Resiliency of Smart Manufacturing Enterprises via Information Integration

Abstract

Smart Manufacturing enterprises emerge as interconnected, geographically distributed, data driven, and adaptive. While smartness is improved by the integration of information, this also leads to complexity. In this paper, smart manufacturing enterprises are modeled as a complex adaptive system with resiliency as a property. Resiliency is indicated by the enterprises' ability to comprehensively understand risks and adapt to changes, and information integration plays an important role. A systematic literature review reveals that the current perspectives on manufacturing resiliency are narrow as they are concentrated on isolated parts of the manufacturing process and do not account for enterprise-wide risks that are typical to a smart manufacturing enterprise. An expanded set of risk sources is important for resiliency and information integration has a key role to play in reducing these risks. The complex adaptive systems lens employed in the paper prescribes a five-part framework to organize key risk sources including: external environment, internal environment, manufacturing processes, technology; and demand-supply networks. Additionally, for each key risk source, the role of integrated information is discussed. Lastly, complexity of a single function (logistics) is described and the rational for a CAS view is provided.

Keywords: smart manufacturing, complex adaptive systems, enterprise resilience, risk and resiliency, industrial information integration, industry 4.0

Funding sources: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

1. Introduction

1.1. Motivation

Smart manufacturing is an emerging form of production rooted in the concept of cyber-physical systems and digital twins [1,2]. The physical (machines, processes, devices) and organizational manufacturing assets (strategy, project management, conflict resolution systems) are integrated with cyber information and communication assets (data platforms, computing models, artificial intelligence). Smart manufacturing embraces new business models such as geographically distributed production. It addresses location-specific demand variations that can be responded to with greater efficiency and waste reduction.

The paradigm shift from traditional manufacturing to smart is driven by the proliferation of low-cost sensors to measure production activities and digitize them, developments in data science allowing to make use of data, and the promise of a more efficient and sustainable manufacturing. These advances are part of the field of Industrial information integration engineering (IIIE) [3–5]. Thus, smart manufacturing is a product of the integration between Internet of Things (IoT) and IIIE [6].

Smart manufacturing includes concepts of resilient and sustainable manufacturing [7]. This paper focuses on resiliency and argues that IIIE has a key role to play in achieving manufacturing resiliency via the reduction of risks. Previous studies have established that resilient systems require understanding the landscape of dynamic risks [8], yet knowledge of integrated risks is missing. In the smart manufacturing environment, risks cannot be considered in isolation, rather their source and their impact on the broader enterprise must be acknowledged. In this paper, an enterprise-level resiliency, beyond manufacturing processes, supply chains, and cybersecurity is considered. There is merit in this approach because in connected systems, risks occurring in one part of the system will cascade across the system and affect other parts. This can also lead to complexity, and therefore a theoretical lens that addresses complexity is used.

The paper begins with a systematic literature review of risk and resiliency in manufacturing. The review highlights gaps, and suggestions to bridge these gaps are provided. An important finding is that studies on risks in manufacturing disproportionately focus on singular issues. The bulk of the literature tends to cover supply-chain disruptions, production continuity, and cybersecurity risks (which may themselves cause supply-chain disruptions). Frameworks and solutions presented in the literature have focused on reduced and bounded problems, plausibly failing to capture the entirety of the picture of enterprise resiliency. This is inadequate for smart and integrated enterprises. Secondly, studies tend to consider disruptions as givens leading to an inadequate understanding of risk sources. A more fruitful approach would be to develop an event-based positioning of risks that is contextualized to the manufacturing enterprise. Thus, a five-part framework to characterize resiliency and risks is proposed as an advancement. A case is made to view smart manufacturing as a complex adaptive system (CAS) and the framework is employed on a single integrated enterprise function (i.e., logistics) to draw out risk sources and demonstrate their complexity.

2. Literature Review

The Scopus database indexes approximately 261,950 articles on topics related to Smart/Advanced/Intelligent Manufacturing and Industry 4.0 published over the past 57 years. The exponential uptake in publications over the past decade as shown in Figure 1 indicates accelerated development and rapid maturity.

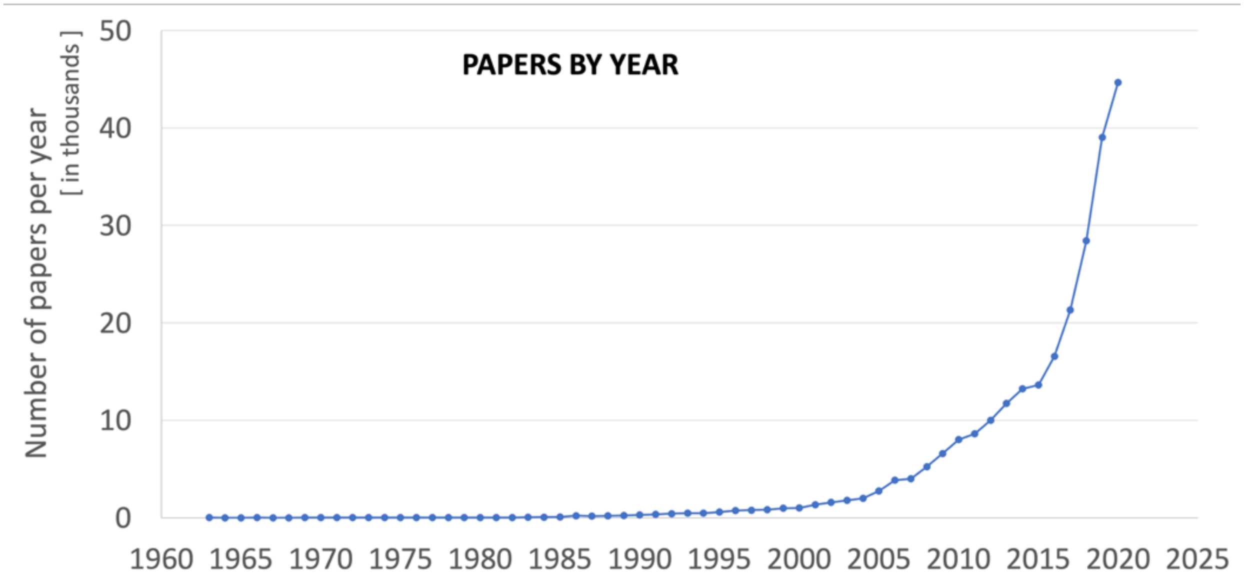

Figure 1. Yearly trend line of the count of papers published on the combined topics of smart/advanced/ intelligent manufacturing and Industry 4.0 (Scopus analysis tool, February 19th, 2021).

Significant constraints posed by the integrated manufacturing enterprise structure affect its resiliency. The discipline structure of industrial information integration engineering (IIIE) proposed by Xu [3,4,9] demonstrates the interaction between IIIE and the various disciplines including management and enterprise. Similarly, Chen [6] highlights the role of IIIE in smart manufacturing. However, our literature review shows that the distribution of publications in smart manufacturing resiliency by subject area is largely concentrated in the engineering and computer science domains. There is an equitable distribution across business management and accounting; mathematics; decision sciences; material sciences; and physics and astronomy domains. This indicates that while there is reasonable and growing awareness in business and management, the topics of risk and resiliency are still very much dominated by purely technical orientations. In this paper, we address smart manufacturing resiliency holistically, considering the integrated context between the manufacturing, technological, and business domains of the enterprise as well as the environment in which the enterprise operates.

