Received November 17, 2017, accepted December 15, 2017, date of publication December 22, 2017,
date of current version February 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2786240

Robustness of Smart Manufacturing Information Systems under Conditions of Resource Failure: A Complex Network Perspective

ZHITING SONG[1], YANMING SUN[2], HEHUA YAN[3], DINGJUAN WU[4], PENG NIU[1], AND XIANGMIAO WU[5]

[1]School of Business Administration, South China University of Technology, Guangzhou 510641, China
[2]School of Business, Guangzhou University, Guangzhou 510006, China
[3]School of Electrical Engineering, Guangdong Mechanical and Electrical College, Guangzhou 510515, China
[4]School of Health Management, Guangzhou Medical University, Guangzhou 510000, China
[5]School of Computing Science and Engineering, South China University of Technology, Guangzhou 510641, China

Corresponding author: Hehua Yan (hehua_yan@126.com)

This work was supported in part by the Natural Science Foundation of China under Grant 71571072, Grant 71071057, and Grant 51208454, in part by the Department of Science and Technology of Guangdong Province under Grant 2014B090901001 and Grant 2015B010103002, in part by the Natural Science Foundation of Guangdong Province, China, under Grant 2015A030313746, in part by the Science and Technology Planning of Guangdong Province under Grant 2016B010108009, and in part by the Research Fund Program of Guangdong Provincial Key Laboratory of Computer Integrated Manufacturing under Grant CIMSOF2016004.

ABSTRACT Resource failures frequently occur in a smart manufacturing information system (SMIS), which exerts significant impacts on the robustness of the system. From a complex network perspective, this paper develops a fresh methodology for analyzing the robustness of an SMIS suffering from resource failures. First, this methodology divides an SMIS into cyber and physical layers, dissects the resources within these layers and the relationships among these resources. Based on complex network thinking, the methodology then builds a network model incorporating different failure modes and link patterns. Finally, extensive simulations are performed using the case of an appliance manufacturer and one of its suppliers. The results show that an SMIS, along with its cyber layer, exhibits the property of being robust-yet-fragile, and that an assortative link pattern is the optimal link pattern to guarantee robustness for the SMIS under targeted failures.

INDEX TERMS Robustness, smart manufacturing, information system, resource failure, complex network.

I. INTRODUCTION

In recent years, manufacturing intelligence has gradually integrated with traditional manufacturing, bringing about an advanced manufacturing paradigm known as smart manufacturing (SM) [1]. Many national manufacturing strategies, such as ‘‘Industry 4.0’’, ‘‘Made in China 2025’’ and ‘‘Industrial Internet’’, give priority to SM. According to research by Smart Manufacturing Leadership Coalition (SMLC) [2], SM is and will continue to be the mainstream manufacturing mode in the 21st century, being driven by disruptive technologies, such as big data [3]–[6], cyber-physical systems [7], [8], cloud computing [9], [10] and network technologies [11], [12]. With the purpose of integrating decentralized resources to fulfill dynamic and diverse customer demands, SM emphasizes vertical integration within enterprises, horizontal integration among enterprises, and end-to-end integration in the same value chain surrounding the product lifecycle [13], [14]. To realize the above integrations, enterprise information systems belonging to different enterprises need to be interconnected to support the provision of products and services. When all enterprise information systems in the same value chain are interconnected, a smart manufacturing information system (SMIS) is created.

Traditional information systems are composed of terminals, servers, software, network communication devices, data, processes, and people [15]. Most of these elements exist only in cyberspace. In contrast, an SMIS not only contains the above elements from multiple enterprises but also incorporates a vast number of additional devices (e.g., digital cameras and machines) from physical space, as well as the plentiful software and data residing on these devices [16], as shown in Fig.1. For various reasons, such as hostile environments and prolonged operations, resource failures can occur gradually or abruptly. With the increasing

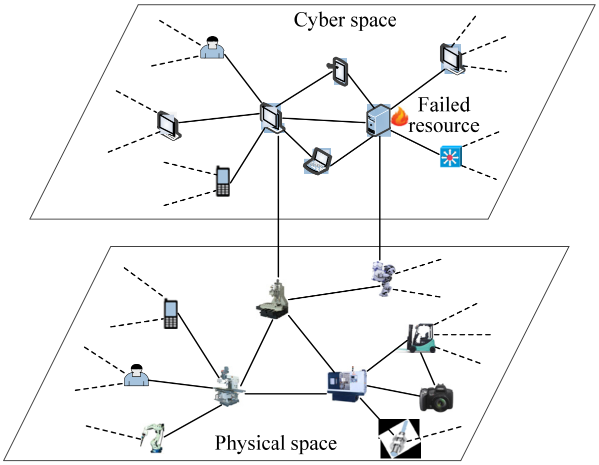


FIGURE 1. A schematic diagram of an SMIS.

use of devices in the physical space of an SMIS, such failures become more serious. Once a resource fails, it may induce abnormal operations in neighboring resources, followed by cascading failures, which could finally cause a widespread outage. In Fig. 1, if the server fails, the terminals cannot access data from the server, and the robot cannot offload its storage and computing processes to the server, leading to the ineffective operations of both the terminals and robot. In time, the neighbors of these devices are affected, eventually causing the failure of system functions and the exponential growth of risk. Thus, robustness is vital for any SMIS, especially when resources frequently fail.

Since the development of SMISs is still at an early stage, existing research mainly focuses on the front-end lifecycles (e.g., system implementation and ICT adoption) of SMISs and hardly involves their robustness. This paper devises a methodology to analyze the robustness of an SMIS from a complex network perspective. The methodology decomposes an SMIS into two interconnected layers and introduces three link patterns between these layers, which underlies the formation of a network model of an SMIS. The methodology also considers and models four kinds of resource failures, then describes the robustness of an SMIS under each failure mode.

