iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83810

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

A Deception Readiness Index for ICS and OT Cybersecurity Programs

Daniel Ward
Department of Computer Science, Southern New Hampshire University, United States

Abstract: ***Deception technology can improve industrial control systems and operational technology cybersecurity by creating high-confidence signals when adversaries interact with assets, credentials, or services that legitimate users should not touch. However, organizations often lack a practical method for determining whether they are ready to deploy deception safely, govern it consistently, and use its alerts effectively. This paper develops a Deception Readiness Index (DRI) for ICS and OT cybersecurity programs. The study uses design science and qualitative document analysis of public cybersecurity standards, OT security guidance, workforce frameworks, and prior deception-technology research. The resulting artifact scores readiness across governance, architecture, monitoring, workforce, and operational safety domains. The index is then applied to three synthetic critical-infrastructure profiles to demonstrate how readiness gaps can be identified before deployment. The results show that deception readiness depends less on tool availability alone and more on the alignment of ownership, safe placement, alert routing, staff capability, and operational approval. The DRI provides a repeatable planning method for organizations seeking to move from initial interest in deception technology to a controlled, auditable deployment.***

Keywords: ***critical infrastructure cybersecurity, cyber deception, deception readiness index, industrial control systems, operational technology, security governance***

I. INTRODUCTION

Industrial control systems (ICS) and operational technology (OT) environments support physical processes in water, manufacturing, energy, transportation, building automation, and other critical infrastructure sectors. Cybersecurity decisions in these environments must account for uptime, safety, deterministic communications, equipment lifecycle constraints, regulatory obligations, and the operational authority of engineering personnel. As a result, a security control that is ordinary in enterprise information technology may be inappropriate in OT if it introduces latency, uncontrolled traffic, operator confusion, or unapproved response actions.

Deception technology is attractive in this setting because it can provide early warning without requiring direct manipulation of production control logic. Decoys, honey credentials, false services, canary files, simulated historian tags, and monitored engineering artifacts can generate high-confidence signals when touched by an unauthorized user. Prior doctoral research on deception technology adoption in manufacturing and critical infrastructure found that compatibility concerns, limited resources, inadequate professional knowledge, infrastructure constraints, and performance concerns affected adoption [1]. A subsequent sector-specific paper demonstrated how deception can be structured for water and wastewater OT environments as an additive, nonintrusive architecture [2]. The remaining problem is readiness. Even when leaders accept the value of deception technology, they may not know whether the organization is prepared to deploy it safely. A tool can be purchased before ownership, alert routing, operator awareness, change approval, or evidence retention are mature enough to support it. That creates a risk that deception becomes an isolated experiment rather than an auditable security capability. The purpose of this paper is to develop a Deception Readiness Index (DRI) to help ICS and OT organizations assess their preparedness to implement deception technology in a controlled manner.

The contribution is a practical scoring artifact. The DRI translates prior architecture, control-mapping, and workforce-readiness work into a measurable readiness model. It is intended for security leaders, OT engineers, incident response teams, compliance personnel, and critical infrastructure managers who need a structured way to evaluate readiness before deploying decoys in safety-sensitive environments.

II. BACKGROUND

A. Deception Technology in OT Security

Deception technology uses controlled false assets or signals to expose activity that legitimate users should not perform. In enterprise environments, this may include honey credentials, decoy shares, fake systems, or canary documents. In ICS and OT environments, the same concept must be adapted to operating constraints. Decoys should observe, alert, and enrich responses; they should not create a pathway for operating pumps, valves, robots, boilers, drives, chemical dosing systems, or other live process equipment.

Recent research on honeypots and honeynets for IoT, IIoT, and cyber-physical systems shows that deception can complement other controls by collecting data on attacker behavior and enriching detection context [10]. Higher-fidelity industrial honeynets, including physics-aware designs, also demonstrate how deception can emulate operational processes for research and threat intelligence [11].

For critical infrastructure operators, however, readiness is not the same as technical capability. A high-fidelity decoy may be useful in a laboratory but inappropriate for a small utility or manufacturing site that lacks change-control discipline, alert triage, or OT engineering support. In real environments, readiness must include governance, architecture, monitoring, workforce, and safety boundaries.

