ZABEZPEČOVÁNÍ JAKOSTI SOFTWARE BEZPEČNOSTNÍCH SYSTÉMŮ V RÁMCI PROJEKTU „OBNOVA SKŘ JE DUKOVANY“

Česlav Karpeta[1)]
Ondřej Povalač[2)]

[1)] Scientech, Inc.-org. složka, A.Staška 30, 140 00 Praha 4, scikar@mbox.vol.cz
[2)] ČEZ, a.s.-JE Dukovany, 675 50 Dukovany, povalo1.edu@mail.cez.cz

Abstrakt
V referátu je presentován přístup k řešení problematiky zabezpečování jakosti software, implementujícího funkce kontroly a řízení důležité pro jadernou bezpečnost, který je aplikován v projektu obnovy systému kontroly a řízení (SKŘ) Jaderné elektrárny Dukovany. Nejprve je uveden přehled požadavků na zabezpečování jakosti software bezpečnostních systémů jaderných zařízení, tj. systémů, které zajišťují provedení ochranných zásahů v případě nastání abnormálních provozních stavů nebo havarijních podmínek. Následuje popis určité části programu zabezpečování jakosti předmětného software - tato část se týká vývojového procesu software u výrobce. Následují informace o činnostech testování software závěrečných fází vývojového procesu u výrobce a o testování jednotlivých dodávaných systémů, které jsou součásti přejímacích zkoušek u výrobce.

Klíčová slova: jakost software, systémový přístup, testování programů, bezpečnost..

1. Úvod

Obnova SKŘ JE Dukovany je rozsáhlá, investičně a organizačně velmi náročná akce, která probíhá etapovitě v rámci plánovaných odstávek jednotlivých bloků, tj. je realizována za standardního provozu elektrárny. Pro účely této akce byl celý systém kontroly a řízení (SKŘ) bloku rozdělen na tzv. moduly. Jako první v pořadí probíhá obnova modulů M1 a M2 na bloku č.3.

Modul M1 sestává z následujících systémů:
- systém rychlého odstavení reaktoru (RTS)
- systém spouštění technických prostředků pro zajištění bezpečnosti (ESFAS)
- automatika postupného spouštění (ELS)
- systém pohavarijního monitorování (PAMS)
- systém pro podpůrné zásahy (SAS)
- systém pro omezení výkonu reaktoru (RLS)
- systém pro řízení výkonu reaktoru (RCS)
- systém pro ovládání havarijních a regulačních kazet (RRCS).

Modul M2 sestává z následujících systémů:
- ochranný systém parogenerátorů (SGPS)
- systém vnitroreaktorové kontroly (IN-CORE)
- počítačový informační systém (PCS).

Generálním dodavatelem modulů M1 a M2 je ŠKODA Jaderné strojírenství (v dalším ŠJS). Jeho subdodavateli jsou:

- konsorcium francouzských firem Framatome ANP (v dalším FRA) a Data Systems & Solutions (v dalším DSS), které zajišťují návrh a výrobu systémů modulu M1, kromě systému RRCS
- česká firma ZAT, a.s,, která zajišťuje návrh systému RRCS, výrobu systému RRCS a systémů modulu M2
- česká firma I&C Energo, která zajišťuje demontáž starých systémů, instalaci nových systémů a řadu dalších činnosti.

Předmětem tohoto příspěvku je stručný popis zabezpečování jakosti software, pomocí kterého jsou implementovány v obnoveném SKŘ JE Dukovany bezpečnostně nejdůležitější funkce kontroly a řízení, tj. funkce:

- iniciace rychlého odstavení reaktoru (zajišťuje systém RTS)
- iniciace technických prostředků zajišťování bezpečnosti (zajišťuje systém ESFAS)
- odpojování a postupné připojování elektrického napájení komponent bezpečnostních systémů při výpadku systému zajištěného elektrického napájení (zajišťuje systém ELS).

2. Požadavky na zabezpečování jakosti software položek důležitých pro jadernou bezpečnost

Požadavky na zabezpečování jakosti software tzv. položek důležitých pro jadernou bezpečnost (viz níže) vyplývají a jsou součástí požadavků na zajišťování jaderné bezpečnosti jaderných zařízení. Zásady zajišťování jaderné bezpečnosti průmyslových jaderných elektráren byly na mezinárodní úrovni zformulovány v programu „Nuclear Safety Standards“ Mezinárodní agentury pro atomovou energii (IAEA). Pro zajišťování bezpečnosti jaderných elektráren při jejich navrhování byly v rámci tohoto programu zformulovány následující tři obecné požadavky [1]:

- návrh jaderné elektrárny musí obsahovat prostředky pro bezpečné odstavení reaktoru a jeho udržení v bezpečném odstaveném stavu a to jak za provozních podmínek (normální a abnormální provoz), tak i během a po havarijních podmínkách
- návrh jaderné elektrárny musí obsahovat prostředky pro odvod zbytkového tepla z aktivní zóny reaktoru po odstavení reaktoru a to i za havarijních podmínek
- návrh jaderné elektrárny musí obsahovat prostředky pro snížení možnosti úniků radioaktivity a zajištění, aby úniky radioaktivity během provozních podmínek byly pod předepsanými hodnotami a během havarijních podmínek byly pod přípustnými hodnotami.

Pro splnění těchto obecných podmínek byl doporučen systematický postup, založený na zajištění v návrhu jaderné elektrárny dosažení určitých cílů, nebo-li vykonání tzv. bezpečnostních funkcí [2]. Tyto bezpečnostní funkce zahrnují jak funkce, které jsou nezbytné pro předcházení havarijním podmínkám, tak i funkce, které jsou nezbytné pro zmírňování následků havarijních podmínek. Pro realizaci těchto funkcí musí být v projektu jaderné elektrárny navrženy příslušné stavební konstrukce, technologické soubory a zařízení souhrnně označované jako položky důležité pro jadernou bezpečnost.

Pro stanovení požadavků na návrh a provedení stavebních konstrukcí, technologických souborů a zařízení, které zajišťují nebo participují na zajišťování vykonání bezpečnostních funkcí jsou brány v úvahu tři faktory a sice:

- důsledky nevykonání dané funkce, když byla vyžádána
- pravděpodobnost, že funkce bude vyžádána

- pravděpodobnost, že funkce nebude při vyžádání vykonána.

Splnění takto stanovených požadavků zajišťuje, aby "součin" uvedených tří faktorů, který je mírou rizika, spojeného s nevykonáním dané funkce, byl přijatelně malý. Mezinárodní konsensus dosažený ve věci požadavků na návrh systémů, které zajišťují provedení funkcí kontroly a řízení, nezbytných pro dosažení splnění výše uvedených bezpečnostních funkcí, je presentován v [3] a [4].

Jestliže některé části položek důležitých pro jadernou bezpečnost jsou realizovány na bázi programovatelných prostředků digitální výpočetní techniky, pak jakost jejich software souvisí bezprostředně s třetím z výše uvedených faktorů.

2.1 Požadavky české legislativy

Českou legislativu pro oblast zajišťování jaderné bezpečností tvoří tzv. „atomový zákon" [5] a vyhlášky Státního úřadu pro jadernou bezpečnost (SÚJB). Oblasti, které atomový zákon upravuje a které jsou relevantní k projektu „Obnova SKŘ JE Dukovany" jsou v §1 zákona vyspecifikovány takto:

- způsob využívání jaderné energie a ionizujícího záření a podmínky vykonávání činností souvisejících s využíváním jaderné energie a činností vedoucích k ozáření
- výkon státní správy a dozoru při využívání jaderné energie, při činnostech vedoucích k ozáření a nad jadernými položkami.

