

## Technická správa

## Predprevádzková bezpečnostná správa

## Kapitola 06.05.02 Systém automatických ochrán reaktora (RTS/DRTS, EXCORE, SMS, RTB)

**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      |
|                                                                                                                                                                                                                                                             |              |                                                | Submitted to Client to / Predložené odberateľovi na: | Approval / Schválenie  | x                                  | Information Only / Len na informáciu |                                  |
| <small>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.</small> |              |                                                |                                                      |                        |                                    |                                      |                                  |
| EPS No / Číslo EPS: PNM34365000                                                                                                                                                                                                                             |              | Revision index / Index revízie: 05             |                                                      | Size / Veľkosť         | Activity Code / Aktivita           | Type / Subtype Typ / Podtyp          | Discipline / Profesia            |
| File name / Názov súboru:                                                                                                                                                                                                                                   |              | SE doc. Code / SE číslo dokumentu: PNM34361052 |                                                      | A4                     | 6.01                               | RS                                   | Z                                |
| <br>* P N M 3 4 3 6 1 0 5 2 0 5 *                                                                                                                                        |              |                                                |                                                      | Sheet / List           | Of / z                             |                                      | Plant System / Systém elektrárne |
|                                                                                                                                                                                                                                                             |              |                                                |                                                      | 1                      | 50                                 |                                      | Component / Komponent            |

|                                                               |   |             |                            |                                                   |              |                    |  |
|---------------------------------------------------------------|---|-------------|----------------------------|---------------------------------------------------|--------------|--------------------|--|
| SE Contract No. / Číslo zmluvy SE: 4600003952                 |   |             |                            | VUJE Contract No. / číslo zmluvy VUJE: 1719/00/09 |              |                    |  |
| Part name / Označenie časti: PNM3436105205_S_C00_V            |   |             |                            | Issued on / Vydané dňa: 21.08.2019                |              |                    |  |
| Sensitivity code <sup>1)</sup> / Kód citlivosti <sup>1)</sup> | 3 | Name / Meno | Organization / Organizácia | Dept. / Útvár                                     | 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 /<br>Identifikácia<br>(part/page/chapter/<br>member/section)<br>(časť/strana/kapitola/<br>článok/odstavce) | Brief description of modification /<br>Stručná charakteristika úpravy<br>(description of modification and manner of implementation)<br>(popis úpravy a spôsobu zapracovanie) | Reason of modification /<br>Dôvod úpravy<br>(author company, number of comments<br>or other stimulation, name of author,<br>comment document No.)<br>(firma autora a číslo pripomienky, resp.<br>iný podnet, meno autora, č. dokumentu<br>pripomienok) |
|---------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| • Celý dokument                                                                                                           | • Zapracovanie pripomienok ÚJD podľa Aarhuského výboru                                                                                                                       | • V súlade s dokumentom<br>PNM34482979                                                                                                                                                                                                                 |
| •                                                                                                                         | •                                                                                                                                                                            | •                                                                                                                                                                                                                                                      |
| •                                                                                                                         | •                                                                                                                                                                            | •                                                                                                                                                                                                                                                      |
| •                                                                                                                         | •                                                                                                                                                                            | •                                                                                                                                                                                                                                                      |
| •                                                                                                                         | •                                                                                                                                                                            | •                                                                                                                                                                                                                                                      |
| •                                                                                                                         | •                                                                                                                                                                            | •                                                                                                                                                                                                                                                      |
| •                                                                                                                         | •                                                                                                                                                                            | •                                                                                                                                                                                                                                                      |
| •                                                                                                                         | •                                                                                                                                                                            | •                                                                                                                                                                                                                                                      |
| •                                                                                                                         | •                                                                                                                                                                            | •                                                                                                                                                                                                                                                      |
| •                                                                                                                         | •                                                                                                                                                                            | •                                                                                                                                                                                                                                                      |
| •                                                                                                                         | •                                                                                                                                                                            | •                                                                                                                                                                                                                                                      |
| •                                                                                                                         | •                                                                                                                                                                            | •                                                                                                                                                                                                                                                      |
| •                                                                                                                         | •                                                                                                                                                                            | •                                                                                                                                                                                                                                                      |
| •                                                                                                                         | •                                                                                                                                                                            | •                                                                                                                                                                                                                                                      |

# List of document part

## Zoznam častí dokumentu

| Por.<br>č.<br>No. | Názov dokumentu<br>Document name | Ev. č. súboru časti dokumentu /<br>File ref. No. of document part | Číslo revízie /<br>Revision No. |
|-------------------|----------------------------------|-------------------------------------------------------------------|---------------------------------|
| 1.                | • Titulný list/Tittle list       | • PNM3436105205_S_C00_V                                           | • 05                            |
| 2.                | • Textová časť/Text part         | • PNM3436105205_S_C01_V                                           | • 05                            |
| 3.                | • Príloha č. 1/Appendix 1        | • PNM3436105205_S_P01_V                                           | • 05                            |
| 4.                | •                                | •                                                                 | •                               |
| 5.                | •                                | •                                                                 | •                               |
| 6.                | •                                | •                                                                 | •                               |
| 7.                | •                                | •                                                                 | •                               |
| 8.                | •                                | •                                                                 | •                               |
| 9.                | •                                | •                                                                 | •                               |
| 10.               | •                                | •                                                                 | •                               |
| 11.               | •                                | •                                                                 | •                               |

## OBSAH

|                                                                              |    |
|------------------------------------------------------------------------------|----|
| ÚVOD.....                                                                    | 6  |
| ZOZNAM SKRATIEK .....                                                        | 7  |
| 6.5.2 SYSTÉM RÝCHLEHO ODSTAVENIA REAKTORA (RTS/DRTS, EXCORE, SMS, RTB) ..... | 9  |
| 6.5.2.1 POPIS SYSTÉMU – RTB .....                                            | 9  |
| 6.5.2.1.1 Účel systému .....                                                 | 9  |
| 6.5.2.1.1.1 Popis konštrukcie a funkčnosti .....                             | 9  |
| 6.5.2.1.1.1.1 Bezpečnostná a seizmická klasifikácia .....                    | 9  |
| 6.5.2.1.1.1.2 Popis systému.....                                             | 9  |
| 6.5.2.1.1.1.3 Funkcie systému .....                                          | 10 |
| 6.5.2.1.1.1.4 Napájanie.....                                                 | 10 |
| 6.5.2.1.1.2 Činnosť obsluhy .....                                            | 10 |
| 6.5.2.1.1.3 Popis prevádzkových stavov .....                                 | 10 |
| 6.5.2.1.1.4 Detailné prvky projektu.....                                     | 10 |
| 6.5.2.1.1.4.1 Dispozičné riešenie RTB .....                                  | 10 |
| 6.5.2.1.1.4.2 Štruktúra systému RTB a jeho charakteristiky .....             | 11 |
| 6.5.2.2 POPIS SYSTÉMU - RTS + DRTS.....                                      | 12 |
| 6.5.2.2.1 Účel systému .....                                                 | 12 |
| 6.5.2.2.1.1 Opis konštrukcie a funkčnosti .....                              | 12 |
| 6.5.2.2.1.1.1 Bezpečnostná a seizmická klasifikácia .....                    | 12 |
| 6.5.2.2.1.1.2 Popis systému.....                                             | 13 |
| 6.5.2.2.1.1.3 Funkcie systémov.....                                          | 15 |
| 6.5.2.2.1.1.4 Elektrické napájanie .....                                     | 15 |
| 6.5.2.2.1.2 Činnosť obsluhy .....                                            | 16 |
| 6.5.2.2.1.3 Popis prevádzky.....                                             | 16 |
| 6.5.2.2.1.4 Detailné prvky projektu.....                                     | 17 |
| 6.5.2.2.1.4.1 Dispozičné riešenie RTS/DRTS.....                              | 17 |
| 6.5.2.2.1.4.2 Štruktúra systému a jeho charakteristiky.....                  | 17 |
| 6.5.2.3 POPIS SYSTÉMU - EXCORE .....                                         | 17 |
| 6.5.2.3.1 Účel systému .....                                                 | 17 |
| 6.5.2.3.1.1 Opis konštrukcie a funkčnosti .....                              | 17 |
| 6.5.2.3.1.1.1 Bezpečnostná a seizmická klasifikácia .....                    | 18 |
| 6.5.2.3.1.1.2 Popis systému.....                                             | 18 |
| 6.5.2.3.1.1.3 Funkcie systému .....                                          | 20 |
| 6.5.2.3.1.1.4 Elektrické napájanie .....                                     | 21 |
| 6.5.2.3.1.2 Činnosť obsluhy .....                                            | 22 |
| 6.5.2.3.1.3 Popis prevádzky.....                                             | 22 |
| 6.5.2.3.1.4 Detailné prvky projektu.....                                     | 22 |
| 6.5.2.3.1.4.1 Dispozičné riešenie .....                                      | 22 |
| 6.5.2.4 POPIS SYSTÉMU - SMS.....                                             | 22 |
| 6.5.2.4.1 Účel systému .....                                                 | 22 |
| 6.5.2.4.1.1 Opis konštrukcie a funkčnosti .....                              | 22 |
| 6.5.2.4.1.1.1 Bezpečnostná a seizmická klasifikácia .....                    | 23 |
| 6.5.2.4.1.1.2 Popis systému.....                                             | 23 |

|                 |                                                       |    |
|-----------------|-------------------------------------------------------|----|
| 6.5.2.4.1.1.3   | Systémové funkcie .....                               | 25 |
| 6.5.2.4.1.1.4   | Elektrické napájanie SMS .....                        | 26 |
| 6.5.2.4.1.2     | Činnosť obsluhy .....                                 | 26 |
| 6.5.2.4.1.3     | Popis prevádzky .....                                 | 26 |
| 6.5.2.4.1.4     | Podrobný popis projektu .....                         | 26 |
| 6.5.2.4.1.4.1   | Dispozičné riešenie SMS .....                         | 26 |
| 6.5.2.4.1.4.2   | Štruktúra systému SMS a jeho charakteristiky .....    | 26 |
| 6.5.2.5         | TECHNICKÉ HODNOTENIE .....                            | 28 |
| 6.5.2.5.1       | Požiadavky na vybrané zariadenia .....                | 28 |
| 6.5.2.5.2       | Seizmická odolnosť .....                              | 28 |
| 6.5.2.5.3       | Princípy bezpečného projektovania .....               | 29 |
| 6.5.2.5.3.1     | Kritérium jednoduchšej poruchy .....                  | 29 |
| 6.5.2.5.3.2     | Kritérium poruchy so spoločnou príčinou .....         | 29 |
| 6.5.2.5.3.2.1   | Diverzita .....                                       | 31 |
| 6.5.2.5.3.2.2   | Nezávislosť .....                                     | 31 |
| 6.5.2.5.3.3     | Kritérium bezpečnej poruchy .....                     | 32 |
| 6.5.2.5.3.4     | Spoľahlivostná analýza .....                          | 33 |
| 6.5.2.5.3.5     | Kvalifikácia systému .....                            | 34 |
| 6.5.2.5.3.6     | Zaistenie kvality softvéru .....                      | 35 |
| 6.5.2.6         | BEZPEČNOSTNÉ ZHODNOTENIE .....                        | 37 |
| 6.5.2.6.1       | Vyhodnotenie plnenia legislatívnych požiadaviek ..... | 37 |
| 6.5.2.6.2       | Bezpečnostné hodnotenie - RTS, DRTS a RTB .....       | 42 |
| 6.5.2.6.3       | Bezpečnostné hodnotenie - EXCORE .....                | 43 |
| 6.5.2.6.4       | Bezpečnostné hodnotenie - SMS .....                   | 43 |
| LITERATÚRA      | .....                                                 | 45 |
| ZOZNAM PRÍLOH   | .....                                                 | 50 |
| ZOZNAM TABULIEK | .....                                                 | 50 |

## ÚVOD

Kapitola 6.5.2 je vypracovaná v súlade so súvisiacou literatúrou IAEA Safety Standards Series NS-R-1 [II.1], IAEA Safety Standards Series No. GS-G-4.1 [II.3], Vyhláškou ÚJD SR č. 58/2006 Z.z. [II.6], Atómovým zákonom [II.16] a BNS I.1.2/2008 [II.2], pričom bolo v primeranom rozsahu prihliadnuté k novému platnému návodu BNS I.1.2/2014 [II.19]. Pri vypracovaní kapitoly 6.5.2 boli rešpektované pripomienky uvedené v Rozhodnutí ÚJD SR č. 267/2008 [II.20]. Ustanovenia Vyhlášky ÚJD SR č. 50/2006 Z.z. sú použité v rozsahu určenom prechodným ustanovením § 7 Vyhlášky ÚJD SR č. 430/2011 Z.z. Ustanovenia vyhlášky ÚJD SR 56/2006 Z.z. použité v rozsahu určenom prechodným ustanovením § 10 Vyhlášky ÚJD SR č. 431/2011 Z.z.

Kapitola popisuje a hodnotí systém automatických ochrán reaktora (RTS/DRTS, EXCORE, SMS, RTB) z hľadiska bezpečnosti.

