkčnej špecifikácie technologického zadania:

- riadenie v uzavretej slučke,
- sekvenčné riadenie,
- riadenie v otvorenej slučke,
- funkcie zberu údajov,
- funkcie riadenia pohonov,
- funkcie signalizácie a informačné funkcie.

Pravidlá priority pre funkcie SKR vykonávané pomocou SAS/PAS sú zaistené návrhom systémového softvéru a návrhom aplikačného softvéru. Vzhľadom na logiku priority implementovaných v softvérových funkčných blokoch, majú príkazy ochrany systému alebo komponentu vyššiu prioritu, ako automatické príkazy a automatické príkazy majú vyššiu prioritu než manuálne príkazy.

6.5.5.7.1.4.4 Abnormálne prevádzkové stavy PCS

SAS

Z dôvodov spoľahlivosti automatizačné procesory s ich vysokou koncentráciou implementovaných funkcií pracujú v 2-redundantnej štruktúre (hlavná konfigurácia/konfigurácia horúcej rezervy).

V prípadoch, kde by jednoduchá porucha na I/O úrovni v SAS viedla k významnému poklesu dostupnosti bloku, sú implementované logiky výberu s meracími kanálmi rozloženými v rôznych I/O moduloch.

V prípade poruchy so spoločnou príčinou (CCF), ktorá by viedla k stavu celkového výpadku SAS, budú vyššie klasifikované SKR zaisťovať bezpečné stavy elektrárne.

Systémové rozdelenie funkcií a použitie viacnásobných meracích kanálov v rámci systému spolu s priradením priorít príkazov medzi rôznymi SKR zaistí, že porucha v rámci SAS nepovedie k havarijnej udalosti, dokonca aj počas údržby a/alebo periodickej skúšky. Potrebné projektové opatrenia sú vykonané v rámci funkčných požiadaviek daných z technologického zadania.

Rozdelenie funkcií po systémoch a použitie viacnásobných meracích kanálov v rámci systému spolu s priradením priorít príkazom medzi rôznymi SKR zaistí, že bezpečnostné funkcie kategórie B môžu byť vykonané pomocou SAS, hoci aj v prípade vzniku jednoduchšej poruchy. Potrebné projektové opatrenia sú vykonané v rámci funkčných požiadaviek vyplývajúcich z technologického zadania.

PAS

Z dôvodov spoľahlivosti automatizačné procesory s ich vysokou koncentráciou implementovaných funkcií pracujú v 2-redundantnej štruktúre (hlavná konfigurácia/konfigurácia horúcej rezervy).

Jednoduchá porucha zariadenia na úrovni I/O modulu PAS je preto obmedzená na jednu divíziu zo strojných a technologických systémov. V prípadoch, keď by jednotlivé zlyhanie na I/O úrovni v PAS viedlo k značnému poklesu disponibility bloku, implementované sú logiky výberu s meracími kanálmi rozloženými v rôznych I/O moduloch.

Bezpečný stav bloku v prípade CCF, ktoré by viedlo k úplnej strate PAS, zabezpečia vyššie klasifikované systémy SKR.

6.5.5.7.1.5 Detailné prvky projektu

6.5.5.7.1.5.1 Dispozičné riešenie

SAS

Systém SAS je inštalovaný v HVB v miestnostiach elektroniky.

Polná inštrumentácia je umiestnená v blízkosti zariadenia, ktoré riadi v priestoroch HVB.

PAS

Systém PAS je inštalovaný v HVB v miestnostiach elektroniky.

Polná inštrumentácia je umiestnená v blízkosti zariadenia, ktoré riadi v priestoroch HVB.0

6.5.5.7.2 TECHNICKÉ HODNOTENIE SYSTÉMU

6.5.5.7.2.1 Požiadavky na vybrané zariadenia

Všetky zariadenia PCS sú zaradené medzi vybrané zariadenia v zmysle Vyhlášky ÚJD SR č. 50/2006 [II.17]. Na úrovni vykonávacieho projektu sú požiadavky na vybrané zariadenia uvedené v PLKVZ [I.22] v plnej miere splnené.