Obecné požadavky na způsob využívání jaderné energie relevantní k danému projektu a problematice, která je předmětem tohoto článku jsou v §4 zákona stanoveny takto:

- Každý, kdo provádí činnosti související s využíváním jaderné energie je povinen postupovat tak, aby byla přednostně zajišťována jaderná bezpečnost.
- Každý, kdo využívá jadernou energii je povinen dodržovat takovou úroveň jaderné bezpečnosti, radiační ochrany, fyzické ochrany a havarijní připravenosti, aby riziko ohrožení života, zdraví osob a životního prostředí bylo tak nízké, jak lze rozumně dosáhnout při uvážení hospodářských a společenských hledisek.
- Každý, kdo provádí nebo zajišťuje činnosti související s využíváním jaderné energie musí mít zaveden systém jakosti způsobem a v rozsahu stanoveném prováděcím předpisem, s cílem dosažení stanovené jakosti příslušné položky s ohledem na její význam z hlediska jaderné bezpečnosti.

Státní správu a dozor při využívání jaderné energie vykonává Státní úřad pro jadernou bezpečnost. Ve vztahu k předmětnému projektu a předmětu tohoto článku:

- SÚJB vykonává státní dozor nad jadernou bezpečností v prostorách jaderného zařízení
- SÚJB vydává povolení k výkonu činnosti „provedení rekonstrukce nebo jiných změn ovlivňujících jadernou bezpečnost"
- SÚJB schvaluje příslušnou bezpečnostní dokumentaci, programy zabezpečování jakosti, seznamy vybraných zařízení, limity a podmínky bezpečného provozu.

Specifikace systému jakosti, který musí být zaveden pro činnosti související s využíváním jaderné energie je předmětem vyhlášky SÚJB č.214/1997Sb. - viz [6]. Tato vyhláška upravuje:

- zavedení systému jakosti
- požadavky na systém jakosti

- požadavky na zabezpečování jakosti vybraných zařízení z ohledem na jejich zařazení do bezpečnostních tříd
- požadavky na náplň programů zabezpečování jakosti
- kritéria pro zařazení a rozdělení vybraných zařízení do bezpečnostních tříd
- rozsah a způsob provedení seznamů vybraných zařízení.

V §23 této vyhlášky jsou uvedeny následující specifické požadavky týkající se tzv. „zvláštních procesů“, do kterých patří rovněž tvorba software:

- Zvláštní procesy, tj. procesy, u kterých se výsledky nemohou plně ověřovat následnou kontrolou a zkoušením musí mít stanoveny kvalifikační kritéria a musí těmto kvalifikačním kritériím vyhovovat.
- Zvláštní procesy provádějí dostatečně kvalifikované osoby, jejichž znalosti a způsobilost k výkonu činností je pravidelně kontrolována.
- Zařízení pro provádění zvláštních procesů musí být způsobilá a tato způsobilost se ověřuje.
- O splnění kvalifikačních kritérií a o ověření způsobilosti se vedou záznamy.

2.2 Specifické požadavky SÚJB relevantní k projektu „Obnova SKŘ JE Dukovany“

Požadavky české legislativy na návrh a provedení stavebních konstrukcí, technologických souborů a zařízení jaderných elektráren jsou uvedeny ve vyhlášce SÚJB č.195/1999Sb. - viz [7]. Požadavky české legislativy na zajištění jaderné bezpečnosti a radiační ochrany jaderných elektráren při jejich uvádění do provozu a při jejich provozu jsou uvedeny ve vyhlášce SÚJB č.106/1998Sb. – viz [8]. Jejich ustanovení, která jsou relevantní k činnosti „provedení rekonstrukce nebo jiných změn ovlivňujících jadernou bezpečnost“ jsou samozřejmě závazná pro projekt „Obnova SKŘ JE Dukovany“.

Aplikace některých z těchto relevantních ustanovení vyhlášky č.195 na specifické podmínky projektu „Obnova SKŘ JE Dukovany“ je předmětem materiálu „Soubor stanovisek SÚJB k vybraným aspektům obnovy SKŘ JE Dukovany“. Týká se následujících deseti tématických oblastí:

1. bezpečnostní klasifikace systémů SKŘ
2. přijatelnost digitálních softwarových systémů SKŘ důležitých pro jadernou bezpečnost
3. požadavky na vývojový proces software systémů SKŘ důležitých pro jadernou bezpečnost
4. požadavky na verifikaci a validaci (V&V) software bezpečnostních systémů SKŘ
5. požadavky na obranu vůči poruchám se společnou příčinou v důsledku chyb v software bezpečnostních systémů
6. požadavky na komunikaci mezi subsystémy bezpečnostních systémů
7. požadavky na testovatelnost za provozu
8. požadavky na plnění kritéria jednoduché poruchy a na redundanci
9. požadavky na kvalifikaci zařízení a problematika jeho certifikace
10. požadavky na spolehlivost.

K předmětu tohoto článku se bezprostředně vztahují požadavky, uvedené v bodech 1 až 5.

Bezpečnostní klasifikace

Jako závaznou klasifikaci systémů SKŘ jenž jsou důležité pro jadernou bezpečnost stanovil SÚJB tu, která je popsána v standardu IEC 61226 [9]. Tato klasifikace je deterministická a vztahuje se na informační a řídicí funkce a systémy a zařízení, kterými jsou tyto funkce realizovány (v dalším budou označovány zkratkou FSZ-KŘ). Zařazuje FSZ-KŘ do tří

bezpečnostních kategorií A, B, C a do kategorie "neklasifikováno z hlediska jaderné bezpečnosti".

Do bezpečnostní kategorie A patří ty FSZ-KŘ, které mají v oblasti kontroly a řízení základní význam pro zajišťování jaderné bezpečnosti. Jako příklady funkcí kategorie A je možno uvést: rychlé odstavení reaktoru, odvádění zbytkového tepla z aktivní zóny reaktoru, havarijní chlazení aktivní zóny reaktoru. Jako příklady systémů, ve kterých jsou implementovány funkce kategorie A je možno uvést: ochranný systém reaktoru, systém spouštění technických prostředků zajišťování bezpečnosti, informační kanály poskytující informace potřebné pro ruční provádění bezpečnostních zásahů.

Do bezpečnostní kategorie B patří ty FSZ-KŘ, které hrají v oblasti kontroly a řízení doplňkovou roli k úkolům, zajišťovaným FSZ-KŘ bezpečnostní kategorie A. Do bezpečnostní kategorie C patří ty FSZ-KŘ, které hrají v oblasti kontroly a řízení pomocnou úlohu v zajišťování jaderné bezpečnosti. Z jiného zorného úhlu je možno je charakterizovat jako ty FSZ-KŘ, které jsou důležité z hlediska jaderné bezpečnosti avšak nespadají ani do kategorie A ani do kategorie B.