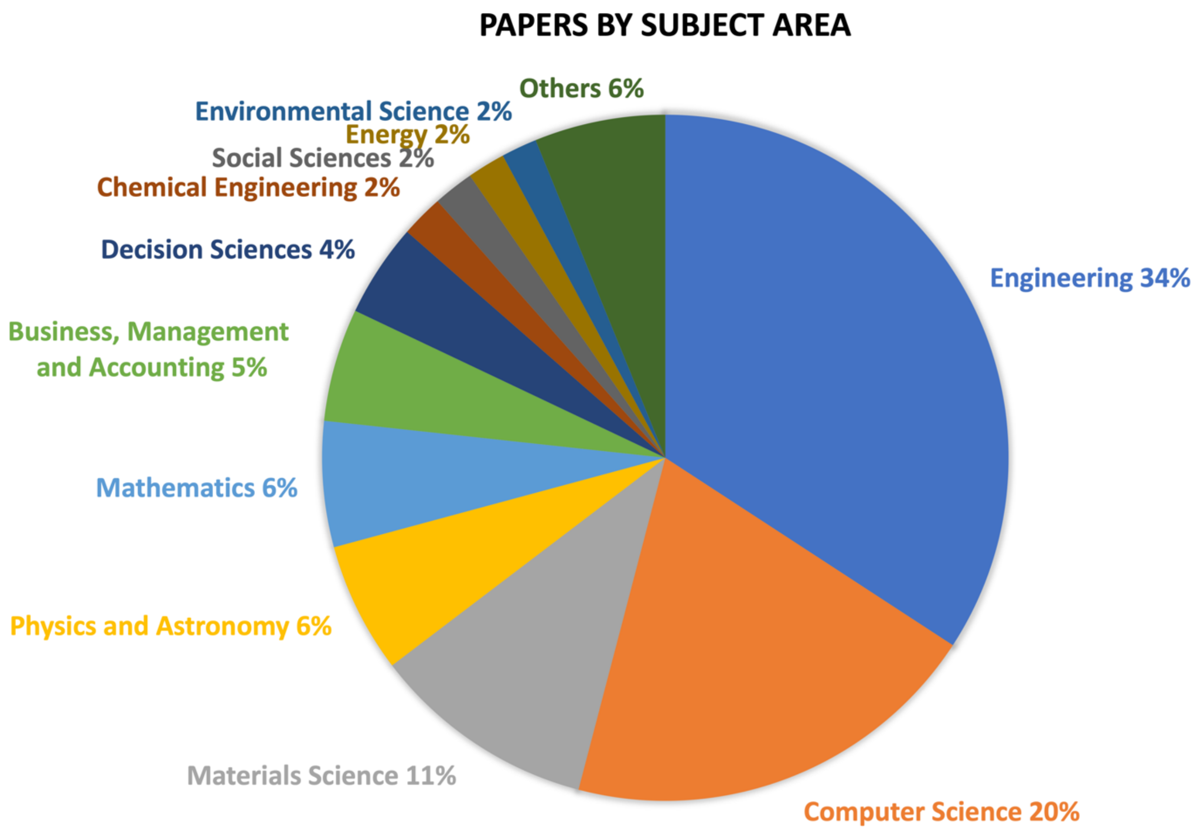

Figure 2. Subject area distribution of 260,950 published papers on the combined topics of smart/advanced/intelligent manufacturing and Industry 4.0 (Scopus analysis tool, February 19th, 2021).

The increased frequency of global events spilling over onto enterprises further motivates the immediate need for manufacturing enterprise resiliency. A systematic literature review is conducted. Papers are found using the search expression below on the Scopus database.

(risk AND (“smart manufacturing” OR “industry 4.0” OR “intelligent manufacturing” OR “advanced manufacturing”) AND “resilien*”)*

The Boolean search expression has a wildcard symbol (*), which comprehensively covers the search space for the terms risk(s), resilien(t), resilien(cy), and resilien(ce) when they are used along with the terms industry 4.0 and/or intelligent/advanced/smart manufacturing. The wildcard symbol reduces the chances of missed papers.

2.1. Research gap

The goal of the systematic literature review was to discern focus and create a roadmap for targeted research in the area of risk and resiliency for integrated smart manufacturing. Based on relevance, 40 out of 155 publications were selected. These ranged from forthcoming articles to those dating back to the early 2010’s. As expected of a rapidly growing field, there was considerable duplication of concepts [10] and rapid evolution, leading to a maturity of the topic with vision papers, position papers, review papers, sense-making frameworks, and most importantly- consistently well-defined terminologies. Ultimately, 25 publications were deemed most important to the objective of the research and studied carefully. They are tabulated in Table 2 along with summaries of their contribution to the topic of manufacturing resiliency. Table 1 partitions the 25 papers based on the focus of risk considered in them and the level of analysis at which risk mitigation was approached. The publications are clustered into 4 groups based on their focus of type of risks: (1) enterprise risks; (2) supply chain disruption; (3) production system failure; and (4) cybersecurity, and 4 cross-groups based on the level of risk mitigation suggested in them: (a) technology; (b) design or architecture; (c) value creation and delivery system; and (d) multi-level and integrated. They are organized in Table 1.

The literature review pointed to three major themes. First, we observed that manufacturing resiliency is conceptualized differently across studies. Specifically, we noticed that 21 of the 25 papers focused on isolated risks and only 4 papers recognized risk sources at the enterprise level [11–14]. Among these 4, Ivanov, Das, and Choi introduce a broad concept of flexibility by surveying literature on various forms of dynamic change and response. Although they have a broad basis and wide coverage, the paper maintains an operations and supply chain focus. Adriaensen, Decré, and Pintelon perform a cross-sector review focusing on occupational safety risk. Their finding is that the smart manufacturing context makes risks more opaque to users. Importantly, they suggest that a complexity perspective would be fruitful. Morisse and Prigge look at business resiliency for smart manufacturing systems and offer a practice-oriented model. Importantly, they recognize that resilience strategies can be complex and therefore need to be optimized for the context of smart manufacturing. Their model is conceptually similar to the one developed in this paper. However, here the focus is on risk and the role of information integration in mitigating those risks. Lastly, Kibira, Morris, and Kumaraguru conduct a truly multi-level study on the performance of smart manufacturing systems. Theirs is the only paper to take a comprehensive view of potential threats impacting manufacturing systems. Although majority papers considered risks in a reduced manner, there was considerable variation in the levels at which risk mitigation is suggested. For example, papers studying production system failures, addressed mitigation via technological solutions [15–17], architectural solutions [18], as well as solutions focused on the manufacturing and logistics system [19]. This observation was extended to other clusters as well. Please see table 1 for the remaining clusters and references. This is encouraging because it indicates that scholars recognize the integrated context of smart manufacturing, the plurality of risks, and consequences of isolated solutions. Most importantly, for smart manufacturing resiliency, an expanded set of risk foci beyond isolated parts of the manufacturing enterprise such as the production system and supply chain disruption, is important. Going forward we expect to see studies focusing on enterprise level risks that go beyond traditional manufacturing or supply chain functions and expect to see studies on their integrated multi-level effects. Overall, the multi-level and integrated risk mitigation of enterprise risks is crucial for smart manufacturing resiliency.

Second, it appears that the majority papers did not investigate the sources of risks i.e., actual hazards to individual manufacturing components or events that trigger them, and simply assumed risks to manufacturing enterprises as a given. A comprehensive view of risks is warranted and arguably crucial for resiliency as recent global events such as the Covid-19 pandemic, extended trade wars, and Brexit have highlighted the broad extent and rippling impact of events on the integrated manufacturing enterprise. Out of the four enterprise level studies highlighted above, only one [13] attempted to delve into the precise sources of enterprise risk. Based on these observations, the sources of risks could be studied for individual components of the manufacturing enterprise. For a deeper view of smart manufacturing technologies and attributes see Mittal et al. (2019) and Kusiak (2018, 2019). An event-driven study of risks, which will likely lead to a better understanding of event-risk-smart manufacturing component interactions, could be considered.

Third, we found that studies do discuss the cascading effects posed by risk events for manufacturing, although they limit themselves to implications for supply chain disruptions. 'Ripple effect' in the organization due to supply chain disruptions was described and methods to exert controls to curtail it were considered [21–23]. We believe that the notion of cascading impact is extendible beyond the supply chain and should be part of the discussion on resiliency of integrated manufacturing enterprises. In fact, the spillover effects across the system can be attributed to the dense interconnection of the enterprise and lends itself well to the notion of a goal-oriented complex adaptive system [24]. As indicated by several papers in the review, we expect complexity science to play a more prominent role in contributing to advancement of the field. Thus, a complexity viewpoint is important for resiliency of manufacturing enterprises.

The remainder of the paper addresses the issues raised above by initiating a road map. Based on the first observation, a 5-part framework is developed with the main components for enterprise level risks. It includes: (1) The external/operating environment; (2) The internal/enterprise environment; (3) Manufacturing processes; (4) Technological advancements; and (5) Demand-supply networks and people's role. The 5 parts are described in the section below and the role of information integration in risk identification and/or mitigation is discussed. The framework should be used to contextualize specific risks to corresponding smart manufacturing components- i.e., the various physical and cyber assets. This is because risk events are primary drivers of consequences (perturbations to the CAS), and when used this way, the framework generates the integrated view of resiliency. We call this perspective 'the integrated view of resiliency'. Figure 3 is a visual representation.

Table 1. Synthesis of the systematic literature review by focus of risk and level of risk mitigation.

