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

ABSTRACT

Manufacturing organizations worldwide are embracing Industry 4.0 (I4.0) and its associated technologies that include 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 prioritizes the critical risks linked with the implementation of I4.0 in SMEs. Empirical results using the Fuzzy-Analytical Hierarchy Process suggest a hierarchy in risks associated with SMEs' transition to I4.0, with financial and operational 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.

Keywords:

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

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 (Lee et al., 2014; Tseng et al., 2018). It leads engineering into a completely digitalized, networked, and decentralized value-creation system (Kiel et al., 2017). As in the case of social media, the exponential transformation resulting from it can impact all industry sectors (Li, 2018). 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).

I4.0 is more than a technology-focused transformation. Its real opportunity lies in unlocking digitalization's full potential, going beyond technologies, and harnessing its abilities to influence society (Tseng et al., 2018). I4.0 technologies improve organizations' productivity, quality, cost, delivery, environmental, and safety levels (Rüßmann et al., 2015). Notably, while it carries massive benefits, it also opens 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). In sharp contrast to this, 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). For instance, SMEs contribute to nearly 40 % of industrial output in India but face significant challenges in adopting these new technologies (Bhoganadam et al., 2017).

They contribute more than 50% of the total industrial output in Europe and China. Still, the implementation of I4.0 is relatively low, with more than half of German and Chinese SMEs reporting minimal adoption of digital technologies (Müller and Voigt, 2018).

As SMEs navigate through this new emergent paradigm, there is a compelling need for them to prepare for the potential disruptions posed by I4.0 (Mittal et al., 2018; Rauch et al., 2018; Bolesnikov et al., 2019). It appears that there is limited evidence available concerning the risks associated with deploying I4.0 initiatives in small and medium-sized businesses, although there has been a call for a thorough empirical analysis of such risks (Matt et al., 2016; Birkel et al., 2019). This paper aims to investigate the following question: What are the critical risks of implementing I4.0 that can impede its adoption by SMEs in an emerging economy?

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 prioritize 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. The third section 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. THEORETICAL BACKGROUND

Industry 4.0 is associated with transforming the manufacturing industries using hi-tech smart technologies (Rauch et al., 2018; Bolesnikov et al., 2019). By integrating the Industrial Internet of Things (IIoT) into its value creation process, Industry 4.0 enables real-time collaboration from within and outside the enterprise (Erol et al., 2016; Ghobakhloo, 2020). A crucial aspect of I4.0 is the usage of digital technologies such as cyber-physical systems (CPS) and 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; Ghobakhloo 2018, Leos et al., 2018). The emergence and adoption of these technologies can fundamentally alter how industries function (Erol et al., 2016; Rauch et al., 2018; Bolesnikov et al., 2019), 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 (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 optimizing the processes (Ghobakhloo, 2018; Leos, 2018; Tseng, 2018).

Firms need to use the six design principles of decentralization, virtualization, interoperability, real-time capability, modularity, and service orientation to leverage the benefits of the I4.0 technologies. (Hermann et al., 2015). The decentralization principle refers to the ability of CPS to decide autonomously and make manufacturing decisions locally (Almada-Lobo, 2015). The principle of virtualization 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 analyzing data in real-time (Ghobakhloo, 2020). The modularity principle refers to the ability to build a production line that is flexible, adaptable, and customizable 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, minimizing wastage, and developing into a sustainable organization (Müller and Voigt, 2018; Matt and Rauch, 2020).

An emerging body of literature examines the role of I4.0 for SMEs (Böllhofer et al., 2016; 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; Erol et al., 2016). Notwithstanding the benefits, SMEs are not sure if, when, and in what way they should start the transition to I4.0 (Sommer, 2015). A summary of the literature review of potential risks associated with Industry 4.0 is provided in Table 1.

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 amortization	
	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; Matt et al., 2018; Birkel et al., 2019
	Higher complexity	
	Low awareness	
	Industrial espionage	
	Re-design 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	
	Organizational 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., 2019; Snieška et al., 2020
	Low degree of maturity of I4.0 technologies	
	Technical integration	
	Lacking standards/international standards differ	
	Increasing dependence on technology	
	Retrofitting	
	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 organizational 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; Matt et al., 2018
	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)	Jayaram, 2016; 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 unauthorized devices	Brettel et al., 2014; Lasi et al., 2014; Sommer, 2015; Kiel et al., 2017; Müller et al., 2018; Ben-Daya et al., 2019; Birkel et al., 2019; Snieška et al., 2020
	Data breach/theft/tampering and spoofing	
	IT security	
	IoT security	
	Manipulation of data/communication/hardware/software	
	Repudiation attacks	
	Information security	
	Eavesdropping	
	Cloud Abuse	
	Malware attack	
	Hacking	
	Insider threats	
	Shadow IT Systems	
	Outdated hardware and software	
	Form jacking	
	Manipulation of communication	

Table 1: Summary of Industry 4.0 associated risks

As Table 1 suggests, several risks are associated with the implementation of I4.0 technologies. These include financial risks, operational risks, technological risks, business risks, societal and environmental risks, supply chain risks, and cybersecurity risks.

One of the key financial risks is that the deployment of I4.0 technologies requires large-scale investments, with an unknown payback period combined with uncertainty in success (Ghanbari et al., 2017; Kiel et al., 2017; Birkel et al., 2019). Many processes of operational value creation can be theoretically automated, digitized, and networked (Tupa et al., 20). Despite that, huge investments are required to build and implement this infrastructure, as well as to 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 that is required for I4.0 implementation (Birkel et al., 2019). In light of the rapid development of digital adoption and transformation, numerous organizations are struggling to find and equip their talent with the appropriate skills and knowledge (Matt et al., 2018; 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). In most enterprises, it is difficult to connect all the machines and employees on a factory floor 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 at the same time (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; Lezzi et al., 2019).

The business risks include difficulties in configuring advanced processes and digital technologies that are 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).

