IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Journal Européen des Systèmes Automatisés
Vol. 59, No. 3, March, 2026, pp. 717-728
Journal homepage: http://iieta.org/journals/jesa

A Systematic and Bibliometric Review of Formal Methods for Securing Industrial Control Systems and Programmable Logic Controllers (2002-2025)

Salwa Amazigh*, Hassan Echoukairi, Soumia Ziti

Equipe of Intelligent Processing and Security of Systems, Faculty of Science, Mohammed V University in Rabat, Rabat 1014, Morocco

Corresponding Author Email: salwa_amazigh@um5.ac.ma

https://doi.org/10.18280/jesa.590315

Received: 5 November 2025
Revised: 3 February 2026
Accepted: 12 February 2026
Available online: 31 March 2026

Keywords:
Industrial Control Systems, Programmable Logic Controllers, Petri nets, Security, Supervisory Control and Data Acquisition, PRISMA

ABSTRACT

The Industrial Control Systems (ICS) and Programmable Logic Controllers (PLCs) are important parts of current industrial infrastructures, and the breach of security in them can cause serious safety and economic implications. The increasing connectivity of industrial environments between industrial settings has augmented the attack area of such systems, and effective security assurance software is therefore crucial. Formal techniques offer mathematically sound strategies for testing the safety and security characteristics of ICS and PLC-based systems. The presented paper presents a systematic and bibliometric review of the literature on the use of formal methods to secure ICS and PLC systems. The literature review research was done through the Scopus database, which contains publications from 2002 to 2025. This paper uses the PRISMA approach to a clear and reproducible selection of the related studies. The bibliometric analysis was used to determine the tendencies of publications and prevailing research topics, whereas the qualitative comparative analysis was used to study the frequently used formal methods such as Petri nets, automata-based methods, model checking, theorem proving, and hybrid system methods. These findings indicate the growing research focus on security-by-design frameworks and model checking tools. Moreover, the paper pinpoints critical issues associated with scalability, modelling complexity, and implementation in industry and provides possible research paths on how the security of the industrial control system can be enhanced.

1. INTRODUCTION

Industrial Control Systems (ICS) and Programmable Logic Controllers (PLCs) are vital elements of infrastructure charged with the responsibility of managing the physical process of manufacturing systems, energy networks, utilities, and other vital services. These systems are critical to safety and are also getting exposed to networked environments, thus making security assurance a significant research question. In that regard, the use of formal methods has been of great interest, being the mathematically sound means of checking both the security and safety properties of various abstraction layers.

Formal verification is the method that allows demonstrating or disproving whether a program or a system meets its specifications or other desired aspects based on logical arguments [1].

In industrial control applications, both safety and security requirements are often included in the specifications, and formal methods are especially suited to this area. Formal approaches to risk reduction, through the provision of exhaustive and sound verification guarantees, alleviate risks related to software defects, malicious attacks, and unintended behaviors of the system.

A rich assortment of formal methods can be used when industrial cyber-physical systems are modelled as hybrid systems, which are discrete control logic and continuous physical dynamics. They are model checking, satisfiability modulo theories (SMT) solving, non-standard analysis, process calculus, concolic testing, and theorem proving [2-5]. Although they have theoretical strength, one of the primary problems of methodology implementation is the inability to establish correct formal models that adequately describe the interactions of PLC programs with the physical processes that occur [3].

The use of formal verification on industrial control logic has been subject to development over the last three decades. Initial experience with the verification of control logic programs proved that the latter was indeed possible, with more recent work indicating that PLC software is specific to formal verification because it is written in graph-based programming languages, it runs in a deterministic manner, and its code is not particularly large [1, 6]. There are two primary paradigms of formalization, in general, in this field: model checking, which uses temporal logic and state-space exploration to prove the correctness of systems, and theorem proving, which interprets systems in the form of logical formulas and demonstrates their correctness by using deductive reasoning [1]. These methods have been used in numerous studies that have been able to increase the safety and security of PLC programs [7].

Parallel to verification-oriented methods, security-by-

design models have also become a proactive method of securing ICS. Instead of applying retrofitting to address the deployed security mechanisms, these frameworks incorporate security requirements into the system development cycle and use the published industrial standards to inform the design of secure PLC applications.

A prominent one is that the IEC 61499 function block standard is utilized to enable security-conscious PLC development. This practice allows the designers to mark important parts in the design phase that are then automatically secured by appropriate security measures at the deployment stage [8]. These are achieved with the help of IEC 61499 Service Interface Function Blocks (SIFBs), which incorporate Intrusion Detection and Prevention System (IDPS) functionality, which is automatically compiled into the application [8].

Even though formal verification and industrial cybersecurity have been the focus of more and more studies, there are still a number of limitations associated with the existing literature. The literature is typically dedicated to particular verification methods or particular industrial standards without giving a clear picture of the various formal methods to provide security to ICS and PLC systems. Moreover, numerous studies focus on theoretical points and fail to explicitly discuss the practical issues regarding scalability, model complexity, as well as its application to the real-world industrial environment.

Thus, the goal of this paper is to deliver a systematic and bibliometric review of security strategies using formal methods in the context of ICS and PLCs. The aim of the analysis will be to examine the development of the research trends, the most common formal techniques applied, and to pinpoint the key challenges and gaps in the research in this field.

The rest of this paper will be structured in the following way. Section 2 is the research methodology with the choice of the database, establishment of keywords, and the inclusion and exclusion criteria. Section 3 provides the findings of the bibliometric analysis, including the description of the retrieved data, the development of the scientific production, citation and impact analysis, the major publication sources, geographical distribution of research production, and the analysis of the keywords, including word clouds, thematic systematization, trend topics, co-occurrence networks, and international collaboration patterns. In Section 4, we have presented a comparative analysis of formal-method-based security solutions of the ICS and Programmable Logic Controllers (PLCs).

Section 5 concentrates on the formal-method-based anomaly detection methods for ICS and PLC systems, whereas Section 6 provides a summary and comparison of formal tools that are employed in securing the industrial control environment. The key issues and constraints are addressed in Section 7. Lastly, the paper concludes with a discussion of future work in Section 8.

2. RESEARCH METHODOLOGY

This section aims to describe and explain the methods followed in the bibliometric mapping and systematic evaluation of the scientific literature covering the subject of the security of the ICS and PLCs assessment in formal methods. The overall methodological background that was followed by this study in carrying out the literature review is shown in Figure 1. The review is conducted in a systematic fashion using the PRISMA (Preferred Reporting Items to Systematic Reviews and Meta-Analyses) methodology that guarantees transparency and reproducibility of the selection of the relevant studies.

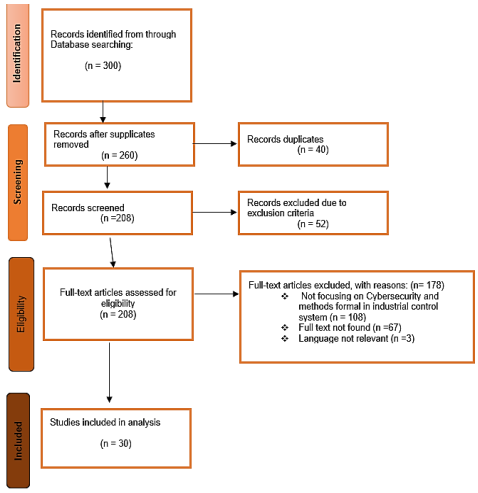

Figure 1. Methodology for conducting a bibliometric analysis

This section will explain the bibliometric and systematic review processes that will be employed to chart and examine the research environment at the cross-section of ICS and PLC security measures and formal verification methods. The methodology entails a number of steps, which constitute identification of databases, keyword search, screening of titles and abstracts, eligibility evaluation, and eventually selection of the relevant publications to be subjected to bibliometric analysis. The chosen bibliometrics techniques offer a highly organized and reproducible structure for attaining the research aims and objectives, and allow establishing the influential publications, leading authors, high-profile journals and conferences, and new research topics concerning the use of formal methods in industrial control settings.

The methodology selected enables the systematic investigation of the research trends in the context of the protective safety and resiliency of ICS and PLC-based systems, especially in the context of the growing complexity of systems and the cyber-physical integration.

Quantitative bibliometric indicators were used to measure the performance of publications, authors, venues, and countries, such as performance analysis and science mapping methods [9, 10]. These methods contribute to the measurement of the productivity of research, patterns of collaboration, and developmental trends in the sphere. Also, bibliometric analysis allows studying the knowledge diffusion and research impact in the academic and industrial spheres. The study offers an intellectual organization of the practice through the analysis of publication dynamics, authorship dynamics, keyword co-occurrence, source distribution, and citation dynamics based on a corpus of research articles that were published in the period between 2002 and 2025.

2.1 Database selection

The initial phase of the process of selecting the appropriate publications was the identification and assessment of the

appropriate data sources. The reason behind using Scopus was its wide and multidisciplinary coverage of the academic literature, including the works of the major publishing houses, including IEEE, Elsevier, Wiley, Springer, and Taylor and Francis. Scopus was used instead of the Web of Science due to its extensive citation index that offers a more extensive platform to base citation research. The research follows these guiding questions to structure its bibliometric evaluation:

Main questions (RQ)

- **RQ1:** What has changed in terms of publications, venue, and such citations (2002-2025) in research on formal methods to ICS and PLC security?
- **RQ2:** What are the significant thematic groups related to the literature on formal verification and anomaly detection of ICS/PLC security?
- **RQ3:** What are the most frequently employed formal means of identifying anomalies and security threats associated with ICS and PLC systems?
- **RQ4:** What are the new formal method-based security strategies that are occurring, and when did they become prominent?

2.2 Keyword selection and Inclusion/exclusion criteria

The choice of keywords was informed by this research purpose, for which the research objective was to have a comprehensive search on the research regarding the security of the ICS and PLCs and the use of formal verification in industrial cyber-physical systems.

The keywords were categorized into two broad conceptual domains to assure the use of a systematic and reproducible search strategy: (1) ICS and automation technologies, and (2) formal verification and security analysis methods.

On these dimensions, a search query was formulated and implemented on the Scopus database. The query was a combination of the terms concerning industrial control technologies (PLC, ICS, SCADA, and Industrial Internet of Things) and formal verification methods (Petri nets, automata, state machines, and model checking) and security-related concepts.

The search query that will be used in the study is as follows:

((plc OR "programmable logic controller" OR "ICS" OR "SCADA" OR "industrial internet of things" OR "function block") AND ("Petri net*" OR automata OR "state machine" OR "model checking" OR "formal verification" OR "timed automata") AND (security OR intrusion OR attack OR verification)).

This query was designed to capture publications addressing both formal-modelling techniques and cybersecurity aspects in industrial control environments.

In order to guarantee the quality and topicality of the chosen publications, a group of inclusion and exclusion criteria was utilized in the course of the screening. Table 1 shows the summary of these criteria.

Table 1. Inclusion and exclusion criteria used for the selection of relevant studies

Criteria Type	Inclusion Criteria	Exclusion Criteria
Publication type	Peer-reviewed journal articles and conference papers	Books, editorials, short surveys, errata, conference summaries
Language	Publications written in English	Publications in other languages
Time period	Publications between 2002-2025	Publications outside this period
Access type	Open-access publications	Restricted access publications
Subject area	Computer science, cybersecurity, industrial automation, control systems	Biochemistry, medicine, agriculture, psychology, arts, economics, pharmacology
Topic relevance	Studies related to ICS, PLC, SCADA security and formal methods	Studies not related to ICS or formal verification
Screening stage	Papers validated through title, abstract and keyword analysis	Papers with irrelevant titles or abstracts

3. RESULTS OF THE BIBLIOMETRIC ANALYSIS

3.1 Overview of retrieved data

Figure 2 gives an overall summary of the key bibliometric measures, calculated based on the quantified dataset, consisting of 800 articles published between the years 2002 and 2025 and in 226 different sources, such as journals and conference proceedings. It is a corpus varied with 1,709 authors and reflecting the working as a group aspect of studying the subject area, which is formal methods applied to the security of ICS and PLCs. Notably, no single-authored publications were identified, indicating that research in this domain is predominantly conducted through collaborative efforts. The consideration of a scientific growth rate of 5.15 percent per year is an indication of a constant and sustained interest in research in the field of study, as it indicates the rising significance of security and formal verification of ICS. The estimate of international co-authorship is 20.25%, and it is important to note that the average number of co-authors per document is relatively high (6.7), which indicates that the field is multidisciplinary and it may need skill at the level of cybersecurity, control engineering, and formal methods. The data has a total of 5,178 cited sources, which represent a good theoretical base and a high level of dependence on previous academic literature. Moreover, the mean document age of 10.2 years and mean of 12.5 citations per document indicate that the field incorporates the well-established foundational research with a steady flow of new contributions and makes formal-method-based security of ICS and PLCs an active and dynamic field of research.

Figure 2. Descriptive statistics of publications, which were extracted between 2002 and 2025

3.2 History of the development of scientific production

As it is presented in Figure 3, there was a comparatively low level of scientific production connected with the application of formal methods to assure ICS and Programmable Logic Controllers (PLCs) in the early years of the research period, the period between 2002 and around 2008. It can be seen thereafter that a gradual increase is followed by moderate growth between 2009 and 2014. Since 2015, the pattern of publications has started showing a stronger increasing trend, as this signifies the increasing research topic owing to the increasing issues with cybersecurity in industrial and cyber-physical settings.

The sharpest increase is after 2016, which is associated with the growing interest in Industry 4.0, the industrial connection, and the necessity of the strict security guarantee methods. The peak of the trend is expected to be observed in 2023-2024, which means that the research activity on formal-method-based security measures in ICS and PLC systems will be at its peak. The fact that the numbers have been slightly reduced in 2025 is probably because the year has not been completely published.

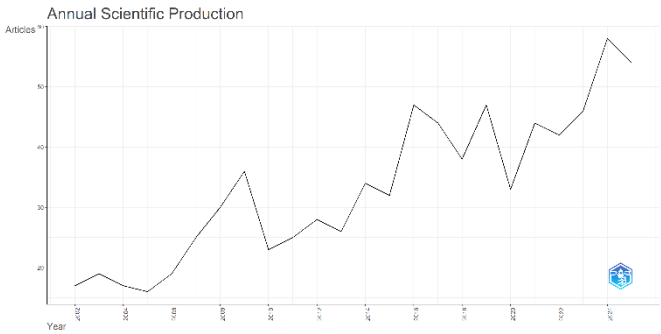

Figure 3. Annual publication count of journal articles

3.3 Citation and impact analysis

Figure 4 illustrates how the popularity of the field of formal method-based security in ICS and PLC systems has changed over the years in terms of the number of citations. Some definite peaks can be found in the late 2000s and once more in the late 2019-2020, which can be attributed to the influence of some underlying and modern research. This is because the number of new publications is decreasing over the last few years, mostly because of the little time left before the newly published articles can gather many citations.

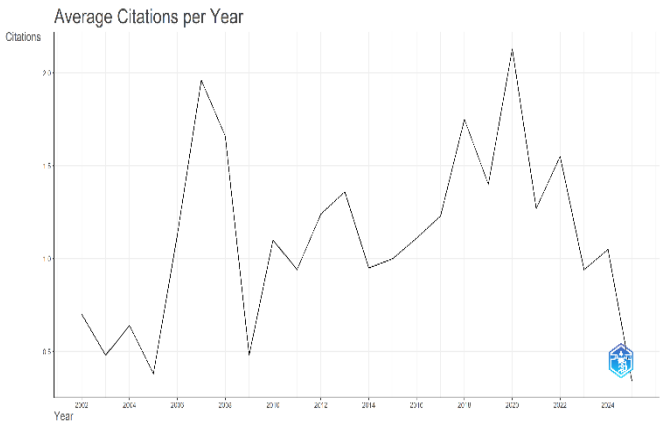

Figure 4. Citation and impact analysis

3.4 Mapping affiliation authors, sources, and thematic domains

Figure 5 shows the mapping of authors' affiliations and sources of publications and thematic field in the subject matter of formal method-based security of ICS PLCs. The number shows that academic and research institutions are very active in producing leading journals and conference proceedings, including Lecture Notes in Computer Science, IEEE Access, and major IEEE conferences. The primary themes of focus are PLCs, model checking, formal verification, ICS, and network security, which show a strong resonance between the institutional research knowledge, publication sites, and the prevailing research interests in the field.

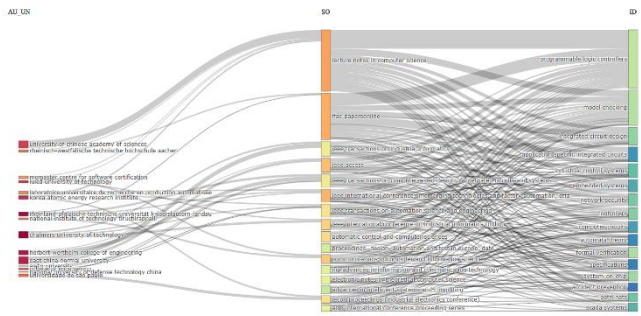

Figure 5. Mapping affiliation authors, sources, and thematic domains

3.5 Core publication sources

Figure 6 points out core publication sources in the area of security in ICS and PLCs by means of the formal approach. Lecture Notes in Computer Science is the most prolific with 65 publications, and this is an indicator of the powerful influence of the research based on conference-oriented research in this field.

It is preceded by IFAC-Papers Online (28 documents), IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) (16 documents) that confirm the significance of automation and industrial informatics forums. Different IEEE journals and conference papers, such as IEEE Access, IEEE Transactions on automation science and engineering, and IEEE International Conference on industrial informatics, are also sources of literature. Such a distribution shows a peer-reviewed conference and high-impact journal literature-dominated research landscape, the interdisciplinary character of ICS and PLC security research, which cuts across formal methods, automation, and industrial informatics.

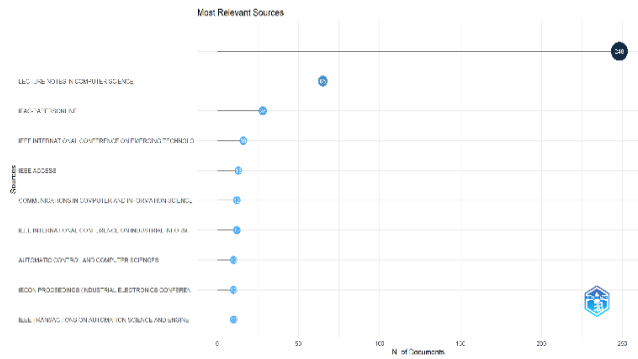

Figure 6. Core publication sources

3.6 Scientific output by country

Figure 7 shows how publications are distributed by country using the respective author, differentiating between single-country publications (SCPs) and multiple-country publications (MCPs). It has been revealed that China, the United States, and Germany have the highest contributions to the scientific output concerning formal-method-based security in the field of ICS and PLCs. The compensation of the publications on the countries is a significant percentage of global collaboration; it demonstrates that there is an active involvement in the global research networks. Other European nations such as France, Italy, Sweden, and the United Kingdom are also showing commendable contributions despite a decreased volume. On the whole, the presence of MCPs in a number of countries indicates the increased significance of international research cooperation in the development of formal verification and cybersecurity systems to protect ICS, which allow the exchange of knowledge and innovation on a global scale.

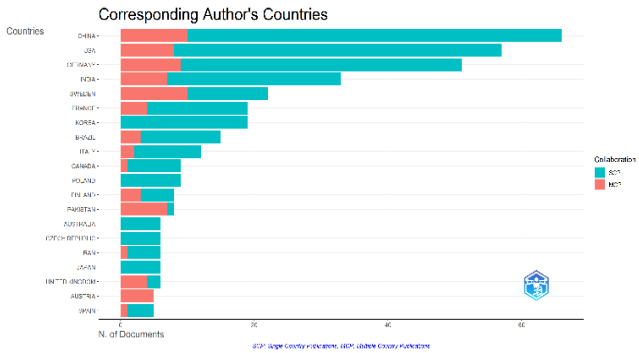

Figure 7. Countries and international collaboration of the corresponding author

3.7 Word cloud representation

Figure 8 presents the prevailing themes of research on formal method-based security of ICS and PLC systems. The keywords like “Programmable Logic Controllers”, “model checking”, and “formal verification” are placed in the central position, and such keywords as “Petri nets” and “network security” are used to show the emerging and complementary directions of research.

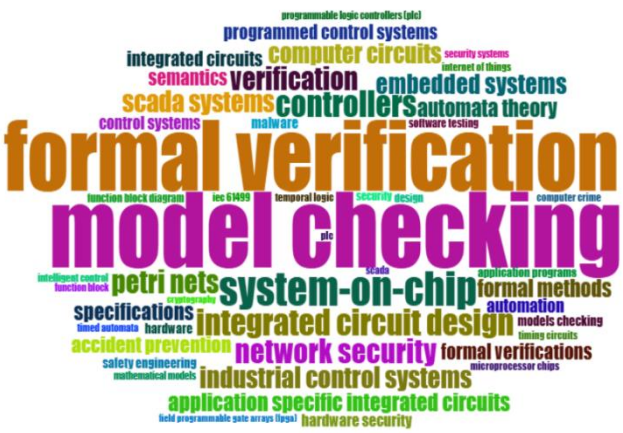

Figure 8. Word cloud representation

3.8 Thematic systematization of research on formal-method based security of Industrial Control Systems and Programmable Logic Controller systems

Table 2 presents a summary of the thematic distribution of the publications that deal with the security of ICS and PLCs via formal methods. Those results indicate that the most noticeable research theme is PLC verification (25.0%), then model checking methods of the ICS/SCADA and Petri-net based methods, each taking 19.0% of the literature. The automata and state machine-based approaches (15.0%), and formal method-supported intrusion and anomaly detection (16.0%) based approaches are also significant research topics. Conversely, the topics connected with testing and reconfiguration constitute a less significant portion (6.0%), which points to new directions that can become more important as the requirements of industrial security continually advance.

Table 2. Thematic distribution of publications on formal method-based security for Industrial Control Systems (ICS) and Programmable Logic Controllers (PLCs) systems

Thematic Category	Documents	%	Dominant Terms (Examples)
PLC Verification	200	25.0	PLC, formal semantics, Coq, ladder diagram, program verification
Model Checking for ICS/SCADA	150	19.0	model checking, ICS security, SCADA properties, anomaly detection
Petri Nets & Whitelisting	150	19.0	Petri nets, whitelist PLC, SFC modelling, safe PLC programs
Automata & State Machines	120	15.0	timed automata, state machine, security properties, fallback control
Intrusion / Anomaly Detection	130	16.0	intrusion detection, cyber-attacks, anomaly detection, IIoT
Other (Testing / Reconfiguration)	50	6.0	function block testing, reconfiguration, Schedulability analysis

3.9 Trend topics

Figure 9 shows how the research topics in the area of formal-method-based security in industrial systems have changed over the years. During the initial years of the research time frame (2002-2008), the research primarily involved the study of basic notions of formal languages, automata theory, and the synthesis of control systems, which formed the conceptual basis of the subsequent progress in formal verification.

The direction of research changed during the years 2010-2016, when greater attention was paid to the use of formal techniques in industrial settings. It became dominated by topics like Petri nets, model checking, PLC verification, and SCADA systems as an expression of growing interest in the application of formal verification to ICS.

Since 2018, there has been a shift in the area of research,

with the focus on the issues of cybersecurity. Cyber-attacks, network security, embedded systems, and system-on-chip architecture also became more important issues, and this indicates that there was increased concern over the protection of industrial infrastructures against cyber attacks.

The trend of the research tends to shift towards a growing interest in cyber-physical security and industrial systems in the framework of Industry 4.0 in the last few years (2022-2024). This change is undergoing an increasing convergence of the ICS and advanced communication systems, and intelligent manufacturing space. Such trends suggest a recent global trend to security assurance of ICS, and more and more emphasis is given to formal verification, intrusion detection, and resilience of connected ICS and PLC environments to the changing threats of Industry 4.0.

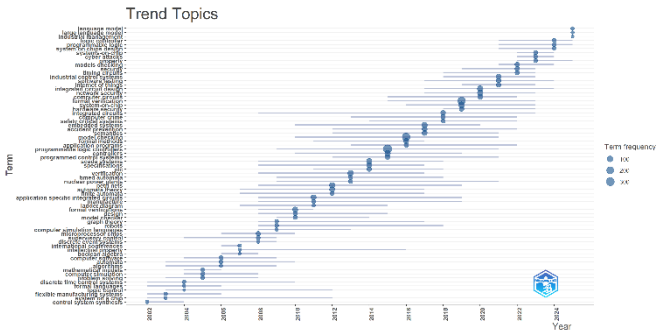

Figure 9. Trend topics

3.10 Co-occurrence network of keywords

Figure 10 displays a network of co-occurrence of keywords, indicating that these words are at the center of the literature: it is evident that “Programmable Logic Controllers”, “model checking”, and “formal verification” are core ideas of the literature. Tightly-knit families around “ICS”, “SCADA systems”, and “Petri nets” point to the high degree of integration between formal-modelling and industrial security issues. Less central, though more applicable clusters, such as “network security”, “embedded systems”, and “system-on-chip”, indicate the incorporation of cyber, software, and hardware viewpoints in securing contemporary industrial and cyber-physical systems.

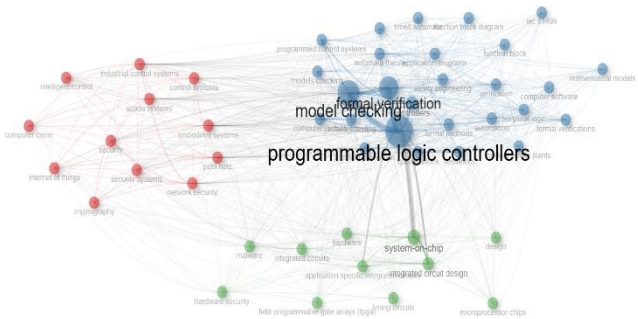

Figure 10. Co-occurrence network

3.11 World map of scientific collaborations

Figure 11 of the map of the world scientific production proves that China, the United States, and some European nations have the largest contribution to the formal method-based security of ICS. The high research activity has been centralized in North America, Europe, and East Asia, with good academic and industrial ecosystems existing in these areas. Conversely, other parts of Africa, Latin America, and certain parts of Asia have lower rates of scientific output meaning that they have fewer involvement in this field of research. In general, the identified distribution indicates that the topic of international research is globally relevant, but the capacity of countries and the cooperation stay unequal, and the prospects of the enhancement of cross-regional collaboration and exchange of knowledge in securing ICS can be identified.

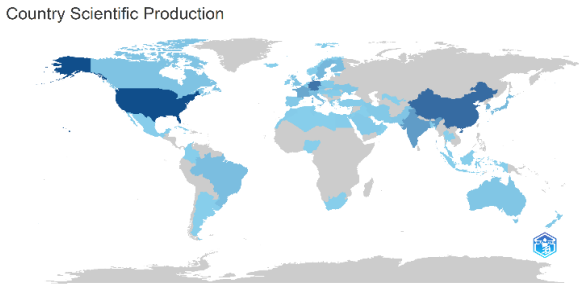

Figure 11. Geographical network of collaborations by country

3.12 Best cited references in the research on industrial cyber security

Table 3 provides the most referred publications in the sphere of industrial cybersecurity and features some of the seminal works, which made a significant impact on the research of the ICS, SCADA settings, and the security issues therein. Vulnerability assessment, intrusion detection, and secure modelling of industrial communication protocols are the most cited studies, which is why they were chosen as they formed the basis of future research. The predominance of the articles published in 2006-2014 shows that a great number of fundamental ideas related to industrial cybersecurity were developed in the specified time-frame and remained one of the primary references.

On balance, the reference rates of these works indicate the relevance and the prospects of the future development of security analysis, detection systems, and protection measures of industrial and cyber-physical networks.

4. COMPARATIVE STUDY OF FORMAL-METHOD-BASED SECURITY SOLUTION OF ICS AND PLC SYSTEMS

This part gives a comparative study of the primary security strategies according to formalized approaches to ICS and PLCs. Table 4 provides an overview of the typical studies that use formal methods to improve the security and reliability of industrial control settings.

As can be seen, the existing solutions consider various levels of the system architecture, starting with PLC firmware and control software and moving to networks of distributed controllers and cyber-physical interactions. These works are dedicated to a broad spectrum of security risks, such as software vulnerabilities, network attacks, malicious code infections, and malicious control logic, including Ladder Logic Bombs.

Table 3. Most cited articles in Industrial Control Systems (ICS)/SCADA and industrial cybersecurity research

Document Title	Authors	Source	Year	Citations
Vulnerability assessment of cybersecurity for SCADA systems [11]	Ten et al.	IEEE Transactions on Power Systems	2008	539
Active hardware metering for intellectual property protection and security [12]	Alkabani and Koushanfar	USENIX Security Symposium	2007	325
Accurate modelling of Modbus/TCP for intrusion detection in SCADA systems [13]	Goldenberg and Wool	International Journal of Critical Infrastructure Protection	2013	286
Case study: Detecting hardware Trojans in third-party digital IP cores [14]	Zhang and Tehranipoor	IEEE HST	2011	201
Remote activation of ICs for piracy prevention and digital rights management [15]	Alkabani et al.	IEEE/ACM ICCAD	2007	165
High-performance pattern-matching for intrusion detection [16]	Van Lunteren	IEEE INFOCOM	2006	161
TABOR: A graphical model-based approach for anomaly detection in ICS [17]	Lin et al.	ACM ASIACCS	2018	150
Provably secure active IC metering techniques for piracy avoidance and digital rights management [18]	Koushanfar	IEEE Transactions on Information Forensics and Security	2012	147
Concurrent secrets [19]	Badouel et al.	Discrete Event Dynamic Systems	2007	129
Reverse engineering digital circuits using structural and functional analyses [20]	Subramanyan et al.	IEEE Transactions on Emerging Topics in Computing	2014	112

Table 4. Comparative analysis of formal-method-based security approaches for Industrial Control Systems (ICS) and Programmable Logic Controllers (PLCs) systems

Target System Components	Security Vulnerabilities Addressed	Formal Method / Tool	Protection Measures and Verification Goal
PLC firmware, operation, and control programs [21]	Firmware, operation, and program-level security defects	Code formal verification	Verifiability protocol encoding, formal code analysis to detect and avoid PLC security flaws.
Distributed sequential controllers, IIoT controllers, CIPN-based control applications and firmware [22]	Network-based attacks (DoS, ACK spoofing, impersonation, replay, message modification)	Control Interpreted Petri-Nets (CIPN), Time Petri Nets (TPN)	MAC based authentication, attack detection, security patching, system-level safety verification in the presence of attacks
Networks of PLCs, actuator commands, sensor readings, inter-controller communications [23]	Cyber-physical attacks, mal-ware, tampered actuator commands and sensor readings	Edit Automata, Timed Process Language	Checking of the specification by runtime verification through secure proxies and monitors in compromised controller net-works
Programmable Logic Controllers (PLCs), Ladder Logic programs [24]	Ladder Logic Bombs	Formal verification	Formal verification architecture of detection of malicious logic (LLBs) in PLC programs.

The literature makes use of several formal verification methods, such as code-level formal verification, Petri-net-based modelling, edit automata, and runtime enforcement mechanisms. These methods offer strict mathematical models of system behavior analysis, safety and security property verification, abnormal and malicious system behavior detection in industrial settings.

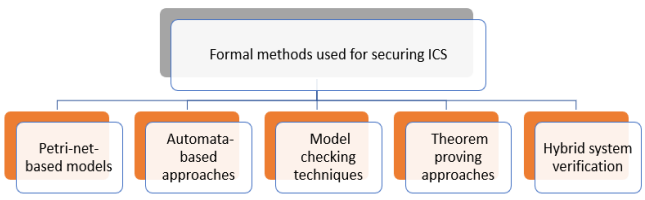

Figure 12. Classification of formal methods used for securing Industrial Control Systems (ICS) and Programmable Logic Controllers (PLCs) systems

As shown in Figure 12, formal techniques of securities of ICS and PLC systems can be classified broadly based on their modelling and verification principles. The key ones are Petri-net-based models, automata-based models, model-checking techniques, theorem-proving techniques, and hybrid verification of systems. In general, the literature demonstrates an increasing inclination to combine formal verification algorithms with proactive security issues like attack identifiers, authentication measures, and run-time monitors in preparation to enhance the quality and sustainability of industrial control frameworks to respond to changing cyber threats.

In order to further organize the various formal approaches found in literature, Figure 12 gives a classification of the major categories of formal methods of securing ICS and PLC systems.

5. FORMAL METHOD-BASED ANOMALY DETECTION IN ICS AND PLC SYSTEMS

In this section, we will have a comparative analysis of the major anomaly detection techniques used on ICS and PLCs using formal methods. They are based on formal models, which are used to model normal system behavior and identify any deviation that can be a sign of system faults or cyber-attacks.

Table 5 gives an overview of the representative anomaly detection methods that apply to formal methods of industrial control settings. The methods reviewed use formal modelling models like Petri nets, timed automata, reachability analysis, and process mining to describe the normal operation patterns

and detect the abnormal behaviors. These methods counter a large spectrum of attacks, such as control logic manipulation, network-based attacks, timing attacks, and cyberspace anomalies in cyber-physical interactions. Formal methods allow identifying deviations in the expected system behavior by modelling the expected system behavior, which in turn can be malicious activity or faults in the operation of the system.

Table 5. Formal methods- based anomaly detection approach for Industrial Control Systems (ICS) and Programmable Logic Controllers (PLCs) systems

Anomaly Detection Approach	Description
Whitelisting [25-27]	PLC programs transformed into Petri nets (SFC→Petri); non-listed operations detected.
Model-based IDS [28, 29]	Formal ICS Petri net models of devices and communications; comparison between observed traffic/behavior and formal models.
Process Mining [30]	Petri net recovery of sensor logs; checking conformance with normal executions.
Distance-based Methods [31]	Calculation of distances between current states and critical states of a system by means of Petri nets and process models.
Formal-Method-Assisted ML [32]	Formally guided outlier scoring; encoding malware behavior rules using timed automata and Petri nets.
Reachability & P-Invariants [33, 34]	P-invariants to detect sensor and actuator faults combined with reachability analysis and model checking.

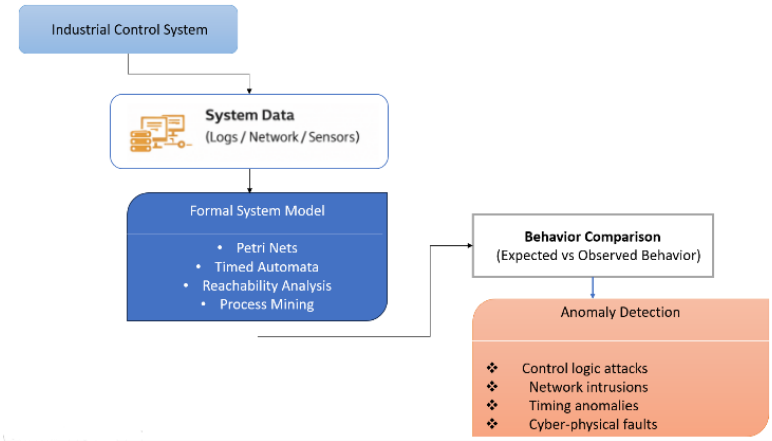

Figure 13. Formal-method-based anomaly detection framework for Industrial Control Systems (ICS)

In general, the findings that are summarized in Table 5 reveal that formal models can offer interpretable, state-aware, and proactive anomaly detection mechanisms in industrial settings. The analysis, however, also identifies that there are several practical limitations such as the accuracy of system models, scalability issues, and the complexity of implementing formal verification methods in large-scale industrial infrastructures.

Figure 13 shows a conceptual structure of anomaly detection in ICS and PLCs based on formal methods. It starts with the gathering of system data, logs, network traffic, and sensor measurements that the industrial control environment creates.

They are then analyzed with the help of formal system models, i.e. Petri nets, timed automata, reachability analysis, and process mining systems that are applied to the model, and check the anticipated system behavior.

The system behavior observed is then checked against the one that is to be experienced as per the formal model to measure deviations that may arise. Lastly, the anomaly detection phase detects events that are abnormal, which can be related to control logic attacks, network intrusion, timing anomalies, or cyber-physical faults of the industrial process. To demonstrate how formal models can be applied to the detection of anomaly in an industrial setting, Figure 13 shows a conceptual model of the key steps of the overall detection process.

6. COMPARISON OF THE FORMAL TOOLS OF SECURING INDUSTRIAL CONTROL SYSTEMS AND PLC SYSTEMS

This part is a systematic comparative study on the primary formal techniques of analyzing, verifying, and enhancing the security of ICS and PLCs. The comparison will concentrate on some of the main aspects: the nature of the threats being dealt with, the assessment metrics commonly used in evaluation, and the benefits and constraints of each of the formal techniques. Table 6 is the summary of the best-known formal techniques used in ICS and PLC security, consisting of Petri nets, automated models, model checking, protocol inference methods, hybrid modeling, and so on.

The comparison points out that Petri-net-based models and model checking techniques are some of the most popular methods of checking the correctness of control logic, safety breaches, and sequence anomaly existence with regard to industrial control programs. Recent works in 2024 and 2025 also substantiate the topicality of these practices, especially to identify manipulation of control logic and perform verification of the program behavior of the PLCs. Indicatively, in the recent past, PLC control-logic structural analysis has been shown to be effective in identifying malicious modification and logic-based attacks on an industrial controller using formal representations of control logic.

Timed automata and timed Petri nets are quite useful in the

analysis of time-related vulnerabilities and identification of timing-based attacks in real-time industrial systems. Similar studies also examine the topic of hybrid methods that can be used to merge formal modeling with behavioral analysis to enhance anomaly detection in cyber-physical industries. Moreover, protocol inference and behavior modeling approaches have also been used in recent times to identify unknown or zero-day attacks based on learning communication patterns and state transitions in industrial networks.

Even though these formal techniques have rigorous and interpretable security guarantees, a number of practical constraints exist. Table 6 shows that state-space explosion, scalability problems, and the expensive modeling of complex industrial infrastructures remain some of the barriers to their large-scale implementation in the industry. In general, the comparison points out the trade-offs between expressiveness, detection accuracy, and more practical usability in using formal methods to secure the ICS and PLC systems, as well as the increasing trend of using hybrid and intelligent verification frameworks in recent studies.

Table 6. Formal methods for securing Industrial Control Systems (ICS) and Programmable Logic Controllers (PLCs)

Formal Method	Threat Types Analysed	Commonly Used Metrics	Advantages	Limitations
Petri-Nets (2025) [35]	Logic attacks, failure mode, sequence, anomaly.	Size of state-space, verification time, state coverage	Successful concurrency and industrial process modelling.	Poor scalability of the large scale systems.
Timed Petri-Nets (2024) [36]	Timing attacks, maladaptive delays.	Detection latency, timing constraint satisfaction.	Brings in time into security analysis.	Computational complexity High complexity.
Timed Automata (2022) [37]	Attacks based on delay, replay attacks.	Exploration latency, detected states.	Properly adapted to real-time systems.	State space explosion.
Model Checking (LTL/CTL) (2025) [38]	Manipulation of logic, property violation.	verification time, states explored.	Intense and diligent for mality checking.	Expensive and time-intensive modelling.
Model Protocol Inference (2025) [39]	Unknown (zero-day) at-tacks.	Accuracy of inferences, error.	Appropriate to proprietary or un-documented proto-cols.	Kind of dependent on the quality of traffic and representativeness.
Control-logic structural analysis + behavioral modelling (2025) [40]	PLC code manipulation, logic bombs.	Detection accuracy, false positive rate.	Detects malicious PLC logic modifications.	Requires access to PLC code.
behavioral modelling + anomaly detection (2025) [41]	abnormal industrial processes, cyber attacks.	F1-score(95,42) detection rate.	Effective for dynamic systems.	Data dependency.
digital twin + formal system modelling (2025) [42]	cyber-physical attacks.	system deviation detection, reliability.	Real-time monitoring.	Complex implementation.

7. DISCUSSION

The bibliometric analysis reveals that the research on the topic of formal security verification of the ICS and PLCs is dominated by model checking and Petri-net-based technology. Nonetheless, the review of the literature indicates that much of the available literature is primarily theoretical validation instead of a large-scale application in industries. This observation correlates with established drawbacks of the formal verification methods, especially the state-space explosion problem and scalability concerns, in the context of their implementation in the complex industrial settings. Nevertheless, even with solid mathematical backgrounds, there are multiple technical and operational difficulties with the practical use of the formal methods for the security of ICS and PLC systems. Among the most outstanding ones, there is the discrepancy between the research-based validation and the actual industry practice. The fact that most ICS security architectures have been tested by simulation or in controlled experimental settings, formal approaches are seldom used to model and prove working industrial infrastructures and are still mostly limited to research [43]. Besides this gap of implementation, there is also another significant constraint that relates to the scope of verification. The majority of the current solutions are mostly concerned with the software analysis of the PLC source code, and do not address other essential areas like compile-time bugs, binary-level attacks, and program behavior during runtime. Thus, a number of types of attacks that take place during the execution of the program, as well as at the firmware level, cannot be properly identified with the help of the existing formal verification methods [44]. Furthermore, formal models using specifications often impose a large amount of manual work on the domain expert, or even direct access to PLC code, which is not readily accessible in the industrial world. Although data-driven and machine-learning-informed methods are more flexible and adaptable, they are not always interpretable and do not have formal guarantees, which restricts the application of such methods in

safety-critical industrial processes [45]. Moreover, scalability is also a significant challenge since the growing complexity of the modern ICS networks only intensifies the problem of state-space explosion, which becomes computationally challenging to exhaustively verify. Formal verification techniques also necessitate specialized experience that is usually limited in an operational setting where formal verification techniques are integrated into industrial operational workflow.

To address these issues, recent research trends show that there has been increased interest in integrating formal methods of verification with smart and information-rich methods in an effort to eliminate the shortcomings of the strictly formal models. More specifically, formal verification combined with artificial intelligence has become one of the promising areas of research that can enhance scalability and adaptability in industrial cybersecurity. Hybrid methods seek to use the mathematical assurances of formal methods and take advantage of the learning and pattern recognition of artificial intelligence to identify complex or shifting patterns of attack. The other research direction is of importance as it focuses on the automation of formal model generation, which is a process that is known to be expensive and time-consuming. Machine learning algorithms could be useful in deriving formal models of PLC programs, forming state machines out of network traces, and creating Petri-net-like forms out of sensor and actuator logs. These automated model extraction methods may enormously cut the manual labor needed in the system specification as well, as speed up the verification process in the real-life industry setup. Moreover, the combination of runtime verification and adaptive anomaly detection mechanisms is also discussed as a topic of recent research. Formal models in this case can be used to specify valid system states as well as safety constraints, whereas AI-based detectors can be used to monitor real-time operation data and detect abnormal behavior. The runtime enforcement mechanisms may be activated when the two mechanisms confirm the occurrence of anomalous activity in order to stop unsafe system actions. Such an overlay verification approach enhances the strength, readability, and safety of ICS as well as the formal correctness assurances. The latest trends in anomaly detection methods in ICS and PLC environments also indicate these new areas of research. Specifically, a few of the studies suggest anomaly detection tools that examine the structures of the PLC control logic and the operational data to determine any malicious code modifications or abnormal control flows present in industrial settings [40]. As an example, Lee et al. [40] presented a control-logic-based anomaly detection model that can detect malicious changes to the PLC program through learning the structural properties of control logic instructions. Equally, there are other works that discuss more sophisticated hybrid detection constructs that integrate machine learning or deep learning models with formal system behavior modelling to enhance the accuracy of detection in industrial settings [46]. Other recent strategies also seek to solve the problem of small industrial datasets by synthesizing synthetic ICS time-series data on generative models to enhance the performance of anomaly detection [41]. Furthermore, other proposals are made on the use of ensemble and unsupervised learning techniques to identify abnormalities in PLC-based industrial processes without the need for labeled attack datasets [47]. In addition to these methods, more recent studies also cover how formal verification tools like model checking and Petri-net-based models may be combined with runtime monitoring tools to detect cyber-physical anomalies during execution [48]. Additional new frameworks can also integrate digital twin models and causal reasoning algorithms to have a more informed perspective of system behavior and false alarm rate when identifying attacks in cyber-physical industrial contexts [42]. On the whole, all these changes testify to the shift that the research environment has passed in the trend topic analysis shown in Figure 9. The number shows that there has been an increased interest in industrial cybersecurity, anomaly detection, formal verification, and cyber-physical system security in the past decade, although the research activity has grown significantly after 2020. This tendency is manifested in the growing sophistication of the modern industrial infrastructure and the expansion of the necessity to have scalable security systems, uniting formal approaches with intelligent monitoring systems.

8. CONCLUSION

The current paper was a systematic and bibliometric review of formal approaches used to secure an ICS and PLCs. The findings indicate that there has been an increasing research focus on methods, e.g., model checking, Petri nets, and automation-based methods, to verify industrial control logic and identify anomalies. Nonetheless, the formal approaches are not widely applied practically because of the modeling complexity, the question of scalability, and the problem of introducing the approach into the reality of an industrial setting. Further studies are required in the form of scalable verification methods and hybrid security that will bring together formal techniques and data-driven mechanisms, and intelligent mechanisms of monitoring.

ACKNOWLEDGMENT

It is also desirable that the author would like to admit the assistance of the National Center of Scientific and Technical Research (CNRST) (https://www.cnrst.ma/fr/) Morocco, in financing this research that has made the research a success.

REFERENCES

[1] Sun, R., Mera, A., Lu, L., Choffnes, D. (2021). SoK: Attacks on industrial control logic and formal verification-based defenses. In 2021 IEEE European Symposium on Security and Privacy (EuroS&P), Vienna, Austria, pp. 385-402. https://doi.org/10.1109/EuroSP51992.2021.00034

[2] Quesel, J.D., Mitsch, S., Loos, S., Aréchiga, N., Platzer, A. (2016). How to model and prove hybrid systems with KeYmaera: A tutorial on safety. International Journal on Software Tools for Technology Transfer, 18(1): 67-91. https://doi.org/10.1007/s10009-015-0367-0

[3] Chen, Y., Poskitt, C.M., Sun, J., Adepu, S., Zhang, F. (2019). Learning-guided network fuzzing for testing cyber-physical system defences. In 2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE), San Diego, CA, USA, pp. 962-973. https://doi.org/10.1109/ASE.2019.00093

[4] Lanotte, R., Merro, M., Muradore, R., Viganò, L. (2017). A formal approach to cyber-physical attacks. In 2017 IEEE 30th Computer Security Foundations Symposium

(CSF), Santa Barbara, CA, USA, pp. 436-450. https://doi.org/10.1109/CSF.2017.12

[5] Wang, J., Sun, J., Jia, Y., Qin, S., Xu, Z. (2018). Towards 'verifying'a water treatment system. In International Symposium on Formal Methods, pp. 73-92. https://doi.org/10.1007/978-3-319-95582-7_5

[6] Moon, I., Powers, G.J., Burch, J.R. and Clarke, E.M. (1992), Automatic verification of sequential control systems using temporal logic. AIChE Journal, 38(1): 67-75. https://doi.org/10.1002/aic.690380107

[7] Alsabbagh, W., Langendörfer, P. (2023). Security of programmable logic controllers and related systems: Today and tomorrow. IEEE Open Journal of the Industrial Electronics Society, 4: 659-693. https://doi.org/10.1109/OJIES.2023.3335976

[8] Tanveer, A., Sinha, R., MacDonell, S.G., Leitao, P., Vyatkin, V. (2019). Designing actively secure, highly available industrial automation applications. In 2019 IEEE 17th International Conference on Industrial Informatics (INDIN), Helsinki, Finland, pp. 374-379. https://doi.org/10.1109/INDIN41052.2019.8972262

[9] Salwa, A., Hassan, E., Soumia, Z. (2026). Security challenges in the industrial internet of things (IIoT): A bibliometric analysis. In Proceedings of the 4th International Conference on Big Data and Artificial Intelligence Applications (ICBDAIA'25), pp. 405-417. https://doi.org/10.1007/978-3-032-10895-1_33

[10] Tranfield, D., Denyer, D., Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British Journal of Management, 14(3): 207-222. https://doi.org/10.1111/1467-8551.00375

[11] Ten, C.W., Liu, C.C., Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. IEEE Transactions on Power Systems, 23(4): 1836-1846. https://doi.org/10.1109/TPWRS.2008.2002298

[12] Alkabani, Y., Koushanfar, F. (2007). Active hardware metering for intellectual property protection and security. USENIX Security Symposium, 20: 1-20.

[13] Goldenberg, N., Wool, A. (2013). Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. International Journal of Critical Infrastructure Protection, 6(2): 63-75. https://doi.org/10.1016/j.ijcip.2013.05.001

[14] Zhang, X., Tehranipoor, M. (2011). Case study: Detecting hardware Trojans in third-party digital IP cores. In 2011 IEEE International Symposium on Hardware-Oriented Security and Trust, San Diego, CA, USA, pp. 67-70. https://doi.org/10.1109/HST.2011.5954998

[15] Alkabani, Y., Koushanfar, F., Potkonjak, M. (2007). Remote activation of ICs for piracy prevention and digital right management. In 2007 IEEE/ACM International Conference on Computer-Aided Design, San Jose, CA, USA, pp. 674-677. https://doi.org/10.1109/IC CAD.2007.4397343

[16] Van Lunteren, J. (2006). High-performance pattern-matching for intrusion detection. In 25th IEEE International Conference on Computer Communications, Barcelona, Spain, pp. 1-13. https://doi.org/10.1109/INFOCOM.2006.204

[17] Lin, Q., Adepu, S., Verwer, S., Mathur, A. (2018). TABOR: A graphical model-based approach for anomaly detection in industrial control systems. In Proceedings of the 2018 on Asia Conference on Computer and Communications Security, Incheon Republic of Korea, pp. 525-536. https://doi.org/10.1145/3196494.3196546

[18] Koushanfar, F. (2011). Provably secure active IC metering techniques for piracy avoidance and digital rights management. IEEE Transactions on Information Forensics and Security, 7(1): 51-63. https://doi.org/10.1109/TIFS.2011.2163307

[19] Badouel, E., Bednarczyk, M., Borzyszkowski, A., Caillaud, B., Darondeau, P. (2007). Concurrent secrets. Discrete Event Dynamic Systems, 17(4): 425-446. https://doi.org/10.1007/s10626-007-0020-5

[20] Subramanyan, P., Tsiskaridze, N., Li, W., Gascón, A., Tan, W. Y., Tiwari, A., Shankar, N., Seshia, S.A., Malik, S. (2013). Reverse engineering digital circuits using structural and functional analyses. IEEE Transactions on Emerging Topics in Computing, 2(1): 63-80. https://doi.org/10.1109/TETC.2013.2294918

[21] Wu, H., Geng, Y., Liu, K., Liu, W. (2019). Research on programmable logic controller security. IOP Conference Series: Materials Science and Engineering, 569(4): 042031. https://doi.org/10.1088/1757-899X/569/4/042031

[22] Lesi, V., Jakovljevic, Z., Pajic, M. (2021). Security analysis for distributed IoT-based industrial automation. IEEE Transactions on Automation Science and Engineering, 19(4): 3093-3108. https://doi.org/10.1109/TASE.2021.3106335

[23] Unniyankal, H., Ancona, D., Ferrando, A., Parodi, F., Alessi, A., Bottino, F. (2025). Runtime verification of program organization units in safe programmable logic controller systems. In 2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S), Naples, Italy, pp. 112-118. https://doi.org/10.1109/DSN-S65789.2025.00050

[24] Iacobelli, A., Rinieri, L., Melis, A., Al Sadi, A., Prandini, M., Callegati, F. (2024). Detection of ladder logic bombs in plc control programs: An architecture based on formal verification.In 2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS), St. Louis, MO, USA, pp. 1-7. https://doi.org/10.1109/ICPS59941.2024.10639995

[25] Fujita, S., Sawada, K., Shin, S., Hosokawa, S. (2019). Model verification and exhaustive testing for whitelist function of industrial control system. In IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society, Lisbon, Portugal, pp. 5874-5879. https://doi.org/10.1109/IECON.2019.8927252

[26] Bandyopadhyay, S., Sarkar, S. (2025). Verifying correctness of PLC software during system evolution using model containment approach. arXiv preprint arXiv:2509.05596. https://doi.org/10.48550/arXiv.2509.05596

[27] Fujita, S., Rata, K., Mochizuki, A., Sawada, K., Shin, S., Hosokawa, S. (2018). On experimental validation of whitelist auto-generation method for secured programmable logic controllers. In IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, pp. 2385-2390. https://doi.org/10.1109/IECON.2018.8591275

[28] Amer, E., Al-rimy, B.A.S., El-Sappagh, S. (2025). Strengthening ICS defense: Modbus-NFA behavior model for enhanced anomaly detection. Journal of Information Security and Applications, 89: 103990.

https://doi.org/10.1016/j.jisa.2025.103990
[29] Ghazi, Z., Doustmohammadi, A. (2018). Intrusion detection in cyber-physical systems based on petri net. Information Technology and Control, 47(2): 220-235. https://doi.org/10.5755/j01.itc.47.2.16277
[30] Vitale, F., Dall'Ora, N., Gaiardelli, S., Fraccaroli, E., Mazzocca, N., Fummi, F. (2026). Process mining-driven modeling and simulation to enhance fault diagnosis in cyber–physical systems. Journal of Manufacturing Systems, 84: 189-206. https://doi.org/10.1016/j.jmsy.2025.12.005
[31] Ndonda, G.K., Sadre, R. (2022). Exploiting the temporal behavior of state transitions for intrusion detection in ICS/SCADA. IEEE Access, 10: 111171-111187. https://doi.org/10.1109/AC CESS.2022.3213080
[32] Wang, G., Zhuang, L., Liu, T., Li, S., Yang, S., Lan, J. (2020). Formal analysis and verification of industrial control system security via timed automata. In 2020 International Conference on Internet of Things and Intelligent Applications (ITIA), Zhenjiang, China, pp. 1-5. https://doi.org/10.1109/ITIA50152.2020.9312289
[33] Li, Y., Wang, Y., Zhu, G., Yin, L., Zhang, H. (2022). Fault diagnosis of PLC-based discrete event systems using Petri nets. Measurement and Control, 55(9-10): 960-973. https://doi.org/10.1177/00202940221117098
[34] Ghosh, A., Qin, S., Lee, J., Wang, G.N. (2016). PLAT: An automated fault and behavioural anomaly detection tool for PLC controlled manufacturing systems. Computational Intelligence and Neuroscience, 2016(1): 1652475. https://doi.org/10.1155/2016/1652475
[35] Bandyopadhyay, S., Jetley, R. (2025). Pn4PLC: Verification of software upgrade for PLC code. In Proceedings of the 33rd ACM International Conference on the Foundations of Software Engineering, Trondheim Norway, pp. 1244-1245. https://doi.org/10.1145/3696630.3731434
[36] Luo, J., Yi, S., Lin, Z., Zhang, H., Zhou, J. (2024). Petri-net-based deep reinforcement learning for real-time scheduling of automated manufacturing systems. Journal of Manufacturing Systems, 74: 995-1008. https://doi.org/10.1016/j.jmsy.2024.05.006
[37] Mercaldo, F., Martinelli, F., Santone, A. (2022). Timed Automata networks for SCADA attacks real-time mitigation. In Intelligent Decision Technologies: Proceedings of the 14th KES-IDT 2022 Conference, pp. 549-559. https://doi.org/10.1007/978-981-19-3444-5_47
[38] Ausberger, T., Kubicek, K., Medvedcova, P. (2025). Functionally-equivalent formalization and automated model checking of function block diagrams. IEEE Access, 13: 22197-22229. https://doi.org/10.1109/ACCESS.2025.3535890
[39] Yang, Y., Geng, Y., Wei, Q., Ma, R., Wei, Z. (2025). IPSMInfer: Industrial proprietary protocol state machine inference from network traces. International Journal of Critical Infrastructure Protection, 49: 100765. https://doi.org/10.1016/j.ijcip.2025.100765
[40] Lee, J.H., Ji, I.H., Jeon, S.H., Seo, J.T. (2025). Anomaly detection method considering PLC control logic structure for ICS cyber threat detection. Applied Sciences, 15(7): 3507. https://doi.org/10.3390/app15073507
[41] Han, C., Gim, G. (2025). Time-series-based anomaly detection in industrial control systems using generative adversarial networks. Processes, 13(9): 2885. https://doi.org/10.3390/pr13092885
[42] Homaei, M., Tarif, M., Rodríguez, P.G., Caro, A., Ávila, M. (2025). Causal digital twins for cyber-physical security in water systems: A framework for robust anomaly detection. Machine Learning with Applications, 100824. https://doi.org/10.1016/j.mlwa.2025.100824
[43] Lanotte, R., Merro, M., Munteanu, A. (2021). A process calculus approach to detection and mitigation of PLC malware. Theoretical Computer Science, 890: 125-146. https://doi.org/10.1016/j.tcs.2021.08.021
[44] Zhang, X., Li, J., Wu, J., Chen, G., Meng, Y., Zhu, H., Zhang, X. (2024). Binary-level formal verification based automatic security ensurement for PLC in Industrial IoT. IEEE Transactions on Dependable and Secure Computing, 22(3): 2211-2226. https://doi.org/10.1109/TDSC.2024.3481433.
[45] Zhou, H., Sourav, S., Chen, B., Yu, K. (2025). SRLR: Symbolic regression-based logic recovery to counter programmable logic controller attacks. IEEE Transactions on Information Forensics and Security, 20: 12491-12506. https://doi.org/10.1109/TIFS.2025.3634027
[46] Aslam, M.M., Tufail, A., Gul, H., Irshad, M.N., Namoun, A. (2025). Artificial intelligence for secure and sustainable industrial control systems-A Survey of challenges and solutions. Artificial Intelligence Review, 58(11): 349. https://doi.org/10.1007/s10462-025-11320-9
[47] Boateng, E.A. (2023). Unsupervised ensemble methods for anomaly detection in plc-based process control. arXiv preprint arXiv:2302.02097. https://doi.org/10.48550/arXiv.2302.02097
[48] Fraser, D., Miller, A., Cook, M., Pezaros, D. (2025). Online model checking for anomaly detection in industrial control systems. In International Conference on Integrated Formal Methods, Cham: Springer Nature Switzerland, pp. 162-181. https://doi.org/10.1007/978-3-032-10794-7_9