International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 06 | Jun 2026 www.irjet.net p-ISSN: 2395-0072

A Workforce Readiness Model for Deception Technology in ICS and OT Cybersecurity Programs

Daniel Ward

Associate Professor, Department of Computer Science, Southern New Hampshire University, United States

---

Abstract - *Critical infrastructure organizations increasingly need personnel who can operate deception technology safely in industrial control systems and operational technology environments. Honeypots, honeytokens, decoy services, simulated engineering files, and false credentials can generate high confidence indicators when adversaries interact with assets that legitimate operators should not use. However, prior research on deception technology adoption in manufacturing and critical infrastructure found that implementation is constrained by compatibility concerns, limited resources, inadequate professional knowledge, infrastructure constraints, and limited practical awareness. This paper updates a prior policy framework into an engineering-oriented workforce readiness model suitable for practical program adoption. Using design science and qualitative document analysis, the paper synthesizes public cybersecurity standards, operational technology guidance, workforce frameworks, incident response guidance, and deception technology literature. The result is the Deception Workforce Readiness Model, which defines five domains: governance literacy, OT context awareness, deception design, cyber intelligence translation, and response integration. The model provides a staged implementation sequence and evidence artifacts that organizations can use to convert deception technology from a tool concept into a governed workforce capability. The paper contributes a non-human subjects framework for improving readiness before deception technology is piloted in safety-sensitive environments.*

Key Words: critical infrastructure, cyber deception, honeypots, industrial control systems, operational technology, workforce readiness

1. INTRODUCTION

Industrial control systems (ICS) and operational technology (OT) environments support physical processes in manufacturing, water and wastewater, energy, transportation, building automation, and other critical infrastructure sectors. Cybersecurity decisions in these environments differ from ordinary enterprise information technology decisions because they must account for uptime, deterministic communications, safety, equipment lifecycle constraints, change control, and the division of responsibility between engineering and information security teams. For that reason, a security capability that appears straightforward in enterprise networks can become difficult to implement in an OT environment if it introduces unapproved scanning, unstable traffic, ambiguous alerts, or response actions that are not coordinated with operations.

Deception technology offers a useful detection and intelligence capability for this environment. Rather than relying only on perimeter controls or signature-based alerts, deception technology uses decoy hosts, fake credentials, monitored files, simulated services, and false operational artifacts that legitimate personnel should not normally touch. Interaction with a decoy can therefore produce a high confidence signal of reconnaissance, credential misuse, lateral movement, unauthorized access, or attacker staging. Recent deception research emphasizes the value of honeypots and deception strategies for threat detection and adversary observation [6]. In OT, however, the value of a deception signal depends on whether the workforce is prepared to govern, interpret, and act on it safely.

Prior dissertation research on deception technology integration in manufacturing and critical infrastructure found that adoption was constrained by compatibility concerns, limited resources, inadequate professional knowledge, infrastructure constraints, and concerns about system performance impacts [1]. The same research found that awareness and practical skill were important to adoption and effective utilization [1]. These findings suggest that deception technology is not only a tool selection issue. It is also a workforce readiness issue. Organizations need personnel who can translate deception concepts into authorized designs, safe deployment rules, monitoring procedures, incident response workflows, and evidence artifacts.

The purpose of this paper is to convert that adoption problem into an applied workforce readiness model. The paper does not collect new human participant data and does not use private operational logs. It synthesizes public standards and guidance to define a practical model that critical infrastructure organizations can use before piloting deception technology in safety-sensitive ICS and OT environments.

1.1 Problem statement

The central problem is that deception technology is often introduced as a technical experiment rather than as a

governed cybersecurity capability. A decoy can be technically sound but operationally risky if it is deployed without approval, placed too close to live process control, routed to analysts who do not understand OT context, or treated as an ordinary low-priority alert. Conversely, a low risk honeytoken or monitored engineering file can provide useful intelligence if it is tied to documented ownership, evidence handling, escalation paths, and periodic review. Workforce readiness is, therefore, the bridge between deception technology architecture and safe operational use.

1.2 Research objectives

Three objectives guide the paper. First, identify workforce capabilities required to operationalize deception technology in ICS and OT programs. Second, map those capabilities to public cybersecurity guidance and deception technology literature. Third, present a staged model that organizations can use to plan training, governance, implementation, and evidence collection without using live critical infrastructure as a test environment.

