

THE TRUST-BREAKER IN CLINICAL AUTOMATION: A SOCIO-TECHNICAL REVIEW OF HUMAN-ROBOT INTERACTION AND SYSTEM ABANDONMENT IN NURSING AND TELEMETRY ECOSYSTEMS

Won Kang SONG

Capitol Technology University, Laurel, MD, USA

wsong@captechu.edu

ORCID: <https://orcid.org/0009-0004-8644-4987>

ABSTRACT

The Fourth Industrial Revolution has integrated autonomous systems into high-stakes medical ecosystems, yet a critical adoption gap persists, driven by socio-technical failure rather than mechanical insufficiency. This paper introduces the “trust-breaker” framework to analyze why clinicians strategically abandon advanced robotics, such as Robot on Wheels (RoW) medication units and biomimetic telemetry drones. A trust-breaker is defined as a discrete moment of robotic unpredictability, ranging from operational path-planning errors to sensor-fusion desynchronization, that violates the supervisor’s mental model. This study posits that the Registered Nurse’s role has transitioned from a physical provider to a system supervisor, creating a supervisory paradox in which monitoring inconsistent, autonomous agents increases cognitive load beyond the demands of manual labor. When this load exceeds operator capacity, it triggers cognitive collapse, leading to the strategic abandonment of the system. From an engineering management perspective, this abandonment transforms significant capital investments into stranded assets with zero return on investment. The paper concludes by proposing a shift toward Industry 5.0 human-centricity, advocating for reflexive feedback loops, global compliance with data sovereignty, and a collaborative standard of care to foster trust-resilient clinical ecosystems.

KEYWORDS: autonomous mobile robots, clinical automation, engineering management, human-robot interaction, nursing informatics

**Submission Received: 04 April 2026; Revised: 05 May 2026;
Accepted: 11 May 2026; Published: June 2026**

1. Introduction

1.1. Background of the Study

The Fourth Industrial Revolution has propelled autonomous systems from controlled laboratory environments into the dynamic, high-stakes domain of integrated medical ecosystems (Ryalat et al., 2025). While advancements in sensor fusion and

path-planning algorithms have reached near-total technical maturity, Urrea and Kern (2025) confirm that a significant adoption gap persists. Within the discipline of engineering management, the success of an autonomous system, such as the Robot on Wheels (RoW) medication units or the telemetry drones, is traditionally quantified

by operational efficiency, reliability, and throughput (Tarek & Paran, 2024); however, achieving these metrics is fundamentally contingent on sustained human-robot collaboration (Song et al., 2026).

This paper argues that the prevailing adoption gap in healthcare is not a product of mechanical insufficiency, but rather a socio-technical failure to manage the *trust-breaker* (Afroogh et al., 2024). A trust-breaker is a discrete moment of robotic unpredictability – such as a ‘Dragonfly’ vital-scanner failing to sync or a RoW unit obstructing an emergency path – that violates the clinician’s mental model. In high-density medical environments, the Registered Nurse’s (RN) role has transitioned from a physical provider to a system supervisor, a shift that paradoxically increases cognitive load and heightens the psychological impact of system errors (Schroepfer, 2025). When a supervisor encounters a trust-breaker, the subsequent decision to abandon automation in favor of manual labor reduces technical efficiency to zero. Consequently, this abandonment represents a total failure of engineering management and capital investment, necessitating a new predictive framework that integrates human factor audit data into the technical lifecycle of clinical robotics.

1.2. Problem Statement

The core problem addressed in this study is the critical misalignment between the technical reliability of nursing robotics and the psychological trust of the human operator (Campagna & Rehm, 2025). While autonomous systems are engineered for high-throughput efficiency, their operational success is gated by a socio-technical threshold. Current engineering management frameworks often overlook the trust-breaker phenomenon in clinical workflows, leading to three interconnected failures.

Operational instability – The transition from manual bedside care to system supervision has introduced a

cognitive overload gap. When autonomous telemetry or medication systems behave unpredictably, the RN lacks a robust mental model to reconcile the error (Hancock, 2022), leading to immediate abandonment of the system.

Methodological Inadequacy – Existing human-robot interaction (HRI) models lack a predictive framework to quantify trust-breakers in high-density, real-world hospital environments (Afroogh et al., 2024). Without empirical data on these clinical friction points, engineers cannot design systems that prevent the catastrophic collapse of user confidence.

Economic Risk – In ward automation, reverting to manual delivery due to trust failure results in a 100% loss of technical efficiency. This abandonment results in a total failure of capital investment and engineering management, as the advanced sensor suits and algorithms become *Stranded Assets* with zero return on investment (ROI; Schroepfer, 2025). Beyond the immediate technical failure, the lack of trust in human-robot interaction (HRI) directly leads to the systematic disuse of the robotic agent (Schäfer et al., 2024). In the context of precision agriculture, this disuse results in a situation in which highly complex autonomous systems fail to improve the competency of the human-robot team, effectively transforming capital investments into *Stranded Assets* that yield zero return on investment (Schroepfer, 2025).

1.3. Engineering Management Thesis

Historically, engineering management focused on *mean time between failures*, a mechanical metric (Aji & Uchendu, 2025). In the modern era, the definition of system failure has undergone a fundamental shift: it is no longer characterized by mechanical failure of the robot, but by the cognitive collapse of the human supervisor (Bassi et al., 2025). As industrial systems move toward Industry 5.0, the focus has shifted

from mechanical uptime to human-centricity (Song et al., 2026). A 2025 study in *Frontiers in Robotics and AI* explicitly notes that directing worker attention and managing perceived workload is now fundamental to implementing safe, fluent, and efficient collaborative applications (Billing et al., 2025).

1.4. Cognitive Collapse and the Trust-Breaker

This research posits that, within the modern socio-technical landscape, system failure must be redefined: it is no longer merely a mechanical breakdown but rather the supervisor's strategic decision to abandon the autonomous system in response to unpredictable robotic behavior. Research indicates that when a robot's behavior violates a human's mental model, an event termed a trust-breaker (Afroogh et al., 2024), it triggers immediate disuse of automation. This occurs because the human supervisor prioritizes risk mitigation over the potential efficiency of an unpredictable agent (Schäfer et al., 2024).

