EAI Endorsed Transactions
on Security and Safety
Research Article EAI.EU

Enhancing Information Security in Industry 5.0: A Human-Centric LL-ISMS Framework to Bridge PDCA Gaps

Masoud Hayeri Khyavi[1*]

[1] Department of ICT Security, ICT Research Institute (ITRC), TEHRAN, IRAN

Abstract

Industry 5.0 is transforming the industrial paradigm by placing humans at the center of manufacturing and service processes. This approach, which emphasizes the synergistic collaboration between humans and cyber-physical systems (CPS), goes beyond the purely productivity-oriented goals of Industry 4.0 and prioritizes sustainability, resilience, and human well-being. However, the evolving nature of human-machine interactions poses complex security challenges. Traditional information security management systems (ISMS), which are based on the PDCA cycle and top-down approaches, face limitations in adapting to operational dynamics and receiving qualitative feedback from frontline workers. This paper introduces a complementary human-centric framework, "Low-Level ISMS" (LL-ISMS), while identifying emerging security risks in these complex ecosystems. The framework operates as a bottom-up feedback loop and focuses on four key stages: purposeful preparation (Do'), practical perception (Feel), critical analysis (Think), and active participation (Help). By connecting operational insights from employees to management decisions, LL-ISMS significantly increases the effectiveness of security management in Industry 5.0 environments and fosters a shared and dynamic security culture.

Keywords: Industry 4.0, Industry 5.0, Security, Information Security Management System (ISMS), Low-Level ISMS (LL-ISMS), PDCA Cycle, Human-Robot Collaboration, Cybersecurity Resilience

Received on 21 October 2025, accepted on 26 May 2026, published on 03 June 2026

doi: 10.4108/eetss.10667

*Corresponding author. Email: m.hayery@itrc.ac.ir

1. Introduction

Previous industrial revolutions focused on automation and efficiency. Industry 4.0 took this trend further by integrating technologies such as the Industrial Internet of Things (IIoT), big data, artificial intelligence (AI), and cloud computing [3]. In contrast, Industry 5.0 represents a fundamental shift that brings humans back into the process [2]. Collaborative robots (cobots) work alongside humans, intelligent systems help make local decisions, and data is collected and analyzed at scale to generate outcomes tailored to human needs.

This rich synergy, while promising, increases cybersecurity risks in complex cyber-physical-human ecosystems. Traditional ISMS models, mainly based on ISO 27001 and the PDCA cycle [6], provide robust risk management frameworks, but they are largely top-down and policy-based, focusing on formal controls. As a result, they inadequately capture dynamic operator behaviors, daily system interactions, and experiential feedback from frontline employees. This paper argues for the need for an operational and perceptual layer that directly engages employees and conveys their feedback to management. The LL-ISMS framework complements the PDCA model to transform ISMS into a dynamic, human-centered, and actionable system [1].

1.1 The Human-Centric Essence of Industry 5.0

Industry 5.0 extends the foundation of technology established by the 4.0 industry through the introduction of human creativity, situational awareness, and emotional intelligence to intelligent production environments. The European Commission explicitly frames Industry 5.0 as a human-centric, sustainable, and resilience industrial model, with an emphasis on balanced co-operation among state-of-the-art technology and human value systems. The individual three pillars support the evolution of contemporary production differently:

- Human-Centric: Humans act as decision-makers and co-designers in operations, promoting dignity, well-being, and inclusion in human-machine teams. For instance, operators guide cobots in adaptive assembly lines, requiring intuitive interfaces to avoid errors [11].
- Sustainable: Emphasizes environmental responsibility and resource efficiency, ensuring technology supports long-term societal and planetary health, such as through energy-optimized AI-driven processes [2].
- Resilient: Embeds adaptability and recovery in socio-technical systems to withstand disruptions, from cyber-attacks to supply-chain issues, via real-time human-AI collaboration [11].

These pillars necessitate security frameworks that evolve beyond technical controls to include human perceptual and behavioral dynamics [11].