The neoteric aspects in this research are: (1) In terms of system modeling, this paper adopts complex network thinking to establish a network model for an SMIS, which fills gaps in the current research marked by the structural modeling in the design phase of an SMIS; (2) In terms of robustness, this paper quantitatively analyzes the robustness of an SMIS affected by resource failures, which presents a novel attempt to address robustness at the root of an SMIS. Our methodology synthesizes previous research on network robustness to provide a pragmatic framework for analyzing robustness under conditions of resource failure.

The remainder of the paper is organized as follows: Section II reviews the relevant literature. Section III describes a network model for an SMIS and simulations of different resource failures. Section IV presents a numerical analysis of how resource failures influence the robustness of an SMIS. Finally, Section V gives our conclusions.

II. LIRERATURE REVIEW

Two streams of literature are relevant to our research. The first stream regards SMISs, and the second relates to the metrics of network robustness.

The research on SMISs approaches the field from several perspectives. Li *et al.* [17] constructed a three-level framework to integrate wireless networks and cloud services into information systems. Kadiri *et al.* [18] proposed some strategies for information systems supported by advanced ICT technologies, such as big data. Fayoumi [19] presented an ecosystem-inspired modeling framework to design collaborative and networked manufacturing systems. Papazoglou *et al.* [20] established a reference architecture for devising highly-connected smart manufacturing networks. Lu and Cecil [21] outlined an internet of things-based framework for collaborative manufacturing systems. Yang *et al.* [22] designed a new tabular document exchange method to implement semantic interoperability in heterogeneous information systems. Tao and Qi [23] put forward a framework to support the adoption of new ICT and service-oriented technologies. González-Rojas and Ochoa-Venegas [24] excogitated a decision-making model to assess and manage the implementation of information systems. Niemimaa [25] emphasized that the social part of information systems should be valued and provided some conceptual foundations to address the social part during the lifecycle of information systems. In summary, the above research has mainly focused on the front-end lifecycle of information systems but barely on system robustness, though robustness is critical for an SMIS.

To analyze network robustness in a quantitative manner, many metrics have emerged, but there is no unified measurement system. Robustness metrics proposed in the literature include geometric connectivity [26], assortativity [27], endurance [28], natural connectivity [29], information entropy [30], giant components [31], the proportion of failed nodes [32], the proportion of failed edges [33], global efficiency [34], reliability and average degree [35], algebraic connectivity [36], degree diversity [37], clustering coefficient [38], and betweenness centrality [39]. Of these metrics, global efficiency assumes that two nodes transfer data through the shortest path to minimize data-transfer time and an SMIS should be designed to quickly provide information to users. This high correspondence motivates us to adopt global efficiency to quantify the robustness of an SMIS.

III. MODEL

A. NETWORK STRUCTURE OF SMIS

In SM, information systems break through traditional cyberspace and gradually extend to physical space. Thus, the structure of an SMIS can be divided into a cyber structure and a physical structure.

Resources in the cyber layer of an SMIS cover cyber-layer devices (e.g., servers, routers, and laptops), software, data, and people. The relationships among these four kinds of resources are that software and data reside on cyber-layer devices, some of which collaborate with people. As such, we view cyber-layer devices and people as cyber entities that synergistically handle business data within the scope of traditional enterprise informatization, the data from the external internet (e.g., social media data), and the data collected from devices in the physical layer. After processing, these entities send feedback to the physical and decision-making layers. Here, we treat each cyber entity as a node and the cooperative relationship between two cyber entities as an edge. The network structure of the cyber layer of an SMIS can be represented by:

$$G_c = (V_c, E_c) \tag{1}$$

where $V_c = \{v_{c1}, v_{c2}, \ldots, v_{cn}\}$ and $E_c = \{e_{cij} | e_{cij} \in (0, 1), 1 \leq i \neq j \leq n\}$ represent the sets of nodes and edges, respectively, in the cyber layer. Here,$e_{cij} = 1$ indicates that there exists an edge between nodes v_{ci} and v_{cj} while $e_{cij} = 0$ indicates no edge.

Resources in the physical layer of an SMIS contain physical-layer devices (e.g., robots, sensors, and cameras), software, data, and people. For the same reason as the cyber layer, we consider physical-layer devices and people as physical entities, which collaboratively produce and collect the data mirroring the states of the devices and products (e.g., work conditions and environmental parameters), and become new elements of an information system by connecting with the cyber layer. Similarly, we view physical entities as nodes (supposing that the number of the nodes in a cyber layer equals that in the physical layer) and the relationship between two physical entities as an edge. The network structure of the physical layer of an SMIS is denoted as:

$$G_p = (V_p, E_p) \tag{2}$$

where $V_p = \{v_{p1}, v_{p2}, \ldots, v_{pn}\}$ and $E_p = \{e_{pij} | e_{pij} \in (0, 1), 1 \leq i \neq j \leq n\}$ represent the sets of nodes and edges, respectively, in the physical layer. Similarly, $e_{pij} = 1$ signifies that there exists an edge between nodes v_{pi} and v_{pj} while $e_{pij} = 0$ signifies no edge.

