Date of publication SEP-30, 2025, date of current version AUG-08, 2025.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.19.3.XX

From Security Informed Safety to Safety Informed Security: Methodology and Case for PLC-based I&C Assessment

OLEKSANDR IVASIUK, VYACHESLAV KHARCHENKO, HEORHII ZEMLIANKO
National Aerospace University "KhAI", Kharkiv, 61070, Ukraine (E-mail:o.ivasiuk@csn.khai.edu, v.kharchenko@csn.khai.edu, g.zemlynko@csn.khai.edu)
Corresponding author: Heorhii Zemlianko (e-mail: g.zemlynko@csn.khai.edu).

ABSTRACT The paper introduces the Safety-Informed Security (SfISc) concept, which proposes that a system's functional safety (FS) properties can inherently enhance its cybersecurity (CS). The main goal is to show that the self-diagnostics and fault-tolerance mechanisms of safety-critical programmable logic controllers (PLCs) and PLC-based instrumentation and control systems (ICSs), designed for high FS, can effectively detect and mitigate cyberattacks and decrease efforts to assess cybersecurity metrics against requirements to ICSs. The study presents a methodology based on a "three-equivalence principle": 1) the equivalence of the consequences of dangerous failures and cyberattacks; 2) the equivalent perception of consequences caused by CS by self-diagnostic tools, which are initially oriented towards supporting FS; 3) equivalent actions (countermeasures) related to transitioning the PLC into a protected state. Two theorems are formulated to justify concept SfISc. Industrial cases are described to demonstrate how FS evaluation results can be used to significantly simplify and reduce the cost of CS analysis.

KEYWORDS Functional Safety, Cybersecurity, Industrial Control Systems, PLC, Safety-Informed Security, Security-Informed Safety, Cyber-Physical Systems, Risk Analysis.

I. INTRODUCTION

The number of incidents specifically affecting Critical Infrastructure increased by 10% in the same period (2023 to 2024). Reported incidents in the critical infrastructure sector surged from 50 (globally) in 2022 to 384 in 2024, marking a staggering 668% rise [1].

The primary target of a cyberattack on critical infrastructure is an Instrumental and Control System (ICS) and Programmable Logic Controller (PLC), which perform functions related to gathering and processing operational data, generating commands, and sending them to actuators or displays. Incidents involving critical infrastructure have generated a broad discourse on the concept of Security Informed Safety (ScISf) [2], since new threats of unsafe ICS behavior were caused by insider intrusions, cyberattacks, backdoors, and so on. One of its originators is considered to be Professor Robin Bloomfield, who formulated a simple statement to argue for ScISf regarding safety-critical ICS: "If it's not secure, it's not safe." The main tenets of this concept have been detailed and developed in numerous scientific works, for example, [3, 4]. The key idea of the concept is the necessity of considering the impact of breaches in information and cybersecurity (CS) when analyzing the risks of a system's functional safety (FS), as it has been and remains a key property of critical ICS. Based on this concept, standards and regulatory documents have been released [5, 6].

However, the relationship between the processes of evaluating FS and CS has so far been a "one-way street." The influence of FS on CS, or certain interdependencies in the reverse evaluation direction, has been practically unexamined. This circumstance was highlighted in [7], which illustrated the possibility and feasibility of analyzing such an influence.

Therefore, the development of a unified concept for the analysis, evaluation, and assurance of functional safety and

cybersecurity in ICSs is a relevant scientific and practical problem. This primarily concerns how to utilize the results of FS evaluation in CS risk analysis, as the tasks of such analysis are becoming increasingly urgent and complex.

II. STATE-OF-THE-ART

A. RELATED WORK

The paper [8] conducts a comparative analysis of U.S. and international nuclear cybersecurity regulations, standards, and rules to assess their adequacy in protecting energy infrastructure from cyber threats and ensuring accountability. It also reviews recent government and private-sector initiatives aimed at strengthening cybersecurity in the nuclear industry, identifying best practices for enhancing safety and resilience. Given the sector's high-stakes nature, these measures are critically important. At the same time, the article does not examine the relationship between safety and security properties of ICS in the nuclear industry, even though these terms are frequently mentioned together in the same context.

The paper [9] emphasizes the critical role of PLCs in industrial ICS and critical infrastructure. The authors provide a comprehensive analysis of PLC security, covering vulnerabilities, potential attacks (including control logic injection and firmware modification), and existing security solutions. They highlight common vulnerabilities like stack-based overflows and improper input validation, alongside PLC-specific issues in program verification and memory. The paper examines both system-level and PLC-specific vulnerabilities, providing insights for both scientists and industrial engineers. Finally, the authors offer concrete recommendations for PLC manufacturers, researchers, and engineers to enhance the security of current and future PLC designs, aiming to safeguard critical infrastructure from evolving cyber threats.

While the primary focus of the paper is on the security vulnerabilities and threats to PLCs, it acknowledges and implicitly addresses the profound impact that security breaches can have on the safety of industrial processes. The paper's discussion of vulnerabilities, potential attacks like "control logic injection," and the need for robust security solutions, all implicitly aim to prevent scenarios that would compromise operational safety.

This article, like many similar publications, for example [10, 11], establishes the direct relationship between the safety and security features of the PLC. It is obvious because the main risk of the PLC security breaches is the potential harm to the environment, which is the responsibility of PLC safety.

Article [12] analyzes the differences in the implementation of safety functions and conventional control functions, which require a different approach to HW and SW design. A method is proposed that allows developing safety function software for PLC-based ICSs using a functional behavior model. A duplicated architecture reduces the risks of systematic errors in application software, and provides detecting shortcomings that arose in earlier phases of the life cycle.

More redundant solutions for safety critical systems are suggested and investigated using analytical models in [13, 14]. However, these studies do not consider the aspect of cybersecurity and do not analyze risks in the context of the ScISf approach.

On the other side, there are many publications related to investigating industrial FPGA and PLC-based applications where cybersecurity of the systems is discussed without deep analysis of its impact on unsafe system behavior [15,16]. The publications explore formal methods of cybersecurity analysis [17-19], as well as functional safety taking into account the provisions of the ScISf concept [20].

It should be noted, at the same time, the lack of a clear definition of the "safety" and "security" terms in each particular context of use could lead to incorrect conclusions because these two terms are integrated features of PLC that contain several different aspects of it.

An analysis of the main research trends indicates that, until recently, the primary focus has been on the impact of security on the safety properties of PLCs. This research direction is clearly justified because PLCs inherently possess safety properties, while security properties emerged as a response to new threats, specifically cyberattacks.

However, the influence of PLC safety properties on its security has not received attention. It is precisely the investigation of this interrelationship that is presented below.

B. TASKS AND SUBJECT AREA OF RESEARCH

The goal of this paper is to develop elements of a methodology for analyzing CS, considering the results of FS evaluation of PLC-based ICSs, in order to reduce the efforts of such analysis. The research tasks are:

– analysis of PLC-based systems as an object for functional safety and cybersecurity analysis (section 2). At this stage of research, the concepts of FS and CS for such systems are clarified, and the subject of the research is defined;

– formulation of the key provisions of a new concept Safety Informed Security (SfISc), which complements the ScISf concept (section 3). In addition, two theorems are formulated that define the main theoretical basis of the methodology;

– discussion of examples and limits of applicability of the formulated statements (section 4). The examples (cases) are based on real-world industrial experience in the development, testing, and application of PLC-based ICSs;

– section 5 discusses the research results and identifies future directions.

The research methodology is based on the postulating dualistic nature and mutual influence of FS and CS. The core hypothesis is that the results from a system's FS verification and validation can not only be used for CS compliance checks, but also significantly reduce the scope of such checks.

Functional safety of a PLC is a complex property

defined by the ability to minimize the risks of a system transitioning into a dangerous state and the consequences of such a transition. This and next definitions are based on the key standards dedicated to functional safety (such as IEC 61508 [21]), cyber security of ICSs (IEC62443 [22]) and analysis of publications [2-6]. FS of a PLC is characterized by:

– a defined level of reliability;

– a certain completeness (degree of coverage) of self-diagnostics;

– the ability to transition to a safe state in the event of a critical single random hardware failure.

Cybersecurity of a PLC is a property that is ensured by a set of software and hardware mechanisms for protection against unauthorized intrusion, which can affect:

– the integrity of digital information circulating through the PLC;

– the availability of the PLC to perform functions on demand;

– unauthorized influence on operation (changing application logic parameters).

It should also be noted that a cyber-secure PLC must have the ability to automatically apply a mitigating action upon detecting an attack on it.

The object of the study is a PLC (safety-critical PLC), which is a key element for building safety-critical I&C systems. The subject of the research is the processes of evaluating the cybersecurity and functional safety properties of a PLC that meets the requirements for ensuring a safety integrity level (SIL) in accordance with IEC 61508.

This means that it implements deep self-diagnostic coverage of single hardware failures, and also has a defined safety state (de-energize to trip or energize to trip) into which the safety-critical PLC transitions when critical failures (dangerous faults) are detected. An example of such a PLC is the Teleperm XS Compact from Framatome [23].

III. THEORETICAL JUSTIFICATION

A. SfInSc CONCEPT. PRINCIPLE OF THREE EQUIVALENCES

The SfISc concept is based on the following provisions:

a) cyberattacks or other unspecified intrusions can lead to an unacceptable breach of data integrity or a blocking of the execution of przocess control functions;

b) risk analysis of such attacks, from the perspective of their impact on safety, should be conducted in the same way as the analysis of the consequences of any failures that is traditionally performed during FS analysis;

c) methodologies for evaluating the influence of FS on CS must ensure the completeness and reliability of the results and be based on sufficient information and a set of analysis tools.

SfISc concept is the hypothesis that a PLC's self-diagnostic system will perceive a single random hardware failure related to data transfer interfaces and an attempt to violate the established hardware configuration of a running PLC in the same way. The self-diagnostic system will register a discrepancy between the expected value of a monitored parameter and the value received.

However, the mere fact of detecting an attempted unauthorized connection may not be sufficient to prevent the likely negative consequences of a cyberattack. To minimize these negative consequences, the PLC must automatically take risk-mitigation measures—to transition to an appropriate safe state.

Thus, a PLC operating in "online" mode has explicit cybersecurity properties that are based on the principle of three equivalences, which forms the basis of the SfISc concept (Figure 1):

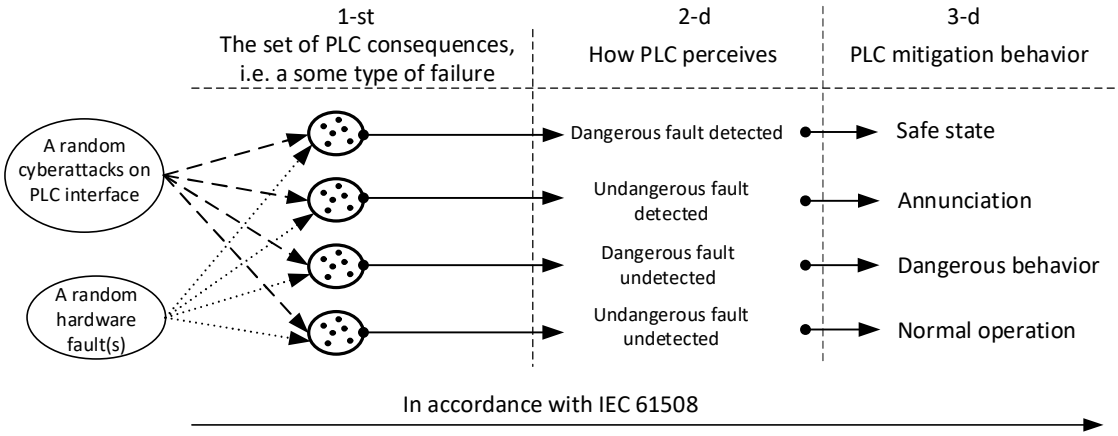

Figure 1. SfISc concept

a) the equivalence of the consequences of dangerous failures and cyberattacks (information intrusions). Explanation: the nature of the PLC fault could be different. For example, an intruder disconnected the module from the PLC to interrupt the existing configuration, or the module has a failure of the power unit. In both cases, the PLC detected a loss of communication with a particular module (see part 1 of Figure 1);

b) the equivalent perception of consequences caused by CS by self-diagnostic tools, which are initially oriented

towards supporting FS in full compliance with FS requirements. For safety PLCs, all possible faults are divided into four groups, which are represented in part 2 of Figure 1;

c) equivalent actions (countermeasures) related to transitioning the PLC into a protected state. The PLC's behavior depends on what type of fault is detected (see part 3 of Figure 1).

B. KEY ASSERTIONS

A shorter formulation of the principle of three equivalences, which explains Figure 1, is as follows: "For any cyberattack on a digital asset of a PLC, there is a single or multiple hardware faults, or a combination thereof that leads to consequences (failures or malfunctions) identical to the consequences of the cyberattack."

Based on the three-equivalence principle, the next two theorems have been formulated and proved [7]. These theorems allow for a first estimation of a safety PLC's cybersecurity level. The proof of the validity of these theorems is determined by the results of the analyzing the architecture of the PLC-based ICSs, the sets of their vulnerabilities and inputs through which attacks (intrusions) can be carried out, taking into account hardware barriers, as well as the manifestation and consequences of such attacks.

Theorem 1. Unauthorized overcoming of the hardware configuration level of a safety PLC in "online" mode is a necessary condition for a successful cyberattack.

Note: overcoming is considered successful if it was not detected by the PLC's means. While a PLC is in run mode, the state of its internal and external interfaces is continuously monitored, and any unauthorized connection would be detected. That is why overcoming the hardware interface level is so important for a successful cyberattack.

Theorem 2. The cybersecurity level of a PLC is higher, the higher its functional safety level.

The higher the self-diagnostic coverage, the lower the probability of a cyberattack succeeding. This means that a higher self-diagnostic coverage rate defines the number of PLC parameters under continuous monitoring, and as a result, the number of PLC weaknesses that could be treated as vulnerabilities decreases.

C. METRICS FOR SfISc ANALYSIS

Let's illustrate the case when some set of hardware faults (F) based on FMEDA might be considered as vulnerabilities (V) related to cybersecurity based on IMECA, see Figure 2. The shaded area means the faults that may use for making a cyber-intrusion.

Based on Figure 2 and examples [22] the following metrics to evaluate the part of certain set faults or vulnerabilities that have dual nature are proposed:

$$\text{MFV} = [(F_{cs} \div F)] \times 100\%, \quad (1)$$

where F – the total numbers of possible faults based of FMEDA (Failure Modes, Effects and Diagnostics Analysis [24,25], Fcs – the numbers of possible faults based of FMEDA that threads as vulnerabilities too.

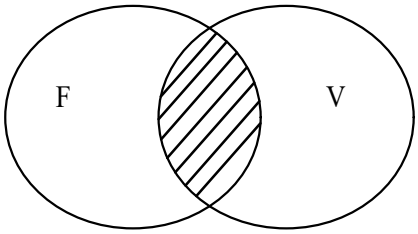

Figure 2. Faults that can be exploited to carry out a cyber-intrusion

$$\text{MFV} = [(F_{cs} \div V)] \times 100\%, \quad (2)$$

where V – the total numbers of possible vulnerabilities based of IMECA (Intrusion Modes and Effect Criticality Analysis [24] .

These metrics allows estimating an approximated level of resources that may be saved during estimation of the CS level of the PLC by using already obtained results of a FS estimation.

IV. CASE STUDY

The several cases are describing below to demonstrate how this the three-equivalence principle might be used in practice.

A. CYBERATTACK TO CHANGE THE PLC HW CONFIGURATIONS

The initial condition is a safety PLC is in a run mode. A malefactor intent to change the existing hardware configuration via cyberattack the first step is taken out one of the operating modules from PLC's chassis, see Figure 3.

A set of PLC consequences – in this case a PLC detect the loss communication between main module and extracted module. Also, these consequences could be as a result the next possible single hardware random failure – the corruption of the internal channel; failure of the communication unit; critical failure in the of the module.

PLC's perceiving – if a PLC's self-diagnostic cover the internal communication this attack would be detected. The safety PLC, for example with SIL-3 level of safety functional, covering it, and this attack, i.e. discrepancy from normal operating mode, is been detecting as a dangerous event.

PLC's mitigation behavior – is what PLC shall to do for mitigate probability of harm from incorrect action due to attack. If the PLC has high level of safety functional it means that PLC has predefined safety state into that state PLC is transited automatic due to detection a dangerous hardware fault.

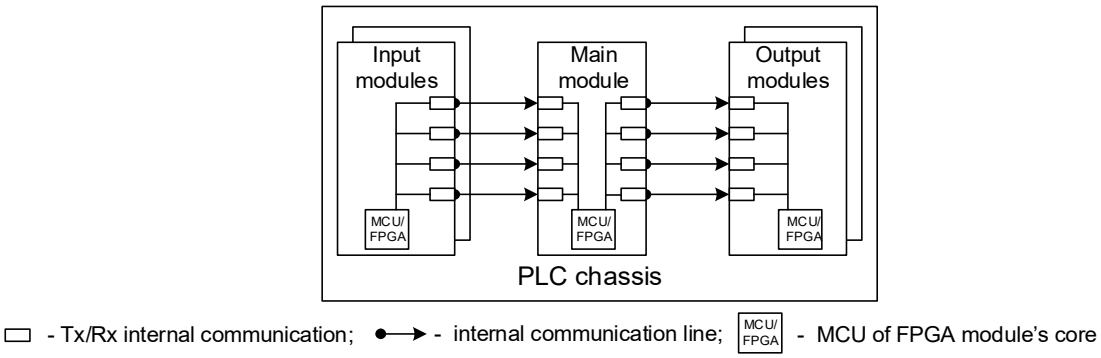

Figure 3. The attack on the PLC's internal hardware configuration

Before the second case is described, it is worth noting that a Safety PLC, in accordance with IEC 61508, must include mechanisms for detecting hardware failures that can negatively affect information during its circulation over communication channels. For this purpose, the standard proposes using various approaches, for example, the calculation of CRC or Checksum for data packets, HearBeat, and packet numerators for digital communication interfaces. Thus, any influence on the communication interfaces during the controller's operation will be detected, since its consequences for a Safety PLC will be identical to one of the possible failures. The importance of the Safety PLC's communication channel, where the diagnostic system finds a failure and determines the subsequent behavior of the Safety PLC.

The next case is related to an interruption of the external digital communication link, let's exploring it based on the three-equivalence principle.

B. CYBERATTACK TO INTERRUPT THE DIGITAL EXTERNAL COMMUNICATION LINK

The initial condition there are two safety PLC are in a run mode. These PLSs have established five digital links that are set point to point connections, i.e. 1-st port (PLC-1) to 1-st port (PLC- 2), the 2-d port (PLC-1) to 2-st port (PLC-2), and so on. The digital external Tx\Rx could be configurable in a different way, one -way or bidirectional link. A malefactor intent to change the existing external connection by shifting 1-st port (PLC-1) to 3-d port (PLC-2) connection, see Figure 4.

A set of PLC consequences – in this case at the first of all (when cable is disconnected) a PLC detect the interruption data transferring with external source based on the one or more mechanisms for controlling data integrity describing above. Secondly (when the cable put in the wrong port) PLC detect the configuration doesn't match with it had been defined during the developing process.

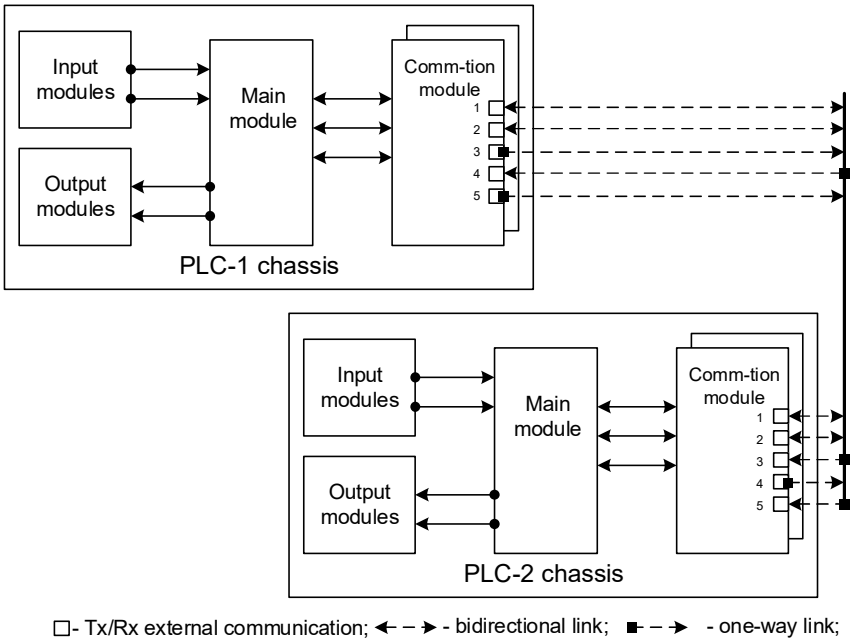

Figure 4. The attack on the PLC's internal hardware configuration

Table 1. List of examples of correspondence between failures and vulnerabilities for safety PLC

#	Failures	The essential of symptom	The corresponding cyber attack	Expected results/ Mitigation strategy
1	MCU of 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
2	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
3	No incompatible (non-safety or non-interfering) module is installed.	A module that is not related to the verified modules is being installed in safety PLC.	The wrong module is installed to change the configuration of the safety PLC	The main module detects it when wrong module replaces the correct module while the normal operation mode and transit entire safety PLC in to safe state The main module detects it when wrong module replaces the correct module before operation starts and transit entire safety PLC in the safe state immediately without normal operation mode.
4	Fault of external connected module occurs	The external connected module has the critical fault	The malefactor tries to break the external connected module from another safety PLC to change the configuration of entire I&C	The main module of safety PLC detects it and make the annunciation about the detected fault and staying in the normal operation mode

Let's considering, as it was in previous study case, the possible single hardware random failure that could be the reason of these consequences – the failure of the integrity data calculation mechanism; failure of the communication unit; critical failure in the of the module.

PLC's perceiving – a safety PLC will treat this attack, as a detected unsafe random hardware failure.

PLC's mitigation behavior – the PLC has some type of annunciation after detecting unsafe random hardware failure.

At the same time, it's should be noted that the PLC treats of fault might be slightly changeable by perceiving unsafe faults as a dangerous one. It's depending on in what specific application a PLC is going to be used.

Some additional PLC hardware faults and possible cyberattacks that produce PLC to the same consequences are listed in the Table 1. In concerns such failures as MCU of FPGA configuration memory soft faults, FPGA user RAM soft faults, and so on [26,27], for which the corresponding cyberattacks can be found.

At the end of this section would like to give some values of metrics based on data provided in [19,24,25]. The results of list FMEDA faults for one communication module has been analyzed and the MFV=0.263. Based on expertise of authors it approximate equal to 240 labor hours. If it's suggest that PLC module family consist of minimum of 4 different type of modules it means that in real case total the resource saving may achieve a high numbers. More precise estimation may be get by considering the specific PLC but as a usually this evaluation is confidential data.

V. CONCLUSION

This study introduces and substantiates the concept of Safety-Informed Security (SfISc), which posits that functional safety mechanisms embedded in safety-critical Programmable Logic Controllers (PLCs) inherently contribute to their cybersecurity posture. The theoretical foundation of SfISc is built upon the principle of three equivalences: equivalence of consequences between hazardous failures and cyberattacks, equivalence of detection via self-diagnostic mechanisms, and equivalence of mitigation through transition to predefined safe states.

The main scientific contributions of this work are as follows:

1. the formulation of the SfISc concept and its theoretical justification through two key statements that define the conditions under which functional safety enhances cybersecurity;
2. the identification of "natural" security properties in safety PLCs, which enable the reuse of functional safety evaluation results for cybersecurity assessment of both the PLC and the Instrumentation and Control (I&C) systems built upon it;
3. the development of MFV (Mitigation-Failure-Vulnerability) metrics that quantify the overlap between failure modes and potential vulnerabilities, offering a practical tool for estimating resource savings in cybersecurity analysis;
4. the demonstration of the concept's applicability through industrial case studies involving hardware configuration changes and external communication disruptions, where safety mechanisms effectively detect and mitigate attack-like conditions.

While it cannot be claimed that safety PLCs are immune to all cyberattacks, the findings confirm that their high level of built-in security can only be compromised through the use of specialized and targeted methods. The SfISc approach does not replace comprehensive cybersecurity measures but provides a structured methodology for

leveraging functional safety insights to enhance security evaluations.

Future research will focus on developing formal procedures and quantitative indicators for assessing the completeness and effectiveness of integrated safety and security evaluations. These efforts will extend to systems based on PLC and FPGA technologies and aim to validate the SfISc concept across a broader range of industrial applications.

References

[1] "2024 Global threat roundup report," Forescout reseach, Veder Labs. [Online]. Available at: https://static.rainfocus.com/rsac/us25/exh/1435012077880001wh3P/exhibitorboothresource/2024%20Global%20Threat_1742234299083001M3n8.pdf

[2] R. Bloomfield, K. Netkachova, and R. Stroud, "Security-informed safety: If it's not secure, it's not safe," in *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berl. Heidelberg, 2013, pp. 17–32. https://doi.org/10.1007/978-3-642-40894-6_2.

[3] R. Bloomfield, "Security informed safety why its easy, why its hard," cyber.southampton.ac.uk. [Online]. Available: https://cyber.southampton.ac.uk/sites/cyber.southampton.ac.uk/files/bloomfield_ncsc_workshop2019v01d.pdf

[4] R. E. Bloomfield, P. G., Bishop, E. Butler & R. Stroud, "Security-informed safety - supporting stakeholders with codes of practice," City University of London Institutional Repository. [Online]. Available at: https://openaccess.city.ac.uk/id/eprint/20338/1/Security-Informed%20Safety%20Pre%20 Publication.pdf

[5] National Protective Security Authority, "Rail code of practice for security-informed safety," [Online]. Available at: https://www.npsa.gov.uk/system/files/documents/npsa-rail-code-practice-security-informed-safety.pdf

[6] R. Bloomfield, P. Bishop, E. Butler, and R. Stroud, "Security-Informed safety: Supporting stakeholders with codes of practice," *Computer*, vol. 51, no. 8, pp. 60–65, 2018. https://doi.org/10.1109/MC.2018.3191260.

[7] O. Ivasiuk and V. Kharchenko, "Principles of mutual information in analyzing the functionality and cybersecurity of information management systems based on programmable logic controllers," *Aerospace Technic and Technology*, no. 2, pp. 108–119, 2025. https://doi.org/10.32620/aktt.2025.2.10. (in Ukrainian).

[8] V. Greiman, "Nuclear cyber attacks: A study of sabotage and regulation of critical infrastructure," *Proceedings of the International Conference on Cyber Warfare and Security*, vol. 18, no. 1, pp. 103–110, 2023. https://doi.org/10.34190/iccws.18.1.1042.

[9] W. Alsabbagh and P. Langendörfer, "Security of programmable logic controllers and related systems: Today and tomorrow," *IEEE Open Journal of the Industrial Electronics Society*, pp. 1–35, 2023. https://doi.org/10.1109/OJIES.2023.3335976.

[10] M. Da Silva, M. Puys, H. Thevenon, and S. Mocanu, "PLC logic-based cybersecurity risks identification for ICS," *Proceedings of the 18th ACM International Conference on Availability, Reliability and Security ARES 2023*, Benevento, Italy, 2023. https://doi.org/10.1145/3600160.3605067.

[11] H. Cui, J. Hong, and R. Louden, "An overview of the security of programmable logic controllers in industrial control systems," *Encyclopedia*, vol. 4, no. 2, pp. 874–887, 2024. https://doi.org/10.3390/encyclopedia4020056.

[12] M. Medvedík, J. Ždánsky, K. Rástočný, J. Hrbček, and M. Gregor, "Safety of control systems with dual architecture based on plcs," *Applied Sciences*, vol. 12, no. 19, p. 9799, 2022. https://doi.org/10.3390/app12199799.

[13] L. Ozirkovskyy, B. Volochiy, O. Shkiliuk, M. Zmysnyi, and P. Kazan, "Functional safety analysis of safety-critical system using state transition diagram," *Radioelectronic and Computer Systems*, no. 2, pp. 145–158, 2022. https://doi.org/10.32620/reks.2022.2.12.

[14] A. Yanko, V. Krasnobayev, and A. Martynenko, "Influence of the number system in residual classes on the fault tolerance of the computer system," *Radioelectronic and Computer Systems*, no. 3, pp. 159–172, 2023. https://doi.org/10.32620/reks.2023.3.13.

[15] H. Cui, J. Hong, and R. Louden, "An overview of the security of programmable logic controllers in industrial control systems," *Encyclopedia*, vol. 4, no. 2, pp. 874–887, 2024. https://doi.org/10.3390/encyclopedia4020056.

[16] A. Tetskyi, A. Perepelitsyn, O. Illiashenko, O. Morozova, and D. Uzun, "Ensuring cybersecurity of FPGA as a service with the use of penetration testing of components," *Radioelectronic and Computer Systems*, vol. 2024, no. 2, pp. 160–172, 2024. https://doi.org/10.32620/reks.2024.2.13.

[17] X. Zhang *et al.*, "Binary-Level formal verification based automatic security ensurement for PLC in industrial IoT," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–16, 2024. https://doi.org/10.1109/tdsc.2024.3481433.

[18] H. Unniyankal, D. Ancona, A. Ferrando, F. Parodi, A. Alessi, and F. Bottino, "Runtime verification of program organization units in safe programmable logic controller systems," *Proceedings of the 2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)*, Naples, Italy, Jun. 23–26, 2025, pp. 112–118. https://doi.org/10.1109/dsn-s65789.2025.00050.

[19] A. Elmarkez, S. Mesli-Kesraoui, P. Berruet, and F. Oquendo, "Security by design for industrial control systems from a cyber–physical system perspective: A systematic mapping study," *Machines*, vol. 13, no. 7, p. 538, 2025. https://doi.org/10.3390/machines13070538.

[20] P. Bhosale, W. Kastner, and T. Sauter, "Integrated safety-security risk assessment for industrial control system: An ontology-based approach," *Proceedings of the 2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sinaia, Romania, Sep. 12–15, 2023. https://doi.org/10.1109/etfa54631.2023.10275530.

[21] A. Nouri and J. Warmuth, "IEC 61508 and ISO 26262 – A comparison study," *Proceedings of the 2021 IEEE 5th International Conference on System Reliability and Safety (ICSRS)*, Palermo, Italy, Nov. 24–26, 2021. https://doi.org/10.1109/icsrs53853.2021.9660661.

[22] G. B. Gaggero, A. Armellin, P. Girdinio, and M. Marchese, "An IEC 62443-based framework for secure-by-desing energy communities," *IEEE Access*, p. 1, 2024. https://doi.org/10.1109/access.2024.3492316.

[23] Areva NP Inc., "The digital I&C system for functions important to safety in Nuclear Power Plants. Firmendruck," Nuclear Regulatory Commission. [Online]. Available at: https://www.nrc.gov/docs/ML0910/ML091050576.pdf.

[24] O. Illiashenko, V. Kharchenko, I. Babeshko, H. Fesenko, and F. Di Giandomenico, "Security-Informed safety analysis of autonomous transport systems considering AI-powered cyberattacks and protection," *Entropy*, vol. 25, no. 8, p. 1123, 2023. https://doi.org/10.3390/e25081123.

[25] K.-L. Lu, Y.-Y. Chen, "Safety-oriented system hardware architecture exploration in compliance with ISO 26262," *Applied Sciences*, vol. 12, issue 11, p. 5456, 2022. https://doi.org/10.3390/app12115456.

[26] M. Monopoli, M. Biondi, P. Nannipieri, S. Moranti, and L. Fanucci, "RADSAFiE: A netlist-level fault injection user interface application for fpga-based digital systems," *IEEE Access*, p. 1, 2025. https://doi.org/10.1109/access.2025.3539932.

[27] Z. Gao *et al.*, "Detect and replace: Efficient soft error protection of fpga-based CNN accelerators," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, pp. 1–9, 2024. https://doi.org/10.1109/tvlsi.2024.3443834.

***OLEKSANDR IVASIUK**, graduated Kharkiv Military University (1996), PhD (2006) Poltava Military Institute of Communication. Now he is a PhD on Engineering, Doctor of Science Student at the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine. Scientific interests: PLC fault insertion testing, safety and cyber security of a I&C systems, validation of a I&C, project management of a I&C for nuclear market.*

***Prof. VYACHESLAV KHARCHENKO**, graduated Kharkiv High Military Eng. College of Rocket Troops, Dr of Sciences on Engineering (1995), Corr. Member of National Academy of Science of Ukraine (2025). Head of Dept of Computer Systems, Networks and Cybersecurity, National Aerospace University "KhAI", Kharkiv, Ukraine. Scientific interests: Dependable and resilient computing, safety and cyber security of I&C systems and critical infrastructures; Intelligent UXV systems for dangerous spaces; Explainable AI as a Service, AI vs AI scenarios.*

***PhD, HEORHII ZEMLIANKO**, obtained: MSc (2019), PhD (2024), from National Aerospace University "KhAI". Senior Lecturer of Dept. of Computer Systems, Networks and Cybersecurity, National Aerospace University "KhAI", Kharkiv, Ukraine. Scientific interests: cybersecurity of UAV systems, game information technologies, UX/UI Design, Internet of Things and Smart-technologies.*