Cyber Situational Awareness for Oil & Gas Pipeline Networks: A Systematized Review of Methods, Models, and Engineering Practice

Fei Song[1], Tieliang Sun[1], Shuai Jiang[1], Yuqin Wang[1], Shiyin Zhu[2]*

[1] PipeChina North Pipeline Company, China
[2] Beijing Information Science and Technology University, China
songfei@pipechina.com.cn, suntl@pipechina.com.cn, jiangshuai01@pipechina.com.cn, wangyq@pipechina.com.cn, 20141903@bistu.edu.cn

Abstract

This review systematizes cyber situational awareness (CSA) for oil & gas pipeline networks with an application-oriented workflow spanning data inputs, processing pipelines, and decision outputs. Building on recent literature, we distill three recurrent strands into reusable engineering dimensions-representative evidence, methods, constraints, and evaluation: (i) joint communication–process anomaly identification that fuses cyber telemetry with process signals; (ii) cross-domain situation modeling capable of spanning OT/IT boundaries under cloudified and remote O&M; and (iii) knowledge-driven context fusion with event-to-process-impact scoring to link alerts to operational risk. We synthesize method families covering spatiotemporal graph/Transformer learning, semi/self-supervision for scarce labels, evidential risk aggregation (e.g., Dempster–Shafer), hierarchical indicators and weighting (AHP), and SOC-oriented visualization that couples algorithmic metrics with operational KPIs. A critical appraisal reveals persistent gaps: non-uniform indicator definitions and weightings, the lack of pipeline-specific OT/ICS benchmarks, fragile cross-domain generalization, and detection-centric designs that seldom progress into explainable, auditable, and cost-aware response. To bridge research and deployment, we propose a practical agenda: establish harmonized benchmarks and evaluation protocols aligned with O&M KPIs; adopt governance-first multi-source integration with an ontology/knowledge-graph backbone; co-design models and runtime for edge/regional constraints via compression, distillation, and event-driven inference; and advance toward closed-loop defense through policy learning and playbook-guided automation. The review consolidates fragmented advances into a transferable, scalable, and measurable pathway for CSA in real pipeline environments.

Keywords: Cyber situational awareness, OT/ICS (SCADA) security, Spatiotemporal graph/transformer, Closed-loop defense

1 Research Status

1.1 Research Progress on Cyber Situational Awareness for Oil & Gas Pipeline Networks

Oil and gas pipeline networks are geographically distributed cyber-physical systems operated within integrated OT/IT environments that comprise field stations and valve rooms (sensors and RTU/PLC), heterogeneous wide-area communications (leased lines/public Internet/satellite), and central SCADA, data historians, and security operations capabilities; within this context, cyber situational awareness (CSA) aims to aggregate, correlate, and project multi-source evidence-including industrial protocol communications, process time series, and system/security logs-along the perception -comprehension–projection cycle to produce explainable and auditable risk representations aligned with operational objectives [1]. To provide a rigorous bridge from concepts to engineering use, we formalize an application-oriented CSA reference workflow with three stages-data inputs, processing pipeline, decision outputs (Figure 1). This choice is methodologically supported by systematic evidence from cyber situation-awareness research and SOC-oriented situation-awareness studies [1-2]. Building on this foundation, Table 1 maps three commonly reported research strands-joint communication–process modeling, cross-domain situation modeling, knowledge-driven impact scoring-onto a set of reusable engineering dimensions (representative evidence, methods, constraints, evaluation). This mapping standardizes reporting and facilitates apples-to-apples evaluation and replication across heterogeneous proposals [3-8].

(i) Joint Communication–process Anomaly Identification.

Within industrial control system (ICS) security, relying on a single data modality (only traffic or only logs) rarely yields high-confidence detection; a comprehensive survey shows that multi-modal fusion of OT protocol flows (e.g., Modbus, DNP3, IEC-104, OPC UA), host/system events, and process variables has become a dominant trend for improving detectability and deployability in operational environments [3]. A focused review of machine learning

*Corresponding Author: Shiyin Zhu; Email: 20141903@bistu.edu.cn
DOI: https://doi.org/10.70003/160792642025112606008

methods for ICS security further indicates that deep temporal models (e.g., CNN-LSTM and self-attention) are suited to capture dynamic dependencies in process behavior, and that lightweight inference at the edge is advisable to satisfy millisecond-to-second latency constraints typical of industrial processes [4]. From a learning-paradigm viewpoint, a survey centered on intrusion detection contrasts supervised, semi-supervised, and unsupervised strategies and argues that semi-/self-supervised designs are more robust under scarce labeling, which is common in ICS datasets [5]. For cross-station correlation, a correlation-based multivariate anomaly detection framework constructs intra-/inter-station variable-relation graphs and then performs combined statistical/learning tests to suppress false positives, which naturally fits the hierarchical topology of "station-segment-center" in pipeline systems [6]. On the process side, a method that combines process invariants with swarm-intelligence search automatically derives verifiable detection rules to mitigate label scarcity while enforcing physical consistency; this design is directly applicable to oil-and-gas variables such as pressure, flow, and valve position [7].