Driven by various cutting-edge technologies, such as the internet of things and cyber-physical systems, physical entities can link to cyber entities. This paper considers three common link patterns which are depicted as follows:

1) Random link (RL). Randomly select a node v_{ci} in network G_c and a node $v_{pj}(1 \leq i, j \leq n)$ in network G_p. If v_{ci} has no link with other nodes in G_p and v_{pi} has no link with other nodes in G_c, then connect v_{ci} with v_{pi}; otherwise, do not connect. Repeat this process until the degree of the whole network increases by $2np$, where p denotes the link strength between the cyber and physical layers.
2) Assortative link (AL). Sort the nodes of G_c according to the descending order of the node degree, marked as $v_{cd1}, v_{cd2}, \ldots, v_{cdn}$. If two or more nodes have the same degree, randomly rank them. Sort the nodes of G_p in the same manner, marked as $v_{pd1}, v_{pd2}, \ldots, v_{pdn}$. Randomly choose a node $v_{cdi}(1 \leq i \leq n)$ in G_c, then connect node v_{cdi} with node v_{pdi} in G_p. Repeat this process until the degree of the whole network increases by $2np$.
3) Disassortative link (DL). Arrange the nodes in G_c and G_p in the same manner as AL. Randomly select a node $v_{cdi}(1 \leq i \leq n)$ in G_c, then connect node v_{cdi} with node $v_{pd(n+1-i)}$ in G_p. Repeat this process until the degree of the whole network increases by $2np$.

B. RESOURCE FAILURE MODELING

An SMIS is a networked system that covers many cyber and physical entities. Through mutual collaboration, these entities convert data into information, information into knowledge, and knowledge into actions through decision-making. In a dynamic and uncertain SM environment, the entities may fail in a gradual or sudden way. The failures either hinder the entities from realizing their functions or destroy the collaborative relationships among the entities, finally impairing the robustness of the SMIS. The factors inducing resource failures can be roughly divided into two categories, which are random and intended attacks. Random attacks refer to random adverse causes, such as extreme environments and human errors, and are of two types: attacks against an entity or the relationship between two entities. Intended attacks are goal-directed interference, such as purposive physical attacks, and are also of two types: attacks against the entity that has the maximum number of links with other entities or against the relationship between two entities that has the largest link product.

Attacking an entity causes it to lose operational capacity, which is modeled as the removal of the corresponding node from the network structure of an SMIS. Attacking the relationship between two entities allows the entities to operate but causes their collaboration to fail, which is modeled as the removal of the corresponding edge. In accordance with the above four types of attacks, the entities in an SMIS can have four failure modes, which are modeled as follows:

1) Random node failure (RNF). Randomly select and remove a node in G (which denotes the network structure of an SMIS).
2) Random edge failure (REF). Randomly select and remove an edge in G.
3) High degree failure (HDF). Select and remove the node with the largest degree in G.
4) Degree product failure (DPF). Select and remove the node with the largest degree product in G. We calculate the degree product of an edge by multiplying the degrees of the two nodes at the ends of the edge with each other.

Failed nodes or edges cannot continue transferring data. The less time the remaining nodes take to transfer data to the targeted node, the more robust is the network. This paper assumes that the shortest time to transfer data between

TABLE 1. Basic statistical features of networks G_c and G_p.

	G_c	G_p
Number of nodes	100	100
Number of edges	159	200
Average degree	3.1800	4.0000
Average path length	3.6574	3.9115
Clustering coefficient	0.0783	0.2219
Power exponent	2.6249	—

two entities is proportional to the length of the shortest path between them. In this case, global efficiency E is an excellent metric for the robustness of network G:

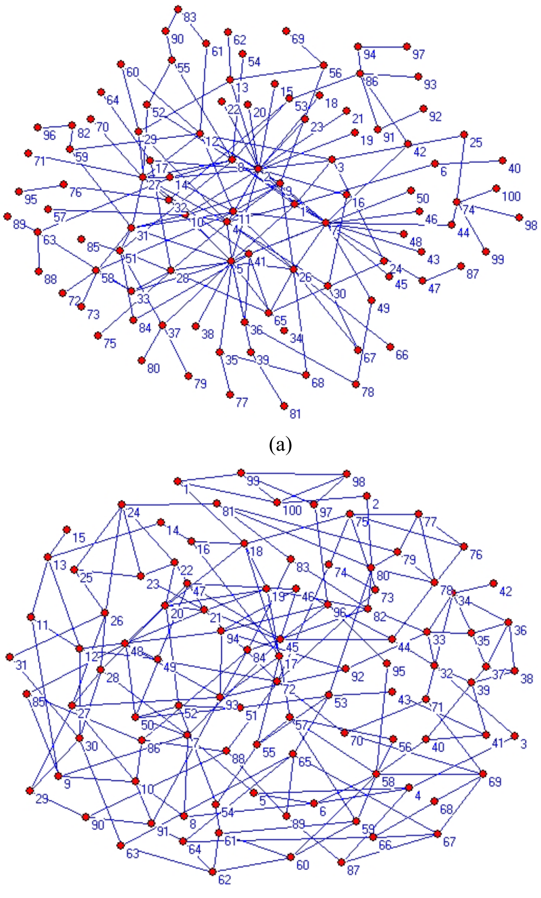
$$E = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \tag{3}$$

where N denotes the number of nodes in network G. Parameter d_{ij} represents the length of the shortest path between nodes i and j. If there are no paths between nodes i and j, then $d_{ij} = \infty$.

IV. SIMULATIONS

This section describes the simulations of an appliance manufacturer and one of its suppliers. This cooperative unit gives priority to SM and focuses on strengthening the intelligence related to product development, manufacturing, decision-making, logistics, services, etc. On the information level, the promotion of intelligence in the above aspects relies heavily on the capacities of the inter-organizational information system (which is an SMIS), which supports the cooperative unit in intelligently acquiring and handling data. Practical investigations show that resource failures occur frequently. Based on the business processes of the cooperative unit, we were able to obtain the relationships among the resources within the cyber and physical layers, as well as the cyber and physical entities. Before establishing the network structure G, we preprocessed the entities as follows: treat redundant entities and entities that merely have relationships of parallel, sequential or exclusive operations as the same node. After preprocessing, the number of nodes in both layers satisfies $N_c = N_p = 100$. The topologies of the layers (i.e., networks G_c and G_p) were generated using Pajek, as shown in Fig. 2. Since the development of SM in the cooperative unit is still in its infancy, the connections between G_c and G_p are very imperfect. To facilitate our work, we neglect the existing connections and apply the three common link patterns.