B. Standards and Readiness Context

The DRI is grounded in current public guidance. The NIST Cybersecurity Framework 2.0 organizes cybersecurity outcomes around govern, identify, protect, detect, respond, and recover functions [3]. NIST SP 800-82 Revision 3 describes OT security for systems that interact with physical processes and emphasizes performance, reliability, and safety requirements [4]. NIST SP 800-53 Revision 5 provides a flexible catalog of controls for organizational risk management [5]. IEC 62443-2-1:2024 specifies asset-owner security program requirements for industrial automation and control systems [6]. CISA Cross-Sector Cybersecurity Performance Goals provide baseline practices that critical infrastructure organizations can use to prioritize high-impact security outcomes [7]. The NICE Framework describes cybersecurity work through tasks, knowledge, and skill statements that support workforce planning [8]. MITRE ATT&CK for ICS provides a structured adversary-technique model that can help connect deception alerts to recognizable attacker behavior [9].

Together, these sources show that deception readiness is a multidimensional problem. It is not enough to ask whether an organization owns a deception product. The organization must also understand its OT assets, define safe placement zones, approve monitoring boundaries, route alerts to the right people, train staff to interpret decoy events, and preserve evidence in a response workflow. The DRI was designed to measure those conditions.

III. MATERIALS AND METHODS

This paper uses design science supported by qualitative document analysis. The research objective is to produce and demonstrate a planning artifact rather than to evaluate a commercial product or collect new human-subjects data. Design science is appropriate because the result is a structured model intended to solve a practical organizational problem: determining the readiness of deception deployment in ICS and OT cybersecurity programs.

A. Source Corpus

The document corpus included public standards and guidance that are widely used in critical infrastructure cybersecurity: NIST CSF 2.0, NIST SP 800-82 Revision 3, NIST SP 800-53 Revision 5, IEC 62443-2-1:2024, CISA Cross-Sector Cybersecurity Performance Goals, the NICE Workforce Framework, and MITRE ATT&CK for ICS. Prior dissertation findings and published sector-specific deception architecture work were used to define the adoption and operational context [1], [2]. Recent deception and honeynet literature were used to confirm that fidelity, alert value, monitoring, and evidence of attacker interaction remain important design concerns [10], [11].

B. Coding and Model Construction

The document-analysis procedure followed five steps. First, statements related to governance, ownership, inventory, monitoring, response, training, and operational safety were extracted from the source corpus. Second, those statements were grouped into readiness domains. Third, each domain was converted to a 0-4 scoring scale. Fourth, the scoring scale was applied to three synthetic critical-infrastructure profiles. Fifth, the results were interpreted as readiness categories and priority actions. The synthetic profiles were not intended to represent specific organizations. They were constructed to demonstrate how organizations of varying sizes and maturity levels can use the index.

C. Evaluation Criteria

The DRI artifact was evaluated conceptually against four criteria. First, traceability means each readiness domain must connect to public guidance or prior deception research. Second, usability means each score must be understandable by both OT engineering and cybersecurity personnel. Third, safety alignment means the model must discourage uncontrolled deployment in production environments. Fourth, actionability means the score must lead to practical next steps rather than a generic maturity label.

IV. DECEPTION READINESS INDEX

The Deception Readiness Index evaluates readiness across five domains: governance, architecture, monitoring, workforce, and operational safety. Each domain is scored from 0 to 4, where 0 indicates the capability is absent and 4 means it is optimized and continuously improved. The maximum raw score is 20.

TABLE I
DRI DOMAIN AND INDICATOR STRUCTURE

Domain	Primary Question	Representative Indicators
Governance readiness	Is deception owned, approved, and auditable?	Policy ownership, risk acceptance, change approval, scope definition, evidence-retention expectations
Architecture readiness	Can decoys be placed safely and realistically?	Asset inventory, segmentation, Purdue-level awareness, remote-access mapping, approved no-touch zones
Monitoring readiness	Will deception events reach the right response path?	SIEM/SOC routing, alert enrichment, playbook linkage, escalation contacts, log retention
Workforce readiness	Can staff interpret and act on deception events?	Role-based training, OT/security coordination, engineering awareness, tabletop exercises
Operational safety readiness	Can deception operate without disrupting physical processes?	Noninterference rules, rollback planning, maintenance windows, operator notification, live-control isolation

The scoring scale is intentionally simple. The purpose is not to replace a detailed risk assessment or compliance audit. The purpose is to create a defensible go/no-go planning measure for deception deployment. The scoring logic is shown in Table II.

