INPLASY

Cyber-Resilience of Decentralized Cyber-Physical Systems: A PRISMA-Guided Systematic Mapping Review, Taxonomy, and Evidence-Based Assessment Framework

INPLASY2026100097

doi: 10.37766/inplasy2026.10.0097

Received: 22 October 2026

Published: 22 October 2026

Sagindykov, K; Mukusheva, N; Tokseit, D; Urynbassarova, A; Tutkyshbayeva, S.

Corresponding author:
Kakim Sagindykov

sagindykov_km@enu.kz

Author Affiliation:
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

ADMINISTRATIVE INFORMATION

Support - No support.

Review Stage at time of this submission - Completed but not published.

Conflicts of interest - None declared.

INPLASY registration number: INPLASY2026100097

Amendments - This protocol was registered with the International Platform of Registered Systematic Review and Meta-Analysis Protocols (INPLASY) on 22 October 2026 and was last updated on 22 October 2026.

INTRODUCTION

Review question / Objective Review objective: To systematically map, classify, and critically assess existing approaches to cyber-resilience in decentralized cyber-physical systems (CPS), with particular emphasis on multi-vector cyberattacks, detection and mitigation mechanisms, resilient control and consensus methods, validation environments, and evidence quality.

P (Population/Problem): Decentralized and distributed cyber-physical systems, including multi-agent CPS, industrial CPS, energy systems, autonomous systems, and related networked infrastructures.
I (Intervention): Cyber-resilience mechanisms, including attack detection, anomaly detection, resilient consensus, secure and fault-tolerant control, mitigation, recovery, and adaptive protection techniques.
C (Comparator): Conventional centralized or non-resilient approaches, baseline methods, alternative protection mechanisms, or cases without protection, where such comparisons are reported.
O (Outcomes): Detection performance, false-positive/false-negative rates, response time, system safety, stability, service availability, resilience, recovery, robustness, communication performance, and quality of experimental validation.
S (Study design): Simulation studies, experimental testbeds, real-world case studies, digital-twin studies, and other empirical evaluations relevant to decentralized CPS cybersecurity.

The review further aims to identify research gaps and to develop an evidence-based assessment framework for comparing cyber-resilience approaches in decentralized CPS.

Rationale Decentralized cyber-physical systems are increasingly used in critical and distributed infrastructures, where cyberattacks can propagate across communication, control, sensing, and decision-making layers. Existing studies address individual threats and protection mechanisms, but

Sagindykov et al. INPLASY protocol 2026100097. doi:10.37766/inplasy2026.10.0097 Downloaded from https://inplasy.com/inplasy-2026-10-0097/

the evidence is fragmented across different CPS domains, attack models, resilience mechanisms, validation environments, and evaluation metrics. This fragmentation makes it difficult to compare approaches, assess the maturity of existing solutions, and identify methods that provide robust protection against multi-vector and coordinated attacks.

A systematic mapping review is therefore needed to organize the available evidence, classify attack types and cyber-resilience mechanisms, evaluate the quality and scope of experimental validation, and identify underexplored research areas. The review also aims to provide an evidence-based framework for comparing cyber-resilience approaches in decentralized CPS and to support the design of future research and experimental studies.

Condition being studied The condition studied is the cyber-resilience of decentralized cyber-physical systems (CPS) exposed to cyberattacks, including multi-vector, coordinated, and cross-layer attacks. The review focuses on how such attacks affect sensing, communication, control, coordination, decision-making, safety, stability, availability, and recovery in distributed CPS architectures.

The scope includes decentralized and multi-agent CPS, industrial control systems, smart energy and microgrid environments, autonomous and robotic systems, networked control systems, and other distributed infrastructures in which cyber and physical processes are tightly coupled.

The threats considered include, where reported in the literature, denial-of-service and distributed denial-of-service attacks, false data injection, spoofing, replay, man-in-the-middle attacks, communication jamming, malicious or compromised nodes, insider threats, and hybrid or combined attack scenarios.