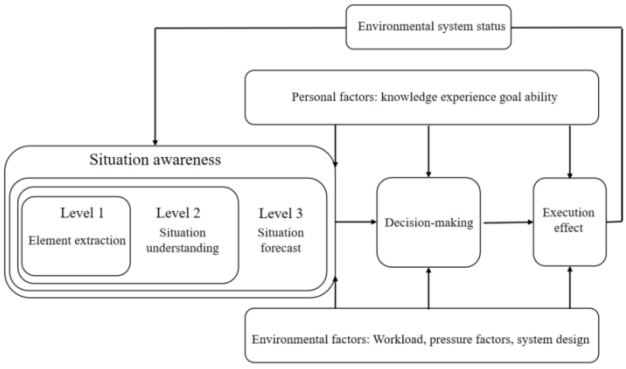

Figure 1. Endsley-based situation awareness–decision–action closed-loop reference model

Table 1. Alignment of evidence, methods, constraints, and evaluation across CSA research strands for oil & gas pipeline networks

Strand	Representative evidence	Representative methods	Key characteristics	Adaptation points
Joint communication–process anomaly identification	Industrial-protocol DPI, system/security logs, pressure/flow/valve time series	Deep temporal models (CNN-LSTM/Transformer), correlation-based detection, semi-/self-supervised learning	Multi-modal fusion, low-latency edge inference, cross-station association	Cope with long-haullink instability; limited labels; maintain explainability
Cross-domain situation modeling (cloud/remote)	Identity & access auditing, cloud API logs, link-quality metrics	Zero-trust & continuous evaluation, evidence fusion with visual analytics	End-to-cloud evidence loop, stronger traceability	Continuous assessment for remote supervision/ inspection
Knowledge-driven semantic fusion and impact scoring	Asset/process/topology/ event knowledge; work-order records	Knowledge-graph representation & reasoning; representation learning	Evidence alignment, causal tracing, quantitative impact scoring	Harmonize with NIST/ IEC baselines and API 1164

(ii) Cross-domain situation modeling under cloudification and remote operations.

As pipeline enterprises migrate historians, disaster recovery, and selected applications to cloud platforms-while simultaneously operating over mixed wide-area media (leased/public/satellite)-CSA must explicitly incorporate cloud-side observability (identity and access auditing, API invocation traces) and link-quality measurements (loss, latency, jitter) as first-class evidence. A recent survey on cloud-based SCADA systems synthesizes the resulting risks from shared resources, access-boundary management, and protocol weaknesses, and recommends building zero-trust, least-privilege, continuously evaluated cross-domain situation graphs for remote operation paths [8]. From an energy-sector perspective, a systematic review demonstrates that coupling the "alert aggregation → situation interpretation → response orchestration" workflow with visual analytics and human-in-the-loop interfaces reduces operational burden and improves response consistency-capabilities that are critical for remote supervision and inspection in pipeline scenarios [9].

(iii) Knowledge-driven context fusion and "event-to-process-impact" quantification.

In asset- and process-rich environments, a knowledge layer can unify assets, process flows, topology, event semantics, and work-order records into a single semantic space. A state-of-the-art review on cybersecurity knowledge graphs details construction pipelines, entity–relation representations, and reasoning mechanisms, and shows that knowledge representation and reasoning enhance cross-source evidence alignment, causal tracing, and automated orchestration [10]. An engineering-oriented survey on knowledge-graph construction further

proposes combining representation learning with ontology constraints to realize robust matching and explainable inference across heterogeneous evidence [11]. For industry alignment, authoritative baselines are essential: NIST SP 800-82 Rev.3 specifies OT-centric zoning/segmentation, metrics, and control requirements, offering a principled basis for defining knowledge-layer control objectives and measurement loops [12]; API Standard 1164 (3rd ed.) provides graded protection and audit requirements for pipeline control systems and thus an implementation guideline for mapping security events to quantitative impacts on pressure, flow, and transport capacity [13]. Complementing these, Ma survey synthesizes recent advances across attack/defense, detection, risk assessment, response, and protection in ICS, underscoring the importance of linking detection outcomes with risk evaluation and response strategies to close the evidence-to-action loop-an approach that aligns closely with CSA deployment in pipeline operations [14].

(iv) Evaluation paradigm: beyond model scores to operations-oriented KPIs.

Exclusive reliance on Precision/Recall, F1, and AUC is insufficient to reflect operational value in pipeline contexts. A systematic review of SOC situation awareness advocates incorporating operations-oriented KPIs-e.g., mean time to acknowledge and repair, alert deduplication ratio, and end-to-end response SLAs-and enhancing situation explainability to reduce human workload [2]. Together with correlation-driven anomaly detection and process-invariant constraints, these practices enable quantification of impact duration and magnitude on transport continuity, thereby aligning evaluation with process objectives [6-7].

1.2 Research on Network Security Situational Awareness Models and Risk-Assessment Methods

Networked situational awareness (NSSA) in cyberspace can be framed as a data-driven pipeline that links layered sensing to semantic interpretation and forward projection; Abuabid articulates this as a unified, ML-centric approach that operationalizes SA with supervised learning over enterprise telemetry [15]. In SOC practice, Forsberg introduces a metric design framework that turns the "alert aggregation → situation interpretation → response" workflow into measurable, operations-oriented performance indicators, offering a concrete basis for evaluating SA effectiveness [16].

In situational modeling, Kiflay demonstrates that multimodal fusion of flow and payload features improves robustness over single-modality NIDS, underscoring fusion as a first-class design choice for deployability [17]; Xu further shows a few-shot, multimodal scheme that merges traffic-feature graphs with packet-feature sets to maintain performance under scarce labels [18]. From a learning-paradigm viewpoint, Nakıp proposes an online self-supervised IDS that continuously adapts feature representations during streaming operation, while Shyaa surveys concept drift handling and feature-engineering tactics essential for sustaining accuracy as threats evolve [19-20]. For correlation modeling, Birihanu presents an explainable correlation-based anomaly detection approach that exploits inter-sensor relationships to trace anomaly propagation-providing a reusable pattern for multi-variable, cross-segment detection without relying on heavy labeling [21].

For risk assessment that fuses subjective and objective information, the classical Dempster–Shafer (DS) evidence theory has remained widely used in recent years for risk aggregation in networks and critical infrastructure. In maritime-network risk studies, Uflaz et al. fused expert evidence via DS to quantify potential risks under different attack scenarios, demonstrating DS's applicability to uncertainty representation and conflict handling [22]. For smart-city and sectoral digitalization scenarios, Al Sharif et al. embedded DS into a comprehensive risk-analysis pipeline-from evidence modeling to synthesis and decision making-offering a transferable template for risk metrics in network and IoT contexts [23]. In terms of formal advances in evidential reasoning, Chen et al. introduced an evidential model on an ordered frame of discernment to address limitations of traditional DS in frame granularity and conflict management, providing a reusable inference pipeline for quantitative assessment in software and network security [24].

With respect to hierarchical indicators and weight determination, Analytic Hierarchy Process (AHP) remains a common tool for constructing situational scores, while recent work stresses its integration with imbalance-aware learning and ensemble classifiers. Aimed at the IIoT, Yi et al. proposed an AHP-driven quantitative assessment pipeline that combines AUOS re-sampling with an XGBoost classifier to mitigate class imbalance and feature heterogeneity, significantly improving classification stability and interpretability [25]. In a more general network-SA setting, Zhang et al. presented a concrete implementation of "AHP decomposition-weight estimation-composite scoring," which serves as a baseline paradigm for multi-indicator evaluation [26].

In the measurement and visualization direction-specifically, how to quantify situational cognition-Wong and McNeese proposed a metric framework that crosses the Cyber Operations Five-Plane model with Endsley's three levels, producing a reusable question bank and rating scales for quantitative SA measurement under varied task contexts [27]. For immersive situational awareness, Ahmad et al. surveyed visualization and interaction techniques and summarized evaluation mechanisms aligned with SA levels (perception, comprehension, projection), providing synthesized evidence for designing large-scale visual-analytics systems [28]. From the resilience-engineering perspective, a cross-review of resilience and SA argued that absorption, recovery, and adaptive capacity should be integrated into SA modeling and measurement, forming a closed-loop indicator system spanning threat–vulnerability–impact [29].

Under information sharing and national/regional scales, Serini proposed a concept model of "collective situational awareness" at the EU level, stressing standardized exchange mechanisms among member states and institutions to reduce decision uncertainty under cross-

domain threats [30]. At the organizational level, Renaud and Goucher developed a cyber-SA model for SMEs and showed empirically that an organization's SA level is positively associated with the strength of its control implementation, making the model a practical measure for capability building [31]. At the national level, a framework for cyber SA with simplified metrics and crisis-management orientation was proposed to support macro-level decision making and early warning [32]. To support method selection and reproducibility, the studies discussed in this subsection are aligned into a five-tuple- "methods/models, core idea, strengths, limitations, representative refs." -as summarized in Table 2.

Table 2. Structured alignment of methods–core ideas–strengths–limitations–representative references for NSSA modeling and risk assessment

Strand	Methods / Models	Core idea	Strengths	Limitations
Foundational SA pipeline & SOC metrics	Data-driven SA framing; SOC KPI design	Frame SA as layered sensing → semantic interpretation → projection; operationalize "alert → interpretation → response" as KPIs	Unified terminology; KPI-based evaluation	Abstract; needs concrete modeling
Multimodal SA modeling	Fusion of flow + payload; few-shot multimodal fusion	Treat fusion as first-class; sustain performance under scarce labels	Robust and deployable	Alignment overhead; feature work
Learning under drift / scarce labels	Online self-supervised IDS; concept-drift handling	Adapt representations to evolving threats; engineer features against drift	Maintains accuracy in streams	Stability/complexity trade-off
Correlation-based, explainable detection	Inter-sensor/variable correlation; explainability	Trace anomaly propagation via relation graphs	Label-light; cross-segment	Depends on topology quality
Evidential risk assessment	DS fusion; ordered frame of discernment	Fuse subjective + objective evidence; manage uncertainty/conflict	Works with incomplete/conflicting info	Sensitive to fusion rules
Hierarchical indicators & weighting	AHP + imbalance-aware resampling + ensembles	Decompose indicators → weights → composite score	Interpretable, practical	Expert bias risk
Measurement & visualization	Metric frameworks; immersive visual analytics	Cross Endsley levels with cyber planes; quantitative SA	Reusable question banks; design guidance	Cost; generalizability
Resilience-oriented SA	SA × resilience (absorb–recover–adapt)	Integrate resilience into SA metrics loop	Links threat→vulnerability→impact	Needs longitudinal data
Collective / organizational / national SA	Collective SA; SME model; national framework	Standardized sharing; capacity building; macro early warning	Reduces decision uncertainty	Governance & data sovereignty

1.3 Survey of Cyber Situational Awareness: Toward Information Security and Intelligent Challenges

Cyber network situational awareness (NSSA) underpins rational response through the loop of "behavior identification-intent understanding-impact assessment," and recent reviews converge on a three-stage pipeline of "element extraction-assessment-prediction," while highlighting the growing role of AI models in multi-source fusion and projection accuracy [33]. From an engineering standpoint, an integrated route that couples NSSA with data-security protection is taking shape: end-to-end frameworks align threat identification, vulnerability hardening, and data-protection controls with classification/analytics policies so that sensing, inference and protection can be co-designed rather than bolted on [34]. At the governance layer, collective awareness increasingly depends on standardized cyber-threat-intelligence (CTI) sharing and common evaluation vocabularies; recent syntheses show that well-specified sharing formats and exchange processes improve cross-domain decision certainty and the explainability of actions taken under time pressure [35].

In critical infrastructure and ICS/OT contexts, new surveys emphasize "attack surface-detection-risk assessment-response" as a closed loop, and propose hybrid threat-modelling that blends system-, attacker- and risk-centric views to keep situational reasoning consistent across IT/OT convergence scenarios [36]. In enterprise digitalization, big-data-driven modelling-combining complex-network analysis with ML risk predictors-has been shown to raise identification efficiency under heterogeneous telemetry and to support real-time posture tracking at scale, making data-centric NSSA a practical default for modern organizations [37].

In detection and prediction, Zhang et al. propose a smarter traffic-based detection scheme using real PCAP files; via feature engineering and classifier optimization it improves the practicality and efficiency of intrusion recognition and serves as an effective front-end for situational assessment [38]. Regarding learning paradigms, Chen employs regression and support-vector methods to achieve lower prediction error on historical attack data and strengthen situational capability [39]; In parallel, an IEEE study operationalizes forecasting of post-exploitation steps by learning from CTI reports and system logs, so measurement and response can form a closed loop **earlier** within enterprise EDR workflows [40]. For IoT, an IEEE edge-centric security state-awareness model fuses device-state signals and local traffic at the **edge**, enabling real-time situational assessment under heterogeneous endpoints and massive-connectivity [41]. Under large-scale heterogeneous telemetry, recent work shows that self-supervised, online, and lightweight anomaly/event detection at the IoT edge-using compact sequence models and on-device feature learning-can deliver strong label-free performance, thereby improving assessment throughput and accuracy for global situational awareness [42]. In parallel, for complex attack surfaces, a decentralized dynamic-state estimation framework explicitly modeling DoS, bias-injection, and replay attacks sustains real-time state prediction and robust estimation under partial observability, offering a practical basis for online resource orchestration [43].

To reduce cross-paper comparison and reproduction overhead, Table 3 structurally aligns the studies discussed in this subsection along "Author | Scenario | Core method | Key techniques/models | Main contribution." The table only consolidates claims already argued in the text, mapping methods to data and contributions to help readers quickly choose reproducible input–method–metric combinations and comparison baselines.

Table 3. Structured alignment of Author–Scenario–Method–Technique–Contribution for NSSA studies

Author (Year)	Application scenario	Core method	Key techniques / models	Main contribution
Wang (2023) [33]	NSSA overview (AI-centric)	Three-stage NSSA pipeline	Multi-source fusion; ML-based assessment & prediction	Unifies "element extraction–assessment–prediction"; highlights AI for fusion & projection accuracy
Wang (2025) [34]	Network & data security (overall)	Integrated route: NSSA + data-security	Threat identification, vulnerability hardening, data-protection controls; classification/analytics	End-to-end engineering so sensing–inference–protection are co-designed rather than bolted on
Fang et al. (2025) [35]	Macro governance / CTI sharing	Collective SA via standardized CTI exchange	Standardized formats & exchange workflows; common evaluation vocabulary	Improves cross-domain decision certainty and explainability under time pressure
Badawy (2024) [36]	ICS/OT (critical infrastructure)	Closed loop "attack surface–detection–risk–response"	Hybrid threat-modeling (system/attacker/risk views); IT/OT convergence	Keeps situational reasoning consistent across convergence scenarios
Li (2025) [37]	Enterprise digitalization / big data	Data-driven SA modeling at scale	Complex-network analysis + ML risk predictors; heterogeneous telemetry	Higher identification efficiency; supports real-time posture tracking
Zhang et al. (2024) [38]	Network traffic detection	PCAP-based intrusion recognition	Feature engineering; classifier optimization	Practical, efficient front-end for situational assessment
Chen (2017) [39]	Historical threat prediction	Regression & SVM	Feature selection; error-aware modeling	Lower prediction error; stronger predictive SA capability
Zhu (2025) [40]	Post-exploitation forecasting	CTI/log-driven threat step prediction	Time-series projection; NLP extraction; uncertainty-aware evaluation; EDR workflow	"Shift-left" closed loop-earlier coupling of measurement and response
Lei (2021) [41]	IoT security (edge)	Edge-centric security state awareness	Device-state signals + local traffic; lightweight ML at edge	Real-time assessment under endpoint heterogeneity and massive connectivity
Abououf (2022) [42]	Large-scale heterogeneous IoT telemetry	Self-supervised online anomaly/event detection	On-device feature learning; sequence autoencoding; lightweight runtime	Strong **label-free** detection; boosts assessment throughput & accuracy
Qu (2025) [43]	Complex attack surfaces (power grid)	Decentralized dynamic-state estimation under cyber-attacks	Robustness to DoS, bias-injection, replay; partial-observability handling	Real-time state prediction & robust estimation for online orchestration

2 Unresolved Challenges

Current research on network security situational awareness has progressed in multiple areas. Building on the preceding sections, at the scenario-and-framework level, an OT/IT integrated environment for oil and gas pipeline networks has converged on a tiered, collaborative paradigm centered on "edge–regional–central." At the methods-and-models level, multi-source data fusion, temporal/graph learning, and knowledge representation have advanced the perception, comprehension, and projection of situational awareness. At the application level, practice targeting SOCs, ICS/OT, IoT, and large-scale data has continued to expand, forming comparable input–method–metric combinations.

In risk assessment and measurement, the integration of multi-source evidence with AI has enabled more accurate and dynamic evaluation models, while indicator systems have gradually extended from algorithmic accuracy to operational efficiency and business impact, thereby strengthening protection and response capabilities.

At the same time, several open problems remain:

2.1 Inadequate Model Construction and Algorithm Optimization

Although significant progress has been made in the construction of models and optimization of algorithms for network security situational awareness, current research still falls short in several aspects. On one hand, existing models lack a comprehensive consideration of complex network environments and fail to effectively capture the dynamic evolution of security situations, resulting in insufficient accuracy and adaptability in real-world applications. On the other hand, algorithm optimization still relies heavily on traditional computational methods, lacking innovative algorithmic designs capable of handling massive datasets and high-dimensional features. Moreover, existing models and algorithms face limitations in processing multi-source heterogeneous data and integrating information from different layers, making them inadequate for the demands of complex situational awareness in practical network environments. Sun et al. (2024) propose a GNN-based intrusion detection system (GNN-IDS) that fuses a static attack graph with dynamic runtime telemetry into a single graph input and performs inference with a graph neural network. Evaluated on two public IDS datasets, the method reports consistently strong Precision/Recall/F1 and, compared with non-graph baselines, an average reduction of prediction uncertainty of about 5% [44].

2.2 Unresolved Challenges in Security Assessment and Defense

Network security situational awareness technologies face numerous difficulties in the areas of security evaluation and defense. First, the selection and fusion of security assessment indicators lack unified standards and specifications, leading to significant subjectivity and uncertainty in evaluation results. Second, the formulation of defense strategies often relies on static models and algorithms, which struggle to adapt to the dynamic nature of cybersecurity threats. Furthermore, current defense mechanisms are insufficient in responding to novel attack methods and complex threat scenarios, making it difficult to achieve real-time and effective protection. Therefore, more accurate security evaluation methods and more targeted defense strategies are urgently needed to enhance the defensive capabilities of situational awareness systems. Recent work by Sayghe [45] introduces a digital-twin–driven intrusion detection (DT-ID) framework for industrial SCADA. In simulation studies, DT-ID reports an F1-score of 96.3%, false-positive rate < 2.5%, and average detection latency < 500 ms, outperforming a rule-based Snort IDS and a physics-only anomaly detector. These figures suggest meaningful gains in evaluation accuracy and timeliness. However, the design still centers on detection rather than closed-loop, self-adaptive defense; translating high detection scores into online response policies (e.g., RL-based mitigation, moving-target strategies) and proving cross-domain robustness on OT traffic from pipeline SCADA remain open problems-precisely the gaps highlighted in this section.

2.3 Incomplete Strategies for Addressing Intelligent Challenges

With the rapid advancement of information technologies, the field of network security situational awareness is encountering increasingly complex intelligent challenges. First, current research lacks innovation in algorithm design and struggles to improve computational efficiency, making it difficult to handle large-scale data and high-dimensional feature sets. Second, the application of big data and artificial intelligence in situational awareness systems remains at an early stage, without a well-established theoretical system or technical framework. Additionally, the strategies for addressing intelligent cybersecurity threats lack systematic integration, hindering cross-domain and cross-technology collaboration. Thus, it is imperative to improve strategic frameworks for intelligent threat response and drive further development in network security situational awareness technologies. A recent study by Govindarajan [46] proposes a modular IDS that fuses graph-based feature extraction, a Transformer autoencoder, and contrastive learning for high-throughput cloud environments. Evaluated on NSL-KDD and CIC-IDS2018, it reports average accuracy 99.97% with low false-positive rates and real-time inference under modest resources, indicating gains in both algorithmic effectiveness and computational efficiency. Yet, despite strong IT-cloud results, the work stops short of a unified theory/architecture for cross-domain SA and does not verify performance on OT/ICS telemetry typical of oil & gas-mirroring the "incomplete strategies" gap identified in this subsection.

3 Conclusion

Research on network security situational awareness

(NSSA) for oil & gas pipeline systems is evolving from concept- and checklist-style advances toward an engineering-oriented system that is driven by business processes, led by data governance, and evaluated with comparable metrics. The first part of the paper surfaces the main threads in current research and practice: (i) joint communication–process anomaly identification is becoming a consensus, as single-modality inputs (traffic-only or log-only) cannot reliably capture causal mechanisms; (ii) with the deepening of cloudification and remote O&M, situational modeling must characterize spatiotemporal correlations across domains, layers, and stations; (iii) knowledge-driven contextual fusion and quantitative "event-to-process impact" mapping are key to turning detection outputs into executable decisions; (iv) metric quantification and visualization determine whether situational cognition can be used by SOC/control-room operators; and (v) under broader information sharing and sector-level collaboration, models and evaluations need portability, comparability, and reproducibility. The second part complements these threads methodologically: Dempster–Shafer (DS)–style evidence fusion for uncertainty, hierarchical indicators and weight determination (e.g., AHP) for multi-dimensional assessment, attack-graph/dependency modeling for causal structure, and quantification/visualization paradigms that enhance cognitive usability-together with structured summary tables to lower reproduction cost and to expose the key gaps between research and engineering.

Synthesizing the convergences and gaps across Parts One and Two, current strengths lie in the emergence of multi-source fusion, spatiotemporal correlation, and knowledge context as standard modeling elements, and in the shift of evaluation from single-point accuracy toward latency, explainability, and O&M usability. Limitations persist in non-uniform indicator/weight definitions, unverified cross-domain generalization, insufficient closed-loop coupling, and the lack of comparable baselines under real OT/ICS conditions. Accordingly, four actionable recommendations are offered:

(1) Unified evaluation and benchmark construction. Build same-domain, same-metric benchmark datasets and protocols around typical oil & gas SCADA scenarios, aligning algorithmic scores with O&M KPIs (e.g., alert acknowledgement/repair time, impact on transport capacity) to support cross-study and cross-site comparability and transferability.

(2) Data-governance-first with a semantic backbone. Prioritize data quality, spatiotemporal alignment, and semantic disambiguation; use ontologies/knowledge graphs to align alarms, operating conditions, work orders, and equipment states to a shared semantic coordinate system, establishing a consistent fact base for risk quantification and coordinated response.

(3) Joint modeling with engineering-constraint co-design. Maintain a "communication + process" multi-modal approach and combine spatiotemporal graph modeling with attention to capture cross-site correlations; on the engineering side, use edge/regional collaborative inference, model compression, and event-driven computation to achieve a compute–latency–reliability balance.

(4) From detection to closed loop. Integrate detection–assessment–decision–action into a closed-loop policy, jointly optimizing false-positive cost, response latency, and process safety; constrain with explainable policies and auditable playbooks to form replicable, evolvable runbooks and toolchains that support continual learning and policy evolution.

The above synthesis condenses the trajectories and methods developed in the first two parts into a transferable, scalable, and measurable NSSA and active-defense framework oriented to real oil & gas pipeline operations, providing a reproducible technical and governance pathway for sector-level security operations.

For an at-a-glance alignment of strengths and gaps, this section includes a bar chart comparing capability readiness across five core dimensions (see Figure 2). Multi-source fusion and data governance exhibit moderate maturity (~68% and ~62%), whereas indicator standardization (45%), cross-domain generalization (38%), and closed-loop defense (32%) remain the primary bottlenecks-highlighting the need to prioritize unified evaluation baselines and end-to-end strategy integration from detection to response.

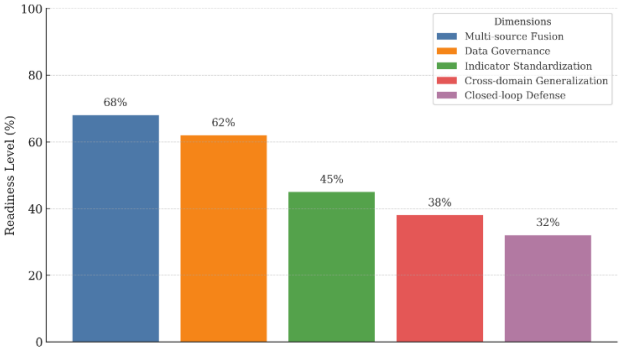

Figure 2. Maturity of five core CSA capabilities

Acknowledgement

This work is supported by National Key Research and Development Program Project (Grant No. 2023YFB3107700); Provincial Science and Technology Plan Project of Hebei Province (Grant No. 253A7634D).

References

[1] H. Alavizadeh, J. Jang-Jaccard, S. Y. Enoch, H. Al-Sahaf, I. Welch, S. A. Camtepe, D. D. Kim, A Survey on Cyber Situation-Awareness Systems: Framework, Techniques, and Insights, *ACM Computing Surveys*, Vol. 55, No. 5, pp. 1–37, May, 2023. https://doi.org/10.1145/3530809

[2] H. J. Ofte, S. Katsikas, Understanding Situation Awareness in SOCs: A Systematic Literature Review, *Computers & Security*, Vol. 126, Article No. 103069, March, 2023. https://doi.org/10.1016/j.cose.2022.103069

[3] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, N. Meskin, Cybersecurity for Industrial Control Systems: A

Survey, *Computers & Security*, Vol. 89, Article No. 101677, February, 2020.
https://doi.org/10.1016/j.cose.2019.101677

[4] A. M. Y. Koay, R. K. L. Ko, H. Hettema, K. Radke, Machine Learning in Industrial Control System (ICS) Security: Current Landscape, Opportunities and Challenges, *Journal of Intelligent Information Systems*, Vol. 60, No. 2, pp. 377–405, April, 2023.
https://doi.org/10.1007/s10844-022-00753-1

[5] M. A. Umer, K. N. Junejo, M. T. Jilani, A. P. Mathur, Machine Learning for Intrusion Detection in Industrial Control Systems: Applications, Challenges, and Recommendations, *International Journal of Critical Infrastructure Protection*, Vol. 38, Article No. 100516, September, 2022.
https://doi.org/10.1016/j.ijcip.2022.100516

[6] Z. Jadidi, S. Pal, M. Hussain, K. N. Thanh, Correlation-Based Anomaly Detection in Industrial Control Systems, *Sensors*, Vol. 23, No. 3, Article No. 1561, February, 2023.
https://doi.org/10.3390/s23031561

[7] Y. Song, H. Huang, H. Wang, Q. Wei, Leveraging Swarm Intelligence for Invariant Rule Generation and Anomaly Detection in Industrial Control Systems, *Applied Sciences*, Vol. 14, No. 22, Article No. 10705, November, 2024.
https://doi.org/10.3390/app142210705

[8] A. Wali, F. Alshehry, A Survey of Security Challenges in Cloud-Based SCADA Systems, *Computers*, Vol. 13, No. 4, Article No. 97, April, 2024.
https://doi.org/10.3390/computers13040097

[9] S. Saeed, H. Gull, M. M. Aldossary, A. F. Altamimi, M. S. Alshahrani, M. Saqib, S. Z. Iqbal, A. M. Almuhaideb, Digital Transformation in Energy Sector: Cybersecurity Challenges and Implications, *Information*, Vol. 15, No. 12, Article No. 764, December, 2024.
https://doi.org/10.3390/info15120764

[10] L. F. Sikos, Cybersecurity Knowledge Graphs, *Knowledge and Information Systems*, Vol. 65, No. 9, pp. 3511–3531, September, 2023.
https://doi.org/10.1007/s10115-023-01860-3

[11] X. Zhao, R. Jiang, Y. Han, A. Li, Z. Peng, A Survey on Cybersecurity Knowledge Graph Construction, *Computers & Security*, Vol. 136, Article No. 103524, January, 2024.
https://doi.org/10.1016/j.cose.2023.103524

[12] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, M. Thompson, *Guide to Operational Technology (OT) Security*, National Institute of Standards and Technology Report, NIST SP 800-82 Rev. 3, September, 2023.
https://doi.org/10.6028/NIST.SP.800-82r3

[13] American Petroleum Institute, API Standard 1164: Pipeline Control Systems Cybersecurity (3rd Edition), *American Petroleum Institute Standard*, August, 2021.

[14] Y.-W. Ma, Y.-H. Tu, C.-W. Tsou, Y.-N. Chiang, J.-L. Chen, A Survey of Cyber Security and Safety in Industrial Control Systems, *Journal of Internet Technology*, Vol. 25, No. 4, pp. 541–550, July, 2024.
https://doi.org/10.70003/160792642024072504005

[15] A. A. Abuabid, A Data-Driven Approach to Cybersecurity Situational Awareness: Insights from Machine Learning, *Journal of Innovative Digital Transformation*, Vol. 2, No. 2, pp. 131–155, July, 2025.
https://doi.org/10.1108/JIDT-03-2025-0013

[16] J. Forsberg, T. Frantti, Technical Performance Metrics of a Security Operations Center, *Computers & Security*, Vol. 135, Article No. 103529, December, 2023.
https://doi.org/10.1016/j.cose.2023.103529

[17] A. Kiflay, A. Tsokanos, M. Fazlali, R. Kirner, Network Intrusion Detection Leveraging Multimodal Features, *Array*, Vol. 22, Article No. 100349, July, 2024.
https://doi.org/10.1016/j.array.2024.100349

[18] C. Xu, Y. Zhan, Z. Wang, J. Yang, Multimodal Fusion Based Few-Shot Network Intrusion Detection System, *Scientific Reports*, Vol. 15, No. 1, pp. 1–23, July, 2025.
https://doi.org/10.1038/s41598-025-05217-4

[19] M. Nakip, E. Gelenbe, Online Self-Supervised Deep Learning for Intrusion Detection Systems, *IEEE Transactions on Information Forensics and Security*, Vol. 19, pp. 5668–5683, May, 2024.
https://doi.org/10.1109/TIFS.2024.3402148

[20] M. A. Shyaa, N. F. Ibrahim, Z. Zainol, R. Abdullah, M. Anbar, L. Alzubaidi, Evolving Cybersecurity Frontiers: A Comprehensive Survey on Concept Drift and Feature Dynamics Aware Machine and Deep Learning in Intrusion Detection Systems, *Engineering Applications of Artificial Intelligence*, Vol. 137, Article No. 109143, November, 2024.
https://doi.org/10.1016/j.engappai.2024.109143

[21] E. Birihanu, I. Lendák, Explainable Correlation-Based Anomaly Detection for Industrial Control Systems, *Frontiers in Artificial Intelligence*, Vol. 7, Article No. 1508821, February, 2025.
https://doi.org/10.3389/frai.2024.1508821

[22] E. Uflaz, S. I. Sezer, A. L. Tunçel, M. Aydin, E. Akyuz, O. Arslan, Quantifying Potential Cyber-Attack Risks in Maritime Transportation under Dempster–Shafer Theory FMECA and Rule-Based Bayesian Network Modelling, *Reliability Engineering & System Safety*, Vol. 243, Article No. 109825, March, 2024.
https://doi.org/10.1016/j.ress.2023.109825

[23] R. Al Sharif, S. Pokharel, Risk Analysis with the Dempster–Shafer Theory for Smart City Planning: The Case of Qatar, *Electronics*, Vol. 10, No. 24, Article No. 3080, December, 2021.
https://doi.org/10.3390/electronics10243080

[24] X. Chen, Y. Deng, Evidential Software Risk Assessment Model on Ordered Frame of Discernment, *Expert Systems with Applications*, Vol. 250, Article No. 123786, September, 2024.
https://doi.org/10.1016/j.eswa.2024.123786

[25] J. Yi, L. Guo, AHP-Based Network Security Situation Assessment for Industrial Internet of Things, *Electronics*, Vol. 12, No. 16, Article No. 3458, August, 2023.
https://doi.org/10.3390/electronics12163458

[26] S. Zhang, J. Jiang, T. Wang, Build a Network Security Situation Assessment Model Based on AHP, *Proceedings of the 2025 ACM International Conference on Computer Network Security and Software Engineering (CNSSE)*, Qingdao, China, 2025, pp. 29–32.
https://doi.org/10.1145/3732365.3732370

[27] J. H. Wong, K. Van Orden, B. R. Abrams, R. M. Iden, J. Viraldo, A Framework for Measuring Situation Awareness in Cyberspace Operations, *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 65, No. 1, pp. 358–362, September, 2021.
https://doi.org/10.1177/1071181321651059

[28] H. Ahmad, F. Ullah, R. Jafri, A Survey on Immersive Cyber Situational Awareness Systems, *Journal of Cybersecurity and Privacy*, Vol. 5, No. 2, Article No. 33, June, 2025.
https://doi.org/10.3390/jcp5020033

[29] E. Bellini, G. D'Aniello, F. Flammini, R. Gaeta, Situation

Awareness for Cyber Resilience: A Review, *International Journal of Critical Infrastructure Protection*, Vol. 49, Article No. 100755, July, 2025. https://doi.org/10.1016/j.ijcip.2025.100755

[30] F. Serini, Collective Cyber Situational Awareness in EU: A political project of difficult legal realisation?, *Computer Law & Security Review*, Vol. 55, Article No. 106055, November, 2024. https://doi.org/10.1016/j.clsr.2024.106055

[31] K. Renaud, J. Ophoff, A Cyber Situational Awareness Model to Predict the implementation of cyber security controls and precautions by SMEs, *Organizational Cybersecurity Journal: Practice, Process and People*, Vol. 1, No. 1, pp. 24–46, October, 2021. https://doi.org/10.1108/OCJ-03-2021-0004

[32] L. Leonard, W. Glodek, HACSAW: A Trusted Framework for Cyber Situational Awareness, *Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security (HoTSoS'18)*, Raleigh, North Carolina, USA, 2018, Article No. 12. https://doi.org/10.1145/3190619.3190641

[33] M. Wang, G. Song, Y. Yu, B. Zhang, The Current Research Status of AI-Based Network Security Situational Awareness, *Electronics*, Vol. 12, No. 10, Article No. 2309, May, 2023. https://doi.org/10.3390/electronics12102309

[34] P. Wang, N. Yuan, Y. Li, An Integrated Framework for Data Security Using Advanced Machine Learning Classification and Best Practices, *Informatica*, Vol. 49, No. 12, pp. 191–206, February, 2025. https://doi.org/10.31449/inf.v49i12.7838

[35] J. Fang, Y. Tang, M. Guo, Comprehensive Review of Cyber Threat Intelligence Sharing: Challenges and Methodologies, *Proceedings of the 4th Asia-Pacific Artificial Intelligence and Big Data Forum (AIBDF 2024)*, Ganzhou, China, 2024, pp. 455–461. https://doi.org/10.1145/3718491.3718565

[36] M. Badawy, N. H. Sherief, A. A. Abdel-Hamid, Legacy ICS Cybersecurity Assessment Using Hybrid Threat-Modeling—An Oil and Gas Sector Case Study, *Applied Sciences*, Vol. 14, No. 18, Article No. 8398, September, 2024. https://doi.org/10.3390/app14188398

[37] P. Li, L. Zhang, Application of Big Data Technology in Enterprise Information Security management, *Scientific Reports*, Vol. 15, Article No. 1022, January, 2025. https://doi.org/10.1038/s41598-025-85403-6

[38] Z. Zhang, G. Tang, B. Ren, H. Li, Y. Shen, TV-ADS: A Smarter Attack Detection Scheme Based on Traffic Visualization of Wireless Network Event Cell, *Journal of Internet Technology*, Vol. 25, No. 2, pp. 301–311, March, 2024. https://doi.org/10.53106/160792642024032502012

[39] G. Chen, Y.-Q. Zhao, RF-SVM Based Awareness Algorithm in Intelligent Network Security Situation Awareness System, *Proceedings of the 3rd Workshop on Advanced Research and Technology in Industry Applications (WARTIA 2017)*, Guilin, China, 2017, pp. 224–228. https://doi.org/10.2991/wartia-17.2017.45

[40] T. Zhu, J. Ying, T. Chen, C. Xiong, W. Cheng, Q. Yuan, A. Zheng, M. Lv, Y. Chen, Nip in the Bud: Forecasting and Interpreting Post-Exploitation Attacks in Real-Time Through Cyber Threat Intelligence Reports, *IEEE Transactions on Dependable and Secure Computing*, Vol. 22, No. 2, pp. 1431–1447, March–April, 2025. https://doi.org/10.1109/TDSC.2024.3444781

[41] W. Lei, H. Wen, W. Hou, X. Xu, New Security State Awareness Model for IoT Devices With Edge Intelligence, *IEEE Access*, Vol. 9, pp. 69756–69765, April, 2021. https://doi.org/10.1109/ACCESS.2021.3075220

[42] M. Abououf, R. Mizouni, S. Singh, H. Otrok, E. Damiani, Self-Supervised Online and Lightweight Anomaly and Event Detection for IoT Devices, *IEEE Internet of Things Journal*, Vol. 9, No. 24, pp. 25285–25299, December, 2022. https://doi.org/10.1109/JIOT.2022.3196049

[43] B. Qu, Z. Wang, B. Shen, D. Peng, D. Yue, Dynamic State Estimation for Multi-Machine Power Grids Under Randomly Occurring Cyber-Attacks: A Decentralized Framework, *IEEE Transactions on Sustainable Computing*, Vol. 10, No. 2, pp. 396–407, March–April, 2025. https://doi.org/10.1109/TSUSC.2024.3448225

[44] Z. Sun, A. M. H. Teixeira, S. Toor, GNN-IDS: Graph Neural Network Based Intrusion Detection System, *Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES 2024)*, Vienna, Austria, 2024, pp. 1–12. https://doi.org/10.1145/3664476.3664515

[45] A. Sayghe, Digital Twin-Driven Intrusion Detection for Industrial SCADA: A Cyber-Physical Case Study, *Sensors*, Vol. 25, No. 16, Article No. 4963, August, 2025. https://doi.org/10.3390/s25164963

[46] V. Govindarajan, J. H. Muzamal, Advanced Cloud Intrusion Detection Framework Using Graph Based Features Transformers and Contrastive Learning, *Scientific Reports*, Vol. 15, Article No. 20511, July, 2025. https://doi.org/10.1038/s41598-025-07956-w

Biographies

Fei Song works at PipeChina North Pipeline Company. His interests include industrial cybersecurity, digital control, and intelligent O&M. He has led projects on industrial internet security architecture and contributed to R&D of intelligent control systems.

Tieliang Sun works at China Oil & Gas Pipeline Network Corporation, focusing on oil and gas dispatching, pipeline operations, and ICS cybersecurity. He has participated in multiple research projects and brings hands-on experience across operations and industrial control network protection.

Shuai Jiang holds an MBA from China University of Petroleum (Beijing) and is an engineer at the Technical Support Center, PipeChina North Pipeline Company. His interests include ICS cybersecurity, automation, and pipeline operations, with experience in safety assurance and O&M.

Yuqin Wang works at PipeChina North Pipeline Company and holds a master's degree. Her research focuses on oil and gas pipeline integrity and industrial control network security, with extensive experience in related scientific and engineering projects.

Shiyin Zhu received the B.Eng. in 2022 from Chongqing University of Posts and Telecommunications. He is pursuing the M.Eng. in Electronic Information at Beijing Information Science and Technology University. His interests include affective computing and speech emotion recognition.