2. Security and Technological Challenges in Industry 5.0 Ecosystems

The human-centric focus of Industry 5.0 shifts security risks across the spectrum of technical challenges to complex human-machine-cyber situations. Addressing these security challenges will entail careful engagement from the management and operational levels. This is the body text with indent. This is the body text with indent. This is the body text with indent. This is the body text with indent. This is the body text with indent. This is the body text with indent. This is the body text with indent. This is the body text with indent. This is the body text with indent. This is the body text with indent. This is the body text with indent. This is the body text with indent.

2.1. Increasing Complexity of Trust Boundaries

In Industry 4.0, trust boundaries were primarily defined between information technology (IT) and operational technology (OT) networks [3]. In Industry 5.0, however, these boundaries have become blurred and fluid with the widespread connectivity of edge devices, sensors, and collaborative robots (cobots). A cyber-physical attack can manipulate sensor data (e.g., the temperature of an oven or the position of a robotic arm) and causing the robot to issue malicious commands that cause physical damage or product quality degradation. On the other hand, over-reliance on intelligent systems becomes a vulnerability. If an operator follows the advice of an AI system that has been secretly manipulated by an attacker, they could inadvertently open a security backdoor or stop a critical process [4].

2.2 AI Vulnerabilities

Artificial intelligence (AI) plays a critical role in real-time decision-making in Industry 5.0, but its inherent vulnerabilities pose serious risks to process security:

- Adversarial Attacks: Small, subtle changes in inputs (such as quality control images or sensor data) can cause machine learning models to make completely wrong decisions [5]. For example, a small change in the pixels of a part image can cause an AI-based quality control system to classify it as healthy when it is actually defective.

$$Input_{Adversarial} = Input_{Original} + \delta$$

Where δ is a minimal, crafted noise vector optimized to evade detection while altering outputs [5].

- Data Poisoning: Injecting malicious data into a model during its training or reinforcement phase can permanently degrade its performance and compromise security [8]. For example, one could poison a cooperative robot by training it to exhibit unsafe behaviors under certain conditions.

2.3 Active Human Role and Cognitive Risks

Unlike full automation, Industry 5.0 leaves crucial tasks such as machine monitoring, complex problem-solving, and final interaction to humans. This shift places the human-machine interface at the centre of modern manufacturing operations [9], which requires a renewed focus on cognitive security aspects.

- Decision Fatigue: Simultaneously monitoring multiple intelligent systems and analysing large amounts of information can be mentally exhausting, leading to reduced alertness and ignoring important security alerts [7].
- Advanced Social Engineering: Using contextual information from the workplace (such as understanding interactions between operators and

robots), attackers can design highly convincing phishing or psychological manipulation scenarios that target key operators. For example, Attackers exploit workplace context for targeted phishing, e.g., fake "cobotsupport@company.com" emails prompting script execution [7].

Transitioning to management, these risks highlight the need for experiential security layers [1].

2.4 Compliance and Privacy Concerns in Operational Data

The core tenet of human-centricity necessitates extensive data collection on performance, task completion times, stress levels (potentially via wearables), and interaction patterns. This extensive biometric and performance data collection introduces complex privacy issues under stringent regulations like GDPR. Ensuring the integrity and confidentiality of workers' sensitive operational and personal data requires rigorous ISMS controls, especially concerning data retention, access logging, and transparent feedback channels regarding how personal data influences operational security decisions [6].

2.5. Evolution of Information Security Management Systems (ISMS)

From a management system perspective, the implementation and governance structure of security remain crucial. The ISO/IEC 27001:2022 standard [6] remains the central norm guiding policy based and audit-oriented ISMS development. Its structure mandates the application of the Plan-Do-Check-Act (PDCA) cycle to ensure continuous improvement of the Information Security Management System (ISMS). Nevertheless, classical PDCA oriented systems were criticized for inadequate bottom-up feedback. Audits based on ISO 27001 tend to rely on documented evidence gathered through formal channels, often failing to capture the nuances of day-to-day operational security challenges faced by frontline staff. [1] Proposed the idea of a Low-Level ISMS (LL-ISMS) framework.

This framework explicitly seeks to complement the PDCA cycle through participatory feedback mechanisms involving frontline workers. The LL-ISMS concept recognizes that security risks manifest operationally before they are visible in management documentation, necessitating structured, low-level reporting and feedback loops. This concept laid the groundwork for perception-based security improvement, moving security management from a purely compliance-driven activity to an experiential discipline [1].

