

Article

Process-Embedded Ethics in OT Digital Forensics: A Principled Investigation Framework for Water Infrastructure ICS/SCADA Systems

Tosin Akinsowon * and Bing Zhou *

Department of Computer Science, Sam Houston State University, Huntsville, TX 77341, USA

* Correspondence: tba015@shsu.edu (T.A.); bxz003@shsu.edu (B.Z.)

Abstract

The integration of information technologies into operational technology (OT) environments that encompass industrial control systems (ICSs), Supervisory Control and Data Acquisition (SCADA) systems, and critical infrastructure such as water and wastewater management facilities has introduced significant cybersecurity vulnerabilities alongside urgent questions of ethics and accountability. The existing digital forensic ethics frameworks were developed for enterprise IT contexts and provide no specific governance for investigations conducted within safety-critical OT environments, where a forensic misstep can disrupt water delivery or disable safety controls. This paper employs a four-stage qualitative research design that consists of a systematic literature review, ethical framework analysis grounded in principled cyberethics principles, forensic process mapping, and multi-case analysis of five documented real-world incidents to address this gap. The paper identifies and categorizes six primary ethical challenges that are unique to OT/ICS/SCADA digital forensics, maps each to the investigative phase at which it arises, proposes the Water ICS SCADA Ethical Digital Forensics (WISE-DF) framework as a six-phase principled investigation model with ethical safeguards embedded as mandatory procedural gates, and provides actionable recommendations for investigators, organizations, and policymakers. Validation employs three complementary approaches: standards-alignment against the National Institute of Standards and Technology (NIST) Special Publications (SP800-82r3) and Internal Report (IR 8428), the Americas Water Infrastructure Act of 2018 (AWIA 2018), and the Environmental Protection Agency (EPA 2024); counter-argument testing of each recommendation; and Daubert-consistency evaluation assessing whether WISE-DF compliance produces forensic evidence that is capable of meeting U.S. federal admissibility requirements. Although the Daubert standard applies specifically to U.S. federal proceedings, the ethical framework and WISE-DF gates are designed to be generalizable across jurisdictions. Water and wastewater management serves as the primary illustrative case domain; the framework is designed to be generalizable across OT sectors.



Academic Editor: Hung-Yu Chien

Received: 30 June 2026

Revised: 24 July 2026

Accepted: 27 July 2026

Published: 1 August 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

Keywords: operational technology; digital forensics; ICS; SCADA; wastewater; PLC; water infrastructure; cyberethics; critical infrastructure; forensic readiness; WISE-DF framework; Daubert standard

1. Introduction

Critical infrastructure includes the systems and assets that are essential to the functioning of modern society, and it has become an increasingly common target of cyberattacks.

Among the consequential targets are operational technology (OT) environments, including industrial control systems (ICSs), Supervisory Control and Data Acquisition (SCADA) systems, and facilities that are central to public health, such as water and wastewater treatment plants. Unlike traditional information technology (IT) systems, OT environments were historically designed for reliability, safety, and continuity rather than security, leaving them particularly exposed to modern cyber threats [1,2]. The consequences of a successful attack extend well beyond financial loss or data theft. They threaten human safety, environmental integrity, and national security. In response to this growing threat landscape, digital forensics has emerged as an indispensable discipline to investigate cyber incidents within OT environments [3].

The application of digital forensic methods to OT/ICS/SCADA systems presents challenges that fundamentally differ from those encountered in conventional IT forensics. OT systems frequently operate on legacy platforms with proprietary protocols, limited logging capabilities, and minimal tolerance for downtime [4,5]. The ethical dimensions of digital forensics in OT environments remain critically underexplored. Cook et al. [4], whose 2023 IEEE survey is one of the most comprehensive works covering ICS digital forensics to date, explicitly confirm that few existing studies address the ethics dimension of OT forensic practice. The National Institute of Standards and Technology Internal Reports (NISTIR 8428) [5], the closest available OT-specific Digital Forensic and Incident Response (DFIR) framework, contains no ethical governance provisions. Professional ethics codes from the International Association of Computer Investigative Specialists (IACIS) and Scientific Working Group on Digital Evidence (SWGDE) were developed for enterprise IT contexts and do not address the specific obligations of investigators working in safety-critical OT environments where a forensic misstep could disrupt the water supply for an entire city or trigger a safety failure [6]. This paper addresses that gap directly.

Water and wastewater management serves throughout this paper as the primary illustrative case domain for three reasons. First, water systems directly affect human life, making the principle of non-maleficence particularly acute: contamination attacks can reach public harm in seconds to minutes, a fundamentally different ethical environment from an enterprise breach. Second, the U.S. Government Accountability Office (GAO) [7] found that nearly 170,000 U.S. water systems face escalating cyber risks while relying on voluntary practices and aging SCADA infrastructure, which is making this sector structurally more vulnerable than energy or transportation OT, which operates under more prescriptive federal mandates. Third, the water sector offers a rich publicly documented incident record that provides concrete analytical material.

1.1. Research Questions

- RQ1: What ethical challenges uniquely arise in OT/ICS digital forensic investigations?
- RQ2: At which investigative phases do these challenges become operationally significant?
- RQ3: How can ethical safeguards be embedded within OT forensic processes?

1.2. Contributions

- First, it provides a systematic taxonomy of six primary ethical challenges that are unique to OT/ICS/SCADA digital forensics, grounded in the principlism of Beauchamp [8] and Childress and anchored to the specific investigative phases where each challenge arises.
- Second, it maps those challenges to the OT forensic process in a process-embedded ethics model that makes obligations operationally actionable rather than declarative.
- Third, it tests the taxonomy against five documented real-world incidents as empirical grounding.

- Fourth, it proposes the WISE-DF framework, a six-phase investigative model in which ethical safeguards function as mandatory procedural gates, and derives seven actionable recommendations validated through three complementary approaches: standards-alignment with current regulatory frameworks, counter-argument testing, and Daubert-consistency evaluation [9].

The remainder of this paper is structured as follows. Section 2 reviews the existing literature. Section 3 describes the research methodology. Section 4 identifies the six ethical challenges. Section 5 maps each principlism principle to the specific forensic phase where it becomes operationally binding. Section 6 presents five real-world case scenarios. Section 7 introduces the WISE-DF framework. Section 8 provides seven recommendations. Section 9 synthesizes the findings and discusses limitations. Section 10 proposes future research directions.

2. Background and Related Works

2.1. Operational Technology and Industrial Control Systems

Operational technology refers to hardware and software used to monitor and control physical processes, devices, and infrastructure. ICS is the overarching category that encompasses control systems used in energy, manufacturing, transportation, and water management [1]. Within ICSs, SCADA systems represent the most widely deployed architecture for monitoring and control of large-scale infrastructure. A typical water SCADA deployment consists of remote terminal units (RTUs) or programmable logic controllers (PLCs) at pumping stations and treatment facilities, a central master station aggregating process data, human-machine interfaces (HMIs) for operator interaction, and communication networks linking these components over protocols such as Modbus TCP/IP, DNP3 and OPC-UA [10]. These functions, if disrupted or manipulated, could result in immediate public health emergencies [11]. The EPA and NIST have identified SCADA-dependent water utilities as high-priority targets given their societal importance and historical underinvestment in cybersecurity [7,12,13].

2.2. Digital Forensics in OT Environments

Traditional digital forensic methodologies developed for enterprise IT systems include the phases of identification, preservation, collection, examination, analysis, and reporting [3,14]. These phases require significant adaptation in OT contexts: data are often stored in non-standard formats tied to proprietary vendor protocols; many ICS devices lack the memory capacity or logging functionality needed to generate a reliable audit trail; and the live safety-critical nature of OT systems makes conventional acquisition techniques such as system shutdown or disk imaging impractical or prohibited [4,5,10].

Live forensics is the collection of volatile data from running systems without powering them down, which has also emerged as the primary methodology that is applicable to OT environments [15,16]. However, live forensics introduces ethical and evidentiary complications, including the risk of altering the evidence being collected and challenges to legal admissibility without full chain-of-custody controls [17,18]. Van der Knijff [19] provides the foundational characterization of this problem: OT investigations cannot be treated as a simple extension of IT forensics because the object of investigation is a live control environment in which digital actions propagate into physical consequences. Cook et al. [4] confirm live-system acquisition, evidence integrity, and proprietary protocol decoding as dominant challenges yet explicitly note that no existing work addresses the ethics dimension.

2.3. Ethical Frameworks Applicable to OT Forensics

Principlism, as articulated by Beauchamp and Childress [8] and applied to computing by Spinello [6], identifies four foundational ethical principles that are relevant to cyberspace: autonomy (respect for individual rights and informed consent), non-maleficence (the duty to avoid harm), beneficence (the obligation to act in the public good), and justice (fair and equitable treatment of all parties). Non-maleficence is especially salient in OT forensics, where the act of investigation itself, if conducted improperly, could cause physical harm to the public. Professional ethics in digital forensics is governed by codes from bodies such as the IACIS and SWGDE, which emphasize accuracy, objectivity, and harm minimization [20,21]. These frameworks were developed for IT contexts and do not address the specific obligations of investigators in safety-critical OT environments. Stoykova [22] argues that three categories of unaddressed threats, improper application of technology, outdated procedural safeguards, and absence of reliability testing, systematically undermine fairness in digital evidence proceedings. In OT forensics all three threats are intensified: OT-specific tools routinely lack independent validation; procedural safeguards derive from IT frameworks that are inapplicable to live industrial systems; and reliability testing programs for OT forensic tools do not currently exist.

