ÚRAD
JADROVÉHO DOZORU
SLOVENSKEJ REPUBLIKY

EDÍCIA

Bezpečnosť jadrových zariadení

2019

BN 1/2019

Požiadavky na zabezpečovanie kvality softvéru pre analýzy bezpečnosti
(4. vydanie – revidované a doplnené)

Požiadavky na zabezpečovanie kvality softvéru pre analýzy bezpečnosti
(4. vydanie – revidované a doplnené)

Vydal Úrad jadrového dozoru Slovenskej republiky
Neperiodická publikácia

Spracovateľ: Ing. Ján Husárček, CSc., riaditeľ odboru bezpečnostných analýz a technickej podpory, Úrad jadrového dozoru Slovenskej republiky
Gestor: Ing. Ján Husárček, CSc., riaditeľ odboru bezpečnostných analýz a technickej podpory, Úrad jadrového dozoru Slovenskej republiky
Recenzenti : Ing. Teodor Zajíček, Jadrová a vyraďovacia spoločnosť, a.s.
Ing. Miroslav Mlčúch, Jadrová energetická spoločnosť Slovenska, a. s.
Ing. Peter Lisický, PhD., Slovenské elektrárne, a.s.
Ing. Boris Kvizda, VUJE, a.s.

BN 1/2019
ISBN 978-80-89706-25-9
EAN 9788089706259

Bratislava, apríl 2019

Anotácia

V bezpečnostnom návode sú zhrnuté základné požiadavky Úradu jadrového dozoru Slovenskej republiky kladené na zabezpečovanie kvality softvéru pre analýzy bezpečnosti. Odporúčania sa týkajú vývoja, zaobstarávania, údržby a využitia softvéru, ktoré vo väzbe na analýzy bezpečnosti nachádzajú uplatnenie pri navrhovaní, projektovaní a umiestňovaní, výstavbe, uvádzaní do prevádzky, prevádzke, opravách, rekonštrukciách i vyraďovaní z prevádzky jadrových zariadení na Slovensku.

---

bezpečnosť, návod, softvér, kvalita, jadrové zariadenie

Abstract

The safety guideline summarises the basic requirements of the Nuclear Regulatory Authority of the Slovak Republic laid down for the quality assurance of software for safety analyses. These concern the development, procurement, maintenance and use of computer information software as applied to the design, sitting, construction, operation, repair, and upgrade and decommissioning of nuclear facilities in Slovakia.

---

guideline, safety, software, quality assurance, nuclear facility

Obsah

Úvod ... 1
1 Predmet a účel ... 1
2 Rozsah platnosti ... 2
3 Vymedzenie pojmov ... 3
4 Životný cyklus softvéru ... 4
4.1 Štádium formulovania požiadaviek ... 4
4.2 Štádium projektovania ... 5
4.3 Štádium implementácie ... 5
4.4 Štádium testovania ... 5
4.5 Štádium inštalácie a kontroly ... 6
4.6 Štádium používania a údržby ... 6
4.7 Štádium vyradenia softvéru z používania ... 6
5 Verifikácia a validácia softvéru ... 7
5.1 Verifikácia softvéru ... 7
5.2 Validácia softvéru ... 7
5.2.1 Validácia s použitím údajov z experimentov uskutočnených na experimentálnych zariadeniach ... 8
5.2.2 Validácia s použitím reálnych údajov z jadrových zariadení ... 8
5.2.3 Validácia porovnaním s výsledkami výpočtov vykonaných iným už overeným a validovaným softvérom ... 8
5.3 Presnosť predikcie softvéru ... 9
6 Riadenie konfigurácie ... 9
6.1 Identifikácia konfigurácie ... 9
6.2 Kontrola zmien konfigurácie ... 10
6.3 Evidencia stavu konfigurácie ... 10
6.4 Oznamovanie konfigurácie ... 10
7 Dokumentácia ... 10
7.1 Plán kvality ... 11
7.2 Dokumentácia k požiadavkám na softvér ... 11
7.3 Dokumentácia k projektovaniu softvéru a jeho implementácii ... 11
7.4 Dokumentácia k verifikácii a validácii softvéru ... 12
7.5 Užívateľská dokumentácia ... 12
8 Oznamovanie nesúladov a nápravné opatrenia ... 13
9 Kontrola prístupu a uchovávanie ... 13
10 Nadobúdanie softvéru ... 13
10.1 Softvérové služby ... 13
10.2 Softvér vyvinutý pri použití zodpovedajúceho plánu kvality ... 14
10.3 Softvér vyvinutý bez použitia zodpovedajúceho plánu kvality ... 14
11 Záznamy ... 14
12 Kľúčové požiadavky úradu kladené na softvér ... 14

13 Zoznam literatúry 16

Predhovor

Úrad jadrového dozoru Slovenskej republiky začal v roku 1995 vydávať vlastné neperiodické publikácie, ako edíciu Bezpečnosť jadrových zariadení, s cieľom zverejňovať vybrané všeobecne záväzné právne predpisy, bezpečnostné požiadavky, odporúčania a návody súvisiace s činnosťou Úradu jadrového dozoru Slovenskej republiky.

V rámci edície Bezpečnosť jadrových zariadení Úrad jadrového dozoru Slovenskej republiky vydáva tri skupiny publikácií.

Obsahom prvej skupiny publikácií sú vybrané všeobecne záväzné právne predpisy a medzinárodné zmluvy z oblasti mierového využívania jadrovej energie; sú označené červeným pruhom.

V druhej skupine sú dokumenty z oblasti jadrovej bezpečnosti charakteru odporúčaní a návodov, ktoré konkretizujú a dopĺňajú požiadavky všeobecne záväzných právnych predpisov; sú označené modrým pruhom.

Obsahom tretej skupiny publikácií sú ostatné dokumenty z oblasti jadrovej bezpečnosti informatívneho charakteru; sú označené sivým pruhom.

Pri spracovaní dokumentov druhej a tretej skupiny sa využívajú dokumenty Medzinárodnej agentúry pre atómovú energiu vo Viedni a iných medzinárodných organizácií, medzinárodné a národné technické normy, ako aj dokumenty vydané zahraničnými dozornými orgánmi a odbornými organizáciami. Dokumenty sú spracované na základe rozhodnutia predsedu Úradu jadrového dozoru Slovenskej republiky zamestnancami úradu alebo externými organizáciami i s využitím vlastných skúseností a poznatkov. Pred ich vydaním a zverejnením sú schválené predsedom úradu.

Predmetná publikácia Požiadavky na zabezpečovanie kvality softvéru pre analýzy bezpečnosti (4. vydanie – revidované a doplnené) je bezpečnostným návodom.

Pripomienky a doplnky k tejto publikácii zasielajte na Úrad jadrového dozoru Slovenskej republiky, odbor legislatívno-právny, Bajkalská 27, P. O. Box 24, 820 07 Bratislava 27.

Úvod

Jedným z nástrojov na hodnotenie správania sa jadrových zariadení sú výpočtové programy. Tie zahrňujú rôzne typy výpočtových programov od vysokošpecializovaných zameraných napríklad na fyziku jadrového reaktora či pevnosť stavebných konštrukcií až po komplexné termicko-hydraulické výpočtové programy. Mnohé z nich sú široko akceptované a využívané v rôznych krajinách a aplikáciách vzťahujúcich sa k spracovávaniu technických zdôvodnení pre projekty jadrových zariadení alebo k posudzovaniu bezpečnosti jadrových zariadení. Výber výpočtového programu na konkrétnu aplikáciu a napočítané výsledky závisia od rôznych faktorov vrátane použitých modelov zabudovaných do výpočtového programu, dokumentácie k výpočtovému programu, dosiahnutej úrovne jeho overenia a validácie, presnosti modelovania, použitých údajov, metodiky, ale aj kvalifikácie užívateľa.

Spomedzi faktorov, ktoré ovplyvňujú kvalitu analýz bezpečnosti, sa tento bezpečnostný návod zameriava na zabezpečovanie kvality výpočtových programov pre ich použitie v analýzach bezpečnosti (ďalej len „softvér“).

Softvér použitý na analýzy bezpečnosti má byť podrobený verifikácii a validácii (GSR Part 4, požiadavka 18 /2/).

Všetky činnosti, ktoré ovplyvňujú kvalitu softvéru, sa majú riadiť pomocou postupov, ktoré sú špecifické pre zabezpečovanie kvality softvéru. Majú sa uplatňovať zavedené postupy softvérového inžinierstva, ktoré sa vzťahujú na vývoj a údržbu softvéru pre bezpečnosť. Formalizované postupy a pokyny majú byť zavedené pre celý životný cyklus softvéru vrátane vývoja softvéru, verifikácie (overenia) a validácie a pokračujúceho procesu údržby s dôrazom na hlásenie a opravu chýb.

Aby sa minimalizovali ľudské chyby v softvéri, na vývoji, overovaní a validácii softvéru by sa mali podieľať len osoby s vhodnou kvalifikáciou alebo pod dohľadom osôb s takouto kvalifikáciou. Podobne, v užívateľských organizáciách by softvér mali používať iba kvalifikovaní pracovníci alebo pracovníci pod dohľadom.

1 Predmet a účel

Tento bezpečnostný návod (ďalej len „návod“) poskytuje odporúčanie Úradu jadrového dozoru Slovenskej republiky (ďalej len „úrad“) na možný spôsob zabezpečovania kvality softvéru pre analýzy bezpečnosti. Požiadavky úradu sa týkajú vývoja, zaobstarávania, údržby a využitia softvéru, ktorý vo väzbe na analýzy bezpečnosti nachádza uplatnenie pri navrhovaní, projektovaní a umiestňovaní, výstavbe, uvádzaní do prevádzky, prevádzke, opravách, rekonštrukciách i vyraďovaní z prevádzky jadrových zariadení na Slovensku.

Pri stanovovaní požiadaviek a podmienok kladených na softvér sa vychádzalo z dokumentu vydaného v Spojených štátoch amerických /1/ i v Medzinárodnej agentúre pre atómovú energiu vo Viedni /2/ pri zohľadnení skúseností z využívania softvéru na Slovensku.

Požiadavky uvedené v návode majú byť primerane transformované do dokumentácie systému manažérstva kvality držiteľa povolenia alebo žiadateľa o povolenie, respektíve do systémov manažérstva kvality dodávateľov analýz bezpečnosti, a to v závislosti od štádia životného cyklu softvéru, na ktorom sú prevádzkovateľ alebo jeho spracovatelia analýz bezpečnosti zúčastnení.

Vo všeobecnej časti návodu (kapitola 4) je stručne charakterizovaný životný cyklus softvéru a činnosť vykonávaná v každom jeho štádiu. Keďže väčšina softvéru používaného na technické zdôvodnenie projektu a hodnotenie jadrovej bezpečnosti jadrových zariadení na Slovensku bola vyvinutá a odladená v zahraničí a následne prispôsobená zmenám v užívateľskom prostredí u nás, sú v konkrétnej časti návodu opísané a uvedené odporúčania a podmienky úradu len pre tie činnosti, ktoré sú považované zo strany úradu za najdôležitejšie a majú byť vykonané alebo zabezpečené užívateľom nadobudnutého softvéru. V súlade s tým je v návode odporučený postup na verifikáciu a validáciu softvéru (kapitola 5), riadenie konfigurácie (kapitola 6), užívateľská dokumentácia, ktorá má byť súčasťou softvéru spôsobilého na používanie (sekcia 7.5), oznamovanie nesúladov a nápravné opatrenia (kapitola 8), kontrola prístupu a uchovávanie (kapitola 9), nadobúdanie softvéru (kapitola 10) a záznamy (kapitola 11). Zdôraznená je potreba plánov kvality na používanie a údržbu softvéru (sekcia 7.1) ako aj kvalifikovanej práce so softvérom. Zhrnutie požiadaviek úradu kladených na používanie a údržbu softvéru pre analýzy bezpečnosti je vykonané v kapitole 12 návodu.

Potenciálnymi užívateľmi návodu sú organizácie, ktoré používajú softvér pre analýzy bezpečnosti podliehajúce štátnemu dozoru nad jadrovou bezpečnosťou jadrových zariadení. Návod je určený i pre vnútorné potreby úradu.

2 Rozsah platnosti

Vydávaný návod má charakter odporúčania, a teda nie je pre zodpovedné organizácie záväzný. Naplnenie jeho obsahu však zvyšuje kvalitu softvéru pre analýzy bezpečnosti, dôveryhodnosť výsledkov jeho použitia a zároveň pôsobí ako určitá podmienka pri kladnom odsúhlasovaní, schvaľovaní alebo posudzovaní zo strany úradu tej dokumentácie, ktorá je predkladaná držiteľom povolenia/žiadateľom o povolenie a podklady k nej boli spracované použitím softvéru.

Na bezpečnostný softvér pre systémy kontroly a riadenia jadrových zariadení sa tento návod nevzťahuje.

Predmetný návod je použiteľný pre nový, vyvíjaný softvér i pre softvér, ktorý bol jeho užívateľom nadobudnutý.

Bezpečnostné návody nie sú právne záväzné, avšak ich dodržiavanie napomáha zabezpečiť podmienky bezpečného využívania jadrovej energie alebo vykonávania činností súvisiacich s využívaním jadrovej energie.

Tento bezpečnostný návod je revidovaným a doplneným 4. vydaním bezpečnostného návodu ÚJD SR s označením BNS I.12.1/2012 Požiadavky na zabezpečovanie kvality softvéru pre analýzy bezpečnosti, ktorý sa týmto v plnom rozsahu nahradzuje.

Tento bezpečnostný návod sa vydáva bez časového obmedzenia.

3 Vymedzenie pojmov

Pojmy vymedzené pre účely tohto bezpečnostného návodu sú zhrnuté v nasledujúcom texte.

Evidencia stavu konfigurácie je zaznamenávanie a oznamovanie informácie, ktorá je potrebná na efektívne riadenie konfigurácie, na identifikovanie konfigurácie, identifikovanie stavu navrhovaných zmien a na realizáciu odsúhlasených zmien.

Identifikácia konfigurácie je proces označovania konfiguračných položiek v nejakom výpočtovom systéme a zaznamenávanie ich charakteristík.

Konfiguračná kontrola je proces vyhodnocovania, odsúhlasovania (alebo neodsúhlasovania) a zosúlaďovania zmien konfiguračných položiek po identifikovaní konfigurácie.

Konfiguračná položka je súbor hardwarových a softvérových elementov považovaných za jednotku pre účely konfiguračnej kontroly.

Konfigurácia je určovaná konfiguračnými položkami.

Program zabezpečovania kvality sú plánované a systematické činnosti vykonávané počas vývoja, používania a údržby softvéru, ktoré sú nevyhnutné pre získanie náležitej dôvery, že softvér vyhovuje požiadavkám, ktoré sú na neho kladené.

Projekt softvéru je konkrétny návrh na vypracovanie softvéru.

Riadenie konfigurácie je proces identifikácie a stanovovania zmien konfiguračných položiek v nejakom výpočtovom systéme, ktorým sa kontrolujú zmeny týchto položiek počas životného cyklu softvéru, zaznamenávajú a oznamujú stavy konfiguračných položiek a zmeny požiadaviek ako aj overovanie úplnosti a správnosti identifikácie konfigurácie, konfiguračnej kontroly, evidencie stavu konfigurácie a auditu.

Softvér sú výpočtové programy, procedúry, pravidlá a pripojená k nim dokumentácia vrátane údajov pre prevádzku výpočtového systému.

Softvérová organizácia je organizácia zodpovedajúca za pôvodný projekt softvéru alebo organizácia poverená schvaľovaním zmien v softvéri.

Testovanie je proces preskúšania alebo vyhodnotenia systému alebo konštrukcie (komponentu), ktorý je vykonávaný buď na overenie, či systém alebo konštrukcia (komponent)

vyhovuje stanoveným požiadavkám, alebo na stanovenie rozdielov medzi očakávanými a aktuálnymi výsledkami.

Validácia je preukázanie a vyhodnotenie schopnosti produktu verne modelovať správanie jadrového zariadenia a plniť stanovené požiadavky.

Verifikácia je overenie, či produkt v každom štádiu svojho životného cyklu (vývoja) spĺňa alebo nespĺňa stanovené požiadavky a je pripravený na použitie.

Výpočtový program je postupnosť inštrukcií vhodných pre ich spracovanie na počítači. Spracovanie môže zahrňovať i použitie prekladača, aby mohol byť výpočtový program vykonaný.

Životný cyklus softvéru je časové obdobie, ktoré začína zahájením vývoja softvéru a končí vyradením softvéru z užívateľského používania. Životný cyklus softvéru obyčajne pozostáva zo štádií – formulovanie požiadaviek, projektovanie, implementácia, testovanie, inštalácia a kontrola, používanie a údržba, vyradenie softvéru.

4 Životný cyklus softvéru

Požiadavky návodu sú založené na modeli životného cyklu softvéru pozostávajúceho zo siedmych štádií (formulovanie požiadaviek, projektovanie, implementácia, testovanie, inštalácia a kontrola, používanie a údržba, vyradenie softvéru), ktoré sú spoločne s činnosťou vykonávanou na každom z nich obecne charakterizované v nasledujúcom texte. Uvádzané činnosti sú síce priradené k jednotlivým štádiám životného cyklu softvéru, ale vzájomne na seba nadväzujú a môžu sa prekrývať. Počet štádií a dôraz kladený na každé z nich závisí od druhu softvéru a od jeho komplexnosti. Do užívateľského používania sa softvér dostáva v štádiu jeho inštalácie a kontroly.

4.1 Štádium formulovania požiadaviek

Štádium formulovania požiadaviek je prvým, počiatočným štádiom životného cyklu softvéru. Počas tohto štádia sú zadané, zdokumentované a preverené požiadavky, ktorým má softvér vyhovovať, vzhľadom na jeho správnosť (miera splnenia požiadaviek kladených na softvér), použiteľnosť (miera naplnenia potrieb užívateľa), robustnosť (miera odolnosti softvéru voči nepriaznivým vplyvom okolitého prostredia, napríklad zadanie nepovolených vstupov), spoľahlivosť (miera frekvencie a kritickosti zlyhania softvéru počas používania), výkonnosť (napríklad nároky na pamäť, rýchlosť výpočtu), presnosť, bezpečnosť (miera odolnosti voči neoprávneným zásahom alebo nevykonávanie žiadnych nezamýšľaných funkcií, ktoré by buď samy, alebo v kombinácii s inými funkciami mohli znehodnotiť výpočtový systém) a vonkajšie prepojenia softvéru (komunikácia s človekom, s iným softvérom). Sformulované požiadavky určujú odozvu softvéru na očakávané vstupné údaje a zároveň poskytujú informáciu, ktorá je nevyhnutná pre navrhnutie matematického modelu a zostavenie výpočtového programu.

Štádium formulovania požiadaviek zahrňuje i prípravu programu pre verifikáciu a validáciu softvéru. Program verifikácie a validácie softvéru obsahuje ciele a kritériá verifikácie a validácie, opis metodiky, požiadavky, ktoré má softvér spĺňať, program testovania a opatrenia na riadenie verifikácie a validácie softvéru.

4.2 Štádium projektovania

V priebehu tohto štádia je vypracovaný, zdokumentovaný a prekontrolovaný projekt softvéru podľa požiadaviek, ktoré sú na softvér kladené. V projekte softvéru je presne vymedzená jeho stavba, použité fyzikálne riešenia a ich transformácia do matematického modelu (algoritmus, riadiaca logika, korelácie, štruktúry údajov) i obmedzenia softvéru. V štádiu projektovania môže dôjsť k úprave už zdokumentovaných požiadaviek na softvér.

Činnosť verifikácie a validácie softvéru v štádiu projektovania pozostáva z:

a) vytvorenia programu testovania vychádzajúceho z projektu softvéru a z požiadaviek, ktoré sú na softvér kladené,

b) vytvorenia testovacích príkladov (napríklad angl. „ISP – International Standard Problems“),

c) preverenia projektu softvéru vrátane stavby softvéru, použitých algoritmov a údajov, s cieľom uistiť sa, že je vyhovené požiadavkám, ktoré sú na neho kladené.

4.3 Štádium implementácie

Počas tohto štádia zostavený výpočtový program je preložený do počítačového jazyka, aby mohol byť vykonaný s cieľom odhaliť a opraviť chyby.

Činnosť verifikácie v štádiu implementácie pozostáva z preskúšania a opravy softvéru, aby bol zabezpečený súlad so štandardom programovacieho jazyka a s prijatými zvyklosťami.

4.4 Štádium testovania

Štádium testovania je dôležitou súčasťou procesu vývoja softvéru, počas ktorého je projekt softvéru, realizovaný vo výpočtovom programe, preskúšaný na testovacích príkladoch. Počas tohto štádia sú odhalené chyby a softvér je dôkladne preverený, aby bolo zrejmé, aké úpravy je potrebné urobiť v matematickom modeli, vo výpočtovom programe, v testovacích príkladoch a prípadne aj v požiadavkách kladených na softvér.

Testovanie sa vykonáva podľa vopred odsúhlaseného programu a s použitím vhodnej metodiky.

Validácia vykonaná v štádiu testovania preukazuje, že softvér vyhovuje stanoveným požiadavkám a produkuje správne výsledky pre testovacie príklady. Pre účely vyhodnotenia technickej dostatočnosti je urobená analýza citlivosti. Výsledky z testovacích príkladov sú porovnané s výsledkami získanými prostredníctvom:

a) experimentov uskutočnených na experimentálnych zariadeniach a procesov, ktoré prebehli na jadrových zariadeniach,

b) štandardných testovacích príkladov so známym riešením,

c) porovnania s výsledkami výpočtov vykonaných iným už overeným a validovaným softvérom,

d) analýz bez počítačovej účasti,

e) potvrdených, publikovaných údajov a korelácií.

Porovnanie je zdokumentované a vyhodnotené vzhľadom na stanovené kritériá.

4.5 Štádium inštalácie a kontroly

V priebehu tohto štádia sa softvér stáva súčasťou výpočtového systému, ktorý integruje použiteľné softvérové elementy, hardvér a vstupné údaje. Proces integrácie spočíva v inštalácii softvéru, hardvéru, v pripojení vstupných údajov a overovaní, či všetky potrebné elementy boli do výpočtového systému zahrnuté.

Činnosť verifikácie a validácie v štádiu inštalácie a kontroly softvéru obsahuje:

a) vykonanie testov pre inštaláciu a integráciu,
b) vykonanie kontrolného výpočtu pre predpokladanú oblasť používania softvéru, ktorého výsledky okrem iného slúžia i na preukazovanie toho, že užívateľ si osvojil nadobudnutý softvér a vie s ním pracovať kvalifikovane,
c) vyhotovenie dokumentácie o inštalácii softvéru a vykonaných kontrolných výpočtoch.

4.6 Štádium používania a údržby

Pred týmto štádiom je už softvér daný do užívateľského použitia. Ďalšia činnosť vo vývoji softvéru pozostáva z údržby softvéru, ktorá je zameraná na odstránenie skrytých chýb alebo zohľadnenie v softvéri nových, upravených požiadaviek, nových teoretických poznatkov a experimentálnych výsledkov, ale aj z prispôsobovania softvéru k zmenám v užívateľskom prostredí. Úpravy robené v softvéri sú odsúhlasené softvérovou organizáciou (autorom), sú náležite zdokumentované, overené, validované a samozrejme skontrolované.

Vo verifikácii a validácii softvéru sa podľa okolností pokračuje i v štádiu jeho používania a údržby.

4.7 Štádium vyradenia softvéru z používania

Štádium vyradenia softvéru z používania je posledným záverečným štádiom, ktorým sa končí životný cyklus softvéru. Ďalšiemu bežnému používaniu softvéru je zabránené. Po ukončení používania softvéru môžu platiť obmedzenia na ochranu informácií o softvéri.

5 Verifikácia a validácia softvéru

Softvér má byť podrobený verifikácii a validácii pre oblasť jeho použitia (GSR Part 4, požiadavka 18 /2/). Proces i výsledky procesu verifikácie a validácie je potrebné vyhodnotiť a zdokumentovať. Osoby vykonávajúce verifikáciu a validáciu majú byť iné ako tie, čo navrhovali softvér.

Činnosť vykonávaná pri verifikácii a validácii preukazuje a zabezpečuje, aby softvér spĺňal stanovené požiadavky.

5.1 Verifikácia softvéru

Verifikácia softvéru sa má vykonávať hlavne počas vývoja softvéru, aby bolo zabezpečené, že výstupy z každého štádia životného cyklu softvéru plnia požiadavky predchádzajúceho štádia alebo štádií a stanovené požiadavky kladené na softvér.

Verifikácia sa vykonáva podľa programu verifikácie softvéru (viď sekcia 4.1) a je dokumentovaná.

5.2 Validácia softvéru

Validácia softvéru sa má vykonávať od konca štádia implementácie, aby bolo zabezpečené, že softvér vyhovuje stanoveným požiadavkám. Softvér má byť validovaný pre oblasť, ktorá zodpovedá jeho použitiu.

Vo validácii softvéru sa má pokračovať aj v štádiu používania a údržby.

Predmetom validácie má byť nielen nový, vyvíjaný softvér, ale aj už používaný a modifikovaný softvér. Najdôležitejšou metódou validácie je testovanie.

Pre validáciu komplexného softvéru je vhodné spracovať validačnú maticu.

Z kvalitatívneho hľadiska validácia má preveriť správnosť modelovania jednotlivých mechanizmov a procesov (napríklad prúdenie tekutiny, prenos hmoty, šírenie tepla a pod.), spôsob akým sú tieto mechanizmy a procesy pospájané, prijaté zjednodušujúce predpoklady a zároveň má vyšetriť, či pri vývoji softvéru boli vzaté do úvahy všetky dôležité skutočnosti.

Z kvantitatívneho hľadiska validácia má stanoviť a vyhodnotiť mieru presnosti s akou hodnotený softvér vystihuje ukázané hodnoty. Hodnoty napočítané softvérom majú by porovnané predovšetkým s experimentálnymi hodnotami, so štandardnými testovacími príkladmi, s výsledkami napočítanými iným, už overeným a validovaným softvérom alebo aj s reálnymi údajmi z jadrových zariadení (ďalej len „JZ“), pokiaľ sú takéto údaje k dispozícii.

V praktickom zmysle slova validácia má zahrňovať formulovanie modelu (hypotézy), navrhnutie a vykonanie validačných testov a experimentov, zozbieranie experimentálnych hodnôt, analýzy týchto hodnôt, porovnanie stanovených hodnôt s hodnotami napočítanými softvérom podrobovaným validácii a úpravu softvéru (ak je potrebná). Potreba úpravy softvéru

sa má stanoviť podľa toho, ako bol softvér vyhodnotený, t. j. či splnil alebo nesplnil ciele a kritériá validácie, ktoré boli vopred stanovené.

Úrad odporúča, aby sa na validácii softvéru podieľal aj jeho užívateľ.

V nasledujúcej časti návodu je charakterizovaná validácia vykonaná s použitím údajov z experimentov uskutočnených na experimentálnych zariadeniach, údajov z procesov, ktoré prebehli na jadrových zariadeniach a porovnaním s výsledkami výpočtov vykonaných pomocou iného už overeného a validovaného softvéru.

5.2.1 Validácia s použitím údajov z experimentov uskutočnených na experimentálnych zariadeniach

Nevyhnutnou podmienkou validačného procesu s použitím údajov získaných z experimentálnych zariadení je mať vhodné experimentálne údaje. Pojem vhodné experimentálne údaje znamená, že sú vybrané hlavné veličiny, že je experimentmi pokrytý dostatočný rozsah zmien týchto veličín, že merania sú urobené dôkladne a experimentálne chyby v údajoch sú dostatočne malé, aby bolo možné porovnať namerané hodnoty s napočítanými.

5.2.2 Validácia s použitím reálnych údajov z jadrových zariadení

Pretože experimentálne zariadenia sú obyčajne malorozmernými modelmi JZ, alebo jednotlivých častí JZ, čo nie vždy plne vyhovuje, niektoré druhy softvéru majú byť validované i s použitím hodnôt získaných v reálnych podmienkach práce JZ, ako sú testy (spúšťanie jadrovej elektrárne) alebo prechodové procesy, ktoré nastali počas prevádzky JZ.

Testy spúšťania sú obyčajne dobre technicky aj organizačne zabezpečené a majú k dispozícii potrebné meracie zariadenia, aby bolo získané maximum vhodných údajov. Avšak z bezpečnostných i ekonomických dôvodov vyšetrované veličiny sú držané ďaleko od uvažovaných limitných hodnôt týchto veličín v softvéri, a preto údaje len z testov spúšťania nie sú dostatočné pre validáciu softvéru v celej oblasti jeho použitia.

Prechodové procesy na jadrových zariadeniach, naproti tomu, pre uvedené účely poskytujú obvykle len skromné údaje. Podmienky, pri ktorých JZ pracuje, sú pre potreby validácie softvéru v širšom rozsahu často známe nedostatočne a neraz chýba i informácia o činnosti obsluhy JZ. Preto analýza prevádzkových udalostí si vyžaduje vykonať značné množstvo parametrických výpočtov s rôznymi podmienkami, aby boli poskytnuté kvalitné výsledky. V prípade, že zariadenia alebo zásahy obsluhy JZ nie sú v softvéri dostatočne modelované a hrajú dôležitú úlohu, potom je potrebné softvér modifikovať, prispôsobiť ho k špecifickým podmienkam a opätovne verifikovať a validovať. Táto otázka je čiastočne ošetrená v sekcii 6.2 – Kontrola zmien konfigurácie.

5.2.3 Validácia porovnaním s výsledkami výpočtov vykonaných iným už overeným a validovaným softvérom

Porovnanie výsledkov získaných z rôznych softvérov môže byť využité na kontrolu výpočtov a to i v prípade, keď použité výpočtové modely sú rôzne.

Napriek rozdielom vo výsledkoch, ktoré je možné očakávať, dôležitosť porovnania výsledkov medzi sebou z rôznych softvérov spočíva v odhalení a preanalyzovaní príčin ich rozdielnosti i vo vyhodnotení neurčitostí.

5.3 Presnosť predikcie softvéru

Cieľom validácie softvéru, z kvantitatívneho a kvalitatívneho hľadiska, je stanovenie a hodnotenie miery presnosti s akou softvér vystihuje ukázané hodnoty.

Mieru presnosti softvéru ovplyvňujú neurčitosti spojené s modelmi a koreláciami použitými v softvéri, výpočtovými schémami, užívateľskými voľbami, nemodelovanými procesmi a javmi, dátovými knižnicami, počítačovou platformou ako aj nedostatkami v samotnom výpočtovom programe. Vplyv užívateľa softvéru na presnosť predikcie softvéru charakterizuje tzv. „užívateľský efekt“.

Pri hodnotení miery presnosti predikcie softvéru je zvyčajne potrebné zohľadniť:

a) identifikovanie dôležitých trendov v podporných experimentálnych údajoch a očakávanom správaní sa jadrového zariadenia,

b) ocenenie presnosti celkových výsledkov napočítaných výpočtovým programom spojených s použitým základným numerickým prístupom,

c) ocenenie presnosti v kľúčových modeloch a celkových výsledkoch napočítaných výpočtovým programom,

d) stanovenie citlivosti pre dôležité procesy,

e) presnosť experimentálnych údajov, vzhľadom na ktoré je presnosť predikcie softvéru vyhodnotená.

Presnosť softvéru sa stanovuje analytickými metódami, ktoré preverujú kvalitatívne a kvantitatívne hľadisko. Takéto hodnotenie zvyčajne vyžaduje porovnanie výsledkov softvéru s údajmi pochádzajúcimi z:

a) experimentálnych zariadení,
b) reálnych jadrových zariadení,
c) výsledkov iných overených výpočtových kódov.

Pri použití dát z neplno-rozmerových experimentálnych zariadení sa zohľadňujú rozdiely spojené s rozmerom experimentálneho zariadenia.

6 Riadenie konfigurácie

6.1 Identifikácia konfigurácie

Po dokončení vývoja softvéru má byť stanovená a zdokumentovaná konfigurácia referenčnej verzie softvéru. Odsúhlasené zmeny, ktoré sú robené na referenčnej verzii

dodatočne, majú byť do nej tiež zahrnuté. Referenčná verzia by mala definovať poslednú odsúhlasenú konfiguráciu softvéru.

Pre konfiguračné položky má byť zavedený systém označovania, aby bolo možné:

a) jednoznačne identifikovať všetky konfiguračné položky,

b) identifikovať zmeny konfiguračných položiek,

c) jednoznačne identifikovať každú konfiguráciu opraveného (modifikovaného) softvéru, ktorý je daný do používania.

6.2 Kontrola zmien konfigurácie

Zmeny, ktoré boli urobené v softvéri, majú byť zdokumentované. Príslušná dokumentácia má obsahovať opis zmien, podstatu zmien a má identifikovať referenčnú verziu softvéru, kde boli tieto zmeny urobené.

Zmeny urobené v softvéri by mali byť vyhodnotené a schválené organizáciou, ktorá zodpovedá za pôvodný projekt softvéru, hoci schvaľovaním zmien bola poverená aj alternatívna organizácia. Činnosť spojená s overovaním zmien má byť vykonávaná tak, aby bolo zabezpečené, že zmeny sú v dokumentácii k softvéru primerane opísané. Taktiež má byť zachovaná prehľadnosť dokumentácie.

Softvér s vykonanými zmenami má byť v primeranom rozsahu opätovne podrobený validácii.

6.3 Evidencia stavu konfigurácie

Každá informácia, ktorá je potrebná na opísanie stavu konfigurácie, má byť zaznamenaná. Táto informácia má identifikovať odsúhlasenú konfiguráciu, stav schválených i navrhovaných zmien ako aj informáciu slúžiacu pre konfiguračnú kontrolu.

6.4 Oznamovanie konfigurácie

Užívateľ vykonáva zmeny v konfigurácii softvéru, keď mu to softvérová organizácia umožní a dá mu na to oprávnenie. S navrhovanými alebo uskutočnenými zmenami, vykonanými užívateľom v konfigurácii softvéru, má byť oboznámená softvérová organizácia.

Treba vytvoriť systém, ktorým softvérová organizácia oznamuje užívateľom softvéru aktualizáciu konfigurácie referenčnej verzie softvéru.

7 Dokumentácia

Nasledujúca časť návodu opisuje rozsah i obsah dokumentácie požadovanej úradom, ktorá má byť súčasťou softvéru. K vypracovávaniu a zhromažďovaniu dokumentácie k softvéru je potrebné pristupovať zodpovedne. Dokumentácia k softvéru má byť prehľadná,

kontrolovateľná a spracovaná v takom rozsahu a úplnosti, aby preukazovala, že softvér je spôsobilý na používanie.

7.1 Plán kvality

Plán kvality obsahuje požiadavky na zabezpečovanie kvality softvéru a má byť spracovaný pre každý softvér. Plán kvality softvéru má existovať pre nový, vyvíjaný softvér od štádia zahájenia jeho životného cyklu a pre nadobudnutý softvér od chvíle, keď ho preberá užívateľská organizácia. Môže byť pripravený pre každý jednotlivý softvér individuálne alebo ako všeobecný dokument, použiteľný pre softvér vyvíjaný vo vnútri organizácie alebo nadobudnutý touto organizáciou.

Plán kvality softvéru má byť zapracovaný do systému manažérstva kvality organizácie. V pláne kvality má byť uvedené:

a) softvér, na ktorý sa vzťahuje,

b) názov organizácie (resp. organizačnej jednotky) zodpovednej za realizáciu programu zabezpečovania kvality, rozdelenie úloh a vymedzenie zodpovedností,

c) požadovaná dokumentácia,

d) štandardy, zvyklosti, metódy, metodológie, požiadavky a kritériá, podľa ktorých je softvér vyvíjaný, overovaný, validovaný, ako aj postupy pre zabezpečenie súladu s nimi,

e) požadované previerky softvéru,

f) postup pre ohlasovanie nesúladov softvéru a nápravné opatrenia,

g) kontrola prístupu a uchovávanie referenčnej verzie softvéru,

h) požiadavky na kvalifikáciu osôb pracujúcich so softvérom, ktoré spracovávajú technické zdôvodnenia projektu alebo hodnotia jadrovú bezpečnosť jadrových zariadení.

7.2 Dokumentácia k požiadavkám na softvér

Dokumentácia k požiadavkám na softvér má obsahovať požiadavky, ktorým má softvér vyhovovať. Tieto požiadavky majú byť podľa možnosti zamerané na správnosť, použiteľnosť, robustnosť, spoľahlivosť, výkonnosť, presnosť, bezpečnosť a vonkajšie prepojenia softvéru.

7.3 Dokumentácia k projektovaniu softvéru a jeho implementácii

Dokumentácia k projektovaniu softvéru a jeho implementácii zahrňuje dokument alebo sériu dokumentov, ktoré majú obsahovať:

a) opis hlavných častí vývoja softvéru,

b) technický opis softvéru zameraný na jeho teoretickú bázu, použitý matematický model (korelácie, rovnice, diskretizácia rovníc, metódy riešenia rovníc a pod.), riadiacu logiku, štruktúry údajov,

c) opis vstupov a výstupov,

d) samotný výpočtový program s komentármi, ktorý je napísaný takým spôsobom, že môže byť preložený do počítačového jazyka.

Zdrojový kódu softvéru má spravidla len softvérová organizácia. Užívateľ softvéru k nemu nemusí mať prístup.

7.4 Dokumentácia k verifikácii a validácii softvéru

Dokumentácia k verifikácii a validácii softvéru má opisovať testovacie úlohy a kritériá, ktoré sú dané pre vykonanie verifikácie a validácie softvéru v každom štádiu jeho životného cyklu. Dokumentácia má takisto špecifikovať konfiguráciu softvéru i hardwaru týkajúcu sa verifikácie a validácie softvéru. Dokumentácia má byť organizovaná takým spôsobom, aby bolo možné porovnať medzi sebou požiadavky kladené na softvér s jeho projektom. Rozhodujúcou časťou dokumentácie sú výsledky verifikácie softvéru a jeho validácie, výsledky testov a previerok. Zhodnotený má byť i dosiahnutý stav vývoja a použiteľnosti softvéru, neúplnosť uskutočnenia zámerov projektu, či neúplnosť zohľadnenia všetkých požiadaviek, či parametrov stanovených vopred.

7.5 Užívateľská dokumentácia

Užívateľská dokumentácia má byť zrozumiteľná. Má prinajmenšom obsahovať:

a) abstrakt softvéru,

b) teoretický manuál, ktorý obsahuje opis použitého matematického modelu, odkazy na použité korelácie a zdrojové dokumenty,

c) užívateľský manuál

- inštrukcie potrebné pre zvládnutie komunikácie medzi užívateľom a softwarom (v prípade, že je potrebné zaučenie do práce so softvérom, táto skutočnosť má byť v dokumentácii uvedená),
- opis vstupov a výstupov, požiadavky na vstup a výstup, tvorenie vstupov a výstupov, príklady vstupov a výstupov,
- opis oblasti použitia softvéru a jeho obmedzení,
- opis ošetrených nesúladov v softvéri a spôsob ako ich užívateľ vyrieši,

d) vzorové testovacie príklady vrátane vstupov a výstupov,

e) validačnú správu, ktorá obsahuje súhrnné výsledky validácie softvéru, porovnanie napočítaných a nameraných hodnôt a ich vyhodnotenie, odkazy na vykonané experimenty a ďalšiu dokumentáciu, kde je uvedená podrobnejšia informácia.

8 Oznamovanie nesúladov a nápravné opatrenia

Procedúra oznamovania nesúladov softvéru a nápravných opatrení sa má vykonávať za účelom odhalenia a odstránenia chýb v softvéri. Systém oznamovania nesúladov medzi užívateľom a softvérovou organizáciou má zabezpečiť, že o problémoch so softvérom je upovedomovaná softvérová organizácia, aby problémy mohli byť riešené. Zistené chyby a nedostatky v softvéri môžu, ale nemusia byť hodnotené organizáciou zodpovednou za vývoj softvéru. Použitý systém hodnotenia chýb však má byť založený na kritériách odvíjajúcich sa od vplyvu chýb na výsledok. Nápravné opatrenia vykonané softvérovou organizáciou majú zaručiť, že:

a) problémy sú vyhodnotené, dokumentované a v prípade, ak sa to požaduje sú aj vyriešené,

b) chyby sú ohodnotené a odstránené,

c) opravy alebo zmeny vykonané v softvéri sú skontrolované v súlade so sekciou 6.2 tohto návodu,

d) zásahy do softvéru, ktoré boli vykonané na predchádzanie alebo opravu nesúladov sú poskytnuté užívateľom softvéru.

9 Kontrola prístupu a uchovávanie

V rozsahu, v akom to okolnosti dovoľujú, má byť zabezpečená kontrola, ktorá dovoľuje autorizovaný a zabraňuje neautorizovanému prístupu k softvéru a k jeho použitiu.

Referenčná verzia softvéru má byť uchovaná v riadenom režime.

10 Nadobúdanie softvéru

Na používanie nadobudnutého softvéru je potrebný súhlas poskytujúcej organizácie.

10.1 Softvérové služby

Organizácia poskytujúca softvérové služby má mať pre dodávaný softvér prijatý plán kvality, ktorý vyhovuje požiadavkám sformulovaným v sekcii 7.1. Užívateľ má porovnať plán kvality s požiadavkami na jeho obsah a formu a zabezpečiť jeho prípadné doplnenie.

Plán kvality pre softvér má byť súčasťou systému manažérstva kvality organizácie poskytujúcej softvérové služby.

Rozsah softvérových služieb poskytovaných softvérovou organizáciou užívateľovi softvéru má byť zmluvne stanovený.

10.2 Softvér vyvinutý pri použití zodpovedajúceho plánu kvality

Od organizácií vyvíjajúcich alebo poskytujúcich softvér má užívateľ požadovať, aby mali pre softvér zavedený plán kvality vrátane postupov, ktoré odrážajú požiadavky tohto dokumentu.

Softvérová organizácia má mať všetku dokumentáciu, ktorá je súčasťou softvéru spôsobilého na používanie (kapitola 7).

Testy pre inštaláciu a integráciu vykonané užívateľom softvéru, v rámci jeho verifikácie a validácie, majú zahrňovať i kontrolný výpočet vykonaný pre predpokladanú oblasť použitia softvéru užívateľom. Kontrolný výpočet má byť zdokumentovaný a jeho výsledky vyhodnotené. Výsledky kontrolného výpočtu slúžia okrem iného i na preukazovanie toho, že užívateľ si osvojil nadobudnutý softvér a vie s ním pracovať kvalifikovane.

Užívateľ softvéru má mať užívateľskú dokumentáciu (sekcia 7.5).

10.3 Softvér vyvinutý bez použitia zodpovedajúceho plánu kvality

Softvér, ktorý bol vyvinutý bez uplatnenia zodpovedajúceho plánu kvality má byť pred použitím podrobený konfiguračnej kontrole, ako je ďalej požadované. Užívateľ pred vykonaním konfiguračnej kontroly vyhodnotí a zdokumentuje softvér za účelom:

a) stanovenia jeho spôsobilosti pre používanie a údržbu,

b) stanovenia činností, ktoré majú byť vykonané, aby softvér mohol byť podrobený konfiguračnej kontrole; uvedené má byť zdokumentované a má prinajmenšom obsahovať:

- požiadavky užívateľa kladené na softvér,
- program testovania a testovacie príklady pre validáciu softvéru a jeho odsúhlasenie pre používanie,
- užívateľskú dokumentáciu požadovanú podľa sekcie 7.5 tohto návodu.

Keď sú uvedené činnosti urobené, preverené a odsúhlasené, potom je softvér podrobený konfiguračnej kontrole.

11 Záznamy

Požadovaná dokumentácia má byť uchovávaná spolu so záznamami ako je požadované príslušnými štandardami, dokumentmi a postupmi systému manažérstva kvality.

12 Kľúčové požiadavky úradu kladené na softvér

V tejto časti sú zhrnuté odporúčania, ktoré úrad kladie na zabezpečovanie kvality softvéru pre analýzy bezpečnosti, a ktoré sú diskutované v bezpečnostnom návode:

a) pre používanie a údržbu softvéru má u jeho užívateľa existovať plán kvality, ktorý je súčasťou jeho systému manažérstva kvality,

b) na používanie nadobudnutého softvéru je potrebný súhlas poskytujúcej organizácie,

c) so softvérom môže pracovať len kvalifikovaná osoba, ktorej kvalifikácia je preukázaná,

d) užívateľ softvéru má mať užívateľskú dokumentáciu, ktorá je súčasťou softvéru spôsobilého na používanie,

e) používaný softvér má byť verifikovaný a validovaný pre oblasť jeho použitia.

13 Zoznam literatúry

/1/ U. S. NUCLEAR REGULATORY COMMISSION, Software Quality Assurance Program and Guidelines. Washington DC: U. S. NRC, 1993. NUREG/BR-0167. [zobrazené 15. marca 2019]. Dostupné na internete: https://www.nrc.gov/docs/ML0127/ML012750471.pdf.

/2/ INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, *IAEA Safety Standards Series* No. GSR Part 4 (Rev.1). Vienna: IAEA, 2016, 26-27. [zobrazené 15. marca 2019]. ISBN 978-92-0-109115-4. ISSN 1020-525X. Dostupné na internete: https://www.iaea.org/publications/10884/safety-assessment-for-facilities-and-activities

---

Oznámenie

K odkazu /2/ zo Zoznamu literatúry: