Adopting New Technology is a Distant Dream? The Risks of Implementing Industry 4.0 in Emerging Economy SMEs

Jagannadha Pawan Tamvada[1] Sanjiv Narula[2] David Audretsch[3] Harish Puppala[4] Anil Kumar[5]

ABSTRACT

Manufacturing organisations worldwide are embracing Industry 4.0 (I4.0) and its associated technologies, such as the Internet of Things (IoT), Advanced Robotics, Big Data, and Cybersecurity. However, its implementation poses considerable risks for SMEs in emerging economies. Based on a survey of industry experts and business leaders associated with implementing I4.0 in the dynamically evolving economy of India, this paper identifies and prioritises the critical risks linked with implementing I4.0 in SMEs. Empirical results using the Fuzzy-Analytical Hierarchy Process suggest a hierarchy of risks associated with SMEs' transition to I4.0, with financial and technological risks posing the most significant barriers to I4.0 adoption. The novel results presented here can enable strategy development to effectively manage the risks of implementing new technologies in emerging economy contexts.

Forthcoming, *Technological Forecasting and Social Change* **(Accepted version)**

Keywords: Industry 4.0; Digitalisation; Risks; SMEs; Fuzzy-AHP

[1] Southampton Business School, University of Southampton, United Kingdom. jp.tamvada@soton.ac.uk
[2] BML Munjal University, India. sanjiv.narula.17pd@bmu.edu.in
[3] Indiana University, Bloomington, USA. daudrets@indiana.edu
[4] BML Munjal University, India. harish.puppala@bmu.edu.in
[5] London Metropolitan University, United Kingdom A.Kumar@londonmet.ac.uk

1. INTRODUCTION

The fourth industrial revolution (I4.0) and the related technology diffusion drive are expected to affect dramatic shifts in modern industry, leading to significant socioeconomic changes (Kiel et al., 2017; Tortorella et al., 2020; Yadav et al., 2020). I4.0 integrates the digital and physical worlds and blurs the boundaries of these two domains by combining modern digital technologies with traditional technologies and big data analytics (Liao et al., 2017; Tseng et al., 2018; Ardito et al., 2019). It leads engineering into a digitalised, networked, and decentralised value-creation system (Kiel et al., 2017; Ardito et al., 2018).

As in the case of social media, the exponential digital transformation resulting from it is likely to impact all industry sectors (Li, 2018; Appio et al., 2021). To exploit opportunities arising from I4.0, firms must integrate new digital technologies and competencies into their businesses and legacy assets (Kiel et al., 2017; Ardito et al., 2018; Ardito et al., 2019).

I4.0 is more than a technology-focused transformation (Liao et al., 2017; Ardito et al., 2019). Its real opportunity lies in unlocking digitalisation's full potential, going beyond technologies, and harnessing its abilities to influence society (Liao et al., 2017; Tseng et al., 2018). I4.0 technologies improve organisations' productivity, quality, cost, delivery, environmental, and safety levels (Rüßmann et al., 2015; Ardito et al., 2018). During the past decade, scholars have examined the implications of I4.0, digital transformation for management and organisational studies (Ardito et al., 2019; Correani et al., 2020; D'Ippolito et al., 2019; Usai et al., 2021).

While I4.0 has multiple benefits, it is associated with high investments, personnel costs, unclear economic benefits, and long and uncertain amortisation periods (Sommer, 2015, Ghanbari et al., 2017; Kiel et al., 2017; Kovacs, 2018; Piccarozzi et al., 2018; Birkel et al., 2019). It involves technological risks that arise from technical complexity, the lack of maturity of I4.0 technologies, device integration, and infrastructure deficiencies/network congestion (Sommer, 2015; Müller et al., 2018; Ben-Daya et al., 2019; Birkel et al., 2019), and operational/ social risks arising from job losses, internal resistance, inadequate qualifications, the shift in competencies, and lack of expertise (Piccarozzi et al. 2018; Stock et al., 2018).

Notably, it also leads to unprecedented challenges for SMEs (Sommer, 2015; Mittal et al., 2018). Large manufacturing firms can configure advanced processes and I4.0 digital technologies to create smart working environments and transition to I4.0 (Lee et al., 2016). By contrast, most manufacturing SMEs find imposing barriers impeding the adoption of I4.0 technologies, although they can significantly advance their competitiveness (Sommer, 2015; Ganzarain and Errasti, 2016; Horváth and Szabó, 2019). However, extant research has mainly concentrated on large companies in developed countries, with a limited examination of risks of I4.0 for SMEs in emerging countries. Furthermore, barriers to I4.0 implementation haven't been fully explored in the literature.

Thus, the absence of consensus on the I4.0 implementation risks, the disproportionate focus on large firms in the literature, the absence of guidance on the prioritisation of risks, and the lack of sufficient evidence from emerging economies are compelling gaps in the extant literature. These research gaps underscore the need to validate and prioritise critical risks in implementing I4.0 for SMEs in emerging economies. This paper contributes to the emerging literature on digitalisation and I4.0 by identifying the risks associated with the digital transformation of SMEs in the context of I4.0 in SMEs in an emerging economy-- India, the sixth largest manufacturing country in the world (Sharma et al., 2019). In particular, the paper prioritises risks to identify the most significant bottlenecks to the adoption of I4.0 by SMEs.

India has a strong focus on manufacturing and has taken new initiatives such as the "Make in India" program to accelerate manufacturing in the country and increase the share of manufacturing in GDP to 25 per cent (Kamble et al., 2018). India's industrial policy aims to make the country a leader in the usage and implementation of Industry 4.0 (Liao et al., 2017; Srivastava et al., 2018; Kamble et al., 2018; Kumar et al., 2022).

Based on expert surveys of industry leaders working towards implementing I4.0 in their SMEs, the empirical results, using the AHP-Fuzzy methodology, shed light on risks in seven categories that can arise in the context of the digital transformation of SMEs. The results demonstrate that financial, technological, and operational risks are the most significant risks facing SMEs implementing the technologies of I4.0, accounting for nearly three-fourths of the total risk profile. To the best of the authors' knowledge, these novel results are the first to empirically validate and prioritise the implementation risks associated with the successful digital transformation of SMEs in an emerging economy context.

The following section presents a comprehensive literature review of I4.0-related technologies and their associated risks. Section three discusses the research methodology. The fourth section presents the results identifying the critical risks associated with implementing I4.0 in SMEs. The final section offers a discussion and concludes the paper.

2. IDENTIFICATION OF RISK CATEGORIES AND RISKS

2.1. Literature review

Industry 4.0 is associated with transforming the manufacturing industries using hi-tech smart technologies (Rauch et al., 2018; Bolesnikov et al., 2019; Ardito et al., 2019). Integrating the Industrial Internet of Things (IIoT) into its value creation process, I4.0 enables real-time collaboration from within and outside the enterprise (Ghobakhloo, 2020).

A crucial aspect of I4.0 is the usage of digital technologies such as cyber-physical systems (CPS), IIoT, cognitive computing and cloud computing, augmented reality (AR), advanced robotics, 3D printing, simulation, cybersecurity, and big data analytics (Hermann et al., 2015; Matt et al., 2016; Liao et al., 2017; Ghobakhloo 2018, Leos et al., 2018). The emergence and adoption of these technologies can fundamentally alter how industries function (Liao **et al.,** 2017; Rauch et al., 2018; Bolesnikov et al., 2019; Ceipek et al., 2021; Usai et al., 2021), as implementing them can enable businesses to deal with the unpredictability of markets, reduce the complexity of business processes, and the duration of innovation cycles (Ardito et al., 2018; Fareri et al., 2020). Companies can gain unprecedented visibility and control of their supply chains, machines, and facilities by integrating smart factories, warehouses, and factories into their operations and optimising the processes through digital technologies (Ghobakhloo, 2018; Leos, 2018; Tseng, 2018; Ceipek et al., 2021; Usai et al., 2021).

The application of Internet of Things (IoT) technologies can manage the challenges in engineering value formation, such as smaller technology and invention cycles, increasing marketplace unpredictability, and an extremely dynamic atmosphere in the aspect of snowballing competitive pressure (Ceipek et al., 2021; D'Ippolito et al., 2019; Kumar et al., 2022).

I4.0 is a relatively new way of managing manufacturing processes (Rüßmann et al., 2015; Liao et al., 2017; Ardito et al., 2019). In numerous cases, the application of I4.0 has revealed that the networks between products, processes, and systems have created a more intricate, dynamic, and real-time optimised web (Almada-Lobo, 2015; Lee et al., 2015; Rüßmann et al., 2015; Liao et al., 2017). Due to changes in business settings caused by I4.0, organisations will increasingly face new challenges (Fareri et al., 2020).

Firms need to use the six design principles of decentralisation, virtualisation, interoperability, real-time capability, modularity, and service orientation to leverage the benefits of the I4.0 technologies. (Hermann et al., 2015). The decentralisation principle refers to the ability of CPS to decide autonomously and make manufacturing decisions locally (Almada-Lobo, 2015). The principle of virtualisation refers to a computer-generated copy of a smart industrial unit that is created by connecting device information with simulated models of an industrial plant (Hermann et al., 2015). The interoperability principle provides individuals and smart factories with real-time communication capabilities (Ghobakhloo, 2018). The real-time capability refers to collecting and analysing data in real-time (Ghobakhloo, 2020). The modularity principle refers to the ability to build a production line that is flexible, adaptable, and customisable to the needs of customers (Matt et al., 2016; Ghobakhloo, 2018; Leos et al., 2018), and service orientation is the ability to anticipate, identify, and meet the needs even before they are articulated (Hermann et al., 2015; Ghobakhloo, 2018). The main objectives for implementing I4.0 are growth, customer-centric transformation, efficiency, minimising wastage, and developing into a sustainable organisation (Liao et al., 2017; Müller and Voigt, 2018; Matt and Rauch, 2020).

An emerging body of literature examines the role of I4.0 for SMEs (Matt et al., 2016; Radzi et al., 2017; Leos et al., 2018; Horváth and Szabó, 2019; Masood and Sonntag,2020; Yadav et al., 2020). I4.0 provides a more interlinked and well-rounded manufacturing approach to SMEs by connecting the physical world with the digital (Leos et al., 2018; Matt and Rauch, 2020; Moeuf et al., 2020). This interconnection, in turn, empowers collaboration and access across people, products, processes, and systems during value creation (Rüßmann et al., 2015; Liao et al., 2017; Ardito et al., 2018). Notwithstanding the benefits, SMEs are not sure if, when, and in what way they should start the transition to I4.0 (Sommer, 2015).

Extant research does not extensively examine and identify the entire spectrum of potential risks associated with the implementation of I4.0 in SMEs in a developing country context. Hamzeh et al. (2018), in a survey with manufacturing managers and consultants in New Zealand, consider that I4.0 will lessen manufacturing expenses and improve agility and service offerings. However, this work is prospective and was carried out with a very homogeneous cluster of consulting members of SMEs. Decker (2017) examined these in the context of Danish SMEs using case study research and found that skill gaps are the major issues in the transformation towards I4.0. Mittal et al. (2018) present a literature review of the I4.0 framework, maturity model, readiness assessment framework, and associated risks but without stating the risks related to SMEs. Matt et al. (2020) highlighted that SMEs' lack of financial resources, skills, and people's competency and problems with old machines are the key issues in implementing I4.0 technologies.

While the role of I4.0 for SMEs and its benefits have been examined (Ganzarain and Errasti, 2016; Decker and Jørsfeldt; 2017; Radzi et al., 2017; Leos et al., 2018; Bolesnikov et al., 2019; Horváth and Szabó, 2019; Masood and Sonntag,2020; Moeuf et al., 2020; Yadav et al., 2020), the extant scholarship has mainly limited its focus to the returns associated with the application of I4.0. It has not explicitly focused on empirical testing and validating the critical risks associated with its implementation, particularly in an emerging economy SME context. The few case studies that have examined this have led to diverging views on I4.0 implementation risks. More specifically, the extant research has not tested the significance of prioritising I4.0 risks and has yet validated the extensive set of risks associated with implementing I4.0 technologies in SMEs in emerging economies.

SMEs in emerging economies have significantly more limitations in accessing capital and technology and rely more on manual processes (Coad and Tamvada 2012). Without adequate integration with the broader industrial context that is adopting I4.0, SMEs may face compelling challenges in survival, particularly in an environment marked by uncertainty (Sommer, 2015; Kamble et al., 2018; Dutta et al., 2020; Raj et al., 2020; Snieška et al., 2020). There is an imminent need for SME leaders to prepare for the coming digital era to prevent intellectual property loss, sabotage of manufacturing, and damages arising from downtime (Dutta et al., 2020; Raj et al., 2022).

In this paper, we examine the risks in the context of India, the sixth largest manufacturing country. India's industrial policy aims to make the country a leader in using and implementing Industry 4.0. However, today, in the context of adopting I4.0, India lags compared to the other nations (Dutta et al., 2020). In a significant fraction of the manufacturing sector, the systems that can function independently are limited, and the implementation of I4.0 in India is still in the nascent stages (Dutta et al., 2020; Raj et al., 2020). As a major driver of India's economic growth, manufacturing accounts for 15–16% of the national GDP and employs nearly 12 per cent of its working population (Mehta et al., 2017; Kamble et al.,2018). In the next few years, the GDP of the Indian manufacturing industry is expected to rise by 25 per cent, which can create 100 million new jobs (Kamble et al.,2018).

With SMEs contributing a significant share to India's manufacturing ambitions, I4.0 is an exciting opportunity to help India realise its manufacturing targets by 2025 (Kamble et al.,2018). Srivastava et al. (2018) suggest that the defense, aviation, railway, automobile, automotive component, electronics, pharmaceutical, textile, and pharmaceutical industries are key sectors of India that can contribute $80-100 billion a year to India's GDP by 2025 if they quickly adopt I4.0. However, such adoption remains uncertain (Srivastava et al., 2018; Kamble et al., 2018). Even though SMEs are eager to employ I4.0 to advance the level of their manufacturing, there are numerous risks to be overcome (Srivastava et al., 2018; Kamble et al., 2018; Dutta et al., 2020; Raj et al., 2020).
For example, SMEs have limited access to technology due to its high costs. Several factors, such as high investment levels and unclear cost-benefit analyses for I4.0, contribute to this (Kamble et al., 2018).