As a result of I4.0, businesses must rethink the way they design their supply chains. As well as adapting, such supply chains 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 identify potential risk areas proactively, or be able to respond more quickly (Brettel et al., 2014; Sanders et al., 2016). However, digitizing 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). This increased complexity can place an additional burden on managing dynamically evolving scenarios where human intervention can be more efficient.

There are multiple societal and environmental risks associated with the implementation of I4.0. This entails resistance to learning to use 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 result in numerous impacts on the jobs markets (Birkel et al., 2019). Despite gradual shifts towards automation, some sectors may still see rising unemployment. This can have a significant impact on broader society and multiple economic actors (Horváth and Szabó, 2019).

Manufacturing cyberattacks are increasing exponentially, and cybersecurity poses a significant risk for firms implementing I4.0. A wide range of 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 is 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 to meet the health and safety needs of their workforce, numerous manufacturers have adopted remote working practices, and all these have increased the risks associated with cybersecurity (Birkel et al., 2019). The majority of the risks identified above are associated with the implementation of I4.0 in large firms, while similar risks for small and medium-sized businesses (SMEs) have received little attention in the literature. There is a lack of a comprehensive evaluation of the risks of implementing I4.0 from the perspective of SMEs, especially those in emerging economies. SMEs in emerging economies have significantly more limitations in accessing capital, technology, and are more reliant on manual processes (Coad and Tamvada 2012), although they play a crucial role in the supply chains. Without adequate integration with the wider industrial context that is adopting I4.0, SMEs may face compelling challenges in survival, particularly in an environment marked by uncertainty. There is an imminent need for SMEs leaders to prepare for the coming digital era to prevent intellectual property loss, sabotage of manufacturing, and damages arising from downtime.

Thus, given the significance of digital technologies in the future of the industry, it is crucial to appreciate the fundamental challenges related to their implementation in SMEs. However, the lack of consensus on the I4.0 implementation risks, the disproportionate focus on large firms in the literature, the absence of guidance on the prioritization of risks, and the lack of sufficient evidence from emerging economies, are compelling gaps in the literature. These research gaps underscore the need to validate and prioritize critical risks in implementing I4.0 for SMEs in emerging economies. This paper will examine the risks of implementing I4.0 by SMEs in the context of an emerging economy to identify the risks that require the greatest attention from SME entrepreneurs and policymakers in emerging countries.

3. RESEARCH METHODOLOGY

This section presents the research methodology employed in this work to identify and prioritize the critical risk connected with the implementation of I4.0 in SMEs, as summarized in Figure 1.

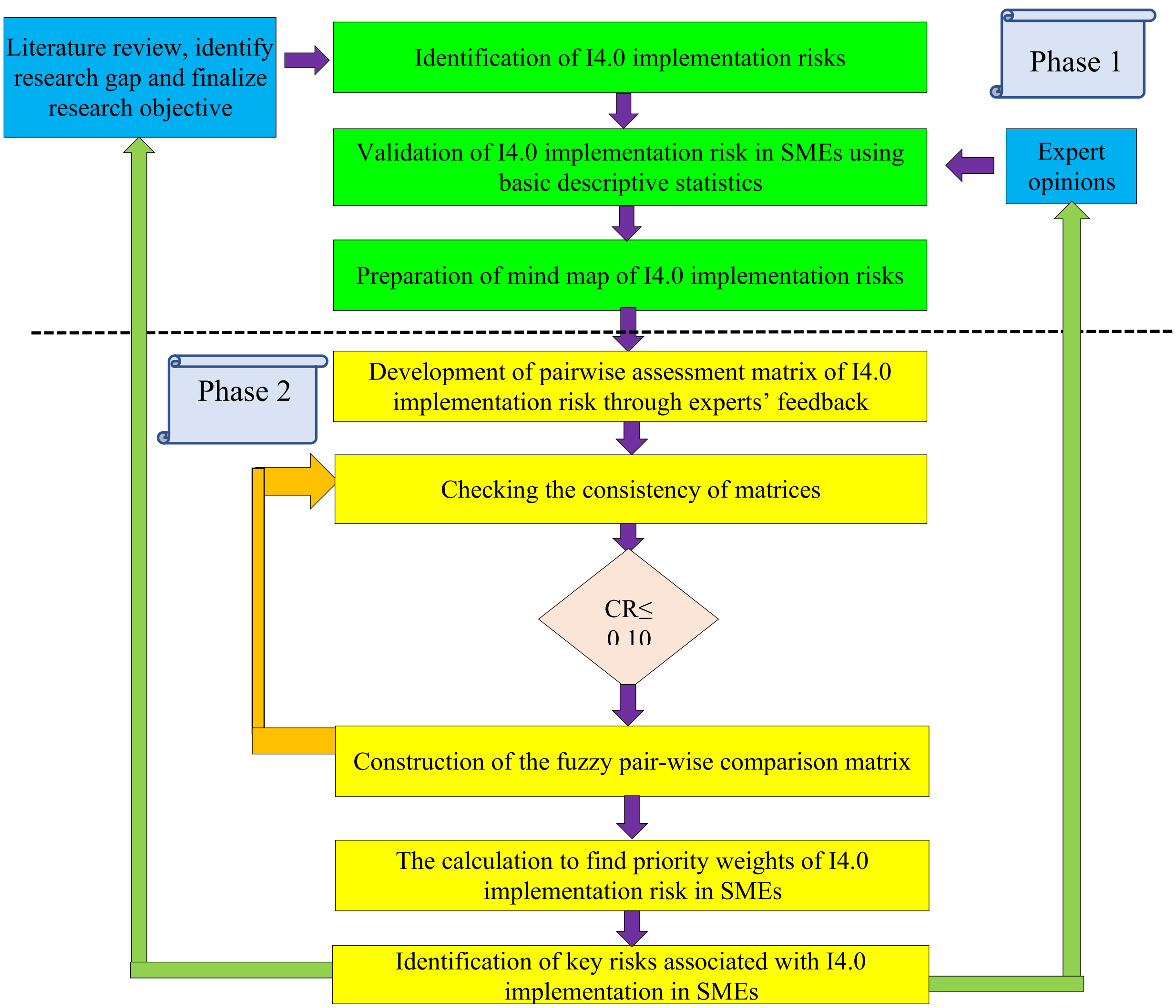

Figure 1: Research methodology

The broad steps include a comprehensive review of the extant literature on I4.0 implementation risk and a survey with industry leaders and policymakers for validation and prioritization of identified risks in the context of SMEs. We reviewed contemporary literature on I4.0 and its associated risk from the following databases: Scopus, Web of Science, Taylor & Francis, and Science direct. Initially, we identified a total of 794 papers from the databases; the breakup of papers from each database was as follows: (Scopus 215, Taylor and Francis 260, Scopus 212, and Science direct 210). From them, we shortlisted 64 papers as per the above-mentioned inclusion criteria.