		Risk focus			
		Cybersecurity	Production system failure	Supply chain disruption	Enterprise risks
Level of risk mitigation	Multi-level and integrated	Gajek, Lees, and Jansen (2020)		Farahani, Meier, and Wilke (2016) Ivanov, Dolgui, and Sokolov (2019) Ralston and Blackhurst (2020) Belhadi et al. (2021)	Ivanov, Das, and Choi (2018) Morisse and Prigge (2017) Kibira, Morris, and Kumaraguru (2016) Adriaensen, Decré, and Pintelon (2019)
	Value creation and delivery system		Lee, Jin, and Bagheri (2017)	Ivanov et al. (2019) Ivanov and Dolgui (2020)	
	Design / architectural	Zhou et al. (2020) Babiceanu and Seker (2019)	Siafara et al. (2017)		
	Technological	Wallis et al. (2018) Huang et al. (2019) Ahram et al. (2017) Gupta et al. (2020) Komolafe et al. (2019)	Brik, Bettayeb B , M'hammed Sahnoun, and Duval (2018) Nayak et al. (2016) Rivera Torres et al. (2018)	Cavalcante et al. (2019) Lohmer, Bugert, and Lasch (2020)	

Table 2. Summary of the papers included in the literature review.

Authors	Remarks	Risk focus	Level of risk mitigation
Ivanov et al. (2019); Ivanov and Dolgui (2020)	The study provides a data-driven SC disruption modeling framework, and how a digital SC twin can lead to resilience via greater visibility	Supply chain disruption	Value creation and delivery system
Cavalcante et al. (2019)	The focus is on one aspect of SC resilience (timely delivery). Use simulation and supervised machine learning to create a predictive model of supplier resilience	Supply chain disruption	Technology
Farahani, Meier, and Wilke (2016)	It provides a view of automotive supply chain managers on how to bring new technological innovations on a cohesive agenda. 17 digital SCM use cases, being identified within expert interviews, form the basis for the creation of the digital supply chain management agenda	Supply chain disruption	Multi-level and integrated
Ivanov, Dolgui, and Sokolov (2019)	The study evaluates the impact of digitalization on SC risk management. The contribution is the review of related studies and the introduction of a framework for SC risk management in the Industry 4.0 context	Supply chain disruption	Multi-level and integrated
Ivanov et al. (2018)	The study reviews control theory and discusses its application in managing supply chain in the context of Industry 4.0. Although the discussion is around optimized supply chains the theory's application in managing supply chain disruptions is inferred	Supply chain disruption	Value creation and delivery system
Ralston and Blackhurst (2020)	The study gauges practitioner viewpoints on the potential of smart manufacturing to enhance and/or mitigate SC risks derived in a smart manufacturing context. It suggests practitioners view smart manufacturing systems as a method to gain competitive advantage and do not affect human capability loss	Supply chain disruption	Multi-level and integrated
Lohmer, Bugert, and Lasch (2020)	The study simulates smart manufacturing systems using blockchain and determines that the use of smart contracts can have positive impact on SC resiliency	Supply chain disruption	Technology

Belhadi et al. (2021)	It is a sector level study indicating integrated risk management is a long-term supply chain resilience proactive response strategy	Supply chain disruption	Multi-level and integrated
Lee, Jin, and Bagheri (2017)	The paper focuses on prediction of production failures by implementing cyber-physical systems to inject resilience and interoperability with a goal to optimize the manufacturing productivity	Production system failure	Value creation and delivery system
Brik, Bettayeb B , M'hammed Sahnoun, and Duval (2018)	the study simulates disruptions in scheduling due to resource localization issues and proposes a ML model to predict this type of disruption	Production system failure	Technology
Nayak et al. (2016)	the study introduces a resource sharing based framework for modeling cyber physical systems in real applications. Even at a theoretical level, the study acknowledges complexity in implementing cyber physical systems, and shows sector agnostic applicability of the framework	Production system failure	Technology
Rivera Torres et al. (2018)	this study proposes technological interventions to prevent manufacturing process failures by providing a bio-inspired stochastic Boolean model for preventative maintenance schedules	Production system failure	Technology
Siafara et al. (2017)	This study recognizes the inability of conventional centralized architectures to effectively control distributed cyber-physical manufacturing systems and proposes a self-aware process health monitoring architecture that is inspired from biological systems	Production system failure	Design or Architecture
Ivanov, Das, and Choi (2018)	This study introduces a broad concept of flexibility by surveying literature on various forms of dynamic change and response. Although it has a broad basis, the study maintains its operations/SC focus	Enterprise risks	Multi-level and integrated
Morisse and Prigge (2017)	This paper looks at resiliency in information systems for smart manufacturing. The study offers a practice-oriented model of business resiliency for smart manufacturing which has 6 parts to it. However, there is evident overlap between the proposed structure. It is however at a broad enough level for smart manufacturing resiliency	Enterprise risks	Multi-level and integrated

Kibira, Morris, and Kumaraguru (2016)	This study focuses on the performance of smart manufacturing systems and takes a comprehensive view of potential threats that can reduce the expected performance of smart manufacturing systems	Enterprise risks	Multi-level and integrated
Adriaensen, Decré, and Pintelon (2019)	This cross-sector review focuses on occupational safety risk and suggest using a complexity perspective to address the workplace safety risks introduced by smart manufacturing. There is no one solution fits all method for ensuring safety in the context of smart manufacturing as smart manufacturing makes failures more opaque to users (more difficult to point out the source of failures)	Enterprise risks	Multi-level and integrated
Zhou et al. (2020)	The study proposes an architectural framework for layer-by-layer protection of industrial control systems such that physical assets can be protected from cyber attacks	Cybersecurity	Design or Architecture
Gajek, Lees, and Jansen (2020)	The study recognizes the global vulnerability of smart manufacturing systems and suggests that blockchain technology is a solution to enterprise-wide cyber threats	Cybersecurity	Multi-level and integrated
Wallis et al. (2018)	The study focuses on security risks enhanced by the connect smart manufacturing context. The study proposes a technology solution to prevent a specific attack on machine tool commands	Cybersecurity	Technological
Huang et al. (2019)	The study proposes a specific type of blockchain solution that aims for network security in smart manufacturing	Cybersecurity	Technological
Ahram et al. (2017)	This study proposes blockchain as an appropriate technological solution to cyber threats in the smart manufacturing context	Cybersecurity	Technological
Gupta et al. (2020)	This paper views blockchain technology as a solution to cyber threats in the Autonomous Vehicles industry	Cybersecurity	Technological
Komolafe et al. (2019)	This paper focuses on a novel hardware-based technological solution to authenticate part and processes, thereby reducing the risks of cyber threat to smart manufacturing systems	Cybersecurity	Technology
Babiceanu and Seker (2019)	This study proposes multiple connected architectural solutions for protection of the production control system in a smart manufacturing context	Cybersecurity	Design or Architecture

3. An Integrated View of Resiliency

3.1. Understanding risks to build smart manufacturing resiliency

Resiliency is the ability of a system to recover from an undesired state to its desired state [39–41]. This definition is typically referred to as 'engineering resilience', which views the system as designed and controllable, and focuses on system elasticity i.e., return to the steady state following some type of shock. Thus, shocks and other system disruptions are risks. Researchers have highlighted that understanding and managing risks is fundamental to achieving system resiliency [42–47]. This implies identifying risks to the different system parts, and actively gauging their occurrence probabilities and consequences for a dynamical system [8]. Once risk ownership is understood, corresponding parts of the system can be reinforced to mitigate vulnerabilities. Thus, although resiliency encompasses risk, a focus on risk is core to resiliency. Industrial information integration

Smart manufacturing is constituted by six pillars: (1) Manufacturing technology and processes; (2) Materials; (3) Data; (4) Predictive engineering; (5) Sustainability; and (6) Resource sharing and networking [20]. Thus, resiliency of smart manufacturing implies resiliency of its six pillars, and information integration impacts them all. Furthermore, table 4 describes the ten attributes of resiliency for manufacturing that have been discussed in the literature [1,7]. They were primarily organized around the manufacturing functions with a limited focus on the societal and business context. In contrast, the lens put forward here is an enterprise lens and not limited to risks originating directly within the manufacturing organization (which has been the tendency in the literature). Table 4 maps risks to the manufacturing resiliency attributes providing a more granular view of the risk-resiliency relationship for manufacturing.

Risk source 1: External environment

Enterprises operate in an environment with factors and forces beyond their control [48]. This includes industry characteristics (e.g., nascent, growing, mature, declining) and competition characteristics (e.g., fragmented, consolidated). Industrial information such as the state of industry reports and competitive analyses are developed by business and investment research companies. Bloomberg and The London Stock Exchange Group are two examples.