A summary of the literature review of potential risks associated with Industry 4.0 is provided in Table 1. To identify the risk categories and the risks of implementing I4.0, we have examined the databases of Scopus, Web of Science, Taylor & Francis, and Science Direct. Initially, we identified 685 papers from different scholarly databases (Scopus 215, Taylor and Francis 260, and Science Direct 210). The identified risks from these papers were grouped into different categories. These categories include financial risks, operational risks, technological risks, business risks, societal and environmental risks, supply chain risks, and cybersecurity risks. Following this, the generated list of risks was shared with industry experts to identify the relevance of each risk in the context of SMEs. We used this as a starting point for validating and prioritising the risks in the Indian context.

Table 1: Summary of Industry 4.0 associated risks

Risk	Sub-Risk	Citation
Financial risks	High investments	Sommer, 2015; Ghanbari et al., 2017; Kovacs, 2018; Piccarozzi et al., 2018; Birkel et al., 2019; Snieška et al., 2020
	Personnel costs	
	Long and uncertain amortisation	
	Too late investments	
	Risk of obsolescence of an investment in technology	
	Unclear economic benefit	
	Risk of false investments	
	A decision in what to invest when	
Operational risks	Maintenance	Sommer, 2015; Sanders et al., 2016; Tupa et al., 2017; Giotopoulos et al., 2017; Birkel et al., 2019; Fareri et al., 2020)
	Higher complexity	
	Low awareness	
	Industrial espionage	
	Redesign of facility layout	
	Inadequate qualification of employees	
	Restrictions by employees' representatives	
	Sabotage by employees	
	Internal resistance and corporate culture	
	Shifts of competencies	
	Manufacturing process management-based risk	
	Operation method and tool-based risks	
	Denial-of-Service (DoS)	
	Infrastructure shortcomings	
	Lack of expertise	
	Organisational risk	
	Fear of employees	
Technological risk	Technical complexity	Brettel et al., 2014; Lasi et al., 2014; Sommer, 2015; Müller et al., 2018; Ben-Daya et al., 2019; Birkel et al.,
	Low degree of maturity of I4.0 technologies	
	Technical integration	
	Lacking standards/international standards differ	
	Increasing dependence on technology	

	Retrofitting	2019; Snieška et al., 2020
	IT-interface problems	
	Availability of fast internet	
	Communication between devices	
	Lack of decision logic	
	Stability of the internet-based communication	
	Availability of adequate IT Infrastructure	
	Increased system maintenance/incompatibilities	
	Lacking understanding of data-driven business models	
	Infrastructure shortcomings/network congestions	
	Awareness and organisational structure	
Business risk	Losing a competitive advantage	Sommer, 2015; Birkel et al., 2019; Oesterreich and Teuteberg, 2016; Moeuf et al., 2020
	Transformation of business models	
	Loss of core competencies	
	Power shifts	
	Transparency of data can be misused	
	Diminishing barriers to market entrance	
	Additional demands of customers	
	New competitors	
	Legal and political aspects	
	Theft of industrial trade secrets and intellectual property	
	Dependence on technology providers	
	Short-term strategy	
Societal and environmental risks	Job losses	Sommer, 2015; Oesterreich and Teuteberg, 2016; Birkel et al., 2019
	Acceptance by society	
	Mental stress	
	Concerns regarding AI	
	Manufacturing relocation	
	New requirements for training	
	Emissions	
	System overload	
	Wastages	
Supply chain risks	Loss of suppliers (barriers to technologies)	Tupa et al., 2017; Yin et al., 2018; Wang et al.,2020; Snieška et al., 2020
	Coordination complexity	
	Radical changes in supply chain	
	Loss of bargaining power over the supplier	
	Different standards used along the supply chain	
	Loss of competitive advantages	
Cybersecurity risk	Transfer data from and to unauthorised devices	Brettel et al., 2014; Lasi et al., 2014; Sommer, 2015; Kiel et al., 2017; Müller et al., 2018; Ben-Daya et al., 2019;
	Data breach/theft/tampering and spoofing	
	IT security	
	IoT security	
	Manipulation of data/communication/hardware/software	

	Repudiation attacks	Birkel et al., 2019; Snieška et al., 2020
	Information security	
	Eavesdropping	
	Cloud Abuse	
	Malware attack	
	Hacking	
	Insider threats	
	Shadow IT Systems	
	Outdated hardware and software	
	Form jacking	
	Manipulation of communication	

One of the key financial risks is that deploying I4.0 technologies requires large-scale investments, with an unknown payback period and uncertainty of success (Ghanbari et al., 2017; Kiel et al., 2017; Birkel et al., 2019). Many processes of operational value creation can be theoretically automated, digitised, and networked (Tupa et al., 2017). Despite that, huge investments are required to build and implement this infrastructure and maintain it over time (Birkel et al., 2019).

Most of the challenges in operations can be attributed to the costs, complexity, lack of skills, and technical expertise required for I4.0 implementation (Birkel et al., 2019). In light of the rapid development of digital adoption and transformation, numerous organisations struggle to find and equip their talent with the appropriate skills and knowledge (Piccarozzi et al., 2018; Stock et al., 2018; Snieška et al., 2020). Moreover, the management of conventional businesses and the introduction of digital innovations concurrently require added managerial skills and substantial staff support (Matt et al., 2018; Birkel et al., 2019; Moeuf et al., 2020; Snieška et al., 2020; Appio et al.,2021). In most enterprises, connecting all the machines and employees on a factory floor is difficult due to a lack of infrastructure and skilled personnel (Moeuf et al., 2020; Snieška et al., 2020).

Apart from offering clear business advantages, technologies of I4.0 such as the Internet of Things (IoT) technology, have enabled manufacturers to become more interconnected, sophisticated, and heterogeneous simultaneously (Hermann et al., 2015; Ghobakhloo, 2018; Birkel et al., 2019). Consequently, smart factories are vulnerable to malware, denial-of-service attacks, device hacks, and exploitation (Birkel et al., 2019). As a result, manufacturing networks in I4.0 may operate with an increased risk of cyber incidents (Kovacs, 2018; Birkel et al., 2019).

The business risks include difficulties configuring advanced processes and digital technologies needed to create smart working environments and transition to I4.0 (Lee et al., 2016). Most manufacturing SMEs find imposing barriers impeding the adoption of such technologies, although they can significantly advance their competitiveness (Sommer, 2015; Ganzarain and Errasti, 2016; Horváth and Szabó, 2019).

Similarly, businesses must rethink how they design their supply chains that will have the potential to reach the next level of operational efficiency (Lasi et al., 2014; Sanders et al., 2016). For instance, by leveraging I4.0 technology to increase real-time visibility across the value chain, manufacturers can proactively identify potential risk areas or respond more quickly (Brettel et al., 2014; Sanders et al., 2016). However, digitising and interconnecting the industrial value creation process can result in a high level of complexity (Tupa et al., 2017; Giotopoulos et al., 2017; Matt et al., 2018; Birkel et al., 2019) that can burden managing dynamically evolving scenarios where human intervention can be more efficient.

Furthermore, multiple societal and environmental risks are associated with implementing I4.0. These include resistance to learning the adoption of the emerging technologies, ethical and security issues involved with replacing the workplace with machines, and the fear of adopting smart systems across the value chain (Matt. et al., 2018; Piccarozzi et al., 2018; Stock et al., 2018; Snieška et al., 2020). These can impact the jobs markets (Birkel et al., 2019). Despite gradual shifts towards automation, some sectors may still see rising unemployment. This can significantly impact broader society and multiple economic actors (Horváth and Szabó, 2019).

As manufacturing cyberattacks are increasing exponentially, cybersecurity poses a significant risk for firms implementing I4.0. Many risks confront manufacturers, including malware, distributed denial-of-service attacks, and device hacking (Birkel et al., 2019). Manufacturing environments are becoming more interconnected than ever before because of I4.0. Internet of things (IoT) devices are increasingly used to monitor and control production systems, while brownfield plants are being upgraded by integrating wireless IoT devices (Sanders et al., 2016). To maintain operational continuity and meet the health and safety needs of their workforce, numerous manufacturers have adopted remote working practices, which have increased the risks associated with cybersecurity (Birkel et al., 2019). Given these identified risks, determining the relevance of each risk in the context of SMEs will enable the evaluation of the relative hierarchy of the risks of implementing I4.0.

3. METHODS

This section presents the research methodology we use to identify and prioritise the critical risks connected with the implementation of I4.0 in SMEs.

3.1 Empirical Model

The schematic illustration of the steps involved in this study are presented in Figure 1.

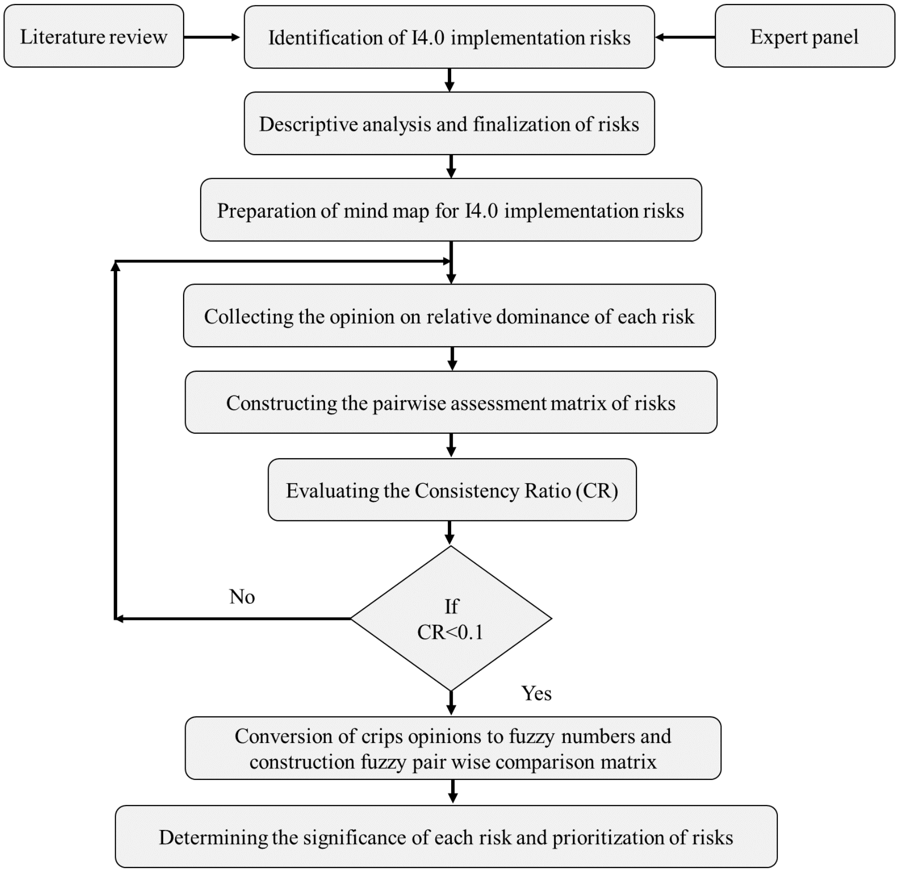

Literature review
Identification of I4.0 implementation risks
Expert panel
Descriptive analysis and finalization of risks
Preparation of mind map for I4.0 implementation risks
Collecting the opinion on relative dominance of each risk
Constructing the pairwise assessment matrix of risks
Evaluating the Consistency Ratio (CR)
No
If
CR<0.1
Yes
Conversion of crips opinions to fuzzy numbers and
construction fuzzy pair wise comparison matrix
Determining the significance of each risk and prioritization of risks

Figure 1: Schematic illustration of the steps involved in analysing the risk for implementing I4.0 in SME's

The analysis starts with identifying I4.0 implementation risks in SMEs with the help of extant literature survey, which is further reviewed by the constituted expert panel. A Likert scale of 1-5 is adopted to obtain the opinion regarding the relevance of each risk from the experts. The obtained responses are used to perform descriptive analysis, which aids in finalising the list of risks for further analysis and establishing prioritisation.

Determining the relative hierarchy of identified risks is a multi-criteria decision-making (MCDM) problem. Various MCDM techniques such as Analytical Network Process (ANP), Technique for Order of Preference by Similarity to Ideal Situations (TOPSIS), and Elimination and Choice Translating Reality (ELECTRE) have been adopted in literature to address such multi-criteria problems. The Analytical Hierarchy Process (AHP) technique is applied in this study for determining the local and global significance of the identified risks. This technique is superior compared to various other multi-criteria techniques such as TOPSIS, ANP, and ELECTRE (Harputlugil et al., 2011). This well-known method provides a structure for resolving various multi-criteria decision problems based on a comparative prioritisation allocated to each 'criterion's role in achieving the stated objective (Satty 1980).

However, AHP works on crisp decisions to resolve ambiguity and may not emulate human thinking (Kahraman et al. 2003). Despite being a robust method, this method fails in dealing with the haziness in judgment, especially while collecting the responses. Because of the ambiguity involved, different variants of AHP, such as Fuzzy AHP, have come into existence (Van Laarhoven and Pedrycz, 1983; Mangla et al., 2017). In the Fuzzy AHP technique, instead of a crisp opinion, a fuzzy opinion in the form of a fuzzy number is drawn based on each response of the experts. Applications of Fuzzy AHP are extended to various domains (Avikal et al., 2014, Karakaşoğlu and Ertuğrul, 2008, and Mangla et al., 2017).

This process makes a more reasonable evaluation of the weight of the criteria and better decisions thereof. In line with Van Laarhoven and Pedrcyz (1983), Deng (1999) also introduced a fuzzy methodology for managing multi-criteria decision-making. This method can handle the uncertainty caused by the subjective decisions of experts by applying a fuzzy set as a substitute for precise values (Chen and Pham, 2000). The use of a fuzzy approach in decision-making is beneficial to deal with the haziness of individual thoughts and intricacies and ambiguity in decision difficulties (Kahraman et al., 2003; Wang et al., 2008, Kumar et al., 2019).