The most directly relevant legal standard to the admissibility of forensic evidence derived from OT investigations in U.S. federal proceedings is the Daubert standard, established in *Daubert v. Merrell Dow Pharmaceuticals, Inc.* [9] and codified in Federal Rule of Evidence 702. The Daubert standard requires that expert scientific testimony satisfy four criteria: testability; peer review and publication; known or potential error rate; and general acceptance within the relevant scientific community. In OT forensic practice, all four criteria are not documented to have been proved or routinely unmet: proprietary forensic tools are untestable by defendants; methodologies are not published or independently reviewed; error rates for AI-assisted detection tools on specific OT environments are undisclosed; and no general acceptance standard exists for OT-specific forensic tools. While the case scenarios in Section 6 include international incidents analyzed for their ethical dimensions, the Daubert evaluation applies specifically to OT forensic practice in U.S. federal proceedings; the ethical obligations it operationalizes are, however, generalizable across jurisdictions.

2.4. Research Gaps

Cook et al. [4] provide a comprehensive survey of ICS digital forensics to date and confirm live-system acquisition, evidence integrity, and proprietary protocol decoding as dominant challenges. However, there is no treatment of the ethics dimension. Ahmed et al. [10] provide a foundational examination of SCADA-specific forensic challenges. Fabro and Cornelius [16] offer practical guidance on creating forensic plans for control systems. Eden et al. [18] address forensic readiness for SCADA/ICS incident response. The NIST [5] in NISTIR 8428 provides the closest available OT-specific DFIR framework but similarly omits the ethics dimension. Jeong [23] and Stoykova [22] examine fairness and professional responsibility in forensic practice but in IT contexts only.

Table 1 demonstrates that the existing frameworks address either OT forensic procedures or ethical obligations independently. NISTIR 8428 and prior OT forensic studies provide valuable technical guidance but do not embed ethical governance within the investigative process. Conversely, professional ethics codes such as the IACIS and SWGDE provide ethical guidance but lack OT-specific investigative procedures. WISE-DF uniquely integrates OT-specific forensic processes, principlism-based ethical governance, process-phase mapping, and validation mechanisms within a single framework.

The gap is precise and confirmed: no published work integrates digital forensic methodology, OT/ICS security, and applied cyberethics into a water-sector-specific inves-

tigative framework. No prior publication provides: (a) a systematic taxonomy of ethical challenges that are unique to water SCADA forensic investigations; (b) a mapping of those challenges to the investigative process phases at which they arise; or (c) a structured investigative framework that embeds ethical safeguards as procedural requirements rather than advisory recommendations.

Table 1. Comparison of existing frameworks and WISE-DF. A ✓ indicates a dimension is addressed; × indicates it is not.

Framework	OT-Specific	Ethics	Process Mapping	Validation
NISTIR 8428 [5]	✓	×	×	✓
Cook et al. (2023) [4]	✓	×	×	✓
Ahmed et al. [10]	✓	×	×	✓
IACIS Code	×	✓	×	✓
SWGDE Code	×	✓	×	✓
WISE-DF	✓	✓	✓	✓

3. Research Methodology

This paper employs a four-stage qualitative research design appropriate for conceptual and framework-building research. No primary data collection, surveys, or practitioner interviews were conducted. However, to ground the framework in empirical forensic evidence, the study draws on a physical OT/ICS testbed comprising a Siemens S7-1200 1212C PLC programmed via TIA Portal v20, WinCC HMI integrated within TIA Portal, Factory IO water tank simulation software, and a managed switch enabling Profinet and Modbus TCP communication with port mirroring capability [24]. The testbed replicates the communication architecture and SCADA control logic of a water-sector OT environment and is used in Section 7 to validate the forensic artifact landscape defined by the WISE-DF framework. Full details of the testbed design, hardware configuration, and communication architecture are provided in [24].

3.1. Stage 1: Background Synthesis and Domain Scoping

Building on the literature reviewed in Section 2, three independently developed bodies of work were examined to characterize the research gap: the OT/ICS security and forensics literature [4,10,16,19]; the digital forensic methodology literature [3,14,15,17]; and the cyberethics and forensic ethics literature [6,20–22]. Inclusion criteria: peer-reviewed publications, government technical standards (NIST, EPA, and GAO), and professional codes (IACIS and SWGDE) that address at least one of the three domains. Exclusion criteria: vendor white papers without independent peer review; publications addressing only physical security without digital forensic components.

3.2. Stage 2: Ethical Framework Analysis

Drawing on principlism as originally formulated by Beauchamp and Childress [8], Spinello [6] adapted four cyberethics principles (non-maleficence, beneficence, justice, and autonomy) as the theoretical lens for analyzing how existing ethical obligations translate to OT investigative contexts. The six ethical challenges were derived through a two-step process. First, each principlism principle was examined against the documented technical constraints of OT forensics identified in Section 2, specifically live system operation, proprietary protocol dependency, and no-downtime mandates (Section 2.2), to identify where existing IT-oriented ethics codes fail to provide adequate guidance.

Second, the resulting obligation gaps were cross-referenced against the five case scenarios in Section 6 to confirm that each derived challenge manifests in documented practice. This process produced exactly six challenges. Each corresponds to a distinct ethical obligation that is either absent from or inadequately specified in existing IT forensic ethics codes when applied to OT environments. This constitutes contribution-by-application: established ethical theory is applied to a domain in which it had not previously been systematically deployed.

3.3. Stage 3: Forensic Process Mapping

The six ethical challenges derived in Stage 2 were mapped to the four-phase standard digital forensic process model (identification and scoping, preservation and acquisition, analysis and interpretation, and reporting and disclosure), as defined by Casey [3] [Chapter 3] and Carrier and Spafford [14], adapted to OT/ICS environments following the OT-specific DFIR framework structure in NISTIR 8428 Section 3 [5]. The mapping criterion was the phase at which each principlism principle first becomes the primary operative ethical obligation on the investigator. Each phase is assigned a dominant principle (autonomy at scoping; non-maleficence at acquisition; justice and transparency at analysis; justice and beneficence at reporting). This process-embedded approach, where ethics are located procedurally rather than discussed as advisory guidance, is the key structural contribution of Section 5 and the direct analytical precursor to the WISE-DF framework gates in Section 7.

3.4. Stage 4: Multi-Case Analysis of Documented Incidents

Five publicly documented real-world incidents were selected for case analysis. The selection criteria were: (a) public availability of sufficient incident detail to support ethical challenge analysis; (b) collective coverage of all six ethical challenges across the case set (no single case illustrates all six, but collectively the five cases illustrate all six); and (c) inclusion of primary water sector cases (S1 and S5) and OT analogue cases (S2, S3, and S4) that extend coverage to attribution, transparency, and geopolitical dimensions absent from water-only incidents. Each case was analyzed using the Section 4 ethical challenge taxonomy as the analytical lens, not as primary empirical research.

Three validation approaches are employed. Standards-alignment validation benchmarks each recommendation against NIST SP 800-82r3, NISTIR 8428, AWIA 2018, and EPA 2024 guidance. Counter-argument testing stress tests each recommendation against a practical objection with a rebuttal. Daubert-consistency evaluation assesses each WISE-DF phase gate against the four Daubert criteria [9], testability, peer review and publication, known error rate, and general acceptance, to determine whether WISE-DF compliance produces evidence that is capable of meeting the U.S. federal admissibility requirements. All three approaches explicitly acknowledge that practitioner validation has not yet been conducted.

4. Ethical Challenges in OT/ICS/SCADA Digital Forensics

The ethical challenges arising in SCADA system investigations within OT environments are both numerous and interconnected. The analytical principle of this paper is *process-embedded ethics*: each challenge is located at the specific forensic process stage where it first becomes operationally binding, making ethical obligations actionable rather than declarative. Building on the research workflow presented in Figure 1, the following section identifies the six ethical challenges.

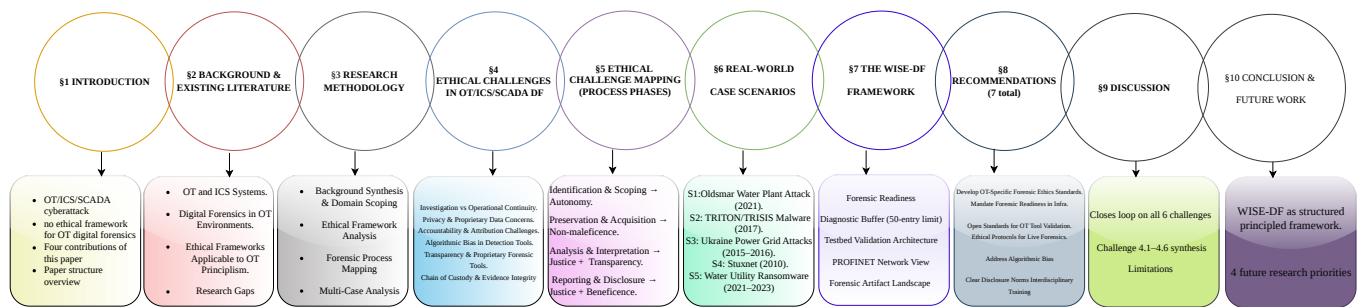


Figure 1. Research workflow illustrating the analytical chain from problem identification through literature synthesis, framework development, case analysis, and validated recommendations.

4.1. The Tension Between Investigation and Operational Continuity

The most fundamental ethical challenge in OT forensics is the tension between the investigator's duty to collect comprehensive evidence and the operator's legal obligation to maintain continuous system operations. In water treatment facilities, taking systems offline could interrupt potable water delivery, disable safety controls, or trigger cascading failures [1,5]. This reflects a direct conflict between beneficence, the duty to investigate criminal activity in the public interest, and non-maleficence, the duty to avoid harm caused by the investigation itself. The existing forensic standards provide no specific protocols for managing the risk of investigation-induced harm in safety-critical environments [15,25].

4.2. Privacy and Proprietary Data Concerns

Digital forensic investigations in OT environments inevitably involve the acquisition of operational data, process histories, sensor logs, control commands, and network traffic that organizations regard as commercially sensitive or security-critical. Detailed operational data, if disclosed through legal proceedings, could provide adversaries with a blueprint for future attacks. The principle of justice requires that forensic evidence be available to defendants for challenge [6,21], yet this transparency obligation may directly conflict with the imperative to protect sensitive infrastructure information.

4.3. Accountability and Attribution Challenges

Establishing accountability is a core purpose of digital forensic investigation. In OT environments, attribution is technically and ethically complex: attacks are frequently perpetrated by sophisticated threat actors, including nation states, who employ techniques specifically designed to obscure their identity [26,27]. Attribution decisions carry geopolitical consequences that extend far beyond the conventional scope of forensic investigation.

4.4. Algorithmic Bias in Automated Detection Tools

The increasing deployment of AI and machine learning tools for anomaly detection in OT environments introduces the risk of algorithmic bias, a concern documented in digital forensic contexts by Jinad et al. [28] and Sunde and Dror [29]. Systems trained on data from specific industrial configurations may perform poorly in different operational environments, generating disproportionate false positives or false negatives for certain facility types [30,31]. The ethical principle of justice demands that forensic tools perform equitably across the full spectrum of facilities they investigate [32,33].

4.5. Transparency and the Use of Proprietary Forensic Tools

A recurring ethical concern in digital forensics is the use of closed-source proprietary forensic tools whose algorithmic logic is not subject to independent scrutiny [21]. When evidence derived from such tools is introduced in legal proceedings, the inability of defen-

dants or independent experts to examine and challenge the methodology undermines the fundamental right to a fair trial [22,33]. The ethical obligation of transparency is difficult to fulfill when investigators themselves may not have access to the source code of the tools they employ [20].

4.6. Chain of Custody and Evidence Integrity

Maintaining an unbroken chain of custody is a foundational requirement of digital forensics and a prerequisite for legal admissibility [3,14]. Live forensic collection from a running PLC or SCADA HMI necessarily involves interaction with the system, raising questions about whether evidence has been altered by the collection process itself [5,15]. Investigators have an ethical obligation to clearly communicate this uncertainty to legal authorities rather than presenting findings with unwarranted confidence. The tendency toward a “technological infallibility fallacy”, the unwarranted assumption that digital evidence is inherently more reliable than other evidence forms, is a recognized source of injustice in digital forensics [28,34].

The six challenges identified, operational continuity, proprietary data, attribution, algorithmic bias, transparency, and chain of custody, are not independent phenomena. They interact and compound one another in practice, as the case analyses in Section 6 demonstrate directly.

5. Ethical Challenge Mapping Within the OT Forensic Process

The six ethical challenges identified in Section 4 do not arise uniformly across an investigation. Rather, they emerge at specific identifiable stages of the forensic process. This section maps each principlism principle and its corresponding challenge to the investigative phase at which it becomes operationally binding. The mapping adapts the standard four-phase digital forensic process model as defined by Casey [3] and Carrier and Spafford [14] to OT/ICS/SCADA environments following the OT-specific DFIR framework structure specified in NISTIR 8428 Section 3 [5]. Table 2 summarizes the integrated mapping.

Table 2. Ethical principle-to-forensic phase mapping in OT/ICS/SCADA environments.

Forensic Phase	Principlism Principle	Challenges	Core Tension
Identification & Scoping	Autonomy	4.1, 4.2	Evidence boundaries must be defined without disrupting active control processes or exposing sensitive operational data.
Preservation & Acquisition	Non-maleficence	4.6, 4.1	Any live forensic action on a water control system risks process disruption and potential public harm.
Analysis & Interpretation	Justice + Transparency	4.4, 4.5	Algorithmic bias in forensic tools and opacity of proprietary vendor software produce inequitable and unverifiable outcomes.
Reporting & Disclosure	Justice + Beneficence	4.2, 4.3	Attribution complexity and regulatory disclosure obligations create accountability challenges requiring balanced ethical judgment.

5.1. Identification and Scoping: Autonomy

The initial forensic phase is the point at which the principle of autonomy is most directly implicated. Autonomy, as articulated by Beauchamp and Childress [8] and applied to computing by Spinello [6], requires respect for individual rights and informed consent, including the right of system operators and affected parties to maintain appropriate control over their systems and data. Investigators must determine the scope of the investigation without disrupting

active control processes and without treating the facility as an unrestricted evidence repository simply because legal authority to investigate exists. Challenge 4.1 (operational continuity) and Challenge 4.2 (proprietary data) collide at this phase: over-scoping violates autonomy by exposing sensitive operational data beyond what the investigation requires; under-scoping violates beneficence by compromising evidentiary completeness. Investigators must document scoping decisions and the rationale behind them with full transparency [17,25].

5.2. Preservation and Acquisition: Non-Maleficence

Non-maleficence, the duty to avoid harm, is the dominant ethical principle at the preservation and acquisition phase. As Spinello (Chapter 2 of [6]) establishes, non-maleficence requires not merely passive avoidance of harm but active assessment of whether a proposed action poses foreseeable harm to others. Any live forensic action on an operational control system risks process disruption that can translate directly into public harm [1,5]. The ethical obligation at this phase is therefore double: investigators must minimize the risk of operational harm (non-maleficence toward the public) and disclose transparently any uncertainty introduced by live acquisition to legal authorities (non-maleficence toward the justice process). Forensic readiness planning directly reduces the non-maleficence tension by enabling less intrusive post-incident acquisition [17,18].

5.3. Analysis and Interpretation: Justice and Transparency

The analysis phase is where two ethical principles operate concurrently. Justice (Chapter 2 of [6]) requires fair and equitable treatment of all parties investigated, including equitable performance of the tools used to investigate them. Transparency requires that investigators disclose the methods, tools, and limitations of their analysis so that findings can be independently challenged. Challenge 4.4 (algorithmic bias) arises because systems trained on data from large or well-instrumented industrial facilities perform poorly when applied to smaller less standardized water utilities [30,32]. Challenge 4.5 (transparency) arises because the opacity of proprietary vendor software prevents defendants and their experts from examining and challenging the methodology [21,22]. Both challenges must be addressed together: a tool that performs equitably but is opaque fails transparency; a tool that is transparent but performs inequitably fails justice. NISTIR 8428 Section 3 does not address these concerns, which is precisely the governance gap this paper addresses.

5.4. Reporting and Disclosure: Justice and Beneficence

The reporting phase engages both justice and beneficence in tension with each other and with the security obligations unique to critical infrastructure forensics. Beneficence is the obligation to act in the public good (p. 71 of [6]) and requires that forensic findings be disclosed to regulatory authorities, peer operators, and the public in ways that enable sector-wide learning. Justice requires that evidence be disclosed to defendants and their counsel for challenge. These two obligations are in tension when technical details of a forensic investigation, if fully disclosed, could provide adversaries with a blueprint for future attacks. Challenge 4.3 (attribution) intensifies the justice concern: attribution findings in nation-state OT attacks carry geopolitical consequences that extend far beyond the immediate case [26,27]. The WISE-DF Phase 5 four-tier disclosure matrix in Section 7 is designed specifically to govern the reporting phase obligations.

6. Real-World Case Scenarios

The following five case scenarios apply the ethical challenge taxonomy developed in Section 4 to publicly documented real-world incidents. Cases were selected according to the three criteria described in Section 3. Table 3 provides an overview; Table 4 provides

the challenge coverage matrix confirming that all six challenges are collectively illustrated across the case set.

Table 3. Case scenarios and primary ethical challenges.

