Computers & Industrial Engineering 206 (2025) 111177

Contents lists available at ScienceDirect

Computers & Industrial Engineering

journal homepage: www.elsevier.com/locate/caie

Modeling and analysis of cascade failures in Industrial Internet of Things based on task decomposition and service communities

Lingli Zhu [a], Xiuwen Fu [b], Xiangwei Liu [b], Shichang Du [c,*]

[a] Institute of Logistics Science and Engineering, Shanghai Maritime University, Shanghai 201306, China
[b] Logistics Engineering College, Shanghai Maritime University, Shanghai 201306, China
[c] Department of Industrial Engineering and Management, Shanghai Jiao Tong University, Shanghai 200240, China

ARTICLE INFO

Keywords:
Industrial Internet of things
Cascade failures
Service community
Task decomposition
Interdependent network model

ABSTRACT

In Industrial Internet of Things (IIoT) systems, the overload of certain nodes may lead to the failure of the entire network, a phenomenon known as cascade failures. This occurrence has an immeasurable impact on industrial production. Establishing a realistic IIoT cascade failure model is crucial for enhancing the cascade reliability of IIoT systems. However, existing research on cascade failures in IIoT lacks an in-depth exploration of the actual characteristics in industrial scenarios, hindering accurate modeling of the cascade failure process in IIoT. To better characterize the cascade failure process of IIoT, this study proposes an interdependent network model from a cyber-service coupling perspective, considering task decomposition, service community structure, and coupling patterns. On this basis, we design a realistic cascade failure model that is based on production supply relationships between manufacturing units. In the experiments, we first validate the rationality of the proposed model through load distribution and load probability density analysis. Furthermore, the study of key modeling parameters then reveals that cyber network attacks cause more damage than service network attacks. Finally, we apply the model to four industrial manufacturing scenarios and explore their cascade failure performance.

1. Introduction

With the evolution of economic globalization and industrial integration towards digitization, the Industrial Internet of Things (IIoT) has experienced rapid development, revolutionizing industrial production and operational modes (Coito et al., 2022). IIoT shows great potential in intelligent manufacturing by integrating various communication devices and industrial assets (such as machines and control systems), monitoring, collecting, exchanging, and analyzing information generated by devices, performing production tasks (Ali & Khan, 2022). In IIoT systems, when a node or device fails, it may subsequently trigger failures in other nodes or devices. These initial failures may be caused by various factors, including technical issues, human errors, natural disasters, or deliberate attacks (Zhong & Liu, 2024). Many instances highlight the potential threat of cascade failures. For example, the German Federal Office for Information Security (BSI) reported a case where a cyber attack disrupted the production network of a steel plant (Lin, Wu, & Lee, 2017). The cyber attack caused the core data processing node to fail, forcing data to be rerouted to other nodes. The high data volume caused these nodes to become overloaded and eventually fail. This disrupted the production data needed for the rolling process, resulting in equipment malfunctions. Since the rolling equipment is closely related to other production steps, the failure spread throughout the production chain, halting the rolling services. Under the influence of cascade failures, the failure of a small number of nodes may lead to the paralysis of the entire IIoT system. Therefore, cascade failures are considered one of the major bottlenecks affecting IIoT reliability.

Currently, there is a wealth of research on cascade failures in the Internet of Things (IoT), but these studies primarily focus on general types of IoT systems (Yang et al., 2022; Zhao, Sun, & Liu, 2024). In general IoT systems, node devices are usually sensor nodes with wireless communication capabilities that do not perform additional tasks beyond data collection and forwarding (Gulati et al., 2022). However, in IIoT systems, node devices are intelligent manufacturing units with communication, sensing, and processing capabilities. On the one hand, these intelligent manufacturing units need to establish end-to-end communication with other units to achieve real-time sharing and interaction of manufacturing process data, forming a visible cyber network. On the other hand, these units also need to collaborate and share resources based on service production supply relationships, forming a tightly connected service network. The dual role of intelligent manufacturing units as both information forwarders and service participants leads to a tight coupling between the cyber network and the service

* Corresponding author.
E-mail address: lovbin@sjtu.edu.cn (S. Du).

https://doi.org/10.1016/j.cie.2025.111177
Received 27 June 2024; Received in revised form 31 December 2024; Accepted 25 April 2025
Available online 26 May 2025
0360-8352/© 2025 Elsevier Ltd. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

network. This tight coupling enables IIoT systems to flexibly and intelligently accomplish production tasks, but it also significantly increases the sensitivity of the entire system to cascade failures. This is because, influenced by the cyber-service coupling characteristics of IIoT, cascade failures not only propagate along the direction of information transmission or along the direction of production chains horizontally, but also propagate between the cyber network and the service network vertically, resulting in failure propagation across layers.

Existing research on cascade failures in IIoT primarily focuses on the single-component level, which is limited to understanding the relationships between components and the probabilities of failure occurrence (Li, Cheng, & Tao, 2020; Lv, Wu, Zhang, Jiang, & Gao, 2022). However, these analytical methods lack a comprehensive consideration of overall system functionality. To better understand cascade failures in IIoT systems, it is essential to consider not only component-level failures but also their impact on the entire service production process. Although some researchers have constructed cascade failure models for IIoT systems from the cyber-service coupling perspective, in addition to conducting cascade failure analysis at the system component level but also explored the interdependencies between the cyber network and the service network. However, these models are still too simplistic compared to real-world IIoT systems, due to three key limitations: (1) insufficient definition of the service community structure within the service production chain; (2) inadequate characterization of the characteristics of task decomposition in the manufacturing process; (3) incomplete characterization of the complex coupling between the cyber network and the service network. These limitations hinder the accurate modeling of cascade failures in IIoT systems. Therefore, this paper proposes a new IIoT cascade failure model based on task decomposition and service communities, focusing on system reliability in the context of cascade failures. Our main contributions are as follows:

- Modeling IIoT as a cyber-service interdependent network. In this model, the cyber network is modeled as a hierarchical architecture. Nodes in the service network are divided by functional type, forming distinct service communities. The mutual dependency between cyber nodes and service nodes is modeled as multiple coupling relationships, including one-to-many, many-to-one, and one-to-one.
- Establishing a cascade failure model to describe the cascade failure propagation process in IIoT. In our model, the load of cyber nodes is represented by data flows generated by themselves or routed, while the load of service nodes is represented by the number of decomposed sub-tasks. The load update of service nodes is divided into within-community and cross-community. In this model, cascade failures can propagate horizontally within the same-layer network and through cross-layer interdependent edges.
- Through experimental simulations, we analyze the load distribution characteristics of the cyber network and the service network, validating the rationality of the proposed system model. Additionally, we explore the impact of modeling parameters on the cascade reliability of IIoT. Finally, using the proposed modeling approach, we analyze cascade reliability performance in four typical industrial manufacturing scenarios.

The remainder of the paper is organized as follows. Section 2 reviews related research. Section 3 introduces the interdependent network model of IIoT. Section 4 describes the IIoT cascade failure model in detail. Section 5 presents simulation experiment results and case studies. Finally, Section 6 concludes the main findings and indicates future research directions.

2. Literature review

System reliability is one of the most prominent concerns in the technology and application domains of IIoT. However, research on cascade failures within IIoT is relatively scarce. Therefore, this section first reviews research on cascade failures in general IoT and then outlines research on cascade failures in IIoT.

2.1. Cascade failures in general IoT

IoT is a data-centric network self-organized via multi-hop relay transmission of nodes. Its load distribution is highly susceptible to internal and external factors such as node energy depletion, wireless interference, hardware/software malfunctions, and malicious intrusions (Liang, Parlikad, Srinivasan, & Rasmekomen, 2017). In many practical scenarios, the node capacity of IoT is strictly limited, and nodes are prone to overload due to data overflow. Once a node becomes overloaded, the data stream on these overloaded nodes will choose a new route for data delivery. During the load redistribution process, new overloaded nodes may be triggered, leading to another round of load redistribution. This continuous process of node failures is a typical cascade failure process. Cascade failures are considered one of the main bottlenecks to IoT reliability, and many scholars have conducted in-depth research on it from various perspectives.

Yin, Liu, Liu, and Li (2014) introduced a cascade failure model for IoT based on the degree of sensor nodes, where node load is exponentially determined by its own degree. On this basis, they explored the relationship between node critical load and the largest connected component in the network. Zhao et al. (2024) developed a multi-state cascade failure model for IoT and investigated the impact of initial disturbance and a total number of nodes on the scale of cascade failures in IoT. Yang et al. (2022) studied the cascade failure process in heterogeneous IoT under selective attack strategies based on percolation theory. Ye, Wen, Liu, Song, and Fu (2016) analyzed the reliability of scale-free IoT to cascade failures using the probability generating function method. Simulation results demonstrate that the scale of the cascade failure is positively correlated with the power-law exponent of scale-free networks. Xing, Morrissette, and Dugan (2014) modeled the cascade failure behavior of IoT mesh storage area networks using dynamic fault trees and discussed the cascade reliability of IoT systems with functional dependencies and incomplete coverage. Zhao and Xing (2020) established a probabilistic function dependency-based cascade failure model for IoT and utilized a combined hierarchical approach to analyze the cascade reliability of IoT under stochastic fault propagation. In Fu, Wang, Yang, and Postolache (2022), we proposed a congestion-driven cascade failure model for edge-computing IoT and investigated how the data processing and compression capabilities of edge computing nodes affect the cascade failure process of the network. In Fu, Pace, Aloi, Li, and Fortino (2021), we developed a routing-driven cascade failure model. Numerous experiments demonstrate that compared to the global routing mode, networks utilizing the local routing mode exhibit higher cascade reliability.

2.2. Cascade failures in IIoT

The IIoT is an application and extension of the IoT tailored for the industrial field. Compared to general IoT, IIoT node devices are responsible not only for data forwarding but also for production tasks. As an important branch of IoT systems, research on cascade failures of IIoT is still in its initial stage. Zhang, Guo, Qian, and Li (2018) introduced the concept of “IoT manufacturing” and designed an IIoT architecture focusing on proactive sensing during the manufacturing process. In their study, they explicitly defined the collaborative interaction between production information and manufacturing services in IIoT systems, emphasizing that cyber-service coupling is crucial for the efficient operation of IIoT. Li et al. (2020) explored six possible types of failures in manufacturing service collaboration within IIoT and analyzed the cascading propagation process of different failures. Cheng, Gao, Wang, Tao, and Wang (2023) considered the discreteness, dynamics, and uncertainties of IIoT platforms and proposed a graph-based reliability analysis method for Manufacturing Service Collaboration

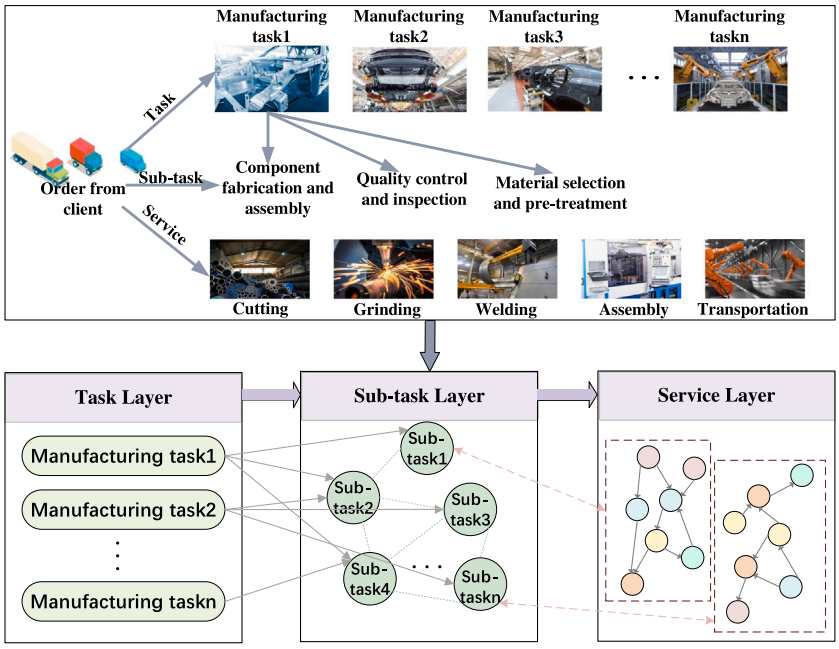


Fig. 1. Decomposition structure based on aggregated manufacturing tasks.

(MSC) in IIoT platforms. In Fu, Pace, et al. (2023), we established an IIoT cascade failure model from the cyber-service coupling perspective, taking into account that nodes in IIoT serve as both data forwarders and service providers. In Fu, Li, and Li (2023), fully considering the routing-driven characteristics of the cyber network and the selective load distribution characteristics of the service network, we further improved the cyber-service coupling IIoT cascade failure model and validated the rationality of the proposed model through case studies.

From the above description, it is easy to see that existing research on cascade failures in IoT mainly focuses on general IoT systems, where the IoT node can only be considered a data collection and forwarding device. These research findings are not applicable to IIoT due to its cyber-service coupling characteristic. In addition, although a few researchers have recognized the cyber-service coupling characteristics of IIoT systems and have conducted cascade failure studies, the real characteristics of IIoT (such as service community structure, task decomposition, and diverse cross-network coupling relationships) have not been accurately depicted. These limitations have resulted in existing research failing to accurately characterize the true cascade failure process in IIoT systems.

3. Cyber-service interdependent network model

3.1. Cyber network

The cyber network in the IIoT is a distributed network composed of cyber nodes and their communication links. To better meet the data processing needs at various levels, the cyber network in the IIoT adopts a hierarchical architecture. Based on functional differences, the nodes of the cyber network can be divided into three types: terminal nodes, routing nodes, and gateway nodes. In the IIoT system, terminal nodes cannot directly communicate with each other but with routing nodes. Each terminal node needs to establish a communication link with only one routing node. Routing nodes can establish communication links with each other and some routing nodes are also capable of establishing communication links with gateway nodes.

