Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Deception Architecture for Water and Wastewater Operational Technology Environments

Daniel Ward

Department of Computer Science, Southern New Hampshire University, Manchester, United States
ORCID: 0009-0002-4466-6739

Abstract **- Water and wastewater utilities rely on operational technology (OT), including SCADA, HMIs, PLCs, RTUs, pumps, lift stations, treatment processes, and remote telemetry. Cybersecurity guidance for the sector emphasizes asset inventory, incident response, reduced public exposure, credential security, backups, assessments, and awareness training. This paper proposes a nonintrusive deception architecture for OT in water and wastewater systems that maps decoys, honey credentials, false historian artifacts, and protocol lures to utility zones. The architecture is derived through design science and document analysis of public water-sector cybersecurity guidance, OT security standards, and recent deception literature. It emphasizes passive observation, staged deployment, utility approval, alert enrichment, and evidence retention. The contribution is a sector-specific reference model that helps utilities generate high-confidence indicators of reconnaissance, credential misuse, remote-access abuse, and lateral movement without introducing unsafe control actions into treatment or distribution processes.**

Keywords - critical infrastructure; cyber deception; operational technology; SCADA; water cybersecurity; wastewater systems

I. INTRODUCTION

Water and wastewater systems are lifeline infrastructures that support public health, sanitation, municipal services, industrial activity, and emergency response. They increasingly depend on operational technology (OT), including supervisory control and data acquisition (SCADA), human-machine interfaces (HMIs), programmable logic controllers (PLCs), remote terminal units (RTUs), telemetry networks, pumps, lift stations, treatment processes, storage facilities, and distribution systems. In these environments, cybersecurity controls must account for uptime, operator safety, water quality, process reliability, equipment lifecycle constraints, and emergency operating procedures.

The U.S. Environmental Protection Agency (EPA) describes OT in water and wastewater systems as hardware and software that detect or cause changes through direct monitoring or control of physical devices, processes, and events [2]. This definition is important because it distinguishes water-sector OT from ordinary business information technology. A security tool that is useful in enterprise IT may be unsuitable in OT if it introduces scan traffic, latency, uncontrolled command pathways, or confusion for operators who must maintain physical processes.

Current water-sector cybersecurity guidance emphasizes practical actions: reduce public Internet exposure, assess cybersecurity posture, change default passwords, inventory OT and IT assets, develop and exercise incident-response and recovery plans, back up systems, reduce exposure to known vulnerabilities, and train the workforce [3]. These are necessary baseline activities, but they do not always produce high-confidence early warning when an adversary performs reconnaissance, tests remote access, attempts credential misuse, or moves laterally toward SCADA assets.

Cyber deception can address that gap by deploying monitored assets, credentials, documents, services, or protocol lures that legitimate operators should not touch. Interaction with a decoy can provide a high-confidence signal of misuse or unauthorized activity. This paper proposes a sector-specific deception architecture for water and wastewater OT environments. The architecture is intended to help utilities plan safe, low-risk, and auditable deployments that support detection, response, and evidence retention without allowing decoys to control production treatment or distribution processes.

II. SECTOR CONTEXT AND RELATED WORK

A. Water and Wastewater OT as Municipal Infrastructure

Water and wastewater utilities may operate centralized treatment plants, wells, reservoirs, tanks, pressure zones, pumping stations, lift stations, disinfection processes, chemical dosing systems, laboratory systems, and field telemetry. These assets are often distributed across large geographic areas and may connect through leased lines, cellular modems, radio links, municipal networks, vendor access pathways, or OT demilitarized zones. The result is a complex environment in which visibility gaps and remote-site dependencies can limit the effectiveness of perimeter-focused monitoring.

A deception event in this setting should not be treated like an ordinary signature alert. If a false VPN profile, decoy historian endpoint, bogus engineering project file, or RTU-like service is touched, the event may indicate reconnaissance, credential testing, lateral movement, or unsafe probing. The value of deception, therefore, depends on sector-specific placement, alert routing, and operational interpretation.

B. OT Security and Response Baselines

The design of water-sector deception must begin with OT constraints. NIST SP 800-82 Revision 3 defines OT security around the protection of systems that monitor or control physical processes and emphasizes the need to preserve safety, availability, and process integrity [8]. The NIST Cybersecurity Framework 2.0 also frames cybersecurity outcomes across

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

govern, identify, protect, detect, respond, and recover functions [9]. Deception technology is most directly relevant to detection and response, but it also depends on governance, asset visibility, change control, and recovery planning.

Asset visibility is foundational. Joint 2025 guidance from CISA and partners identifies OT asset inventory and taxonomy as prerequisites for risk identification, vulnerability management, incident response, and defensible architecture [7]. For deception, an inventory is also required to avoid misleading operators or creating lures that resemble live assets too closely. Deception should be planned from an approved asset taxonomy rather than improvised inside production networks.

The water-sector incident-response context is equally important. The Water and Wastewater Sector Incident Response Guide stresses validation, escalation, coordination, and evidence handling during cyber incidents [5]. A deception system should therefore feed into an existing response process rather than creating isolated alerts that no one owns.

C. Cyber Deception and ICS Honeypots

Recent deception literature supports the use of honeypots, honeynets, and decoy services for adversary interaction, threat intelligence, and early warning [11], [15]. Industrial-control-system honeypot research has also advanced toward higher-fidelity and physics-aware designs. HoneyICS, for example, presents a high-interaction, physics-aware honeynet for industrial control systems [13], while ICSNet proposes a hybrid-interaction honeynet for ICS environments [14].

However, water-sector deployment differs from laboratory honeynet research. Many utilities lack dedicated OT security engineering teams, permissive maintenance windows, or cyber ranges. A practical architecture must start with low-risk lures, integrate with existing incident response paths, and avoid any mechanism that could manipulate real pumps, valves, chemical feeds, blowers, storage levels, or treatment processes.

III. MATERIALS AND METHODS

This paper uses design science supported by qualitative document analysis. The goal is to create a practical artifact rather than to test a commercial deception product or collect new human-subject data. The source base includes water-sector cybersecurity guidance, OT security standards, current control frameworks, recent ICS honeypot literature, MITRE ATT&CK for ICS, and the author's prior dissertation on deception technology adoption in manufacturing and critical infrastructure [1].

The document-analysis procedure followed five steps. First, water-sector OT assets and operating processes were identified from EPA guidance, including SCADA, HMIs, PLCs, RTUs, source-water intake, treatment, storage, pumps, and distribution [2]. Second, baseline cyber actions and incident-response requirements were extracted from CISA, EPA, and FBI guidance [3], [5]. Third, asset-inventory and taxonomy requirements were mapped from CISA's 2025 OT asset-inventory guidance [7]. Fourth, deception patterns were derived from recent honeypot and ICS deception literature [11]-[15]. Fifth, the patterns were organized into a water/wastewater reference architecture and implementation sequence.

The artifact was evaluated conceptually against four criteria. Safety means that deception components must not issue commands to live treatment, distribution, or collection equipment. Operational fit means that lures should correspond to plausible utility assets and workflows. Evidence value means that each interaction should generate an alert, context, ownership, and retainable evidence. Maintainability means the architecture should remain feasible for small- and mid-sized utilities with limited cyber staff.

IV. RESULTS: WATER/WASTEWATER DECEPTION ARCHITECTURE

The primary result is a zone-based architecture for water and wastewater deception. It places decoys and honeytokens at trust boundaries where unauthorized interaction has high evidentiary value: enterprise IT, OT demilitarized zones, SCADA engineering workstations, historian pathways, remote access, remote sites, and controller-adjacent segments. The architecture intentionally separates deception from control. It is designed to observe and alert, not to operate treatment equipment.