The sample for this research involved 116 industry leaders from 46 SMEs in the electrical, electronics, casting, molding, 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: 1) the minimum requirement for the respondent was a bachelor 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 organization and 3) willingness to participate in the study throughout the research period.

During the first phase, experts were asked to rate the validity of I4.0 implementation risks identified in the literature review in Table 1 for their SMEs. This was measured on a Likert scale of 1 to 5 wherein 5 indicates very highly valid, 4 highly valid, 3 moderately valid, 2 slightly valid, and 1 signifies not valid. In the second phase, the Fuzzy analytical hierarchy process is used to determine the hierarchy of identified risks in SMEs. Experts were asked to rate their perception of the significance of I4.0 implementation challenges on the Satty scale of 1 to 9 through an online survey. Participants took on average nearly thirty minutes to fill out a survey. The internal consistency of the survey instrument was evaluated with Cronbach's alpha, which was observed > 0.8, indicating that the instrument is extremely reliable.

Numerous techniques are recommended in the literature for analyzing multi-criteria decision-making, such as AHP, analytical network process (ANP), multi-objective programming, and data envelopment analysis (Köne and Büke, 2007; Xiong et al., 2019). Of these techniques, AHP is a structured method for analyzing multifaceted decisions concerning both perception and judgments having long-term effects (Xi and Qin, 2013). AHP provides a structure for resolving various multi-criteria decision problems based on a comparative prioritization allocated to each 'criterion's role in achieving the stated objective (Satty 1980). Furthermore, the actual process of implementing AHP aids the decision-makers in prioritizing the criteria in a technique that otherwise may not be possible (Chen and Pham 2001; Kahraman et al., 2003). However, AHP works on crisp decisions to resolve ambiguity and may not emulate human thinking (Kahraman et al. 2003). To overcome these issues, the Fuzzy AHP technique makes a more reasonable evaluation of the weight of criteria (Van Laarhoven and Pedrcyz 1983) and can be extended to manage multi-criteria decision-making (Deng 1999). This method can manage uncertainty due to the subjective decisions of experts by applying a fuzzy set as a substitute for precise values (Chen and Pham, 2001). THE fuzzy AHP method is extensively used in numerous decision-making problems like the selection of suppliers (Tahriri et al., 2014), evaluating performance (Karakaşoğlu and Ertuğrul, 2009), sustainability in production (Mangla et al., 2017), line balancing (Avikal et al., 2014), and prioritization of risks (Kumar et al., 2019).

Kahraman et al. (2003) and Wang et al. (2008) suggest that using a fuzzy approach in making decisions can deal with the haziness of individual thought and ambiguity in decision making. It has been demonstrated in several studies that fuzzy numbers can be either triangular fuzzy numbers (TFNs) or trapezoidal fuzzy numbers (Kahraman et al., 2003; Wang et al., 2008). 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, 2009). Thus, the Fuzzy AHP method is used here, as it helps to make the multifaceted decision processes of prioritization of I4.0 implementation risks in SMEs by synthesizing all of the information about the decisions in a methodical manner. The results were subsequently verified by interviews with a subsample of the experts to ensure validation and robustness of the findings.

4. DATA ANALYSIS AND RESULTS

This section provides a summary of the analysis of experts' views about the validation and prioritization of the risks identified during the literature review (refer to Table 1) in the context of SMEs. Subsection 4.1 offers the validation of risks-sub-risks across different sectors, but the significance of each risk remains unevaluated. Subsection 4.2 offers the hierarchy of risks associated with SMEs' transition to I4.0 using the Fuzzy AHP.

4.1 Descriptive Analysis and Finalization of Risks

Table 2 (a) and (b) provide an overview of the mean score of experts' feedback on I4.0 implementation risks in the casting, molding, fabrication, electrical, forging, machining, and electronics industries. The feedback from experts indicates high mean risk, ranging from 3.8 to 4.8

in 70 risks out 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 consequently establishes that these risks are valid during the digital transformation of SMEs.

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

TABLE 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

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

4.2 Prioritization of I4.0 Implementation Risk in SMEs

The 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 ELECTREE (Harputlugil et al., 2011). 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, Bayesian AHP have come into existence (Van Laarhoven and Pedrycz, 1983; Mangla et al., 2017). Applications of Fuzzy AHP are extended to various domains. Studies of Avikal et al. (2014), Karakaşoğlu and Ertuğrul (2009), and Mangla et al. (2017) are a few of the examples. This section of the study employs Fuzzy AHP in order to assess the risks related to the adoption of I4.0 in SMEs.[1]

The steps involved in Fuzzy AHP are discussed below.

Step-1: Selection of the scale on which the responses are to be collected from the chosen decision-makers. Subsequently, the obtained responses are used to develop pairwise comparison matrices. In this study, the Satty scale, as shown in Table 3, was adopted to collect the responses for the developed questionnaire. The general representation of the criteria-criteria matrix is shown in Eq 1.

[1] Global weight aids the users to understand the relative significance of risks in the context of implementation risks in SMEs, while the local priority drawn in each risk type helps understand the relative dominance risks within the category. Appendix A1 outlines the steps involved in Fuzzy AHP. In Figures 2 (a) and 2 (b), we see that each risk gets a cumulative weighting.

'Saaty's crisp values (x)	Judgment definition	Fuzzified Saaty's value
1	Equal dominance	(1, 1, 1 + δ)
3	Week dominance	(3 – δ, 3, 3 + δ)
5	Strong dominance	(5 – δ, 5, 5 + δ)
7	Demonstrated dominance	(7 – δ, 7, 7 + δ)
9	Absolute dominance	(9 – δ, 9, 9)
2, 4, 6, 8	Intermediate values	(x – 1, x, x + 1), x = 2, 4, 6, 8

Table 3: Judgment scale adopted to obtain the responses

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

Where, R_{ij}= 1 for the diagonal members of the matrix, and R_{ij}= 1/R_{ji}. The rationale for this can be interpreted with the fact that the dominance of one risk over the other will be null.

It has to be noted that a similar exercise is performed in the micro-level categorization of the criteria. This results in a pairwise comparison matrix of risk categories and the pair-wise comparison matrices at the sub-risk level. The obtained pair-wise responses from one of the experts are shown in Eq. 2.

$$E^1 = \begin{pmatrix} & FR & OR & TR & BR & SER & SC & CS \\ FR & 1 & 5 & 4 & 5 & 6 & 6 & 6 \\ OR & 0.2 & 1 & 0.33 & 0.33 & 6 & 5 & 7 \\ TR & 0.25 & 3 & 1 & 5 & 6 & 6 & 7 \\ BR & 0.2 & 3 & 0.2 & 1 & 5 & 5 & 4 \\ SER & 0.17 & 0.16 & 0.16 & 0.2 & 1 & 0.2 & 5 \\ SC & 0.17 & 0.20 & 0.16 & 0.2 & 5 & 1 & 1 \\ CS & 0.17 & 0.14 & 0.14 & 0.25 & 0.2 & 1 & 1 \end{pmatrix} \quad (2)$$

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

Similarly, the obtained pairwise matrices from expert-1 for each of the categories is shown in Eq 3-9.

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

where, FR1= High investments; FR2= Long and uncertain amortization; 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.

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

Where, OR1= Maintenance; OR2= Higher complexity; OR3= Low awareness; OR4= Re-design 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= Organizational risk; OR13= Fear of employees I4.0 as a means of increasing surveillance of their work

$$
E^{1} = \begin{pmatrix} & SER1 & SER2 & SER3 & SER4 & SER5 & SER6 \\ SER1 & 1 & 4 & 5 & 5 & 5 & 5 \\ SER2 & 0.25 & 1 & 4 & 4 & 4 & 5 \\ SER3 & 0.2 & 0.25 & 1 & 5 & 5 & 5 \\ SER4 & 0.2 & 0.25 & 0.2 & 1 & 4 & 4 \\ SER5 & 0.2 & 0.25 & 0.2 & 0.25 & 1 & 4 \\ SER6 & 0.2 & 0.2 & 0.2 & 0.25 & 0.25 & 1 \end{pmatrix} \quad (5)
$$

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

$$
E^{1} = \begin{pmatrix} & SC1 & SC2 & SC3 & SC4 & SC5 & SC6 \\ SC1 & 1 & 0.2 & 0.2 & 0.33 & 0.33 & 0.33 \\ SC2 & 5 & 1 & 4 & 5 & 0.2 & 4 \\ SC3 & 5 & 0.25 & 1 & 5 & 4 & 5 \\ SC4 & 3 & 0.20 & 0.2 & 1 & 0.2 & 0.2 \\ SC5 & 3 & 5 & 0.25 & 5 & 1 & 4 \\ SC6 & 3 & 0.25 & 0.2 & 5 & 0.25 & 1 \end{pmatrix} \quad (6)
$$

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

$$
E^{1} = \begin{pmatrix} & CS1 & CS2 & CS3 & CS4 & CS5 & CS6 & CS7 & CS8 & CS9 & CS10 & CS11 & CS12 & CS13 \\ CS1 & 1 & 0.33 & 5 & 5 & 0.33 & 0.2 & 5 & 5 & 4 & 4 & 0.33 & 0.2 & 0.33 \\ CS2 & 3.0 & 1 & 5 & 3 & 4 & 1 & 2 & 4 & 2 & 3 & 3 & 5 & 3 \\ CS3 & 0.2 & 0.2 & 1.0 & 1 & 2 & 4 & 3 & 4 & 4 & 4 & 3 & 1 & 4 \\ CS4 & 0.2 & 0.33 & 1 & 1 & 1 & 5 & 4 & 5 & 4 & 5 & 4 & 3 & 4 \\ CS5 & 3.0 & 0.2 & 0.5 & 1 & 1.0 & 0.33 & 4 & 2 & 4 & 3 & 4.0 & 0.2 & 3 \\ CS6 & 5.0 & 1 & 0.25 & 0.2 & 3 & 1 & 3 & 3 & 3 & 3 & 1.0 & 3 & 5 \\ CS7 & 0.2 & 0.5 & 0.33 & 0.2 & 0.2 & 0.33 & 1.0 & 2 & 2 & 2 & 3 & 3 & 4 \\ CS8 & 0.2 & 0.2 & 0.2 & 0.2 & 0.5 & 0.33 & 0.5 & 1 & 0.33 & 4 & 0.33 & 0.33 & 3 \\ CS9 & 0.2 & 0.5 & 0.2 & 0.2 & 0.2 & 0.33 & 0.5 & 3 & 1 & 1 & 3 & 0.33 & 4 \\ CS10 & 0.2 & 0.33 & 0.2 & 0.33 & 0.33 & 0.33 & 0.33 & 0.2 & 1 & 1 & 3 & 3 & 3 \\ CS11 & 3.0 & 0.33 & 0.33 & 0.25 & 0.2 & 1.0 & 0.33 & 3 & 0.33 & 0.33 & 1.0 & 3 & 4 \\ CS12 & 5.0 & 0.2 & 1.0 & 0.33 & 5 & 0.33 & 0.33 & 3 & 3 & 0.33 & 0.33 & 1 & 4 \\ CS13 & 3 & 0.33 & 0.25 & 0.25 & 0.33 & 0.2 & 0.2 & 0.33 & 0.33 & 0.33 & 0.33 & 0.33 & 1 \end{pmatrix} \quad (7)
$$

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

E¹ = (8)

	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

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 organizational structure

E1= (9)

	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

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

Step-2: Considering the crisp responses obtained in step-1, the fuzzy pairwise assessment matrix is developed using the fuzzified Saaty values shown in Table 2. Triangular membership functions were adopted in this study to fuzzy the crips matrices. The general representation of the fuzzy weight can be shown as (a_l, b_l, c_l). The expression used for evaluating the range of ratings of experts is provided as Eq. 7.

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

$$a_{ij} = \min_K(a_{ijK}),\ b_{ij} = \frac{1}{K} * \sum_{k=1}^{K}(a_{ijk}), c_{ij} = \max_K(a_{ijK}) \qquad (7)$$

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

A sample fuzzified matrix developed by considering the responses of each decision-maker for the sub-criteria "Societal and environmental risks" is eluded below.

	SER1			SER2			SER3			SER4			SER 5			SER6		
	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
SER1	1.0	1.0	2.0	0.16	0.2	0.25	0.16	0.2	0.25	0.25	0.33	0.5	0.25	0.33	0.5	0.25	0.33	0.5
SER2	4.0	5.0	6.0	1.0	1.0	2.0	3.0	4.0	5.0	4.0	5.0	6.0	0.16	0.2	0.25	3.0	4.0	5.0
SER3	4.0	5.0	6.0	0.2	0.25	0.33	1.0	1.0	2.0	4.0	5.0	6.0	3.0	4.0	5.0	4.0	5.0	6.0
SER4	2.0	3.0	4.0	0.16	0.20	0.25	0.16	0.2	0.25	1.0	1.0	2.0	0.16	0.2	0.25	0.16	0.2	0.25
SER5	2.0	3.0	4.0	4.0	5.0	6.0	0.2	0.25	0.33	4.0	5.0	6.0	1.0	1.0	2.0	3.0	4.0	5.0
SER 6	2.0	3.0	4.0	0.2	0.25	0.33	0.16	0.2	0.25	4.0	5.0	6.0	0.2	0.25	0.33	1.0	1.0	2.0

Step-3: The equivalent weight of each risk is assessed using a fuzzy synthetic method, which can be articulated as Eq 8. The evaluated cumulative weight of each risk is shown in Figure 3 (a) and 3(b)

Let X={x_1, x_2, ...x_n} be the set of alternatives and C={c_1, c_2, c_3.......c_m} are the set of criteria. 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 i^{th} object for an m^{th} aim. The synthetic fuzzy value can be defined as

$$S_i = \sum_{j=1}^{m} M_{gi}^i \otimes \left[\sum_{i=1}^{n}\sum_{j=1}^{m} M_{gi}^j\right]^{-1}, i = 1, 2, \ldots \ldots . . N \qquad (8)$$

All w_i, *i=1, M,* are normalized fuzzy numbers with medium values equaling 1. ⊗ denotes fuzzy multiplication operation. It may have to be noted that the fuzzy extent can also be defined as the result of fuzzy arithmetic or by using the extension numbers, Let us consider two triangular fuzzy numbers, then, $M_1 = (a_1, b_1, c_1)$ *and* $M_2 = (a_2, b_2, c_2)$, then the operations are as follows:

$$(a1, b1, c1) \oplus (a2, b2, c2) = (a1 + a2, b1 + b2, c1 + c2)$$

$$(a1, b1, c1) \odot (a2, b2, c2) = (a1a2, b1b2, c1c2)$$

Step-3: The equivalent weight of each risk is assessed using a fuzzy synthetic method, which can be articulated as Eq. 9. The cumulative evaluated weight of each risk is shown in Figures 3 (a) and (b).

$$w_i = \sum_{j=1}^{N} P_{ij} \otimes \left[\sum_{k=1}^{N} \sum_{l=1}^{N} P_{ij}\right]^{-1}, i = 1, 2, \dots \dots . N \quad (9)$$

where w_i is a normalized fuzzy integer with medium numbers as unity, and i = 1...N (number of criteria).

Industry 4.0 implementation risks in SMEs

Risk and weight		Local rank		Local Priority	Global priority
FR: Financial risk (0.2935)	FR1	1	High investments	0.285	0.084
	FR5	2	Unclear economic benefit	0.278	0.081
	FR6	3	Long and uncertain amortization	0.183	0.054
	FR4	4	Risk of false investments	0.136	0.016
	FR7	5	A decision in what to invest when	0.076	0.022
	FR3	6	Too late investments	0.065	0.019
	FR4	7	Risk of obsolescence of an investment in technology	0.053	0.016
OR: Operational risks (0.1782)	OR5	1	Inadequate qualification of employees	0.153	0.027
	OR4	2	Re-design of facility layout	0.148	0.026
	OR7	3	Shifts of competencies	0.116	0.021
	OR6	4	Internal resistance and corporate culture	0.095	0.017
	OR11	5	Lack of expertise	0.093	0.017
	OR3	6	Low awareness	0.091	0.016
	OR13	1	Fear of employees: I4.0 as a means of increasing surveillance of their work	0.088	0.016
	OR1	2	Maintenance	0.088	0.016
	OR10	3	Infrastructure shortcomings	0.074	0.013
	OR9	4	Operation method and tool-based risks	0.070	0.012
	OR8	5	Manufacturing process management-based risk	0.045	0.008
	OR2	6	Higher complexity	0.035	0.006
	OR12	7	Organizational risk	0.01802	0.00321
TR: Technological risk (0.2512)	TR4	1	Lacking standards/international standards differ	0.141	0.036
	TR7	2	IT-interface problems	0.127	0.032
	TR14	3	Infrastructure shortcomings/network congestions	0.124	0.031
	TR8	4	Availability of adequate IT Infrastructure	0.119	0.030
	TR2	5	Low degree of maturity of I4.0 technologies	0.110	0.028
	TR1	6	Technical complexity	0.106	0.027
	TR3	7	Technical integration	0.096	0.024
	TR10	8	Lack of decision logic	0.073	0.018
	TR12	9	Increased system maintenance/incompatibilities	0.071	0.018
	TR8	10	Availability of fast internet	0.056	0.014
	TR9	11	Communication between devices	0.055	0.014
	TR13	12	Lacking understanding of data-driven business models	0.045	0.011
	TR6	13	Retrofitting	0.044	0.011
	TR15	14	Awareness and organizational structure	0.030	0.008
	TR12	15	Increasing dependence on technology	0.025	0.006

Figure 2(a): Global and the local scores of financial, operational risks, and technological risks

Industry 4.0 implementation risks in SMEs

Risk and weight	Code	Local rank	Risk	Local Priority	Global priority
BR – Business risk (0.1662)	BR10	1	Short-term strategy	0.211	0.035
	BR8	2	Theft of industrial trade secrets and IP	0.170	0.028
	BR1	3	Losing a competitive advantage	0.165	0.027
	BR2	4	Transformation of business models	0.129	0.021
	BR3	5	Loss of core competencies	0.091	0.015
	BR4	6	Power shifts	0.085	0.014
	BR7	7	New competitors	0.082	0.014
	BR6	8	Diminishing barriers to market entrance	0.062	0.010
	BR5	9	Transparency of data can be misused	0.056	0.009
	BR9	10	Dependence on technology providers	0.044	0.007
SER – Societal and environmental risks (0.0642)	SER-1	1	Job losses	0.252	0.016
	SER-2	2	Acceptance by society	0.227	0.015
	SER-3	3	Mental stress	0.136	0.021
	SER-4	4	Concerns regarding AI	0.085	0.002
	SER-5	5	New requirements for training	0.039	0.002
	SER-6	6	Manufacturing relocation	0.034	0.002
SC – Supply chain risks (0.0747)	SC2	1	Coordination complexity increase in cross-channel logistics	0.278	0.021
	SC5	2	Different standards used along the supply chain	0.265	0.020
	SC3	3	Radical changes in supply chain and manufacturing process organization	0.252	0.019
	SC6	4	Loss of competitive advantages	0.137	0.010
	SC1	5	Loss of suppliers (barriers to technologies)	0.110	0.008
	SC4	6	Loss of bargaining power over the supplier	0.106	0.007
CS – Cybersecurity risk (0.032)	CS2	1	Data breach/theft/tampering and spoofing	0.143	0.005
	CS11	2	Hacking	0.137	0.004
	CS6	3	Repudiation attacks	0.117	0.004
	CS10	4	Malware attack	0.117	0.004
	CS3	5	IT security	0.111	0.004
	CS5	6	Manipulation of data/communication/hardware/software	0.098	0.003
	CS12	7	Outdated hardware and software	0.088	0.003
	CS7	8	Information security	0.070	0.002
	CS1	9	Transfer data from and to unauthorized devices	0.065	0.002
	CS9	10	Cloud Abuse	0.056	0.002
	CS4	11	IoT security	0.051	0.002
	CS8	12	Eavesdropping	0.043	0.001
	CS13	13	Manipulation of communication	0.028	0.001

Figure 2(b): Global and the local score of Financial risks, operational risks, and technological risks

Step 4: In this phase of analysis, the local and global hierarchy of each sub-risk based on the cumulative score evaluated, is obtained, which helps in the understanding interpretation of each identified risk.

The defuzzified score of each risk in Figures 2 (a) and 2 (b) recognizes that among all the risks related to the changeover of SMEs to I4.0, financial, operational, business, technical, and social risks are the most significant. As per the experts' feedback, financial risks seem to have the highest impact considering its high score (0.29).

Among the financial risks, the “high investment” attained the highest priority (0.285) followed by “unclear economic benefits (0.278)”, “long and uncertain amortization (0.182)”, “risk of false investments (0.136)”, “a decision on what to invest when (0.076)” in the last order. Herein, it is significant to note that execution of any new-fangled technology requires huge investments; importantly, there may not be any clear-cut timeframe within which returns on the investment could be expected (Ghanbari et al., 2017), and the same is indicated with the high score corresponding to high investments, unclear economic benefits in Figure2 (a).

This is likely to pose concerns in SMEs about new investments, particularly because the tools of I4.0 take some time to show tangible benefits. Furthermore, most of the benefits, such as effective analytics and transparency may not necessarily give clear paybacks in the short term (Birkel et al., 2019). For SMEs, finance is the backbone for their survival. Thus, the dilemma that the SMEs face is that they are not sure if and when, and in what way they should initiate the transition to I4.0 due to unclear economic benefits, as indicated by the high score (0.278) in Figure 2 (a).

Operational risks followed financial risks with a high mean score of 0.178, 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)”, "low awareness (0.09) and “fear of employees. The tools of I4.0 are technically complex, and SMEs have relatively less competency in learning and understanding these technologies (Giotopoulos et al., 2017; Hariharasudan and Kot 2018). This can also be because SMEs are generally not comfortable investing in an expensive workforce, which may be technologically competent but functionally not as flexible as they are used to (Radzi et al., 2017). Importantly, the maintenance of the latest technologies demands new equipment and higher competence in employees (Tupa et al., 2017). The same 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)". The relatively lower score of the infrastructure, maintenance, and process-based risks, in comparison to the soft aspects like awareness and skill, determines the importance of improving the competency of SMEs on the I4.0 implementing technologies.

Following this, we have technological risks, with a mean score of 0.25. 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 2 (a) and 2 (b) 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)". These can also be due to the low degree of maturity for newer technologies and low awareness (Tupa et al., 2017; Hirman et al., 2019). SMEs do not have adequate infrastructure and resources to understand and implement new technologies (Radzi et al., 2017).

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, the risks of cybersecurity include data transfer from and to unauthorized devices. With using the IoT, a huge amount of data is generated. Once gathered, the organization must convert it into meaningful information. This data is essential for organizational performance. However, this data, if not stored appropriately, can be a threat to the organization if leaked.

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 risk related to "different standards used along the supply chain (0.265) and radical changes in supply chain and manufacturing process organization (0.252)". In line with the findings of previous scholars (Jayaram, 2016; Yin et al., 2018), these findings have also been supported by the literature. Thus, SMEs need to ensure that they are well-coordinated regarding their logistical activities across different channels. This becomes difficult due to the usage of different standards across the value chain (Lasi et al., 2014). The strength of SMEs lies in their low cost and quick management of change. However, the process of adopting newer technologies would make their operation expensive and time-consuming. This, in turn, would increase operating costs, resulting thereby in a loss of competitive advantage, which in turn, would be a threat to their survival. The same was also validated from the score of 0.137 evaluated from the experts' feedback in Figure 2 (b).

Following this, business risks have a cumulative score of 0.166. 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). These findings are also in line with the observations of preceding scholars (Lasi et al., 2014; Sommer, 2015; Birkel et al., 2019). Furthermore, societal and environmental risks came next, with 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 for workforces. At the same time, there is a potential risk that numerous professions may disappear while new occupations are created. Thus, there may be a risk for technological unemployment in the long term. This is highlighted in the high score of job losses (0.252), its 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 for businesses to deal with this: hire new workforces who master these skills; mechanize certain jobs, or reskill contemporary workforces. This is also evident by the score of 0.339 in the new training requirements in Figure 2 (b).

Any new technology brings with it a new set of challenges. When critical data of an organization is in a digital form, it can become prone to theft. SMEs generally do not spend on technology for theft prevention, which often results in the loss of important data to hackers. Herein, the possibility of compromising data breach/theft/tampering, hacking, repudiation attacks, malware attack, and manipulation of data/communication/hardware/software increases, which is also indicated in the expert's feedback in Figure 3 (b). While implementing newer technologies, the fear of losing their traditional customer base increases as their customers are only interested in low-cost products without any worry about technological improvements at the supplier end. In parallel with the growth of smart factories across the global footprint of companies, cyber security risks are likely to increase. However, in the research, the authors have found that cyber security risk poses a low concern to SMEs given its low score of 0.064. This can be due to low awareness about cyber security among SMEs.

5. DISCUSSION AND CONCLUSIONS

Business leaders worldwide face challenges in preparing for potential risks related to digital transformation for business continuity. SMEs, in particular, will have to endure in a competitive digital business landscape in the future. However, employing digital technologies increases the risks. In this context, there is little discussion in the literature about the risks associated with the adoption of Industry 4.0 technologies by SMEs. This paper addresses this gap and contributes to the extant literature by emphasizing the risks associated with the implementation of Industry 4.0 in manufacturing across various subsectors of an emerging economy. The study is one of the first to identify and empirically validate the importance of I4.0 implementation risks within small and medium-sized manufacturing industries.

SMEs across the globe are embarking on journeys to become smart factories. The value chains of SMEs are complex given their relationships with multiple original equipment manufacturers. The process of converting them into interoperable, smart, and connected systems is a work in progress worldwide. The proposed conceptual model and prioritizing the risks can be useful to SMEs and universities in recognizing the significant risks associated with I4.0. According to this study, financial risks account for 29 % of the relative weighting out of risk types, followed by technological risks at 25 % and operational risks at 17 %. Investments with unclear future economic benefits and risks of false investments present high financial risks.

Additionally, only 17 percent (12/70) of the cumulative sub-risks are very crucial among the analyzed risks. The reasons for this include high investment, insufficient employee qualification, re-designing of facilities, lack of standards, IT interface problems, infrastructure deficiencies, short-term strategy, theft of industrial trade secrets, job losses, acceptance by society, coordination complexity in cross-channel logistics, and different standards along supply chains. Companies that are aware of these risks are likely to transform into organizations that are constantly innovating in products, services, processes, systems, and business models. As India's SME adoption of I4.0 is still at its earliest stages, the sample size of this study is fairly small. Furthermore, as SMEs implement I4.0 technologies at a much larger scale, they will be able to offer instantaneous and tangible data. In addition, they will be able to reflect on the risks they face. Future research can examine the interdependence among the risks identified here. 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

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), pp.1306-1317.

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

Bakkari, M. and Khatory, A., 2017, April. Industry 4.0: Strategy for more sustainable industrial development in SMEs. In Proceedings of the IEOM 7th International Conference on Industrial Engineering and Operations Management, Rabat, Morocco (pp. 11-13).

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

Bhoganadam, S., Rao, N. and Dasaraju, S., 2017. A study on Issues and Challenges faced by SMEs: A Literature Review. Research Journal of SRNMC, 1, pp.48-56.

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

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

Bollhöfer, E., Buschak, D. and Moll, C., 2016. Dienstleistungsbasierte Geschäftsmodelle für Industrie 4.0–aktueller Stand und Potenziale für KMU. In Multikonferenz Wirtschaftsinformatik (pp. 1287-1298).

Brettel, M., Friederichsen, N., Keller, M. and Rosenberg, M., 2017. How virtualization, decentralization and network building change the manufacturing landscape: an industry 4.0 perspective. FormaMente, 12.

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 in India. Small Business Economics, 39(2), pp.383-400.

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.

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

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

Erol, S., Jäger, A., Hold, P., Ott, K. and Sihn, W., 2016. Tangible Industry 4.0: a scenario-based approach to learning for the future of production. Procedia CiRp, 54, pp.13-18.

Ertuğrul, İ. and Karakaşoğlu, N., 2008. Comparison of fuzzy AHP and fuzzy TOPSIS methods for facility location selection. The International Journal of Advanced Manufacturing Technology, 39(7-8), pp.783-795.

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

Ganzarain Epelde, J. and Errasti Lozares, N., 2016. Three stage maturity model in SME's towards Industry 4.0.

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

Ghobakhloo, M., 2018. The future of manufacturing industry: a strategic roadmap toward Industry 4.0. Journal of Manufacturing Technology Management.

Ghobakhloo, M., 2020. Industry 4.0, digitization, and opportunities for sustainability. Journal of cleaner production, 252, p.119869.

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

Goerzig, D. and Bauernhansl, T., 2018. Enterprise architectures for the digital transformation in small and medium-sized enterprises. Procedia Cirp, 67, pp.540-545.

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

Hariharasudan, A. and Kot, S., 2018. A scoping review on Digital English and Education 4.0 for Industry 4.0. Social sciences, 7(11), p.227.

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, M., Pentek, T. and Otto, B., 2016, January. Design principles for industrie 4.0 scenarios. In 2016 49th Hawaii international conference on system sciences (HICSS) (pp. 3928-3937). IEEE.

Hirman, M., Benesova, A., Steiner, F. and Tupa, J., 2019. Project management during the Industry 4.0 implementation with risk factor analysis. Procedia Manufacturing, 38, pp.1181-1188.

Hofmann, E. and Rüsch, M., 2017. Industry 4.0 and the current status as well as future prospects on logistics. Computers in industry, 89, pp.23-34.

Horváth, D. and 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, pp.119-132.

Jayaram, A., 2016, December. Lean six sigma approach for global supply chain management using industry 4.0 and IIoT. In 2016 2nd international conference on contemporary computing and informatics (IC3I) (pp. 89-94). IEEE.

Jones, M., Zarzycki, L. and Murray, G., 2018, January. Does industry 4.0 pose a challenge for the sme machine builder? A case study and reflection of readiness for a uk sme. In International Precision Assembly Seminar (pp. 183-197). Springer, Cham.

Kahraman, C., Cebeci, U. and Ulukan, Z., 2003. Multi-criteria supplier selection using fuzzy AHP. Logistics information management.

Khanzode, A.G., Sarma, P.R., Mangla, S.K. and Yuan, H., 2021. Modeling the Industry 4.0 adoption for sustainable production in Micro, Small & Medium Enterprises. Journal of Cleaner Production, 279, p.123489.

Kiel, D., Müller, J.M., Arnold, C. and Voigt, K.I., 2020. Sustainable industrial value creation: Benefits and challenges of industry 4.0. In Digital Disruptive Innovation (pp. 231-270).

Köne, A.Ç. and Büke, T., 2007. An Analytical Network Process (ANP) evaluation of alternative fuels for electricity generation in Turkey. Energy policy, 35(10), pp.5220-5228.

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

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.

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

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

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

Lee, J., Bagheri, B. and Kao, H.A., 2015. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing letters, 3, pp.18-23.

Lee, J., Kao, H.A. and Yang, S., 2014. Service innovation and smart analytics for industry 4.0 and big data environment. Procedia Cirp, 16, pp.3-8.

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. https://doi.org/10.18421/TEM73-20

Lezzi, M., Lazoi, M. and Corallo, A., 2018. Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, 103, pp.97-110.

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, pp.66-74.

Li, X., Li, D., Wan, J., Vasilakos, A.V., Lai, C.F. and Wang, S., 2017. A review of industrial wireless networks in the context of industry 4.0. Wireless networks, 23(1), pp.23-41.

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

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

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

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.

Matt, D.T., Rauch, E. and Fraccaroli, D., 2016. Smart Factory für den Mittelstand. Zeitschrift für wirtschaftlichen Fabrikbetrieb, 111(1-2), pp.52-55.

Brunet-Thornton, R. and Martinez, F. eds., 2018. Analyzing the impacts of industry 4.0 in modern business environments. IGI Global.

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, pp.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), pp.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), pp.659-670.

Müller, J.M., Kiel, D. and Voigt, K.I., 2018. What drives the implementation of Industry 4.0? The role of opportunities and challenges in the context of sustainability. Sustainability, 10(1), p.247.

Oesterreich, T.D. and 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, pp.121-139.

Piccarozzi, M., Aquilani, B. and Gatti, C., 2018. Industry 4.0 in management studies: A systematic literature review. Sustainability, 10(10), p.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), pp.719-724.

Rauch, E., Dallasega, P. and Matt, D.T., 2017. Critical factors for introducing lean product development to small and medium sized enterprises in Italy. Procedia Cirp, 60, pp.362-367.

Rauch, E., Spena, P.R. and Matt, D.T., 2019. Axiomatic design guidelines for the design of flexible and agile manufacturing and assembly systems for SMEs. International Journal on Interactive Design and Manufacturing (IJIDeM), 13(1), pp.1-22.

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.

Sahal, R., Breslin, J.G. and Ali, M.I., 2020. Big data and stream processing platforms for Industry 4.0 requirements mapping for a predictive maintenance use case. Journal of Manufacturing Systems, 54, pp.138-151.

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), pp.811-833.

Santy, T.L., 1980. The analytical hierarchy process: Planning, priority setting, resource allocation. McGrawrHill International Book Co., London, England.

Snieška, V., Navickas, V., Havierniková, K., Okręglicka, M. and 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), pp.1269-1284.

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), pp.1512-1532.

Stock, T., Obenaus, M., Kunz, S. and 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, pp.254-267.

Tahriri, F., Mousavi, M., Haghighi, S.H. and Dawal, S.Z.M., 2014. The application of fuzzy Delphi and fuzzy inference system in supplier ranking and selection. Journal of Industrial Engineering International, 10(3), pp.1-16.

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

Tseng, M.L., Tan, R.R., Chiu, A.S., Chien, C.F. and Kuo, T.C., 2018. Circular economy meets industry 4.0: can big data drive industrial symbiosis?. Resources, Conservation and Recycling, 131, pp.146-147.

Tupa, J., Simota, J. and Steiner, F., 2017. Aspects of risk management implementation for Industry 4.0. Procedia manufacturing, 11, pp.1223-1230.

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

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), pp.735-747.

Wang, M., Asian, S., Wood, L.C. and Wang, B., 2020. Logistics innovation capability and its impacts on the supply chain risks in the Industry 4.0 era. Modern Supply Chain Research and Applications.

Xi, X. and Qin, Q., 2013. Product quality evaluation system based on AHP fuzzy comprehensive evaluation. Journal of Industrial Engineering and Management (JIEM), 6(1), pp.356-366.

Xiong, B., Chen, H., An, Q. and Wu, J., 2019. A multi-objective distance friction minimization model for performance assessment through data envelopment analysis. European Journal of Operational Research, 279(1), pp.132-142.

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

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

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