Case	Incident	Primary Ethical Challenges
S1	Oldsmar Water Plant Attack (2021)	4.1 Operational continuity; 4.6 Chain of custody; 4.2 Proprietary data
S2	TRITON/TRISIS Malware (2017)	4.3 Attribution; 4.2 Proprietary data; 4.5 Transparency
S3	Ukraine Power Grid Attacks (2015–2016)	4.5 Transparency; 4.3 Attribution; 4.2 Proprietary data
S4	Stuxnet (2010)	4.3 Attribution; 4.1 Non-maleficence; 4.5 Transparency
S5	Water Utility Ransomware (2021–2023)	4.4 Algorithmic bias; 4.2 Privacy; 4.1 Operational continuity

Table 4. Six-challenge coverage matrix across five case scenarios.

Case	4.1	4.2	4.3	4.4	4.5	4.6
S1	✓	✓	×	×	×	✓
S2	×	✓	✓	×	✓	×
S3	×	✓	✓	×	✓	×
S4	✓	×	✓	×	✓	×
S5	✓	✓	×	✓	×	×
Total	3	4	3	1	3	1

6.1. Scenario 1: The Oldsmar Water Plant Attack (2021)

In February 2021, an unidentified threat actor gained remote access to the SCADA system of the Oldsmar, Florida, water treatment plant and increased the sodium hydroxide setpoint from approximately 111 ppm to 11,100 ppm, a level that could have caused serious harm to approximately 15,000 residents had a plant operator not detected and reversed the change in real time [11,12].

Challenge 4.1 (operational continuity): investigators faced the dilemma of conducting a thorough digital investigation while the plant continued to serve the public. Challenge 4.6 (chain of custody): live forensic methods were required with attendant risks to evidence integrity, and the facility’s TeamViewer software, the likely attack vector, had not been configured to generate audit logs [17,18], leaving an irrecoverably incomplete evidential record. Oldsmar is the foundational case for the WISE-DF framework’s Phase 1 forensic readiness gate.

6.2. Scenario 2: TRITON/TRISIS Malware (2017)

In 2017, investigators at a Middle Eastern petrochemical facility discovered a malware framework specifically engineered to manipulate Triconex Safety Instrumented Systems (SIS) [26]. The malware could reprogram SIS controllers to fail in an unsafe state, potentially causing explosions or toxic releases. Challenge 4.3 (attribution) and Challenge 4.5 (transparency) were most acute: forensic findings were closely held by the affected organization and its cybersecurity contractor, and the opacity of private-sector methodologies meant that attribution findings, however accurate, could not be independently verified [27].

6.3. Scenario 3: Ukraine Power Grid Attacks (2015–2016)

Coordinated cyberattacks on Ukrainian power distribution companies in December 2015 and 2016 resulted in widespread power outages affecting hundreds of thousands of civilians [35]. Much of the forensic analysis was conducted by private cybersecurity firms whose methodologies were not fully disclosed, making independent verification difficult [21,22]. This case is the clearest illustration of Challenge 4.5 (transparency): when

investigators cannot disclose their methods, attribution findings lose legal and geopolitical acceptance regardless of their precision.

6.4. Scenario 4: Stuxnet (2010)

The Stuxnet worm was widely attributed to a joint United States–Israeli intelligence operation, which represents the first publicly known cyberweapon specifically designed to cause physical destruction to industrial infrastructure [27,35]. Challenge 4.5: the ethics of publicly disclosing the capabilities of an active cyberweapon were not resolved before disclosure occurred. Challenge 4.1: detailed public disclosure provided a blueprint for future attacks by threat actors who lacked the original developers' sophistication [6], a direct example of investigation-related harm. Stuxnet and TRITON together demonstrate that excessive secrecy (TRITON) and over-disclosure (Stuxnet) are opposite failure modes that the WISE-DF Phase 5 disclosure matrix is specifically designed to mediate.

6.5. Scenario 5: Water Utility Ransomware Incidents (2021–2023)

Between 2021 and 2023, multiple U.S. water utilities were targeted by ransomware attacks that encrypted operational systems and threatened to release sensitive infrastructure data [7,12]. Challenge 4.4 (algorithmic bias) was most directly illustrated: automated detection tools trained primarily on large industrial facility data demonstrated elevated false positive rates when applied to smaller utilities' less standardized operational environments [30,32]. Legitimate operational behaviors were flagged as potentially malicious, leading to unnecessary investigative scrutiny of utility staff.

7. The WISE-DF Framework

The six ethical challenges documented in Section 4 and validated through the case analysis in Section 6 share a structural feature: they cannot be resolved through isolated policy recommendations appended to an otherwise technical investigation. These interdependencies confirm that a framework approach is required, one in which ethical safeguards are embedded as procedural requirements throughout the investigation, not treated as advisory guidance.

This paper proposes the Water ICS SCADA Ethical Digital Forensics (WISE-DF) framework: a six-phase principle-grounded model for digital forensic investigations of water and wastewater OT environments. The defining structural innovation of WISE-DF is that ethical safeguards function as mandatory procedural gates: investigators must satisfy the ethical obligations of each phase before advancing to the next. This distinguishes WISE-DF from all prior frameworks, including NISTIR 8428 [5], which provide technical guidance without embedding ethical constraints as investigative prerequisites.

A clarification of the relationship between Table 2 and the WISE-DF framework is that Table 2 is a diagnostic mapping that identifies *where* each ethical challenge first becomes operationally binding within the standard four-phase digital forensic process. The WISE-DF framework is an operational governance architecture that specifies *how* those challenges will be addressed through mandatory procedural gates. WISE-DF extends beyond the standard four-phase model in three specific ways. First, Phase 1 (forensic readiness) operates entirely *before* any incident occurs and therefore falls outside the standard forensic process altogether; its absence, as the Oldsmar case demonstrates, structurally constrains every subsequent phase. Second, preservation and acquisition are split into two separate phases (Phase 2 and Phase 3) because safety obligations (Challenge 4.1) and chain-of-custody obligations (Challenge 4.6) are ethically distinct and require independent gates; combining them would allow one obligation to be satisfied at the expense of the other. Third, Phase 6 (post-incident review) operates entirely *after* the investigation concludes; it

is absent from all the prior OT forensic frameworks and is motivated by our finding that no structured sector-wide learning mechanism existed in any of the five case scenarios. The six-phase structure is therefore not a duplication of the four-phase mapping but a governance extension of it: two additional phases outside the standard process, one phase split into two, and mandatory gates replacing advisory observations at every stage.

Table 5 shows that, while NIST NISTIR 8428 covers basic OT forensic phases, the WISE-DF framework extends it by adding comprehensive ethical, legal, and accountability features, such as mandatory ethics gates, bias checks, disclosure controls, and structured post-incident review.

Table 5. WISE-DF framework vs. NISTIR 8428: feature comparison. A ✓ indicates the feature is present; × indicates it is absent.

Feature	NISTIR 8428	WISE-DF
OT-specific forensic phases	✓	✓
Ethics dimension addressed	×	✓
Mandatory ethical gates	×	✓
Principlism principle mapping	×	✓
Daubert-consistency evaluation	×	✓
Algorithmic bias requirements	×	✓
Four-tier disclosure matrix	×	✓
Forensic readiness as mandatory pre-condition	×	✓
Post-incident review obligation	×	✓

7.1. Phase 1: Forensic Readiness

Forensic readiness addresses Challenge 4.6 before any incident occurs. Prior to any investigation, utilities must establish: mandatory pre-incident configuration of key log sources; a documented tool inventory specifying the validation status of each forensic tool; and a scoping protocol that defines proportionality limits for evidence collection. Forensic readiness is the only WISE-DF phase that can be completed before an incident occurs, and its absence, as demonstrated in Scenario 1, directly constrains every subsequent investigation phase. **Ethical gate:** The utility must demonstrate that mandatory logging is operational and that a documented scoping protocol exists before any incident response begins. The absence of pre-incident readiness must be disclosed to legal authorities as a structural limitation of the subsequent investigation.

The criticality of Phase 1 is concretely illustrated by the forensic characteristics of the Siemens S7-1200 1212C PLC used in our physical SCADA testbed (integrating TIA Portal v20, WinCC HMI, Factory IO water tank simulation, and a managed switch supporting Profinet and Modbus TCP). The S7-1200 1212C CPU stores all diagnostic events in a fixed capacity of 50 entries. Without pre-incident external diagnostic event forwarding, for example, syslog export via the managed switch SPAN port, the forensic evidence of an attack is architecturally ephemeral: it cannot be recovered post-stabilization regardless of investigator skill.

Figure 2 confirms this constraint empirically; the diagnostic buffer of the testbed S7-1200 1212C records a maximum of 50 events in a circular overwrite structure, meaning that, in an active attack scenario generating sustained diagnostic activity, pre-attack baseline events are overwritten within minutes, permanently eliminating recoverable forensic evidence regardless of investigator skill or tool sophistication.

The TIA Portal v20 project archive (.ap20) provides a second concrete example: this file contains the complete ladder logic program, WinCC HMI configuration, hardware network topology, and version history of the testbed. It is simultaneously the primary artifact for establishing pre-attack configuration integrity (Section 7.2) and the most sensitive artifact under Challenge 4.2 because full disclosure in legal proceedings would expose the complete operational design of the facility.

