Received: 15 September 2022 | Accepted: 12 September 2023

DOI: 10.1002/jsc.2555

SPECIAL ISSUE ARTICLE

WILEY

Aspects of resilience for smart manufacturing systems

Daniel S. Fowler | Gregory Epiphaniou | Matthew D. Higgins | Carsten Maple

WMG, University of Warwick, Coventry, UK

Correspondence
Daniel S. Fowler, WMG, University of Warwick, Coventry CV4 7AL, UK.
Email: dan.fowler@warwick.ac.uk

Funding information
High Value Manufacturing Catapult, Grant/Award Number: 8261

Abstract

An external disruptor to a manufacturing process (e.g., a supply chain failure, or a cyber-attack) can affect more than a factory's output; it can have wider societal concerns, raising the issue of industrial resilience at different levels. In this work, manufacturing resilience is revisited, reviewing the applicability of the resilience concept to the industrial domain, particularly the smart factories enabled by newer digital technologies. The meaning of resilience within manufacturing is shown to be composed of several factors that operate at three levels (macro, meso, and micro). The factors have been united from a variety of sources to unify the traits within manufacturing resilience. Furthermore, a summary of the advanced digital technologies that can aid (or detract) from resilience is discussed, along with some of their challenges around digital complexity, legacy equipment support, high-performance wireless communications, and cybersecurity. Although it is seen that digital manufacturing systems can aid resilience within the industrial sector and contribute to wider societal goals, the biggest impact is likely to be at the lowest (micro) level. Opportunities exist to quantify resilience factors and their use within manufacturing systems support software, and how to influence the resilience requirements of the wider stakeholders.

KEYWORDS
CPPS, digital factory, resilience, security, smart manufacturing

JEL CLASSIFICATION
D20, E23, L23, L60, M11, O14

Investment in innovative smart manufacturing technology is aimed at production efficiencies and output sustainability goals, plus, if the design of a smart system considers factors relevant to resilience it can mitigate against future external disruptors of production at the macro, meso, and micro levels.

1 | INTRODUCTION

Global events from 2019 onward have renewed interest in the concept of resilience in the industrial domain (Kusiak, 2020). Examples of external disruptions to manufacturers included the COVID-19 pandemic (Remko, 2020), the Suez Canal blockage (de Bodt et al., 2021), shortages of semiconductors (Voas et al., 2021), supply chain cyber-

attacks (Peisert et al., 2021), armed conflict impacts (Mbah & Wasum, 2022), and the UK's exit from the European single market. Manufacturing industries are seen as a core contributor to strong economic well-being and such disruptive events distract from industrial resilience (European Commission Directorate-General for Research and Innovation, 2021). Yet, potential disruptors to manufacturing outputs are not new; they include competition from emerging industrial countries, cyber-attacks, terrorist attacks, activism, extreme weather events and future global warming impacts. The need for manufacturers to understand and allow for such unpredictable events, often under the topic of risk management, keeps resilience as a recurring consideration (Thoma, 2014). Furthermore, the multifaceted nature of resilience touches upon many aspects of the manufacturing ecosystem (Kusiak, 2020; Wied et al., 2020).

There have been previous studies on the meaning and design of a *resilient manufacturing system* (Gu et al., 2015; Tomiyama & Moyen, 2018; Zhang & van Luttervelt, 2011), and consideration of resilient manufacturing cannot be decoupled from the growth of advanced digital technologies which enable the Cyber-Physical Production System (CPPS) in the *smart factory* (acatech (Ed.), 2011). A Cyber-Physical System (CPS) combines actuated machines with computer control enabling software to physically interact with the environment. Whilst manufacturing has always embraced CPSs to improve production processes, the digitalization of factories now connects production cells and lines with the supply chain to enable the CPPS and the emergence of smart factories. However, these newer so-called smart or intelligent manufacturing technologies, if not correctly considered, instead of aiding the incorporation of resilience into system design, may detract from it. The objectives of this work are twofold. First, to revisit the concept of manufacturing resilience to gather together and gain an understanding of its various aspects. Second, to examine some of the digital technologies that smart manufacturing may incorporate, and how those technologies may relate to resilience. These objectives are achieved by extracting and collating a variety of aspects of resilience from published sources, examining the newer manufacturing digital technologies that have emerged, and expanding upon some of the technology features that may be particularly relevant to future manufacturing resilience. Organizations having this holistic overview will have an insight into how the design and management of a CPPS can allow for resilience aspects.

The next section provides a brief overview and background to the meaning of resilience and related topics. Section 3 examines potential manufacturing disruptors in further detail. In Section 4, resilience is examined in terms of a variety of desirable properties for any CPPS. Section 5 examines the incentives for resilience and benefits to various stakeholders. Finally, the intersection of resilience and the digital technologies underpinning emergent smart manufacturing is covered in Section 6 before a discussion and conclusion.

2 | BACKGROUND TO THE RESILIENCE CONCEPT

Resilience originally referred to the ability of a material to spring back or resume its original shape. It then referred to the ability of people to bounce back from difficulties, and can now mean the ability to continue to perform despite challenging circumstances (Oxford University Press, 2021). Performing under challenging circumstances has long been a requirement for defense and space organizations. These organizations plan for *mission assurance* to ensure a successful mission outcome (Grimaila et al., 2010; Lalli, 1998). As part of mission assurance, the need for *operational resilience* is a required aspect of the supporting systems (Alderson et al., 2013; Grimaila et al., 2010).

