Enhancing Digital Resilience through AI in Industry 5.0: A Technology Management Perspective

Amara Atif[1], Muhammad Atif Qureshi[2]
[1] Faculty of Engineering and IT, University of Technology Sydney, Australia
[2] Design and Creative Technology Vertical, Torrens University, Sydney, Australia

***Abstract*—The proposed literature review aims to investigate the emerging concept of "Digital Resilience" within the context of Industry 5.0, focusing on integrating technology management strategies and continuous improvement practices in the era of artificial intelligence (AI). The research paper explores how the integration of Industry 5.0 and AI can help organisations establish feedback loops that enhance their digital resilience against disruptions. The review explores the intersection of Industry 5.0, characterised by technology, with the transformative power of AI on principles such as human-centricity, environmental stewardship, and social benefit. It assesses existing literature to identify key frameworks, models, best practices, challenges, and empirical evidence that support the establishment of feedback loops, emphasizing their role in fostering digital resilience and the synergies between technology management, continuous improvement, and Industry 5.0. The review further highlights the significance of understanding how organisations navigate the complex landscape of Industry 5.0, leveraging AI-driven technologies to improve operational efficiency and responsiveness. In conclusion, this review aims to provide a comprehensive synthesis of current knowledge, offering insights into the strategic integration of technology management, continuous improvement, and Industry 5.0 to navigate the complexities of the AI era.**

I. Introduction

In the era of Industry 5.0 (also referred to as the Fifth Industrial Revolution or I5.0 or human-centric industrial revolution) and the ongoing digital transformation, businesses are witnessing remarkable growth and opportunities characterised by several key features associated with Industry 5.0. These features include human-centricity, sustainability, resilience, digitalisation of processes in advanced technologies, e.g., Artificial Intelligence (AI), and seamless connectivity between various components of the industrial ecosystem [1]. In the AI era, the digital landscape, covering small businesses to multinational corporations, has not only opened up opportunities and facilitated innovative tools for operational efficiency but has also highlighted the significance of digital aims to enhance efficiency by seamlessly integrating digital technologies into manufacturing and business processes that incorporates technology management strategies, embraces continuous improvement, and aligns with Industry 5.0 principles.

In today's business landscape, especially in the context of Industry 5.0 and AI, Digital Resilience is crucial. It empowers organisations to proactively tackle digital challenges, protect assets, and sustain operations in the ever-changing digital environment [2]. *Digital Resilience* refers to an organisation's ability to adapt, recover, and thrive despite digital challenges such as pandemics, natural disasters, cyberattacks and technological disruptions while sustaining financial and security assets [3]. Key elements include adaptability, recovery, risk management, strategic planning, and continuous improvement [3][4]. Digital Resilience helps organisations maintain their reputation, minimise disruptions, build customer trust by securing data, and stay competitive by adapting to change and seizing new opportunities [5].

Industry 5.0 represents the latest paradigm in industrial development, building upon the foundations of previous industrial revolutions. It emphasizes the integration of advanced technologies, including the Internet of Things (IoT), AI, robotics, and data analytics, to create a more connected, intelligent, and human-centric industrial environment [6]. The key principles of Industry 5.0 include *human-centricity*, *environmental stewardship*, and *social benefit*. These principles are discussed below, with reference to [7][8][9][10].

- **Human-centricity:** Industry 5.0 places a strong emphasis on the collaboration between humans and machines. It envisions a work environment where humans and AI-powered technologies work together synergistically, with each contributing their unique strengths. This principle seeks to enhance the well-being and creativity of the workforce.
- **Environmental Stewardship:** Industry 5.0 promotes sustainable and eco-friendly practices in industrial processes. Through the use of smart technologies and data analytics, organisations can optimise resource utilisation, reduce waste, and minimise environmental impact.
- **Social Benefit:** Industry 5.0 aims to contribute positively to society by fostering innovation, creating highly skilled jobs, and addressing societal challenges. It envisions technology as a means to enhance the quality of life and create a more inclusive and equitable society.

The convergence of Industry 5.0 and AI has a profound impact on organisational dynamics, shaping how businesses operate, innovate, and engage.

TABLE I. IMPACT OF INDUSTRY 5.0 AND ARTIFICIAL INTELLIGENCE ON ORGANISATIONAL DYNAMICS

Impact	Industry 5.0	AI
Integration of Technologies	Highlights collaboration between humans and machines and the exchange of information	Acts as a driver for smart automation and decision-making, enhancing the abilities of machines and systems
Human-Centricity	Prioritises human-centric approaches, cultivating a collaborative environment where humans collaborate with intelligent technologies	Improves human capabilities, automates repetitive tasks, and enables employees to concentrate on more intricate and creative aspects of their responsibilities
Operational Efficiency	Aims to improve efficiency through seamlessly integrating digital technologies in manufacturing and business processes	Improves operations by analysing extensive datasets, predicting trends, and offering actionable insights for informed decision-making
Adaptability and Flexibility	Promotes flexibility in manufacturing processes, allowing rapid adaptation to shifting market demands	Facilitates adaptive systems that learn from data, empowering organisations to adjust strategies and operations based on real-time information
Data-Driven Decision Making *ML (Machine Learning)	Utilises data collection and analysis to inform decision-making processes	Uses advanced analytics and *ML to extract meaningful insights from data, helping organisations make informed and strategic decisions
Environmental Stewardship	Promotes sustainable and eco-friendly practices in manufacturing and production	Promotes environmental stewardship by using resources efficiently, reducing energy consumption, and minimising waste
Social Impact	Promotes the development of socially responsible products and services	Influences society through applications such as healthcare innovations, personalised services, and addressing social challenges
Innovation and Competitiveness *NLP (Natural Language Processing)	Drives innovation by integrating technologies, boosting competitiveness in the global market	Drives innovation by facilitating breakthroughs in fields such as ML, *NLP, and computer vision

Table I outlines the effects of Industry 5.0 and AI on organisational dynamics concerning technology integration [6], human centricity [9][11], operational efficiency [6], adaptability and flexibility [6][12][13], data-driven decision-making [12], social impact [14], innovation and competitiveness [13][14]. The combination of Industry 5.0 and AI reshapes organisational dynamics by fostering collaboration between humans and machines, improving efficiency, cultivating flexibility, and influencing social and environmental responsibility. These technological trends redefine how organisations operate, positioning them to excel in an ever-growing, digitised and interconnected world.

The feedback loop, a concept derived from systems theory [40], is increasingly applied in organisational management to iteratively improve and adapt processes. Its significance is particularly notable in the context of Industry 5.0 and AI, where dynamic challenges require effective mechanisms for adaptation and response. This paper emphasizes the feedback loop as a crucial tool for integrating core principles such as human-centricity, environmental stewardship, and social benefit into organisational strategies, reflecting the transformative influences of AI.

In Industry 5.0, where AI plays a transformative role, establishing an effective feedback loop is essential not only for coping with technological disruptions but also for leveraging these disruptions to enhance operational efficiency and strategic innovation. Given the nascent stage of Industry 5.0, this paper aims to explore the integration of Industry 5.0 and AI to establish effective feedback loops within organisations, enhancing their digital resilience. This study focuses on how these advanced technologies influence organisational principles and adaptability in the face of digital disruptions.

This literature review examines existing research to identify key frameworks, models, best practices, challenges, and empirical evidence that support the establishment of feedback loops. The focus is on their role in fostering digital resilience and the synergies between technology management, continuous improvement, and Industry 5.0. Additionally, this review provides insights into future research directions and opportunities within the Industry 5.0 domain.

The subsequent sections of this paper are organised as follows: Section II provides details on the key components of the feedback loop, its role in enhancing digital resilience, and connections between the feedback loop, technology management, continuous improvement, and Industry 5.0. Section III elaborates on the research methodology employed. Section IV outlines the data analysis and discussion for the research question, how can the integration of Industry 5.0 and AI help organisations establish feedback loops that enhance their digital resilience against disruptions? Finally, Section V presents the conclusion.

II. FEEDBACK LOOP AND DIGITAL RESILIENCE

A feedback loop is a fundamental concept in enhancing digital resilience, serving as a dynamic mechanism for continuous improvement and adaptation. In the context of digital resilience, a feedback loop involves the iterative process of collecting, analysing, and applying information to enhance an organisation's ability to withstand and recover from digital disruptions and cyber threats [15][16]. The feedback loop is crucial for staying responsive to evolving challenges, identifying weaknesses, and optimising strategies to fortify digital resilience.

A. Key Components of the Feedback Loop

The feedback loop begins with the *collection of data* from various sources, including security systems, monitoring tools, and incident reports. Data can encompass information on

system performance, user behaviour, and potential security incidents. The collected data undergoes *analysis through monitoring tools*, machine learning algorithms, and data analytics. This phase involves assessing patterns, identifying anomalies, and evaluating the overall health of digital systems. In the event of a security incident, the feedback loop includes an *incident response* component. This involves immediate actions to mitigate the impact, isolate affected systems, and initiate recovery procedures. Following a security incident, a thorough *post-incident review* is conducted. This phase involves analysing the incident's root causes, evaluating the effectiveness of response measures, and identifying areas for improvement.

Figure 1 presents the key components of the feedback loop. Each component of the feedback loop plays a crucial role in enhancing digital resilience by fostering a proactive, adaptive, and learning-oriented cybersecurity approach [17]. The feedback loop aligns with technology management, continuous improvement, and Industry 5.0 principles (from Section I), contributing to optimising digital processes, adaptive responses, and a human-centric industrial environment.

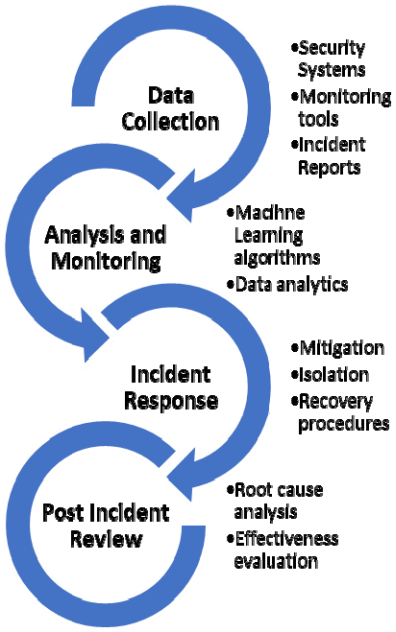

Fig. 1. Key Components of the Feedback Loop

B. Role of Feedback Loop in Enhancing Digital Resilience

The feedback loop facilitates continuous monitoring of the digital environment, including networks, systems, and data. Regular assessments help organisations identify potential vulnerabilities, threats, and areas of improvement [18]. Through real-time analysis and anomaly detection, the feedback loop enables the early identification of irregularities or suspicious activities [19]. This proactive approach is essential for minimising the impact of security incidents. A well-established feedback loop allows organisations to adapt their response strategies based on the analysis of past incidents [19][20]. This adaptability ensures that response measures evolve with the changing nature of cyber threats.

Post-incident analysis within the feedback loop facilitates learning from past incidents. This learning process helps organisations understand the root causes of disruptions and implement measures to prevent similar incidents in the future [19]. Continuous feedback enables organisations to optimise their digital resilience measures. By assessing the effectiveness of existing strategies, organisations can make informed decisions on resource allocation and strategic enhancements. The feedback loop integrates with risk management processes, providing insights into emerging risks and enabling organisations to adjust risk mitigation strategies in real-time [21]. Feedback loops contribute to informed strategic decision-making by providing data-driven insights. This ensures that decisions related to digital resilience align with the organisation's overall goals and risk tolerance.

C. Connections between Feedback Loop, Technology Management, Continuous Improvement, and Industry 5.0:

The feedback loop aligns with technology management by providing insights into the performance, security, and reliability of digital technologies [22]. It ensures that technology assets are effectively managed and optimised to meet organisational goals. The feedback loop is a cornerstone of continuous improvement efforts. By learning from incidents and analysing data, organisations can iteratively enhance their digital resilience measures [23]. This aligns with the principles of continuous improvement in optimising processes over time. In the context of Industry 5.0, the feedback loop is integral to creating a responsive and adaptive industrial environment [1]. It aligns with the principles of human-centricity and innovation by enabling organisations to learn from digital disruptions and improve their industrial processes continually.

III. RESEARCH METHODOLOGY

In this study, we employed the PRISMA method (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) 2020 guideline to conduct a comprehensive analysis of previously published works [24]. This method is widely recognized for its effectiveness in identifying research gaps and providing valuable insights for further investigations. The PRISMA method consists of three distinct phases: (i) identification, (ii) screening and eligibility, and (iii) inclusion and exclusion. These phases are essential for ensuring that the collection of articles aligns closely with the study's objectives and are commonly utilised across various research fields.

Figure 2 illustrates a visual representation of the systematic review process based on the PRISMA guidelines. This figure serves as a roadmap, guiding researchers through each phase of the review process, from the initial identification of relevant literature to the final selection of articles for inclusion in the study.

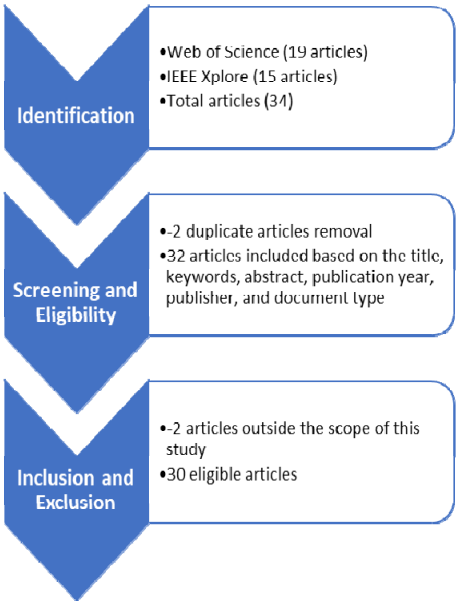

Fig. 2. PRISMA Flow Chart

A. *Data Gathering and Preprocessing*

The data-gathering process involved identifying and extracting data from published research articles from scholarly databases. The databases used to extract data for this study include Web of Science (WoS) Core Collection and IEEE (Institute of Electrical and Electronic Engineers) Explore (Xplore). These two meta-databases were chosen because they extensively cover various scientific disciplines, provide excellent indexing for journals and conference proceedings, include citation tracking features, and have a reputable and credible standing within the scientific community. Additionally, both databases offer advanced search capabilities, allowing users to refine search criteria and customise searches according to specific requirements [25].

- *Identification:* To identify a comprehensive set of journal articles and conference papers, the search string was constructed through the combination of the Boolean operators 'AND' and 'OR' between the specified terms. Additionally, a criterion was applied to filter for articles published exclusively in the English language. The terms used for the search included 'Digital Resilience' and 'Industry 5.0' along with the operator 'OR' applied among the terms 'Industry 5.0', 'Fifth Industrial Revolution', '5th Industrial Revolution', 'I5.0', and 'Human-Centric Manufacturing'. This inclusive search yielded 19 WoS Core Collection publications and 15 IEEE Xplore publications (up to December 2023). The time range for these documents is 2019-2023, indicating the earliest publication on digital resilience at the intersection of Industry 5.0 was in 2020.
- *Screening and Eligibility:* After the screening phase, 32 publications were selected for further analysis (2 duplicate publications were eliminated). The data collected included the title, keywords, abstract, publication year, publisher, and document type for each publication retrieved.
- *Inclusion and Exclusion:* After reading each publication, two articles were excluded from the final results since they were outside the scope of this study. Finally, 30 eligible publications were studied in detail and classified into diverse sub-categories of the inclusion criteria.

The collected data were analysed by applying both qualitative and quantitative methods. Microsoft Office Excel and FreeWordCloudGenerator.com tools were used to process the data further.

IV. Data Analysis and Discussion

This section presents the fundamental data analysis of the resulting publications to provide an overall picture of the publications included, followed by key themes to answer the question.

A. *Descriptive Analysis of Resulting Publications*

The initial analysis concentrated on the publication dates, geographical locations, and types of articles eligible for inclusion in the study. While the search initially had no time restrictions, the articles retrieved were notably recent, spanning from 2019 to 2023. This trend highlights the increasing research interest in the realms of Digital Resilience and Industry 5.0. Notably, there were a high number of publications in the year 2023 (refer to Figure 3).

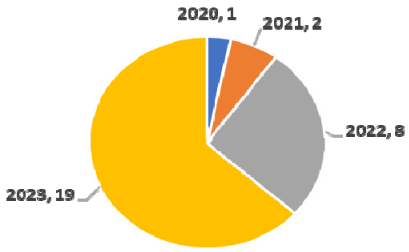

Fig. 3. Number of Articles Published by Year (Year, Number of Publications)

The second phase of the descriptive analysis examined the nature of articles generated and published on this contemporary theme. Out of the 30 articles chosen for inclusion in this review, the predominant category is journal research articles, comprising 19 journal articles, followed by 7 conference papers. Particularly, within this relatively brief timeframe, four reviews covering various topics and facets of Industry 5.0 have already been undertaken, as illustrated in Figure 4.

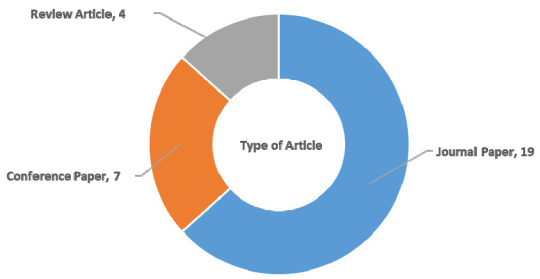

Fig. 4. Types of Articles

Another aspect examined was the distribution of publications by location, as shown in Figure 5. For consistency, the location of the first author or their affiliated institution was selected for all articles included in the review. Italy and Germany emerged as the countries with the highest number of published articles, followed by China, England, and France. These nations boast significant industrial development, indicating a strong potential for research and innovation.

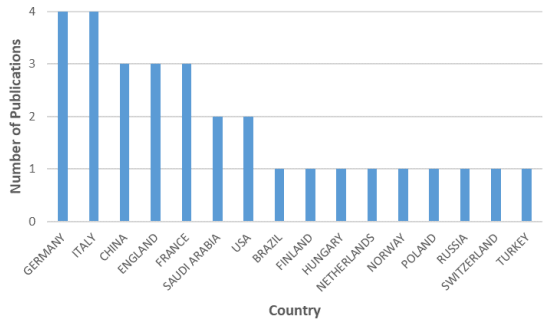

Fig. 5. Graphic Representation of the Number of Articles Published by Location (Country, Number of Publications)

B. *Analysis of Publications Keywords*

Recognising relevant keywords is crucial for understanding the fundamental concepts and themes explored in a particular publication. A comprehensive analysis of explicitly mentioned keywords in the included publications was conducted to gain a deeper understanding of research focuses, domains, and features related to Industry 5.0. This initial examination lays the groundwork for understanding the research landscape and provides context for subsequent analyses.

Initially, 150 keywords were collected, and after removing duplicates, 86 unique keywords remained. These keywords were organised into clusters based on their closely related meanings. For instance, keywords like 'Industry 5.0', 'Artificial Intelligence', and 'Human-Centric Innovation' were grouped into the "Industry 5.0, Artificial Intelligence, and Technology" cluster. The resulting five clusters are: "Industry 5.0, Artificial Intelligence, and Technology" (43 keywords), "Innovation and Ecosystems" (15 keywords), "Supply Chain and Manufacturing" (15 keywords), "Healthcare and Services" (5 keywords), and "Metaverse and Emerging Topics" (8 keywords).

A visual representation of these keywords is presented in Figure 6, depicted as a word cloud generated using Free-WordCloudGenerator.com. This word cloud offers a visually intuitive way to showcase the prominent themes and emphases found within the analysed publications. Its visual appeal and intuitive presentation contribute to the overall effectiveness of the research findings and facilitate comprehension for both researchers and readers alike.

C. *Conceptual Analysis*

The conceptual analysis is conducted next to understand the key frameworks, models, best practices, challenges, and empirical evidence on establishing a feedback loop, highlighting its role in developing digital resilience, incorporating elements of technology management, continuous improvement, and Industry 5.0. This involves breaking down concepts in the resulting publications into their constituent parts, examining their relationships, and clarifying their meanings to construct a coherent and logically structured conceptual framework that guides this study.

Fig. 6. Keyword Frequency Cloud

Table II summarises the frameworks, models, and best practices that provide a set of guidelines for managing and improving an organisation's digital and operational resilience. Digital resilience frameworks are crucial for organisations operating in today's dynamic and technology-driven landscape. These frameworks serve as structured guides, offering systematic approaches to navigate challenges related to cybersecurity threats, rapid technological changes, and disruptions.

TABLE II. CONCEPTUAL ANALYSIS

Concept	Frameworks/Models/Best Practice Guide
Digital Resilience	NIST (National Institute of Standards and Technology) cybersecurity framework, CERT Resilience Management Model (CERT-RMM), ISACA's cyber resilience framework, MITRE ATT&CK framework, ISO/IEC 27001
Technology Management	ITIL (Information Technology Infrastructure Library), COBIT (Control Objectives for Information and Related Technologies), TOGAF (The Open Group Architecture Framework), Six Sigma, Agile and Scrum, DevOps, PMI's PMBOK (Project Management Body of Knowledge), Capability Maturity Model Integration (CMMI)
Continuous Improvement	Lean Thinking, Six Sigma, Kaizen, PDCA (Plan-Do-Check-Act), Baldrige Excellence Framework, ISO 9001 Quality Management System, Scrum, Kanban, Total Quality Management (TQM), Agile Improvement Frameworks (e.g., Agile Retrospectives)

Key reasons for their importance include helping organisations adapt to evolving technologies, ensuring cybersecurity preparedness, facilitating business continuity and recovery, managing digital risks, complying with regulations, protecting data and privacy, enhancing supply chain resilience, enabling crisis management, supporting innovation and digital transformation securely, fostering employee training and awareness, aiding strategic decision-making, and building and maintaining customer trust and reputation [26].

AI is playing a transformative role in enhancing the capabilities of various frameworks and models, particularly in the realms of digital resilience, technology management, and continuous improvement. Table III organises information on key AI integrations and their respective applications within the specified frameworks (from Table II). It is important to recognise that the integration of AI into frameworks is an evolving process, and organisations must stay informed about the latest advancements in AI technologies to leverage cutting-edge tools and techniques for improved outcomes.

Moreover, ethical considerations and responsible AI practices should be integral to the incorporation of AI into any framework, ensuring that the benefits of AI are harnessed ethically and responsibly [38].

TABLE III. INTEGRATION OF ARTIFICIAL INTELLIGENCE ACROSS FRAMEWORKS

Framework/ Application	Artificial Intelligence Integration
Digital Resilience	• Threat Intelligence and Predictive Analysis [27] • Behavioural Analytics [28] • Automated Incident Response [29]
Technology Management	• AI in IT Service Management (ITSM) [30] • Predictive Maintenance [31] • Automated IT Governance [32]
Continuous Improvement	• Data-Driven Decision Making [33] • Process Automation [34] • Machine Learning in Quality Control [35] • Adaptive Agile Practices [36]
Cross-Cutting AI Applications	• Natural Language Processing [13][14] • Advanced Analytics for Performance Metrics [12] • AI in Risk Management [3][4][21] • Smart Monitoring and Reporting [37]

In the context of digital resilience frameworks, AI is applied to provide advanced threat intelligence and predictive analysis. Algorithms analyse extensive datasets, enabling organisations to anticipate cyber threats and vulnerabilities, thereby fortifying their digital resilience. Additionally, AI-driven behavioural analytics enhances security by detecting anomalous patterns in user behaviour, contributing to the identification of potential security incidents and unauthorised access. Automated incident response systems powered by AI further strengthen digital resilience by swiftly detecting and mitigating security incidents, reducing response times.

In technology management models, AI is integrated into ITSM frameworks through the deployment of chatbots and virtual assistants. These AI-driven solutions provide real-time support, automate routine tasks, and enhance overall IT service efficiency. Predictive maintenance benefits from AI algorithms analysing historical data to forecast equipment failures or performance issues, enabling proactive measures and optimisation of technology resources. Moreover, AI contributes to automated decision-making processes within IT governance frameworks, fostering dynamic and adaptive governance structures.

Within continuous improvement frameworks, AI facilitates data-driven decision-making by analysing large datasets to provide real-time insights. Robotic Process Automation (RPA), powered by AI, automates routine tasks and streamlines processes in quality control, reducing human errors and enhancing efficiency [34]. Machine learning algorithms are integrated into continuous improvement processes, particularly in quality control, to identify patterns and trends that can lead to process enhancements. AI also aids in analysing project data in Agile frameworks, offering insights into team performance, identifying areas for improvement, and predicting potential challenges.

Cross-cutting AI applications, such as NLP, are employed across frameworks to analyse and understand unstructured data, facilitating better decision-making and insight extraction. AI-powered analytics tools provide advanced insights into performance metrics, enabling continuous improvement efforts based on data-driven analysis. In risk management frameworks, AI is utilised to assess and predict risks, providing organisations with a proactive approach to risk mitigation and resilience. Additionally, AI enhances monitoring capabilities by intelligently processing and interpreting data, providing real-time reports, and enabling more informed decision-making across various frameworks.

D. Answering the Research Question: How can the integration of Industry 5.0 and AI help organisations establish feedback loops that enhance their digital resilience against disruptions?

Digital resilience reflects the capability of systems to adapt to and thrive amid digital disruptions. This subsection explores how organisations can establish effective feedback loops to foster this resilience, focusing on the profound and multifaceted intersection of Industry 5.0 principles (from Section I) with the transformative power of AI.

a) Intersection of Industry 5.0 principals with AI

The integration of AI technologies with Industry 5.0 principles is instrumental in realising a human-centric vision that augments human capabilities, automates routine tasks, and fosters a collaborative working environment. This intersection significantly enhances operational efficiency and enables personalised, adaptive interactions between humans and machines. Furthermore, AI's role in Industry 5.0 extends to environmental stewardship by optimising energy usage and reducing waste in manufacturing processes through smart automation and predictive maintenance [8][9]. These actions not only prevent resource-intensive breakdowns but also contribute to a higher level of resource efficiency and sustainability [2][4][11]. Social benefits are equally notable, as the deployment of AI in Industry 5.0 leads to the creation of highly skilled jobs in data science, machine learning, and AI development [10][14]. Additionally, AI-driven solutions in

Industry 5.0 address societal challenges, promoting a broader positive social impact.

Effective technology management is central to the implementation of AI in Industry 5.0. It involves strategic planning, resource allocation, and the management of technological assets to ensure that AI technologies are seamlessly integrated and are continually enhancing organisational capabilities. Continuous improvement, a key component of technology management, involves iterative processes that leverage feedback to refine operations and technologies continuously. In the context of Industry 5.0, continuous improvement is driven by data gathered from AI and automation systems. This data informs the feedback loops, allowing organisations to not only react to changes but also proactively improve processes based on predictive insights.

To enhance digital resilience, it is critical for organisations to establish feedback loops that incorporate AI-enhanced capabilities along with effective technology management and continuous improvement practices. Such loops involve continuous monitoring and adaptation based on AI-generated insights, which allow organisations to respond dynamically to changes and disruptions. Feedback loops serve as a crucial mechanism for iterative improvement, aligning Industry 5.0 initiatives with ongoing technological advancements and shifting market demands.

b) Reshaping Industry 5.0 Principles by AI Technologies

AI technologies significantly reshape Industry 5.0 principles by providing new possibilities for innovation and efficiency. These technologies amplify a human-centric approach by enabling more personalised experiences and adaptable workplaces, enhancing the interaction between humans and machines. Through the lens of technology management, organisations must strategically manage the integration of AI to ensure these technologies are implemented effectively and sustainably. This includes planning, deployment, and the continuous monitoring of AI systems through feedback loops. Such feedback mechanisms are crucial for gathering insights on system performance and user engagement, which inform decisions on necessary adjustments or enhancements.

Environmental stewardship is advanced through AI-driven optimisations that minimise waste, reduce energy consumption, and enhance overall sustainability. Here, continuous improvement practices are crucial, as they involve the iterative refinement of AI applications through feedback loops. These loops enable organisations to monitor and adjust their operations dynamically, ensuring they remain efficient and aligned with environmental goals over time. This process helps organisations adapt to regulatory changes and technological advancements, maintaining a balance between innovation and sustainability.

Social benefits are extended through AI applications that tackle complex challenges, improve healthcare, and contribute to societal well-being. However, the integration of AI into Industry 5.0 also raises important considerations related to ethics, transparency, and the responsible use of technology. Establishing feedback loops in this context also involves assessing the societal impact of AI applications, ensuring they adhere to ethical standards and are transparent in their operations.

Balancing technological advancements with ethical considerations becomes crucial to ensure that AI in Industry 5.0 aligns with societal values and fosters positive outcomes. Feedback loops support this balance by enabling organisations to continuously assess and refine their AI strategies in response to emerging ethical challenges and societal expectations.

c) Best Practices for Establishing a Digital Resilience Feedback Loop in Organisations

Organisations navigating the complex landscape of Industry 5.0 must strategically integrate technologies and foster a culture of adaptability to thrive in the era of interconnected industrial processes. Leveraging AI-driven technologies, these organisations improve operational efficiency and responsiveness, which is essential for thriving in today's digital economy. Establishing an effective feedback loop for digital resilience is crucial and involves a combination of technical, organisational, and procedural best practices. Below are key best practices employed by organisations, summarised and supported by relevant literature, as referenced in [10][14][15][17][19][26][29][30][32][35][38][39].

By embedding these feedback loop mechanisms into technology management and continuous improvement practices, organisations can establish a dynamic system that not only responds to current security and operational challenges but also proactively adapts and evolves to meet future demands. This holistic approach is key to building and maintaining robust digital resilience in the face of a rapidly changing digital landscape.

- Establish robust monitoring mechanisms to continuously collect data on the performance, security, and integrity of digital assets. Automated tools enable real-time data collection, forming the basis of the feedback loop for immediate response to anomalies and security threats.
- Deploy advanced threat detection tools and utilise AI-driven solutions for early detection of security incidents. This practice provides timely data that is critical for quick decision-making and helps keep the organisation ahead in security readiness.
- Apply data analytics and machine learning to analyse large datasets for continuous insights. This analysis identifies patterns, anomalies, and potential threats, feeding actionable insights back into the organisation's strategic planning and operational adjustments.
- Conduct thorough post-incident reviews to understand the underlying causes of security incidents and integrate these lessons into future strategies. This process enhances both security measures and organisational resilience, supported by technology management that requires regular assessments and updates of tools and processes based on feedback from operational data and post-incident analyses.
- Foster a collaborative environment where cybersecurity teams, IT teams, and other relevant departments work together, sharing insights and best practices. Establish

clear communication channels for an effective feedback loop, promoting a culture of shared responsibility and continuous improvement.

- Automate routine tasks within the feedback loop, such as data collection, analysis, and incident response, to enhance efficiency, reduce human error, and allow teams to focus on complex and strategic tasks.
- Align the feedback loop with overall organisational risk management processes to ensure that digital resilience efforts are in sync with the company's risk tolerance. This integration helps continuously update risk profiles based on new insights, making the organisation's response proactive rather than reactive.
- Invest in employee training and awareness programs to educate staff about cybersecurity best practices. Well-informed employees play a critical role in detecting and reporting incidents, forming a crucial component of the feedback loop.
- Conduct regular testing and simulation exercises to evaluate the effectiveness of the feedback loop and the organisation's incident response plans. These exercises help identify gaps and areas for improvement, ensuring the feedback loop functions as intended.
- Integrate the feedback loop with ITSM processes to ensure a seamless flow of information between cybersecurity and IT teams, enhancing overall IT service efficiency and resilience.
- Establish a knowledge management system to capture and share insights from each incident, facilitating continuous learning and improvement within the feedback loop.
- Secure support from organisational leadership for feedback loop initiatives. Leadership support provides the necessary resources and ensures that these efforts align with broader organisational goals while promoting accountability and transparency.
- Maintain alignment with relevant cybersecurity standards and regulations, regularly reviewing and updating policies and procedures to ensure compliance and integration of new insights from the feedback loop.
- Prioritise ethical considerations when incorporating AI into the feedback loop. Ensure that AI implementations are transparent, fair, and accountable to maintain trust and align with organisational values.

By adopting these best practices, organisations can establish a robust feedback loop for digital resilience, enabling them to manage and adapt to the dynamic cybersecurity landscape proactively. Continuous improvement and a holistic approach to cybersecurity are key principles in building and maintaining a strong digital resilience strategy.

V. Conclusions

In conclusion, the intersection of Industry 5.0 principles with AI technologies represents a powerful force for positive transformation in industrial processes. The integration of human-centricity, environmental stewardship, and social benefit principles with AI capabilities has the potential to redefine how industries operate, innovate, and contribute to the well-being of individuals and society at large. In addition, the feedback loop is a vital mechanism for enhancing digital resilience by enabling organisations to monitor, adapt, and optimise their cybersecurity measures. Its key components, when integrated with technology management, continuous improvement, and Industry 5.0 principles, contribute to creating a resilient, adaptive, and human-centric digital and industrial landscape. Navigating the complexities of Industry 5.0 requires a strategic approach that embraces a human-centric ethos, effectively integrates advanced technologies, prioritises data-driven decision-making, and maintains a proactive stance toward cybersecurity challenges. This dynamic landscape demands agility, adaptability, and a continuous commitment to innovation.

Considering the findings outlined in this study, it is important to acknowledge several limitations. First, the review's scope was limited to publications from specific databases, leading to a relatively small sample size. For future research, it is suggested that aggregated dimensions be explored instead of focusing solely on individual aspects. Second, the search criteria for this review were limited to keywords related to "Digital Resilience" and "Industry 5.0" in the last four years, unintentionally excluding research on distinct keywords like human-centricity and sustainability. To foster a more comprehensive understanding, future studies should extend the timeframe and include all relevant keywords associated with Industry 5.0. Addressing these limitations and broadening the scope will contribute to advancing insights into Digital Resilience and Industry 5.0, facilitating the development of more robust frameworks.

References

[1] M. Ghobakhloo, M. Iranmanesh, M. L. Tseng, A. Grybauskas, A. Stefanini, and A. Amran, "Behind the definition of Industry 5.0: a systematic review of technologies, principles, components, and values," Journal of Industrial and Production Engineering, vol. 40, no. 6, pp. 432-447, 2023, doi: https://doi.org/10.1080/21681015.2023.2216701

[2] R. Martinez-Pelaez, A. Ochoa-Brust, S. Rivera, V. G. Felix, R. Ostos, H. Brito, and L. J. Mena, "Role of digital transformation for achieving sustainability: mediated role of stakeholders, key capabilities, and technology," Sustainability, vol. 15, no. 14, p. 11221, 2023, doi: https://doi.org/10.3390/su151411221.

[3] DigitalEurope, *The Digital Front Line: 15 Actions to Boost Europe's Digital Resilience*, 2023. [Online]. Available: https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2023/03/DIGITALEUROPE-TECHNOLOGY-IN-THE-FACE-OF-HYBRID-THREATS-FINAL-WEB-1.pdf

[4] A. Miceli, B. Hagen, M. P. Riccardi, F. Sotti, and D. Settembre-Blundo, "Thriving, not just surviving in changing times: How sustainability, agility and digitalisation intertwine with organisational resilience," *Sustainability*, vol. 13, no. 4, p. 2052, 2021, doi: https://doi.org/10.3390/su13042052.

[5] V. B. Klein and J. L. Todesco, "COVID-19 crisis and SMEs responses: The role of digital transformation," *Knowledge and Process Management*, vol. 28, no. 2, pp. 117-133, 2021, doi: https://doi.org/10.1002/kpm.1660.

[6] P. K. R. Maddikunta, Q. V. Pham, B. Prabadevi, N. Deepa, K. Dev, T. R. Gadekallu, and M. Liyanage, "Industry 5.0: A survey on enabling technologies and potential applications," *Journal of Industrial Information Integration*, vol. 26, p. 100257, 2022, doi: https://doi.org/10.1016/j.jii.2021.100257.

[7] A. Akundi, D. Euresti, S. Luna, W. Ankobiah, A. Lopes, and I. Edinbarough, "State of Industry 5.0 - Analysis and identification of current research trends," *Applied System Innovation*, vol. 5, no. 1, p. 27, 2022, doi: https://doi.org/10.3390/asi5010027.

[8] M. C. Zizic, M. Mladineo, N. Gjeldum, and L. Celent, "From Industry 4.0 towards Industry 5.0: A review and analysis of paradigm shift for the people, organisation and technology," *Energies*, vol. 15, no. 14, p. 5221, 2022, doi: https://doi.org/10.3390/en15145221.

[9] J. Alves, T. M. Lima, and P. D. Gaspar, "Is Industry 5.0 a Human-Centred Approach? A Systematic Review," *Processes*, vol. 11, no. 1, p. 193, 2023, doi: https://doi.org/10.3390/pr11010193.

[10] D. Mourtzis, J. Angelopoulos, and N. Panopoulos, "A literature review of the challenges and opportunities of the transition from Industry 4.0 to Society 5.0," *Energies*, vol. 15, no. 17, p. 6276, 2022, doi: https://doi.org/10.3390/en15176276.

[11] D. Ivanov, "The Industry 5.0 framework: Viability-based integration of the resilience, sustainability, and human-centricity perspectives," *International Journal of Production Research*, vol. 61, no. 5, pp. 1683-1695, 2023, doi: https://doi.org/10.1080/00207543.2022.2118892.

[12] D. Paschek, A. Mocan, and A. Draghici, "Industry 5.0 - The expected impact of next industrial revolution," in *Proceedings MakeLearn and TIIM International Conference, Thriving on Future Education, Industry, Business, and Society*, Piran, Slovenia, May 2019, pp. 15-17. [Online]. Available: https://toknowpress.net/ISBN/978-961-6914-25-3/papers/ML19-017.pdf.

[13] X. Xu, Y. Lu, B. Vogel-Heuser, and L. Wang, "Industry 4.0 and Industry 5.0 - Inception, conception and perception," *Journal of Manufacturing Systems*, vol. 61, pp. 530-535, 2021, doi: https://doi.org/10.1016/j.jmsy.2021.10.006.

[14] V. Ozdemir and N. Hekim, "Birth of Industry 5.0: Making sense of big data with artificial intelligence," *The Internet of Things and Next-Generation Technology Policy*, vol. 22, no. 1, pp. 65-76, 2018, doi: https://doi.org/10.1089/omi.2017.019.

[15] K. Burnard, R. Bhamra, and C. Tsinopoulos, "Building organisational resilience: Four configurations," *IEEE Transactions on Engineering Management*, vol. 65, no. 3, pp. 351-362, 2018, doi: https://doi.org/10.1109/TEM.2018.2796181.

[16] Y. Brun et al., "Engineering Self-Adaptive Systems through Feedback Loops," in *Software Engineering for Self-Adaptive Systems*, B. H. C. Cheng, R. de Lemos, H. Giese, P. Inverardi, and J. Magee, Eds., Lecture Notes in Computer Science, vol. 5525, Springer, Berlin, Heidelberg, 2009. [Online]. Available: https://doi.org/10.1007/978-3-642-02161-9_3.

[17] E. Brucherseifer, H. Winter, A. Mentges, M. Mühlhäuser, and M. Hellmann, "Digital Twin conceptual framework for improving critical infrastructure resilience," *Automatisierungstechnik*, vol. 69, no. 12, pp. 1062-1080, 2021, https://doi.org/10.1515/auto-2021-0104.

[18] S. McManus, E. Seville, D. Brunsdon, and J. Vargo, "Resilience management: a framework for assessing and improving the resilience of organisations," 2007. [Online]. Available: http://hdl.handle.net/10092/2810.

[19] B. Steenwinckel, D. De Paepe, S. V. Hautte, P. Heyvaert, M. Bentefrit, P. Moens, et al., "FLAGS: A methodology for adaptive anomaly detection and root cause analysis on sensor data streams by fusing expert knowledge with machine learning," *Future Generation Computer Systems*, vol. 116, pp. 30-48, 2021, doi: https://doi.org/10.1016/j.future.2020.10.015.

[20] O. Renn, M. Laubichler, K. Lucas, W. Kroger, J. Schanze, R. W. Scholz, and P. J. Schweizer, "Systemic risks from different perspectives," *Risk Analysis*, vol. 42, no. 9, pp. 1902-1920, 2022, doi: https://doi.org/10.1111/risa.13657.

[21] O. M. Araz, T. M. Choi, D. L. Olson, and F. S. Salman, "Role of analytics for operational risk management in the era of big data," *Decision Sciences*, vol. 51, no. 6, pp. 1320-1346, 2020, doi: https://doi.org/10.1111/deci.12451.

[22] D. Sjodin, V. Parida, M. Palmie, and J. Wincent, "How AI capabilities enable business model innovation: Scaling AI through co-evolutionary processes and feedback loops," *Journal of Business Research*, vol. 134, pp. 574-587, 2021, doi: https://doi.org/10.1016/j.jbusres.2021.05.009.

[23] A. Aldoseri, K. Al-Khalifa, and A. Hamouda, "A Roadmap for Integrating Automation with Process Optimization for AI-powered Digital Transformation," *Preprints*, 2023, 2023101055, https://doi.org/10.20944/preprints202310.1055.v1.

[24] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *Systematic Reviews*, vol. 10, no. 1, pp. 1-11, 2021, doi: https://doi.org/10.1136/bmj.n71.

[25] M. Gusenbauer and N. R. Haddaway, "Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources," *Research Synthesis Methods*, vol. 11, no. 2, pp. 181-217, 2020, doi: https://doi.org/10.1002/jrsm.1378.

[26] D. A. S. Estay, R. Sahay, M. B. Barfod, and C. D. Jensen, "A systematic review of cyber-resilience assessment frameworks," *Computers & Security*, vol. 97, p. 101996, 2020, doi: https://doi.org/10.1016/j.cose.2020.101996.

[27] P. Radanliev, D. De Roure, K. Page, et al., "Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments – cyber risk in the colonisation of Mars," *Safety in Extreme Environments*, vol. 2, pp. 219-230, 2020, doi: https://doi.org/10.1007/s42797-021-00025-1.

[28] Q. Hu, Y. Lu, Z. Pan, and B. Wang, "How does AI use drive individual digital resilience? A conservation of resources (COR) theory perspective," *Behaviour & Information Technology*, vol. 42, no. 15, pp. 2654-2673, 2023, doi: https://doi.org/10.1080/0144929X.2022.2137698.

[29] K. Fysarakis et al., "PHOENI2X – A European Cyber Resilience Framework With Artificial-Intelligence-Assisted Orchestration, Automation & Response Capabilities for Business Continuity and Recovery, Incident Response, and Information Exchange," in *IEEE International Conference on Cyber Security and Resilience (CSR)*, Venice, Italy, 2023, pp. 538-545, doi: 10.1109/CSR57506.2023.10224995.

[30] N. Shahsavarani and S. Ji, "Research in Information Technology Service Management (ITSM): Theoretical Foundation and Research Topic Perspectives," in *CONF-IRM Proceedings*, 2011, paper 30. [Online]. Available: https://aisel.aisnet.org/confirm2011/30.

[31] T. Zonta, C. A. Da Costa, R. da Rosa Righi, M. J. de Lima, E. S. da Trindade, and G. P. Li, "Predictive maintenance in the Industry 4.0: A systematic literature review," *Computers & Industrial Engineering*, vol. 150, p. 106889, 2020, doi: https://doi.org/10.1016/j.cie.2020.106889.

[32] M. Spremic, "Governing digital technology - how mature IT governance can help in digital transformation?" *International Journal of Economics and Management Systems*, vol. 2, 2017. [Online]. Available: https://www.iaras.org/iaras/filedownloads/ijems/2017/007-0029(2017).pdf.

[33] S. V. Buer, G. I. Fragapane, and J. O. Strandhagen, "The data-driven process improvement cycle: Using digitalisation for continuous improvement," *IFAC-PapersOnLine*, vol. 51, no. 11, pp. 1035-1040, 2018, doi: https://doi.org/10.1016/j.ifacol.2018.08.471.

[34] A. R. Kunduru, "Cloud BPM Application (Appian) Robotic Process Automation Capabilities," *Asian Journal of Research in Computer Science*, vol. 16, no. 3, pp. 267-280, 2023, doi: https://doi.org/10.9734/ajrcos/2023/v16i3361.

[35] M. Woschank, E. Rauch, and H. Zsifkovits, "A review of further directions for artificial intelligence, machine learning, and deep learning in smart logistics," *Sustainability*, vol. 12, no. 9, p. 3760, 2020, doi: https://doi.org/10.3390/su12093760.

[36] P. Meso and R. Jain, "Agile Software Development: Adaptive Systems Principles and Best Practices," *Information Systems Management*, vol. 23, no. 3, pp. 19-30, 2006, doi: 10.1201/1078.10580530/46108.23.3.20060601/93704.3.

[37] H.-M. Heyn et al., "Requirement Engineering Challenges for AI-intense Systems Development," *IEEE/ACM 1st Workshop on AI Engineering - Software Engineering for AI (WAIN)*, Madrid, Spain, 2021, pp. 89-96, doi: 10.1109/WAIN52551.2021.00020.

[38] B. C. Stahl, *Artificial intelligence for a better future: an ecosystem perspective on the ethics of AI and emerging digital technologies*, Springer Nature, 2021. doi: 10.1007/978-3-030-69978-9.

[39] V. B. Klein and J. L. Todesco, "COVID-19 crisis and SMEs responses: The role of digital transformation," *Knowledge and Process Management*, vol. 28, no. 2, pp. 117–133, 2021. doi: 10.1002/kpm.1660.

[40] M. C. Jackson, Systems Thinking: Creative Holism for Managers. John Wiley & Sons, Inc., 2016. [Online]. Available: http://dspace.vnbrims.org:13000/jspui/bitstream/123456789/1166/1/Systems%20Thinking.pdf