

Technická správa

Predprevádzková bezpečnostná správa

Kapitola 06.05.03 Systém zaistenia bezpečnosti
- ESFAS

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
			Submitted 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: PNM34365000		Revision index / Index revízie: 10		Size / Veľkosť	Activity Code / Aktivita	Type / Subtype Typ / Podtyp	Discipline / Profesia
File name / Názov súboru:		SE doc. Code / SE číslo dokumentu: PNM34361053		A4	6.01	RS	Z
 * P N M 3 4 3 6 1 0 5 3 1 0 *				Sheet / List	Of / z	Plant System / Systém elektrárne	Component / Komponent
				1	34		

SE Contract No. / Číslo zmluvy SE: 4600003952				VUJE Contract No. / číslo zmluvy VUJE: 1719/00/09			
Part name / Označenie časti: PNM3436105310_S_C00_V				Issued on / Vydané dňa: 21.08.2019			
Kód citlivosti ¹⁾ / Sensitivity code ¹⁾	3	Name / Meno	Organization / Organizácia	Dept. / Útvar	Date / Dátum	Signature / Podpis	
Author / Vypracoval:			VUJE, a.s.	0530	21.08.2019		
Co-author / Spolupracoval:							
Checked by / Kontroloval:			VUJE, a.s.	0520	21.08.2019		
Verified by / Overil:			VUJE, a.s.	0720	21.08.2019		
Approved by / Schválil:			VUJE, a.s.	1703	21.08.2019		

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/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	• PNM3436105310_S_C00_V	• 10
2.	• Textová časť	• PNM3436105310_S_C01_V	• 10
3.	• Prílohy	• PNM3436105310_S_P01_V	• 10
4.	•	•	•
5.	•	•	•
6.	•	•	•
7.	•	•	•
8.	•	•	•
9.	•	•	•
10.	•	•	•
11.	•	•	•

OBSAH

ÚVOD	5
ZOZNAM SKRATIEK	6
6.5.3 SYSTÉM AKTIVÁCIE TECHNICKÝCH PROSTRIEDKOV ZAISTENIA BEZPEČNOSTI - ESFAS	9
6.5.3.1 POPIS SYSTÉMU	9
6.5.3.1.1 Účel systému	9
6.5.3.1.2 Opis konštrukcie a funkčnosti	9
6.5.3.1.2.1 Bezpečnostná funkcia	10
6.5.3.1.2.2 Bezpečnostná a seizmická klasifikácia	10
6.5.3.1.2.3 Popis systému	10
6.5.3.1.2.3.1 Softvér	13
6.5.3.1.2.3.2 Vizualizácia na BD a ND	13
6.5.3.1.2.3.3 Monitorovanie vstupných signálov	13
6.5.3.1.2.3.4 Monitorovanie stavu pamäti:	14
6.5.3.1.2.3.5 Monitorovanie výstupných signálov	14
6.5.3.1.2.3.6 Systém testovania a diagnostiky	15
6.5.3.1.2.3.7 Archivácia signálov	15
6.5.3.1.2.3.8 Degradácia logika systému ESFAS	15
6.5.3.1.2.3.9 Logika spätnej kontroly (<i>check back logic</i>)	16
6.5.3.1.2.3.10 Vázby ESFAS na ostatné SKR, BD, ND a technológiu	16
6.5.3.1.2.4 Funkcie systému ESFAS	16
6.5.3.1.2.5 Napájanie	16
6.5.3.1.2.6 Činnosť obsluhy	16
6.5.3.1.2.7 Popis prevádzkových režimov ESFAS	18
6.5.3.1.2.8 Dispozičné riešenie a štruktúra systému	18
6.5.3.1.2.8.1 Dispozičné riešenie	18
6.5.3.1.2.8.2 Štruktúra systému a jeho charakteristiky	18
6.5.3.2 TECHNICKÉ HODNOTENIE SYSTÉMU	19
6.5.3.2.1 Požiadavky na vybrané zariadenia	19
6.5.3.2.2 Seizmická odolnosť	19
6.5.3.2.3 Zásady pre bezpečné projektovanie	19
6.5.3.2.3.1 Kritérium jednoduchej poruchy	19
6.5.3.2.3.2 Kritérium poruchy so spoločnou príčinou	20
6.5.3.2.3.3 Diverzita	20
6.5.3.2.3.4 Nezávislosť	21
6.5.3.2.3.5 Kritérium bezpečnej poruchy	21
6.5.3.2.4 Spoľahlivosť analýza	22
6.5.3.2.5 Kvalifikácia systému	22
6.5.3.2.6 Zabezpečenie kvality softvéru	22
6.5.3.3 BEZPEČNOSTNÉ ZHODNOTENIE	24
6.5.3.3.1 Preukázanie plnenia legislatívnych požiadaviek	24
LITERATÚRA	30
ZOZNAM PRÍLOH	34
ZOZNAM TABULIEK	34

ÚVOD

Kapitola bola vypracovaná v súlade s príslušnou legislatívou Zákona č. 541/2004 Z.z. o mierovom využívaní jadrovej energie (Atómový zákon) o doplnení a zmene niektorých zákonov, Vyhlášky č. 31/2012 Z.z. meniacu a doplňujúcu Vyhlášku ÚJD SR č. 58/2008 Z.z., ktorou sa ustanovujú podrobnosti o rozsahu, obsahu a spôsobe vyhotovenia dokumentácie jadrových zariadení potrebnej k jednotlivým rozhodnutiam.

Kapitola PpBS 6.5.3 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.20].

Systém aktivácie technických prostriedkov zaistenia bezpečnosti (ESFAS) je súčasťou systému ochrany reaktora (RPS).

Kapitola vypracovaná na vyššie uvedených dokumentoch pojednáva o bezpečnostnom systéme ESFAS. Táto popisuje stručne systém, jeho architektúru, bezpečnostné funkcie, použité technické prostriedky, softvér a činnosti prevádzkového personálu pri rôznych prevádzkových režimoch. Kapitola hodnotí bezpečnosť a spoľahlivosť z hľadiska architektúry, hardvéru a softvéru na základe dokumentov o vykonaných spoľahlivostných analýzach a medzinárodných štandardoch.

ZOZNAM SKRATIEK

AP	automatizačný procesor riadiaceho systému T-2000
APS	automatika postupného spúšťania
APU	zberná a spracovateľská jednotka
RTS	Systém rýchleho odstavenia reaktora
BD	bloková dozorňa
BREAKER	výkonový vypínač rýchleho odstavenia reaktora
CCF	porucha so spoločnou príčinou
CPU	centrálna jednotka spracovania
CRC	cyklická kontrola redundancií
DG	dieselgenerátor
DPS	dielčí prevádzkový súbor
DRTS	Diverzitný systém rýchleho odstavenia reaktora (Diverse Reactor Trip System)
ECR	núdzová dozorňa
EEPS	systém zaisteného elektrického napájania (Emergency Electric Power Supply System)
ELS	automatika postupného spúšťania (Emergency Load Sequencer)
EMC	elektromagnetická kompatibilita
ESFAS	Systém aktivácie technických prostriedkov zaistenia bezpečnosti (Engineered Safety Features Actuation System)
ESW	technická voda dôležitá (essential service water)
FAT	výrobné preberacie testy
FMEA	analýza príčin a účinkov porúch
GW	Gateway
HCČ	hlavné cirkulačné čerpadlo
HSCHZ	havarijný systém chladenia zóny
HMI	rozhranie človek-stroj
HN	havarijné napájanie
HP	vysokotlakový
HPK	hlavný parný kolektor
HRK	havarijná a regulačná kazeta
HVS	horúce vetvy slučiek
HZ	hermetická zóna
I&C	systém kontroly a riadenia

I.O.	primárny okruh
IAEA	Medzinárodná agentúra pre atómovú energiu
IEC	Medzinárodná elektrotechnická komisia
II.O.	sekundárny okruh
KO	kompensátor objemu
LOCA	havária so stratou chladiva
LP	nízkotlakový
MCR	bloková dozorňa
MI	počítačové komunikačné rozhranie s BD a ND
MO34	Jadrová elektráreň Mochovce, 3. a 4. blok
MSI	počítačové komunikačné rozhranie s APU a VOTER ESFAS
ND	núdzová dozorňa
NPP	jadrová elektráreň
NT	nízkotlaký
OM	prevádzkový a monitorovací systém (operation and monitoring system)
PACS	Systém prioritného riadenia pohonov (Priority and Actuator Control System)
PAMS	Pohavarijný monitorovací systém (Post Accident Monitoring System)
PAS	Systém automatizácie procesov (Process Automation System)
PCS	Systém riadenia procesov (Process Control System)
PG	parogenerátor
PICS	Počítačový informačný a riadiaci systém (Process Information and Control System))
PIE	postulovaná iniciačná udalosť
PRISE	únik primárneho chladiva do sekundárneho okruhu
PROFIBUS	informačná/riadiaca zbernica technologického procesu
PSA	pravdepodobnostné hodnotenie bezpečnosti
PS-A	prepúšťacia stanica do atmosféry
PV	poistný ventil
QAV	rýchločinná armatúra
RCP	hlavné cirkulačné čerpadlo
RLS	Systém obmedzenia výkonu reaktora (Reactor Limitation System)
RPP	panel ochrany reaktora (bezpečnostný panel)
RPS	Systém ochrany reaktora (Reactor Protection System)
RTB	vypínač rýchleho odstavenia reaktora (Reactor Trip Breaker)
RTS	Systém rýchleho odstavenia reaktora (Reactor Trip System)
SAS	Bezpečnostný automatizačný systém (Safety Automation System)