**ZOZNAM SKRATIEK**

|        |                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------|
| ACB    | vzduchový vypínač                                                                                             |
| AO1    | signál rýchleho odstavenia reaktora                                                                           |
| ASFES  | Analytické stredisko fyzikálneho a energetického spúšťania                                                    |
| ATU    | automatické testovacie zariadenie                                                                             |
| AZ     | aktívna zóna reaktora                                                                                         |
| BD     | bloková dozorňa                                                                                               |
| CCF    | poruchy so spoločnou príčinou                                                                                 |
| CPU    | centrálne procesorová jednotka                                                                                |
| DARC   | počítač pre zobrazovanie parametrov a výpočet reaktivity                                                      |
| DNCS   | Systém kontroly reaktivity a zobrazovania (Display and Nuclear Control System)                                |
| DRTS   | Diverzitný systém rýchleho odstavenia reaktora (Diverse Reactor Trip System)                                  |
| ESFAS  | Systém aktivácie technických prostriedkov zaistenia bezpečnosti (Engineered Safety Features Actuation System) |
| DPS    | dielčí prevádzkový súbor                                                                                      |
| EXCORE | Systém merania neutrónového toku (Neutron Flux Measurement System)                                            |
| FAT    | výrobné preberacie skúšky                                                                                     |
| FMEA   | analýza príčin a účinkov porúch                                                                               |
| GW     | gateway                                                                                                       |
| HZ     | hermetická zóna                                                                                               |
| HČČ    | hlavné cirkulačné čerpadlo                                                                                    |
| HMI    | rozhranie človek-stroj                                                                                        |
| HNK    | hlavný napájací kolektor                                                                                      |
| HRK    | havarijná a regulačná kazeta                                                                                  |
| HVS    | horúce vety slučiek                                                                                           |
| HW     | hardvér                                                                                                       |
| I.O.   | primárny okruh                                                                                                |
| IAEA   | Medzinárodná agentúra pre atómovú energiu                                                                     |
| IEC    | Medzinárodná elektrotechnická komisia                                                                         |
| INCORE | Systém vnútroreaktorovej kontroly                                                                             |
| JE     | jadrová elektrárň                                                                                             |
| KO     | kompensátor objemu                                                                                            |
| LDU    | jednotka lokálneho zobrazovania                                                                               |
| MI     | monitorovacie rozhranie                                                                                       |
| MO34   | jadrová elektrárň Mochovce 3. a 4. blok                                                                       |
| MSI    | monitorovacie a servisné rozhranie                                                                            |
| NCC    | centrum riadenia siete                                                                                        |
| ND     | núdzová dozorňa                                                                                               |
| NDCU   | jednotka úpravy detekcie neutrónov                                                                            |

|         |                                                                                   |
|---------|-----------------------------------------------------------------------------------|
| NPPS    | system spracovania neutrónových parametrov                                        |
| NPPU    | jednotka spracovania neutrónových parametrov                                      |
| NV      | napájacia voda                                                                    |
| OM      | prevádzkový a monitorovací systém (operation and monitoring system)               |
| PACS    | Systém prioritného riadenia pohonov (Priority Actuator Control System)            |
| PAMS    | Pohavarijný monitorovací systém (Post Accident Monitoring System)                 |
| PCS     | Systém riadenia procesov (Process Control System)                                 |
| PFD     | pravdepodobnosť poruchy na požiadanie                                             |
| PFH     | pravdepodobnosť poruchy za hodinu                                                 |
| PG      | parogenerátor                                                                     |
| PICS    | Počítačový informačný a riadiaci systém (Process Information and Control System)  |
| PIU     | postulovaná iniciačná udalosť                                                     |
| PR      | výkonové pásmo                                                                    |
| RCS     | Systém regulácie výkonu reaktora (Reactor Control System)                         |
| red.    | redundancia                                                                       |
| RLS     | Systém obmedzenia výkonu reaktora (Reactor Limitation System)                     |
| RPP     | panel ochrany reaktora (bezpečnostný panel)                                       |
| RPS     | Systém ochrany reaktora (Reactor Protection System)                               |
| RRCS    | Systém skupinového a individuálneho riadenia HRK (Reactor Rod Control System)     |
| RTB     | vypínač rýchleho odstavenia reaktora (Reactor Trip Breaker)                       |
| RTE     | prostredie reálneho času                                                          |
| RTS     | Systém rýchleho odstavenia reaktora (Reactor Trip System)                         |
| SC      | úprava signálov                                                                   |
| SAT     | preberacie skúšky v prevádzke                                                     |
| SICS    | Bezpečnostný informačný a riadiaci systém (Safety Information and Control System) |
| SKR     | system kontroly a riadenia                                                        |
| SMS     | system monitorovania seizmicity (Seismic Monitoring System)                       |
| SR      | pásmo zdroja                                                                      |
| SU      | servisná jednotka                                                                 |
| SW      | softvér                                                                           |
| TCS     | Riadiaci systém turbíny (Turbine Control System)                                  |
| ÚJD SR  | Úrad Jadrového dozoru Slovenskej republiky                                        |
| ÚP      | úvodný projekt                                                                    |
| V&V     | verifikácia a validácia                                                           |
| V, W, X | označenie redundancie v dokumentácii AREVA                                        |

## 6.5.2 SYSTÉM RÝCHLEHO ODSTAVENIA REAKTORA (RTS/DRTS, EXCORE, SMS, RTB)

Zabezpečuje rýchle odstavenie reaktora.

### Bezpečnostné funkcie

Systém podľa IAEA Bezpečnostné štandardy série No. SSR-2/1 Bezpečnosť JE: Projektovanie - Špecifické bezpečnostné požiadavky [II.1] a v zmysle Vyhlášky ÚJD SR č. 50/2006 Z.z vykonáva základnú bezpečnostnú funkciu:

- regulácia reaktivity.

### 6.5.2.1 POPIS SYSTÉMU – RTB

#### 6.5.2.1.1 Účel systému

Účelom bezpečnostného systému RTB je rýchle odstaviť reaktor.

##### 6.5.2.1.1.1 Popis konštrukcie a funkčnosti

Každý zo systémov má logickú časť a výkonovú časť.

Logická časť je hlavne tvorená Programovateľnými logickými modulmi, SPLM 1, kde sú signály spracovávané.

Diverzita systému je zaistená použitím stýkačov od dvoch rôznych dodávateľov (ABB a Siemens)

##### 6.5.2.1.1.1.1 Bezpečnostná a seizmická klasifikácia

Systém plní bezpečnostnú funkciu.

##### 6.5.2.1.1.1.2 Popis systému

Funkciou systému BREAKER-ov rýchleho odstavenia reaktora je rýchle odstaviť reaktor odpojením napájania mechanizmov pohonov regulačných tyčí na základe príslušných signálov.

Ako je vysvetlené v kap. 6.5.2.1.1.1, majú logickú časť, ktorá spracováva vstupné signály a vysiela výstupné signály, ktoré sú v normálnom stave pod napätím, do iných systémov a výkonovej časti. Odpojenie napájania mechanizmov pohonov regulačných tyčí je vykonané výkonomým vypínačom (ACB) vo výkonovej časti

Vzhľadom na redundantné silové napájanie musia byť odpojené oba napájacie prívody.

##### 6.5.2.1.1.1.2.1 Logická časť RTB

Logická časť je postavená na programovateľných logických moduloch, ktoré realizujú napevno nadržované logické funkcie.

Signály rýchleho odstavenia vstupujú do logickej časti kanálov príslušných redundancií nadväzujúcich systémov. Je dostatočné, že jeden spomedzi výsledkov výberov je nastavený na aktívny stav, ktorý bude vydaný logickou časťou BREAKER-ov a poslaný do výkonovej časti na bezprostredné odpojenie pohonných mechanizmov riadiacich tyčí.

##### 6.5.2.1.1.1.2.2 Výkonová časť RTB

Výkonová časť RTB je tvorená stýkačmi.

#### **6.5.2.1.1.1.2.3 Vizualizácia**

##### **Výstražná signalizácia**

#### **6.5.2.1.1.1.3 Funkcie systému**

Funkcie RTB sú popísané v kap. 6.5.2.1.1.1.2, 6.5.2.1.1.1.2.1 a 6.5.2.1.1.1.2.2.

#### **6.5.2.1.1.1.4 Napájanie**

Koncept elektrickej časti a pomocného napájania je popísaný v kapitole 6.6 PpBS – Elektrické napájanie [I.58].

V tejto kapitole sú stanovené:

- Spoločné a základné princípy riešenia pomocných systémov napájania JE
- Požiadavky spotrebičov na elektrické napájanie (popis údajov a hodnoty) [I.58]
- Popis schémy systému pomocného napájania JE – Zdroje a siete systému pomocného napájania

Koncept riešenia napájania SKR je zrejmý z výkresu [I.57].

#### **6.5.2.1.1.2 Činnosť obsluhy**

Systém RTB pracuje plne automaticky bez zásahu operátora. V prípade potreby môže operátor aktivovať ručne funkciu rýchleho odstavenia reaktora tlačidlami v paneli rýchleho zásahu na pulte pracoviska operátora reaktora. Pôsobenie aktivačného signálu je neprerušiteľné (akčný signál je zaznamenaný).

#### **6.5.2.1.1.3 Popis prevádzkových stavov**

RTB má režim prevádzky a režim skúšok. RTB je funkčný nielen počas špecifikovanej normálnej prevádzky a očakávaných prevádzkových udalostí, ale aj pri vzniku PIU.

Čo sa týka skúšok, logická časť BREAKER-ov je podrobená stanovenému skúšobnému postupu, t.j. periodickému testovaniu.

Periodické testovanie logickej časti zahŕňa funkčné skúšky simulovaných vstupov (a zodpovedajúcich výstupov, bez rozpojenia kontaktu BREAKER-a) a má byť iniciované manuálne (aktivovaním prepínača na umožnenie skúšky).

Testovanie výkonovej časti RTB má za účel overiť rozpojenie BREAKER-ov. BREAKER-e sa manuálne rozpoja zo skrine a signály spätnej kontroly indikujú úspešnosť testu.

Pokiaľ je v režime testu, je pod napätím iba pomocný a signalizačný obvod ACB. Údržba a skúšky po údržbe počas normálnej prevádzky môžu byť vykonávané v súlade s platnými prevádzkovými predpismi bez akéhokoľvek dopadu na funkčnosť RTB.

#### **6.5.2.1.1.4 Detailné prvky projektu**

##### **6.5.2.1.1.4.1 Dispozičné riešenie RTB**

Zariadenia systému RTB sú umiestnené v HVB podľa projektovej dokumentácie.

#### **6.5.2.1.1.4.2 Štruktúra systému RTB a jeho charakteristiky**

Systém RTB má dve redundancie: Každá redundancia má logickú a výkonovú časť. Podrobnejší popis RTB - pozrite si kap. 6.5.2.1.1.1.2.

## 6.5.2.2 POPIS SYSTÉMU - RTS + DRTS

### 6.5.2.2.1 Účel systému

RTS a DRTS sú projektované na spôsobenie automatického prerušenia štiepnej reakcie, ak boli dosiahnuté iniciačné kritériá od technologických parametrov.

#### 6.5.2.2.1.1 Opis konštrukcie a funkčnosti

Architektúra RTS + DRTS je založená na počítačovej platforme od spoločnosti Areva.

Systém je implementovaný v troch identických a oddelených redundanciách: a každá z nich je vybavená tromi kanálmi. Kvôli zabezpečeniu diverzity je systém realizovaný ako dva systémy (RTS a DRTS) s rôznymi iniciačnými kritériami (pozrite si kap. 6.5.2.2.1.1.3).

Každá redundancia môže byť fiktívne rozdelená na:

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

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, poskytované prevodníkmi a snímačmi, diskkrétne signály sú upravené a všetky bezpečnostné premenné sú potom prenesené na *digitálnu úroveň spracovania*. Táto „úroveň“ taktiež zabezpečuje napájanie prevodníkov.

- **Úroveň digitálneho spracovania**

V tejto úrovni sú zahrnuté APU (pozrite si kap. 6.5.2.2.1.1.2). Na tejto úrovni sú bezpečnostné premenné konvertované (analogový signál – digitálny signál), sú generované a validované signály medzí, sú generované iniciačné kritériá a výberové logiky (a následne aj signály pôsobenia, ktoré sú následne poskytnuté do *riadiacej úrovne* cez výstupné moduly).

- **Úroveň riadenia**

V tejto úrovni sú zahrnuté logika RTB a moduly PACS.

Všetky kanály komunikujú cez zbernicovú sieť z optických vlákien. Toto zabezpečuje neinteraktívne oddelenie voči prepätiam tak, že porucha jedného subsystému neovplyvní iné. Redundancie sú úplne nezávislé a nepredpokladá sa medzi nimi žiadna komunikácia.

RTS a DRTS majú funkčné rozhrania s nasledujúcimi inými systémami:

- BREAKER-e
- SMS a EXCORE
- bezpečnostné panely SICS cez MSI a MI
- signály z/do technológie cez ranžirovacie skrine
- PICS cez redundantné gateway-e (GW)

#### 6.5.2.2.1.1.1 Bezpečnostná a seizmická klasifikácia

Priradenie RTS + DRTS do jednotlivých kategórií bezpečnosti a seizmickej odolnosti podľa Vyhlášky ÚJD SR č. 50/2006 Z.z., STN IEC 61226, STN IEC 61513 a IAEA NS-G-1.6 je v tabuľke 6.5.2-2.

RTS a DRTS sú zaradené do BTII a podľa STN IEC 61226 do triedy A.

Po uplynutí platnosti Po uplynutí platnosti prechodného ustanovenia uvedeného vo Vyhláške ÚJD SR č. 430/2011 Z.z. (viď [II.17], §7 „Prechodné ustanovenie, t.j. 31.12.2014) je v platnosti §3 „Kategorizácia vybraných zariadení do bezpečnostných tried“ predmetnej vyhlášky [II.17].

Porovnaním vyhlášok [II.17] a [II.4] môžeme konštatovať, že zaradenie systému RTS a DRTS do bezpečnostných tried a priradenie bezpečnostnej funkcie sa nemení.

Kritérium EMC podľa EN 61000-6-2 je A [I.60]

Podmienky prostredia pre komponenty RTS a DRTS sú [I.6]

#### **6.5.2.2.1.1.2 Popis systému**

RTS/DRTS sú vytvorené z nasledujúcich komponentov:

- Úprava signálov (SC)

Dáta z technológie a dáta z poľa alebo od iných systémov kontroly a riadenia ako SMS, EXCORE sú zberané cez skrine SC. Jednotky SC zabezpečujú napájanie snímačov/prevodníkov ako aj štandardizáciu signálov, oddelenie a distribúciu signálov pre APU jednotky v iných bezpečnostných systémoch a pre iné systémy kontroly a riadenia alebo dozorne.

Pre SC je použitý princíp troch kanálov pre každú redundanciu.

- Jednotka zberu a spracovania signálov (APU)

Jednotky APU RTS, DRTS zabezpečujú zber vstupných signálov RTS, DRTS z jednotiek úpravy signálov (SC), vykonávajú ich logické spracovanie a vydávajú signály odstavenia reaktora do výberovej logiky 2 z 3-och v BREAKEROCH.

Pre každú redundanciu sú 3 skrine APU RTS/DRTS.

- Monitorovacie a servisné rozhranie (MSI)

V princípe MSI RTS, MSI DRTS príslušnej redundancie vykonáva monitorovanie APU.

MSI prenáša dáta cez počítače monitorovania (MI) tej istej redundancie z/do príslušných bezpečnostných panelov SICS. MSI tvorí aj rozhranie k servisným jednotkám (SU) príslušnej redundancie, ako aj kanálové rozhranie (GW) k PICS.

- Jednotky MI-BD, MI-ND (Monitorovacie rozhranie)

MI zberajú vybrané signály z počítačov MSI, ktoré sa zobrazujú na signalizačných tabľách bezpečnostných panelov a poskytujú informácie o stave RPS.

Počítač MI zabezpečuje tiež vstupy z tlačidiel (kvitovanie a nulovanie signalizácie) umiestnených na bezpečnostných paneloch - RPP.

- Gateway-e (GW)

Gateway-e sú priemyselné PC s pevnými diskami, na ktorých beží systémový softvér LINUX. Tieto gateway-e sú klasifikované v bezpečnostnej triede II podľa Vyhlášky ÚJD SR č. 50/2006 Z.z. kategórie C (podľa IEC 61226). Gateway-e majú za úlohu konvertovanie komunikačného mechanizmu TXS (PROFIBUS) do komunikačného mechanizmu MODBUS TCP/IP.

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

Počítače GW umožňujú tok dát medzi systémami Teleperm-XS a SPPA-T2000 (blokovou zbernicou cez moduly CM104). Počítače GW posielajú veličiny procesu a hlásenia do systému SPPA-T2000. Časové značky sú dátam priradené v prijímacom module CM104 systému SPPA-T2000.

Počítače GW sú umiestnené spolu s počítačmi MSI v štandardných skriniach .

- Servisná jednotka (SU)

Úlohou servisnej jednotky je:

- podpora periodických skúšok
- úprava parametrov
- diaľková aktualizácia softvéru počítačov pripojených on-line (uvolňovaná použitím hardvérového kľúča)..

Počítače SU sú umiestnené v štandardnej. SU je z pohľadu bezpečnosti neklasifikované zariadenie.

- Vnútorne komunikačné prostriedky

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

- Ranžirovacie skrine

Ranžirovacie skrine sú použité na jednoduché pripojenie signálov zo zariadení technológie alebo iných systémov z technológie k systému TXS a naspäť do technológie.

