Protective Security Within Industry 5.0: A Socio-Technical Perspective

Robert Kennedy

University of Portsmouth, School of Criminology and Criminal Justice, Portsmouth, United Kingdom

Abstract

Abstract
The transition toward Industry 5.0 expands an organization's attack surface, exposing hyper-interconnected digital-physical systems to converged, multi-vector threats. This position paper argues that traditional, siloed risk management frameworks are structurally inadequate for protecting these collaborative human-machine ecosystems. To bridge these defensive gaps, security practitioners must move away from purely technology-centric controls and adopt a converged protective security paradigm. By embedding Enterprise Security Risk Management (ESRM) principles within a Socio-Technical System Design (STS-D) framework, organizations can synchronously optimize human behavior and technical controls. Ultimately, this paper demonstrates that a comprehensive socio-technical perspective is an operational necessity to engineer system resilience and cultivate human-machine trust.

Keywords
Industry 5.0, Socio-Technical System Design, Protective Security, ESRM, Security Convergence.

1. Introduction

Industry 5.0 is underpinned by the harmonious collaboration between humans and machines, incorporating the core values of sustainability, human-centricity, and resilience [2,5,43,62]. As many societies aspire to progress from the current Industry 4.0 framework toward Industry 5.0, this transition introduces an enhanced attack surface for adversaries to target. Industry 5.0 emphasizes collaboration, advocating that technology can be used to enhance human capabilities [3,5]. This enhancement occurs via the interaction of technological systems with human operators, who ultimately provide the core value to the system [19].

Parallel advances in Artificial Intelligence (AI), Internet of Things (IoT) technologies, and big data analytics have driven the progression toward Industry 5.0, highlighting the profound convergence of the physical and digital worlds [38]. Industry 5.0 aims to support higher levels of automation, customization, and efficiency while safeguarding workers in high-risk

STPIS2026: Proceedings of the 12th International Conference on Socio-Technical Perspectives in IS, September 16-17th L'Aquila, Italy

Robert.kennedy1@myport.ac.uk
0009-0008-7818-9372

© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-4334/paper1.pdf

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2026-11-19

operations and ensuring resources are used sustainably [43]. From a critical socio-technical perspective, this physical-digital convergence cannot be analyzed through generalized, technology-centric security models; rather, security must be understood as a context-dependent, emergent property of human activity. Because every human actor possesses an individually unique life-world and interpretation of their operational environment, a system's true security posture shifts continuously through an ongoing dialectic of device use and reflection-upon-use. Ultimately, Industry 5.0 introduces a novel paradigm by prioritizing human well-being, demanding security architectures that respect individual uniqueness and contextual dependencies to enable and support its foundational values [55].

This position paper reviews the following core arguments:

Argument 1: Industry 5.0 technologies will present a greater attack surface for adversaries to target.

Argument 2: Security risk management must adopt a collaborative and converged approach, incorporating the primary disciplines of protective security to mitigate Industry 5.0-enabled attack vectors.

Argument 3: Socio-technical system design (STS-D) does not act as an independent security solution but rather serves as an analytical and design approach to support the co-creation of contextually appropriate security arrangements.

To substantiate these claims, the next section of this paper analyses the specific impacts that Industry 5.0 technologies exert on an organization's attack surface. This is followed by an evaluation of the protective security requirements inherent to Industry 5.0. A subsequent section examines these dynamics from a socio-technical systems perspective, leading to a final conclusion summarizing the core insights of this position paper.

2. Industry 5.0 Enabling Technologies Influence on an Organizations Attack Surface

Xu et al. [62] identify that smart materials, bio-inspired technology, and structural enhancements to data storage, transmission, and analysis capabilities to improve system interoperability underpin Industry 5.0. This paradigm is further sustained by the use of Artificial Intelligence (AI) to detect causality within systems through actionable intelligence, alongside the deployment of energy-efficient technologies.

Complementing this baseline, Raja Santhi and Muthuswamy [49] identify the following eleven core Industry 5.0 enabling technologies:

- Collaborative robots (cobots): Robotic systems designed to collaborate and work under human supervision, supported by advancements in AI, Machine Learning (ML), and conventional robotics.
- Smart sensors: Advanced sensor nodes that build on conventional hardware by incorporating independent data collection, data conversion/processing, and external communication capabilities.