In our model, we use $G_C = \{V_C, E_C\}$ to represent the cyber network. $V_C = \{p_i | i = 1, 2, \ldots, N_C\}$ is the set of cyber nodes, and N_C is the total number of cyber nodes. $E_C = \{a_{i,j} = 1, 0 \mid i, j \in V_C\}$ is the set of communication links between cyber nodes. There are no communication links between terminal nodes. The communication links between terminal nodes and routing nodes are directed. If terminal node p_i transmits sensing data to routing node p_j, then $a_{i,j} = 1$. The communication links between routing nodes are undirected. If routing node p_i communicates with routing node p_j, then $a_{i,j} = 1$. The communication links between routing nodes and gateway nodes are also undirected. If there is a communication link between routing node p_i and gateway node p_j, then $a_{i,j} = 1$. If cyber node p_i does not communicate with cyber node p_j, then $a_{i,j} = a_{j,i} = 0$.

3.2. Service network

In practical industrial scenarios, when a factory receives user requirements, it distributes them to workshops, generating multiple orders accordingly, and then organizing them into an aggregated manufacturing task set. Each task can be further decomposed into subtasks, with each corresponding to a specific operation in production (Ren, Luo, Li, Xing, & Xiang, 2022). To complete these subtasks, manufacturing capabilities, processing costs, and quality standards must be considered. Based on these criteria, appropriate manufacturing units are matched to each subtask, operating under system-defined scheduling and optimization rules for efficient collaboration. The task decomposition structure based on aggregated manufacturing tasks is shown in Fig. 1. It is worth noting that these manufacturing units with specific functions exist in the service network in a community structure, where service nodes with similar functions are grouped into the same service communities. Although service nodes within the same community have identical functions, they perform different production tasks, allowing them to act as independent service units and form production dependencies within the same chain. Nodes within the same community are connected by undirected similarity edges, which allow tasks to be transferred from failed nodes to normal nodes and transmit the compensatory loads of the production tasks taken over by the normal nodes back to failed nodes, maintaining the basic service function of failed nodes.

In our model, we use $G_S = \{V_S, C_S, E_S^m, E_S^{m,n}\}$ to represent the service network. $V_S = \{s_i \mid i = 1, 2, \ldots, N_S\}$ is the set of service nodes, and N_S is the total number of service nodes. $F_S = \{f_S^m \mid m = 1, 2, \ldots, N_C\}$ is the set of service communities, and N_F is the total number of service communities. The functional attribute of service nodes is represented

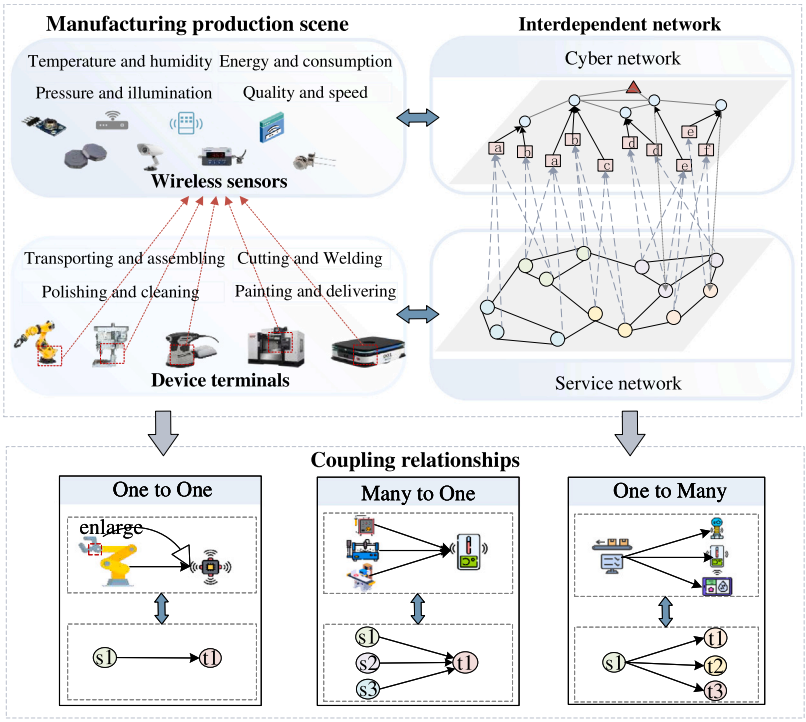


Fig. 2. Interdependent network model of IIoT based on cyber-service coupling.

by $w^{s_i} = [\alpha_1^{s_i}, \alpha_2^{s_i}, \ldots, \alpha_M^{s_i}]$, indicating the relationship between service node s_i and service community. If the function of service node s_i is m, meaning that service node s_i belongs to service community f_S^m, which is denoted as $\alpha_m^{s_i} = 1$. $f_S^m = \{s_i \mid \alpha_m^{s_i} = 1, i = 1, 2, \ldots, N_S\}$ is the set of service nodes contained in the same service community. $E_S^m = \{e_{i,j} = 0, 1 \mid i, j \in s_i\}$ is the set of undirected similarity edges within the same service functional community. $E_S^{m,n} = \{e_{m,n} = 0, 1 | m, n \in V_S\}$ is the set of directed service production dependency edges connecting service nodes s_m and s_n. If the output of service node s_m is the input of service node s_n, then $e_{m,n} = 1$. If there is no production-supply relationships between service node s_m and service node s_n, then $e_{m,n} = 0$.

3.3. Interdependent network

In our model, the directed edge from the service node to the cyber node represents the collection of production data from the service node by the terminal node, while the directed edge from the cyber node to the service node denotes scheduling instructions issued by the cyber node. To address dynamic task demands, terminal nodes and service nodes exhibit diverse coupling patterns: one-to-one, one-to-many, and many-to-one. One-to-one coupling enables direct communication between specific equipment and control systems for high customization and real-time response, as in a sensor on a robotic arm exchanging data with its control system for precise control. One-to-many coupling distributes data from a single source to multiple manufacturing units, ideal for applications like quality control, such as a temperature sensor sharing data with both inspection units and manufacturing units. Many-to-one coupling integrates data from multiple sources to govern a single service node, as in packaging production where multiple sensors (e.g., weight, temperature, humidity) are combined to ensure product quality. Therefore, in modeling of IIoT, we should account for these diverse coupling patterns.

In our model, we use $G_{CS} = \{G_C, G_S, E_{CS}\}$ to represent the interdependent network, where G_C is the cyber network and G_S is the service network. Considering the interaction between cyber nodes and service nodes in the IIoT, we use $E_{CS} = [c_{i,j}]_{N_C \times N_S}$ to represent the set of interdependent edges between the cyber network and the service network. If service node s_i provides production data to terminal node p_j, then $c_{i,j} = 1$. If cyber node p_j issues scheduling instructions to service node s_i, then $c_{j,i} = 1$. The interdependent IIoT model we proposed is shown in Fig. 2.

4. Cascade failures model for IIoT

4.1. Analysis of cascade failure characteristics in IIoT

4.1.1. Heterogeneous routing of cyber nodes

In the cyber network, terminal nodes only upload data to routing nodes after generating sensing data flows and do not participate in relaying and forwarding data. Therefore, the failure of terminal nodes does not cause failures in other nodes nor directly trigger cascade failures in the cyber network. Routing nodes are nodes with computing and forwarding capabilities in the network. They cannot only forward data collected from terminal nodes but also from other routing nodes. When a routing node fails, data routed through it will be rerouted to other routing nodes, leading to load redistribution among routing nodes, which may trigger cascade failure in the cyber network. It should be noted that once a cyber node fails, we need to remove the failed node and the links connected to it from the network.

4.1.2. Load update within the same community

In the actual IIoT system, manufacturing processes are typically orderly and continuous. If equipment fails and there is no backup equipment to take over its operation, it could directly lead to a halt in the entire service production chain. To prevent the collapse of the entire service network due to the failure of a single service node, the failed node and its service production dependency edges are retained during the cascade failure process in the service network. At the same time, when a service node fails, other normal nodes within the same community can take over all production tasks previously handled by the failed node. Additionally, during the next round of load update, although the failed node cannot directly participate in production, it can still undertake additional load taken over by production tasks redistributed from other nodes within the same community.

4.1.3. Load update across communities

In cascade failures of the service network, the load redistribution of overloaded or failed nodes is typically confined to their own community, and does not propagate across communities. Therefore, it does not directly cause node failure in other communities. However, the load redistribution may increase the production burden on certain nodes, reducing their efficiency and output. This impact can propagate upstream or downstream along the production chain, eventually affecting the normal operation of nodes in other service communities. For example, in a practical IIoT scenario, if an assembly unit cannot complete its scheduled production tasks due to a hardware failure, these tasks may be transferred to a nearby assembly unit. However, this load transfer could increase the production burden on the receiving unit, reducing production efficiency. As a result, other manufacturing units downstream and upstream, which rely on the output or input of these units, will also experience reduced efficiency, ultimately leading to a decline in the overall production efficiency and output of the entire IIoT system.

4.2. Initial load of IIoT nodes

4.2.1. Cyber nodes

In IIoT, the load of a cyber node refers to the workload it generates or routes for data streams. The initial load of each cyber node varies significantly based on its routing role and functionality. For terminal nodes, they only need to send the data they generate and do not need to forward data from other nodes. Therefore, their initial load is not influenced by other nodes but by the data streams they generate. Thus, the initial load of terminal node p_i is defined as:

$$L_i^T(0) = \frac{z_i}{\sum_{k\in V_T} z_k}, \tag{1}$$

where V_T is the set of terminal nodes; z_i is the data stream density of node p_i, which is a value in the interval $(0, 1]$; the value of z_i is related to the sensor types and sampling frequency settings of the corresponding intelligent production unit.

The data sources of routing nodes primarily come from two aspects: data transmitted from terminal nodes and data forwarded from other routing nodes. In IIoT, data typically travels along the shortest path for data transmission. Thus, the initial load of routing node p_i is defined as:

$$L_i^R(0) = \sum_{j\in V_T} L_j^T(0)\frac{\omega_{j,i}(0)}{\omega_j(0)}, \tag{2}$$

where $L_j^T(0)$ is the initial load of terminal node p_j; $\omega_{j,i}(0)$ is the shortest path number from terminal node p_j to the nearest gateway node via routing node p_i at the initial moment; $\omega_j(0)$ is the shortest path number from terminal node p_j to its nearest gateway node at the initial moment. According to (2), if all the sensing data collected by terminal nodes passes through routing node p_i to its nearest gateway nodes, $L_i^R(0)$ takes the maximum value of 1. Conversely, if none of the terminal node data passes through routing node p_i to its nearest gateway nodes, $L_i^R(0)$ takes the minimum value of 0.

4.2.2. Service nodes

Upon the arrival of a task, it can be decomposed into different subtasks. Then, based on the subtasks that need to be completed, service nodes are scheduled to form a service production chain. When dividing tasks, we need to consider task dependencies. For example, manufacturing a vehicle can be divided into six major tasks: component manufacturing, assembly, quality control, painting, final assembly, and testing. Each task has sequential dependencies, and only after the previous task is completed can the next task be executed. Each task is further refined into subtasks that involve processing and production specific to particular structures and parts. Suppose a factory receives an order to produce m types of products, with M_k productions needed for the k-th type of product. When producing the k-th type of product, it can be divided into N_k tasks, and the j-th task can be divided into $N_{k,j}$ subtasks. Then, the total number of subtasks required to complete this order is:

$$L^{ST} = \sum_{k=1}^{m}\sum_{j=1}^{N_k}\sum_{i=1}^{N_{k,j}} M_k \cdot \alpha_{k,j,i}, \tag{3}$$

where $\alpha_{k,j,i}$ is the adjustment coefficient for the i-th sub-task of the j-th task in the k-th product type, reflecting the complexity and dependencies of the sub-task. Setting an adjustment coefficient to each subtask during the production process is used to slightly adjust production parameters, ensuring consistent quality, performance, and adherence to standards across batches. The subtask coefficient is in the interval $[0.8, 1.2]$, allowing the basic load to vary within ±20% (Xiao, Li, Song, Yang, & Su, 2021).

After task decomposition, we can finally obtain the production subtasks taken by each service node. The production load of a service node includes the basic production load imposed by production scheduling tasks and the load generated by the material supply from upstream nodes in the service production chain. Thus, the initial load of service nodes is defined as:

$$L_i^S(0) = \frac{L^{ST}\eta_i}{n_i\sum_{k\in VC_i^S} L_k^S} + \sum_{j\in\Omega_i^{\text{in}}}\frac{L_j^S}{k_j^{\text{out}}}, \tag{4}$$

where VC_i^S is the set of nodes that belong to the same community as service node s_i; n_i is the number of scheduled nodes of the same type as the service node s_i; η_i is related to its own service resources, representing the weight in the distribution of service node s_i. The more service resources, the larger the value of η_i. L_j^S is the load number of service node s_i pointing to the service node s_j; Ω_i^{in} is the set of in-degree neighboring service nodes of node s_i; k_j^{out} is the out-degree value of the service node s_j.

4.3. Node capacity

4.3.1. Capacity upper limit

In the cyber network, node capacity refers to the data processing ability of nodes. The classic capacity-load model assumes a linear relationship between node capacity and initial load. However, many studies show that in real networks, nodes with smaller initial loads tend to have larger redundant capacities, while nodes with larger initial loads have smaller redundant capacities (Dong et al., 2023). Thus, node capacity and initial load exhibit a nonlinear relationship. Therefore, we adopt a nonlinear load-capacity model and define the normal capacity of cyber nodes as:

$$M_i^{CN} = L_i^C(0) + \beta_c L_i^C(0)^{\alpha_c}, \tag{5}$$

where $L_i^C(0)$ is the initial load of cyber node p_i; α_c is the growth exponent, determining the rate at which load growth affects capacity growth; β_c is the load adjustment coefficient, adjusting the impact of load on capacity.