This paper first analyzes some basic statistical features of G_c and G_p, as shown in Table 1. The power-law exponent of G_c is 2.6249, denoting that G_c is a scale-free network (where a few nodes have many links and most nodes have few links) and exhibits power-law degree distribution. However, the degree distribution of G_p is relatively uniform and does not conform to a power-law distribution. The average path length of G_c and G_p is small, but G_p has a greater clustering coefficient than does G_c, indicating that the degree of the aggregation of the nodes in G_p is higher.



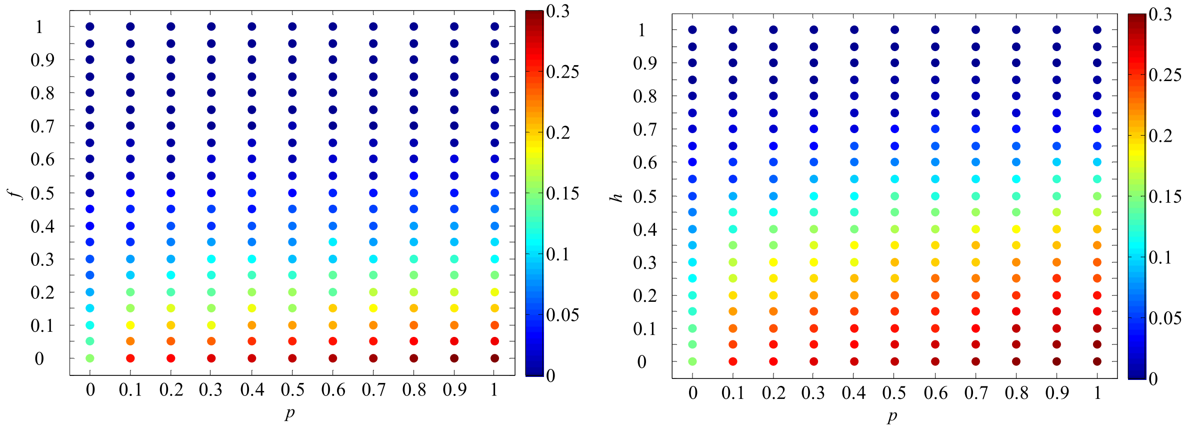
(a)

(b)

FIGURE 2. The topologies of the cyber and physical layers in the SMIS. (a) Network G_c. (b) Network G_p.

Understanding the basic features of G_c and G_p is beneficial to analyzing the robustness of the SMIS when resources fail. Let parameters f and h represent the proportion of failed nodes and edges, respectively. To explore how p, f and h influence the robustness (i.e., E) of the SMIS, we establish two panoramas, as shown in Fig. 3. Each point represents a value of E, and the color represents the exact value of E under the corresponding condition. E can be seen to be positively correlated with p but negatively with f or h. The positive (negative) relation weakens when p (f or h) increases. The details of the above two panoramas are presented in Fig. 4, which also shows that the value of E tends to be stable and is hardly subjected to p when f reaches 0.7 or h reaches 0.8. It should be noted that, without loss of generality, the link pattern between G_c and G_p, in this case, is RL and the failure mode is random failure.

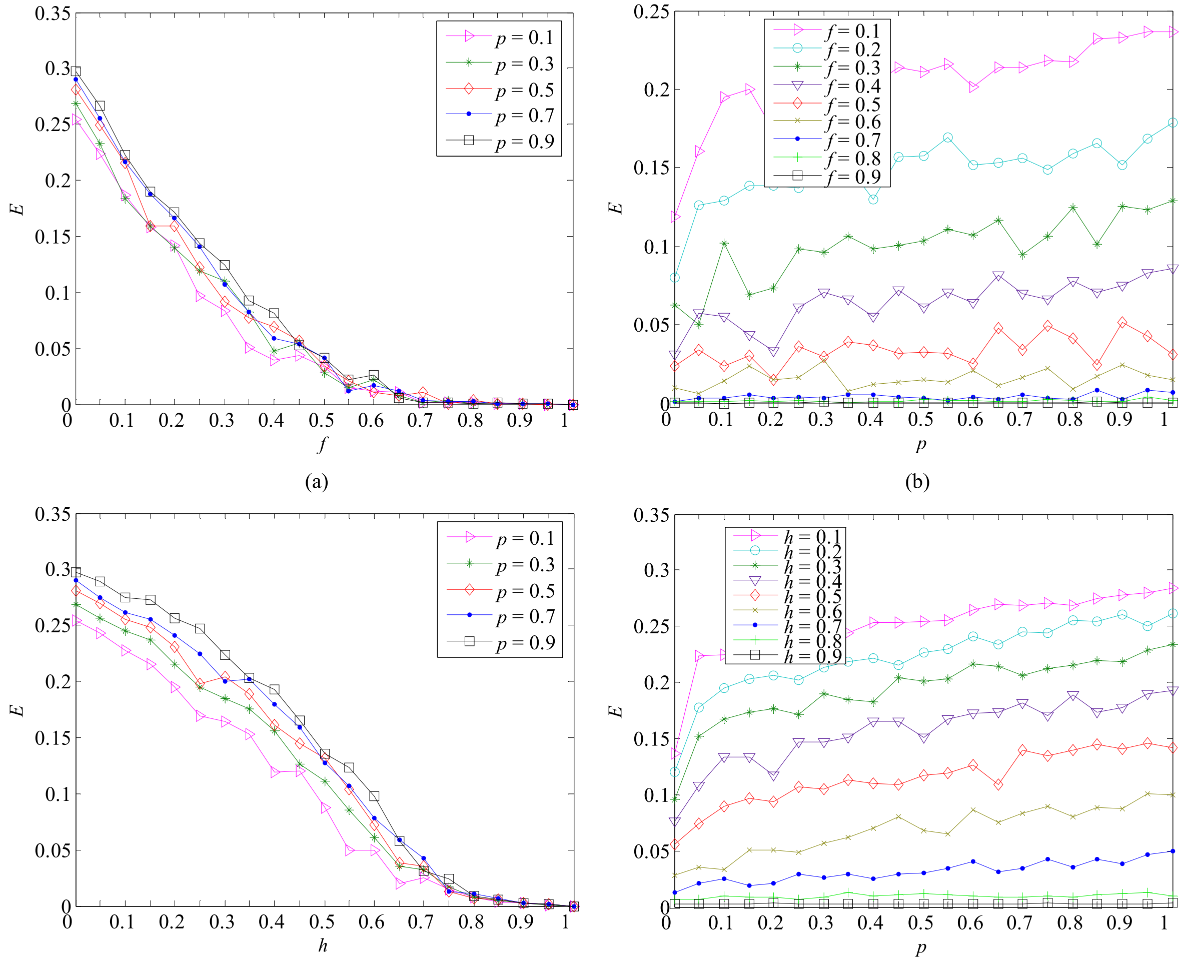
To investigate how E varies by different link patterns and failure modes, let $p = 0.7$. Based on previous analysis, let f and h range within intervals [0, 0.7] and [0, 0.8], respectively. Fig. 5 shows that E changes according to different link patterns and failure modes. From Fig. 5(a), we can see that, on the one hand, under the same link pattern, the robustness is weaker (i.e., the value of E is smaller) under HDF than



(a)

(b)

FIGURE 3. The effects of multiple parameters on *E*: (a) *p* and *f*, (b) *p* and *h*.



(a)

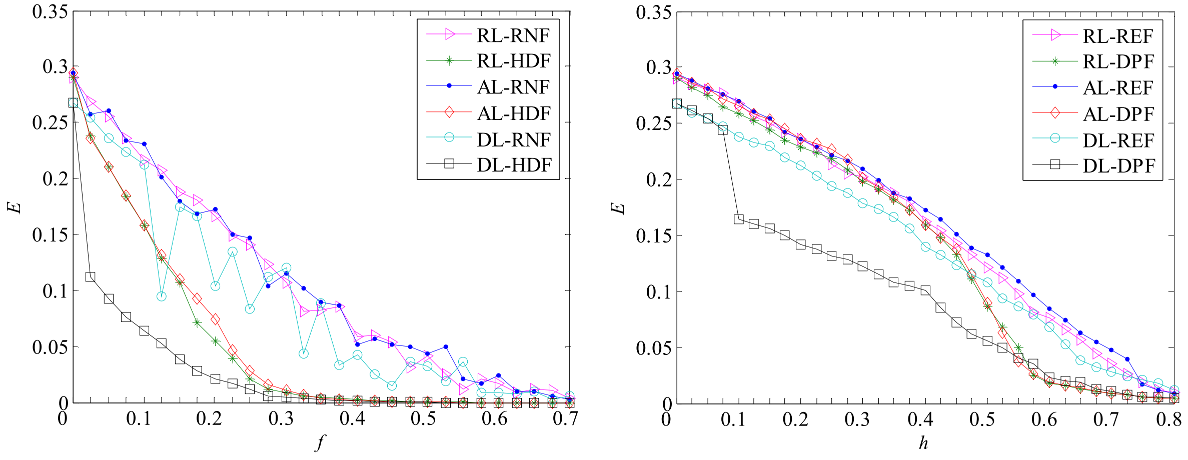
(b)

(c)

(d)

FIGURE 4. The effects of a single parameter on *E*: (a) *f* with fixed *p*, (b) *p* with fixed *f*, (c) *h* with fixed *p*, and (d) *p* with fixed *h*.

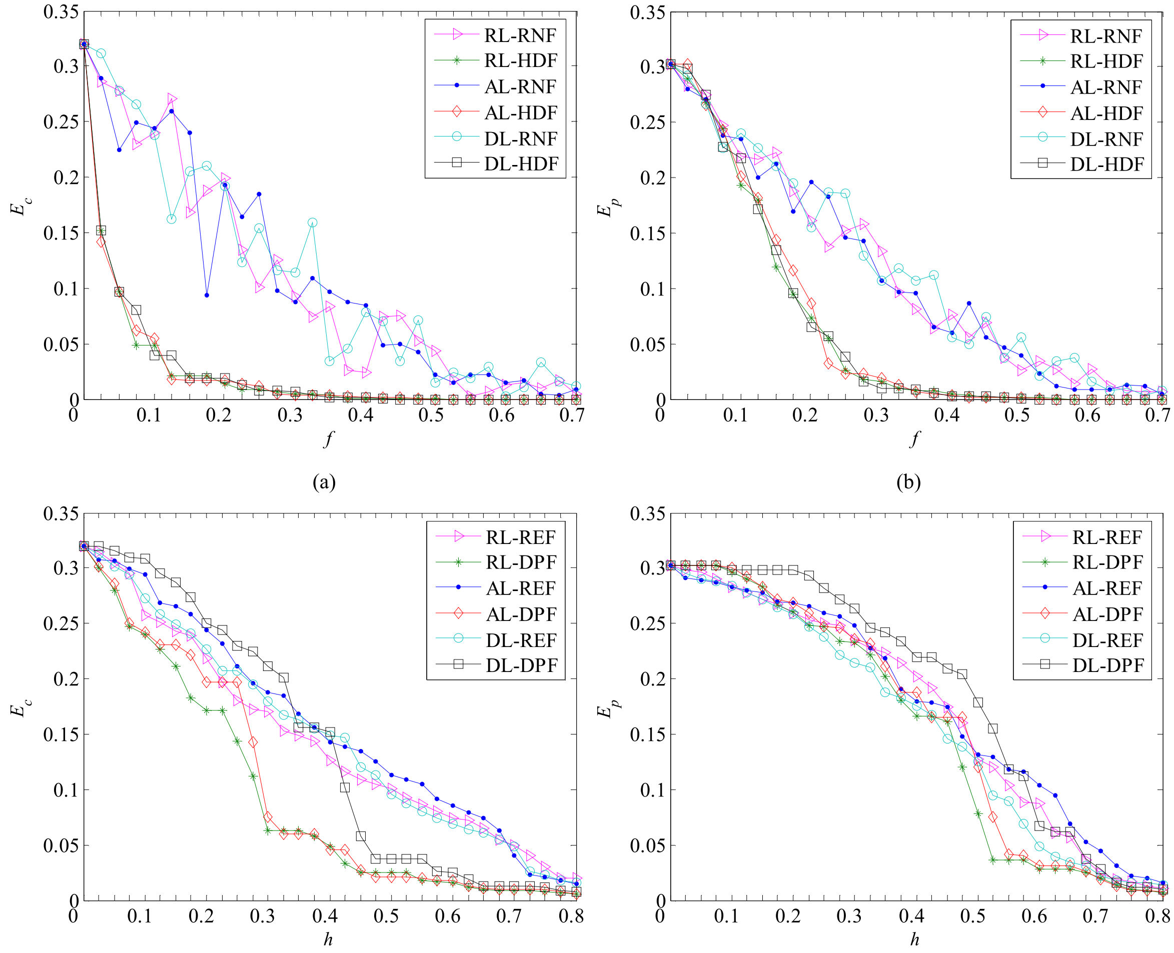
under RNF, denoting that the SMIS has the properties of being robust-yet-fragile and heterogeneous. The reason for this outcome is: 1) The basic features calculated in Table 1 reveal that the degree distribution is extremely non-uniform in G_c but relatively uniform in G_p. When f is small, the randomly failed nodes have small degrees



(a)

(b)

FIGURE 5. The effects of different link patterns and failure modes on E when $p = 0.7$: three link patterns (RL, AL, and DL) and (a) two node failure modes (RNF and HDF), and (b) two edge failure modes (REF and DPF).



(a)

(b)

(c)

(d)

FIGURE 6. The effects of the three link patterns (RL, AL, and DL) and failure modes on E_c and E_p: (a) node failure modes, RNF and HDF, on E_c, and (b) E_p; (c) edge failure modes, REF and DPF, on E_c, and (d) E_p.

and are randomly distributed across G_c and G_p. The failures of these nodes affect system robustness slightly; therefore, the SMIS is robust under RNF. 2) Due to the heterogeneity of G_c, a few nodes have high degrees and their failure could seriously impair the robustness of G_c and have a great impact on E. Thus, the SMIS is fragile under HDF. Fig. 6(a) and Fig. 6(b) illustrate the above explanation.

On the other hand, affected by HDF, E tends to be stable when f reaches 0.3 and the order of the optimal link pattern is AL $>$ RL $>$ DL. The reason for this outcome is, under HDF, the same number of failed nodes destroys the most direct connections under DL, followed by RL and AL. Thus, AL is the best for improving robustness.

In Fig. 5(b), we can see that, under the same link pattern, the values of E under different failure modes differ slightly from each other when $h \leq h_{t1}$ or $h \geq h_{t2}$ (where h_{t1} equals 0.325, 0.275, and 0.075 under RL, AL and DL, respectively, and $h_{t2} = 0.8$). Moreover, when $h_{t1} < h < h_{t2}$, the value of E is smaller under DPF than under REF. The reason for this outcome is: 1) Under RL and AL, the damage that REF and DPF exert on G_c and G_p, respectively, meet conditions REF $>$ DPF and REF $<$ DPF when $h \leq h_{t1}$. These two failure modes have nearly equal effects on E, as shown in Fig. 6(c) and Fig. 6(d). Under DL, different failure modes slightly damage connectivity when $h \leq 0.075$. When $h \geq h_{t2}$, connectivity suffers huge damage regardless of the failure modes and link patterns. Therefore, E under REF and DPF approximates. 2) Compared to REF, DPF destroys connectivity to a larger extent when $h_{t1} < h < h_{t2}$. Thus, the SMIS is more fragile under DPF. Moreover, Fig. 5(b) reveals that the order of the optimal link pattern under DPF is AL $=$ RL $>$ DL when $h < 0.8$. The main reason for this priority is, under DL, DPF primarily attacks the edges between G_c and G_p, then those within both layers. However, DPF primarily attacks the edges outside G_p, then within G_p under the remaining two link patterns, as shown in Fig. 6(c) and Fig. 6(d). Obviously, the order of edge failure under DL-DPF could impair robustness more quickly than under AL-DPF or RL-DPF. By comparing Fig. 5(a) and Fig. 5(b), we find that node failures impact system robustness to a larger degree than do edge failures. This result is intuitive.

Faced with node failures, E_c and E_p (i.e., the robustness of G_c and G_p) do not significantly vary by link patterns, and the robust-yet-fragile property is significant in G_c, as shown in Fig. 6(a) and Fig. 6(b). Due to the differences between G_c and G_p, HDF first makes E_c decline sharply but markedly impacts E_p only when f increases to a certain value. However, E_c and E_p under DPF significantly vary by link patterns, which is very different from under HDF. To be specific, compared to RL and AL, DL under DPF can preferentially protect the edges within G_c and G_p from failures. Thus, DL is best for the resistance of G_c and G_p against DPF, as shown in Fig. 6(c) and Fig. 6(d). Moreover, under DPF, more edges in G_c than in G_p fail when h is small. As a result, the declining rate of E_c is higher than that of E_p. It should be noted that DL is best for G_c and G_p against DPF, but causes the biggest damage to the SMIS.

V. CONCLUSIONS

From a complex network perspective, this paper describes a novel methodology to quantitatively examine the robustness of SMIS experiencing resource failures. The analysis of system elements and modeling of resource failures underlie the formation of a network model for an SMIS, by which we analyze how different failure modes and link patterns affect robustness. The results of the simulations indicate that, for an SMIS, especially its cyber layer, with the properties of being robust-yet-fragile and heterogeneous, AL is the best link pattern against targeted failures. In addition, node failures have greater impact on robustness than do edge failures. These findings are conducive to the front-end design and the back-end control of an SMIS.

Despite the advantages of our research, there exists one primary limitation. Our network model specifically views the links among entities as bidirectional while real-world information systems contain many unidirectional links. Therefore, it is significant to develop more practical network models that take unidirectional links into account. This will be the priority for our future research.

REFERENCES

[1] J. Davis, T. Edgar, J. Porter, J. Bernaden, and M. Sarli, "Smart manufacturing, manufacturing intelligence and demand-dynamic performance," *Comput. Chem. Eng.*, vol. 47, pp. 145–156, Dec. 2012.

[2] Smart Manufacturing Leadership Coalition (SMLC). (Jun. 24, 2011). *Implementing 21st Century Smart Manufacturing*. [Online]. Available: https://smartmanufacturingcoalition.org/reading-materials

[3] J. Wan *et al.*, "A manufacturing big data solution for active preventive maintenance," *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 2039–2047, Aug. 2017.

[4] W. Yuan, P. Deng, T. Taleb, J. Wan, and C. Bi, "An unlicensed taxi identification model based on big data analysis," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 6, pp. 1703–1713, Jun. 2016.

[5] Y. Xu, Y. Sun, J. Wan, X. Liu, and Z. Song, "Industrial big data for fault diagnosis: Taxonomy, review, and applications," *IEEE Access*, to be published, doi: 10.1109/ACCESS.2017.2731945.

[6] J. Xiong, Q. Zhang, J. Wan, L. Liang, P. Cheng, and Q. Liang, "Data fusion method based on mutual dimensionless," *IEEE/ASME Trans. Mechatronics*, to be published, doi: 10.1109/TMECH.2017.2759791.

[7] Z. Shu, J. Wan, D. Zhang, and D. Li, "Cloud-integrated cyber-physical systems for complex industrial applications," *Mobile Netw. Appl.*, vol. 21, no. 5, pp. 865–878, Oct. 2016.

[8] J. Wan, D. Zhang, Y. Sun, K. Lin, C. Zou, and H. Cai, "VCMIA: A novel architecture for integrating vehicular cyber-physical systems and mobile cloud computing," *Mobile Netw. Appl.*, vol. 19, no. 2, pp. 153–160, 2014.

[9] Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, "Security in software-defined networking: Threats and countermeasures," *Mobile Netw. Appl.*, vol. 21, no. 5, pp. 764–776, Oct. 2016.

[10] J. Wan, S. Tang, Q. Hua, D. Li, C. Liu, and J. Lloret, "Context-aware cloud robotics for material handling in cognitive industrial Internet of Things," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2017.2728722.

[11] X. Li, D. Li, J. Wan, A. V. Vasilakos, C.-F. Lai, and S. Wang, "A review of industrial wireless networks in the context of industry 4.0," *Wireless Netw.*, vol. 23, no. 1, pp. 23–41, Jan. 2017.

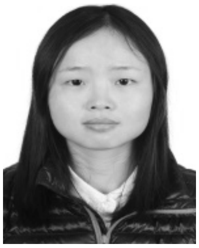
[12] J. Wan *et al.*, "Software-defined industrial Internet of Things in the context of industry 4.0," *IEEE Sensors J.*, vol. 16, no. 20, pp. 7373–7380, Oct. 2016.

[13] S. Wang, J. Wan, M. Imran, D. Li, and C. Hua, "Cloud-based smart manufacturing for personalized candy packing application," *J. Supercomput.*, to be published, doi: 10.1007/s11227-016-1879-4.

[14] Z. Song, Y. Sun, J. Wan, L. Huang, and Y. Xu, "Exploring robustness management of social internet of things for customization manufacturing," *Future Generat. Comput. Syst.*, to be published, doi: 10.1016/j.future.2017.10.030.

[15] D. Romero and F. Vernadat, "Enterprise information systems state of the art: Past, present and future trends," *Comput. Ind.*, vol. 79, pp. 3–13, Jun. 2016.

[16] R. Agarwal and A. Tiwana, "Editorial-evolvable systems: Through the looking glass of IS," *Inf. Syst. Res.*, vol. 26, no. 3, pp. 473–479, Sep. 2015.
[17] S. Li, L. Xu, X. Wang, and J. Wang, "Integration of hybrid wireless networks in cloud services oriented enterprise information systems," *Enterprise Inf. Syst.*, vol. 6, no. 2, pp. 165–187, May 2012.
[18] S. El Kadiri *et al.*, "Current trends on ICT technologies for enterprise information systems," *Comput. Ind.*, vol. 79, pp. 14–33, Jun. 2016.
[19] A. Fayoumi, "Ecosystem-inspired enterprise modelling framework for collaborative and networked manufacturing systems," *Comput. Ind.*, vol. 80, pp. 54–68, Aug. 2016.
[20] M. P. Papazoglou, W.-J. van den Heuvel, and J. E. Mascolo, "A reference architecture and knowledge-based structures for smart manufacturing networks," *IEEE Softw.*, vol. 32, no. 3, pp. 61–69, May/Jun. 2015.
[21] Y. Lu and J. Cecil, "An internet of things (IoT)-based collaborative framework for advanced manufacturing," *Int. J. Adv. Manuf. Technol.*, vol. 84, nos. 5–8, pp. 1141–1152, May 2016.
[22] S. Yang, J. Guo, and R. Wei, "Semantic interoperability with heterogeneous information systems on the internet through automatic tabular document exchange," *Inf. Syst.*, vol. 69, pp. 195–217, Sep. 2017.
[23] F. Tao and Q. Qi, "New IT driven service-oriented smart manufacturing: Framework and characteristics," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published, doi: 10.1109/TSMC.2017.2723764.
[24] O. González-Rojas and L. Ochoa-Venegas, "A decision model and system for planning and adapting the configuration of enterprise information systems," *Comput. Ind.*, vols. 92–93, pp. 161–177, Nov. 2017.
[25] M. Niemimaa, "Information systems continuity process: Conceptual foundations for the study of the 'social,'" *Comput. Secur.*, vol. 65, pp. 1–13, Mar. 2017.
[26] O. A. Osman and S. Ishak, "A network level connectivity robustness measure for connected vehicle environments," *Transp. Res. C, Emerg. Technol.*, vol. 53, pp. 48–58, Apr. 2015.
[27] D. Shizuka and D. R. Farine, "Measuring the robustness of network community structure using assortativity," *Animal Behaviour*, vol. 112, pp. 237–246, Feb. 2016.
[28] M. Manzano, E. Calle, V. Torres-Padrosa, J. Segovia, and D. Harle, "Endurance: A new robustness measure for complex networks under multiple failure scenarios," *Comput. Netw.*, vol. 57, no. 17, pp. 3641–3653, Dec. 2013.
[29] G.-S. Peng and J. Wu, "Optimal network topology for structural robustness based on natural connectivity," *Phys. A, Statist. Mech. Appl.*, vol. 443, pp. 212–220, Feb. 2016.
[30] T. A. Schieber, L. Carpi, A. C. Frery, O. A. Rosso, P. M. Pardalos, and M. G. Ravetti, "Information theory perspective on network robustness," *Phys. Lett. A*, vol. 380, no. 3, pp. 359–364, Jan. 2016.
[31] X.-J. Zhang, G.-Q. Xu, Y.-B. Zhu, and Y.-X. Xia, "Cascade-robustness optimization of coupling preference in interconnected networks," *Chaos, Solitons Fractals*, vol. 92, pp. 123–129, Nov. 2016.
[32] J. Liu, Q. Xiong, X. Shi, K. Wang, and W. Shi, "Robustness of complex networks with an improved breakdown probability against cascading failures," *Phys. A, Statist. Mech. Appl.*, vol. 456, pp. 302–309, Aug. 2016.
[33] J. Wang, Y. Li, and Q. Zheng, "Cascading load model in interdependent networks with coupled strength," *Phys. A, Statist. Mech. Appl.*, vol. 430, pp. 242–253, Jul. 2015.
[34] Z. Zhao, P. Zhang, and H. Yang, "Cascading failures in interconnected networks with dynamical redistribution of loads," *Phys. A, Statist. Mech. Appl.*, vol. 433, pp. 204–210, Sep. 2015.
[35] X. Wang, Y. Koç, S. Derrible, S. N. Ahmad, W. J. A. Pino, and R. E. Kooij, "Multi-criteria robustness analysis of metro networks," *Phys. A, Statist. Mech. Appl.*, vol. 474, pp. 19–31, May 2017.
[36] J. Martín-Hernández, H. Wang, P. Van Mieghem, and G. D'Agostino, "Algebraic connectivity of interdependent networks," *Phys. A, Statist. Mech. Appl.*, vol. 404, pp. 92–105, Jun. 2014.
[37] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, "Resilience of the Internet to random breakdowns," *Phys. Rev. Lett.*, vol. 85, no. 21, pp. 4626–4628, Nov. 2000.
[38] W. K. Ghamry and K. M. F. Elsayed, "Network design methods for mitigation of intentional attacks in scale-free networks," *Telecommun. Syst.*, vol. 49, no. 3, pp. 313–327, Mar. 2012.
[39] E. Estrada, "Network robustness to targeted attacks. The interplay of expansibility and degree distribution," *Eur. Phys. J. B-Condens. Matter Complex Syst.*, vol. 52, no. 4, pp. 563–574, Aug. 2006.



ZHITING SONG received the B.A. degree in industrial engineering from East China Jiaotong University, China, in 2013. She is currently pursuing the Ph.D. degree with the School of Business Administration, South China University of Technology, China. Her research interests include smart manufacturing, cyber-physical systems, information systems, and complex systems.

YANMING SUN is currently a Professor with the School of Business, Guangzhou University, China. He has directed over 20 research projects, including the National Natural Science Foundation of China. He has authored or co-authored over 120 scientific papers. His research interests are information systems, smart manufacturing, big data, complex systems, and fault diagnosis.

HEHUA YAN is currently an Associate Professor with the School of Electrical Engineering, Guangdong Mechanical and Electrical College, China. She has directed three research projects, including the National Science Foundation of Guangdong Province. She has authored or co-authored over 20 scientific papers. Her research interests include embedded systems, Internet of Things, and cyber-physical systems.

DINGJUAN WU received the Ph.D. degree from the South China University of Technology, China, in 2016. She is currently a Lecturer with the School of Health Management, Guangzhou Medical University, China. She has authored over ten scientific papers. Her research interests include complex systems, integration system of informatization and industrialization, smart manufacturing, and complex network.

PENG NIU received the B.A. degree from the Henan University of Economics and Law. She is currently pursuing the Ph.D. degree with the School of Business Administration, South China University of Technology, China. Her research interests are smart manufacturing systems, complex network, and fault diagnosis.

XIANGMIAO WU was born in China, in 1975. He is currently a Senior Engineer with the School of Computing Science and Engineering, South China University of Technology, China. He has authored or co-authored over 20 papers. His research interests include computer applications, Internet of Things, intelligent transportation, embedded systems, and welding automation.