The shift from manual labor to system supervision increases cognitive monitoring demands; when a robot behaves inconsistently, the resulting load often exceeds the operator's capacity. From an engineering management perspective, even a mechanically perfect system becomes a stranded asset the moment the human-in-the-loop (HITL) ceases to trust its outputs (Song et al., 2026). Studies in neuroergonomics suggest that the shift from manual labor to system supervision increases cognitive monitoring demands (Parasuraman, 2015). When a robot behaves inconsistently, the resulting cognitive load often exceeds the operator's capacity, leading to cognitive collapse in which the user reverts to manual processes to regain a sense of control (Bassi et al., 2025). From an engineering management perspective, this abandonment represents a 100% loss of technical efficiency. Even a mechanically perfect

system becomes a stranded asset with zero ROI the moment the HITL ceases to trust its outputs (Schroepfer, 2025), thereby violating the user's mental model and leading to abandonment.

2. The Taxonomy of Clinical Autonomy

2.1. The RoW in Ward Automation

The integration of the RoW into acute care environments represents a fundamental shift in the delivery of pharmaceutical and medical supplies. In this context, ward automation is no longer characterized by static dispensing machines, but by mobile, autonomous units capable of navigating high-density clinical corridors to facilitate medication delivery and smart IV pole management. In engineering management, the success of these systems is traditionally measured by their ability to optimize performance and control strategies (Tarek & Paran, 2024).

Historically, the RN maintained direct, tactile control over the medication administration record (MAR) and the physical delivery of fluids. As autonomous RoW units assume responsibility for transport and delivery, the RN's role evolves into that of a system supervisor. Urrea and Kern (2025) note that while these technological trends offer significant advances in industrial-grade robotics, their application in healthcare is gated by the *supervisory paradox*. In this state, the nurse must maintain a high level of situational awareness to monitor the RoW's path-planning and delivery accuracy. If the system's behavior deviates from the clinical workflow, a *Trust-Breaker*, the resulting cognitive load can exceed that of the original manual task, leading to system disuse (Schroepfer, 2025).

2.2. Autonomous Mobile Sensing Platforms (Remote Vital Sign Acquisition)

The integration of autonomous mobile systems into healthcare environments

represents a paradigm shift from stationary to dynamic, *always-on* monitoring. This section evaluates the engineering requirements and clinical efficacy of mobile sensing agents, specifically, small-scale Unmanned Aerial Vehicles (UAVs) and Ground-Based Autonomous Units, for continuous acquisition of patient vitals.

Biomimetic and multi-rotor flight architectures – Research into biomimetic flight platforms (e.g., insect-inspired wing kinematics) and multi-rotor configurations has revealed significant advantages in indoor clinical navigation (Wang et al., 2023). According to Wang et al. (2023), unlike traditional fixed-wing systems, these platforms provide the high-maneuverability and hovering capabilities necessary for stable sensor-to-target alignment:

➤ *Engineering constraint* - The primary challenge identified in current literature is the *signal-to-noise* ratio during non-contact sensing. Rotor vibration and propwash from a flight unit can interfere with micro-Doppler radar or photoplethysmography (rPPG) sensors used to detect heart rate and respiratory frequency (Gharamohammadi, 2024).

Sensor fusion and real-time physiological telemetry – The efficacy of remote sensing platforms depends on the *sensor fusion architecture*, which simultaneously processes data from LiDAR (for spatial awareness), thermal infrared (for thermoregulation monitoring), and high-definition optical sensors (for hemodynamics):

➤ *Data integrity*: In the context of telemetry nursing, Vishweshwara and Ramya (2025) emphasize the need for low-latency data transmission. Engineering Management frameworks must account for the *quality of service (QoS)* in hospital Wi-Fi/5G networks to ensure that *real-time* alerts for oxygen desaturation or tachycardia are delivered to the clinical dashboard without packet loss (Mishra et al., 2024).

➤ *Clinical integration*: As noted in recent scoping reviews by Angelucci et al. (2025), while standard continuous ECG and cuff-based NIBP remain the clinical gold standards for ICU monitoring, they present significant barriers to patient mobility and skin-to-skin contact (particularly in neonatal care). The engineering of autonomous mobile sensing platforms aims to achieve parity with these gold standards through non-contact methods like rPPG and Doppler radar, effectively extending high-acuity surveillance into lower-resource settings and standard hospital wards (Angelucci et al., 2025).

Human-robot interaction (HRI) in nursing informatics – A critical subset of the literature (Mehl et al., 2023; Harari, 2023) focuses on the psychological and social engineering of mobile sensing units.

➤ *Privacy and ethics* – Academic inquiry into remote acquisition highlights the necessity of *edge computing* (Kong et al., 2022), where physiological data is processed locally on the mobile unit rather than in a vulnerable cloud, ensuring HIPAA and GDPR compliance for sensitive biometric data.

Engineering systems analysis: Remote patient monitoring (RPM) vs. physical nurse assessment – The divergence between RPM and manual physical assessment represents a shift from *intermittent, high-fidelity human observation* to *continuous, sensor-driven data streams* (Coffey et al., 2022). From an engineering management perspective, this comparison centers on the critical trade-offs between system autonomy and clinical intuition, specifically regarding data acquisition models.

➤ *Comparative data acquisition models* – Traditional physical nurse assessment operates as a heuristic model in which the clinician functions as a “multi-modal sensor”, utilizing tactile palpation, auditory auscultation, and visual pattern recognition. While this model provides high-

fidelity insights, it is inherently limited by sampling bias, as data are captured only at specific 4- to 8-hour intervals, creating clinical blind spots between assessments. In contrast, RPM engineering utilizes a continuous model supported by a network of wearable or ambient sensors that provide high-frequency longitudinal data (Du, 2026). This engineering advantage enables the detection of micro-trends, such as gradual decreases in heart rate variability over a 24-hour period, that a human nurse might overlook during a brief 5-minute physical encounter (Gao et al., 2025).