In practical industrial scenarios, when the load of cyber nodes exceeds its normal capacity, it does not immediately fail but enters a tolerable overload state, with reduced data transmission capability. The cyber node can still forward data from its redundant capacity and may return to normal as the redundant capacity depletes. However, if the overloaded load continues to rise beyond a certain threshold does the cyber node fail due to severe overload, exhibiting delay characteristics. To ensure smooth operation, redundant capacity is typically allocated to handle additional loads. Thus, momentary overload is permissible, and the greater the load on the cyber node, the more redundant capacity is required to maintain normal operation during peak periods. We define the redundant capacity of cyber node p_i as:

$$M_i^{CR} = \delta_c\frac{L_i^C(0)}{\langle L^C\rangle}M_i^{CN}, \tag{6}$$

where $\delta_c \geq 0$ is the overload coefficient; $\langle L^C \rangle = \sum_{m \in V_I} L_m^C / N$ is the average load of all cyber nodes in the network; $L_i^C(0)/\langle L^C \rangle$ is used to describe the relative load size of the cyber node p_i throughout the network; M_i^{CN} is the normal capacity of the cyber node p_i.

Similar to cyber nodes, the normal capacity and redundant capacity of service node s_i are defined as:

$$C_i^{SN} = L_i^S(0) + \beta_s L_i^S(0)^{\alpha_s}, \tag{7}$$

$$C_i^{SR} = \delta_s \frac{L_i^S(0)}{\langle L^S \rangle} C_i^{SN}, \tag{8}$$

where $L_i^S(0)$ is the initial load of the service node s_i; $\alpha_s \in [0,1]$, $\beta_s \geq 0$ is the capacity coefficient; α_s is the growth exponent, determining the rate at which load growth affects capacity growth; β_s is the load adjustment coefficient; $\delta_s \geq 0$ is the overload coefficient; $\langle L^S \rangle = \sum_{m \in V_S} L_m^S / N$ is the average load of all service nodes in the network; $L_i^S(0)/\langle L^S \rangle$ is used to describe the relative load size of service node s_i in the entire network; C_i^{SN} is the normal capacity of the service node s_i.

4.3.2. Capacity lower limit of service nodes

Each service node has technical requirements that define the minimum performance standards for safe operation, and equipment must exceed these standards to maximize business benefits while balancing costs and outputs. Therefore, equipment must operate above a defined capacity lower limit. This limit is also linked to the node's adaptability, which refers to its ability to respond to sudden events. Nodes with higher adaptability have lower capacity lower limits. In IIoT, the degree reflects the number of production dependency relationships of a service node, nodes with more dependencies have higher adaptability (Li, Long, He, & Li, 2024). Thus, we define the lower limit of service node s_i capacity as:

$$C_i^{SL} = \gamma_s L_i^S(0), \tag{9}$$

where $\gamma_s \in [0,1]$ is the capacity lower limit coefficient.

4.4. Node failure types in IIoT

4.4.1. Cyber node failure states

Cyber nodes have three types of failure states: isolation failure state, overload failure state, and interdependent failure state. The tolerable overload of a cyber node refers to the state that load of the cyber node exceeds its capacity, causing reduced data transmission efficiency without immediate failure. As described in Section 4.3, only when the load continues to increase, occupying all redundant capacity, does the node enter an overload failure state. The isolation of a cyber node refers to the state where the path from the node to the gateway node is interrupted, preventing data exchange. The interdependent failure of a cyber node refers to the state where all service nodes supported by the cyber node are unable to provide production service functions, causing the node's data communication function to cease. The state transition of cyber nodes during the cascade failure process is shown in Fig. 3. We use an indicator function $f_i^C(t)$ to represent the state transition process of cyber node p_i at time t to better capture the dynamic changes of cyber nodes operational state over time.

$$f_i^C(t) = \begin{cases} 0 & L_i^C(t) \leq M_i^{CN} \\ \frac{L_i^C(t) - M_i^{CN}}{M_i^{CR}} & M_i^{CN} < L_i^C(t) < M_i^{CN} + M_i^{CR} \\ 1 & L_i^C(t) \geq M_i^{CN} + M_i^{CR}, \end{cases} \tag{10}$$

where $L_i^C(t)$ is the real-time load of the cyber node p_i at time t. When $L_i^C(t) \leq M_i^{CN}$, the node is functioning normally. When $M_i^{CN} < L_i^C(t) \leq M_i^{CN} + M_i^{CR}$, the node is in a tolerable overload state, indicating that the cyber node is still functioning normally but with reduced efficiency. At this point, the node is using redundant capacity to handle the overload data. Once the redundant capacity is exhausted, the node will enter an overload failure state. When $M_i^{CN} < L_i^C(t) \leq M_i^{CN} + M_i^{CR}$, the node is in an overload failure state, completely losing its operational capability. The relationship between the real-time load of the cyber node and the state transition is shown in Fig. 4.

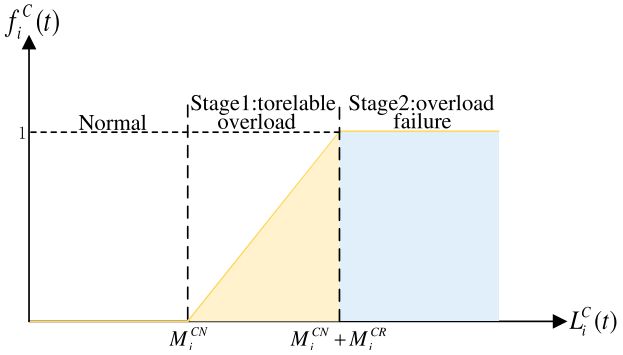


Fig. 3. The relationship between real-time load and state transitions of cyber nodes.

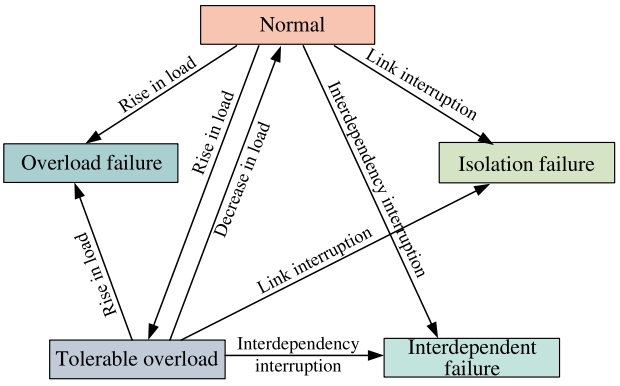


Fig. 4. State transitions of cyber nodes.

4.4.2. Service node failure states

Service nodes have three types of failure states: underload failure state, overload failure state, and interdependent failure state. The overload failure state occurs when a service node is burdened with tasks beyond its capacity, leading to performance degradation or service interruption. Like cyber nodes, service nodes in overload also exhibit delay characteristics. Underload failure arises from reduced efficiency, often due to decreased production demand or insufficient supply, causing the load to fall below the operational capacity lower limit, making it unable to meet maintenance costs. Interdependent failure of a service node refers to the failure type caused by the failure of the cyber node supporting it. In IIoT, if a cyber node fails and cannot collect data, the service node cannot execute production tasks, leading to failure. Therefore, in our cascade failure model, a cyber node failure results in the failure of all connected service nodes. The state transition of service nodes during the cascade failure process is shown in Fig. 5. We use an indicator function $f_i^S(t)$ to represent the state transition process of service node s_i at time t:

$$f_i^S(t) = \begin{cases} 0 & C_i^{SL} < L_i^S(t) \leq C_i^{SN} \\ \frac{L_i^S(t) - C_i^{SN}}{C_i^{IR}} & C_i^{SN} < L_i^S(t) < C_i^{SN} + C_i^{SR} \\ 1 & L_i^S(t) \leq C_i^{SL} \bigcup L_i^S(t) \geq C_i^{SN} + C_i^{SR}, \end{cases} \tag{11}$$

where $L_i^S(t)$ is the real-time load of the service node s_i at time t. According to (11), when $L_i^S(t) > C_i^{SN} + C_i^{SR}$, the node is functioning

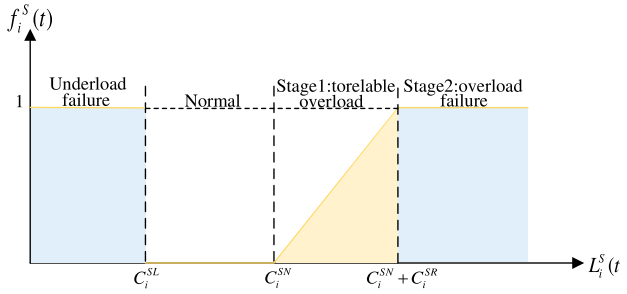


Fig. 5. The relationship between real-time load and state transitions of service nodes.

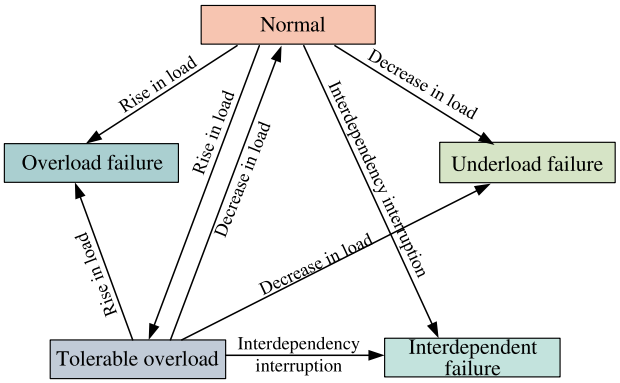


Fig. 6. State transitions of service nodes.

and providing services. When $C_i^{SN} \le L_i^S(t) < C_i^{SN} + C_i^{SR}$, the node is in a tolerable overload state, indicating that the service node is still functioning but with reduced efficiency. The production capacity of the node decreases as the load increases. When $L_i^S(t) \le C_i^{SL}$ or $L_i^S(t) > C_i^{SN} + C_i^{SR}$, the former represents the node being in an underload failure state and all services are shut down. The latter represents the node being in an overload failure state and completely losing its operational capability. The relationship between the real-time load and state transitions of service nodes is shown in Fig. 6.

4.5. Load reallocation

4.5.1. Load redistribution in the cyber network

In the cyber network, terminal node failures only result in data loss, while routing node failures cause load redistribution by rerouting data to other nodes. To capture the impact of overloaded and failed nodes on load redistribution in the cyber network, our cascade failure model performs two rounds of redistribution per time unit. In the first redistribution round at time t, we check the interdependence status, overload status, and connection status of each cyber node, removing failed nodes and links from the network. In the second redistribution round at time t, the load of the tolerable overload nodes and overloaded failure nodes is transferred to the normal nodes. The load of routing node p_i in the first redistribution round at time t is calculated as follows:

$$L_i^C(t^*) = \sum_{j \in V_T(t^*)} L_j^T(0) \frac{\omega_{j,i}(t^*)}{\omega_j(t^*)}, \tag{12}$$

where $V_T(t^*)$ is the set of terminal nodes at the first round of the load update; $\omega_{j,i}(t^*)$ is the number of shortest paths from terminal node p_j to the nearest gateway node via routing node p_i at the first round of the load update; $\omega_j(t^*)$ is the number of shortest paths from terminal nodes p_j to the nearest gateway node at the first round of the load update; $L_j^T(0)$ is the initial load of terminal node p_j. In the first round of cyber network load update, the load is calculated according to (12) without considering the redistributed load caused by other failed nodes. Therefore, we further discuss the load of routing nodes at time t:

$$L_i^C(t) \begin{cases} L_i^C(t^*) + \sum_{j \in V^{CT}(t)} \Delta L_{j,i}^C(t) \\ \quad + \sum_{m \in V^{CF}(t)} \Delta L_{m,i}^C(t) & L_i^C(t^*) < M_i^{CN} \\ C_i^{CN} & M_i^{CN} \le L_i^C(t^*) \le M_i^{CN} + M_i^{CR} \\ 0 & L_i^C(t^*) > M_i^{CN} + M_i^{CR}, \end{cases} \tag{13}$$

$$\Delta L_{j,i}^C(t) = [L_j^C(t^*) - M_j^C] \frac{M_i^C - L_i^C(t^*)}{\sum_{k \in \Gamma_i^{CT}(t)} [M_k^C - L_k^C(t^*)]}, \tag{14}$$

$$\Delta L_{m,i}^C(t) = L_m^C(t^*) \frac{M_i^C - L_i^C(t^*)}{\sum_{n \in \Gamma_i^{CF}(t)} [M_n^C - L_n^C(t^*)]}, \tag{15}$$

where $V^{CT}(t)$ is the set of tolerable overload state nodes in the cyber network after the first round of the load update at time t; $\Delta L_{j,i}^C(t)$ is the load increment transmitted from tolerable overload node p_j to normal node p_i at time t. $V^{CF}(t)$ is the set of overload failure state nodes in the cyber network after the first round of the load update at time t; $\Delta L_{m,i}^C(t)$ is the load increment transmitted from overload failure node p_m to normal node p_i at time t; $\Gamma_i^{CT}(t)$ is the set of normal nodes closest to the tolerable overload nodes routing node p_j at time t; $\Gamma_i^{CF}(t)$ is the set of normal nodes closest to the overload failure routing node p_m at time t.

4.5.2. Load update in the service network

The service network undergoes two rounds of load update in each time unit. In the first round of the update at time t, we first check the interdependence status, overload status, and connection status of each service node, and then set the capacity of the failed nodes to 0. Then, we update the load of service nodes both within the same community and across different communities in the second round.