2. MATERIALS AND METHODS

This paper uses design science supported by qualitative document analysis. Design science is appropriate because the research output is an artifact intended to address a practical organizational problem: how to prepare a critical infrastructure workforce to use deception technology safely. Qualitative document analysis is appropriate because the study uses public standards, guidance, and prior research rather than human subjects, interviews, or proprietary operational records.

The document corpus included sources relevant to OT cybersecurity, workforce development, deception technology, incident response, and control governance. The corpus included Ward's dissertation on deception technology adoption [1], CISA operational technology guidance [2], CISA Cross Sector Cybersecurity Performance Goals [3], IEC 62443 security program requirements for asset owners [4], MITRE ATT&CK for ICS [5], NIST CSF 2.0 [7], NIST incident response guidance [8], the NICE Workforce Framework [9], OT workforce research [10], NIST OT security guidance [11], and NICE competency guidance [12]. The sources were selected because they address the capabilities, constraints, roles, and evidence structures needed to convert cyber deception into a repeatable program capability.

2.1 Coding procedure

The analysis followed four steps. First, statements relevant to workforce capability, OT operational constraints, governance, monitoring, incident response, role-based training, threat intelligence, and evidence artifacts were extracted from the corpus. Second, similar statements were grouped into recurring capability categories. Third, each category was tested against the prior adoption barriers identified in the dissertation, including lack of awareness, limited skill, compatibility concerns, resource limits, and infrastructure constraints [1]. Fourth, the categories were reorganized into a staged readiness model with domains, roles, outputs, and evidence artifacts.

2.2 Non-human subjects basis

The paper did not involve human participants, surveys, interviews, focus groups, private organizational records, operational telemetry, or live critical infrastructure systems. It should therefore be treated as a non-human subjects design and document analysis paper. Its value is in creating a practical engineering management artifact that can be validated in later empirical work, pilots, cyber ranges, or sector specific implementations.

3. RESULTS AND FINDINGS

The primary result is the Deception Workforce Readiness Model. The model defines workforce readiness as the ability of an organization to authorize, design, operate, interpret, and improve deception technology in ways that support security outcomes without creating unnecessary operational risk. Five domains emerged from the document analysis: governance literacy, OT context awareness, deception design, cyber intelligence translation, and response integration. These domains are mutually reinforcing. Governance defines what is allowed. OT context defines what is safe. Deception design defines what is technically useful. Cyber intelligence translation defines how raw decoy events become meaningful information. Response integration defines how alerts become action.

3.1 Source corpus contribution

Table -1: Source Corpus and Model Contribution

Source category	Use in workforce readiness model
Prior adoption research	Identifies awareness, skill, compatibility, resource, and infrastructure barriers that the model must address [1].
OT security guidance	Defines safety, reliability, segmentation, asset visibility, and operational constraints for deception planning [2], [11].
Governance and control frameworks	Supports policy ownership, risk decisions, role assignment, and security program evidence [3], [4], [7].
Workforce	Defines role based skills, job

frameworks and studies	readiness, training outcomes, and practical competency needs [9], [10], [12].
Deception and ATT&CK sources	Links decoy events to adversary behavior, threat intelligence, and response enrichment [5], [6].

3.2 Workforce readiness domains

Governance literacy is the foundation of the model. Deception technology intentionally creates false or monitored artifacts, so organizations must define who may authorize deception assets, what segments are prohibited, how decoys are labeled internally, and how legal or privacy concerns will be reviewed. IEC 62443-2-1 emphasizes security program requirements for asset owners, while the NIST CSF 2.0 emphasizes governance, risk management, and organizational roles [4], [7]. These sources support the conclusion that deception technology should be governed as part of the security program rather than left to informal experimentation.

OT context awareness ensures that deception remains aligned with operational reality. CISA emphasizes that OT systems have safety, reliability, and availability constraints that differ from enterprise IT [2]. Personnel should understand Purdue model zones, remote access paths, engineering workstations, historian systems, controller adjacent networks, maintenance windows, and change control. Without this context, a workforce may deploy realistic decoys in unrealistic places or may misinterpret normal engineering behavior as malicious activity.