➤ *Signal precision and “clinical noise”* – A primary engineering challenge in RPM systems is managing signal precision and mitigating “clinical noise”. While a physical nurse can immediately identify and correct a displaced blood pressure cuff through direct observation, an automated RPM unit must rely on sophisticated signal-processing algorithms to filter out artifacts and environmental interference (Prabakaran & Rufus, 2022). This transition from subjective observation to quantifiable metrics – such as the use of RPPG sensors to determine a Perfusion Index – transforms clinical decision support into a data-driven discipline (Pannunzio et al., 2024). However, the engineering framework must address the risk of alarm fatigue by designing intelligent thresholds. These systems must be engineered to alert the clinician only during true physiological deviations rather than triggering for every temporary loss of sensor contact, thereby maintaining the integrity of the clinical response (Ko et al., 2023).

➤ *System architecture: closing the feedback loop* – The architectural design of RPM essentially functions as a closed-loop feedback system comprising automated sensing, cloud-based AI processing, and autonomous action. In this architecture, the AI clinical data cloud compares real-time acquisition against historical baselines to determine whether to log the event or

trigger an emergency intervention, such as dispatching a mobile unit for closer inspection. Unlike purely automated industrial environments, healthcare RPM engineering must maintain HITL architecture (Lundy et al., 2026). The objective of this design is not the total replacement of physical assessment but its augmentation; by using RPM to prioritize which patients require “gold-standard” manual intervention, the system optimizes labor allocation in high-stress clinical environments.

➤ *Engineering reliability vs. clinical intuition* – Furthermore, engineering management evaluates these systems using the metric mean time to detection (MTTD) for physiological instability (Vejjanugraha et al., 2025). Emerging research into small-scale biomimetic UAVs optimized for indoor flight (Diaz-Parra et al., 2025) aims to reduce MTTD to near-zero. These autonomous agents facilitate persistent surveillance and a continuous data loop that exceeds the capabilities of intermittent nursing rounds. Despite these technical leaps, the literature acknowledges that human nurses possess tacit knowledge and the ability to sense “impending doom” through nonverbal cues – such as skin turgor or emotional affect – that current sensor arrays cannot fully digitize (Zhang et al., 2025). Consequently, the engineering objective is to create a hybrid telemetry model. In this hierarchical structure, autonomous mobile sensors serve as the primary high-frequency detection layer, while a secondary AI Clinical Data Cloud filters signals to eliminate false positives. This leads to a tertiary layer where the physical nurse provides the definitive diagnostic intervention only when the system validates a true clinical deviation.

3. The Socio-Technical Barrier: The “Trust-Breaker” Framework

The *Violation Loop* serves as a diagnostic conceptual framework for

explaining the iterative decline in trust following a technical anomaly. The cycle begins with *Anticipated Behavior*, in which the human operator maintains a stable mental model of the robot's expected performance and reliability. This stability is disrupted by a Technical Anomaly, a trust-breaking event in which the machine's real-time actions – such as a path-planning error or data-sync latency – deviate from the operator's predictions. This divergence triggers *Cognitive Dissonance*, forcing the operator to reconcile the mission's urgency with the machine's erratic behavior. If the anomaly is not resolved through transparent

communication or recalibration of the system, the process culminates in *Strategic Abandonment*. In this final phase, the human operator makes a rational, goal-oriented decision to bypass the autonomous system and revert to manual labor. This abandonment represents a critical failure in engineering management, resulting in a total loss of the system's projected return on investment (ROI) and a return to inefficient, high-workload manual processes. Figure no. 1 illustrates this cycle, mapping the path from expectation to strategic abandonment.

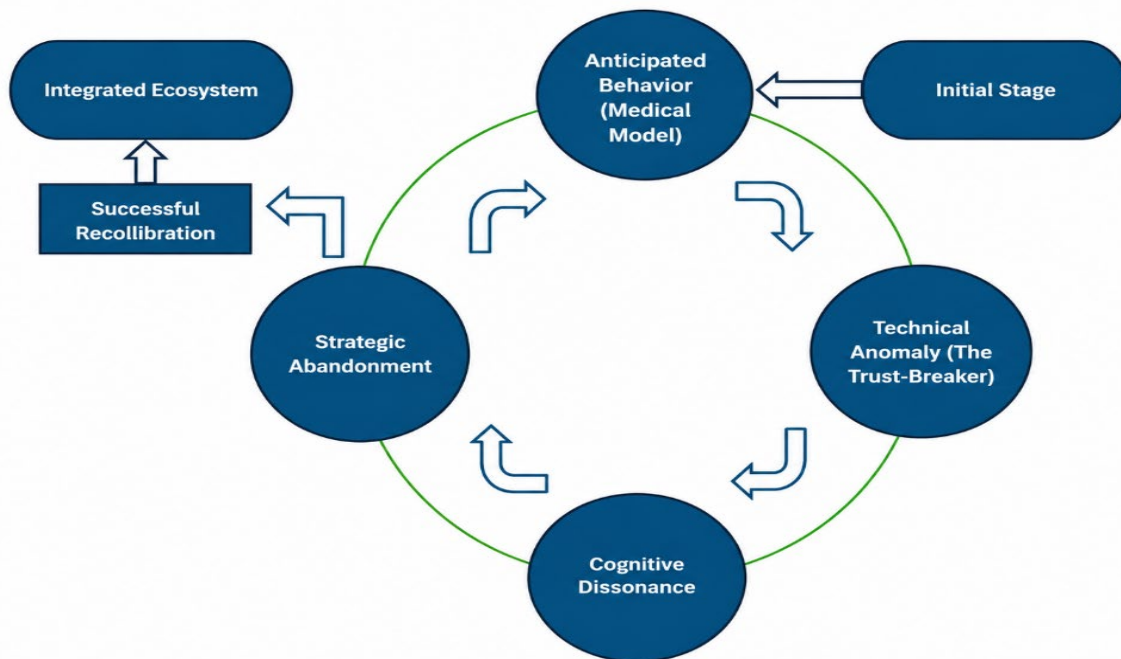


Figure no. 1: *The Violation Loop. A visualization of the socio-technical process where a technical anomaly triggers a violation of the clinician's mental model, leading to system abandonment*
(Source: Author's own elaboration)