TABLE II
DECEPTION READINESS SCORING SCALE

Score	Label	Description
0	Absent	No defined capability, owner, process, or evidence exists for the domain.
1	Ad hoc	Some activity exists, but it is informal, undocumented, inconsistent, or dependent on individual effort.
2	Defined	The domain has documented expectations, but integration with OT operations or response workflows is incomplete.
3	Integrated	The domain is connected to OT architecture, monitoring, response, and governance processes.
4	Optimized	The domain is measured, exercised, reviewed, improved, and updated as the environment changes.

$$DRI = ((G + A + M + W + S) / 20) \times 100$$

In the formula, G represents governance readiness, A represents architecture readiness, M represents monitoring readiness, W represents workforce readiness, and S represents operational safety readiness. The resulting percentage is interpreted using the readiness categories in Table III.

TABLE III
DRI SCORE INTERPRETATION

DRI Range	Readiness Category	Interpretation
0-24	Not ready	Do not deploy deception beyond isolated planning. Establish ownership, inventory, safety rules, and monitoring first.
25-49	Foundational	Limited low-risk lures may be considered only after governance and response ownership are documented.
50-74	Pilot ready	A controlled pilot can be deployed in approved zones with playbooks and operator awareness.
75-89	Deployment ready	Deception can be integrated into security operations with routine review and evidence retention.
90-100	Optimized	Deception is governed, measured, refreshed, exercised, and continuously improved.

V. RESULTS AND FINDINGS

The DRI was applied to three synthetic profiles to demonstrate how the scoring model identifies readiness gaps. The profiles represent common critical-infrastructure situations: a small municipal utility, a mid-sized manufacturer, and a large critical infrastructure operator. The scoring values are illustrative and based on the assumptions described in each profile, rather than on data from actual organizations.

A. Synthetic Profile Descriptions

Profile 1 is a small municipal utility with limited IT support, contractor-managed OT systems, basic backups, informal incident-response procedures, and limited monitoring. The utility has strong operational knowledge but little cybersecurity specialization. Profile 2 is a mid-sized manufacturer with segmented production networks, partial asset inventory, an enterprise security operations center, and limited OT-specific playbooks. Profile 3 is a large, critical infrastructure operator with formal governance, dedicated OT engineering, segmented architecture, incident response processes, and routine security exercises.

TABLE IV
SYNTHETIC PROFILE SCORING RESULTS

Profile	G	A	M	W	S	DRI	Category
Small municipal utility	1	1	1	1	2	30%	Foundational
Mid-sized manufacturer	2	2	2	2	2	50%	Pilot ready
Large critical infrastructure operator	3	3	3	3	3	75%	Deployment ready

B. Result 1: Tool Ownership Is Not Enough

The small municipal utility scored 30 percent. This result shows that deception may be attractive because it can produce high-confidence early warning, but the organization is not ready for SCADA-adjacent decoys. Its most practical first step is not technology acquisition. It should establish deception ownership, identify zones where lures are permitted, document incident contacts, and begin with low-risk honey credentials or canary files outside live control segments.

C. Result 2: Pilot Readiness Requires Integration

The mid-sized manufacturer scored 50 percent. This profile has enough structure to pilot deception, but only if the pilot is narrow. The most suitable initial deployment would involve engineering-workstation-adjacent files, decoy historian endpoints, or monitored remote-access artifacts with no production privileges. The organization should not proceed to controller-adjacent emulation until monitoring and OT response ownership are better integrated.