Pre všetky vybrané zariadenia je preukázané, že ich výroba, dodávka, montáž spĺňajú požiadavky definované v príslušnom pláne kvality viažucemu sa ku konkrétnemu komponentu použitému v projekte. Použité štandardy, normy a predpisy platné pre projektovanie jadroveoenergetických zariadení sa vzťahujú na materiály, postup výroby a kontroly počas výroby a v etape prevádzky.

Splnenie požiadaviek plánu kvality je dokladované v STD pre príslušné zariadenie.

6.5.5.7.2.2 Seizmická odolnosť

Komponenty SAS sú zaradené do seizmickej kategórie 1a [I.20]. Nasledujúce požiadavky sú definované v dokumente S041200004T - WP 04.1 Koncepcia bezpečnej prevádzky jadrovej elektrárne [I.23]:

- Systémy a komponenty zaradené do seizmickej kategórie 1a si musia zachovať plnú funkčnosť počas a/alebo po zemetrasení.

Komponenty PAS sú zaradené do seizmickej kategórie 1a a 2a a sú primerane kvalifikované [I.1]. Nasledujúce požiadavky sú definované vo - WP 04.1 Koncepcia bezpečnej prevádzky jadrovej elektrárne [I.18]:

- Systémy a komponenty zaradené do seizmickej kategórie 1a si musia zachovať plnú funkčnosť počas a po zemetrasení.
- Stabilita objektov zaradených do seizmickej kategórie 2a musí byť počas a po zemetrasení zachovaná. Sú umiestnené tak, aby nedošlo k poškodeniu žiadneho zariadenia s vyššou seizmickou klasifikáciou.

6.5.5.7.2.3 Princípy bezpečného projektovania

6.5.5.7.2.3.1 Kritérium jednoduchkej poruchy

SAS

Plnenie kritéria jednoduchkej poruchy pre SAS systém nie je požadované.

Pri SAS1 je funkčnosť realizovaná pomocou redundantných a oddelených prostriedkov (usporiadanie divízie), ako je to definované pre kategóriu B podľa STN IEC 61226 [II.7].

Vlastnosti redundancie sú implementované vo všetkých poskytovaných redundantných komponentoch systému, kedy je možné vykonávať údržbu počas výkonnej prevádzky a môžu byť vymenené počas prevádzky bez dopadu na prevádzku bloku.

Oddelenie vo vnútri SAS je dosiahnuté vo viacerých úrovniach:

- odlišne kategorizované funkcie sú vytvorené v rôznych systémoch (v SAS1 resp. SAS2);
- redundantné systémy sú inštalované v rôznych protipožiarnych oddeleniach a napájané rôznym EEPS
- komunikačné prostriedky sú oddelené (pri zberniciach SAS1 a SAS2)
- rošty AP a FUM majú rôzne poistky
- komunikačné procesory a prepojenia sú oddelené

Pokiaľ ide o SAS2, kritérium jednoduchkej poruchy nie je aplikované na komponenty alebo systémy kategórie C podľa IEC 61226 [II.7]. Napriek tomu sú v návrhu SAS implementované vlastnosti redundancie aj pre komponenty a systémy kategórie C. Existujúca redundancia technologických systémov je ďalej zachovaná návrhom SAS.

PAS

Plnenie kritéria jednoduchkej poruchy pre PAS systém nie je požadované. Napriek tomu sú v návrhu PAS implementované funkcie redundancie z dôvodov disponibility. Existujúca redundancia prevádzkových

systémov je ďalej zachovaná návrhom PAS. Samostatnosť podsystémov PAS rôznych systémov je dosiahnutá:

- inštaláciou v rôznych požiarňoch úsekoch a použitím rôznych systémov napájania,
- oddelenými komunikačnými prostriedkami

6.5.5.7.2.4 Kritérium poruchy so spoločnou príčinou

6.5.5.7.2.4.1 Diverzita

U PCS nie sú žiadne požiadavky na diverzitu.

6.5.5.7.2.4.2 Nezávislosť

PCS je funkčne nezávislý a oddelený od konštrukcií a komponentov SKR vyššej bezpečnostnej triedy.