The need for dynamic adaptation in intelligent industrial environments further underscores the limitations of static policy enforcement. Subsequent research by [8] on reinforcement learning poisoning and adversarial behaviour demonstrated the need for continuous and adaptive protection models within intelligent industrial environments. Attacks on the learning mechanisms themselves—where manipulated data systematically degrades the AI's future policy decisions—require real-time detection and rapid policy adjustment that traditional, slower PDCA cycles cannot easily accommodate.

2.6. Synthesis and Research Gap

Literature evolves from Industry 4.0's connectivity [3] to Industry 5.0's human integration [2], revealing divides in governance [6], human factors [4, 7], and adaptive tech [8]. This study bridges these by integrating PDCA with LL-ISMS for resilient, human-aligned security [1].

The literature clearly shows a divide:

1. Strategic Governance: Dominated by ISO 27001 and the top-down PDCA structure [6].
2. Operational Human Factors: Detailed analyses of collaboration risks [4] and cognitive security issues [7].
3. Adaptive Technology: Recognition of the need for dynamic resilience against advanced machine learning attacks [8].

The current study addresses the gap between these domains. Specifically, it builds upon these directions by merging the strategic PDCA model (ensuring formal governance and auditability) with the operational LL-ISMS layer (incorporating experiential, bottom-up feedback from human-machine interfaces). This integration is designed to bridge traditional governance structures with crucial experiential feedback loops, ultimately aiming to achieve truly resilient and sustainable information security aligned with the core tenets of Industry 5.0.

3. Related Works

Several studies have explored the evolution of industrial security frameworks leading to human centric management approaches, setting the stage for LL-ISMS:

Studies trace security frameworks toward human-centric approaches: Lasi et al. [3] laid Industry 4.0's ICT foundations, necessitating cybersecurity maturity. The European Commission [2] positions Industry 5.0 as value-driven, requiring human-reflective security. Hayeri Khyavi and Rahimi [1] introduced LL-ISMS for feedback loops bridging policy and operations. Hong et al. [4] analyzed human-robot collaboration risks, advocating real-time validation—data LL-ISMS captures. Baruwal et al. [7] explored cognitive risks in human-AI teams, addressed by LL-ISMS's Feel and Think phases. Ma et al. [8] highlighted policy poisoning, mitigated via human-validated AI outputs. Financier Worldwide [9] emphasized responsive interfaces, underscoring LL-ISMS's frontline dynamics. Recent implementations in manufacturing validate this shift [11]. Collectively, these underscore

integrating operational and cognitive insights for Industry 5.0 security [12].These contributions collectively illustrate the transition from purely technical governance to human inclusive security management, underscoring the necessity of frameworks integrating operational, cognitive, and organizational insights.

4. The PDCA Cycle: Foundational Management Framework

A fundamental management framework, the ISMS serves as a global standard and promotes a proactive and continuous protection strategy based on the PDCA model [6]:

- **Plan:** Define the scope of the ISMS, conduct thorough risk assessments that include technological and organizational risks, set security objectives, and create policies that meet legal and contractual requirements. In Industry 5.0, this phase includes risks associated with human-machine interactions.
- **Do:** Implement planned technical, physical, and organizational controls, including security training, firewalls, access management, and incident response.
- **Check:** Continuously assess the effectiveness of controls through internal and external audits, security incident reports, and key performance indicators.
- **Act:** Take corrective and preventive actions based on the results of the review phase, and drive continuous improvement in processes and controls.

4.1 Limitations of PDCA in the context of Industry 5.0

The PDCA cycle is essential as a top-down strategic framework for defining policies and monitoring technical compliance. However, in the human-centric environments of Industry 5.0, the cycle has blind spots**:**

- Operational feedback gap: The Do phase focuses primarily on implementing procedures and neglects qualitative feedback on the impact of controls on user experience and everyday behaviors. For example, a security control may be effective on paper, but in practice, it is so cumbersome that employees look for ways to bypass it**.**
- Focus on technical compliance rather than behavioral compliance: The Check phase emphasizes technical compliance (such as "Are security patches installed?") over behavioral compliance (such as "Do employees understand why these patches are important and participate in reporting suspicious cases?").

5. The Complementary LL-ISMS Framework: Human-Centric Layer

LL-ISMS acts as a bottom-up complementary cycle, bridging high-level policy intentions and the lived reality of operational security [1]. The LL-ISMS framework introduces a human-centric operational layer that complements traditional PDCA-based ISMS structures. While the PDCA cycle focuses on strategic planning, policy definition, and formal review processes, LL-ISMS captures operational insights directly from employees who interact with security controls in their daily work. By incorporating bottom-up feedback regarding usability, workflow disruptions, and perceived security effectiveness, LL-ISMS helps bridge the gap between high-level security policies and real operational conditions. It focuses on capturing perceptual, behavioral, and situational data. LL-ISMS introduces four iterative phases:

5.1 Do' (Purposeful Preparation and Execution)

This phase, which comes immediately after the Plan phase and coincides with the Do phase of the PDCA cycle, goes beyond traditional training and focuses on preparing employees mentally and practically to adopt the new controls:

- Explain the "why": Rather than simply stating a command (e.g., "From now on, the password must be changed every 30 days"), it should be clearly explained why the control is being implemented. For example: "Given the increase in targeted brute-force attacks against robot control systems, periodic password changes reduce the risk of unauthorized access to robotic arms and physical incidents."
- Simulation and Practical Practice: For complex controls, such as access protocols for collaborative robots, interactive simulations or security labs can be provided so that employees can practice the controls in a secure environment and reduce their resistance to change.

Metrics: like Pre/post-training quizzes[10].

5.2 Feel (Practical Experience and Understanding)

After implementing controls and before formal reviews (the Check phase of PDCA), this phase allows employees to experience and evaluate the impact of security controls on their efficiency, job satisfaction, and workflow:

- Qualitative Data Collection (SUE): Through short surveys, informal interviews, or workshops, qualitative data on "Security User Experience" (SUE) is collected. Questions such as: "Which security control slows you down?", "Is the multi-factor authentication process confusing to log into the bot

console?". In this framework, SUE (Security User Experience) refers to employees' perceptions of how security controls affect their daily tasks, including usability, delays, operational friction, and perceived effectiveness. SUE can be captured through short surveys, informal interviews, or workshops to systematically incorporate frontline feedback into continuous improvement.

- Establish rapid feedback channels: Create quick and accessible channels (such as a mobile app, a simple dashboard, or even a QR code on the side of the device) for reporting problems or ineffective controls. This prevents "shadow solutions" that employees devise to circumvent controls.

Metrics: like Net Promoter Score for controls [10].

5.3 Think (Organizational Reflection and Analysis)

This phase, which falls between the Check and Act phases of the PDCA cycle, encourages deeper analysis of the success or failure of controls with employee participation, rather than focusing solely on audit reports:

- Micro-Incident Analysis Sessions: Instead of focusing solely on large incidents, teams can analyze minor security alerts (such as a failed login attempt) from an operational perspective. Perhaps the failed attempt was due to a new password being too complex, rather than an actual attack.
- Leverage Frontline Insights for Risk Modeling: Insights from frontline employees can help uncover overlooked threats. For example, an operator might report that a particular peripheral device (such as a barcode scanner) is frequently disconnecting and reconnecting, which could be a vulnerability for malicious command injection.

Metrics: Incident resolution time reduction [10].

5.4 Help (Support Collaborative Improvement)

The outputs from the previous three phases feed directly into the next Plan phase in the PDCA cycle, completing the feedback loop. This phase transforms employee engagement from a passive activity to an active responsibility:

- Suggestion Scoring Systems: A scoring or reward system can be implemented for suggestions that significantly reduce risks or increase efficiency. This encourages employees to provide high-quality input.
- Review Draft Policies: Draft new security policies are provided to frontline employee representatives for review before finalization to ensure that they are practical and enforceable in the dynamic Industry 5.0 environment.

As shown in Figure 1, the LL-ISMS cycle acts as an operational loop within the strategic PDCA cycle, creating key points of contact between the two.

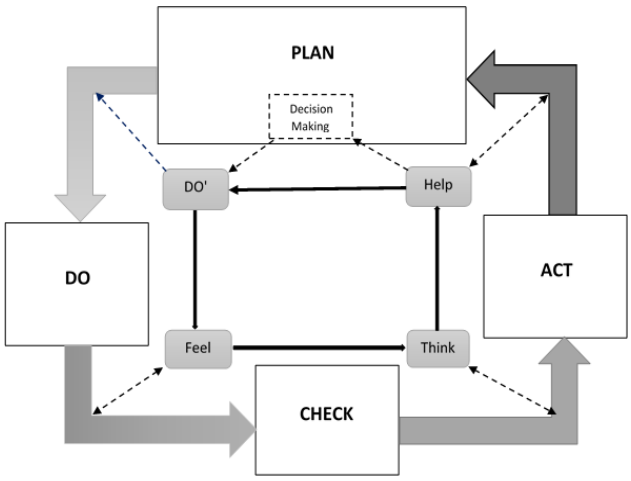

Figure 1. Integration of the LL-ISMS cycle with the traditional PDCA-based ISMS framework

The LL-ISMS loop functions as a human-centric operational layer within the broader PDCA management cycle, collecting frontline security experiences and user feedback and translating them into insights that support continuous improvement of organizational security practices.

6. Effects of LL-ISMS and PDCA Integration in Industry 5.0

The synergy between the top-down mandates of PDCA and the bottom-up experiential learning of LL-ISMS creates a robust security posture necessary for Industry 5.0's socio-technical complexity.

6.1 Enhancing Resilience against Human Errors

Many human errors are caused by misunderstanding or intentional circumvention of policies due to their ineffectiveness. The Do' and Feel phases of LL-ISMS help to find the root causes of these behaviors. For example, if the multi-factor authentication (MFA) process is designed to be too complex for an operator who needs to quickly access multiple systems, the likelihood that he will share his password with a colleague or write it on a sticker increases. Feedback from the Feel phase can help the security team suggest lower-friction alternatives, such as biometrics or physical tokens (two-factor) that are both secure and user-friendly.

6.2 Dynamic Cyber Risk Management

In dynamic operational environments where threats and configurations are rapidly evolving, relying on traditional, annual audit cycles is impossible. By creating a continuous communication channel from the frontline, LL-ISMS reduces threat dwell time and detection latency. An employee may notice unusual behavior from a bot long before central monitoring systems identify it as a threat.

6.3 Strengthening Security Culture as a Shared Value

The effectiveness of an ISMS largely relies on how well it is embraced culturally. LL-ISMS fosters a feeling of ownership by showing that employee contributions can influence official policies. This framework shifts security from being a collection of enforced regulations to a collective duty where everyone is engaged in safeguarding the organization [1].

6.4 Integrative Perspective: Linking PDCA+LL-ISMS to the Pillars of Industry 5.0

The dual-cycle model (PDCA reinforced by LL-ISMS) operationalizes the three pillars of Industry 5.0. The Human-centric principle corresponds to the Do' and Feel phases, where frontline engagement transforms security control adoption. Resilience emerges from the Think and Help phases, enabling continuous adaptation through collaborative learning. Finally, Sustainability is achieved when PDCA governance is coupled with bottom-up LL-ISMS feedback loops, ensuring that information security practices evolve harmoniously with human and technological dimensions (Table 1).

Table 1. Effects of LL-ISMS and PDCA Integration in Industry 5.0

Industry 5.0 Pillar	Corresponding Phase in PDCA + LL-ISMS Cycle	Nature of Relationship
Human-centric	Do' and Feel phases	Direct worker involvement in preparation, experience, and feedback on implemented security controls; establishes human-centered decision-making.
Resilient	Think and Help phases	Enables adaptive learning and collective problem-solving; enhances organizational resilience through continuous improvement and error recovery.
Sustainable	Entire PDCA cycle reinforced by LL-ISMS	Transforms security management from a reactive task into an ongoing cultural and systemic process; ensures long-term sustainability of security operations.

The LL-ISMS cycle ensures that resilience is not just about system recovery (PDCA Act), but about preventing the failure from happening due to human-system misalignment (LL-ISMS Do' and Feel).

