УДК 629.039.58 **doi: 10.26906/SUNZ.2020.3.090**

О. М. Одарущенко

Науково-виробниче підприємство «Радікс», Кропивницький, Україна

ОЦІНЮВАННЯ ТА ЗАБЕЗПЕЧЕННЯ ФУНКЦІЙНОЇ БЕЗПЕКИ ПРИ РОЗРОБЛЕННІ ТА ЛІЦЕНЗУВАННІ МОДУЛІВ І ПЛАТФОРМ ДЛЯ ПРОГРАМНО-ТЕХНІЧНИХ КОМПЛЕКСІВ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ

Анотація. Виконано аналіз сучасного стану досліджень в галузі надійності та функційної безпеки програмно-технічних комплексів інформаційно-керуючих систем (ПТК ІКС). Встановлено, що не зважаючи на використання нової елементної бази в ході модернізації та розроблення нових ПТК ІКС, застосування сучасних технологій розробки їх апаратної та програмної компонент, підвищення ефективності технологічних процесів, зниження ресурсємності виробництва не призвело до достатнього прогресу у вирішені завдань проектування ПТК з необхідним і гарантованим рівнем надійності і функційної безпеки. Крім того, встановлено, що не зважаючи на інтенсивні дослідження впродовж останніх десятиліть залишається низка нерозв'язаних задач і обмежень існуючих методів і засобів, а саме: моделі, які описують надійнісну і безпекову складові, не ураховують розмірність задач і обмежень існуючих методів; у сучасних методах оцінювання функційної безпеки аспекти безвідмовності апаратних і програмних засобів розглядаються відокремлено, без спільного кількісного аналізу результатів верифікації; методи розроблення й забезпечення відмовостійкості ПТК з використанням програмових платформ недостатньо ураховують можливості, обмеження і похибки вбудованих засобів контролю і діагностування на рівні електронних проектів, модулів і каналів. Представлений в роботі метод частково вирішує перелічені задачі.

Ключові слова: програмно-технічний комплекс, інформаційно-керуюча система, дефект, надійність, функційна безпека, етапи моделі життєвого циклу.

Вступ

В забезпеченні безпеки АЕС, авіаційних і ракетно-космічних комплексів інших критичних об'єктів важливу роль відіграють інформаційні-керуючі системи (ІКС), ядром яких є програмно-технічні комплекси (ПТК). Вартість відмов апаратних, програмних, програмовних засобів ПТК ІКС, є надзвичайно високою.

Найважливішою характеристикою ІКС є функційна безпека, яка відповідно до міжнародних і національних стандартів [1, 2] визначає здатність систем мінімізувати ризики переходу в аварійний (небезпечний) стан та/або його наслідки. Для України актуальність нормування, моніторингу, оцінювання та забезпечення функційної безпеки підтверджується наявністю великої кількості аварійно небезпечних об'єктів, перш за все, реакторів АЕС.

Це зумовлює необхідність: по-перше, гарантованого виконання вимог до стійкості до відмов програмних, програмовних, апаратних засобів, збурень різної природи та змін характеристик фізичного та інформаційного середовища; по-друге, забезпечення якості розроблення і точності відтворення реальних потреб використання ПТК ІКС за призначенням; потретє, мінімізації часових, енергетичних та інших ресурсів, які використовуються.

Сьогоденні процеси модернізації існуючих та розробки перспективних ПТК ґрунтуються на використанні нової елементної бази, сучасних технологіях розробки їх апаратної та програмної компонент. Це, з одного боку, розширює можливості ІКС, призводить до підвищення ефективності технологічних процесів, знижує ресурсємність виробництва, а з іншого боку – призводить, до зростання ризиків, які супроводжують процес підвищення залежності функціональності, надійності і безпеки від якості проектних рішень. Тобто збільшення можливостей сучасної елементної бази, впровадження індустріальних технологій розробки програмного забезпечення не привело до такого ж прогресу у проектуванні ПТК з необхідним і гарантованим рівнем надійності і функційної безпеки.

Слід зазначити, що такий стан речей склався, не зважаючи на інтенсивні дослідження впродовж останніх десятиліть, які виконувалися в Україні та за її межами рядом науковців, зокрема, T. Anderson, A. Avizienis, J.-C. Laprie, P. Popov, B. Randell, A. Romanovsky, S. Russo, F. Saglietti, K. Trivedi, J. Vain, Б.Ю. Волочиєм, О.В. Дроздом, Д.А. Маевським, В.М. Опанасенко, О.М. Романкевичем, В.І. Хахановим, М.А. Ястребенецким та інш.

На сьогодні залишається низка нерозв'язаних задач і обмежень існуючих методів і засобів, а саме:

- моделі, які описують надійнісну і безпекову (як інформаційну так і функційну) складові, не ураховують реальну розмірність задач оцінювання з огляду на складність індустріальних ІКС і ПТК, змінність параметрів відмов і відновлень;
- у методах оцінювання функційної безпеки, насамперед, аспекти безвідмовності апаратних і програмних засобів розглядаються відокремлено, без спільного кількісного аналізу результатів верифікації;
- методи розроблення й забезпечення відмовостійкості ПТК з використанням програмових платформ недостатньо ураховують можливості, обмеження і похибки вбудованих засобів контролю і діагностування на рівні електронних проектів, модулів і каналів тощо.

Таким чином, можливо зробити висновок що на сьогодні існує невідповідність між розширенням

множини причин порушення працездатності ПТК ІКС внаслідок фізичних і проектних дефектів їх компонентів, зміною параметрів потоків відмов, відновлень і оновлень, апаратних, програмних і інформаційних ресурсів і рівнем розвитку сучасних методів і засобів оцінювання та забезпечення надійності та функційної безпеки ПТК.

Подолати цю невідповідність можливо шляхом вирішення проблеми комплексного оцінювання і забезпечення надійності і функційної безпеки ПТК для ІКС критичного застосування з урахуванням відмов, обумовлених проектними, фізичними дефектами і вразливостями програмних і апаратних засобів (включаючи відмови з загальної причини), а також зміни параметрів потоків їх відмов і відновлень.

Мета статті – представлення основних етапів методу оцінювання та забезпечення функційної безпеки при розробленні та ліцензуванні модулів і платформ для програмно-технічних комплексів інформаційно-керуючих систем.

Основна частина

У відповідності до вимог стандартів [1, 3] узагальнена V - модель життєвого циклу (ЖЦ) розроблення та тестування ПТК ІКС має вигляд (рис. 1).

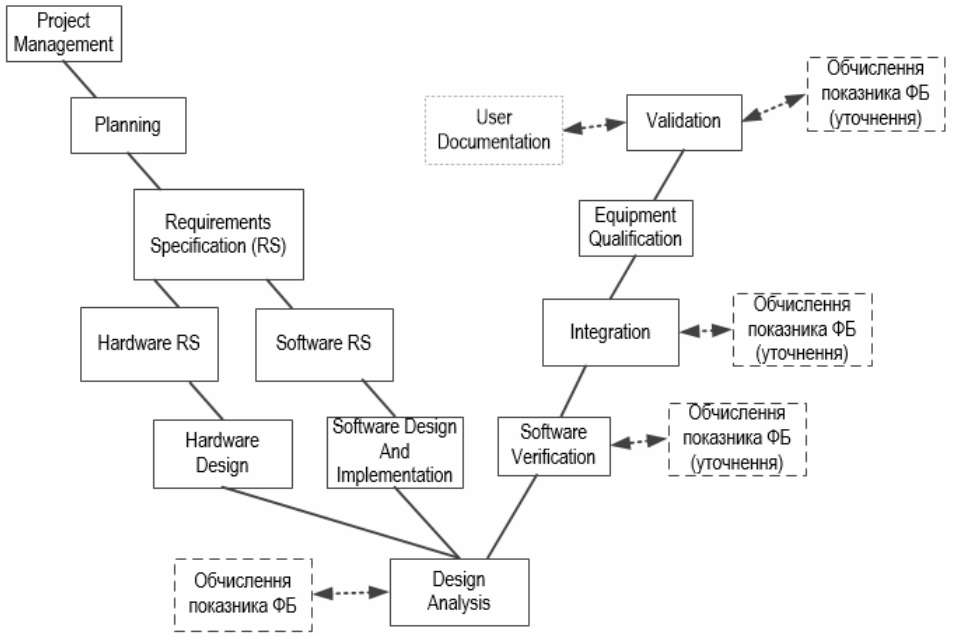

Рис.1. V – модель життєвого циклу розроблення та тестування ПТК ІКС

До основних етапів розроблення ПТК ІКС життєвого циклу відносяться:

- Project Management (етап взаємодії замовника і виробника, на якому документально встановлюються юридичні відносини між майбутніми учасниками проекту: вивчення тендерних замовлень, специфікації на продукт замовника, розроблення основних проектних планів менеджменту тощо);
- Planning (етап розроблення проектних планів);
- Requiremens Specification (RS) (етап розроблення специфікації вимог на систему в цілому);
- Hardware RS та Software RS (етапи розроблення специфікацій вимог до HW та SW);
- Hardware Design та Software Design and Implementation (етапи детального дизайну та реалізації HW та SW компонент системи);
- Design Analysis (етап аналізу прийнятих проектних рішень). Етап характеризується можливістю первинного оцінювання показників функційної безпеки;
- Software Verification (етап тестування SW компонент системи). Етап характеризується можливістю уточнення показника ФБ на підставі обробки статистичних даних про відмови SW;
- Integration (етап інтеграційного тестування системи). Етап характеризується можливістю уточнення показника ФБ з урахуванням оброблених статистичних даних відмов SW та HW;
- Equipment Qualification (етап кваліфікаційних випробувань системи – на сейсмічну стійкість, електромагнітну сумісність тощо);
- Validation (етап перевірки виконання системних вимог ПТК ІКС). Етап характеризується фінальним оцінюванням показника ФБ.

Оцінювання показників ФБ на відповідних етапах ЖЦ здійснюється із застосуванням методу оцінювання та забезпечення функційної безпеки при розробленні та ліцензуванні модулів і платформ для ІКС на програмовних логічних інтегральних схемах (рис. 2).

Етап 1 – застосування послідовності оцінювання надійності ПЗ шляхом комплексування моделей оцінювання надійності програмного забезпечення (МНПЗ) та урахування їх вторинних дефектів [4÷15].

Початкові дані етапу наступні:
специфікація системних вимог,
специфікація вимог до ПЗ,
детальний дизайн та реалізація ПЗ,

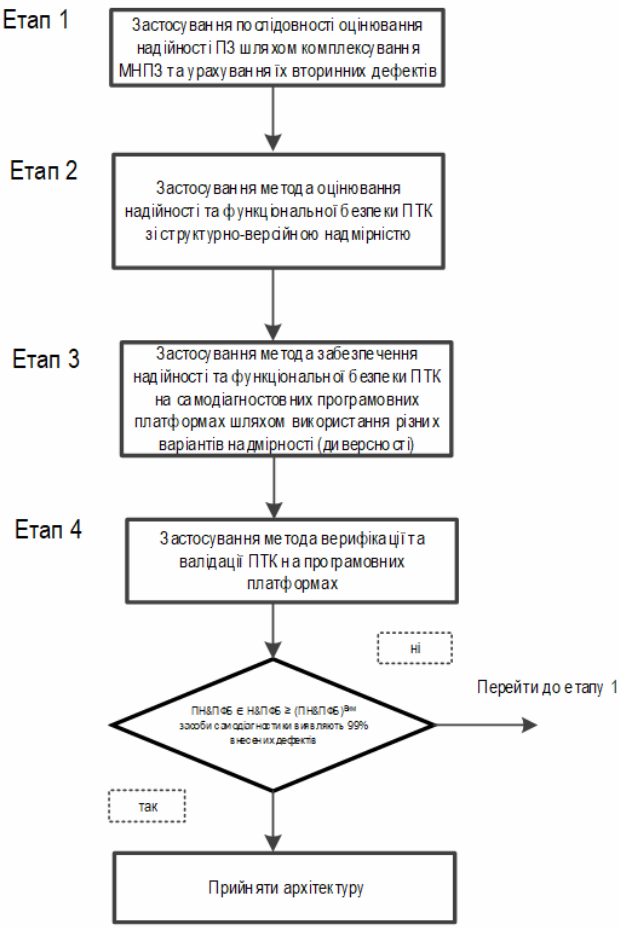

Рис. 2. Основні етапи методу оцінювання та забезпечення функційної безпеки

статистичні дані про дефекти проектування програмних засобів (ДП ПЗ),

одержані в результаті такого аналізу лінія регресії, рівняння лінії регресії та коефіцієнт кореляції.

Результатами виконання етапу є значення функції ризику $\lambda_{дп}$ (t) та величини її зміни $\Delta\lambda_{дп}$ (t) на основі обраних та модифікованих МНПЗ.

Етап 2 – застосування метода оцінювання надійності та функційної безпеки ПТК зі структурно-версійною надмірністю [12].

Початкові дані етапу такі:

- специфікація системних вимог (опис системних функцій,

опис сценаріїв функціонування,

функціональні вимоги,

вимоги до інтерфейсів,

вимоги до продуктивності,

вимоги до оточуючого середовища,

вимоги до інформаційної безпеки,

вимоги до надійності та функційної безпеки),

специфікація вимог до Software,

специфікація вимог до Hardware,

архітектурні вимоги до ПТК,

детальний дизайн SW та HW.

Результатами виконання етапу є обчислені прогнозні значення показників надійності та функційної безпеки ПТК за обраною архітектурою.

Етап 3 – застосування метода забезпечення надійності та функційної безпеки ПТК на самодіагностовних програмових платформах шляхом використання варіантів надмірності (диверсності) [8].

Початкові дані етапу такі:

- специфікація системних вимог (опис системних функцій, опис сценаріїв функціонування, функціональні вимоги, вимоги до інтерфейсів, вимоги до продуктивності, вимоги до оточуючого середовища, вимоги до інформаційної безпеки, вимоги до надійності);

- специфікація вимог до Software;

- специфікація вимог до Hardware, архітектурні вимоги до ПТК;

- детальний дизайн SW та HW; результати Етапу 2;

- результати тестування.

Результатами виконання етапу є обчислені прогнозні значення показників функційної безпеки ПТК з урахуванням особливостей застосування самодіагностовних програмових платформ для їх побудови.

Етап 4 – застосування метода верифікації та валідації ПТК на самодіагностовних програмових платформах [9].

Початковими даними для виконання етапу є результати виконання попередніх етапів.

Результатами виконання етапу є виконання завдань з SW та HW Fault Insertion Testing, які полягають у виконанні тестів з внесенням дефектів в апаратні та програмні компоненти системи. Проведення даного виду тестування дає можливість перевірити якість проектних рішень щодо побудови підсистем вбудованої програмної та апаратної діагностики.

Далі виконується перевірка значень обчислених показників надійності та функційної безпеки на відповідність заданим в специфікації системних вимог.

За умовою позитивної відповіді оцінювання показників надійності та функційної безпеки вважається завершеним, а обрана архітектура ПТК приймається для подальшої розробки.

У протилежному випадку здійснюється перехід до етапу 1.

Висновки

Одержано комплексний метод оцінювання та забезпечення функційної безпеки при розробленні та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмових логічних інтегральних схемах. Метод послідовно об’єднує:

- послідовність оцінювання надійності ПЗ шляхом комплексування МНПЗ та урахування їх вторинних дефектів;

- метод оцінювання надійності та функційної безпеки програмно-технічних комплексів зі структурно-версійною надмірністю;

- метод забезпечення надійності та функційної безпеки ПТК на самодіагностовних програмових платформах шляхом використання різних варіантів надмірності (диверсності);

- метода верифікації та валідації ПТК на самодіагностовних програмовних платформах.

Метод застосовується в ході реалізації V-моделі життєвого циклу розроблення, тестування і ліцензування модулів і платформ ПТК ІКС і дозволяє оперативно вносити корегуючі дії щодо проектних рішень їх апаратних та програмних компонент.

СПИСОК ЛІТЕРАТУРИ

1. IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems [Text]. Published. 2010-04. – IEC Standards, 2010. – 594 p.2 International standard ISO/IEC FDIS 25010. System and software quality models. – 2010, 34 p.
2. IEC 61513. Nuclear power plants – instrumentation and control for systems important for safety – general requirements for systems [Text]. Published. 2011-08-25. – IEC Standards, 2011. – II, 86 p.
3. Michel D. Medoff, Rainer I. Faller. Functional Safety – An IEC 61508 SIL 3 Compatible Development process [Text] / exida.com.L.L.C., 2010.- 282 p.
4. Полонников Р.И. Методы оценки показателей надежности программного обеспечения / Р.И. Полонников, А.В. Никандров. – СПб.: Политехника – 1992. – 78 с.
5. Одарущенко О. Н. Учет вторичных дефектов в моделях надежности программных средств / О. Н. Одарущенко, А.А. Руденко, В.С. Харченко // Математичні машини і системи. – Київ: ІПММС НАН України, 2010. – № 1. – С. 205-217.
6. Руденко А. А. Информационная технология оценки надежности программных средств с учетом вторичных дефектов / А. А. Руденко, Е. Б. Одарущенко, О. Н.Одарущенко // Системи управління, навігації та зв'язку. – Полтава: ПолтНТУ, 2015. – Випуск 1 (33). – С. 146-150.
7. Харченко В.С. Анализ сценариев и определение параметров для оценки надежности программных средств с учетом вторичных дефектов / В.С.Харченко, О. Н. Одарущенко, А. А. Руденко, Е. Б. Одарущенко // Системи управління, навігації та зв'язку. – Київ: Державне підприємство „Центральний науково-дослідний інститут навігації і управління", 2011. – Випуск 2 (18). – С.273-280.
8. Скляр, В. В. Модели отказов информационно-управляющих систем на основе самодиагностируемых программируемых платформ в системах аварийной защиты реакторов [Текст]/ В. В. Скляр, О.Н. Одарущенко, Ю.Л. Поночовный, Е.Н. Бульба, А.О. Ивасюк// Радіоелектронні і комп'ютерні системи. – 2015. – № 4(74). – С. 19-24.
9. Odarushchenko, O., Strjuk, O., Leontiiev, K., Ivasyuk, A., Kharchenko, V Fault-Insertion Testing: SW & HW FIT-Ability, Procedure and Tools for Safety PLC-Based System SIL Certification. Proceeding of The 9th IEEE International Conference on Dependable Systems, Services and Technologies,DESSERT'2018 24-27 May, 2018, Kyiv, Ukraine.
10. Зиков І. С., Кучук Н. Г., Шматков С. І. Синтез архітектури комп'ютерної системи управління транзакціями e-learning. *Сучасні інформаційні системи*. 2018. Т. 2, № 3. С. 60–66. DOI: https://doi.org/10.20998/2522-9052.2018.3.10
11. Nechausov A., Mamusuĉ I., Kuchuk N. Synthesis of the air pollution level control system on the basis of hyperconvergent infrastructures. *Сучасні інформаційні системи*. 2017. Т. 1, № 2. С. 21-26. DOI: https://doi.org/10.20998/2522-9052.2017.2.04
12. Кучук Н.Г., Гавриленко С.Ю., Лукова-Чуйко Н.В., Собчук В.В. Перерозподіл інформаційних потоків у гіперконвергентній системі / С.Ю. Гавриленко. *Сучасні інформаційні системи*. 2019. Т. 3, № 2. С. 116-121. DOI: https://doi.org/10.20998/2522-9052.2019.2.20
13. Ястребенецкий, М.А. Безопасность атомных станций: системы управления и защиты ядерных реакторов: [Текст] : монография/ М. А. Ястребенецкий, Ю. В. Розен, С. В. Виноградская, Г. Джонсон, В. В. Елисеев, А. А. Сиора, В. В. Скляр, Л. И. Спектор, В. С. Харченко; под ред. М. А. Ястребенецкого. – К.: Основа-Принт, 2011. – 768 с. 11.
14. Ястребенецкий, М.А. Безопасность атомных станций: Информационные и управляющие системы [Текст] : монография / М. А. Ястребенецкий, В. Н. Васильченко, С. В. Виноградская, В. М. Гольдрин, Ю. В. Розен, Л. И. Спектор, В. С. Харченко; под ред. М. А. Ястребенецкого. – К. : Техніка, 2004. – 472 с.
15. Технологии высокой готовности для программно-технических комплексов [Текст]: монография/ В.С. Харченко [и др.], под ред. В.С. Харченко, Б.М. Конорева; Гос. центр. регулирования качества поставок и услуг, Нац. Аэрокосм.ун-т им. Н.Е. Жуковского «ХАИ».-Х.: ХАИ, 2010.-372с. ISBN 978-966-662-198-9.

Received (Надійшла) 25.05.2020
Accepted for publication (Прийнята до друку) 29.07.2020

Assessment and safety functions providing during development and licensing of modules and platforms for safety based instrumentation and control systems

O. Odarushchenko

Abstract. An analysis of the current state of research in the field of reliability and functional safety has been performed. It has been established that despite the use of a new element base during the modernization and development of new software and hardware systems for Instrumentation and Control systems (I&C), the use of modern technologies for the development of their hardware and software components, increasing the efficiency of technological processes, and reducing the resource consumption of production did not lead to sufficient progress in solving the problems of designing a hardware and software complex with the necessary and guaranteed level of reliability and functional safety. In addition, it has been established that, despite intensive research over the past decades, a number of unresolved problems and limitations of existing methods and tools remain, namely: in the methods of functional safety assessment, first of all, aspects of hardware and software reliability are considered separately, without a joint quantitative analysis of the verification results; methods of development and maintenance of fault tolerance of I&C with use of software platforms insufficiently consider possibilities, limitations and errors of the built-in means of control and diagnostics at the level of electronic projects, modules and channels. The method presented in the work partially solves these problems.

Keywords: Instrumentation and Control system, defect, reliability, functional safety, stages of the life cycle model