Additionally, a given competitive environment will likely have new entrants with productivity or price-based competition. Furthermore, manufacturing enterprises will operate in a globalized context, i.e., they will likely have geographically distributed, multinational operations leading to vulnerabilities created by any threat to free-market dynamics such as trade wars and tariffs. Thus, shifts of political power, variable interpretation of regulation, and protectionism by national governments are all legitimate sources of risk. News agencies and political outlets cover such events globally. Furthermore, global event databases such as the GDELT project monitor the world's broadcast, print, and web news from nearly every corner of every country in over 100 languages and identify the people, locations, organizations, themes, sources, emotions, counts, quotes, images and events driving our global society every second of every day, creating a free open platform for computing on the entire world.

Lastly, the external environment is impacted by both short- and long-term trends. Recent events are illustrations of the global nature of shock events, and the overall increased demand for products points to the changing nature of global consumption. Short-term shocks and long-term stressors build trends, which pose critical risk sources for the smart manufacturing enterprise.

Thus, information plays an important role in quickly identifying risks generating in the external environment and integrating it to situate the enterprise is crucial to building resiliency.

Risk source 2: Internal environment

Top-down leadership is a key differentiator of enterprise performance. Top management vision guides the course of the enterprise amidst its external context. Thus, executive buy-in to support on-going enterprise initiatives often becomes the determinant of its success or failure. Executive tenure and succession have been reported has being internal sources of risk. Greater data-driven decision making on the part of leaders enabled by IIIE methods can reduce agent risk.

Additionally, operating successfully in highly dynamic business environments i.e., where the rate of change (e.g., technological, competitive) is rapid, requires strategic flexibility and nimbleness, as well as access to resources such as investment capital and talent. These resources are crucial for technological upgrades for the cyber-physical assets in a smart manufacturing enterprise. Enterprises with low levels of free cash flow and/or saturated credit lines from the open market find it extremely challenging to fuel sustained growth, which is the currently dominant measure of success in for-profit public companies. However, credit markets support evidence-based proposals, which rely on integrated information on initiative performance.

Sustained corporate growth is often achieved via the purchase of smaller but valuable companies, or via mergers with competitors. However, the success of such moves depends largely on post-merger integration. The efficient implementation of integration plans has direct impact on enterprise resiliency, which is measured during due-diligence and enhanced by improved data and information.

Therefore, integrated information provides greater clarity on technological needs, integration potential, and leads to data-driven decision making at the top levels.

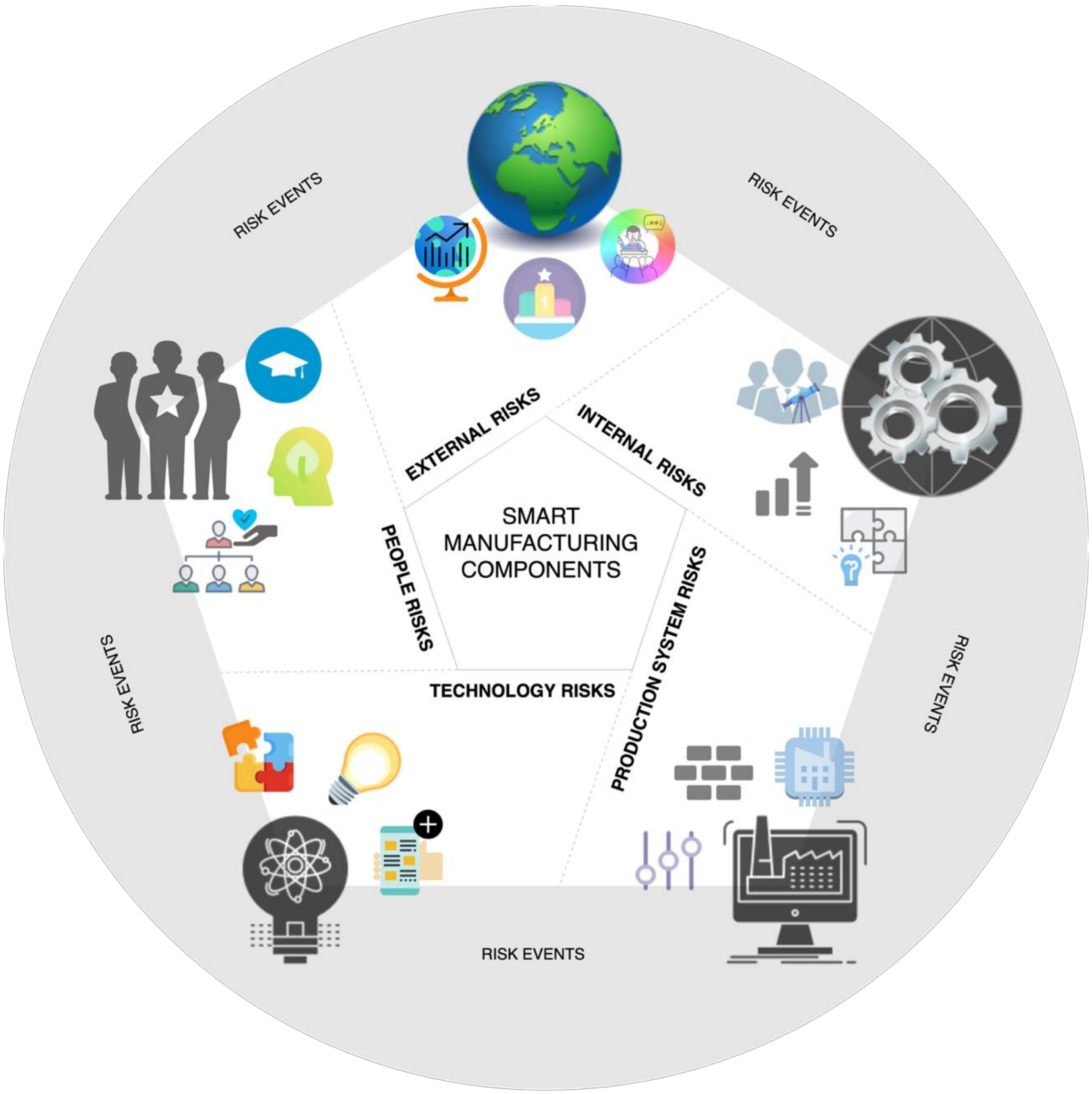

Figure 3. The integrated lens on smart manufacturing resiliency.

Risk source 3: Manufacturing processes and systems

This is one of the six pillars of smart manufacturing. It includes developing and maintaining cyber-physical infrastructure (e.g., standardized design of architectural components for modularity and interoperability, and optimized processes for data-driven intelligence and predictive engineering). An enterprise inevitably depends on technology developed outside its sphere of influence (e.g., open source) to develop and maintain its manufacturing assets. Therefore, with new developments, production processes and systems need to be updated for seamless functioning, which forms a key source of risk. So far, IIIE has made its largest impact on this risk source and will continue to reduce it further. However, it also implies that IIIE must go beyond the manufacturing process and technological advances to address the enterprise level.

Risk source 4: Technological advances

Leading technological advancements and innovation necessitates considerable capital expenses in exploratory research and development. These risky projects are not guaranteed to succeed and therefore, expenses are difficult to justify upfront. Furthermore, enterprises may not have the necessary expertise in-house, thereby making innovation even more challenging. To lower risk of research and development conversion failures, enterprises often choose to adopt successful technologies and business models rather than invent new ones. Their success depends on the level of integration with existent technologies and already deployed business models. Collectively, technological upkeep is a key source of risk to all components of smart manufacturing, and improvements in information integration will continue to reduce the risk of making technological updates in enterprises.

Risk source 5: Demand-Supply networks and people's role

Manufacturing enterprises exist to cater to the product demands generated by end consumers. Lately, we are witnessing the large impact of social trends and consumer perception on demand owing to greater connectivity and the vast expansion in consumer choice. Unexpected demand drops in the short-term and long-term trends such as the ecological awareness of consumers and consumer privacy concerns are real enterprise risks.

Information communication technologies (ICT) and information integration quickly identifying demand-supply and inventory risks. For instance, with the advent of real-time information processing (in contrast to batch-processing), information on customer purchases and fluctuating demand for particular products is relayed back to manufacturing plants in real-time, thereby mitigating the risk of under or over-stocking due to changing consumer tastes. Another example is the hyper-customization of customer-market segments, which leads to reduced production and inventory risks.

On the supply side, a more aware workforce is a key stakeholder for decision makers. Furthermore, organizational culture issues such as operational ethics and attrition rates pose real risks. Importantly, the workforce needs continuing education, training, and up-skilling, which needs integrated information and knowledge as its basis.

Each risk source and sub-source discussed above is listed below in Table 3.

Table 3. Five parts of the integrated lens on smart manufacturing resiliency.

1. External environment
    a. Market dynamism and competition
        i. Sector fragmentation
        ii. New entrants
        iii. Productivity and price competition
    b. Globalized context
        i. Multinational operations
        ii. Political changes
        iii. Threats to free-market operation
    c. Short and Long-term trends

        i. Global impact events
        ii. Changing nature of consumption
        iii. Changing nature of production
2. Internal environment
    a. Top management vision and leadership
        i. Buy-in and support through initiatives
        ii. Tenure and succession
    b. Adaptive agility of the enterprise
        i. Strategic flexibility
        ii. Access to investment capital and talent
    c. Growth and Integration
        i. Profitable earnings
        ii. Sustainable growth (Organic and inorganic)
        iii. Post-merger integration
3. Manufacturing/Production system processes
    a. Infrastructure
        i. Cyber-physical assets development and maintenance
        ii. Production process control logic
    b. Modularity and Interoperability
        i. Design of architectural components
        ii. Seamless communication
    c. Predictive, adaptive, and optimized processes
        i. Data operations
        ii. Advanced computing
4. Technological advances
    a. Leading invention
        i. R&D capability and conversion
        ii. IP development
    b. Leading adoption
        i. Locating and adopting new technology
        ii. IP landscape monitoring
    c. Integration ability
        i. Modular and interoperable design
        ii. Minimal interruptions
5. Demand-supply networks and people's role
    a. Social trends impacting perception and demand-supply
        i. Ecological awareness of consumers
        ii. Workforce voice
        iii. Privacy
    b. Training and Upskilling
        i. Continuous education
        ii. New skill development
    c. Organizational culture
        i. Ethics
        ii. Attrition rates

Table 4. Manufacturing resiliency attributes and key risks.

Resiliency Attribute	**Industry 4.0 context**	**Key risks** (illustrative and non-exhaustive)
Logistics	Vulnerability caused by cloud integration and associated portability	Cyber-attacks, trade wars, regulation
Efficiency	Diminishing manufacturing efficiency as well as energy efficiency	Competitive threat driven by cost competition and price sensitive customers, lack of capital investment
Productivity	Diminishing productivity driven by technological backwardness	Lack of capital investment, lack of skilled labor, failure to grow inorganically
Capacity	Increased complexity of managing shared globally distributed capacity dynamically	Failure of demand forecasting models, geopolitical risks, localized disruptive events
Dependability	Perennial availability and reliability of interconnected manufacturing systems	Input failures, connection failures, translational failures, failures of human-machine interaction
Quality	Variable product quality driven by dynamic changes operations	Dynamic changes in equipment, process, operators
Compatibility	Reduced seamless replicability of manufacturing capability across cyber-physical assets and distributed locations	Non-standardization (inputs, equipment and processes), idiosyncratic data models, erroneous model, errors during transfer
Societal values	Changing motivational drivers based on evolving social consciousness	Global social trends, social media smear campaigns
Workforce	Reduced flexibility and lack of upskilling of the workforce for distributed production	Global workforce, cultural challenges, up-skilling challenges, lack of equally skilled labor
Sustainability	Reduced ability to produce in a sustained fashion over a long-term in order to recover capital investments	Lack of input, regulatory pressures, judicial rulings, political power shifts, nationalistic behavior or protectionism, inconsistency in law interpretation, inability to afford litigation costs

4. The Logistics Function in a Smart Enterprise

Logistics is critical manufacturing function. Its significance to the question of resiliency has only increased with the advent of digital twins supplementing the physical supply chain for increased visibility (Kritzinger et al. 2018; Schleich et al. 2021; Haag and Anderl 2018; Boschert and Rosen 2016; Tao et al. 2021). We used a simplified view of logistics processes and associated risks that was provided by researchers [54]. Intuitively, there is significant parallelization across the logistics function. Table 5 represents the logistics process and groups its sub-activities. A literature search was conducted to locate risks to specific processes. It is synthesized in Table 6.

From Table 6, we find a many-to-many mapping between the logistics process parts, highlighting inherent complexity. The integrated lens separates the logistics processes by risk source. For example, the material handling and transportation process parts have the highest order of connectivity closely followed by demand planning and inventory management. This implies greater centrality of these parts and therefore, their higher vulnerability to system disruption. Further, transportation and demand planning are affected by all five risk sources, implying their greater exposure to many more risks than other logistics process parts. Intuitively, we can presume that focusing on more central parts that are subject to diverse risk sources should lead to greater resiliency. Collectively, these two facts imply that the complex logistics function can be easily impacted by risks outside the enterprise's direct sphere of control. One can calculate the impact of a single change in the risk on the rest of the logistics function to illustrate the complexity quantitatively.

Alternatively, each process part can be individually viewed through the proposed lens to evaluate for riskiness and information integration engineering can be utilized to reduce risk. A detailed synthesis of this is provided in Table 6. For instance, except warehousing, the external environment (risk source 1) impacts all logistics processes. Global benchmarks in customer service and order processing established by service businesses outside the manufacturing domain (e.g., customer facing businesses such as Amazon) set expectations for manufacturing enterprises. Similarly, social short-term demand trends such as popularity fluctuations and long-term societal trends such as environmental awareness (risk source 5) impact demand and manufacturing forecasts, inventory buffer levels, and cause order processing jams, thereby creating capacity concerns for warehousing. However, customer behavior data from such stores and online platforms can be integrated with partner suppliers to affect efficient manufacturing, warehousing, and informed pricing.

Similarly, regionally varying labor regulations greatly impact material handling, transportation, and warehousing processes. Yet, data-driven insights at the unit level such as on individual materials (materials requiring highest and lowest handling) and individual transporters (optimal and non-optimal routes or best or worst driving performance linked to psychometric data) can help mitigate risk and perhaps also shape regulation in the long-term.

Another risk of competition from vertically integrated businesses such as big box retailers starting their own manufacturing and launching their own brands (e.g., Walmart, Amazon) impacts procurement as supplier power increases. This in-turn exerts earnings and growth pressure on the manufacturing enterprise and challenges its strategic vision (risk source 2). Insights on customer preference trends can partly reduce this risk as companies can quickly turnaround their product strategy to meet trending demand.

Technological advances in logistics processes (risk source 4) require upgrades and investment of free cash into labor upskilling. Continuous learning, training, and up-skilling of the enterprise workforce (risk source 5) can only be achieved via dissemination of information and knowledge that is integrated with what was previously known to workers.

Lastly, physical and cyber assets require maintenance and protection. They also benefit by continuous optimization using data collected via advanced computing tools. These tools are value added services, which are often highly expensive and difficult to integrate or customize. These impact all processes of the logistics function (risk source 3). IIIE has already made an impact in this area.

Since connectedness is the essence of smart manufacturing, its resiliency depends on identifying, quantifying, and mitigating interconnected risks. It is imaginable that information integrated across the process parts will aid to reduce the risks by improving the performance visibility of each process function. Specifically, process parts along a series such as ‘material handling’, ‘order processing’, ‘transportation’, and ‘warehousing’, that are affected by interlinked risks will be reduce via IIIE. Table 6 provides a detailed synthesis of logistics processes, interlinkage, and areas where solutions created by IIIE. In summary, the complexity created by potential risks needs to be recognized and reduced via information integration.

Table 5. Smart logistics processes and activity grouping.

Order info, claims, complaints, returns	Product tracking	Demand forecast		Safety stock level	Layout / slotting design
Needs assessment	Stockout level	Manufacturing forecast		Economic order quantity, re-order level	
Sorting	Transporting	Call center management	Consignee management	Location, size, and number of facilities	
Order picking procedure		Order entry / fulfilment		Facility demand allocation	
Strategic sourcing	Purchasing	Mode	Routing	Stock layout	Dock design
Supplier management		Scheduling		Stock placement	Order picking/ selection

Legend:

customer service	demand planning	inventory mgmt.
material handling	order processing	facility planning
procurement	transportation	warehousing

Table 6. The logistics function and associated process-activities, and their complexity.

From	To	Description	Reference	Integrated risk lens
Material handling	Demand planning	Intelligent sensor networks link material handling to customer service, demand planning	Konyha and Bányai (2017)	Manufacturing, technology, people
Material handling	Customer service			
Inventory management	Demand planning	For smart manufacturing, ML enabled PPC- production planning and control modules need to be coupled with logistics for smart logistics, but we rarely consider people (customer and human-in-the-loop) aspects of using ML in PPC.	Usuga Cadavid et al. (2020)	External, internal, manufacturing, technology, people
Facility planning	Transportation	Current manufacturing service platforms, which integrate distributed manufacturing services to complete complicated manufacturing tasks have issues because they must navigate complex on-ground geographical constraints such as routes and non-straight-line distances, and Internal enterprise constraints such as costs, and profitability targets.	Wang et al. (2019)	External, internal
Facility planning	Transportation	Paper shows how unique organizational structures (fractal and modular) need to be implemented to realize highly complex patterns for manufacturing that merges all the enterprise functions of an integrated organization to improving the speed of operations and the ability to adapt quickly to changes in the environment.	Prause and Atari (2017)	External, internal, manufacturing
Transportation	Warehousing	The article focuses on links between manufacturing and logistics functions in the Steel production process, and specifically speaks about 'transportation', and 'warehousing' linkages. It speaks of the impact of smart manufacturing on these, and the need for	Beham et al. (2020)	Internal, manufacturing, technology, people

		prescriptive analytics to automate or support human resources in handling logistics.		
Material handling	Transportation	The paper proposes a model that links material handling and transportation components to eventually link logistics to manufacturing in smart manufacturing.	Funke and Becker (2020)	Manufacturing, technology
Material handling	Facility planning	This paper proposes a model-based solution to link facilities, material handling, transportation, and warehousing via a common underlying abstraction	Sprock and Bock (2020)	Internal, technology, people
Material handling	Warehousing			
Material handling	Transportation			
Facility planning	Warehousing			
Facility planning	Transportation			
Facility planning	Transportation	This paper investigates the correlations between facility planning and local and regional transportation networks keeping the smart manufacturing context in mind	Altafini, Braga, and Cutini (2021)	External
Inventory management	Transportation	This paper introduces self-similar architecture for supply chain, which is a concept from complex adaptive systems. It also links facility, inventory, transportation in logistics	Sprock (2018)	Internal, manufacturing, technology
Inventory management	Facility planning			
Transportation	Facility planning			
Facility planning	Transportation	This paper considers links between facility planning, procurement, and transportation functions in order to minimize and internal performance metric - costs of logistics	Lucchese, Marino, and Ranieri (2020)	Internal
Facility planning	Procurement			
Transportation	Procurement			

5. Smart Enterprise as a Complex Adaptive System (CAS)

5.1. CAS and its characteristics

The theory of CAS builds on system complexity, i.e., when systems contain several components and/or a large number of interconnections between them. There is non-linear system response to external perturbations, which leads to the non-predictability of its behavior. CAS are characterized by emergence i.e., behaviors that are not witnessed in parts of the system but emerge when parts interact as a whole. Architecturally, CAS are multilevel and show self-similarity, i.e., system components and sub-components tend to show similar structures at multiple levels. A very interesting characteristic of CAS in the context of smart manufacturing is homeostasis or adaptation i.e., the CAS ability to change internally in order to absorb external pressures while remaining aligned to the system goal. As noted by researchers in the field of industrial information integration (cite all), the increased volume of information adds to system complexity. Yet, statistical techniques of data science such as machine learning allow us to at least develop algorithms that perform tasks at levels similar to human judgement. Albeit gradually, artificial intelligence is progressing towards sense-making based on volumes of big data, which can lead to complex adaptive manufacturing systems that would be able to self-learn and adapt.

CAS have been categorized into two broad types – type 1, such as the human brain, which are CAS in and of themselves and optimized for achieving best outcomes for the CAS; and type 2, such as the biosphere, which are composed of several type 1 CAS and not optimized for the global best outcome [65]. A manufacturing enterprise may be viewed as a goal-oriented CAS 1 within larger CAS (e.g., the macroeconomy and/or the ecology) with multiple objectives including resiliency and sustainability. Thus, we envision the future manufacturing enterprise as a CAS 1 that is optimized for the enterprise. Doing so, enables the study of drivers of adaptive behavior and adaptation mechanisms in manufacturing enterprises.

5.2. Why complex adaptive system (CAS)?

Engineering resilience described previously focuses only on the bouncing back or return or the system from disruption. Thus, it primarily refers to system stability and is reactive by nature. This conceptualization is flawed because recent events have demonstrated that enterprises are impacted by disruptions caused by factors beyond their control. For instance, in a case study of the semi-conductor ecosystem, Sawik [66] showed the global cascading impact of a single manufacturing failure across sectors. Such cascades can be attributed to factors broader than just the supple chain (which has been the focus of the literature thus far). Therefore, resilient manufacturing enterprises must be proactive in continuous adaptation and learning rather than reactive (return to normalcy). Thus, resiliency is more than stability [67]. In fact, we may even argue that non-stable or continuously changing systems may also be resilient (referred to as enterprise agility in business literature). Fortunately, CAS theory is well positioned to accommodate this proactive view of enterprise resiliency. CAS's adaptive, goal-seeking, selfpreserving, and sometimes evolutionary behavior [24,68] makes it an ideal abstraction for future manufacturing enterprises.

It is encouraging to see that operations research is already progressing in this direction. Studies exploring supply chain architectures that are rooted in CAS theory have recently been published. For instance, Sprock [63] introduced self-similar architecture in the design of smart manufacturing supply chain and logistics, linking the facility planning, inventory management, and transportation processes. Similarly, Prause and Atari [58] showed how unique organizational structures (fractal and modular) can be implemented to merge the functions of an enterprise toward an overarching objective such as to improve the speed of operations or develop the ability to adapt quickly to changes in the environment [69]. Recently, CAS theory was used to re-conceptualize supply chain resiliency [70,71]. We expect concepts from CAS theory such as multi-level system objectives, self-organization, and adaptation to be discussed more frequently in the context of future manufacturing enterprises.

6. Conclusion

The Covid-19 pandemic exposed vulnerabilities of manufacturing enterprises. However, it is not the first time that disruptions in manufacturing have gained attention of the research community. Several factors (some outside its direct control) affect the resiliency of a manufacturing enterprise such as its external operating environment, the enterprise's business constraints, technological advancement, and long- and short-term societal trends. Therefore, an enterprise view that integrates the largely technical orientation of manufacturing risks to its enterprise system risks is important for resiliency. It is argued that an integrated view of risk is important as manufacturing resiliency depends on identifying and mitigating vulnerabilities pre-event and learning, adapting, and transforming post-event. Yet, a systematic literature review suggests that studies on risk and resiliency in smart manufacturing currently operate only at singular levels focusing on domain specific risks. However, in a smart manufacturing context, risks need to be multi-level and integrated. Thus, the paper advances the current view on manufacturing resiliency by surpassing singular domains such as the supply chain or cyber resiliency to focus on enterprise-wide risks. In addition, the paper provides an integrated lens to view five key sources of risk in manufacturing, namely the enterprises' external context, internal context, manufacturing processes and systems, technological advancements, and supply chains. Solution. Furthermore, the paper shows via literature review that advancements in information integration across 5 key risk sources and IIIE techniques will likely improve manufacturing resiliency.

In addition to the above, the paper proposes a conceptual advancement in the way resilience in manufacturing enterprises is discussed. Currently, manufacturing resilience is conceptualized as system stability (adopted in most reviewed papers). In contrast, the concept developed herein goes beyond the notion of stability and instead focuses on continuous adaptation. Therefore, the ultimate goal of a resilient manufacturing system is more than simply continuing to perform as it is orginially designed but to instead change as required by external and internal forces. This view is grounded in complex adaptive systems (CAS) theory, which also provides methods to tackle the problem of increasing complexity of a highly integrated system. In the paper, the CAS lens is applied to the logistics function, demonstrating the inherent complexity of the smart manufacturing paradigm, further advocating the use of complex adaptive systems (CAS) theory, which is currently lacking.

Manufacturing has been at the center of the industrial revolution and the manufacturing activity impacts society at scale with both positive and negative consequences. As we envision future manufacturing, it must be centered on the needs of the society with a resilient and sustainable manufacturing enterprise. This implies that we embrace the inherent complexity added by several interconnected stakeholders. A CAS lens is appropriate for studying future manufacturing enterprises as it enables considering resiliency as an attribute of the CAS.

References

[1] R. Schmitt, E. Permin, J. Kerkhoff, M. Plutz, M.G. Böckmann, Enhancing Resiliency in Production Facilities Through Cyber Physical Systems, in: 2017: pp. 287–313. https://doi.org/10.1007/978-3-319-42559-7_11.

[2] F. Tao, Q. Qi, L. Wang, A.Y.C. Nee, Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison, Engineering. 5 (2019) 653–661. https://doi.org/10.1016/j.eng.2019.01.014.

[3] L. Da Xu, Enterprise integration and information architecture: a systems perspective on industrial information integration, 2014.

[4] L. Xu, L. Cai, S. Zhao, B. Ge, Editorial: Inaugural Issue, J. Ind. Integr. Manag. 01 (2016) 1601001. https://doi.org/10.1142/S2424862216010016.

[5] C. Chen, Grand Challenges in Measuring and Characterizing Scholarly Impact, Front. Res. Metrics Anal. 1 (2016) 2014–2017. https://doi.org/10.3389/frma.2016.00004.

[6] Y. Chen, A survey on industrial information integration 2016–2019, J. Ind. Integr. Manag. 5 (2020) 33–163. https://doi.org/10.1142/S2424862219500167.

[7] A. Kusiak, Fundamentals of smart manufacturing: A multi-thread perspective, Annu. Rev. Control. 47 (2019) 214–220. https://doi.org/10.1016/j.arcontrol.2019.02.001.

[8] G.S. van der Vegt, P. Essens, M. Wahlström, G. George, Managing Risk and Resilience, Acad. Manag. J. 58 (2015) 971–980. https://doi.org/10.5465/amj.2015.4004.

[9] Y. Chen, Industrial information integration—A literature review 2006–2015, J. Ind. Inf. Integr. 2 (2016) 30–64. https://doi.org/10.1016/J.JII.2016.04.004.

[10] S. Mittal, M.A. Khan, D. Romero, T. Wuest, Smart manufacturing: Characteristics, technologies and enabling factors, Proc. Inst. Mech. Eng. Part B J. Eng. Manuf. 233 (2019) 1342–1361. https://doi.org/10.1177/0954405417736547.

[11] D. Ivanov, A. Das, T.-M. Choi, New flexibility drivers for manufacturing, supply chain and service operations, Int. J. Prod. Res. 56 (2018) 3359–3368. https://doi.org/10.1080/00207543.2018.1457813.

[12] M. Morisse, C. Prigge, Design of a Business Resilience Model for Industry 4.0 Manufacturers, AMCIS 2017 Proc. (2017).

[13] D. Kibira, K.C. Morris, S. Kumaraguru, Methods and Tools for Performance Assurance of Smart Manufacturing Systems, 121 (2016). https://doi.org/10.6028/jres.121.013.

[14] Adriaensen, Decré, Pintelon, Can Complexity-Thinking Methods Contribute to Improving Occupational Safety in Industry 4.0? A Review of Safety Analysis Methods and Their Concepts, Safety. 5 (2019) 65. https://doi.org/10.3390/safety5040065.
[15] B. Brik, B. Bettayeb, M. Sahnoun, F. Duval, Towards Predicting System Disruption in Industry 4.0: Machine Learning-Based Approach, Procedia Comput. Sci. 151 (2019) 667–674. https://doi.org/10.1016/j.procs.2019.04.089.
[16] A. Nayak, R. Reyes Levalle, S. Lee, S.Y. Nof, Resource sharing in cyber-physical systems: modelling framework and case studies, Int. J. Prod. Res. 54 (2016) 6969–6983. https://doi.org/10.1080/00207543.2016.1146419.
[17] P.J. Rivera Torres, E.I. Serrano Mercado, O. Llanes Santiago, L. Anido Rifón, Modeling preventive maintenance of manufacturing processes with probabilistic Boolean networks with interventions, J. Intell. Manuf. 29 (2018) 1941–1952. https://doi.org/10.1007/s10845-016-1226-x.
[18] L.C. Siafara, H.A. Kholerdi, A. Bratukhin, N. Taherinejad, A. Wendt, A. Jantsch, A. Treytl, T. Sauter, SAMBA: A self-aware health monitoring architecture for distributed industrial systems, in: Proc. IECON 2017 - 43rd Annu. Conf. IEEE Ind. Electron. Soc., Institute of Electrical and Electronics Engineers Inc., 2017: pp. 3512–3517. https://doi.org/10.1109/IECON.2017.8216594.
[19] J. Lee, C. Jin, B. Bagheri, Cyber physical systems for predictive production systems, Prod. Eng. 11 (2017) 155–165. https://doi.org/10.1007/s11740-017-0729-4.
[20] A. Kusiak, Smart manufacturing, Int. J. Prod. Res. 56 (2018) 508–517. https://doi.org/10.1080/00207543.2017.1351644.
[21] D. Ivanov, A. Dolgui, A. Das, B. Sokolov, Digital Supply Chain Twins: Managing the Ripple Effect, Resilience, and Disruption Risks by Data-Driven Optimization, Simulation, and Visibility, in: Int. Ser. Oper. Res. Manag. Sci., Springer New York LLC, 2019: pp. 309–332. https://doi.org/10.1007/978-3-030-14302-2_15.
[22] D. Ivanov, A. Dolgui, B. Sokolov, The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics, Int. J. Prod. Res. 57 (2019) 829–846. https://doi.org/10.1080/00207543.2018.1488086.
[23] J. Lohmer, N. Bugert, R. Lasch, Analysis of resilience strategies and ripple effect in blockchain-coordinated supply chains: An agent-based simulation study, Int. J. Prod. Econ. 228 (2020) 107882. https://doi.org/10.1016/j.ijpe.2020.107882.
[24] J. Liu, T.W. Tong, J. V Sinfield, Toward a resilient complex adaptive system view of business models, Long Range Plann. (2020) 102030. https://doi.org/10.1016/j.lrp.2020.102030.
[25] S. Gajek, M. Lees, C. Jansen, IIoT and cyber-resilience: Could blockchain have thwarted the Stuxnet attack?, AI Soc. 1 (2020) 3. https://doi.org/10.1007/s00146-020-01023-w.
[26] P. Farahani, C. Meier, J. Wilke, Digital supply chain management agenda for the automotive supplier industry, in: Shap. Digit. Enterp. Trends Use Cases Digit. Innov. Transform., Springer International Publishing, 2016: pp. 157–172. https://doi.org/10.1007/978-3-319-40967-2_8.
[27] P. Ralston, J. Blackhurst, Industry 4.0 and resilience in the supply chain: a driver of capability enhancement or capability loss?, Int. J. Prod. Res. 58 (2020) 5006–5019. https://doi.org/10.1080/00207543.2020.1736724.

[28] A. Belhadi, S. Kamble, C.J.C. Jabbour, A. Gunasekaran, N.O. Ndubisi, M. Venkatesh, Manufacturing and service supply chain resilience to the COVID-19 outbreak: Lessons learned from the automobile and airline industries, Technol. Forecast. Soc. Change. 163 (2021) 120447. https://doi.org/10.1016/j.techfore.2020.120447.
[29] D. Ivanov, A. Dolgui, A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0, Prod. Plan. Control. (2020). https://doi.org/10.1080/09537287.2020.1768450.
[30] C. Zhou, B. Hu, Y. Shi, Y.C. Tian, X. Li, Y. Zhao, A Unified Architectural Approach for Cyberattack-Resilient Industrial Control Systems, Proc. IEEE. (2020). https://doi.org/10.1109/JPROC.2020.3034595.
[31] R.F. Babiceanu, R. Seker, Cyber resilience protection for industrial internet of things: A software-defined networking approach, Comput. Ind. 104 (2019) 47–58. https://doi.org/10.1016/j.compind.2018.10.004.
[32] K. Wallis, M. Hüffmeyer, A. Soner Koca, C. Reich, Access Rules Enhanced by Dynamic IIoT Context, in: Proc. 3rd Int. Conf. Internet Things, Big Data Secur., SCITEPRESS - Science and Technology Publications, 2018: pp. 204–211. https://doi.org/10.5220/0006688502040211.
[33] J. Huang, L. Kong, G. Chen, M.Y. Wu, X. Liu, P. Zeng, Towards secure industrial iot: Blockchain system with credit-based consensus mechanism, IEEE Trans. Ind. Informatics. 15 (2019) 3680–3689. https://doi.org/10.1109/TII.2019.2903342.
[34] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, B. Amaba, Blockchain technology innovations, in: 2017 IEEE Technol. Eng. Manag. Soc. Conf. TEMSCON 2017, Institute of Electrical and Electronics Engineers Inc., 2017: pp. 137–141. https://doi.org/10.1109/TEMSCON.2017.7998367.
[35] R. Gupta, S. Tanwar, N. Kumar, S. Tyagi, Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review, Comput. Electr. Eng. 86 (2020) 106717. https://doi.org/10.1016/j.compeleceng.2020.106717.
[36] T. Komolafe, W. Tian, G.T. Purdy, M. Albakri, P. Tarazaga, J. Camelio, Repeatable part authentication using impedance based analysis for side-channel monitoring, J. Manuf. Syst. 51 (2019) 42–51. https://doi.org/10.1016/j.jmsy.2019.01.007.
[37] I.M. Cavalcante, E.M. Frazzon, F.A. Forcellini, D. Ivanov, A supervised machine learning approach to data-driven simulation of resilient supplier selection in digital manufacturing, Int. J. Inf. Manage. 49 (2019) 86–97. https://doi.org/10.1016/j.ijinfomgt.2019.03.004.
[38] D. Ivanov, S. Sethi, A. Dolgui, B. Sokolov, A survey on control theory applications to operational systems, supply chain management, and Industry 4.0, Annu. Rev. Control. 46 (2018) 134–147. https://doi.org/10.1016/j.arcontrol.2018.10.014.
[39] E. Hollnagel, D.D. Woods, N. Leveson, Resilience Engineering : Concepts and Precepts, Ashgate Publishing Ltd., 2006.
[40] Y. Sheffi, The Resilient Enterprise, The MIT Press, 2005.
[41] Y. Sheffi, J.B.J. Rice, A supply chain view of the resilient enterprise, MIT Sloan Manag. Rev. 47 (2005).
[42] T.A. Williams, D.A. Gruber, K.M. Sutcliffe, Organizational Response to Adversity: Fusing Crisis Management and Resilience Research Streams Article in The Academy of

Management Annals, Journals.Aom.Org. 11 (2017) 733–769. https://doi.org/10.5465/annals.2015.0134.
[43] M. DesJardine, P. Bansal, Y. Yang, Bouncing Back: Building Resilience Through Social and Environmental Practices in the Context of the 2008 Global Financial Crisis, J. Manage. 45 (2019) 1434–1460. https://doi.org/10.1177/0149206317708854.
[44] J. Blackhurst, M.J. Rungtusanatham, K. Scheibe, S. Ambulkar, Supply chain vulnerability assessment: A network based visualization and clustering analysis approach, J. Purch. Supply Manag. 24 (2018) 21–30. https://doi.org/10.1016/j.pursup.2017.10.004.
[45] J. Wolbers, K. Boersma, P. Groenewegen, Introducing a Fragmentation Perspective on Coordination in Crisis Management, Organ. Stud. 39 (2018) 1521–1546. https://doi.org/10.1177/0170840617717095.
[46] M. Morais-Storz, R. Stoud Platou, K. Berild Norheim, Innovation and metamorphosis towards strategic resilience, Int. J. Entrep. Behav. Res. 24 (2018) 1181–1199. https://doi.org/10.1108/IJEBR-11-2016-0369.
[47] K. Scholten, B. Fynes, Risk and Uncertainty Management for Sustainable Supply Chains, in: Springer, Cham, 2017: pp. 413–436. https://doi.org/10.1007/978-3-319-29791-0_19.
[48] R. Hayes, S. Wheelwright, Restoring our competitive edge: competing through manufacturing, Wiley, New York, 1984.
[49] W. Kritzinger, M. Karner, G. Traar, J. Henjes, W. Sihn, Digital Twin in manufacturing: A categorical literature review and classification, IFAC-PapersOnLine. 51 (2018) 1016–1022. https://doi.org/10.1016/j.ifacol.2018.08.474.
[50] B. Schleich, N. Anwer, L. Mathieu, S. Wartzack, Shaping the digital twin for design and production engineering, CIRP Ann. 66 (2017) 141–144. https://doi.org/10.1016/j.cirp.2017.04.040.
[51] S. Haag, R. Anderl, Digital twin – Proof of concept, Manuf. Lett. 15 (2018) 64–66. https://doi.org/10.1016/j.mfglet.2018.02.006.
[52] S. Boschert, R. Rosen, Digital twin-the simulation aspect, in: Mechatron. Futur. Challenges Solut. Mechatron. Syst. Their Des., Springer International Publishing, 2016: pp. 59–74. https://doi.org/10.1007/978-3-319-32156-1_5.
[53] F. Tao, H. Zhang, A. Liu, A.Y.C. Nee, Digital Twin in Industry: State-of-the-Art, IEEE Trans. Ind. Informatics. 15 (2019) 2405–2415. https://doi.org/10.1109/TII.2018.2873186.
[54] P. Verma, V. Dixit, J. Kushwaha, Risk and Resilience Analysis for Industry 4.0 in Achieving the Goals of Smart Logistics: An Overview, in: Proc. Int. Conf. Ind. Eng. Oper. Manag. Dubai, UAE, March 10-12, 2020.
[55] J. Konyha, T. Bányai, Sensor networks for smart manufacturing processes, in: Solid State Phenom., Trans Tech Publications Ltd, 2017: pp. 456–462. https://doi.org/10.4028/www.scientific.net/SSP.261.456.
[56] J.P. Usuga Cadavid, S. Lamouri, B. Grabot, R. Pellerin, A. Fortin, Machine learning applied in production planning and control: a state-of-the-art in the era of industry 4.0, J. Intell. Manuf. 31 (2020) 1531–1558. https://doi.org/10.1007/s10845-019-01531-7.
[57] Y. Wang, Y. Zhang, F. Tao, T. Chen, Y. Cheng, S. Yang, Logistics-aware manufacturing service collaboration optimisation towards industrial internet platform, Int. J. Prod. Res. 57 (2019) 4007–4026. https://doi.org/10.1080/00207543.2018.1543967.
[58] G. Prause, S. Atari, On sustainable production networks for industry 4.0, Entrep. Sustain.

Issues. 4 (2017) 421–431. https://doi.org/10.9770/jesi.2017.4.4(2).
[59] A. Beham, S. Raggl, V.A. Hauder, J. Karder, S. Wagner, M. Affenzeller, Performance, quality, and control in steel logistics 4.0, in: Procedia Manuf., Elsevier B.V., 2020: pp. 429–433. https://doi.org/10.1016/j.promfg.2020.02.053.
[60] T. Funke, T. Becker, Complex networks of material flow in manufacturing and logistics: Modeling, analysis, and prediction using stochastic block models, J. Manuf. Syst. 56 (2020) 296–311. https://doi.org/10.1016/j.jmsy.2020.06.015.
[61] T. Sprock, C. Bock, SysML Models for Discrete Event Logistics Systems, J Res Natl Inst Stan. 125 (2020) 125023. https://doi.org/10.6028/jres.125.023.
[62] D. Altafini, A. Braga, V. Cutini, Planning sustainable urban-industrial configurations: relations among industrial complexes and the centralities of a regional continuum, Int. Plan. Stud. (2021) 1–21. https://doi.org/10.1080/13563475.2021.1875810.
[63] T. Sprock, Self-similar architectures for smart manufacturing and logistics systems, Manuf. Lett. 15 (2018) 101–103. https://doi.org/10.1016/j.mfglet.2018.02.002.
[64] A. Lucchese, A. Marino, L. Ranieri, Minimization of the Logistic Costs in Healthcare supply chain: A hybrid model, in: Procedia Manuf., Elsevier B.V., 2020: pp. 76–83. https://doi.org/10.1016/j.promfg.2020.02.025.
[65] D.S. Wilson, A. Kirman, Complexity and evolution: Toward a new synthesis for economics, MIT Press, 2016.
[66] T. Sawik, Supply chain disruption management, Springer International Publishing, 2020.
[67] A. Wieland, C.F. Durach, Two perspectives on supply chain resilience, J. Bus. Logist. (2021) jbl.12271. https://doi.org/10.1111/jbl.12271.
[68] S.A. Levin, Ecosystems and the biosphere as complex adaptive systems, Ecosystems. 1 (1998) 431–436.
[69] M. Shin, J. Mun, M. Jung, Self-evolution framework of manufacturing systems based on fractal organization, Comput. Ind. Eng. 56 (2009) 1029–1039. https://doi.org/10.1016/j.cie.2008.09.014.
[70] D.C. Novak, Z. Wu, K.J. Dooley, Whose resilience matters? Addressing issues of scale in supply chain resilience, J. Bus. Logist. (2021) jbl.12270. https://doi.org/10.1111/jbl.12270.
[71] R. Wiedmer, Z.S. Rogers, M. Polyviou, C. Mena, S. Chae, The Dark and Bright Sides of Complexity: A Dual Perspective on Supply Network Resilience, J. Bus. Logist. (2021) jbl.12264. https://doi.org/10.1111/jbl.12264.