Several studies have demonstrated that fuzzy numbers can be either triangular fuzzy numbers (TFNs) or trapezoidal fuzzy numbers (Chen and Pham, 2000; Kahraman et al., 2003; Wang et al., 2008; Kumar et al., 2019). In uncertain environments, TFNs are more appropriate as compared to trapezoidal fuzzy numbers since TFNs have an easier mathematical formulation and are capable of aiding in the interpretation of information (Ertugrul and Karakasoglu, 2008). During the applications, fuzzy numbers are either triangular fuzzy numbers (TFNs) or trapezoidal fuzzy numbers (Kahraman et al., 2003; Wang et al., 2008). TFNs are used in this study, as they are more appropriate than trapezoidal fuzzy numbers because of their computational straightforwardness and their benefit in processing information in uncertain settings (Ertugrul and Karakasoglu, 2009).

The steps involved in determining the significance of each risk are presented below.

Step-1: The opinion of experts regarding the relative dominance of each risk over the other is collected on a scale of 1-9 well known as Saaty scale. Judgment definition and the corresponding crisp and fuzzy values of the scale are shown in Table. 2. The obtained opinions are further used to construct the pair-wise comparison matrix. Eq.1 presents the generic representation of the pair-wise comparison matrix.

Table 2. Saaty Judgment scale adopted to obtain the responses

Crisp values and the judgement definition (n)	**Fuzzified Saaty's value**
1 (Significance level is the same)	(1, 1, 1 + n)
3 (Somewhat more significant)	(3 – n, 3, 3 + n)
5 (Strong significance)	(5 – n, 5, 5 + n)
7 (Demonstrated significance)	(7 – n, 7, 7 + n)
9 (Absolute significance)	(9 – n, 9, 9)
2, 4, 6, 8 (Intermittent scale)	(n – 1, n, n + 1), n = 2, 4, 6, 8

$$\begin{matrix} V_{11} & \cdots & V_{1N} \\ \vdots & V_{22} & \vdots \\ V_{N1} & \cdots & V_{NN} \end{matrix} \qquad (1)$$

Where, $V_{ij} = 1$ for the diagonal members of the matrix, and $V_{ij} = 1/V_{ji}$.

Same analysis is conducted at the sub-category analysis and the corresponding decision matrices are constructed. This results in a pairwise comparison matrix of risk categories and the pair-wise comparison matrices at the sub-risk level.

Step-2: The constructed decision matrices with crisp attributes are fuzzified using triangular membership functions to develop fuzzy pair-wise comparison matrix. Fuzzy weight can be represented as (a_1, b_1, c_1). The expression used for evaluating the range of ratings of experts is provided as Eq. 2.

$$x_{ij} = (a_{ij}, b_{ij,}c_{ij})$$

$$a_{ij} = \min_{K}(a_{ijK}),\ b_{ij} = \frac{1}{K} * \sum_{k=1}^{K}(a_{ijk}), c_{ij} = \max_{K}(a_{ijK}) \qquad (2)$$

Where i =*1, 2, ……..., n*; j =*1, 2, 3……..., m*; and k = *1, 2,*…….. number of experts

Step-3: In this step, the equivalent weight of each risk is assessed using a fuzzy synthetic method.

Let X={x_1, x_2, ………x_n} be the set of alternatives under evaluation

C={c_1, c_2, c_3……c_m} are the set of criteria based on which evaluation is to be conducted.

Then, as per the synthetic extent analysis, m values for each alternative will be obtained and can generally be written as:

M_{gi}^{1}, M_{gi}^{2}, ………… M_{gi}^{m}, i=1, 2, 3……..,n

where, M_{gi}^{1}, M_{gi}^{2}, ………… M_{gi}^{m} is the extent analysis values of the *ith* object for an *mth* aim. The synthetic fuzzy value can be defined as

$$S_i = \sum_{j=1}^{m} M_{gi}^{i} \otimes \left[\sum_{i=1}^{n}\sum_{j=1}^{m} M_{gi}^{j}\right]^{-1}, i = 1, 2, \dots\dots.. N \tag{3}$$

All *we, i=1, M*, are normalised fuzzy numbers with medium values equalling 1. ⊗ denotes fuzzy multiplication operation.

Step 4: Lastly, the local and global hierarchy of each sub-risk is evaluated based on defuzzified score computed using Eq.4.

$$D = (\mathrm{p} + \ \mathrm{q} + \ \mathrm{r})/3 \tag{4}$$

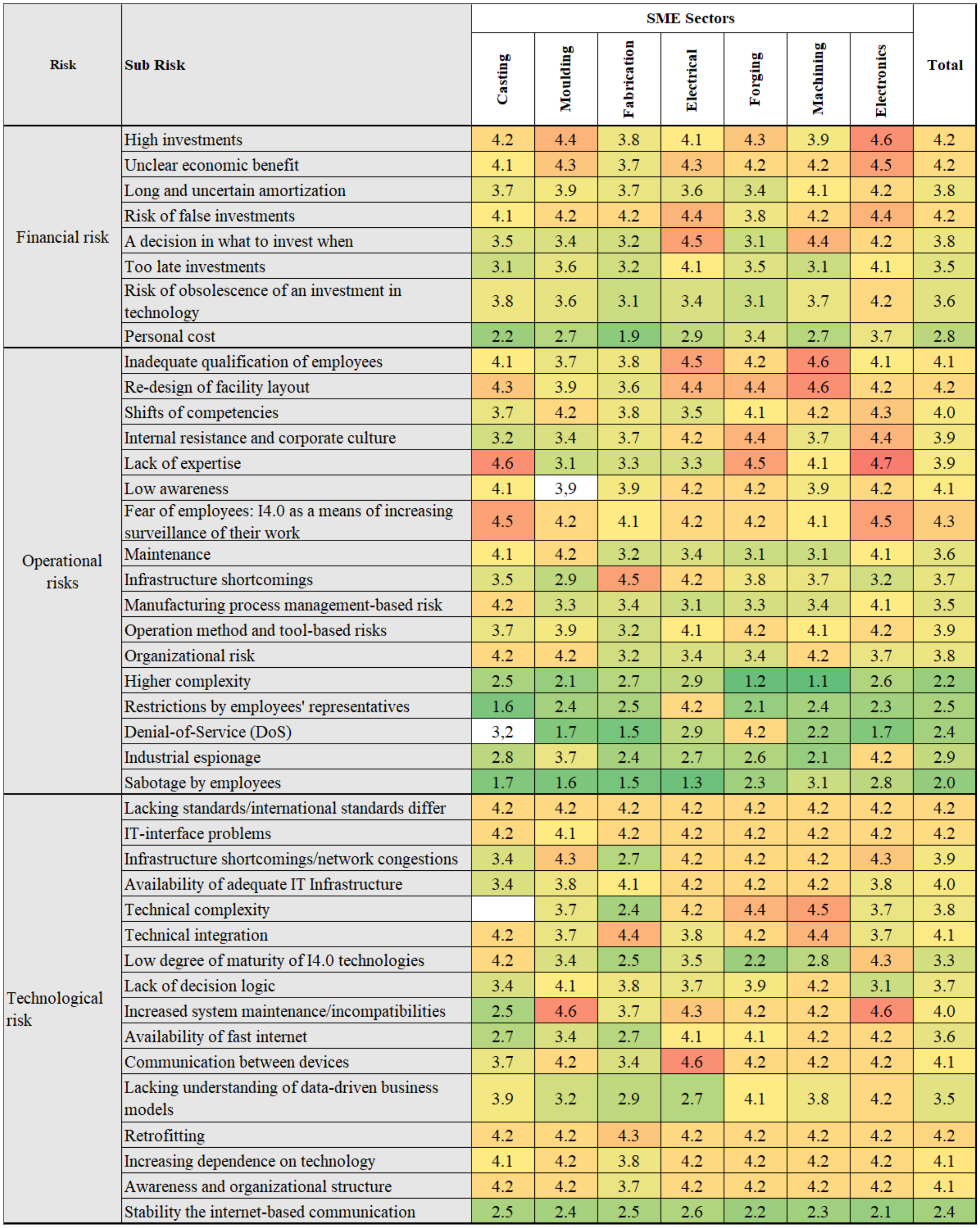
As described in the methodology, the identified list of risks are grouped under different categories and shared with the expert panel to know their response on their relevance in the context of SMEs in emerging countries. These attributes are further used to perform descriptive analysis and prepare the final list of risks to study the relative significance using the research methods discussed in section 3. A detailed insight into the descriptive analysis and the Fuzzy AHP analysis is given in the following sections.

3.2 Sample

This paper employs Fuzzy AHP in order to assess the risks related to the adoption of I4.0 in SMEs. As I4.0 adoption in Indian SMEs is in its initial stages, this study explores a targeted sample rather than a general one. The sample for this research involved 116 industry leaders from 46 SMEs in the electrical, electronics, casting, moulding, fabrication, forging, and machining sectors. The experts hold high-level positions in the SMEs as directors, chief operating officers, heads of operations, or plant heads of I4.0 implementing SMEs. The experts have an average experience of 17 years in the industry. The authors have used the following criteria to select the experts: they have 1) at least a bachelor's degree in technology/engineering; 2) work experience as a manager or above in the manufacturing sector, with leadership connection to lean and I4.0 implementation in the organisation and 3) willingness to participate in the study throughout the research period. An online survey was used for the data collection from Mar 2021 to Aug 2021. The average response time for carrying out the survey was nearly thirty minutes. The sample size of the research is adequate and in line with research pragmatism (Buchholz et al., 2009). The internal consistency of the survey instrument was evaluated using Cronbach's alpha, which was observed > 0.8, indicating that the instrument is highly reliable.

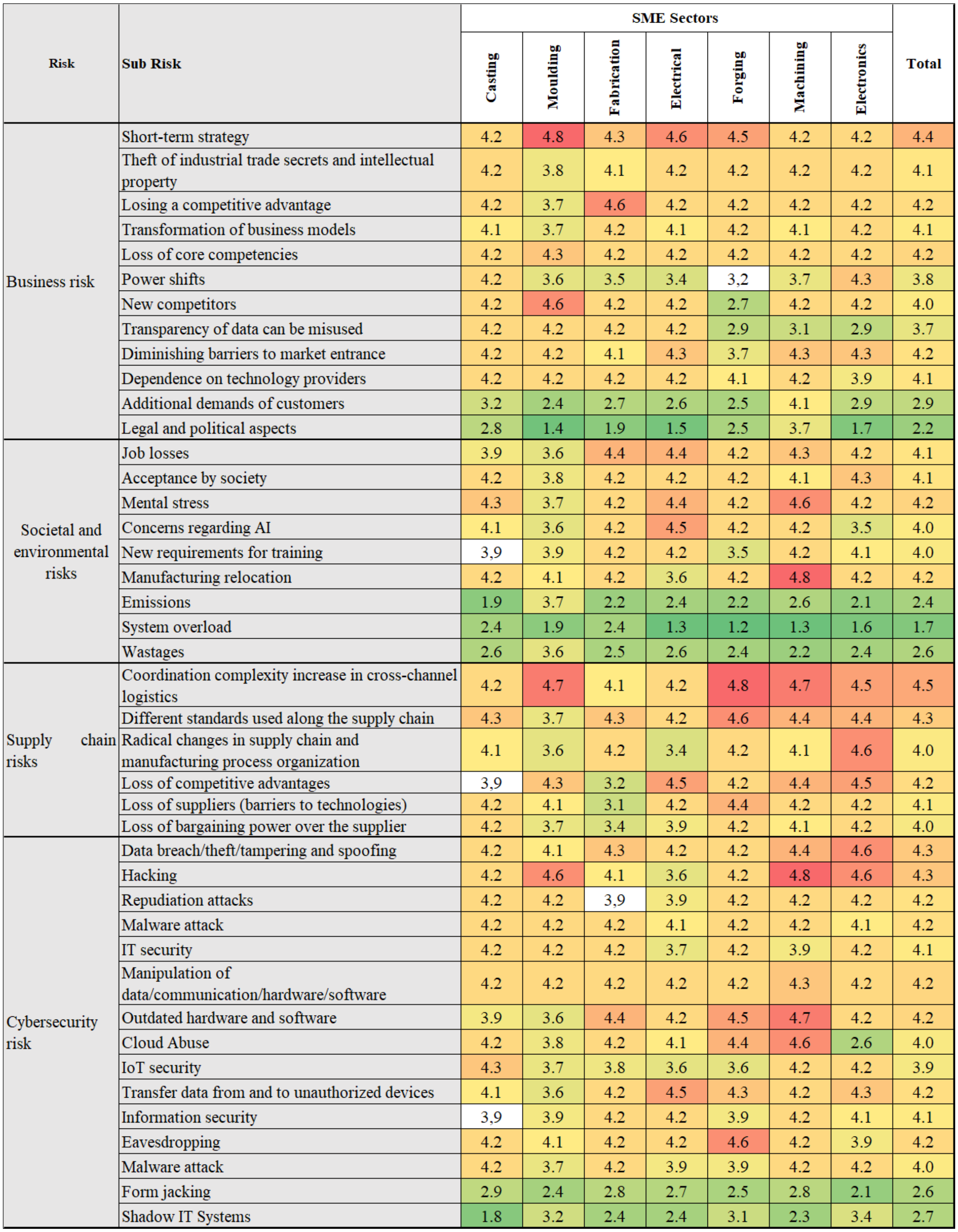
3.3 Descriptive Analysis

Figure 2 provides an overview of the mean score of experts' feedback on I4.0 implementation risks in the casting, moulding, fabrication, electrical, forging, machining, and electronics industries. The feedback from experts indicates high mean risk, ranging from 3.8 to 4.8 in 70 of the 80 risks identified during the literature review (Table 1). Besides, the standard deviation of these risks is low (0.12 to 0.39). This establishes that these risks are valid during the digital transformation of SMEs. In Figure 3, the finalised risks under each category are presented.



Risk	Sub Risk	SME Sectors							Total
		Casting	Moulding	Fabrication	Electrical	Forging	Machining	Electronics	
Financial risk	High investments	4.2	4.4	3.8	4.1	4.3	3.9	4.6	4.2
	Unclear economic benefit	4.1	4.3	3.7	4.3	4.2	4.2	4.5	4.2
	Long and uncertain amortization	3.7	3.9	3.7	3.6	3.4	4.1	4.2	3.8
	Risk of false investments	4.1	4.2	4.2	4.4	3.8	4.2	4.4	4.2
	A decision in what to invest when	3.5	3.4	3.2	4.5	3.1	4.4	4.2	3.8
	Too late investments	3.1	3.6	3.2	4.1	3.5	3.1	4.1	3.5
	Risk of obsolescence of an investment in technology	3.8	3.6	3.1	3.4	3.1	3.7	4.2	3.6
	Personal cost	2.2	2.7	1.9	2.9	3.4	2.7	3.7	2.8
Operational risks	Inadequate qualification of employees	4.1	3.7	3.8	4.5	4.2	4.6	4.1	4.1
	Re-design of facility layout	4.3	3.9	3.6	4.4	4.4	4.6	4.2	4.2
	Shifts of competencies	3.7	4.2	3.8	3.5	4.1	4.2	4.3	4.0
	Internal resistance and corporate culture	3.2	3.4	3.7	4.2	4.4	3.7	4.4	3.9
	Lack of expertise	4.6	3.1	3.3	3.3	4.5	4.1	4.7	3.9
	Low awareness	4.1	3,9	3.9	4.2	4.2	3.9	4.2	4.1
	Fear of employees: I4.0 as a means of increasing surveillance of their work	4.5	4.2	4.1	4.2	4.2	4.1	4.5	4.3
	Maintenance	4.1	4.2	3.2	3.4	3.1	3.1	4.1	3.6
	Infrastructure shortcomings	3.5	2.9	4.5	4.2	3.8	3.7	3.2	3.7
	Manufacturing process management-based risk	4.2	3.3	3.4	3.1	3.3	3.4	4.1	3.5
	Operation method and tool-based risks	3.7	3.9	3.2	4.1	4.2	4.1	4.2	3.9
	Organizational risk	4.2	4.2	3.2	3.4	3.4	4.2	3.7	3.8
	Higher complexity	2.5	2.1	2.7	2.9	1.2	1.1	2.6	2.2
	Restrictions by employees' representatives	1.6	2.4	2.5	4.2	2.1	2.4	2.3	2.5
	Denial-of-Service (DoS)	3,2	1.7	1.5	2.9	4.2	2.2	1.7	2.4
	Industrial espionage	2.8	3.7	2.4	2.7	2.6	2.1	4.2	2.9
	Sabotage by employees	1.7	1.6	1.5	1.3	2.3	3.1	2.8	2.0
Technological risk	Lacking standards/international standards differ	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2
	IT-interface problems	4.2	4.1	4.2	4.2	4.2	4.2	4.2	4.2
	Infrastructure shortcomings/network congestions	3.4	4.3	2.7	4.2	4.2	4.2	4.3	3.9
	Availability of adequate IT Infrastructure	3.4	3.8	4.1	4.2	4.2	4.2	3.8	4.0
	Technical complexity		3.7	2.4	4.2	4.4	4.5	3.7	3.8
	Technical integration	4.2	3.7	4.4	3.8	4.2	4.4	3.7	4.1
	Low degree of maturity of I4.0 technologies	4.2	3.4	2.5	3.5	2.2	2.8	4.3	3.3
	Lack of decision logic	3.4	4.1	3.8	3.7	3.9	4.2	3.1	3.7
	Increased system maintenance/incompatibilities	2.5	4.6	3.7	4.3	4.2	4.2	4.6	4.0
	Availability of fast internet	2.7	3.4	2.7	4.1	4.1	4.2	4.2	3.6
	Communication between devices	3.7	4.2	3.4	4.6	4.2	4.2	4.2	4.1
	Lacking understanding of data-driven business models	3.9	3.2	2.9	2.7	4.1	3.8	4.2	3.5
	Retrofitting	4.2	4.2	4.3	4.2	4.2	4.2	4.2	4.2
	Increasing dependence on technology	4.1	4.2	3.8	4.2	4.2	4.2	4.2	4.1
	Awareness and organizational structure	4.2	4.2	3.7	4.2	4.2	4.2	4.2	4.1
	Stability the internet-based communication	2.5	2.4	2.5	2.6	2.2	2.3	2.1	2.4

Figure 2(a): The average expert opinion score of the experts' opinions pertaining to the risks associated with I4.0 implementation in SMEs



Risk	Sub Risk	SME Sectors							Total
		Casting	Moulding	Fabrication	Electrical	Forging	Machining	Electronics	
Business risk	Short-term strategy	4.2	4.8	4.3	4.6	4.5	4.2	4.2	4.4
	Theft of industrial trade secrets and intellectual property	4.2	3.8	4.1	4.2	4.2	4.2	4.2	4.1
	Losing a competitive advantage	4.2	3.7	4.6	4.2	4.2	4.2	4.2	4.2
	Transformation of business models	4.1	3.7	4.2	4.1	4.2	4.1	4.2	4.1
	Loss of core competencies	4.2	4.3	4.2	4.2	4.2	4.2	4.2	4.2
	Power shifts	4.2	3.6	3.5	3.4	3,2	3.7	4.3	3.8
	New competitors	4.2	4.6	4.2	4.2	2.7	4.2	4.2	4.0
	Transparency of data can be misused	4.2	4.2	4.2	4.2	2.9	3.1	2.9	3.7
	Diminishing barriers to market entrance	4.2	4.2	4.1	4.3	3.7	4.3	4.3	4.2
	Dependence on technology providers	4.2	4.2	4.2	4.2	4.1	4.2	3.9	4.1
	Additional demands of customers	3.2	2.4	2.7	2.6	2.5	4.1	2.9	2.9
	Legal and political aspects	2.8	1.4	1.9	1.5	2.5	3.7	1.7	2.2
Societal and environmental risks	Job losses	3.9	3.6	4.4	4.4	4.2	4.3	4.2	4.1
	Acceptance by society	4.2	3.8	4.2	4.2	4.2	4.1	4.3	4.1
	Mental stress	4.3	3.7	4.2	4.4	4.2	4.6	4.2	4.2
	Concerns regarding AI	4.1	3.6	4.2	4.5	4.2	4.2	3.5	4.0
	New requirements for training	3,9	3.9	4.2	4.2	3.5	4.2	4.1	4.0
	Manufacturing relocation	4.2	4.1	4.2	3.6	4.2	4.8	4.2	4.2
	Emissions	1.9	3.7	2.2	2.4	2.2	2.6	2.1	2.4
	System overload	2.4	1.9	2.4	1.3	1.2	1.3	1.6	1.7
	Wastages	2.6	3.6	2.5	2.6	2.4	2.2	2.4	2.6
Supply chain risks	Coordination complexity increase in cross-channel logistics	4.2	4.7	4.1	4.2	4.8	4.7	4.5	4.5
	Different standards used along the supply chain	4.3	3.7	4.3	4.2	4.6	4.4	4.4	4.3
	Radical changes in supply chain and manufacturing process organization	4.1	3.6	4.2	3.4	4.2	4.1	4.6	4.0
	Loss of competitive advantages	3,9	4.3	3.2	4.5	4.2	4.4	4.5	4.2
	Loss of suppliers (barriers to technologies)	4.2	4.1	3.1	4.2	4.4	4.2	4.2	4.1
	Loss of bargaining power over the supplier	4.2	3.7	3.4	3.9	4.2	4.1	4.2	4.0
Cybersecurity risk	Data breach/theft/tampering and spoofing	4.2	4.1	4.3	4.2	4.2	4.4	4.6	4.3
	Hacking	4.2	4.6	4.1	3.6	4.2	4.8	4.6	4.3
	Repudiation attacks	4.2	4.2	3,9	3.9	4.2	4.2	4.2	4.2
	Malware attack	4.2	4.2	4.2	4.1	4.2	4.2	4.1	4.2
	IT security	4.2	4.2	4.2	3.7	4.2	3.9	4.2	4.1
	Manipulation of data/communication/hardware/software	4.2	4.2	4.2	4.2	4.2	4.3	4.2	4.2
	Outdated hardware and software	3.9	3.6	4.4	4.2	4.5	4.7	4.2	4.2
	Cloud Abuse	4.2	3.8	4.2	4.1	4.4	4.6	2.6	4.0
	IoT security	4.3	3.7	3.8	3.6	3.6	4.2	4.2	3.9
	Transfer data from and to unauthorized devices	4.1	3.6	4.2	4.5	4.3	4.2	4.3	4.2
	Information security	3,9	3.9	4.2	4.2	3.9	4.2	4.1	4.1
	Eavesdropping	4.2	4.1	4.2	4.2	4.6	4.2	3.9	4.2
	Malware attack	4.2	3.7	4.2	3.9	3.9	4.2	4.2	4.0
	Form jacking	2.9	2.4	2.8	2.7	2.5	2.8	2.1	2.6
	Shadow IT Systems	1.8	3.2	2.4	2.4	3.1	2.3	3.4	2.7

Figure 2(b): The average expert opinion score of the experts' opinions pertaining to the risks associated with I4.0 implementation in SMEs

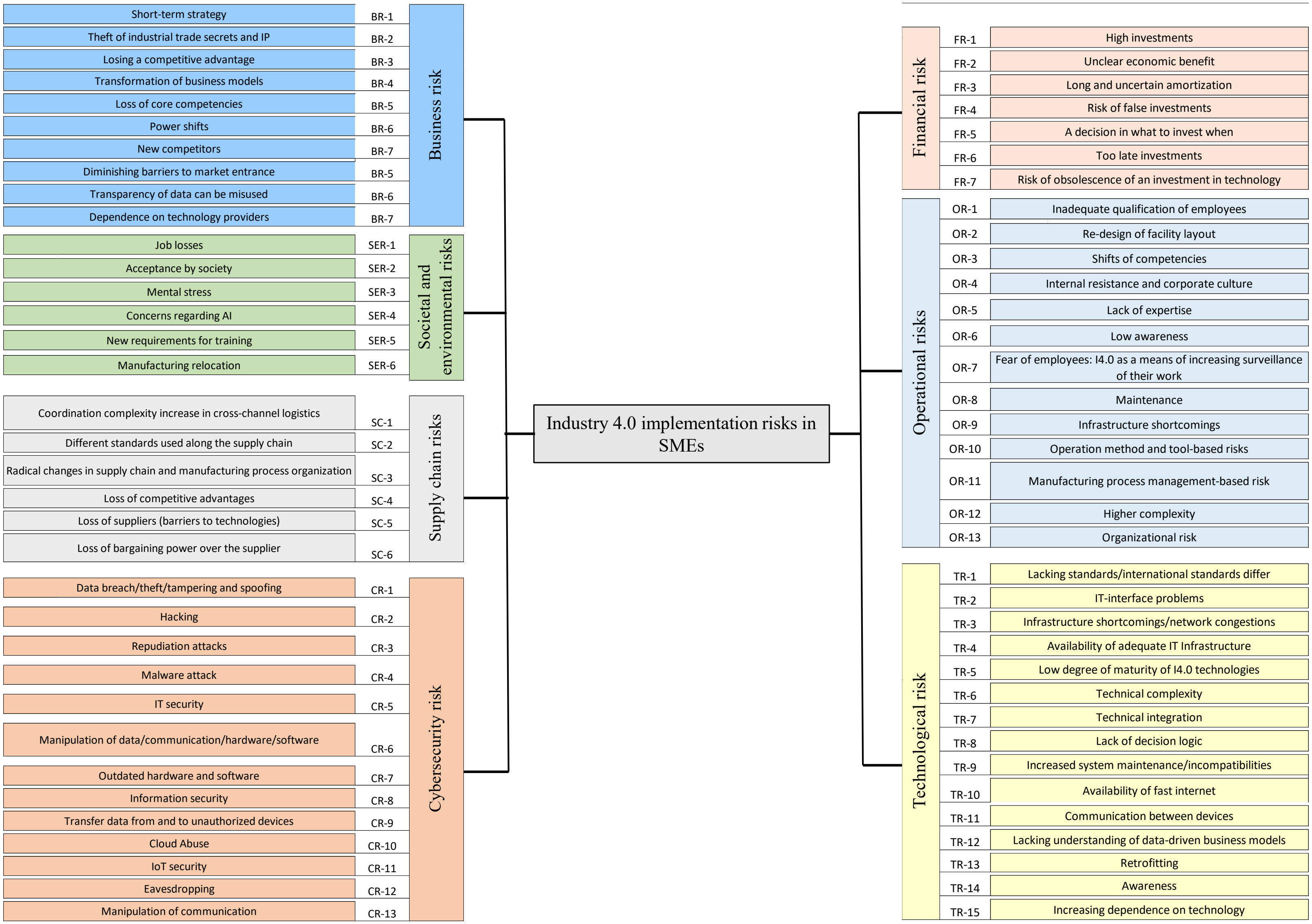

Industry 4.0 implementation risks in SMEs
Business risk
Short-term strategy BR-1
Theft of industrial trade secrets and IP BR-2
Losing a competitive advantage BR-3
Transformation of business models BR-4
Loss of core competencies BR-5
Power shifts BR-6
New competitors BR-7
Diminishing barriers to market entrance BR-5
Transparency of data can be misused BR-6
Dependence on technology providers BR-7
Societal and environmental risks
Job losses SER-1
Acceptance by society SER-2
Mental stress SER-3
Concerns regarding AI SER-4
New requirements for training SER-5
Manufacturing relocation SER-6
Supply chain risks
Coordination complexity increase in cross-channel logistics SC-1
Different standards used along the supply chain SC-2
Radical changes in supply chain and manufacturing process organization SC-3
Loss of competitive advantages SC-4
Loss of suppliers (barriers to technologies) SC-5
Loss of bargaining power over the supplier SC-6
Cybersecurity risk
Data breach/theft/tampering and spoofing CR-1
Hacking CR-2
Repudiation attacks CR-3
Malware attack CR-4
IT security CR-5
Manipulation of data/communication/hardware/software CR-6
Outdated hardware and software CR-7
Information security CR-8
Transfer data from and to unauthorized devices CR-9
Cloud Abuse CR-10
IoT security CR-11
Eavesdropping CR-12
Manipulation of communication CR-13
Financial risk
FR-1 High investments
FR-2 Unclear economic benefit
FR-3 Long and uncertain amortization
FR-4 Risk of false investments
FR-5 A decision in what to invest when
FR-6 Too late investments
FR-7 Risk of obsolescence of an investment in technology
Operational risks
OR-1 Inadequate qualification of employees
OR-2 Re-design of facility layout
OR-3 Shifts of competencies
OR-4 Internal resistance and corporate culture
OR-5 Lack of expertise
OR-6 Low awareness
OR-7 Fear of employees: I4.0 as a means of increasing surveillance of their work
OR-8 Maintenance
OR-9 Infrastructure shortcomings
OR-10 Operation method and tool-based risks
OR-11 Manufacturing process management-based risk
OR-12 Higher complexity
OR-13 Organizational risk
Technological risk
TR-1 Lacking standards/international standards differ
TR-2 IT-interface problems
TR-3 Infrastructure shortcomings/network congestions
TR-4 Availability of adequate IT Infrastructure
TR-5 Low degree of maturity of I4.0 technologies
TR-6 Technical complexity
TR-7 Technical integration
TR-8 Lack of decision logic
TR-9 Increased system maintenance/incompatibilities
TR-10 Availability of fast internet
TR-11 Communication between devices
TR-12 Lacking understanding of data-driven business models
TR-13 Retrofitting
TR-14 Awareness
TR-15 Increasing dependence on technology

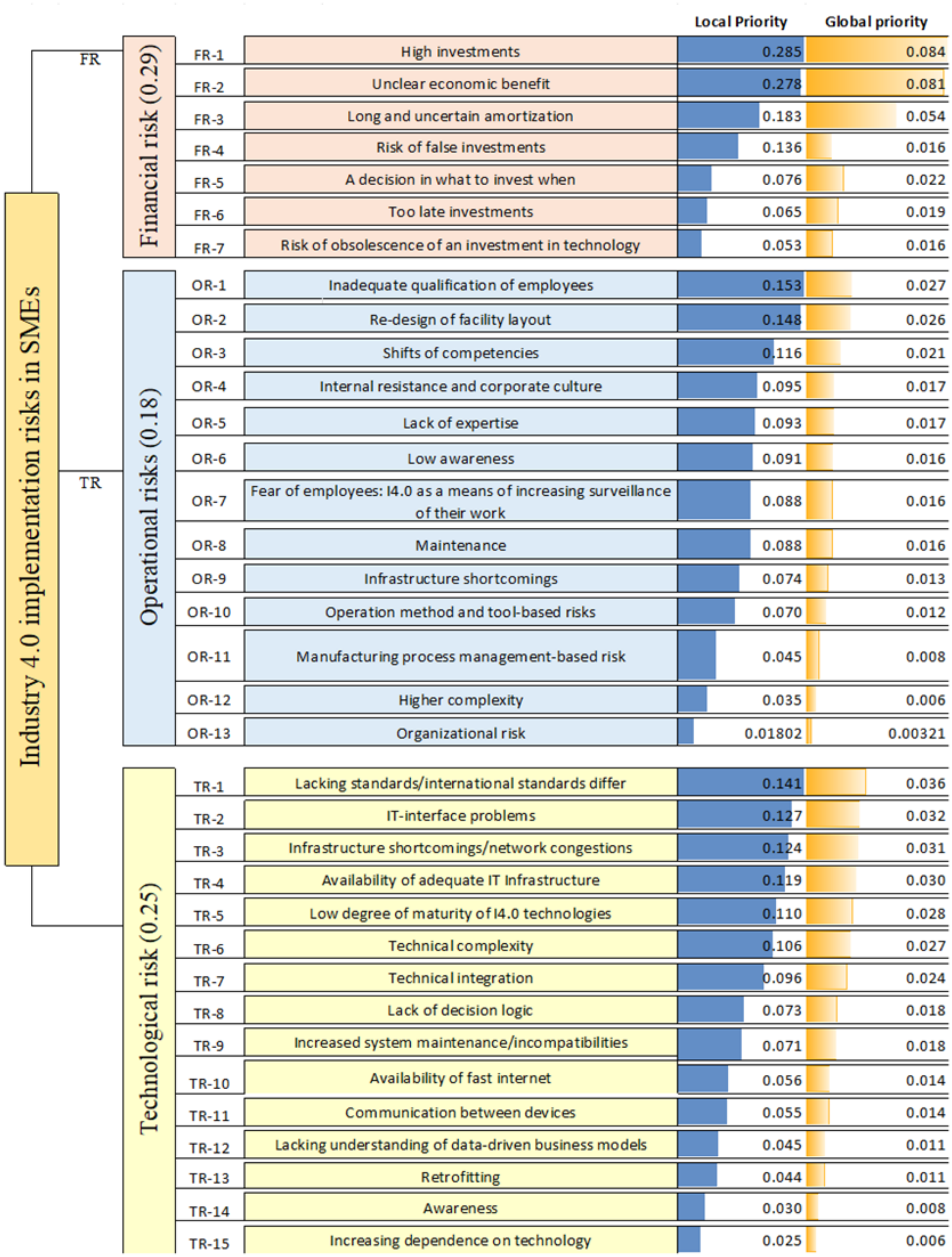
Figure.3 Hierarchy model to analyse the risks involved in implementing I4.0 at the SMEs of emerging countries.

4. EMPIRICAL RESULTS

Following the identification of the finalised risks, the Fuzzy AHP method is used to generate the hierarchy of risks in implementing I4.0. The extensive steps of the Fuzzy AHP analysis are detailed systematically in Appendix 1.

The final results of the Fuzzy AHP analysis are presented in Figure 4(a) and 4(b). The defuzzified scores of all the risks in Figures 4(a) and 4(b) suggest a hierarchy in the risks, with financial risks posing the most significant barriers to I4.0. Following this, technological, operational, business, supply chain, societal and environmental, and cybersecurity risks pose barriers to I4.0 implementation in this order. The estimated weights of each risk category in Figures 4(a) and 4(b) suggest that financial (0.29), technological (0.25), operational (0.18) and business risks (0.17) explain nearly 89% of the I4.0 implementation risks for Indian SMEs based on the opinions of the experts. The global priority columns in Figures 4(a) and 4(b) allow cross-comparison across the risk categories. The local priority columns provide the relative hierarchy within each risk category.

In the order of the established hierarchy of the risk categories, the local priority scores for each risk category are discussed in detail in the following. The results suggest that among financial risks, the "high investment" attained the highest priority (0.285) followed by "unclear economic benefits (0.278)", "long and uncertain amortisation (0.182)", "risk of false investments (0.136)", and "a decision on what to invest when (0.076)". The limited financial resources of India's SMEs and their inability to invest in new technologies are significant challenges for implementing I4.0. Furthermore, as I4.0 tools have unclear benefits or take a significant amount of time to deliver tangible benefits, Indian SMEs may be hesitant to invest in them.



			Local Priority	Global priority
Fiancial risk (0.29)	FR-1	High investments	0.285	0.084
	FR-2	Unclear economic benefit	0.278	0.081
	FR-3	Long and uncertain amortization	0.183	0.054
	FR-4	Risk of false investments	0.136	0.016
	FR-5	A decision in what to invest when	0.076	0.022
	FR-6	Too late investments	0.065	0.019
	FR-7	Risk of obsolescence of an investment in technology	0.053	0.016
Operational risks (0.18)	OR-1	Inadequate qualification of employees	0.153	0.027
	OR-2	Re-design of facility layout	0.148	0.026
	OR-3	Shifts of competencies	0.116	0.021
	OR-4	Internal resistance and corporate culture	0.095	0.017
	OR-5	Lack of expertise	0.093	0.017
	OR-6	Low awareness	0.091	0.016
	OR-7	Fear of employees: I4.0 as a means of increasing surveillance of their work	0.088	0.016
	OR-8	Maintenance	0.088	0.016
	OR-9	Infrastructure shortcomings	0.074	0.013
	OR-10	Operation method and tool-based risks	0.070	0.012
	OR-11	Manufacturing process management-based risk	0.045	0.008
	OR-12	Higher complexity	0.035	0.006
	OR-13	Organizational risk	0.01802	0.00321
Technological risk (0.25)	TR-1	Lacking standards/international standards differ	0.141	0.036
	TR-2	IT-interface problems	0.127	0.032
	TR-3	Infrastructure shortcomings/network congestions	0.124	0.031
	TR-4	Availability of adequate IT Infrastructure	0.119	0.030
	TR-5	Low degree of maturity of I4.0 technologies	0.110	0.028
	TR-6	Technical complexity	0.106	0.027
	TR-7	Technical integration	0.096	0.024
	TR-8	Lack of decision logic	0.073	0.018
	TR-9	Increased system maintenance/incompatibilities	0.071	0.018
	TR-10	Availability of fast internet	0.056	0.014
	TR-11	Communication between devices	0.055	0.014
	TR-12	Lacking understanding of data-driven business models	0.045	0.011
	TR-13	Retrofitting	0.044	0.011
	TR-14	Awareness	0.030	0.008
	TR-15	Increasing dependence on technology	0.025	0.006

Figure 4(a). Weights of risk categories and the local, global weights of risks within each category

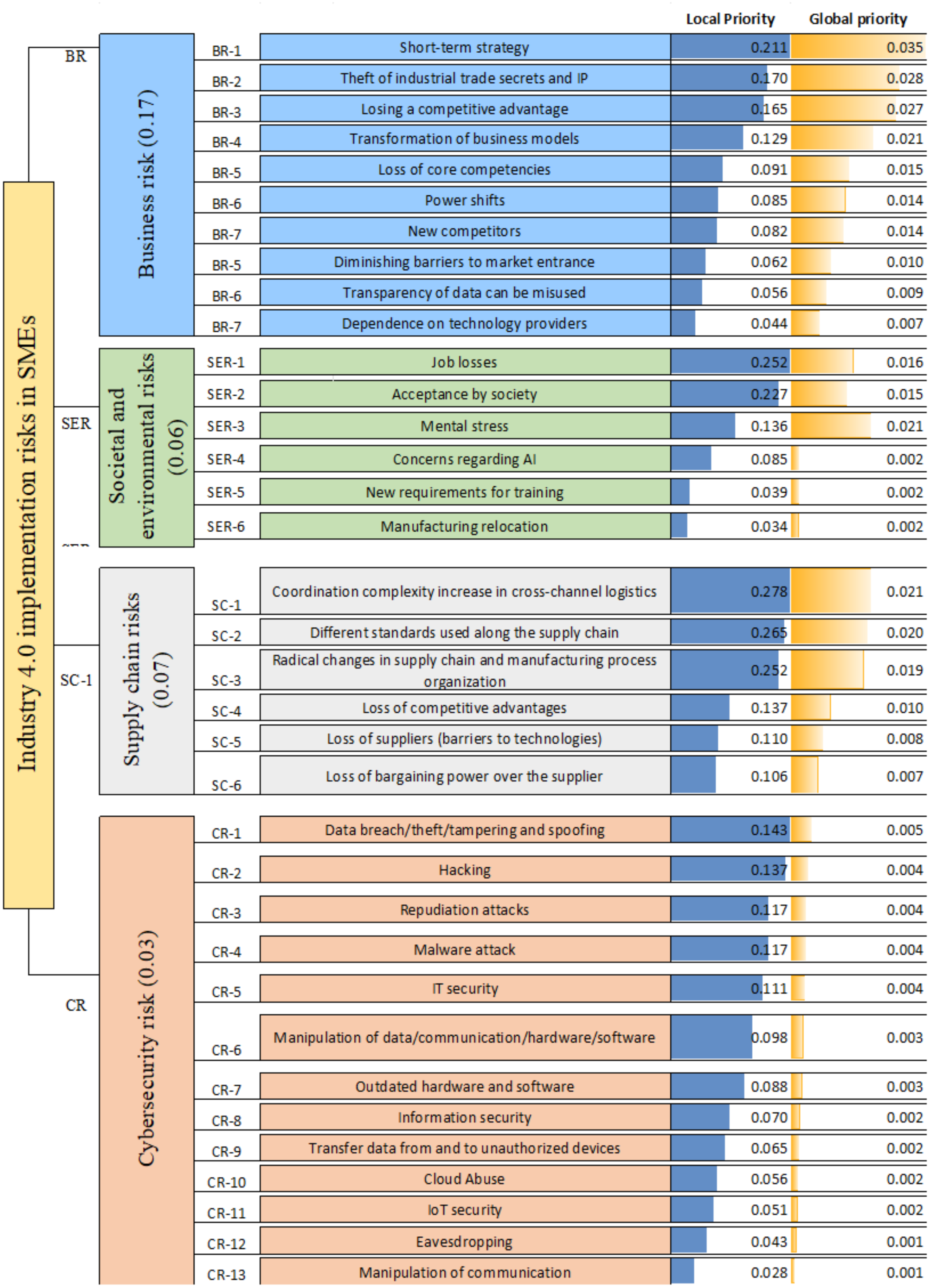


Figure 4(b). Weights of risk categories and the local, global weights of risks within each category

Several other developed country researchers have also focused on financial issues as a major obstacle to I4.0 implementation (Erol et al., 2016; Kiel et al., 2017; Müller and Voigt, 2018), which supports our findings in India.

Among technological risks, "lacking standards/international standards differ" attained the highest score (0.141), followed by IT-interface problems (0.127), availability of adequate IT Infrastructure (0.119), and low degree of maturity of I4.0 technologies (0.110). Furthermore, the expert's feedback in Figure.4 indicates the risks related to technical complexity in integrating digital technologies with traditional equipment (0.104), technical integration (0.096) coupled with "lack of decision logic (0.073) along with the "increased system maintenance/incompatibilities (0.071)". The lack of technology infrastructure, technology integration issues, and system maintenance/incompatibility problems hinder the adoption of new technologies by Indian SMEs. Notably, the maintenance of the latest technologies demands new equipment and higher employee competence (Tupa et al., 2017). This is indicated in the expert's feedback on the risks related to "maintenance (0.085)", "infrastructure shortcomings (0.074)", "operation method and tool-based risks (0.070)", and "manufacturing process management-based risk (0.045)".

Operational risks followed technological risks as the next most significant barriers. Among the operation risks, "inadequate qualification of employees" received the highest priority which is followed by the "redesign of facility layout (0.148)", "internal resistance and corporate culture (0.095)", “lack of expertise (0.093)”, and “low awareness (0.09)”. Thus, inadequate qualifications of the workforce, concerns arising from redesigning production facilities and organisational resistance are barriers to I4.0 implementation. These findings align with the view that managing organisational resistance and achieving cultural acceptance of innovations is generally a priority task during Industry 4.0 projects (Kiel et al., 2017).

Business risks followed operational risks as the next set of barriers. These include “short-term strategy (0.211)”, “theft of industrial trade secrets and intellectual property (0.170)”, “losing a competitive advantage (0.165)”, “transforming business models (0.129)”, and “loss of core competencies (0.091)”. When the organisation's critical data is in digital form, it can become prone to theft. SME's may not adequately invest in technology theft prevention leading to loss of important data to hackers. The possibility of compromising IPR increases leading to erosion of competitive advantage. These findings align with German SMEs' similar challenges when implementing I4.0 (Sommer, 2015).

Risks in the supply chain came next, with a mean score of 0.176. Among the supply chain risks, the coordination complexity increase in cross-channel logistics" seems to be of highest priority (0.278), followed by risks related to "different standards used along the supply chain (0.265)" and "radical changes in supply chain and manufacturing process organisation (0.252)". In challenges related to new technology, 'cybersecurity', which includes data breach/theft/tampering, repudiation attacks, malware attack, insider threats, and manipulation of information (Ben-Daya et al., 2019; Birkel et al., 2019), emerges as a significant risk. Notably, cybersecurity risks include data transfer from and to unauthorised devices. By using the IoT, a tremendous amount of data is generated. Once gathered, the organisation must convert it into meaningful information. This data is essential for organisational performance. However, if not stored appropriately, this data can be a threat to the organisation if leaked. Due to limited cyber security awareness, data captured across multiple processes is vulnerable to theft by both internal and external stakeholders.

Following this, societal and environmental risks have a mean score of 0.165. I4.0 is a paradigm shift in industrial evolution rooted in technological advances that can significantly alter the conditions of workforces. As a result, there may be a risk of technological unemployment in India in the long run, as many professions may disappear as new ones emerge. This is highlighted in the high score in the of "job losses (0.252)", "acceptance by society (0.227)", "mental stress (0.136)", and "concerns regarding artificial intelligence (0.085)". With a shifting job market, shifting roles in the workplace can be expected. There may be three ways businesses can deal with this: hire new workforces who master these skills; mechanise certain jobs, or reskill contemporary workforces. This is also evident by the score of 0.339 in the new training requirements in Figure.4(b). This is in line with research on developed countries suggesting that limited skilled workforce is a constraint for implementing I4.0 (Sanders et al. 2016; Tupa et al. 2017; Giotopoulos et al. 2017; Birkel et al. 2017; Müller and Voigt, 2018). We summarise these results into the following propositions in the context of emerging economy SMEs:

Proposition 1: SMEs face a hierarchy of risks in implementing I4.0.

Proposition 2: Financial barriers are the most significant barriers to the implementation of I4.0 for SMEs.

Proposition 3: Low degree of standardisation of I4.0 technologies poses challenges for integrating traditional equipment with digital technologies.

Proposition 4: Operations risks that reflect the need to redesign production lines for I4.0 and the availability of a qualified workforce constrain the implementation of I4.0.

Proposition 5: Unless the entire supply chain has a high degree of technical competence, SMEs face significant challenges in managing their logistics I4.0.

5. DISCUSSION AND CONCLUSION

Business leaders worldwide face challenges in preparing for potential risks related to digital transformation for business continuity. The Industry 4.0 movement is characterised by adopting advanced technologies to optimise manufacturing processes and create innovative business models continuously. Such optimisation relies on seamless, internet-supported integration of systems, which depends on compliance with commonly recognised standards and reference frameworks that facilitate compatibility among machines, interoperability in applications, and communication among systems.

For SMEs, in particular, employing digital technologies of I4.0 is associated with several risks. In this context, there is little discussion in the literature on the risks associated with adopting I4.0 technologies by SMEs in emerging economies. This paper addresses this compelling gap in the extant literature. It makes novel contributions by examining the risks associated with the implementation of I4.0 in Indian manufacturing.

The expert-based survey and analysis of findings by the AHP-Fuzzy approach established that financial, operational, business, technological, and social risks are the most significant risks for the employment of I4.0 in the background of its design principles, along with societal and cybersecurity risks. The literature review of I4.0-associated risks and the prioritisation of the critical risks from SMEs' point of view can become a solid basis for the digital transformation of SMEs. This empirical study aligns with the emerging need for more structured models for transitioning towards I4.0. This is one of the first empirical works to identify, validate and prioritise I4.0 implementation risks in an emerging economy SME context.

Contributions to Theory and Practice

I4.0 has gained the attention of academic scholars as well as industry practitioners. However, multiple perspectives have resulted in fragmented research landscapes in the context of I4.0 implementation. Extant research has mainly focused on large companies in developed countries, and there is a lack of literature on how risk prioritisation is performed in I4.0, particularly when it comes to SMEs in emerging economies. This paper contributes to the emerging literature on digitalisation by addressing the research gap noted above. Its novelty lies in an expert-based investigation that identifies, validates, and prioritises the risks associated with the implementation of I4.0 in SMEs in emerging economies, which will serve policymakers, manufacturers, and researchers as a ready reckoner. We introduced a novel empirical strategy of Fuzzy AHP to establish a hierarchy of risks involved in implementing I4.0 at the SMEs of India.

As per National Statistical Office's Second Advanced Estimates, India's real GDP is expected to grow by 8.9% in FY 2021-22, bouncing back from a contraction in FY 2020-21 and SMEs have a major role in this. Based on a survey of industry experts and business leaders associated with implementing I4.0 in the dynamically evolving economy of India, this paper identifies and prioritises the critical risks linked with the implementation of I4.0 in Indian SMEs.

This study outlines that SMEs which are contributing to nearly 40 % of industrial output in India face significant financial and technological challenges in adopting I4.0 technologies. The empirical results validate these risks and suggest that financial risks account for 29 % of the relative weighting out of risk types, followed by technological risks at 25 %, operational risks at 17 % and business risks at 16% suggesting that these risks account for nearly 89% of the total risks involved in the implementation of I4.0 by Indian SMEs.

Digitisation of the Indian economy and higher finance penetration will play a pivotal role in shaping the face of the industry in the years to come. The value chains of Indian SMEs are complex due to their relationships with multiple original equipment manufacturers. Converting them into interoperable, smart, and connected systems is a work in progress. Taking a careful look at the risks outlined here will make organisations more aware of the associated challenges and develop strategies to mitigate these risks.

Limitations and Directions of Future Research

The I4.0 implementation in SMEs is in the initial phase; henceforth, the sample of the research is moderately small, considering the novel nature of the work. Moreover, as the SMEs will implement the I4.0 technologies on a full scale, they will offer instantaneous and tangible data, and reflection, on the numerous risks they may face. The classification may need rearranging, and diverse relationships may appear, which might be an area of forthcoming investigation.

Future research can empirically establish the interdependencies between the risks identified in our work. I4.0 does not yet come under the umbrella of a professionally organised international body.

Consequently, experts have not organised an international group to create internationally recognised risk management models for I4.0. We require a globally accepted assessment tool for measuring the management of I4.0-associated risks for smart factories. It is also important to note that there is currently no globally accepted method for assessing the management of risks associated with I4.0 within smart factories. A tool for such an assessment is a desirable area for future research and policy development.

REFERENCES

Almada-Lobo, F. (2015). The Industry 4.0 revolution and the future of Manufacturing Execution Systems (MES). *Journal of innovation management*, *3*(4), 16-21.

Appio, F. P., Frattini, F., Petruzzelli, A. M., & Neirotti, P. (2021). Digital transformation and innovation management: A synthesis of existing research and an agenda for future studies. *Journal of Product Innovation Management*, *38*(1), 4-20.

Ardito, L., D'Adda, D., & Petruzzelli, A. M. (2018). Mapping innovation dynamics in the Internet of Things domain: Evidence from patent analysis. *Technological Forecasting and Social Change*, *136*, 317-330.

Ardito, L., Petruzzelli, A.M., Panniello, U. and Garavelli, AC (2019), "Towards Industry 4.0: Mapping digital technologies for supply chain management-marketing integration", *Business Process Management Journal*, 25,323-346

Avikal, S., Mishra, P.K. and Jain, R., 2014. A Fuzzy AHP and PROMETHEE method-based heuristic for disassembly line balancing problems. *International Journal of Production Research*, 52(5),1306-1317

Ben-Daya, M., Hassini, E., & Bahroun, Z. (2019). Internet of things and supply chain management: a literature review. *International Journal of Production Research*, 57(15-16), 4719-4742

Bolesnikov, M., Popović Stijačić, M., Radišić, M., Takači, A., Borocki, J., Bolesnikov, & Dzieńdziora, J. (2019). Development of a business model by introducing sustainable and tailor-made value proposition for SME clients. *Sustainability*, 11(4), 1157

Brettel, M., Friederichsen, N., Keller, M., & Rosenberg, M. (2014). How virtualisation, decentralisation and network building change the manufacturing landscape: An Industry 4.0 Perspective. *International Journal of Information and Communication Engineering*, 8(1), 37-44

Birkel, H. S., Veile, J. W., Müller, J. M., Hartmann, E., & Voigt, K. I. (2019). Development of a risk framework for Industry 4.0 in the context of sustainability for established manufacturers. *Sustainability*, 11(2), 384.

Ceipek, R., Hautz, J., Petruzzelli, A. M., De Massis, A., & Matzler, K. (2021). A motivation and ability perspective on engagement in emerging digital technologies: The case of Internet of Things solutions. *Long Range Planning*, 54(5), 101991

Cimini, C., Pinto, R., Pezzotta, G., & Gaiardelli, P. (2017, September). The transition towards industry 4.0: business opportunities and expected impacts for suppliers and manufacturers. In IFIP *International Conference on Advances in Production Management systems* (pp. 119-126). Springer, Cham.

Chen, G. and Pham, T.T., 2000. Introduction to fuzzy sets, fuzzy logic, and fuzzy control systems. CRC press

Coad, A. and Tamvada, J.P., 2012. Firm growth and barriers to growth among small firms i India. *Small Business Economics*, 39(2), 383-400

Correani, A., De Massis, A., Frattini, F., Petruzzelli, A. M., & Natalicchio, A. (2020). Implementing a digital strategy: Learning from the experience of three digital transformation projects. *California Management Review*, 62(4), 37-56

Decker, A. and Jørsfeldt, L.M., 2017. Digitally enabled platforms: Generating innovation and entrepreneurial opportunities for SMEs. In Motivating SMEs to Cooperate and Internationalise (pp. 93-111). Routledge

Decker, A., 2017. Industry 4.0 and SMEs in the Northern Jutland Region. In Value Creation in International Business (pp. 309-335). Palgrave Macmillan, Cham

Deng, H.,1999. Multicriteria analysis with the fuzzy pair-wise comparison. International Journal of Approximate Reasoning, 21, 215–231

D'Ippolito, B., Messeni Petruzzelli, A., Panniello, U. (2019). Archetypes of incumbents' strategic responses to digital innovation. Journal of Intellectual Capital, 20, 662-679

Dutta, G., Kumar, R., Sindhwani, R. and Singh, R.K. (2020), "Digital transformation priorities of India’s discrete manufacturing SMEs – a conceptual study in perspective of Industry 4.0", Competitiveness Review,30 (3), 289-314

Ertuğrul, İ., & Karakaşoğlu, N. (2009). Performance evaluation of Turkish cement firms with fuzzy analytic hierarchy process and TOPSIS methods. Expert Systems with Applications, 36(1), 702-715.

Ertuğrul, İ., & Karakaşoğlu, N. (2009). Performance evaluation of Turkish cement firms with fuzzy analytic hierarchy process and TOPSIS methods. Expert Systems with Applications, 36(1), 702-715

Fareri, S., Fantoni, G., Chiarello, F., Coli, E., & Binda, A. (2020). Estimating Industry 4.0 impact on job profiles and skills using text mining. Computers in industry, 118, 103222.

Ganzarain, J., & Errasti, N. (2016). Three stage maturity model in SME's toward industry 4.0. Journal of Industrial Engineering and Management (JIEM), 9(5), 1119-1128.

Ghanbari, A., Laya, A., Alonso-Zarate, J., & Markendahl, J. (2017). Business development in the Internet of Things: A matter of vertical cooperation. IEEE Communications Magazine, 55(2), 135–141

Ghobakhloo, M. (2018), "The future of manufacturing industry: a strategic roadmap toward Industry 4.0", Journal of Manufacturing Technology Management, 29 (6), 910-936.

Ghobakhloo, M. (2020). Industry 4.0, digitisation, and opportunities for sustainability. Journal of cleaner production, 252, 119869.

Giotopoulos, I., Kontolaimou, A., Korra, E., & Tsakanikas, A. (2017). What drives ICT adoption by SMEs? Evidence from a large-scale survey in Greece. Journal of Business Research, 81, 60-69.

Hamzeh, R., Zhong, R. and Xu, X.W., 2018. A survey study on industry 4.0 for New Zealand manufacturing. Procedia Manufacturing, 26, 49-57

Harputlugil, T.I.M.U.C.I.N., Prins, M.A.T.T.H.I.J.S., Gültekin, A.T. and Topçu, Y.I., 2011. Conceptual framework for potential implementations of multi-criteria decision making (MCDM) methods for design quality assessment

Hermann, T. Pentek and B. Otto, "Design Principles for Industrie 4.0 Scenarios (2015) 49th Hawaii International Conference on System Sciences (HICSS). 3928-393

Horváth, D., & Szabó, R. Z. (2019). Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities? Technological forecasting and social change, 146, 119-132.

Kamble, S. S., Gunasekaran, A., & Gawankar, S. A. (2018). Sustainable Industry 4.0 framework: A systematic literature review identifying the current trends and future perspectives. Process safety and environmental protection, 117, 408-425

Kovacs, O., 2018. The dark corners of industry 4.0–Grounding economic governance 2.0. Technology in Society, 55, pp.140-145.

Kahraman, C., Cebeci, U. and Ulukan, Z. (2003), "Multi-criteria supplier selection using fuzzy AHP", Logistics Information Management, Vol. 16 (6), 382-394.

Kiel, D., Müller, J.M. and Voigt, K.I. (2017), "Sustainable industrial value creation: benefits and challenges of industry 4.0", International Journal of Innovation Management, 21 (8), 1-34

Kiel, D, Veile., J.W., K., Müller, J.M. and Voigt, K.-I. (2020), "Lessons learned from Industry 4.0 implementation in the German manufacturing industry", Journal of Manufacturing Technology Management, 31 (5), 977-997

Kumar, A., Zavadskas, E.K., Mangla, S.K., Agrawal, V., Sharma, K. and Gupta, D., 2019. When risks need attention: adoption of green supply chain initiatives in the pharmaceutical industry. International Journal of Production Research, 57(11), pp.3554-3576.

Kumar, G., Bakshi, A., Khandelwal, A., Panchal, A., & Soni, U. (2022). Analysing Industry 4.0 Implementation

Barriers in Indian SMEs. Journal of Industrial Integration and Management, 7(01), 153-169.

Lasi, H., Fettke, P., Kemper, H. G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. Business & information systems engineering, 6(4), 239-242.

Lee, I. and Lee, K., 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440

Lee, J., Bagheri, B. and Jin, C., 2016. Introduction to cyber manufacturing. Manufacturing Letters, 8, 11-15.

Leos, S., J. Sopko, S. Bednar, and R. Poklemba., 2018. Concept of SME business model for Industry 4.0 environment. TEM Journal, 7(3), 626.

Li, L., 2018. China's manufacturing locus in 2025: With a comparison of "Made-in-China 2025" and "Industry 4.0". Technological Forecasting and Social Change, 135, 66-74.

Liao, Y., Deschamps, F., Loures, E. D. F. R., & Ramos, L. F. P. (2017). Past, present and future of Industry 4.0-a systematic literature review and research agenda proposal. International journal of production research, 55(12), 3609-3629

Mangla, S.K., Govindan, K. and Luthra, S., 2017. Prioritising the barriers to achieving sustainable consumption and production trends in supply chains using fuzzy Analytical Hierarchy Process. Journal of cleaner production, 151,509-525

Masood, T. and Sonntag, P., 2020. Industry 4.0: Adoption challenges and benefits for SMEs. Computers in Industry, 121, 103261.

Matt, D.T., Rauch, E. and Fraccaroli, D., 2016. Smart Factory für den Mittelstand. Zeitschrift für wirtschaftlichen Fabrikbetrieb, 111(12), 52-55.

Matt, D.T. and Rauch, E., 2020. SME 4.0: the role of small and medium-sized enterprises in the digital transformation. In Industry 4.0 for SMEs (pp. 3-36). Palgrave Macmillan. Cham

Mehta, Y., & Rajan, A.J. (2017). Manufacturing sectors in India: Outlook and challenges. Procedia Engineering, 174, 90-104.

Mittal, S., Khan, M.A., Romero, D. and Wuest, T., 2018. A critical review of smart manufacturing & Industry 4.0 maturity models: Implications for small and medium-sized enterprises (SMEs). Journal of manufacturing systems, 49, 194-214.

Moeuf, A., Lamouri, S., Pellerin, R., Tamayo-Giraldo, S., Tobon-Valencia, E. and Eburdy, R., 2020. Identification of critical success factors, risks and opportunities of Industry 4.0 in SMEs. International Journal of Production Research, 58(5),1384-1400.

Müller, J.M. and Voigt, K.I., 2018. Sustainable industrial value creation in SMEs: A comparison between industry 4.0 and made in China 2025. International Journal of Precision Engineering and Manufacturing-Green Technology, 5(5),659-670

Oesterreich, T. D., & Teuteberg, F. (2016). Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry. Computers in industry, 83, 121-139

Piccarozzi, M., Aquilani, B. and Gatti, C., 2018. Industry 4.0 in management studies: A systematic literature review. Sustainability, 10(10),3821.

Radzi, N.M., Shamsuddin, A. and Wahab, E., 2017. Enhancing the competitiveness of Malaysian SMEs through
technological capability: A perspective. The Social Sciences, 12(4), 719-724.

Raj, A., Dwivedi, G., Sharma, A., de Sousa Jabbour, A. B. L., & Rajak, S. (2020). Barriers to the adoption of industry 4.0 technologies in the manufacturing sector: An inter-country comparative perspective. International Journal of Production Economics, 224, 107546

Rauch, E., Dallasega, P., & Linder, C. (2018). Industry 4.0 as an enabler of proximity for construction supply chains: A systematic literature review. Computers in industry, 99, 205-225

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P. and Harnisch, M., 2015. Industry 4.0: The future of productivity and growth in manufacturing industries. Boston Consulting Group, 9(1), pp.54-89.

Saaty, T.L., 1980. The analytical hierarchy process: Planning, priority setting, resource allocation. McGraw-Hill International Book Co., London, England.

Sanders, A., Elangeswaran, C. and Wulfsberg, J.P., 2016. Industry 4.0 implies lean manufacturing: Research activities in industry 4.0 function as enablers for lean manufacturing. Journal of Industrial Engineering and Management (JIEM), 9(3), 811-833.

Sharma, S., Upadhyay, S., & Singh, B. (2019). Employment opportunities with promoting waste management in India. *Journal Clean WAS (JCleanWAS)*, *3*(1), 10-15.

Sommer, L. (2015). Industrial revolution-industry 4.0: Are German manufacturing SMEs the first victims of this revolution? Journal of Industrial Engineering and Management, 8(5), 1512-1532

Snieška, V., Navickas, V., Havierniková, K., Okręglicka, M., & Gajda, W. (2020). Technical, information and innovation risks of industry 4.0 in small and medium-sized enterprises–case of Slovakia and Poland. Journal of business economics and management, 21(5), 1269-1284

Srivastava, D. K., Kumar, V., Ekren, B. Y., Upadhyay, A., Tyagi, M., & Kumari, A. (2022). Adopting Industry 4.0 by leveraging organisational factors. Technological Forecasting and Social Change, 176, 121439

Stock, T., Obenaus, M., Kunz, S., & Kohl, H. (2018). Industry 4.0 as enabler for a sustainable development: A qualitative assessment of its ecological and social potential. Process Safety and Environmental Protection, 118, 254-267.

Tortorella, G.L., Vergara, A.M.C., Garza-Reyes, J.A. and Sawhney, R., 2020. Organisational learning paths based upon industry 4.0 adoption: An empirical study with Brazilian manufacturers. International Journal of Production Economics, 219,.284-294.

Tseng, M. L., Tan, R. R., Chiu, A. S., Chien, C. F., & Kuo, T. C. (2018). Circular economy meets industry 4.0: Can big data drive industrial symbiosis? Resources, conservation and recycling, 131, 146-147.

Tupa, J., Simota, J., & Steiner, F. (2017). Aspects of risk management implementation for Industry 4.0. Procedia Manufacturing, 11, 1223-1230.

Usai, A., Fiano, F., Petruzzelli, A. M., Paoloni, P., Briamonte, M. F., & Orlando, B. (2021). Unveiling the impact of the adoption of digital technologies on firms' innovation performance. Journal of Business Research, 133, 327-336

Van Laarhoven, P. J., & Pedrycz, W. (1983). A fuzzy extension of Saaty's priority theory. Fuzzy sets and Systems, 11(1-3), 229-241.

Yin, Y., Stecke, K. E., & Li, D. (2018). The evolution of production systems from Industry 2.0 through Industry 4.0. International Journal of Production Research, 56(1-2), 848-861.

Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: state of the art and future trends. International journal of production research, 56(8), 2941-2962

Yadav, G., Kumar, A., Luthra, S., Garza-Reyes, J. A., Kumar, V., & Batista, L. (2020). A framework to achieve sustainability in manufacturing organisations of developing economies using industry 4.0 technologies' enablers. Computers in industry, 122, 103280

Wang, Y.M., Luo, Y. and Hua, Z., 2008. On the extent analysis method for fuzzy AHP and its applications. European journal of operational research, 186(2).735-747

Wu, Y., Dai, H. N., & Wang, H. (2020). Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. IEEE Internet of Things Journal, 8(4), 2300-2317.

APPENDIX-1

The relative significance of each barrier is computed using the proposed methodology discussed in the previous section. Firstly, the finalised list of risks (in Figure 3) are shared with the experts and their crisp responses about the relative significance of risks under each category are collected using Satty scale. Based on these crisp responses, pairwise comparison of risk categories and the risks within each category are constructed as matrices. An example of which is given below for the aggregate risk categories based on the crisp responses of one of the experts.[6]

$$\mathrm{E}^{1}=\left(\begin{array}{cccccccc} & FR & OR & TR & BR & SER & SC & CS \\ FR & 1 & 5 & 4 & 5 & 6 & 6 & 6 \\ OR & 0.2 & 1 & 0.33 & 0.33 & 6 & 5 & 7 \\ TR & 0.25 & 3 & 1 & 5 & 6 & 6 & 7 \\ BR & 0.2 & 3 & 0.2 & 1 & 5 & 5 & 4 \\ SER & 0.17 & 0.16 & 0.16 & 0.2 & 1 & 0.2 & 5 \\ SC & 0.17 & 0.20 & 0.16 & 0.2 & 5 & 1 & 1 \\ CS & 0.17 & 0.14 & 0.14 & 0.25 & 0.2 & 1 & 1 \end{array}\right)$$

where FR= Financial risk; OR= Operational risks; TR= Technological risk; BR= Business risk; SER5= Societal and environmental risks; R6= Supply chain risks; CS= Cybersecurity risk.

Considering the crisp responses of the experts, fuzzified scores with an offset distance of 1 are used to create fuzzy responses.[7]

[6] The matrices of sub-risks within each individual risk category are provided in Appendix 1. Consistency ratio is evaluated for all the developed pairwise comparison matrices is noted that the magnitude is within 0.1 which is acceptable.

[7] The attributes of Table.2 are used in creating the fuzzified decision matrices.

A sample fuzzified matrix developed by considering the responses of each decision-maker for the sub-criteria "Societal and Environmental" risks shown in Table.3. The equivalent attributes of fuzzified score corresponding to all other matrices is further used to eventually compute defuzzified score.

In this appendix, pair-wise comparison of risks is shown by considering the sample response obtained from the expert panel

(a) The following is a pairwise comparison matrix for the risks falling under the category of financial risks

$$E^{1}=\left(\begin{array}{cccccccc} & FR1 & FR2 & FR3 & FR4 & FR5 & FR6 & FR7 \\ FR1 & 2 & 5 & 4 & 4 & 3 & 6 & 6 \\ FR2 & 0.2 & 1 & 5 & 5 & 0.2 & 4 & 4 \\ FR3 & 0.25 & 0.25 & 1 & 0.3 & 0.2 & 0.2 & 4 \\ FR4 & 0.25 & 0.2 & 3 & 1 & 0.2 & 0.2 & 0.2 \\ FR5 & 0.33 & 5 & 5 & 5 & 1 & 5 & 7 \\ FR6 & 0.16 & 0.25 & 5 & 5 & 0.2 & 1 & 2 \\ FR7 & 0.16 & 0.25 & 0.25 & 5 & 0.14 & 0.5 & 1 \end{array}\right)$$

where, FR1= High investments; FR2= Long and uncertain amortisation; FR3 = Too-late investments; FR4 = Risk of obsolescence of an investment in technology; FR5= Unclear economic benefit; FR6 = Risk of false investments; FR7= A decision in what to invest when.

(b) The following is the pair-wise comparison matrix of risks falling under the category of operational risks

$$\mathrm{E}^{1}=\left(\begin{array}{cccccccccccccc}
 & OR1 & OR2 & OR3 & OR4 & OR5 & OR6 & OR7 & OR8 & OR9 & OR10 & OR11 & OR12 & OR13 \\
OR1 & 1 & 4 & 0.33 & 0.2 & 0.2 & 2 & 0.33 & 4 & 4 & 0.2 & 0.33 & 4 & 0.33 \\
OR2 & 0.25 & 1 & 0.2 & 0.2 & 0.2 & 0.33 & 0.33 & 1 & 1 & 0.33 & 0.5 & 3.0 & 0.33 \\
OR3 & 3.0 & 5.0 & 1.0 & 0.33 & 0.33 & 0.33 & 0.33 & 0.33 & 5 & 3.0 & 0.33 & 3 & 3 \\
OR4 & 5.0 & 5.0 & 3.0 & 1 & 0.33 & 3.0 & 0.33 & 5 & 5 & 4.0 & 3.0 & 4 & 4 \\
OR5 & 5.0 & 5.0 & 3.0 & 3 & 1.0 & 4 & 3.0 & 4 & 4 & 3 & 4.0 & 3 & 3 \\
OR6 & 0.5 & 3.0 & 3.0 & 0.33 & 0.33 & 1 & 1.0 & 3 & 5 & 3 & 1.0 & 3 & 2 \\
OR7 & 3.0 & 3.0 & 3.0 & 3.0 & 0.33 & 1.0 & 1.0 & 4 & 4.5 & 3 & 0.33 & 3 & 4 \\
OR8 & 0.2 & 1.0 & 3.0 & 0.2 & 0.2 & 0.33 & 0.33 & 1 & 5 & 4 & 3.0 & 4 & 4 \\
OR9 & 0.25 & 1.0 & 0.2 & 0.2 & 0.25 & 0.2 & 0.2 & 0.2 & 1 & 4 & 4.0 & 3 & 5 \\
OR10 & 5.0 & 3.0 & 0.33 & 0.33 & 0.33 & 0.33 & 0.33 & 0.25 & 0.25 & 1 & 5.0 & 5 & 4 \\
OR11 & 3.0 & 2.0 & 3.0 & 0.33 & 0.33 & 1.0 & 3.0 & 0.33 & 0.25 & 0.2 & 1.0 & 5 & 6 \\
OR12 & 0.25 & 0.33 & 0.33 & 0.33 & 0.33 & 0.33 & 0.33 & 0.25 & 0.33 & 0.2 & 0.2 & 1 & 0.33 \\
OR13 & 3 & 3 & 0.33 & 0.2 & 0.33 & 0.5 & 0.2 & 0.2 & 0.2 & 0.2 & 0.2 & 3 & 1
\end{array}\right)$$

Where, OR1= Maintenance; OR2= Higher complexity; OR3= Low awareness; OR4= Redesign of facility layout; OR5 = Inadequate qualification of the employee; OR6 = Internal resistance and corporate culture; OR7= Shifts of competencies; OR8= Manufacturing process management-based risk; OR9= Operation method and tool-based risks; OR10= Infrastructure shortcomings; OR11= Lack of expertise; OR12= Organisational risk; OR13=

(c) The following is a pairwise comparison matrix for the risks falling under the category of technical risks.

E^{1} =

$$\left(\begin{array}{cccccccccccccccc}
 & TR1 & TR2 & TR3 & TR4 & TR5 & TR6 & TR7 & TR8 & TR9 & TR10 & TR11 & TR12 & TR13 & TR14 & TR15 \\
TR1 & 1 & 5 & 2 & 0.33 & 5 & 3 & 4 & 0.33 & 3 & 0.2 & 1 & 5 & 3 & 0.33 & 3 \\
TR2 & 0.2 & 1 & 3 & 3 & 5 & 5 & 0.33 & 3 & 0.33 & 2 & 4 & 3 & 2 & 0.2 & 3 \\
TR3 & 0.5 & 0.33 & 1.0 & 0.33 & 5 & 1 & 0.2 & 0.33 & 1 & 1 & 0.33 & 0.2 & 0.33 & 0.2 & 1 \\
TR4 & 3 & 0.33 & 3 & 1 & 5 & 3 & 1 & 5 & 5 & 1 & 5 & 5 & 5 & 1 & 3 \\
TR5 & 0.2 & 0.2 & 0.2 & 0.2 & 1.0 & 0.33 & 0.2 & 0.2 & 0.2 & 1 & 0.33 & 0.33 & 0.33 & 1 & 1 \\
TR6 & 0.3 & 0.2 & 1 & 0.33 & 3 & 1 & 5 & 3 & 5 & 5 & 5 & 5 & 3 & 1 & 1 \\
TR7 & 0.2 & 3 & 5 & 0.33 & 5 & 0.2 & 1 & 3 & 1 & 5 & 1 & 3 & 5 & 5 & 3 \\
TR8 & 3 & 0.33 & 3 & 0.2 & 5 & 0.33 & 0.33 & 1 & 5 & 3 & 5 & 5 & 5 & 5 & 1 \\
TR9 & 0.33 & 3 & 1 & 0.2 & 5 & 0.2 & 1 & 0.2 & 1 & 0.33 & 0.2 & 1 & 0.2 & 0.33 & 3 \\
TR10 & 5 & 0.5 & 1 & 1 & 1 & 0.2 & 0.2 & 0.33 & 3 & 1 & 3 & 3 & 2 & 0.33 & 1 \\
TR11 & 1 & 0.2 & 3 & 0.2 & 3 & 0.2 & 1 & 0.2 & 0.33 & 0.33 & 1 & 2 & 4 & 1 & 5 \\
TR12 & 0.2 & 0.33 & 5 & 0.2 & 3 & 0.33 & 0.33 & 0.2 & 0.33 & 0.33 & 0.5 & 1 & 4 & 0.33 & 2 \\
TR13 & 0.33 & 0.5 & 3 & 0.2 & 3 & 0.2 & 0.2 & 0.2 & 0.5 & 0.5 & 0.2 & 0.2 & 1 & 0.33 & 4 \\
TR14 & 3 & 5 & 5 & 1 & 1 & 0.2 & 0.2 & 0.2 & 3 & 1 & 1 & 3 & 3 & 1 & 3 \\
TR15 & 0.33 & 0.3 & 1 & 0.33 & 1 & 0.33 & 0.33 & 1 & 1 & 0.2 & 0.2 & 0.5 & 0.2 & 0.33 & 1
\end{array}\right)$$

TR1- Technical complexity; TR2- Low degree of maturity of I4.0 technologies; TR3- Technical integration; TR4- Lacking standards/international standards differ; TR5- Increasing dependence on technology; TR6- Retrofitting; TR7- IT-interface problems; TR8- Availability of fast internet;

TR9- Communication between devices; TR10- Lack of decision logic; TR11- Availability of adequate IT Infrastructure; TR12- Increased system maintenance/incompatibilities; TR13- Lacking understanding of data-driven business models; TR14- Infrastructure shortcomings/network congestions; TR15- Awareness and organisational structure

(d) The following is a pairwise comparison matrix for the risks falling under the category of business risks.

$$\text{E1=}\left(\begin{array}{ccccccccccc} & BR1 & BR2 & BR3 & BR4 & BR5 & BR6 & BR7 & BR8 & BR9 & B10 \\ BR1 & 1 & 4 & 4 & 4 & 5 & 5 & 4 & 4 & 4 & 4 \\ BR2 & 0.2 & 1 & 3 & 4 & 4 & 5 & 4 & 5 & 5 & 0.2 \\ BR3 & 0.2 & 0.33 & 1.0 & 4 & 3 & 4 & 0.33 & 0.2 & 3 & 0.33 \\ BR4 & 0.2 & 0.2 & 0.2 & 1 & 1 & 5 & 3 & 0.2 & 4 & 0.2 \\ BR5 & 0.2 & 0.2 & 0.33 & 1 & 1.0 & 3 & 0.2 & 0.2 & 3 & 0.33 \\ BR6 & 0.2 & 0.2 & 0.33 & 0.33 & 0.33 & 1 & 3 & 0.33 & 5 & 0.33 \\ BR7 & 0.2 & 0.2 & 3 & 0.33 & 5 & 0.33 & 1.0 & 0.33 & 4 & 0.33 \\ BR8 & 0.2 & 0.2 & 5 & 5 & 5 & 3 & 3 & 1 & 4 & 4 \\ BR9 & 0.2 & 0.2 & 0.33 & 0.2 & 0.33 & 0.2 & 0.2 & 0.2 & 1 & 5 \\ BR10 & 0.2 & 5 & 3 & 5 & 3 & 3 & 3 & 0.2 & 0.2 & 1 \end{array}\right)$$

BR1- Losing a competitive advantage; BR2- Transformation of business models; BR3- Loss of core competencies; BR4- Power shifts; BR5- Transparency of data can be misused; BR6- Diminishing barriers to the market entrance; BR7- New competitors; BR8- Theft of industrial trade secrets and intellectual property; BR9- Dependence on technology providers; BR10- Short-term strategy

(e) The following is a pairwise comparison matrix for the risks falling under the category of Societal and environmental risks

$$\text{E}^{1} = \left(\begin{array}{ccccccc} & SER1 & SER2 & SER3 & SER4 & SER5 & SER6 \\ SER1 & 1 & 4 & 5 & 5 & 5 & 5 \\ SER2 & 0.25 & 1 & 4 & 4 & 4 & 5 \\ SER3 & 0.2 & 0.25 & 1 & 5 & 5 & 5 \\ SER4 & 0.2 & 0.25 & 0.2 & 1 & 4 & 4 \\ SER5 & 0.2 & 0.25 & 0.2 & 0.25 & 1 & 4 \\ SER6 & 0.2 & 0.2 & 0.2 & 0.25 & 0.25 & 1 \end{array}\right)$$

SER1- Job losses; SER2- Acceptance by society; SER3- Mental stress; SER4- Concerns regarding AI; SER5- New requirements for training; SER6- Manufacturing relocation

(f) The following is a pairwise comparison matrix for the risks falling under the category of Supply chain risks

$$E^{1} = \begin{pmatrix} & SC1 & SC2 & SC3 & SC4 & SC5 & SC6 \\ SC1 & 1 & 0.2 & 0.2 & 0.33 & 0.33 & 0.33 \\ SC2 & 5 & 1 & 4 & 5 & 0.2 & 4 \\ SC3 & 5 & 0.25 & 1 & 5 & 4 & 5 \\ SC4 & 3 & 0.20 & 0.2 & 1 & 0.2 & 0.2 \\ SC5 & 3 & 5 & 0.25 & 5 & 1 & 4 \\ SC6 & 3 & 0.25 & 0.2 & 5 & 0.25 & 1 \end{pmatrix}$$

SC1- Loss of suppliers (barriers to technologies); SC2-Coordination complexity increases in cross-channel logistics; SC3- Radical changes in supply chain and manufacturing process organisation; SC4- Loss of bargaining power over the supplier; SC5- Different standards used along the supply chain; SC6- Loss of competitive advantages.

(g) The following is a pairwise comparison matrix for the risks falling under the category of Societal and environmental risks Cybersecurity risk

$$E^{1} = \begin{pmatrix} & CS1 & CS2 & CS3 & CS4 & CS5 & CS6 & CS7 & CS8 & CS9 & CS10 & CS11 & CS12 & CS13 \\ CS1 & 1 & 0.33 & 5 & 5 & 0.33 & 0.2 & 5 & 5 & 4 & 4 & 0.33 & 0.2 & 0.33 \\ CS2 & 3.0 & 1 & 5 & 3 & 4 & 1 & 2 & 4 & 2 & 3 & 3 & 5 & 3 \\ CS3 & 0.2 & 0.2 & 1.0 & 1 & 2 & 4 & 3 & 4 & 4 & 4 & 3 & 1 & 4 \\ CS4 & 0.2 & 0.33 & 1 & 1 & 1 & 5 & 4 & 5 & 4 & 5 & 4 & 3 & 4 \\ CS5 & 3.0 & 0.2 & 0.5 & 1 & 1.0 & 0.33 & 4 & 2 & 4 & 3 & 4.0 & 0.2 & 3 \\ CS6 & 5.0 & 1 & 0.25 & 0.2 & 3 & 1 & 3 & 3 & 3 & 3 & 1.0 & 3 & 5 \\ CS7 & 0.2 & 0.5 & 0.33 & 0.2 & 0.2 & 0.33 & 1.0 & 2 & 2 & 2 & 3 & 3 & 4 \\ CS8 & 0.2 & 0.2 & 0.2 & 0.2 & 0.5 & 0.33 & 0.5 & 1 & 0.33 & 4 & 0.33 & 0.33 & 3 \\ CS9 & 0.2 & 0.5 & 0.2 & 0.2 & 0.2 & 0.33 & 0.5 & 3 & 1 & 1 & 3 & 0.33 & 4 \\ CS10 & 0.2 & 0.33 & 0.2 & 0.33 & 0.33 & 0.33 & 0.33 & 0.2 & 1 & 1 & 3 & 3 & 3 \\ CS11 & 3.0 & 0.33 & 0.33 & 0.25 & 0.2 & 1.0 & 0.33 & 3 & 0.33 & 0.33 & 1.0 & 3 & 4 \\ CS12 & 5.0 & 0.2 & 1.0 & 0.33 & 5 & 0.33 & 0.33 & 3 & 3 & 0.33 & 0.33 & 1 & 4 \\ CS13 & 3 & 0.33 & 0.25 & 0.25 & 0.33 & 0.2 & 0.2 & 0.33 & 0.33 & 0.33 & 0.33 & 0.33 & 1 \end{pmatrix}$$

CS1- Transfer data from and to unauthorized devices; CS2- Data breach/theft/tampering and spoofing; CS3- IT security; CS4- IoT security; CS5- Manipulation of data; CS6- Repudiation attacks; CS7- Information security; CS8- Eavesdropping; CS9- Cloud Abuse; CS10- Malware attack; CS11- Hacking; CS12- Outdated hardware and software; CS13- Manipulation of communication.

The obtained crisp responses are fuzzified using the Saaty scale presented in Table.2 of the manuscript. A sample of the fuzzy pair-wise comparison matrix is shown below

Table.2(A) Fuzzified pair-wise comparison matrix of risk categories

Financial risk			Operational risks			Societal and environmental risks			…..	Supply chain risks			Cybersecurity risk		
a	b	c	a	b	c	a	b	c		a	b	c	a	b	c
1.00	1.00	2.00	4.00	5.00	6.00	5.00	6.00	7.00	…..	5.00	6.00	7.00	5.00	6.00	7.00
0.17	0.20	0.25	1.00	1.00	2.00	5.00	6.00	7.00	…..	4.00	5.00	6.00	6.00	7.00	8.00
0.20	0.25	0.33	2.00	3.00	4.00	5.00	6.00	7.00	……	5.00	6.00	7.00	6.00	7.00	8.00
0.17	0.20	0.25	2.00	3.00	4.00	4.00	5.00	6.00	……	4.00	5.00	6.00	3.00	4.00	5.00
0.14	0.17	0.20	0.14	0.17	0.20	1.00	1.00	2.00	……	0.17	0.20	0.25	4.00	5.00	6.00
0.14	0.17	0.20	0.17	0.20	0.25	4.00	5.00	6.00	……	1.00	1.00	2.00	1.00	1.00	2.00
0.14	0.17	0.20	0.13	0.14	0.17	0.17	0.20	0.25	……	1.00	1.00	2.00	1.00	1.00	2.00

Equivalent pair-wise comparison matrices are generated for all the risk categories but is not presented in view of space constraint. These fuzzy pair-wise comparison matrices are used to compute the fuzzy weight of each category and the risks within, using the philosophy of Fuzzy AHP. The computed weights of risk categories are shown below.

Table.2 (B). Fuzzy weight of risk categories.

Risk category	a	b	c
Financial risk	0.183423	0.28192	0.415179
Operational risks	0.113226	0.169721	0.251702
Technological risk	0.157608	0.24134	0.356362
Business risk	0.097377	0.157192	0.243918
Societal and environmental risks	0.039151	0.058955	0.094453
Supply chain risks	0.044973	0.066072	0.113136
Cybersecurity risk	0.01875	0.0248	0.053115

Similarly, the fuzzy weight of each risk within all the categories is evaluated using the framework of Fuzzy AHP. The evaluated attributes are further used to compute the defuzzified scores using Eq.4, presented in the manuscript. Table II(C) presents the sample weights of risk categories

Table 2 (C). Defuzzified weights of risk categories

Financial risk	0.29
Operational risks	0.17
Technological risk	0.25
Business risk	0.16
Societal and environmental risks	0.06
Supply chain risks	0.07
Cybersecurity risk	0.03