The condition of interest is therefore not a medical condition, but the degradation or loss of cyber-resilience caused by adversarial interference in decentralized CPS. The review examines mechanisms intended to detect, tolerate, mitigate, recover from, or otherwise reduce the impact of such attacks while maintaining acceptable levels of system safety, stability, performance, and service availability.

METHODS

Search strategy The primary electronic database used for the quantitative identification of studies was Scopus. The search was conducted on 14 September 2026 and covered the publication period 2013–2026. The working protocol specified a three-block TITLE-ABS-KEY search combining terms related to: (1) cyber-physical systems, (2) decentralization/distributed operation, and (3) cyber-resilience and cybersecurity mechanisms.

The protocol-defined Scopus query was:

TITLE-ABS-KEY(("cyber-physical system*" OR "industrial cyber-physical system*" OR "networked control system*" OR "multi-agent system*" OR microgrid* OR "UAV swarm*" OR "robot swarm*" OR IIoT OR "industrial internet of things") AND (decentral* OR distribut* OR "multi-agent" OR "peer-to-peer" OR consensus OR federated) AND ("cyber resilien*" OR "resilient control" OR "resilient consensus" OR "attack-resilient" OR "secure control" OR "attack detection" OR "intrusion detection" OR "anomaly detection" OR "false data injection" OR replay OR "denial of service" OR Byzantine OR adversar* OR "self-healing" OR reconfiguration))

The executed Scopus export contained 366 records. However, the exported spreadsheet did not preserve the exact executed query text or the historical interface filters. Therefore, although the protocol-defined query is documented, its exact equivalence to the executed Scopus search yielding 366 records cannot be independently verified.

After publication-type filtering, 337 primary records proceeded to title and abstract screening. Publisher platforms, institutional repositories, and DOI records were subsequently used to retrieve full texts, accepted manuscripts, or authoritative extended records for eligibility assessment and quality appraisal. These supplementary retrieval sources were used only for document retrieval and did not contribute additional records to the primary PRISMA identification count.

Participant or population This review does not involve human participants or patients. The population of interest comprises decentralized, distributed, and multi-agent cyber-physical systems (CPS) studied in the cybersecurity and cyber-resilience literature. Eligible systems include industrial cyber-physical systems, networked control systems, microgrids and smart-energy environments, multi-agent and autonomous systems, UAV or robotic swarms, Industrial Internet of Things (IIoT) environments, and other

Sagindykov et al. INPLASY protocol 2026100097. doi:10.37766/inplasy2026.10.0097 Downloaded from https://inplasy.com/inplasy-2026-10-0097/

distributed CPS architectures in which sensing, communication, computation, and physical control are tightly coupled. Studies are included when the investigated system exhibits decentralized or distributed operation and is evaluated under a malicious cyber threat or adversarial condition relevant to cyber-resilience.

Intervention The interventions of interest are cybersecurity and cyber-resilience mechanisms designed to detect, tolerate, mitigate, respond to, or recover from malicious cyberattacks in decentralized cyber-physical systems. These include attack and anomaly detection methods, intrusion detection, false-data-injection detection, resilient control, resilient consensus, secure distributed control, fault- and attack-tolerant coordination, adaptive or reconfigurable defense mechanisms, self-healing approaches, and recovery strategies. Studies evaluating combinations of detection, mitigation, control, communication protection, and recovery mechanisms are also included. The review assesses how these interventions contribute to maintaining or restoring system safety, stability, availability, coordination, and service performance under adversarial conditions.

Comparator No single mandatory comparator was required for study inclusion. Where reported, cyber-resilience interventions were compared with conventional centralized or non-resilient approaches, baseline control or detection methods, alternative protection mechanisms, nominal operation without attack, or operation under attack without protection. Studies without an explicit comparator were also eligible when they provided sufficient technical evidence to characterize the threat model, resilience mechanism, and validation procedure. Comparative evidence was extracted and synthesized where available, but the absence of a formal control group was not, by itself, an exclusion criterion.