3.1. The Anatomy of a Trust-Breaker

In the transition from mechanical reliability to socio-technical integration, the primary point of system failure shifts from the machine to the human-robot interaction (HRI) interface. This study defines a *Trust-*

Breaker as a discrete, observable event of robotic unpredictability that violates the operator's internal mental model of the system's functional logic (Afroogh et al., 2024). Unlike a mechanical breakdown, which is often a binary state of "operational"

or “failed”, a trust-breaker is a qualitative disruption that can occur while the system is still technically functioning. Within high-stakes clinical environments, these disruptions are categorized into three primary anatomical layers: operational unpredictability, data desynchronization, and technical integrity failures.

Operational unpredictability occurs when an autonomous agent, such as a ground-based medication delivery unit, executes path-planning maneuvers that conflict with the urgent, non-linear workflows of a clinical unit. For instance, if a RoW fails to yield during an emergency resuscitation event or obstructs a high-traffic corridor due to a conservative obstacle-avoidance algorithm, the clinician perceives the unit not as a tool but as a liability. This friction creates immediate cognitive dissonance: the RN, whose role has evolved into that of a system supervisor, must now allocate cognitive resources to “babysitting” the technology rather than focusing on patient care (Song et al., 2026).

Data desynchronization represents a second, more insidious layer of the trust-breaker. In the context of aerial telemetry platforms, such as biomimetic drones designed for vital sign scanning, the trust-breaker often manifests as a failure in real-time sensor fusion. If a remote photoplethysmography (rPPG) sensor fails to sync with the central clinical data cloud due to latency or environmental noise, the resulting data gap is not merely a technical glitch; it violates the clinician’s expectation of transparency and continuity (Vishweshwara & Ramya, 2025). When the information provided by the autonomous system contradicts the manual “gold standard” assessment, the human supervisor begins to perceive the system as a “black box”, leading to a rapid decay in reliance.

Finally, technical integrity failures involve the subtle degradation of sensor accuracy. For example, rotor vibrations in

biomimetic aerial units can introduce artifacts into telemetry data, leading to false-positive alarms. In a high-density medical ecosystem, the cumulative effect of these minor inconsistencies triggers a “crying wolf” phenomenon. As established by the intelligent sociotechnical systems (iSTS) framework, once a threshold of unpredictability is reached, the clinician prioritizes risk mitigation over technical efficiency (Xu & Gao, 2024). The anatomy of the trust-breaker is therefore not found in the broken gear or the crashed software, but in the moment the human supervisor decides that the cost of monitoring the technology exceeds the benefit of its autonomy, leading to permanent system abandonment and the creation of a “stranded asset”. This transition represents the breakdown of the human-machine team.

3.2. Cognitive Collapse & The Supervisory Paradox

The RN’s transition from a direct physical provider to a system supervisor introduces a phenomenon defined in this framework as the *Supervisory Paradox*. In traditional nursing workflows, physical tasks, such as manual telemetry monitoring or medication transport, are labor-intensive but cognitively linear. However, as autonomous systems like mobile telemetry units and ground-based delivery robots are integrated into the clinical environment, the RN’s role shifts toward high-level cognitive oversight. According to the intelligent sociotechnical systems (iSTS) framework, this transition does not necessarily reduce the clinician’s workload; instead, it fundamentally alters the nature of the effort, shifting from physical exertion to continuous mental monitoring of robotic path planning and data integrity (Xu & Gao, 2024).

The paradox lies in the fact that supervising an autonomous agent often requires greater situational awareness than performing the task manually. For a system

to remain “trusted”, the supervisor must maintain a transparent mental model of the robot’s logic. When the system operates within expected parameters, the cognitive load is manageable. However, the introduction of a trust-breaker, such as a sensing platform failing to distinguish between clinical signals and environmental noise, triggers a state of *Cognitive Collapse*, a process-oriented failure where the internal mental frame of the observer destabilizes under structural tension (A-Hakam & Elnoor, 2025). In this state, the mental effort required to troubleshoot, override, or “babysit” an unpredictable autonomous agent exceeds the cognitive energy needed simply to revert to manual labor (Song et al., 2026).

This collapse is driven by a failure in *Teaming* dynamics. As Wang et al. (2024) explored, the effectiveness of human-AI teaming is highly sensitive to the consistency of the automated partner. In a high-stakes medical ecosystem, where time-to-intervention is the critical metric, a clinician cannot afford the “latency of doubt”. When an autonomous unit violates established clinical protocols, the human supervisor experiences a rapid decay in reliance. This is not merely a psychological reaction but a strategic engineering management decision: the supervisor prioritizes risk mitigation over the theoretical efficiency of the autonomous system (Schäfer et al., 2024).

Consequently, the *Supervisory Paradox* results in system abandonment. To the clinician, the manual performance of a task offers a *Gold Standard* of certainty that the autonomous system, once compromised by a trust-breaker, can no longer provide. Even if the robotic unit is 95% accurate, the 5% unpredictability creates a “monitoring tax” that the exhausted clinician is unwilling to pay. This leads to the phenomenon of *Stranded Assets* (Schroepfer, 2025), where multi-million-dollar investments in clinical automation sit

idle because the socio-technical interface failed to account for the threshold of human cognitive endurance (Urrea & Kern, 2025). The resolution of this paradox requires a shift from *Total Autonomy* to *Human-Centric Collaborative Intelligence* (Zheng et al., 2023), in which the system is designed to reduce, rather than replace, the supervisory burden on the clinical expert.