- Digital twins: Accurate digital replications of physical systems that employ real-time data from the original physical asset to simulate operational behavior.
- Internet of Everything (IoE): An expansive framework connecting data, processes, people, and physical things, differing from the Internet of Things (IoT) which focuses strictly on physical device connectivity.
- Artificial Intelligence of Things (AIoT): The evolution of IoT devices to provide connected hardware with localized decision-making and autonomous problem-solving capabilities.
- Blockchain: A distributed digital ledger designed to securely store and track both tangible and intangible assets within a business network.
- Edge/Fog computing: Architecture that addresses cloud computing inefficiencies by distributing processing and storage frameworks closer to the local network data source.
- Cognitive computing: Systems designed to mimic human thought processes to solve highly complex organizational challenges.
- 6G and beyond: Next-generation wireless networks required to meet the extreme connectivity demands of intelligent devices and services.
- Augmented reality (AR) / Mixed reality (MR): Immersive visualization tools that superimpose digital data onto physical environments or blend real and virtual worlds to enable interactive manipulation.
- Holography: Three-dimensional tools utilized to visualize and reproduce physical objects with high geometric accuracy.

Industry 5.0 establishes a highly interconnected architecture where ubiquitous devices enable massive volumes of telemetry to move across distributed networks [1,54]. From a critical socio-technical lens, this hyper-interconnected operational landscape does not merely shift data; it fundamentally disrupts individual sense-making and the multiple levels of contextual dependencies through which workers interpret reality [18]. As Checkland and Holwell [22] theorize, raw data stream inputs are structurally distinct from the actionable information created when a human actor interprets those signals within a specific operational context. When technologies like Digital Twins or AIoT abstract physical operations into algorithmic models, they introduce severe interpretive risks. Because human beings communicate with intentions that are deeply context-dependent, any opacity or "black-box" behavior within cognitive computing artifacts impairs the worker's ability to maintain a reliable baseline of what constitutes normal versus anomalous system activity [18, 54].

Consequently, the emergence of ambient IoE and AIoT networks will likely expose organizations to a vastly expanded and unpredictable attack surface for adversaries to exploit [1,27,52]. An organization's structural vulnerability to targeted cyber-attacks scales exponentially with the deployment of these technologies, directly threatening the systemic stability of an organization. Crucially, within a robust risk management paradigm, confidentiality, integrity, and availability do not represent the strategic objectives of security in themselves; rather, they are core security properties of the technical artifact. The true strategic objective of the enterprise is to dynamically maintain an acceptable level of risk relative to these properties amid constant operational uncertainty [1,27,43,52,55,57].

Critical vulnerabilities observed during the deployment of legacy IoT nodes have already demonstrated how easily cyber-physical attack vectors can be compromised when technical design overlooks the social layer [7,37]. In an Industry 5.0 setting, this vulnerability becomes an emergent property of the human-machine interaction itself. Highly interconnected IoT environments introduce significant internal threats [50]. Critically, this internal risk is exacerbated by the integration of autonomous AI agents [29,31] and decision-making code architectures [59]. These technologies should not be viewed as independent 'insiders,' but rather as complex algorithmic artifacts that fundamentally distort informational transparency, altering the context in which human operators make safety decisions. Therefore, it would be naive for modern strategies to treat security purely as a static IT boundary; instead, risk management frameworks must be designed as flexible, open socio-technical work systems capable of navigating the complex intersection of physical, technical, and human-centric insider vectors [29].

3. Industry 5.0 Protective Security

Industry 5.0 requires effective security embedded within systems from the outset [5,27, 46]. However, to deliver effective defenses, the underlying causes of insecurity must be understood in the first instance to support organizations in both predicting and managing security risks [60, 61]. Because Industry 5.0 is built upon harmonious human-machine collaboration and is heavily reliant on the IoE to connect people, data, processes, and physical things [52], it provides adversaries with a diverse range of exploitable vulnerabilities. This architecture will likely encourage adversaries to employ converged or blended attack methodologies [23]. Such complex vectors are challenging to mitigate without a correspondingly converged security risk management paradigm [29, 56]. As Mumford [41] observed, emerging electronic fraud structures and cyber-enabled dangers represent complex societal risks that completely overwhelm established, linear practices of problem-solving.