SAT	preberacie skúšky v prevádzke
SFC	kritérium jednoduchkej poruchy
SHN	superhavarijné napájanie
SC	modul na úpravu signálov
SICS	Bezpečnostný informačný a riadiaci systém (Safety Information and Control System)
SMS	Systém monitorovania seizmicity (Seismic Monitoring System)
SU	servisná jednotka
SVE	počítač zberu a spracovania dát
TVD	technická voda dôležitá
ÚJD SR	Úrad jadrového dozoru Slovenskej republiky
UVT	podpäťové vypínanie
VOTER	skriňa výberovej logiky
VT	vysokotlakový

6.5.3 SYSTÉM AKTIVÁCIE TECHNICKÝCH PROSTRIEDKOV ZAISTENIA BEZPEČNOSTI - ESFAS

6.5.3.1 POPIS SYSTÉMU

6.5.3.1.1 Účel systému

Systém aktivácie technických prostriedkov zaistenia bezpečnosti (ESFAS) je súčasťou systémov ochrany reaktorového bloku. Jeho úlohou je identifikácia vzniku havarijných podmienok na reaktorovom bloku a riadenie systémov určených na zmiernenie následkov týchto podmienok, aby sa dosiahol kontrolovaný stav a elektrárň sa udržala v bezpečnom stave.

Udalosti vedúce k vzniku havarijných podmienok sú v projekte elektrárne definované ako postulované iniciačné udalosti PIU. Každá iniciačná udalosť je charakterizovaná prekročením medzí technologických parametrov, ktoré sú spracované systémom aktivácie technických prostriedkov zaistenia bezpečnosti.

ESFAS pracuje automaticky. Ručné ovládanie akčných členov je umožnené z bezpečnostných panelov SICS na BD a ND (po uvoľnení spínača OPDIS) použitím konvenčných ovládacích prvkov zapojených priamo do rozvádzačov alebo jednotky priority riadenia (PACS).

Pre každú iniciačnú udalosť bezpečnostný systém ESFAS spolu s akčnými orgánmi plní konkrétnu bezpečnostnú úlohu (viď kap. 6.5.3.1.2.4, Funkcie, kritériá, pôsobenie a nastavenia ESFAS).

6.5.3.1.2 Opis konštrukcie a funkčnosti

Systém je implementovaný v troch identických a oddelených redundanciách: redundancia V, redundancia W a redundancia X, z ktorých každá je vybavená tromi kanálmi.

Redundancie ESFAS aktivujú BREAKRE po výbere 2 z 3 medzi redundanciami.

Každá redundancia môže byť fiktívne rozdelená na:

- **Úroveň úpravy (SC) a distribúcie signálov**

V tejto úrovni sú zahrnuté SC moduly (pozrite si kap. 6.5.2.2.1.1.2). Na tejto úrovni sú prijímané všetky bezpečnostné premenné veličiny poskytnuté prevodníkmi a snímačmi, diskrétné signály sú upravené a všetky bezpečnostné premenlivé veličiny sú potom prenesené do *úrovne digitálneho spracovania*. Táto úroveň takisto zabezpečuje napájanie pre prevodníky.

- **Úroveň digitálneho spracovania**

V tejto úrovni sú zahrnuté APU a VOTER (pozrite si kap. 6.5.2.2.1.1.2). V tejto úrovni sú konvertované bezpečnostné premenné veličiny (analogové na digitálne), generované a validované sú signály medzí, generované sú počiatkové kritériá a výberová logika) a následne počiatkové signály, ktoré sú následne poskytnuté do úrovne ovládania cez výstupné moduly).

- **Úroveň ovládania**

V tejto úrovni sú zahrnuté relé (rozdávzače) na prerušenie napájania cez BREAKRE a PACS.

Všetky kanály komunikujú cez sieť so zbernicou z optického vlákna. Táto zaisťuje neinteraktívne oddelenie voči prepätiu tak, že porucha jedného podsystému neovplyvní iné podsystémy. Redundancie sú úplne nezávislé a nie je predpokladaná medzi nimi žiadna komunikácia.

ESFAS má rozhrania s nasledujúcimi ostatnými systémami:

- BREAKRE
- SMS a EXCORE
- Bezpečnostné panely v MCR, ECR (SICS)
- Signály z/do poľa cez ranžirovacie skrine

- Prepojenia z MCR/ECR k AV42 (alebo PACS)
- PICS (OM690) cez redundantné gateway-e (GW)

Gateway-e sú realizované takým spôsobom, že tok dát je predpokladaný iba v jednom smere (z ESFAS k prevádzkovému SKR), a že nemôže nastať spätný vplyv.

6.5.3.1.2.1 Bezpečnostná funkcia

ESFAS je zaradený do tretej línie ochrany do hĺbky.

V súlade s vyhláškou ÚJD SR č. 50/2006 Z.z. [II.21] a dokumentom „Zoznam vybraných zariadení pre 3. blok MO34 a spoločné zariadenia 3. a 4. bloku - textová časť“ [I.32] schváleného rozhodnutím ÚJD SR č. 63/2015 [II.19] a taktiež kapitolou 5.3 tejto PpBS [III.15] je systém ESFAS zaradený do BT II.

Systém ESFAS plní špecifickú bezpečnostnú funkciu podľa Vyhlášky č.50/2006 Z.z.:

2b - na odstavenie jadrového reaktora za stavu abnormálnej prevádzky, ktorý by mohol viesť k havarijným podmienkam a na odstavenie jadrového reaktora s cieľom zmierniť následky havarijných podmienok

a podľa ÚJD SR č. 50/2006 Z.z. [II.21] (Príloha 3) spĺňa základné bezpečnostné funkcie:

- reguláciu reaktivity,
- odvod tepla,
- zadržanie rádioaktívnych látok vnútri fyzických bariér,
- reguláciu a obmedzenie množstva a druhu rádioaktívnych látok uvoľnených do životného prostredia.

6.5.3.1.2.2 Bezpečnostná a seizmická klasifikácia

Kategorizácia ESFAS do jednotlivých kategórií bezpečnosti a seizmickej odolnosti podľa vyhlášky

ÚJD SR č.50/2006 Z.z., STN IEC 61226 je v zaradená do BT II a podľa funkcie do triedy A.

Zariadenia systému ESFAS sú navrhnuté, skonštruované, dodané a inštalované v zmysle Vyhlášky ÚJD SR č. 50/2006 [II.21] a v súlade s dokumentom „Zoznam vybraných zariadení pre 3. blok MO34 a spoločné zariadenia 3. a 4. bloku - textová časť“ [I.32] a príslušnými Plánmi kvality vybraných zariadení pre dané zariadenia systému ESFAS [I.27], [I.34], vydanými na základe zákona č. 541/2004 Z.z. [II.13], 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, časť B ods. II, pre vybrané zariadenia systému ESFAS sú dodatočné požiadavky v porovnaní s vyhláškou ÚJD SR č. 50/2006 [II.21], ktoré sú uvedené v kap. 6.5.3.3.

Z uvedeného a s odvolaním na obsah a konštatovania kap. 6.5.3.1.2.1 vyššie vyplýva, že zariadenia ESFAS 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).

ESFAS spĺňa kritériá seizmickej odolnosti triedy 1a podľa návodu IAEA NS-G-1.6 [II.23].

Kritérium EMC podľa EN 61000-6-2 je A [III.9].

Podmienky prostredia pre komponenty ESFAS sú uvedené v [I.3]:

6.5.3.1.2.3 Popis systému

ESFAS je tvorený nasledovnými komponentmi:

- Úprava signálu (SC)

Údaje z technológie a údaje z poľa alebo iných systémov SKR, ako sú SMS, EXCORE, sú získané prostredníctvom skriň SC. Jednotky SC vykonávajú napájanie snímačov/prevodníkov, ako aj štandardizáciu signálov, oddelenie a rozdelenie vstupných signálov pre APU v ostatných bezpečnostných systémoch pre iné systémy SKR alebo blokové dozorne.

Pri SC je takisto aplikovaný princíp troch kanálov pre každú redundanciu.

- Jednotka zberu a spracovania údajov (APU)

Jednotky APU poskytujú zber vstupných signálov ESFAS-u z jednotiek úpravy signálov (SC), vykonávajú ich logické spracovanie.

Akčné signály sú vydávané VOTER-om ESFAS-u ako binárne diskkrétne signály, ktoré sú prenášané k rozvážaču alebo do príslušnej jednotky priority a riadenia (PACS).

- ESFAS VOTER (VO)

Každá redundancia je vybavená VOTER-om. Vo VOTER-och sú medzné parametre vybrané vo výberovej logike 2 z 3 a sú vydané povely na pôsobenie ESFAS-u cez skrine oddelenia a jednotky PACS na akčné členy.

Signály pôsobenia sú spustené VOTER-om ESFAS-u vo forme binárnych diskretných signálov. a prenášaných jednotlivými káblami do rozvážačov (úpravy signálov SC) alebo do príslušnej jednotky riadenia priority a akčných členov (PACS).

- Skrine elektrického oddelenia ESFAS

Pre potrebu elektrického oddelenia ESFAS od PACS sú medzi VOTER-y ESFAS a skrine PACS vložené skrine elektrického oddelenia.