Projekt a výroba komponentov SAS sú realizované podľa predpisov aplikovateľných pre systémy a komponenty zariadení triedy B a C.

Oddelenie vo vnútri PCS je dosiahnuté vo viacerých úrovniach:

- odlišne kategorizované funkcie sú vytvorené v rôznych systémoch (v SAS1 resp. SAS2);
- redundantné systémy sú inštalované v rôznych protipožiarňoch oddeleniach a napájané rôznym EEPS
- komunikačné procesory sú oddelené
- rošty AP a FUM majú rôzne poistky
- komunikačné procesory a prepojenia sú oddelené

Najmä SAS zbernice sú oddelené zbernice použité pre prenos signálov rozdielných kategórií medzi dvomi automatizačnými systémami SAS nezávisle na tom, v ktorej divízii sú umiestnené. Všetky signály medzi automatizačnými procesormi SAS1 sú prenášané cez zbernicu SAS1. Všetky signály medzi automatizačnými procesormi SAS2 sú prenášané cez zbernicu SAS2.

Aby bola zaručená nezávislosť, zbernica SAS nemá žiadne fyzické prepojenie na žiadne iné zbernicové systémy alebo na žiadne iné komponenty s výnimkou príslušných systémov SAS.

Konkrétne, oddelená SAS zbernica je redundantná zbernica s dvomi nezávislými optickými linkami. Použitím tejto štruktúry je dosiahnuté, že systém je tolerantný voči jednoduchej poruche. Pretože zbernica SAS nemá žiadne priame prepojenie na blokovú zbernicu alebo sieť ostrovných zberníc a žiadny komponent nižšej bezpečnostnej triedy nie je pripojený na zbernicu SAS, je dosiahnuté úplné oddelenie kategórie C od nižšie kategorizovanej komunikácie, ako aj úplné oddelenie kategórie C od nekategorizovanej komunikácie,

Pre PCS systém nie je požadované plnenie kritéria poruchy so spoločnou príčinou.

Aby bolo možné oddeliť funkcie rôznych kategórií, je SAS rozdelený do dvoch podsystémov: SAS 1 (ovládanie funkcií kategórie B) a SAS 2 (ovládanie funkcií kategórie C). Redundantné komponenty z jedného podsystému sú namontované do tej istej skrine, ale fyzické oddelenie nie je požadované.

6.5.5.7.2.5 Kritérium bezpečnej poruchy

Pri systémoch SAS a PAS kritérium bezpečnej poruchy nie je uplatňované.

Skúšobný interval pre testovanie PCS je rovnaký ako pre príslušný akčný člen alebo kratší.

SAS je podrobený periodickému testovaniu. Periodické testy sú vykonávané v intervaloch špecifikovaných pravdepodobnostnými požiadavkami pre funkčnosťnych kategórie podľa STN IEC 61226 [II.7]. SAS bude testovaný v návaznosti na ovládané mechanické komponenty

Systém podlieha systému normálnej údržby [I.16].

6.5.5.7.2.6 Analýza spoľahlivosti

Spoľahlivosť systému bola hodnotená kvalitatívne ako vhodná [I.26]. Využitie systému nie je spojené s neakceptovateľným nebezpečenstvom. Tieto argumenty sa spoliehajú na nasledujúci dôkaz:

1. Certifikovaný systém kvality dodávateľa systému po celú dobu životného cyklu celej výroby.
2. Použitý prístup tolerancie chyby dodávateľa systému pri projektovaní systému:

Intenzity porúch jednotlivých komponentov SKR boli vypočítané na základe metódy počítania prvkov (parts count method), ktorá sa zakladá na pozorovaných intenzitách porúch bežných elektrických komponentov, Pre získanie očakávanej intenzity porúch modulov boli sčítané publikované intenzity porúch každého komponentu na module. Okrem toho boli pridané intenzity porúch dosiek s plošnými spojmi a každého spojenia (či už zasúvacieho alebo spájkovaného spoju). Prístup počítania prvkov je prediktívny (očakávaná intenzita porúch) a veľmi konzervatívny. Výpočet intenzity porúch bol vykonaný a potvrdený nezávislými odborníkmi ako súčasť typového skúšania pre všetky komponenty riadiaceho systému.