FIGURE 1 The cycle of Resilience Engineering (Thoma, 2014). [Color figure can be viewed at wileyonlinelibrary.com]

Resilience as a concept has long spread into many aspects of the supporting systems for society with the need to protect critical national infrastructure (CNI) from unexpected events, for example, terrorist attacks and natural disasters (Thoma, 2014). The operational risk from climate change continues to be studied (Pankratz & Schiller, 2021), and the need for resilience within complex supply chain systems was demonstrated during some of the events mentioned in the introduction. It can be argued that some events are too extreme to predict, yet the objective of stakeholders to design systems to withstand or overcome severe disruption is the goal of Resilience Engineering (RE) (Thoma et al., 2016). RE emerged from studying the need for CNI and society structures to survive, minimize damage, and overcome large-scale and unexpected disruptive events. RE has the *resilience cycle*, Figure 1, to help address issues arising from external events.

However, resilience aspects equally apply to groupings below the international or national, that is, *macro*, level. Indeed, operational risk and business continuity concepts are well-established within many business and industrial sectors (Suresh et al., 2020). The International Organization for Standardization (commonly known as ISO) publishes an international standard on Business Continuity Management Systems (BCMS) (ISO, 2019) that includes a goal of contributing to organizational resilience; we will refer to this as the *meso* level (Baumann et al., 2019). Furthermore, the day-to-day operation of production systems and services has always used monitoring, testing, and maintenance (including predictive maintenance) to keep output and processes going. This is the *micro* level within a factory. The meso and micro levels are where organizations reduce risk, for example, Key Performance Indicators (KPIs) are used in operational management,

TABLE 1 Macro, meso, and micro resilience levels.

Level	Coverage	Applicability	Examples
Macro	National and multinational	Governments and large organizations with considerations covering critical infrastructure over multiple sites	Networks of power, communications and transportation, supply chains and logistics, social structures, law and order, health systems, financial systems, and labor markets
Meso	Limited geographical areas and buildings	Local facilities and branches of organizations, medium and small enterprises	Business and industrial parks, factories and offices, and public facilities and spaces
Micro	Building internals and worker groups	Internal systems and subsystems, operational systems, and individuals	Plant and machinery, equipment, processes, and procedures

primarily for day-to-day reliability (Weber & Thomas, 2005). A BCMS, along with health and safety procedures, and site security all contribute to the challenge of resilience management (Caralli et al., 2016). Table 1 summarizes the macro, meso, and micro levels when addressing resilience at the different levels of scale, and those levels can be considered to be impacted by the other levels, with dependencies through them.

3 | THE NEED TO HANDLE DISRUPTORS

In the previous section, resilience is defined as the ability to continue to perform under challenging circumstances. What are those circumstances? The ISO BCMS targets the "need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption" (ISO, 2019). Gu et al. (2015) state: "Resilience is defined as the ability of a system to withstand potentially high-impact disruptions, and it is characterized by the capability of the system to mitigate or absorb the impact of disruptions, and quickly recover to normal conditions." Table 2 has some examples of sources of disruption.

Knowing that potential disruptors exist that can impact the operation of systems naturally leads to how systems can be protected from disruption. As discussed in Section 2, processes and procedures already exist to minimize certain disruptions. However, some disruptors may need a greater focus because of an increasing occurrence, or a higher likelihood.

The disruptors (Table 2) are either intentional (a deliberate act) or not (an accident or *Act of God*). For example, an unintentional event could be a storm (rain, flood, and winds) or a heatwave. Severe weather can cause damage and destruction, interrupt power, and affect supply chains and transportation networks. Many of the potential intentional disruptors are driven by human behavior, particularly *threat agents* (ISO, 2014), these can include:

1. Cybercriminals
2. Nation-state actors
3. Terrorists
4. Activists pursuing direct action and civil disobedience
5. Lone wolfs (e.g., via social exclusion, mental illness, or radicalization)
6. Disgruntled employees
7. Drunken or drug-induced behavior
8. Vandals

TABLE 2 Disruptors impacting an organization's resilience.

Level	Disruptors
Macro	Natural disasters (e.g., volcanoes or earthquakes) Disease outbreak (epidemic or pandemic) Extreme or severe weather events Market forces and new startups Changes in laws, regulations, and standards Changes in societal behavior Technology obsolescence
Meso	Local power outage Animal or insect plagues Riots, protests, and activism Trade unionism or strike action Raw material and parts shortages
Micro	Malfunctions Equipment fires Security breaches (e.g., theft or burglary) Deviation from procedures Cyber-attack Disgruntled, badly behaved, or ill employee

Some of the threat agents overlap, for example, nation-states encouraging certain cybercriminal groups, or activists encouraging vandalism. Many of the disruptors discussed in this section are already a consideration within an organization's BCMS processes. The next section examines the individual factors or system properties that can contribute to resilience and mitigate the effect of disruptors.

4 | FACTORS FOR MANUFACTURING RESILIENCE

Resilience is similar to health and safety, or security, in that these desired non-functional attributes do not appear to impact daily system operation. These attributes are secondary to a manufacturing system's primary function of production output. However, a disruptor impinging those non-functional aspects may impact the primary manufacturing purpose. Further, the non-functional aspects can be

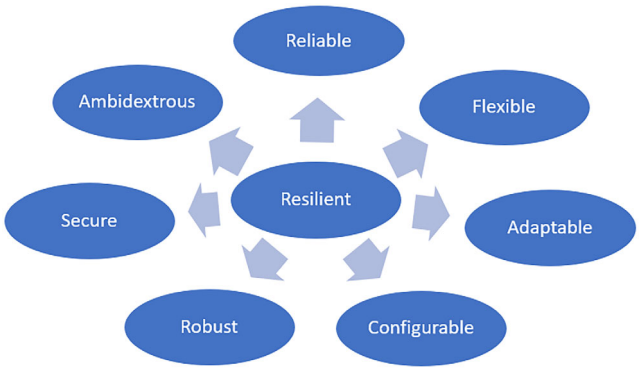

FIGURE 2 Contributory factors to resilience. [Color figure can be viewed at wileyonlinelibrary.com]

harder to incorporate into a system. The primary system function is achieved by engineering solutions to concrete requirements. Catering for non-functional aspects in the overall system design is challenging, which is amplified when considering the wider meso and macro levels of the super-systems that make up the supply chains and services consumed by a factory.