- Rozhranie monitorovania a služieb (MSI)

Všetky APU a VOTER-y ESFAS sú pripojené k počítačom MSI tej istej redundancie. MSI prenáša dáta cez počítače monitorovania (MI) tej istej redundancie z/do príslušných SICS (bezpečnostných panelov). MSI tvorí aj rozhranie k servisnej stanici (SU) príslušnej redundancie, ako aj rozhranie (GW) k PICS..

- Počítače MI-MCR, MI-ECR (Rozhranie monitorovania)

Počítače MI. získavajú vybrané signály z MSI počítačov, ktoré budú zobrazené na signalizačných tabľách bezpečnostných panelov, poskytujúcich informácie o stave ESFAS-u.

Počítač MI zaisťuje takisto vstupy z tlačidiel (potvrdenie signalizácie a vymazanie) umiestnených na bezpečnostných paneloch – RPP.

- Gateway-e (GW)

Gateway-e sú priemyselné PC s polovodičovými diskami, klasifikované podľa ÚJD SR č. 50/2006, do bezpečnostnej kategórie C (podľa IEC 61226).

Na MSI každej redundancie sú pripojené počítače GW, aby sa dosiahla vysoká spoľahlivosť.

- Systém riadenia priority a akčného člena (PACS)

V prípadoch, ak niekoľko systémov SKR posiela akčné signály rôznych bezpečnostných tried na ten istý akčný člen (napr. motor, ventil so servomotorom alebo solenoidový ventil), je zabezpečené riadenie priority riadiaceho povelu cez modul AV-42.

Modul riadenia priority a akčného orgánu AV-42 vykonáva nasledujúce funkcie:

- Riadenie priority,
- Riadenie akčného člena,

- Monitorovanie akčného orgánu.

- Servisná stanica (SU)

Úlohou SU je:

- podpora periodických testov (pozrite si kap. 6.5.2.2.1.3)
- systémová diagnostika
- modifikácia parametrov
- diaľková aktualizácia softvéru počítačov pripojených on-line (uvoľnená použitím hardvérového kľúča).

Počítače SU sú je z pohľadu bezpečnosti neklasifikované zariadenia.

- Vnútorne komunikačné prostriedky

Pre prenos dát medzi jednotlivými APU počítačmi a MSI, medzi MSI a MI, MSI, GW a SU sú implementované štandardné siete.

- Ranžirovacie skrine

Ranžirovacie skrine sú použité na jednotlivé prepojenia signálov od zariadení poľa alebo iných systémov z poľa a späť do poľa.

Ranžirovacie skrine poskytujú možnosť na prepojenie rôznych prevodníkov (napr. dvojvodičových alebo štvorvodičových s napájaním alebo bez napájania) a signálov z iných systémov SKR (EXCORE, SMS) ľahko do skríň signálov úpravy signálov (SC).

Ako je vysvetlené v kap. 6.5.2.2.1.1, ESFAS má trojredundantnú štruktúru s tromi kanálmi v každej redundancii. Tri jednotky zberu a spracovania údajov každej redundancie systému prijímajú analógové signály z troch meracích kanálov, konvertujú ich z analógových na digitálne signály a formujú „medzný signál“. Logické spracovanie signálu rýchleho odstavenia reaktora je preto vykonané vo všetkých APU pre obe diverzity. Výstup z každej APU (pre každú redundanciu obidvoch diverzít) je potom vedený do programovateľných logických modulov z ktorých každý vykonáva výber 2 z 3.

Počítače vydania akčných povelov vydávajú po výbere 2 z 3-och dielčích akčných signálov kanálov ESFAS cez skrine elektrických oddelení akčné signály do jednotiek prioritného riadenia akčných orgánov PACS . Tieto počítače sú konfigurované ako dvojice vedúci / kontrolór (master/checker).

Akčné signály sú v systéme ESFAS tvorené elektrickým nabudením. Každý pohon riadený systémom ESFAS má samostatný modul PACS, ktorý má elektrické rozhranie s elektrickým rozvádzačom pohonu.

6.5.3.1.2.3.1 Softvér

Systémy SKR sú typicky implementované ako distribuované počítačové systémy. Ich funkčnosť je rozsiahle definovaná softvérom.

Systémový softvér môže byť rozdelený na dve základné časti:

- Offline softvér – ktorý slúži na inžiniering, konfigurovanie, verifikovanie, testovanie a údržbu. Tento softvér beží na servisnej stanici alebo na počítači nezávislom od prevádzky elektrárne a nemá priamy vplyv na vykonávanie funkcií SKR.
- Online softvér – ktorý beží v počítačových moduloch systému a priamo vykonáva počas prevádzky funkcie SKR, funkcie komunikácie a úlohy on-line automonitorovania.

On-line softvér sa ďalej delí na:

- užívateľský softvér
- softvér riadenia behu programu a softvér operačného systému

Užívateľský softvér je nástroj, cez ktorý sú realizované inžinierske funkcie. V tomto softvéri sú vytvorené funkčné blokové moduly (predprogramované a kvalifikované moduly, vykonávajúce elementárne SKR funkcie, ako sú AND, OR, 2 z 3, atď.) a sú prepojené vzájomne do funkčných schém SKR. Ku každej funkčnej schéme SKR prislúcha softvérový modul, ku ktorému sú pripojené všetky dotknuté funkčné blokové moduly.

Tieto funkčné schémy sú potom volané do prostredia reálneho času, ktoré je súčasťou softvéru systému reálneho času a softvéru operačného systému. Tento systém preberá starostlivosť o vypracovanie informácií spustením načítavania a kontroly všetkých vstupov, kontrolujúc vykonávanie funkčných schém a dotknutých komunikácií až po výstup vypočítaných výsledkov.

Celý inžiniering je vytvorený v grafickom inžinierskom systéme. Tento systém je databázovo orientovaný projektový systém, ktorý poskytuje všetky práce týkajúce sa projektovania a činnosti systému SKR.

Všetky súčasti online softvéru sa zúčastňujú na inicializácii automatických opatrení, t.j. programy v ceste automatického zásahu sú v princípe vykonávané cyklicky.

Čas každého cyklu, ktorý nie je použitý na vypracovanie výsledkov, je využitý na automonitorovanie s cyklickým automonitorovaním. Cyklické automonitorovanie je softvérový program so špeciálnym účelom na umiestnenie chýb hardvéru SKR. V prípade, že chyba je detekovaná, je okamžite signalizovaná na skriniach a sú prijaté príslušné zásahy.

6.5.3.1.2.3.2 Vizualizácia na BD a ND

Všetky monitorovacie signály a výstrahy sú spracované v MSI a cez gateway-e odosielané do informačného a riadiaceho systému PICS a cez MI BD a MI ND na panely dozorne na prezentáciu operátorom.

. Prezentácia vyššie uvedených varovných hlásení a indikácií je na PICS a bezpečnostných paneloch SICS.

Zobrazenia PICS pre ESFAS

Všetky monitorovacie signály a výstrahy sú spracované v MSI a zaslané do informačného a riadiaceho systému PICS cez gateway.

Signalizácie a informácie o stave indikované na PICS vybavujú operátora s prehľadom o stave bezpečnostného SKR v každom čase.

Zobrazenia PICS sú navrhnuté takým spôsobom, že poznávacia ergonómika operátora je vylepšená a poskytuje úplný prehľad a navedie operátora pomocou signalizácií na vykonanie správnych zásahov.

6.5.3.1.2.3.3 Monitorovanie vstupných signálov

Vstup analógových signálov do ESFAS je monitorovaný z nasledujúceho hľadiska:

- platnosti hodnôt signálov,

- poruchy vstupnej karty,
- prekročenia rozsahu,
- obvodov redundantných analógových vstupných signálov,
- odchýlky signálu od ostatných dvoch (2. Max).

Vstup binárnych vstupných signálov je monitorovaný z hľadiska:

- platnosti hodnôt signálov
- zistenej poruchy vstupnej karty
- zhody redundantných binárnych signálov
- spracovania výberom 2 z 3.

6.5.3.1.2.3.4 Monitorovanie stavu pamäti:

Vybrané spúšťacie signály a ďalšie dôležité stavové signály sú uložené v pamätiach. Zhoda signálov stavu pamäti kanálov je kontrolovaná podobne ako kontrola binárnych signálov (funkčným blokom 2 z 3).

6.5.3.1.2.3.5 Monitorovanie výstupných signálov

Kvôli lepšiemu prehľadu obsluhy sú signály ESFAS z aktívnej cesty (hlavnej automatickej cesty) prechádzajúce cez jednotky VOTER do PACS monitorované prostredníctvom signalizácií a indikačných signálov o stave. Tieto signály sú archivované v PICS (ako jednotlivé signalizácie) a prezentované aj na bezpečnostných paneloch SICS ako skupinové signalizácie.

6.5.3.1.2.3.6 Systém testovania a diagnostiky

Testovanie TXS pozostáva z on-line monitorovania a periodicky vykonávaných testov.

On-line monitorovanie sa vykonáva cyklicky v každej CPU-TXS a V/V kartách a je rozdelené na automatické autotestovanie zabudované v TXS a projektovo stanovené on-line testovanie vstupov, výstupov skriň a roštov.