Study designs to be included Simulation studies, experimental testbed studies, real-world or field case studies, digital-twin studies, and other empirical evaluations of decentralized or distributed cyber-physical systems under malicious cyber threats. Studies using analytical or control-theoretic models are also eligible when they include a clear threat model, resilience mechanism, and technical validation. Purely conceptual papers without sufficient technical evidence are excluded.

Eligibility criteria Eligible records had to be primary studies addressing a cyber-physical or networked-control application with decentralized, distributed, or multi-agent operation; consider a malicious or cybersecurity-relevant threat; propose or evaluate a cyber-resilience or security mechanism; and provide sufficient technical evidence to identify the threat model, response mechanism, and validation basis. Purely centralized approaches, accidental-fault-only studies, non-primary publication types, studies without a qualifying malicious cyber threat, studies without a relevant resilience/security mechanism, records outside the CPS/application scope, and records with insufficient technical evidence were excluded. The review covered publications from 2013 to 2026.

Information sources The primary electronic information source was Scopus, which provided the quantitative identification stream for the review. The executed Scopus export was dated 14 September 2026 and covered publications from 2013 to 2026.

After the initial database search, publisher websites, institutional repositories, and DOI-based records were used to retrieve full texts, accepted manuscripts, or authoritative extended records for eligibility assessment and quality appraisal when necessary. These supplementary sources were used for document retrieval and verification only and did not contribute additional records to the primary PRISMA identification count.

No separate systematic search of trial registries, author-contact sources, or grey-literature databases was conducted. No additional electronic database was included in the final quantitative identification stream. The review therefore reports Scopus as the sole primary database and explicitly distinguishes supplementary full-text retrieval sources from sources used for study identification.

Main outcome(s) The main outcomes were the types and reported performance of cyber-resilience mechanisms in decentralized cyber-physical systems under malicious attack. Outcomes were grouped into five primary categories: (1) consensus, coordination, or tracking performance; (2) voltage, frequency, or power regulation; (3) attack detection, isolation, or localization; (4) system stability or resilient operation; and (5) safety or constraint preservation.

Outcomes were extracted using the measures and evaluation horizons reported by each primary

Sagindykov et al. INPLASY protocol 2026100097. doi:10.37766/inplasy2026.10.0097 Downloaded from https://inplasy.com/inplasy-2026-10-0097/

study. These included, where available, convergence or tracking error, regulation performance, detection accuracy and related detection metrics, stability indicators, safety or constraint satisfaction, communication/service availability, and recovery-related measures.

Because the included studies used heterogeneous CPS domains, attack models, experimental settings, metrics, and observation periods, no common follow-up time or pooled intervention effect measure was defined. The review therefore used descriptive categorical synthesis, reporting the number and proportion of Core studies in each outcome category and comparing the strength and type of validation evidence.

Additional outcome(s) Additional outcomes included the distribution of studies across CPS application domains, attack families, resilience mechanisms, architecture profiles, and validation approaches. The review also assessed the prevalence of explicit multi-vector or hybrid attack scenarios, the maturity of experimental validation, and the methodological quality of the included studies.

These outcomes were summarized using counts and proportions of the 72 Core studies. Validation strength was categorized as simulation/numerical study, experimental or strong validation, hardware-in-the-loop/real-time testbed, physical/laboratory experiment, or co-simulation/cyber-physical testbed. Methodological quality was assessed using a six-dimension 0–2 scoring framework covering threat-model clarity, decentralization/topology assumptions, reproducibility, validation strength, adequacy of baselines and metrics, and transparency of limitations or implementation details.

The synthesis was descriptive and comparative; no pooled effect estimate was calculated because the included studies were heterogeneous in system domains, attack models, interventions, metrics, and validation settings.

Data management Records and extracted data were managed electronically using the original Scopus export together with structured working spreadsheets maintained by the authors. The Scopus export served as the master identification set. Screening decisions, eligibility status, exclusion reasons, quality-appraisal scores, and evidence-extraction variables were recorded in the working files throughout the review.

A structured extraction workbook was used to record, for each included study, bibliographic metadata, CPS domain, primary and secondary attack categories, architecture profile, resilience or defense mechanism, validation type, reported outcome category, and methodological quality score. The 79 eligible studies were assessed using the predefined six-dimension quality-appraisal framework, and 72 studies meeting the quality threshold were retained for the Core synthesis.

During manuscript development, the electronic screening records, eligibility decisions, and study classifications were independently checked by co-authors. Identified discrepancies and suggested corrections were discussed and incorporated before final evidence synthesis. This verification was an internal quality-control procedure rather than a prospectively designed blinded duplicate-screening process; therefore, no formal inter-rater agreement statistic was calculated.

Publisher-copyrighted full texts were used only for review and verification and were not redistributed.

Quality assessment / Risk of bias analysis Methodological quality was assessed for all 79 eligible primary studies using a six-dimension scoring rubric. Each dimension was scored from 0 to 2 points: Q1, clarity of the threat/adversary model; Q2, clarity of decentralization and topology assumptions; Q3, reproducibility of the algorithm or architecture; Q4, strength of validation evidence; Q5, adequacy of baselines, metrics, and repeated or statistical analysis; and Q6, transparency of limitations, implementation details, or code/data availability. The maximum total score was 12.

Studies scoring at least 7/12 were retained for the Core comparative synthesis, while lower-scoring studies were retained only as contextual evidence. This procedure resulted in 72 Core studies and 7 contextual studies.

The quality appraisal was used to characterize methodological strength and evidence maturity rather than as a validated formal study-level risk-of-bias instrument. No separate validated risk-of-bias tool, such as those developed for clinical intervention studies, was applied because the included evidence consisted of heterogeneous engineering, control, detection, simulation, and experimental studies. No formal certainty-of-evidence framework or publication-bias analysis was performed.

Strategy of data synthesis Data synthesis was conducted using a structured descriptive and

Sagindykov et al. INPLASY protocol 2026100097. doi:10.37766/inplasy2026.10.0097 Downloaded from https://inplasy.com/inplasy-2026-10-0097/

comparative mapping approach. Because the included studies were heterogeneous in CPS domain, attack model, architecture, intervention type, validation environment, outcome metrics, and evaluation horizon, no quantitative meta-analysis or pooled effect estimate was performed.

For each Core study, extracted data were coded using predefined categories covering CPS domain, primary and secondary attack types, architecture profile, resilience or defense mechanism, validation approach, reported outcome category, and methodological quality score.

Mutually exclusive primary categories were used to summarize CPS domains, primary attack families, validation approaches, and main reported outcomes. Frequencies and proportions were calculated across the 72 Core studies. Defense mechanisms were analysed using multi-label coding because a single study could combine several functions, such as detection, observer-based compensation, resilient consensus, isolation, reconfiguration, and recovery.

Evidence maturity was evaluated descriptively by comparing simulation-only studies with hardware-in-the-loop, real-time, laboratory, co-simulation, and other experimentally validated studies. The synthesis was then interpreted according to the review research questions to identify dominant research themes, underrepresented attack scenarios, methodological limitations, validation gaps, and priorities for future research.

The final synthesis was used to support the proposed taxonomy and evidence-based assessment framework rather than to estimate a single common intervention effect.

Subgroup analysis No formal statistical subgroup analysis was performed because no pooled effect estimate was calculated. Heterogeneity was explored descriptively by grouping and comparing studies according to CPS application domain, primary attack family, resilience mechanism, architecture profile, validation type, and reported outcome category.

Descriptive subgroup comparisons were used to identify differences in the distribution and maturity of evidence across, for example, power systems and microgrids, autonomous or multi-agent systems, industrial CPS, and other decentralized CPS domains; single-vector versus multi-vector or hybrid attacks; and simulation-only versus stronger experimental, real-time, hardware-in-the-loop, laboratory, or co-simulation validation.

These comparisons were based on study counts, proportions, and qualitative interpretation rather than statistical tests of subgroup effects.

Sensitivity analysis No formal statistical sensitivity analysis was performed because the review did not conduct a meta-analysis or estimate a pooled intervention effect. The evidence synthesis was descriptive and categorical, and the included studies were highly heterogeneous in CPS domain, attack model, architecture, resilience mechanism, validation design, outcome metric, and evaluation horizon.

Robustness of the synthesis was addressed qualitatively through structured comparison of study categories and through the methodological quality appraisal. The 79 eligible studies were scored using the six-dimension Q1–Q6 framework, and the primary Core synthesis was restricted to the 72 studies meeting the predefined quality threshold of at least 7/12. The remaining seven studies were retained as contextual evidence rather than combined with the Core comparative synthesis.

No sensitivity analysis based on alternative pooled models, effect-size assumptions, or statistical heterogeneity was applicable. This limitation is reported explicitly.

Language restriction No prespecified language restriction; however, the historical Scopus export did not preserve interface language filters, so exact search-level language limits cannot be independently verified.

Country(ies) involved Republic of Republic of Kazakhstan.

Other relevant information This registration is retrospective. The systematic mapping review had already been completed and the manuscript submitted to Future Internet before registration in INPLASY. Registration was undertaken following an editorial request to provide a publicly accessible review protocol and registration identifier. A working review protocol had been documented internally during the review process but was not prospectively registered or publicly archived. Therefore, this INPLASY record should not be interpreted as prospective preregistration. It documents, as accurately as possible, the methodology actually used in the completed review. No substantive changes to the study results or evidence synthesis were introduced for the purpose of retrospective registration. The review followed a descriptive systematic mapping

Sagindykov et al. INPLASY protocol 2026100097. doi:10.37766/inplasy2026.10.0097 Downloaded from https://inplasy.com/inplasy-2026-10-0097/

approach; because of substantial heterogeneity across CPS domains, attack models, interventions, validation settings, and outcome measures, no meta-analysis or pooled effect estimate was performed.

Keywords cyber-physical systems; cyber-resilience; decentralized systems; systematic mapping; PRISMA; resilient control; multi-agent systems; false data injection; denial-of-service; resilience assessment.

Dissemination plans The findings of this review are being prepared for dissemination through peer-reviewed publication in the journal Future Internet. The review protocol is being retrospectively registered in INPLASY to provide a public and citable record of the methods used. After journal publication, the authors intend to disseminate the results through institutional and academic channels, including conference presentations, research seminars, and scholarly communication with researchers working on cyber-physical systems and cybersecurity. Where permitted, supplementary materials describing the search strategy, study selection, quality appraisal, and evidence mapping will be made available to support transparency and reproducibility. The authors may also update the review in the future if substantial new evidence becomes available.

Contributions of each author

Author 1 - Kakim Sagindykov - Contributed to conceptualization, methodology, formal analysis, supervision, project administration, and writing—review and editing.
Email: sagindykov_km@enu.kz
Author 2 - Nazym Mukusheva - Contributed to conceptualization, methodology, formal analysis, investigation, data curation, visualization, writing—original draft, and writing—review and editing.
Email: nazymmg@gmail.com
Author 3 - Dinara Tokseit - Contributed to methodology, investigation, validation, and writing—review and editing.
Email: tokseit1990@gmail.com
Author 4 - Altyn Urynbassarova - Contributed to investigation, data curation, validation, and writing—review and editing.
Email: urynbassarova_azh@enu.kz
Author 5 - Shyryn Tutkyshbayeva - Contributed to investigation, validation, visualization, and writing—review and editing.
Email: sh.tutkyshbayeva@astanait.edu.kz

Sagindykov et al. INPLASY protocol 2026100097. doi:10.37766/inplasy2026.10.0097 Downloaded from https://inplasy.com/inplasy-2026-10-0097/