Požadovaná vysoká spoľahlivosť komponentov riadiaceho systému (napr. moduly FUM) je dosiahnutá a overená viacerými kontrolami kvality. Typový test verifikuje funkčnú výkonnosť modulu za normálnych a hraničných podmienok podľa údajových listov a pred uvoľnením na dodávku. Testy vo výrobe sú vykonávané pre každý štandardný modul počas výroby a po výrobe. Nedostatky objavené počas testovania modulov vo výrobe a nedostatky modulov vrátených na opravu sú zaznamenané a vyhodnotené výrobcom, aby sa stanovili intenzity porúch a implementovali nápravné činnosti v prípade viacnásobných nedostatkov.

Spoľahlivosť SAS a PAS je zvýšená redundanciami, i keď tieto redundancie nie sú požadované. Redundancia je implementovaná z dôvodov dostupnosti. Vlastnosti redundancie umožňujú vykonávať údržbu počas výkonnej prevádzky a vymieňať komponenty počas prevádzky bez dopadu na prevádzku bloku.

6.5.5.7.2.7 Preukázanie kvalifikácie systému

Doklady o kvalifikácii a vysvetlenie činností kvalifikácie pre platformu systému SPPT-T2000 sú uvedené v dokumente [I.26] a v jeho prílohách. Prvotné posúdenie platformy riadiaceho systému (hardvérových a softvérových komponentov), na ktorej je postavený PCS, bolo vykonané v rokoch 1999 až 2001 odborníkmi dodávateľskej spoločnosti, ako aj nezávislými odborníkmi, aby bol prijatý dostatočný stupeň dôvery ohľadne aplikácií so vzťahom k bezpečnosti v jadrových elektrárnach.

Doplnkové činnosti kvalifikácie riadiaceho systému boli nezávislými odborníkmi zahájené pre riadiaci systém v roku 2005. Toto hodnotenie bolo vedené s ohľadom na požiadavky jadrových štandardov IEC 61513 [II.9] a IEC 62138 [II.15] pre systémy triedy 2, vykonávajúce aplikácie kategórie B alebo C podľa normy IEC 61226 [II.7].

Kvalifikácia hardvéru riadiaceho systému je ukončená. Všetky skúšky boli vykonané na vyzbrojených skriniach, vrátane pridružených komponentov siete.

Program kvalifikácie prebehol úspešne v súlade s RCC-E (2005) [II.16] a bol rozšírený o konkrétne požiadavky zákazníka, vrátane [I.28], [I.27]

- typových skúšok na overenie vlastností zariadenia/specifikovaných aplikačných údajov
- programu starnutia na overenie robustnosti/správania sa nad stanovenú životnosť
- EMC skúšok
- skúšok seizmického zaťaženia

Na udržanie kvalifikácie riadiaceho systému (hardvér a softvér) bolo v apríli 2009 zahájené všeobecné kvalifikačné hodnotenie vykonané nezávislým úradom .

Platforma riadiaceho systému, ktorá je určená pre použitie aj v jadrových aplikáciách, a ktorá pozostáva z komponentov AS620B (vrátane siete SAS, koncovej zbernice, ako aj blokovej a ostrovnej zbernice, a bola hodnotená ohľadne súladu s príslušnými normami. Softvérové a hardvérové moduly, ako aj charakteristické údaje generického systému AS620B FUM B, vrátane siete SAS, vrátane koncovej zbernice a blokovej a ostrovnej zbernice spĺňajú požiadavky pre vopred vyvinuté platformy systémov IEC 61513, IEC 62138, IEC60987 a IEC 60780, ako aj RCC-E 2005 [II.16].

OM690 vrátane koncovej zbernice a blokovej a ostrovnej zbernice sú použiteľné pre systémy SKR, ktoré plnia funkcie kategórie C podľa IEC 61226 a F2 podľa RCC-E [II.16].

Podsystém AS 620B riadiaceho systému je kvalifikovaný pre aplikácie v systémoch so vzťahom k bezpečnosti v jadrových elektrárnach. Doplnková kvalifikácia hardvéru bola vykonaná.

Seizmická odolnosť riadiaceho systému bola odskúšaná. Použité skúšobné metódy sú plne v súlade s požiadavkami [I.14]. Pre overenie seizmickej odolnosti bola použitá skúšobná metóda trojosového časovej histórie v súlade so štandardom IEC 60980.

Hodnotenia dokazujú, že platforma riadiaceho systému nespĺňa časť požiadaviek na elektromagnetickú kompatibilitu, ktorá je stanovená v[I.21].

Požiadavky na kvalifikáciu pozostávajú zo stanovenia kvalifikačných požiadaviek, preukázania a dokladovania plnenia kvalifikačných požiadaviek v zmysle príslušných plánov kvality. Dokladovanie funkčných vlastností a odolnosti voči prostrediu je preukázané výsledkami typových skúšok. HW a SW sú kvalifikované v súlade s normami určenými pre digitálne SKR a v súlade s požiadavkami na kvalifikáciu.

Kvalifikácia systému PCS je tiež preukázaná na podmienky prostredia, v ktorých je systém umiestnený.

Systém PCS je schopný plniť v projekte stanovené funkcie vo všetkých uvažovaných režimoch, pri seizmickej udalosti, interných vplyvoch (extrémne podmienky pracovného prostredia, letiace predmety, požiare).

6.5.5.7.3 BEZPEČNOSTNÉ ZHODNOTENIE

Požiadavky na bezpečnostné systémy jadrových zariadení sú stanovené v Prílohe č. 3 Vyhlášky ÚJD SR č. 50/2006, časť B, I, L.

Z dôvodov uvedených v kap. 6.5.5.7.1.2.2 vyššie na systém PCS sú uplatňované požiadavky definované vo vyhláške ÚJD SR č. 50/2006 Z.z. [II.17] v prílohe č.3 v časti B/I (posúdenie plnenia požiadaviek platnej vyhlášky ÚJD SR č. 430/2011 Z.z. [II.3] voči požiadavkám vyhlášky ÚJD SR. č. 50/2006 Z. z. [II.17] je uvedené na konci tejto kapitoly).

Hodnotenie bezpečnosti podľa Vyhlášky ÚJD SR č. 50/2006 Z.z. [II.17] Príloha č. 3, časť B, I.:

L. Bezpečnostné a riadiace systémy

(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.

Splnené - Plány kvality sú vypracované pre všetky etapy projektu, počnúc od fázy projektu, cez výrobu a montáž. Funkčnosť systému je testovaná a preskúmaná počas FAT. Systémy sú kvalifikované podľa špecifických kvalifikačných postupov, vyvinutých v súlade s klasifikáciou systému a požiadavkami na systém. Výsledky procesu sú uvedené v dotknutých správach o kvalifikácii [I.27].

(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 dopĺňajúce prostriedky v každej fáze vývoja procesu, so zohľadnením efektívnej metódy analýz a testovania, ako aj stratégie validácie s cieľom potvrdenia požiadaviek na projekt.

Splnené - Požadovaná úroveň spoľahlivosti systému PCS bola dosiahnutá návrhom zodpovedajúcej štruktúry, výberom vhodných HW a SW komponentov. Spoľahlivosť systému bola hodnotená kvalitatívne ako vhodná [I.26].

(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.

Splnené - Celý proces od návrhu cez dodávky, testovanie a zmenový manažment je dokumentovaný v súlade s dokumentáciou kvality s výstupmi v podobe analýz a správ z jednotlivých etáp projektu. Viď kapitola literatúra.

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

Splnené - Podsystem AS 620B riadiaceho systému, na ktorom je založený PCS je kvalifikovaný pre aplikácie v systémoch so vzťahom k bezpečnosti v jadrových elektrárnach. Bola vykonaná doplnková kvalifikácia hardvéru. Seizmická kvalifikácia systému je plne v súlade s požiadavkami [I.14]. Platforma riadiaceho systému nespĺňa časť požiadaviek na elektromagnetickú kompatibilitu [I.21].

(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.

Splnené - Riadiaci systém, na ktorom je postavený aj PCS má bohaté referencie v JE a v priemyselných aplikáciách. Výpočet intenzity porúch bol vykonaný s konzervatívnym prístupom pre všetky komponenty.

(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.

Splnené – PCS je funkčne nezávislý a oddelený od konštrukcií a komponentov SKR vyššej bezpečnostnej triedy. SAS je rozdelený do 2 podsystémov SAS 1 a SAS 2 (ovládanie funkcií roznych kategórií). Oddelená SAS zbernica je redundantná zbernica s dvomi nezávislými optickými linkami. Zbernica SAS nemá žiadne priame prepojenie na blokovú zbernicu alebo sieť ostrovných zberníc a žiadny komponent nižšej

bezpečnostnej triedy nie je pripojený na zbernicu SAS, je dosiahnuté úplné oddelenie kategórie C od nižšie kategorizovanej komunikácie, ako aj úplné oddelenie kategórie C od nekategorizovanej komunikácie,

(12) 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.

Splnené – Systém PCS vykonáva svoju funkciu plne automaticky, bez potreby zásahu operátora. Informácie o činnosti systému sú k dispozícii na paneloch SICS a hlavne v PICS, kde sa vykonáva aj ich archivácia

(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.

Splnené – SAS a PAS získavajú namerané hodnoty a informácie o stave technológie, vykonávajú funkcie riadenia v otvorenej a v uzavretej slučke a ovládajú technologické akčné členy. PCS poskytuje vybrané signály na panely SICS a hlavne poskytuje signály (hodnoty vstupných a výstupných premenných, stavové signály aj alarmy) do PICS, kde môžu byť signály následne prezentované, spracované a archivované.

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

Splnené – Ako je uvedené vyššie, PCS poskytuje vybrané signály na panely SICS a hlavne poskytuje signály (hodnoty vstupných a výstupných premenných, stavové signály aj alarmy) do PICS, kde môžu byť signály následne prezentované, spracované a archivované [I.41], [I.42].

A. Základné požiadavky na jadrovú bezpečnosť

SAS a PAS sú projektované v súlade s požiadavkami zaistenia spoľahlivosti dodržaním odpovedajúcej kategorizácie, odolnosti voči jednoduchej poruche a poruchám zo spoločnej príčiny, redundancie, elektrickej separácie a fyzickej separácie.

V prípade poruchy so spoločnou príčinou (CCF), ktorá by viedla k stavu celkového výpadku SAS, vyššie klasifikované SKR zaistia bezpečné stavy elektrárne. Bezpečné stavy elektrárne v prípade porúch so spoločnou príčinou, ktoré by zapríčinili úplný výpadok PAS, zabezpečia takisto vyššie klasifikované systémy SKR.

Rozdelenie funkcií po systémoch a použitie viacnásobných meracích kanálov v rámci systému spolu s priradením priorít príkazom medzi rôznymi SKR zaistí, že bezpečnostné funkcie kategórie B môžu byť vykonané pomocou SAS, hoci aj v prípade vzniku jednoduchej poruchy.

Na komponenty alebo systémy kategórie C podľa IEC 61226 [II.7] sa kritérium jednoduchej poruchy nevzťahuje. Napriek tomu sú v návrhu SAS implementované redundancie aj pre komponenty a systémy kategórie C.

Komponenty SAS sú zaradené do seizmickej kategórie 1a. Systémy a komponenty zaradené do seizmickej kategórie 1a si musia zachovať plnú funkčnosť počas a po zemetrasení.

Keďže PAS nie je kategorizovaný z pohľadu bezpečnosti, na komponenty a systémy kategórie C podľa IEC 61226 [II.7] sa kritérium jednoduchej poruchy nevzťahuje. Avšak, z dôvodov spoľahlivosti automatizačné

procesory s ich vysokou koncentráciou implementovaných funkcií pracujú v 2-redundantnej štruktúre (hlavná konfigurácia/konfigurácia horúcej rezervy).

PAS je funkčne nezávislý a oddelený od ostatných konštrukcií a komponentov SKR vyššej bezpečnostnej triedy. Komponenty PAS sú zaradené do seizmickej kategórie 1a a 2a. Systémy a komponenty zaradené do seizmickej kategórie 1a si musia zachovať plnú funkčnosť počas a po zemetrasení. Stabilita objektov zaradených do seizmickej kategórie 2a musí byť počas a po zemetrasení zachovaná. Tieto sú umiestnené tak, aby nedošlo k poškodeniu žiadneho zariadenia s vyššou seizmickou klasifikáciou.

Projektové riešenie systému PCS obsahuje požiadavky na kvalifikáciu zariadení tak, aby bola zaručená jeho prevádzkyschopnosť počas celej projektovanej životnosti, vrátane záťaže od okolitého prostredia počas ťažkej havárie a seizmickej udalosti.

Uvedené vlastnosti systému sú potvrdené splnením požiadaviek, obsiahnutých v plánoch kvality.

Riešenie systému PCS je v súlade s požiadavkami na funkcie a signály k nim určené technologickým zadaním.

B. Ochrana do hĺbky

Koncepcia ochrany do hĺbky [III.4] vyžaduje dostatočnú nezávislosť medzi trasami ochrany. SAS je priradený k prvej línii ochrany do hĺbky, ale jeho použitie môže byť rozšírené na iné línie ochrany do hĺbky, ak to je vhodné. PAS je takisto priradený do prvej línie ochrany do hĺbky, ale jeho použitie môže byť rozšírené na iné línie ochrany do hĺbky, ak to je vhodné.

Systémy SKR normálnej prevádzky na 1. línii rutinne zabraňujú prechodu reaktora do oblasti abnormálnych podmienok prevádzkových podmienok a udržiavajú teda reaktor v bezpečnej prevádzkovej oblasti.

Zariadenia PCS spĺňajú všetky požiadavky na funkčnosť, výkonnosť, spoľahlivosť, odolnosť voči prostrediu, zaistenie kvality a riadenie kvality, ktoré sú stanovené [II.7] a súvisiacimi normami. Systém PCS vo fáze vykonávacieho projektu spĺňa kritériá pre riadiaci systém stanovené v prílohe č. 3 časť B, I., L Vyhlášky ÚJD SR č. 50/2006 Z. z.

SAS podľa Vyhlášky ÚJD SR č. 50/2006 Z.z. [II.17] spĺňa bezpečnostnú funkciu III k, podľa Vyhlášky ÚJD SR Regulation č. 430/2011 Z.z. spĺňa bezpečnostnú funkciu III j.

Podľa Vyhlášky ÚJD č. 430/2011 Z.z. nepribudli žiadne nové požiadavky na PCS.

Záverom možno konštatovať, že projekt systému PCS spĺňa všetky požiadavky definované pre riadiaci systém vo vyhláške ÚJD SR č. 50/2006 Z. z., ako aj v súčasne platnej Vyhláške č. 430/2011 Z.z.

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

- [I.1] Popis SKR PAS,
- [I.2] Popis SKR SAS,
- [I.3] SPPA - T2000 Bus System,
- [I.4] Konceptia regulácie s otvorenou slučkou,
- [I.5] Konceptia regulácie s uzavretou slučkou,
- [I.6] Concept for Component Protection,
- [I.7] Konceptia riadenia aktuátora,
- [I.8] Functional Grouping,
- [I.9] Úprava signálov prevádzkového SKR,
- [I.10] Všeobecná konceptia havarijnej signalizácie,
- [I.11] Controls, annunciation and indication principles,
- [I.12] Koncept galvanického oddeľovania,
- [I.13] Zablokovanie jednotlivých HMI (PICS, SICS, MCR, ECR),
- [I.14] Systémy SPPA - T2000 a parameter prostredia,
- [I.15] Criteria for arrangements on desk and panels in the control rooms,
- [I.16] Koncept údržby a periodických skúšok;
- [I.17] I&C Power Supply – Single Line Diagram,
- [I.18] Electrical Load Tables,
- [I.19] Koncept napájania hlavného SKR;
- [I.20] Požiadavky na hodnotenie seizmickej odolnosti konštrukcií, systémov a komponentov JE Mochovce,
- [I.21] EMC concept
- [I.22] Plán kvality vybraného zariadenia pre skrine SICS, PICS, SAS, PAS a RCS (fáza projektovania a výrobná fáza),
- [I.23] WP 04.1 Concept of NPP safe operation,
- [I.24] Zoznam vybraných zariadení pre 3. Blok MO34 a spoločné zariadenia 3. a 4. bloku - textová časť,
- [I.25] 3LP/1001 – Limity a podmienky bezpečnej prevádzky,
- [I.26] Analýza všeobecnej vhodnosti: platformy riadiaceho systému,
- [I.27] Qualification report for control system,