(1) Load redistribution within the same community

The service network adopts a community structure. If a service node becomes overloaded or failed, some or all of its load will be redistributed to neighboring nodes within the same community that are not overloaded. Similarly, we divide the load redistribution strategy into overload failure nodes and tolerable overload nodes. After the first round of the load redistribution, the current load of the service node s_i is:

$$L_i^S(t^*) = \begin{cases} L_i^S(t-1) + \sum_{j \in V^{ST}(t^*)} \Delta L_{j,i}^S(t) \\ \quad + \sum_{m \in V^{SF}(t^*)} \Delta L_{m,i}^S(t) & C_i^{SL} \le L_i^S(t-1) \le C_i^{SN} \\ C_i^{SN} & C_i^{SN} < L_i^S(t-1) < C_i^{SN} + C_i^{SR} \\ 0 & L_i^S(t-1) \le C_i^{SN} \\ & \cup L_i^S(t-1) \ge C_i^{SN} + C_i^{SR}, \end{cases} \tag{16}$$

where $L_i^S(t^*)$ is the real-time load value of service node s_i at the first round of the load redistribution; $V^{ST}(t^*)$ is the set of tolerable overload nodes in the service network at the first round of the load redistribution; $\Delta L_{j,i}^S(t^*)$ is the load increment transmitted from tolerable overload node s_j to normal node s_i at the first round of the load redistribution; $V^{SF}(t^*)$ is the set of overload failure state nodes in the service network at the first round of the load redistribution; $\Delta L_{m,i}^S(t^*)$ is the load increment transmitted from overload failure node s_m to normal node s_i at the first round of the load redistribution. Similarly, the incremental expression can be calculated as:

$$\Delta L_{j,i}^S(t^*) = [L_j^E(t-1) - C_j^S] \frac{C_i^S - L_i^S(t-1)}{\sum_{k \in \Gamma_i^{ST}(t^*)} [C_k^S - L_k^S(t-1)]}, \tag{17}$$

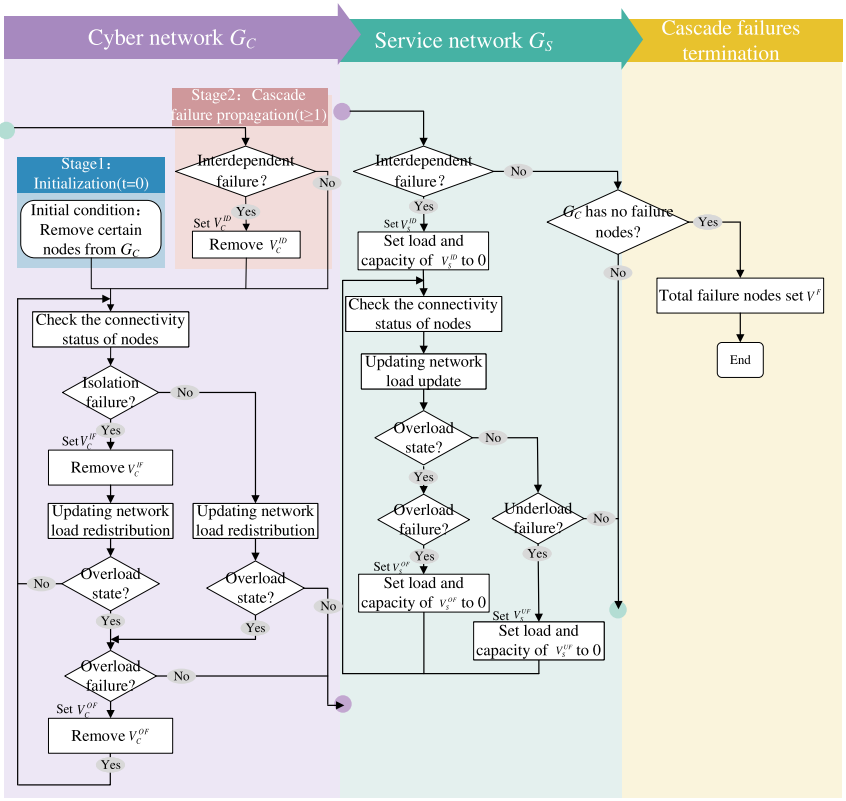


Fig. 7. The flowchart of the cascade failure process initiated by the cyber network.

$$\Delta L_{m,i}^{S}(t^*) = L_m^S(t-1)\frac{C_i^S - L_i^S(t-1)}{\sum_{k\in\Gamma_i^{SF}(t^*)}[C_k^S - L_k^S(t-1)]}, \tag{18}$$

where $\Gamma_j^{ST}(t^*)$ is the set of normal nodes closest to the tolerable overload nodes s_j within the same community at the first round of the load redistribution; $\Gamma_m^{SF}(t^*)$ is the set of normal nodes closest to the overload failure node s_m within the same community at the first round of the load redistribution.

(2) Load update across the different community

After the load redistribution within the same community, the state of the upstream node s_a and the downstream node s_b of service node s_i can be updated to four different conditions. We can use a status function $g_i^S(t)$ to represent these conditions.

$$g_i^S(t) = \begin{cases} 0 & L_a^S < C_a^{SN} + C_a^{SR}, \quad L_b^S < C_b^{SN} + C_b^{SR} \\ 1 & L_a^S \geq C_a^{SN} + C_a^{SR}, \quad L_b^S < C_b^{SN} + C_b^{SR} \\ 2 & L_a^S < C_a^{SN} + C_a^{SR}, \quad L_b^S \geq C_b^{SN} + C_b^{SR} \\ 3 & L_a^S \geq C_a^{SN} + C_a^{SR}, \quad L_b^S \geq C_b^{SN} + C_b^{SR}. \end{cases} \tag{19}$$

Next, we proceed with the second round of load update for the service node s_i, the final load of node s_i at time t can be calculated as:

$$L_i^S(t) = \begin{cases} L_i^{S*}(t) & g_i^S(t) = 0 \\ L_i^{S*}(t) - \Delta L_{a,i}^S(t) & g_i^S(t) = 1 \\ L_i^{S*}(t) - L_{a,i}^S(t) & g_i^S(t) = 2 \\ L_i^{S*}(t) - L_{a,i}^S(t) - L_{b,i}^S(t) & g_i^S(t) = 3. \end{cases} \tag{20}$$

In (20), the reduced values of service node s_i due to the failure of upstream node s_a and downstream node s_b are as follows:

$$\Delta L_{a,i}^S(t) = L_i^S(t^*)\frac{w_{a,i}(t)}{\sum_{c\in\Omega_i^{\mathrm{up}}(t)} w_{c,i}(t) + \sum_{d\in\Omega_i^{\mathrm{down}}(t)} w_{i,d}(t)}, \tag{21}$$

$$\Delta L_{i,b}^S(t) = L_i^S(t^*)\frac{w_{i,b}(t)}{\sum_{c\in\Omega_i^{\mathrm{up}}(t)} w_{c,i}(t) + \sum_{d\in\Omega_i^{\mathrm{down}}(t)} w_{i,d}(t)}, \tag{22}$$

$$w_{a,i}(t) = \frac{1}{k_i^{\mathrm{in}}}\frac{\Delta L_{a,i}^S(t-1)}{L_i^S(t^*)}, \tag{23}$$

$$w_{i,b}(t) = \frac{1}{k_i^{\mathrm{out}}}\frac{\Delta L_{i,b}^S(t-1)}{L_i^S(t^*)}, \tag{24}$$

where $\Omega_i^{\mathrm{up}}(t)$ and $\Omega_i^{\mathrm{down}}(t)$ are respectively the set of upstream neighboring nodes and the set of downstream neighboring nodes for node s_i at time t; $w_{a,i}(t)$ is the degree of close connection between node s_i and its upstream neighboring node s_a at time t; $w_{i,b}(t)$ is the degree of close connection between node s_i and its downstream neighboring node s_b at time t. The degree of close connection reflects the likelihood of interaction between service nodes on the same production chain and is directly proportional to the reduced load from the previous moment. $\Delta L_{a,i}^S(t-1)$ is the load reduction for the upstream node s_a of node s_i at time $t-1$; $\Delta L_{i,b}^S(t-1)$ is the load reduction for the downstream node s_b of node s_i at time $t-1$.

4.6. Cascade failure mechanism

Many existing cascade failure models for dual-layer networks (Yin, Huang, Shuai, Liu, & Zhang, 2022; Yu, Xiao, & Cui, 2023) assume identical failure mechanisms in both networks, which is only applicable to networks with similar structures and functions. However, the functions and configurations of the cyber network and the service network in IIoT are completely different, and the node state transitions also vary. Therefore, we propose a new cascade failure mechanism with two stages: the initialization stage and the failure propagation stage. In the initialization stage, certain nodes in the network are set to a failure state according to a hardware/software malfunction to trigger the cascade failure process. During the propagation stage, nodes in the network may gradually fail due to overload, isolation, and interdependent failures. The cascade failure processes triggered by different networks are respectively shown in Figs. 7 and 8.

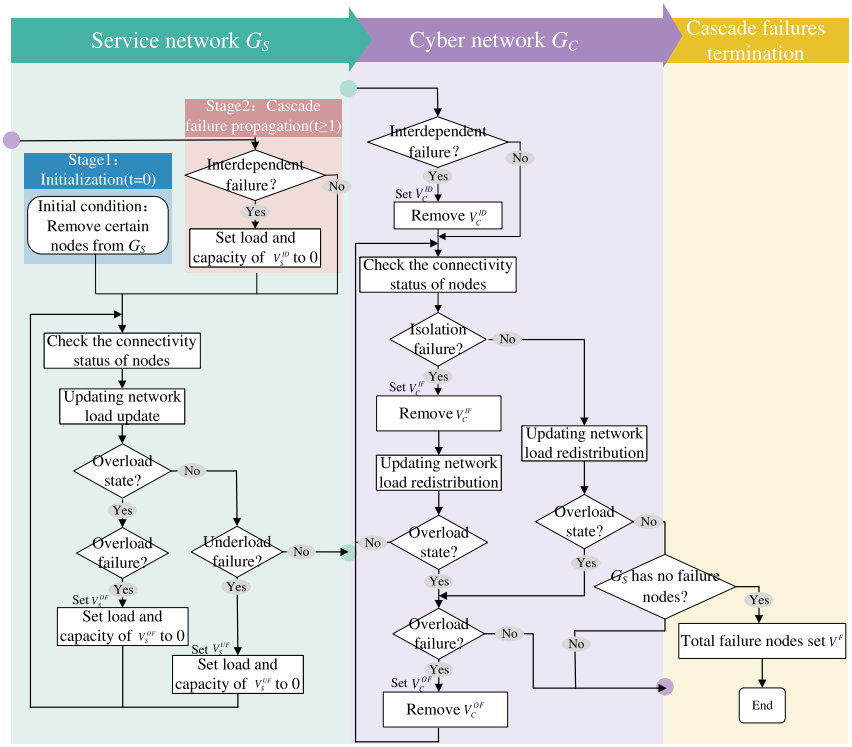
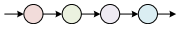
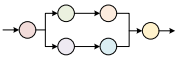
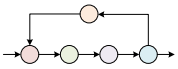
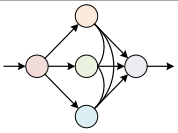


Fig. 8. The flowchart of the cascade failure process initiated by the service network.

Table 1
Four typical production dependency structures.

Structure	Serial structure	Parallel structure	Loop structure	Selection structure
Structure topology				
Applicable scenarios	Applicable to production processes that require a clear sequence of operations.	Applicable to production processes that require multiple independent operations to run in parallel.	Applicable to customized production or production with high product diversity.	Applicable to production processes that require feedback.

4.6.1. Example of cascade failure process

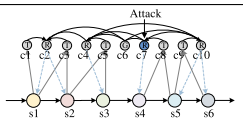
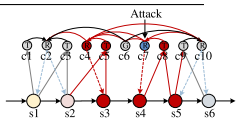
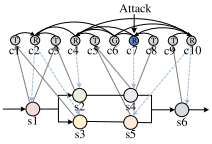
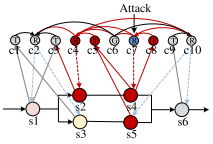
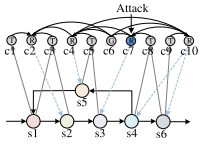
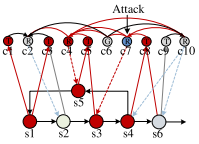
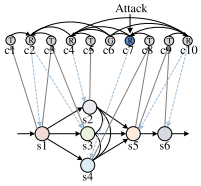
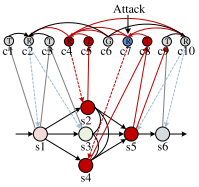
For ease of understanding the proposed cascade failure mechanism, we present an example of the cascade failure process based on four typical production dependency structures shown in Table 1 (serial structure, parallel structure, selection structure, and loop structure). As shown in Table 2, the initial IIoT system for these four topologies includes a cyber network with 10 nodes, comprising 5 terminal nodes, 4 routing nodes, and 1 gateway node. The service network consists of 6 service nodes, covering 3 types of services.

In this example, blue nodes represent failure sources, and red nodes represent failed nodes. Attack node c7 to trigger a cascade failure. During the cascade failure propagation, failures can spread within the same network, leading to overload or isolation failures in other cyber nodes (e.g., due to communication disruption, c8 in the serial structure enters isolation failure; and due to load redistribution from failed nodes, c4 enters overload failure). Simultaneously, the failed cyber nodes cause the service nodes to lose their interdependent links and data support from the cyber nodes, leading to interdependent failures of service nodes and cross-network propagation (e.g., in the serial structure, s4 enters interdependent failure due to the loss of interdependent links from all terminal nodes). In various structures of the service network, load redistribution allows the task of failed service nodes to be transferred to normal nodes with the same function, which may lead to overload failures in these nodes. However, during this process, it is important to note that failed service nodes can receive compensatory loads from other normal nodes to maintain the normal operation of the production chain. Therefore, the failed service nodes in Table 2 (e.g., s3, s4, s5 in the serial structure, s2, s4, s5 in the parallel structure, and s2, s4, s5 in the selection structure) continue to maintain production through the load redistribution mechanism. However, due to the failure of nodes s1 and s3 within the same community in the loop structure, and there are no other nodes within the same community to take over their production tasks. Then, the entire production chain can be considered as stalled, with the output reduced to zero. Additionally, it is worth noting that these failed service nodes can further trigger cyber node failures via interdependency links (e.g., in the serial structure, overloaded failure node s5 through the interdependent link leads to cyber node c8 failing), until the entire IIoT system isolates failed nodes functionally, and cascade failure propagation terminates.

4.7. Cascade failures reliability metric

Existing studies on cascade failures in interdependent networks typically assume that a node remains operational if it is not overloaded

Table 2
Example of cascade failure propagation in IIoT.