D. Result 3: Safety Readiness Limits Deployment Scope

The large critical infrastructure operator scored 75 percent. This profile is deployment-ready because governance, architecture, monitoring, workforce, and safety practices are integrated. Even so, the DRI does not recommend unrestricted deployment. It recommends controlled expansion, recurring exercises, quarterly review of decoy realism, mapping to ATT&CK for ICS techniques, and evidence retention for incident response and audit purposes.

TABLE V
PRIORITY ACTIONS BY READINESS CATEGORY

Category	Priority Actions
Not ready	Create ownership, inventory critical OT assets, define prohibited zones, and establish response contacts.
Foundational	Deploy only low-risk enterprise or DMZ lures; document alert ownership and evidence retention.
Pilot ready	Run a controlled pilot, connect alerts to playbooks, notify OT owners, and evaluate operational burden.
Deployment ready	Expand across approved OT zones, integrate with SOC workflows, and perform recurring tabletop validation.
Optimized	Refresh deception content, evaluate alert quality, test evasion resistance, and report metrics to leadership.

VI. DISCUSSION

The DRI reframes deception technology from a product decision into a readiness decision. This distinction matters because deception produces value only when its signals are understood, trusted, and acted upon. A decoy alert that no one owns, cannot validate, or cannot safely respond to has limited value. Conversely, even a simple honeytoken can be valuable when ownership, alerting, and response are clear.

The five-domain structure also reflects the operating reality of ICS and OT programs. Governance readiness ensures that deception is approved and auditable. Architecture readiness ensures that decoys are placed where they are plausible but safe. Monitoring readiness ensures that events reach the security operations or incident-response workflow. Workforce readiness ensures that OT and security personnel understand how to interpret deception signals. Operational safety readiness ensures that the deployment does not interfere with live processes.

The synthetic results also show why a single maturity score can be misleading. An organization may have strong monitoring but weak OT safety planning. Another may have experienced engineers, but limited incident-response documentation. The DRI helps identify which domain constrains deployment. In practice, the lowest domain score may be more important than the average because a serious weakness in safety, monitoring, or governance can undermine the entire deployment.

This model is intentionally additive to existing cybersecurity programs. It does not replace asset inventory, segmentation, vulnerability management, passive monitoring, endpoint protection, incident response, or backup and recovery. Instead, it helps determine whether deception can be added to that stack in a way that produces useful evidence about adversary behavior. When other tools miss or under-prioritize early activity, deception can provide clarity by showing that someone interacted with an object that should not be used by normal operators, vendors, or processes.

VII. IMPLEMENTATION GUIDANCE

Organizations can implement the DRI as a brief planning exercise before procurement, a pilot deployment, or an architecture review. The recommended process has five steps. First, identify the OT owner, security owner, and response owner for the deception initiative. Second, score each readiness domain using available evidence such as network diagrams, asset inventories, policy documents, playbooks, training records, and monitoring tickets. Third, document the lowest-scoring domains and define corrective actions. Fourth, select deception patterns that match the readiness category. Fifth, repeat the assessment after the pilot or exercise.

For low-readiness organizations, the safest initial patterns are honey credentials with no production privileges, canary documents, fake vendor folders, and decoy network diagrams placed in monitored enterprise or OT demilitarized-zone locations. For pilot-ready organizations, historian lures, engineering-project canaries, and read-only protocol decoys may be appropriate if operators approve the scope. For deployment-ready organizations, deception can be expanded into multiple OT zones, but only with evidence retention, alert-quality metrics, and periodic review.

The DRI can also support reporting. Leadership often asks whether deception technology is worth deploying. A readiness score helps reframe the answer. If readiness is low, the recommendation may be to invest first in governance, monitoring, or workforce training. If readiness is moderate, the recommendation may be a limited pilot. If readiness is high, the recommendation may be governed deployment with metrics such as decoy interaction rate, mean time to validate, alert enrichment completeness, and response-playbook activation rate.

VIII. LIMITATIONS AND FUTURE WORK

This paper develops and demonstrates a readiness artifact using public documents and synthetic profiles. It does not validate the DRI through live deployment, practitioner survey, expert panel review, cyber-range testing, or production telemetry. The profile scores should therefore be read as a demonstration of the method, not as empirical findings about all utilities, manufacturers, or critical-infrastructure operators.

