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

УДК 004.02:004.38

doi: 10.32620/aktt.2025.2.10

О. О. ІВАСЮК, В. С. ХАРЧЕНКО

Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут»,

ПРИНЦИПИ ВЗАЄМНОЇ ІНФОРМОВАНОСТІ ПРИ АНАЛІЗІ ФУНКЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ НА ПРОГРАМОВАНИХ ЛОГІЧНИХ КОНТРОЛЕРАХ

Предметом *вивчення статті є такі властивості інформаційно-керуючих систем (ІКС), як функційна безпека (ФБ) і кібербезпека (КБ). У роботі досліджуються ФБ і КБ ІКС, які побудовані на основі цифрових програмованих логічних контролерів (ПЛК) і реалізують важливі для безпеки функції.* ***Метою*** *є розробка елементів методології аналізу КБ з урахуванням результатів оцінювання ФБ ПЛК-систем (ІКС, що базуються на ПЛК) для оптимізації витрат на такий аналіз.* ***Завдання:*** *аналіз ПЛК-систем, як об'єкта оцінювання ФБ і КБ; формулювання і доказ ключових положень концепції Safety Informed Security (SfISc); обговорення прикладів і меж застосовності сформульованих тверджень. Отримані такі* ***результати.*** *Запропоновано принцип трьох еквівалентностей і побудована узагальнена структурна схема його представлення. Сформульовано та доказано дві базові теореми, які встановлюють зв'язок між рівнем кібербезпеки ПЛК, у разі наявності відомостей про рівень його функціональної безпечності. На основі вперше доведених теорем була побудована основна модель станів ПЛК з рівнем функціональної безпечності SIL-3 у разі одиничної апаратної відмови та/або кібератаки. Доповнено існуючу онтологічну модель SISMECA, яка базується на принципі Security Informed Safety (ScISf). Проаналізовано відомий кіберінцидент, який відбувся з ПЛК-системою, у якої був високий рівень функціональної безпеки. Був оцінений на основі запропонованої концепції один з найімовірніший сценаріїв здійснення кібератаки на ПЛК в «онлайн» режимі.* ***Висновки.*** *Вперше, запропонована концепція взаємної інформованості функційної та кібербезпеки ІКС на основі ПЛК - SfISc. Сформульовані у роботі теоретичні постулати надають можливості проводити оцінку кібербезпеки ПЛК на основі вже здійсненої оцінки його функційної безпечності. Принцип SfISc може бути використаний в таких практичних випадках: у процесі ліцензування нової або модернізованої функційно безпечної ІКС; при визначенні рівня відповідності наявних систем, важливих для функційної безпечності новим вимогам з кібербезпеки; при формуванні вимог до функційно безпечної ІКС.*

Ключові слова: *інформаційно-керуючі системи; програмований логічний контролер; самодіагностування; кібербезпека; функційна безпечність; принцип трьох еквівалентностей; принципи ScISf-SfISc.*

Вступ

1.1. Мотивація

Тривалий час важливі для безпеки індустріальні інформаційно-керуючі системи (ІКС) вважалися не вразливими з точки зору кіберзагроз. Це пояснювалося їхньою ізольованістю та специфічністю засобів і умов для організації вторгнення. Однак, вірус Stuxnet на заводі зі збагачення урану «відкрив» нову еру кібератак - атаки на спеціалізовані програмовані логічні контролери (ПЛК). Зокрема, вірус, виявлений у ІКС АЕС Бушер, став причиною одного з перших серйозних кіберінцидентів, низка яких продовжилася [1, 2].

Ці та інші епізоди, пов'язані з критичною інфраструктурою, сформували широкий дискурс щодо такої концепції як Security Informed Safety (ScISf) [3]. Одним із її родоначальників вважається професор Robin Bloomfield. Основні положення цієї концепції представлені в багатьох наукових роботах, наприклад, [4, 5]. Ключова ідея концепції полягає в необхідності врахування ризиків порушення інформаційної та кібербезпеки (КБ) під час аналізу функційної безпечності (ФБ) системи, оскільки вона була і залишається ключовою властивістю критичних ІКС. На основі цієї концепції було випущено стандарти та нормативні документи [6,7].

У 2024 році US NRC (Nuclear Regulatory Committee) розробив Cybersecurity Audits Alongside a Digital Instrumentation and Controls Licensing Review, де розглядаються підходи щодо ліцензування

цифрових систем управління, не лише шляхом оцінки аспектів ФБ, але й так званих кіберзахисних функцій. Як наслідок, у документі пропонується підхід до ліцензування системи, в основі якого лежить ідея про паралельний процес оцінювання рівня функціональної безпеки системи та її стійкості до кіберзагроз [8]. Однак, досі взаємозв'язок процесів оцінювання ФБ та КБ був дорогою з «одностороннім рухом» і аспекти впливу ФБ на КБ практично не розглядалися. На цю обставину було звернено увагу в роботі [9] та проілюстровано можливість і доцільність аналізу такого впливу.

Тому, питання розроблення єдиної концепції аналізу, оцінювання та забезпечення функційної безпечності та кібербезпеки ІКС є актуальною наукового-практичною проблемою.

1.2. Аналіз публікацій

Тема взаємного зв'язку ФБ і КБ під різними кутами аналізується в багатьох роботах. Водночас варто зазначити, що такий взаємозв'язок здебільшого розглядають з точки зору впливу КБ на забезпечення ФБ.

Наприклад, у роботі [10] аналізується вплив КБ на ФБ ПЛК, який будується з використанням FPGA. В основі такої оцінки лежить методологія оцінки ФБ, що базується на спільному використанні методів аналізу безпеки (GAP-аналіз та аналіз режимів вторгнення, ефектів і критичності IMECA), а також їхньому відображенні на підсумковій картині оцінки безпеки системи з двома каналами. Ця методологія формує так званий підхід до забезпечення ФБ на основі КБ (принцип ScISf).

У [11, 12] розглядаються питання оцінювання ризиків кібербезпеки індустріальних систем управління, а також роль міжнародних стандартів у виконанні такої активності. Обговорюється важливість питань інтеграції ФБ і КБ в індустріальних системах управління. Зокрема, це аргументується тим, що в основі забезпечення ФБ і КБ лежить однаковий підхід, який базується на аналізі ризиків.

Питанням порівняльного аналізу ФБ і КБ присвячено звіт [13]. Цей звіт є результатом досліджень, спрямованих на вивчення того, як кібербезпека і функціональна безпека взаємодіють у контексті сучасних ІКС. Проведено оцінку основних схожих аспектів і відмінностей у забезпеченні ФБ і КБ. У результаті дослідження робиться висновок про те, що інтеграція в забезпеченні ФБ і КБ може значно підвищити стійкість систем до різних типів загроз. До аналогічних результатів і висновків добігає робота [14, 15]. У [16] подано рекомендації щодо розгляду та імплементації вимог із забезпечення КБ протягом так званого життєвого циклу функціональної безпеки.

У роботі [17] проаналізовано проблеми кібербезпеки АЕС і можливі катастрофічні наслідки в разі успішної кібератаки. Автори підкреслюють відсутність комплексної системи інформаційної безпеки для захисту АЕС від внутрішніх і зовнішніх загроз. У статті представлено аналіз кіберінцидентів, ініціатив урядів та регуляторних органів, а також запропоновано модель загроз для систем управління та контролю АЕС. Дослідження показує, що АЕС недостатньо захищені від кібератак, і обґрунтовує необхідність проведення детальних оцінок загроз і вразливостей, включно з аналізом ризиків інформаційної безпеки.

Питанням захисту ІКС АЕС від кібератак також присвячено матеріал у [18]. Автори наголошують на необхідності оцінювання безпеки таких систем і пропонують методологію для аналізу наслідків кіберінцидентів, засновану на «ефекто-орієнтованому» підході. Методологію застосовують для аналізу історичних та гіпотетичних атак з метою розроблення ефективних заходів захисту. Стаття акцентує увагу на подоланні розриву між питаннями кібербезпеки та безпеки АЕС, що є ключовим завданням для всіх зацікавлених сторін.

У 2017 році на конференції S4x17 (Smart Grid Security Summit) пан Нігел Стенлі, CTO Operational Technology and Industrial Cybersecurity в TÜV Rheinland, виступив із доповіддю «Functional Safety Meets Cybersecurity», у якій обговорено необхідність інтеграції функціональної безпеки та кібербезпеки в промислових системах, зокрема й атомних електростанціях. У доповіді обговорюються ризики, пов'язані з кібератаками на критично важливі об'єкти, і підкреслюється необхідність спільного підходу до забезпечення як безпеки процесів (functional safety), так і захисту від кіберзагроз [15, 19].

У [16, 20] проводиться дослідження найпоширеніших кіберзагроз із застосуванням структури MITRE ATT&CK для індустріальних ІКС. Проводиться аналіз різних варіантів архітектури систем управління з урахуванням задоволення вимог щодо функційної безпечності. Головна ідея статті – це побудова системи управління з використанням методу, заснованого на врахуванні потенційних кіберзагроз.

Аналіз відомих джерел свідчить про те, що в них акцентуються на різних аспектах розвитку та імплементації принципу ScISf. Публікації, присвячені аналізу та забезпеченню кібербезпеки індустріальних систем управління, зокрема ІКС АЕС, жодним чином не враховують той факт, що ФБ може певним чином, опосередковано впливати на КБ, або

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

те, що результати її аналізу можуть бути використані для оцінювання кібербезпеки. Перші публікації [9, 21], в яких автори цієї роботи аналізують такі можливості та відповідні приклади, не дають методологічного обґрунтування подібних фактів та потенційних закономірностей для ІКС певного класу. Саме, закриттю цієї методологічної прогалини і присвячена ця стаття.

1.3. Задачі і методологія дослідження

Метою цієї статті є розроблення елементів методології аналізу КБ з урахуванням результатів оцінювання ФБ ПЛК-систем (ІКС, що базуються на ПЛК, PLC-based I&C) для оптимізації витрат на такий аналіз. Задачі дослідження:

– аналіз ПЛК-систем як об'єкта оцінювання ФБ і КБ;

– формулювання і доказ ключових положень концепції Safety Informed Security (SfISc);

– обговорення прикладів і меж застосовності сформульованих тверджень.

Статтю структуровано наступним чином: спочатку аналізуються особливості ІКС, важливої для безпеки як об'єкта дослідження, поняття ФБ та КБ для ІКС; далі формулюється концепція SfISc та принцип трьох еквівалентностей під час аналізу ФБ і КБ; у наступному розділі обговорюється, як формуються кібератаки на ПЛК-систему; наступний розділ включає формулювання двох теорем, що визначають сутність і умови реалізації концепції SfISc; далі аналізуються приклади того, як можуть бути застосовані на практиці елементи концепції: фінальні розділи обговорюють онтологію процедур аналізу безпеки, висновки та напрямки подальших досліджень.

1.4. Об'єкт і предмет дослідження

Об'єктом дослідження є ПЛК (safety critical PLC), які є ключовим елементом для побудови важливих для безпеки систем керування (safety critical I&C) [9]. Предметом дослідження є процес оцінювання властивостей кібербезпеки та функційної безпечності ПЛК, який відповідає таким параметрам:

– функційну безпечність оцінено за стандартом IEC 61508 на рівні SIL-3;

– відсутність двонаправлених онлайн-інтерфейсів передачі даних;

– побудова з'єднання тільки за правилом точка - точка;

– відсутність інтерфейсів для підключення сторонніх носіїв інформації;

– використання протоколів передачі даних власної розробки;

– відсутність використання програмного забезпечення третьої сторони;

– відсутність бездротових інтерфейсів.

Прикладом такого ПЛК може слугувати Teleperm XS Compact компанії Framatome [22].

2. Початкові умови

Розглянемо safety ІКС, ядром якої є safety PLC, і яка перебуває у стані виконання функцій безпеки («online»).

Системи безпеки мають свої особливості, виражені в тому, що вони складаються з декількох резервних каналів, які здійснюють одночасне приймання, оброблення, формування та видавання сигналів керування на виконавчі механізми, а також інформаційні сигнали в інші системи [21, 22].

Усі цифрові інтерфейси safety system, через які цифрова інформація може потрапити в логіку застосунку системи, є інтерфейсами ПЛК. Під логікою застосунку розуміється спосіб формування команд ПЛК на виконавче обладнання відповідно до алгоритмів керування, описаних у технічній специфікації до системи. У ПЛК є внутрішні інтерфейси (під'єднання модулів, завантаження прошивки) і зовнішні інтерфейси для зв'язку з іншими ПЛК і периферійним обладнанням.

Усі інтерфейси, включно із зовнішніми, відносяться до настроюваного і постійно контрольованого ПЛК рівня апаратної конфігурації. Тому, безліч зовнішніх довірених підключень до ПЛК будемо називати валідним кіберпростором ПЛК. Схематично це представлено на рисунку 1.

Проаналізуємо шлях, яким цифрова інформація рухається в ПЛК.

Для того щоб цифрова інформація потрапила до ПЛК, до нього має бути здійснено фізичне під’єднання. Об'єктом, що під’єднується, може бути елемент із валідного кіберпростору, такий як: ПЛК з іншого каналу системи; інженерна станція; комутатор або несанкціоноване підключення. Щоб інформація була передана каналами передачі, вона має бути представлена у форматі пакета даних, які циркулюють у ПЛК. У такому форматі інформація може бути доставлена в логіку програми. Інформація, що циркулює на цьому рівні, доступна алгоритмам управління і впливає на генерацію команд, як ручних (оператором), так і автоматичних (алгоритмами управління). Етапи проходження (циркуляції) цифрової інформації в ПЛК наведено на рисунку 2.

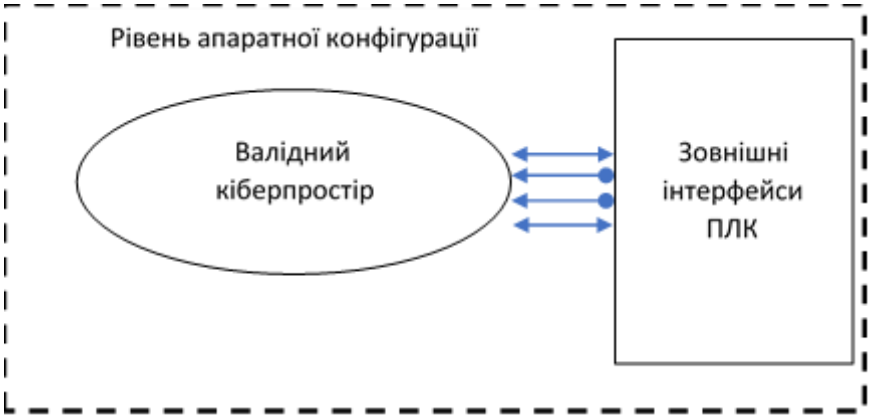

Рис. 1. Узагальнена схема інтерфейсних підключень апаратного рівня ПЛК

Рис. 2. Діаграма циркуляції цифрової інформації в ПЛК

З аналізу діаграми (див. рис. 2) можна зробити наступні висновки:

– датчики і виконавчі механізми не належать до джерел і одержувачів цифрової інформації;

– кожен рівень має зв'язок тільки із сусіднім;

– для потрапляння на рівень логіки застосунку інформація має успішно пройти два попередні рівні.

2.1. Визначення кібербезпеки та функціональної безпеки ПЛК

Функціональна безпека ПЛК – це комплексна властивість, що визначається здатністю мінімізувати ризики переходу і наслідків переходу системи в небезпечний стан. ФБ ПЛК характеризується:

– заданим рівнем надійності;

– певною повнотою (ступенем охоплення) самодіагностування;

– переходом у безпечний стан у разі виникнення і виявлення критичної одиничної випадкової апаратної відмови.

Кібербезпека ПЛК – властивість, яка забезпечується набором програмно-технічних механізмів захисту від несанкціонованого впливу, який може вплинути на:

– цілісність цифрової інформації, що циркулює через ПЛК;

– доступність ПЛК для виконання функцій за запитом;

– неавторизований вплив на роботу (зміна параметрів логіки застосунку).

Окремо слід зазначити, що кібербезпечний ПЛК повинен мати таку можливість як автоматичне застосування пом'якшувальної дії при виявленні атаки на нього.

2.2. Концепція SfInSc і принцип трьох еквівалентностей

Концепція ScISf базується на положеннях про те, що:

а) кібератаки або інші неспецифіковані втручання можуть призвести до неприйнятного порушення цілісності даних або блокування виконання функцій управління технологічними процесами;

б) аналіз ризиків таких атак з погляду їхнього впливу на безпеку має проводитися так само, як і аналіз наслідків будь-яких відмов, що традиційно проводиться під час аналізу ФБ;

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

в) методики оцінювання впливу ФБ на КБ повинні забезпечувати повноту та достовірність результатів і базуватися на достатній інформації та наборі інструментів аналізу.

В основі концепції SfInSc знаходиться гіпотеза про те, що випадкову одиничну апаратну відмову, пов'язану з інтерфейсами передавання даних, і спробу порушення встановленої апаратної конфігурації ПЛК, який працює, система самодіагностування ПЛК сприйматиме однаково. Система самодіагностування зафіксує розбіжність між очікуваним значенням контрольованого параметра й отриманим. Однак, самого факту виявлення спроби несанкціонованого підключення може бути недостатньо для запобігання імовірним негативним наслідкам кібератаки. Для того, щоб звести негативні наслідки до мінімуму, ПЛК має автоматично вжити заходи щодо зниження ризику – перейти у відповідний безпечний стан. Таким чином, ПЛК, що працює в «онлайн» режимі, має явні властивості кібербезпеки, які базуються на принципі трьох еквівалентностей, що є основою концепції SfISc (рисунок 3):

а) еквівалентності наслідків небезпечних відмов і кібератак (інформаційних вторгнень);

б) еквівалентному сприйняттю таких наслідків, обумовлених КБ, засобами самодіагностування, від самого початку орієнтованими на підтримку ФБ у повній відповідності з вимогами до ФБ;

в) еквівалентних діях (контрзаходах), пов'язаних із переведенням ПЛК у захисний стан.

2.3. Аналіз кібератак на ПЛК

Приймемо, що атака з боку зловмисника може бути або «позитивним», або «негативним» впливом, за аналогією з тестуванням.

Під кібератакою через «позитивний» вплив вважається дія, спрямована на підключення до системи. Валідний кіберпростір порушується шляхом здійснення підключення у «вільний» інтерфейс.

Під кібератакою через «негативний» вплив вважається дія, що порушує будь-що в існуючих підключеннях. Наприклад, від'єднання каналу передачі даних, вимкнення ПЛК реципієнта або вилучення з ПЛК одного юніта (модуля або карти).

Зловмисник може здійснити атаку на ІКС (ПЛК) на таких рівнях:

Рівень апаратної конфігурації (1-й рівень):

Зловмисник повинен здійснити «позитивний» або «негативний» вплив на апаратний рівень ІКС, а саме на ПЛК. Тобто змінити апаратну конфігурацію, зазначену файлами налаштування та відповідним набором апаратних засобів.

Атака проявляється в реальному фізичному впливі на систему. Наприклад, під'єднання до інтерфейсу через наявний порт/слот, але не використовуваний у поточній апаратній конфігурації. Можливий інший варіант – через вимкнення кабелю або модуля.

Пакетний рівень (2-й рівень):

Якщо зловмисник успішно подолав рівень апаратної конфігурації, і система не виявила її порушення, у такому разі він може або порушити передачу валідних пакетів у каналі, або передавати «свої» пакети, але без корисної інформації (DDoS). Для цього йому треба знати форму пакетів і таймінги (робочий цикл), тобто протокол передачі даних.

Інформаційний (смисловий) рівень (3-й рівень):

Якщо зловмисник успішно під'єднався до системи фізично і може формувати валідний, з погляду системи, пакет і передавати у відповідні часові проміжки, то він може сформувати валідну, з погляду системи, команду і «нав'язати» її для виконання.

Узагальнений вигляд ієрархії або захисту в глибину від кібератаки за умови фізичного доступу до системи для описаних вище рівнів показано на рисунку 4.

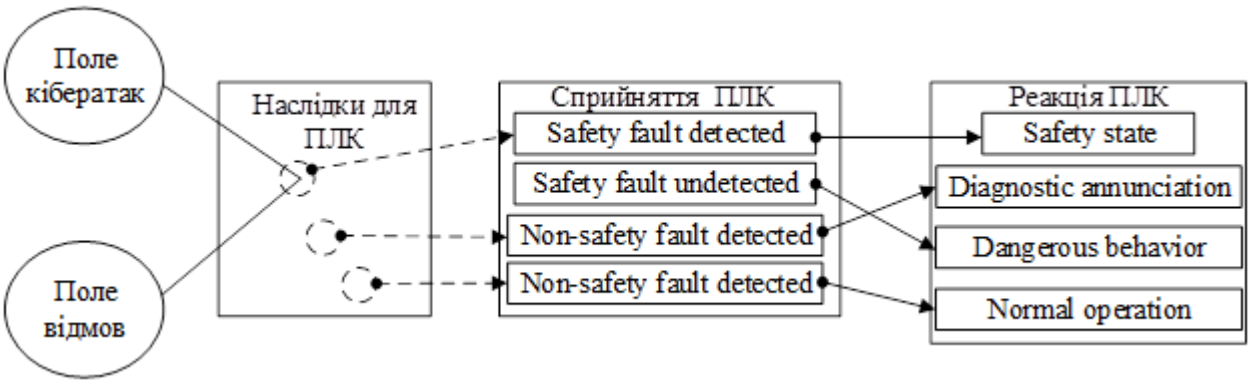

Рис. 3 Узагальнена структурна схема реалізації принципу 3-х еквівалентностей

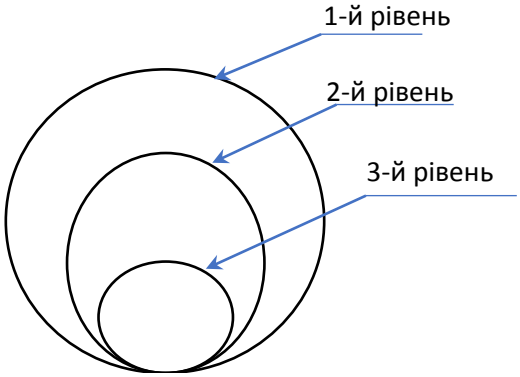

Рис. 4. Ієрархія рівнів (ієрархія атак на ІКС)

3. Ключові теореми

На основі поданої вище інформації сформулюємо і доведемо такі дві теореми.

Теорема 1. Несанкціоноване подолання рівня апаратної конфігурації safety PLC в «online» режимі є необхідною умовою успішного проведення кібератаки.

Примітка: подолання вважається успішним у тому разі, якщо воно не було виявлено засобами ПЛК.

Доведення

Несанкціонований доступ на рівні апаратної конфігурації може вплинути або на цілісність циркулюючої інформації, або на доступність ПЛК для виконання функцій за запитом.

Для порушення цілісності даних і доступності ПЛК необхідно, щоб через здійснене підключення стався збій у роботі логіки застосунку У такому разі, ПЛК не виконає функцію за запитом. Є такі шляхи досягнення цієї мети:

– заміна одного з юнітів (модулів) ПЛК на юніт (модуль) зловмисника (наслідок –ПЛК стане недоступним);

– вплив на параметри виконуваної логіки застосунку (ПЛК буде доступним, але не виконає функцію за запитом);

– розрив, під'єднання (man-in the - middle) або помилкове перепідключення встановленого апаратною конфігурацією цифрового інтерфейсу (порушення цілісності даних, переданих у каналі).

Перелічені вище випадки можуть бути здійснені тільки за умови, що зловмисник успішно подолав рівень апаратної конфігурації.

Варто також зазначити, що в «online» режимі у ПЛК можуть бути не задіяні інтерфейси, що враховується апаратною конфігурацією ПЛК. Тому й атака через них не буде успішною, оскільки дані, які можуть бути теоретично передані через них, не обробляються ПЛК.

Теорема 2. Рівень кібербезпеки ПЛК тим вищий, чим вищий рівень його функціональної безпеки.

Доведення

Рівень апаратної конфігурації відноситься до апаратної складової ПЛК. До цього рівня належать модулі (юніти), з яких складається ПЛК, а безпосередньо на модулі до нього відносяться всі елементи, на яких реалізовується схемотехніка модуля (юніта). Тобто множина інтерфейсів, через які здійснюється під'єднання модуля до ПЛК або до іншої системи є підмножиною всіх елементів модуля.

Якщо в ПЛК застосовується механізм для своєчасного детектування одиничної випадкової відмови в кожному з його модулів, це означає, що здійснюється постійна онлайн верифікація правильності роботи кожного з його вузлів, згідно зі встановленою апаратною конфігурацією ПЛК.

Серед множини інтерфейсів ПЛК, з погляду кіберпростору, до таких належать цифрові інтерфейси (двонаправлені або односпрямовані) (рис. 1). Іншими словами, множина інформаційних інтерфейсів ПЛК, через які інформація потрапляє в ПЛК, є підмножиною множини всіх вузлів модуля (юніта) або ПЛК відповідно.

Як було сказано вище, функційно безпечні ПЛК, які оцінено відповідно до вимог стандарту IEC 61508, наприклад, на рівні SIL-3, мають 99% безпечних відмов. Це, своєю чергою, означає, що самодіагностування модуля має повноту охоплення понад 99% усіх можливих випадкових апаратних відмов. Тобто будь-яке відхилення в роботі вузла модуля від поведінки, заданої апаратною конфігурацією, буде детектуватись системою самодіагностування ПЛК.

З іншого боку, чим менший рівень функційної безпечності ПЛК, тим менший відсоток безпечних відмов має забезпечувати пристрій і тим менша глибина його самодіагностування. Це означає, що в разі виникнення відмови ймовірність того, що її буде

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

виявлено і ПЛК автоматично застосує заходи щодо зниження імовірних негативних наслідків, буде також знижуватися.

Наприклад, охоплення самодіагностуванням для рівня SIL-1 визначається щонайменше 60%, а для відповідності рівню SIL-2 пристрій повинен мати рівень самодігностування щонайменше 90%.

Розглянемо модель станів ПЛК у разі виникнення відмови або кібератаки на його рівень апаратної конфігурації (рисунок 5).

У цій моделі можна виділити три зони. Перша зона характеризує порушення на апаратному рівні. За відсутності або часткового покриття самодіагностуванням із зони 1 з різними інтенсивностями відбуватимуться переходи в зони 2 і 3 відповідно. Ці інтенсивності для другої зони залежать від ймовірності виявлення відмови елементної бази ПЛК, а для третьої зони - від ймовірності виявлення факту проникнення в ПЛК.

Для функційно безпечного ПЛК ця модель має такий вигляд (рис. 6).

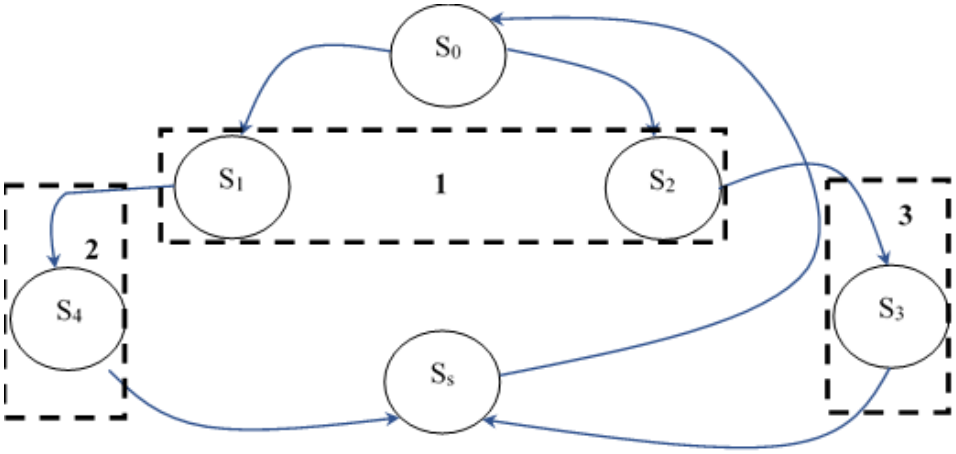

Рис. 5. Узагальнена модель станів ПЛК у разі одиничної апаратної відмови і\ або кібератаки:
S_0 – справний стан без кібератак і апаратних відмов; S_1 - стан системи, коли сталася одинична відмова; S_2 – стан системи, коли сталася кібератака на апаратний рівень; S_3 – стан системи, коли кібератака успішно реалізована і не задетектована; S_4 – стан системи, коли апаратна відмова не задетектована; Ss – безпечний стан системи, у який вона переходить після того, як факт атаки було виявлено або було виявлено факт апаратної відмови

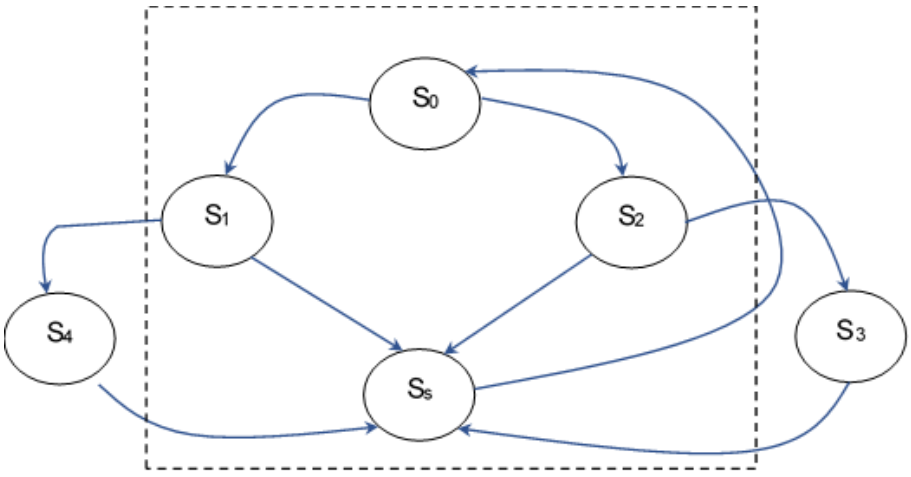

Рис. 6. Модель станів ПЛК рівня ФБ SIL-3 у разі одиничної апаратної відмови та/або кібератаки:
S_0 – система у справному стані без кібератаки та апаратних відмов; S_1 – стан системи, коли одинична відмова сталася; S_2 – стан системи, коли відбувається кібератака на апаратний рівень; S_3 – стан системи, коли кібератака успішно реалізована і недетектована; S_4 – стан системи, коли апаратна відмова не детектована; Ss – безпечний стан системи, у якому система перебуває після того, як факт атаки було виявлено або було виявлено факт апаратної відмови

Ця модель відрізняється від моделі на рис.5 наявністю зв'язків між станами S1 і Ss, а також S2 і Ss, які з'являються через наявність глибокого рівня самодіагностичного покриття. Фактично, модель рисунку 5 трансформується в ту її частину, яка позначена пунктирною лінією. Ймовірність переходу в стани S3 і S4 зворотно залежить від рівня самодіагностичного охоплення ПЛК, однак, вона не дорівнює 0.

4. Приклади та обговорення результатів

4.1 Практичний case застосування запропонованих теоретичних положень

Розглянемо атаку на safety ПЛК в «онлайн» режимі, коли зловмисник хоче зробити заміну одного з працездатних штатних модулів на «заражений». Заміна модуля в ПЛК – це досить поширена функція індустріальних контролерів, яка називається «hot swappable». Аналіз цього випадку виконаємо з точки зору принципу трьох еквівалентностей. Атака – видалення валідного модуля з ПЛК. **Наслідок** для ПЛК – відсутність зв'язку між логікою застосунку і модулем з апаратної конфігурації. **Сприйняття** ПЛК – виникнення критичної відмови. **Реакція** ПЛК – перехід у безпечний стан. Подібні наслідки для ПЛК можуть наставати в разі відмови в блоці прийомо-передавача модуля ПЛК або порушення фізичної лінії зв'язку між модулями.

У 2017 році була здійснена атака цифрових ПЛК Triconex компанії Schneider зловмисним програмним забезпеченням (ПЗ) TRITON [23, 24]. Дані ПЛК мають рівень функціональної безпеки SIL-3. Незважаючи на те, що атака була проведена в «офлайн» режимі, а її аналіз виконано з точки зору кібербезпеки побудови промислових комп'ютерних мереж, спробуємо проаналізувати цей випадок з точки зору принципу трьох еквівалентностей [25]. Отже, ПЛК в «офлайн» режимі отримав зловмисне ПЗ. При подачі живлення на ПЛК починається фаза ініціалізації – підготовки до роботи. Під час цієї фази ПЛК Triconex перейшов у безпечний стан. Ключовий момент полягає в тому, що факт атаки на ПЛК був виявлений вже після того, як ПЛК перейшов у безпечний стан і зупинив увесь технологічний процес. Таким чином:

– **атака** – завантаження зловмисного ПЗ;

– **наслідки** для ПЛК – завантажене ПЗ не відповідає апаратній конфігурації;

– **сприйняття** ПЛК – система самодіагностики ПЛК фіксує виникнення критичного відмови;

– **реакція** ПЛК – перехід у безпечний стан після завершення фази ініціалізації.

Можна припустити, що система самодіагностування сприйняла зловмисне ПЗ як відмову регістрів пам’яті контролера, і тому функція CRC, обчислена для зловмисного ПЗ, не співпала з очікуваною. Оскільки ПЛК Triconex має потрійне резервування логіки застосунку, також, можливий варіант невідповідності зловмисного ПЗ з валідним, яке було завантажене в два резервних модулі логіки застосунку.

4.2. Дискусія

Чи достатньо наявності засобів кіберзахисту у safety PLC, щоб вважати, що вся система ICS буде кіберзахищеною? Відповідь на це питання – негативна з таких причин. ПЛК-система складається не лише з ПЛК; одним з основних її компонентів та важливим цифровим активом є інженерна станція. Тому, незважаючи на те, що ПЛК з глибокою системою самодіагностики мають "розумний" рівень кіберзахисту, це не виключає паралельного застосування комплексних організаційно-технічних засобів забезпечення кібербезпеки ПЛК-системи.

Яке місце в загальному сімействі різних процедур (методик) аналізу ФБ і КБ, представлених онтологічною моделлю в [26], займає аналіз SfISc? На основі аналізу SfISc можна виконати такі аналізи кібербезпеки ПЛК, як SfIScMECA і SfIScMEDA. Ці аналізи можуть бути застосовані для виконання аналізу видів ScMECA і ScMEDA, взаємозв’язки яких представлено на рисунку 7.

Варто зазначити, що для забезпечення повноти онтологічної моделі, представленої в [26], необхідно додати такий вид аналізу як SafMEDA, до якого, в свою чергу, входитимуть FMEDA та ScISfMEDA. Однак, розгляд цього напряму розвитку онтологічної моделі SISMECA виходить за рамки цієї статті.

5. Висновки

Запропонована концепція взаємної інформо-ваності функційної та кібербезпеки ІКС на основі ПЛК будується на двох взаємодоповнюючих принципах ScISf і SfISc. Часто, складнощі, пов'язані зі значними фінансовими та часовими ресурсами для оцінювання властивостей нової або модернізованої safety ІКС з боку регулюючих органів, стають перешкодою для вкладення інвестицій з боку бізнесу, а отже, не реалізується формула: вкладення коштів у безпеку − це не додаткові витрати, а інновації.

Саме такий принцип як ScISf та його, на думку авторів, природне продовження - принцип SfISc, спрямовані на трансформацію процесу оцінювання в

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

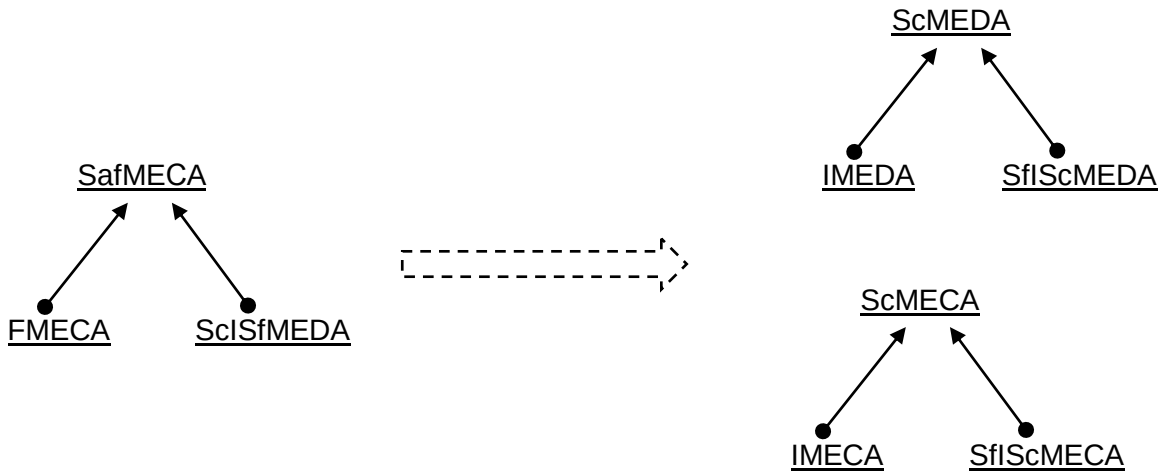

Рис. 7. Розвиток онтологічної моделі SISMECA

бік зменшення затрачуваних ресурсів при збереженні необхідного рівня захисту та надійності safety ІКС. Принцип SfISc, якому було надано основну увагу в статті, може бути використаний в таких практичних випадках:

– у процесі ліцензування нової або модернізованої функційно безпечної ІКС;

– при визначенні рівня відповідності наявних систем, важливих для функційної безпечності новим вимогам з кібербезпеки;

– при формуванні вимог до функційно безпечної ІКС.

Також, варто зазначити, що зловмисники не мають ні регуляторних, ні будь-яких інших обмежень, у той час як у більшості випадків стратегія забезпечення кібербезпеки націлена на протидію вже "відомим", іншими словами "минулим", атакам. Тому, своєчасність впровадження нових або оновлення існуючих систем керування безпекою набуває важливого значення.

Подальшим продовженням наукових досліджень, що розвиває запропоновану в статті концепцію, є розроблення процедур тестування системи самодіагностування функційно безпечного ПЛК, яка перевірятиме її здатність виявляти як апаратні відмови, так і кібератаки на його активи.

Внесок авторів: зробив розробку теоретичних положень концепції Safety Informed Security – **О. О. Івасюк**; запропонував логічну структуру побудови запропонованих теоретичних положень і здійснив аналіз щодо узгодженості нової концепції вже існуючим – **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. *Baezner, M. Hotspot Analysis: Stuxnet. Center for Security Studies (CSS) [Text] / M. Baezner, & P. Robin. – ETH Zürich, 2017. – 15 p.*

2. *Mohee, A. A Realistic Analysis of the Stuxnet Cyber-attack [Text] / A. Mohee. – MA Arabic Studies – Political Sciences, Cairo March 2022. – 11 p. DOI: 10.33774/apsa-2022-qs797.*

3. *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.*

4. *Bloomfield, R. Security Informed Safety. Why It's Easy, Why It's Hard. Adelard LLP [Text] / R. Bloomfield. – City, University of London, 2019.*

5. *Bloomfield, R. Impact of security on safety. Body of Knowledge 1.4 – cross-domain practical*

guidance. Adelard LLP [Text] / R Bloomfield, P. Bishop, & G. Fletcher. – University of York, 2020.

6. *National Protective Security Authority. Code of Practice for railways security informed safety – Available https://www.npsa.gov.uk/system/files/documents/npsa-rail-code-practice-security-informed-safety.pdf. (accessed 11.12.2024).*

7. *The British Standards Institution. Connected automotive ecosystems – Impact of security on safety – Code of practice. Revision PAS 11281:2018. 2018.*

8. *U.S. Nuclear Regulatory Commission. Cybersecurity Audits Alongside a Digital Instrumentation and Controls Licensing Review, Revision RIL 2024-09. May 2024.*

9. *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.*

10. *Security Informed Safety Assessment of Industrial FPGA-Based Systems [Text] / V. Kharchenko, O. Illiashenko, E. Brezhnev, A. Boyarchuk, & V. Golovanevskiy // Probabilistic Safety Assessment and Management PSAM, 2014. – Vol. 12. – Honolulu, Hawaii.*

11. *Shikhaliyev, R. Cybersecurity risks management of industrial control systems: A review [Text] / R. Shikhaliyev // Problems of Information Technology. – 2024. – Vol. 15, no. 1. – P. 37-43.*

12. *Kosmowski, K. Systems engineering approach to functional safety and cyber security of industrial critical installations [Text] / K. Kosmowski // Safety and Reliability of Systems and Processes, Summer Safety and Reliability Seminar 2020. – Gdynia Maritime University. P. 135 – 151.*

13. *Comparison of cybersecurity and functional safety risk assessments [Text] / T. Malm, J. Berger, R. Tiusanen, A. Ranta, J. Seppälä, B. Silverajan, & H. Zhao // Research Report VTT-R-00499-24. – VTT Technical Research Centre of Finland, 2024.*

14. *Spiteller, F. Dependencies Standards Pragmatic approaches [Text] / F. Spiteller // Seminar "Functional Safety and Validation". – Pune, 2023.*

15. *Oliveira, P. Functional Safety and Cybersecurity [Text] / P. Oliveira // FSCySec T65 Symposium. – DEKRA, 2024.*

16. *The 61508 Association Guide of Compliance. Considerations for Cybersecurity during the Functional Safety Lifecycle. Version 1 [Text] – 2020. – 16 p.*

17. *Masood, R. Assessment of Cyber Security Challenges in Nuclear Power Plants Security Incidents, Threats, and Initiatives. [Text] / R. Masood // Current Affiliation: National University of Sciences & Technology (NUST). Report GW-CSPRI-2016-03. – 2016.*

18. *Choi, J.-S. An Effect-Centric Approach to Assessing the Risks of Cyber Attacks Against the Digital Instrumentation and Control Systems at Nuclear Power Plants [Text] / J.-S. Choi, N. Gallagher, & C. Harry. – Center for International and Security Studies at Maryland. CISSM Working Paper. – 2020.*

19. *Stanley, N. Functional Safety Meets Cybersecurity [Text] / N. Stanley // Smart Grid Security Summit. Miami, USA. – 2017.*

20. *Srinivasan, H. Threat-based security controls to protect industrial control systems [Text] / H. Srinivasan, & M. Karimi // Cryptography and Security Cornell University. Ithaca, USA, 2025. – 10 p.*

21. *Івасюк, О. Використання методу верифікації FMEDA/FIT для оцінювання кібербезпеки програмовного логічного контролера: нова інтерпретація принципу SIS [Текст] / О. Івасюк, & В. Харченко // Авіаційно-космічна техніка і технологія. – 2024. – № 1(193). – С. 76-90. DOI: 10.32620/aktt.2024.1.07.*

22. *TXS Compact Platform Topical Report. NRC/Framatome Phase "0" Meeting [Text]. – Framatome, 2024. – Available at: https://www.nrc.gov/docs/ML2419/ML24193A231.pdf. (accessed 12.12.2024).*

23. *How Does Triton Attack Triconex Industrial Safety Systems? // Cisco Blogs IoT Security Research Lab, 2021. – Available at: https://blogs.cisco.com/security/how-does-triton-attack-triconex-industrial-safety-systems. (accessed 12.12.2024).*

24. *How Does Triton Attack Triconex Industrial Safety Systems? – Glocomp, 2020. – Available at: https://www.glocomp.com/how-does-triton-attack-triconex-industrial-safety-systems. (accessed 12.12.2024).*

25. *Analyzing the TRITON industrial malware. – Midnight Blue, 2018. – Available at: https://www.midnightblue.nl/blog/analyzing-the-triton-industrial-malware. (accessed 12.12.2024).*

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 Giandomenico // Entropy. – 2023. – Vol. 25, iss. 8. – Article No. 1123. – 35 p. – DOI: 10.3390/e25081123.*

References

1. Baezner M., & Robin P. *Hotspot Analysis: Stuxnet. Center for Security Studies (CSS*), ETH Zürich, 2017. 15 p.

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

2. Mohee, A. *A Realistic Analysis of the Stuxnet Cyber-attack*. MA Arabic Studies – Political Sciences, Cairo March 2022. 11 p. DOI: 10.33774/apsa-2022-qs797.

3. 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.

4. Bloomfield, R. *Security Informed Safety. Why It's Easy, Why It's Hard. Adelard LLP*. City, University of London, 2019.

5. Bloomfield, R., Bishop P., & Fletcher G. *Impact of security on safety. Body of Knowledge 1.4 – cross-domain practical guidance. Adelard LLP*. University of York, 2020.

6. *National Protective Security Authority. Code of Practice for railways security informed safety*. Available https://www.npsa.gov.uk/system/files/documents/npsa-rail-code-practice-security-informed-safety.pdf. (accessed 11.12.2024).

7. *The British Standards Institution. Connected automotive ecosystems – Impact of security on safety – Code of practice*. Revision PAS 11281:2018. 2018.

8. *U.S. Nuclear Regulatory Commission. Cybersecurity Audits Alongside a Digital Instrumentation and Controls Licensing Review*, Revision RIL 2024-09. May 2024.

9. 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).

10. Kharchenko, V. Illiashenko, O., Brezhnev, E., Boyarchuk, A., & Golovanevskiy, V. Security Informed Safety Assessment of Industrial FPGA-Based Systems. *Probabilistic Safety Assessment and Management PSAM*, 2014, vol. 12. Honolulu, Hawaii.

11. Shikhaliyev, R. Cybersecurity risks management of industrial control systems: A review. *Problems of Information Technology*, 2024, vol. 15, no. 1, pp. 37-43.

12. Kosmowski. K. Systems engineering approach to functional safety and cyber security of industrial critical installations. *Safety and Reliability of Systems and Processes, Summer Safety and Reliability Seminar 2020*, Gdynia Maritime University, 2020, pp. 135-151.

13. Malm, T., Berger, J., Tiusanen, R., Ranta, A., Seppälä, J., Silverajan, B., & Zhao, H. Comparison of cybersecurity and functional safety risk assessments. *Research Report VTT-R-00499-24*, VTT Technical Research Centre of Finland, 2024.

14. Spiteller, F. Dependencies Standards Pragmatic approaches. *Seminar "Functional Safety and Validation"*, Pune, 2023.

15. Oliveira, P. Functional Safety and Cybersecurity. *FSCySec T65 Symposium*, DEKRA. 2024.

16. *The 61508 Association Guide of Compliance. Considerations for Cybersecurity during the Functional Safety Lifecycle, Version 1*, 2020. 16 p.

17. Masood, R. Assessment of Cyber Security Challenges in Nuclear Power Plants Security Incidents, Threats, and Initiatives. *Current Affiliation: National University of Sciences & Technology (NUST). Report GW-CSPRI-2016-03. 2016.*

18. Choi, J-S., Gallagher, N., Harry, C. *An Effect-Centric Approach to Assessing the Risks of Cyber Attacks Against the Digital Instrumentation and Control Systems at Nuclear Power Plants*. Center for International and Security Studies at Maryland. CISSM Working Paper. 2020.

19. Stanley, N. Functional Safety Meets Cybersecurity. *Smart Grid Security Summit*. Miami, USA. 2017.

20. Srinivasan H., Karimi M., Threat-based security controls to protect industrial control systems. *Cryptography and Security Cornell University*, Ithaca, USA, 2025. 10 p.

21. Ivasyuk, O., & Kharchenko, V. Vykorystannya metodu veryfikatsiyi FMEDA/FIT dlya otsinyuvannya kiberbezpeky prohramovnoho lohichnoho kontrolera: nova interpretatsiya pryntsypu SIS [Application of the FMEDA/FIT Verification Method for Assessing Cybersecurity of a Programmable Logic Controller: A New Interpretation of the SIS Principle]. *Aerospace Engineering and Technology*, 2024, no. 1(193), pp. 76-90. DOI: 10.32620/aktt.2024.1.07. (In Ukrainian).

22. *TXS Compact Platform Topical Report. NRC/Framatome Phase "0" Meeting*. Framatome, 2024. Available at: https://www.nrc.gov/docs/ML2419/ML24193A231.pdf. (accessed 12.12.2024).

23. *How Does Triton Attack Triconex Industrial Safety Systems?* Cisco Blogs IoT Security Research Lab, 2021. Available at: https://blogs.cisco.com/security/how-does-triton-attack-triconex-industrial-safety-systems. (accessed 12.12.2024).

24. *How Does Triton Attack Triconex Industrial Safety Systems?* Glocomp, 2020. Available at: https://www.glocomp.com/how-does-triton-attack-triconex-industrial-safety-systems. (accessed 12.12.2024).

25. *Analyzing the TRITON industrial malware*. Midnight Blue, 2018. Available at: https://www.midnightblue.nl/blog/analyzing-the-triton-industrial-malware. (accessed 12.12.2024).

26. Illiashenko, O., Kharchenko, V., Babeshko, I., & Fesenko, H., Giandomenico F. Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection. *Entropy*, 2023, vol. 25, iss. 8, article no. 1123. 35 p. DOI: 10.3390/e25081123.

Надійшла до редакції 15.12.2024, розглянута на редколегії 17.03.2025

PRINCIPLES OF MUTUAL AWARENESS IN ANALYSIS OF FUNCTIONAL AND CYBERSECURITY OF INFORMATION AND MANAGEMENT SYSTEMS ON PROGRAMMED LOGIC CONTROLLERS

Oleksandr Ivasiuk, Vyacheslav Kharchenko

The **subject** of this paper is the properties of instrumental and control systems (ICS) in terms of functional safety (FS) and cybersecurity (CS). This paper investigates the FS and CS of ICS, which are based on digital programmable logic controllers (PLC) and performing the safety related functions. The **goal** is to develop elements of the methodology for analyzing the design basis by considering the results of the evaluation of the FS of PLC systems (PLC-based ICS) to optimize the costs of such analysis. **Objectives**: to analyze PLC systems as an object of FS and CS assessment; to formulate and prove the key ideas of the Safety Informed Security (SfISc) concept; to discuss examples and limits of applicability of the formulated statements. The following **results** are obtained. The principle of the three equivalences is proposed and a generalized structural scheme for its representation is constructed. Two basic theorems are described and proved to establish a relationship between the level of cybersecurity of a PLC, in the presence of information about its functional safety. Based on the first-proven theorems, a basic model of PLC states with a functional safety level of SIL-3 is built in the case of a single hardware failure and/or cyberattack. The existing ontological model SISMECA, which is based on the principle of Security Informed Safety (ScISf), is supplemented. A well-known cyberattack involving a PLC system with high safety level is analyzed. Based on the proposed concept, one of the most likely scenarios of a cyberattack on a PLC in the "online" is evaluated. **Conclusions**. For the first time, the concept of mutual awareness of the function and cybersecurity of ICS based on PLC - SfISc - is proposed. The theoretical postulates described in this paper make it possible to assess the cybersecurity of a PLC based on previously performed safety assessments. The SfISc principle can be used in the following practical cases: in the process of licensing a new or modernized functional safety ICS; in determining the level of compliance of existing systems that are important for safety with new cybersecurity requirements; and in developing the requirements for a safety-related ICS.

Keywords: information and control systems; programmable logic controller; self-diagnosis; cybersecurity; functional safety; principle of three equivalences; ScISf-SfISc principles.

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.