	Initial network	Post-cascade termination network
Sequence structure		
Parallel structure		
Loop structure		
Selection structure		

after cascade failures and still belongs to the largest connected component within the same layer (Chen et al., 2022; Huang, Zhang, & Yao, 2022). While this assumption is reasonable for networks such as supply chains, it is not applicable to the IIoT, which has a more complex structure and distinct requirements. In the IIoT, nodes are not only expected to maintain connectivity but also to perform critical functions, including data transmission and service delivery. Specifically, users are more concerned about two aspects: (1) how many cyber nodes are still able to transmit sensing data to gateway nodes after cascade failures; (2) how many service nodes can continue to provide services after cascade failures. Thus, unlike traditional interdependent networks, the IIoT places greater emphasis on whether nodes can continue to perform their intended functions.

In the cyber network, nodes often fail due to hardware or software issues, while in the service network, failures are typically caused by material shortages or process interruptions. Given the central role of node functionality, this study focuses on cascade failures in IIoT caused by such node failures. To quantify the impact of these failures, we use the ratio of failed nodes to total nodes when the network reaches a stable state. This ratio reflects the node survival rate, which serves as an indicator of cascade reliability in IIoT systems. It is defined as:

$$Z(t) = \frac{N_C(t) + N_S(t)}{N_C + N_S}, \tag{25}$$

where $N_C(t)$ and $N_S(t)$ respectively denote the number of surviving nodes in the cyber network and the service network at time t. We use $Z(\infty)$ to denote the survival rate of nodes in IIoT when the cascade failure process reaches a stable state (i.e., no new failed nodes appear). Clearly, the larger $Z(\infty)$ is, the better cascade reliability of the IIoT.

5. Experimental results

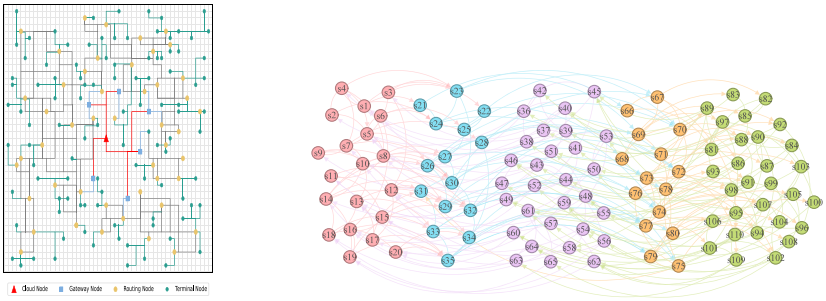
5.1. Experimental setup

The simulation experiments were conducted based on Matlab 2021b. The data used to construct the IIoT topology in the experiment is grounded in actual automotive manufacturing cases (Romero et al., 2023; Tanase, Serban, Dobrin, Banta, et al., 2023). Based on the configuration of IoT device found in automotive production workshops, the cyber network consists of 158 nodes, and the service network contains 110 nodes, covering typical production processes in automotive manufacturing scenarios, ranging from assembly lines to quality inspection (Giampieri, Ling-Chin, Ma, Smallbone, & Roskilly, 2020; Lee et al., 2023). We conducted cross-validation of the proposed network topology with similar use cases from the automotive manufacturing sector and compared it with established IIoT standards. This comparative analysis served to substantiate the practicality and relevance of the proposed model, demonstrating its capacity to accurately simulate IIoT networks within the context of automotive production. Additionally, this approach not only confirmed the technical feasibility of the proposed model but also highlighted its potential for optimizing real-world IIoT implementations in the automotive industry.

The initial settings of experiment are as follows: (1) all nodes in the network are in normal working condition, and the network topology is fully connected; (2) the cyber network consists of 104 terminal nodes, 48 routing nodes, and 6 gateway nodes; (3) the service network includes 110 service nodes of five different types, distributed according to the production task demands; (4) we do not consider the potential influence of the MAC layer in real IIoT environments, such as channel contention and path loss; (5) terminal nodes and routing nodes transmit data along the shortest path to the nearest gateway nodes according to the principle of minimum delivery delay; (6) we employed a multi-point attack strategy to trigger cascade failures, with all experimental results being the average of 50 simulations. The network layout of the cyber-service IIoT used in the experiments is illustrated in Fig. 9.

5.2. Rationality of the system model

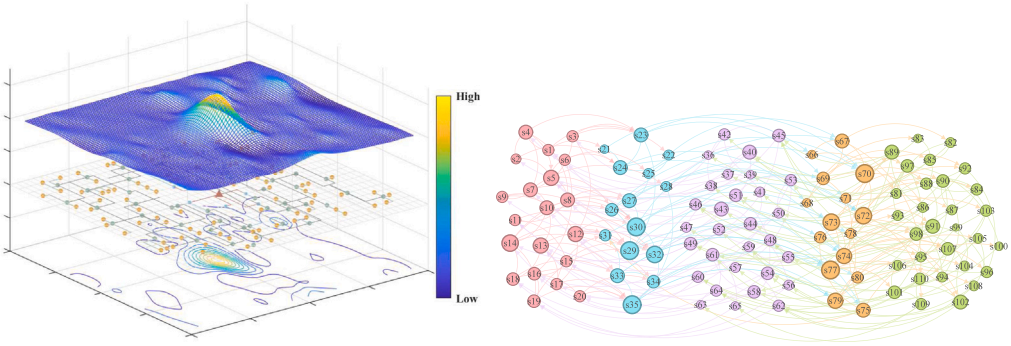
In the cyber network, data generated by terminal nodes is first processed by routing nodes and then aggregated to the cloud via gateway nodes. This leads to routing nodes near gateway nodes bearing heavier loads, which is a phenomenon known as the hotspot effect (Wang, Fu, Yang, & Postolache, 2021). This phenomenon is an important indicator that distinguishes IIoT from general data transmission networks. Fig. 10(a) shows the load distribution in the cyber network of our system model, illustrating a clear hotspot effect with higher loads near gateway nodes, thus validating the rationality of the cyber network. In the service network, the load of each service node depends on its own production load and service relationships with other nodes.



(a) Cyber network (b) Service network

(c) Cyber-service coupling network

Fig. 9. The IIoT structure with cyber-service coupling.



(a) Cyber network (b) Service network

Fig. 10. Load distributions of the cyber network and the service network in IIoT.

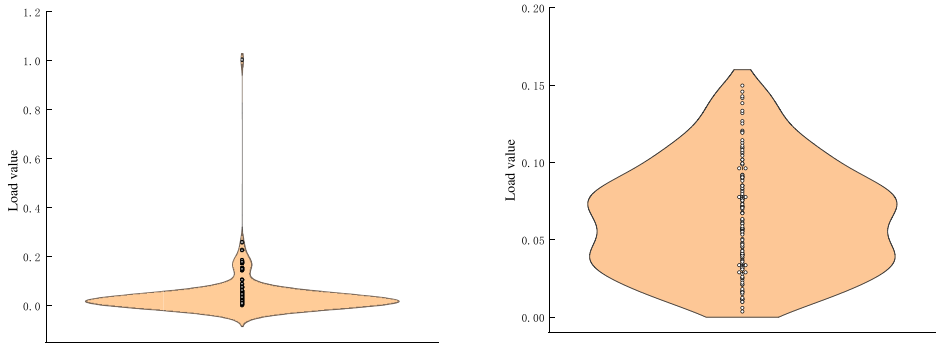
This networking pattern makes the high in-degree nodes more loaded because they receive and process more service requests, thus exhibiting a typical positive in-degree to load correlation. Fig. 10(b) shows the load distribution of the service network, where nodes with higher in-degrees have significantly higher loads, validating rationality of the service network.

Fig. 11 shows the probability distributions of node load in the cyber and service networks, which differ significantly. As shown in Fig. 12(a), the load probability distribution in the cyber network follows a long-tail distribution, with a power-law distribution characteristic. In this distribution, a few nodes, (particularly those near gateway nodes) handle the majority of the data traffic in the network. The power-law characteristic has been widely validated (Fu, Yao, & Yang, 2019; Qiu, Lu, Li, Xue, & Wu, 2020). Fig. 12(b) shows the probability distribution of node loads in the service network. Compared to the cyber network, the load distribution in the service network is more balanced and approximates a normal distribution. In actual industrial scenarios, the production subtasks of service nodes are influenced by both internal factors and the production or supply statuses of other nodes, resulting in a balanced load distribution. This normal distribution has been verified in several studies (Fu, Li, & Li, 2023; Sefati, Mousavinasab, & Zareh Farkhady, 2022). These observations further validate the rationality of the proposed system model.

5.3. Impact of modeling parameters

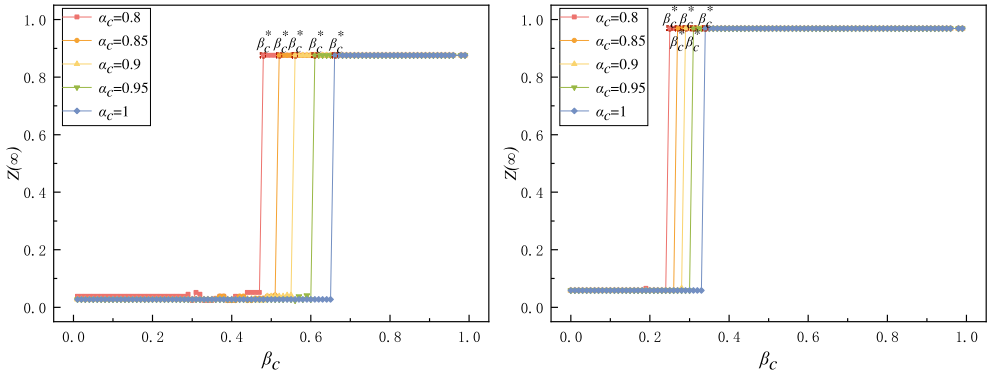
5.3.1. Cyber network

Fig. 12 shows the network cascade reliability in two attack scenarios with varying α_c and β_c. As α_c increases, the cascade reliability decreases. The cascade reliability improves with β_c increasing, but there is a step value β_c^*, beyond which the reliability sharply increases and then stabilizes. In the proposed system model, α_c is the growth exponent. As α_c increases, the contribution of each load unit to total capacity diminishes. This reduces the difference between nodes with high and low initial loads, leading to a higher probability of node failure once load redistribution occurs. β_c is the load adjustment coefficient. As β_c increases, the total capacity of the system is higher for the same initial



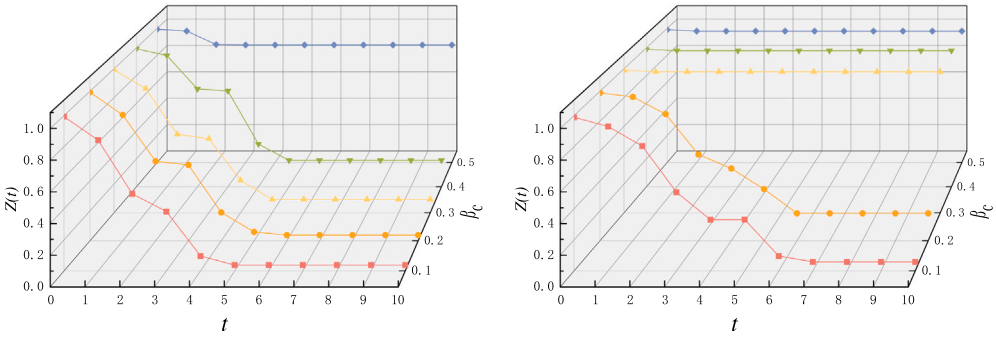
(a) Cyber network (b) Service network

Fig. 11. The probability distribution of the cyber network and the service network in IIoT.



(a) Node attack on the cyber network (b) Node attack on the service network

Fig. 12. Network cascade reliability with varying α_c and β_c in the two attack scenarios ($\delta_c = 0.5$, $\alpha_s = 0.8$, $\beta_s = 0.3$, $\delta_s = 0.5$, $\gamma_s = 0$, $q = 0.06$).



(a) Node attack on the cyber network (b) Node attack on the service network

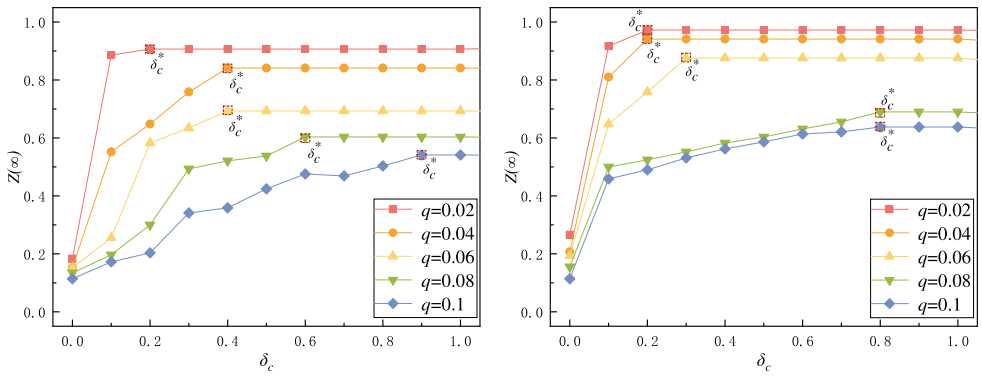
Fig. 13. Network cascade failure process with varying β_c in the two attack scenarios ($\alpha_c = 0.8$, $\delta_c = 0.5$, $\alpha_s = 0.8$, $\beta_s = 0.3$, $\delta_s = 0.5$, $\gamma_s = 0$, $q = 0.06$).

load and can respond to load growth more effectively. The initial low reliability is due to the slow response of the system to load growth.

Fig. 13 shows the cascade failure process of the network in two attack scenarios with varying β_c. In the cyber network attacked scenario, within β_c in the range [0.1, 0.4], increasing β_c improves cascade reliability but does not affect the failure duration. However, when β_c exceeds 0.4, further increases significantly reduce the number of failure steps and enhance reliability. In the service network attacked scenario, within β_c in the range [0.1, 0.2], increasing β_c does not change the failure steps. When β_c exceeds 0.2, increasing β_c results in fewer cascade failure steps and substantially boosts reliability. This is because at lower β_c values, the response to load growth is slow, and the node capacity is too small to handle the load transferred from other nodes. As β_c increases, the node capacity of cyber nodes improves, and only a few nodes become overloaded after load redistribution, greatly reducing cascade failure steps.

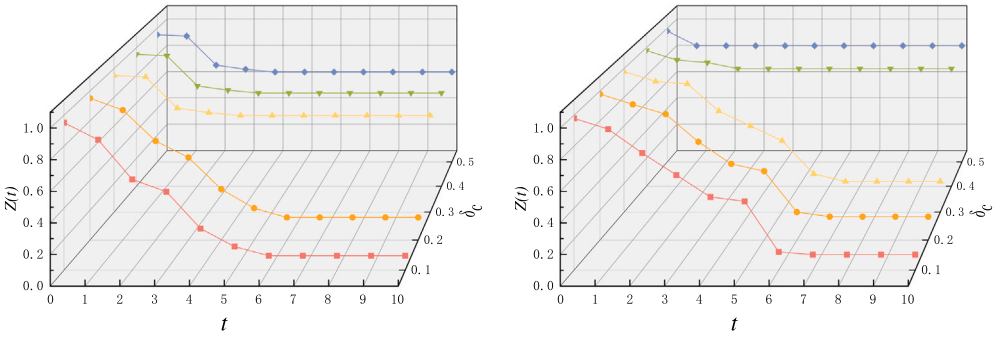
Fig. 14 shows the network cascade reliability in two attack scenarios with varying δ_c. Increasing δ_c significantly enhances cascade reliability, but beyond a critical threshold δ_c^*, further increases δ_c no longer result in any improvement. The overload coefficient δ_c reflects the ability of cyber nodes to handle redundant loads that exceed their normal capacity. The higher the value, the more additional load cyber nodes can withstand, and the lower the probability of failure. Additionally, attacks on the cyber network have a greater impact on IIoT than attacks on the service network.

Fig. 15 shows the cascade failure process of the network in two attack scenarios with varying δ_c. In the cyber network attack scenario, with δ_c in the range [0.1, 0.2], increasing δ_c improves cascade



(a) Node attack on the cyber network (b) Node attack on the service network

Fig. 14. Network cascade reliability with varying δ_c in the two attack scenarios ($\alpha_c = 0.8$, $\beta_c = 0.8$, $\alpha_s = 0.8$, $\beta_s = 0.3$, $\delta_s = 0.5$, $\gamma_s = 0$).



(a) Node attack on the cyber network (b) Node attack on the service network

Fig. 15. Network cascade failure process with varying δ_c in the two attack scenarios ($\alpha_c = 0.8$, $\beta_c = 0.8$, $\alpha_s = 0.8$, $\beta_s = 0.3$, $\delta_s = 0.5$, $\gamma_s = 0$, $q = 0.06$).

reliability without affecting the failure process. However, when δ_c exceeds 0.2, further increases in δ_c reduce failure steps and significantly enhance cascade reliability. When the service network is attacked, the phenomenon is similar to the cyber network attacked scenario. As δ_c increases, the risk of cyber nodes entering overload failure decreases, without altering node states. Therefore, at lower δ_c, although increasing δ_c slightly improves cascade reliability, failure steps remain constant. When δ_c reaches a level that supports all tolerable overload nodes, failure steps decrease significantly, and cascade reliability is greatly enhanced.

Fig. 16 shows the heatmap of IIoT system cascade reliability within the parameter space $[\delta_c, \beta_c]$ in the two attack scenarios, further confirming the existence of the previously mentioned critical threshold value δ_c^* and step value β_c^*. These thresholds form a reliability extremum region, where cascade reliability reaches its maximum. Comparing the size and reliability values of this region in both scenarios, we observe that cyber network attacks have a greater impact on IIoT than service network attacks. This is because a cyber node supports multiple service nodes, so its failure can trigger the simultaneous failure of several service nodes. However, a service node depend on a cyber node. After a service node fails, the cyber node can no longer provide data to the service node, causing the cyber node to be unable to continue functioning and enter an interdependent failure state.

5.3.2. Service network

Fig. 17 shows the network cascade reliability in two attack scenarios with varying α_s and β_s. It is evident that in the service network attack scenario, a slight increase in α_s and β_s can significantly help the system resist attacks on the service network. This suggests that different capacity allocation strategies should be adopted for different attack types: more capacity should be allocated to service nodes in response to service network attacks and to cyber nodes for cyber network attacks. Similarly, a step value β_s^* is observed, beyond which the cascade reliability reaches its upper limit.

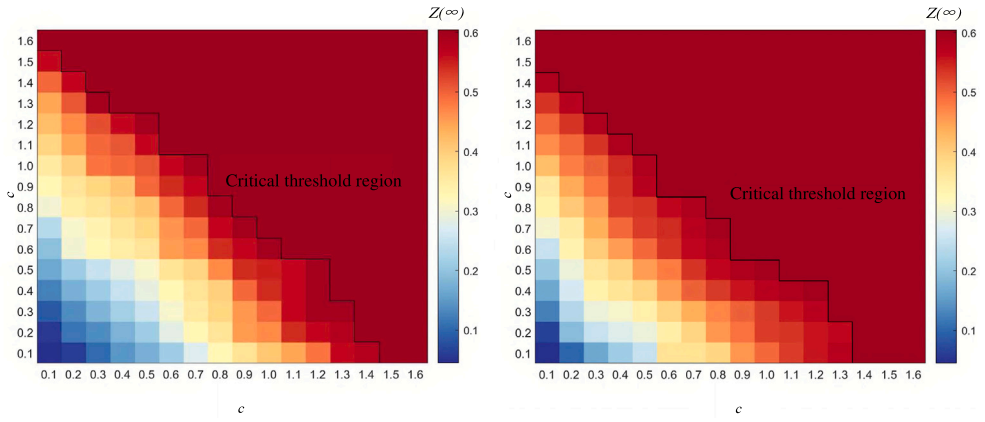
Fig. 18 shows the cascade failure process of the network in two attack scenarios with varying β_s. In the service network attack scenario, optimizing β_s leads to a faster and more significant improvement in cascade reliability compared to the optimization of β_c, which further emphasizes the need for different capacity allocation strategies based on attack types.

Fig. 19 shows the network cascade reliability in two attack scenarios with varying δ_s. As δ_s increases, cascade reliability improves. Similar to δ_c, there exists a critical threshold δ_s^*. Once δ_c exceeds δ_s^*, the cascade reliability no longer increases. In the actual industrial system, increasing δ_s enhances the overload tolerance of service nodes. This improvement provides a longer time window to address faults, thereby reducing the risk of production interruptions.

Fig. 20 shows the cascade failure process of the network in two attack scenarios with varying δ_s. Similar to δ_c, increasing δ_s within a specific range slightly improves cascade reliability without affecting the failure steps. However, once δ_s exceeds the maximum value in this range, further increases significantly reduce failure steps and enhance cascade reliability.

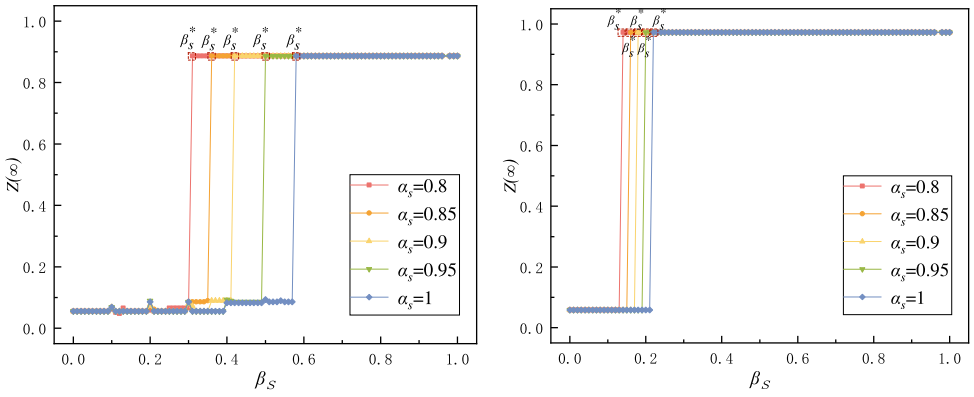
Fig. 21 shows the heatmap of IIoT system cascade reliability within the parameter space $[\delta_s, \beta_s]$ in the two attack scenarios. The result further confirms the critical thresholds δ_s^* and step values β_s^*, forming a reliability extremum region. Comparing the size and cascade reliability in both attack scenarios further confirms that cyber network attacks cause more significant damage to IIoT than service network attacks.

Fig. 22 shows the network cascade reliability in two attack scenarios with varying γ_s. As γ_s increases, the node survival rate shows a decreasing trend, indicating a reduction in cascade reliability. This



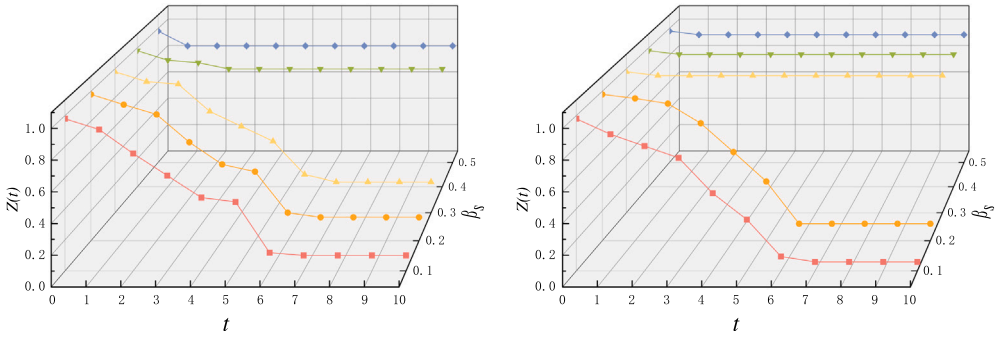
(a) Node attack on the cyber network (b) Node attack on the service network

Fig. 16. Network cascade reliability within the parameter space $[\delta_c, \beta_c]$ in the two attack scenarios ($\alpha_c = 0.8$, $\alpha_s = 0.8$, $\beta_s = 0.3$, $\delta_s = 0.5$, $\gamma_s = 0$, $q = 0.1$).



(a) Node attack on the cyber network (b) Node attack on the service network

Fig. 17. Network cascade reliability with varying α_s and β_s in the two attack scenarios ($\alpha_c = 0.8$, $\beta_c = 0.3$, $\delta_c = 0.5$, $\delta_s = 0.5$, $\gamma_s = 0$, $q = 0.06$).



(a) Node attack on the cyber network (b) Node attack on the service network

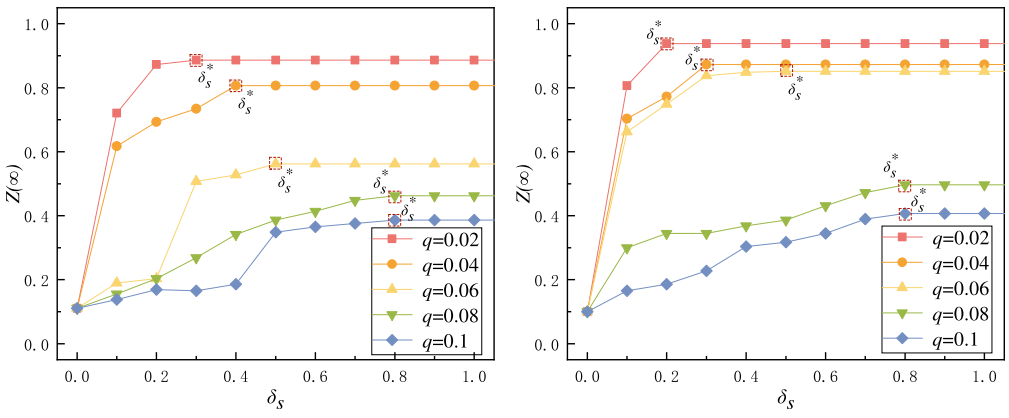
Fig. 18. Network cascade failure process with varying β_s in the two attack scenarios ($\alpha_c = 0.8$, $\beta_c = 0.3$, $\delta_c = 0.5$, $\alpha_s = 0.8$, $\delta_s = 0.5$, $\gamma_s = 0$, $q = 0.06$).

phenomenon can be attributed to two factors: (1) higher γ_s increases the minimum load threshold for service nodes, leading to higher initial loads and a greater risk of overload; (2) the increase of γ_s weakens the ability of service nodes to withstand cascade failures, making them more vulnerable to underloaded and triggering further failures in the IIoT system.

Fig. 23 shows the cascade failure process of the network in two attack scenarios with varying γ_s. As γ_s increases, the cascade failure steps tend to increase. This is due to the differentiation of nodes within the same community and nodes across communities in our load update of service nodes. Tolerable overload in the previous round of load update, may be influenced by upstream and downstream nodes in the next round, leading to a reduction in load and a recovery to normal states. Therefore, the service network can handle more load, which leads to an increase in cascade steps.

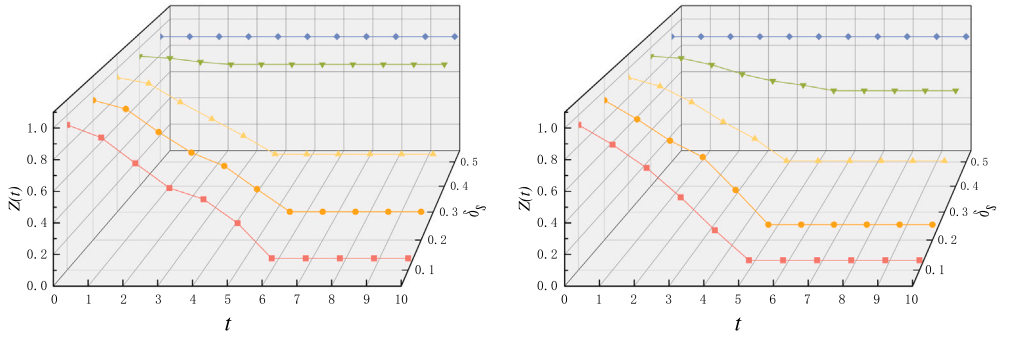
5.4. Composition of failed nodes

Fig. 24 shows the composition of failed nodes in the cyber and service network in two attack scenarios. It is easy to observe that isolated failure nodes account for the largest proportion in the cyber network. This is because in our proposed cascade failure model, a



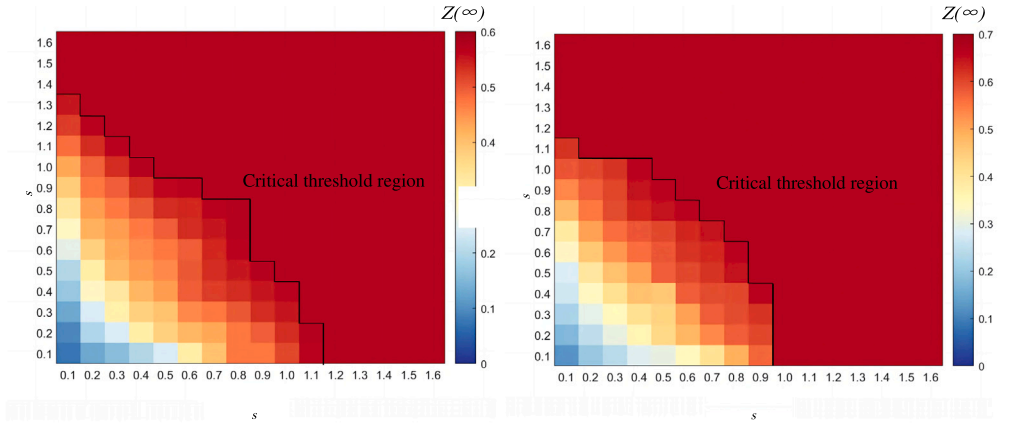
(a) Node attack on the cyber network (b) Node attack on the service network

Fig. 19. Network cascade failure process with varying δ_s in the two attack scenarios ($\alpha_c = 0.8$, $\beta_c = 0.3$, $\delta_c = 0.5$, $\alpha_s = 0.8$, $\delta_s = 0.5$, $\gamma_s = 0$, $q = 0.06$).



(a) Node attack on the cyber network (b) Node attack on the service network

Fig. 20. Network cascade failure process with varying δ_s in the two attack scenarios ($\alpha_c = 0.8$, $\beta_c = 0.3$, $\delta_c = 0.5$, $\alpha_s = 0.8$, $\beta_s = 0.3$, $\gamma_s = 0$, $q = 0.06$).



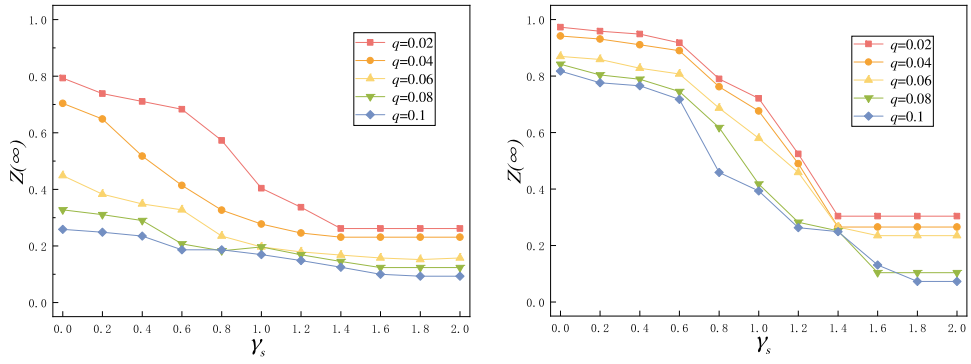
(a) Node attack on the cyber network (b) Node attack on the service network

Fig. 21. Network cascade reliability within the parameter space $[\delta_s, \beta_s]$ in the two attack scenarios ($\alpha_c = 0.8$, $\beta_c = 0.3$, $\delta_c = 0.5$, $\gamma_s = 0$, $q = 0.1$).

routing node can communicate with multiple terminal nodes. When a routing node fails, a large number of terminal nodes become isolated due to their inability to communicate with the routing node. In the service network, interdependent failure nodes are most prevalent in the cyber node attack scenario, while overloaded failure nodes are most common in the service node attack scenario. This is because the failure of a cyber node causes all connected service nodes to fail, whereas the failure of a service node only causes the connected routing node to fail. This differential failure propagation pattern makes the service network more sensitive to cyber node failures, while service node failures are less likely to propagate to the cyber network.

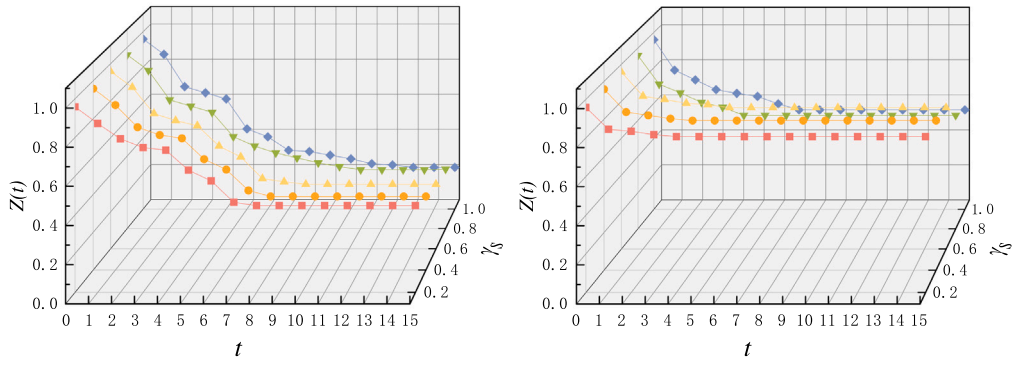
5.5. Case study

Through the above experiments, we validated the rationality of the proposed cascade failure model and studied the impact of key parameters on IIoT cascade failures through simulations. To further assess the applicability of the proposed system model, we apply it to different industrial manufacturing scenarios. Then, we explore the



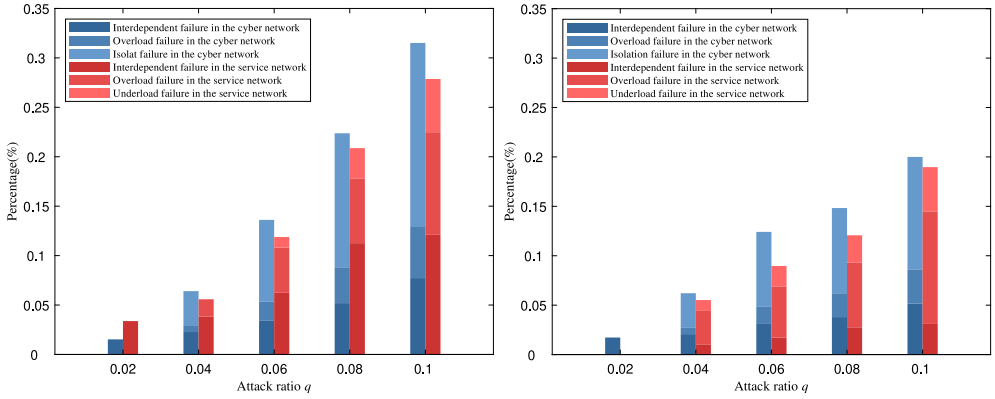
(a) Node attack on the cyber network (b) Node attack on the service network

Fig. 22. Network cascade reliability with varying γ_s in the two attack scenarios ($\alpha_c = 0.8$, $\beta_c = 0.3$, $\delta_c = 0.5$, $\alpha_s = 0.8$, $\beta_s = 0.3$, $\delta_s = 0.5$).



(a) Node attack on the cyber network (b) Node attack on the service network

Fig. 23. Network cascade failure process with varying γ_s in the two attack scenarios ($\alpha_c = 0.8$, $\beta_c = 0.3$, $\delta_c = 0.5$, $\alpha_s = 0.8$, $\beta_s = 0.3$, $\delta_s = 0.5$, $q = 0.06$).



(a) Node attack on the cyber network (b) Node attack on the service network

Fig. 24. Composition of failed nodes with different attack ratio q ($\alpha_c = 0.8$, $\beta_c = 0.3$, $\delta_c = 0.5$, $\alpha_s = 0.8$, $\beta_s = 0.3$, $\delta_s = 0.5$, $\gamma_s = 0.2$, $q = 0.06$).

performance of these systems in responding to cascade failures. Based on of Electronics Industry (2023), Sweeney, Nair, and Cormican (2023), we select four typical IIoT scenarios: household appliance manufacturing scenario, chemical equipment manufacturing scenario, medical device manufacturing scenario, and engineering vehicle manufacturing scenario. The simulation design involved two steps: (1) constructing a dual-layer network model for each scenario using the proposed IIoT modeling method and defining network parameters; (2) initiating cascade failures via a multi-point attack strategy to visualize the failure propagation.

Table 3 presents the dual-layer IIoT layouts for four typical industrial manufacturing scenarios with different sizes and complexities. The household appliance scenario has 53 cyber nodes and 22 service nodes; the chemical equipment scenario has 166 cyber nodes and 45 service nodes; the medical device scenario has 311 cyber nodes and 75 service nodes; and the engineering vehicle scenario has 209 cyber nodes and 100 service nodes. The household appliance scenario has a smaller network scale due to simpler processes and less data tracking. In contrast, the chemical equipment scenario is more complex and larger. Medical device and engineering vehicle manufacturing involve more intricate processes and higher precision demands, leading to a larger network. The medical device scenario, which requires stricter control and more tracking data, has the largest cyber network.

Table 3
The dual-layer IIoT layout for four different industrial manufacturing scenarios.

The layout of IIoT				
Industrial manufacturing scenarios	Household appliance manufacturing	Chemical equipment manufacturing	Medical device manufacturing	Engineering vehicle manufacturing

Table 4
Node attributes in the cyber network.

Industrial scenarios	c_i	Type
Household appliance manufacturing	c_1	Cloud
	$c_2 \sim c_4$	Gateway nodes
	$c_5 \sim c_{22}$	Routing nodes
	$c_{23} \sim c_{53}$	Terminal nodes
Chemical equipment manufacturing	c_1	Cloud
	$c_2 \sim c_7$	Gateway nodes
	$c_8 \sim c_{57}$	Routing nodes
	$c_{58} \sim c_{166}$	Terminal nodes
Medical device manufacturing	c_1	Cloud
	$c_2 \sim c_{11}$	Gateway nodes
	$c_{12} \sim c_{81}$	Routing nodes
	$c_{82} \sim c_{311}$	Terminal nodes
Engineering vehicle manufacturing	c_1	Gloud
	$c_2 \sim c_7$	Gateway nodes
	$c_8 \sim c_{63}$	Routing nodes
	$c_{64} \sim c_{209}$	Terminal nodes

Table 5
Node attributes in the service network.

Industrial scenarios	s_i	Type	$\alpha_{i,j,k}$	η_i
Household appliances manufacturing	$s_1 \sim s_5$	Cutting nodes	1.01~1.2	0.70~0.88
	$s_6 \sim s_{10}$	Drying nodes	0.96~1.11	0.70~0.88
	$s_{11} \sim s_{18}$	Trimming nodes	0.96~1.15	0.60~0.82
	$s_{19} \sim s_{22}$	Material handling nodes	0.88~0.96	0.72~0.92
Chemical equipment manufacturing	$s_1 \sim s_{15}$	Mechanical assembly nodes	0.80~1.02	0.62~0.72
	$s_{16} \sim s_{26}$	Welding nodes	0.92~1.12	0.66~0.83
	$s_{27} \sim s_{34}$	Bolt fastening nodes	0.99~1.20	0.71~0.89
	$s_{35} \sim s_{45}$	Material handling nodes	0.92~1.12	0.66~0.83
Medical device manufacturing	$s_1 \sim s_{16}$	Etching nodes	0.92~1.12	0.60~0.73
	$s_{17} \sim s_{34}$	Printing nodes	1.08~1.20	0.77~0.83
	$s_{35} \sim s_{42}$	Drilling nodes	1.02~1.20	0.65~0.86
	$s_{43} \sim s_{56}$	Reflow soldering nodes	0.85~1.05	0.60~0.80
	$s_{57} \sim s_{75}$	Material handling nodes	0.99~1.16	0.55~0.77
Engineering vehicle manufacturing	$s_1 \sim s_{18}$	Inspection nodes	0.82~0.98	0.62~0.80
	$s_{19} \sim s_{38}$	Classification nodes	0.88~1.08	0.60~0.78
	$s_{39} \sim s_{80}$	Reinspection nodes	0.80~1.07	0.50~0.66
	$s_{81} \sim s_{100}$	Material handling nodes	0.83~1.09	0.60~0.78

Building on the above analysis, we set the data flow density at each cyber node to follow a normal distribution, based on statistical research results on data flows in IIoT (Tang, Zhu, Zhang, Guizani, & Rodrigues, 2022). Additionally, we have provided detailed attributes for the dual-layer IIoT models in four different manufacturing scenarios, considering the assumptions made in Njah and Cheriet (2021) on task distribution for service units and the characteristics of each scenario. These attributes are presented in Tables 4 and 5.

Tables 6 and 7 show the cascade failure propagation performance and cascade reliability in the four different manufacturing scenarios. Through comparative analysis, significant differences in the cascade failure propagation process across different industrial manufacturing scenarios are observed, and we can draw the following conclusions.

The household appliance manufacturing scenario exhibits the widest range of cascade failures and the worst reliability. Among the four different manufacturing scenarios, the household appliance manufacturing scenario has the smallest network size. Typically, a smaller network size leads to fewer connections between nodes and limited backup and redundant resources, making the entire system more vulnerable to cascade failures. Comparing cascade failure situations in the medical device and engineering vehicle manufacturing scenarios, the former shows higher cascade reliability when cyber nodes are attacked due to its larger cyber network. In contrast, despite similar cyber network scales for the chemical equipment and engineering vehicle manufacturing scenarios, the engineering vehicle manufacturing scenario exhibits lower cascade reliability than the chemical equipment scenario. This is due to its more complex production process and larger service network. When network scales are large and attack proportions are high, service network failures are similar, but cyber network failures differ significantly. This phenomenon occurs due to the special load update mechanism of the service network and the special coupling mechanism of the dual-layer network.

Based on the above analysis, the applicability of the proposed model is first verified. Secondly, applying it to real industrial scenarios can provide a unique cyber-service coupling perspective, along with a detailed and in-depth study of IIoT. This not only enhances our

Table 6
The cascade failure propagation performance for four different manufacturing scenarios.

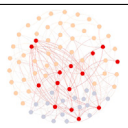
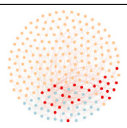
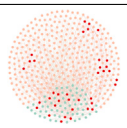
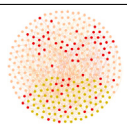
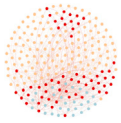
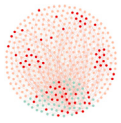
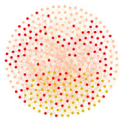
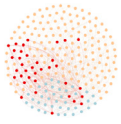
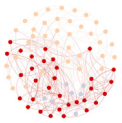
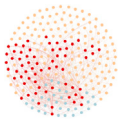
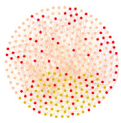
			Household appliance manufacturing	Chemical equipment manufacturing	Medical device manufacturing	Engineering vehicle manufacturing
Cascade failure propagation performance	Node attack on the service network	$q = 0.05$				
		$q = 0.1$				
	Node attack on the cyber network	$q = 0.05$				
		$q = 0.1$				

Table 7
The cascade reliability for four different manufacturing scenarios.

		Household appliance manufacturing	Chemical equipment manufacturing	Medical device manufacturing	Engineering vehicle manufacturing
Node attack on the service network	$q = 0.05$	0.80	0.82	0.86	0.78
	$q = 0.1$	0.05	0.62	0.60	0.50
Node attack on the cyber network	$q = 0.05$	0.87	0.86	0.91	0.84
	$q = 0.1$	0.56	0.75	0.82	0.54

understanding of industrial production process but also provides strong guidance for studying potential cascade failures in actual industrial production scenarios.

6. Conclusions and the future work

This paper proposes an industrial IIoT cascade failure model based on task decomposition and service communities. Through extensive experiments, the rationality of the proposed system model is verified and the effects of modeling parameters are explored. The findings offer theoretical guidance for constructing reliable IIoT systems in several aspects:

- Cascade failures caused by attack on the cyber network result in much more damage to the IIoT than the attack on the service network. This observation suggests that we should emphasize the security and stability of the cyber network when designing attack-resistant network strategies;
- Isolated failures are the main cause of performance degradation of the cyber network in cascade failures;
- Interdependent failures are the main cause for the decline of service network performance in cascade failures;
- IIoT cascade reliability can be improved by increasing capacity resources and enhancing equipment overload capabilities. However, these methods will inevitably increase construction costs, thus a balance between cost and benefit should be considered in practical applications;
- In IIoT cascade failures, a system with a larger network size implies more connections between nodes and more backup and redundant resources among nodes, and thus systems with larger network sizes typically show better cascade failure performance.

Many studies have shown that network optimization strategies can effectively help networks resist cascade failures (Guo, Tu, Guo, Hu, & Su, 2023; Zhou, Coit, Felder, & Tsianikas, 2023). Therefore, in our future work, we will focus on optimizing IIoT cascade reliability. We consider that the cascade reliability of the entire IIoT system should be improved by co-optimizing both the cyber network and the service network. According to the different characteristics of the cyber network and the service network, we can adopt different optimization strategies. For the cyber network, we can choose network topology optimization strategy. The topology structure is a key factor affecting cascade reliability, and optimizing the cyber network topology can effectively enhance the cascade reliability of the cyber network. For the service network, we cannot change its topology because the connections of the production chain and the production process are fixed. Therefore, we can choose to optimize the resource configurations to improve the cascade reliability of the service network.

CRediT authorship contribution statement

Lingli Zhu: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Resources, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Xiuwen Fu:** Writing – review & editing, Writing – original draft, Validation, Supervision, Resources, Project administration, Methodology, Funding acquisition, Formal analysis, Conceptualization. **Xiangwei Liu:** Writing – review & editing, Visualization, Validation, Supervision, Resources,

Project administration, Investigation, Formal analysis. **Shichang Du:** Writing – review & editing, Visualization, Validation, Supervision, Project administration, Methodology, Investigation, Formal analysis.

Acknowledgments

This work is supported by National Natural Science Foundation of China under Grant No. 92467101 and 52275499; Shanghai Soft Science Research Project, China under No. 24692113700.

Data availability

No data was used for the research described in the article.

References

Ali, Y., & Khan, H. U. (2022). GTM approach towards engineering a features-oriented evaluation framework for secure authentication in IIoT environment. *Computers & Industrial Engineering*, *168*, Article 108119.

Chen, D., Sun, D., Yin, Y., Dhamotharan, L., Kumar, A., & Guo, Y. (2022). The resilience of logistics network against node failures. *International Journal of Production Economics*, *244*, Article 108373.

Cheng, Y., Gao, Y., Wang, L., Tao, F., & Wang, Q.-G. (2023). Graph-based operational robustness analysis of industrial Internet of things platform for manufacturing service collaboration. *International Journal of Production Research*, *61*(13), 4237–4264.

Coito, T., Firme, B., Martins, M. S., Costigliola, A., Lucas, R., Figueiredo, J., et al. (2022). Integration of IIoT architectures for dynamic scheduling. *Computers & Industrial Engineering*, *171*, Article 108387.

Dong, R., Wang, Z., Liu, R., Li, H., Jia, X., & Wang, F. (2023). Robustness analysis of chemical process systems based on complex network non-linear load capacity model. *Canadian Journal of Chemical Engineering*, *101*(2), 953–966.

of Electronics Industry, P. H. (2023). *China internet development report 2022: Blue book for world internet conference*. Springer Nature.

Fu, X., Li, Q., & Li, W. (2023). Modeling and analysis of Industrial IoT reliability to cascade failures: An information-service coupling perspective. *Reliability Engineering & System Safety*, *239*, Article 109517.

Fu, X., Pace, P., Aloi, G., Guerrieri, A., Li, W., & Fortino, G. (2023). Tolerance analysis of cyber-manufacturing systems to cascading failures. *ACM Transactions on Internet Technology*, *23*(4), 1–23.

Fu, X., Pace, P., Aloi, G., Li, W., & Fortino, G. (2021). Cascade failures analysis of Internet of Things under global/local routing mode. *IEEE Sensors Journal*, *22*(2), 1705–1719.

Fu, X., Wang, Y., Yang, Y., & Postolache, O. (2022). Analysis on cascading reliability of edge-assisted Internet of Things. *Reliability Engineering & System Safety*, *223*, Article 108463.

Fu, X., Yao, H., & Yang, Y. (2019). Exploring the invulnerability of wireless sensor networks against cascading failures. *Information Sciences*, *491*, 289–305.

Giampieri, A., Ling-Chin, J., Ma, Z., Smallbone, A., & Roskilly, A. (2020). A review of the current automotive manufacturing practice from an energy perspective. *Applied Energy*, *261*, Article 114074.

Gulati, K., Boddu, R. S. K., Kapila, D., Bangare, S. L., Chandnani, N., & Saravanan, G. (2022). A review paper on wireless sensor network techniques in Internet of Things (IoT). *Materials Today: Proceedings*, *51*, 161–165.

Guo, T., Tu, L., Guo, Y., Hu, J., & Su, Q. (2023). Control-capacity analysis and optimized construction for controlled interdependent networks. *Physica A. Statistical Mechanics and its Applications*, *616*, Article 128597.

Huang, W., Zhang, T., & Yao, X. (2022). Optimization for sequential communication line attack in interdependent power-communication network. *Physica A. Statistical Mechanics and its Applications*, *592*, Article 126837.

Lee, J., Chua, P. C., Chen, L., Ng, P. H. N., Kim, Y., Wu, Q., et al. (2023). Key enabling technologies for smart factory in automotive industry: Status and applications. *International Journal of Precision Engineering and Manufacturing-Smart Technology*, *1*(1), 93–105.

Li, P., Cheng, Y., & Tao, F. (2020). Failures detection and cascading analysis of manufacturing services collaboration toward industrial internet platforms. *Journal of Manufacturing Systems*, *57*, 169–181.

Li, R., Long, C., He, J., & Li, L. (2024). Accelerating smart manufacturing technology adoption: An interdependency perspective on technology adoption. *Technology Analysis & Strategic Management*, 1–18.

Liang, Z., Parlikad, A. K., Srinivasan, R., & Rasmekomen, N. (2017). On fault propagation in deterioration of multi-component systems. *Reliability Engineering & System Safety*, *162*, 72–80.

Lin, C.-T., Wu, S.-L., & Lee, M.-L. (2017). Cyber attack and defense on industry control systems. In *2017 IEEE conference on dependable and secure computing* (pp. 524–526).

Lv, H., Wu, Z., Zhang, X., Jiang, B., & Gao, Q. (2022). Cascading failure analysis of hierarchical industrial wireless sensor networks under the impact of data overload. *Machines*, *10*(5), 380.

Njah, Y., & Cheriet, M. (2021). Parallel route optimization and service assurance in energy-efficient software-defined industrial IoT networks. *IEEE Access*, *9*, 24682–24696.

Qiu, T., Lu, Z., Li, K., Xue, G., & Wu, D. O. (2020). An adaptive robustness evolution algorithm with self-competition for scale-free Internet of Things. In *IEEE INFOCOM 2020-IEEE conference on computer communications* (pp. 2106–2115). IEEE.

Ren, T., Luo, T., Li, S., Xing, L., & Xiang, S. (2022). Review on R&D task integrated management of intelligent manufacturing equipment. *Neural Computing and Applications*, *34*(8), 5813–5837.

Romero, D., Taisch, M., Acerbi, F., Khan, M. A., Andersen, A.-L., Arioli, V., et al. (2023). *2023 world manufacturing report: New business models for the manufacturing of the future* (Ph.D. thesis), World Manufacturing Foundation.

Sefati, S., Mousavinasab, M., & Zareh Farkhady, R. (2022). Load balancing in cloud computing environment using the Grey wolf optimization algorithm based on the reliability: Performance evaluation. *Journal of Supercomputing*, *78*(1), 18–42.

Sweeney, D., Nair, S., & Cormican, K. (2023). Scaling AI-based industry 4.0 projects in the medical device industry: An exploratory analysis. *Procedia Computer Science*, *219*, 759–766.

Tanase, A. G., Serban, D., Dobrin, C.-O., Banta, V., et al. (2023). The impact of intelligent technologies in the context of industry 4.0 on the production processes found in the automotive industry. A case study of investment. *Annals of the University of Craiova, Economic Sciences Series*, *1*(51).

Tang, C., Zhu, C., Zhang, N., Guizani, M., & Rodrigues, J. J. (2022). Sdn-assisted mobile edge computing for collaborative computation offloading in Industrial Internet of Things. *IEEE Internet of Things Journal*, *9*(23), 24253–24263.

Wang, Y., Fu, X., Yang, Y., & Postolache, O. (2021). Analysis on cascading robustness of energy-balanced scale-free wireless sensor networks. *AEU-International Journal of Electronics and Communications*, *140*, Article 153933.

Xiao, Y., Li, C., Song, L., Yang, J., & Su, J. (2021). A multidimensional information fusion-based matching decision method for manufacturing service resource. *IEEE Access*, *9*, 39839–39851.

Xing, L., Morrissette, B. A., & Dugan, J. B. (2014). Combinatorial reliability analysis of imperfect coverage systems subject to functional dependence. *IEEE Transactions on Reliability*, *63*(1), 367–382.

Yang, X., Qian, Z., Zhang, X., Zhao, D., Peng, H., Zhu, D., et al. (2022). Cascading-failures effect on heterogeneous internet of things systems under targeted selective attack. *Security and Communication Networks*, *2022*(1), Article 6848156.

Ye, Z., Wen, T., Liu, Z., Song, X., & Fu, C. (2016). Fault-tolerant scheme for cascading failure of scale-free wireless sensor networks. In *2016 IEEE international conference on information and automation* (pp. 2006–2011). IEEE.

Yin, D., Huang, W., Shuai, B., Liu, H., & Zhang, Y. (2022). Structural characteristics analysis and cascading failure impact analysis of urban rail transit network: From the perspective of multi-layer network. *Reliability Engineering & System Safety*, *218*, Article 108161.

Yin, R.-R., Liu, B., Liu, H.-R., & Li, Y.-Q. (2014). The critical load of scale-free fault-tolerant topology in wireless sensor networks for cascading failures. *Physica A. Statistical Mechanics and its Applications*, *409*, 8–16.

Yu, J., Xiao, B., & Cui, Y. (2023). Robustness of double-layer group-dependent combat network with cascading failure. *Electronics*, *12*(14), 3061.

Zhang, Y., Guo, Z., Qian, C., & Li, R. (2018). Investigation on process-aware based intelligent modeling of bottom layer manufacturing resources and self-adaptive collaborative optimization methodology. *Journal of Mechanical Engineering*, *54*(16), 1–10.

Zhao, Y., Sun, T., & Liu, Y. (2024). Reliability analysis of a loading dependent system with cascading failures considering overloads. *Quality and Reliability Engineering International*, *40*(3), 1182–1196.

Zhao, G., & Xing, L. (2020). Reliability analysis of IoT systems with competitions from cascading probabilistic function dependence. *Reliability Engineering & System Safety*, *198*, Article 106812.

Zhong, X., & Liu, R. (2024). Robustness analysis of large scientific facilities development network with different cascading failure modes. *Computers & Industrial Engineering*, Article 110281.

Zhou, J., Coit, D. W., Felder, F. A., & Tsianikas, S. (2023). Combined optimization of system reliability improvement and resilience with mixed cascading failures in dependent network systems. *Reliability Engineering & System Safety*, *237*, Article 109376.