Ranžirovacie skrine poskytujú možnosť pripojenia rôznych prevodníkov (napr. dvojvodičových alebo štvorvodičových s napájaním alebo bez napájania) a pripojenie signálov z iných systémov kontroly a riadenia (EXCORE, SMS) jednoducho do skríň úpravy signálov SC.

Ako je vysvetlené v kap. 6.5.2.2.1.1, aj systémy RTS aj DRTS majú trojnásobnú redundantnú štruktúru s tromi kanálmi v každej redundancii.

#### **6.5.2.2.1.1.2.1 Popis softvéru**

Bezpečnostné systémy kontroly a riadenia sú typicky implementované ako distribuované počítačové systémy. Ich funkčnosť je rozsiahle definovaná softvérom.

Systémový softvér môže byť rozdelený do dvoch základných častí:

- Offline softvér – ktorý slúži na projektovanie, konfiguráciu, verifikáciu, testovanie a údržbu. Tento softvér beží na servisnej jednotke alebo na projektovom počítači, ktorý je nezávislý od prevádzky elektrárne a nemá priamy vplyv na výkon funkcií SKR.
- Online softvér – ktorý beží v počítačových moduloch systému a priamo vykonáva funkcie SKR, komunikačné funkcie a úlohy on-line automonitorovania počas prevádzky elektrárne. Online softvér môže byť ďalej rozdelený na
  - *Aplikačný softvér*
  - *Systém reálneho času a softvér operačného systému*

*Aplikačný softvér* je nástroj, ktorým sa realizujú funkcie inžinieringu. V tomto softvéri sú vytvorené funkčné blokové moduly (predprogramované a kvalifikované moduly, ktoré vykonávajú elementárne funkcie SKR (ako AND, OR, výber 2 z 3 atď.) a sú pripojené k funkčným schémam SKR.

Tieto funkčné schémy sú potom volané do prostredia reálneho času, ktoré je súčasťou *systému reálneho času a softvéru operačného systému*. Tento systém sa stará o vypracovanie informácií počnúc od čítania a kontrolovania všetkých vstupov, kontrolovania vykonávania funkčných schém a dotknutých komunikácií až k výstupu vypočítaných výsledkov.

Celý inžiniering je vytvorený v grafickom vývojovom prostredí. Tento systém je databázovo orientovaný projektový systém, ktorý zabezpečuje všetky práce spojené s projektovaním a činnosťou systému.

Všetky časti on-line softvéru, ktoré sa podieľajú na iniciácii automatických opatrení, t.j. programy v trase automatického zásahu, sú väčšinou vykonávané cyklicky.

Čas každého cyklu, ktorý nie je použitý na vypracovávanie výsledkov je použitý na autodiagnostiku s cyklickým automonitorovaním. Cyklické automonitorovanie je softvérový program so špeciálnym určením na identifikáciu porúch v hardvéri SKR. V prípade, že porucha je zistená, je to okamžite signalizované na skriniach a sú podniknuté príslušné zákroky .

#### **6.5.2.2.1.1.2.2 HMI - vizualizácia**

Preferovaným systémom pre prevádzkovanie a monitorovanie je PICS. Na obrazovke operátorského terminálu je graficky zobrazovaný prehľad o stave a hlásenia o výstražných signalizáciách bezpečnostného systému. Vizualne zobrazenie je založené na funkčných schémach..

Na bezpečnostnom paneli ochrany reaktora (RPP) na BD, ktorý je súčasťou SICS, je signalizované v oblasti výstražnej signalizácie:

- Pôsobenie (vypínač rýchleho odstavenia)  
Porucha komponentu (vypínač rýchleho odstavenia)

V oblasti indikácie a riadenia v časti rýchleho odstavenia reaktora sú zobrazované stavy funkcií:

- Iniciačné kritérium
- Pôsobenie
- Aktivácia rýchleho odstavenia
- Vypínače a akčné členy sú kompletné:
- Tlačidlo rýchleho odstavenia reaktora

#### **6.5.2.2.1.1.3 Funkcie systémov**

Jednotlivé kanály systému RTS a DRTS redundancí V, W, X generujú signály odstavenia reaktora do výberovej logiky 2 z 3 v RTB A a RTB B, ak boli splnené iniciačné kritériá od technologických parametrov. Funkcie rýchleho odstavenia reaktora od technologických parametrov sú rozdelené na dve diverzity RTS a DRTS. Funkcie a nastavenie systému je v [I.28].

#### **6.5.2.2.1.1.4 Elektrické napájanie**

Koncept elektrickej časti a pomocného napájania je popísaný v kapitole 6.6 PpBS – Elektrické napájanie [I.58].

V tejto kapitole je stanovené:

- Spoločné a základné princípy riešenia pomocných systémov napájania JE
- Požiadavky spotrebičov na elektrické napájanie (popis údajov a hodnoty),
- Popis systémovej schémy napájania JE – Zdroje a siete systému pomocného napájania

Koncept riešenia napájania SKR je zrejmy z výkresu Napájanie SKR - jednopólová schéma [I.57].

Každá skriňa RTS/DRTS je napájaná z dvoch napájacích zdrojov 24V DC s diódami.

Skrine napájania SKR redundancie sú napájané zdrojmi I. kategórie príslušného systému zaisteného elektrického napájania. Kvôli diverzite je pre každú redundanciu jedna skriňa napájania SKR napájaná zo 400 V AC a druhá skriňa napájania SKR je napájaná z 220 V DC.. V týchto skriniach napájania SKR sú prevodníky AC/DC alebo DC/DC, ktoré generujú 24 V DC.

#### 6.5.2.2.1.2 Činnosť obsluhy

Nato aby systémy RTS a DRTS bezpečnostné systémy vykonávali ich bezpečnostné funkcie, sa zásah operátora nepredpokladá.

Operátori podľa predpísaných testovacích postupov musia iniciovať periodické testovanie komponentov (intervaly testov sú definované v súlade s požadovanou spoľahlivosťou systému) (pozrite si kap. 6.5.2.2.1.3).

#### 6.5.2.2.1.3 Popis prevádzky

Systém pracuje automaticky, t.j. že pri vykonávaní bezpečnostných funkcií sa nepredpokladajú žiadne ľudské zásahy.

Čo sa týka testov, RTS/DRTS týchto systémov sú podrobené normálnym testovacím postupom, ktoré sa predpokladajú pre: TXS, t.j.

- autotestovanie
- technické monitorovanie
- periodické testovanie.

Autotestovanie je použité pre všetky procesorové moduly TXS. Všetky komponenty ako CPU, RAM, ROM a rošty sa testujú a kontrolujú cyklicky.

Technické monitorovanie je vykonávané systémom vo vnútri MSI a umožňuje detekovať všetky poruchy a rozdielnosti redundantných meracích signálov od snímačov, prevodníkov, vstupných modulov počítačov atď.

Periodické testovanie zahŕňa funkčné testovanie softvéru a hardvéru a musí byť iniciované manuálne cez SU. V rámci testu (vrátane modulov na prenos signálu a vstupných modulov počítača) sú signály simulované, výstupné kanály sú aktivované a výsledky sú kontrolované pomocou signálov spätnej kontroly a sú automaticky zaznamenané.

Testy sú navrhnuté tak, aby sa prekrývali, a aby boli schopné testovať celý reťazec kontinuálne a mnohonásobnými testami.

Testy počas údržby a po údržbe počas normálnej prevádzky môžu byť vykonávané v súlade s platnými prevádzkovými predpismi bez akéhokoľvek vplyvu na funkčnosť RTBSystému.

Základom jednotiek APU systémov RTS/DRTS sú moduly spracovania CPU SVE2 - 32 bitové mikropočítače. SU má prístup k SVE2 APU cez MSI (vytvorenom takisto z SVE2 modulov).

SVE2 TXS Tieto je možné prevádzkovať hlavne v troch rôznych režimoch prevádzky:

- PREVÁDZKA
- TEST
- DIAGNOSTIKA.

Prechod z jedného prevádzkového režimu do druhého znázorňuje obrázok 6.5.2-9 prílohy 1 tejto kapitoly.

Po zapnutí SVE2 (Stop → Štartmodulu) vykoná tento inicializáciu, úlohy samotestovania a automaticky prechádza do režimu PREVÁDZKA, v ktorom sa v definovanom časovom cykle načítajú vstupné signály, (nadrátované alebo cez sieť), spracúvajú sa moduly funkčných schém a generujú výstupné signály. Prepnutie z režimu PREVÁDZKY do ostatných režimov medzi režimami možno vykonať servisnou jednotkou (SU).

- Každý užívateľ musí mať prístupový kód v servisnej jednotke
- Každému užívateľovi sa prideli úroveň oprávnenia od 0 do 6, pričom vyššia úroveň oprávnení (napr. 4) vždy obsahuje oprávnenia nižších úrovní.

#### **6.5.2.2.1.4 Detailné prvky projektu**

##### **6.5.2.2.1.4.1 Dispozičné riešenie RTS/DRTS**

- Všetky zariadenia a prvky systému RTS a DRTS sú umiestnené v priestoroch HVB.

##### **6.5.2.2.1.4.2 Štruktúra systému a jeho charakteristiky**

RTS a aj DRTS od technologických parametrov má trojredundantnú štruktúru s tromi kanálmi v každej redundancii. Podrobnejší popis RTS, DRTS si pozrite v kap. 6.5.2.2.1.1.

### **6.5.2.3 POPIS SYSTÉMU - EXCORE**

#### **6.5.2.3.1 Účel systému**

Systém merania neutrónového toku EXCORE zaisťuje reguláciu výkonu reaktora, kontrolu periódy a výpočet reaktivity vo všetkých režimoch prevádzky reaktora. Za účelom rýchleho odstavenia reaktora systém EXCORE generuje signály do systému RTB po prekročení medzí výkonu alebo periódy reaktora.

Výsledný signál odstavenia reaktora je vytvorený výberovou logikou systému RTB (pozrite si kap. 6.5.2.1.1.1.2.1).

##### **6.5.2.3.1.1 Opis konštrukcie a funkčnosti**

Systém je usporiadaný v troch identických divíziách, z ktorých každá riadi tri proporcionálne čítače a tri kompenzované ionizačné komory v záujme pokrytia celého potrebného rozsahu detekcie.

Hlavné funkcie systému sú:

- Monitorovanie neutrónového toku pre účely monitorovania aj ochrany.
- Meranie výkonu reaktora
- Výpočet periódy reaktora (, ak bola prekročená príslušná prahová úroveň)

Hardvérová konfigurácia všetkých zariadení pozostáva z nasledujúcich častí (podrobný popis je v kap. 6.5.2.3.1.1.2.1):

- Detektory v technológii
- Systém spracovania neutrónových parametrov (NPPS),
  - o Jednotka úpravy detekcie neutrónov (NDCU).
  - o Jednotka spracovania neutrónových parametrov (NPPU) spracováva vstupy z NDCU, generuje signály výstražnej signalizácie, vydáva signály, riadi testy.
- Systém kontroly reaktivity a zobrazenia (DNCS)
  - o Počítač pre zobrazovanie parametrov a výpočet reaktivity (DARC),

Počas údržby systému sa používajú iba dva nástroje:

- Lokálna jednotka zobrazenia (LDU), ktorá používa PC na zobrazovanie a modifikáciu parametrov

- Automatické testovacie zariadenie (ATU) používaná na vykonávanie testov

Všetky komponenty komunikujú cez optickú sieť (ATU a LDU sú pripojené priamo na predmetnú skriňu).

Podrobný popis vyššie uvedených komponentov je v kap. 6.5.2.3.1.1.2.1.

EXCORE poskytuje signály do nasledovných systémov a zariadení:

- RTS, DRTS
- RCS
- RLS
- RRCS
- PICS,
- na riadiace pracovisko operátora reaktora na dozorniach
- na zavážací stroj
- PAMS
- INCORE
- signály pôsobenia do RTB A a RTB B
- ASFES
- MSI RPS na zobrazenie na dozorniach

a prijíma vstupy z napájania a zo systému jednotného času.

Každá redundancia systému merania neutrónového toku poskytne signály príčin o zapracovaní a poruchovú signalizáciu o stave systému do bezpečnostných panelov SICS.

#### **6.5.2.3.1.1.1 Bezpečnostná a seizmická klasifikácia**

Systém EXCORE je klasifikovaný ako bezpečnostný systém v jednotlivých kategóriach bezpečnosti a seizmickej odolnosti podľa Vyhlášky ÚJD SR č. 50/2006 Z.z., STN IEC 61226, STN IEC 61513 a IAEA NS-G-1.6.

Po uplynutí platnosti Po uplynutí platnosti prechodného ustanovenia uvedeného vo Vyhláške ÚJD SR č. 430/2011 (viď [II.17], §7 „Prechodné ustanovenie, t.j. 31.12.2014) je v platnosti §3 „Kategorizácia vybraných zariadení do bezpečnostných tried“ predmetnej vyhlášky [II.17].

Porovnaním vyhlášok [II.17] a [II.4] môžeme konštatovať, že zaradenie systému EXCORE do bezpečnostných tried a priradenie bezpečnostnej funkcie sa nemení.

EMC kritérium je A [I.61], [I.62]

Podmienky prostredia [I.61]

#### **6.5.2.3.1.1.2 Popis systému**

##### **6.5.2.3.1.1.2.1 Popis hardvéru**

#### **Detektory v technológii**

Ako bolo vysvetlené vyššie, celý rozsah detekcie výkonu je riadený prostredníctvom dvoch druhov detektorov (tri z každého druhu pre každú divíziu):

- vysoko citlivé proporcionálne čítače. Kvôli ich vysokej citlivosti pokrývajú dolný rozsah výkonu a sú preto použité na monitorovanie neutrónového toku keď je reaktor odstavený alebo počas nábehu/výmeny paliva.

- kompenzované ionizačné komory (detektory pásma výkonu), sú použité na pokrytie vysokého pásma výkonu, a preto sa používajú na meranie neutrónového toku keď reaktor pracuje na plný výkon

Detektory pásma zdroja aj detektory pásma výkonu sú nainštalované v pevnej polohe okolo nádoby reaktora.

### **Systém spracovania neutrónových parametrov (NPPS)**

Systém spracovania neutrónových parametrov NPPS pozostáva z:

- jednotky úpravy neutrónovej detekcie (NDCU)
- jednotky spracovania neutrónových parametrov (NPPU)

#### **Jednotka úpravy neutrónovej detekcie (NDCU)**

NDCU predstavuje elektronické rozhranie s neutrónovými detektormi. Obsahuje všetky moduly a dosky, ktoré sú potrebné pre riadenie dvoch typov detektorov, ale zaisťuje rozdielne funkcie v závislosti od dotknutého detektora.

Signály, zbierané jednotkou NDCU sú posielané do jednotky spracovania jadrových parametrov (NPPU, pozri nižšie).

#### **Jednotka spracovania neutrónových parametrov (NPPU)**

Jednotka NPPU prijíma signály z NDCU a spracováva ich.

Tieto vypočítané hodnoty (perióda reaktora a výkon reaktora) sú potom porovnávané v NPPU s prahovými úrovňami a v závislosti od výsledkov porovnania, NPPU môže:

- Vyslať aktivačný signál a dáta, ktoré ho generujú do MSI RPS (RTS/DRTS), cez ktoré budú príslušne zobrazené v dozorniach
- Riadiť vizuálne výstražné signalizácie na dozorniach
- Vyslať aktivačné signály do RTB..
- Vyslať aktivačné signály do RRCS.
- Generovať povely pre zavážací stroj.

Prahové úrovne sú riadené samotnou NPPU. Takže len čo sú žiadané hodnoty zmenené, NPPU vydá indikačné signály pre operátorov, ktorí musia kvitovať zmenu v nastavení prahovej úrovne stlačením tlačidiel na paneli operátora.

### **Systém kontroly reaktivity a zobrazovania (DNCS)**

Systém kontroly reaktivity a zobrazovania zhromažďuje všetky funkcie EXCORE.

DNCS zahrňuje počítač pre zobrazenie parametrov a výpočet reaktivity (DARC), signálov prahových úrovní na pracovisko operátora a prenos dát do PICS a ASFES.

#### **Automatické testovacie zariadenie (ATU)**

ATU je skriňa, určená na periodické testovanie jednotiek NPPU, jednotiek NDCU a detektorov. Pre tento účel je vybavená počítačom, generátorom signálov a tlačiarňou. Jednotka ATU sa taktiež používa pre korekciu žiadaných hodnôt (pozrite si kap. 6.5.2.3.1.2, 6.5.2.3.1.3).

#### **Jednotka lokálneho zobrazenia (LDU)**

Jednotka LDU je aplikácia ktorá je použitá na zobrazenie parametrov a ich modifikáciu.

#### 6.5.2.3.1.1.2.2 Popis softvéru

Projekt softvéru a etapy kódovania sú ľahšie a bezpečnejšie kvôli používaniu vývojového prostredia systému, ktorý slúži na špecifikovanie, projektovanie, kódovanie a verifikáciu systému kontroly a riadenia.

Softvér operačného systému zabezpečuje inicializáciu, autonómne skúšky a rozhrania so I/O doskami a sieťami.

Systémový softvér bol vyvinutý a overený podľa jadrových štandardov pre bezpečnostné systémy 1E založené na softvéri, hlavne podľa IEC60880.

#### 6.5.2.3.1.1.3 Funkcie systému

Systém merania neutrónového toku EXCORE vykonáva nasledovné funkcie [I.47]:

##### 1. Funkcia neutrónových detektorov a káblov

Neutrónové detektory a káble sú zaradené do bezpečnostnej triedy II (podľa Vyhlášky č. 50/2006 Z.z.), Kat A (podľa IEC 61226) a seizmickej kategórie 1a (podľa IAEA NS-G-1.6). Na pokrytie požadovaného rozsahu detekcie sú navrhnuté dva druhy detektorov: detektory pásma zdroja a detektory pásma výkonu.

Nasledujúce funkcie vykonávané neutrónovými detektormi sú súčasťou bezpečnostnej funkcie (podľa Vyhlášky č. 430/2011 Z.z.):

- Funkcia detektorov pásma zdroja:
- Funkcia detektorov pásma výkonu:.

##### 2. Funkcie NPPS

NPPS je klasifikovaný do bezpečnostnej triedy II (podľa Vyhlášky č. 50/2006 Z.z.), Kat A (podľa IEC 61226) a seizmickej kategórie 1a (podľa IAEA NS-G-1.6). NPPS plní nasledovné funkcie:

- Výpočet neutrónového toku v reaktore od dvoch typov detektorov, ktoré sú usporiadané okolo reaktorovej nádoby tak, aby pokrývali celý rozsah detekcie neutrónového
- Výpočet periódy reaktora
- Porovnanie neutrónového výkonu a periódy reaktora s hodnotou zadanej prahovej úrovne odstavenia
- Generovanie signálov do susedných systémov:
  - Systém rýchleho odstavenia reaktora (neutrónový výkon, perióda)
  - Diverzitný systém odstavenia reaktora (neutrónový výkon, perióda)
  - Limitačný systém reaktora (neutrónový výkon, perióda)
  - Systém regulácie výkonu reaktora (neutrónový výkon, perióda),
  - Systém ovládania riadiacich tyčí (neutrónový výkon, perióda),
  - Pohavarijný monitorovací systém (neutrónový výkon, perióda),
  - Systém vnútro reaktorovej kontroly INCORE (neutrónový výkon, perióda)
  - Výkonové vypínače – BREAKER-e
- Riadenie povoľovania nárastu výkonu pásma zdroja
- Riadenie výstražnej signalizácie v dozorniach
- Porovnanie neutrónového toku pásma zdroja pre zavážací stroj
- Zasielanie neutrónových dát do DNCS

### 3. Funkcie DNCS

a) Funkcie bezpečnostnej triedy III (podľa Vyhlášky č. 50/2006 Z.z.):

- Generovanie aktivačných signálov na zavážací stroj

b) Funkcie bezpečnostnej triedy IV (podľa Vyhlášky č. 50/2006 Z.z.):

- Výpočet reaktivity z detekcie pásma zdroja a pásma výkonu.
- Zobrazenie digitálnych hodnôt vypočítaných parametrov, aby mal operátor aktuálne výsledky o meraniach a výpočtoch .
- Zobrazenie porúch hardvéru pre účely diagnostiky.
- Posielanie dát z displeja na monitory blokovej dozorne.
- Audio kanál: Generovanie audio signálu impulzov s frekvenciou priamo úmernou neutrónovému toku pásma zdroja do zosilňovača a reproduktora na dozorniach a na zavážacom stroji.
- Kontrola kontroliek na zavážacom stroji.
- Kontrola kontroliek na paneli rýchleho zásahu pre povolenie nárastu výkonu pásma zdroja.
- Prenos dát do PICS.
- Prenos údajov do analytického strediska fyzikálneho a energetického spúšťania ASFES pomocou siete.

V porovnaní Prílohy č. 1 vyhlášky ÚJD SR č. 50/2006 Z.z. [II.4] a Prílohy č.1 vyhlášky ÚJD SR č. 430/2011 Z.z. [II.17] je zmena v označení bezpečnostnej funkcie IIIk [II.4] na IIIj [II.17], pričom význam popisu funkcie sa nemení. Ostatné bezpečnostné funkcie podľa [II.4] sú voči [II.17] nezmenené.

Funkcie a nastavenie systému je v , [I.28].

#### **6.5.2.3.1.1.4 Elektrické napájanie**

Koncept elektrickej časti a pomocného napájania je popísaný v kapitole 6.6 PpBS – Elektrické napájanie [I.58].

V tejto kapitole je stanovené:

- Spoločné a základné princípy riešení pomocných systémov napájania JE
- Požiadavky spotrebičov na elektrické napájanie,
- Popis schémy systému napájania JE – Zdroje a siete systému pomocného napájania

Koncept riešenia napájania SKR je vidieť na výkrese Napájanie SKR – jedнопólová schéma [I.57].

Všetky skrine NPPS sú napájané vývodmi 230V AC I. kategórie príslušného systému zaisteného elektrického napájania.

Každá redundancia má svoj vlastný zdroj napájania, ktorý je nezávislý od iných redundancií .

#### 6.5.2.3.1.2 Činnosť obsluhy

Počas zvýšenia výkonu alebo počas spustenia blokov musí operátor potvrdiť medzné hodnoty, aby umožnil zvýšenie výkonu.

Taktiež počas kalibrácie musí operátor stlačiť tlačidlá v paneli operátora pre kvitovanie zmeny žiadaných hodnôt. Kalibrácia systému je vykonávaná cez jednotku LDU pripojenú do skríň NPPS.

#### 6.5.2.3.1.3 Popis prevádzky

Počas normálnej prevádzky sú vykonávané merania a systém je schopný produkovať bezpečnostné riadenia. Počas normálnej prevádzky môže byť jednotka LDU zasunutá, aby sa načítali niektoré vnútorné parametre alebo aby sa zmenili niektoré okrajové parametre, také ako je kalibrácia.

Periodický test systému je vykonávaný automatickým testovacím zariadením. Kedykoľvek je NPPS nastavený do režimu testu, je vyslaný signál na vypnutie vysokého napätia do príslušnej jednotky pre detektor pásma zdroja. Týmto spôsobom sú príslušné detektory vypnuté a test môže byť vykonaný bez rizika, že detektor pásma zdroja bude zapnutý, pokiaľ je reaktor na plnom výkone.

Jednotka NPPU cyklicky vykonáva autotestovanie, aby sa verifikovala správna prevádzka komponentov počítača. Autotestovanie sa vykonáva softvérom a kedykoľvek je zistená porucha v systéme, je výstup nastavený do bezpečného stavu, čo zaručuje prístup bezpečnej poruchy systému.

Úlohou periodických testov je odhaliť pomocou autotestov nedetekované poruchy. Periodické testy sa vykonávajú naraz na jednej jednotke NPPU. Jednotka ATU je pripojená a vstupy a výstupy sú simulované. Na konci tejto simulácie sú očakávané výsledky porovnané so skutočnými získanými výsledkami, aby sa stanovilo či jednotka prešla alebo neprešla testom.

#### 6.5.2.3.1.4 Detailné prvky projektu

##### 6.5.2.3.1.4.1 Dispozičné riešenie

Systém EXCORE je umiestnený v priestoroch HVB:

Snímače systému EXCORE sú umiestnené v kanáloch ionizačných komôr.

### 6.5.2.4 POPIS SYSTÉMU - SMS

#### 6.5.2.4.1 Účel systému

Účelom systému SMS je poskytovať signály o prekročení nastavenej medze zrýchlenia v horizontálnom a vertikálnom smere do naväzujúcich systémov.

SMS tiež kontinuálne hodnotí priebeh seizmickej situácie, v prípade výskytu seizmickej udalosti analyzuje a poskytuje vyhodnotenie údajov pre ďalšie použitie.

##### 6.5.2.4.1.1 Opis konštrukcie a funkčnosti

Charakteristiky (frekvencia, amplitúda a fáza) seizmického pohybu podlažia sú poskytnuté systémom SMS prostredníctvom zaznamenávania a vyhodnotenia:

- vstupných pohybov, meraných trojosovými akcelerometrami

- účinkov na príslušné budovy, systémy a komponenty, hodnotené cez zaznamenané dáta vstupných pohybov.

Vyhodnotenia sú vykonávané na PC, ktorý porovnáva projektové spektrum odozvy s vypočítaným spektrom odozvy.

Hlavné komponenty systému SMS sú (pozrite si kap. 6.5.2.4.1.1.2 ohľadne úplného popisu):

- snímače zrýchlenia
- zapisovač pohybov
- seizmický spínač + zapisovač silných pohybov (zodpovedné za signály na rýchle odstavenie reaktora)
- centrum riadenia siete (NCC)

Jeden akcelerometer je taktiež inštalovaný vo vnútri MRB a vydáva signály do PICS, ako aj akcelerometer inštalovaný vo vonkajšom priestore na území JE.

#### **6.5.2.4.1.1.1 Bezpečnostná a seizmická klasifikácia**

SMS je zaradený do BTII a III.

Po uplynutí platnosti Po uplynutí platnosti prechodného ustanovenia uvedeného vo vyhláške ÚJD SR č. 430/2011 (viď [II.17], §7 „Prechodné ustanovenie, t.j. 31.12.2014) je v platnosti §3 „Kategorizácia vybraných zariadení do bezpečnostných tried“ predmetnej vyhlášky [II.17].

Porovnaním vyhlášok [II.4] a [II.17] môžeme konštatovať, že zaradenie systému SMS do bezpečnostných tried sa nemení.

Porovnaním Prílohy č. 1 [II.4] a Prílohy č.1 [II.17] je zmena v označení bezpečnostnej funkcie IIIk [II.4] na IIIj [II.17], pričom význam popisu funkcie sa nemení. Ostatné bezpečnostné funkcie podľa [II.4] sú voči [II.17] nezmenené.

EMC kritérium je A [I.44] príloha 1.

Podmienky prostredia [I.46].

#### **6.5.2.4.1.1.2 Popis systému**

##### **6.5.2.4.1.1.2.1 Popis hardvéru**

Ako je uvedené vyššie, hlavnými súčasťami systému SMS sú:

- snímače zrýchlenia
- zapisovač pohybu
- seizmický spínač + zapisovač silných pohybov
- riadiace centrum siete (NCC)

Snímače zrýchlenia sú priamo napojené k príslušnému zapisovaču pohybu. Týmto spôsobom tvoria autonómnu jednotku, ktorá je priamo pripojená k NCC.

#### **Snímače zrýchlenia**

Snímače zrýchlenia pozostávajú z trojosových akcelerometrov, ktoré merajú zrýchlenie v troch pravouhlých smeroch karteziánskeho priestoru. Zrýchlenie v troch priestorových smeroch je merané tromi kapacitnými

komorami s integrovanými obvodmi (a predzosilňovačmi). Nakoľko snímače reagujú aj na statické zrýchlenie, je vertikálna os kompenzovaná na gravitáciu.

#### **Zapisovač pohybu**

Zapisovač pohybu je riadený procesorom CMOS. Zapisovač filtruje všetky signály prichádzajúce od snímačov v záujme eliminovať falošné javy a zaznamenáva ich do tzv. "pred-udalostnej pamäte". Kedykoľvek je prekročená nastavená prahová úroveň, dáta sú ukladané do záznamovej pamäte až kým, signál znova nepoklesne pod prahovú úroveň.

Celková záznamová doba jednej udalosti je suma doby pred udalosťou, doby udalosti a doby po udalosti. Doby pred a po udalosti môžu byť nastavené používateľom, priamo použitím prenosného PC alebo diaľkovo cez NCC.

#### **Seizmický spínač + zapisovač silného pohybu**

Akcelerometer meria zrýchlenie v troch pravouhlých smeroch karteziánskeho priestoru s tromi kapacitnými komorami s integrovaným obvodom (a predzosilňovačmi). Nakoľko snímače reagujú aj na statické zrýchlenie, je vertikálna os kompenzovaná na gravitáciu.

Zapisovač silného pohybu je riadený procesorom CMOS. Zapisovač filtruje všetky signály prichádzajúce od snímačov v záujme eliminovať falošné javy a zaznamenáva ich do tzv. pred-udalostnej pamäte. Ak je prekročený prah, dáta sú ukladané do záznamovej pamäte až kým, signál znova nepoklesne pod prahovú úroveň.

Aby boli splnené bezpečnostné požiadavky, je funkčnosť spínača oddelená od zapisovača. Tieto sú namontované na rovnakej doske, ale bežia na úplne oddelených procesoroch, ktoré komunikujú nepriamo (cez sériovú linku) zo spínača do zapisovača.

Celková záznamová doba jednej udalosti je suma doba pred udalosťou, doby udalosti a doby po udalosti. Doby pred a po udalosti môžu byť nastavené užívateľom, cez užívateľské sériové rozhranie. Bezpečnostné sériové rozhranie umožňuje prístup k parametrom takým ako sú úrovne výstražných signalizácií a môžu byť sprístupnené iba vnútorne po fyzickom zásahu v zapisovači.

#### **Skriňa riadiaceho centra siete (NCC)**

NCC je riadené procesorom. Ten zahŕňa všetky vlastnosti potrebné na riadenie jednotlivého zapisovača pohybu, ako aj displej a výstup nameraných údajov.

NCC je vybavené s PC, klávesnicou, displejom a tlačiarňou.

Ako je vysvetlené vyššie v popise jednotlivých komponentov, NCC umožňuje prístup k lokálnym jednotkám záznamu, uľahčuje nastavenie parametrov a to, že dáta sú automaticky prenášané do PC na analýzu (pozrite si kap. 6.5.2.4.1.1.2.2).

#### **6.5.2.4.1.1.2.2 Popis softvéru**

Vyhodnocovacie PC je vybavené softvérovým balíkom s tromi modulmi:

- **Modul monitorovania zemetrasenia**, tento modul monitoruje správnu funkciu seizmickej inštrumentácie. V prípade zlyhania NCC, poskytuje všetky potrebné informácie o udalosti a je schopný poskytovať dáta potrebné na preventívnu údržbu systému.

- **Modul analýzy údajov o zemetrasení**, tento modul poskytuje všetky potrebné nástroje na automatizovanú analýzu o zemetrasení, ako bolo zaznamenané zapisovačom pohybu. Počíta:
  - o Čas a hodnotu vrcholového zrýchlenia pre každé miesto
  - o Spektrá odozvy pre každé miesto
  - o Kumulatívnu absolútnu rýchlosť pre každé miesto a každú os.
- **Komunikačný nástroj** umožňuje užívateľovi čítať všetky parametre zapisovača pohybu a NCC a nastaviť nové parametre, ak je to potrebné. Okrem toho komunikačný nástroj ponúka vlastnosti pre manuálny prenos dátových súborov zo zapisovača pohybu.

#### 6.5.2.4.1.1.2.3 Vizualizácia rozhrania človek - stroj

Nasledujúce signály budú zobrazené na displejoch systému PICS:

- prekročenie výstražnej prahovej úrovne jednotlivo pre každý zo snímačov pohybu
- prekročenie prahovej úrovne pre rýchle odstavenie individuálne pre každý zo snímačov pohybu na základovej doske hlavného výrobného bloku,
- prekročenie prahu snímača pohybu na voľnom priestranstve,
- prekročenie referenčného spektra odozvy snímača na voľnom priestranstve,
- začiatok záznamu ktoréhokoľvek zapisovača pohybu (sumárny signál),
- výstraha alebo chyba ktoréhokoľvek zapisovača pohybu alebo NCC (sumárny signál).

Na paneloch SICS budú zobrazované nasledujúce signály cez PCS:

- prekročenie výstražnej prahovej úrovne u ktoréhokoľvek snímača pohybu
- prekročenie prahovej úrovne pre rýchle odstavenie z ktoréhokoľvek snímača na základovej doske hlavného výrobného bloku,
- prekročenie referenčného spektra odozvy snímača pohybu na voľnom priestranstve,
- prekročenie prahu snímača pohybu vo voľnom poli

Nasledujúce signály budú zobrazované na paneloch SICS:

- prekročenie prahovej úrovne pre rýchle odstavenie na viacerých ako jednom snímači pohybu na základovej doske hlavného výrobného bloku v rámci redundancie (2 z 3 indikácií),
- prekročenie prahovej úrovne pre rýchle odstavenie aspoň jedného snímača pohybu na základovej doske hlavného výrobného bloku v rámci redundancie (integrované do sumárnej výstražnej signalizácie „Porucha vstupu z technológie“),
- neplatný signál pre rýchle odstavenie od ktoréhokoľvek snímača na základovej doske hlavného výrobného bloku (integrované do sumárnej výstražnej signalizácie „Porucha vstupu z technológie“),

#### 6.5.2.4.1.1.3 Systémové funkcie

Základné funkcie systému SMS sú:

- zabezpečenie on-line signálov o prekročení nastavenej medze zrýchlenia v horizontálnom a vertikálnom smere do naväzujúcich systémov,
- vyhodnotenie kontinuálneho priebehu seizmickej situácie a pri výskyte seizmickej udalosti analyzovanie a zabezpečenie vyhodnotenia dát pre neskoršie použitie.

#### **6.5.2.4.1.1.4 Elektrické napájanie SMS**

Koncept elektrickej časti a pomocného napájania je popísaný v kapitole 6.6 PpBS – Elektrické napájanie [I.58].

V tejto kapitole je stanovené:

- Spoločné a základné princípy riešenia pomocných systémov napájania JE
- Požiadavky spotrebičov na elektrické napájanie (popis údajov a hodnoty)
- Popis schémy systému napájania JE – Zdroje a siete systému pomocného napájania

Koncept riešenia napájania SKR je zrejmý z výkresu Napájanie SKR – jednopólová schéma [I.57].

Každá systémová skriňa SMS je napájaná z dvoch 24V DC zdrojov s diódami. Skrine napájania SKR redundancie sú napájané zo zdrojov I. kategórie príslušného systému zaisteného elektrického napájania. Kvôli diverzite je pre každú redundanciu jedna napájacia skriňa SKR napájaná zo 400 V AC a druhá napájacia skriňa SKR je napájaná 220V DC z príslušného systému zaisteného elektrického napájania. V skrinách napájania SKR sú prevodníky AC/DC a DC/DC, ktoré generujú 24V DC.

Nesystémová skriňa SMS je napájaná z dvoch zdrojov 24V DC s diódami. Skriňa má dva napájacie privody 24V DC. Každý z privodov 24V DC je napájaný z napájacej skrine SKR.

Skriňa napájania SKR je napájaná zo zdrojov III/I. kategórie systému zaisteného napájania. Kvôli diverzite je jedna napájacia skriňa SKR napájaná zo 400 V AC. a druhá napájacia skriňa SKR je napájaná pomocou 220 V DC.

Skriňa NCC je napájaná redundantným napájaním 24 V DC..

#### **6.5.2.4.1.2 Činnosť obsluhy**

Počas prevádzky pracuje seizmický monitorovací systém automaticky.

#### **6.5.2.4.1.3 Popis prevádzky**

Pri normálnych prevádzkových podmienkach elektrárne a počas všetkých abnormálnych prevádzkových podmienok je seizmický monitorovací systém v aktívnom stave a vykonáva svoje funkcie.

SMS je navrhnutý a inštalovaný takým spôsobom, že je zaručený ľahký prístup a vykonávanie periodických testov a kontrol v prevádzke.

SMS je vybavený vyčerpávajúcou rutinou autotestovania, ktoré monitoruje hlavné vlastnosti zariadenia. Autotest môže byť vykonávaný počas normálnej prevádzky, nakoľko bezpečnostné funkcie systému nie sú ovplyvnené (falošnému pôsobeniu signálov je zabránené).

#### **6.5.2.4.1.4 Podrobný popis projektu**

##### **6.5.2.4.1.4.1 Dispozičné riešenie SMS**

Umiestnenie snímačov zrýchlenia a príslušných zapisovačov pohybu je v priestoroch HVB a vo voľnom poli. Zapisovače pohybu sú inštalované v najbližších miestach v okolí príslušných snímačov zrýchlenia.

##### **6.5.2.4.1.4.2 Štruktúra systému SMS a jeho charakteristiky**

System SMS sa skladá z nasledujúcich zariadení priradených:

- komponenty, ktoré poskytujú aktivačné povely
- komponenty, ktoré poskytujú informácie a nevykonávajú žiadny automatický zásah na bloku.

Zapísovače pohybu sú s NCC prepojené optickými káblami.

## 6.5.2.5 TECHNICKÉ HODNOTENIE

### 6.5.2.5.1 Požiadavky na vybrané zariadenia

Pre celý systém rýchleho odstavenia reaktora, ako je popísaný v tejto kapitole (RTS/DRTS, RTB, EXCORE a SMS), boli vypracované plány kvality 1. a 2. etapy [I.29], [I.34], [I.38], [I.40], [I.41].

Plány kvality obsahujú projektové požiadavky, procesy, postupy a zdroje použité na dosiahnutie bezpečnostných a kvalitatívnych požiadaviek podľa štandardov IEC 61513, IEC 61226 a IEC 60880 a individuálnych požiadaviek Vyhlášky ÚJD SR č. 50/2006 Z.z..

Na splnenie legislatívnych a normatívnych požiadaviek boli použité nasledujúce predpisy, štandardy a príručky:

- Ustanovenia Vyhlášky ÚJD SR č. 50/2006 Z.z.. použité v rozsahu stanovenom prechodným ustanovením §7 Vyhlášky ÚJD SR č. 430/2011 Z.z.
- Ustanovenia Vyhlášky ÚJD SR č. 56/2006 Z.z. použité v rozsahu stanovenom prechodným ustanovením §10 Vyhlášky ÚJD SR č. 431/2011 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 projektovanie hardvéru pre počítačové systémy
- IEC 60980 Doporučené praktiky pre seizmickú kvalifikáciu elektrických zariadení bezpečnostného systému pre jadrové elektrárne
- IEC 60780 Elektrické zariadenia bezpečnostných systémov – kvalifikácia
- IEC 60880 Systémy kontroly a riadenia dôležité pre bezpečnosť – softvérové aspekty pre počítačové systémy, ktoré vykonávajú funkcie kategórie A
- Bezpečnostná príručka IAEA NS-G-1.6.

Systémy RTS (RTS/DRTS, SMS, EXCORE, RTB) prešli takisto cez výrobné preberacie texty (FAT) ([I.71], [I.72], [I.73], [I.74], [I.75], [I.76]). Výsledky týchto testov sú uvedené v správach ([I.77], [I.78], [I.79], [I.80], [I.81], [I.82]).

### 6.5.2.5.2 Seizmická odolnosť

#### – RTB

Seizmická odolnosť zariadení (modulov) použitých aj v logickej časti RTB je zhrnutá v dokumente [I.3] so záverom, že spĺňajú požiadavky pre seizmickú kategóriu 1a.

Dokument [I.17] popisuje plnenie kvalifikačných požiadaviek rozvádzača výkonovej časti RTB. Dokument uvádza súhrn výsledkov skúšok: výkonových vypínačov (breaker-ov) a nízkonapäťového systému s odvolaním sa na príslušné osvedčenia o skúškach / referencie.

#### – RTS/DRTS

Seizmická odolnosť zariadení (modulov) je zhrnutá v dokumente [I.3] so záverom, že spĺňajú požiadavky pre seizmickú kategóriu 1a. Skriňa sa považuje za kvalifikovanú prostredníctvom analýzy.

– **EXCORE**

Systém EXCORE spĺňa seizmické požiadavky ako je preukázané v dokumente kvalifikácia robustnosti zariadenia a seizmická správa [I.22]. V prípade seizmickej udalosti bude systém pokračovať v prevádzke.

– **SMS**

Ako je preukázané v kvalifikačnej správe SMS [I.44], systém je schopný zostať funkčný počas seizmickej udalosti, čo potvrdzuje jeho klasifikáciu 1a.

### 6.5.2.5.3 Princípy bezpečného projektovania

#### 6.5.2.5.3.1 Kritérium jednoduchkej poruchy

– **RTB**

Systém RTB je projektovaný ako dva fyzicky a funkčne oddelené subsystemy (BREAKER A a BREAKER B), a preto je schopný odolať účinkom jednoduchkej poruchy. Projekt zabezpečuje splnenie kritéria jednoduchkej poruchy pre systém ako celok.

– **RTS/DRTS**

Systém RTS(DRTS) spĺňa kritérium jednoduchkej poruchy nasledovne:

- aj systém RTS aj DRTS sú nainštalované v troch fyzicky a funkčne oddelených redundanciách
- každá redundancia RTS, DRTS pozostáva z troch funkčne oddelených kanálov.

Každý kanál redundancie je napájaný z dvoch prívodov, zo skrine napájania. Výpadok jedného z dvoch prívodov nemá za následok nefunkčnosť a nevyvolá ani zapracovanie kanála RTS/DRTS.

Navyše, funkcie rýchleho odstavenia reaktora sú rozdelené do dvoch diverzitných systémov: RTS a DRTS.

– **EXCORE**

Kritérium jednoduchkej poruchy je splnené s vysokou úrovňou redundancie pre systém EXCORE, ktorý pozostáva z deviatich jednotiek spracovania a úpravy neutrónových signálov ktoré sa delia na tri nezávislé redundancie a v každej z troch redundancií sú 3 nezávislé kanály.

– **SMS**

Kritérium jednoduchkej poruchy, v súlade s IEC 61226 je splnené, snímače sú inštalované v troch fyzicky a funkčne oddelených meracích kanáloch (pre funkciu rýchleho odstavenia) v troch redundanciách. Snímače pohybu a zapisovače pohybu sú taktiež vybavené napájaním z príslušnej redundancie.

#### 6.5.2.5.3.2 Kritérium poruchy so spoločnou príčinou

– **RTB**

Aby sa minimalizovali následky poruchy so spoločnou príčinou, RTB je navrhnutý tak, že:

- Hardvérová diverzita je zaručená pre výkonovú časť RTB tak, že sú realizované od dvoch rôznych dodávateľov.
- Dve časti RTB (BREAKER A a BREAKER B sú inštalované v dvoch fyzicky oddelených miestnostiach
- Medzi subsystemami neexistuje žiadna výmena signálov (sú úplne nezávislé).

– **RTS/DRTS**

Na zmiernenie následkov CCF má RTS(DRTS) tieto vlastnosti:

- systémy RTS a DRTS sú funkčne diverzitné
- nie je výmena informácií medzi RTS a DRTS
- umiestnenie troch troj-kanálových subsystémov RTS a DRTS v troch fyzicky oddelených redundanciách
- žiadna výmena signálov medzi subsystémami umiestnenými v uvedených troch redundanciách
- sieťové pripojenia na báze optických vlákien medzi tromi kanálmi redundancie
- tri redundancie majú rozdielne napájacie zdroje.

#### – EXCORE

Medzi tromi redundanciami systému EXCORE sa uplatňuje princíp fyzickej, funkčnej a elektrickej nezávislosti: zostava skriň (NPPS a DNCS) tvoriaca redundanciu sa nachádza v rôznych nezávislých miestnostiach požiarne oddelených od iných redundancií, pričom medzi redundanciami nie je žiadne funkčné ani elektrické spojenie, to znamená, že každá redundancia vykonáva rovnaké funkcie nezávisle od inej redundancie. Tento princíp zabezpečuje predovšetkým ochranu voči poruche so spoločnou príčinou.

#### – SMS

Aby sa zmiernili následky CCF, SMS má tieto vlastnosti:

- tri fyzicky a funkčne oddelené meracie kanály (pre funkciu rýchleho odstavenia) pre príslušnú redundanciu
- medzi redundanciami meracích kanálov SMS nie je výmena informácií
- elektrické napájanie redundancií je vzájomne nezávislé.

Na základe rozhodnutia ÚJD SR č. 449/2011, fáza II, boli vykonané deterministické analýzy na poľnej inštrumentácii pre poruchy so spoločnou príčinou. Boli analyzované nasledujúce reprezentatívne merania:

1. meranie hladín v PG1÷6
2. meranie hladín v kompenzátore objemu,
3. meranie tlaku v parnom kolektore PG1÷6,
4. meranie tlaku v primárnom okruhu reaktora.

Predpísané analýzy zahrnovali:

**(I) Verifikáciu správneho pripojenia odberu impulznej rúrky** t.j. zdieľanie (snímače z rôznych redundancií nesmú byť pripojené k tomu istému odberu).

**Splnené** - Všetky uvažované potrubné odbery a ich usporiadanie zabezpečujú odolnosť voči poruche so spoločnou príčinou. Ak sa vyskytne zlyhanie na jednom odbere, logika odchýlky kanálu zapne výstražnú signalizáciu odchýlky, avšak pôsobenie RTS a ESFAS nezlyhá, ani nenastane falošná zapracovanie RTS ani ESFAS. .

**(II) Verifikácia vedenia signálu cez priechodky kontejnmentu** (napr. v prípade zaplavenia priechodky, signály vedené k rôznym redundanciám nesmú byť ohrozené).

**Splnené** - Všetky uvažované hermetické káblové priechodky a hermetické potrubné priechodky zaisťujú odolnosť voči poruche so spoločnou príčinou. Snímače od rozdielných redundancií sú umiestnené do oddelených hermetických buniek a signály sú vedené nezávislými signálovými cestami. Nie je prepojenie medzi redundanciami a ani medzi kanálmi. Zlyhanie jednej priechodky

spôsobí výstražnú signalizáciu odchýlky kanálu, avšak pôsobenie RTS a ESFAS nezlyhá, ani nenastane falošná zapracovanie RTS ani ESFAS.

**(III) Verifikácia oddeľovacích schopností oddeľovacích ventilov napr., 5-cestné ventily, pre snímače tlakovej diferencie (v prípade nespoľahlivého oddelenie snímača od zberného kolektora ESW, kolísanie tlaku v zbernom kolektore bude ovplyvňovať všetky merania s nedostatočnou synchrónnosťou)**

**Splnené** - Všetky uvažované meracie obvody sú realizované tak, že každý snímač je oddelený od technologického odberu, ako aj od preplachovacieho a zberného kolektora dvomi oddeľovacími ventilmi zapojenými v sérii. Toto usporiadanie zabezpečí dostatočné oddelenie od drenážneho kolektora a technologických odberov.

**(IV) Verifikácia správneho spádu impulzného potrubia** - ak spád nie je dodržaný, prirodzené plyny / vzduch nemôže byť prirodzene odstránený gravitačnými silami z impulzného potrubie a môže nastať systematická chyba merania.

**Splnené** - Všetky uvažované meracie obvody sú dvoch typov trasovania: typ L101-S (meranie hladín v PG1÷6, merania hladín v kompenzátor objemu) a P101-S (meranie tlaku v parnom kolektore PG1÷6, meranie tlaku v primárnom okruhu. Oba typy trasovania poskytujú minimálny spád 5%. Tak je požiadavka splnená.

Ohľadne viac podrobností si pozrite Bezpečnostné a spoľahlivostné analýzy systému ochrany reaktora JE MO34 [I.53]

#### **6.5.2.5.3.2.1 Diverzita**

– **RTB**

Pri RTB je garantovaná hardvérová diverzita tak, že dva BREAKER-e sú výrobky dvoch rôznych výrobcov.

– **RTS/DRTS**

Funkcie rýchleho odstavenia reaktora od technologických parametrov sú rozdelené na dve diverzity RTS a DRTS.

– **EXCORE**

Diverzita nie je uplatnená.

– **SMS**

Diverzita nie je uplatnená.

#### **6.5.2.5.3.2.2 Nezávislosť**

– **RTB**

Funkčná izolácia BREAKER-a A od BREAKER-a B je garantovaná skutočnosťou, že nie je žiadna výmena signálov medzi týmito dvomi subsystémami: tieto dva BREAKER-e sú elektricky oddelené. To znamená, že BREAKER A môže vykonávať svoju funkciu nezávisle od BREAKER-a B a naopak.

Fyzická separácia týchto dvoch subsystémov je zaistená skutočnosťou, že sú fyzicky inštalované v dvoch samostatných miestnostiach.

**– RTS/DRTS**

Nezávislosť RTS a DRTS je zabezpečen:

Funkčnou izoláciou, ktorá neumožňuje interakcie medzi zariadeniami a komponentmi jednotlivých redundancií RTS(DRTS) (použité sú prepäťové bariéry, optické káble, galvanické oddelenie v jednotkách SC).

Fyzickou separáciou: Tri trojkanálové RTS a DRTS sú umiestnené v troch fyzicky separovaných redundanciách so separovanými káblovými trasami.

Separáciou dát, ktorá neumožňuje prenos dát z iných systémov do RTS, DRTS (jednosmerný prenos dát do systémov nižšej bezpečnostnej triedy)

Oddelenie napájania skríň

Do skrine systému sa privádzajú dva nezávislé prívody napájania cez diódové oddelenie (oddelenie dvoch zdrojov napájania).

**– EXCORE**

Funkčná separácia v EXCORE je zaistená:

Inštrumentácia vykonávajúca funkcie bezpečnostnej triedy II (Vyhláška č. 50/2006 Z.z.) je umiestnená v skrinách oddelených od inštrumentácie, ktorá vykonáva funkcie bezpečnostnej triedy III alebo nižšej. Fyzické oddelenie je realizované na mieste (vzdialenosť medzi skriňami), čím sa zaisťuje ochrana pred interakciou, ktorá môže nastať v prípade seizmicity medzi zariadeniami rozličných bezpečnostných tried.

Elektrické oddelenie je realizované medzi zariadením bezpečnostnej triedy II a bezpečnostnej triedy III alebo nižšej [I.47]:

**– SMS**

Za účelom splnenia požiadaviek triedy 1 podľa normy IEC 61513 je funkčnosť spínača oddelená od zapisovača. Takto je zachovaná celková funkčnosť, vrátane kompatibility siete, zatiaľ čo bezpečnostná časť je oddelená od zostávajúcej časti. Obidve časti sú umiestnené na jednej samostatnej doske, ale sú úplne oddelené z pohľadu firmvéru, t.j. obidve časti bežia nezávisle na oddelených procesoroch. Jediná interakcia medzi obidvoma procesormi je cez vedenie jednosmernej sériovej komunikácie z bezpečnostnej kategórie A do procesora bezpečnostnej kategórie C. Vzájomné pôsobenie v opačnom smere nie je možné.

Zapisovače pohybu sú s NCC prepojené optickými káblami.

**6.5.2.5.3.3 Kritérium bezpečnej poruchy****– RTB**

Aktívny stav pre logickú časť RTB zodpovedá bezpečnému stavu LOW=0. Vo výkonovej časti v skutočnosti je podpätťová cievka v normálnom stave pripojená na stav HIGH=1, zatiaľ čo zapínacia cievka je v normálnom stave odpojená pri stave LOW =0. To znamená, len čo sa prichádzajúci signál zmení na stav LOW =0 aj podpätťová aj zapínacia cievka sú odpojené a prúd do CRDM netečie. To isté sa stane v prípade výpadku výkonovej časti od logickej časti (stav bezpečnej poruchy LOW =0).

**– RTS/DRTS**

Detekovaná porucha vo vnútri jednotlivého APU nastaví výstup APU do bezpečného stavu, t.j. signál na prívode do RTB na „0“V - iniciačný signál.

**– EXCORE**

Systém EXCORE je vybavený systémom autodiagnostiky. Ak autodiagnostika zistí poruchu, NPPU informuje operátora na dozorniach nastavením signalizácie pre príslušný NPPU a nastaví binárne výstupné signály do bezpečného stavu.

Pri zistení chyby na karte CPU, softvér preruší činnosť, analógové výstupy sa nastavujú na definovanú hodnotu podľa typu výstupu, binárne výstupy sa nastavujú na preddefinovaný neriadený stav. Následne podpäťový výstup riadi iniciačný signál, pozrite si [I.26].

#### – SMS

Keď je automatickým autotestom zapisovača pohybu alebo NCC detekovaná porucha, zobrazené je varovné alebo chybové hlásenie. V prípade akejkoľvek poruchy je v jednotke riadenia siete aktivované chybové relé a výstražná signalizácia je prenesená do PCS.

Navyše, zapisovače pohybu sú vybavené vnútornou batériou.

#### 6.5.2.5.3.4 Spôľahlivostná analýza

##### – RTS/DRTS, RTB

Pre systém RPS (RTS/DRTS a ESFAS) MO34 boli dodávateľom vypracované pravdepodobnostné spoľahlivostné analýzy, literatúra [I.4], [I.5]. V analýze [I.4] pre funkciu odstavenia reaktora bola modelovaná a analyzovaná nepohotovosť a falošné zapracovanie systému rýchleho odstavenia reaktora od definovaných kritérií.

Predpokladá sa, že:

- Nezávislá porucha softvéru je v modeli konzervatívne uvažovaná pomocou primárnej udalosti s definovanou pravdepodobnosťou.
- Je definovaná pravdepodobnosť poruchy softvéru so spoločnou príčinou v rámci každej redundancie.

Požiadavky a výsledky analýz pre RTS/DRTS a RTB sú v [I.4], [I.5].

Systémy RTS/DRTS a RTB spĺňajú prezentované požiadavky.

Pravdepodobnosť zlyhania systému kontroly a riadenia rýchleho odstavenia reaktora pri výskyte iniciačnej udalosti LB LOCA je malá:

Dominantný príspevok k nepohotovosti je od porúch hardvéru (výkonová a logická časť). Najväčší príspevok k systémovej nepohotovosti (čiastkový príspevok (FC)) je od nedetekovaných porúch jedného kanála programovateľných logických modulov a nedetekovaných porúch hlavných vypínačov (breakerov).

Vysoká úroveň spoľahlivosti systému je daná vysokou úrovňou zálohovania systému využitím nezávislých redundancií a diverzít. Čiastkový príspevok poruchy softvéru CCF v redundancii je relatívne nízky. Príspevok hardvéru a meracích kanálov k nepohotovosti systému je zanedbateľný.

Dominantný príspevok k udalosti falošného zapracovania je od kombinácií porúch hardvéru RTB (výkonová a logická časť). Najväčší príspevok tvoria detekované poruchy programovateľných logických modulov všetkých kanálov, nedetekované opraviteľné poruchy programovateľných logických modulov - jeden kanál a všetky kanály, detekované poruchy programovateľných logických modulov - jeden kanál a detekované poruchy hlavných vypínačov (breakerov) rýchleho odstavenia reaktora.

Príspevok hardvérových modulov je zanedbateľný, pretože majú veľmi vysokú spoľahlivosť a musia zlyhať najmenej štyri rôzne moduly, aby spôsobili falošné odstavenie reaktora.

- **EXCORE**

Podrobná analýza a výpočet spoľahlivosti EXCORE sú uvedené v dokumente [I.25].

Každý kanál každej redundancie systému EXCORE dosahuje vysokú úroveň spoľahlivosti prostredníctvom verifikovaného projektu a kvalifikácie komponentov.

- **SMS**

Pre systém SMS bola vypracovaná analýza spoľahlivosti [I.45]. Výsledné údaje analýzy spoľahlivosti pre systém SMS sú v prílohe 2 dokumentu [I.45].

Výsledky samostatných analýz spoľahlivosti systémov kontroly a riadenia - RTS/DRTS/ESFAS/RTB ([I.4], EXCORE ([I.25]) a SMS ([I.45]) boli použité v spoľahlivostnej analýze [I.5]. V dokumente [I.5] bolo vykonané porovnanie a zjednotenie predpokladov v rôznych analýzach. Výsledky analýz vykonaných v dokumente [I.5] sú reprezentatívne pre všetky iniciačné udalosti. Dokument [I.51] je rozšírením spoľahlivostnej analýzy z [I.5] so zahrnutím snímačov a napájania.

Súhrn výsledkov je v nasledujúcej tabuľke [I.51]:

#### 6.5.2.5.3.5 Kvalifikácia systému

- **RTB**

Kvalifikácia výkonovej časti BREAKER-ov je vykonaná v súlade s Kvalifikačnou špecifikáciou zariadení výkonovej časti RTB [I.12], kde je špecifikovaný príslušný rozsah a všeobecný prístup, vrátane dokumentácie pre kvalifikáciu, príslušné kvalifikačné kroky a podrobný prístup pre kvalifikáciu špecifického druhu elektrického zariadenia. Syntéza výsledkov kvalifikačného procesu sa nachádza v dokumente [I.17], Správa o kvalifikácii. Ako je preukázané v tomto dokumente, výkonová časť RTB spĺňa všetky požiadavky na tento systém. Konkrétne v tomto dokumente.

Čo sa týka logickej časti, kvalifikačný proces je vykonávaný v súlade s požiadavkami dokumentu [I.69] a splnenie týchto požiadaviek je dokumentované v dokumente [I.3] Generická analýza vhodnosti:

- **RTS/DRTS**

Výsledky kvalifikácie hardvéru RTS/DRTS sú zhrnuté v kvalifikačnej správe, dokument [I.3]. Výsledky poskytujú dôkaz, že systém spĺňa požiadavky na výkonnosť v podmienkach prostredia ako sú špecifikované v pláne kvalifikácie systému [I.34].

V tejto správe je ukázané, že komponenty hardvéru RTS/DRTS vyhovujú predpísanému prostrediu.

Kvalifikačná správa taktiež sumarizuje výsledky EMC testu. Zariadenia RTS/DRTS vyhovujú požiadavkám na elektromagnetickú kompatibilitu.

Schopnosť systému SMS zostať funkčný počas seizmických udalostí je preukázaný testovaním.

Správanie sa komponentov v čase je overené aplikovaným programom starnutia.

- **EXCORE**

Kvalifikácia zariadení a komponentov EXCORE je v súlade s ich bezpečnostnou triedou podľa Vyhlášky ÚJD SR č. 50/2006. Podrobnosti o kvalifikačných požiadavkách a pláne kvalifikácie aplikovanom v prípade zariadení a komponentov EXCORE sú uvedené v dokumente [I.64].

V dokumente [I.22] Kvalifikácia robustnosti zariadenia a seizmická správa je zdokumentovaná robustnosť zariadenia EXCORE (testy starnutia) a seizmicita.

Súlad systému s požiadavkami na EMC je zdokumentovaný v dokumente [I.65].

#### – SMS

Výsledky kvalifikácie hardvéru SMS sú zhrnuté v kvalifikačnej správe pre SMS [I.44]. Výsledky poskytujú dôkaz, že SMS spĺňa výkonnostné požiadavky pri podmienkach prostredia ako je stanovené v pláne kvalifikácie systému pre SMS [I.50].

Kvalifikačná správa sumarizuje výsledky skúšok EMC. Zariadenie SMS je v súlade s požiadavkami na elektromagnetickú kompatibilitu ako je požadované v [I.50].

Schopnosť SMS zostať funkčný počas seizmickej udalosti je preukázaná skúškami.

Správanie sa komponentov nad stanovený čas prevádzky je verifikované aplikovaným programom starnutia.

Generická analýza vhodnosti komponentov systému SMS je uvedená v [I.87].

#### 6.5.2.5.3.6 Zaistenie kvality softvéru

#### – RTS(DRTS)

Vývoj SW, integrácia SW a HW, verifikácia, validácia a licencovanie SW sú realizované v súlade s požiadavkami STN IEC 60880 a IEC60880 (5/2006).

##### **Špecifikácia softvéru**

V prípade použitia platformy pre RTS a DRTS, projektovanie systému je prevažne zabezpečené použitím špeciálnych nástrojov systému, ktoré v priebehu tvorby SKR vo veľkej miere podporuje V&V. Špecifikácia softvéru je ukončená jej validáciou.

##### **Výrobné preberacie testy (FAT)**

Za účelom vykonania funkčných testov sú systémy kontroly a riadenia, vrátane skúšobného prostredia, napájania a ostatného potrebného zariadenia, nainštalované na skúšobnom poli. Systém je zostavený presne tak, ako bude inštalovaný na stavbe v rámci architektúry, redundantnosti, diverzity a prepojení medzi rôznymi časťami systému. Vybrané I/O signály sú prepojené so skúšobným prostredím.

Cieľom tejto fázy je verifikovať správnosť funkcie integrovaného systému kontroly a riadenia s jeho užívateľským programovým vybavením podľa programu skúšok, ktorý bol vypracovaný vo fáze projektovania. Na verifikáciu špecifických vlastností systému a systémovú validáciu sú použité systémové testy, radené postupne za sebou.

Táto fáza je ukončená Výrobným preberacím testom (FAT), ktorý demonštruje výsledky funkčných testov podľa skúšobných programov, vopred schválených Zákazníkom.

##### **Verifikácia a validácia**

Verifikácia a validácia (V&V) softvéru prebiehala v dvoch etapách:

- V&V systémových softvérových komponentov (generická kvalifikácia systémového softvéru)
- V&V užívateľského aplikačného softvéru (aplikačný softvér pre MO34 s cyklom vývoja podľa „V“-krivky a jej odpovedajúcim vstupom a výstupom po ukončeníach jednotlivých fáz vývoja)..

Prvá etapa V&V bola vykonaná počas vývoja platformy, pozrite si [I.3].

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

- verifikácie formálnej špecifikácie, použitím špeciálnych nástrojov
- validácie softvéru použitím simulačného nástroja pre validáciu
- testov konfigurácie, správania 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 v zmysle [I.67].

– **EXCORE**

Dodávateľ systému vyvinul softvér podľa medzinárodného štandardu normy IEC60880 pre jadrový bezpečnostný softvér. Využíva sa aplikačne orientovaná knižnica overených opätovne použiteľných softvérových komponentov. Rozsiahle autonómne monitorovanie zabezpečuje veľmi vysokú úroveň pokrytia zistenia potenciálnych porúch prostredníctvom množstva kontrol, ako napríklad vierohodnosť údajov, kontrola rozsahu parametrov, časovanie slučky a pod.

Systém je naprojektovaný od začiatku ako SKR platforma jadrovej bezpečnosti, pričom bol navrhnutý a kvalifikovaný tak, aby spĺňal Európske požiadavky jadrovej bezpečnosti. Systémový softvér sa vyvinul a overil podľa jadrových štandardov pre bezpečnostné systémy 1E založené na softvéri, hlavne podľa IEC 60880. Plán verifikácie a validácie softvéru je uvedený v [I.43].

Systém je navrhnutý ako čo najjednoduchší tak, aby sa zamedzilo jeho zložitosti (jednoduchá slučka, žiadne prerušenia, žiadne pridelenie dynamickej pamäte, žiadna podpora multitaskingu na základe udalosti). Softvér operačného systému zabezpečuje inicializáciu, autonómne skúšky a rozhrania s I/O doskami a sieťami.

Všetky procesné jednotky pracujú asynchrónne tak, že funguje cyklická a sekvenčná samostatná slučka s pevnými cyklami v akýchkoľvek podmienkach zaťaženia (t.j. nezávisle od profilu požiadaviek). Komunikácie medzi rozličnými kanálmi a medzi bezpečnostnými systémami a nebezpečnostnými gateway-mi zaisťujú funkčné oddelenie cez deterministický protokol.

– **SMS**

Zabezpečenie kvality softvéru SMS pre uvedené funkcie je popísané v prílohe č. 1 analýzy spoľahlivosti [I.45]. Plán bezpečnosti podľa IEC 61508 (MRSK2002 – Safety Plan Managementtätigkeit zur funktionalen Sicherheit) bol použitý ako plán zaistenia kvality pre hardvér a softvér. Obsahuje potrebné informácie podľa IEC 60880.

Verifikácia softvéru je plánovaná použitím celkového plánu V&V zariadenia dodatočným základným plánom skúšok pre špecifické položky. Počas vývoja zapisovača silného pohybu boli všetky požiadavky verifikácie softvéru zo štandardu IEC 60880 sledovateľné. Väčšina verifikácie softvéru bola urobená v rámci typovej skúšky pre kompletné zariadenie (integrovaný softvér a hardvér).

Validácia zariadenia bola vykonaná použitím požiadaviek IEC 61508.

### 6.5.2.6 BEZPEČNOSTNÉ ZHODNOTENIE

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

Posúdenie plnenia požiadaviek platnej vyhlášky ÚJD SR č. 430/2011 Z.z. [II.17] voči požiadavkám vyhlášky ÚJD SR č. 50/2006 Z.z. [II.4] je uvedené na konci tejto kapitoly.

#### 6.5.2.6.1 Vyhodnotenie plnenia legislatívnych požiadaviek

Hodnotenie bezpečnosti podľa [II.4] Príloha č. 3, časť B, článok I, ad 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** – 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 ochrannej funkcie.*

**Splnené** – pri RTS/DRTS, on-line monitorovanie je vykonávané cyklicky v každej CPU a I/O doskách.

Periodické testy zahŕňujú:

- Skúšky vstupných kanálov od snímačov alebo iných SKR vstupujúcich do funkčnej schémy
- Skúšky výstupných kanálov od funkčných schém k akčným členom
- Kontrolu integrity implementovaného SW vo všetkých jednotkách CPU
- Kontrolu integrity spúšťačích testov na všetkých 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 ich rozpojenie. Keď sú v skúšobnom móde, napájané sú iba pomocné a signalizačné obvody.

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 I/O 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 ochrannej funkcie, 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. Pozrite si časti kap. 6.5.2.5.1 a 6.5.2.1.1.1.

- (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 paragraf 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 (pozrite si kap. 6.5.2.1.1.1). 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. Výsledky a metóda sú uvedené v 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 [I.66].

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

**Splnené** – softvér pre RTS/DRTS, EXCORE a SMS 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 sú softvéry bezpečnostných systémov s rokmi prevádzkových skúseností, bola pre systémy urobená Analýza spoľahlivosti s dostatočnou dávkou konzervatizmu, ako je dokumentované 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 systémov RTS/DRTS, EXCORE, RTB, SMS 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** – RTS/DRTS, RTB, EXCORE, SMS 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, 6.5.2.4.1.1.2.3 - HMI).

(13) *Bezpečnostný systém sa musí navrhnuť tak, aby sa neprekročili projektové parametre ani pri chybných funkciách 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 pred 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 v Pláne verifikácie a validácie softvéru [I.43] a v Pláne verifikácie a validácie pre hlavný SKR [I.67].

(15) *Bezpečnostný systém musí byť navrhnutý tak, aby rozoznával postulované iniciačné udalosti a uviedol do činnosti systémy 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 kap. 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 systémy RTB, RTS/DRTS, EXCORE a SMS sú vybavené s vhodným HMI (pozrite si bod 12), ktorý umožňuje operátorovi mať úplný prehľad nad technologickými parametrami. Len čo je niektorá z prahových úrovní prekročená alebo nastanú nejaké iniciačné udalosti, sú generované signalizácie a sú ukázané 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.

Všetky dôležité parametre zo systémov RTB, RTS/DRTS, EXCORE a SMS sú správne zaznamenané.

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

**Splnené** – Všetky dôležité parametre zo systémov RTB, RTS/DRTS, EXCORE a SMS 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, systémy RTB, RTS/DRTS, EXCORE a SMS 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 si pozrite kapitolu 5.6 PpBS Ľudské faktory centier riadenia a ovládania [I.63]), vo všeobecnosti je potreba fyzického potvrdzovacieho zásahu vykonaného 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.

**V porovnaní vyhlášok ÚJD SR č. 50/2006 Z.z. [II.4] a 430/2011 Z.z. [II.17] sú v Prílohe č.3 časť B, I. článok L niektoré rozdiely v požiadavkách na bezpečnostné systémy a riadiace systémy.**

Bodu (11) podľa [II.4] zodpovedá bod (14) podľa [II.17], zmena znenia nemá vplyv na splnenie uvedeného kritéria.

Bodu (13) podľa [II.4] zodpovedá bod (16) podľa [II.17], zmena znenia nemá vplyv na splnenie uvedeného kritéria.

Bodu (16) podľa [II.4] zodpovedá bod (19) a (20) podľa [II.17], zmena znenia nemá vplyv na splnenie uvedeného kritéria.

Okrem uvedených rozdielov v znení požiadaviek, sú v Prílohe č.3 , časť B, I., článok L vyhlášky ÚJD SR č. 430/2011 Z.z. [II.17] aj nové požiadavky (7), (8) a (12) (Číslovanie hodnotenia bezpečnosti na začiatku tejto kapitoly je podľa [II.4] Príloha č. 3, časť B, článok I, ad L).

Hodnotenie bezpečnosti podľa nových požiadaviek vyhlášky ÚJD SR č. 430/2011 Z.z.:

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

**Čiastočne splnené** – Pre všetky systémy popísané v tejto kapitole PpBS bol nezávislou organizáciou ISTEK posúdený užívateľský SW počas skúšok FAT tak ako je to uvedené v Pláne nezávislej V&V počítačovo riadených bezpečnostných systémov na potvrdenie ich spoľahlivosti [I.59]. Skúšky SAT budú vykonané po úplnom nainštalovaní systémov na mieste. Následne bude preverený užívateľský SW organizáciou nezávislou od výrobcov jednotlivých systémov tak ako je to uvedené v [I.59]. Výsledky skúšok SAT budú následne zhodnotené v dokumentoch [I.83], [I.84], [I.85], [I.86].

(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 zmiernenie ich následkov.*

**Splnené** – Pre všetky systémy popísané v tejto kapitole PpBS sú vypracované dokumenty, ktoré dokladujú vhodnosť použitej projektovej stratégie pri ich vývoji, výrobe a inštalovaní na JE [I.3], [I.5], [I.25], [I.51] a [I.53].

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

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

**Splnené** - Preukázanie splnenia jednotlivých častí bodu (12) sa nachádzajú v predchádzajúcich (6.5.2.5.3.4, 6.5.2.5.3.6) a nasledujúcich podkapitolách tejto kapitoly 6.5.2 PpBS (6.5.2.6.2, 6.5.2.6.3 a 6.5.2.6.4).

**Záverom možno konštatovať, že hodnotené systémy spĺňajú všetky požiadavky Vyhlášky ÚJD SR č. 50/2006 Z.z. [II.21].**

**Vyhláška ÚJD SR č. 430/2011 Z.z. [II.3] v porovnaní s Vyhláškou ÚJD SR č. 50/2006 Z.z. [II.21] obsahuje navyše ďalšie požiadavky podľa Prílohy č. 3, časť B, I., L (7), (8), (12), pričom požiadavku bodu (7), spĺňa čiastočne.**

#### **6.5.2.6.2 Bezpečnostné hodnotenie - RTS, DRTS a RTB**

Tri fyzicky a funkčne oddelené redundancie RTS/DRTS zaisťujú vykonanie bezpečnostnej funkcie aj pri jednoduchej poruche akéhokoľvek komponentu systému. Systém RTS a DRTS je projektovaný s redundanciou 3x100%.

Systém RTB je projektovaný ako dvojredundantný: RTB A a RTB B. Redundancie sú vzájomne nezávislé.

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

Akčný signál je zapamätaný, vykoná sa bez možnosti prerušenia.

Bezpečnostný systém RTS/DRTS, RTB je správne kvalifikovaný na účinky podmienok prostredia (relatívna vlhkosť, teplota okolia) v súlade so špecifikáciou BDA 003 [I.54], pozrite si takisto § 6.5.2.1.1.1.

Hardvérové a softvérové komponenty použité v aplikáciách bezpečnostného SKR projektu 3. a 4. bloku JE Mochovce sú uvedené so súvisiacimi osvedčeniami o skúškach v prehľade dát špecifických pre Mochovce v dokumente [I.30].

Dokument [I.17] popisuje kvalifikačné požiadavky rozvádzača výkonovej časti RTB. Dokument uvádza súhrn výsledkov skúšok: výkonových odpojovačov (BREAKER-ov) a nízkonapäťového systému.

Kvalifikácia špecifická pre konkrétnu elektrárňu využíva štandardizovaný proces projektovania systému, ktorý je podporovaný súborom kvalifikovaných nástrojov. Tento proces projektovania identifikuje činnosti pri verifikácii a validácii a navrhuje dokumentáciu, ktorá má byť predložená na schválenie. Zoznam vybraných zariadení pre JE Mochovce blok 3 a 4 je uvedený v príslušných plánoch kvality vybraných zariadení ([I.29] pre systém ochrany reaktora).

Hlavné predpisy a štandardy platné pre proces schvaľovania typu:

- pre hardvér: KTA 3503 , IEC 60780, IEEE 323
- pre softvér: IEC 60880, IEEE 1012 ISO 90003

Výrobcovia skrií a hardvérových komponentov musia spĺňať požiadavky noriem pre QM:

- ISO 9001,
- IAEA GS-R3,
- KTA 3507.

Všetky komponenty, klasifikované podľa normy IEC 61226 pre funkcie kategórie A, kompletne spĺňajú požiadavky z „Konceptu EMC“ [I.3] berúc do úvahy zdôvodnenie odchýlok v dokumente [I.27].

#### **6.5.2.6.3 Bezpečnostné hodnotenie - EXCORE**

Systém merania neutrónového toku sa skladá z HW a SW prostriedkov a neutrónovými detektormi.

Pre systém EXCORE boli vypracované PLKVZ pre 1. a 2.etapu

[I.38], [I.39], [I.40], [I.41]. PLKVZ pre 1.etapu [I.40] špecifikuje a určuje požiadavky týkajúce sa etapy projektovania: Systém merania neutrónového toku EXCORE, skrine a neutrónové detektory, ktoré sú inštalované na JE MOCHOVCE blok 3 a 4, vrátane súvisiacich kvalitatívnych a bezpečnostných požiadaviek podľa príslušnej legislatívy.

Výroba a spúšťanie systému EXCORE je v súlade s PLKVZ, etapa 2 [I.41].

PLKVZ pre 2.etapu špecifikuje a určuje požiadavky týkajúce sa etapy výroby / prepravy / skladovania na mieste / spúšťania a prevádzky pre: Neutrónové detektory, káble neutrónových detektorov a skrine systému spracovania neutrónových parametrov, ktoré sú súčasťou EXCORE, inštalovaného na JE MOCHOVCE blok 3, vrátane súvisiacich kvalitatívnych a bezpečnostných požiadaviek podľa príslušnej legislatívy.

Všetky tri redundancie systému sú úplne nezávislé z funkčného aj elektrického hľadiska. Každá z nich je umiestnená v rôznych skriniach a rôznych miestnostiach. Každá redundancia má vlastné nepretržité napájanie. Každá redundancia prijíma dáta z rôznych detektorov a posiela nezávisle výstupné signály pomocou galvanicky oddeleného prijímača.

Porucha jedného meracieho kanála neovplyvňuje kanály inej redundancie a neovplyvňuje rovnako ostatné kanály tej istej redundancie.

Porucha na jednom vyhodnocovacom alebo záznamovom zariadení nespôsobí poruchu rozsahu meracieho kanála.

Porucha v skrini DNCS neovplyvní funkčnosť kanálov ochrany v každej redundancii. Skrine DNCS prijímajú dáta z galvanicky oddelených skríň ochrany prostredníctvom siete.

Pripojenie testera a siete nespôsobí poruchu počas odstavenia testera. Tester neposiela dáta po sieti.

Spĺnenie požiadaviek na zariadenie sa overuje testami FAT [I.42].

#### **6.5.2.6.4 Bezpečnostné hodnotenie - SMS**

Zariadenie SMS spĺňa požiadavky podľa plánu kvalifikácie pre SMS Seizmická odolnosť systému SMS je zhrnutá v kvalifikačnej správe a schopnosť SMS zostať funkčný počas seizmickej udalosti je preukázaná testovaním [I.44].

Na zmiernenie následkov CCF má SMS tieto vlastnosti:

- tri fyzicky a funkčne oddelené meracie kanály (pre funkciu rýchleho odstavenia) pre príslušnú redundanciu
- medzi redundanciami meracích kanálov SMS nie je výmena informácií
- elektrické napájanie redundancií je vzájomne nezávislé

Spoľahlivosť pre SMS je preukázaná v prílohe č. 2 dokumentu „Spoľahlivostná analýza“ [I.45].

### **Záver**

Výsledky analýz bezpečnosti všetkých iniciačných udalostí preukázali, že nedôjde k porušeniu bezpečnostných medzí, ani k porušeniu príslušných akceptačných kritérií. Zhrnutie a vyhodnotenie výsledkov analýz bezpečnosti je uvedené v PpBS, kapitola 7.4 [I.52].

Systém RTS/DRTS, RTB, EXCORE, SMS JE MO34 spĺňa požiadavky na funkčnosť, výkonnosť, spoľahlivosť, minimalizáciu dôsledkov porúch so spoločnou príčinou, požiadavky na kvalifikáciu, diverzitu (diverzita nie je uplatnená v SMS a v EXCORE), podmienky prostredia, na EMC, seizmickú odolnosť a zaistenie kvality.

Technické prostriedky a aj architektúra použitá v projekte MO34 sú overené vo viacerých aplikáciách (JE EBO V2, JE PAKS) s dobrými skúsenosťami.

Splnenie požiadaviek na systémy uvedené v tejto kapitole bolo preukázané úspešným vykonaním skúšok FAT a ich posúdení nezávislou V&V.

Samotné skúšky SAT a ich vyhodnotenia pre systémy RTS/DRTS, RTB, EXCORE, SMS nezávislou skupinou V&V budú vykonané pred zavezením paliva do reaktora 3. bloku MO34. Ich vyhodnotenie bude doplnené do PpBS v rámci jej úpravy vzhľadom na výsledky spúšťania bloku.

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

- [I.1] POSAR EMO 1, 2 arch. č. 254/97 Sign.5986 z 12.12.1997
- [I.2] Kapitola 6.4.2 Systém automatickej ochrany reaktora, PBS pre MO34, VÚJE
- [I.3] Generická analýza vhodnosti: Platforma Teleperm XS,
- [I.4] RPS. Spoľahlivostná analýza,
- [I.5] Spoľahlivostná analýza kombinácie rôznych SKR;
- [I.6] Systémová špecifikácia RPS,
- [I.7] RTS a DRTS. Zoznam vstupných signálov,
- [I.8] RTS & DRTS. Zoznam výstupných signálov,
- [I.9] RTS & DRTS. SKR Špecifikácia funkcií (Level 3),
- [I.10] Systémová špecifikácia RTB, logická časť,
- [I.11] Technická špecifikácia pre výkonovú časť RTB,
- [I.12] Kvalifikačná špecifikácia zariadenia RTB výkonová časť 3. a 4. blok JE Mochovce,
- [I.13] RTB. Zoznam vstupných signálov,
- [I.14] RTB. Zoznam výstupných signálov, P
- [I.15] RTB. SKR Špecifikácia funkcií (Level 3),
- [I.16] RTB. SKR Špecifikácia funkcií (Level 4),
- [I.17] RTB. Správa o kvalifikácii zariadení (Výkonová časť),
- [I.18] Hodnotenie neurčitosti pre signály RTS, DRTS a ESFAS pre bezpečnostné analýzy,
- [I.19] Koncept oddeľovania,
- [I.20] Koncept napájania „hlavného SKR“,
- [I.21] Koncept prevádzky a bezpečnosti bezpečnostného SKR,
- [I.22] Kvalifikácia zariadenia robustnosť a seizmická správa
- [I.23] Tabuľka záťaží, príloha 2, Jednopolové schémy,
- [I.24] Koncept riešenia panelu ochrán reaktora, 2
- [I.25] EXCORE - Pravdepodobnostné hodnotenie spoľahlivosti a bezpečnosti dodaného systému - vykonávací projekt (3. a 4. blok),
- [I.26] EXCORE - Špecifikácia systému Vykonávací projekt (blok 3&4),
- [I.27] Podporný dokument pre zdôvodnenie odchýlok CAS v koncepte EMC,
- [I.28] 3LP/1001 Limity a podmienky bezpečnej prevádzky,
- [I.29] Plán kvality vybraného zariadenia pre systém reaktorovej ochrany (RTS, DRTS, ESFAS/PACS a RTB (logická časť)), fáza projektovania;
- [I.30] Kvalifikácia zariadení SKR „QN101“ pre komponenty bezpečnostného systému SKR,
- [I.31] EXCORE - SFC Zdôvodnenie vykonávacieho projektu (Blok3&4),
- [I.32] Revízia úvodného projektu 3. a 4. bloku JE Mochovce a štúdia realizovateľnosti. Pokyny pre vypracovanie technických dokumentov zhotoviteľa

- [I.33] Nezávislá verifikácia a validácia počítačových bezpečnostných riadiacich systémov,
- [I.34] Plán kvality vybraného zariadenia pre skrine bezpečnostného systému SKR a ranžirovacie skrine pre bezpečnostné systémy, výrobná fáza,
- [I.35] Technologický predpis 3TP/6003 Systém EXCORE,
- [I.36] Plán kvalifikácie EXCORE,
- [I.37] Dokument: WP 04.1 Revize a dopracování Úvodního projektu pro MO34, DPS 3.10.01 SMS Technická zpráva
- [I.38] Revízia IPZK – Kanály ionizačných komôr (3.blok),
- [I.39] Plán zaistenia kvality softvéru,
- [I.40] Plán kvality pre vybrané zariadenie 1.etapa, NPPS & Detektory,
- [I.41] Plán kvality pre vybrané zariadenie 2.etapa, Neutrónové detektory a káble, skrine NPPS,
- [I.42] EXCORE – Postup akceptačných skúšok u výrobcu – 3. blok,
- [I.43] Plán verifikácie a validácie softvéru,
- [I.44] Kvalifikačná správa pre SMS,
- [I.45] Analýza spoľahlivosti SMS,
- [I.46] Popis systému monitorovania seizmicity,
- [I.47] Zdôvodnenie bezpečnostných tried Excore,
- [I.48] TELEPERM XS Product Manuals
- [I.49] Koncept bezpečnej prevádzky JE,
- [I.50] Plán systémovej kvalifikácie pre systém monitorovania seizmicity (SMS),
- [I.51] Kapitola 7.4 Spoľahlivostné analýzy bezpečnostných systémov a ich poľnej inštrumentácie,
- [I.52] Zhrnutie a vyhodnotenie výsledkov analýz bezpečnosti,
- [I.53] Analýza bezpečnosti a spoľahlivosti systému ochrany reaktora JE MO34,
- [I.54] Dod. č. 3 Charakteristiky prostredia - sprievodná technická správa,
- [I.55] Dod. č.. 12 - EMC Koncept - sprievodná technická správa,
- [I.56] Pokyny pre inštaláciu, prevádzku a údržbu výkonovej časti RTB,
- [I.57] Napájanie SKR - jednopólová schéma,
- [I.58] Kapitola 6.6 Elektrické napájanie,
- [I.59] Plán nezávislej V&V počítačovo riadených bezpečnostných systémov na potvrdenie ich spoľahlivosti,
- [I.60] Usporiadanie skriň,
- [I.61] EXCORE Obchodná technická špecifikácia,
- [I.62] Správa o zhode EMC,
- [I.63] Kapitola 5.6 Ľudské faktory centier riadenia a ovládania,
- [I.64] Správa o kvalifikácii zariadení,
- [I.65] Analýza požiadaviek EMC,
- [I.66] Referenčný program zaistenia kvality pre bloky 3 a 4 JE Mochovce,
- [I.67] Plán verifikácie a validácie pre hlavný SKR,

- [I.68] Systémová špecifikácia RLS,
- [I.69] TXS. Kvalifikačný protokol,
- [I.70] RPS-V, Test procedure A1.0.3 software configuration check,
- [I.71] U3, RPS-V, Test procedure A1.3.0 „Function test of RTS functionality“,
- [I.72] U3, RPS-V, Test procedure A1.3.1 „Function test of DRTS functionality“,
- [I.73] U3, RPS-V, System test report A1.4, PNM34521665
- [I.74] Functional test instruction for Seismic monitoring system. Unit 3,
- [I.75] EXCORE- Factory acceptance test procedure – Unit 3,
- [I.76] RTB. FAT procedure. Unit 3,
- [I.77] U3, RPS-V, FAT report, factory acceptance certificate,
- [I.78] U3, RPS-W, FAT report, factory acceptance certificate,
- [I.79] U3, RPS-X, FAT report, factory acceptance certificate,
- [I.80] FAT report for SMS SC=II & SMS SC=III. Unit 3,
- [I.81] EXCORE- Factory acceptance test report – Unit 3,
- [I.82] RTB. FAT report. Unit 3,
- [I.83] Independent V&V safety I&C MO34 evaluation of the SAT RPS Unit 3,
- [I.84] Independent V&V safety I&C MO34 evaluation of the SAT SMS Unit 3,
- [I.85] Independent V&V safety I&C MO34 evaluation of the SAT EXCORE Unit 3,
- [I.86] Independent V&V safety I&C MO34 evaluation of the SAT RTB (Logic part) Unit 3,
- [I.87] Generic Suitability Analysis of Seismic Monitoring System (SMS),

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

- [II.1] IAEA Bezpečnostné štandardy série No. SSR-2/1 - Bezpečnosť JE: Projektovanie - Špecifické bezpečnostné požiadavky, 2/2012
- [II.2] BNS I.1.2/2008 Rozsah a obsah bezpečnostnej správy, ÚJD SR, Bratislava, 11/2008
- [II.3] 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.4] Regulation ÚJD SR No. 50/2006 Coll. on details concerning the nuclear safety requirements for nuclear facilities
- [II.5] Vyhláška ÚJD SR č. 56/2006 Z.z. o požiadavkách na dokumentáciu kvality
- [II.6] 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 v znení Vyhlášky ÚJD SR č. 31/2012 Z.z
- [II.7] Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, IAEA Safety Guide, NS-G-1.3, Vienna 2002
- [II.8] IEC 61508-1-7 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1-7
- [II.9] IEC 61226 : 2009 Nuclear power plants - Instrumentation and control systems important to safety - Classification of instrumentation and control functions

- [II.10] IEC 62340 : 2009 Nuclear power plants-Instrumentation and control systems important to safety-Requirements for coping with common cause failure (CCF)
- [II.11] STN IEC 61513 Jadrové elektrárne. Meranie a regulácia systémov dôležitých pre bezpečnosť. Všeobecné požiadavky na systémy (Jadrová elektrárne. Meranie a regulácia systémov dôležitých pre bezpečnosť. Všeobecné požiadavky na systémy)
- [II.12] IEC 61225 : 2005 Nuclear power plants - Instrumentation and control systems important to safety - Requirements for electrical supplies
- [II.13] IEC 60987 : 2007 Nuclear power plants- Instrumentation and control important to safety - Hardware design requirements for computer -based systems
- [II.14] IEC 60880 : 2006 Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions
- [II.15] IEC 60709 : 2004 Nuclear power plants - Instrumentation and control systems important to safety – Separation
- [II.16] Zákon NR SR č.541/2004 Z.z. o mierovom využívaní jadrovej energie (Atómový zákon) a o zmene a doplnení niektorých zákonov
- [II.17] Vyhláška ÚJD SR č. 430/2011 Z.z o požiadavkách na jadrovú bezpečnosť
- [II.18] Vyhláška ÚJD SR č. 431/2011 Z.z o systéme riadenia kvality
- [II.19] BNS I.1.2/2014 Rozsah a obsah bezpečnostnej správy, ÚJD SR, Bratislava, 01/2014
- [II.20] Rozhodnutie ÚJD SR č. 267/2008Pripomienky k rozsahu a obsahu PBS pre MO34

### III Zdrojové dokumenty, ktoré sú spravidla vytvorené VUJE, a.s.

- [III.1] Technologické zadanie pre ochranné systémy RTS, ESFAS a limitačný systém RLS,
- [III.1] Legislatíva, licencovanie a normatívne požiadavky vo vzťahu k dozorným orgánom,
- [III.2] Kategorizácia systémov SKR a požiadavky na kvalifikáciu,
- [III.3] Priradenie systémov SKR do línií ochrany do hĺbky,
- [III.4] Koncept zberu a spracovania signálov,
- [III.5] Koncept napájania vo všetkých úrovniach riadenia a ovládania,
- [III.6] Koncept EMC, Celková koncepcia a návrh štruktúry SKR,
- [III.7] Kategorizácia vybraných zariadení do bezpečnostných tried - textová časť,
- [III.8] Manuál pre stanovenie, preukazovanie a dokladovanie plnenia kvalifikačných požiadaviek pre nové zariadenia a komponenty,
- [III.9] Parametre prostredia pre normálne a havarijné podmienky DB pre kvalifikáciu
- [III.10] Zpráva; Požadavky na seizmickou odolnosť zařízení pro JE Mochovce ve Slovenské republice. Název přílohy so spektrami: PŘÍLOHA I, Seizmická spektra odezvy v úrovni terénu pro lokalitu EMO (5% útlum, úroveň MVZ = SL2 = RLE) a tabulka amplifikačních faktorů budovy
- [III.11] Systém merania neutrónového toku (EXCORE),
- [III.12] Systém zaistenia bezpečnosti (ESFAS, APS, PV II),
- [III.13] Scenár pre uvedenie bloku do bezpečného stavu po seizmickej udalosti
- [III.14] EMC požiadavky, ÚJV- EGP
- [III.15] EMC koncept, EGP 5030-F-070880

- [III.16] Výkonové vypínače AO (RTS) BREAKER-e,
- [III.17] Podporné T-H analýzy pre „Technologické zadanie pre ochranné systémy RTS, ESFAS a limitačný systém“ vypracované pre MO34.
- [III.18] Systém ochrany reaktora AO (RTS, DRTS) DPS 3.10.01,
- [III.19] Systém zaistenia bezpečnosti (ESFAS) DPS 3.10.01,
- [III.20] Systém merania neutrónového toku (EXCORE) DPS 3.10.01,
- [III.21] Výkonové vypínače AO (RTS) BREAKER-e DPS 3.10.01,
- [III.22] Technická správa pre DCA MO34 0030

**ZOZNAM PRÍLOH**

**ZOZNAM TABULIEK**