ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

УДК 004.312.466.056 **doi: 10.32620/aktt.2024.1.07**

О. О. ІВАСЮК, В. С. ХАРЧЕНКО

Національний аерокосмічний університет імені М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

ВИКОРИСТАННЯ МЕТОДУ ВЕРИФІКАЦІЇ FMEDA/FIT ДЛЯ ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ ПРОГРАМОВАНОГО ЛОГІЧНОГО КОНТРОЛЕРА: НОВА ІНТЕРПРЕТАЦІЯ ПРИНЦИПУ SIS

Об'єктом дослідження *роботи є програмований логічний контролер (safety PLC), що входить до складу інформаційно-керуючої системи призначеною для здійснення безпечного управління важливими технологічними процесами.* ***Предметом дослідження*** *є обґрунтування правомірності повторного використання результатів, які були отримані під час розробки safety PLC згідно вимог функційної безпечності, для оцінки рівня його кібербезпеки.* ***Метою*** *роботи є дослідження можливості «перехресного» оцінювання безпечних характеристик safety PLC, а саме можливість оцінити рівень кібербезпеки програмованого логічного контролеру на основі відомих даних щодо його рівня функційної безпечності, задля оптимізації використання наявних ресурсів у проєкті.* ***Завдання****: надати теоретичне підґрунтя взаємозв'язку між такими характеристиками safety PLC як функційна безпечність та кібербезпека. Визначити показники якості за якими можна буде оцінити ступень повторного використання вже існуючих результатів. Виконати аналіз потенційних кібератак в залежності від архітектури побудови інформаційно-керуючої системи, яка виконує функції безпечності, а також, від можливих режимів її використання. Визначити та оцінити ступень «перехресного» впливу критичних характеристик об'єкту дослідження. Здійснити розрахунковий аналіз потенційного фінансового та часового виграшу від повторного використання вже відомих результатів для safety PLC мінімальної конфігурації.* ***Висновки****. У дослідженні продемонстрована актуальність питання оцінки кібербезпеки програмованого логічного контролеру на основі використання вже існуючих даних, щодо його рівня функційної безпечності. Запропонований підхід надає можливості значної оптимізації використання ресурсів в проєкті сертифікації safety PLC. Але основним є методологічний висновок, що широко відомий принцип Security Informed Safety (SIS) може бути сформульований і використаний на практиці в оберненому варіанті як Security supported/assessed by Safety (SAS). Тобто до принципу «оцінювання функційної безпечності з врахуванням/на підставі інформаційної (кібер)безпеки» додається принцип «оцінювання інформаційної (кібер)безпеки за підтримки/з урахуванням результатів оцінювання функційної безпечності».*

Ключові слова: *safety PLC; функційна безпечність; кібербезпека; вразливість; відмова; SIS; SAS.*

Вступ

Згідно звіту World Nuclear Organization [1] у США робота багатьох атомних станцій буде продовжена або вже була продовжена на наступні 20 років, що, в цілому, буде складати 80 років безперервної експлуатації об'єктів критичної інфраструктури. Як наслідок, обладнання АЕС, яке входить до складу інформаційно-керуючих систем (instrumental and control system, ІКС) має бути оновлено (reverse engineering) або модернізовано для забезпечення подальшої безпечної експлуатації. Така ситуація не є виключенням, а релевантна у тому чи іншому ступені до атомного ринку будь-якої країни.

Вимоги, якім мають задовольняти ІКС, постійно змінюються у бік «суворості». Так, сучасні ІКС, окрім вимог до надійності, мають додатково відповідати як вимогам з функційної безпечності, так і вимогам з кібербезпеки.

«Нові» і вже існуючі вимоги мають бути упорядковані і узгоджені між собою. Це, як правило, досягається через розробку та імплементацію нових регуляторних документів. Але цей процес є складним і тривалим, до того ж, країни світу не використовують один загальний для усіх набір документів.

Відповідно, технічні засоби, які призначені для виконання функцій безпеки на критичному об'єкті, мають відповідати широкому спектру вимог і потребують не тільки значних фінансових але і часових інвестицій. Особливе місце обіймають індустріальні галузі, події в яких пов'язані із ризиком завдання шкоди великої кількості людей. Наприклад авіаційна галузь і нещодавні катастрофи літака

Boeing 737 max або космічна галузь. В залежності від типу обладнання мова може йти про мільйоні доларів та декілька років розробки.

До того ж, нове технічне рішення має бути затверджено відповідним державним органом контролю та регулювання і цей процес не тільки потребує значних ресурсів, але має шанс отримати рекомендації на подальше опрацювання і повторне розглядання. Тому, недивно, коли компанії-власники атомних станцій віддають перевагу використанню підходу reverse engineering або, навіть, поповненню запасних частин, оскільки для цього обладнання немає необхідності оновлення дозволу на подальше використання.

З огляду на вище зазначене можна зробити висновок, що науково-технічна задача з обґрунтування можливості використання вже існуючих результатів, які свідчать про ті чи інші без пекові властивості технічних засобів із складу ІКС, для обґрунтування інших їхніх властивостей є актуальною.

Об’єкт та предмет дослідження

У статті досліджуються програмовні логічні контролери (programmable logic controller, PLC), які використовуються для побудови систем важливих для безпеки (ІКСВБ), до складу яких входять, як системи безпеки (ІКСБ), так і системи, пов’язані із безпекою (ІКСПБ) [2, 3].

Вимоги до таких ІКС транслюються до їхніх складових частин, а саме до PLC з урахуванням того, що контролер є «мозком» ІКС і визначає як система буде реагувати або при надходженні запиту на виконання функції безпеки, або при виникненні критичної чи не критичної відмові, або у випадку кібератаки.

Оскільки, вимоги до ІКСВБ в основному базуються на вимогах функційної безпечності та надійності відповідно до обраного інтегрального рівня безпечності (safety integrity level, SIL), який визначений у [4] або у його «дочірніх» галузевих стандартах, наприклад таких як [5, 6], то, в першу чергу, цим вимогам має відповідати PLC. Тому, далі у роботі, PLC, який використовується для побудови ІКСВБ, буде називатись safety PLC.

safety PLC може бути побудований на різних технологіях: мікроконтролер, мікропроцесор, різні типи FPGA або взагалі на «hardware» логікі. У свою чергу, FPGA можуть бути використані з готовим програмним забезпеченням від постачальника мікросхем так і без нього. Це знаходить своє відображення у реалізації зовнішніх інтерфейсів PLC, які можуть будуватись або на власних протоколах розробника PLC, або на загальних (індустріальних) протоколах, або мати у своєму складі ці та інші протоколи. Наведена вище інформація яскраво свідчить про велику ступінь варіативності реалізації safety PLC, але у той же час, дослідження не можуть бути проведені для абстрактного об’єкту.

Тому, для подальших розмірковувань вкрай важливо визначитись з особливостями safety PLC, який буде досліджуватись у роботі.

Об’єктом дослідження обраний safety PLC, який використовує FPGA технологію без будь-якого програмного забезпечення третьої сторони. Обраний safety PLC має наступні особливості:

- відсутність двоспрямованих онлайн-інтерфейсів передачі даних;
- побудова з’єднання тільки за правилом точка – точка;
- відсутніть інтерфейсів для підключення сторонніх носіїв інформації;
- забезпечення рівня SIL-3 у одному каналі без використання резервування;
- використання протоколів передачі даних власної розробки.

Предметом дослідження є обґрунтування правомірності повторного використання результатів, які були отримані під час розробки safety PLC згідно вимог функційної безпечності, для оцінки рівня його кібербезпеки.

Додатково, необхідно зазначити, що при використанні терміну «програмне забезпечення (software, SW)» у контексті safety PLC, відповідно до [7] мається на увазі або прошивка (firmware), або логіка застосунку користувача (user application logic, UAL), яку він розробляє за допомогою інструментів, які не призначені для загального використання. На рисунку 1 наведено схематичне зображення розподілення HW і SW частин у safety PLC на основі даних, наведених у [7].

Для отримання цілісної картини досліджування окрім об’єкту та предмету дослідження також необхідно визначити умови практичного застосування safety PLC. Отже, практичним кейсом є випадок, коли вже існує і використовується на практиці safety PLC з рівнем функціональної безпеки SIL-3. Тобто, safety PLC неможливо змінити. Його концепт функційної безпечності є сталим і оцінений незалежними експертами. Таким чином, неможливо спиратись на концепцію врахування ризиків кібербезпеки на етапі його розробки, як наприклад було запропоновано у [8].

Також, слід зазначити, що HW і SW складові safety PLC утворюють його інформаційну складову, яка визначає порядок отримання, оброблення та видачі інформації.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

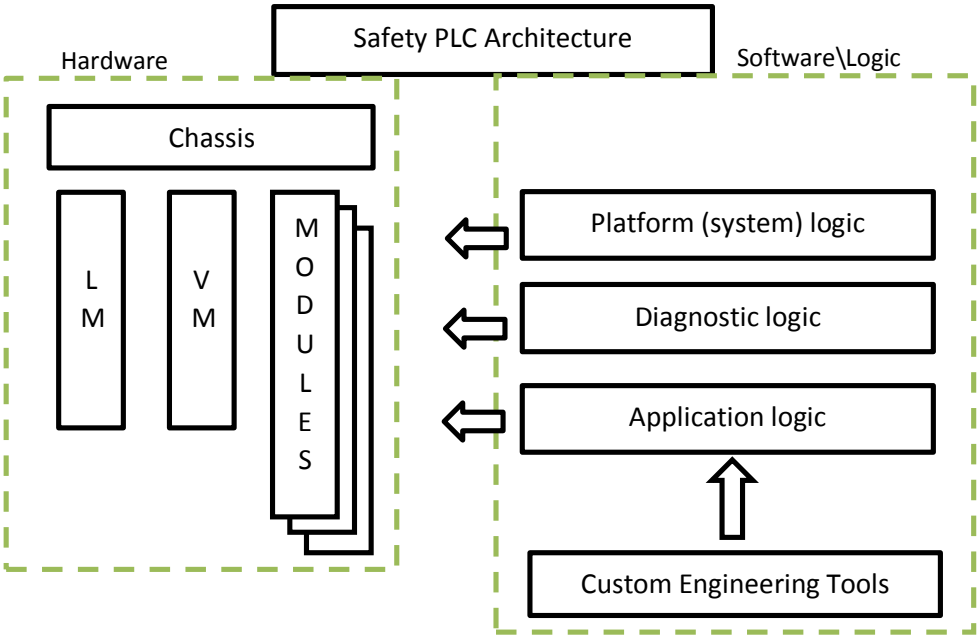

Рис. 1. Схематичне зображення розподілення HW і SW частин у safety PLC на основі даних, наведених у [7]

Обґрунтування та обрання показників якості

Життєвий цикл продукту складається не тільки з етапу розробки, а також з етапу тестування, експлуатації та ін. На етапі розробки виконується аналіз за методом Failure Mode Effect and Diagnostic Analysis (FMEDA), під час якого визначаються відмови (дефекти), які мають діагностуватись safety PLC для забезпечення необхідного рівня SIL. Слід підкреслити, що вже з цього переліку відмов з'являється можливість визначити ті відмови, які можуть розглядатись у якості потенційних вразливостей для здійснення кібератак і, таким чином, не проводити додатковий аналіз з використанням методу Intrusion Mode Effect and Criticality Analysis (IMECA), під час якого і визначаються критичні кібервразливості [9].

Як було визначено у [10] показник якості для визначення частини дефектів за результатами FMEDA, які можна вважати одночасно і кібервразливостями, має наступний вираз

$$\alpha = \text{Card}\,(F \cap I) / \text{Card}\,F\,,$$

де F – множина дефектів за результатами FMEDA;

I – множина вразливостей за результатами IMECA.

Для оцінювання співвідношень між множинами дефектів і вразливостей та подальшого аналізу складових безпеки надамо коефіцієнти

$$\alpha 1 = \text{Card}\,(F_{hw} \cap I) / \text{Card}\,F_{hw},$$
$$\alpha 2 = \text{Card}\,(F_{sw} \cap I) / \text{Card}\,F_{sw},$$

де α1 – визначає частку апаратних дефектів, які можуть бути одночасно і кібервразливостями, від загальної кількості апаратних дефектів;

α2 – визначає частку програмних дефектів, які можуть бути одночасно і кібервразливостями, від загальної кількості програмних дефектів;

F_{hw} – множина апаратних дефектів за результатами FMEDA;

F_{sw} – множина програмних дефектів за результатами FMEDA.

Для safety PLC у випадку дослідження програмної і апаратної складових вірним буде наступне твердження

$$F = F_{hw} \cup F_{sw}\,,$$

яке трансформується у вираз

$$F = F_{hw},$$

у разі відсутності у safety PLC програмної складової.

Результати FMEDA ще не гарантують того, що safety PLC забезпечує на практиці необхідний рівень діагностування безпечних та небезпечних відмов. Для отримання об'єктивної оцінки рівня самодіагностичного охоплення проводиться тестування шляхом засіву дефектів (fault injection testing, FIT) з переліку, який був отриманий за результатами FMEDA [11].

Враховуючи обмеження обсягу даної роботи, оцінка ступеню повторного використання результатів, отриманих під час FIT, проводитись не буде.

1. Аналіз публікацій

У роботі [12] розглядається можливість застосування ризик-інформованого підходу до оцінювання кіберзахисту ІКС АЕС, який має реалізовуватися на протязі усього життєвого циклу створення системи. Це дозволить збільшити імовірність завчасного визначення потенційних кібервразливостей системи, яка проєктується і виготовляється. У свою чергу, така системна робота дозволить розробити контрзаходи для певних типів атак. Як зазначено у [10] розглянуті підходи до оцінювання кібербезпеки досліджуються у статті без врахування специфіки об'єкту оцінювання. Додатково слід зазначити, про те, що у даній статті досліджується тільки етап проєктування системи і не розглядається випадок оцінки рівня кіберзахисту вже працюючої ІКС.

Якщо брати до уваги, що оцінка функційної безпечності ІКСВБ також базується на використанні ризик-орієнтованого підходу, то можна зробити висновок, що інформація, яка представлена у [12], засвідчує схожість у підходах до проведення оцінки як кібербезпеки, так і функційної безпеки ІКСВБ.

У схожому напрямку викладено ідею комплексного оцінювання функційної безпечності та кібербезпеки системи за рахунок використання методики XMECA [13, 14]. XMECA - це розширення FMECA, яке на відміну від FMECA може бути застосоване для аналізу різних аспектів безпеки ІКС, а не тільки тих, які пов'язані із аналізом відмов. У якості прикладу у роботі [13] наведено використання XMECA як аналізу метод IMECA для оцінки кібербезпеки системи. Автори наголошують на можливості застосування запропонованого методу для оцінки різних типів вбудованих систем на основі як мікроконтроллерів, так і FPGA. Також слід зазначити, що у роботах [13, 14] не розглядається прив'язка до ІКСБ або до певного рівня функційної безпечності і не досліджується можливість перехресного використання вже отриманих оцінок властивостей системи для оцінки інших її властивостей. Але у той же час, аналіз роботи свідчить про можливість використання одних і тих самих методів аналізу та оцінки функційних та кібервластивостей систем.

У роботі [15] на основі аналізу існуючих підходів, які викладені у відповідних публікаціях і стандартах [16-18] для визначення рівня функційної безпечності та кібербезпеки, був запропонований метод розрахунку рівня SIL для індустріальної ІКС на основі врахування ризиків, пов'язаних із кібербезпекою. Базуючись на запропонованому підході, була наведена матриця потенційної кореляції між рівнями кібербезпеки та функційної безпечності в залежності від класифікації функції, яку необхідно виконати системі. У статті не розглядаються PLC, на основі яких мають будуватись системи керування, а також не зовсім зрозуміло, наскільки достовірними будуть оцінки у разі, системи, ізольованої від зовнішніх мереж передачі даних, з рівнем функційної безпечності, який відповідає третьому рівню. Також, висловлена у роботі ідея можливого зменшення рівня SIL на основі обрання певного рівня кібербезпеки виглядає суперечливою.

Питання кібербезпеки PLC, які використовуються у індустріальних ІКС також розглядається у [19]. В статті аналізуються джерела загроз і відповідні ризики експлуатації PLC з точки зору людських, апаратних та програмних аспектів. Розглядаються вразливості індустріальних протоколів обміну даних і можливі варіанти реалізації кібератак. У той же час, у роботі робиться акцент тільки на PLC на базі мікроконтролерів, ІКС розглядаються за умови їхнього зв'язку з іншими комп'ютерними мережами, а також не досліджується питання PLC, які відповідають вимогам функційної безпечності.

Питання кібервразливостей індустріальних PLC досліджується у [20]. На прикладі одного з широко розповсюджених PLC фірми Siemens, який має у своєму складі двоспрямований інтернет-порт і може з'єднуватись з іншими PLC за допомогою промислового протоколу за рахунок використання IP-адреси. Дослідження проводилось шляхом створення і розповсюдження «черв'яка», який був розроблений саме для цього PLC. В експерименті джерелом атаки був заздалегідь інфікований PLC. Такий підхід надав можливості обійти захист PLC від атак із зовнішніх мереж. Тому, такий «черв'як» не може бути знайденим стандартними антивірусними засобами. Але у такої атаки також є «слабкі» місця, які ускладнюють її реалізацію у реальному житті. Ці «слабкі» місця пов'язані з тим, як інфікувати перший PLC. Це може бути здійснено або під час порушення вимог стандарті підприємства щодо закупівлі у офіційних дилерів, або порушення правил виготовлення виробником, або під час транспортування і цей «черв» має бути з відкладеним активуванням, оскільки на етапі налагодження ІКС він не має себе проявити. У той же час, такий експеримент яскраво свідчить про те, що широко розповсюджені PLC, які не відповідають вимогам функційної безпечності і використовують без

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

обмежень двоспрямовані інтерфейси, можуть бути успішно атакованими, за рахунок широкого розповсюдження інформації щодо їхньої архітектури, апаратної та програмної складових.

Безпека індустріальних мереж через здійснення атаки на PLC досліджується у [22]. Зазначається, що вразливим місцем таких мереж є використання загально відомих протоколів передачі даних. У статті запропонований механізм моніторингу здійснення атаки через використання методу контролю перетворення даних. Запропонований підхід базується на контролі вхідних значень від датчиків і генерація сигналу керування на актуатори відбувається коли декілька різних значень відповідають певному контексту. Це надає можливості детектувати атаки, які відбуваються тільки через зміну даних одно чи двох датчиків. Слід відзначити, що даний підхід вже давно використовується у роботі алгоритмів ІКСБ.

Взагалі, потенційний зв'язок між кібербезпекою та функційною безпечністю досліджується у багатьох роботах, які мають державне фінансування [8, 23]. Наприклад, у [23] надані базові відомості про ці властивості автоматичних систем керування на основі двох базових стандартів [4] і [17]. Але, оскільки, при поясненні функційної безпечності системи береться до уваги тільки імовірність відмови у обслуговуванні і не враховується рівень діагностування безпечних і небезпечних відмов, а також, нехтується властивість пристрою, як «безпечний стан», то, як наслідок, робиться висновок про близькість, але не збіжність, кібербезпеки та функційної безпечності. Однак навіть, при такому підході у роботі висловлені ідеї, про можливу схожість між цими властивостями, особливо під час робочої експлуатації та обслуговування системи.

На відміну від [23] у [24] надано описання функційної безпечності з урахуванням кількості відмов, які мають бути детектовані системою внутрішньої діагностики PLC. Взагалі, у рамках парадигми Industry 4.0 у [24] аналізується вплив фукційної безпечності не тільки на кібербезпеку, але і на роботів, інтегральні мікросхеми, канали передачі даних та програмне забезпечення. Окрім цього, висвітлюється питання про можливість співставлення рівнів SIL на базі IEC 61508 і рівнів Security Level (SL) на базі IEC 62443.

Таким чином, на підставі аналізу робимо висновок про те, що у відомих публікаціях, які стосуються безпекових характеристик (функційної та кібербезпеки), аспекти їх можливого «перехресного» оцінювання, коли певні результати при аналізі однієї з характеристик використовуються для оцінки іншої задля зменшення часових і вартісних витрат або для додаткової верифікації результатів оцінювання, досліджено недостатньо системно і глибоко.

2. Теоретичне обґрунтування взаємозв'язку між кібербезпекою і функціональною безпечністю для safety PLC

Як було зазначено у попередніх розділах об'єктом дослідження є safety PLC, який вже існує і його не можливо змінити, тому що у випадку внесення змін необхідно буде проводити повторну ре-сертифікацію на відповідність вимогам стандарту IEC 61508 [4].

Теоретичне обґрунтування слід почати із з'ясування «проекції» поняття кібербезпеки на I&C і безпосередньо на safety PLC. Відповідно до [17, 18] основні ризики, які оцінюються при розгляданні кібербезпеки, це: доступність інформації, цілісність інформації та конфіденційність інформації. Зазначені властивості піддаються атакам, які надходять з інформаційного (кібер) простору. Це стосується безпосередньо індустріальних систем, комп'ютерних мереж або інтернету речей,, оскільки вони мають не один, а велику кількість двонаправлених каналів передачі даних, які з'єднують їх із «зовнішнім» інформаційним (кібер) простором.

Зазначимо, що safety PLC мають особливості використання, які необхідно враховувати при оцінці властивостей. На рис. 2 наведена спрощена структурна схема використання safety PLC на прикладі системи безпеки реактора (safety I&C) для атомних станцій.

Аналіз наведеної схеми свідчить про те, що, фактично, safety PLC не має під'єднання до кіберпростору. Точніше, під час функціонування він має тільки односпрямований зв'язок до комп'ютерної частини систем відображення інформації, яка, у свою чергу, не підключена до загальних комп'ютерних мереж. Інформація від датчиків до актуаторів передається за допомогою мідних кабелів, або, як наприклад у сучасних I&C, додатково можуть використовуватись і оптичні кабелі.

В одній I&C одночасно використовується 3 або 4 канали прийому та обробки вхідних сигналів для реалізації схеми 2oo3 та 2oo4 відповідно. В кожному з каналів є safety PLC, а єдиним двостороннім каналом передачі даних є канал обміну даних між safety PLC в середині системи (рис. 3). Однак, не всі стандарти [21] дозволяють результатам міжканального обміну враховуватись при формуванні сигналів захисту, що дозволяє, таким чином, забезпечити незалежність каналів один від одного.

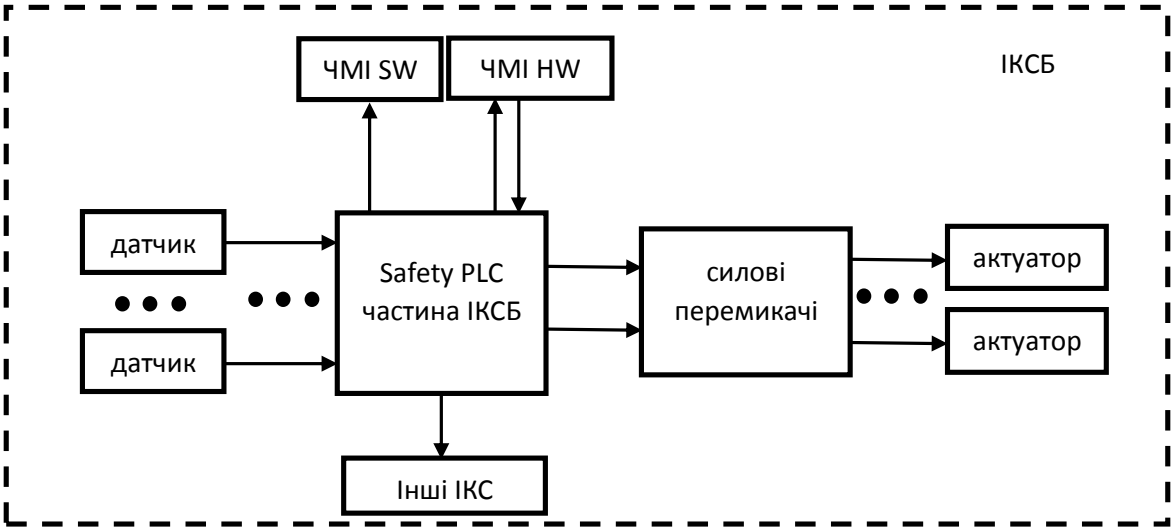

Рис. 2. Спрощена структурна схема ІКСБ для атомних станцій

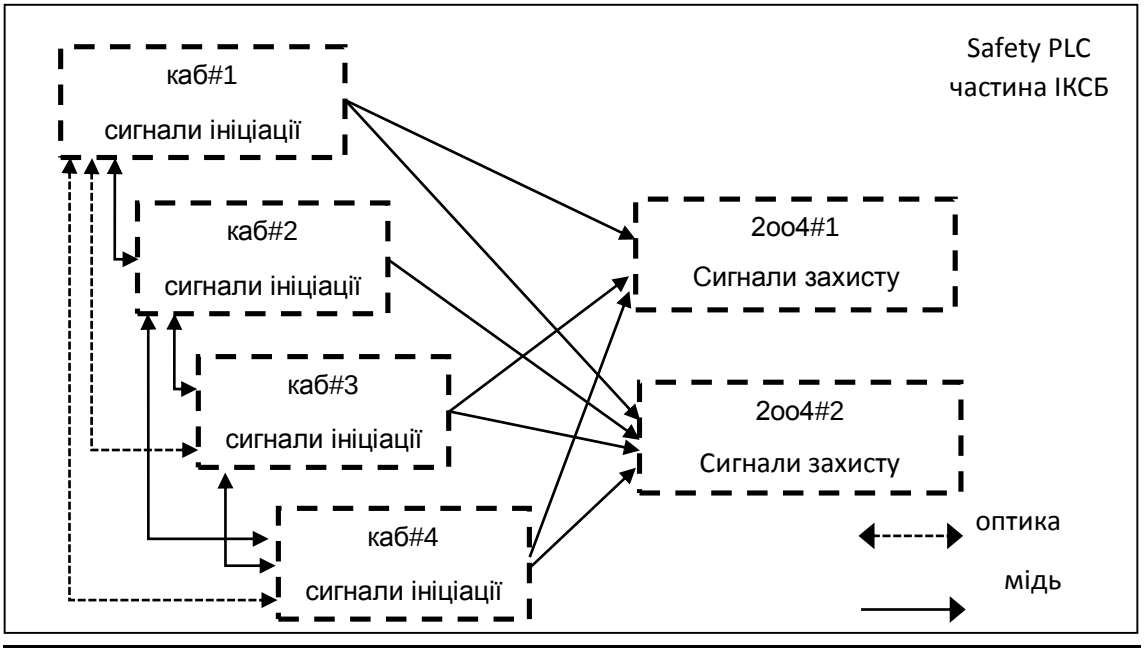

Рис. 3. Safety PLC частина ІКСБ

На підставі зазначеного зробимо висновок, що під час виконання операційної діяльності (on-line mode) safety PLC у складі ІКСБ не є вразливим до кібератак у їх класичному розумінні, тобто до дистанційних атак, джерелом яких є інформаційний (кібер) простір. Але, деякі кібератаки можуть бути здійснені зловмисником через реалізацію безпосередніх маніпуляцій з обладнанням. Наприклад, він може спробувати внести зміни у safety PLC, які призведуть до того, що safety PLC буде не змозі виконати функцію безпеки за запитом. Ці зміни не фізичного руйнування, а спрямовані на інформаційну складову safety PLC. У таблиці 1 наведений перелік кібератак, які зловмисник може здійснити по відношенню до safety PLC у режимі онлайн управління технологічним процесом.

До множини валідних об'єктів – модуля, порта, слота та пристрою, належать такі об'єкти, які прописані у поточній конфігурації safety PLC. До невалідних об'єктів належать ті, що входять до складу safety PLC, але у поточній конфігурації не використовуються. Множина невірних об'єктів утворюється усіма об'єктами, які не входять до складу safety PLC взагалі.

Особливо звертає увагу на себе той факт, що для здійснення будь-якої атаки з таблиці 1 зловмисник має подолати декілька серйозних перевірок безпосередньо на об'єкті або захопити об'єкт критичної інфраструктури.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Таблиця 1

Атаки на інформаційну складову safety PLC під виконання операційного функціонування (on-line mode)

Тип атаки	Імплементація атаки	Властивості інформації, що пошкоджується		
		доступність	цілісність	конфіденційність
Атака на апаратну конфігурацію	Інсталяція не валідного модуля			+
	Вилучення валідного модуля	+		
	Інсталяція валідного модуля у невалідний слот	+		
	Зміна слотів валідних модулів	+	+	
Атака на міжканальний обмін	Від'єднання оптичного кабелю	+		
	Під'єднання у невірний порт		+	
	Хибне під'єднання оптичних кабелів			+
Атака на HMI інтерфейс	Від'єднання існуючого підключення	+		
	Утворення невірного підключення			+
	Утворення невалідного підключення			
Атака на передачу даних в середині ІКС	Невірне підключення портів	+		+
	Розривання підключення		+	
	Невалідне підключення портів	+		
	Підключення до невалідного пристрою			+
Атака на зовнішнє підключення	Від'єднання вхідних кабелів	+		
	Від'єднання вихідних кабелів	+		

Також, перед залишенням об'єкту зловмисник може зробити відповідну «закладку», яка буде активована згодом. Саме до такого типу кібератак вразливі аналогові системи керування, оскільки в них відсутній механізм контролю апаратної конфігурації. Отже, дуже важливим є висновок, що стійка до кібератак у класичному розумінні аналогова система керування стає вразливою для такої нетипової атаки.

Якщо дослідити атаки на safety PLC під час від'єднання від операційного функціонування (off-line mode), то перший висновок – їхня кількість стає в значно більше. Тому що, саме у off-line mode рахунок внаслідок таких атак може здійснюватися:

- зміна параметрів алгоритмів UAL;
- завантаження оновленої UAL;
- заміна модуля із складу ЗІП;
- зміна platform (system) програмної частини safety PLC.

Перелік потенційних кібератак у off-line mode наведений у таблиці 2 з прив'язкою до об'єктів атаки. У таблиці враховується атаки, які можуть бути здійснені під час підключення safety PLC до будь-якого комп'ютера з метою здійснення вище зазначених дій.

У таблиці 2 атаки наведені у згрупованому виді, тому що кожна з імплементацій може бути реалізована через декілька вразливостей, а з точки зору функційної безпечності, – відмов. Декілька імплементацій належать до поширеної кібератаки – «людина в середині». Також, усі атаки з таблиці 1 можуть бути здійснені під час виведення safety I&C з роботи із технологічним процесом.

На основі даних, наведених у таблицях 1 і 2, надамо опис природи кібервразливостей через використання понять з теорії функційної безпечності. Будь-яка атака базується на використанні вразливості. Механізм вразливості для індустріальних контролерів базується на існуванні можливості досліджувати його апаратну і програмну реалізації, особливо протоколи обміну даних та визначати місця, через які можна його атакувати. Тобто визначати точку проникнення у safety PLC та структуру інформаційного пакету, який буде спроба «перетворити» або «спотворити» і передати індустріальному контролеру. Критична вразливість – це будь-яка частина контролеру, яка не контролюється системою внутрішнього діагностування. Тому, зловмисник користуючись

Таблиця 2

Атаки на інформаційну складову safety PLC off-line mode

Об'єкт атаки	**Імплементація атаки**	**Властивості інформації що пошкоджується**		
		доступність	**цілісність**	**конфіденційність**
FPGA	Спотворення firmware (platform software)	+	+	+
	Підміна firmware (platform software)	+	+	+
	Вплив на внутрішньою пам'ять		+	
	Спотворення алгоритмів розрахунку цілісності (CRC)		+	
Файл прошивки відповідно до UAL	Підміна файлу HW конфігурації за рахунок додання невірного HW	+		+
	Активація порту не за призначенням	+		+
	Спотворення пакету даних UAL у комунікаційному каналі за усіма можливими параметрами		+	+
	Завантаження невірного файлу UAL			+
	Спотворення файлу UAL до того як він почав завантажуватись			+
	Спотворення файлу UAL підчас завантаження		+	+
	Встановлення значення setpoints за межами обраного діапазону			+
	Підключення до хибного safety PLC для зміни setpoint			+
	Підміна значення setpoint під час завантаження на невалідне		+	
	Підміна значення setpoint під час завантаження на невірне		+	
	Спотворення файлу SW конфігурації	+		

цією неконтрольованою частиною PLC здійснює атаку на інформацію, яка циркулює в контролері. В такому випадку імовірність вдалої атаки можна записати наступним виразом

$$P_{cyber}=f(P_s, P_{contr}),$$

$$P_{cyber} \rightarrow 1, \text{ якщо } P_s \rightarrow 0, P_{contr} \rightarrow 0,$$

де P_{cyber} – імовірність здійснення вдалої кібератаки;

P_s – імовірність, що внутрішня потенційна відмова охоплена діагностуванням (або певна частина контролера охоплена системою самодіагностування);

P_{contr} – імовірність наявності відповідного контрзаходу.

Наявність відповідного контрзаходу вкрай важлива властивість контролеру, оскільки, атака може бути детектована, але у разі відсутності реалізації алгоритму протидії P_{cyber} буде наближатись до 1. Наприклад, система спостереження будинку визначила порушення периметру, але не активувала будь-яке оповіщення. Тому ніхто і ніщо, в такому разі, не завадить зловмиснику реалізувати злочинні наміри.

Таким чином, з одного боку, наявність системи діагностування і ступень (глибина) її покриття а, з іншого боку, наявність контрзаходу, а саме, запрограмована поведінка контролера у разі атаки, яке не дасть можливості нанести шкоду людині, характеризують здатність PLC вдало протидіяти кібератакам.

Глибина діагностичного покриття safety PLC – SD_{sdplc} визначається, як відношення кількості відмов охоплених системою внутрішнього діагностування до кількості усіх можливих відмов [4]

$$SD_{plc}= (m/n)*100,$$

де n – загальна кількість відмов;

m – кількість відмов, які детектує система самодіагностування.

З точки зору safety PLC, який досліджується у статті, самодіагностування контролеру має глибину

охоплення 99,998%, що відповідає глибині системи внутрішньої самодіагностики для рівня SIL-3 [4], тобто $P_s \rightarrow 1$.

Тому імовірність здійснення успішної кібератаки буде визначатись наступним виразом

$$P_{cyber} = f(P_{contr}).$$

Safety PLC відповідно до вимог стандарту IEC 61508 має певний стан (safety state) в який він зобов'язаний перейти при детектуванні відмови. Тобто, у випадку, коли система діагностування знаходить відмову, контролер, в залежності від того яка відмова – критична чи ні, автоматично виконує певні дії.

Таким чином, на основі вище зазначеного будь-який вплив на контролер (навмисний – атака, випадковий - відмова) діагностується його системою самодіагностування і автоматично реалізуються захисні дії.

Отже, з огляду на надане обґрунтування, схематичне представлення запропонованого методу наведено на рис. 4.

На основі множини відмов, яка відповідає обраному рівню SIL, на відповідність якому вже був оцінений safety PLC, шляхом аналізу обираються ті відмови, які можуть розглядатись як вразливості. Для перевірки кожної такої вразливості має бути виконаний тест на проникнення. Але, в запропонованому методі немає необхідності його проводити. Для цього аналізуються результати вже виконаного FIT для обраної відмови. Також при використанні запропонованого методу немає необхідності проводити таку активність як IMECA, тому що набір вразливостей буде сформований з множини відмов.

Таким чином, кожній атаці з таблиць 1 і 2 має бути поставлена мінімум одна відмова, яку має виявляти контролер. Наприклад так, як це було представлено у [10] або на основі прикладів, наведених у таблиці 3.

3. Практичний кейс застосування запропонованого підходу

Як правило, safety PLC складається з модулів прийому та обробки вхідних сигналів від зовнішніх датчиків та наступної передачі їх до головного модуля, в якому імплементовані алгоритми керування, на основі яких формуються вихідні сигнали і надсилаються до вихідних модулів, які у свою чергу надсилають їх до виконавчих механізмів. Додатково, до складу safety PLC можуть входити модуль живлення, модуль комунікації та модуль діагностування. Таким чином, склад safety PLC нараховує від 3 до 12 різних модулів. Для кожного з цих модулів обчислюються показники за методом FMEDA і проводиться наступне тестування для отримання об'єктивних доказів, що система самодіагностування виявляє всі відмови і safety PLC детерміновано реагує.

Атаки на UAL стосується головного модуля та її наслідки розраховуються для safety PLC один раз. Оскільки всі відмови програмної складової safety PLC можуть за певних умов вважатись як кібератаки, тому $\alpha 2=1$.

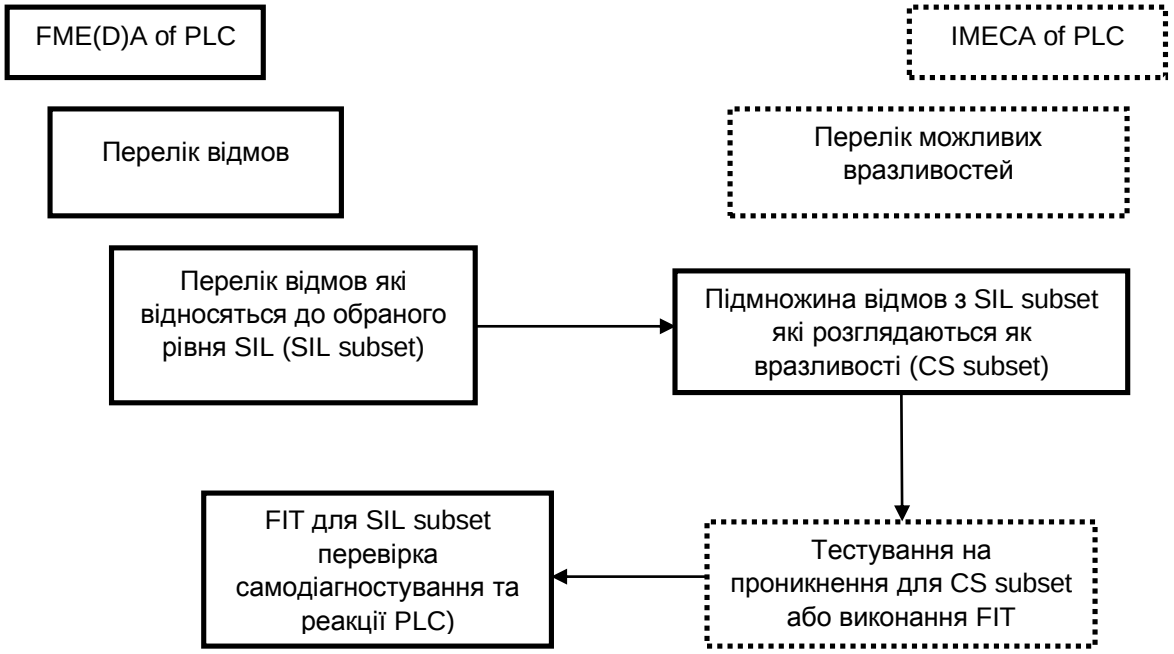

Рис. 4. Схематичне представлення запропонованого методу

Таблиця 3

Перелік прикладів відповідність між відмовами та вразливостями для safety PLC

Відмова safety PLC	**Вразливість**	**Атака**	**Поведінка safety PLC при виявленні відмови (атаки)**
Відмова у пристрою прм\прд	Відсутність контроля наявності модуля	Видалити валідний модуль з шасі	Перехід у безпечний стан
Відмова механізму контролю цілісності системного по модуля	Відсутність контролю цілісності пакету даних	Підміна системного ПО модуля	Перехід у безпечний стан
Відмова регістра пам'яті у середині FPGA	Відсутність механізму контролю цілісності даних в середині FPGA	Спотворення даних в середині FPGA	Перехід у безпечний стан
Відмова механізму контроля введеного значення setpoints	Відсутність контроля значення setpoints	Встановлення значення setpoints за межами обраного діапазону	Сигналізація і оповіщення
Відмова механізму контроля введеного значення setpoints	Відсутність контроля значення setpoints	Підміна значення setpoint під час завантаження на невірне	Сигналізація і оповіщення

Якщо взяти за основу розрахунки, які були наведені у [10], де показано, що, в середньому, для модуля комунікацій коефіцієнт α1=0,263 і для спрощення процедури оцінювання будемо вважати, що α1=0,25 від загальної кількості відмов за результатами FMEDA. Для вхідних і вихідних модулів будемо вважати, що α1=0,2, оскільки немає ліній передачі і прийому інформації від інших модулів. Для головного модуля коефіцієнт α1=0,25, оскільки значна кількість відмов, які можуть розглядатись як кібератака належать до програмної складової.

Якщо врахувати, що для перевірки одного дефекту необхідно витратити 24 людино/годин (виконання одного FIT) і як, було показано у [10] для одного модуля α1=0,25, що відповідає 10 виконаним FIT, то економія буде складати 240 людино/годин. Для модулів входу та виходу вони будуть дорівнювати по 192 людино/годин на кожного. Економія для апаратної частини головного модуля складатиме 240 людино/годин, а його програмної складової – орієнтовно 672 людино/годин. Таким чином, для мінімального safety PLC економія буде складати 1486 людино/годин. В цілому це дозволяє заощадити майже 4 місяці роботи, а при мінімальній вартості людино/годин у 2000 грн., економія в проєкті по даній активності в цілому буде дорівнювати майже 3000000000 грн. Такі розрахунки можна вважати мінімально можливими, на які слід орієнтуватися.

Висновок

Функційна безпечність та кібербезпека є важливими характеристиками систем управління технологічними процесами, які представляють потенційну загрозу для життя людей, але без яких неможливо представити сучасну індустрію, транспорт, енергетику інші галузі.

Формування і впровадження вимог щодо забезпечення кібербезпеки ІКС має відбуватись з урахуванням умов її функціонування системи та властивостей апаратних і програмних складових.

Можливість повторного використання вже існуючих результатів оцінки функційної безпечності для оцінювання кібербезпеки підвищує ступень повернення вартості вкладених інвестицій і суттєво заощаджує час. Це особливо актуально, тому що процес розробки, тестування та сертифікації сучасних цифрових систем з високим рівнем функційної безпечності є вкрай ресурсовитратним процесом.

Тому, додаткові вимоги щодо кібербезпеки для вже існуючих систем і тих, що знаходяться на етапі розробки, мають не уповільнювати і не ускладнювати ці процеси, а гармонічно імплементовуватись і надавати значні переваги з огляду на зусилля та витрати. Запропонована методологія може також підвищити достовірність оцінювання, оскільки в дослідженні продемонстрована наявність, так званої, природної надмірності процесів, що надає змогу

мати додаткові артефакти для «перехресної» верифікації.

Слід сформулювати важливий методологічний висновок на підставі даного дослідження, яке є логічним продовженням попередньої публікації авторів [10]. Відомий принцип Security Informed Safety (SIS), який був запропонований Робіном Блумфілдом та його колегами [25] та імплементований в засобах Assurance Safety/Security Case, нами доповнюється його, так би мовити, оберненим варіантом Security supported/assessed by Safety (SAS). Тобто до принципу «оцінювання функційної безпечності з врахуванням/на підставі інформаційної (кібер)безпеки» додається принцип «оцінювання інформаційної (кібер)безпеки за підтримки/з урахуванням результатів оцінювання функційної безпечності».

Наведені вище прості розрахунки демонструють економічну ефективність його впровадження та обумовлюють доцільність подальших досліджень і розробок за цим напрямом з урахуванням результатів [26], де принцип SIS був представлений модифікованим методом IMECA, а саме SISMECA-аналізом.

Внесок авторів: запропонував підхід до оцінки рівня кіберзахисту safety PLC на основі вже існуючих даних, щодо рівня функціональної безпечності контролера – **О.О. Івасюк**; провів аналіз щодо узгодженості запропонованого методу теоретичним основам побудови гарантоздатних систем – **В. С. Харченко**.

Конфлікт інтересів

Автори заявляють, що немає конфлікту інтересів щодо цього дослідження, фінансового, особистого, авторського чи іншого, який міг би вплинути на дослідження та його результати, представлені в цій статті.

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Рукопис не має пов'язаних даних.

Використання засобів штучного інтелекту

Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

Усі автори прочитали та погодилися з опублікованою версією рукопису.

Література

1. *World Nuclear Association. Nuclear Power in the USA. Report, October 2023 [Електронний ресурс]. – Режим доступу: https://world-nuclear.org/information-library/country-profiles/countries-t-z/usa-nuclear-power.aspx – 05.01.2024.*

2. *U.S. Nuclear Regulatory Commission. Regulatory Guide 1.168. Verification, validation, reviews, and audits for digital computer software used in safety systems of nuclear power plants, Revision . July 2013 [Електронний ресурс]. – Режим доступу: https://www.nrc.gov/docs/ML1307/ML13073A210.pdf – 15.01.2024.*

3. *Safety Classification for I&C Systems in Nuclear Power Plants – Current Status & Difficulties. Report No. 2015/008, World Nuclear Association. – September 2015. – 27 p. [Електронний ресурс]. – Режим доступу: https://www.world-nuclear.org/uploadedFiles/org/WNA/Publications/Working_Group_Reports/safety-classification-for-iandc-systems-in-npps.pdf – 05.01.2024.*

4. *IEC 61508:2010. Functional safety of electrical / electronic / programmable electronic safety related systems. Part 1-7. International Electrotechnical Commission [Електронний ресурс]. – Режим доступу: https://www.iec.ch/global/search?keyword=IEC%2061508%3A2010#gsc.tab=0&gsc.q=IEC%2061508%3A2010 – 05.01.2024.*

5. *IEC 61513:2011. Nuclear power plants – Instrumentation and control important to safety – General requirements for systems. International Electrotechnical Commission, 2011-08-25. [Електронний ресурс]. – Режим доступу: https://webstore.iec.ch/publication/5532 – 05.01.2024.*

6. *ISO 26262-1:2018. Road vehicles – Functional safety. Part 1-4. International Organization for Standardization, 2018-12-01. [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/68386.html – 05.01.2024.*

7. *RadlCS Topical Report. Part I – NRC Safety Evaluation. Document ID: 2016-RPC003-TR-001 NP-A. [Електронний ресурс]. – Режим доступу: https://www.nrc.gov/docs/ML1923/ML19233A177.pdf – 05.01.2024.*

8. *Бабешко, Є. Функційна безпека індустріальних систем. Стандарт IEC 61508 [Текст] / Є. Бабешко, О. Ілляшенко, & В. Харченко. – Київ, Технічний Комітет 185 «Промислова Автоматизація», 2019. – 37 с. Available at: https://tk185.appau.org.ua/whitepapers/aCampus-whitepaper-IEC-61508+++.pdf – 05.01.2024.*

9. *Kovalenko, A. Gap-and-IMECA-Based Approach to Assessment of complex I&C Systems cyber security [Текст] / A. Kovalenko, & O. Rudenko //*

Информационные технологии в управлении, образовании, науке и промышленности : монография / под ред. В. С. Пономаренко. – Х. : Издатель Рожко С. Г., 2016. – Разд. 2.– С. 27-40. [Електронний ресурс]. – Режим доступу: http://www.repository.hneu.edu.ua/jspui/handle/123456789/13389 – 05.01.2024.

10. *Харченко, В. С. Використання методу верифікації FMEDA/FIT для оцінювання кібербезпеки програмовного логічного контролера [Текст] / В.С. Харченко, О. О. Івасюк // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2023. – Т. 4 (74). – С. 114-119. DOI: 10.26906/SUNZ.2023.4.114.*

11. *Fault insertion testing of FPGA-based NPP I&C systems: SIL certification issues [Text] / V. Kharchenko V. Sklyar, A. Ivasuyk, & O. Odarushenko // Proceedings of 22nd International Conference on Nuclear Engineering. Technical Publication ICONE22. – 2014. –Vol. 6. Nuclear Education, Public Acceptance and Related Issues; Instrumentation and Controls (I&C); Fusion Engineering; Beyond Design Basis Events. DOI: 10.1115/ICONE22-31163.*

12. *Кіберзахист інформаційних та керуючих систем АЕС: оцінювання ризиків [Текст] / А. А. Симонов, О. Л. Клевцов, С. О. Трубчанінов, А. А. Симонова // Ядерна та радіаційна безпека. – 2022. – Т. 4(96). – P. 62-70. DOI: 10.32918/nrs.2022.4(96).08.*

13. *Towards Trustworthy Safety Assessment by Providing Expert and Tool-Based XMECA Techniques [Text] / E. Babeshko, O. Illiashenko, V. Kharchenko, & K. Leontiev // Mathematics. – 2022. – Vol. 10, iss. 13. – Article no. 2297. DOI: 10.3390/math10132297.*

14. *Application of Assumption Modes and Effects Analysis to XMECA [Text] / I. Babeshko, K. Leontiiev, V. Kharchenko, A. Kovalenko, & E. Brezhniev // Theory and Engineering of Dependable Computer Systems and Networks. DepCoS-RELCOMEX 2021. – Springer, Cham, 2021. – Vol. 1389. – P. 1-11. DOI: 10.1007/978-3-030-76773-0_1.*

15. *Śliwiński, M. Integrated approach for functional safety and cyber security management in maritime critical infrastructures [Text] / M. Śliwiński, & E. Piesik // Journal of Polish Safety and Reliability Association Summer Safety and Reliability Seminars. – 2019. – Vol. 10, iss. 1-2. – P. 137-149. Available at: http://jpsra.am.gdynia.pl/wp-content/uploads/2019/04/JPSRA2019-VOL10-Sliwinski_Piesik.pdf – 05.01.2024.*

16. *Yastrebenetsky, M. A. Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems [Text] / M. A. Yastrebenetsky, & V. S. Kharchenko (editors). – IGI Global, 2020. – 501 p. DOI: 10.4018/978-1-7998-3277-5.*

17. *ISA/IEC 62443 Series of Standards. Consensus-Based Automation and Control Systems Cybersecurity Standards. Parts 1-13, International Electrotechnical Commission [Електронний ресурс]. – Режим доступу: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards – 05.01.2024.*

18. *ISO/IEC 15408:2009. Information technology Security techniques – Evaluation criteria for IT security. Part 1-3. International Electrotechnical Commission, Geneva. Available at: https://standards.iteh.ai/catalog/standards/cen/a964a0a1-56f3-4a0d-a485-4ca5a03f0a77/en-iso-iec-15408-1-2020. – 05.01.2024.*

19. *Hajda, J., Jakuszewski, R., & Ogonowski, S. Security Challenges in Industry 4.0 PLC Systems [Text] / J. Hajda, R. Jakuszewski, & S. Ogonowski // Appl. Sci. – 2021. – Vol. 11, iss. 21. – Article no. 9785. DOI: 10.3390/app11219785.*

20. *PLC-Blaster: A Worm Living Solely in the PLC [Electronic resource] / R. Spenneberg, M. Brüggemann, & H. Schwartke. – Available at: https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf – 08.09.2021.*

21. *603-2018 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Revision of IEEE Std 603-2009) [Electronic resource]. – IEEE New York, 2018. – Available at: https://www.scribd.com/document/498969031/603-2018-IEEE-Standard-Criteria-for-Safety-Systems-for-Nuclear-Power-Generating-Stations (accessed 08 Jan. 2024).*

22. *Detecting Safety and Security Faults in PLC Systems with Data Provenance [Text] / A. Al Farooq, J. Marquard, K. George, & T. Moyer // 2019 IEEE International Symposium on Technologies for Homeland Security (HST). – Woburn, MA, USA, 2019. – P. 1-6. DOI: 10.1109/HST47167.2019.9032992.*

23. *Sino-German White Paper on Functional Safety for Industrie 4.0 and Intelligent Manufacturing [Electronic resource]. – Federal Ministry for Economic Affairs and Energy Public Relations Division, July 2020. – Available at: https://www.scribd.com/document/498969031/603-2018-IEEE-Standard-Criteria-for-Safety-Systems-for-Nuclear-Power-Generating-Stations – 15.01.2024.*

24. *Meany, T. Functional safety and Industrie 4.0 [Text] / T. Meany // 28th Irish Signals and Systems Conference (ISSC). – Killarney, Ireland, June 2017. – P. 1-7. DOI: 10.1109/ISSC.2017.7983633.*

25. *Bloomfield, R. Security-Informed Safety: If It's Not Secure, It's Not Safe [Text] / R. Bloomfield, K. Netkachova, & R. Stroud // Software Engineering for Resilient Systems. SERENE 2013. Lecture Notes in Computer Science, Springer. – Berlin, Heidelberg, 2013, vol. 8166. DOI: 10.1007/978-3-642-40894-6_2.*

26. *Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection [Text] / O. Illiashenko, V. Kharchenko, I. Babeshko, H. Fesenko, & F. Di Giandomenico // Entropy. – 2023. – Vol. 25. – Article no. 1123. DOI: 10.3390/e25081123.*

References

1. *World Nuclear Association. Nuclear Power in the USA. Report, October 2023.* Available at: https://world-nuclear.org/information-library/country-profiles/countries-t-z/usa-nuclear-power.aspx (accessed 05 Jan 2024).

2. *U.S. Nuclear Regulatory Commission. Regulatory Guide 1.168. Verification, validation, reviews, and audits for digital computer software used in safety systems of nuclear power plants, Revision 2*. July 2013. 15 p. Available at: https://www.nrc.gov/docs/ML1307/ML13073A210.pdf (accessed 05 Jan 2024).

3. *Safety Classification for I&C Systems in Nuclear Power Plants – Current Status & Difficulties. Report No. 2015/008*, World Nuclear Association, September 2015. 27 p. Available at: https://www.world-nuclear.org/uploadedFiles/org/WNA/Publications/Working_Group_Reports/safety-classification-for-iandc-systems-in-npps.pdf (accessed 05 Jan 2024).

4. *IEC 61508:2010. Functional safety of electrical / electronic / programmable electronic safety related systems. Part 1-7*. International Electrotechnical Commission. Available at: https://www.iec.ch/global/search?keyword=IEC%2061508%3A2010#gsc.tab=0&gsc.q=IEC%2061508%3A2010 (accessed 05 Jan 2024).

5. *IEC 61513:2011. Nuclear power plants – Instrumentation and control important to safety – General requirements for systems.* International Electrotechnical Commission, 2011-08-25. Available at: https://webstore.iec.ch/publication/5532 (accessed 05 Jan 2024).

6. *ISO 26262-1:2018. Road vehicles – Functional safety. Part 1-4.* International Organization for Standardization, 2018-12-01. Available at: https://www.iso.org/standard/68386.html (accessed 05 Jan 2024).

7. *RadlCS Topical Report. Part I – NRC Safety Evaluation. Document ID: 2016-RPC003-TR-001 NP-A.* Available at: https://www.nrc.gov/docs/ML1923/ML19233A177.pdf (accessed 05 Jan 2024).

8. Babeshko, Ye., Illyashenko, O., & Kharchenko, V. *Funktsiyna bezpeka industrial'nykh system. Standart IEC 61508* [Functional safety of industrial systems. Standard IEC 61508]. Kyiv, Tekhnichnyy Komitet 185 «Promyslova Avtomatyzatsiya» Publ., 2019. 37 p. Available at: https://tk185.appau.org.ua/whitepapers/aCampus-whitepaper-IEC-61508+++.pdf (accessed 05 Jan 2024).

9. Kovalenko, A., & Rudenko, O. Gap-and-IMECA-Based Approach to Assessment of complex I&C Systems cyber security. *Informatsionnyye tekhnologii v upravlenii, obrazovanii, nauke i promyshlennosti : monografiya* [Information technologies in management, education, science and industry : monograph]. Kharkiv, Izdatel' Rozhko S. G. Publ., 2016. Razd. 2, pp. 27-40. Available at: http://www.repository.hneu.edu.ua/jspui/handle/123456789/13389 (accessed 05 Jan 2024).

10. Kharchenko, V. S., & Ivasiuk, O. O. Vykorystannya metodu veryfikatsiyi FMEDA/FIT dlya otsinyuvannya kiberbezpeky prohramovnoho lohichnoho kontrolera [Using the FMEDA/FIT verification method to assess the cybersecurity of a programmatic logic controller]. *Systemy upravlinnya, navihatsiyi ta zv"yazku. Zbirnyk naukovykh prats' – Control, navigation and communication systems. Collection of scientific works.* Poltava, PNTU Publ., 2023, vol. 4 (74), pp. 114-119. DOI: 10.26906/SUNZ.2023.4.114. (In Ukrainian).

11. Kharchenko, V., Odarushenko, O., Sklyar, V., & Ivasyuk, A. Fault insertion testing of FPGA-based NPP I&C systems: SIL certification issues. *Proceedings of 22nd International Conference on Nuclear Engineering. Technical Publication ICONE22*, 2014, vol. 6. Nuclear Education, Public Acceptance and Related Issues; Instrumentation and Controls (I&C); Fusion Engineering; Beyond Design Basis Events. DOI: 10.1115/ICONE22-31163.

12. Symonov, A., Klevtsov, O., Trubchaninov, S., & Symonova, A. Kiberzakhyst informatsiynykh ta keruyuchykh system AES: otsinyuvannya ryzykiv [Cyber protection of NPP information and control systems: risk assessment]. *Yaderna ta radiatsiyna bezpeka – Nuclear and radiation safety*, 2022, vol. 4(96), pp. 62-70. DOI: 10.32918/nrs.2022.4(96).08. (In Ukrainian).

13. Babeshko, E., Illiashenko, O., Kharchenko, V., & Leontiev, K. Towards Trustworthy Safety Assessment by Providing Expert and Tool-Based XMECA Techniques. *Mathematics*, 2022, vol. 10, iss. 13, article no. 2297. DOI: 10.3390/math10132297.

14. Babeshko, I., Leontiiev, K., Kharchenko, V., Kovalenko, A., & Brezhniev, E. Application of Assumption Modes and Effects Analysis to XMECA. *Theory and Engineering of Dependable Computer Systems and Networks.* DepCoS-RELCOMEX 2021, Springer, Cham, 2021, vol. 1389, pp. 1-11. DOI: 10.1007/978-3-030-76773-0_1.

15. Śliwiński, M., & Piesik, E. Integrated approach for functional safety and cyber security management in maritime critical infrastructures. *Journal of Polish Safety and Reliability Association Summer Safety and Reliability Seminars*, 2019, vol. 10, iss. 1-2, pp. 137-149.

Available at: http://jpsra.am.gdynia.pl/wp-content/uploads/2019/04/JPSRA2019-VOL10-Sliwinski_Piesik.pdf (accessed 05 Jan 2024).

16. Yastrebenetsky, M. A., & Kharchenko, V. S. (editors). *Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems.* IGI Global, 2020. 501 p. DOI: 10.4018/978-1-7998-3277-5.

17. *ISA/IEC 62443 Series of Standards. Consensus-Based Automation and Control Systems Cybersecurity Standards. Parts 1-13.* International Electrotechnical Commission. Available at: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards – (accessed 05 Jan 2024).

18. *ISO/IEC 15408:2009. Information technology Security techniques – Evaluation criteria for IT security. Part 1-3.* International Electrotechnical Commission, Geneva. Available at: https://standards.iteh.ai/catalog/standards/cen/a964a0a1-56f3-4a0d-a485-4ca5a03f0a77/en-iso-iec-15408-1-2020 (accessed 05 Jan 2024).

19. Hajda, J., Jakuszewski, R., & Ogonowski, S. Security Challenges in Industry 4.0 PLC Systems. *Appl. Sci.*, 2021, vol. 11, iss. 21, article no. 9785. DOI: 10.3390/app11219785.

20. Spenneberg, R., Brüggemann, M., & Schwartke, H. *PLC-Blaster: A Worm Living Solely in the PLC*. Available at: https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf (accessed 08 Sept. 2021).

21. *603-2018 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Revision of IEEE Std 603-2009)*, IEEE New York, 2018. Available at: https://www.scribd.com/document/498969031/603-2018-IEEE-Standard-Criteria-for-Safety-Systems-for-Nuclear-Power-Generating-Stations (accessed 08 Jan. 2024).

22. Al Farooq A., Marquard, J., George, K., & Moyer, T. Detecting Safety and Security Faults in PLC Systems with Data Provenance. *2019 IEEE International Symposium on Technologies for Homeland Security (HST)*, Woburn, MA, USA, 2019, pp. 1-6. DOI: 10.1109/HST47167.2019.9032992.

23. *Sino-German White Paper on Functional Safety for Industrie 4.0 and Intelligent Manufacturing.* Federal Ministry for Economic Affairs and Energy Public Relations Division, July 2020. Available at: https://www.scribd.com/document/498969031/603-2018-IEEE-Standard-Criteria-for-Safety-Systems-for-Nuclear-Power-Generating-Stations (accessed 15 Jan. 2024).

24. Meany, T. Functional safety and Industrie 4.0. *28th Irish Signals and Systems Conference (ISSC)*, Killarney, Ireland, June 2017, pp. 1-7. DOI: 10.1109/ISSC.2017.7983633.

25. Bloomfield, R., Netkachova, K., & Stroud, R. Security-Informed Safety: If It's Not Secure, It's Not Safe. In: Gorbenko, A., Romanovsky, A., Kharchenko, V. (eds) *Software Engineering for Resilient Systems. SERENE 2013*. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2013, vol. 8166. DOI: 10.1007/978-3-642-40894-6_2.

26. Illiashenko, O., Kharchenko, V., Babeshko, I., Fesenko, H., & Di Giandomenico, F. Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection. *Entropy*, 2023, vol. 25, article no. 1123. DOI: 10.3390/e25081123.

Надійшла до редакції 05.01.2024, розглянута на редколегії 20.02.2024

USING THE FMEDA/FIT VERIFICATION METHOD TO ASSESS THE CYBERSECURITY OF A PROGRAMABLE LOGIC CONTROLLER: A NEW INTERPRETATION OF THE SIS PRINCIPLE

Oleksandr Ivasiuk, Vyacheslav Kharchenko

The object of this study is a programmable logic controller (safety PLC), which is part of an information and control system designed for safe management of important technological processes. **The subject** of this study is the substantiation of the legality of reusing the results obtained during the development of the safety PLC in accordance with the requirements of functional safety to assess the level of its cyber security. **The purpose** of this work is to investigate the possibility of "cross" evaluation of the safety characteristics of the safety PLC, namely, the possibility of evaluating the level of cyber security of the programmable logic controller based on known data regarding its level of functional safety, in order to optimize the use of available resources in the project. **The study tasks** are following: to provide a theoretical basis for the relationship between safety PLC characteristics such as functional safety and cybersecurity. Determine the metrics by which it will be possible to assess the degree of reuse of existing results. Perform an analysis of potential cyberattacks depending on the architecture of the information and control system, which performs security functions, as well as on the possible modes of its use. Determine and evaluate the degree of "cross" influence of critical characteristics of the research object. To perform a calculation analysis of the potential

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

financial and time gain from the reuse of already known results for the minimum configuration of the safety PLC. **Conclusions**. The study demonstrated the relevance of the question of assessing the cybersecurity of a programmable logic controller based on the use of existing data, regarding its level of functional security (SIL). The proposed approach provides opportunities to significantly optimize the use of resources in safety PLC certification projects. However, the main methodological conclusion is that the well-known principle of Security Informed Safety can be developed and used in practice in the opposite direction, as Security supported/assessed by Safety. That is, to the principle of "assessment of functional safety taking into account/on information (cyber) security" the principle of "assessment of information (cyber) security with the support of/taking into account the results of the assessment of functional security" is added.

Keywords: safety PLC; functional safety; cybersecurity; vulnerability; failure: SIS; SAS.

Івасюк Олександр Олегович – канд. техн. наук, докторант каф. комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Харченко Вячеслав Сергійович – д-р техн. наук, проф., зав. каф. комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Oleksandr Ivasiuk – PhD, Doctor of Science Student of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: o.ivasiuk@csn.khai.edu, ORCID: 0009-0005-4354-4328, Scopus Author ID: 56426377300.

Vyacheslav Kharchenko – Doctor of Technical Science, Professor, Head of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: v.kharchenko@csn.khai.edu, ORCID: 0000-0001-5352-077X, Scopus Author ID: 22034616000.