On-line monitorovanie

Autodiagnostika systému ESFAS je zabezpečená v HW a systémovým SW a nie je potrebné ju projektovať. On-line monitorovanie zahŕňa:

- V/V testy
 - Testy jednotky spracovania
 - Testy komunikácie
 - Ostatné funkcie automonitorovania,
-

Autodiagnostika na úrovni užívateľského návrhu je:

- zabezpečená aplikačným softvérom a
 - hardvérovými opatreniami monitorovania:
- Sumárne hlášky poruchy systému sa prenášajú do BD.

Periodické skúšky

Doplňujúcimi opatreniami k on-line monitorovaniu sú periodické skúšky, ktoré obsahujú:

- Skúšky vstupných kanálov od snímačov alebo iných SKR vstupujúcich do funkčnej schémy
- Skúšky výstupných kanálov od funkčných schém SKR k akčným členom
- Kontrola integrity zavedeného SW na jednotkách CPU
- Kontrola integrity spúšťačích testov na všetkých CPU
- .

6.5.3.1.2.3.7 Archivácia signálov

Archivácia signálov systému ESFAS je riešená prenosom všetkých relevantných signálov (vstupných signálov, spätných hlásení, signálov o stave systému) cez jednotky rozhrania MSI a gateway-e (GW) do systému PICS.

6.5.3.1.2.3.8 Degradáčna logika systému ESFAS

Signály ESFAS majú vždy hodnotu (analogovú alebo binárnu, v závislosti na povahe signálov) a stave príznaku: "CHYBA" alebo "TEST".

Binárne signály sú zvyčajne vyhodnocované vo výbere 2 z 3 a analogové signály sú vyhodnocované a spracované v logike 2.MIN/2.MAX.

Pri binárnych signáloch - ak jeden z týchto signálov nesie stav "CHYBA", potom sa spustí degradačná logika a je vydané hlásenie o chybe. To znamená, že výberová logika je prepnutá z výberu 2 z 3 na výber 1 z 2 a ďalšia porucha degraduje výber na 1 z 1.

Pri analogových signáloch – ak je vyhodnotený ako poruchový jeden signál, to znamená, že tento signál so stavom "CHYBY" nie je v logike 2.MIN/2.MAX viac uvažovaný.

Aby sa vyhlo šíreniu sa poruchového stavu, musí byť každý 3-kanálový vstup validovaný:

- na vstupe každej APU
- na vstupe každého VOTER-a

6.5.3.1.2.3.9 Logika spätnej kontroly (*check back logic*)

Pre najrýchlejšiu signalizáciu poruchy komponentu sú všetky akčné členy, ktoré aktivuje funkcia ESFAS, zoskupené do skupiny podľa ich očakávaného času odozvy. Napr. všetky rýchle akčné členy, ktoré vysielajú spätné hlášky (*check back*) okamžite, sú zoskupené do jednej skupiny, všetky ostatné akčné členy, ktoré majú dlhší čas odozvy do Y sekúnd sú zoskupené v druhej skupine. Po uplynutí vopred definovaného času spätnej hlášky sa vyhodnocuje, či sú ukončené všetky spätné hlášky v príslušnej skupine.

6.5.3.1.2.3.10 Väzby ESFAS na ostatné SKR, BD, ND a technológiu

Väzby ESFAS na ostatné systémy SKR, blokovú dozorňu, núdzovú dozorňu sú znázornené v Prílohe 1 tejto kapitoly, Obr. 6.5.3-4 a 6.5.3-5.

Väzba s technológiou je cez jednotky SC a jednotky riadenia priority a akčných orgánov.

Väzby na bezpečnostné panely blokovej a núdzovej dozorne (RPP panely SICS) sú realizované cez jednotky monitorovania MSI a MI a cez konvenčné drátované prepojenia do jednotiek APU, VOTER a PACS (manuálna iniciácia funkcie ESFAS).

Väzba ESFAS na systémy PAS, SAS a PICS sú realizované cez MSI, komunikačné brány GW a systémovú zbernicu bloku a tiež cez komunikačné prepojenia PROFIBUS medzi jednotkami APU - SAS a APU - PAS.

Servisné stanice SU príslušnej redundancie v prevádzkovej miestnosti a jednotky APU-ESFAS a VOTER-y sú prepojené cez monitorovacie rozhranie MSI.

6.5.3.1.2.4 Funkcie systému ESFAS

Funkcie systému ESFAS sú definované v projekte a sú implementované v systéme SKR pomocou HW a SW vybavenia, tak aby systém plnil svoju funkciu.

6.5.3.1.2.5 Napájanie

Koncept elektrickej časti a pomocné napájanie sú popísané v kap. 6.6 tejto PpBS - Elektrické napájanie [III.17].

V kapitole sú uvedené:

- Spoločné a základné zásady riešení systému pomocného napájania JE
- Požiadavky spotrebiča na elektrické napájanie (popis údajov a hodnôt)
- Popis schémy systému pomocného napájania JE - Zdroje a siete systému pomocného napájania

Koncept napájania SKR je uvedený v [III.18].

6.5.3.1.2.6 Činnosť obsluhy

Systém ESFAS pracuje plne automaticky. Ručné ovládanie akčných orgánov systémom ESFAS je umožnené z panelov (SICS) prostredníctvom konvenčných ovládacích prvkov priamo prepojených na APU ESFAS, VOTER a PACS (jednotku riadenia priority a akčných členov, modul AV42).

Simulované povely

Spravidla sa tieto povely používajú pri činnostiach počas údržby. Tieto povely môžu byť použité aj pri havarijných (núdzových) opatreniach.

Povely generované pomocou ESFAS, RTS, RLS:

Povely z bezpečnostného SKR majú ďalšiu vyššiu prioritu ako povely z prevádzkového SKR a z ručných ovládacích prvkov.

Povely z dohliadacích obvodov AV42:

Spoločne s prioritným modulom je implementovaná aj autonómna ochrana spotrebiča signálmi od momentových spínačov, koncových spínačov, vypnutia ističa a stráženia podpätia.

Prevádzkové povely cez zbernice:

Automatické povely ako napr. skupinové riadenie, riadenie podskupín, riadenie slučiek, ochranné uvoľňovacie/blokovacie logiky, atď. sú implementované do AP a z AP riadiaceho systému sú automaticky prenášané cez rozhranie do modulu riadenia priority.

Ručné povely zo SICS:

Povely generované z prevádzkových SKR a prenášané cez zbernicu (autonómne ochrany zariadení a povely z PCS) majú prioritu nad ručnými povelmi z panelov, kým signál OPDIS nie je aktívny. Manuálne povely z OM majú nižšiu prioritu ako manuálne povely z ovládacích prvkov. Ak OPDIS je aktívny, z hľadiska bezpečnosti sú povely z ovládacích prvkov považované za bezpečnostne relevantné (a preto dostávajú vyššiu prioritu a sú spracovávané v PLD AV42 namiesto procesora).

Aktivovania OPDIS je možné vyvolať prostredníctvom zamknuteľných prepínačov ENOPDIS..

Aktivácia "OPDIS" pozastaví spracovanie signálov od:

- Dohliadacích funkcií prebiehajúcich v samotnej AV42
- Prevádzkového SKR
- Ručných povelov cez OM
- Autonómnych ochrán zariadení cez zbernicu

Ak povel „OPDIS“ nie je nastavený, riadiace povely z ovládacích prvkov pre styk s obsluhou sú spracovávané procesorom rovnakým spôsobom ako prevádzkové povely.

Táto vlastnosť sa zvolila, aby sa splnila požiadavka na vyššiu prioritu pre prípad poruchy ESFAS z Úvodného projektu.

6.5.3.1.2.7 Popis prevádzkových režimov ESFAS

Bezpečnostný riadiaci systém ESFAS je v trvalej prevádzke vo všetkých režimoch bloku. Procesorový modul (SVE2) môže pracovať v troch rôznych prevádzkových režimoch:

- PREVÁDZKA
- TEST
- DIAGNOSTIKA

Prepínanie medzi prevádzkovými režimami je vykonávané zo servisnej stanice (SU). Po zapnutí SVE2 vykonáva inicializáciu, úlohy autotestovania a automaticky je prepnutý do režimu PREVÁDZKA, v ktorom sa v definovanom časovom cykle vykonáva odčítanie vstupných signálov (hardvérovo alebo cez sieť), spracovanie modulov funkčných schém a tvorba výstupných signálov (hardvérovo alebo cez sieť).

- Na zabránenie neautorizovanému prístupu do on-line systému je použité opatrenie registrovaného povolenia prístupu v servisnej stanici (SU)

:Implementácia kľúčových prepínačov, ktoré poskytujú doplňujúce povolenie na zmenu prevádzkových režimov

6.5.3.1.2.8 Dispozičné riešenie a štruktúra systému

6.5.3.1.2.8.1 Dispozičné riešenie

Systém ESFAS a jeho komponenty sú umiestnené v priestoroch HVB podľa projektovej dokumentácie.

6.5.3.1.2.8.2 Štruktúra systému a jeho charakteristiky

Počítačový systém ESFAS pozostáva z troch identických úplne oddelených divízií – redundancií. Každá redundancia je schopná samostatne realizovať všetky bezpečnostné funkcie systému ESFAS.

Počítače zberu a spracovania dát (APU kanálov) každej redundancie prijímajú analógové signály z meracích kanálov, konvertujú ich z analógových na digitálne signály a tie sú po následnej validácii spracované identickým algoritmom v každom kanáli.