Within the United Kingdom, the Cabinet Office [21] identifies Protective Security through the distinct domains of Cyber, Personnel, Physical, and Technical security. However, simply grouping these four administrative categories under a single umbrella does not automatically resolve the siloed trap of traditional risk management. If managed as isolated compliance checklists, these domains remain fundamentally fragmented. To achieve genuine convergence, these protective security pillars must be operationalized through an open socio-technical system framework, treating them as interdependent dimensions of a single, unified work system. Schneller et al. [56] reinforce this by arguing that an organization's security function should be fully converged operating as a single, unified model that supports organizational defense through an integrated approach. Traditionally, organizational risk management frameworks have assigned single individuals or siloed teams to develop specific risk mitigations [4]. However, recognizing that security is an intrinsic subset of an organization's overall risk management environment provides an opportunity to understand what systemic interdependencies exist to better manage security risks [4, 26, 32].

The modern operating environment is frequently characterized as volatile, uncertain, complex, and ambiguous (VUCA), requiring a deeply strategic approach to risk management [32]. This landscape has led progressive security practitioners to transition from traditional Enterprise Risk Management (ERM) toward an Enterprise Security Risk Management (ESRM)

philosophy. However, as Bednar, Anderson, and Welch [15] caution, organizational frameworks frequently collapse into an epistemological trap when they assume complex human activities can be managed via linear, predictable controls. When applied to protective security, this means that treating risk mitigation as a standardized checklist rather than a complex method of context-dependent inquiry creates an inconsistent theory of defense, one that fails to account for the unique ways individuals interpret and react to ambient vulnerabilities.

ESRM is a pragmatic process and philosophy that encourages the management of organizational security risks through a holistic framework [9, 48]. Marquez-Tejon et al. [32] identify ESRM as a core element of broader ERM designed to better support collaboration between multiple and varied specialisms across an enterprise. This integration enables improved identification and evaluation of security risks to the business [6] and requires direct input from all aspects of an organization to proactively address vulnerability [9, 6, 33, 35], aligning closely with the foundational principles of security risk management detailed by Harris and Sadok [26]. ESRM is formally defined as:

> *"Enterprise security risk management is the application of fundamental risk principles to manage all security risks, whether related to information, cyber, physical security, asset management, or business continuity, in a comprehensive, holistic, all-encompassing approach" [6, p. 4].*

However, standard corporate risk frameworks frequently fall into a first-order rationalist trap, treating security variables, such as tasks, protocols, and technical firewalls, as purely objective elements to which human pegs must be fitted. This creates a severe disconnect between espoused corporate security policies and the actual, everyday security practices of individuals. A genuinely resilient Industry 5.0 posture requires second-order systems thinking [51], where managers act as 'cultivators of context' rather than static planners. Security must be embedded into the workplace not as a coercive mechanism, but as an adaptable framework that aligns with the professional desire to achieve excellence and meaning in practice.

It must be noted that despite substantive support from industry bodies toward ESRM, little empirical evidence exists to confirm its widespread or successful adoption by organizations [9]. Furthermore, while the standard definition of ESRM incorporates business continuity, it does not explicitly detail the main disciplines of protective security as identified by the Cabinet Office [21], namely: cyber, personnel, physical, and technical security. The absence of explicit focus on insider risk, be it from a human actor or an autonomous digital entity [29], and technical security attack vectors, such as close-access acquisition or hardware manipulation [21], presents a critical vulnerability as societies transition toward the heightened interconnectedness of Industry 5.0. This vulnerability highlights a fundamental misconception within modern risk frameworks regarding what or whom security practitioners are attempting to manage [44]. By treating complex, self-evolving human-machine ecosystems as static assets to be governed by top-down decrees, standard compliance models ignore the subjective sense-making of the unique individuals who navigate these systems. This failure illustrates the systemic friction between what Argyris and Schön [10] define as an organization's 'espoused theory', the formalized corporate policies written on paper, and its true 'theory-in-use', the actual, everyday practices executed by operators on the ground. When rigid security checklists are decoupled from operational realities, they trigger defensive routines that widen this

disconnect, blinding management to systemic vulnerabilities as societies transition toward the heightened interconnectedness of Industry 5.0.

4. Socio-Technical Systems

Hassan et al. [27] highlight that a unique synergy is formed when humans and machines work together, as humans are generally adaptable, skilled at problem-solving, and capable of making subtle decisions that complement machine deficiencies. The vision of Industry 5.0, based on a harmonious human-machine relationship, provides the essential component parts of a socio-technical system [18]. As the impacts of these enabling technologies are realized within the industry, the efficiency and effectiveness of how humans and machines interact will become crucial, requiring organizations to actively employ socio-technical system methodologies [54]. Grounded in the Strategic Systemic Thinking (SST) framework, this collaborative interaction can be mathematically modelled through Langefors' infological equation, (I = i (D, S, t)), which asserts that security information ((I)) is an emergent product of raw technical data ((D)) and an individual's unique pre-knowledge and life-world experience ((S)), synthesized through an active interpretation process ((i)) over time ((t)) [14]. Because technology-centric security systems are intrinsically incomplete, treating threat logs or AI alerts as objective security 'facts' ignores the subjective sense-making required by human operators to convert ambient data into coherent context [14]. While the term ‘socio-technical system’ was initially applied to describe production units within British coal mining by the Tavistock Institute [13,39], numerous operational benefits arise when organizations are treated as ‘open technical systems’ that influence, react, and respond to their wider operating environments [20,42]. Socio-technical system design (STS-D) was viewed by many in the post-WWII decades as the deliberate merging of human intelligence and skill with emerging technology [17], a perspective that directly complements the contemporary vision of Industry 5.0.

Sadok et al. [54] highlight systemic flaws when a siloed approach to system design is undertaken, where technical and social systems are viewed as separate, isolated structures. Technical analysis frequently focuses on linear steps, tasks, and processes; alternatively, social system analysis considers human interactions, coordination methods, and worker motivation [13]. Pava [47] argues that isolating system analyses, even when conducted simultaneously, is unlikely to yield a combined, effective, and optimal design. This supports the notion that socio-technical systems are an organizational necessity rather than an academic luxury. While technology can be used to address complex problems faced by modern societies, it cannot influence social structures or human behavior constructively in a vacuum [25].

Bednar and Welch [18] argue that organizational effectiveness is a phenomenon fundamentally underpinned by socio-technical principles. This presents organizations with a unique challenge: the technical element of the socio-technical system must be designed to be adaptive to meet changing user needs, while the social element must continuously evolve alongside shifting human behaviors and emerging trends [25, 40]. Mohr and Amelsvoort [39, p. 2] define STS-D as:

> *“The participative, multidisciplinary study and improvement of how jobs, single organizations, networks, and ecosystems function, internally and in relation to their*

environmental context, with a special focus on the mutual interactions of the entity's... value-creation processes... and its control/adjustment mechanisms... The goal of all STS-D based analysis and (re)design is the creation of either jobs, single organizations, networks, or eco-systems that are adaptive, innovative, good to work in, and work well as measured by human, economic, and societal metrics."

STS-D therefore requires a design framework that synchronously incorporates human, social, organizational, and technical factors [11,13,36,64]. Crucially, STS-D is not itself an operational security solution, but rather an analytical and design methodology of inquiry [14]. Grounded in the 'Double Helix' paradigm, it provides the structural mechanisms necessary to support the continuous development of adaptive security arrangements that accommodate individual uniqueness and subjective sense-making. This participatory methodology directly bridges the systemic disconnect between top-down, espoused corporate safety rules and actual, everyday workplace practices. Consequently, socio-technical systems represent more than a simple connection between the human and technical elements; they achieve an integration that yields superior, emergent system properties [25]. Multiple academics describe STS-D as an architecture that fully integrates structure, culture, methods, and machines [34,63,45], with Mujinga et al. [40] framing this baseline as 'task and technology'.

Security management research provides empirical evidence that technology-centered mitigations alone without considering people and processes frequently introduce critical flaws into the design and implementation of security controls [12,16,30,53,58]. This vulnerability is rooted in a systemic failure to recognize that technical systems are intrinsically incomplete until they are engaged by human agency. Furthermore, as Edmondson [24] demonstrates, an organizational climate lacking in psychological safety severely inhibits team learning behaviors and error reporting. If protective security mandates are experienced as coercive, they destroy this psychological safety, triggering organizational defenses and systematic patterns of misinforming. Human actors, fearful of administrative penalties or perceived incompetence, will actively conceal system anomalies and bypass rigid controls to ensure their 'jobs get crafted' [24].

This vulnerability can be mitigated by developing an appropriate 'work system' described as a system involving human participants and machines that cooperate using targeted resources to securely deliver a service or product [8,53]. Organizations must take care, however, to ensure the work system operates as a socio-technical whole, taking precautions not to weigh the social over the technical, or the technical over the social [36]. This balance requires moving away from traditional, reactive 'Safety-I' thinking—which views human behavioral variability as an operational failure to be suppressed through rigid compliance checklists [28]. Instead, an Industry 5.0 posture demands a 'Safety-II' perspective, recognizing that true systemic resilience depends on human adaptability to continuously align 'Work-As-Imagined' corporate policy with the messy realities of 'Work-As-Done' in practice [28]. By treating human agents as an essential source of protective flexibility rather than a structural weakness, organizations can co-design work systems that dynamically respond to emergent vulnerabilities.

5. Conclusion

This position paper argues that the emerging technologies underpinning Industry 5.0 will inherently expose organizations to an expanded, unpredictable, and context-dependent attack surface. This vulnerability is not merely a product of technical code defects, but is an emergent property driven by the heightened digital-physical interconnectedness and autonomous operations characteristic of the Industry 5.0 paradigm shift. Such advancements allow adversaries to deploy converged, multi-vector attack methodologies capable of exploiting systemic gaps across the cyber, physical, insider (encompassing both human operators and autonomous digital entities), and technical security domains. By introducing black-box algorithmic abstractions into everyday operations, these technologies disrupt individual sense-making and fracture the informational transparency required for human actors to maintain situational awareness.

Mitigating these blended, cross-domain threats requires a fundamental departure from traditional, rationalist planning models that attempt to force unique human actors into rigid, prescriptive workflows. Progressing into hyper-connected environments means embracing what Mumford [41] defined as complex problem-solving competencies, acknowledging that security is an ongoing, dynamic process rather than a static technical checklist. Security practitioners can only achieve genuine resilience by adapting the holistic philosophy of Enterprise Security Risk Management (ESRM) to deploy adaptive protective security frameworks that respect local contextual dependencies.

Furthermore, this paper demonstrates that Socio-Technical System Design (STS-D) is not a static security fix, but an analytical and design approach that provides security practitioners with a vital framework to support the development of appropriate security arrangements. Because the core vision of Industry 5.0 relies on a harmonious, symbiotic collaboration between humans and machines, it can only be effectively realized by moving away from purely technology-centric controls that trigger defensive behavior and patterns of misinforming. Ultimately, organizational security must be re-imagined as an open work system, where security managers transition from static rule enforcers into cultivators of context, nurturing environments where technical controls directly empower professionals to safely pursue excellence and craft meaningful work.

Declaration on Generative AI

During the preparation of this work, the author used Google and Gemini in order to check grammar and spelling.

References

[1] Abishek, B. A., Kavyashree, T., Jayalakshmi, R., Tharunkumar, S., & Raffik, R. [2023]. Collaborative robots and cyber security in industry 5.0. In *2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation [ICAECA]* [pp. 1-6]. IEEE. 10.1109/ICAECA56562.2023.10200319

[2] Adel, A. [2022]. Future of industry 5.0 in society: human-centric solutions, challenges and prospective research areas. *Journal of cloud computing*, *11*[1], 40. https://doi.org/10.1186/s13677-022-00314-5

[3] Al-Hawawreh, M., & Hossain, M. S. [2025]. A human-centered quantum machine learning framework for attack detection in IoT-based healthcare Industry 5.0. *IEEE Internet of Things Journal*. DOI: 10.1109/JIOT.2025.3565687

[4] Aleem, A., Wakefield, A., & Button, M. [2013]. Addressing the weakest link: Implementing converged security. *Security Journal*, *26*, 236-248. https://doi.org/10.1057/sj.2013.14

[5] Aleisa, M. A. [2025]. Enhancing security in CPS industry 5.0 using lightweight mobileNetV3 with adaptive optimization technique. *Scientific Reports*, *15*[1] https://doi.org/10.1038/s41598-025-00496-3

[6] Allen, B., & Loyear, R. [2017]. *Enterprise security risk management: Concepts and applications*. Rothstein.

[7] Alsufyani, A., Rana, O., & Perera, C. [2024]. Knowledge-based cyber physical security at smart home: a review. *ACM Computing Surveys*, *57*[3], 1-36. https://doi.org/10.1145/3698768

[8] Alter, S. [2013]. Work system theory: overview of core concepts, extensions, and challenges for the future. *Journal of the Association for Information Systems*, 72. https://repository.usfca.edu/at/35

[9] Amuya, L. O., & Kariuki, P. M. [2024]. Organisational characteristics as antecedents of enterprise security risk management adoption in Kenya's accredited universities. *Journal of Higher Education Policy and Management*, *46*[1], 1-17. https://doi.org/10.1080/1360080X.2023.2235772

[10] Argyris, C and Schön, D. A. [1978] Organizational Learning: A Theory of Action Perspective. Reading, MA: Addison-Wesley

[11] Asiri, M., Arunasalam, A., Saxena, N., & Celik, Z. B. [2025]. Frontline responders: Rethinking indicators of compromise for industrial control system security. *Computers & Security*, *154*, 104421. https://doi.org/10.1016/j.cose.2025.104421

[12] Baskerville, R. [1991]. Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems*, *1*[2], 121-130. https://doi.org/10.1057/ejis.1991.20

[13] Baxter, G., & Sommerville, I. [2011]. Socio-technical systems: From design methods to systems engineering. *Interacting with computers*, *23*[1], 4-17. https://doi.org/10.1016/j.intcom.2010.07.003

[14] Bednar, P. [2000]. A Contextual Integration of Individual and Organizational Learning Perspectives as Part of IS Analysis. Informing Science: the International Journal of An Emerging Transdiscipline, 3[3], 145-156. http://inform.nu/Articles/Vol3/v3n3p145-156.pdf
[15] Bednar, P., Anderson, D., & Welch, C. [2005]. Knowledge Creation and Sharing – Complex Methods of Inquiry and Inconsistent Theory. In D. Remenyi [Ed.], Proceedings of the European Conference on Knowledge Management [ECKM]. [pp. 59-66]. Academic Conferences.
[16] Bednar, P., & Katos, V. [2009]. Addressing the human factor in information systems security. In *MCIS2009: 4th Mediterranean Conference on Information Systems* [pp. 900-912]. Athens University of Economics and Business.
[17] Bednar, P. & Welch, C [2016]. Enid Mumford: the ETHICS methodology and its legacy. In B. Mohr & P. V. Amelsvoort, *Co-Creating Humane and Innovative Organizations*, 274-288, Global STS-D Network Press.
[18] Bednar, P. M., & Welch, C. [2019]. Socio-technical perspectives on smart working: Creating meaningful and sustainable systems. *Information Systems Frontiers*, *22*[2], 281-298. https://doi.org/10.1007/s10796-019-09921-1
[19] Boopathy, V., Lakshmi, R., Santhosh, J., Kannadhasan, S., Ambika, A., & Arun, K. K. [2025]. An Effective Methodology for Integrating Design Thinking Approach with Industry 5.0. In *2025 2nd International Conference on New Frontiers in Communication, Automation, Management and Security [ICCAMS]* [pp. 1-4]. DOI: 10.1109/ICCAMS65118.2025.11234068
[20] Borodzicz, E. P. [2005]. *Risk, crisis and security management.* Wiley.
[21] Cabinet Office [2021]. *Government Functional Standard 007: Security.* Government Functional Standard GovS 007: Security - GOV.UK
[22] Checkland, P., & Holwell, S. [1998]. Information, systems and information systems: Making sense of the field. John Wiley & Sons.
[23] Devanny, J., Martin, C., & Stevens, T. [2021]. On the strategic consequences of digital espionage. *Journal of Cyber Policy*, *6*(3), 429-450 https://doi.org/10.1080/23738871.2021.2000628
[24] Edmondson, A. [1999] 'Psychological safety and learning behavior in work teams', Admin. Sci. Q., vol. 44, no. 2, pp. 350–383, doi:10.2307/2666999.
[25] Fischer, G., & Herrmann, T. [2011]. Socio-technical systems: a meta-design perspective. *International Journal of Sociotechnology and Knowledge Development [IJSKD],* 3[1], 1-33. DOI:10.4018/jskd.2011010101
[26] Harris, W., & Sadok, M. [2023]. How do professionals assess security risks in practice? An exploratory study. Security Journal, 1-15. https://doi.org/10.1057/s41284-023-00389-y
[27] Hassan, M. A., Zardari, S., Farooq, M. U., Alansari, M. M., & Nagro, S. A. [2024]. Systematic analysis of risks in Industry 5.0 architecture. *Applied Sciences*, *14*[4], 1466. https://doi.org/10.3390/app14041466
[28] Hollnagel, E. [2014]. Safety-I and Safety-II: The Past and Future of Safety Management. Farnham, UK: Ashgate Publishing.
[29] Kennedy, R. [2025]. *Managing insider risk 'entities' as the route to security convergence. Proceedings from the 11th International Workshop on Socio-Technical Perspectives in IS. paper3.pdf*
[30] Martin, P. [2023]. *Insider risk and personnel security: An introduction.* Routledge.
[31] Martin, P., & Mercer, S. [2025]. *We Need to Talk About the Insider Risk from AI.* We Need to Talk About the Insider Risk from AI | Royal United Services Institute

[32] Marquez-Tejon, J., Jimenez-Partearroyo, M., & Benito-Osorio, D. [2021]. Security as a key contributor to organisational resilience: a bibliometric analysis of enterprise security risk management. *Security Journal*, *35*[2], 600. https://doi.org/10.1057/s41284-021-00292-4
[33] Marquez-Tejon, J., Jimenez-Partearroyo, M., & Benito-Osorio, D. [2023]. Integrated security management model: a proposal applied to organisational resilience. *Security Journal*,[37],375–398. https://doi.org/10.1057/s41284-023-00381-6
[34] McEvoy, T., & Kowalski, S. [2019]. Deriving cyber security risks from human and organizational factors–a socio-technical approach. *Complex systems informatics and modeling quarterly*, [18], 47-64. https://doi.org/10.7250/csimq.2019-18.03
[35] McCreight, T. [2024]. Building resilience: The role of enterprise security risk management in developing a resilient organisation. *Journal of Business Continuity & Emergency Planning*, *17*[4], 363-374.
[36] Michael, K., Vogel, K. M., Pitt, J., & Zafeirakopoulos, M. [2024]. Artificial intelligence in cybersecurity: A socio-technical framing. *IEEE Transactions on Technology and Society,* 15-30. 10.1109/TTS.2024.3460740
[37] Mishchenko, D., Oleinikova, I., Erdődi, L., & Pokhrel, B. R. [2024]. Multidomain cyber-physical testbed for power system vulnerability assessment. *IEEE Access*, *12*, 38135-38149. https://doi.org/10.1109/ACCESS.2024.3375401
[38] Mittal, D., & Damle, M. [2025]. An appraisal in internal control frameworks implementation of COSO, ISO 27001 and NIST for opportunities in Industry 5.0. In *2025 Seventh International Conference on Computational Intelligence and Communication Technologies (CCICT)* [pp. 345-352]. DOI: 10.1109/CCICT65753.2025.00061
[39] Mohr, B. J., & Amelsvoort, P. V. [2016]. Waves of Evolution in Socio-technical Systems Design (STS-D). In B. Mohr & P. V. Amelsvoort, *Co-Creating Humane and Innovative Organizations*, 1-15, Global STS-D Network Press.
[40] Mujinga, M., Eloff, M., Kroeze, J. H. [2017], A Socio-Technical Approach to Information Security. *AMCIS 2017 Proceedings*. 10. https://aisel.aisnet.org/amcis2017/SocialTechincal/Presentations/10
[41] Mumford, E. [1999]. *Dangerous decisions: Problem solving in tomorrow's world*. Kluwer Academic/Plenum Publishers.
[42] Mumford, E. [2006]. The story of socio-technical design: Reflections on its successes, failures and potential. *Information Systems Journal*, 16[4], 317-342. https://doi.org/10.1111/j.1365-2575.2006.00221.x
[43] Navale, G. S., Madala, R., Managuli, M., Jayalakshmi, N., Kadiravan, G., & Rawat, R. [2023, September]. Research and innovation in next generation security and privacy in Industry 5.0 IoT. In *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)* [Vol. 6, pp. 1384-1390]. IEEE. DOI: 10.1109/IC3I59117.2023.10397984
[44] Nissen, H.-E. [2012]. What or whom do knowledge-managers manage? In J. G. Cegarra (Ed.), Proceedings of the 13th European Conference on Knowledge Management [pp. 839–847]. Academic Conferences and Publishing International Limited.
[45] Østby, G., Kowalski, S. J., & Katt, B. [2020]. Towards a maturity improvement process–systemically closing the socio-technical gap. CEUR Workshop Proceedings. https://hdl.handle.net/11250/2737120
[46] Pant, P., Rajawat, A. S., Goyal, S. B., Singh, D., Constantin, N. B., Raboaca, M. S., & Verma, C. [2022, December]. Using machine learning for industry 5.0 efficiency prediction based on

security and proposing models to enhance efficiency. In *2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART)* (pp. 909-914). https://doi.org/10.1109/SMART55829.2022.10047387
[47] Pava, C. H. [1983]. Designing managerial and professional work for high performance: A sociotechnical approach. *National Productivity Review*, *2*(2), 126-135. https://doi.org/10.1002/npr.4040020204
[48] Petruzzi, J., & Loyear, R. [2016]. Improving organisational resilience through enterprise security risk management. *Journal of business continuity & emergency planning*, *10*[1], 44-56.
[49] Raja Santhi, A., & Muthuswamy, P. [2023]. Industry 5.0 or industry 4.0 S? Introduction to industry 4.0 and a peek into the prospective industry 5.0 technologies. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, *17*[2], 947-979. https://doi.org/10.1007/s12008-023-01217-8
[50] Renaud, K., Warkentin, M., Pogrebna, G., & van der Schyff, K. [2024]. VISTA: An inclusive insider threat taxonomy, with mitigation strategies. *Information & Management*, *61*[1], 103877 https://doi.org/10.1016/j.im.2023.103877
[51] Reynolds, M. [2024]. Systems thinking principles for making change. *Systems*, *12*[10], 437.
[52] Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. [2022]. Internet of things: Security and solutions survey. *Sensors*, *22*[19], 7433. https://doi.org/10.3390/s22197433
[53] Sadok, M., Alter, S., & Bednar, P. [2020]. It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information & Computer Security*, *28*[3], 467-483. https://doi.org/10.1108/ICS-01-2019-0010
[54] Sadok, M., Welch, C., & Bednar, P. [2019]. A socio-technical perspective to counter cyber-enabled industrial espionage. *Security Journal*, *33*, 27-42 https://doi.org/10.1057/s41284-018-00198-2
[55] Sahoo, P., Saraf, P. K., & Uchil, R. [2025]. Identification of challenges to Industry 5.0 adoption in Indian manufacturing firms: an emerging economy perspective. *International Journal of Computer Integrated Manufacturing*, *38*[5], 649-674. https://doi.org/10.1080/0951192X.2024.2382186
[56] Schneller, L., Porter, C. N., & Wakefield, A. [2023]. Implementing converged security risk management: Drivers, barriers, and facilitators. *Security Journal*, *36*(2), 333-349. https://doi.org/10.1057/s41284-022-00341-6