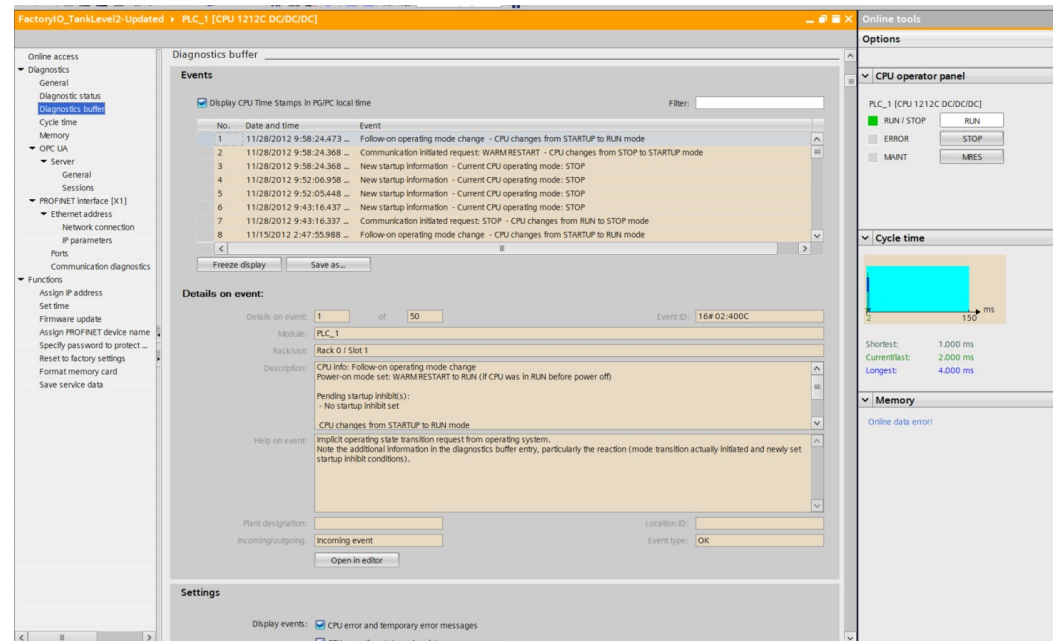


Figure 2. TIA Portal v20 online diagnostic buffer of the Siemens S7-1200 1212C CPU (PLC_1), showing eight timestamped operational mode-change events. The panel confirms a fixed capacity of 50 entries (“Details on event: 1 of 50”), after which the oldest entries are overwritten in circular fashion. Forensic events occurring before the 50-entry threshold is reached are permanently lost without pre-incident external log forwarding, directly illustrating the architectural ephemerality constraint that motivates the WISE-DF Phase 1 forensic readiness gate.

7.2. Phase 2: Preservation and Acquisition

Evidence preservation mandates live forensics with read-only tools, hash verification of all acquired data at the point of collection, and dual-witness documentation of every system interaction.

Ethical gate: Before collection begins, investigators must confirm that read-only collection tools are available, establish a hash verification protocol, and identify a second qualified witness for all system interactions. No collection may begin without this documentation baseline.

7.3. Phase 3: Safety-First Collection

The safety-first gate is the non-maleficence gate addressing Challenge 4.1. Before any collection action begins, investigators must conduct a written operational risk assessment identifying: the minimum operational safeguards that must remain active during collection; the specific conditions under which collection will be immediately suspended to protect public safety; and the alternative evidence sources that can be pursued if direct system interaction poses unacceptable risk.

Ethical gate: Collection does not begin until a written risk assessment is complete and approved by the facility’s operational authority. Safety suspension triggers must be defined and agreed before any investigative tool is connected to the OT network.

7.4. Phase 4: Analysis and Tool Validation

Every AI-assisted forensic tool must undergo pre-deployment bias assessment using explainable AI (XAI) techniques before its outputs are used in the investigation. An attribution confidence matrix specifying the strength of evidence required to support each level of attribution finding governs what conclusions the available evidence can warrant.

Ethical gate: No AI-assisted finding may be presented in a forensic report without accompanying documentation of the tool's bias assessment and a clear statement of the confidence level warranted by the evidence. Closed-source tools must be flagged as subject to transparency limitations affecting their legal admissibility.

The Phase 4 gate requirements map directly onto the four Daubert admissibility criteria [9]. Testability: every forensic tool must have been tested against a dataset representative of the facility type under investigation; untested tools fail Daubert criterion 1 and must be disclosed as such. Peer review and publication: tools whose methodology has not been independently reviewed and published fail Daubert criterion 2. Known or potential error rate: AI-assisted tools must disclose their false positive and false negative rates for the specific operational environment; tools with undisclosed error rates fail Daubert criterion 3, directly grounding the algorithmic bias concerns of Challenge 4.4. General acceptance: tools not accepted within the OT forensic scientific community fail Daubert criterion 4, directly grounding the transparency concerns of Challenge 4.5.

7.5. Phase 5: Ethical Disclosure

Forensic findings are disclosed through a four-tier framework: (1) mandatory regulatory disclosure to the EPA and CISA under the AWIA; (2) voluntary peer disclosure through the WaterISAC or equivalent information-sharing mechanisms; (3) controlled disclosure in legal proceedings, subject to appropriate protective orders; and (4) public disclosure, governed by norms that distinguish between information necessary for sector-wide learning and technical details that could function as attack blueprints.

Ethical gate: Before any external disclosure is made, investigators must apply the four-tier matrix to determine the appropriate scope and level of technical detail for each audience. Investigators may not default to full disclosure or complete secrecy without this documented analysis.

7.6. Phase 6: Post-Incident Review

Following each investigation, a structured debrief updates the forensic readiness protocols, tool inventory, and scoping procedures for the next investigation cycle. Phase 6 closes the loop back to Phase 1, ensuring that each investigation strengthens the ethical and evidentiary foundation for future investigations.

Ethical gate: Post-incident review is a mandatory deliverable of every investigation. Its findings must be shared through at least the regulatory disclosure tier. Failure to complete the post-incident review means that the Phase 1 in readiness for the next investigation will not be better than the current.

Table 6 maps each phase of the WISE-DF framework to the specific ethical challenges and real-world cases, showing how failures at each stage (from readiness to post-incident review) led to issues such as poor evidence handling, unsafe operations, unvalidated tools, and ineffective knowledge sharing across incidents.

Table 6. WISE-DF phase-to-challenge traceability matrix.

Phase	Name	Challenges	Case Grounding
1	Forensic Readiness	4.1, 4.6	S1: absent readiness constrained all evidence
2	Preservation & Acquisition	4.6	S1, S5: live collection without dual-witness or hash verification
3	Safety-First Collection	4.1	S1: no safety gate before live forensics on active plant
4	Analysis & Tool Validation	4.4, 4.5	S3, S5: unvalidated AI tools; opaque private methodologies
5	Ethical Disclosure	4.2, 4.3	S2, S4: opposite failure modes: secrecy vs. over-disclosure
6	Post-Incident Review	All	All cases: no structured sector learning mechanism existed

7.7. Forensic Artifact Landscape: WISE-DF Testbed Validation Architecture

The empirical testbed research was conducted on a physical OT/ICS testbed comprising a Siemens S7-1200 1212C PLC programmed via TIA Portal v20, WinCC HMI integrated within TIA Portal, Factory IO water tank simulation software, and a managed switch enabling Profinet and Modbus TCP communication with port mirroring capability. The testbed replicates the communication architecture and SCADA control logic of a water-sector OT environment [24]. The forensic artifact landscape documented in Table 7 is derived from direct examination of this testbed environment; full hardware and communication architecture details are provided in [24].

Figure 3 illustrates the PROFINET network topology connecting the S7-1200 PLC to the WinCC RT Advanced HMI, establishing the physical and logical boundaries within which forensic artifacts are generated and collected.

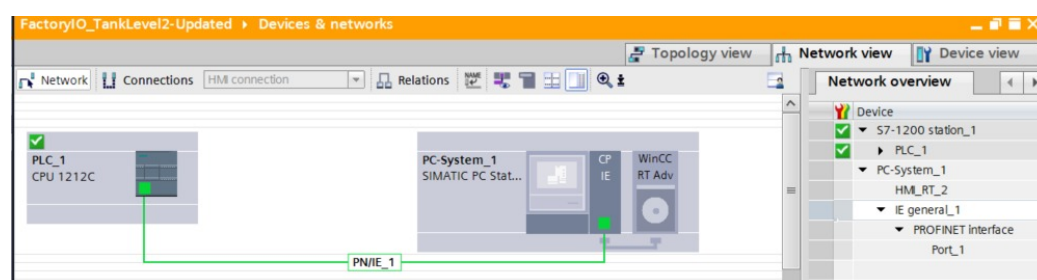


Figure 3. TIA Portal v20 network view showing the PROFINET connection (PN/IE_1) between the Siemens S7-1200 1212C PLC (PLC_1, CPU 1212C) and the WinCC RT Advanced HMI (PC-System_1). This network topology defines the communication boundary within which Modbus TCP and PROFINET forensic artifacts are generated and establishes the managed switch SPAN port capture point required by the WISE-DF Phase 1 forensic readiness gate and Phase 2 acquisition protocol.