Systém ESFAS má dvojúrovňovú architektúru, aby zamedzil vzniku poruchy (validácia signálu merania založená na výbere 2 z 3 (výmena informácií medzi kanálmi) a výber 2 z 3 signálov z kanálov príslušnej redundancie vo VOTER-i).

Logické funkcie systému ESFAS sú implementované a akčné signály sú tvorené v počítačoch VOTER. Spracovanie signálu je realizované pomocou dvojice nezávislých procesorov MASTER a CHECKER.

Diverzita funkcií systému ESFAS je založená na manuálnej iniciácii požadovanej funkcie ESFAS z panelov havarijnej ochrany SICS, eventuálne aj priamym manuálnym ovládaním jednotlivých akčných členov z panelov SICS.

6.5.3.2 TECHNICKÉ HODNOTENIE SYSTÉMU

6.5.3.2.1 Požiadavky na vybrané zariadenia

Plány kvality pre 1. a 2. fázu pre ESFAS boli vypracované v dokumentoch [I.27], [I.34].

Plány kvality obsahujú projektové požiadavky, procesy, postupy a prostriedky použité na dosiahnutie bezpečnosti a kvalitatívne požiadavky podľa štandardov IEC 61513, IEC 61226 a IEC 60880 a jednotlivé požiadavky Vyhlášky ÚJD SR č. 50/2006 Z.z.

Aby boli splnené legislatívne a normatívne požiadavky boli použité nasledujúce vyhlášky, štandardy a príručky:

- Vyhláška ÚJD SR č. 50/2006 Z.z.
- Vyhláška ÚJD SR č. 56/2006 Z.z.
- IEC 61226 Systémy kontroly a riadenia dôležité pre bezpečnosť - Klasifikácia kontrolných a riadiacich funkcií
- IEC 61513 Systémy kontroly a riadenia dôležité pre bezpečnosť - Všeobecné požiadavky na bezpečnosť
- IEC 60987 Systémy kontroly a riadenia dôležité pre bezpečnosť - Požiadavky na návrh hardvéru pre počítačové systémy
- IEC 60980 Doporučená prax pre seizmickú kvalifikáciu elektrických zariadení bezpečnostného systému pre jadrové elektrárne
- IEC 60780 Elektrické zariadenia bezpečnostného systému – Kvalifikácia
- IEC 60880 Systémy kontroly a riadenia dôležité pre bezpečnosť - Softvérové aspekty pre počítačové systémy vykonávajúce funkcie kategórie A
- IAEA Bezpečnostná príručka NS-G-1.6.

Systém ESFAS prešiel takisto cez výrobné preberacie testy (FAT), počas ktorých bola preukázaná správna funkčnosť komponentov ([I.35], [I.36], [I.37]).

6.5.3.2.2 Seizmická odolnosť

Systém ESFAS je klasifikovaný ako seizmicky odolný a je zaradený do seizmickej kategórie 1a podľa NS-G 1.6. Seizmická kvalifikácia je založená na požiadavkách IEC 60980 a zaoberá sa hodnotením komponentov pri prevádzkovom zemetrasení a zemetrasení s úrovňou bezpečného odstavenia (viď [I.8]).

6.5.3.2.3 Zásady pre bezpečné projektovanie

6.5.3.2.3.1 Kritérium jednoduchej poruchy

Systém ESFAS spĺňa kritérium jednoduchej poruchy nasledovným spôsobom:

- Systém ESFAS pozostáva z troch fyzicky a funkčne oddelených redundancií (odolnosť voči jednoduchej poruche systému ESFAS ako celku).
- Každá redundancia pozostáva z troch funkčne oddelených kanálov (odolnosť voči jednoduchej poruche kanálov, obmedzenie falošných zapracovaní).

6.5.3.2.3.2 Kritérium poruchy so spoločnou príčinou

Aby boli zmiernené následky CCF, má systém ESFAS nasledujúce vlastnosti:

- Všetky akčné členy ovládané systémom ESFAS môžu byť ovládané príslušným tlačidlom v paneloch SICS
- Inštalácia troch trojitých kanálových podsystémov RPS v troch fyzicky oddelených redundanciách,
- Nie je tu žiadna výmena signálov medzi podsystémami umiestnenými v troch redundanciách,
- Sieťové prepojenia medzi tromi kanálmi v jednej redundancii sú založené na optických vláknach (zaistujúce neinteraktívne oddelenie voči prepätiam)

Na základe Rozhodnutia ÚJD SR č. 449/2011, Fáza II bola vykonaná deterministická analýza na poruchu so spoločnou príčinou poľnej inštrumentácie.

Predpísaná analýza obsahuje:

- (I) **Overenie správneho zapojenia odberov impulzných potrubí**, t.j. prienik (snímače z rôznych redundancií nesmú byť napájané z rovnakého odberu).

Splnené –Všetky uvažované potrubné odbery a ich usporiadanie zaistujú odolnosť voči poruche so spoločnou príčinou. Ak nastane nesprávna funkcia v jednom odbere, logika odchýlky kanála podnieti signalizáciu odchýlky, avšak pôsobenie RTS a ESFAS nezlyhá, nenastane ani nesprávne pôsobenie RTS ani ESFAS

- (II) **Overenie vedenia signálu cez priechodky kontejnmentu** (napr. v prípade zaplavenia priechodky signály vedené do rôznych redundancií nesmú byť ohrozené).

Splnené –Všetky uvažované hermetické káblové priechodky a hermetické potrubné priechodky zaistujú odolnosť voči poruche so spoločnou príčinou. Snímače z rôznych redundancií sú umiestnené tak, aby oddeľovali hermetickú kobku a signály boli vedené cez nezávislú signálnu cestu. Nie je tu žiadny prepoj medzi redundanciami ako aj kanálmi. Výpadok jednej priechodky spustí signalizáciu odchýlky kanála, avšak pôsobenie RTS a ESFAS nezlyhá, nenastane ani nesprávne pôsobenie RTS ani ESFAS.

- (III) **Overenie izolačnej schopnosti oddel'ovacích armatúr**, napr. 5-cestné ventily, pre snímače diferenciálneho tlaku (v prípade nespoľahlivého oddelenia snímača od drenážneho kolektora 0,9 MPa, výkyvy tlaku v drenážnom kolektore budú ovplyvňovať všetky merania nedostatočne, synchronne)

Splnené –Všetky uvažované meracie obvody sú realizované spôsobom, že každý snímač je oddelený od technologických odberov, ako aj od preplachovacieho a drenážneho kolektora pomocou dvoch odberových ventilov zapojených do série. Toto usporiadanie zaistuje uspokojivé oddelenie od drenážneho kolektora a technologických odberov.

- (IV) **Verifikácia správneho sklonu impulzného potrubia** – ak nie zachovaný sklon, prírodné plyny/vzduch nemôžu byť odstránené prirodzene gravitačnými silami z impulzných potrubí a mohla by nastať systematická chyba.

Splnené –Všetky uvažované meracie obvody sú z dvoch trasovacích typov: typ L101-S (merania hladín v PG, merania hladín v kompenzátore objemu) a P101-S (tlakové merania v parnom kolektore PG, tlakové meranie v primárnom okruhu reaktora). Oba trasovacie typy poskytujú minimálny sklon 5%. Takto je požiadavka splnená.

Detailne je hodnotenie uvedené v dokumente "Bezpečnostné a spoľahlivostné analýzy systému ochrany reaktora JE MO34" [I.30].

6.5.3.2.3.3 Diverzita

Diverzita funkcií ESFAS je realizovaná ručným ovládaním z panelov SICS na pracoviskách operátora.

Aj pri málo pravdepodobnom zlyhaní ESFAS operátor môže manuálne spusti vybranú funkciu z panela ochrany reaktora a ručné ovládanie všetkých bezpečnostných akčných členov z panelov SICS (realizácia podľa kapitoly 6.5.3.1.2.6).

6.5.3.2.3.4 Nezávislosť

Nezávislosť systémov ESFAS je zabezpečená nasledovným spôsobom:

Funkčnou izoláciou, ktorá neumožňuje interferencie medzi zariadeniami a komponentmi jednotlivých redundancií systému ESFAS (galvanickým oddelením, prepäťovými ochranami, použitím optických káblov, optočlenov, oddeľovacích relé, riadením priority v spojení s galvanickým oddelením v AV42, galvanickým oddelením a výberom pri spoločnom využívaní snímačov).

Fyzickou separáciou, jednotlivé redundancie sú umiestnené v oddelených miestnostiach, majú oddelené káblové trasy, miestnosti sú v rôznych požiarnych zónach (ostrovny koncept)

Separáciou dát, ktorá neumožňuje prenos do ESFAS-u zo systémov s nižšou bezpečnostnou triedou).

Separáciou elektrického napájania skriň SKR:

6.5.3.2.3.5 Kritérium bezpečnej poruchy

Kritérium bezpečnej poruchy pre systém ESFAS vyžaduje, že v prípade poruchy nastavenie systému nespôsobilo falošné zapracovanie a nepriaznivý prechodový stav v technológii. Funkčný blok pre výber a výberovú logiku používaný v softvéri TXS je založený na aktívnom spracovaní stavu vstupného signálu. Poruchový stav meracích obvodov vo všetkých obvodoch príslušnej redundancie znamená, že výstupy VOTER-a ESFAS-u (iniciačné signály kanálov) sú nastavené na elektricky nulový stav tak, že nespôsobia pôsobenie ESFAS (oproti RTS/DRTS).