7. Conclusion and Future Work

The fusion of human ingenuity and advanced technology in Industry 5.0 not only amplifies productivity and innovation but also elevates cybersecurity to unprecedented levels of complexity. Traditional PDCA-based ISMS frameworks provide essential governance and strategic oversight; however, their top-down structure often struggles to capture the dynamic and experiential realities of frontline operations.

By integrating LL-ISMS as a complementary human-centric layer—through its iterative phases of Do' (preparation), Feel (perception), Think (analysis), and Help (collaboration)—this study proposes a hybrid model that transforms ISMS from a compliance-driven mechanism into a more adaptive and resilient socio-technical ecosystem. This integration helps bridge critical gaps in PDCA-based governance by incorporating operational feedback from employees who directly interact with security controls.

Compared with conventional risk-based continuous monitoring frameworks and other adaptive ISMS approaches, LL-ISMS places greater emphasis on frontline human experience and bottom-up feedback. While many adaptive models focus primarily on automated risk detection and technical indicators, LL-ISMS complements these mechanisms by capturing operational friction, perceived security burden, and contextual issues that may not be visible in technical logs alone. This human-centric orientation makes the framework particularly suitable for Industry 5.0 environments characterized by close human–machine collaboration.

Through this synergy between strategic governance and operational insight, organizations can improve security awareness, strengthen resilience against emerging AI-driven threats, and cultivate trust in human–machine interactions. Ultimately, the PDCA + LL-ISMS integration supports a security culture aligned with the core values of Industry 5.0, emphasizing human well-being, resilience, and sustainable technological development.

Future research should focus on empirically validating the LL-ISMS framework through pilot implementations in real-world Industry 5.0 environments, such as IIoT-enabled factories. Such studies could provide quantitative evidence by evaluating metrics such as incident response time, reduction of human-induced security errors, user satisfaction with security controls, and the effectiveness of feedback-driven improvements. Additionally, integrating AI-driven analytics to support real-time Security User Experience (SUE) dashboards could further enhance the responsiveness of the LL-ISMS feedback loop. Exploring applications of the framework in other sectors—such as healthcare, logistics, or smart infrastructure—may also help assess its broader applicability and generalizability.

References

[1] Khyavi MH, Rahimi M. The missing circle of ISMS (LL-ISMS). In: Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research; 2015 Jun 4–6; Newport Beach, CA, USA. New York: ACM; 2015. p. 73–77.

[2] European Commission. Industry 5.0: Towards a sustainable, human-centric and resilient European industry [Internet]. Brussels: European Commission; 2021 [cited 2026 May 29]. Available from: https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/industry-50-towards-more-sustainable-resilient-and-human-centric-industry-2021-01-07_en

[3] Lasi H, Fettke P, Kemper HG, Feld T, Hoffmann M. Industry 4.0. Bus Inf Syst Eng. 2014;6(4):239–242.

[4] Hong Y, Wu J, Guan X. A survey of joint security-safety for function, information and human in Industry 5.0. Secur Saf. 2025; 4:2024014.

[5] Goodfellow I, Shlens J, Szegedy C. Explaining and harnessing adversarial examples. In: 3rd International Conference on Learning Representations (ICLR); 2015 May 7–9; San Diego, CA, USA.

[6] International Organization for Standardization. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO; 2022.

[7] Chhetri MB, Tariq S, Singh R, Jalalvand F, Paris C, Nepal S. Towards human-AI teaming to mitigate alert fatigue in security operations centres. ACM Trans Internet Technol. 2024;24(3):1–22.

[8] Ma Y, Zhang X, Zhu X, et al. Policy poisoning in batch reinforcement learning and control. In: Advances in Neural Information Processing Systems 32 (NeurIPS 2019); 2019 Dec 8–14; Vancouver, Canada. p. 14570–14580.

[9] Future of work: the human-machine interface [Internet]. Financier Worldwide; 2024 [cited 2026 May 29]. Available from: https://www.financierworldwide.com/future-of-work-the-human-machine-interface

[10] Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Comput Secur. 2014; 42:165–176.

[11] Nahavandi S. Industry 5.0—A human-centric solution. Sustainability. 2019;11(16):4371.

[12] Adel A. Future of Industry 5.0 in society: human-centric solutions, challenges and prospective research areas. J Cloud Comput. 2022;11(1):40.