Deception design converts governance and context into deployable patterns. Personnel should understand the difference between honeytokens, service decoys, low interaction honeypots, high interaction honeypots, fake engineering documents, false credentials, and simulated OT services. The safest starting points are passive and isolated lures that do not write to process control devices. More realistic decoys can be added only after ownership, alert routing, and approval workflows are documented.

Cyber intelligence translation turns decoy interaction into useful security knowledge. MITRE ATT&CK for ICS provides a shared vocabulary for adversary behavior in ICS environments [5]. A decoy event should therefore be enriched with technique mapping, source context, likely intent, affected zone, and confidence level. This prevents deception alerts from becoming isolated technical events and makes them useful to analysts, engineers, managers, and incident response personnel.

Response integration is the final domain. NIST incident response guidance emphasizes preparation, detection, analysis, containment, eradication, recovery, and improvement [8]. Deception technology supports this cycle only when alerts have playbooks, escalation rules, evidence preservation procedures, false positive review, and post-incident learning. A decoy that nobody owns or investigates is not a workforce capability; it is an unattended sensor.

Table -2: Deception Workforce Readiness Domains

Domain	Readiness outcome and minimum evidence
Governance literacy	Approved policy addendum, accountable owner, prohibited zones, legal and privacy review path.
OT context awareness	Asset zone map, change control rules, engineering review, no control command boundary.
Deception design	Approved decoy types, placement plan, monitoring path, fidelity review, refresh schedule.
Cyber intelligence translation	ATT&CK for ICS mapping, alert enrichment fields, confidence rating, reporting format.
Response integration	Escalation rule, playbook trigger, evidence preservation steps, post incident improvement log.

3.3 Implementation sequence

The model uses a staged implementation sequence because critical infrastructure organizations differ in size, sector, maturity, staffing, and budget. The baseline stage establishes authority, policy boundaries, and ownership. The pilot stage deploys low risk deception artifacts such as honeytokens, monitored files, or remote access lures in controlled segments. The operational stage integrates decoy events with monitoring, incident response, and reporting. The improvement stage refreshes decoy realism, updates training, maps events to ATT&CK for ICS, and reports lessons learned to governance stakeholders.

This sequence prevents organizations from treating deception as a one time product deployment. Instead, it frames deception as a cycle of authorization, controlled placement, alert interpretation, response, evidence collection, and continuous improvement. The sequence also addresses workforce concerns found in OT job analysis research. Ramezan et al. found that OT cybersecurity employers frequently seek prior experience, education, certifications, communication skills, and knowledge of OT frameworks and standards [10]. The DWRM converts those broad expectations into role specific deception tasks.

Table -3: Implementation Sequence and Evidence Artifacts

Stage	Primary action	Evidence artifact
Baseline	Assign owner and define allowed deception use	Policy addendum and approval record
Pilot	Deploy low risk honeytokens or monitored files	Pilot scope, alert route, change record
Operational	Integrate alerts with SOC or OT monitoring	Playbook, triage queue, response log
Improvement	Review events and refresh artifacts	Metrics report and lessons learned

4. DISCUSSION

The model has three practical implications. First, deception technology should be governed before it is deployed. Critical infrastructure operators should write deception into an existing cybersecurity policy or OT security procedure. That policy should define approved decoy types, prohibited deployment locations, change control rules, ownership, monitoring requirements, and review frequency. This does not require a large program at the beginning. It requires enough structure to prevent an experimental tool from becoming an unmanaged operational risk.

Second, workforce readiness should be role-based. Executives and governance personnel need to understand risk, approval boundaries, and evidence requirements. OT engineers need to understand where deception can be placed without affecting process reliability. SOC analysts need to understand what a decoy interaction means and when to escalate. Incident responders need to understand evidence handling and the coordination of containment. Threat intelligence personnel need to convert observed behavior into technique mapping and program learning. The NICE Workforce Framework supports this role-based perspective by organizing cybersecurity work into tasks, knowledge, and skills [9].

Third, deception technology can improve cyber intelligence only when telemetry is interpreted. A single interaction with a fake credential, fake historian tag, or decoy service can reveal reconnaissance or misuse. However, the signal becomes useful only when it is enriched with zone, asset, user, protocol, source, time, and likely technique. MITRE ATT&CK for ICS supports this translation by providing a framework for describing adversary behavior in industrial environments [5].

4.1 Limitations

The model has limitations. It is not an empirical validation of deception technology effectiveness. It does not measure detection latency, false positive reduction, or incident response outcomes in a live environment. It also does not prove that all organizations can implement deception at the same maturity level. Small utilities and manufacturers may begin with honeytokens and policy artifacts, while larger organizations may operate decoy services, historian lures, and cyber range validation. The model should therefore be treated as a planning and readiness artifact that can be refined through future pilots, simulations, and sector specific testing.

5. CONCLUSION AND FUTURE WORK

Deception technology can improve critical infrastructure cybersecurity by producing high confidence indicators of unauthorized activity and by supporting adversary behavior analysis. In ICS and OT environments, however, the workforce must be prepared before deception technology is deployed. The Deception Workforce Readiness Model provides a practical structure for that preparation. It defines five workforce domains, links them to public cybersecurity guidance, and gives organizations a staged sequence for moving from policy readiness to governed operation.

The paper updates a prior policy framework into a journal ready engineering model suitable for low risk program planning. It also addresses a key adoption issue identified in prior research: awareness and practical skill are central to effective utilization of deception technology [1]. Future work should validate the model through simulation, cyber range exercises, tabletop exercises, or sector specific pilots in manufacturing, water and wastewater, energy, and transportation environments. Future work should also develop metrics for readiness scoring, role based training completion, alert enrichment quality, and response playbook effectiveness.

ACKNOWLEDGEMENT

No external funding was received for this paper. The author declares no conflict of interest.

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, 2025. Available: https://www.proquest.com/dissertations-theses/

[2] Cybersecurity and Infrastructure Security Agency, "Principles of Operational Technology Cyber Security,"

2024. Available: https://www.cisa.gov/resources-tools/resources/principles-operational-technology-cyber-security

[3] Cybersecurity and Infrastructure Security Agency, "Cross-Sector Cybersecurity Performance Goals, Version 2.0," 2025. Available: https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[4] 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

[5] MITRE, "MITRE ATT&CK for ICS, Version 19.1," 2026. Available: https://attack.mitre.org/matrices/ics/

[6] Z. Moric, V. Dakic, and D. Regvart, "Advancing Cybersecurity with Honeypots and Deception Strategies," Informatics, vol. 12, no. 1, article 14, 2025, doi: 10.3390/informatics12010014.

[7] National Institute of Standards and Technology, "The NIST Cybersecurity Framework 2.0," NIST Cybersecurity White Paper 29, 2024, doi: 10.6028/NIST.CSWP.29.

[8] A. Nelson, S. Rekhi, K. Scarfone, and M. Souppaya, "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile," NIST Special Publication 800-61 Revision 3, 2025, doi: 10.6028/NIST.SP.800-61r3.

[9] R. Petersen, D. Santos, K. Wetzel, M. Smith, and G. Witte, "Workforce Framework for Cybersecurity (NICE Framework)," NIST Special Publication 800-181 Revision 1, 2020, doi: 10.6028/NIST.SP.800-181r1.

[10] C. A. Ramezan, P. M. Coffy, and J. Lemons, "Building the Operational Technology (OT) Cybersecurity Workforce: What are Employers Looking for?" Journal of Cybersecurity Education, Research and Practice, vol. 2024, no. 1, article 6, 2023, doi: 10.32727/8.2023.31.

[11] K. Stouffer, M. Pease, C. Y. 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, 2023, doi: 10.6028/NIST.SP.800-82r3.

[12] K. Wetzel, "NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce," NIST Interagency/Internal Report 8355, 2023, doi: 10.6028/NIST.IR.8355.

BIOGRAPHIES

Daniel Ward is an information technology and cybersecurity scholar-practitioner whose work focuses on industrial control systems, operational technology, critical infrastructure cybersecurity, deception technology, governance, and cyber risk. His research agenda extends doctoral work on deception technology adoption into control frameworks, workforce readiness, decoy placement, and sector specific implementation models.