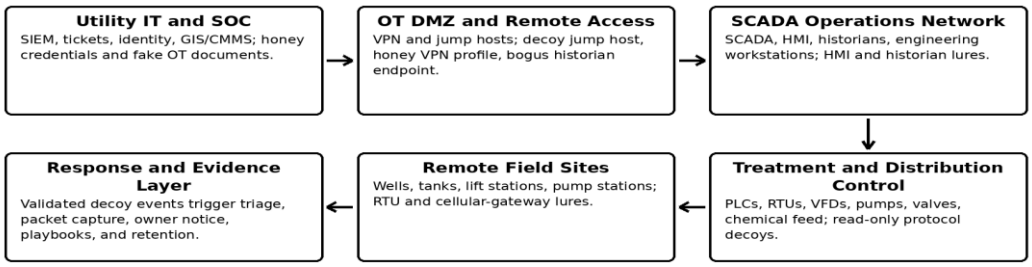

Fig. 1. Zone-based deception architecture for water and wastewater OT environments.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

A. Architecture Principles

The architecture is governed by six principles. First, decoys should observe and alert rather than control. A decoy should never manipulate a real pump, valve, chemical feed, blower, or tank process. Second, decoys should be placed where legitimate traffic is rare or well understood, which increases alert confidence. Third, each decoy must have an owner, a monitoring destination, response instructions, and a retirement plan.

Fourth, deception should be staged. A utility may begin with honey credentials and fake engineering files in enterprise or DMZ locations, then progress to read-only protocol decoys, false historian endpoints, and controlled remote-site lures. Fifth, each pattern should produce evidence artifacts such as source host, credential name, timestamp, attempted service, protocol request, and response action. Sixth, deception events should feed incident response playbooks rather than remain isolated within a security tool.

B. Zone-to-Pattern Mapping

Table I maps water utility zones to deception patterns and primary alert signals. The patterns are modular. A small utility may begin with one or two low-interaction patterns, while a larger utility may deploy multiple patterns across enterprise, DMZ, SCADA, remote-site, and historian environments.

Table I. Water/Wastewater Zone-to-Deception Mapping.

Utility zone	Deception pattern	Primary signal
Enterprise IT	Fake OT diagrams, honey credentials, decoy vendor folders	Credential use, document access, phishing follow-on
OT DMZ / remote access	Decoy jump host, fake VPN profile, bogus historian endpoint	Remote-access misuse, lateral movement, reconnaissance
SCADA / HMI zone	False HMI screen name, fake engineering file, canary tag	Unauthorized browsing, project-file access, tag lookup
Historian / reporting	Canary historian tags, false process query, decoy report export	Data staging, historian reconnaissance, unusual queries
Remote pump or lift station	RTU-like service, cellular-gateway lure, fake pump-station host	Remote-site probing, protocol scanning, source geolocation
Controller-adjacent segment	Low-interaction PLC or protocol emulator with no production control	Protocol request, function-code pattern, scan timing

C. Detection Use Cases

The architecture supports seven recurring detection use cases. These use cases are framed so that each event can be validated and escalated through the utility response process.

Table II. Detection Use Cases and Evidence Artifacts.

Use case	Example decoy	Evidence artifact
Internet-exposed probing	RTU or gateway lure	Source IP, protocol, banner request, scan timing
Credential misuse	Honey VPN or jump-host credential	Account name, attempted service, source host
Engineering workstation reconnaissance	Fake project file or HMI screen name	File path, user context, endpoint, timestamp
Historian reconnaissance	Canary tag or false historian endpoint	Query string, account, source application
Remote-site probing	Pump-station or lift-station lure	Remote segment, function code, session metadata
Lateral movement	Decoy server or bogus share	SMB/RDP/SSH attempt, source system, sequence
Playbook validation	Exercise honeytoken or tabletop lure	Alert route, owner response, time to validation

D. Telemetry and Response Workflow

The architecture routes decoy events to a response workflow rather than treating them as stand-alone alarms. The workflow has six steps: detect, enrich, validate, classify, respond, and retain evidence. Detection occurs when a decoy, honey credential, canary tag, or false service is touched. Enrichment adds asset owner, subnet, protocol, source, timestamp, and MITRE ATT&CK for ICS context. Validation determines whether the event is authorized testing, misconfiguration, vendor activity, insider misuse, or suspected adversary behavior.

Classification assigns the event to a response category, such as reconnaissance, credential misuse, remote-access abuse, lateral movement, or protocol probing. Response actions may include disabling credentials, blocking a source, notifying OT operations, preserving logs, opening an incident ticket, or escalating to external partners. Evidence retention preserves packet captures, logs, screen captures, configuration state, and response notes for after-action improvement. This workflow aligns with water-sector incident-response guidance that emphasizes validation, reporting, analysis, and coordination [5].

V. IMPLEMENTATION MODEL

A. Governance and Inventory

The first phase is governance and inventory. The utility identifies owners for enterprise IT, OT operations, SCADA engineering, remote access, incident response, and executive risk acceptance. It also defines zones where deception is permitted, zones where deception is prohibited, and conditions for removal. Decoys should be documented in a restricted inventory so that authorized teams understand which are fake,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

which are monitored, and what actions must be taken when an event occurs.

B. Enterprise and DMZ Lures

The second phase deploys low-risk lures in enterprise and DMZ locations. Examples include fake OT network diagrams in monitored shares, honey credentials with no production privileges, decoy vendor folders, a false VPN profile, or a non-production jump-host service. These lures are useful because they can generate evidence without touching control networks. They also support CISA's baseline guidance for controlling remote access, inventorying assets, training users, and exercising incident response plans [3], [6].

C. SCADA and Historian Deception

The third phase adds SCADA-adjacent deception. Examples include false historian endpoints, canary historian tags, fake HMI screen names, or decoy engineering-project files. These lures should be coordinated with operators to avoid confusion during maintenance or emergencies. Historian deception is especially useful because adversaries often seek process context before attempting disruptive action.

D. Remote-Site and Protocol Decoys

The fourth phase introduces remote-site and protocol decoys. A utility may deploy a low-interaction RTU-like service, a Modbus/TCP or vendor-protocol emulator, a pump-station lure, or a cellular-gateway decoy. These assets must remain isolated from production control and should be limited to observation and alerting. This phase provides higher OT fidelity but also requires stronger change control, network segmentation, and operational approval.

E. Exercises and Improvement

The fifth phase integrates decoys into tabletop and technical exercises. The utility can test whether a honey credential creates an alert, whether the alert reaches the correct queue, whether OT owners are notified, whether logs are preserved, and whether the playbook produces a safe operational decision. Lessons learned should be used to update asset inventories, playbooks, contact lists, decoy naming conventions, and alert thresholds.

VI. DISCUSSION

The proposed architecture addresses the sector-specific problem that many water and wastewater utilities need higher confidence in early warning without adding operational risk. Traditional detection systems can produce high volumes of alerts, many of which require contextual interpretation. Deception events can be more actionable because legitimate operators should not use honey credentials, browse decoy shares, query false historian tags, or connect to fake remote-site services.

The most important design tradeoff is fidelity versus risk. Low-fidelity lures are cheap and safe, but sophisticated attackers may detect them. High-fidelity honeynets are more believable, but they require stronger engineering support, monitoring, and isolation. For utilities with limited staff, the architecture recommends starting with enterprise and DMZ lures before introducing SCADA-adjacent or protocol-level deception.

The architecture also creates governance evidence. A utility can document decoy scope, asset-owner approval, change-control tickets, alert routing, incident playbook links, tabletop results, and after-action improvements. This evidence can support cybersecurity planning, board reporting, regulatory discussions, and internal risk management. Prior dissertation research found that awareness and skill influence the adoption and effective utilization of deception in ICS/OT contexts [1]. A utility cannot gain value from deception merely by installing a tool; it must train staff to interpret decoy events and respond safely.

VII. LIMITATIONS AND FUTURE WORK

This paper develops a design artifact from public guidance and current literature. It does not test the architecture in a live utility, cyber range, or laboratory simulation. The artifact should therefore be treated as a planning and implementation model rather than a validated performance benchmark. Future work should evaluate the architecture using synthetic traffic, tabletop exercises, cyber-range scenarios, or controlled utility testbeds.

A second limitation is that water utilities differ significantly in size, staffing, ownership, technology, vendor support, network architecture, and regulatory obligations. A large metropolitan utility may support a dedicated security operations center and multiple treatment plants, while a small rural utility may rely on contractors and part-time IT support. The architecture is intentionally modular, but local implementation must be tailored to each utility's operational reality.

A third limitation is that deception can create operational confusion if it is not governed. Fake assets, documents, or credentials must be managed carefully to prevent them from misleading authorized operators, auditors, vendors, or emergency responders. Future work should develop a utility-specific scoring model for deception readiness, alert quality, and operational burden.

VIII. CONCLUSION

Water and wastewater utilities depend on OT for source-water intake, treatment, distribution, storage, pumping, monitoring, and incident response. As these systems become more connected, utilities need methods to detect unauthorized reconnaissance, credential misuse, remote-access abuse, and lateral movement before adversaries gain live control of systems. Deception technology can support that need when it is designed as a governed, passive, and evidence-producing capability rather than as an uncontrolled experiment.

The architecture proposed in this paper maps deception patterns to utility zones, detection use cases, telemetry paths, and staged implementation phases. It emphasizes passive observation, operational fit, approved placement, alert enrichment, evidence retention, and continuous improvement. The resulting model provides water and wastewater utilities with a practical starting point for using cyber deception to support detection and response while respecting the safety and availability requirements of OT environments.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

ACKNOWLEDGMENT

The author acknowledges the prior dissertation research that informed this extension paper and the public cybersecurity guidance issued for the water and wastewater sector.

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/

[2] U.S. Environmental Protection Agency, “Assessing if a Water & Wastewater System has Operational Technology,” Washington, DC, USA, 2024. Available: https://www.epa.gov/system/files/documents/2024-03/assessing-if-a-wws-has-ot_508_c.pdf

[3] Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and U.S. Environmental Protection Agency, “Top Cyber Actions for Securing Water Systems,” Washington, DC, USA, 2024. Available: https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems

[4] U.S. Environmental Protection Agency, “Cybersecurity Planning,” Washington, DC, USA, 2026. Accessed: Jun. 15, 2026. Available: https://www.epa.gov/cyberwater/cybersecurity-planning

[5] Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and U.S. Environmental Protection Agency, “Incident Response Guide: Water and Wastewater Sector,” Washington, DC, USA, 2024. Available: https://www.epa.gov/system/files/documents/2024-01/wws-sector_incident-response-guide.pdf

[6] Cybersecurity and Infrastructure Security Agency, “Cross-Sector Cybersecurity Performance Goals, Version 2.0,” Washington, DC, USA, 2025. Available: https://www.cisa.gov/sites/default/files/2025-12/CPG_Report_2.0_508c.pdf

[7] Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, National Security Agency, Environmental Protection Agency, and international partners, “Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators,” Washington, DC, USA, 2025. Available: https://www.cisa.gov/sites/default/files/2025-08/joint-guide-foundations-for-OT-cybersecurity-asset-inventory-guidance_508c.pdf

[8] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, et al., “Guide to Operational Technology (OT) Security,” National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST SP 800-82 Rev. 3, 2023. doi: 10.6028/NIST.SP.800-82r3

[9] National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” Gaithersburg, MD, USA, NIST CSWP 29, 2024. doi: 10.6028/NIST.CSWP.29

[10] MITRE, “ATT&CK for ICS Matrix,” McLean, VA, USA, 2026. Accessed: Jun. 15, 2026. Available: https://attack.mitre.org/matrices/ics/

[11] Z. Morić, V. Dakić, and D. Regvart, “Advancing cybersecurity with honeypots and deception strategies,” Informatics, vol. 12, no. 1, p. 14, 2025. doi: 10.3390/informatics12010014

[12] S. Maesschalck, “Next-Generation Industrial Control System (ICS) Security: Towards ICS Honeypots for Defence-in-Depth Security,” Ph.D. dissertation, Lancaster University, Lancaster, UK, 2023. doi: 10.17635/lancaster/thesis/2099

[13] 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 Proc. 18th Int. Conf. Availability, Reliability and Security (ARES), 2023, Art. 113. doi: 10.1145/3600160.3604984

[14] L. Salazar, E. Lopez-Morales, J. Lozano, C. Rubio-Medrano, and A. A. Cardenas, “ICSNet: A hybrid-interaction honeynet for industrial control systems,” in Proc. Sixth Workshop on CPS&IoT Security and Privacy, 2024, pp. 68-79. doi: 10.1145/3690134.3694813

[15] A. Javadpour, F. Ja’fari, T. Taleb, M. Shojafar, and C. Benzaïd, “A comprehensive survey on cyber deception techniques to improve honeypot performance,” Computers & Security, vol. 140, p. 103792, 2024. doi: 10.1016/j.cose.2024.103792