4. Engineering Management for Clinical Trust

4.1. Beyond Mechanical Metrics

In the traditional engineering management of clinical robotics, success has historically been quantified through mechanical key performance indicators (KPIs) such as *mean time between failures*, *battery cycle life*, and *navigational throughput* (Aji & Uchendu, 2025; Tarek & Paran, 2024). However, as industrial systems transition toward Industry 5.0, these metrics are increasingly criticized for failing to account for the human-centricity required in high-acuity nursing environments (Song et al., 2026). The focus has shifted from mere “mechanical uptime” to *Collaborative Fluency* (Natarajan et al., 2023), the degree to which an autonomous agent and a human supervisor can synchronize their workflows without cognitive friction.

To achieve this fluency, a framework for *Organizational Development* is required to foster “cyberliterate cultures” within healthcare institutions (Lundy et al., 2026). According to Lundy et al., cyberliteracy is not merely technical proficiency, but an organizational DNA that treats clinical staff as active participants in a secure, adaptive ecosystem rather than passive users of hardware. This shift, Lundy et al. posit, requires engineering managers to move beyond procurement-focused leadership and toward a model of human-centric collaborative intelligence. In a cyberliterate culture, the deployment of autonomous mobile robots (AMRs) is managed through

a lens of socio-technical resilience, ensuring that the technology supports the RN clinical judgment rather than competing for their limited cognitive resources (Xu & Gao, 2024).

4.2. Recovery of Trust

A critical and often overlooked component of engineering management is the *Recovery of Trust* following a system failure. When a robot commits a navigation error, such as a ground-based delivery unit obstructing a critical path or an aerial sensing platform providing inconsistent telemetry, the *Trust-Breaker* event triggers an immediate decline in reliance (Afroogh et al., 2024). The management challenge lies in the “latency of recovery”: how long it takes for a nurse to trust an autonomous agent again after a perceived failure. Research into human-robot teaming suggests that trust is “asymmetric” (Zahedi et al., 2024); it builds slowly through hundreds of successful interactions but can be destroyed by a single high-consequence error. If a medication delivery unit fails to reach its destination due to a path-planning logic error, the RN often reverts to manual labor to mitigate risk, leading to the creation of a “stranded asset” (Urrea & Kern, 2025).

Effective “repair strategies” in a hospital setting must therefore go beyond technical recalibration. They require transparent error-reporting protocols where the system explicitly communicates the cause of the failure to the supervisor. According to the intelligent sociotechnical systems (iSTS) framework, trust recovery is accelerated when the autonomous agent provides “reflexive feedback”, allowing the human supervisor to understand the limitations of the robot’s current state (Wang, Gao, & Agarwal, 2024). Without these managed recovery protocols, a single navigational error can result in permanent system abandonment, regardless of the robot’s subsequent mechanical reliability.

4.3. The Economic Risk of Stranded Assets and ROI Recovery

The ultimate consequence of a managed *Trust-Breaker* is the transformation of high-capital medical technology into *Stranded Assets* (Schroepfer, 2025). In the context of engineering management, a stranded asset is defined as an investment that fails to deliver its projected economic life or operational utility due to premature abandonment (Urrea & Kern, 2025). Within the healthcare robotics sector, where procurement costs for autonomous mobile units and aerial sensing platforms reach hundreds of thousands of dollars per unit, the “adoption gap” represents a significant fiscal risk. When a clinician reverts to manual labor after a navigational error or data desynchronization, the system’s ROI drops to zero, while the operational overhead of maintaining the idle hardware persists.

Traditional ROI models in clinical automation often focus exclusively on labor-saving hours and throughput efficiency. However, these models are fundamentally flawed because they do not account for the “monitoring tax”, the hidden cost of the supervisory burden imposed on RNs. If the cognitive load of supervising an autonomous agent exceeds the labor saved by the machine, the system fails the cost-benefit analysis for the primary stakeholder: the frontline clinician. As highlighted by the intelligent sociotechnical systems (iSTS) framework, true economic sustainability in Industry 5.0 is achieved only when the system functions as a “force multiplier” that reduces, rather than redistributes, clinical labor (Xu & Gao, 2024).

The implementation of *Trust-Repair* strategies, such as error transparency and reflexive feedback, is therefore not merely a psychological intervention, but a financial imperative. By investing in the socio-technical interface and fostering a *Cyberliterate Organizational Culture*, institutions can significantly reduce the latency of trust recovery (Lundy et al.,

2026). Reducing this latency ensures that autonomous systems remain in active service after a technical anomaly, thereby protecting the asset's lifecycle value.

Furthermore, the economic case for trust-repair is bolstered by the reduction of “switching costs”. Every time a clinician abandons an automated process and returns to a manual one, the disruption to the clinical workflow introduces the potential for medical error and increased patient length of stay. By utilizing shared-control models and graceful degradation protocols, engineering managers can ensure that the system remains “useful” even when it is not “fully autonomous” (Wang et al., 2024). This prevents the platform from being completely abandoned and ensures that the clinical institution realizes the long-term efficiency gains promised by the *Fourth Industrial Revolution*. In summary, the “business case” for human-centric robotics lies in recognizing that technical maturity is worthless without sustained cognitive buy-in from the human operator (Song et al., 2026).

5. Regulatory and Ethical Governance of Autonomous Nursing Systems

5.1. Global Data Sovereignty and Telemetry Integrity

As autonomous nursing systems transition from developmental phases to clinical deployment, they encounter a complex global regulatory landscape. In a peer-reviewed context, the protection of patient telemetry data is benchmarked against rigorous international standards. This includes the General Data Protection Regulation (GDPR; Issaoui et al., 2023; Piispanen et al., 2024; Rahardja et al., 2022), which emphasizes the “right to explanation”, and the Health Insurance Portability and Accountability Act (HIPAA; Ettaloui et al., 2023), which serves as a global reference for data security. Furthermore, engineering management must increasingly align with

ISO/IEC 27001 (Malatji, 2023) and ISO 81001-1 standards, which provide a universal framework for cybersecurity and software safety in the health sector.

These frameworks necessitate a *Privacy-by-Design* approach, ensuring that cybersecurity is a core functional requirement rather than a peripheral concern (Ettaloui et al., 2023; Issaoui et al., 2023; Malatji, 2023; Piispanen et al., 2024; Rahardja et al., 2022). The technical challenge lies in ensuring that real-time, autonomous vital-scanning and sensor fusion do not compromise patient privacy rights or breach data sovereignty protocols. An ethical *Trust-Breaker* occurs when a perceived lack of transparency in AI-powered telemetry processing creates a *Black Box* effect for the human supervisor (Afroogh et al., 2024). If a clinician perceives that an autonomous unit is insecure or that its data-handling protocols are opaque, the resulting resistance leads to immediate abandonment of the system to protect the patient's fundamental ethical rights.

5.2. Liability and the Universal “Standard of Care”

The integration of clinical automation introduces significant legal questions regarding liability and the evolving *Standard of Care*. In high-acuity healthcare environments, the trust-breaker phenomenon carries substantial weight in professional liability frameworks. If an autonomous agent fails to yield during a critical clinical event or delivers an inconsistent telemetry scan, even if the error stems from a sensor-fusion anomaly rather than mechanical failure, assigning legal responsibility remains a point of intense academic contention (Xu & Gao, 2024). Current legal frameworks often struggle to distribute accountability between the equipment manufacturer, the hospital's engineering management team, and the supervising clinician (Xu & Gao, 2024).

This ambiguity is a primary driver of *Strategic Abandonment*. A nurse may rationally reject the use of an autonomous medication cart or a smart infusion system if they perceive that technology increases their professional liability without providing a corresponding legal *Safe Harbor*. Consequently, the future of clinical automation is fundamentally contingent on establishing clear ethical and legal governance that protects the clinician-robot “team” from the repercussions of a technical trust-breaker. As industrial systems move toward Industry 5.0, the *Standard of Care* must be redefined to include the collaborative interactions between humans and machines, ensuring that autonomous systems are viewed as protective assets rather than legal liabilities (Schäfer et al., 2024).

A *Collaborative Standard of Care* for Industry 5.0 shifts the legal and professional benchmark from the performance of a single human to the functional integrity of the *Human-Robot Team*. In traditional clinical practice, according to Copeland (2023), the *Standard of Care* is defined by what a “reasonably prudent” nurse would do under similar circumstances. In an automated ward, this is no longer sufficient because the nurse cannot “reasonably” be expected to manually verify every sub-millisecond calculation of an AI.

A Collaborative Standard of Care would likely include the following four pillars:

I. The Duty of Transparency (manufacturer liability) – The standard of care would ensure that an autonomous agent (like a medication robot or telemetry drone) has a legal “duty” to signal its own uncertainty (Kuntardjo et al., 2023). If a robot encounters a sensor-fusion error but remains silent, the liability shifts entirely to the manufacturer. A “reasonably prudent” system must provide **explainable feedback** so the human supervisor can make an informed decision to intervene.

II. Safe Harbor for supervised autonomy (clinician protection) – To prevent *Strategic Abandonment*, legal frameworks must provide a *Safe Harbor* for clinicians. If a nurse follows the established organizational protocols for supervising a robot, they should not be held personally liable for a *Black Box* algorithmic failure that was impossible to predict. This protects the clinician’s license and encourages the continued use of technology.

III. Joint liability protocols (organizational responsibility) – Instead of a *Human vs. Machine* blame model, the standard would move toward *Joint Liability*. Responsibility is distributed based on the “Failure Point”:

- *Engineering management*: Liable for maintenance and *Cyberliterate* training.

- *The algorithm*: Liable for *Unprovoked* logic errors.

- *The clinician*: Liable only for *Negligent Supervision* (e.g., ignoring a high-priority alert).

IV. Dynamic competency requirements: *The Standard of Care* would evolve to include *System-Supervisory Competence*. A nurse would be evaluated not just on their manual clinical skills, but on their ability to manage the socio-technical interface. Failure to respond to a robot’s “uncertainty signal” would constitute a breach of this new standard, just as failing to check a manual pulse would today. By establishing these protocols, the healthcare industry moves away from the *Trust-Breaker* trap and toward a resilient ecosystem where humans and machines share the burden of patient safety.

6. Conclusions and Future Directions

The synthesis of this literature review reveals that the fundamental challenge of the *Fourth Industrial Revolution* in healthcare is not a lack of mechanical reliability, but a deficit in *Socio-Technical Trust*. Traditional Engineering Management has historically

prioritized the *Reliability of Movement*, focusing on navigation, battery life, and algorithmic accuracy (Tarek & Paran, 2024). However, the true barrier to clinical adoption is the *Reliability of Trust*. By defining the *Trust-Breaker* as the pivotal moment of human abandonment, driven by cognitive collapse (A-Hakam & Elnoor, 2025), ethical transparency concerns, or legal ambiguity, we can begin to move toward more resilient clinical systems. For an integrated medical ecosystem to succeed globally, it must move beyond Industry 4.0's efficiency metrics and embrace the *Industry 5.0* mandate of human-centricity.

Future research in this field must focus on three critical *Trust-Resilient* areas:

- Reflexive Feedback Loops: Designing autonomous agents that can communicate their own limitations to the supervisor in real-time.

- Standardization of *Safe Harbors*: Developing global legal frameworks that protect the clinician-robot team from the repercussions of technical anomalies.

- Cyberliterate Organizational Development: Moving beyond hardware procurement and focusing on the *Organizational DNA* required to support a hybrid human-machine workforce (Lundy et al., 2026).

Only when the system is managed as a trusted partner rather than a *Black Box* monitoring burden can the full economic and clinical potential of healthcare robotics be realized. The future of nursing automation lies in engineering for *Collaborative Fluency*, ensuring that technology serves as a force multiplier for care rather than a source of cognitive friction.