A second limitation is that the index uses equal weighting across all five domains. Equal weighting improves usability, but some organizations may decide that safety or monitoring readiness should carry more weight than governance or workforce readiness. Future work should test weighted versions of the index with OT security practitioners or through tabletop exercises.

A third limitation is sector variation. Water utilities, manufacturers, energy operators, transportation systems, and healthcare facilities have different operating models and risk tolerances. Future research should produce sector-specific DRI profiles and compare readiness thresholds across industries. Additional work should also evaluate whether DRI scores correlate with measurable deployment outcomes such as alert quality, detection latency, operational burden, and response effectiveness.

IX. CONCLUSION

Deception technology can provide ICS and OT defenders with high-confidence early-warning signals and clearer evidence of attacker behavior. Its value, however, depends on more than the existence of decoys. Organizations must be ready to govern, place, monitor, interpret, and safely operate deception capabilities. This paper developed a Deception Readiness Index to help organizations assess their readiness before deployment.

The DRI scores governance, architecture, monitoring, workforce, and operational safety readiness on a 0 to 4 scale and converts the result into a percentage-based readiness category. Applying the index to three synthetic profiles demonstrated that the model can distinguish between foundational, pilot, and deployment readiness. The index gives critical-infrastructure organizations a practical way to decide whether to defer deception, pilot it narrowly, or integrate it into a mature OT cybersecurity program.

The broader contribution is a shift from advocating deception technology to operationalizing it responsibly. In safety-sensitive environments, deception should not be treated as a standalone tool or experiment. It should be deployed as an additive, governed, evidence-producing capability that improves clarity when adversaries interact with assets they should never touch.

X. ACKNOWLEDGMENT

The author acknowledges the dissertation research and subsequent extension papers that informed this work, as well as the public cybersecurity guidance issued by NIST, CISA, MITRE, IEC, and the broader ICS/OT security community.

REFERENCES

[1] D. Ward, Enhancing Security: A Comprehensive Study on Deception Technology Integration in Manufacturing and Critical Infrastructure, Ph.D. dissertation, University of the Cumberlands, Williamsburg, KY, USA, 2025. Available: https://www.proquest.com/dissertations-theses/enhancing-security-comprehensive-study-on/docview/3222626522/se-2

[2] D. Ward, "Deception Architecture for Water and Wastewater Operational Technology Environments," International Journal of Engineering Research & Technology, vol. 15, no. 06, Jun. 2026, doi: 10.5281/zenodo.20745399. Available: https://www.ijert.org/deception-architecture-for-water-and-wastewater-operational-technology-environments-ijertv15is060682

[3] C. Pascoe, S. Quinn, and K. Scarfone, The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Paper 29, National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.CSWP.29. Available: https://doi.org/10.6028/NIST.CSWP.29

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

[5] Joint Task Force, Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5, National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-53r5. Available: https://doi.org/10.6028/NIST.SP.800-53r5

[6] International Electrotechnical Commission, IEC 62443-2-1:2024, Security for Industrial Automation and Control Systems - Part 2-1: Security Program Requirements for IACS Asset Owners, 2024. Available: https://webstore.iec.ch/en/publication/62883

