УДК 004.9 **doi: 10.26906/SUNZ.2023.4.114**

В. С. Харченко, О. О. Івасюк

Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків, Україна

ВИКОРИСТАННЯ МЕТОДУ ВЕРИФІКАЦІЇ FMEDA/FIT ДЛЯ ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ ПРОГРАМОВНОГО ЛОГІЧНОГО КОНТРОЛЕРА

Анотація. З кожним роком зростає кількість атак на критичну інфраструктуру, яка відіграє ключову роль у життєдіяльності людини. Основною ціллю зловмисників при здійсненні такого типу кібератак є програмовані логічні контролери, які використовуються для побудови ІКС технологічних процесів. Як правило, до такого типу ІКС та програмованих логічних контролерів висуваються вимоги щодо забезпечення функційної безпечності, яка оцінюється шляхом проведення FIT на базі FMEDA. А для оцінювання рівня кібербезпеки програмованого логічного контролеру використовується PnT на базі IMECA. Таким чином, для оцінки рівня функційної безпечності та кібербезпеки необхідно прикладати подвійні зусилля. Але у той же час, слід враховувати значні часові та фінансові інвестиції для визначення ступеня відповідності навіть до однієї з них. Тому, задача обґрунтування можливості використання вже отриманих результатів, щодо відповідності вимогам функційної безпечності для оцінки рівня кібербезпеки програмованого логічного контролеру є актуальною і такою, що має практичне значення. У статті розглядаються питання оцінювання рівня кібербезпеки SPLC, побудованих на основі використання технології FPGA. SPLC відповідають вимогам функційної безпечності рівня SIL-3 і вони є ядром ІКС, на які покладається завдання по забезпеченню безпечного управління критичними технологічними процесами. Обґрунтовується можливість використання результатів FIT на базі FMEDA для апаратної частини SPLC у якості результатів виконання PnT на базі IMECA. Введена метріка для оцінки загальної кількості апаратних відмов, які одночасно можуть бути розглянуті у якості кібератак. За обраним показником була виконана оцінка результатів FMEDA для одного з модулів SPLC. Використання запропонованого підходу надає змоги економії мінімум 240 людино/годин.

Ключові слова: функційна безпечність, кібербезпека, апаратний дефект, кібервразливість.

Вступ

Мотивація. Останні десятиліття визначаються всеосяжним переходом від аналогових технологій до цифрових, суцільною дижиталізацією та інтелектуалізацією промислових систем, в контексті впровадження концепцій Індустрія 4/5.0. Якщо в деяких сферах цей процес відбувається швидко та всебічно, то у галузях, критичних для безпеки людини, такі процеси є доволі повільними, з огляду на їх більш консервативний характер. Інформаційно-керуюча система (ІКС) є одним із ключових елементів у забезпеченні безпечного та контрольованого перебігу технологічних процесів, небезпечних для людини. Тому, до таких систем висуваються високі вимоги, щодо забезпечення надійності, функційної безпечності та кібербезпеки.

Цифрові системи стикаються з новими видами загроз - кіберзагрозами, які не були актуальними для аналогових систем. У [1] показано, що рівень кібератак ІКС збільшився на 41% за першу половину 2021, і з них 71% класифікувались як серйозні або критичні. Яскравим прикладом кібератаки на промислову інфраструктуру став інцидент з трубопроводом Cologne Pipeline у 2021 [2]. Прикладом однієї з останніх потужних атак, яка відбулась наприкінці серпня 2023р., є атака на компанію Energy One Limited, яка є постачальником програмного забезпечення для енергетичних компаній [3]. У той же час, дослідження свідчать, що менше половини (44%) респондентів вищої ланки вважають, що їм необхідно провести термінові поліпшення в найближчі кілька років, щоб запобігти серйозній атаці на їхній бізнес, а більш як третина (35%) фахівців у галузі енергетики стверджують, що їхнім компаніям доведеться зіткнутися з серйозним інцидентом, перш ніж інвестувати у свій захист [4]. Це має пояснення, оскільки забезпечення і підтримка високого рівня кібербезпеки потребує постійних та значних інвестицій. Тому, задача пошуку шляхів, які надають змогу виконати, хоча б часткове оцінювання кібербезпеки продукту без залучення великих додаткових інвестицій, за рахунок використання вже отриманих результатів, стосовно інших складових безпеки, зокрема, функційної безпечності, є актуальною і має суттєву практичну користь.

Аналіз публікацій розпочнемо з висловлювання Caitie McCaffrey з Microsoft Research, яке стисло передає важливість та необхідність тестування шляхом засіву дефектів: «Ви ніколи не дізнаєтесь, яким чином поведе себе система під час збою або нештатної ситуації, до тих пір, поки не відтворите її».

Як сказано у [5], серія стандартів IEC 62443 була розроблена для забезпечення безпеки систем промислової автоматизації та управління протягом усього їхнього життєвого циклу. Наразі, він включає дев'ять стандартів, технічних звітів і технічних специфікацій. У стандарті IEC 62443 застосовується підхід до кібербезпеки, що ґрунтується на оцінці ризиків, який заснований на концепції, згідно з якою спроби захистити всі активи однаковою мірою, не є ні ефективними, ні стійкими. Він стосується не тільки технології, що входить до складу системи керування, а й робочих процесів, заходів протидії та співробітників [5].

У [6-10] визначені підходи оцінки кібербезпеки систем, речей та процесів через виконання тестування на проникнення (PnT – penetration testing). Наведені основні етапи, з яких складається виконання такого тестування та графічні схеми їхньої послідовності і взаємозв’язку. Надається стисле описання змісту кожного з етапів. Але, переважно досліджується сегмент інтернету речей, комп’ютерних бездротових мереж та системи забезпечення з якості підприємств, яке характеризується використанням комерційних засобів.

У статті [11] наводяться детальні приклади розробки коду для конфігурації мікросхем ASICS. Досліджуються кейси із імплементацією у код апаратної закладки на етапі розробки. Особливістю такого типу мікросхем є те, що вони не можуть бути ні перекон-фігуровані, ні стерті користувачем. Тому єдине, що в такому випадку є у користувача, це проведення тестування готового рішення за методом “black box”. Таким чином, користувач отримує виріб, який при настанні «тригерної» події, наприклад, натискання певної послідовності кнопок, активує «апаратну закладку». Хоча автор і продемонстрував «непомітність» такої закладки, але вона може бути досить легко знайдена на етапі верифікації коду, в рамках побудови функційно- безпечних PLC, згідно вимог IEC 61508. Додатково, слід відмітити, як даний матеріал яскраво демонструє ризики використання програмних продуктів третьої сторони.

У [12] надано детальний опис техніки засіву дефектів для відтворення одиничних апаратних відмов комірок пам’яті у FPGA (field-programmable gate array), які мають назву «soft fault» і характеризуються зміною значення біта, що зберігається. Техніка розроблена для тестування FPGA з використання static random access memory, які виготовляє фірма Xilinx. Засів дефектів проводиться з використанням спеціально призначеного програмного забезпечення (soft error mitigation) з використанням (intellectual property core.). Ця техніка пристосована виключно для FPGA, фірми Xilinx і може бути використана для перевірки одного типу дефектів. У той же час, у статті наведені рівні, на яких засів може відбутися, а саме: апаратний (безпосередній вплив на комірку пам’яті), програмний (закладка у файлі конфігурацій, яка активується у разі настання тригерної ситуації) рівень симуляції (створення моделі комірок пам’яті, за допомогою Hardware Description Language та їхня перевірка) та рівень емуляції (коли відбувається внесення дефекту безпосередньо в «розгорнутий» у FPGA код, за допомогою спеціального інструментарію). Також ці чотири методи засіву дефектів аналізувались у [13].

У стандарті IEC 61508 розглядаються шляхи забезпечення функційної безпеки електронних і програмованих електронних пристроїв, і оцінюється парирування випадкових одиничних апаратних відмов [14, 15]. У той же час, стандарт не надає інформації яким чином здійснити імітації таких відмов та нічого не говориться про кібербезпеку таких пристроїв. Пристрій може бути безпечним, але чи можемо ми довіряти його реакціям?

В існуючому на даний час єдиному стандарті по засіву дефектів (fault injection testing, FIT) [16] описується методологія для оцінки надійності та безпечності цифрових систем керування у ядерних енергетичних установках, за допомогою впровадження помилок (дефектів). Розглядаються методи застосування даного інструментарію для оцінки ІКС, які побудовані або на FPGA технології, або на основі мікропроцесорів. Але у стандарті не розглядається можливий зв'язок між апаратними відмовами та кібервразливостями.

У роботах [17-19] висвітлюється близькість функційної та інформаційної безпечності комп’ютерних систем, які керують критичними технологічними процесами. Набір інструкцій по практичній реалізації засіву дефектів та приклади їхньої імплементації під час тестування програмованого логічного контролеру (ПЛК, programmer logical controller – PLC) було надано у [20, 21].

Висновок: єдиним шляхом перевірки поведінки системи під час виникнення апаратного дефекту або намагання зловмисника скористатись апаратною вразливістю, є виконання тестів, які відтворюють ці події. До сьогоднішнього дня таки типи тестів, як FIT та PnT, розглядались як цілком окремі типи тестування. Тому, вирішення завдання з визначення точок їхнього «перетину» надають можливості перехресного використання результатів їхнього проведення, що у свою чергу, дозволить скоротити час та інвестиції, необхідні для виконання оцінки кібербезпеки та функційної безпечності PLC.

Мета та структура роботи. Метою статті є визначення кількості тестів із засівом дефектів, результати яких можуть бути використанні у якості виконання тестів на проникнення.

Основний матеріал статті наведений у 2-у та 3-у розділах, а висновки у розділі 4. У розділі 2 пропонується методика FIT, результати виконання якої під час оцінювання функційної безпечності одночасно можуть бути використані і у якості результатів виконання PnT, під час оцінювання кібербезпеки. У розділі 3 надаються практичні приклади використання запропонованої методики для оцінки кібербезпеки PLC.

Методологія оцінювання кібербезпеки за результатами оцінювання функційної безпечності

Визначення об’єкту дослідження. Ядром будь-якої цифрової ІКС, пов’язаної з безпекою – є PLC, який може бути побудований на основі мікроконтролеру чи FPGA. Саме PLC стає об’єктом кібератак зловмисників [7, 21].

PLC складається з апаратної (HW) та програмної (SW) частин. Програмна частина поділяється на платформну (system software) та алгоритмічну (application software) складові [14].

У рамках статті об’єктом досліджень є апаратна частина PLC, на базі FPGA, який розробляється у відповідності до вимог стандарту IEC 61508 і відповідає рівню функційної безпечності SIL-3. Як правило, PLC такого типу використовуються в ІКС, які виконують функції безпеки [23]. За кордоном, такі системи називають «safety» [24], тому надалі обраний об’єкт дослідження для простоти використання пропонується називати SPLC.

Розглянемо особливості SPLC. Вони не мають інтерфейсів із зовнішніми комп’ютерними мережами, та в них не використовуються програмні продукти третіх сторін. SPLC складаються із окремих (програмно-апаратних) модулів отримання сигналів від польових сенсорів, модуля або модулів реалізації прикладних алгоритмів керування, модулів виходу для передачі електричних команд та комунікаційних модулів для з’єднання з іншим SPLC. Усі модулі розміщуються у спеціально призначеному для цього

шасі. Обмін інформацією між модулями одного SPLC відбувається за рахунок внутрішніх комунікаційних ліній. Якщо у склад ІКС входить робоче місце оператора та додатковий сервер для зберігання і відображення поточної технологічної інформації, то використовуються односпрямовані інтерфейси або апаратні інформаційні діоди (data diode). Процес зміни уставок відбувається тільки при відключенні ІКС від операційної технологічної діяльності та з використанням спеціального програмного забезпечення [15, 17].

Апаратна частина SPLC може стати об'єктом таких кібератак, як: порушення конфігурації SPLC (зміна кількості та типу модулів у шасі); інсталяція невалідного модуля у шасі; атака на файл конфігурації FPGA; атака на внутрішні інтерфейси; атака на зовнішні інтерфейси; «soft faults» кристалу FPGA, які дорівнюють атаці на системну логіку, яка виконується у даний час.

Аспект кібербезпеки у контексті FIT. Для оцінки функційної безпечності SPLC використовуються стандартизовані і відпрацьовані методи FMEDA (Failure Modes and Effects Diagnostics Analysis) & FIT – ці методи зосереджені на оцінюванні ризиків відмов (критичних та некритичних), обумовлених фізичними дефектами апаратних засобів (випадкові одиночні відмови) є достатнім, якщо неможливі кібератаки або інші втручання в систему [15, 17].

Але, якщо такі атаки можливі, необхідно виконувати оцінювання кібербезпеки. Для оцінювання кібербезпеки використовуються аналоги FMEDA & FIT, а саме IMECA (Intrusion Modes and Effects Criticality Analysis) & PnT, сутність яких полягає в тому, що аналізується ланцюг «загроза-вразливість-атака-наслідки-критичність» для кібербезпеки.

Таким чином, маємо два операційних комплекси (процедури) оцінювання Proc FS = {FMEDA, FIT} – функційної безпечності і Proc CS = {IMECA, PnT} – кібербезпеки, які зазвичай, розглядаються, як незалежні. Отже, часові і економічні витрати в такому випадку є сумою часових і економічних витрат двох процедур: Proc FS та Proc CS.

На основі вищевикладеного сформулюємо гіпотезу про те, що при виконанні Proc FS = {FMEDA, FIT} можлива ситуація, коли окремі визначенні дефекти і відповідні їм FIT, можуть бути використані для аналізу кібербезпеки (повторювати результати операцій процедури Proc CS). Також, може бути сформульована симетрична друга гіпотеза – при виконанні Proc CS можлива ситуація, коли окремі результати виконаних операцій аналізу вразливостей та PnT можуть бути використані для аналізу функційної безпечності (повторювати за результатами операції процедури Proc FS). Тобто апаратний дефект і є апаратною вразливістю, та навпаки.

Визначення відносної потужності множини PnT на множини FIT. Для визначення підмножини тестів PnT на підставі множини FIT, необхідно провести аналіз і відібрати ті, що повною мірою відповідають або еквівалентно імітують спробу зловмисника вплинути на роботу контролера. Це саме апаратні дефекти, які потенційно можуть бути використані зловмисником для порушення конфіденційності, достовірності, цілісності або доступності інформації, як в середині, так із зовні SPLC (рис. 1, де, F – множина дефектів за результатами FMEDA, які мають бути перевірені під час FIT, у відповідності до обраного рівня SIL; I – множина вразливостей за результатами IMECA, які мають бути перевірені під час PnT).

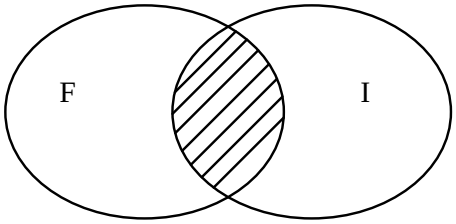

Рис. 1. Схематичне зображення області вразливостей на множині апаратних дефектів

Введемо наступну метрику перетину, за проявом вразливостей і дефектів,

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

яка визначає, яку частину апаратних дефектів за результатами FMEDA можна вважати одночасно і кібервразливостями.

У наступному розділі розглянемо приклади, які засвідчать практичну застосовність гіпотези, яка було сформульована у цьому розділі.

Практичне застосування та висновки

Однією з найважливіших вимог до SPLC є його повністю детермінована поведінка. Тобто, він повинен очікувано переходити з одного дозволеного стану в інший, у разі настання одиничної апаратної випадкової відмови. Переходи між станами також мають бути чітко детерміновані. З точки зору кібербезпеки, SPLC має поводитися відповідно до стратегій зниження негативного впливу (mitigation strategy) під час кібератаки, через його апаратну вразливість. Таким чином, неважливо, що буде причиною відмови, але поведінка SPLC має бути строго детермінована.

У разі виникнення критичної апаратної відмови SPLC, у відповідності до [14], має переходити в «безпечний стан», який визначається технічним завданням і може бути або de-energize-to-trip, або energize-to-trip. При виникненні некритичної відмови SPLC має її діагностувати (детектувати) та супроводжувати оповіщенням [14, 15, 17].

Розглянемо практичний приклад, коли дефекти взяті з FMEDA, і побудовані на їхній основі тести для FIT, можуть бути використані під час виконання оцінки кібербезпеки SPLC. Результати цього огляду представлені в табл. 1.

У колонці «FMEDA symptom» надано результати виконання FMEDA для SPLC. У стовпчику «The essential of symptom» надано опис суті симптому, тобто події, яку було оцінено в FMEDA. Кібератака, яка відповідає опису суті симптому, представлена в колонці «The corresponding cyber-attack», а в колонці «Expected results/Mitigation strategy» записаний очікуваний результат поведінки SPLC і стратегія пом'якшення негативних наслідків у разі кібератаки.

Таблиця 1 – Порівняльний аналіз апаратних відмов і кібератак

#	FMEDA symptom	The essential of symptom	The corresponding cyber attack	Expected results/ Mitigation strategy
1	Loss of comm to each IOM	The physical corruption of internal communication lines between main module and I/O modules.	The malefactor tries to disrupt the internal communication link	Each SPLC modules detects it and the SPLC transits to the safe state due to severity level of fault
2	FPGA config memory soft fault	While the bitstream is being transferred from an external device into the FPGA the error occurs.	The malefactor tries to replace the correct firmware	The module detects it and not to transit in to normal operation mode
3	FPGA user RAM soft fault	The error occurs into the logic of FPGA algorithms.	The malefactor tries to implement the wrong path into the existing logic algorithm	The module detects it and transit in to safe state from the normal operation mode
4	No incompatible (non-safety or non-interfering) module is installed.	A module that is not related to the verified modules is being installed in SPLC.	The wrong module is installed to change the configuration of the SPLC	The main module detects it when wrong module replaces the correct module while the normal operation mode and transit entire SPLC in to safe state The main module detects it when wrong module replaces the correct module before operation starts and transit entire SPLC in the safe state immediately without normal operation mode.
5	Fault of external connected module occurs	The external connected module has the critical fault	The malefactor tries to break the external connected module from the another SPLC to change the configuration of entire I&C	The main module of SPLC detects it and make the annunciation about the detected fault and staying in the normal operation mode

Які висновки можна зробити при аналізі інформації в табл. 1: насамперед, постає питання про причину збігу очікуваних результатів при виконанні FIT і стратегії пом'якшення негативних наслідків кібератаки у разі виконання PnT. Очевидно, що причиною настання відмови, розглянутої в FMEDA, може бути, як одиничний випадковий апаратний дефект, так і навмисне втручання в роботу SPLC. Оскільки реакція SPLC на негативну подію з FMEDA має бути однаковою, незалежно від причини, що її викликала, відбувається збіг в останній колонці. Саме «Expected results» і «Mitigation strategy» якраз і розглядають поведінку (реакцію) SPLC на негативну подію.

Позначимо множину тестових кейсів засівання дефектів на основі FMEDA, як TCFIT, а її завдання у вигляді

$$TCFIT(n)=\{TCFIT(\sum_{i=1}^{n} i)\},$$

де n – кількість відмов із FMEDA, які мать бути протестовані; TCFIT(i) – і-й тест кейс засіву дефекту, для перевірки і-ої події із списку FMEDA.

Оскільки множина апаратних кібервразливостей TCPn(m) є підмножиною можливих одиничних апаратних дефектів, то кількість тестових кейсів виконання PnT є підмножиною тестових кейсів засівання дефектів TCFIT(n):

$$TCPn(m1)\subset TCFIT(n).$$

З іншого боку, множина TCPn(m1) є частиною множини тестових кейсів PnT по перевірці усіх можливих кібервразливостей (TCVIT (m)), які визначені за результатами IMECA для апаратної і програмної частин SPLC, тому

$$TCPn(m1)\subset TCVIT(m).$$

На підставі цього, робимо висновок про те, що

$$TCVIT\ (m)\ \cap\ TCFIT\ (n)\neq \emptyset.$$

Визначення кількості тестів, які одночасно задовольняють вимогам, як FIT, так і PnT, надаємо у наступному вигляді

$$TCPn=\{TCFIT(i)|Pn(TCFIT(i))\}, \quad (1)$$

де Pn(TCFIT(i)) – властивість тестового кейсу TCFIT(i), з множини TCFIT, одночасно імітувати, і одиничний апаратний дефект і кібератаку.

На основі записаного вище правила (1), було виконано оцінку кількості тестових сценаріїв тестування на проникнення, на основі тестових сценаріїв засіву одиничних випадкових апаратних дефектів, для одного з модулів SPLC. Результати оцінювання наведено в табл. 2. Аналізуючи ці дані, робимо висновок, що кількість тестів на проникнення, у даному випадку, дорівнює 10 і, таким чином, обрана метрика буде дорівнювати α=10\38=0,263. Особливо цікавим є випадок із 36 і 37 тестовими сценаріями, які відповідають 10-му тестовому сценарію тестування на проникнення. Це свідчить про те, що одна кіберзагроза, а саме розрив зв'язку із зовнішнім SPLC може статися через різні апаратні дефекти (бути еквівалентною за наслідками). Висновок: У статті для обраного об’єкту дослідження, а саме апаратної частини SPLC на базі FPGA, який розробляється у відповідності до вимог IEC 61508, було сформульовано і доведено гіпотезу, що до можливості застосування результатів аналізу апаратних дефектів FMEDA та виконання FIT, у якості частини результатів аналізу вразливостей IMECA та виконання PnT. На основі якої було розраховано кількість FIT, результати яких

можуть бути використанні у якості PnT, без їхньої окремої реалізації. З урахуванням того, що для виконання одного FIT в середньому витрачається від 24 людино/годин, то для 10 FIT часові витрати будуть дорівнювати 240 людино/годинам і це тільки для одного модуля, і тільки для апаратної частини.

Таблиця 2 – **Визначення апаратних відмов, які одночасно є кібератаками**

FIT/Pn		**DX.XX.X/Module on 2018-02-26 / 7:58:27 from FMEDA3.wk3- LISTS OF FIT TESTS PER PHYSICAL MODULE**	
TC_{FIT}	TC_{Pn}	**Requirement/Solution Text**	**notes**
1		[CM 5v low]	
2		[CM VCCA 2.5v lost]	
3		[CM VCCL 1.1v lost]	
4		[DELETED--CM VCCL 1.5v lost]	
5		[CM VCC 0.9v lost]	
6		[CM VCCIO 2.5v lost]	
7	1	[CM F-Optic fault]	In operating mode
8	2	[CM LVDS fault]	In operating mode/during installation
9	3	[CM RS232/485 corruption]	In operating mode
10		[CM clock A fault]	
11		[CM clock B fault]	
12		[CM clock C fault]	
13	4	[CM FPGA package failure]	during installation
14	5	[CM fpga config hard failure]	during installation
15	6	[CM fpga user logic gates ram hard faults]	during installation
16	7	[CM fpga config soft faults]	during installation
17	8	[CM fpga user ram soft faults]	during installation
18		[CM.PS 3.3v low]	
19		[CM.PS 3.3v high]	
20		[CM.PS 5v low]	
21		[CM.PS 5v high]	
22		[CM.PS VCCL 1.1V lost]	
23		[CM.PS VCCL 1.1V low]	
24		[CM.PS VCCL 1.1V high]	
25		[CM.PS VCCH 1.5V lost]	
26		[CM.PS VCCH 1.5V low]	
27		[CM.PS VCCH 1.5V high]	
28		[CM.PS VCC 0.9v lost]	
29		[CM.PS VCC 0.9v low]	
30		[CM.PS VCC 0.9v high]	
31		[CM.PS VCCIO 2.5v lost]	
32		[CM.PS VCCIO 2.5v low]	
33		[CM.PS VCCIO 2.5v high]	
34		[CM.PS clock B fault]	
35	9	[CM routing - corrupt CRC]	In operating mode
36	10	[CM.PS 3.3v lost *IT loss of comm'n sensed by {local MM} + {remote MM} + {remote CM}]	In operating mode
37	10	[CM.PS 5.0v lost *IT loss of comm'n sensed by {local LM} + {remote LM} + {remote OCM}]	In operating mode

Подальшими напрямками розвитку цієї тематики є визначення набору PnT, як апаратної частині SPLC, так і програмної. Таким чином, може з'явиться перспектива використання результатів, отриманих впродовж оцінювання функційної безпечності, для аналізу або певної верифікації результатів оцінки кібербезпеки без проведення окремої процедури. Додатково планується провести оцінку фінансових та часових витрат, які можуть бути скорочені при використанні даного підходу в цілому.

СПИСОК ЛІТЕРАТУРИ

1. *S. Coble* ICS Vulnerabilities Increase 41% // Infosecurity Magazine, 18 august 2021. Available at: https://www.infosecurity-magazine.com/news/ics-vulnerabilities-increase-41/

2. https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/
3. *B. Maundrill* Cyber-Attack on Australian Utility Firm Energy One Spreads to UK Systems // Infosecurity Magazine, 22 august 2023. Available at: https://www.infosecurity-magazine.com/news/cyberattack-australian-utility/
4. *R. A. Coveney* Energy executives expect more extreme cyber-attacks but defensive action is lagging, new DNV research reveals // DNV, 19 may 2022. Available at: https://www.dnv.com/news/energy-executives-expect-more-extreme-cyber-attacks-but-defensive-action-is-lagging-new-dnv-research-reveals-224890
5. International Electrotechnical Commission. (2010-11-10). IEC 62443:2010. Industrial communication networks. Network and system security – Part 1-4.
6. *M. Tayag, M. Emmalyn* Compromising systems: implementing hacking phases // International Journal of Computer Science & Information Technology (IJCSIT), Vol 11, N 2, p. 27-35, April 2019.
7. *B. Mahar* Penetration Testing Industrial Control Systems: What to Know // KROLL, 5 april 2022 Available at: https://www.kroll.com/en/insights/publications/cyber/pentesting-industrial-control-systems
8. Pentest-standard.org (2011), PTES Technical Guidelines - The Penetration Testing Execution Standard. Available at: http://www.pentest-standard.org/index.php/PTES_Technical_ Guidelines
9. А.І. Абакумов, В.С. Харченко «Тестування на проникнення систем інтернету речей: кіберзагрози, методи та аналізи» // Electronic Modeling, V. 44. № 4, с. 79-104, 2022.
10. International Standart ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements
11. https://ryancor.medium.com/hardware-trojans-under-a-microscope-bf542acbcc29
12. *Óscar Ruano, Francisco García-Herrero, Luis Alberto Aranda, Alfonso Sánchez-Macián, Laura Rodriguez and Juan Antonio Maestro* Fault Injection Emulation for Systems in FPGAs: Tools, Techniques and Methodology, a Tutorial // https://www.mdpi.com/1424-8220/21/4/1392
13. *В.А. Куланов, В.А. Куланов, А.С. Скрынник* Инструментальное средство засева и моделирования константных неисправностей встроенных систем на ПЛИС // Радіоелектронні і компютерні системи, № 7, с. 225-229, 2010 р.
14. International Electrotechnical Commission. IEC 61508:2010. Functional safety of electrical/electronic/programmable electronic safety related systems – Part 1-7.
15. *Федоров Ю. Н.* Справочник инженера по АСУТП: проектирование и разработка. Учебно – практическое пособие // Инфа-Инженерия, 2-е изд., Том 1 - 2018, с. 448.
16. US NRC, NUREG/CR-7151: Development of a fault Injection-Based Dependability Assessment Methodology for Digital I&C System, Vol 1-4, 2011
17. *Скляр В. В.* Обеспечение безопасности АСУТП в соответствии с современными стандартами: Методическое пособие // Инфа-Инженерия, 2018, с. 384.
18. *Харченко В. С.* "Гарантоздатність комп'ютерних систем: межа універсальності у контексті інформаційно-технічних станів", Радіоелектронні і комп'ютерні системи, № 8, с. 7-14, 2007.
19. *Харченко В. С.* "Гарантоздатні системи та багатоверсійні обчислення: аспекти еволюції", Радіоелектронні і комп'ютерні системи, № 7, с. 46-59, 2009.
20. *V. Kharchenko V. Sklyar, A. Ivasuyk, "*Fault-Injection Testing: FIT-Ability, Optimal Procedure and Tool for FPGA-Based Systems SIL Certification*"//* Proceedings of East-West Design&Test Symposium (EWDTS"2013). 2013. P.188-192.
21. *V. Kharchenko V. Sklyar, A. Ivasuyk, O. Odarushenko* "Fault insertion testing of FPGA-based NPP I&C systems: SIL certification issues"// Proceedings of 22nd International Conference on Nuclear Engineering. Technical Publication ICONE22. Nuclear Education, Public Acceptance and Related Issues; Instrumentation and Controls (I&C); Fusion Engineering; Beyond Design Basis Events. 2014. Vol. 6.
22. https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html
23. СТАНДАРТ Державного підприємства «Національна Атомна Енергогенеруюча Компанія «ЕНЕРГОАТОМ» Інформаційні та керуючі системи, важливі для безпеки атомних електричних станцій загальні технічні вимоги – СОУ НАЕК 100:2022.
24. International Electrotechnical Commission. IEC 61513:2011 – Nuclear power plants - Instrumentation and control important to safety - General requirements for systems.

Received (Надійшла) 30.09.2023
Accepted for publication (Прийнята до друку) 29.11.2023

Using the FMEDA/FIT verification method to assess the cybersecurity of a programmatic logic controller

Oleksandr Ivasiuk, Vyacheslav Kharchenko

Abstract. Every year, the number of attacks on critical infrastructure, which plays a key role in human life, is growing. The main target of malefactor in this type of cyberattack is programmable logic controllers used to build I&CS. As a rule, this type of I&CS and programmable logic controllers have to meet the requirements of ensure functional safety, which is assessed by conducting FIT based on FMEDA. Additionally, to assess the cybersecurity level of a programmable logic controller, PnT based on IMECA is used. Hence, to assess the level of functional safety and cybersecurity, it is necessary to make double efforts. However, at the same time, significant time and financial investments should be taken into account to determine the degree of compliance with even one of them. Therefore, the task of substantiating the possibility of using the results already obtained regarding compliance with the requirements of functional safety to assess the level of cybersecurity of a programmable logic controller is relevant and of practical importance. The article discusses the issues of assessing the cybersecurity level of SPLCs based on FPGA technology. SPLCs meet the functional safety requirements of the SIL-3 level and they are the core of ICS developed to ensure the safety of critical technological processes. The possibility of using the results of FMEDA-based FIT for SPLC hardware as the results of IMECA-based PnT is substantiated. The metric chosen to assess the total number of hardware failures that can be considered as cyberattacks at the same time. The selected metric was used to evaluate the FMEDA results for one of the SPLC modules. The using of the proposed approach allows saving at least 240 labor/hours.

Keywords: functional safety, cybersecurity, hardware defect, cyber vulnerability.