REFERENCES

- A-Hakam, T., & Elnoor, N. (2025). Cerebral small vessel disease–intolerability transient cognitive collapse (CSVD-ITCC): A novel syndrome of reversible cognitive dysfunction in context of severe cerebral small vessel disease (P4-3.016). *Neurology*, 104(7 Supplement 1), 2466. Available at: <https://doi.org/10.1212/WNL.0000000000210359>.
- Afroogh, S., Akbari, A., Malone, E., Kargar, M., & Alambeigi, H. (2024). Trust in AI: Progress, challenges, and future directions. *Humanities and Social Sciences Communications*, 11(1), 1568. Available at: <https://doi.org/10.1057/s41599-024-04044-8>.
- Aji, J.O., & Uchendu, I. (2025). Improving Facility Operations: A Quantitative Evaluation of MTBF, MTTR, and SLA Targets. *European Journal of Innovative Studies and Sustainability*, 1(3), 247-261. Available at: [https://doi.org/10.59324/ejiss.2025.1\(3\).20](https://doi.org/10.59324/ejiss.2025.1(3).20).
- Angelucci, A., Greco, M., Cecconi, M., & Aliverti, A. (2025). Wearable devices for patient monitoring in the intensive care unit. *Intensive Care Medicine Experimental*, 13(1), 26. Available at: <https://doi.org/10.1186/s40635-025-00738-8>.
- Bassi, G., Orso, V., Salcuni, S., & Gamberini, L. (2025). Understanding workers' well-being and cognitive load in human-cobot collaboration: Systematic review. *Journal of Medical Internet Research*, e75658. Available at: <https://doi.org/10.2196/75658>.
- Billing, E.A., Fraboni, F., Gualtieri, L., Rosen, P.H., & Thorvald, P. (2025). Editorial: Human factors and cognitive ergonomics in advanced industrial human-robot interaction. *Frontiers in Robotics and AI*, 12, 1564948. Available at: <https://doi.org/10.3389/frobt.2025.1564948>.
- Campagna, G., & Rehm, M. (2025). A systematic review of trust assessments in human–robot interaction. *ACM Transactions on Human-Robot Interaction*, 14(2), 1-35. Available at: <https://doi.org/10.1145/3706123>.

Coffey, J.D., et al. (2022). Development and implementation of a nurse-based remote patient monitoring program for ambulatory disease management. *Frontiers in digital health*, 4, 1052408. Available at: <https://doi.org/10.3389/fdgth.2022.1052408>.

Copeland, D. (2023). Caring in the context of risk: Moving beyond duty. *Advances in Nursing Science*, 46(1), 2-13. Available at: <https://doi.org/10.1097/ANS.0000000000000458>.

Diaz-Parra, O., et al. (2025). Integrated biomimetics: Natural innovations for urban design, smart technologies, and human health. *Applied Sciences*, 15(13), 7323. Available at: <https://doi.org/10.3390/app15137323>.

Du, Y., Li, J., Zhao, Y., Tong, S., Wang, L., & Wang, J. (2026). Health Monitoring with Earables: A Survey. *ACM Transactions on Internet of Things*, 7(2), 1-36. Available at: <https://doi.org/10.1145/3779303>.

Ettaloui, N., Arezki, S., & Gadi, T. (2023). An overview of blockchain-based electronic health records and compliance with GDPR and HIPAA. *Data and Metadata*, 2(1), 166-178. Available at: <https://doi.org/10.56294/dm2023166>.

Gao, J., et al. (2025). A transferable hybrid convolutional-Mamba network for cross-population emotion recognition from wearable ECG. *IEEE Internet of Things Journal*, 13(7). DOI: 10.1109/JIOT.2026.3651586.

Gharamohammadi, A. (2024). *A radar-based in-cabin health monitoring system* [Doctoral thesis, University of Waterloo]. UWSpace. Available at: <http://hdl.handle.net/10012/20572>.

Hancock, P.A. (2022). Avoiding adverse autonomous agent actions. *Human-Computer Interaction*, 37(3), 211-236. Available at: <https://doi.org/10.1080/07370024.2021.1970556>.

Harari, G.M., & Gosling, S.D. (2023). Understanding behaviours in context using mobile sensing. *Nature Reviews Psychology*, 2(12), 767-779. Available at: <https://doi.org/10.1038/s44159-023-00235-3>.

Issaoui, A., Örtensjö, J., & Islam, M.S. (2023). Exploring the General Data Protection Regulation (GDPR) compliance in cloud services: insights from Swedish public organizations on privacy compliance. *Future Business Journal*, 9(1), 107. Available at: <https://doi.org/10.1186/s43093-023-00285-2>.

Ko, H.Y.K., Tripathi, N.K., Mozumder, C., Muengtaweepongsa, S., & Pal, I. (2023). Real-time remote patient monitoring and alarming system for noncommunicable lifestyle diseases. *International Journal of Telemedicine and Applications*, 2023(1), 9965226. Available at: <https://doi.org/10.1155/2023/9965226>.

Kong, L., et al. (2022). Edge-computing-driven internet of things: A survey. *ACM computing surveys*, 55(8), 1-41. Available at: <https://doi.org/10.1145/3555308>.

Kuntardjo, C., Hernoko, A.Y., & Anand, G. (2023). Transparency Principle to realize justice in health service. *Malaysian Journal of Medicine & Health Sciences*, 19. Available at: <https://www.scopus.com/pages/publications/85159212360>.

Lundy, A., et al. (2026). Human factors: Organizational behavioral perspectives in healthcare cybersecurity for Applied Behavior Analysis (ABA) therapists. Chapter in *Legal and ethical challenges in data privacy rights and cybersecurity* (pp. 75-98). IGI Global.

Malatji, M. (2023, January). Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. In *2023 International conference on cyber management and engineering (CyMaEn)* (pp. 117-122). IEEE. Available at: <https://doi.org/10.1109/CyMaEn57228.2023.10051114>.

Mehl, M.R., et al. (2023). *Mobile sensing in psychology: Methods and applications*. Guilford Publications.

Mishra, A.D., Thakral, B., Jijja, A., & Sharma, N. (2024). Real-time vital signs monitoring and data management using a Low-Cost IoT-based health monitoring system. *Journal of Health Management*, 26(3), 449-459. Available at: <https://doi.org/10.1177/09720634241246926>.

Natarajan, M., et al. (2023). Human-robot teaming: grand challenges. *Current Robotics Reports*, 4(3), 81-100. Available at: <https://doi.org/10.1007/s43154-023-00103-1>.

Pannunzio, V., et al. (2024). Patient and staff experience of remote patient monitoring – what to measure and how: systematic review. *Journal of Medical Internet Research*, 26, e48463. Available at: <https://doi.org/10.2196/48463>.

Parasuraman, R. (2015). *Neuroergonomic perspectives on human systems integration: Mental workload, vigilance, adaptive automation, and training*. In D.A. Boehm-Davis, F.T. Durso, & J.D. Lee (Eds.), *APA handbook of human systems integration* (pp. 163-176). American Psychological Association.

Piispanen, J.R., Myllyviita, T., Vakkuri, V., & Rousi, R. (2024). Smoke screens and scapegoats: The reality of General Data Protection Regulation Compliance—privacy and ethics in the case of Replika AI. *arXiv preprint arXiv:2411.04490*. Available at: <https://doi.org/10.48550/arXiv.2411.04490>.

Prabakaran, A., & Rufus, E. (2022). Review on the wearable health-care monitoring system with robust motion artifacts reduction techniques. *Sensor Review*, 42(1), 19-38. Available at: <https://doi.org/10.1108/SR-05-2021-0150>.

Rahardja, U., Ngad, M.A., Millah, S., Harahap, E.P., & Aini, Q. (2022, September). Blockchain application in educational certificates and verification compliant with general data protection regulations. In *2022 10th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-7). IEEE. Available at: <https://doi.org/10.1109/CITSM56380.2022.9935909>.

Ryalat, M., Almtireen, N., Al-refai, G., Elmoaqet, H., & Rawashdeh, N. (2025). Research and education in robotics: A comprehensive review, trends, challenges, and future directions. *Journal of Sensor and Actuator Networks*, 14(4), 76. Available at: <https://doi.org/10.3390/jsan14040076>.

Schäfer, A., Esterbauer, R., & Kubicek, B. (2024). Trusting robots: A relational trust definition based on human intentionality. *Humanities and Social Sciences Communications*, 11(1), 1-13. Available at: <https://doi.org/10.1057/s41599-024-03897-3>.

Schroepfer, P. (2025). *Bridging realms: Advancing multi-robot systems through trust, shared mental models, and user-centric interfaces* (Publication No. 32309769) [Doctoral dissertation, Georgia Institute of Technology]. ProQuest Dissertations & Theses Global.

Song, W.K., Bird, E., McNerney, G., & Richardson, K. (2026). Categorizing smart farm equipment for sustainable and human-centric food production: A comprehensive review encompassing terrestrial agriculture and aquaculture. *Green Transition and Sustainable Development*, 2(1), 1-17. Available at: [https://doi.org/10.61093/gtsd.2\(1\).1-17.2026](https://doi.org/10.61093/gtsd.2(1).1-17.2026).

Tarek, J.H., & Paran, M.S. (2024). Quantitative assessment of automation and control strategies for performance optimization in US industrial plants. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 4(1), 169-205. Available at: <https://doi.org/10.63125/eqfz8220>.

Urrea, C., & Kern, J. (2025). Recent advances and challenges in industrial robotics: A systematic review of technological trends and emerging applications. *Processes*, 13(3), 832. Available at: <https://doi.org/10.3390/pr13030832>.

Vejjanugraha, P., & Pawasarn, W. (2025, November). Technician utilization-based analysis of Mean Time to Detect (MTTD) and Mean Time to Repair (MTTR) for a strategic approach in failure corrective maintenance system (FCMS). In *2025 20th International Joint Symposium on Artificial Intelligence and Natural Language Processing (iSAI-NLP)* (pp. 1-5). IEEE. Available at: <https://doi.org/10.1109/iSAI-NLP66160.2025.11320480>.

Vishweshwara, A., & Ramya, R. (2025). Transforming telemedicine: Reducing latency through edge computing and 5G—A review. *Biomedical Materials & Devices*, 1-14. Available at: <https://doi.org/10.1007/s44174-025-00312-6>.

Wang, J., Lin, S., & Liu, A. (2023). Bio-inspired perception and navigation of service robots in indoor environments: A review. *Biomimetics*, 8(4), 350. Available at: <https://doi.org/10.3390/biomimetics8040350>.

Wang, W., Gao, G., & Agarwal, R. (2024). Friend or foe? Teaming between artificial intelligence and workers with variation in experience. *Management Science*, 70(9), 5753-5775. Available at: <https://doi.org/10.1287/mnsc.2021.00588>.

Xu, W., & Gao, Z. (2024). An intelligent sociotechnical systems (iSTS) framework: Enabling a hierarchical human-centered AI (hHCAI) approach. *IEEE transactions on technology and society*, 6(1), 31-46. Available at: <https://doi.org/10.1109/TTS.2024.3486254>.

Zahedi, Z., Sengupta, S., & Kambhampati, S. (2024). A game-theoretic model of trust in human–robot teaming: Guiding human observation strategy for monitoring robot behavior. *IEEE Transactions on Human-Machine Systems*, 55(1), 37-47. Available at: <https://doi.org/10.1109/THMS.2024.3488559>.

Zhang, S., Chen, Y., Hua, L., He, Y., & Zhang, L. (2025). Uncovering the tacit: a qualitative study of obstetric nurses' risk recognition and decision-making in perinatal care. *Frontiers in Medicine*, 12, 1701924. Available at: <https://doi.org/10.3389/fmed.2025.1701924>.

Zheng, P., Li, S., Fan, J., Li, C., & Wang, L. (2023). A collaborative intelligence-based approach for handling human-robot collaboration uncertainties. *CIRP Annals*, 72(1), 1-4. Available at: <https://doi.org/10.1016/j.cirp.2023.04.057>.