Výskyt identifikovanej poruchy vo vnútri APU jednotlivého počítača ESFAS-u spôsobí priradenie poruchových stavov ku všetkým signálom, ktoré sú vyslané do VOTER-A. Poruchové signály budú vylúčené z ďalšieho spracovania aktívnym spracovaním stavu signálu pomocou funkčného bloku výberu 2 z 3. Ak všetky počítače z troch počítačov APU vypadnú v rovnakom čase, výstupné signály za funkčným blokom výberu 2 z 3 v počítači VOTER budú mať poruchové stavy a výstupný akčný signál bude nastavený na nulu. Preto, táto udalosť nespôsobí falošné zapracovanie funkcie ESFAS.

Identifikovaná porucha počítačov master-checker VOTER-a nemôže takisto spôsobiť falošnú aktiváciu, pretože tieto spôsobia nastavenie všetkých výstupov na nulu.

6.5.3.2.4 Spôľahlivostná analýza

Pravdepodobnostné spoľahlivostné analýzy [I.25], [I.26], boli vypracované dodávateľom pre RPS (RTS / DRTS a ESFAS). Spoľahlivostné údaje komponentov bezpečnostného SKR a nasledovná FMEA na úrovni modulov vypracovaná dodávateľom ukazuje následky poruchy modulu.

Základné predpoklady modelu spoľahlivosti:

- Nezávislá porucha softvéru je uvažovaná konzervatívne prostredníctvom primárnej udalosti s pravdepodobnosťou poruchy na požiadavku vid' predchádzajúci odstavec.
- Pravdepodobnosť softvérovej poruchy so spoločnou príčinou je predpokladaná konzervatívne [I.25], [I.26], pre každú redundanciu.
- Softvérová diverzita redundancií (divízií) bola predpokladaná

Na zvládnutie CCF softvéru ESFAS je použitá diverzita manuálnou iniciáciou alebo aj manuálnym vykonaním bezpečnostných funkcií.

Diverzitné bezpečnostné funkcie ESFAS pre podchladenie I.O., malú, strednú a veľkú LOCA a pretlak v hermetickej zóne sú realizované manuálnou iniciáciou týchto bezpečnostných funkcií z bezpečnostných panelov.

Diverzitný ESFAS je takisto realizovaný manuálnym vykonávaním bezpečnostných funkcií z panelov SICS s pevným hardvérovým prepojením signálov do jednotiek PACS.

Deterministická analýza je urobená pomocou metód použitých na prípravu užívateľského softvéru ako aj na dokončenie samotného produktu.

Technologické požiadavky na SKR MO34 a kritériá iniciácie bezpečnostných funkcií boli potvrdené deterministickou bezpečnostnou analýzou projektových a vybraných nadprojektových havárií v PpBS kap. 7 „ANALÝZY BEZPEČNOSTI“.

Pre jednotlivé fázy vývoja a integrácie softvéru budú vydané správy v rámci podpornej technickej dokumentácie, o nezávislosti VaV podľa fáz „V“ krivky podľa „V“-krivky [I.9].

V súlade s plánom V&V pre hlavné SKR [I.9] boli predložené správy o úspešných výrobných preberacích testoch (FAT) ([I.39], [I.40], [I.41]).

6.5.3.2.5 Kvalifikácia systému

Výsledky kvalifikácie hardvéru systému ESFAS sú sumarizované v správe o kvalifikácii pre bezpečnostné SKR [I.8]. Výsledky poskytujú dôkaz, že systém spĺňa svoje požiadavky na výkonnosť pri podmienkach prostredia ako sú špecifikované v pláne kvalifikácie systému [I.34].

V tejto správe je znázornený súlad komponentov hardvéru ESFAS s predpísaným prostredím.

Správa o kvalifikácii takisto sumarizuje výsledky skúšok EMC. Zariadenia ESFAS vyhovujú požiadavkám elektromagnetickej kompatibility.

Schopnosť systému ESFAS zostať funkčným počas seizmických udalostí je demonštrovaná testovaním. Správanie sa komponentov v čase je verifikované aplikovaním programu starnutia.

6.5.3.2.6 Zabezpečenie kvality softvéru

Vývoj SW, integrácia HW a SW, verifikácia SW, validácia a licencovanie sú realizované v súlade s požiadavkami STN IEC 60880.

Všetky vlastnosti systémov so vzťahom k bezpečnosti boli certifikované použitím typového testovania, integračnej a systémovej skúšky, takže bezpečnostný systém, ktorý spĺňa konštrukčné kritériá KTA 3501 [II.15], IAEA-NS-G1.3 [II.16] a IEEE 603 [II.17], mohol byť navrhnutý bez väčšieho zásahu do funkcií hardvéru a softvéru.

Kvalifikácia platformy bezpečnostného systému (HW a SW komponenty systému)

Bola vykonaná nezávislými expertmi z organizácií GRS alebo TÜV oprávnenými orgánom pre licencovanie. Typový test softvéru bol vykonaný organizáciami GRS a TÜV Nord.

Skúšky boli vykonané v typickom softvérovom prostredí pričom boli použité nasledujúce testovacie metódy:

- Štatistické testy,
- Testy typu "Black-box",
- Testy typu "White-box",
- Trasovacie testy,
- Testy diagnostického pokrytia,
- Testovanie času vykonávania programu
- Testy medzí.

Špecifikácia softvéru

Softvérové vybavenie systému ESFAS bolo projektované použitím systému SPACE. Následne bolo testované v prostredí SIVAT, ktoré umožňuje virtuálne testovanie užívateľskej aplikácie v úplnom rozsahu.

Výrobné preberacie testy (FAT)

V súlade s plánom verifikácie a validácie pre hlavný SKR [I.38] boli predložené správy o úspešných testoch:

- Testy konfigurácie softvéru (overenie správnosti implementácie užívateľského softvéru do modulov SVE2 a GW, [I.39].
- Testy funkcie ESFAS (skúška správnej funkčnosti modulov v rôznych SVE2, zbernicových prepojení, pevných harvérových prepojení podľa funkčných plánov štvrtej úrovne, [I.40].
- Testy správy systému (výkonové (záťažové) skúšky CPU, doby odozvy, poruchy počítačov alebo kanálov, poruchy I/O modulov, poruchy zberníc, poruchy napájania jednotiek, poruchy nešírenia chýb v systéme, funkčnosť po reštarte systému, [I.41].

Skúšky FAT systému ESFAS boli realizované na skúšobnom poli dodávateľa. Systém bol konfigurovaný tak, ako by bol používaný na reálnom bloku JE. Testovanie bolo vykonávané zadávaním analógových a binárnych signálov na konektory I/O kariet. Rovnako bolo testované rozhranie medzi ESFAS a počítačovým systémom elektrárne.

Verifikácia a validácia

Verifikácia a validácia softvéru prebiehala v dvoch etapách:

- V&V systémových softvérových komponentov (generická kvalifikácia systémového softvéru TXS)
- V&V užívateľskej aplikácie (aplikačný softvér TXS pre MO34 s cyklom vývoja podľa „V“-krivky a jej odpovedajúcim V&V po ukončeníach jednotlivých fáz vývoja)

Prvá etapa V&V bola vykonaná v priebehu vývoja platformy bezpečnostného SKR, pozri [I.8].

Druhá etapa V&V sa zameriava na správnu realizáciu softvéru podľa špecifikácie požiadaviek pre MO34 a pozostáva z:

- verifikácie formálnej špecifikácie, použitím nástrojov SPACE
- softvérovej validácie použitím simulačného nástroja pre validáciu SIVAT
- testov konfigurácie, správy sa počas porúch, testov integrácie softvéru podľa programov FAT a SAT.

K jednotlivým fázam vývoja a integrácie softvéru budú v rámci technickej dokumentácie dodané správy o nezávislej V&V podľa fáz „V“-krivky, viď [I.38].

6.5.3.3 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. 6.5.3.1.2.2 vyššie na systém ESFAS sú uplatňované požiadavky definované vo Vyhláške ÚJD SR č. 50/2006 Z.z. [II.21] v prílohe č.3 v časti A/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.21] je uvedené v závere kap. 6.5.3.3.1.

6.5.3.3.1 Preukázanie plnenia legislatívnych požiadaviek

Hodnotenie bezpečnosti podľa Vyhlášky ÚJD SR č. 50/2006 Z.z. [II.21] Príloha č. 3, časť B, I, L:

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

a) nespôsobilá stratu ochrannej funkcie systému,

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

Splnené – Systémy EXCORE, SMS, RTS/DRTS sú konštruované na troch vzájomne nezávislých redundanciách, každá z nich je vybavená s tromi meracími kanálmi takto zaisťujúcimi odolnosť systémov voči jednoduchej poruche.

Funkcie z RTS sú takisto garantované jeho diverzitným systémom DRTS.

RTB konštruovaný ako redundantný systém, je rozdelený do dvoch vzájomne nezávislých redundancií a na výkonovú časť a logickú časť. Výkonová časť RTB takisto garantuje diverzitu v hardvéri.

- (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 ochranných funkcií.*

Splnené – Systémy RTS/DRTS - on-line monitorovanie je vykonávané cyklicky v každej CPU-TXS a I/O kartách.

Periodické testy zahŕňujú:

- Skúšky vstupných kanálov od snímačov alebo iných SKR vstupujúcich do funkčnej schémy
- Skúšky výstupných kanálov od funkčných schém TXS k akčným členom
- Kontrola integrity implementovaného SW vo všetkých jednotkách CPU
- Kontrola integrity spúšťačích testov na všetkých TXS – CPU

Logická časť BREAKER-ov je testovaná periodicky simulovaním vstupných signálov (a analyzovaním príslušných výstupov), bez rozpojenia kontaktu výkonovej časti. Výkonová časť RTB je skúšaná, aby sa verifikovalo rozpojenie BREAKER-ov. Keď sú v skúšobnom móde, napájané sú iba pomocné a signalizačné obvody ACB.

Z tohto dôvodu môžu byť údržba a skúšky po údržbe vykonávané v súlade s platnými prevádzkovými predpismi bez akéhokoľvek dopadu na funkčnosť RTB.

Systém EXCORE spúšťa periodicky niektoré autotesty, aby verifikoval správnu prevádzku RAM, komponentov CPU a V/V dosky. Autotesty sú vykonávané so softvérom a kedykoľvek je v systéme detekovaná porucha je výstup nastavený do bezpečného stavu, zaručujúci prístup bezpečnej poruchy systému. Periodický test systému je vykonaný pomocou automatického testera (ATU), aby odhalil nedetekované poruchy pomocou autotestov.

Systém SMS je vybavený s komplexnou rutinou autotestov, ktorá monitoruje najdôležitejšie vlastnosti zariadenia. Autotest môže byť vykonávaný počas normálnej prevádzky, keďže bezpečnostné funkcie nie sú ovplyvnené (falošnému zapracovaniu signálov je zabránené).

Kvôli skutočnosti, že všetky systémy si osvojujú prístup bezpečnej poruchy pri generovaní signálov a/alebo pôsobení zariadenia, nevyústi porucha (takisto nedetekovaná) do straty ochranných funkcií, ale môže namiesto toho viesť k stavu bezpečného odstavenia jadrového reaktora.

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

Splnené – systémy vždy pracujú automaticky, t.j. nie je požadovaný žiadny ručný zásah operátora. Navyše automatické zásahy pomocou bezpečnostných systémov nemôžu byť potlačené ručnými zásahmi, ledaže by sa obsluha rozhodla zasiahnuť priamo v oblasti určenej skrine.

- (4) *Bezpečnostný systém sa musí navrhnuť 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.*

Splnené – Systémy RTS/DRTS, SMS, EXCORE a BREAKER-e úspešne prešli kvalifikáciou zariadení ako je to dokladované v kvalifikačných správach, v CEQP a v správach o FAT - kap. 6.5.2.5.1, a kap. 6.5.2.5.3.5

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

(6) *Úroveň požadovanej spoľahlivosti počítačového systému musí byť primeraná jeho bezpečnostnej dôležitosti. Úroveň spoľahlivosti sa musí dosiahnuť komplexnou stratégiou, pri ktorej sa používajú vzájomne sa 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 – CEQP sú vypracované pre všetky etapy projektu, počnúc od fázy projektu, cez výrobu a montáž. Funkčnosť systému je testovaná a preskúmaná počas FAT (pozrite si kap. 6.5.2.5.1). 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 (kap. 6.5.2.5.3.5). Okrem toho je softvér validovaný podľa špecifických postupov V&V ako je to zdokumentované v kap. 6.5.2.5.3.6.

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

Splnené – Pravdepodobnostné spoľahlivostné analýzy boli vypracované dodávateľmi pre všetky systémy - kap. 6.5.2.5.3.4.

(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 – Programy kvality sú vypracované jednotlivými dodávateľmi berúc ako referenciu na požiadavky obsah dokumentu, Referenčný program zaistenia kvality pre bloky 3 a 4 JE Mochovce.

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

Splnené – softvér pre systém ESFAS bol vystavený zdokumentovanému procesu verifikácie a validácie.

(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 – hoci bezpečnostný systém má softvér s dlhoročným prevádzkovým pozadím, boli spoľahlivostné analýzy pre systémy vykonané s dodatočnou hodnotou konzervatizmu, ako je to zdokumentované v kap. 6.5.2.5.3.4.

(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 – nezávislosť systému ESFAS je zaistená funkčným oddelením, fyzickou separáciou, dátovou separáciou, elektrickou separáciou vyššie klasifikovaných systémov od nižšie klasifikovaných systémov. Výmena dát s nižšie klasifikovanými systémami je nepriama (z vyššie klasifikovaného systému na nižšie klasifikovaný systém) a zaistená relevantnými opatreniami, ktoré garantujú funkčné oddelenie systému (pozrite si kap. 6.5.2.5.3.2.2).

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

Splnené – Systém ESFAS pracuje v úplne automatickom režime, t.j. nie je požadovaný žiadny ľudský zásah. Dáta z technológie sú spracované a zobrazené na príslušnej obrazovke na pracoviskách operátora, umožňujúcej operátorovi, aby stále očami sledoval technológiu (pozrite si kap. 6.5.2.1.1.1.2.3, 6.5.2.2.1.1.2.2, 6.5.2.3.1.1.2.2 a 6.5.2.4.1.1.2.3 - HMI)

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

Splnené – Vo všeobecnosti, aktivačné povely pre pôsobenie generované funkciami SKR patriace k vyššej úrovni bezpečnosti majú prioritu pre aktivačnými povelmi generovanými funkciami SKR nižších bezpečnostných úrovní. Táto priorita je garantovaná modulom priority a riadenia akčných členov AV42. Automatická funkcia môže byť potlačená ručnými povelmi priamo vykonanými na skrini.

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

Splnené – Verifikácia a validácia softvéru je zaistená nezávislými organizáciami ako je to zdokumentované v dokumente [I.43] v Pláne verifikácie a validácie softvéru, [I.9] v Pláne verifikácie a validácie pre hlavný SKR.

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

Splnené – systémové funkcie pre RTB sú popísané v kap. 6.5.2.1.1.1.3; systémové funkcie pre RTS/DRTS sú popísané v časti 6.5.2.2.1.1.3; systémové funkcie pre EXCORE sú popísané v kap. 6.5.2.3.1.1.3, zatiaľ čo pre systém SMS sú popísané v kap. 6.5.2.4.1.1.3.

(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 – Všetky bezpečnostné systémy sú vybavené s vhodným HMI (viď bod 12), ktorý umožňuje operátorovi mať úplný prehľad nad technologickými parametrami. Ako náhle je niektorá z prahových úrovní prekročená alebo nastanú nejaké iniciačné udalosti, sú generované signalizácie a sú ukázané teda operátorom na PICS/SICS ako vizuálne a/alebo zvukové

signalizácie. Obrazovky PICS sú vybavené so SPDS (Systém Zobrazovania Bezpečnostných Parametrov), ktoré slúžia operátorovi, aby pochopil, ktoré sú „kritické oblasti“ v technológii a viedli ho pomocou rozhodovacích stromov porúch.

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

Splnené – Všetky dôležité parametre z bezpečnostných systémov SKR sú správne zaznamenané.

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

Splnené – ako je ukázané v bode 12, bezpečnostné systémy sú vybavené vhodným HMI, ktoré umožňuje operátorom mať úplný prehľad o technologických parametroch s jasnými indikáciami prahových úrovní, ktoré boli prekročené. Signalizácie pre bezpečnostné parametre sú zobrazené aj na SICS aj na PICS (objavenie sa závisí na prevádzkovom režime SICS, ohľadne ďalších informácií kap. 5.6 tejto PpBS - Riadiace a regulačné ľudské faktory). Vo všeobecnosti je potreba fyzického kvitovacieho zásahu operátorom (stlačenie tlačidla...). Obrazovky PICS sú vybavené so SPDS (Systém Zobrazovania Bezpečnostných Parametrov), ktorý vedie operátora použitím stromov porúch k pochopeniu technológie. Navyše je dôležité podotknúť, že pri týchto systémoch nie je predpokladaný zásah operátora, keďže tieto sú navrhnuté tak, aby pracovali úplne automaticky.

Požiadavky na bezpečnostné systémy jadrových elektrární sú špecifikované vo Vyhláške ÚJD SR č. 50/2006 Z.z., Príloha 3, I., L. Tri fyzicky a funkčne oddelené redundancie systému ESFAS zaisťujú implementáciu bezpečnostných funkcií aj v prípade jednoduchej poruchy akúkoľvek komponentu systému. Systém ESFAS je projektovaný s redundanciou 3 x 100 %.

Niektoré akčné signály ESFAS sú uložené do pamäti (tam sú takisto nejaké akčné signály bez pamäti, kde trvanie akčného signálu je závislé na trvaní iniciačných udalostí).

Keď bol signál bezpečnostnej funkcie uložený, bezpečnostná funkcia je nepretržitá.

Reset pamäti tlačidlom z panela ESFAS na pracoviskách operátora je možný po nastavenom oneskorení, ak nie sú splnené podmienky pre formovanie signálu.

V prípade málo pravdepodobnej poruchy bezpečnostného systému z dôvodu poruchy so spoločnou príčinou sú dostupné diverzité systémy podľa kap. 6.5.3.2.3.2.

Obrazovky PICS a panely SICS sú navrhnuté takým spôsobom, že je vylepšená poznávacia ergonómia operátora, ktorá mu poskytuje úplný prehľad pri jednom pohľade a vedie ho pomocou signalizácií, aby podnikol správne zásahy.

Bezpečnostný systém ESFAS je kvalifikovaný pre normálnu prevádzku, abnormálnu prevádzku a podmienky projektových havárií, pozrite si takisto kap. 6.5.3.2.5.

Komponenty softvéru a hardvéru použité v aplikáciách bezpečnostných SKR projektu blokov 3 a 4 JE Mochovce sú prezentované so súvisiacimi skúšobnými certifikátmi v prehľade špecifických dát pre Mochovce v dokumente [I.44].

Bezpečnostný systém ESFAS pre MO34 spĺňa požiadavky na funkčnosť, výkonnosť, spoľahlivosť, odolnosť voči poruchám so spoločnou príčinou, kvalifikačné požiadavky, požiadavky na diverzitu a environmentálne podmienky, EMC, seizmickú odolnosť a zaistenie kvality na účinky normálnych prevádzkových podmienok, abnormálnych prevádzkových podmienok a projektové havárie (pozrite si kap. 6.5.3.2).

ESFAS spĺňa požiadavky jadrových štandardov IEC 61513 a IEC 61226 pre projektovanie, čo sa týka spoľahlivosti.

V porovnaní s vyhláškou ÚJD SR č. 50 Z.z. [II.21], vyhláška č. 430/2011 Z.z. [II.3] v časti B, I.,L okrem vyššie uvedených požiadaviek obsahuje navyše tieto body:

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

Čiastočne splnené - Pre ESFAS bol aplikačný SW posúdený nezávislou organizáciou ISTEC počas skúšok FAT [I.45], [I.46], [I.47], [I.48], [I.49], [I.50], [I.51], [I.52], [I.53], [I.54], [I.55], [I.56] ako je to uvedené v Pláne nezávislej V&V počítačovo riadených bezpečnostných systémov na potvrdenie ich spoľahlivosti [I.33]. Skúšky SAT budú vykonané po inštalácii systému ESFAS na mieste. Výsledky skúšok SAT budú zhodnotené v dokumente [I.57].

(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.*

Splnené: - Analýza odolnosti systému ESFAS voči jednoduchej poruche a poruchám so spoločnou príčinou, vyhodnotenie funkčnej diverzity, vyhodnotenie ochrany do hĺbky, adekvátnosť riešenia redundancií, deterministické hodnotenie spoľahlivosti systému ochrany reaktora MO34 pri zabezpečovaní plnenia bezpečnostných funkcií. Taktiež je zameraná na hodnotenie plnenia požiadaviek úvodného projektu (požiadavky na funkčnosť, spoľahlivosť, výkonnosť, odolnosť voči prostrediu a požiadavky na QA). Obsahuje kvalitatívne hodnotenie spoľahlivosti metódou FMEA a SW FMEA.

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

a) *požaduje sa vysoká kvalita použitého hardvéru a softvéru,*

Splnené: - HW and SW komponenty bezpečnostného systému boli kvalifikované pre daný účel použitia - vid' [I.9], [I.31]

b) *celý vývojový proces zahŕňajúci kontrolu, testovanie, uvedenie do prevádzky a zmeny projektu musí byť systematicky dokumentovaný a revidovaný,*

Splnené: - celý proces vývoja od návrhu, testovanie a uvedenie do prevádzky je dokumentovaný v súlade s dokumentáciou kvality s výstupmi v podobe analýz a správ z jednotlivých etáp projektu.

c) *ak nie je možné preukázať spoľahlivosť systému s vysokou mierou dôveryhodnosti, musí byť zabezpečená diverzita plnenia funkcií ochrany.*

Splnené: - diverzita funkcií ESFAS je realizovaná ručným ovládaním vybraných spotrebičov z panelov SICS na pracoviskách operátora. Diverzita nie je vykonávaná automatickou cestou. Požiadavka vyplývajúca z Úvodného projektu porucha na výzvu je splnená (z analýzy [I.25] vyplýva, že požiadavka na falošné zapracovanie je splnená (z analýzy [I.25]

Pri poruche na výzvu sa udáva porucha 1 redundancie, pretože každá redundancia ovláda iný bezpečnostný podsystém.

Naopak, falošné zapracovanie je treba uvádzať pre všetky 3 redundancie, pretože falošný nábeh už jedného podsystému môže spôsobiť iniciačnú udalosť, napr. studené pretlakovanie.

Záverom možno konštatovať, že **projekt systému ESFAS spĺňa všetky požiadavky** definované pre podporný bezpečnostný systém vo vyhláške ÚJD SR č. 50/2006 Z. z. [II.21].

Vyhláška ÚJD SR č. 430/2006 [II.3] v porovnaní s Vyhláškou ÚJD SR č. 50/2006 [II.21] obsahuje navyše ďalšie všeobecné požiadavky, ktoré systém ESFAS taktiež spĺňa.

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

- [I.1] PpBS EMO 1, 2 arch.č.254/97 Sign.5986 z 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 ;
- [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] Koncept riadenia priority a akčných členov;
- [I.13] Design Concept for Reactor Protection Panel;
- [I.14] Koncept prevádzky a bezpečnosti bezpečnostného SKR;
- [I.15] Koncept signalizácie porúch a výstrah systémov založených na TXS;
- [I.16] Revize a dopracováni Úvodného 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 ošetrovanie 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. Spôľahlivostná analýza;
- [I.26] Spôľahlivostná analýza kombinácie rôznych SKR;
- [I.27] Plán kvality vybraného zariadenia pre systém reaktorovej ochrany , fáza projektovania;
- [I.28] Kapitola 07 Analýzy bezpečnosti;
- [I.29] Spôľahlivostné analýzy systémov SKR a ich poľnej inštrumentácie;
- [I.30] Analýzy bezpečnosti a spoľahlivosti systému reaktora JE EMO34;

- [I.31] Zoznam kvalifikačných dokumentov zariadenia SKR "QN101" pre komponenty bezpečnostného SKR
- [I.32] Zoznam vybraných zariadení pre 3. blok MO34 a spoločné zariadenia 3. a 4. bloku - textová časť,
- [I.33] Plán nezávislej V&V počítačovo riadených bezpečnostných systémov na potvrdenie ich spoľahlivosti, ISTECH GmbH
- [I.34] Plán kvality vybraného zariadenia pre systém reaktorovej ochrany ,výrobná fáza;
- [I.35] U3, RPS-V, FAT report, factory acceptance certificate
- [I.36] U3, RPS-W, FAT report, factory acceptance certificate
- [I.37] U3, RPS-X, FAT report, factory acceptance certificate
- [I.38] Plán verifikácia a validácie pre hlavný SKR
- [I.39] RPS-V, Test procedure A1.0.3 software configuration check
- [I.40] U3, RPS-V, Test procedure A1.3.2 „Function test of ESFAS functionality“
- [I.41] U3, RPS-V, System test report A1.4
- [I.42] Reference quality assurance programme for units 3 and 4 in Mochovce NPP,
- [I.43] Software verification and validation plan,
- [I.44] I&C equipment qualification documents „QN101“ for the safety I&C system components,
- [I.45] RPS, Detailed design review report (SW),
- [I.46] RPS, Detailed design review report (HW),
- [I.47] U4, RPS, Detailed design review report (SW),
- [I.48] RPS, Detailed design review report (HW),
- [I.49] RPS-V, TXS SW Validation Test Program # PRS-V. Program testov pre validáciu SW TXS,
- [I.50] RPS-V. TXS SW Validation test program#,
- [I.51] RPS-V. TXS SW Validation test report#,
- [I.52] RPS-V. TXS SW Validation test report#,
- [I.53] RPS-W. TXS SW Validation test plan#RPS-W. TXS plán testov SW validácie,
- [I.54] RPS-W. TXS SW Validation test report#,
- [I.55] RPS-X. TXS SW Validation test plan#RPS-X. TXS plán testov SW validácie,
- [I.56] RPS-X. TXS SW Validation test report#,
- [I.57] Independent V&V safety I&C MO34 evaluation of the SAT RPS Unit 3,
- [I.58] U3. RPS I&C Function Specification (Level 4),

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

- [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] Vyhláška 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 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, Viedeň, 5/2004
- [II.15] Reactor Protection System and Monitoring Equipment of the Safety System - KTA 3501
- [II.16] Instrumentation and Control Systems Important to Safety in Nuclear Power Plants No.NS-G 1.3, Vienna 3/2002
- [II.17] IEEE 603 - 1998 Standard Criteria for Safety Systems for Nuclear Power Generating Stations
- [II.18] BNS I.1.2/2014 Rozsah a obsah bezpečnostnej správy, ÚJD SR, Bratislava, 01/2014
- [II.19] Rozhodnutie ÚJD SR no. 63/2015. Schválenie kategorizácie vybraných zariadení do bezpečnostných tried podľa dokumentov PNM34361188 a PNM34361189
- [II.20] Rozhodnutie ÚJD SR č. 267/2008 Pripomienky k rozsahu a obsahu PBS pre MO34
- [II.21] 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.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
- [II.23] IAEA Safety Standards Series NS-G-1.6 Seismic Design and Qualification for Nuclear Power Plants, IAEA, Vienna, 2003

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,
- [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] Kapitola 05.03 Kategorizácia vybraných zariadení do bezpečnostných tried, VUJE, a. s., Trnava,
- [III.16] Analýzy bezpečnosti a spoľahlivosti systému ochrany reaktora JE MO34, Technická správa,
- [III.17] Kapitola 06.06 Elektrické napájanie,
- [III.18] I&C power supply - single line diagram,

ZOZNAM PRÍLOH

ZOZNAM TABULIEK