Figure 4 presents the TIA Portal v20 project structure and the Main [OB1] ladder logic program. The project tree confirms the full artifact inventory of the testbed: PLC program blocks, Modbus TCP tag data blocks (DB_HR_RAW, DB_Modbus_Conn, DB_Valve_OUT, and TankControl), tag tables, OPC UA configuration, and version history. The ladder logic shows the MB_CLIENT Modbus TCP communication block and the tank-level raw-value conversion network, both of which generate the process-variable artifacts subject to WISE-DF Phase 2 acquisition and Phase 4 analysis. The TIA Portal v20 project archive (.ap20) containing this complete program simultaneously constitutes the primary artifact for establishing pre-attack configuration integrity and the most sensitive artifact under Challenge 4.2 because full disclosure in legal proceedings would expose the complete operational design of the facility.

Figure 5 shows the WinCC RT Advanced HMI runtime screen during testbed operation. The screen displays the water tank level (5.8 units), flow meter gauge reading, process setpoint and timescale controls, and two active alarm indicators (Alarm_SetpointJump, shown active in red; Alarm_TimeScaleJump). These alarm log entries, historian process-variable time series, and event logs constitute the persistent HMI artifacts subject to WISE-

DF Phase 2 acquisition. The active alarm state visible in the screenshot represents precisely the category of forensic artifact that would be prioritized in a post-incident investigation of anomalous setpoint manipulation, directly analogous to the sodium hydroxide setpoint attack in the Oldsmar scenario (Section 6).

Table 7 summarizes all the key forensic artifacts across the S7-1200/TIA Portal/WinCC/Factory IO/Modbus testbed, showing where evidence resides, how volatile it is, and how each artifact maps to WISE-DF phases and ethical challenges, including chain of custody, safety, privacy, and transparency. This preliminary framework is presented as a research design contribution specifying what evidence categories exist, under what ethical constraints each must be collected, and what the empirical work will measure rather than as completed findings.

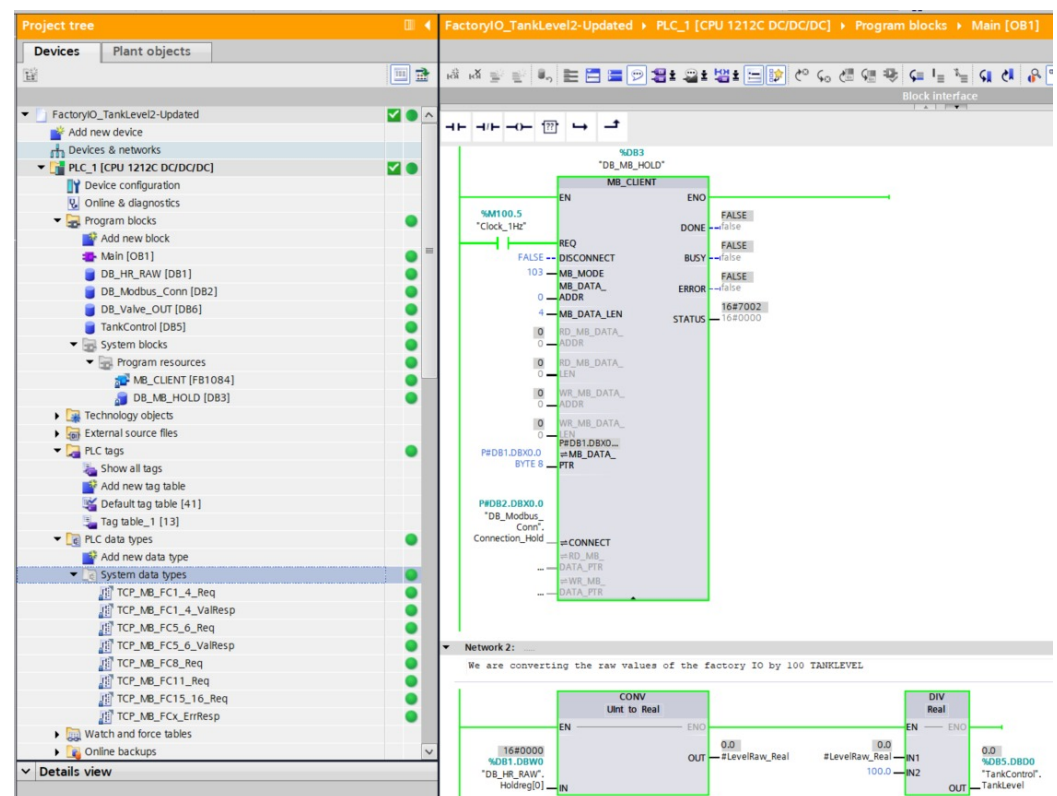


Figure 4. TIA Portal v20 project tree (left) and Main [OB1] ladder logic (right) for the Siemens S7-1200 1212C testbed. The project tree shows the complete artifact inventory, including program blocks, Modbus TCP data blocks (DB_HR_RAW [DB1], DB_Modbus_Conn [DB2], DB_Valve_OUT [DB6], and TankControl [DB5]), PLC tag tables, and OPC UA server configuration. The ladder logic displays the MB_CLIENT Modbus TCP communication block (Network 1) and the tank-level UINT-to-Real conversion network (Network 2). The project archive (.ap20) constitutes the primary forensic artifact for establishing pre-attack configuration integrity under WISE-DF Phase 1 and the most sensitive disclosure artifact under Challenge 4.2.

Table 7. Forensic artifact landscape: S7-1200 1212C/TIA Portal v20/WinCC/Factory IO/Modbus TCP Testbed.

Layer	Component	Artifact Category	Volatility	WISE-DF Phase	Primary Challenge
Field device	S7-1200 1212C CPU	Diagnostic buffer with circular overwrite	Ephemeral; overwritten during stabilization	Ph.1 Readiness; Ph.2 Acquisition	4.6 Chain of custody; 4.1 Operational Continuity

Table 7. Cont.

Layer	Component	Artifact Category	Volatility	WISE-DF Phase	Primary Challenge
Field device	S7-1200 1212C CPU	DB contents, holding registers, I/O states, retentive memory	Semi-volatile; retentive DBs survive power cycle	Ph.2 Acquisition; Ph.3 Safety gate	4.6 Chain of custody; 4.1 Operational Continuity
Engineering WS	TIA Portal v20	Project archive, ladder logic, HMI configuration, topology, version history	Persistent on engineering workstation	Ph.1 Readiness; Ph.5 Disclosure	4.2 Privacy/proprietary data; 4.5 Transparency
SCADA/HMI	WinCC	Alarm logs, event logs, historian data, and process-variable time series	Persistent; retention configurable	Ph.2 Acquisition; Ph.4 Analysis	4.2 Privacy; 4.4 Algorithmic bias
Simulation	Factory IO	Scene file and tag-value history for process-state validation	Persistent	Ph.4 Tool validation; Ph.6 Review	4.5 Transparency
Network	Managed switch/SPAN	Profinet, S7comm, and Modbus TCP packet captures	Ephemeral; requires active SPAN configuration	Ph.1 Readiness; Ph.2 Acquisition	4.5 Transparency; 4.6 Chain of custody
Network	Managed switch	ARP table, MAC table, VLAN configuration, and syslog	Semi-persistent; depends on retention configuration	Ph.1 Readiness; Ph.2 Acquisition	4.6 Chain of custody

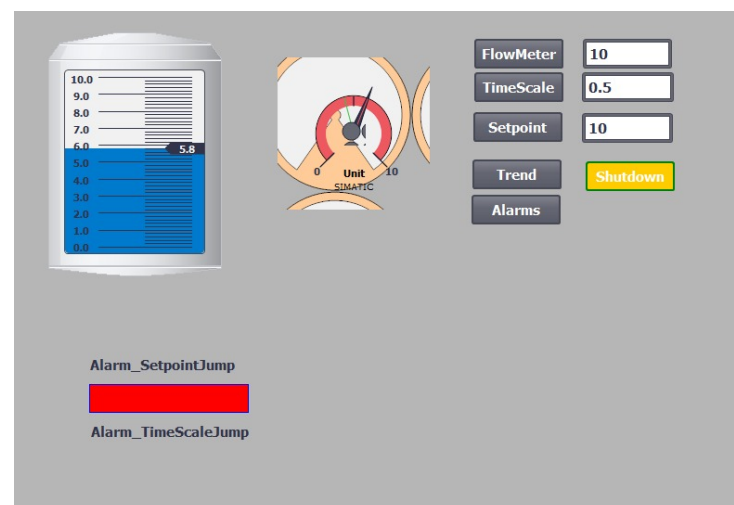


Figure 5. WinCC RT Advanced HMI runtime screen of the water tank testbed, displaying tank level (5.8 units), flow meter gauge, process setpoint (10) and timescale (0.5) controls, and active alarm state (Alarm_SetpointJump, red indicator). The alarm log, historian data, and process-variable time series generated by this HMI constitute persistent forensic artifacts subject to WISE-DF Phase 2 acquisition constraints. The active setpoint alarm illustrated here is forensically analogous to the anomalous sodium hydroxide setpoint manipulation recorded in the Oldsmar Water Plant attack (Scenario S1, Section 6).

8. Recommendations for Ethical OT Digital Forensic Practice

The ethical challenges identified in the previous sections call for a comprehensive multi-layered response from forensic practitioners, critical infrastructure operators, technology vendors, and policymakers. Table 8 maps each recommendation to its relevant scenarios, ethical challenges, and key standards.

Table 8. Summary of recommendations, challenges, and standards.

Rec.	Scenarios	Primary Challenge	Key Standard/Framework	Counter-Argument Addressed
8.1	2, 3	4.3 Attribution; 4.5 Transparency	Spinello [6]; Hughes & Karabiyik [20]	Voluntary uptake → regulatory linkage
8.2	1, 5	4.1 Continuity; 4.6 Chain of custody	AWIA 2018; EPA 2024; Rowlingson [17]	Resource constraints → phased tiers
8.3	3, 5	4.5 Transparency; 4.4 Bias	NIST CFTT; Horsman [21]; Goodman & Flaxman [33]	Dataset complexity → federated corpus
8.4	1	4.6 Chain of custody; 4.1 Continuity	NISTIR 8428; Luttgens et al. [15]	Protocol rigidity → principle-based approach
8.5	5	4.4 Algorithmic bias	Mubarak et al. [30]; Solanke [36]	Data scarcity → regulatory incentives
8.6	2, 4	4.3 Attribution; 4.2 Proprietary data	WaterISAC; ICS-CERT; EPA 2024	Security conflicts → tiered safe harbor
8.7	2, 4, 5	All six challenges	CISA training; Cook et al. [4]	Cost barriers → integrate existing programs

8.1. Develop OT-Specific Forensic Ethics Standards

The existing frameworks provide technical guidance but do not address the ethical dimensions of forensic practice in safety-critical environments. Professional bodies, including the IACIS, SWGDE, and sector organizations such as the WaterISAC, should collaborate to develop an OT Forensic Ethics Code drawing on Spinello [6] and the measurement-science approach of Hughes and Karabiyik [20]. *Case grounding:* Scenarios 2 and 3 demonstrated that investigators lacked professional norms that govern the disclosure scope for nation-state findings. *Counter-argument:* Standards-setting is slow, and voluntary uptake is uncertain. *Response:* Regulatory mandates under the AWIA and CISA frameworks can require compliance as a condition of federal grant eligibility.

8.2. Mandate Forensic Readiness in Critical Infrastructure

Forensic readiness obligations should be integrated into the cybersecurity requirements of the AWIA and EPA Cybersecurity Guidance, specifying minimum standards for industrial network logging, historian data retention, and documentation of system configurations [15,17]. *Case grounding:* Scenario 1 demonstrated that absent audit logging left an irrecoverably incomplete evidential record. *Counter-argument:* Small utilities lack resources. *Response:* A phased compliance framework tiered by utility size allows larger utilities to implement immediately while providing smaller utilities with roadmaps and federal funding mechanisms.

8.3. Establish Open Standards for OT Forensic Tool Validation

An OT-specific tool validation program analogous to the NIST's CFTT program should test tools used in ICS/SCADA investigations against standardized datasets representing the full diversity of industrial environments [21,33]. *Case grounding:* Scenarios 3 and 5. *Counter-argument:* Creating standardized OT forensic datasets is technically complex. *Response:* A federated approach with vendors contributing anonymized data to a shared validation corpus under the NIST NCCoE addresses both proprietary concerns and representativeness limitations.

8.4. Implement Ethical Protocols for Live Forensics in Safety-Critical Systems

Standardized ethical protocols must specify the minimum operational safeguards required before live collection begins, addressing chain-of-custody challenges through hash verification, dual-witness documentation, and read-only collection tools [15,18]. *Case ground-*

ing: Scenario 1. *Counter-argument*: Protocols may be too rigid for diverse OT environments. *Response*: A principle-based protocol specifying required outcomes rather than prescriptive procedures provides flexibility while maintaining ethical and evidentiary standards.

8.5. Address Algorithmic Bias Through Diverse Datasets and Explainability Requirements

Tool developers should demonstrate that their models have been trained and validated on datasets representing the full diversity of OT environments. XAI techniques [31] should be required as part of the validation process for AI-assisted forensic tools. *Case grounding*: Scenario 5. *Counter-argument*: Achieving dataset diversity is difficult. *Response*: Regulatory incentives, including liability protections and federal funding eligibility, can overcome structural disincentives to data sharing.

8.6. Develop Clear Disclosure Norms for Critical Infrastructure Forensic Findings

Sector-specific norms should govern when and how forensic findings are shared, distinguishing between: mandatory regulatory disclosure; voluntary peer disclosure through the WaterISAC or ICS-CERT; disclosure in legal proceedings; and public disclosure [6,22]. *Case grounding*: Scenarios 2 and 4. *Counter-argument*: Sector-specific norms may conflict with national security classifications. *Response*: A tiered disclosure framework can establish safe harbor provisions while ensuring minimum sector-wide learning.

8.7. Promote Interdisciplinary Training for OT Forensic Investigators

Interdisciplinary training curricula combining technical digital forensics, ICS/SCADA system knowledge, and applied ethics should use case-based learning from documented incidents. *Case grounding*: Scenarios 2, 4, and 5. *Counter-argument*: Interdisciplinary training is resource-intensive. *Response*: Integrating OT forensic ethics training into existing CISA and WaterISAC programs maximizes reach without requiring independent investment.

9. Discussion

This paper has presented the first systematic analysis of ethical challenges arising in digital forensic investigations conducted within OT/ICS/SCADA environments. The following discussion closes the loop on each of the six ethical challenges.

Challenge 4.1: Operational Continuity. WISE-DF Phases 1 and 3 together address this tension: pre-incident readiness reduces the forensic burden, and the safety gate establishes mandatory safeguards before live collection begins. The core ethical tension cannot be entirely resolved by technical protocols in OT environments, the principle of non-maleficence may legitimately constrain the investigative process, and evidence collected under safety constraints may be structurally incomplete. This must be acknowledged as a professional norm, not as a limitation.

Challenge 4.2: Privacy and Proprietary Data. WISE-DF Phase 5 provides the structural architecture to navigate competing disclosure obligations simultaneously. The unresolved governance gap (no legally binding mechanism currently compels water utilities to share forensic findings with peer operators) represents the most significant structural limitation of the current regulatory framework.

Challenge 4.3: Attribution and Accountability. The legal frameworks governing digital evidence were designed for criminal proceedings between individuals and organizations, not for incidents involving state actors and classified counterparts. The development of specialized legal frameworks for critical infrastructure forensic findings, analogous to classified evidence provisions in national security proceedings, represents an urgent direction for future legislative work.

Challenge 4.4: Algorithmic Bias. The water utilities that are the most likely to face algorithmic bias in forensic investigations are precisely the smallest and most under-

resourced utilities that are simultaneously the most vulnerable to attack and least likely to contest investigative outcomes in legal proceedings. This creates a systematic justice deficit that individual bias mitigation recommendations cannot fully resolve.

Challenge 4.5: Transparency and Proprietary Tools. A forensic conclusion supported by an unverifiable method is not merely less persuasive: it fails Daubert criterion 2 (peer review and publication) and criterion 4 (general acceptance), rendering it potentially inadmissible in U.S. federal proceedings. The current OT forensic practice, which routinely relies on closed-source tools with no published methodology, is not merely ethically deficient; it produces evidence that is legally vulnerable to a Daubert challenge in every federal proceeding where it is introduced.

Challenge 4.6: Chain of Custody. The chain-of-custody challenge is, in important respects, a downstream consequence of the forensic readiness failure identified in Challenge 4.1. Under Daubert criterion 1, testability, the acquisition methodology must be capable of being tested for reliability; a live forensic acquisition conducted without a documented repeatable protocol on a running system that simultaneously modifies state cannot satisfy this criterion. Stoykova's [22] principle maps precisely onto Daubert criterion 3, which requires disclosure of known or potential error rates.

Limitations

Several limitations of the present study are acknowledged. The case scenarios were selected for their illustrative value and public availability; the full universe of ethical challenges in OT forensics is broader, and many significant incidents remain confidential for national security or commercial reasons, introducing a public-availability bias. The recommendations are necessarily general and will require elaboration as they are applied to specific sectors, jurisdictions, and organizational contexts. This study does not include primary empirical data, such as surveys of forensic practitioners or interviews with critical infrastructure operators, which would substantially strengthen the evidentiary basis for the recommendations. The WISE-DF framework is grounded in ethical theory, literature review, and case analysis; it has not yet been tested with practitioners or applied to a live investigation. Standards-alignment validation confirms regulatory consistency but does not constitute empirical validation of the framework's practical effectiveness. All of these limitations are explicit priorities for future research.

10. Conclusions and Future Work

The WISE-DF framework represents a structured principle-grounded investigation model for OT/ICS/SCADA digital forensics, one in which ethical safeguards are embedded as mandatory procedural gates rather than advisory recommendations. Cook et al.'s [4] landmark survey of ICS digital forensics confirms that the ethics dimension of OT forensic practice has been entirely absent from the literature. This paper addresses that absence directly and provides the ethical foundation on which empirical forensic research in OT environments can be responsibly built.

Four research priorities follow directly from this paper. First is structured empirical validation of the WISE-DF framework through expert panel review (the Delphi method), structured practitioner interviews, and cognitive walkthrough testing with OT forensic investigators. The second priority, and the most directly connected to our ongoing research program, is systematic empirical investigation of the forensic artifact landscape and OT residual log source reliability through planned attack and cyber-attack research on our physical SCADA testbed. The two papers constitute a logical sequence: this paper provides the ethical governance architecture; the testbed paper provides the empirical forensic evidence base. Third is the extension of the ethical analysis to additional critical infrastructure

sectors, including energy and transportation OT environments. The fourth priority involves the development of a formal decision-support tool implementing the WISE-DF Phase 4 attribution confidence framework for use in legal and regulatory proceedings.

Author Contributions: Conceptualization, T.A. and B.Z.; methodology, T.A.; formal analysis, T.A.; investigation, T.A.; writing—original draft preparation, T.A.; writing—review and editing, T.A. and B.Z.; visualization, T.A.; supervision, B.Z.; project administration, B.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. The OT/ICS testbed configuration and forensic artifact landscape that inform the framework are described in reference [24]. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Stouffer, K.A.; Pease, M.; Tang, C.; Zimmerman, T.; Pillitteri, V.Y.; Lightman, S.; Hahn, A.; Saravia, S.; Sherule, A.; Thompson, M. Guide to Operational Technology (OT) Security. National Institute of Standards and Technology. Technical Report NIST SP 800-82 Rev. 3. 2023. Available online: <https://csrc.nist.gov/pubs/sp/800/82/r3/final> (accessed on 29 May 2026).
2. Tuptuk, N.; Hailes, S. Security of smart manufacturing systems. *J. Manuf. Syst.* **2018**, *47*, 93–106. [CrossRef]
3. Casey, E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed.; Chapter 3; Academic Press/Elsevier: Waltham, MA, USA, 2011.
4. Cook, M.M.; Marnerides, A.K.; Johnson, C.; Pezaros, D.P. A survey on industrial control system digital forensics: Challenges, advances and future directions. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1705–1747. [CrossRef]
5. National Institute of Standards and Technology. NISTIR 8428: Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT). Technical Report NISTIR 8428. 2022. Available online: <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8428.pdf> (accessed on 29 May 2026).
6. Spinello, R.A. *Cyberethics: Morality and Law in Cyberspace*, 7th ed.; Chapter 2; Jones & Bartlett Learning: Burlington, MA, USA, 2020.
7. U.S. Government Accountability Office. EPA Urgently Needs a Strategy to Address Cybersecurity Risks to the Nation’s Drinking Water Systems. Technical Report GAO-24-106744. 2024. Available online: <https://www.gao.gov/assets/gao-24-106744.pdf> (accessed on 29 May 2026).
8. Beauchamp, T.L.; Childress, J.F. *Principles of Biomedical Ethics*, 4th ed.; Oxford University Press: New York, NY, USA, 1994.
9. U.S. Supreme Court. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993). Available online: <https://supreme.justia.com/cases/federal/us/509/579/> (accessed on 29 May 2026).
10. Ahmed, I.; Obermeier, S.; Naedele, M.; Richard, G.G. SCADA systems: Challenges for forensic investigators. *Computer* **2012**, *45*, 44–51. [CrossRef]
11. Tuptuk, N.; Hazell, P.; Watson, J.; Hailes, S. A systematic review of the state of cyber-security in water systems. *Water* **2021**, *13*, 81. [CrossRef]
12. U.S. Environmental Protection Agency. Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems. Technical Report EPA 817-B-23-001. 2024. Available online: <https://www.epa.gov/waterresilience> (accessed on 29 May 2026).
13. National Cybersecurity Center of Excellence. Cybersecurity for the Water and Wastewater Sector. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023. Available online: <https://www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities> (accessed on 29 May 2026).
14. Carrier, B.D.; Spafford, E.H. Getting Physical with the Digital Investigation Process. *Int. J. Digit. Evid.* **2003**, *2*, 1–20.
15. Luttgens, J.M.; Pepe, M.; Mandia, K. *Incident Response & Computer Forensics*, 3rd ed.; McGraw-Hill Education: New York, NY, USA, 2014.
16. Fabro, M.; Cornelius, E. Recommended Practice: Creating Cyber Forensics Plans for Control Systems. Idaho National Laboratory/DHS National Cyber Security Division. Technical Report INL/EXT-08-14231. 2008. Available online: https://www.cisa.gov/sites/default/files/recommended_practices/Forensics_RP.pdf (accessed on 29 May 2026).
17. Rowlingson, R. A ten step process for forensic readiness. *Int. J. Digit. Evid.* **2004**, *2*, 1–28.
18. Eden, P.; Blyth, A.; Burnap, P.; Cherdantseva, Y.; Jones, K.; Soulsby, H.; Stoddart, K. Forensic readiness for SCADA/ICS incident response. In *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR)*, Belfast, UK, 23–25 August 2016; BCS Learning & Development Ltd.: Swindon, UK, 2016; pp. 142–150. [CrossRef]
19. van der Knijff, R.M. Control systems/SCADA forensics, what’s the difference? *Digit. Investig.* **2014**, *11*, 160–174. [CrossRef]

20. Hughes, N.; Karabiyik, U. Towards reliable digital forensics investigations through measurement science. *WIREs Forensic Sci.* **2020**, *2*, e1367. [[CrossRef](#)]
21. Horsman, G. Tool testing and reliability issues in the field of digital forensics. *Digit. Investig.* **2019**, *28*, 163–175. [[CrossRef](#)]
22. Stoykova, R. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Comput. Law Secur. Rev.* **2021**, *42*, 105575. [[CrossRef](#)]
23. Jeong, R.S.C. FORZA: Digital forensics investigation framework that incorporates legal issues. *Digit. Investig.* **2006**, *3*, 29–36. [[CrossRef](#)]
24. Akinsowon, T.; Oladimeji, D.; Amar, R.; Baza, M. A real-time hardware-in-the-loop water SCADA testbed for cyber-physical research. In *Proceedings of the IEEE 2nd International Conference on Secure IoT, Assured and Trusted Computing (SATC), Houston, TX, USA, 24–26 March 2026*; IEEE: Piscataway, NJ, USA, 2026; pp. 1–6. [[CrossRef](#)]
25. Kent, K.; Chevalier, S.; Grance, T.; Dang, H. Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology. Technical Report NIST SP 800-86. 2006. Available online: <https://csrc.nist.gov/pubs/sp/800/86/final> (accessed on 29 May 2026).
26. Dragos, Inc. *TRISIS Malware: Analysis of Safety System-Targeted Attack*; Technical Report; Dragos, Inc.: Hanover, MD, USA, 2017. Available online: <https://www.dragos.com/resources/whitepaper/trisis-analyzing-safety-system-targeting-malware/> (accessed on 29 May 2026).
27. Zetter, K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*; Crown Publishers: New York, NY, USA, 2014.
28. Jinad, R.; Gupta, K.; Simsek, E.; Zhou, B. Bias and fairness in software and automation tools in digital forensics. *J. Surveill. Secur. Saf.* **2024**, *5*, 19–35. [[CrossRef](#)]
29. Sunde, N.; Dror, I.E. A hierarchy of expert performance (HEP) applied to digital forensics. *Forensic Sci. Int. Digit. Investig.* **2021**, *37*, 301175. [[CrossRef](#)]
30. Mubarak, S.; Habaeibi, M.H.; Islam, M.R.; Abdul Rahman, F.D.; Tahir, M. Anomaly detection in ICS datasets with machine learning algorithms. *Comput. Syst. Sci. Eng.* **2021**, *37*, 33–46. [[CrossRef](#)]
31. Wang, W.; Wang, Z.; Zhou, Z.; Hu, H.; Han, J.; Liu, C.; Yin, X. Anomaly detection of industrial control systems based on transfer learning. *Tsinghua Sci. Technol.* **2021**, *26*, 821–832. [[CrossRef](#)]
32. Pinto, A.; Herrera, L.-C.; Donoso, Y.; Gutierrez, J.A. Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure. *Sensors* **2023**, *23*, 2415. [[CrossRef](#)] [[PubMed](#)]
33. Goodman, B.; Flaxman, S. European union regulations on algorithmic decision-making and a ‘right to explanation’. *AI Mag.* **2017**, *38*, 50–57. [[CrossRef](#)]
34. Dror, I.E. Cognitive and human factors in expert decision making: Six fallacies and the eight sources of bias. *Anal. Chem.* **2020**, *92*, 7998–8004. [[CrossRef](#)] [[PubMed](#)]
35. Langner, R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Secur. Priv.* **2011**, *9*, 49–51. [[CrossRef](#)]
36. Solanke, A.A. Explainable digital forensics AI: Towards mitigating distrust in AI-based digital forensics analysis using interpretable models. *Forensic Sci. Int. Digit. Investig.* **2022**, *42*, 301403. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.