Přijatelnost digitálních softwarových systémů

SÚJB stanovil, že implementace obnovených systémů SKŘ důležitých pro jadernou bezpečnost na bázi volně programovatelných digitálních systémů je přijatelným řešením za předpokladu, že budou splněny následující obecné podmínky:

- návrh, provedení, instalace, odzkoušení, uvedení do provozu a provoz těchto systémů budou splňovat:
  - všechny relevantní požadavky české legislativy pro oblast zajišťování jaderné bezpečnosti
  - požadavky, uvedené v příslušných rozhodnutích SÚJB
  - požadavky, uvedené v materiálu „Soubor stanovisek SÚJB k vybraným aspektům obnovy SKŘ JE Dukovany"
- návrh a provedení obnovených systémů SKŘ důležitých pro jadernou bezpečnost budou splňovat relevantní požadavky a doporučení pro oblast zajištění jaderné bezpečnosti a zabezpečování jakosti, uvedené v dotčených dokumentech IAEA a standardech IEC, ČSN, ISO a doplňkově IEEE.

Požadavky na vývojový proces software

Pro životní cyklus software systémů SKŘ, ve kterých jsou implementovány funkce bezpečnostní kategorie A byl stanoven požadavek, že to musí být dobře strukturovaný cyklus obsahující následující procesy:

- plánovací proces
- vývojový proces
- průřezové procesy
- provozní procesy.

Cílem činností, prováděných v rámci plánovacího procesu bude vytvoření souboru dokumentace, sloužící k řízení a kontrole celého životního cyklu software. Vývojový proces software bude rozdělen do následujících fází: specifikace požadavků na software, návrh software, implementace software, integrace software a integrace software-hardware, testování. Průřezové procesy budou obsahovat činnosti verifikace a validace, činnosti řízení

konfigurace a činnosti z oblasti analýz nebezpečí. Provozní procesy budou sestávat z instalace u uživatele, provozu a údržby u uživatele.

Požadavky na verifikaci a validaci (V&V)

Pro software, ve kterém jsou implementovány funkce bezpečnostní kategorie A se požaduje:

- provádění činností V&V splňujících požadavky standardu IEC 60880 (viz [10]) a to po celou dobu vývojového procesu a následných částí životního cyklu software
- provádění prověrek procesů životního cyklu software, realizovaných u jednotlivých výrobců software.

Za předpokladu, že skupina, která provádí u výrobce činnosti V&V není žádným způsobem zainteresována na vývojovém procesu prověřovaného software se nepožaduje provedení ověření jakosti výsledných software produktů třetí nezávislou organizací.

Požadavky na obranu vůči poruchám se společnou příčinou

Vznesení požadavků na zajištění obrany proti poruchám se společnou příčinou je motivováno nutností připustit existenci chyb ve složitém software, realizujícím funkce, kterými jsou v případě nastání tzv. projektových iniciačních události iniciovány příslušné projektem stanovené ochranné zásahy. Tento software je implementován v každé z redundantních divizí předmětného ochranného či informačního systému a tudíž vznik poruchy v důsledku těchto postulovaných chyb ochromí funkceschopnost každé divize, přesto že tyto divize jsou funkčně odděleny a prostorově separovány. Jako prostředek pro zajištění obrany proti tomuto druhu poruch je požadováno implementovat přijatelnou úroveň diverzního způsobu iniciace projektových ochranných zásahů. Specifické požadavky, stanovené pro tuto oblast je souhrnně možno charakterizovat takto:

- byl vyspecifikován okruh postulovaných iniciačních událostí pro které je nutné zajistit adekvátní diverzní ochranu
- byl vymezen okruh software, ve kterém není nutno postulovat přítomnost zbytkových chyb
- byly vymezeny atributy diverzity, jejichž dosažení bude považováno za přijatelnou implementaci diverzity.

Z hlediska předmětu tohoto článku je účelné blíže se zmínit o tom, co tvoří okruh software, ve kterém není nutno postulovat přítomnost zbytkových chyb. V terminologii materiálu „Soubor stanovisek SÚJB k vybraným aspektům obnovy SKŘ JE Dukovany“ je to tzv. „100% spolehlivý software“. Věcně to je záruka akceptována SÚJB, že jednotlivé software moduly a výsledný software produkt jako celek byly vytvořeny takovým způsobem a absolvovaly takový soubor testů, že je vyloučena existence jakékoliv jeho vnitřní vady, která by mohla ovlivnit jeho schopnost vykonat jemu příslušející funkce.

2.3 Požadavky zákazníka

Zákazník, tj. ČEZ, a.s.-JE Dukovany, stanovil ve smlouvě o dílo na projekt „Obnova SKŘ – moduly M1 a M2“ celkový soubor požadavků, které musí dílo splňovat. Jsou to v prví řadě samozřejmě relevantní požadavky české legislativy pro oblast zajišťování jaderné bezpečnosti a požadavky SÚJB stanovené specificky pro tento projekt. V dalších liniích to jsou, souhrnně řečeno:

- relevantní požadavky ostatní české legislativy (např. legislativy pro oblast radiační ochrany, havarijní připravenosti, požární ochrany, ochrany životního prostředí, atd.)
- relevantní požadavky českých technických norem pro oblast zajišťování jaderné bezpečnosti a jakosti
- zásady a návody IAEA pro oblast zajišťování jaderné bezpečnosti
- relevantní požadavky mezinárodních technických norem, jako např. International Electrotechnical Commission (IEC) pro oblast zajišťování jaderné bezpečnosti a obecné elektrotechniky, International Organization for Standardization (ISO) pro oblast zabezpečování jakosti
- relevantní požadavky amerických právních předpisů, návodů a technických norem; jedná se o předpisy a návody americké komise pro řízení jaderné oblasti (US NRC), a normy Institute of Electrical and Electronics Engineers (IEEE).

Pro oblast zabezpečování jakosti software to konkrétně jsou: IEC 60880, IEC 60880-part 2, IEEE Std 7-4.3.2, vybrané normy z IEEE Standards Collection – Software Engineering, ISO 9000-3, ISO/IEC 12207, ISO 10007.

3. Program zabezpečování jakosti software systémů kategorie A realizovaných technologií SPINLINE 3

Souhrnným názvem „technologie SPINLINE 3“ je v tomto článku označen soubor technických a programových prostředků distribuovaného digitálního řídicího systému, vyvinutého jadernou divizí francouzské firmy Schneider Electric Industries (nyní nesoucí název „Data Sytems & Solutions“), který je primárně určený pro aplikace v systémech kategorie A jaderných zařízení.

Hardware technologie SPINLINE 3 je tvořen:
- procesními jednotkami na bázi procesorů Motorola
- jednotkami pro vstupy a výstupy
- sítěmi pro přenos dat.

Software technologie SPINLINE 3 je modulární software, sestávající z následujících tří části:
- systémového software
- aplikačního software
- vývojového prostředí CLARISSE.

Všechny tyto programové prostředky byly vyvinuty podle požadavků standardu IEC 60880. Systémový software je univerzální software zajišťující systémové služby a plnící úkoly rozhraní mezi hardware a aplikačním software. Aplikační software je „projektově orientována“ část software, určená pro realizaci funkcí požadovaných zákazníkem. Vývojové prostředí CLARISSE je určeno pro poloautomatický návrh a implementaci software. V případě, že existující knihovna modulů aplikačního software nestačí pro návrh funkcí požadovaných zákazníkem, potřebné moduly aplikačního software jsou naprogramovány ručně v jazyce C, podrobeny verifikaci a validaci podle požadavků IEC 60880 a zavedeny do CLARISSE jako tzv. „importované operátory“.

Prostředky technologie SPINLINE 3 jsou použity v některých francouzských jaderných elektrárnách. Pro projekt „Obnova SKŘ JE Dukovany“ jsou pomocí této technologie navrženy a realizovány následující funkce a systémy bezpečnostní kategorie A:

- iniciace rychlého odstavení reaktoru – systém RTS (*„reactor trip system“*)
- iniciace technických prostředků zajišťování bezpečnosti – systém ESFAS (*„engineered safety features actuation system“*)
- automatika postupného spouštění – systém ELS (*„emergency load sequencer“*).

Každý z těchto systémů se skládá z několika subsystémů (vlastních pro daný systém nebo sdílených vícero systémy), obsahujícími jednu nebo více procesních jednotek. Pro každou z nich byl níže popsaným postupem vyvinut příslušný software.

3.1 Použitý model životního cyklu

Model životního cyklu aplikovaný dodavateli systémů RTS, ESFAS a ELS je znázorněn na Obr.1 (převzato z dokumentu FRA „Software Quality Assurance Plan“). Z uvedeného obrázku je zřejmé, že ta část životního cyklu software, která probíhá u výrobce, je rozdělena do následujících fází:

- specifikace požadavků na software
- návrh software
- programování
- testování software
- instalace software.

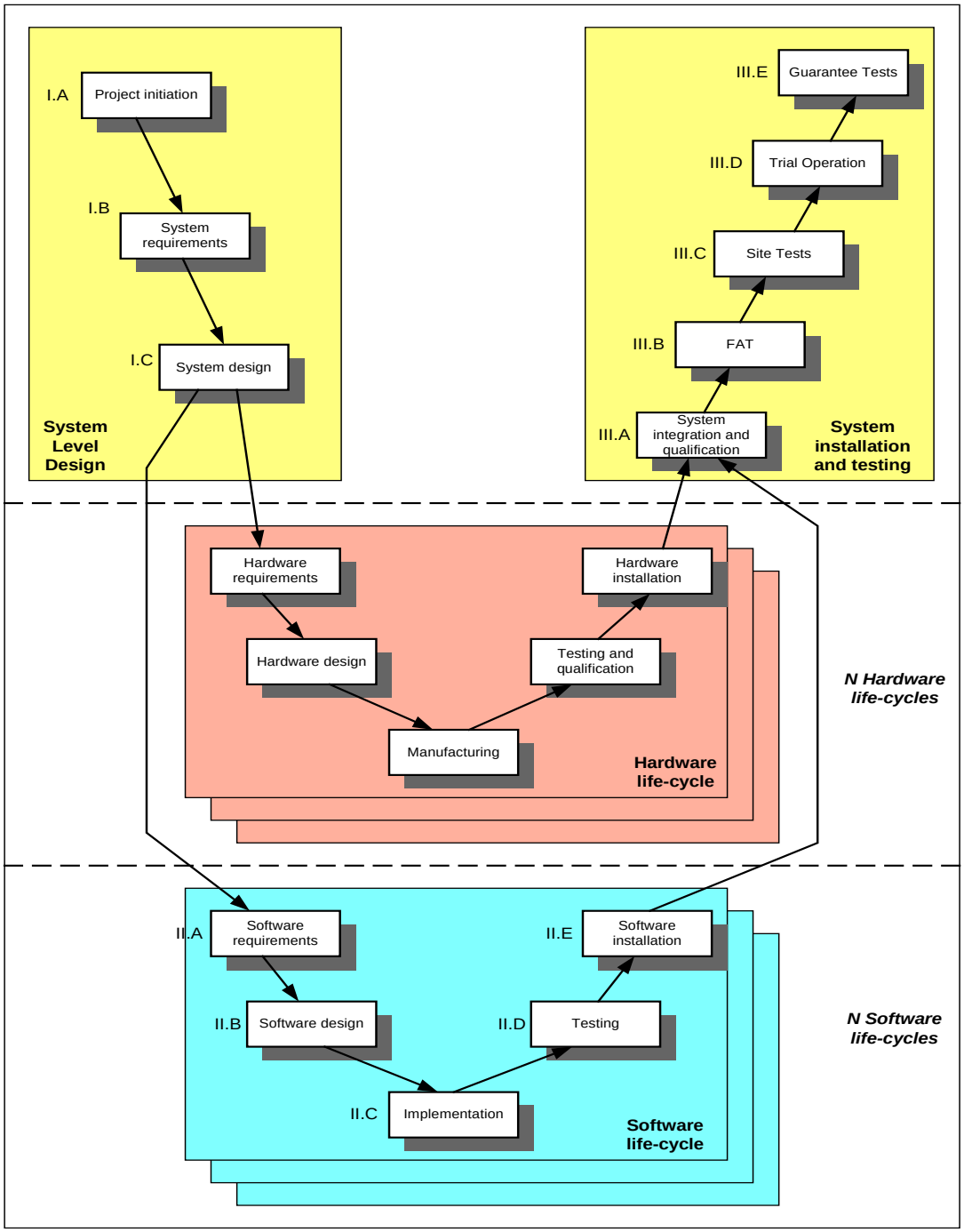
3.2 Přehled plánovacích činností

V rámci plánovacích činnosti byly firmami FRA a DSS zpracovány pro projekt software, který je v rozsahu dodávky dané firmy a který realizuje funkce kontroly a řízení bezpečnostní kategorie A následující dokumenty, které jsou zároveň součástí bezpečnostní dokumentace:

Plán zabezpečování jakosti software
Předmětem tohoto plánu jsou:

- specifikace organizačního zabezpečení projektu
- specifikace činností pro jednotlivé fáze vývojového procesu
- specifikace výstupní dokumentace z jednotlivých fází vývojového procesu
- specifikace kvalifikace a odpovědností jednotlivých týmů, účastnících se projektu
- specifikace metod a postupů, závazných pro projekt
- specifikace software nástrojů, které budou v rámci projektu použity
- specifikace úkolů a záznamů z oblasti zabezpečování jakosti
- problematika řízení rizik.

V obecné rovině se dá konstatovat, že zpracované plány vyhovují požadavkům na tento druh plánovací dokumentace, uvedených v IEC 60880 a IEEE Std 730.



Obr.1 Model životního cyklu

Plán verifikace a validace software

Předmětem tohoto plánu jsou:

- specifikace organizačního zabezpečení procesu V&V
- specifikace úkolů V&V pro jednotlivé fáze vývojového procesu
- specifikace metod a nástrojů pro provádění těchto úkolů
- specifikace dokumentace o provedených úkolech V&V
- problematika řízení rizik.

V obecné rovině se dá konstatovat, že zpracované plány vyhovují požadavkům na tento druh plánovací dokumentace, uvedených v IEC 60880 a IEEE Std 1012.

Plán řízení konfigurace software
Předmětem tohoto plánu jsou:
- specifikace organizačního zabezpečení procesu řízení konfigurace
- specifikace úkolů procesu řízení konfigurace pro jednotlivé fáze vývojového procesu
- specifikace metod a nástrojů pro provádění těchto úkolů
- specifikace dokumentace o provedených úkolech řízení konfigurace.

V obecné rovině se dá konstatovat, že zpracované plány vyhovují požadavkům na tento druh plánovací dokumentace, uvedených v IEEE Std 828.

Plán analýzy bezpečnosti software
Předmětem tohoto plánu jsou:
- specifikace organizačního zabezpečení analýz bezpečnosti software
- specifikace úkolů z oblasti analýz bezpečnosti software pro jednotlivé fáze vývojového procesu
- specifikace metod a nástrojů pro provádění těchto úkolů
- specifikace dokumentace o provedených analýzách bezpečnosti software.

V obecné rovině se dá konstatovat, že zpracované plány vyhovují požadavkům na tento druh plánovací dokumentace, uvedených v IEEE Std 1228.

Plán testování software
Předmětem tohoto plánu jsou:
- specifikace organizačního zabezpečení testování software
- specifikace strategie testování
- návrh testů jednotlivých software komponent
- návrh integračních testů software
- návrh testů výsledného software jednotlivých procesních jednotek
- specifikace metod a nástrojů pro provádění těchto testů
- specifikace dokumentace o provedených testech software.

V obecné rovině se dá konstatovat, že zpracované plány vyhovují požadavkům na tento druh plánovací dokumentace, uvedených v IEC 60880 a IEEE Std 829.

3.3 Přehled činností prováděných v jednotlivých fázích

Fáze „specifikace požadavků na software“
Stanovení požadavků na software pro daný subsystém se provádí na základě vstupní dokumentace pro tuto fázi, kterou tvoří:
- plány projektu software
- výsledky analýzy nebezpečí na systémové úrovni
- výsledky analýzy doby odezvy systému
- specifikace zařízení příslušného subsystému
- specifikace sítí připojených k subsystému
- funkční diagramy subsystému
- specifikace systémového software SPINLINE 3.

Výstupy z této fáze tvoří:
- specifikace požadavků na software (požadavky na funkcionalitu, požadavky na bezpečnost, ostatní požadavky)
- plán testování software
- zprávy o provedených úkolech z oblasti zabezpečování jakosti

- zprávy o provedených úkolech z oblasti verifikace požadavků na software
- zprávy o provedených úkolech z oblasti bezpečnostní analýzy požadavků na software.

Fáze „návrh software“
Návrh software se provádí použitím vývojového prostředí CLARISSE. Vstupními dokumenty pro tuto fázi vývojového procesu jsou:
- plány projektu software
- specifikace požadavků na software
- plán testování software.

Výstupy z této fáze jsou:
- popis návrhu software
- popis návrhu sítí
- zprávy o provedených úkolech z oblasti zabezpečování jakosti
- zprávy o provedených úkolech z oblasti verifikace návrhu software
- zprávy o provedených úkolech z oblasti bezpečnostní analýzy návrhu software.

Fáze „programování“
Zdrojové programy tzv. „importovaných operátorů“ jsou programovány manuálně v jazyce C. Výsledný software procesních jednotek je ve zdrojové i binární podobě generován automaticky příslušnými nástroji vývojového prostředí CLARISSE.

Vstupní dokumentaci pro tuto fázi vývojového procesu tvoří:
- plány projektu software
- popis návrhu software.

Výstupy z této fáze jsou:
- vygenerované programy
- návrh testů, specifikace testů a specifikace postupů pro testování komponent software (tzv. dokument SUTA – *„Software Unit Tests Analysis“*)
- návrh testů, specifikace testů a specifikace postupů pro testování integrace komponent software (tzv. dokument SITA – *„Software Integration Tests Analysis“*)
- návrh testů, specifikace testů a specifikace postupů pro testování software jako celku (tzv. dokument SSTA – *„Software System Tests Analysis“*)
- zprávy o provedených úkolech z oblasti zabezpečování jakosti
- zprávy o provedených úkolech z oblasti verifikace implementace software
- zprávy o provedených úkolech z oblasti bezpečnostní analýzy implementace software.

Fáze „testování“
Vstupní dokumentaci pro tuto fázi vývojového procesu tvoří:
- plány projektu software
- dokumenty SUTA, SITA a SSTA
- specifikace požadavků na software
- popis návrhu software
- popis návrhu sítí

Výstupy z této fáze jsou:
- validovaný software určité procesní jednotky

- zpráva o provedených testech komponent software (tzv. dokument SUTR – *„Software Unit Tests Report“*)
- zpráva o provedených testech integrace komponent software (tzv. dokument SITR – *„Software Integration Tests Report“*)
- zpráva o provedených testech software jako celku (tzv. dokument SSTR – *„Software System Tests Report“*)
- zprávy o provedených úkolech z oblasti zabezpečování jakosti (zejména zpráva o funkční prověrce konfigurace).

Fáze „instalace“
Tato fáze představuje výstupní fázi vývojového procesu software po jeho validaci v rámci fáze „testování“ a před jeho předáním pro tzv. *„interconnected tests“*, tj. validační testy systému jako celku.

Vstupní dokumentace této fáze sestává z:
- plánů projektu software
- specifikace požadavků na software.

Výstupy z této fáze jsou:
- seznam dokumentace software
- uživatelská dokumentace software
- dokumentace pro výrobu software
- závěrečné zprávy o provedených činnostech V&V, analýz bezpečnosti a řízení konfigurace
- zpráva o fyzické prověrce konfigurace.

3.4 Prověrky vývojového procesu software

Průběžné ověřování implementace vývojového procesu software u jednotlivých výrobců probíhá formou technických auditů. Pro software realizující funkce kontroly a řízení spadající do bezpečnostní kategorie A dle IEC 601226, které implementovány technologií SPINLINE 3 jsou tyto audity prováděny u firem FRA a DSS. Jejich cílem je získat nezávislé posouzení plnění požadavků, stanovených na tyto procesy dozorným orgánem a zákazníkem tak, aby byla podpořena důvěra v to, že:
- vývojový proces software byl adekvátně naplánován
- činnosti vývojového procesu software, včetně činností verifikace a validace, řízení konfigurace a analýzy bezpečnosti jsou prováděny v souladu s příslušnými plány.

Audity probíhají podle plánu, zpracovaného firmou Scientech, Inc. V tomto plánu jsou specifikovány:
- zaměření auditů
- požadavky, jejichž plnění bude v rámci auditů ověřováno
- harmonogram provádění auditů
- forma a obsah zpráv z provedených auditů.

Jsou prováděny tři skupiny auditů:
- audity fáze specifikace požadavků na software
- audity fáze návrhu software
- audity fáze výroby a testování software.

Konkrétní požadavky, jejichž plnění je v průběhu jednotlivých auditů ověřováno jsou požadavky a doporučení uvedené v technických normách IEC 60880, 60880-2 a ISO 10007. Tyto požadavky jsou seřazeny do tzv. „formulářů kontrolních otázek“ („*checklists*“). Pro každou položku formuláře je provedeno vyhodnocení jejího plnění a to na základě přezkoumání příslušné dokumentace a pohovorů a diskusí s technickými pracovníky výrobce na pracovištích výrobce. Výsledky vyhodnocení jsou do formuláře zapsány a položce je přiřazen „stav plnění“ jako např. vyhovující, částečně vyhovující apod. Celkové nálezy z jednotlivých auditů jsou formulovány jako tzv. „zjištění“ (*„findings“*), „pozorování“ (*„observations“*) a „otevřené položky“ *(„pending items“*).

Termínem “zjištění” je charakterizována situace, kdy aplikované procesy, činnosti a postupy vykazují významný nesoulad s několika vzájemně souvisejícími položkami checklistů. Vznesení “zjištění” vyjadřuje nález skutečností, které výrazně snižují důvěru v to, že dodaný výrobek bude splňovat stanovené požadavky, tj. že tento výrobek bude dostatečně kvalitní.

Termínem “pozorování” je charakterizována situace, kdy rozdíly mezi ustanoveními technických norem a aplikovanými procesy, činnostmi a postupy nepředstavují v tuto chvíli faktory, způsobující snížení důvěry v dodaný výrobek. Avšak nebudou-li přijatá příslušná nápravná opatření, mohou vést v budoucnu k situacím, které by snížily tuto důvěru.

Termínem “otevřené položky” jsou charakterizovány ty případy, kdy závěr o souladu aplikovaných procesů, činností a postupů s určitými položkami kontrolních seznamů (checklists) mohl být učiněn pouze na základě informací o činnostech, které v době provádění auditu byly aktuálně v chodu nebo byly teprve plánovány. Tyto položky jsou pak projednány v průběhu některého příštího auditu.

K jednotlivým zjištěním a pozorováním auditorský tým specifikuje požadavky a doporučení na jejich řešení. Nálezy a požadavky a doporučení na jejich řešení jsou v závěru auditu projednány s vedením a technickými pracovníky projektového týmu výrobce. Vyhodnocení implementace dohodnutých nápravných opatření se provádí v průběhu příštího auditu.
Každého auditu se v roli pozorovatele účastní specialista SÚJB.

4. Program testování

Testování software realizujícího funkce bezpečnostní kategorie A probíhá ve dvou hlavních etapách:

- testování samotného software jednotlivých procesních jednotek
- testování jednotlivých systémů jako celku.

Náplní první etapy jsou testy komponent software, integrační testy software a validační testy celkového software jednotlivých procesních jednotek na soulad s návrhem software a na soulad s požadavky, stanovenými ve fázi „specifikace požadavků na software“. Testováním systémů jako celku (tzv. *„interconnected tests“*) je ověřován soulad návrhu a provedení jednotlivých systémů se systémovými požadavky na funkcionalitu a výkonnost.

4.1 Testy komponent software

Na této úrovni jsou testovány všechny komponenty aplikačního software pro projekt „Obnova SKŘ JE Dukovany“, které byly programovány manuálně (tzv. importované operátory). Toto testování zahrnuje:

Strukturální statické testy.
Tímto názvem jsou souhrnně označeny následující činnosti:

- kontrola zdrojového programu (provádí se kontrola na soulad s předepsanými pravidly pro programování)
- analýza metrik programu (zjišťuje se např. následující metriky: délka programu, počet instrukcí, počet nepodmíněných skoků apod. a ověřuje se zjištěné hodnoty vůči doporučeným rozmezím hodnot; tuto činnost se provádí nástrojem LOGISCOPE)
- analýza syntaxe programu (provádí se pomoci nástroje LINT).

Funkční dynamické testy
Tímto názvem jsou souhrnně označeny následující činnosti:

- ověření splnění požadavků na funkcionalitu (všechny vstupy komponenty jsou buzeny posloupnostmi hodnot a provádí se porovnání odezev na všech výstupech s požadovanými výsledky; provádění těchto testů je zautomatizováno použitím nástroje ATTOL UNITEST)
- ověření splnění bezpečnostních požadavků
- ověření splnění požadavků na generování a zpracovávání příznaku validity hodnot jednotlivých proměnných
- ověření správnosti fungování programu v nominálních a nenominálních režimech provozu.

Strukturální dynamické testy
Tímto názvem jsou souhrnně označeny následující činnosti:

- kompilace zdrojového programu do instrukcí assembleru ASM
- aktivace vstupů tak, aby předmětnými testy byly pokryty všechny instrukce a větve programu (tyto testy probíhají automaticky pomocí nástrojů ATTOL UNITEST, XRAY DEBUGGER a XRAY SIMULATOR).

Testování komponent aplikačního software probíhá na hardware vývojového prostředí CLARISSE. Soubory testovacích dat jsou konfiguračními položkami spravovanými v rámci tohoto vývojového prostředí. O výsledcích testů je zpracována závěrečná zpráva (dokument SUTR), jejíž součástí jsou záznamy o všech zjištěných neshodách a jejich řešení.

4.2 Integrační testy

Předmětem těchto testů je systémový a aplikační software dané procesní jednotky.
Systémový software technologie SPINLINE 3 byl vyvinut, verifikován a validován v souladu s požadavky normy IEC 60880 a má univerzální použití, tj. je tentýž pro každé nasazení této technologie. Pro dané nasazení však musí být konfigurován. Ověření správnosti provedené konfigurace systémového software probíhá právě v rámci integračních testů. Jejich náplní je:

- ověření správnosti konfiguračních dat ve vztahu k implementované konfiguraci hardware subsystému
- ověření správnosti realizace jednotlivých provozních režimů procesní jednotky a přechodů mezi nimi (inicializace, normální provozní režim, režim „stop“)
- ověření správnosti rozhraní mezi systémovým a aplikačním software.

V případě aplikačního software náplní integračních testů je:

- ověření správnosti vykonávání funkcí, specifikovaných v návrhu aplikačního software
- ověření splnění bezpečnostních požadavků
- ověření přenosu dat mezi jednotlivými funkcemi software
- ověření posloupnosti vykonávání jednotlivých funkcí.

Integrační testy jsou testy typu „bílá skříňka“. Jsou prováděny na cílovém hardware s použitím nástrojů VALLOG a XRAY MONITOR. Soubory testovacích dat jsou konfiguračními položkami spravovanými v rámci vývojového prostředí CLARISSE. O výsledcích testů je zpracována závěrečná zpráva (dokument SITR), jejíž součástí jsou záznamy o všech zjištěných neshodách a jejich řešení.

4.3 Validační testy

Validační testy jsou určeny pro ověření na úrovni subsystému (zpravidla je to jedna vana v jedné ze skříní systému realizovaného technologií SPINLINE 3):

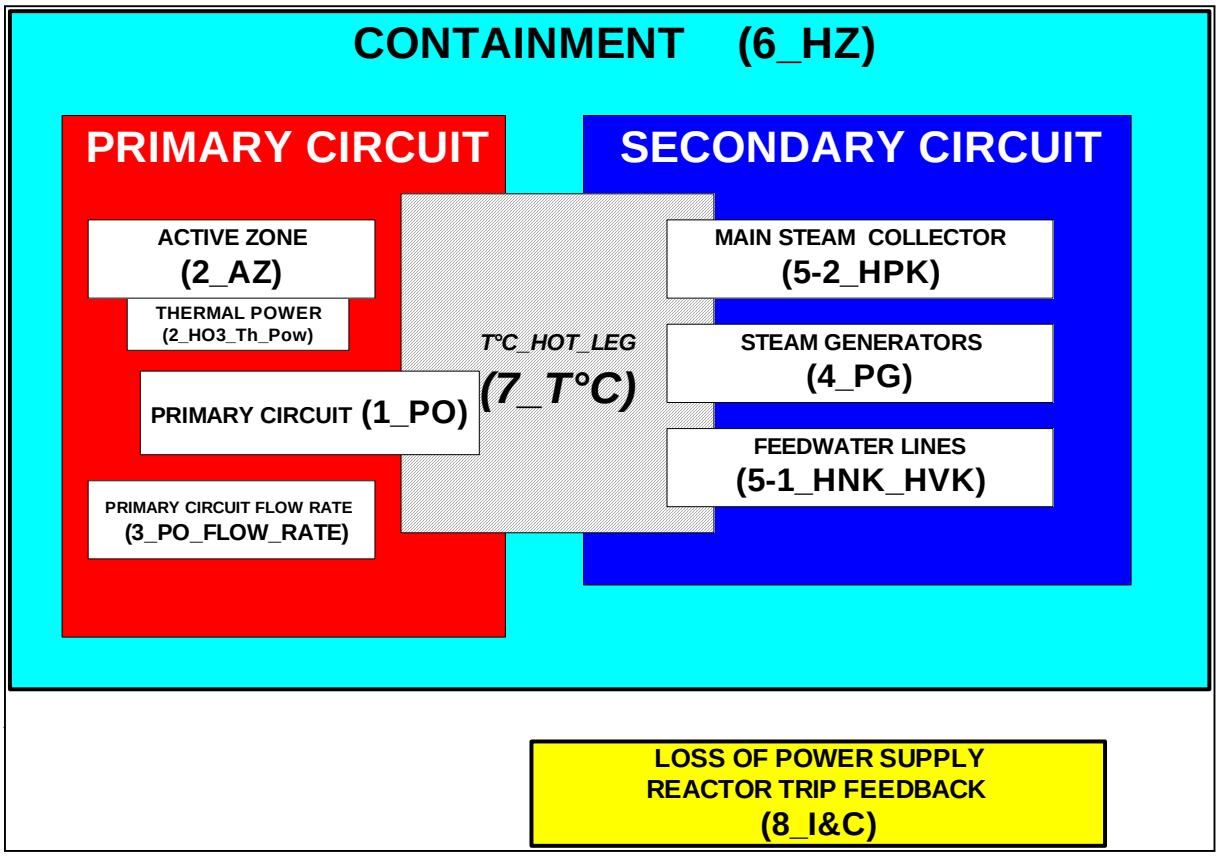
- splnění požadavků na funkcionalitu aplikačního software procesních jednotek daného subsystému, uvedených v dokumentu „specifikace požadavků na software“
- splnění požadavků na rozhraní aplikačního software procesních jednotek daného subsystému, uvedených v dokumentu „specifikace požadavků na software“
- splnění požadavků na výkonnost aplikačního software procesních jednotek daného subsystému, uvedených v dokumentu „specifikace požadavků na software“.

Validační testy jsou testy typu „černá skříňka“. Představují funkční testy první úrovně. Jsou prováděny na cílovém hardware s použitím nástroje VALLOG, v němž je implementován funkční model testovaného software. Soubory testovacích dat jsou konfiguračními položkami spravovanými v rámci vývojového prostředí CLARISSE. O výsledcích testů je zpracována závěrečná zpráva (dokument SSTR), jejíž součástí jsou záznamy o všech zjištěných neshodách a jejich řešení.

4.4 Testy na úrovni systémů („interconnected tests“)

Klíčovou částí těchto testů jsou tzv. funkční testy druhé úrovně. Cílem funkčních testů druhé úrovně je ověření splnění funkčních a výkonnostních požadavků na daný systém. Testované zařízení je oživeno a propojeno na tzv. „*interconnected platform“*, kde je nakonfigurována pokud možno cílová konfigurace zařízení. Jsou zde také prostředky pro simulaci vstupů a vizualizaci výstupů.

Tyto funkční testy jsou organizovány podle tzv. funkčních skupin, které reprezentují určitou úroveň nezávislosti funkcí. Funkční skupiny *(„functional groups“ - FG)*, které jsou základem pro přípravu *„interconnected tests“* jsou znázorněny na Obr.2.



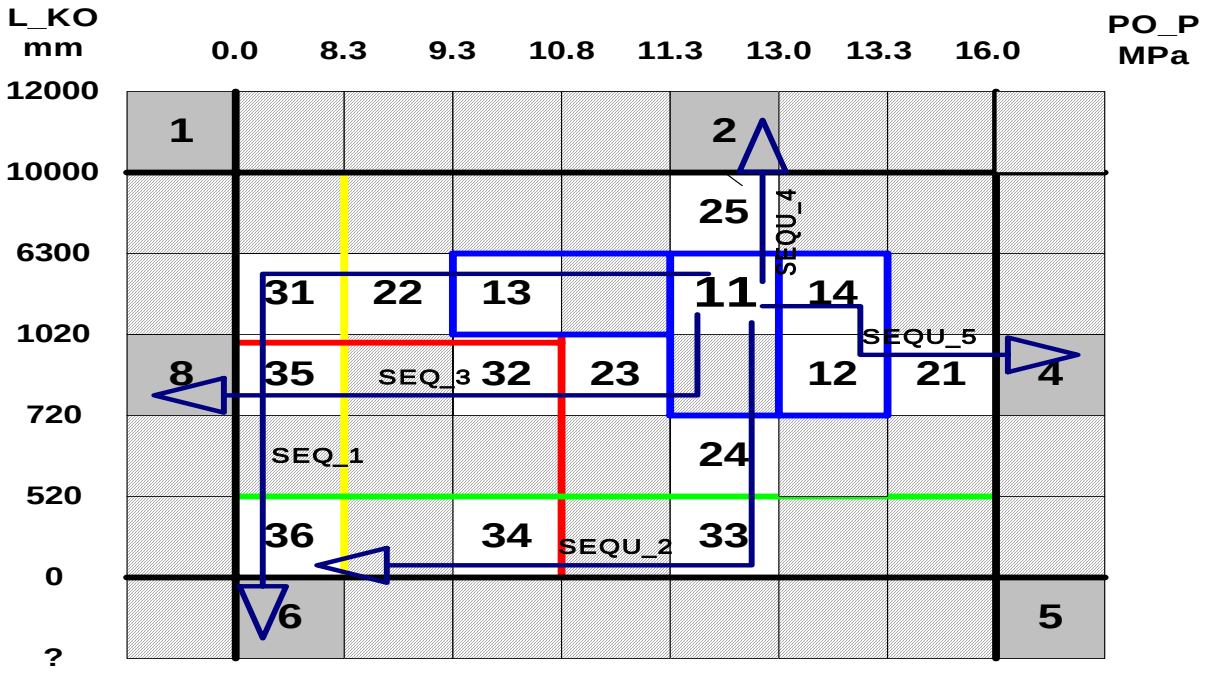
Obr. 2 - Přehled funkčních skupin

Příprava testů každé funkční skupiny sestává z níže popsaných tří fází.

Fáze 1: Příprava grafického funkčního popisu
Uvažované funkční skupiny jsou uvedeny na Obr.2. Každá z nich zahrnuje omezený počet fyzikálních parametrů a jsou dostatečně nezávislé, aby umožnily testování funkčních požadavků odděleně. Pomocí určité matice jsou pro každou část bezpečnostního systému popsány vztahy mezi jednotlivými funkčními skupinami a funkcemi, vyspecifikovanými v systémových funkčních diagramech.

Fáze 2: Příprava specifikace testů
Tato činnost probíhá ve třech krocích.
První krok spočívá v identifikaci všech oblastí (neboli *„test cases“ – TC*) na grafickém popisu, znázorňujícím jednu FG. Tyto TC jsou voleny tak, aby korespondovaly s jedinečnou kombinací vstupů a výstupů. Jinými slovy každá funkční skupina je jakýsi vstupní prostor. Ten je rozdělen na sadu polí, z nichž každé je tzv. *„equivalence class“ - EC*, který odpovídá jednomu TC. Definice EC je založena na tom, že lze předpokládat, že test jedné reprezentativní hodnoty uvnitř EC je ekvivalentní testu jakékoliv jiné hodnoty uvnitř stejného EC, tedy že pokud test s jedním vstupem v rámci EC je správný, pak je program pravděpodobně správný pro všechny vstupy uvnitř tohoto EC – viz [11], odst. 3.2 a 4.3. Tento předpoklad je platný díky vysoké úrovni pokrytí, kterého je dosaženo během validačních testů software.
Potom je provedeno omezení počtu TC, a to na základě následujícího kritéria: Je nutno testovat pouze ty TC, které mají buď rozdílné kombinace vstupů (korespondující odlišným úrovním překročení mezí) nebo rozdílnou konfiguraci výstupů (korespondujícím různým

zásahům/akcím). Na Obr.3 je uveden příklad FG pro závislost dvou parametrů primárního okruhu (L_KO – hladina v kompenzátoru objemu a PO_P – tlak v primárním okruhu) a její rozdělení na jednotlivé TC a vyznačení relevantních TC a jejich číselná identifikace. Použitá metodika identifikuje stav technologie, TC značené číslem 1n označují nominální nebo téměř nominální stav technologie, TC označené 2n označují stav, ve kterém zasahuje systém rychlého odstavení reaktoru (RTS) a TC značené jako 3n označují zásah systémů ESFAS. Čísly 1 až 8 jsou označeny nevěrohodné stavy parametrů, které jsou také testovány.



Obr. 3 – Přehled *„test cases“* pro FG_PO

V druhém kroku je každý TC jednoznačně popsán unikátní kombinací vstupů a výstupů.
Ve třetím kroku se bere v úvahu fyzická konfigurace zařízení, tj. třídivizní uspořádání, přesná testovací konfigurace, testovaná linie ochrany a pod.

Fáze 3: Příprava testovacích sekvencí

V této fázi se připravují elementární sekvence, které budou použity během testu. Jde vlastně o přepis informací, identifikovaných ve fázi 2 do srozumitelnější tabulkové podoby. Jak je vidět z Obr.4, všechny TC musí být pokryty tzv. testovacími sekvencemi, takže je zaručeno, že všechny relevantní TC budou otestovány, včetně limitních hodnot.

Každé takové sekvenci pak přísluší tabulka, která jasně popisuje průběhy vstupních signálů a očekávané výstupy. Příklad takové tabulky pro SEQ_1 je uveden na Obr.4

Step			1	2	3	4	5	6	7	8	9	
Test_Case			**11_00**	**13_**	**22_**	**31_01**	**35_01**	**35_03**	**35_05**	**36**	**6**	
Sensors		T°C	297	297	297	297	297	200	120 Reset 180	200		
	A	PO_P	12,25	10,00	8,80	7,40	7,40	7,40	7,40	7,40	7,40	MPa
			12,250	10,000	8,800	7,400	7,400	7,400	7,400	7,400	7,400	mA
		KO_L	3700	3700	3700	3700	800	800	800	260	-100	mm
			3700	3700	3700	3700	800	800	800	260	-100	mA
	B	PO_P	12,25									
		KO_L	3700									
Signals	HO3			RLS_U09	RLS_U09	RLS_U09	RLS_U09	RLS_U09	RLS_U09	RLS_U09		
	R_Trip						U07_A	U07_A	U07_A	U07_A		
	ESFAS					EU03_A	EU03_A EU04_A	EU04_A		EU04		
Actuation	LPSI					X	X	X		X		
	HPSI					X	X					
	Isol_A					X	X					
	Isol_B					X	X					

Signals EU03, EU04 are switched off after 300s.

Obr. 4 - Příklad sekvence SEQU_1

Uvedená tabulka je již dostatečným podkladem pro vypracování detailního popisu testu, ve kterém jsou uvedeny jak hodnoty vstupních proměnných, tak i očekávané stavy na výstupech systému.
Celé *„interconnected tests“* se potom provádějí podle sborníku procedur popisujících jednotlivé testy, které vznikly právě na základě principů, demonstrovaných na výše uvedeném příkladu.

5. Závěr

Popsaný program zabezpečování jakosti software, ve kterém jsou implementovány ty funkce kontroly a řízení, které zajišťují iniciaci ochranných zásahů v případě nastání abnormálních provozních stavů nebo havarijních podmínek na blocích JE Dukovany je aplikací systémového přístupu k jakosti software. Klade vyvážený důraz na organizační a technické aspekty zabezpečování jakosti výsledného software produktu. Obě tyto skupiny aspektů jsou naplňovány specifickými činnostmi jak u výrobců tak u zákazníka.

U výrobců se jedná zejména o:
- adekvátní implementaci plánovacího procesu
- adekvátní implementaci vývojového procesu
- adekvátní implementaci procesů verifikace a validace, řízení konfigurace a analýz nebezpečí
- adekvátní implementaci procesu testování.

U zákazníka se jedná zejména o:
- vyhodnocování a připomínkování plánovací dokumentace
- vyhodnocování a připomínkování výstupní dokumentace z jednotlivých fází vývojového procesu
- vyhodnocování a připomínkování dokumentace o provedených činnostech verifikace a validace, řízení konfigurace a analýz nebezpečí
- účast při přípravě a provádění *„interconnected tests“*

- prověrky implementace jednotlivých procesů u výrobců a ověřování realizace nápravných opatření.

Literatura:

1. Code on the Safety of Nuclear Power Plants: Design; IAEA Safety Series No. 50-C-D/Rev.1, 1988
2. Safety Functions and Component Classification for BWR, PWR and PTR; IAEA Safety Series No. 50-SG-D1/1979
3. Protection System and Related Features in Nuclear Power Plants; IAEA Safety Series No.50-SG-D3/1980
4. Safety-Related Instrumentation and Control Systems in Nuclear Power Plants; IAEA Safety Series No.50-SG-D8/1984
5. Zákon o mírovém využívání jaderné energie a ionizujícího záření; zákon č.18/1997Sb.
6. Vyhláška SÚJB o zabezpečování jakosti při činnostech souvisejících s využíváním jaderné energie a činnostech vedoucích k ozáření a o stanovení kritérií pro zařazení a rozdělení vybraných zařízení do bezpečnostních tříd; vyhláška č.214/1997Sb.
7. Vyhláška SÚJB o požadavcích na jaderná zařízení k zajištění jaderné bezpečnosti, radiační ochrany a havarijní připravenosti; vyhláška č.195/1999Sb.
8. Vyhláška SÚJB o zajištění jaderné bezpečnosti a radiační ochrany jaderných zařízení při jejich uvádění do provozu a při jejich provozu; vyhláška č.106/1998Sb.
9. Nuclear power plants – Instrumentation and control systems important for safety – Classification; standard IEC 61226
10. Software for computers in the safety systems of nuclear power stations; standard IEC 60880
11. Solutions for cost-effective assessment of software based instrumentation and control systems in nuclear power plants; IAEA TECDOC 1328