- [I.28] Qualification Report for control system
- [I.29] Kapitola 05.01 Všeobecné ciele, princípy a požiadavky na projekt,
- [I.30] Kapitola 06.05.01.01 Popis celkovej architektúry SKR,
- [I.31] Kapitola 06.05.02 Systém automatických ochrán reaktora (RTS/DRTS, EXCORE, SMS, RTB),
- [I.32] Kapitola 06.05.03 Systém zaistenia bezpečnosti ESFAS,
- [I.33] Kapitola 06.05.05.01 Počítačový informačný a riadiaci systém,
- [I.34] Kapitola 06.05.05.02 Automatický regulátor výkonu reaktora,
- [I.35] Kapitola 06.05.05.05 Limitačný systém reaktora RLS,
- [I.36] Kapitola 06.05.06.03 Riadiaci a ochranný systém TG,
- [I.37] Kapitola 06.06 Elektrické napájanie,
- [I.38] Kapitola 10 Limity a podmienky bezpečnej prevádzky,
- [I.39] DOD 003, Charakteristiky prostredí - sprievodná technická správa,
- [I.40] Zoznam vybraných zariadení pre 3. blok MO34 a spoločné zariadenia 3. a 4. bloku - textová časť,
- [I.41] Safety panel and QDS-screen layout,
- [I.42] Popis SKR systému PICS,
- [I.43] Dodatok č. 52 - Hodnocení bezpečnosti navrhované zmeny podle Vyhl. 431/2011 Z.z. § 9, bod 3, ods. F - Technická správa,

II Legislatívne dokumenty (zákony, vyhlášky, normy, dokumenty MAAE, a pod.)

- [II.1] BNS I.1.2/2008 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 jadrovú 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] IEC 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 fauilure (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] IAEA Safety Standards Series NS-G-1.6 Seismic Design and Qualification for Nuclear Power Plants, IAEA, Vienna, 2003
- [II.14] IAEA Safety Standards Series NS-R-1, Safety of Nuclear Power Plants: Design, Vienna, 2000
- [II.15] IEC 62138:2004 Nuclear Power Plants - Instrumentation and control important to safety - Software aspects for computer-based systems performing category B or C functions
- [II.16] Design and Conception Rules for Electrical Equipment of Nuclear Islands, 2005, AFCEN 2005
- [II.17] 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, vyradovaní a pri uzatvorení úložiska, ako aj kritériá pre kategorizáciu vybraných zariadení do bezpečnostných tried
- [II.18] BNS I.1.2/2014 Rozsah a obsah bezpečnostnej správy, ÚJD SR, Bratislava, 01/2014
- [II.19] Rozhodnutie ÚJD SR č. 267/2008 Pripomienky k rozsahu a obsahu PBS pre MO34
- [II.20] Rozhodnutie ÚJD SR no. 63/2015. Schválenie kategorizácie vybraných zariadení do bezpečnostných tried podľa dokumentov PNM34361188 a PNM34361189
- [II.21] Zákon NR SR č. 541/2004 Z.z. o mierovom využívaní jadrovej energie (Atómový zákon) a o zmene a doplnení niektorých zákonov.
- [II.22] 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,
- [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] Koncept EMC,
- [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] Chapter 05.03 Categorization of the classified equipment into safety classes, VUJE, a. s., Trnava,

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK