Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 17 No. 3, September 2026 - www.cisdijournal.net

Static Threshold-Based Detection for Man-in-the-Middle Attacks in Industrial and Oil-and-Gas Cyber-Physical Systems: A Systematic Literature Review

Isah, A.O. (PhD), *Agbu, E.A., Ahmad, S. (PhD) & Noel, M.D. (PhD)
Department of Cyber Security Science
Federal University of Technology, Minna, Nigeria.
E-mail: ao.isah@futminna.edu.ng, agbueamte25270@st.futminna.edu.ng,
ahmads@futminna.edu.ng & moses.noel@futminna.edu.ng
Phone: +2348033118443, +2347032641585, +2348064704717, +2347032200161
***ORCID iD:** 0009-0003-5994-8453

ABSTRACT

Static threshold-based anomaly detection methods continue to be applied in Industrial Control Systems (ICS) and Cyber-Physical Systems (CPS) despite growing evidence of their limitations. This systematic literature review (SLR) investigates the documented limitations of static threshold-based detection methods for Man-in-the-Middle (MitM) attacks in Oil and Gas Cyber-Physical Systems (OGCPS) and identifies adaptive threshold alternatives proposed in the literature. Following the PRISMA 2020 guidelines, a systematic search was conducted across five academic databases for studies published between January 2021 and June 2026 because the most recent systematic literature review dated back 2021. A total of 1,174 records were identified, of which 45 primary studies met the eligibility and quality criteria and were included in the final synthesis. The review identified five major categories of limitations associated with static threshold-based detection methods: failure to adapt to dynamic operational conditions, inability to detect stealthy or low-and-slow attacks, manual tuning requirements, elevated false positive rates, and lack of adaptability to changing data streams. Several adaptive and dynamic threshold alternatives were identified, including reinforcement learning-based thresholding, adaptive Cumulative Sum (CUSUM), dynamic Interquartile Range (IQR) approaches, probabilistic threshold masking, segmented confidence sequences, and multi-scale adaptive confidence segments. This systematic literature reviews highlight some research gaps which provide a foundation for future research on adaptive threshold mechanisms for MitM attack detection in oil and gas infrastructure.

Keywords: Static Threshold; Mitm; Cyber-Physical Systems; Anomaly Detection, Detection Stealthy, Industrial Control System.

CISDI Journal Reference Format
Isah, A.O., Agbu, E.A., Ahmad, S. & Noel, M.D. (2026): Static Threshold-Based Detection for Man-in-the-Middle Attacks in Industrial and Oil-and-Gas Cyber-Physical Systems: A Systematic Literature Review. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 17 No 3, Pp 41-58. Available online at www.isteams.net/cisdijournal.
dx.doi.org/10.22624/AIMS/CISDI/V17N3P2

1. INTRODUCTION

Industrial Control Systems (ICS) and Cyber-Physical Systems (CPS) underpin critical infrastructure sectors, including oil and gas, power generation, manufacturing, transportation, and water treatment.

In the oil and gas industry, the convergence of Operational Technology (OT) and Information Technology (IT), driven by Industry 4.0, has enhanced operational efficiency, automation, and remote monitoring while simultaneously expanding the cyberattack surface of industrial environments (Mohammed *et al.*, 2022).

Among the cyber threats targeting industrial environments, Man-in-the-Middle (MitM) attacks remain particularly challenging because attackers can intercept, modify, or replay communications between industrial devices while allowing physical processes to continue operating apparently normally. Unlike Denial-of-Service (DoS) attacks, which primarily affect service availability, MitM attacks compromise the integrity and authenticity of operational data and may remain undetected for extended periods. In oil and gas facilities, such attacks can manipulate sensor measurements, disrupt process control, and jeopardise operational safety, with incidents affecting critical energy infrastructure demonstrating their potentially severe operational and economic consequences (Mohammed *et al.*, 2025; Wang *et al.*, 2025).

Anomaly detection has become a fundamental component of industrial cybersecurity, with static threshold-based methods remaining widely adopted because of their simplicity, computational efficiency, and ease of deployment. These methods identify anomalies whenever predefined statistical or operational limits are exceeded. However, increasing evidence indicates that fixed thresholds perform poorly in dynamic industrial environments characterised by equipment ageing, changing operating conditions, environmental variations, and concept drift, resulting in frequent manual recalibration, elevated false alarms, and reduced ability to detect stealthy attacks (Mohammed *et al.*, 2022; Mtukushe *et al.*, 2023).

Although anomaly detection has been extensively studied in ICS and CPS, comparatively little attention has been devoted to systematically synthesising the documented limitations of static threshold-based detection methods for MitM attack detection in Oil and Gas Cyber-Physical Systems (OGCPS). Furthermore, while numerous adaptive and dynamic threshold mechanisms have been proposed, evidence regarding their advantages, limitations, and applicability to oil and gas environments remains fragmented across the literature. This lack of consolidated evidence limits the ability of researchers and practitioners to compare existing approaches, identify knowledge gaps, and guide future research.

This study presents a systematic literature review of static threshold-based detection methods for MitM attacks in ICS and CPS, with particular emphasis on oil and gas applications. The review identifies the static threshold-based detection methods reported in recent literature, synthesises their documented limitations, develops a taxonomy of recurring limitation categories, examines adaptive and dynamic threshold alternatives proposed to address these limitations, and consolidates evidence relating to oil and gas cyber-physical systems.

2. RELATED WORK

Existing studies have extensively reviewed anomaly detection, intrusion detection, and cybersecurity in Industrial Control Systems (ICS) and Cyber-Physical Systems (CPS). However, most focus on artificial intelligence, machine learning, adaptive intrusion detection, explainable security models, and broader cybersecurity frameworks. Reviews of artificial intelligence-driven and adaptive anomaly detection have highlighted several challenges.

These challenges include dataset limitations, concept drift, real-time deployment constraints, and limited operational realism, while proposing taxonomies covering attack types, learning paradigms, application domains, and detection algorithms (Seo *et al.*, 2026; Moriano *et al.*, 2024). Hasan *et al.* (2024) similarly reviewed machine learning techniques for securing smart-grid cyber-physical systems, while Abraham *et al.* (2024), Skrodelis and Romanovs (2025), and Abdelkader *et al.* (2025) examined context-aware modelling, digital twins, explainable intrusion detection systems, and hybrid security architectures for ICS and SCADA environments.

Broader surveys have identified adversarial attacks, class imbalance, stealthy attacks, false alarms, zero-day attacks, and model maintenance as persistent cybersecurity challenges in industrial environments (Alanazi *et al.*, 2023; Arunthavanathan *et al.*, 2025; Umer *et al.*, 2023; Xing and Shen, 2024; Pinto *et al.*, 2023; Alyanbaawi, 2025). Experimental studies have further demonstrated the practicality of Man-in-the-Middle (MitM) attacks through Hardware-in-the-Loop (HIL) platforms using simulated Intelligent Electronic Devices (IEDs) and the IEC 61850 communication protocol (Liu *et al.*, 2025). More recently, adaptive threshold adjustment has been recognised as a promising direction for improving anomaly detection in dynamic industrial environments (Wu *et al.*, 2026).

Growing attention has also been directed towards threshold selection. Existing reviews consistently recognise threshold configuration as a critical determinant of anomaly detection performance and conclude that fixed thresholds are poorly suited to non-stationary industrial processes characterised by concept drift and changing operating conditions (Mtukushe *et al.*, 2023; Aghaei Attar *et al.*, 2024). Recent systematic reviews further reinforce the continued reliance on threshold-based detection, the increasing importance of adaptive threshold mechanisms, and the applicability of anomaly detection to critical infrastructure and energy systems, including oil and gas environments (Jeffrey *et al.*, 2023; Abshari and Sridhar, 2025; Aghazadeh Ardebili *et al.*, 2025; Acquaah and Kaushik, 2024).

3. METHODOLOGY

This study employed a Systematic Literature Review (SLR) to identify, evaluate, and synthesise published evidence on static threshold-based detection methods for cyberattacks, particularly Man-in-the-Middle (MitM) attacks, in Industrial Control Systems (ICS), Cyber-Physical Systems (CPS), and Oil and Gas Cyber-Physical Systems (OGCPS). The review followed established SLR guidelines for software engineering and cybersecurity research to ensure methodological rigour, transparency, and reproducibility (Carrera-Rivera *et al.*, 2022). The review protocol comprised four stages: review planning, literature search, study selection, and evidence synthesis.

3.1 Review Protocol

A review protocol was established before the literature search to minimise selection bias and ensure methodological consistency throughout the study. The protocol defined the review scope, search strategy, information sources, study selection criteria, quality assessment procedure, data extraction process, and the research questions that guided the review.

Specifically, the study addressed the following questions:

1. RQ1: What static threshold-based detection methods have been proposed or evaluated for detecting cyberattacks, including Man-in-the-Middle (MitM) attacks, in Industrial Control Systems (ICS) and Cyber-Physical Systems (CPS)?

2. RQ2: What limitations of static threshold-based detection methods are reported in the literature?
3. RQ3: How can these limitations be categorised into theoretical, methodological, operational, and empirical perspectives?
4. RQ4: What adaptive or dynamic threshold alternatives have been proposed?
5. RQ5: What evidence exists regarding the impact of static threshold limitations on Man-in-the-Middle (MitM) attack detection in Oil and Gas Cyber-Physical Systems?

The search strategy was developed using the Population–Intervention–Comparison–Outcome–Context (PICOC) framework to define the review scope and derive the search terms.

Table 1: PICOC Framework

Element	Description	Keywords
Population	ICS, CPS, SCADA, and oil and gas cyber-physical environments	industrial control system, cyber-physical system, SCADA, oil and gas, pipeline, refinery
Intervention	Static threshold-based anomaly/attack detection	static threshold, fixed threshold, threshold-based detection, rule-based detection
Comparison	Adaptive or dynamic threshold-based detection approaches	adaptive threshold, dynamic threshold, adaptive detection, dynamic thresholding
Outcome	Detection performance and documented limitations	limitation, weakness, false positive, false negative, detection accuracy, recall, precision, F1-score
Context	Industrial cybersecurity and cyber-physical environments	ICS, CPS, industrial cybersecurity, oil and gas

Table 1 presents the PICOC Framework used to define the scope of the review and guide the development of the search terms. The population comprises ICS, CPS, SCADA, and oil and gas cyber-physical environments, while the intervention focuses on static threshold-based anomaly and attack detection. Adaptive and dynamic threshold-based detection approaches are considered as the comparison dimension because the review examines alternatives proposed to address the limitations of static thresholding. The outcomes comprise documented limitations and detection performance, while the context is industrial cybersecurity and cyber-physical environments, with particular emphasis on oil and gas applications.

3.2 Search Strategy and Study Selection

A comprehensive literature search was conducted across five electronic databases: IEEE Xplore, ScienceDirect, ACM Digital Library, SpringerLink, and MDPI. These databases were selected because of their broad coverage of cybersecurity, industrial control systems, and cyber-physical systems research. The search covered studies published between January 2021 and June 2026. Two complementary Boolean search strings were constructed from the PICOC framework to maximise retrieval while maintaining relevance to the review objectives.

Table 2: Search Strings Used Across the Databases

Search String	Query
Broad Search (String A)	("industrial control system" OR "cyber-physical system" OR "SCADA" OR "oil and gas" OR "pipeline" OR "refinery") AND ("static threshold" OR "fixed threshold" OR "threshold-based detection") AND ("anomaly detection" OR "intrusion detection" OR "attack detection")
Focused Search (String B)	("ICS" OR "CPS" OR "SCADA") AND ("threshold detection" OR "rule-based detection") AND ("MitM" OR "man-in-the-middle" OR "replay attack" OR "false data injection") AND ("limitation" OR "false positive" OR "weakness")

Table 2 presents the two Boolean search strings used across the selected databases. A broad search string was designed to capture studies on threshold-based detection in ICS, CPS, SCADA, and oil and gas environments, while a focused search string targeted studies specifically addressing Man-in-the-Middle (MitM) and related attacks, together with reported limitations of threshold-based detection methods.

The search identified 1,174 records. Study selection followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. After duplicate removal, 900 unique studies remained for title and abstract screening, resulting in the exclusion of 812 records. The remaining 88 full-text articles were assessed against the predefined eligibility and quality criteria, after which 47 studies were excluded. Consequently, 45 primary studies were included in the final synthesis.

Studies were eligible if they were peer-reviewed journal or conference publications published between 2021 and 2026 that investigated threshold-based detection methods within ICS, CPS, SCADA, or oil and gas environments. Non-English publications, grey literature, and studies unrelated to industrial cybersecurity were excluded from the primary synthesis; however, relevant review papers were retained to contextualise the findings presented in the Related Work section.

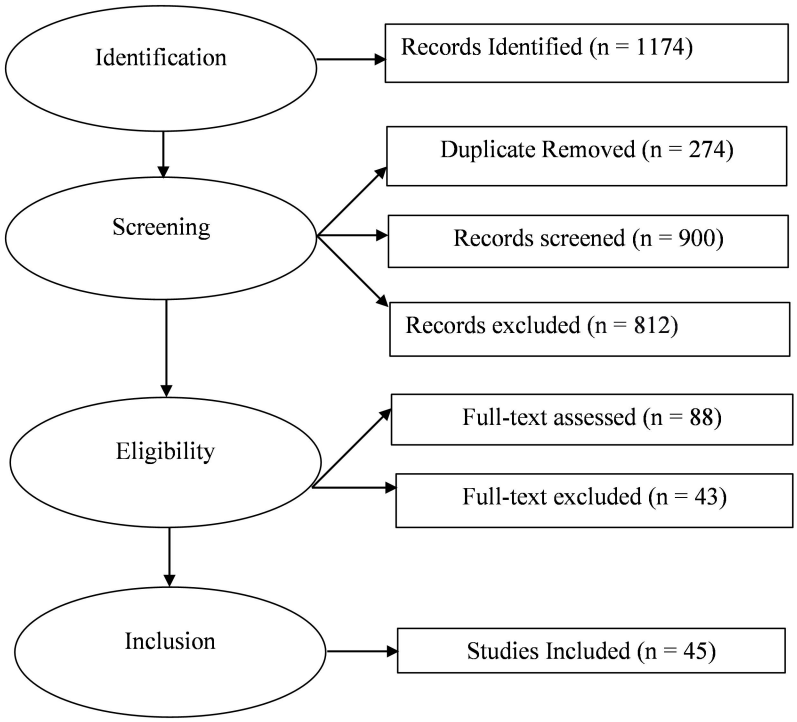

Figure 1. PRISMA flow diagram.

Figure 1 illustrates the PRISMA flow diagram used for the study selection process. An initial 1,174 records were identified through database searching. After duplicate removal, 900 unique studies remained for title and abstract screening, resulting in the exclusion of 812 records. The remaining 88 full-text articles were assessed for eligibility, of which 43 were excluded based on the predefined inclusion, exclusion, and quality assessment criteria. Consequently, 45 primary studies were included in the final qualitative synthesis.

3.3 Quality Assessment and Data Extraction

The methodological quality of each eligible study was assessed using a five-item checklist that evaluated whether the study (i) clearly described the detection method, (ii) was evaluated in an ICS/CPS-relevant environment, (iii) reported quantitative performance metrics, (iv) provided sufficient methodological detail, and (v) discussed or proposed adaptive threshold mechanisms. Each criterion was scored on a binary scale (0 or 1), yielding a maximum score of five. Studies scoring below 2.5 were excluded from further analysis.

A structured data extraction form was used to collect bibliographic information, threshold-based detection methods, attack types, application domains, reported limitations, datasets or experimental testbeds, performance metrics, and adaptive or dynamic threshold alternatives.

4. RESULTS

This section presents the findings of the systematic literature review based on the final set of 45 primary studies that satisfied the predefined inclusion criteria and quality assessment. The results are organised according to the research questions formulated in Section 3 and synthesise evidence relating to static threshold-based detection methods, their reported limitations, proposed adaptive alternatives, and their applicability to Man-in-the-Middle (MitM) attack detection in Oil and Gas Cyber-Physical Systems (OGCPS).

4.1 Bibliometric Overview

The bibliometric analysis provides an overview of the characteristics of the included studies in terms of publication source and temporal distribution. The 45 primary studies were retrieved from five major scientific databases selected for their extensive coverage of cybersecurity, industrial control systems, and cyber-physical systems research.

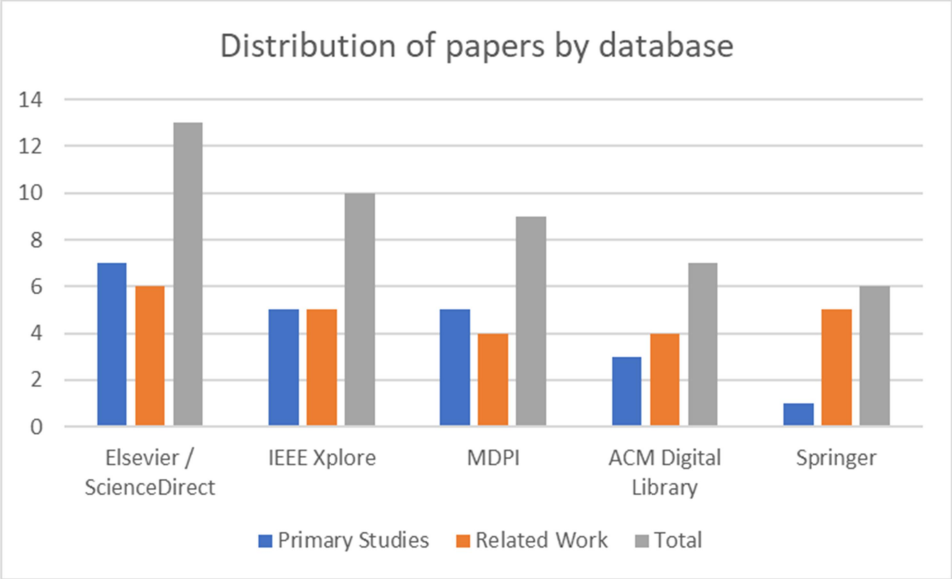

Figure 2. Distribution of Included Studies by Database.

Figure 2 shows the distribution of studies which indicates that ScienceDirect (Elsevier) contributed the largest proportion of the included papers, followed by IEEE Xplore, MDPI, ACM Digital Library, and SpringerLink. The relatively balanced representation across multiple databases demonstrates that research on threshold-based anomaly detection is distributed across several publication venues rather than concentrated within a single publisher, thereby reducing the likelihood of publication-source bias.

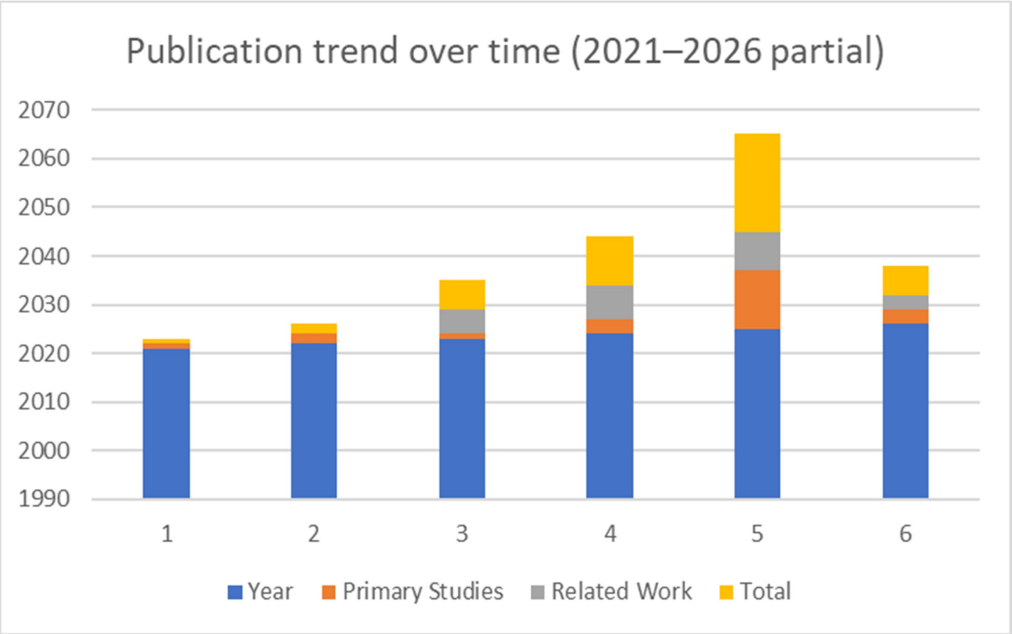

Figure 3. Publication Trend of Included Studies (2021–2026).

Figure 3 illustrate the temporal distribution which reveals a steady increase in publications throughout the review period, with research activity becoming particularly pronounced between 2024 and 2025. This trend reflects growing research interest in securing Industrial Control Systems (ICS) and Cyber-Physical Systems (CPS) against increasingly sophisticated cyber threats. The comparatively smaller number of studies identified in 2026 is expected because the literature search concluded during the first half of the year, resulting in only partial coverage of publications for that period. The bibliometric findings indicate that threshold-based anomaly detection remains an active research area, with increasing attention being devoted to improving detection performance in dynamic industrial environments.

4.2 Static Threshold-Based Detection Methods

The first research question sought to identify the static threshold-based detection methods reported in the literature for detecting cyber-attacks within ICS and CPS environments. The review demonstrates that static thresholding continues to serve as one of the most widely adopted decision mechanisms for anomaly detection because of its computational simplicity, ease of implementation, and compatibility with resource-constrained industrial systems.

Table 3: Static Threshold-Based Detection Methods Identified in the Included Studies

Threshold Method	Description	Primary Studies	Application Domain
Fixed value threshold	Predetermined constant threshold	Obonna *et al.*, 2023; Sun *et al.*, 2025; Mehrpouyan, 2025	Oil and gas, ICS
Statistical threshold (μ ± kσ)	Mean plus or minus k standard deviations	Mohammed *et al.*, 2025; Rodrigues *et al.*, 2025; Oliveira *et al.*, 2025; Sun *et al.*, 2025	Oil and gas, IIoT, CPS
Cumulative Sum (CUSUM)	Sequential change-point detection	Mattos *et al.*, 2024; Nishiuchi *et al.*, 2024; Acharya and Bhalja, 2026	CPS, smart grid
Safety Integrity Level (SIL) threshold	Industry safety standard thresholds	Wang *et al.*, 2025	Oil and gas
Interquartile Range (IQR)	Statistical outlier detection	Oliveira *et al.*, 2025; Rodrigues *et al.*, 2025	Industrial sensors, data rate
Percentile-based threshold	Fixed percentile of historical distribution	Li and Gautam, 2025; Errachidi *et al.*, 2025	Time series, CPS
Prediction error threshold	Deviation between predicted and actual sensor readings	Ahmad *et al.*, 2025	Oil and gas (TEP)

Table 3 reviewed studies that identified several categories of static threshold-based detection methods, including statistical thresholds (μ ± kσ), Cumulative Sum (CUSUM), fixed-value thresholds, percentile-based thresholds, Interquartile Range (IQR), Safety Integrity Level (SIL) thresholds, and prediction-error thresholds. Although these methods differ in their implementation, they all rely on predefined decision boundaries derived from historical data, engineering specifications, or statistical characteristics of normal system behaviour. Their widespread adoption reflects their simplicity, transparency, low computational requirements, and suitability for real-time industrial environments. However, because these thresholds remain fixed during operation, they are unable to adapt to evolving process conditions, concept drift, or changing threat landscapes. Consequently, their detection performance depends heavily on the validity of assumptions made during threshold selection, a common limitation that underpins the findings discussed in the subsequent section. Gülmez *et al.* (2024) similarly demonstrated the application of predefined operational safety thresholds within a marine lubricating oil system to analyse the impact of Man-in-the-Middle attacks on sensor measurements, further illustrating the continued reliance on fixed threshold mechanisms in safety-critical industrial processes.

4.3 Reported Limitations of Static Threshold-Based Detection

The second research question examined the limitations associated with static threshold-based detection methods reported across the reviewed studies. Analysis of the included literature revealed that, although static thresholding remains widely employed in industrial anomaly detection, its effectiveness is consistently constrained by several recurring limitations that reduce detection reliability under dynamic operating conditions.

Table 4: Reported Limitations of Static Threshold-Based Detection Methods

Limitation Category	Description	Supporting Studies
Adaptation failure and sensitivity to concept drift.	Static thresholds cannot adjust to distribution shifts, concept drift, evolving system behaviour, or real-time changes in data streams.	Mohammed *et al.*, 2025; Yang *et al.*, 2024; Ding *et al.*, 2026; Rodrigues *et al.*, 2025; Li and Gautam, 2025; Oliveira *et al.*, 2025; Sun *et al.*, 2025; Errachidi *et al.*, 2025; Aghaei Attar *et al.*, 2024;
Inability to detect stealthy or low-and-slow attacks	Static thresholds fail to identify subtle, gradual anomalies that do not exceed fixed boundaries	Rodrigues *et al.*, 2025; Mattos *et al.*, 2024; Acharya and Bhalja, 2026
Manual tuning requirements	Static thresholds require manual calibration by experts, which is time-consuming and error-prone	Yang *et al.*, 2024; Mattos *et al.*, 2024; Aghaei Attar *et al.*, 2024; Nishiuchi *et al.*, 2024
Elevated false positive rates	Static thresholds misclassify normal operational fluctuations as attacks	Mohammed *et al.*, 2025; Obonna *et al.*, 2023; Sun *et al.*, 2025

Table 4 reviewed studies that consistently identified the inability of static thresholds to adapt to changing operational conditions as the most significant limitation. Industrial environments are characterised by process variability, equipment ageing, changing operating regimes, environmental influences, and concept drift, causing fixed thresholds derived from historical data to become progressively less representative over time. Additional limitations include poor detection of stealthy or low-and-slow attacks, particularly Man-in-the-Middle (MitM) and False Data Injection (FDI) attacks, the need for manual threshold calibration and periodic recalibration, and elevated false-positive or false-negative rates resulting from the trade-off between sensitivity and specificity. Collectively, these findings indicate that the limitations of static threshold-based detection arise primarily from their reliance on fixed decision boundaries and the assumption of stable system behaviour, highlighting the need for adaptive threshold mechanisms capable of responding to evolving industrial environments.

4.4 Taxonomy of Reported Limitations

To address the third research question, the reported limitations were further synthesised into a taxonomy that groups similar challenges according to their underlying characteristics. Rather than considering each reported limitation independently, the taxonomy provides a higher-level conceptual framework for understanding the fundamental sources of performance degradation associated with static threshold-based detection.

Table 5: Taxonomy of Static Threshold-Based Detection Limitations

Category	Definition	Example Limitation	Supporting Studies
Theoretical	Limitations arising from underlying statistical assumptions	Static thresholds assume a stationary data distribution	Ding *et al.*, 2026; Li and Gautam, 2025; Errachidi *et al.*, 2025
Methodological	Limitations in the design or implementation of detection methods	Manual tuning requirements for threshold selection	Yang *et al.*, 2024; Mattos *et al.*, 2024; Nishiuchi *et al.*, 2024
Operational	Limitations related to real-world deployment and execution	Inability to respond to concept drift in streaming data	Ding *et al.*, 2026; Aghaei Attar *et al.*, 2024; Li and Gautam, 2025; Oliveira *et al.*, 2025
Empirical	Limitations demonstrated through experimental results	Elevated false positive rates in specific test environments	Mohammed *et al.*, 2025; Obonna *et al.*, 2023; Sun *et al.*, 2025

Table 5 classified the identified limitations into four complementary categories: theoretical, methodological, operational, and empirical. Theoretical limitations arise from the assumptions underlying static threshold methods, particularly the expectation of stable system behaviour. Methodological limitations relate to threshold selection and calibration procedures, while operational limitations reflect challenges encountered in dynamic industrial environments, including concept drift, equipment ageing, and changing operating conditions. Empirical limitations comprise experimentally observed shortcomings such as elevated false-positive rates, missed detections, and poor resilience to stealthy attacks. Collectively, this taxonomy demonstrates that the weaknesses of static threshold-based detection extend beyond individual algorithms, spanning conceptual, implementation, deployment, and performance dimensions. It also provides a structured framework for comparing conventional static approaches with adaptive threshold mechanisms and highlights that addressing theoretical and operational limitations generally requires adaptive rather than fixed thresholding strategies.

4.5 Adaptive Threshold Alternatives

The fourth research question investigated the adaptive and dynamic threshold mechanisms proposed in the literature to overcome the limitations associated with conventional static threshold-based detection. The review demonstrates a growing transition from fixed decision boundaries towards adaptive thresholding strategies capable of responding to evolving operational conditions within Industrial Control Systems (ICS) and Cyber-Physical Systems (CPS).

Table 6: Adaptive and Dynamic Threshold Alternatives Identified in the Reviewed Studies

Alternative Method	Description	Supporting Studies	Reported Improvement
Agent-based dynamic thresholding	Reinforcement Learning agent adjusts thresholds	Yang *et al.*, 2024; Halder *et al.* (2025)	Outperformed static methods
Adaptive CUSUM	Dynamically adjusted Cumulative Sum parameters	Bhattacharya *et al.*, 2024; Mattos *et al.*, 2024; Acharya and Bhalja, 2026	Improved stealthy attack detection
Dynamic IQR with exponential relaxation	Adaptive interquartile range with time-based decay	Oliveira *et al.*, 2025	99.8 percent precision
Probabilistic threshold masking	Threshold based on probability distributions	Mehrpouyan, 2025	Improved recall over fixed thresholds
Segmented Confidence Sequences (SCS)	Regime-specific confidence bounds	Li and Gautam, 2025	F1 improvement of up to 2.17 times
Multi-Scale Adaptive Confidence Segments (MACS)	Multi-window adaptive confidence	Li and Gautam, 2025	Superior to static percentile approaches

Table 6 reviewed studies that proposed diverse adaptive threshold mechanisms to overcome the limitations of static thresholding. These include reinforcement learning-based threshold optimisation ((Yang *et al.*, 2024; Halder *et al.*, 2025)), adaptive dynamic threshold mechanisms for Industrial IoT environments, adaptive statistical techniques such as adaptive CUSUM (Bhattacharya *et al.*, 2024; Mattos *et al.*, 2024; Acharya and Bhalja, 2026) and dynamic IQR, probabilistic threshold estimation, segmented and multi-scale thresholding, and hybrid frameworks combining statistical methods with machine learning for anomaly detection (e.g., Moila and Velempini, 2025).

Unlike static approaches, these methods continuously adjust decision boundaries to accommodate changing operational conditions, improving resilience to concept drift, stealthy attacks, and false alarms. Although no single adaptive approach has emerged as universally applicable across all industrial domains, the evidence consistently indicates that adaptive thresholding generally outperforms static threshold methods. Overall, the literature demonstrates a clear transition from fixed decision boundaries towards adaptive detection strategies capable of responding to evolving industrial environments.

4.6 Evidence from Oil and Gas Cyber-Physical Systems

The fifth research question examined the extent to which the reviewed literature provides evidence regarding the impact of static threshold limitations on Man-in-the-Middle (MitM) attack detection within Oil and Gas Cyber-Physical Systems (OGCPS). Although a substantial body of research investigates anomaly detection in general ICS and CPS environments, comparatively fewer studies specifically evaluate threshold-based detection within oil and gas applications.

Table 7: Static Threshold-Based Detection and MitM Attacks in Oil and Gas Cyber-Physical Systems

Study	Oil and Gas Context	Static Threshold Evidence	MitM Evidence
Mohammed *et al.*, 2025	Real oil and gas wellhead monitoring testbed	Explicit static threshold limitation documented	Validated MitM attacks
Obonna *et al.*, 2023	Three-phase separator in oil and gas facility	Implied (machine learning as alternative)	Simulated MitM attacks
Wang *et al.*, 2025	Crude oil storage facility in China	SIL threshold degradation under cyber threats	Cyber threats including MitM implied
Xu *et al.*, 2025	Oil field joint station export system (pipeline pressure drop)	Explicit dynamic threshold proposed	Not applicable (operational)
Ahmad *et al.*, 2025	Tennessee Eastman Process (refinery benchmark)	Implied (prediction error threshold)	Detected fuzzification and ping of death MitM attacks
Katale *et al.*, 2025	Gas pipeline networks	Bad-data detectors with χ^2-based detection threshold (τS = 0.005 MPa)	False Data Injection (FDI) attacks
Noorizadeh *et al.*, 2021	Tennessee Eastman Process (refinery benchmark)	Detection algorithms with decision boundaries	Explicit MitM attacks via PROFINET protocol

Table 7 reviewed literature that provides evidence from several oil and gas domains, including wellhead monitoring, refinery process control, pipeline networks, gas transportation, and safety-critical storage facilities, demonstrating both the continued use and limitations of static threshold-based anomaly detection. Mohammed *et al.* (2025) offered the strongest evidence by validating MitM attacks on a real oil and gas wellhead testbed, while acknowledging that static thresholds require dynamic alternatives to maintain long-term effectiveness.

Studies using the Tennessee Eastman Process (TEP) further showed that threshold-based and machine learning approaches can effectively detect MitM and False Data Injection (FDI) attacks in refinery-like environments. Research on pipeline networks also demonstrated that stealthy attacks can evade fixed thresholds, while Safety Integrity Level (SIL) studies indicated that cyber threats can invalidate assumptions underlying static safety thresholds. Despite these contributions, relatively few studies have evaluated adaptive threshold mechanisms in operational oil and gas environments, with most relying on generic ICS/CPS datasets or laboratory testbeds. This evidence highlights a significant research gap and underscores the need for adaptive threshold frameworks specifically designed and validated for MitM detection in Oil and Gas Cyber-Physical Systems.

5. DISCUSSION

This section interprets the findings of the systematic review in relation to existing literature, discusses their implications for research and industrial practice, and identifies the research gap.

5.1 Interpretation of the Findings

The findings demonstrate that static threshold-based detection methods remain widely used for anomaly and intrusion detection in Industrial Control Systems (ICS) and Cyber-Physical Systems (CPS) because of their simplicity, computational efficiency, and ease of implementation. The most frequently reported approaches include statistical thresholds ($\mu \pm k\sigma$), CUSUM, percentile-based thresholds, interquartile range (IQR), prediction-error thresholds, and Safety Integrity Level (SIL)-related thresholds. Despite their widespread adoption, the reviewed studies consistently show that these methods exhibit limited robustness in dynamic industrial environments. The most consistently reported limitation is the inability of static thresholds to adapt to changing operational conditions. As industrial processes evolve due to equipment ageing, maintenance activities, production changes, and environmental variations, fixed thresholds become less representative of normal system behaviour, resulting in increased false alarms and missed detections. This finding suggests that adaptive thresholding should be regarded as a fundamental requirement for modern industrial anomaly detection rather than an optional enhancement.

The review also highlights the vulnerability of static threshold approaches to stealthy attacks, including low-and-slow, replay, and Man-in-the-Middle (MitM) attacks, which introduce subtle deviations that often remain below predefined detection boundaries. This limitation is particularly critical in oil and gas cyber-physical systems, where attackers can manipulate operational data while maintaining apparently normal process behaviour. To address these shortcomings, recent studies have proposed various adaptive threshold mechanisms, including reinforcement learning-based threshold optimisation, adaptive CUSUM, dynamic IQR, probabilistic threshold masking, segmented confidence sequences, and multi-scale adaptive confidence segmentation. Although these approaches generally improve detection performance, no single technique has emerged as universally applicable across all industrial environments, indicating that threshold adaptation remains an active area of research requiring context-specific solutions.

Finally, the review reveals that, despite extensive research on anomaly detection in general ICS and CPS environments, comparatively few studies focus specifically on oil and gas cyber-physical systems or evaluate adaptive threshold mechanisms against realistic MitM attacks using operational datasets and industrial testbeds. This imbalance highlights an important research gap and underscores the need for further domain-specific investigations. The identified limitations highlight several practical challenges associated with deploying static threshold-based detection methods in industrial environments. These include maintaining detection accuracy under changing operating conditions, reducing the need for frequent manual threshold recalibration, balancing false-positive and false-negative rates, and detecting stealthy attacks that remain within predefined decision boundaries. Addressing these challenges will require adaptive threshold mechanisms capable of continuously adjusting to evolving system behaviour while maintaining computational efficiency and operational reliability.

5.2 Current Challenges

Maintaining reliable detection performance under dynamic operating conditions remains difficult because static thresholds cannot accommodate concept drift and evolving process behaviour. Second, detecting stealthy attacks such as low-and-slow MitM and False Data Injection attacks continues to be challenging, as these attacks are specifically designed to remain within predefined decision boundaries. Third, balancing detection sensitivity with acceptable false-positive rates remains an unresolved issue, particularly in safety-critical industrial systems where excessive alarms may reduce operator confidence. In addition, many existing approaches require manual threshold calibration, limiting scalability and increasing maintenance effort. Finally, despite growing interest in adaptive thresholding, relatively few studies have validated these approaches using realistic oil and gas datasets or operational testbeds, making it difficult to assess their practical applicability.

5.3 Future Research Directions

Adaptive threshold mechanisms should be developed and validated for oil and gas cyber-physical systems using realistic operational datasets and industrial communication protocols. Second, hybrid detection frameworks that integrate statistical process monitoring with machine learning and reinforcement learning should be further explored to improve detection robustness under dynamic operating conditions. Future work should also focus on developing publicly available oil and gas cybersecurity datasets containing representative MitM attack scenarios to facilitate objective benchmarking of detection methods. Standardised evaluation frameworks would further support consistent comparison and practical deployment of adaptive threshold techniques. Finally, integrating adaptive cybersecurity mechanisms with functional safety frameworks, particularly dynamic Safety Integrity Level (SIL) assessment under cyberattack conditions, could enhance the resilience of industrial control systems against evolving cyber threats.

6. CONCLUSION

This systematic literature review synthesised evidence from 45 primary studies published between 2021 and 2026 to examine the limitations of static threshold-based methods for detecting Man-in-the-Middle (MitM) attacks in Oil and Gas Cyber-Physical Systems (OGCPS). The review found that statistical thresholding ($\mu \pm k\sigma$) remains the most widely adopted approach, alongside CUSUM, chi-square, Safety Integrity Level (SIL), Interquartile Range (IQR), percentile-based, and prediction-error thresholds. Despite their widespread use, these methods consistently exhibit limitations, including poor adaptability to dynamic operating conditions, vulnerability to stealthy attacks, reliance on manual threshold tuning, elevated false-positive rates, and reduced effectiveness under evolving data distributions.

REFERENCES

1. Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D. A., Bajaj, M., & Blazek, V. (2025). Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. Energy Reports. Elsevier.
2. Abraham, D., Erceylan, G., Gkioulos, V., & Houmb, S. H. (2024). Towards enhanced cybersecurity in industrial control systems: A systematic review of context-based modeling, digital twins, and machine learning approaches. Discover Applied Sciences. Springer.

3. Abshari, D., & Sridhar, M. (2025). Cyber-physical systems security: A comprehensive review of anomaly detection techniques. Computers & Security. Elsevier.
4. Acharya, A., & Bhalja, B. R. (2026). Real-time implementation and detection of stealthy false data injection attacks in active distribution networks using hardware-in-the-loop framework. 2026 IEEE Texas Power and Energy Conference (TPEC). IEEE.
5. Acquaah, Y. T., & Kaushik, R. (2024). Normal-only anomaly detection in environmental sensors in CPS: A comprehensive review. IEEE Access, 12, 191089-191105.
6. Aghaei Attar, A., Fabarisov, T., Bao, K., Hagenmeyer, V., & Morozov, A. (2024). Improving anomaly detection with adaptive dynamic threshold: A review and enhanced method. *IECON 2024 - 50th Annual Conference of the IEEE Industrial Electronics Society*. IEEE.
7. Aghazadeh Ardebili, A., Hasidi, O., Bendaouia, A., Khalil, A., Khalil, S., Luceri, D., Longo, A., Abdelwahed, E. H., Qassimi, S., & Ficarella, A. (2025). Enhancing resilience in complex energy systems through real-time anomaly detection: A systematic literature review. Springer.
8. Ahmad, H., Mansoor, F., Mustafa, G., Khan, A., Khan, A. Q., & Abid, M. (2025). Industrial network intrusion detection using a multilayer perceptron: Experimental evaluation on the Tennessee Eastman process. Expert Systems with Applications. Elsevier.
9. Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. Computers & Security. Elsevier.
10. Alyanbaawi, A. (2025). MITM- and DoS-resistant PUF authentication for industrial WSNs via sensor-initiated registration. Computers, 14(9), 347.
11. Arunthavanathan, R., Khan, F., Sajid, Z., Amin, M. T., Kota, K. R., & Kumar, S. (2025). Are the processing facilities safe and secured against cyber threats? Journal of Loss Prevention in the Process Industries. Elsevier.
12. Bhattacharya, A., Adhikary, S., Koley, I., Majumder, A., & Dey, S. (2024). Adaptive CUSUM-based residue analysis for stealthy attack detection in cyber-physical systems. ACM International Conference Proceedings Series. ACM.
13. Carrera-Rivera, A., Ochoa, W., Larrinaga, F., & Lasa, G. (2022). How-to conduct a systematic literature review: A quick guide for computer science research. MethodsX, 9, 101895.
14. Ding, F., Zhao, Y., Li, Z., Tang, H., Liu, Y., & Guo, D. (2026). Adaptive dynamic thresholds for unsupervised joint anomaly detection and trend prediction. Sensors, 26(1), 257.
15. Errachidi, S., Tasidou, A., Nait Chabane, A., & Beddiar, K. (2025). Reconstruction-based methods for multivariate time series anomaly detection: A review and taxonomy. ICAAI 2025. Manchester, United Kingdom.
16. Gülmez, Y., Konur, O., Erbas, M., & Bauk, S. (2024). Identifying cyber attack vulnerabilities in the main lubricating oil system of marine propulsion units. Ocean Engineering. Elsevier.
17. Halder, S., Ghosal, A., Newe, T., & Das, S. K. (2025). Dynamic anomaly threshold based malicious behavior detection in LoRa-assisted industrial IoT. 2025 IEEE 26th International Symposium on A World of Wireless Mobile and Multimedia Networks (WoWMoM) (pp. 82-91). IEEE.
18. Hasan, M. K., Gadekallu, T. R., Abdulkadir, R. A., & Safie, N. (2024). A review on machine learning techniques for secured cyber-physical systems in smart grid networks. Energy Reports. Elsevier.
19. Jeffrey, N., Tan, Q., & Villar, J. R. (2023). A review of anomaly detection strategies to detect threats to cyber-physical systems. Electronics, 12(15), 3283.
20. Katale, T. S., Gao, L., Zhang, Y., & Senouci, A. (2025). A bilevel optimization framework for adversarial control of gas pipeline operations. Actuators, 14(10), 480.

21. Li, M. A., & Gautam, A. (2025). Segmented confidence sequences and multi-scale adaptive confidence segments for anomaly detection in nonstationary time series. ACM Transactions on Knowledge Discovery from Data. ACM.
22. Liu, K., Song, R., Zhang, W., Guo, H., Han, J., & Zou, H. (2025). Research on hardware-in-the-loop test platform based on simulated IED and man-in-the-middle attack. Processes, 13(9), 2735.
23. Mattos, V., Schmidt, J. H., Bhaya, A., Oliveira de Sá, A., Sadoc Menasché, D., & Srivastava, G. (2024). Design and detection of covert man-in-the-middle cyberattacks on water treatment plants. ACM Digital Library.
24. Mehrpouyan, H. (2025). Fault tolerance vs. attack detection in industrial control systems: A deep learning approach. 2025 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE.
25. Mohammed, A. S., Anthi, E., Rana, O., & Burnap, P. (2025). STADe: An unsupervised time-windows method of detecting anomalies in oil and gas industrial cyber-physical systems (ICPS) networks. International Journal of Critical Infrastructure Protection, 49, 100762.
26. Mohammed, A. S., Anthi, E., Rana, O., Saxena, N., & Burnap, P. (2022). Detection and mitigation of field flooding attacks on oil and gas critical infrastructure communication. Computers & Security. Elsevier.
27. Mohammed, A. S., Reinecke, P., Burnap, P., Rana, O., & Anthi, E. (2022). Cybersecurity challenges in the offshore oil and gas industry: An industrial cyber-physical systems (ICPS) perspective. *ACM Transactions on Cyber-Physical Systems, 6*(3), Article 28.
28. Moila, R. L., & Velempini, M. (2025). Lightweight anomaly-based detection using cuckoo search algorithm and decision tree to mitigate man-in-the-middle attacks in DNS. Applied Sciences, 15(9), 5017.
29. Moriano, P., Hespeler, S. C., Li, M., & Mahbub, M. (2024). Adaptive anomaly detection for identifying attacks in cyber-physical systems: A systematic literature review. Springer Nature Computer Science. Springer.
30. Mtukushe, N., Onaolapo, A. K., Aluko, A., & Dorrell, D. G. (2023). Review of cyberattack implementation, detection, and mitigation methods in cyber-physical systems. Energies, 16(13), 5206.
31. Nishiuchi, T., Abe, Y., Watanabe, Y., Iwamoto, M., Sawada, K., & Shin, S. (2024). On the attack detection performance of information-theoretic method in industrial control system. *IECON 2024 - 50th Annual Conference of the IEEE Industrial Electronics Society*. IEEE.
32. Noorizadeh, M., Shakerpour, M., Meskin, N., Unal, D., & Khorasani, K. (2021). A cyber-security methodology for a cyber-physical industrial control system testbed. IEEE Access, 9, 16239-16252.
33. Obonna, U. O., Opara, F. K., Mbaocha, C. C., Obichere, J. C., Akwukwaegbu, I. O., Amaefule, M. M., & Nwakanma, C. I. (2023). Detection of man-in-the-middle (MitM) cyber-attacks in oil and gas process control networks using machine learning algorithms. Future Internet, 15(8), 280.
34. Oliveira, L. M. de, Saavedra, J. A. D. L. C., El Kattel, M. B., & Antunes, F. L. M. (2025). Adaptive statistical windowing for anomaly detection in industrial sensor signals. IEEE Sensors Letters.
35. Pinto, A., Herrera, L. C., Donoso, Y., & Gutierrez, J. A. (2023). Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure. Sensors, 23(5), 2415.
36. Rodrigues, C., Júnior, W. S. S., Oliveira, W., & Lima, I. (2025). A data rate monitoring approach for cyberattack detection in digital twin communication. Sensors, 25(24), 7476.

37. Seo, J. K., Lee, J., Kim, B., Shim, W., & Seo, J. T. (2026). AI-based anomaly detection in industrial control and cyber-physical systems: A data-type-oriented systematic review. Electronics, 15(1), 20.
38. Skrodelis, H. K., & Romanovs, A. (2025). Explainable hybrid intrusion detection for SCADA/ICS: A review and research agenda. PeerJ Computer Science.
39. Sun, S., Haque, K. A., Huo, X., Sahu, A., Goulart, A., & Davis, K. (2025). Anomaly detection in cyber-physical systems using long-short term memory autoencoders: A case study with man-in-the-middle (MiTM) attack. IEEE Transactions on Power Systems.
40. Umer, M. A., Junejo, K. N., Jilani, M. T., & Mathur, A. P. (2023). Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. Proceedings of the 13th ACM Conference on Data and Application Security and Privacy (CODASPY). ACM.
41. Wang, Z., Wang, J., Wei, Z., Ye, W., & Zhang, L. (2025). Safety integrity level assessment for safety instrumented system in oil and gas station with cyber threat. Reliability Engineering & System Safety. Elsevier.
42. Wu, T., Zhou, D., Ou, Q., & Luo, F. (2026). Intrusion detection systems in industrial control systems: Landscape, challenges and opportunities. Journal of Information Security and Applications. Elsevier.
43. Xing, W., & Shen, J. (2024). Security control of cyber-physical systems under cyber attacks: A survey. Sensors, 24(12), 3815.
44. Xu, G., Wang, Y., Zhou, Z., Lu, Y., & Cai, L. (2025). A data-driven state identification method for intelligent control of the joint station export system. Scientific Reports, 15.
45. Yang, X., Howley, E., & Schukat, M. (2024). ADT: Agent-based dynamic thresholding for anomaly detection. Computers & Security, 141, 103825.