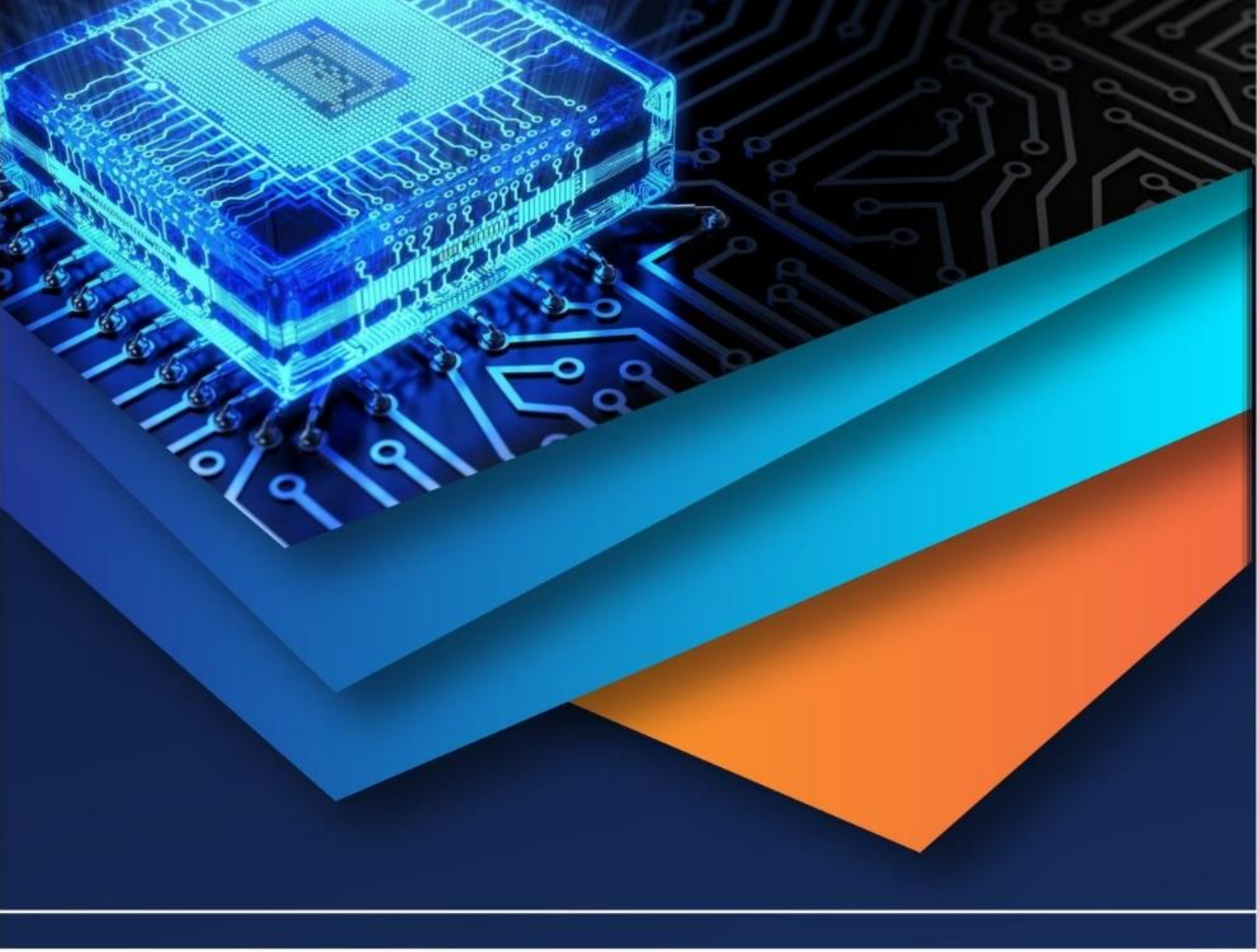
[7] Cybersecurity and Infrastructure Security Agency, Cross-Sector Cybersecurity Performance Goals, Washington, DC, USA, 2026. Available: https://www.cisa.gov/cybersecurity-performance-goals

[8] R. Petersen, D. Santos, K. Wetzel, M. Smith, and G. Witte, Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181 Revision 1, National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-181r1. Available: https://doi.org/10.6028/NIST.SP.800-181r1

[9] MITRE ATT&CK, "ATT&CK for ICS Matrix," version 19.1, MITRE, 2026. Available: https://attack.mitre.org/matrices/ics/ and https://attack.mitre.org/resources/versions/

[10] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for Internet of Things, Industrial Internet of Things, and cyber-physical systems," IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2351-2383, 2021, doi: 10.1109/COMST.2021.3106669. Available: https://doi.org/10.1109/COMST.2021.3106669

[11] M. Lucchese, F. Lupia, M. Merro, F. Paci, N. Zannone, and A. Furfaro, "HoneyICS: A high-interaction physics-aware honeynet for industrial control systems," in Proceedings of the 18th International Conference on Availability, Reliability and Security, 2023, doi: 10.1145/3600160.3604984. Available: https://doi.org/10.1145/3600160.3604984



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY