ENERGETIKA. 2006. Nr. 4. P. 45–49

Branduolinių reaktorių saugos sistemų programinės įrangos patikimumas: vertinimo metodai ir problemos

Vytis Kopustinskas[1, 2],

Kazimieras Padvelskis[2],

Juozas Augutis[1]

[1] *Lietuvos energetikos institutas, Branduolinių įrenginių saugos laboratorija, Breslaujos g. 3, LT-44403, Kaunas, el. paštas: vytis@mail.lei.lt*

[2] *Vytauto Didžiojo universitetas, Matematikos ir statistikos katedra, Vileikos g. 8, LT-44404 Kaunas, el. paštas: imvyko@vdu.lt*

Straipsnyje pateikiama branduolinių elektrinių kompiuterizuotų saugos sistemų programinės įrangos patikimumo metodų apžvalga. Programinės įrangos patikimumo klausimas tampa aktualus ir kitose automatizuotose sistemose, nes programinė įranga – svarbus visos sistemos darbą užtikrinantis elementas. Šiuo metu nėra pripažintų programinės įrangos patikimumo vertinimo metodų, todėl straipsnyje pateikiamos kelios žymiausių Europos mokslinių institutų taikomos metodologijos. Ypač prieštaringai apibūdinamas tikimybinis programinės įrangos patikimumo vertinimas, tačiau jis būtinas atliekant branduolinių reaktorių tikimybinę saugos analizę. Straipsnyje pateikiamas Bajeso tinklo metodas vertinant programinės įrangos gedimo tikimybę.

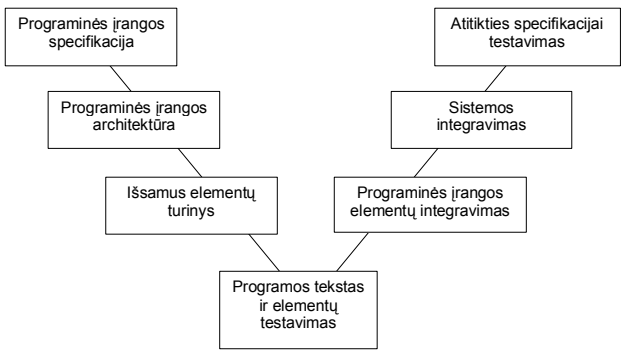
Raktažodžiai: programinės įrangos patikimumas, branduolinių elektrinių saugos sistemų programinė įranga, Bajeso tinklas, tikimybinė saugos analizė

1. ĮVADAS

Šiuo metu naujai statomų branduolinių reaktorių stabdymo ir kontrolės sistemos yra kompiuterizuotos ir jų darbą kontroliuoja programinė įranga. Skaitmeninės sistemos keičia analogines ir atnaujinamuose senesnės statybos branduoliniuose reaktoriuose. Pavyzdžiui, neseniai visiškai nauja kompiuterizuota reaktoriaus stabdymo ir kontrolės sistema įdiegta Vengrijos Paks atominėje elektrinėje, kurią pagamino Framatome ANP. Pažymėtina, kad programinė įranga pradedama naudoti ir visose kitose bent kiek sudėtingesnėse techninėse sistemose ir procesuose. Kompiuteris kontroliuoja ir beveik visų šiuolaikinių automobilių variklių darbą. Todėl programinė įranga pagrįstai tampa dar vienu elementu, kurio gedimas gali sutrikdyti sistemos darbą. Iki šiol atliekamose branduolinių reaktorių tikimybinio saugos įvertinimo studijose programinės įrangos klaidos nebuvo vertinamos. Tačiau visiškai pagrįstas yra klausimas: „Kokia saugos sistemos programinės įrangos klaidos tikimybė?“. Deja, į šį klausimą nėra paprasto atsakymo, nors akivaizdu, kad tokios klaidos egzistuoja ir yra aptinkamos praktikoje. Šiame straipsnyje apžvelgsime pagrindinius saugos sistemų programinės įrangos patikimumo analizės metodus.

2. PROGRAMINĖS ĮRANGOS SUKŪRIMO PAGRINDINIAI ETAPAI IR STANDARTAI

Programinės įrangos sukūrimo proceso pradžia yra jos specifikacijos nustatymas, o pabaiga – atitikimo šiai specifikacijai testavimas. Visas programinės įrangos sukūrimo procesas yra suskirstytas į keletą aiškiai apibrėžtų etapų, dažnai vadinamų V formos sukūrimo ciklu (1 pav.).



1 pav. Apibendrintas programinės įrangos sukūrimo V formos ciklas

Praktikoje taikoma daug V formos ciklo versijų, įvedant naujus etapus ar keičiant etapų ribas. 1 pav. pavaizduotą tipišką programinės įrangos sukūrimo ciklą sudaro šie etapai:

- Programinės įrangos specifikacija. Šiame etape nurodomi reikalavimai, kuriuos turi atitikti programinė įranga, ir užduotys, kurias programa turi atlikti.
- Programinės įrangos architektūra. Šiame etape sukuriama programinės įrangos architektūra, nurodomi tam tikri elementai ir jų tarpusavio ryšys pagal pirmajame etape nurodytą specifikaciją.

• Išsamaus elementų turinio etape nuodugniai nurodoma kiekvieno programinės įrangos elemento struktūra ir reikalavimai.

• Programos tekstas ir elementų testavimas. Šiame etape sukuriamas kiekvieno programos elemento tekstas ir patikrinama, ar jis atitinka išsamaus elementų turinio etape nurodytus reikalavimus.

• Programinės įrangos elementų integravimo etape sujungiami visi programos elementai ir vykdomas visos programos testavimas.

• Sistemos integravimo fazėje sujungiami programinė įranga ir sistemos komponentai (davikliai, kompiuterinė techninė įranga ir kiti) ir pateikiamas galutinis produktas.

• Atitikties specifikacijai testavimo etape panaudojant testus nuodugniai patikrinama, ar sukurta sistema atitinka pirmajame etape nustatytą programinės įrangos specifikaciją.

Ciklo pirmųjų trijų etapų produktas yra programinės įrangos specifikacijų dokumentai. Likusieji keturi etapai apima programinės įrangos testavimą įvairiuose lygiuose pagal atitinkamas testų specifikacijas.

Programinės įrangos specifikacijos sudarymo, realizavimo ir programinės įrangos testavimo procesai yra standartizuoti ir reglamentuojami tiek nacionaliniuose reguliuojančiuose dokumentuose, tiek tarptautiniuose standartuose. Svarbiausias tarptautinis standartas programinės įrangos srityje yra IEC 60880 [1], kurį išleido Tarptautinė elektrotechnikos komisija (angl. *International Electrotechnical Commission*). Tarp nacionalinių dokumentų reikėtų išskirti Prancūzijos saugos sistemų programinės įrangos pagrindinę saugos taisyklę [2] ir Suomijos reglamentą YVL-5.5 [3].

3. PROGRAMINĖS ĮRANGOS PATIKIMUMO VERTINIMO METODŲ IR PRIEMONIŲ APŽVALGA

Europoje yra sukurtos kelios metodologijos, skirtos branduolinių reaktorių valdymo ir kontrolės sistemose naudojamos programinės įrangos saugai ir patikimumui vertinti. Šiame straipsnyje trumpai apžvelgsime IRSN (iki 2003 metų žinomas kaip IPSN) [4], ISTec [5] ir VTT [6] metodologijas. Šios metodologijos buvo pritaikytos 5-osios Europos Bendrosios Programos projekte BE-SECBS vienam KONVOI tipo branduolinio reaktoriaus valdymo ir kontrolės programinės įrangos fragmentui, o gauti rezultatai palyginti [7].

IRSN (Branduolinės saugos institutas, Prancūzija) programinės įrangos vertinimo metodologija išskaidyta į šiuos penkis etapus:

1 etapas: Programinės įrangos kūrimo proceso ir susijusių dokumentų ekspertizė.

Pirmajame etape susipažįstama su programinės įrangos kūrimo procesu ir vertinamas jo atitikimas tarptautiniams ir nacionaliniams standartams [1, 2]. Pagrindiniai vertinimo kriterijai šiame etape yra programinės įrangos specifikacijų korektiškumas, išbaigtumas ir suderinamumas su saugos sistemų projektiniais reikalavimais.

2 etapas: Programos teksto analizė.

IRSN naudoja QAC ir McCabe programas tikrinant programinės įrangos teksto kokybę, ieškant pavojingų, neteisingų arba pernelyg sudėtingų programavimo kalbų konstrukcijų. Taip pat naudojamas Polyspace Verifier, kuris automatiškai atlieka analitinę programos teksto analizę ir nustato galimas programos vykdymo klaidas.

3 etapas: Kritinių programinės įrangos elementų nustatymas.

Šiame etape IRSN taiko gedimų režimų ir pasekmių analizę. Tai yra standartinė analizė, plačiai taikoma ir tikimybinėje saugos analizėje, bei žinoma FMEA trumpiniu (angl. *Failure mode and effect analysis*). Šios analizės metu kiekviena programinės įrangos funkcija yra įvertinama svarbumo indeksu atsižvelgiant į jos galimų sukelti klaidų skaičių ir jų pasekmes. Tuomet tikrinamas programos tekstas, ar svarbiausiose funkcijose negali įvykti klaida. Tikrinimas atliekamas vykdant validacinius testus postuluotoms programinės įrangos klaidoms.

4 etapas: Dinaminė analizė.

Dinaminiam programinės įrangos tikrinimui atlikti IRSN sukūrė programų paketą Claire, kuris gali imituoti programinės įrangos veikimą realiomis sąlygomis. Dinaminės analizės metu atliekamas programinės įrangos veikimo stebėjimas multiprocesorinėje terpėje ir galima kontroliuoti parametrų reikšmes įvairiuose loginiuose kanaluose, kai įvairiai parinktos įvadinių signalų vertės. Dinaminė analizė patikrina pagrindinius programinės įrangos veikimo aspektus realiomis sąlygomis. Naudojant Claire taip pat atliekama robastiškumo analizė, kurios tikslas yra įvertinti programinės įrangos atsaką į ekstremalias avarines situacijas ir netipiškas įvadinių parametrų vertes. Robastiškumo analizės metu ypač atkreipiamas dėmesys į kritinius programinės įrangos elementus, nustatytus trečiajame etape.

5 etapas: Testavimo strategijos sudarymas ir testų parinkimas.

Šiam etapui atlikti IRSN sukūrė programų paketą Gatel, kuris generuoja „abstrakčius“ patikrinimo testus, atsižvelgiant į programinės įrangos specifikaciją ir testo reikalavimus. Sugeneruoti „abstraktūs“ testai, atitinkantys galimas programinės įrangos funkcijas, vėliau įvertinant testuojamo programos kodo ypatumus yra konvertuojami Claire paketu ir įvykdomi.

ISTec (Saugos technologijų institutas, Vokietija) metodologija sukurta mokslinės programos metu 1994–1997 metais. ISTec sukurta programinė įranga RETRANS išskaido automatiškai sugeneruotą programos tekstą į atskirus analizuojamus fragmentus. RETRANS analizė gali patikrinti specifikacijos reikalavimų ir programos teksto funkcinį tapatumą, specifikacijos reikalavimų suderinamumą, programos teksto funkcinį suderinamumą, taip pat dubliuojančių elementų programavimo tapatumą.

Svarbu pažymėti, kad ši metodologija skirta tik automatiškai generuojamam programos tekstui tikrinti. Au-

tomatinio programos teksto generavimo įranga TELEPERM XS sukurta Siemens KWU kompanijoje (šiuo metu Pramatome ANP) ir skirta automatiškai generuoti branduolinių reaktorių stabdymo ir kontrolės sistemų programinės įrangos tekstus.

VTT (Mokslinių tyrimų ir technologijų centras, Espoo, Suomija) metodologija pagrįsta Suomijos branduolinės energetikos reguliuojančios organizacijos STUK reikalavimais [3]. Metodologija skirta įvertinti branduolinių elektrinių kompiuterizuotų sistemų (tarp jų ir programinės įrangos) atitikimą tarptautiniams standartams ir reguliuojantiems dokumentams. Metodologiją sudaro dvi dalys: kokybinė (deterministinė) analizė ir tikimybinis vertinimas.

Kokybinė kompiuterizuotos sistemos analizė apima tokias vertinimo fazes:

– bendras pateiktos dokumentacijos kokybės įvertinimas;

– specifikacijos reikalavimų įvertinimas;

– saugos funkcijų gedimų režimų ir pasekmių analizė;

– testavimų apimties, eksploatacinės patirties ir programos teksto analizė;

– sistemos gamybos proceso įvertinimas.

Kiekvienoje fazėje atliekama atskira analizė ir išvadose pateikiamas apibendrintas saugos ir kokybės lygio vertinimas.

Tikimybinis kompiuterizuotų sistemų patikimumo vertinimas atliekamas remiantis kokybinės analizės rezultatais ir jų pagrindu sudaryto Bajeso tinklo analize [8]. Bajeso tinklo analizę sudaro šios pagrindinės dalys:

– vertinimo požymių nustatymas;

– Bajeso tinklo modelio sudarymas (struktūra, metrika, kintamųjų tarpusavio ryšiai)

– tikimybinis vertinimas ir skaičiavimai;

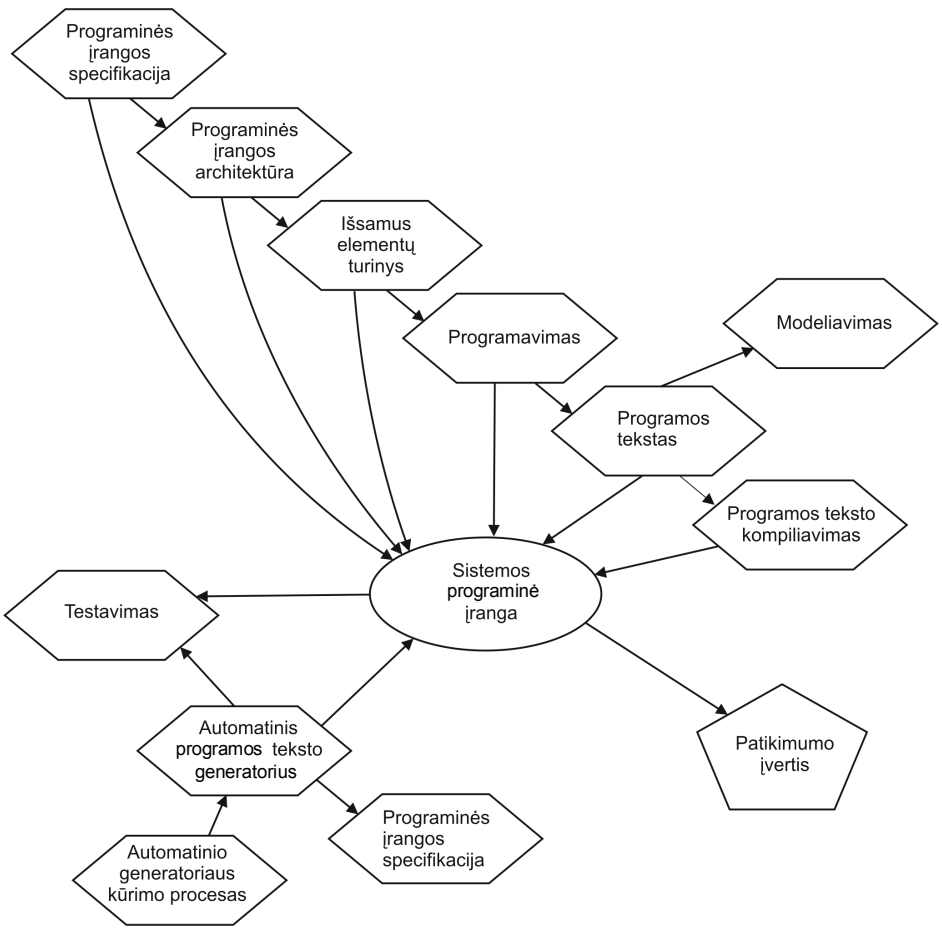
– rezultatų interpretacija ir parametrų jautrumo analizė.

4. PROGRAMINĖS ĮRANGOS PATIKIMUMO TIKIMYBINIS VERTINIMAS

Šiuo metu nėra gerai išvystytų ir visuotinai pripažintų metodų, skirtų įvertinti programinės įrangos klaidingo veikimo tikimybę. Tačiau atliekant branduolinių reaktorių tikimybinės saugos analizės studijas, būtina įvertinti klaidų galimybę kompiuterizuotose reaktoriaus valdymo sistemose. Kita vertus, visiškai pagrįstai galima paklausti – kokia yra programinės įrangos klaidingo veikimo tikimybė?

Literatūroje žinoma nemažai programinės įrangos patikimumo matematinių modelių (Jelinski-Moranda, Shooman, Musa, Goel-Okumoto ir kiti), kurių parametrai gali būti nustatomi pagal eksploatacijos patirtį maksimalaus tikėtinumo metodu [9, 10]. Tačiau branduolinių reaktorių kompiuterizuotų valdymo sistemų atveju šie matematiniai modeliai netinka, nes nėra pakankamai eksploatacinių duomenų, taip pat neaišku, kiek gerai turimi apibendrinti duomenys atitinka konkrečią nagrinėjamą sistemą. Branduolinių reaktorių licencijavimo medžiaga dažniausiai remiasi kokybinių saugos kriterijų inžineriniu vertinimu, tuo pačiu įvairiais aspektais atspindėdama sistemų patikimumą. Ši informacija gali būti panaudojama atliekant tikimybinį vertinimą Bajeso tinklais [8].

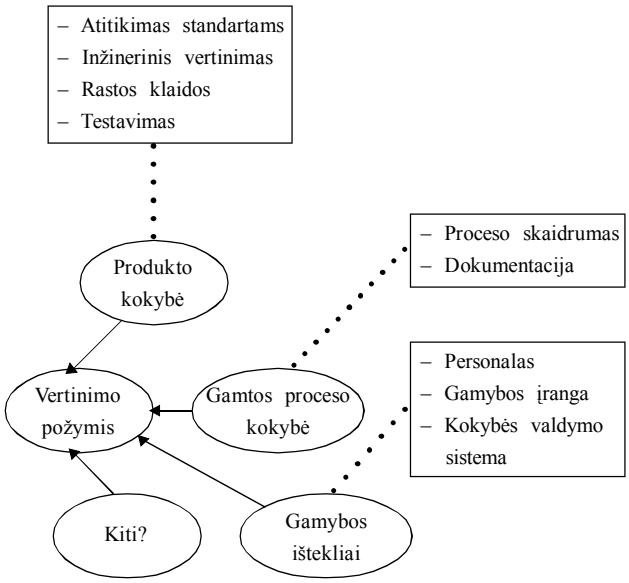
Kaip minėta, Bajeso tinklo sukūrimo procesą sudaro 4 pagrindiniai etapai. Pirmame etape dažniausiai pagal kokybinės saugos analizės rezultatus nustatomi vertinimo požymiai, šių požymių tarpusavio sąryšiai, taip pat sąryšis su sistemos gedimo tikimybe. Vertinimo požymių grafo ir tarpusavio sąryšių pavyzdys parodytas 2 pav. Antrame etape sudaroma Bajeso tinklo struktūra, nustatomi tinklo kintamieji, jų reikšmių skalės ir ryšys



2 pav. Vertinimo požymių grafo pavyzdys (pagal FANP programinės įrangos sukūrimo ciklą [7])

su sistemos klaidos tikimybe (pvz., programinės įrangos testavimo apimties ir klaidos tikimybės ryšys). Trečiame etape dažniausiai ekspertinio vertinimo būdu nustatomos tinklo kintamųjų vertės, tikimybiniai skirstiniai, sąlyginiai svoriai ir atliekami tikimybiniai skaičiavimai bei neapibrėžtumų vertinimas. Ketvirtame etape apibendrinami skaičiavimų rezultatai ir atliekama parametrų jautrumo analizė.

Bajeso tinklo struktūros kintamieji X_i, $i \in [1, N]$ gali būti vertinami nominalioje, ranginėje arba santykių skalėse. Kintamųjų reikšmės kiekybiškai atspindi ekspertinę nuomonę apie požymio kokybę. Požymio kokybės vertinimas atitinkamai susideda iš kelių sudedamųjų dalių vertinimo. Požymio kokybės vertinimo sudedamosios dalys parodytos 3 pav.



3 pav. Vertinimo požymio kokybės sudedamosios dalys

Bajeso tinklo struktūra numato, kad kiekvieno požymio X_i, dažniausiai atitinkančio programinės įrangos kūrimo ciklą, kokybė priklauso nuo ankstesnės ciklo fazės požymio X_{i-1} kokybės ir pačio požymio kokybės C_i. Ši priklausomybė kiekybiškai gali būti įvertinta įvairiais būdais, pavyzdžiui, skaičiuojant svorinį vidurkį:

$$X_i = \omega_0 \cdot C_i + \omega_1 \cdot X_{i-1};$$

čia $\omega_1 + \omega_0 = \omega_1 + \sum_j^{n_j} \omega_0^j = 1$ ir $C_i = \sum_j^{n_j} \omega_0^j \cdot C_i^j$.

Vertinimo požymio kokybė C_i atitinkamai priklauso nuo n_j sudedamųjų dalių C_i^j (3 pav.). Bajeso tinklo parametrų tikimybiniai skirstiniai turi būti įvertinami remiantis patyrusių ekspertų nuomonėmis, gautomis pagal ekspertų apklausoms keliamus reikalavimus [11].

5. IŠVADOS

Šiame apžvalginiame straipsnyje nagrinėjama šiuolaikinėms techninėms sistemoms aktuali programinės įrangos patikimumo problema. Šis klausimas tapo ypač aktualus modernizuojant esamas ar statant naujas branduolines elektrines, kuriose kompiuteriai ne tik apdoroja informaciją, bet ir generuoja valdymo signalus.

Straipsnyje trumpai pateikiamos kelios Europoje taikomos branduolinių elektrinių saugos sistemų programinės įrangos patikimumo vertinimo metodologijos. Šių metodologijų išsamus palyginimas ir taikymas konkrečios saugos sistemos programinės įrangos analizės atveju pateiktas [7]. Atliekant šiuolaikinių branduolinių elektrinių tikimybinę saugos analizę taip pat reikia įvertinti ir saugos sistemų programinės įrangos gedimų tikimybę. Tikimybiniai metodai šioje srityje nėra gerai išplėtoti ir apie tikimybinį programinės įrangos vertinimą dažnai atsiliepiama prieštaringai. Kaip vienas paprasčiausių galimų metodų straipsnyje pateiktas Bajeso tinklų metodas, kuris leidžia sujungti įvairius programinės įrangos darbo ir kūrimo proceso kiekybinius ekspertinius įvertinimus.

Gauta 2006 04 18
Parengta 2006 11 30

Literatūra

1. IEC 60880 – Software for computers in the safety systems of nuclear power stations. Pirmas leidimas, 1986.
2. Basic Safety Rule on software for safety systems-RFS. II.4.1.a – Sūreté Nucléaire en France. Les éditions des Journaux officiels, 2000-06.
3. Intrumentation systems and components at nuclear facilities, YVL-5.5, STUK, 2002.
4. IPSN'S experience with new generation tools for static analysis of safety critical software // International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT 2000), Washington DC, November 2000.
5. Lindner A., Miedl H. Methodology and Tools for Independent Verification and Validation of Computerised I & C Systems Important to Safety // IAEA Specialists Meeting on Computerised Protection and Safety Related Systems in Nuclear Power Plants (IAEA/IWG-NPPCI). Budapest, Hungary, 27–29 October 1997.
6. Haapanen P., Korhonen J., Pulkkinen U. Licensing process for safety-critical software-based systems. STUK-YTO-TR 171. STUK, Helsinki, 2000.
7. Kopustinskas V., Kirchsteiger C. et al. Benchmark exercise of safety evaluation of computer based systems // FISA-2003 konferencijos medžiaga, 2003–11. http://www.cordis.lu/fp5-euratom/src/ev-fisa2003.htm
8. Helminen A., Pulkkinen U. Reliability assessment using Bayesian networks – Case study on quantitative reliability estimation of a software-based motor protection relay // VTT Industrial systems, TAU A 017. Espoo, 2002. 28 p.
9. Friedman M. A., Voas J. M. Software Assessment: Reliability, Safety, Testability. Wiley & Sons, 1996.
10. Bedford T., Cooke R. Probabilistic Risk Analysis: Foundations and Methods. Cambridge University Press, 2001.
11. Cooke R. Experts in Uncertainty. Oxford University Press, 1991.

Vytis Kopustinskas, Kazimieras Padvelskis, Juozas Augutis

RELIABILITY OF NUCLEAR REACTOR SAFETY SYSTEM SOFTWARE: ASSESSMENT METHODS AND PROBLEMS

Summary

The paper presents an overview of programmable safety systems' software reliability analysis methods of nuclear reactors. As software is an important component ensuring a successful operation of the whole system, software reliability becomes an issue of increased importance. The paper presents several software reliability assessment methodologies used by famous European research institutes. At the moment, there are no widely accepted methods of assessing software reliability. Quantitative software reliability assessment is an even more controversial issue, however, it is necessary when performing probabilistic safety assessment. The paper presents the Bayesian network as a tool for estimating software failure probability.

Key words: software reliability, nuclear reactors, programmable safety systems, Bayesian network, probabilistic safety assessment

Витис Копустинскас, Казимерас Падвяльскис, Юозас Аугутис

НАДЕЖНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМ БЕЗОПАСНОСТИ ЯДЕРНЫХ РЕАКТОРОВ: МЕТОДЫ И ПРОБЛЕМЫ

Резюме

В работе рассмотрены методы анализа надежности программного обеспечения систем безопасности ядерных реакторов. Программное обеспечение является важным фактором, влияющим на надежность всей системы, что становится все более актуальным. Представлены некоторые методологии анализа надежности, созданные в ведущих европейских научных институтах. Делается вывод о том, что на данный момент не существует приемлемых методов анализа надежности программного обеспечения. Количественная оценка надежности программного обеспечения является еще более противоречивой, но необходима при вероятностном анализе безопасности. В работе представлен метод сети Байеса для оценки вероятности сбоя программного обеспечения.

Ключевые слова: надежность программного обеспечения, программное обеспечение систем безопасности ядерных реакторов, сеть Байеса, вероятностный анализ безопасности