BEZPEČNOSTNÍ NÁVODY SÚJB

Bezpečné využívání jaderné energie a ionizujícího záření

Zajištění kvality při tvorbě a užívání výpočetních programů pro hodnocení bezpečnosti

Jaderná bezpečnost

BN-JB-2.4 (Rev.0.0)

SÚJB
STÁTNÍ ÚŘAD PRO JADERNOU BEZPEČNOST

HISTORIE REVIZÍ

Revize č./č. j.	Účinnost od	Garant	Popis či komentář změny
0.0/SÚJB/ORFBA/22212/2020	22. 3. 2021	Marková	Vypracování návodu

Jaderná bezpečnost

Bezpečnostní návod ZAJIŠTĚNÍ KVALITY PŘI TVORBĚ A UŽÍVÁNÍ VÝPOČETNÍCH PROGRAMŮ PRO HODNOCENÍ BEZPEČNOSTI

Vydal: Státní úřad pro jadernou bezpečnost, Praha, březen 2021

Č.j: SÚJB/ORFBA/22212/2020

BN-JB-2.4 (Rev. 0.0)

Účelová publikace bez jazykové úpravy, připomínky směřujte na adresu pripominky_navody@sujb.cz

OBSAH NÁVODU

POUŽITÉ ZKRATKY A POJMY

Zkratky

EU	Evropská Unie
IAEA	International Atomic Energy Agency (Mezinárodní Agentura pro Atomovou Energii)
JZ	jaderné zařízení
PrBZ	provozní bezpečnostní zpráva
SKK	systémy, konstrukce a komponenty
SÚJB	Státní úřad pro jadernou bezpečnost
US NRC	United States Nuclear Regulatory Commission

Definice a pojmy

Poznámka: V této části bezpečnostního návodu jsou definovány pojmy, které nejsou přímo definovány v zákoně [1] a jeho prováděcích předpisech, ale jsou v souladu s textem a definicemi uvedenými v zákoně [1] a jeho prováděcích předpisech. Pojmy, které jsou v zákoně [1] a jeho prováděcích předpisech definovány, jsou v tomto bezpečnostním návodu použity ve významu definovaném v legislativních zdrojích, případně je upřesněno použití některých pojmů v oblasti zaměření tohoto bezpečnostního návodu.

Algoritmus: Přesný návod či postup výpočtu popsaný pomocí matematického modelu, kterým lze vyřešit daný typ úlohy pomocí plánovaného výpočetního systému.

Autorská organizace: Organizace (např. právnická osoba, organizační složka státu, konsorcium apod.) nebo její část, která je autorem výpočetního programu.

Deník údržby výpočetního programu: Dokumentace, do které jsou uživatelskou organizací k dané verzi výpočetního programu zaznamenávány všechny vydané a používané verze a revize výpočetního programu (včetně data zahájení jejich využívání) a záznamy o chybách (případně jejich nahlášení autorské organizaci). Pokud má navíc uživatelská organizace přístup ke zdrojovému kódu výpočetního programu, tak jsou zde zaznamenány i případné opravy a úpravy programu.

Matematický model: Matematický model představuje soubor rovnic a konstitutivních vztahů použitých k vyřešení dané úlohy v uvedeném rozsahu vstupních a výstupních parametrů.

Otestovaný výpočetní program: Výpočetní program, který prošel procesem verifikace a validace.

Ověření: Proces hodnocení určující, zda kvalita nebo provedení produktu nebo služby odpovídá požadavku. Ověřením je v tomto významu myšleno ověření uvedené v § 2 písm. b) vyhlášky [2].

Proces: Pro účely tohoto návodu se pojmem proces (vyznačeným vždy podtrženým textem) rozumí: příprava a provádění výpočetního hodnocení bezpečnosti za použití výpočetního programu ve všech fázích jeho životního cyklu. Na tento proces se vztahují požadavky § 29 odst. 3 zákona [1] a vyhlášky [2].

Spolehlivost: Souhrnný termín používaný pro popis pohotovosti a činitelů, které ji ovlivňují: bezporuchovost, udržovatelnost a zajištěnost údržby [18].

Uživatelská organizace: Organizace (např. právnická osoba, organizační složka státu, konsorcium apod.) nebo její část, která vytvořila nebo legálně získala výpočetní program, a která ho zároveň využívá pro účely provádění výpočetního hodnocení bezpečnosti.

Validační matice: Soubor metod a vstupních a výstupních dat sloužících k validaci výpočetního programu tak, aby byly splněny základní požadavky na ověření jeho kvality.

Validace vstupního modelu: Ověřování správnosti vstupního modelu porovnáním výsledků ověřovacích výpočtů, získaných tímto modelem, s referenčními výsledky naměřenými nebo pozorovanými na reálném zařízení, případně s výsledky získanými jiným validovaným modelem. Součástí validace je i porovnání výsledků výpočtů provedených modelem s naměřenými nebo pozorovanými výsledky za účelem ohodnocení a zdůvodnění odchylek[1]. Verifikace vstupního modelu bývá často prováděna společně s širším procesem validace.

Validace výpočetního programu: Testování a hodnocení výpočetního programu nebo jeho částí, které má za účel ověřit shodu s požadavky na funkci programu a shodu výstupů výpočtu programem s ověřenými výsledky jiných stanovení hodnot výstupů z modelovaných procesů[2]. Validace obecně je definována také v § 2 písm. f) vyhlášky [2].

Verifikace výpočetního programu: Proces hodnocení zdrojového kódu určující, zda výpočetní program správně implementuje matematické modely (používání fyzikálních rovnic, korelací, datových souborů nebo jiných modelů probíhajících procesů). Jedná se o metodu ověření.

Vstupní model: Analytické nebo fyzikální znázornění nebo vyjádření hodnoceného systému (např.: části jaderného zařízení, části životního prostředí apod.), které slouží ke zkoumání nebo hodnocení jeho chování a odezvy na jevy za použití zvoleného výpočetního programu. Vstupní

[1] Vychází z definice v [10]: „***model validation.*** The *process* of determining whether a *model* is an adequate representation of the real *system* being modelled, by comparing the predictions of the *model* with observations of the real *system*. Usually contrasted with *model verification*, although *verification* will often be a part of the broader *process* of *validation*."

[2] Vychází z definice v [10]: „***system code validation.*** *Assessment* of the *accuracy* of values predicted by the *system code* against relevant experimental data for the important phenomena expected to occur."

model obvykle zahrnuje geometrii systému, počáteční a okrajové podmínky, časové závislosti a zadání jevů relevantních pro výpočet.[3]

Vykonavatel autorských práv: Organizace (např. právnická osoba, organizační složka státu, konsorcium apod.) nebo její část, která na základě svých autorských práv provádí distribuci výpočetního programu a zodpovídá za jeho údržbu.

Výpočetní hodnocení bezpečnosti: Hodnocení bezpečnosti (ve smyslu § 48 odst. 1 zákona [1] a [9]), které je prováděno výpočetními programy. Jednou z částí je provádění bezpečnostních analýz.

Výpočetní program (také výpočetní kód, výpočetní prostředek): Soubor výpočetních postupů naprogramovaných ve zvoleném programovacím jazyce za účelem simulace dějů a procesů pomocí numerických a analytických metod. Výpočetní program obvykle umožnuje vytvoření tzv. **vstupního modelu**.

Životní cyklus výpočetního programu: Časové období, které začíná identifikací potřeby uplatnění výpočetního programu a pokračuje vývojem výpočetního programu nebo výběrem výpočetního programu, který má být obstarán. Časové období životního cyklu, vyplněné převážně používáním programu, končí vyřazením výpočetního programu z používání.

[3] Vychází z definice v [10]: „***model***. An analytical or physical representation or quantification of a real *system* and the ways in which phenomena occur within that *system*, used to predict or assess the behaviour of the real *system* under specified (often hypothetical) conditions. … These assumptions would normally cover, as a minimum, the geometry and dimensionality of the *system*, initial and boundary conditions, time dependence, and the nature of the relevant physical, chemical and biological *processes* and phenomena.“

1 ÚVOD

(1.1) Zásadním prostředkem k prokázání dosažené úrovně jaderné bezpečnosti, radiační ochrany, technické bezpečnosti a zajištění zvládání radiační mimořádné události jaderného zařízení jsou výpočetní analýzy, prováděné zpravidla pomocí výpočetních programů (jinak také výpočetních prostředků nebo výpočetních kódů). Na provádění hodnocení bezpečnosti včetně využívání výpočetních programů se proto v plné míře vztahují požadavky na systém řízení, procesy a zajištění jejich kvality podle § 5 odst. 7, § 29 odst. 3 a § 30 odst. 2 a 3 zákona č. 263/2016 Sb., atomový zákon [1], a vyhlášky č. 408/2016 Sb., o požadavcích na systém řízení [2] (zejména pak § 4, 5, 8, 14 a 15).

1.1 Důvod vydání

(1.2) Důvodem pro vydání bezpečnostního návodu BN-JB-2.4 „ZAJIŠTĚNÍ KVALITY PŘI TVORBĚ A UŽÍVÁNÍ VÝPOČETNÍCH PROGRAMŮ PRO HODNOCENÍ BEZPEČNOSTI“, je potřeba rozpracovat požadavky na výpočetní programy používané při provádění výpočetního hodnocení bezpečnosti a požadavky na systém řízení a zajištění kvality při jejich používání. Ideové východisko pro vznik tohoto bezpečnostního návodu pochází ze zrušené směrnice „VDS 030 SMĚRNICE K HODNOCENÍ VÝPOČTOVÝCH PROGRAMŮ PRO POSUZOVÁNÍ JADERNÉ BEZPEČNOSTI“.

1.2 Cíl

(1.3) Bezpečnostní návod je zejména určen provozovateli nebo projektantovi jaderného zařízení a jejich dodavatelům výpočetního hodnocení bezpečnosti. Dodržení tohoto návodu má zajistit, že budou plněny požadavky § 5 odst. 7, § 29 odst. 3 a § 30 odst. 2 a 3 zákona [1] a vyhlášky [2], uplatněné pro výpočetní hodnocení bezpečnosti, respektive prokazování a dokladování plnění těchto požadavků, dále budou plněny a zároveň budou reflektovány mezinárodní doporučení (IAEA) a dobrá praxe v tomto oboru (např. podle pokynů a doporučení bezpečnostních návodů vydávaných národními dozory jiných států EU nebo US NRC).

(1.4) Bezpečnostní návod přibližuje principy umožňující dodržování cílů a požadavků výše zmíněných ustanovení během celého životního cyklu výpočetního programu při prokazování bezpečnosti jaderného zařízení jako zvláštního procesu dle § 5 odst. 4, 5 a 6 vyhlášky [2] s ohledem na stanovená specifika ověření a validace v jednotlivých etapách jeho životního cyklu. Dále pak uvádí doporučení ke způsobu prezentování potřebných informací SÚJB, včetně časového rámce.

1.3 Působnost

(1.5) Tento návod lze při uplatnění odstupňovaného přístupu (v souladu s požadavkem § 5 odst. 8 zákona [1]) aplikovat na všechna jaderná zařízení, kde je pomocí výpočetního hodnocení bezpečnosti prokazováno zajištění jaderné bezpečnosti, radiační ochrany, technické bezpečnosti a zvládání radiační mimořádné události jaderného zařízení.

1.4 Jazyková poznámka

(1.6) V celém dokumentu je záměrně u požadavků, jejichž plnění se pokládá za odpovídající závazným požadavkům právních předpisů, použit jednoduchý tvar přítomného nebo budoucího času (např. „je“, „bude“), čímž je popisován požadovaný stav. Pokud je v dokumentu použita vazba „musí být“ (případně s plnovýznamovým slovesem), jedná se o akcentování požadavku nebo opakování textu legislativy. Pokud je v dokumentu použita vazba „měl by být“ nebo „může být“ (případně s plnovýznamovým slovesem), je popisováno doporučené, ale nikoli jediné vhodné řešení.

(1.7) V celém dokumentu jsou používány z důvodů zavedené praxe zkratky anglických odborných termínů v jednotném čísle. V některých případech je užitím zkratky v jednotném čísle zamýšleno množné číslo vzhledem ke skutečnosti, že význam je jasný z kontextu textu v českém jazyce.

1.5 Základní zdroje a základní východiska

(1.8) Základními dokumenty, které definují požadavky na kvalitu procesů s vlivem na jadernou bezpečnost pro provozovatele JZ, jsou zákon [1], konkrétně § 5 odst. 7, § 29 odst. 3 a § 30 odst. 2 a 3 a vyhláška [2].

(1.9) Další doporučení pro využívání výpočetních programů při provádění výpočetního hodnocení bezpečnosti a na systém řízení a zajištění kvality při jejich používání uvádí dokumenty IAEA, zejména [4], [5] a [7].

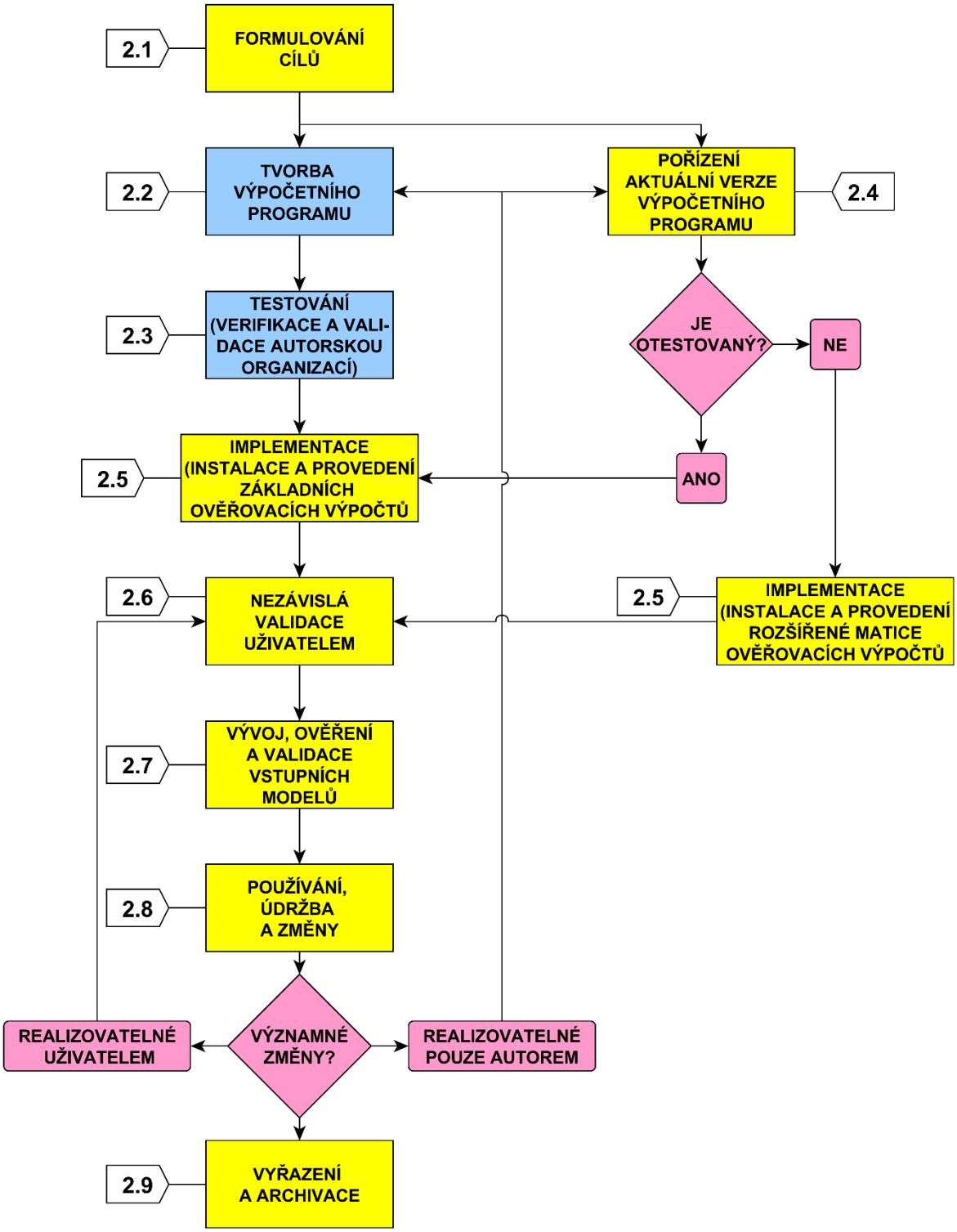
(1.10) Tématem využívání výpočetních programů při výpočetním hodnocení bezpečnosti se také zabývají některé dokumenty národních dozorných orgánů států EU (např. [3]) a dalších orgánů vykonávajících státní dozor nad využíváním jaderné energie (např. [6]).

(1.11) Tento bezpečnostní návod je vhodné využívat zejména při provádění výpočetního hodnocení bezpečnosti v následujících odborných oblastech:

- termohydraulické výpočty,
- neutronově-fyzikální výpočty,
- výpočty pružnosti a pevnosti SKK, únavy, odolnosti a životnosti,
- výpočty chování jaderného paliva včetně jeho skeletu při jeho provozu v jaderném reaktoru a při všech stavech jaderného zařízení,
- výpočty šíření radioaktivních látek a ionizujícího záření prostředím,
- výpočty vlivu radioaktivních látek a ionizujícího záření na osoby a životní prostředí,
- analýzy chování JZ a jeho SKK v havarijních podmínkách včetně těžkých havárií a
- pravděpodobnostní analýzy bezpečnosti.

2 ŽIVOTNÍ CYKLUS VÝPOČETNÍHO PROGRAMU – FÁZE PROCESU

(2.1) Životní cyklus výpočetního programu zahrnuje všechny fáze procesu zmíněné v této kapitole. Životní cyklus lze rozdělit do devíti hlavních fází, které jsou podrobněji popsány níže spolu se zahrnutými činnostmi. Jsou to fáze vyznačené v následujícím diagramu v jasně žlutých a modrých obdélnících, které rovněž představují jednotlivé podkapitoly tohoto návodu.



(2.2) Jednotlivé činnosti ve fázích životního cyklu na sebe nemusí přesně navazovat, a mohou se dokonce i překrývat a opakovat. Každá fáze je doprovázena hodnocením stanovených dílčích cílů procesu. Životní cyklus se může u různých výpočetních programů lišit v závislosti na komplexnosti a druhu výpočetního programu. V praxi může být na některé fáze kladen větší důraz než na jiné, které mohou být v **odůvodněných případech, při uplatnění odstupňovaného přístupu, vynechány**. Životní cyklus se bude např. lišit při vývoji vlastního výpočetního programu nebo při zakoupení hotového a otestovaného výpočetního programu. Vstupy pro tuto kapitolu byly čerpány především z doporučení zdrojů [3] a [6].

2.1 Formulování cílů

(2.3) Počáteční fází životního cyklu výpočetního programu je formulování základních cílů procesu a dále dílčích cílů jeho jednotlivých fází. Tato fáze je důležitá pro samotnou tvorbu, pořízení výpočetního programu nebo pro rozhodnutí o využití programu, kterým uživatelská organizace již disponuje, a pro další fáze životního cyklu [6]. Odpovídá také § 4 odst. 2 písm. a) vyhlášky [2].

(2.4) Cíle jsou formulovány zvláště pro oblasti:

a) úspěšnosti (míry splnění formulovaných dílčích cílů jednotlivých fází),
b) použitelnosti (míry naplnění potřeb uživatele),
c) robustnosti (míry odolnosti výpočetního programu vůči numerickým nestabilitám a nepovolenému zadání vstupních hodnot),
d) spolehlivosti (pravděpodobnosti, že výpočetní program bude vykonávat zamýšlenou funkci v daných podmínkách a pro předpokládaná zadání po specifickou dobu),
e) výkonnosti (nároků na paměť, výpočetní dobu atp.),
f) přesnosti (správnosti, věrohodnosti výsledků),
g) bezpečnosti (míry odolnosti vůči neoprávněným zásahům, které by mohly znehodnotit samotný výpočetní program nebo jeho výsledky) a
h) možnosti vnějšího propojení výpočetního programu (komunikace s člověkem „Human-Machine Interface“, s jiným výpočetním programem „Computer code coupling“) [3].

(2.5) Pro jednotlivé cíle procesu jsou určena kritéria přijatelnosti, jejichž plnění je v závěru každé fáze hodnoceno.

(2.6) Formulované cíle určují požadovanou odezvu výpočetního programu na předpokládaná vstupní data a dále je jejich účelem poskytnout detailní informace (např. pro matematický model) pro sestavení výpočetního programu. Součástí této fáze je také příprava požadavků na verifikaci a validaci výpočetního programu [6].

(2.7) Během procesu se mohou měnit a doplňovat (např. při vzniku nového požadavku na další využití výpočetního programu) i jeho základní cíle a dílčí cíle jednotlivých fází. Veškeré změny musí být zdokumentovány, popsány a musí být vyhodnoceno, zda nebo v jaké míře bude

dosaženo původně stanovených cílů po provedení změn [6], což odpovídá požadavkům § 4 odst. 2 písm. c) a § 14 písm. c) vyhlášky [2].

2.2 Tvorba výpočetního programu

(2.8) Obecně se nový výpočetní program vyvíjí za situace, kdy:

a) není možné koupit výpočetní program,
   i. z důvodů finanční náročnosti nebo ekonomické nevýhodnosti,
   ii. vykonavatel autorských práv nechce licenci prodat,
b) žádný dostupný výpočetní program není schopen splnit všechny stanovené cíle,
c) u autorské organizace nebo vykonavatele autorských práv není možné prokázat schopnost plnění požadavků na zajištění jaderné bezpečnosti (tj. nelze prokázat např. zajištění požadavků na systém řízení, plnění kultury bezpečnosti, poskytování údržby apod.).

(2.9) Tvorba výpočetního programu probíhá v souladu s postupy obsaženými v dokumentaci systému řízení autorské organizace. Postup prokazování shody je stručně naznačen v bodech (2.10) a (2.11).

(2.10) V úvodní fázi tvorby programu je vypracován a nezávisle ověřen plán zajištění kvality výpočetního programu a jeho dokumentace tak, aby splňoval stanovené cíle, definované v předchozí fázi procesu. V dalších dílčích fázích tvorby výpočetního programu je přesně vymezen jeho algoritmus, popisující použité fyzikální řešení, a popsána transformace algoritmu do zdrojového kódu dle pravidel zvoleného programovacího jazyka, respektující omezení daná tímto jazykem.

(2.11) Ve fázi tvorby programu je výpočetní program průběžně verifikován autorskou organizací. Na základě předem definovaných požadavků jsou vytvořeny verifikační úlohy, které vedou především k prověření výpočetního programu z hlediska jeho stavby (algoritmus, struktura, řídící logika, korelace atp.) a z hlediska jeho implementace (soulad s kódovacími standardy zvoleného programovacího jazyka). Součástí průběžné verifikace by mělo být ověřování, že je k výpočetnímu programu vytvořena a vedena odpovídající dokumentace. Rozsah verifikace a validace je podrobně popsán v kapitole 3 tohoto návodu.

2.3 Testování - Verifikace a validace autorskou organizací

(2.12) Výpočetní program obvykle prochází verifikací a validací prováděnou autorskou organizací v průběhu vývoje programu.

(2.13) Verifikace a validace výpočetního programu musí být prováděna podle předem připraveného programu za použití vhodné metodiky. Výsledkem je potvrzení, že výpočetní program splňuje stanovené cíle, a že výsledky výpočtů jím provedených jsou při porovnání

s testovacími úlohami správné, viz [3] a dále § 5 odst. 2 vyhlášky [2]. Komplexní popis verifikace a validace výpočetního programu je v kapitole 3.

(2.14) Výsledkem této fáze je otestovaný výpočetní program.

2.4 Pořízení výpočetního programu

(2.15) Pokud je uživatelem legálně získán otestovaný výpočetní program, resp. jeho licence, pak lze předpokládat, že fáze tvorby výpočetního programu a testování výpočetního programu proběhly u autorské organizace (včetně formování dílčích cílů těchto fází). Totéž platí i v případě, pokud se uživatel rozhodne, že může pro splnění cíle využít otestovaný výpočetní program, kterým již disponuje.

(2.16) Výsledky verifikace výpočetního programu autorskou organizací jsou uživatelskou organizací udržovány jako součást dokumentace k výpočetnímu programu. Pokud není doklad o provedení verifikace autorskou organizací dostupný, nebo není pro potřeby výpočetního hodnocení bezpečnosti dostačující (s ohledem na rozsah hodnocení), jsou součástí dokumentace k výpočetnímu programu buď výsledky verifikace provedené uživatelskou organizací, nebo je potřeba doložit zavedení programu zajištění kvality u autorské organizace, které provedení verifikace výpočetního programu potvrdí.

(2.17) Výsledky validace výpočetního programu autorskou organizací jsou také udržovány uživatelskou organizací jako součást dokumentace k výpočetnímu programu. Pokud nejsou výsledky validace autorskou organizací dostupné, jsou doloženy výsledky nezávislé validace uživatelskou organizací.

(2.18) Ať už uživatel získal nebo delší dobu užívá otestovaný nebo neotestovaný výpočetní program, je nutné, aby uživatelská organizace výpočetní program nezávisle ověřila (viz fáze Implementace 2.5 – instalace výpočetního programu a jeho nezávislé ověření) a validovala (viz fáze 2.6 – nezávislá validace uživatelem).

(2.19) Pro legálně získané výpočetní programy platí, že pro navázání na fázi pořízení programu v rámci životního cyklu stačí SÚJB doložit výsledky odpovídající verifikace a validace (na základě bodů (2.16) a (2.17) tohoto návodu) tohoto programu. Totéž platí i v případě, pokud se uživatel rozhodne, že může pro splnění cíle využít otestovaný výpočetní program, kterým již disponuje. Doporučuje se volit výpočetní programy od důvěryhodných autorských organizací. Pokud již existuje otestovaný program od takových organizací, doporučuje se jeho využití namísto tvorby nového programu.

Během tvorby nebo pořízení výpočetního programu může docházet ke změnám či doplnění základních a dílčích cílů [6].

2.5 Implementace – instalace a nezávislé ověření

(2.20) Implementací je v této fázi myšleno spojení všech částí ověřeného výpočetního programu s daným hardwarem a operačním systémem uživatelské organizace – instalace programu dle předem sjednaných nebo stanovených požadavků a v souladu s jeho účelem a jeho následné nezávislé ověření uživatelskou organizací. Pokud jsou autorskou organizací dány minimální hardwarové požadavky, měly by být uvedeny v dokumentaci výpočetního programu a musí být uživatelem plněny, viz § 4 odst. 2 písm. e) vyhlášky [2].

(2.21) Po instalaci výpočetního programu musí být zkontrolována funkčnost – ověření (viz § 4 odst. 2 písm. e) vyhlášky [2]) otestovaného výpočetního programu a neotestovaného výpočetního programu se liší rozsahem prováděného ověření:

- Otestovaný výpočetní program postačí nezávisle ověřit uživatelskou organizací provedením základních ověřovacích výpočtů.
- Neotestovaný výpočetní program je nutné nezávisle ověřit uživatelskou organizací provedením rozšířené matice ověřovacích výpočtů.

(2.22) Základními ověřovacími výpočty je zde myšleno provedení testů prokazujících úspěšnou instalaci a integraci výpočetního programu. Rozšířená matice ověřovacích výpočtů by měla navíc zahrnovat provedení přepočtu vzorových úloh získaných např. od autorské organizace a porovnání výsledků uživatelské organizace se vzorovými.

2.6 Nezávislá validace uživatelem

(2.23) V této fázi procesu zástupci uživatelské organizace provádějí nezávislou validaci výpočetních programů. Rozsah validace je závislý na rozsahu předpokládaného použití výpočetního programu a je zde uplatněn také odstupňovaný přístup. Požadavky na nezávislou validaci jsou shodné s požadavky na fázi testování a jsou podrobně rozebrány v kapitole 3 tohoto bezpečnostního návodu.

(2.24) Cílem nezávislé validace je nejen prokázání schopnosti výpočetního programu simulovat jevy a procesy relevantní pro výpočetní hodnocení bezpečnosti, ale rovněž prokázání, že si uživatel osvojil daný výpočetní program a je schopen ho správně a kvalifikovaně používat.

(2.25) Posledním krokem této fáze je vyhotovení zpráv o validaci.

2.7 Vývoj, ověření a validace vstupních modelů

(2.26) Uživatelská organizace v této fázi procesu vytváří pro otestovaný výpočetní program vstupní modely, které mohou mít dva základní účely – nezávislá uživatelská validace programu a vlastní použití výpočetního programu. Pro oba typy úloh platí shodné obecné postupy, které definují tvorbu, verifikaci a validaci vstupního modelu. Verifikace a validace vstupního modelu je opět podrobně popsána v kapitole 3.

(2.27) Při tvorbě vstupního modelu je nezbytné postupovat dle postupů definovaných autorskou organizací, dokumentovaných v uživatelských manuálech a na základě systému řízení uživatelské organizace.

(2.28) Nezbytným krokem po vytvoření vstupního modelu je jeho ověření, které by mělo být prováděno kvalifikovanou osobou, která se nepodílela na vývoji modelu. Předmětem ověření je, že všechny předpoklady vstupního modelu a aplikované geometrické, materiálové, fyzikální a další informace k danému řešenému problému byly aplikovány správně a vstupní model je funkční a splňuje cíle konkrétní fáze procesu.

(2.29) Výstupem z této fáze je záznam o provedené validaci vstupního modelu.

(2.30) Na konci této fáze životního cyklu je výpočetní program připraven k použití.

2.8 Používání, údržba a změny

(2.31) V této fázi procesu je otestovaný výpočetní program nainstalován, je nezávisle ověřen a validován a je dokončena verifikace a validace vstupního modelu vytvořeného pro předpokládanou oblast použití. Výpočetní program slouží pro použití v souladu se stanoveným cílem. Uživatel postupuje při použití výpočetního programu pro účel výpočetního hodnocení bezpečnosti vždy podle uživatelské dokumentace. V uživatelské dokumentaci je popsáno, jak zajistit a ověřit kvalitu výstupů práce s výpočetním programem, a tyto postupy musí být uživatelem dodržovány (viz také požadavek § 4 odst. 2 vyhlášky [2]).

(2.32) Pro plnění těchto požadavků je nutné zajistit, aby otestovaný výpočetní program používaly pro výpočetní hodnocení bezpečnosti pouze osoby, které prošly adekvátním školením a dostatečně rozumí metodám aplikovaným ve výpočetním programu pro předpokládanou oblast použití. Je stanoven garant procesu, který odpovídá za kvalifikované používání výpočetního programu v uživatelské organizaci [5].

(2.33) Je nutné stále zohledňovat fakt, že u většiny výpočetních programů mohou být výsledky značně ovlivněny uživatelským efektem, zejména schopnostmi uživatelské organizace, která provádí výpočty. Vliv na výpočty může být významný a z toho důvodu musí být (viz požadavek § 4 odst. 2 písm. e) vyhlášky [2]) zajištěny kvalifikační procedury pro uživatele programu. Uživatelská organizace zajistí výcvik a řízení činnosti jednotlivých uživatelů programu, zajistí detailní uživatelské manuály, vedení uživatelské dokumentace a systém zajištění kvality, viz [2] a [5]. Vliv uživatele je dále rozebrán v bodě (3.18).

(2.34) Uživatelská organizace vede deník údržby výpočetního programu, který je dostupný všem uživatelům (viz kapitola 4.4 a také požadavek § 4 odst. 2 písm. c), d) a e) vyhlášky [2]).

(2.35) Do této fáze procesu spadá i případná údržba výpočetního programu, při které jsou opravovány nalezené chyby ve výpočetním programu, a dále do této fáze patří i případná vylepšení výpočetního programu. Pokud v rámci údržby, nebyly provedeny významné změny ve výpočetním programu, vzniká nová revize (update) a při vylepšení programu (upgrade) vzniká

nová verze výpočetního programu. Pokud je uživatelská organizace zároveň autorskou organizací, může změny provádět sama. U pořízeného programu je údržba zpravidla prováděna vykonavatelem autorských práv, který sbírá podklady od uživatelských organizací a veškeré změny zapracuje v pravidelných revizích na základě smluvních podmínek uzavřeného právního vztahu. Opravy mohou být různé [6]:

a) odstranění skrytých chyb (korektivní údržba),

b) odezva na nové nebo upravené cíle (zdokonalovací údržba),

c) odezva na výsledky verifikace a validace,

d) přizpůsobení programu na změny v uživatelském prostředí (adaptivní údržba) a

e) změny za účelem udržení integrity výpočetního programu.

(2.36) Při každém zásahu do zdrojového kódu výpočetního programu je vytvořena nová verze výpočetního programu „X.0“[4] a veškeré změny jsou zaznamenány do deníku údržby výpočetního programu, pokud je tato verze použita. Do deníku údržby výpočetního programu jsou zaznamenávány i odhalené chyby, které se nepodařilo opravit. Pokud vznikne nová verze výpočetního programu, je třeba:

- provést opětovnou validaci, nebo
- provést sadu srovnávacích výpočtů (minimálně v rozsahu jako při implementaci programu) a prokázat, že nedochází ke změně ve výsledcích, nebo
- jinou formou ověřit, že změny nemají vliv na výsledky.

Za verifikaci a validaci nové verze výpočetního programu obvykle odpovídá vykonavatel autorských práv. Pokud o verifikaci a validaci nové verze výpočetního programu nejsou dostatečné informace, provede potřebné práce s ohledem na odstupňovaný přístup uživatelská organizace před zahájením používání nové verze výpočetního programu pro provádění výpočetního hodnocení bezpečnosti. V každém případě je proveden zápis do deníku údržby výpočetního programu. Při formálních úpravách výpočetního programu (např. změny neovlivňující metodiku výpočtů, fyzikální nebo matematický model, atp.) není nutné vytvářet novou verzi, stačí pouze vytvoření nové revize „1.Y“[4] spolu s vytvořením záznamu do deníku údržby výpočetního programu.

2.9 Vyřazení a archivace

(2.37) Vyřazení výpočetního programu znamená konec používání výpočetního programu uživatelskou organizací, resp. ukončení všech předchozích fází životního cyklu. Po vyřazení je

[4] Označení verzí a revizí použité v tomto bodě je pouze názorným příkladem. Označení verzí a revizí je plně v kompetenci vykonavatele autorských práv.

veškerá dokumentace, spolu s výpočetním programem[5], archivována minimálně po dobu platnosti výpočetního hodnocení bezpečnosti provedeného výpočetním programem [6], nebo po dobu stanovenou v dokumentaci systému řízení, viz požadavek § 15 odst. 1 písm. e) vyhlášky [2].

(2.38) O vyřazení výpočetního programu rozhoduje uživatelská organizace a může se tak rozhodnout z důvodů:

a) konce údržby výpočetního programu autorskou organizací nebo vykonavatelem autorských práv,
b) zastarávání výpočetního programu,
c) přechodu na jiný výpočetní program,
d) naplnění základních cílů použití, které neměly neomezenou časovou platnost (např. ukončení projektu, pro který byly zajišťovány výpočty).

[5] Pokud je to pro výpočetní program možné a smysluplné, např. z hlediska technického, s ohledem na licenci k užívání výpočetního programu apod.

3 VERIFIKACE A VALIDACE

(3.1) Podle požadavku 18 odst. 4.60 [4] a v souladu s požadavkem § 5 odst. 1 vyhlášky [2] platí, že jakýkoliv výpočetní program pro výpočetní hodnocení bezpečnosti má projít verifikačním a validačním procesem v dostatečném rozsahu.

(3.2) Základními charakteristikami validace a verifikace by měly být [11]:

- **opakovatelnost:** opakované hodnocení téhož výpočetního programu podle téže metodiky verifikace a validace týmž hodnotitelem vede k výsledkům, které mohou být považovány za identické,
- **reprodukovatelnost:** verifikace a validace téhož výpočetního programu podle téže metodiky jiným hodnotitelem vede k výsledkům, které mohou být považovány za identické,
- **nestrannost:** verifikace a validace nejsou předpojaté vůči žádnému konkrétnímu výsledku,
- **objektivita:** výsledky verifikace a validace se zakládají na faktech, tj. nejsou ovlivněny subjektivními postoji hodnotitele.

3.1 Verifikace

(3.3) Výpočetní program nemusí vždy reprezentovat konkrétní reálný systém. Pro řešení daného typu úlohy je proto potřeba vytvořit specifický vstupní model, ve kterém je definována konkrétní geometrie (oblast použití nebo architektura modelu) a vlastnosti modelovaného zařízení a další vstupní parametry modelovaného případu. Je třeba oddělovat verifikaci výpočetního programu a vstupního modelu.

(3.4) Obecně lze říct, že verifikací výpočetního programu je ověřeno, že numerické metody, fyzikální rovnice, data, uživatelské možnosti a omezení jsou správně použity a jsou ve shodě se specifikacemi uvedenými v uživatelské dokumentaci programu. Verifikací výpočetního programu je také ověřeno, že byla správně uplatněna pravidla použitého programovacího jazyka [5].

(3.5) Verifikace výpočetního programu autorskou organizací je prováděna ve fázi tvorby výpočetního programu a během jeho testování (viz kapitola 2) tak, aby bylo zabezpečeno, že výstupy z každé části životního cyklu výpočetního programu plní v této části stanovené cíle.

(3.6) Po instalaci výpočetního programu a jeho nezávislé verifikaci a validaci je třeba vytvořit první vstupní model (pokud to není vyžadováno už ve fázi nezávislé verifikace a validace), který je potřeba ověřit. K ověření tohoto vstupního modelu dochází ve fázi vývoje, ověření a validace vstupních modelů (viz podkapitola 2.7), ve které je kontrolována hlavně modelovaná geometrie úlohy, vstupní a výstupní podmínky a je také ověřena volba případných konstitutivních vztahů (tj. korelací, výpočetních vztahů, rovnic apod.) a zadání relevantních jevů pro výpočet. Obdobná

kontrola by měla být provedena pro každý[6] další vyvinutý vstupní model. U některých výpočetních programů se vstupní modely přímo nevytvářejí, ale bývají převzaty z jiných výpočetních programů či jejich modulů. Tyto vstupy by měly být taktéž před prvním použitím zkontrolovány.

(3.7) Při vytváření vstupního modelu je třeba zajistit dostatečně detailní nodalizaci[7] tak, aby mohly být zachyceny všechny důležité jevy, charakteristické pro danou úlohu [5]. Pro vytváření nodalizace musí být dodrženy předepsané postupy, pokud jsou v uživatelské dokumentaci definovány.

(3.8) Komplexní výpočetní programy mohou zahrnovat spojení s jednoduššími podprogramy, resp. moduly. Verifikací komplexních programů by měly být ověřeny nejen tyto moduly, resp. jednodušší programy, ale také správné spojení a funkčnost všech modulů, které reagují s výpočetním programem. Vše by mělo být ve shodě s dokumentací programu.[5]

3.2 Validace

(3.9) U validace je potřeba nejdříve provést validaci výpočetního programu autorskou organizací, která probíhá ve fázi testování. Samostatnou činností je pak nezávislá validace výpočetního programu uživatelskou organizací. Následuje validace vstupního modelu, která je uskutečněna ve fázi vývoj, ověření a validace vstupních modelů (viz podkapitola 2.7). Tato akce je zopakována pro každý nově vyvinutý vstupní model[8]. Souhrnná informace o validaci výpočetního programu i vstupního modelu je zaznamenána a udržována aktuální v dokumentaci uživatelské organizace, viz kapitola 4.

(3.10) Validace výpočetních programů (pokud jsou k dispozici vhodná referenční data) používaných pro výpočetní hodnocení bezpečnosti by měly být prováděny dle [5] především porovnáním vypočtených hodnot s:

- experimentálními daty ze základních testů na ověření vlastností modelů probíhajících fyzikálních jevů (nikoliv pouze na JZ),
- naměřenými daty získanými na experimentálních zařízeních pro zkoumání samostatných specifických jevů,
- naměřenými daty získanými na experimentálních zařízeních, sledujících kombinace jevů v modelových měřítcích,
- naměřenými daty získanými na reálném systému skutečného jaderného zařízení,

[6] Na základě § 5, odst. 1 [2] platí povinnost vstupní kontroly vstupního modelu pro veškeré výpočetní programy. Vzhledem k různým specifikům odlišných výpočetních kódů (účel, složitost apod.) a vstupních modelů (rozsah, komplexnost, pracnost vytvoření modelu, robustnost apod.) lze očekávat, že vstupní kontrola bude provedena s uvážením odstupňovaného přístupu.

[7] Pojem dostatečně detailní nodalizace může mít různý význam u různých výpočetních programů. Je tím především myšlena dostatečně jemná výpočetní síť či dostatečný počet prvků nebo u relevantních výpočetních programů dostatečně přesná a vhodná reprezentace řešeného problému.

[8] Dtto poznámka pod čarou č. 6.

- výsledky ze srovnávacích „benchmarkových“ úloh,
- výsledky analytického řešení problému a
- výsledky jiného otestovaného výpočetního programu („code to code comparison“).

(3.11) Validace vstupních modelů používaných pro provádění výpočetního hodnocení bezpečnosti JZ by měly být prováděny dle [5] a pokud je to možné, především porovnáním vypočtených hodnot s:

- naměřenými daty na modelovaných zařízeních,
- výsledky analytického řešení problému a
- výsledky jiného ověřeného výpočetního programu („code to code comparison“).

(3.12) Během této fáze procesu by mělo být zajištěno, že hodnoty vstupních dat a okrajových podmínek uplatněných při validaci výpočetního programu a vstupního modelu jsou voleny tak, aby byly co nejblíže reálným parametrům jaderného nebo modelovaného zařízení v analyzovaných podmínkách [5].

(3.13) Při validaci výpočetního programu srovnáním s daty získanými na experimentálních zařízeních je nutné mít dostatečně kvalitní experimentální data. To znamená, že jsou vybrány charakteristické veličiny (počítané programem), které jsou prováděnými experimenty stanovitelné v dostatečném rozsahu změn. V průběhu měření je kladen přiměřený důraz na věrohodnost měření a přijatelnou velikost chyb experimentálních dat tak, aby bylo možné porovnat naměřené hodnoty s vypočtenými.

(3.14) Porovnání vypočtených dat s výsledky z jiného otestovaného výpočetního programu a vstupního modelu může být aplikováno i v případě, kdy jsou použity odlišné matematické modely a algoritmy řešení. I přes očekávané rozdíly ve výsledcích tkví důležitost tohoto porovnání dvou různých výpočetních programů ve vyhodnocení a pochopení neurčitostí a v potvrzení předem analyzovaných příčin jejich rozdílnosti. Pokud je jeden z výpočetních programů validován v požadovaném rozsahu na experimentálních datech, lze ten druhý validovat porovnáním s ním (třeba v případě, kdy experimentální data nejsou autorovi nebo uživateli programu dostupná).

(3.15) Pro validaci výpočetního programu je vhodné vypracovat validační matici. V té jsou specifikovány validační metody, dále validační úlohy, resp. dostupná data, která slouží k porovnání výsledků. Cílem validační matice je vytvoření dostatečně rozsáhlého souboru dostupných údajů a experimentálních dat nutných pro validaci výpočetního programu. Výběr experimentálních dat musí zahrnovat dostatečně reprezentativní výběr geometrií, sledovaných jevů a provozních podmínek, pro které byly experimenty provedeny.

(3.16) Některé úlohy lze vyřešit pouze spojením dvou a více výpočetních programů (tzv. *„code coupling“).* Při použití této metody řešení zadané úlohy se musí validace (spolu s verifikací) provést pro nově vzniklý výpočetní celek i přes to, že jsou oba výpočetní programy již verifikovány a validovány.

(3.17) Rozsah použitelnosti výpočetního programu (v některých případech i vstupního modelu) je určen validací programu a použitými ověřenými interpolačními a extrapolačními metodami a měl by být zaznamenán ve výsledné zprávě o validaci výpočetního programu.

(3.18) Podle [7] jsou hlavní zdroje neurčitostí související s výpočetním programem a vstupním modelem a jejich aplikací:

a) **Neurčitost výpočetního programu nebo vstupního modelu**: Nejistota výpočtu související s matematickými modely a korelacemi jevů, schématem řešení, nastavením výpočetního modelu, volbami a vlivy parametrů, nemodelovanými procesy a s knihovnami dat.

b) **Neurčitost reprezentace díla vstupním modelem**: Nejistota výpočtu vznikající při reprezentaci nebo idealizaci skutečné technologie, např. kvůli neschopnosti přesně modelovat složitou geometrii, trojrozměrné efekty, vliv měřítka, zjednodušení řídicího systému.

c) **Vliv uživatele** („User Effect“): Nejistota výpočtu vznikající během interakce uživatele s výpočetním programem. V některých případech může být vyvolána nerespektovanými neurčitostmi ve zdrojích uvedených výše. Jeho rozsah je ovlivněn řadou faktorů:

   - rozsahem zkušeností s používáním výpočetních programů obecně a především zkušenostmi s daným výpočetním programem,
   - úrovní pochopení modelovaných jevů a procesů spolu s volbou počátečních a okrajových podmínek,
   - správnou interpretací provedených experimentů a
   - tvorbou zjednodušení při vytváření matematických modelů.

   Pro snížení vlivu uživatelského efektu je vhodné rozšiřování znalostí uživatele o:

   - nezávislých validacích úloh,
   - fenomenologii procesů na základě nejnovějších poznatků vědy a techniky,
   - simulovaném zařízení,
   - používání obdobných výpočetních programů a
   - používaném výpočetním programu.

   Snížení vlivu uživatelského efektu mimo jiné napomáhá i opakované provádění validačních úloh během životního cyklu výpočetního programu v návaznosti na implementaci nových poznatků vědy a výzkumu do výpočetního programu nebo vstupního modelu.

(3.19) Vliv jednotlivých neurčitostí na neurčitost výsledků výpočetního hodnocení bezpečnosti je při validaci identifikován a stanoven. K tomu účelu slouží citlivostní analýzy, ve kterých je vyhodnocen vliv neurčitostí různých vstupních parametrů, okrajových podmínek, výpočetní metodiky a také opakování jejich uplatnění v průběhu výpočtu. Dále je prokázána porovnatelnost vypočtených a naměřených dat ve stanovených pásmech neurčitostí.

4 PROKAZOVÁNÍ KVALITY PROCESU

(4.1) Cílem kapitoly je doporučit základní pravidla pro dokumentování a prokazování kvality při přípravě a provádění výpočetního hodnocení bezpečnosti za použití výpočetního programu, tj. kvality procesu. Tato doporučení jsou určena všem uživatelským organizacím, které provádí výpočetní hodnocení bezpečnosti pro jaderné zařízení provozované na území České republiky nebo se jinak významným způsobem, schopným ovlivnit kvalitu výstupu, zapojují do procesu.

(4.2) Vzhledem ke skutečnosti, že na kvalitu procesu jsou kladeny požadavky podle § 29 odst. 3 a § 30 odst. 2 a 3 zákona [1] a vyhlášky [2], je potřeba zabývat se zajištěním kvality výpočetního programu a jeho využívání od zahájení jeho životního cyklu po jeho ukončení (viz kapitola 2 tohoto návodu).

(4.3) Za zajištění kvality procesu nese odpovědnost držitel povolení, který musí v souladu s § 30 odst. 4 zákona [1] prokázat, že jsou požadavky na systém řízení procesu plněny i jeho dodavateli, v souladu s § 30 odst. 2 a 3 zákona [1].

(4.4) Dokumentaci prokazující zajištění kvality procesu vede organizace, která proces provádí. Tuto dokumentaci v souladu s požadavky § 4 odst. 2 písm. c), d) a § 15 odst. 1 vyhlášky [2] udržuje aktuální a dostupnou všem osobám vykonávajícím jednotlivé činnosti procesu a osobám schopným významně ovlivnit výstupy procesu. Jedná se o následující dokumenty:

a) abstrakt výpočetního programu,
b) dokument prokazující legální nabytí výpočetního programu,
c) dokumenty prokazující zajištění kvality procesu,
d) podklady prokazující tvrzení uvedená v dokumentech prokazujících zajištění kvality, kterými jsou zejména:
    - uživatelská dokumentace,
    - deník údržby výpočetního programu,
    - souhrnná informace o verifikaci a validaci výpočetního programu autorskou, případně uživatelskou organizací,
    - zpráva prokazující schopnost uživatelské organizace vytvořit a validovat vstupní model.

(4.5) Dokumentaci prokazující zajištění kvality procesu může k hodnocení SÚJB předložit buď držitel povolení, nebo budoucí žadatel o povolení, který využívá nebo bude využívat výstupy procesu nebo organizace, která proces provádí (dále obecně „předkladatelská organizace“)[9].

[9] Pokud se předkladatelská organizace liší od organizace, která proces provádí (např. podklady předkládá držitel povolení za svého dodavatele), stále je předkládána dokumentace organizace, která proces provádí (tj. dle příkladu v předchozí závorce se předkládá dokumentace dodavatele).

Doporučuje se předložení podkladů k hodnocení zajištění kvality procesu minimálně 12 měsíců[10] před plánovaným začátkem využívání výsledků výpočetního hodnocení bezpečnosti (např. před podáním žádosti o povolení k provedení změny projektu JZ, před předáním aktualizace projektové dokumentace v bezpečnostní zprávě apod.). SÚJB provede hodnocení předložených podkladů a vyjádří se k nim formou dopisu (**dopis s vyjádřením**) nejpozději do 2 měsíců od obdržení podkladů. Vyjádření může obsahovat požadavky na doplnění předložených informací (např. konkrétní dotazy nebo požadavek na předložení některého dalšího dokumentu z výčtu v odst. (4.4) nebo jeho části), doporučení k využívání procesu, konstatování nesouladu s legislativou apod. V případě potřeby může být k vyjádření před nebo po jeho provedení svoláno jednání. Vyjádření SÚJB k dokumentaci zajištění kvality (systému řízení) není součástí specifického správního řízení, ale bude k němu přihlédnuto v další činnosti SÚJB (správní řízení k žádosti o povolení, kontrolní činnost apod.).

(4.6) Předkladatelská organizace překládá k hodnocení následující dokumenty:

a) abstrakt výpočetního programu,
b) dokumenty prokazující zajištění kvality procesu,
c) dva posudky nezávislých oponentů,
d) v případě zájmu další relevantní dokumenty, které považuje za zásadní z pohledu hodnocení[11].

(4.7) Předkladatelská organizace předkládá dokumenty k hodnocení oficiální formou, tedy na podatelnu SÚJB nebo do datové schránky SÚJB. Doplňující informace je možné předávat i formou e-mailu na podatelnu SÚJB.[12]

(4.8) Předkladatelská organizace jednoznačně vymezí, které předané informace považuje za obchodní tajemství.

(4.9) Dokumenty podle odstavce (4.6) jsou předkládány v českém, slovenském nebo anglickém jazyce. Předložení v jiném jazyce je možné pouze po předchozí písemné domluvě se SÚJB (v takovém případě je vhodné odeslat dotaz přes e-mail podatelny SÚJB).

(4.10) Dokumentaci podle odstavce (4.6) je třeba předložit k přehodnocení v případě:

a) významné změny ve výpočetním programu,

[10] Pokud není možné toto doporučení dodržet, doporučuje se v obdobném nebo v nejbližším možném termínu informovat SÚJB o záměru předložit podklady a následně předložit podklady k hodnocení v nejbližším možném termínu.

[11] Např. výsledek hodnocení odbornými hodnotícími komisemi, výsledek certifikace dozorným orgánem v oblasti jaderné bezpečnosti k použití v zemi původu výpočetního programu, nebo v zemí provozující jaderné elektrárny nebo významná výzkumná jaderná zařízení apod.

[12] Korespondenci je vhodné adresovat na Sekci jaderné bezpečnosti nebo Odbor hodnocení jaderné bezpečnosti.

b) nejvýše však 5 let po přechozím hodnocení (vzhledem k možným změnám v procesu a ve stávající úrovni vědy a techniky).

(4.11) Za významnou změnu ve výpočetním programu podle písm. a) odstavce (4.10) se považuje změna verze programu autorskou organizací (případně uživatelskou organizací, pokud se liší od autorské organizace a má právo výpočetní program měnit) obsahující změny ve zdrojovém kódu (změna fyzikálních, chemických, materiálových modelů použitých ve výpočtech, změna výpočetních metod apod.), která vyžaduje nezanedbatelné úpravy vytvořených vstupních modelů nebo vytvoření nových vstupních modelů.

(4.12) Pokud je třeba předložit dokumentaci k přehodnocení z důvodu okolností uvedených v písm. a) (4.10), může předkladatelská organizace předložit k hodnocení pouze změněnou dokumentaci. Předložené informace budou SÚJB zhodnoceny a na jejich základě bude do 2 měsíců vydáno nové vyjádření. Pokud si není uživatelská organizace jistá významností změny, resp. nutností předložit změnu k posouzení, může vznést písemný dotaz na SÚJB (např. formou e-mailu na podatelnu SÚJB). Doporučuje se vznést dotazy a předložit informace k posouzení s dostatečným předstihem před zahájením využívání změněného výpočetního programu v rámci procesu.

(4.13) Pokud je třeba dokumentaci předložit k přehodnocení z důvodu uplynutí 5 let od předchozího hodnocení (podle písm. b) odstavce (4.10)), může předkladatelská organizace nejpozději 6 měsíců před uplynutím období 5 let předložit argumentaci, podle které jsou všechny relevantní dokumenty stále aktuální a která bude dokládat, že výpočetní program a proces je stále v souladu se stávající úrovní vědy a techniky. Případně může předložit k hodnocení opět pouze změněnou dokumentaci. Předložené informace budou SÚJB zhodnoceny a na jejich základě bude do 2 měsíců vydáno nové vyjádření.

(4.14) Pokud jsou pro provádění procesu použity spojené výpočetní programy (tzv. *„code coupling“*) nebo jeden hlavní výpočetní program a méně náročný výpočetní program pro zpracování části dat (např. pro přípravu vstupních dat), je vhodné předkládat k hodnocení jejich dokumentaci společně jako jednu dokumentaci.

(4.15) Pro výpočetní programy, které byly hodnoceny před vydáním tohoto bezpečnostního návodu, a mají dosud platné stanovisko hodnotící komise podle „VDS 030 SMĚRNICE K HODNOCENÍ VÝPOČTOVÝCH PROGRAMŮ PRO POSUZOVÁNÍ JADERNÉ BEZPEČNOSTI“ se doporučuje předložit podklady prokazující zajištění kvality procesu minimálně 6 měsíců před koncem platnosti výše zmíněného stanoviska.

4.1 Abstrakt výpočetního programu

(4.16) Abstrakt výpočetního programu obsahuje minimálně následující informace**:**

- název nebo označení programu,

- název nebo označení autorské organizace, případně vykonavatele autorských práv,
- název nebo označení uživatelské organizace, případně také předkladatelské organizace, pokud se liší od autorské organizace,
- minimální požadavky na hardwarovou a softwarovou konfiguraci počítače, pro který je výpočetní program adaptován, operační systém pro který je program určen, případně další operační systémy, pro které je program adaptován,
- účel programu (oblasti možného využití) a oblasti zamýšleného využití, včetně stručného popisu fyzikálních problémů a základních fyzikálních aproximací, použitých při formulaci problému,
- metoda řešení, stručný přehled matematických a numerických postupů a algoritmů použitých při výpočtu, stručný popis fyzikálního modelu s uvedením argumentů u hlavních použitých předpokladů a omezení,
- plánovaný rozsah využití výpočetního programu případně jeho omezení vzhledem k možnostem využití deklarovaným autorskou organizací,
- existující omezení plynoucí z rozsahu výpočetní paměti (např. maximální počet energetických grup použitých pro výpočet, bodů sítě, omezení rozsahu nezávisle proměnných z důvodů použité aproximace apod.),
- další relevantní znaky programu, oblast úloh, které jsou na jejich základě nejefektivněji řešeny,
- porovnání s jinými obecně známými programy umožňujícími využití ve zvolené oblasti, pokud existují,
- návazné a pomocné programy, jejichž využití se plánuje (informace o tom, zda se program plánuje používat ve vazbě na jiný program, pokud jsou další programy užívány v souvislosti s výpočetním programem pro zpracování vstupních nebo výstupních dat, nebo jako podprogram),
- použité knihovny dat,
- použitý programovací jazyk,
- seznam dostupných materiálů, vhodných pro bližší seznámení s programem,
- základní informace o rozsahu verifikace a validace programu autorskou organizací, obecný popis plánované údržby programu autorskou organizací a
- další relevantní informace, pokud existují.

4.2 Dokument prokazující legální nabytí výpočetního programu

(4.17) Tímto dokumentem se myslí zejména:

- smlouva licenční, kupní, o darování, o vypůjčení nebo o pronájmu,
- souhlas s využitím programu, získaného v rámci mezinárodní nebo národní spolupráce (spolupráce s US NRC, projekty Evropské Komise apod.).

4.3 Dokumenty prokazující zajištění kvality procesu

(4.18) Dokumenty musí přiměřeně popisovat zavedení procesu a zajištění jeho kvality v uživatelské organizaci. Předpokládá se, že se jedná o integrovanou část zavedeného systému řízení uživatelské organizace. V dokumentech jsou uvedeny všechny osoby, které vykonávají jednotlivé činnosti v rámci procesu, připravují pro ně vstupy nebo zasahují do procesu jiným způsobem schopným ovlivnit výstupy procesu. Jedná se zejména o následující informace:

- cíle procesu (čeho se má využíváním výpočetního programu dosáhnout), použité postupy (jak dosáhnout cílů procesu, jakými prostředky)[13], popis výstupů procesu (kritéria přijatelnosti, která musí výstupy splňovat, aby bylo dosaženo základních cílů),
- garant, případně garanti procesu,
- procesní role (osoby vykonávající jednotlivé činnosti procesu, osoby schopné významně ovlivnit výstupy procesu (např. připravující vstupní soubory, zpracovávající výstupy, zajišťující komunikaci uživatelů s autorskou organizací apod.)), vztahy mezi nimi, povinnosti a odpovědnosti,
- požadavky na osoby vykonávající jednotlivé činnosti procesu (kvalifikace, zaškolení, počet, dokumentace, se kterou musí být seznámeni, např. manuál výpočetního programu vytvořený autorskou organizací apod., požadavky na zkušenost a praxi osob na jednotlivých pozicích, např. v praxi se samostatným užíváním výpočetního programu, praxi se samostatnou tvorbou vstupních modelů, praxi jako spoluřešitel apod.) a doklad o jejich splnění),
- vstupy (požadavky na vstupní data a vstupní soubory, typy vstupních dat nebo souborů, zdroje apod.), použité prostředky (výpočetní technika apod.),
- způsob provádění jednotlivých činností procesu a doklad o jejich splnění
- postup ověřování jednotlivých činností procesu a kontroly naplnění kritérií přijatelnosti jednotlivých činností procesu a výstupů procesu.

Dokument by měl prokázat, že proces splňuje požadavky vyhlášky [2] a zohledňuje požadavky relevantních norem, např. [15], [16], [17] a [18].

4.4 Podklady prokazující tvrzení uvedená v dokumentech prokazujících zajištění kvality uživatelské dokumentace

(4.19) Tato dokumentace obsahuje podrobný popis, jak je výpočetní program používán, aby byly získány požadované výsledky. Předpokládá se, že bude členěna na části určené pro:

- základní použití podle uživatelské dokumentace pod dozorem jiné osoby (např. způsobilé samostatně používat výpočetní program),
- samostatné používání výpočetního programu,
- pokročilé použití zahrnující úpravu vstupních modelů,

[13] Ve vazbě na fáze životního cyklu výpočetního programu předcházející jeho používání pro výpočetní hodnocení bezpečnosti.

- tvorbu nových vstupních modelů,
- úpravu samotného výpočetního programu.

(4.20) Součástí uživatelské dokumentace je i uživatelský manuál vytvořený autorskou organizací, nebo pokud tento není dostupný, vytvořený uživatelskou organizací, resp. další dokumentace, která je při využívání výpočetního programu potřebná a jejíž nastudování je pro osoby vykonávající jednotlivé činnosti procesu povinné nebo je od nich očekávané. Pro účely hodnocení kvality procesu není nutné SÚJB předkládat všechny manuály a výše zmíněnou využívanou dokumentaci, ale jen její výčet a informaci o způsobu a rozsahu využití.

Deník údržby výpočetního programu

(4.21) V této dokumentaci uživatelské organizace jsou stručnou a přehlednou formou zaznamenány informace o:

- instalované verzi výpočetního programu na začátku procesu,
- všech následně instalovaných verzích a revizích (včetně data zahájení jejich využívání),
- opravách a úpravách výpočetního programu provedených uživatelskou organizací, pokud má uživatelská organizace přístup ke zdrojovému kódu výpočetního programu,
- chybách ve výpočetním programu nalezených během používání a jejich opravách (v případě rozsáhlých programů, a pokud uživatelská organizace není vykonavatelem autorských práv, může být nahrazeno stručnou informací o popisu údržby výpočetního programu vykonavatelem autorských práv na základě smluvních podmínek),
- případných chybách, které nejsou opraveny nebo nejsou opravitelné a zajištění dosažení přijatelných výsledků s těmito chybami.

Souhrnná informace o verifikaci a validaci výpočetního programu autorskou, případně uživatelskou organizací a zpráva prokazující schopnost uživatelské organizace vytvořit a validovat vstupní model

(4.22) Rozsah, metody a výsledky verifikace a validace výpočetního programu jsou zpracovány ve výsledné zprávě. Pokud nejsou dostupné dostatečně podrobné informace o rozsahu, metodách a výsledcích verifikace a validace autorskou organizací, musí být verifikace a validace provedena a dokumentována uživatelskou organizací. Pokud byla verifikace a validace provedena jak autorskou tak uživatelskou organizací, je vhodné, aby uživatelská organizace disponovala všemi dostupnými výstupy. Pokud byla provedena verifikace a validace výpočetního programu uživatelskou organizací, není nutné dále prokazovat schopnost uživatelské organizace vytvořit a validovat vstupní model (viz odstavec (4.23)).

(4.23) Pokud nebyla uživatelskou organizací provedena validace výpočetního programu v rozsahu plánovaného použití výpočetního programu (např. z důvodu uplatnění

odstupňovaného přístupu při použití výpočetního programu verifikovaného a validovaného autorskou organizací), uživatelská organizace vytvoří vstupní model pro úlohu odpovídající plánovanému využití výpočetního programu a pomocí něho provede dílčí validaci. Výsledky této dílčí validace shrne ve výsledné zprávě.

4.5 Požadavky na nezávislé oponenty

(4.24) Postup uživatelské organizace je ověřen nezávislým oponentem. Oponent by měl splňovat následující předpoklady:

- není osobou vykonávající žádnou činnost v procesu v dané uživatelské organizaci ani osobou schopnou ovlivnit proces,
- má a udržuje si aktuální schopnost pracovat s hodnoceným výpočetním programem nebo s obdobným výpočetním programem určeným k řešení obdobného rozsahu úloh a využívajícím obdobné metody včetně provádění validace vstupních modelů vytvořených v uvedeném výpočetním programu,
- má odpovídající vzdělání a další předpoklady, potřebné k posouzení předložených podkladů (např. znalost cizího jazyka, pokud je v něm dokumentace předložena).

(4.25) Předpoklady může oponent doložit např. odborným životopisem obsahujícím identifikaci projektů nebo úloh, které uvedeným výpočetním programem řešil.

4.6 Posudek nezávislého oponenta

(4.26) Posudek nezávislého oponenta zajišťuje předkladatelská organizace. Posudek obsahuje hodnocení minimálně v následujících oblastech:

- abstrakt výpočetního programu,
- splnění požadavků na obsah dokumentu, viz kapitola 4.1,
- srozumitelnost, výstižnost a kompletnost informací,
- vhodnost volby výpočetního programu včetně knihovny dat (pokud je relevantní) vzhledem k jeho plánovanému použití, porovnání s alternativními výpočetními programy vhodnými pro oblast plánovaného použití (obzvláště s ohledem na aktuální stav vědy a technické praxe).

a) uživatelská dokumentace,
   - splnění požadavků na obsah dokumentu, viz kapitola 4.4,
   - srozumitelnost, výstižnost a kompletnost informací,
   - existence a použitelnost uživatelského manuálu,

b) souhrnná informace o verifikaci a validaci výpočetního programu autorskou organizací případně uživatelskou organizací,
   - srozumitelnost, výstižnost a kompletnost informací,

- přiměřenost volby metody pro verifikaci a validaci a rozsahu verifikace a validace výpočetního programu s důrazem na oblast jeho zamýšleného použití,
- posouzení volby validační matice.

Pokud byla provedena verifikace a validace jak autorskou, tak uživatelskou organizací, posudek bude obsahovat vyjádření k oběma souhrnným informacím.

c) zpráva prokazující schopnost uživatelské organizace vytvořit a validovat vstupní model (pokud je samostatně zpracována, viz bod (4.22)),
   - srozumitelnost, výstižnost a kompletnost informací,
   - vhodnost zvolené úlohy k prokázání schopnosti uživatelské organizace vytvořit a validovat vstupní model,
   - přiměřenost volby metody pro validaci vstupního modelu s důrazem na oblast zamýšleného použití výpočetního programu,

d) souhrnné hodnocení podkladů,
   - podmínky a omezení použití výpočetního programu zamýšleným způsobem, v souladu s předloženým programem zajištění kvality,
   - doporučení nebo nedoporučení použití výpočetního programu zamýšleným způsobem.

(4.27) Mohou být uvedeny také další skutečnosti důležité z hlediska hodnocení jakékoli oblasti zajištění kvality procesu, k jakékoli skutečnosti v dokumentaci uvedené nebo naopak chybějící, která je pro zamýšlené použití výpočetního programu relevantní.

(4.28) Posudek obsahuje vyjádření k předpokládanému rozsahu použití výpočetního programu resp. jeho omezení s ohledem na rozsah úloh, které je výpočetním programem možné řešit, pro které jsou doloženy výsledky verifikace a validace, a pro které je prokázána schopnost uživatelské organizace vytvořit a validovat výpočetní model.

(4.29) Posudek nezávislého oponenta má odpovídající délku, hodnotí věcnou část podle stanovených kritérií, které slovně ohodnotí. Posudek je vypracován stručně, výstižně a v kvalitě odpovídající odborné úrovni nezávislého oponenta. Posudek obsahuje stanoviska oponenta k jednotlivým posuzovaným oblastem. Posudek neopakuje části z ostatní předložené dokumentace, pokud to není nutné z důvodu srozumitelnosti posudku. V závěru svého posudku oponent přehledně shrne klady a zápory a konečné stanovisko k oponovanému programu.

5 LITERATURA

[1] Zákon č. 263/2016 Sb., *atomový zákon*.

[2] Vyhláška č. 408/2016 Sb., *o požadavcích na systém řízení*.

[3] BN 1/2019: *Požiadavky na zabezpečovanie kvality softvéru pre analýzy bezpečnosti (4. vydanie – revidované a doplnené).* Bratislava 2019. ISBN: 978-80-89706-25-9.

[4] IAEA, *Safety Assessment for Facilities and Activities.* IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Vídeň 2016. ISBN: 978-92-0-109115-4.

[5] IAEA, *Deterministic Safety Analysis for Nuclear Power Plants*. IAEA Safety Standards Series No. SSG-2 (Rev. 1), Vídeň 2019. ISBN: 978-92-0-102119-9.

[6] NRC, *Software Quality Assurance Program and Guidelines*. NUREG/BR-0167. Washington, D. C. 1993

[7] IAEA, *Accident Analysis for Nuclear Power Plants.* IAEA Safety Reports Series (SRS) No. 23. Vídeň 2002. ISBN: 92-0-115602-2. ISSN: 1020-6450

[8] CNSC, *Safety Analysis: Deterministic Safety Analysis.* Regulatory Document REGDOC-2.4.1. Ottawa 2014. ISBN:978-1-100-23790-9.

[9] Vyhláška č. 162/2017 Sb., *o požadavcích na hodnocení bezpečnosti podle atomového zákona.*

[10] IAEA, *IAEA Safety Glossary: 2018 Edition.* Vídeň 2019. ISBN: 978-92-0-104718-2.

[11] ČSN ISO/IEC 14594-5. *Informační technologie - Hodnocení softwarového produktu - Část 5: Postup pro hodnotitele.* Praha, 1999, 36 s. Třídící znak (369028).

[12] Vyhláška č. 329/2017 Sb., *o požadavcích na projekt jaderného zařízení.*

[13] Vyhláška č. 21/2017 Sb., *o zajišťování jaderné bezpečnosti jaderného zařízení.*

[14] Vyhláška č. 358/2016 Sb. *o požadavcích na zajišťování kvality a technické bezpečnosti a posouzení a prověřování shody vybraných zařízení.*

[15] ISO/IEC 25051. *Software engineering: Systems and software Quality Requirements and Evaluation (SQuaRE); Requirements for quality of Ready to Use Software Product (RUSP) and instructions for testing.* Ženeva 2014, 2. vydání.

[16] ČSN EN ISO 9001:2016. *Systém managementu kvality (QMS).* Praha, 2016.

[17] ČSN EN ISO/IEA 27001. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Požadavky.* Praha, 2014, 28 s. Třídící znak (369797).

[18] ČSN IEC 60050-692. *Mezinárodní elektrotechnický slovník - Část 692: Výroba, přenos a rozvod elektrické energie - Spolehlivost a kvalita služby elektrizačních soustav.* Praha, 2019, 136 s. Třídící znak (330050).

ZPRACOVATELÉ

Tereza Marková, Daniel Vlček

GARANT

Tereza Marková