Software-based engineering tools used to design a manufacturing process do not necessarily allow non-functional qualities to be included. Furthermore, what can make the concept of resilience quantifiable, and therefore addressable, when considering system operations and processes? Literature related to the concept of resilience will discuss a variety of overlapping qualities, these include (see also Figure 2):

1. Reliability—a common facet of daily system operation, a manufacturing system needs to be reliable (Freeman & Varga, 2021; Kott & Linkov, 2019).
2. Flexibility—a manufacturing system can change its operation to cater for changes in process or product parameters or conditions (Freeman & Varga, 2021; Maurer & Schumacher, 2018; McCarthy et al., 2017; Meyer et al., 2020; Thoma et al., 2016).
3. Adaptability—the ability to adapt manufacturing to new products or processes (adaptability is similar to flexibility, but here the difference is between new and existing processes or products; Freeman & Varga, 2021; Maurer & Schumacher, 2018; Meyer et al., 2020; Thoma et al., 2016).
4. Configurability—another quality that can be related to flexibility or adaptability, but being configurable, or reconfigurable, allows manufacturing to quickly change a process or make changes to a product (McCarthy et al., 2017; Zhang & van Luttervelt, 2011).
5. Robustness—a robust system can maintain operational performance despite parametric disturbances (internal or external). Robustness is sometimes used as a synonym for resilience, but here, resilience is multifaceted (Kott & Linkov, 2019; Maurer & Schumacher, 2018).
6. Security—physical security of premises, plants, and machinery is typically addressed in organizations; however, cybersecurity is now a major concern (Kott & Linkov, 2019; Thoma et al., 2016).
7. Ambidexterity—an organization will primarily be concerned with ongoing day-to-day operations. Some disruptors, for example, technology innovations, new regulations, and changing markets, can have an impact. An ambidextrous, or agile, organization will be structured to both manage normal operations and allow for change and innovation (Maurer & Schumacher, 2018; Meyer et al., 2020; O'Reilly & Tushman, 2004).

The above resilience qualities are desirable properties for the operation of any well-designed system. Literature tends to discuss various subsets of the above factors which is why it is important to collate them into one source. Knowing all the aspects of resilience will increase awareness of where management can make contributions to an organization's overall resilience level. In the next section, some of the resultant benefits of resilience to stakeholders are summarized.

5 | INCENTIVES AND BENEFITS TO DESIGN IN RESILIENCE

RE is traditionally targeted at macro disruptors. However, there are gains to be made in incorporating or enhancing the resilience factors within the meso and micro levels of manufacturing systems. Plus, those factors will contribute to system performance overall. The added benefits from these factors, and hence a resilient design, can aid the long-term viability and growth of organizations via:

1. Reductions in operating costs.
2. Inventory reduction.
3. Efficiency gains.
4. Improvements in maintenance, particularly preventive maintenance.
5. Availability of real-time information through improved Management Information Systems.
6. Increase in market competitiveness.
7. Improved change management.

Furthermore, there are advantages to be derived beyond the industrial sector. Resilient manufacturing can benefit societal stakeholders (Thoma, 2014). Our experience at WMG, the applied research and teaching faculty for manufacturing and business at the University of Warwick, allows us to consider the benefits of manufacturing resilience to societal stakeholders, see Table 3. Societal benefits from building resilient systems can contribute to the United Nations' global goals on sustainable development (United Nations, n.d.).

The above sections have discussed the desirable attributes that could be incorporated into a manufacturing system for resiliency. Engineers engaged with process design and implementation may not be able to directly influence the macro-level issues, which can be driven by Government policy, laws, and regulations. However, deployed systems do affect the micro level and can affect wider system issues at the meso level. Furthermore, the combined effort of designing resilient manufacturing systems could be beneficial to society at the macro level.

TABLE 3 Stakeholder benefits from resiliency in manufacturing.

Stakeholder	Example resiliency benefits
Governments	A resilient manufacturing sector benefits a country's wealth creation ability.
Trade bodies	A resilient sector will promote its growth.
Standards bodies	A commonality in practices and techniques can aid resilience and promote mutually beneficial knowledge exchange.
Owners/ shareholders	An organization that has higher resilience than a competitor would better survive a crisis and retain value.
Management	Operational resilience will enable easier management of an organization's response to issues.
Employees	Resilient processes will reduce stress for workers during disruptive events.
Suppliers	How a supplier handles disruptions affects the confidence an OEM or service provider will have in them.
Shippers (logistics)	Minimizing disruptions to transportation services reduces the impact on the onward manufacturers and consumers.
Customers/ consumers	Disruptions to services and flows of goods can affect everyday life.
Educators/ researchers	The upcoming generation of employees can be given the skills to consider and cater for resilience in the operation of industry and society.
Activists	Resiliency can aid in addressing concerns on the environment, sustainability, and circular economies.

6 | ADVANCED SMART MANUFACTURING TECHNOLOGY AND RESILIENCE

There is a wave of digital manufacturing technologies, some still emerging and maturing, that manufacturers can deploy to enable a novel CPPS. Many of these newer digital technologies have been touted as the enablers of the German Industrie 4.0 initiative, that is, Industry 4.0 (I4.0) (Kagermann et al., 2013). In I4.0, the manufacturing process is seen as part of a network of connected CPSs used to optimize the entire supply chain, from initial order to final delivery. In some respects, I4.0 is a response to a resilience issue, a recognition by Germany that the technologies enabling the emergence of smart factories around the globe could threaten its position as a leading manufacturing country.

Despite manufacturing always seeking to adopt new technologies to improve capabilities, the interest in smart or intelligent manufacturing accelerated with the emergence of I4.0 (Wang et al., 2021). WMG has long applied emerging technologies to industry (Bhattacharyya, 1998), and the following digital technologies are embedded in its applied manufacturing research and teaching:

1. Cloud computing—well established for office-based systems, sees an increasing use in factory systems. Servers are moved away from the factory floor which allows access to powerful computation resources. As communication speeds improve, it allows for increased centralized control and management of manufacturing cells and lines.
2. Big Data analytics and visualization—a key enabler of factory digitalization, granular real-time data of production processes, supply chains, and movement of output through the factory improves the production process decision-making.
3. Industrial Internet of Things (IIoT) and smart sensors—new sensors that are smaller and more powerful are allowing the generation of Big Data streams and new sources of information from a CPPS.
4. Systems and communications virtualization—office IT functions and digital services have benefited from virtualization technology (where specialist software that once required dedicated hardware can now run in the cloud). Virtualization is now seeing use in factory and communications systems, helping reduce system costs and improving flexibility of deployment.
5. Additive Manufacturing (AM)—commonly known as three-dimensional (3D) printing, it is now well established and continues to innovate, opening up new options for manufacturing systems.
6. Machine Learning (ML) and Artificial Intelligence (AI)—now appearing in all areas of organizations, ML/AI is finding many applications in manufacturing.
7. Digital twinning and virtualization of physical processes—while simulation technology has always been embraced by industrialists, the high-fidelity simulations provided by Digital Twins (DTs) and virtual models can aid the analysis of what-if scenarios and predictions of output and effects of supply chain issues.
8. Augmented Reality (AR) and Virtual Reality (VR)—are used for training and aiding operators. It can improve human productivity and reduce wastage. Furthermore, it can be used to enhance customer experiences, particularly around options to customize products.
9. Autonomous robots, cobots, and remote operation (teleoperation)—increase mobility options within production systems and aid elimination of unnecessary operator movement. Teleoperation of machinery can improve overall efficiencies with decreased human movement and travel to sites.
10. Newer wireless communications standards—Wi-Fi 6 (802.11ax) is the next iteration of the common Wi-Fi technology; LoRaWAN, a low-cost, low-power wireless technology for sensor networks; 5G, as used in smartphones, supports Ultra-Reliable Low Latency Communications (URLLC) for manufacturing use cases and can be deployed as a private network. These wireless communications standards are useful for the deployment of smart technologies.
11. Software-Defined Networking (SDN)—this removes the need to have hard-coded and hard-wired connections between equipment and machinery, another technology increasingly deployed

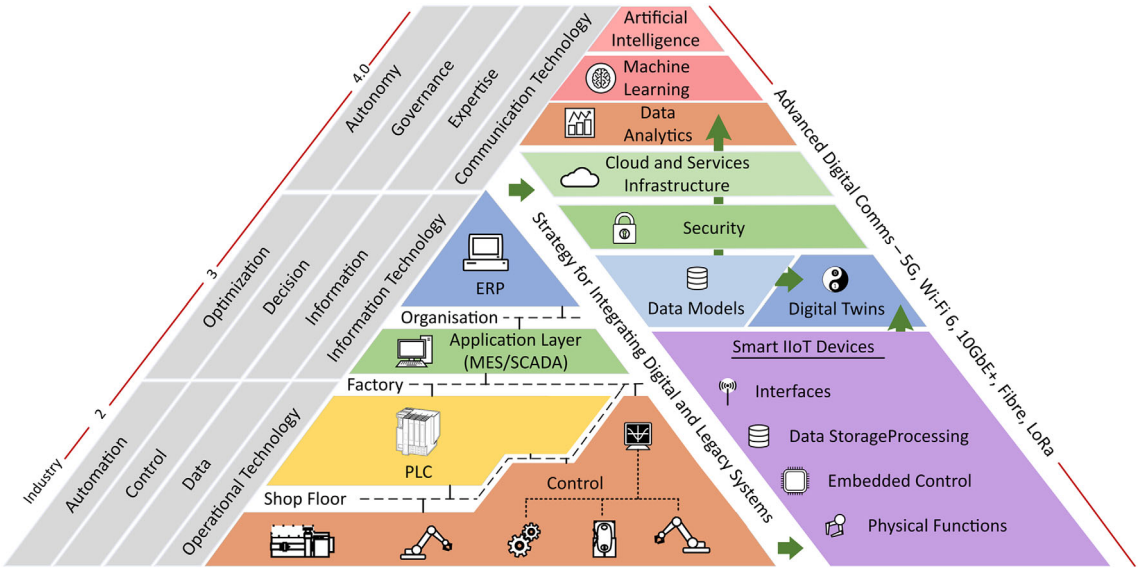

FIGURE 3 Smart manufacturing technologies are expanding the manufacturing pyramid (derived from Harrison et al., 2021). [Color figure can be viewed at wileyonlinelibrary.com]

in office-based and virtualized systems, now finding use in manufacturing systems to increase design options.

If correctly considered and implemented, these technologies provide benefits to manufacturers. They can enable novel manufacturing processes, allow for the introduction of additional mobility and reconfigurability, and remove barriers between an organization's Information Technology (IT), Operational Technology (OT), and Communications Technology (CT) silos (Leiva, 2022) (where manufacturing would operate with IT-based office functions, the shop floor OT functions, and the CT for overall management control). Our research intends to build an evidence-based matrix of the resilience aspects that can be improved by the above smart manufacturing technologies. Currently, an argument can be made for many of those technologies aiding most of the aspects; however, organizations need demonstrable examples.

These newer smart manufacturing technologies can provide instant situational awareness of a process's state, and support control and decision-making with ML/AI-supported insights. This requires rethinking how the new smart manufacturing technologies are organized across operational areas. Indeed, we can consider the newer digital technologies expanding the *automation pyramid*, see Figure 3.

Expanding the automation pyramid brings new considerations in applying digital technologies to manufacturing; some of those considerations are discussed next.

6.1 | Added digital complexity and skill demand

Digital is the commonality among advanced technologies, using connected computers running complex software. Furthermore, the life cycle is complex, through design, programming, deployment, maintenance, and security. The digital complexity and interconnectedness result in challenging cyber-resiliency concerns (Ross et al., 2021). These technologies need to be resilient because the complexity brings with it issues such as emergent behavior, big volumes of data, data veracity, data processing and visualization requirements, data storage and its management issues, and cybersecurity. There is a need for new digital skills that future manufacturing employees will require. A lack of skills and knowledge to build experience and expertise could be a particular problem for small and medium-sized enterprises (SMEs). The technologies can be a particular challenge for SMEs who may not have access to the right resources, or the ability to develop the resources, in-house. If SMEs cannot begin to address the technology directly due to a lack of resources and skills, then they cannot begin to address consideration of the resilience aspects. This is an area that WMG is focused on addressing with its University teaching, research, and short courses.

6.2 | Legacy equipment support

Alongside the challenge of technical complexity is the need to support legacy factory equipment, a recognized problem when digitalizing manufacturing. Some factories continue to use equipment that is decades old, which represents significant capital expenditure to replace, but will not be replaced because it still performs its function. However, that equipment could benefit from augmentation with new technology, for example, using IIoT, to help gain additional insights into processes. Those insights can help improve overall operational efficiency and resilience, applying new applications to legacy equipment; examples include replacing human output inspection, analysis and optimization of power consumption, and introducing alternative maintenance processes, for example, automating predictive maintenance.

6.3 | DTs as a smart manufacturing tool

Incorporating IIoT, sensors, and communications technologies into existing processes is a requirement for the successful implementation of DTs. The use of simulation in manufacturing is long established, but digital twinning is a step up, with additional advantages. High-fidelity virtualized models of the elements of a production process are a requirement for successful twinning within manufacturing. DTs can model a single machine, a manufacturing cell, a production line, or a complete factory. Models need fine-grained data from improved communication and interaction will real production processes and machinery. This builds detail into the model and keeps the twin updated. A DT will consume data provided by sensors from the manufacturing plant to improve the calibration of the modeled elements. A DT can be examined as it runs simulations of different scenarios. The scenarios played out on the twin can inform the configuration, management, and optimization of the physical assets and processes. The virtualized twin can use a fully simulated process or partly simulated with machine-in-the-loop and/or human-in-the-loop elements (where machines and humans can cooperate with the DT when testing scenarios). Digital twinning can be useful for managing the complexity of new technologies, running what-if situations, testing new process designs and process configurations, testing arguments for justification on plant and equipment expenditure, providing a training platform, and allowing experiments with new cybersecurity techniques. DTs can aid digital manufacturing challenges linked to aspects of resilience, these challenges include:

1. Process reconfigurability—DTs can run models of reconfigured processes to determine if the required changes function correctly.
2. Risk and change management—DTs can be used to virtually test changes to reduce risk to the live process.
3. Data analysis—DTs can include detailed analysis and visualizations of live and virtualized processes.
4. Real-time simulation and optimization—virtualized models can be used for the optimization of processes before deployment, preventing potential wastage in the real process.
5. The need for tools to support verification of processes and cybersecurity testing—new process verification and security testing tools can be used on DTs to ensure they work as intended before live deployment.

There is a need to handle the data-intensive nature of DTs, raising other challenges in handling Big Data (see the subsection on complexity above).

6.4 | High-performance wireless networks

The newer high-performance wireless communications, for example, 5G URLLC or Wi-Fi 6, could enhance manufacturing processes, aiding resilience. Removing the tethering of equipment allows support for novel manufacturing cell and production line use cases within factories. It expands the range of existing wireless applications due to improved data bandwidth, latency, and the number of communication channels compared to previous wired and wireless links. Examples include real-time video feeds for multiple cobots and autonomous robots, high-definition video for maintenance and product inspection, data-intensive sensors, at-the-edge processing, and ML/AI capabilities, supporting teleoperation, aiding digital twinning, and gaining access to hard-to-reach areas of a factory (including difficult to cable legacy equipment), and reduce the need for employees to work in hazardous factory locations.

6.5 | The cybersecurity threat

Digital connectivity, both wired and wireless, is an important aspect of a CPPS. However, the connectivity provides an opportunity for systems to be cyber-attacked, locally and from anywhere in the world. Many decades of experience with enterprise office systems and existing Supervisory Control and Data Acquisition systems have demonstrated the continual battle with threat actors. A successful attack could result in one or more issues, including slow or halted production, affecting internal and external communications, disrupting supply chains and logistics operations, losing important data, and damaging reputation. The well-established MITRE ATT&CK matrices are a useful source of information on cybersecurity threats and mitigation (Mitre, 2023). The following are a few of the types of attacks that could be performed:

1. Denial of service (jamming and flooding).
2. Hacking to penetrate systems using known and undiscovered vulnerabilities.
3. Malware, including ransomware, deployment.
4. Eavesdropping of data.
5. Side-channel attacks (e.g., monitoring timing or power signals to elicit information on security keys).
6. Social engineering and phishing of employees.

Fortunately, organizations can use existing experience in protecting office IT systems to deploy CPPS protections. Cyber-attack detection and mitigation techniques and methods include:

1. Firewalls and anti-virus software.
2. Intrusion Detection Systems and Intrusion Prevention Systems.
3. Threat Modeling to understand where weaknesses exist.
4. Threat and Risk Assessment to minimize attack impacts.
5. Cryptography for encryption of data and communications.
6. Honeypots, black holes, and data sinkholes are used to distract attackers and gather evidence.
7. Zero-trust system architecture to enforce security between individual elements within systems.

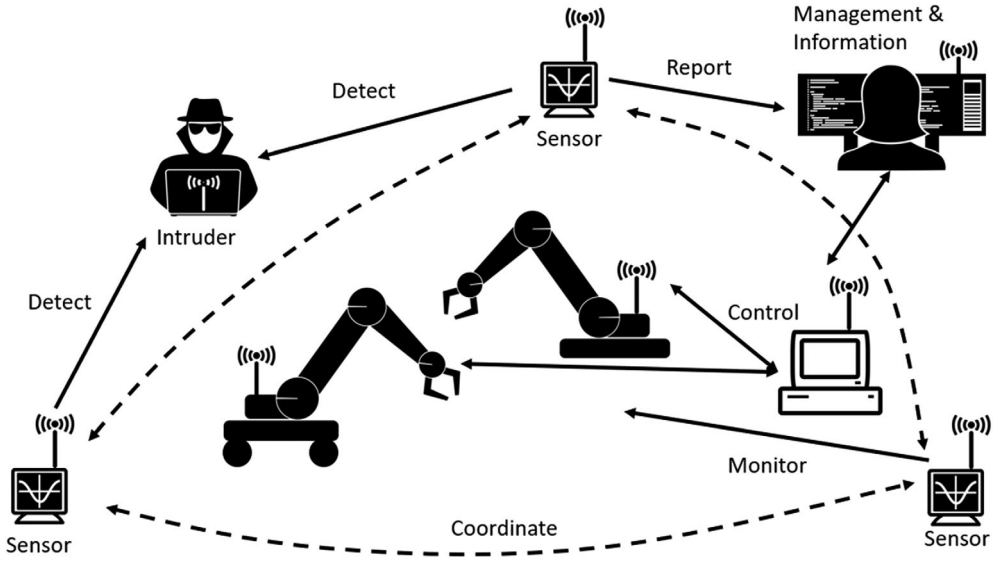

FIGURE 4 Monitoring a smart manufacturing system aids resilience through situational awareness.

6.6 | The resilience of the deployed smart manufacturing system

After digital manufacturing systems are deployed, their lifetime performance is an aspect of the resilience and cyber-resilience goal. They need to be monitored and maintained to ensure the designed performance level is maintained and any external interference is detected. Sensors can monitor the CPPS with the data feeding into analysis and visualization systems, see Figure 4. ML/AI can be used to aid human monitoring for potential issues, automating the analysis of various data streams when helping to identify degradation in performance or cyber threats.

The sections above have discussed some of the technologies focused on improving the functionalities and capabilities of a production process. The process improvements themselves will contribute to addressing some of the resilience factors listed in Section 4. However, specific consideration of the resilience aspects within the CPPS design objectives, whilst challenging, would improve the overall production and organizational resiliency goals. The resilience objectives should include cyber-resilience objectives to mitigate cyber-attacks.

7 | DISCUSSION

There is a requirement for new applied research targeting how digital technologies can measurably improve resilience in manufacturing processes. Research would increase the understanding of the concept of resilience in manufacturing by moving from a qualitative to a more beneficial quantitative focus. Work should examine which specific technologies (Section 6) can be used to improve a resilience factor (Section 4). Plus, research can address ways to measure the overall improvement in resilience, building upon existing work (Yarveisy et al., 2020) to develop suitable industrial resilience metrics. The goal is to provide manufacturers with examples of how to make quantitative gains in overall resilience. Furthermore, researching new resilience knowledge for manufacturing systems will help address the skills gap in RE at micro and meso levels. Although organizations are addressing skills needed to build smart manufacturing systems (Azmat et al., 2020), additional skills for specific technologies to address resilience factors, for example, cyber-resilience techniques or advanced wireless communications, would be beneficial.

Some frameworks support implementing a CPPS, for example, the Smart InforMation PLatform and Ecosystem for manufacturing (SIMPLE) (Harrison et al., 2021), a modular software platform used to develop smart manufacturing applications. SIMPLE can be enhanced to include functionality that targets improvements in resilience. The connectivity layer could be improved with the application of high-performance 5G wireless communications, thereby providing process designers with additional options to add new adaptable and flexible system use cases. These use cases include DT capabilities and enhancements to data handling (processing, storage, and visualization). Another addition to SIMPLE would be to add cyber-resilience to the existing software modules and layers, incorporating modules dedicated to cybersecurity monitoring.

Finally, the new digital manufacturing systems are primarily designed to implement novel processes and to improve existing profitability via improvements in efficiency and productivity. However, there is a new societal focus on achieving sustainability within the industrial sector (United Nations, n.d.; European Commission Directorate-General for Research and Innovation, 2021). If resilience is a consideration when designing a CPPS, it contributes to those societal goals and aids the driving of innovation in factory machinery and processes, waste and materials consumption reduction, improvement of employee experience, and cybersecurity threat reduction, all aiding economic growth.

8 | CONCLUSION

We addressed the objective to provide a holistic view of manufacturing resilience by collating its different aspects (Figure 2) and meaning.

Further, we discussed how digital manufacturing technologies underpinning a CPPS could aid or detract from resilience. The aim of this holistic view of smart manufacturing resilience is to provide a basis for future research and commentary.

8.1 | Academic implications

It is understandable that non-functional properties of a system have a lower priority during a system life cycle. There is a role for University research to address the quantitative measurements of resilience and its factors, and the application of such measurements to demonstrably improve the assessment of industrial resilience. At WMG, our industrial test beds are used to research these challenges. Such research will inform the teaching of the next generation of engineers and managers on resilient smart manufacturing and its wider societal considerations.

8.2 | Managerial implications

Although we found that resilience can be applied to different levels (macro, meso, and micro) within the industrial domain, the new digital technologies are, initially, likely to have the biggest impact on resilience at the micro level, that is, within individual facilities. Managers and executives can concentrate on improving their organization's resilience, and the related supply chains. In doing so, it will contribute to the overall resilience of an economy. To raise resilience, some areas for focus would be on challenges around handling the additional complexity of smart systems, skilling and re-skilling employees, support for legacy machinery, deployment and use of DTs, the use of advanced wireless communications, and addressing cybersecurity. It was noted that the performance of any deployed smart system, sitting alongside the process it is augmenting, needs life cycle consideration through the use of appropriate monitoring and data visualization tools.

8.3 | Limitations and further avenues of research

It is acknowledged the breadth of the topics addressed has limited the depth of some of the analyses. However, it provides a starting point to investigate quantitatively the previously separated aspects of smart manufacturing resilience. There are opportunities for organizations to contribute to the understanding of these aspects. In particular, how the incorporation of measurable resilience factors can be incorporated into system design tools and process frameworks used to roll out smart manufacturing systems.

ACKNOWLEDGMENTS

This work was funded by the High Value Manufacturing Catapult, project number 8261.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no data sets were generated or analyzed during the current study.

ORCID

Daniel S. Fowler https://orcid.org/0000-0001-6730-2802

REFERENCES

acatech (Ed.). (2011). *Cyber-physical systems, driving force for innovation in mobility, health, energy and production* (tech. Rep.). National Academy of Science and Engineering. Springer Verlag. https://doi.org/10.1007/978-3-642-29090-94

Alderson, D. L., Brown, G. G., Carlyle, W. M., & Cox, L. A. (2013). Sometimes there is no "Most-vital" arc: Assessing and improving the operational resilience of systems. *Military Operations Research*, *18*(1), 21–37.

Azmat, F., Ahmed, B., Colombo, W., & Harrison, R. (2020). Closing the skills gap in the era of industrial digitalisation. In *2020 IEEE conference on industrial Cyberphysical systems (ICPS)* (Vol. 1, pp. 365–370). IEEE. https://doi.org/10.1109/ICPS48405.2020.9274788

Baumann, C., Cherry, M., & Chu, W. (2019). Competitive Productivity (CP) at macro–meso–micro levels. *Cross Cultural & Strategic Management*, *26*(2), 118–144. https://doi.org/10.1108/CCSM-08-2018-0118

Bhattacharyya, S. (1998). The international Warwick manufacturing group. *Assembly Automation*, *18*(2). https://doi.org/10.1108/aa.1998.03318baa.002

Caralli, R. A., Allen, J. H., White, D. W., Young, L. R., Mehravari, N., & Cutis, P. D. (2016). *CERT Resilience Management Model, version 1.2* (tech. rep.). Carnegie Mellon Software Engineering Institute.

de Bodt, E., Cousin, J.-G., & Dupire-Declerck, M. (2021). The CSR supply chain risk management hypothesis evidence from the suez canal ever given obstruction. *SSRN*. https://doi.org/10.2139/ssrn.3867169

European Commission Directorate-General for Research and Innovation. (2021). *Industry 5.0: Towards a sustainable, human-centric and resilient European industry* (tech. rep.). Publications Office of the European Union. https://doi.org/10.2777/308407

Freeman, R., & Varga, L. (2021). Analysis of resilience situations for complex engineered systems—The resilience holon. *IEEE Systems Journal*, *1–12*, 2265–2276. https://doi.org/10.1109/JSYST.2021.3100286

Grimaila, M. R., Mills, R. F., Haas, M., & Kelly, D. (2010). *Mission assurance: Issues and challenges* (tech. rep.). Air Force Inst of Tech Wright-Patterson AFB OH Center for Cyberspace Research.

Gu, X., Jin, X., Ni, J., & Koren, Y. (2015). Manufacturing system design for resilience. *Procedia CIRP*, *36*, 135–140. https://doi.org/10.1016/j.procir.2015.02.075

Harrison, R., Vera, D. A., & Ahmad, B. (2021). A connective framework to support the lifecycle of cyber–physical production systems. *Proceedings of the IEEE*, *109*(4), 568–581. https://doi.org/10.1109/JPROC.2020.3046525

ISO. (2014). *ISO/IEC 15408-1:2009(E) Information technology—Security techniques—Evaluation criteria for IT Security* (tech. rep.). International Organization for Standardization.

ISO. (2019). *ISO 22301:2019 Security and resilience—Business continuity management systems—Requirements*.

Kagermann, H., Wahlster, W., & Helbig, J. (2013). *Securing the future of German manufacturing industry: Recommendations for implementing the strategic initiative INDUSTRIE 4.0* (tech. rep.). National Academy of Science and Engineering.

Kott, A., & Linkov, I. (Eds.). (2019). *Cyber resilience of systems and networks*. Springer International Publishing.

Kusiak, A. (2020). Resilient manufacturing. *Journal of Intelligent Manufacturing*, *31*(2), 269. https://doi.org/10.1007/s10845-019-01523-7

Lalli, V. R. (1998). Space-system reliability: A historical perspective. *IEEE Transactions on Reliability*, *47*, SP355–SP360. https://doi.org/10.1109/24.740551

Leiva, C. (2022). First principles of smart manufacturing. *Journal of Advanced Manufacturing and Processing*, *4*, 1–11. https://doi.org/10.1002/amp2.10123

Maurer, F., & Schumacher, J. (2018). Organizational robustness and resilience as catalyst to boost innovation in smart service factories of the future. In *2018 IEEE international conference on engineering, technology and innovation (ICE/ITMC)*. IEEE. https://doi.org/10.1109/ICE.2018.8436364

Mbah, R. E., & Wasum, D. (2022). Russian-Ukraine 2022 war: A review of the economic impact of russianukraine crisis on the USA, UK, Canada, and Europe. *Advances in Social Sciences Research Journal*, *9*(3), 144–153. https://doi.org/10.14738/assrj.93.12005

McCarthy, I. P., Collard, M., & Johnson, M. (2017). Adaptive organizational resilience: An evolutionary perspective. *Current Opinion in Environmental Sustainability*, *28*, 33–40. https://doi.org/10.1016/j.cosust.2017.07.005

Meyer, T., von der Gracht, H. A., & Hartmann, E. (2020). How organizations prepare for the future: A comparative study of firm size and industry. *IEEE Transactions on Engineering Management*, *69*, 511–523. https://doi.org/10.1109/TEM.2020.2992539

MITRE. (2023). *Mitre att&ck*. https://attack.mitre.org/

O'Reilly, C. A., & Tushman, M. L. (2004). The ambidextrous organization. *Harvard Business Review*, *82*(4), 74–83.

Oxford University Press. (2021). *Oxford English Dictionary (OED)*. https://www.oed.com/

Pankratz, N., & Schiller, C. (2021). Climate change and adaptation in global supply-chain networks. In *Proceedings of Paris December 2019 finance meeting EUROFIDAI-ESSEC, European Corporate Governance Institute—Finance working paper, (775)*. Elsevier. https://doi.org/10.2139/ssrn.3475416

Peisert, S., Schneier, B., Okhravi, H., Massacci, F., Benzel, T., Landwehr, C., Mannan, M., Mirkovic, J., Prakash, A., & Michael, J. B. (2021). Perspectives on the solarwinds incident. *IEEE Security & Privacy*, *19*(2), 7–13. https://doi.org/10.1109/MSEC.2021.3051235

Remko, V. H. (2020). Research opportunities for a more resilient post-covid-19 supply chain—Closing the gap between research findings and industry practice. *International Journal of Operations & Production Management*, *40*(4), 341–355.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (tech. rep.). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1

Suresh, N. C., Sanders, G. L., & Braunscheidel, M. J. (2020). Business continuity management for supply chains facing catastrophic events. *IEEE Engineering Management Review*, *48*(3), 129–138. https://doi.org/10.1109/EMR.2020.3005506

Thoma, K. (2014). *Resilien-Tech. Resilience by design: A strategy for the technology issues of the future*. acatech—National Academy of Science and Engineering.

Thoma, K., Scharte, B., Hiller, D., & Leismann, T. (2016). Resilience engineering as part of security research: Definitions, concepts and science approaches. *European Journal for Security Research*, *1*(1), 3–19. https://doi.org/10.1007/s41125-016-0002-4

Tomiyama, T., & Moyen, F. (2018). Resilient architecture for cyber-physical production systems. *CIRP Annals*, *67*(1), 161–164. https://doi.org/10.1016/j.cirp.2018.04.021

United Nations. (n.d.). *Sustainable development goals*. https://sdgs.un.org/goals

Voas, J., Kshetri, N., & DeFranco, J. F. (2021). Scarcity and global insecurity: The semiconductor shortage. *IT Professional*, *23*(5), 78–82. https://doi.org/10.1109/MITP.2021.3105248

Wang, B., Tao, F., Fang, X., Liu, C., Liu, Y., & Freiheit, T. (2021). Smart manufacturing and intelligent manufacturing: A comparative review. *Engineering*, *7*(6), 738–757. https://doi.org/10.1016/j.eng.2020.07.017

Weber, A., & Thomas, R. (2005). *Key performance indicators, measuring and managing the maintenance function* (tech. rep.). Ivara Corporation.

Wied, M., Oehmen, J., & Welo, T. (2020). Conceptualizing resilience in engineering systems: An analysis of the literature. *Systems Engineering*, *23*(1), 3–13. https://doi.org/10.1002/sys.21491

Yarveisy, R., Gao, C., & Khan, F. (2020). A simple yet robust resilience assessment metrics. *Reliability Engineering & System Safety*, *197*, 106810. https://doi.org/10.1016/j.ress.2020.106810

Zhang, W., & van Luttervelt, C. (2011). Toward a resilient manufacturing system. *CIRP Annals*, *60*(1), 469–472. https://doi.org/10.1016/j.cirp.2011.03.041

AUTHOR BIOGRAPHIES

Daniel S. Fowler transitioned from a long career designing and delivering successful industrial and business computer-based systems to research, obtaining a Ph.D. in cybersecurity. His research field is in secure systems and resilient design. He has aided the delivery of several security projects funded by Innovate UK. He is a Chartered Engineer and a member of the IET and ACM.

Gregory Epiphaniou is an Associate Professor of security engineering at the University of Warwick. His role involves bid support, applied research and publications. Part of his current research activities is formalised around cyber effects modelling, wireless communications with the main focus on crypto-key generation, exploiting the time-domain physical attributes of V-V channels and cyber resilience. He led and contributed to several research projects funded by EPSRC, IUK and local authorities totalling over £4M. He currently holds a subject matter expert panel position in the Chartered Institute for Securities and Investments. He acts as a technical committee member for several scientific conferences in Information and network security and served as a key member in the development of WS5 for the formation of the UK Cybersecurity Council.

Matthew D. Higgins received his MEng in Electronic and Communications Engineering and his PhD in Engineering from the School of Engineering at the University of Warwick. He progressed through several Research Fellow positions, in association with some of the UK's leading defence and telecommunications companies. He set up the Vehicular Communications Research Laboratory which aimed to enhance the use of communications systems within the vehicular Space. He leads the Connectivity and Communications Technology Research Group within WMG. He is a Senior Member of the IEEE (SMIEE), a member of the IEEE Communications Society (COMSOC), and a Fellow of the Higher Education Academy (FHEA). He is also a member of the Commnet2 community. He is a regular reviewer of leading international journals and frequently serves for key COMSOC conferences. He is a Member of the EPSRC Peer Review College.

Carsten Maple is a Professor of Cyber Systems Engineering at the University of Warwick, the Principal Investigator for its NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research, and Deputy Pro-ViceChancellor for North America. He has provided evidence and advice to governments and organisations across the world. He is a member of various national and international boards and expert groups and is a fellow of the Alan Turing Institute.

How to cite this article: Fowler, D. S., Epiphaniou, G., Higgins, M. D., & Maple, C. (2023). Aspects of resilience for smart manufacturing systems. *Strategic Change*, 1–11. https://doi.org/10.1002/jsc.2555