IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 21, 2019, accepted December 23, 2019, date of publication January 10, 2020, date of current version January 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2965588

A New Function-Topology-Based Method for Assessing Passive Safety of Mechatronics Systems

SHUAI LIN[1], LIMIN JIA[1], YANHUI WANG[1], AND HENGRUN ZHANG[2]
[1]State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China
[2]Department of Computer Science, Volgenau School of Engineering, George Mason University, Fairfax, VA 22030, USA

Corresponding author: Shuai Lin (linshuai2013@126.com)

This work was supported in part by the Youth Program of the National Natural Science Foundation of China under Grant 71901019.

ABSTRACT Various safety assessment models for predicting the future state of systems based on online monitoring data have been proposed. However, the complexity and interdependencies of mechatronics systems make it improbable to predict and prevent all possible failures/faults. Thus, it is also vital to assess the passive safety of mechatronics systems after a small or local fault occurs in order to make up for the shortcomings of online safety assessment. Hence, this paper proposes a passive safety assessment framework for a holistic system, according to the core chain of events related to component malfunction. The main contributions of this paper include three aspects. First, a component risk coefficient is proposed to more comprehensively reflect the risk degree of the component through analysis of a large number of fault data. Second, the fault propagation mechanism is explored to decrease the subjective effect based on the system topology and fault data. Third, a mapping function between system risk and system safety level is constructed; this function can provide support for management and maintenance personnel. A practical example of the bogie system for a high-speed train is examined to demonstrate the implementation and effectiveness and illustrate a potential application of the proposed passive safety method for assessing mechatronics system safety.

INDEX TERMS Vehicle safety, risk analysis, mechatronics, failure analysis, railway safety.

I. INTRODUCTION

Mechatronics systems [1], [2] include a combination of mechanical systems, electrical systems, telecommunications, a control system and computer science technologies. These systems have been applied in a wide variety of areas in modern society, such as the high-speed rail industry [3], [4], nuclear industry [5], aerospace industry [6] and manufacturing industry [7]. Currently, with mechatronics systems becoming increasingly complicated and demanding higher safety and reliability, the safety assessment of such systems is playing an increasingly important role in prognostics and health management (PHM) [8], [36] to ensure the safety of production. On the other hand, since mechatronics is a multidisciplinary field of engineering, this scenario results, to a large extent, in a trend of increasing difficulty in assessing system safety to cope with mechatronics systems.

The associate editor coordinating the review of this manuscript and approving it for publication was Guilin Yang.

According to different purposes, in current studies, safety can be divided into active safety and passive safety (PS) (see Fig. 1). **Active safety** (i.e., safety early warning) [9] includes and analyzes the set of safety features obtained by means of long-term monitoring and/or failure data to predict potential accidents and injuries as well as trends. **Passive safety** [10] refers to the system safety status and possible failure propagation mechanism derived after a small fault or failure has occurred to help minimize the accident loss and rationally determine the maintaining policy. In nature, accident prevention is the primary focus of the former, whereas the latter focuses on reducing accident losses.

Recently, the assessment of active safety has become increasingly popular with the development of PHM [8]. Various theories and models for evaluating active safety of mechatronics systems have been developed. The classic approaches include Monte Carlo simulation [11], neural networks [12], support vector machine (SVM) [13], belief rule [14], and Dempster–Shafer evidence theory [15]. Although active safety assessment is a sensible method for

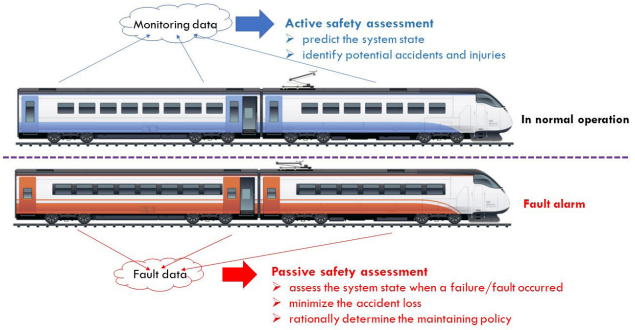


FIGURE 1. The difference between active safety and passive safety.

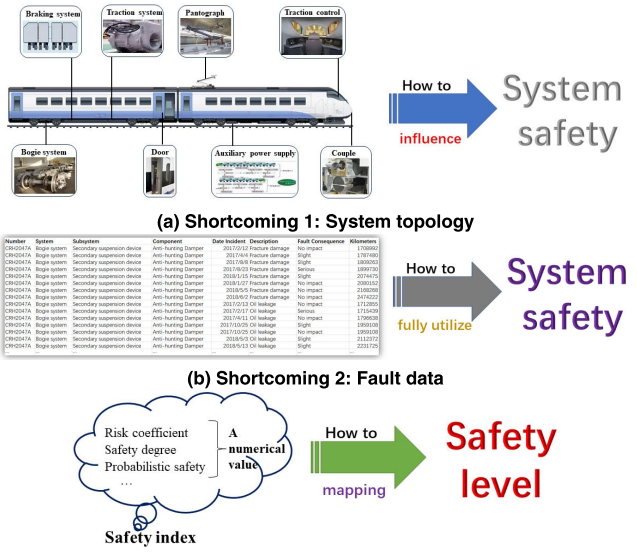


FIGURE 2. Three shortcomings of existing methods.

preventing accidents and reducing the loss of property and lives, it cannot effectively forecast or monitor all possible failures or faults. Analysis of large-scale fault data also proves this point of view. Hence, the evaluation of PS for mechatronics systems still has important practical significance and theoretical value for ensuring system safety. In particular, when a small failure or a local fault has occurred, analyzing the fault propagation mechanism and assessing system safety are essential steps for deciding the follow-up operation program and formulating the maintenance strategy. Thus, PS estimation for mechatronics systems, i.e., system safety assessment after a fault or local fault has occurred, is the main focus of this paper.

Various methods for assessing PS aim to identify the failure or events and their combinations that can lead to severe accidents based on functional relationships and assessing the probability of occurrence of each combination and the fault consequences. Due to a lack of operational data and fault data, several methods, such as Hazard and Operability Study (HAZOP) [16], Systems Theory Process Analysis (STPA) [17], and belief rule base [14], which usually perform qualitative analysis and are applicable at the design stage, mostly depend on expert experience. In addition, as we increase the complexity of the systems under design, traditional bottom-up or top-down safety assessment techniques in the running phase, such as failure mode and effect analysis (FMEA) [18], fault tree analysis (FTA) [19], event tree analysis (ETA) [20], Bayesian analysis [21] and Petri net analysis [22], become insufficient to ensure the system safety [17]. However, the positive is that these traditional approaches focus on addressing safety based on a chain of events related to component malfunction, which provides an effective introduction for assessing system safety. Generally, when these methods are applied to complex electromechanical systems, there are three main shortcomings.

1) For mechatronics systems, the functional relationship model, which reflects the relationships among failures, could not integrally describe the relationship between the system safety and system structure (see Fig. 2(a)). For example, failures are assumed to be independent events in FTA: the failure condition of a given item does not affect the probability of failure of any other block within the system modeled [23]. As another example, the state transition model of a Petri net usually has excessive reliance on the analyst's experience during the process of modeling, which could result in the model being too subjective [24]. Moreover, if the number of components that constitute the mechatronics system is large, the workload of the event trees for this system may also be large [25], which may lead to increased error.

2) Historical fault data usually contain multiple attributes of failure components, such as the fault description, failure time, and failure consequences, but these attributes are not yet fully explored and utilized in system safety assessment (see Fig. 2(b)). For instance, the same failure mode of a component may lead to different fault consequences. However, this diversity of fault consequences for the components is not reflected in the existing methods. In addition, several properties of fault data, such as failure consequences and fault descriptions, are often represented as words or sentences in an artificial language [26]. Considering the differences in knowledge and experience of different personnel, various uncertainties are present in maintenance team members' subjective assessments of fault information, such as imprecision, fuzziness and incompleteness. However, these influences are not considered in the process of system safety assessment.

3) The result of the PS assessment method is the risk probability of the system, while the mapping between the system safety level and this risk probability is never explicitly given (see Fig. 2(c)). For example, computing the probability of accident occurrence based on the Bayesian network has been proposed and used to evaluate system safety [27]. FTA also proposes the basic event failure probability for assessing system safety [28]. The occurrence probabilities of risk are defined to estimate system risk according to the Markov model [29]. However, because of differences in skills and experience, different policymakers could formulate different

operation strategies for the same risk probability, which may make maintenance engineers miss the best time to repair.

In view of the special importance of PS assessment, a novel framework for system safety assessment with respect to PS based on system topology and failure data is proposed to solve the three deficiencies of existing methods in this paper. Failure data are collected by the maintenance department. The system topology could be described as a network based on network theory. For example, in accord with work by Lin et al. [4], [33], [37], a network modeling method is proposed based on the coupling relationships between components (i.e., mechanical connections, electrical connections and informational connections).

The remainder of this paper is organized as follows. In Section 2, a novel safety assessment framework is proposed, and the difficult points in this new framework are described. Section 3 focuses on the system safety assessment method for mechatronics systems in terms of PS. In Section 4, a practical example for the bogie system of a high-speed train is presented to illustrate the application of this research in detail. The paper is concluded in Section 5.

II. NEW SAFETY ASSESSMENT FRAMEWORK AND PROBLEM FORMULATION

A. FRAMEWORK OF THE NEW SAFETY ASSESSMENT MODEL

The structure of the novel system safety assessment framework with respect to PS is composed of four main parts, as shown in Fig. 3. In *Part I*, the risk coefficient of the components is proposed based on historical failure data. In *Part II*, the fault propagation model is established in combination with the system topology and the risk coefficient. In *Part III*, based on the risk coefficient of the components, the system risk indicator is obtained from the perspective of fault propagation. In *Part IV*, a mapping function is introduced to reflect the relationship between the system risk indicator and the system safety level. The final comprehensive safety assessment results are the system's safety level. The modeling process of this framework coincides well with the change in system safety, i.e., component failure leads to fault spreading and ultimately causes system safety issues. In this paper, the new framework is named the PS model for simplicity.

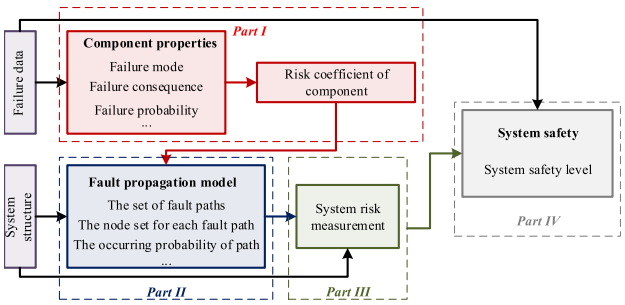


FIGURE 3. Structure of the new safety assessment model.

B. PROBLEM DESCRIPTION FOR SAFETY ASSESSMENT BASED ON THE PS MODEL

Based on the structure of the newly proposed PS model, as shown in Fig. 3, the following four problems must be solved to evaluate the system safety of the mechatronics systems in each part.

Problem 1: The core content for *Part I* is the construction of a risk coefficient measurement for the components by integrating the properties of the components from fault data. Although these properties abstracted from historical failure data can reflect the risk degree of the components, to some extent, some issues remain to be addressed when the risk of the component is evaluated on the basis of these data. First, some properties are too complex or too ill-defined to be reasonably described by traditional quantitative expressions [30]. For example, the severity of the failure effect is usually described by a linguistic variable instead of a crisp value. Second, multiple properties from different sources in the fault data may conflict with each other. Third, the uncertainty of failure data may stem from the lack of complete knowledge of the process and the observation by maintenance personnel or human errors by recorders. Thus, Problem 1 focuses on establishing a risk coefficient measurement of the component based on fault data, and the proposed measurement can overcome the issues outlined before:

$$RC_{v_i}(t) = f_1\left(S_{v_i}(t), F_{v_i}(t), P_{v_i}(t), \cdots\right) \tag{1}$$

where $f_1(\cdot)$ denotes a nonlinear function. $RC_{v_i}(t)$ is the risk coefficient of component v_i at time t. $S_{v_i}(t)$ describes the severity of the failure consequences for component v_i at time t. $F_{v_i}(t)$ is the failure frequency of component v_i at time t. $P_{v_i}(t)$ represents the probability of failure for component v_i at time t.

Problem 2: The purpose of *Part II* is to discuss the process of fault propagation in the mechatronics system when a fault or local fault has occurred, which provides a basis for assessing system safety. However, in view of the shortcomings of the existing fault spreading models [31], we recognize the two core elements that lead to failure propagation in the holistic system. 1) System topology. Fault propagation must be by way of certain media, and the topological structure of the system could provide the necessary medium. 2) Component risk. The risk degree of a component, which reflects the failure degree of the component, influences the breadth and depth of fault propagation. Therefore, Problem 2 focuses on developing a fault propagation model at the system level by using the risk coefficient of components and the holistic system structure:

$$S_t(k) = f_2\left(RC_V(k), G_s, V_f(k-1), \cdots\right) \tag{2}$$

where $S_t(k)$ denotes the system status at the kth step of fault propagation. $f_2(\cdot)$ denotes a nonlinear function. $RC_V = \left[RC_{v_1} \cdots RC_{v_N}\right]$ is the vector of risk coefficients for the components, where N is the number of components in the system. G_s is the topological network of the system. $V_f(k-1)$

represents the set of fault nodes at the $k-1$th step of fault propagation.

Problem 3: Quantifying system risk is a critical step to intuitively describe system safety. Thus, the main task of *Part III* is to construct a novel index to reflect the risk degree of the holistic system. Based on the definition of PS, if the consequences of fault propagation achieve an acceptable level, the system is regarded as safe; otherwise, the system is not regarded as safe. Thus, the consequences of fault spreading are crucial in system safety assessment. Furthermore, the risk degree of components, which are on all fault paths, determines the consequences of fault propagation. In other words, system risk relates to the consequences of fault propagation and component risk. Thus, from the definition of safety, Problem 3 focuses on constructing a system risk index in combination with fault propagation and component risk to quantitatively reflect the system risk level

$$SR(t) = f_3(RC_i(t), G_s, S_t(k)) \tag{3}$$

where $SR(t)$ denotes the system risk index at time t. $f_3(\cdot)$ denotes a nonlinear function.

Problem 4: Multiple people usually participate in the operation and maintenance of mechatronics systems, which may lead to the following situation. Due to the uncertainty and vagueness of different humans' subjective perception and experience in the system operating process, different people may take different approaches to address failure and select a maintenance strategy based on the system risk index, even if the value of this index is the same. To ensure system safety, the mapping relationship between the system risk index and the system safety level must be addressed to help administrators adjust the operation plan and help maintenance personnel formulate maintenance strategies in *Part IV*. Thus, Problem 4 focuses on establishing a mapping function between the system risk and system safety level

$$SL_l \rightarrow f_4(SR(t), SL_l) \tag{4}$$

where SL_l denotes the lth level of system safety. $f_4(\cdot)$ denotes a nonlinear function.

Four strategies to solve the above four problems are presented in the following section.

III. APPROACHES FOR THE SAFETY ASSESSMENT OF MECHATRONICS SYSTEMS

Four strategies are adopted to solve the above four problems in this section. Notably, this paper focuses on the **PS** assessment of a holistic system. Therefore, a basic premise of research on system safety assessment is that a component has failed or local components have failed. For mathematical convenience, assume that the system fails at time t and let $m_{v_i}(t)$ represent the mth fault mode of component v_i that occurred at time t.

A. RISK COEFFICIENT OF COMPONENTS

To solve Problem 1, the risk coefficient of components is proposed based on an improved fuzzy evidential method, taking into account the characteristics of historical failure data. The detailed implementation steps are described as follows.

Step 1: Selection of the properties of the components.

In this paper, three properties of the components, namely, the severity of the failure effect, the frequency of the fault and the failure probability, are selected to assess the risk of components based on the fault data and the definition of system safety. There are two main reasons. 1) In fault data, running time or running kilometers may be only numerical attribute. The frequency of the fault, which reflects the general trend of component failure, and the failure probability of components, which consider the impact of uncertainty, could be calculated based on this attribute. 2) According to the definition of system safety, system safety is related to the failure consequence. Hence, the severity of the failure effect is selected as one of properties.

Let $X_{v_i,m_{v_i}}(t) = \left\{S_{v_i,m_{v_i}}(t), F_{v_i,m_{v_i}}(t), P_{v_i,m_{v_i}}(t)\right\}$ denote the set of properties for component v_i at time t, where $S_{v_i,m_{v_i}}(t)$ is the severity of the failure effect for component v_i when this component experienced the mth fault mode at time t. $F_{v_i,m_{v_i}}(t)$ represents the frequency of failure for component v_i if this component experienced the mth fault mode at time t. $P_{v_i,m_{v_i}}(t)$ denotes the failure probability of component v_i when this component failed and led to the mth fault mode at time t.

Step 2: Calculating the three properties of the components.

To address the shortcomings of fault data, such as the qualitative language description of some attributes and the uncertainty and vagueness of recorders, the above three selected attributes are divided into ten ranks d_l ($l = 1, \cdots, 10$) in turn, and the values of each rank are reported in Table 1.

TABLE 1. The rankings of the three properties.

Ranking	$S_{v_i,m_{v_i}}(t)$		$F_{v_i,m_{v_i}}(t)$ and $P_{v_i,m_{v_i}}(t)$	
	Criteria	Value	Frequency	Value
d_1=1	None	1	Remote	$[0,0.1)$
d_2=2	Very minor	2	Low	$[0.1,0.2)$
d_3=3	Minor	3	Low^{+}	$[0.2,0.3)$
d_4=4	Very low	4	Low^{++}	$[0.3,0.4)$
d_5=5	Low	5	Moderate	$[0.4,0.5)$
d_6=6	Moderate	6	Moderate^{+}	$[0.5,0.6)$
d_7=7	High	7	High	$[0.6,0.7)$
d_8=8	Very high	8	High^{+}	$[0.7,0.8)$
d_9=9	Hazardous with warning	9	Very high	$[0.8,0.9)$
d_{10}=10	Hazardous without warning	10	Very high^{+}	$[0.9,1]$

Then, the severity of the failure effect for component v_i, which failed via the mth fault mode at time t, can be expressed by a set of vectors $\mu_{S_{v_i,m_{v_i}}(t)}$ instead of an exact

number $S_{v_i,m_{v_i}}(t)$.

$$\mu_{S_{v_i,m_{v_i}}(t)} = \left\{\mu_{S_{v_i,m_{v_i}}(t)}(d_1), \cdots, \mu_{S_{v_i,m_{v_i}}(t)}(d_2), \cdots, \mu_{S_{v_i,m_{v_i}}(t)}(d_{10})\right\},$$
$$\mu_{S_{v_i,m_{v_i}}(t)}(d_l) = \begin{cases} \dfrac{S_{v_i,m_{v_i}}(t)}{d_l}, & S_{v_i,m_{v_i}}(t) \subset d_l \quad l = 1, \cdots, 10 \\ 0, & ifelse, \end{cases} \tag{5}$$

Similarly, the frequency of the failure of component v_i could be improved as

$$\mu_{F_{v_i,m_{v_i}}(t)} = \left\{\mu_{F_{v_i,m_{v_i}}(t)}(d_1), \mu_{F_{v_i,m_{v_i}}(t)}(d_2), \cdots, \mu_{F_{v_i,m_{v_i}}(t)}(d_{10})\right\},$$
$$\mu_{F_{v_i,m_{v_i}}(t)}(d_l) = \begin{cases} \dfrac{F_{v_i,m_{v_i}}(t)}{d_l}, & F_{v_i,m_{v_i}}(t) \subset d_l \quad d = 1, \cdots, 10 \\ 0, & if\ else, \end{cases} \tag{6}$$

The failure probability of component v_i can be rewritten as

$$\mu_{P_{v_i,m_{v_i}}(t)} = \left\{\mu_{P_{v_i,m_{v_i}}(t)}(d_1), \mu_{P_{v_i,m_{v_i}}(t)}(d_2), \cdots, \mu_{P_{v_i,m_{v_i}}(t)}(d_{10})\right\},$$
$$\mu_{P_{v_i,m_{v_i}}(t)}(d_l) = \begin{cases} \dfrac{P_{v_i,m_{v_i}}(t)}{d_l}, & P_{v_i,m_{v_i}}(t) \subset d_l \quad l = 1, \cdots, 10 \\ 0, & if\ else, \end{cases} \tag{7}$$

Step 3: Constructing the fuzzy mapping of the three properties.

We define three linguistic variables, low risk (L), medium risk (M) and high risk (H), to express the basic characteristic of the risk degree for the components. In this paper, we assume that the levels d_1 and d_2 of the attributes in Table 1 are absolutely L, d_5 and d_6 are absolutely M, and d_9 and d_{10} are absolutely H. $\mu_L(d)$, $\mu_M(d)$ and $\mu_H(d)$ are defined as the membership functions of L, M and H, where the cosine function is used to simulate the restrictions [32].

$$\mu_L = \begin{cases} 1, & 1 \le d \le 2 \\ 0.5 - 0.5\sin\dfrac{d-5.5}{7}\pi, & 2 \le d \le 9 \\ 0, & else, \end{cases}$$
$$\mu_M = \begin{cases} 0.5 + 0.5\cos\dfrac{d-5}{3}\pi, & 2 \le d \le 5 \\ 1, & 5 \le d \le 6 \\ 0.5 + 0.5\cos\dfrac{d-6}{3}\pi, & 6 \le d \le 9 \\ 0, & else, \end{cases}$$
$$\mu_H = \begin{cases} 0.5 + 0.5\sin\dfrac{d-5.5}{7}\pi, & 2 \le d \le 9 \\ 1, & 9 \le d \le 10 \\ 0, & else \end{cases} \tag{8}$$

Then, the fuzzy mapping of property $S_{v_i,m_{v_i}}(t)$ concerning the cth risk level can be formulated as

$$\rho_{S_{v_i,m_{v_i}}(t)}(c) = \frac{\sum_{l=1,\cdots,10} \mu_{S_{v_i,m_{v_i}}(t)}(d_l) \times \mu_c}{\sum_{A=L,M,H} \sum_{l=1,\cdots,10} \mu_{S_{v_i,m_{v_i}}(t)}(d_l) \times \mu_A}, \quad c \in A = \{L, M, H\} \tag{9}$$

Correspondingly, the fuzzy mapping of properties $F_{v_i,m_{v_i}}(t)$ and $P_{v_i,m_{v_i}}(t)$ concerning the cth risk level can be expressed as, respectively,

$$\rho_{F_{v_i,m_{v_i}}(t)}(c) = \frac{\sum_{l=1,\cdots,10} \mu_{F_{v_i,m_{v_i}}(t)}(d_l) \times \mu_c}{\sum_{A=L,M,H} \sum_{l=1,\cdots,10} \mu_{F_{v_i,m_{v_i}}(t)}(d_l) \times \mu_A}, \quad c \in A = \{L, M, H\} \tag{10}$$
$$\rho_{P_{v_i,m_{v_i}}(t)}(c) = \frac{\sum_{l=1,\cdots,10} \mu_{P_{v_i,m_{v_i}}(t)}(d_l) \times \mu_c}{\sum_{A=L,M,H} \sum_{l=1,\cdots,10} \mu_{P_{v_i,m_{v_i}}(t)}(d_l) \times \mu_A}, \quad c \in A = \{L, M, H\} \tag{11}$$

Step 4: Construction of the risk coefficient for the components.

The belief structures of all properties can be determined via Eqs. ((8)-(10)).

$$\alpha_{S_{v_i,m_{v_i}}(t)} = \left(\rho_{S_{v_i,m_{v_i}}(t)}(L), \rho_{S_{v_i,m_{v_i}}(t)}(M), \rho_{S_{v_i,m_{v_i}}(t)}(H)\right)$$
$$\alpha_{F_{v_i,m_{v_i}}(t)} = \left(\rho_{F_{v_i,m_{v_i}}(t)}(L), \rho_{F_{v_i,m_{v_i}}(t)}(M), \rho_{F_{v_i,m_{v_i}}(t)}(H)\right)$$
$$\alpha_{P_{v_i,m_{v_i}}(t)} = \left(\rho_{P_{v_i,m_{v_i}}(t)}(L), \rho_{P_{v_i,m_{v_i}}(t)}(M), \rho_{P_{v_i,m_{v_i}}(t)}(H)\right) \tag{12}$$

With pignistic probability transformation [33], the basic probability of different risk levels (including L, M and H) for the component v_i can be obtained:

$$p(c) = BetP\left(\left\{\alpha_{S_{v_i,m_{v_i}}(t)}, \alpha_{F_{v_i,m_{v_i}}(t)}, \alpha_{P_{v_i,m_{v_i}}(t)}\right\}\right), \quad c \in A = \{L, M, H\} \tag{13}$$

where Bet is the pignistic probability transformation function.

As a result, the risk coefficient of component v_i is denoted as

$$RC_{v_i}(t) = w_L \times p(L) + w_M \times p(M) + w_H \times p(H) \tag{14}$$

where w_L, w_M and w_H are the weights, which are determined using the center-of-gravity method [32].

B. FAULT PROPAGATION MODEL

In an attempt to overcome Problem 2, a novel fault propagation model is presented based on the system topology and risk coefficient. Due to the complexity of the fault propagation mechanism, we make the following assumptions about the fault propagation model under consideration. 1) The time of fault propagation is negligible. 2) Nodes that failed before repair never fail again. 3) Human factors and environmental

considerations are reflected in the failure data. The main steps of the proposed method to obtain the set of propagation paths are as follows.

Step 1: Construction of the topological network model of the mechatronics system.

According to network theory, the topology of a mechatronics system is modeled as a directed network, where nodes represent components and edges represent the relationships between components, such as mechanical connection, electrical connection and informational connection [31]. This model is called the topological network, and the explicit mathematical expression is given by

$$G_s(V, E, A, RC_V) \begin{cases} A = [a_{ij}]_{N\times N} \\ RC_v = \left[RC_{v_1} \ \cdots \ RC_{v_N} \right] \\ v_i \in V, e_{ij} \in E, i \le N, j \le N \end{cases} \tag{15}$$

where V represents the set of nodes. E is the set of edges. A is the adjacency matrix. $a_{ij} = 1\,(i \neq j)$ if and only if $e_{ij} \in E$; otherwise, $a_{ij} = 0$. N indicates the number of nodes in the topological network. RC_V denotes the vector of risk coefficients for the nodes.

Step 2: Determination of the propagation intensity for the node.

By analyzing the process of fault propagation, the propagation intensity of node v_i in the kth step of spreading is defined according to the principle of step-by-step diffusion:

$$PI_{v_j,e_{ij}}(k) = \left(PI_{v_i,e_{ri}}(k-1) \times SP_{e_{ij}}\right)^k \times RC_{v_j} \quad i \le N,\ j \le N \tag{16}$$

where $PI_{v_j,e_{ij}}(k)$ is the propagation intensity of node v_i at the kth step of spreading caused by fault node v_j. $SP_{e_{ij}}$ denotes the probability of spreading failure for edge e_{ij}. If v_r is the initial fault node, $PI_{v_i,e_{ti}}(0) = 1$.

Step 3: Establishing the system fault propagation model.

Fault propagation in the whole system has diversity and uncertainty. Thus, a fault propagation model at the system level is proposed to obtain all possible fault propagation paths:

$$\begin{aligned} S_t(k) &= \left(PI_V(k), V_f(k), V_0, Pa(k)\right) \\ PI_V(k) &= \left(PI_V(k-1) \times SP_E\right)^k \times RC_V \end{aligned} \tag{17}$$

where $S_t(k)$ is the system state at the kth step of spreading at time t. V_0 represents the set of fault nodes at the initial time. $Pa(k)$ denotes the set of fault paths. SP_E is the matrix of spreading failure for the edges.

Step 4: Determining the stopping conditions of fault propagation.

Numerous examples provide a clear indication that fault propagation is not endless. We summarize the stopping conditions of failure propagation as follows.

- ➢ If $V_0 \cup V_f(k=1) \cup \cdots \cup V_f(k=y) = V$, all nodes in the network fail. Thus, fault propagation stops in the topological network.
- ➢ If $V_f(k-1) \cap V_f(k) \neq \phi$, nodes that failed before maintenance fail again. According to the assumptions, when $V_f(k-1) \cap V_f(k) \neq \phi$, the nodes that belong to $V_f(k-1) \cap V_f(k)$ stop spreading.
- ➢ If $PI_{v_j,e_{ij}}(k) \le 10^{-8}$ [31], the node is safe and can propagate failure to other nodes.

The basic ideas of the fault propagation model are summarized in Fig. 4 below.

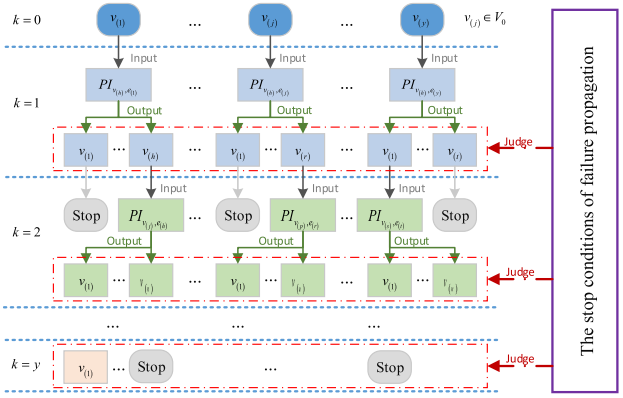


FIGURE 4. The idea of the fault propagation model.

C. SYSTEM RISK MEASUREMENT

Based on the topological network and risk coefficient of the nodes, a system safety measurement is proposed to address Problem 3 from the perspective of fault propagation. The detailed implementation steps are described as follows.

Step 1: Definition of node importance.

The better the connectivity of the network is, the greater the depth and breadth of fault propagation. Thus, a novel node importance is proposed from the perspective of network connectivity. The node importance is given by

$$\omega_{v_i} = \sum_{v_j} s_{ij} \left(\frac{1}{\langle DC \rangle}\right)^{d_{ij}}, \quad j \neq i,\ v_j \in V \tag{18}$$

where DC is the degree centrality. s_{ij} is the number of shortest paths from node v_i to node v_j. $\langle DC \rangle = \sum_{i=1}^{N} DC_i \Big/ N$ is the average degree. d_{ij} is the length of the shortest path from node v_i to node v_j.

Step 2: Construction of the path importance.

For the topological network, the failure of an important path has a greater impact on system safety. Here, the path importance is presented to measure the importance of the fault path from the perspective of network connectivity. The path importance of the path Pa is expressed as

$$\kappa_{Pa} = \delta_{Pa} \times \left(1 - \theta_1 \times \frac{\sum_{G_{Pa}} d_{ij}}{\sum_{G_s} d_{sq}} - \theta_2 \times \frac{\sum_{G_{pa}} g_{v_i}}{\sum_{G_s} g_{v_t}}\right), i \neq j, s \neq q \tag{19}$$

where d_{ij} is the shortest path length from node v_i to node v_j. G_{Pa} is the subgraph where the nodes and edges on the path in set Pa are deleted. g_{v_i} is the betweenness centrality of node v_i. θ_1 and θ_2 are the weights. δ_{Pa} is the probability of occurrence of the path Pa and is equal to the propagation intensity of the node in this path at the step of k_{final}, which is the terminal point. k_{final} is the number of steps of the final propagation.

Step 3: Definition of the system risk measurement.

Due to the complexity of the fault propagation mechanism, one or more fault paths may occur at the same time. The failure propagation model only gives all possible fault propagation paths, while it does not mean all paths occur. Therefore, if the number of fault paths is s, the number of system statuses is 2^s. Based on the node importance and path importance, the system risk index is proposed from a network perspective. Assume that the system status C occurs and there are y fault propagation paths. Then the mathematical expression of system risk index is written as

$$\begin{aligned} SR_C(t) &= \sum_{Pa \subset PA} \gamma_{Pa} \kappa_{Pa} \sum_{v_i \in V_{Pa}} \omega_{v_i} RC_{v_i}(t) \\ &\quad - \sum_{v_j \in V_{fault,C}} \omega_{v_j} RC_{v_j}(t) \\ PA &= \{Pa_1, \cdots, Pa_y\}, \quad V_{fault,C} = V_{Pa_1} \cup \cdots \cup V_{Pa_y} \\ C &= 1, 2, \cdots, 2^s \end{aligned} \tag{20}$$

where γ_{Pa} is the weight of the path Pa. $V_{fault,C}$ is the set of fault nodes at the system status C. V_{Pa_y} represents the set of fault nodes in the path Pa_y.

D. SYSTEM SAFETY ASSESSMENT

As mentioned in the previous section, different maintenance and management personnel may have different judgments about system safety, depending on only the system risk measurement. Therefore, according to the failure data, system safety is determined by the mapping relationship between the system risk and safety level. The detailed implementation steps are described as follows.

Step 1: Classification of the system safety level.

According to fault data and expert experience, system safety is divided into three levels: safe, medium unsafe and serious unsafe. The average system risk of each safety level (i.e., SR_{Safe} for safe level, $SR_{M-unsafe}$ for medium unsafe level and $SR_{S-unsafe}$ for serious unsafe level) is calculated by means of the combination of SVM [34] and a large amount of fault data.

Step 2: Calculation of the credibility of system risk.

For the system risk measurement $SR(t)$ at the time t, if the system is at different safety levels, the credibility is

$$\begin{aligned} \alpha_{SL}(C) &= \left(\frac{\|SR(t) - SR_C\|^2}{\sum_{SL} \|SR(t) - SR_{SL}\|^2} \right)^{\frac{-1}{m-1}}, \\ SL &= \{Safe, Mediumun - safe, Seriousun - safe\} \\ C &= 1, 2, \cdots, 2^s \end{aligned} \tag{21}$$

where SL is the set of system safety levels. m denotes the type of distance adopted in the algorithm, and m is a constant [14]. C represents the Cth failure status of the system.

Step 3: Determination of the system safety level.

Suppose the utility of the safety level SR_{SL} is denoted by $U(SR_{SL})$. The expected utility of system safety for the Cth failure status is given as

$$y(t) = \sum_{C=1}^{s} PI_C \sum_{SR_{SL}} U(SR_{SL}) \times \alpha_{SL}(C) \tag{22}$$

where α_{SL} is credibility. s represents the number of system statuses. PI_C denotes the occurrence probability of the Cth failure status of the system.

IV. CASE STUDY

The bogie system of a high-speed train synergistically integrates mechanics, electronics, control theory, and computer science within product design and manufacturing. Thus, the bogie system is a classic mechatronics system. To verify the proposed safety assessment model for mechatronics systems, the bogie system of CRHX (China Railway High-speed Train, such as CR400AF, CR400BF, CRH2, and CRH5) is used as a practical example in an experimental study, as shown in Fig. 5.

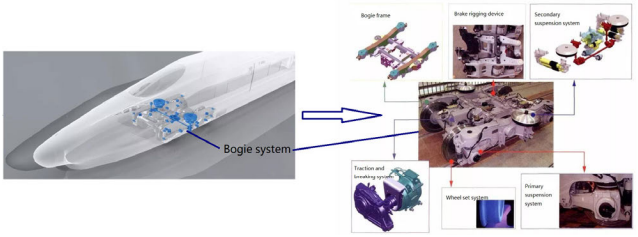


FIGURE 5. Bogie of a high-speed train system.

On the basis of the minimum maintenance unit, the bogie system can be divided into 44 components, as detailed in Table 2.

A. SAFETY ASSESSMENT OF THE BOGIE SYSTEM

Because the proposed method is an assessment approach oriented toward PS, fault data for 12 million kilometers are used as a substantial database for the safety evaluation. The fault data show that node v_2 fails at 12 million kilometers, and its failure mode is wear and tear. Subsequent case studies are based on these fault data.

Based on the above fault data, Fig. 6 plots the risk degree of the components for the bogie system in combination with Section 3.1. Fig. 6(a)-(c) shows the possibility that the components are at a low risk level (Fig. 6(a)), medium risk level (Fig. 6(b)) and high risk level (Fig. 6(c)). Fig. 6(d) expresses the risk coefficient of the components at 12 million kilometers. As revealed in Fig. 6, node v_2 has the highest risk coefficient. Because we assume that no fault propagation occurs at this time, the failed node v_2, in theory, has the

TABLE 2. Components in the bogie system.

Node	Component	Node	Component	Node	Component
v_1	Railway coupling	v_{10}	Boom of gearbox	v_{19}	Corbel for connection
v_2	Brake lining	v_{11}	Axle box cover	v_{20}	Shock absorber for traction motor
v_3	Brake caliper	v_{12}	Rubber pad	v_{21}	Air spring
v_4	Brake cylinder	v_{13}	Rubber Joint	v_{22}	Anti-hunting damper
v_5	Brake disks	v_{14}	Axle box spring	v_{23}	Leveling valve
v_6	Wheel	v_{15}	Primary vertical damper	v_{24}	Control value for air spring
v_7	Axle	v_{16}	Rotating arm axle box body	v_{25}	Secondary lateral damper
v_8	Axle box bearings	v_{17}	Stopping block (Primary)	v_{26}	Anti-roll bar shafts
v_9	Gearbox body	v_{18}	Bogie frame	…	…

highest level of risk. The theoretical results are found to coincide well with the actual results.

To analyze the impact of holistic structure on system safety, the topological network of the bogie system is constructed first in Fig. 7(a) [4] to quantify system structure and participate in quantitative analysis, where the number of edges is 115 and the nodes are in Table 2. Fig. 7(b) shows that the topological properties of the bogie system include degree centrality, betweenness centrality and closeness centrality [35]. One striking result apparent in Fig. 7(b) is that the bogie frame (node v_{18}) is the influential node from the perspective of structure.

According to the fault propagation model in Eq. (14), Table 3 illustrates the grade diffusing process of faults. The step number of fault propagation for the bogie system is 3, and the proportion of fault nodes is 6.8%, which are failure caused by failure spreading. Clearly, the number of failure nodes caused by fault propagation is relatively low because the bogie system, as a mechatronics system, has a high manufacturing cost, and the difficulty of the maintenance procedure calls for vast expenditure. To reduce costs and meet safety requirements, redundant structures and improved component reliability are considered in the design and manufacturing stage. These considerations limit the infinite propagation of faults to some extent.

Based on Eq. (17), Fig. 8(a) shows the importance of 44 nodes. Node v_{18} is the most critical node from the perspective of spreading. In other words, if this node fails, it has the greatest impact on the other nodes in the holistic topological network. Fig. 8(b) indicates the path importance for three possible fault propagation scenarios according to Eq. (18). For status 1, only fault path $v_2 \rightarrow v_3$ exists.

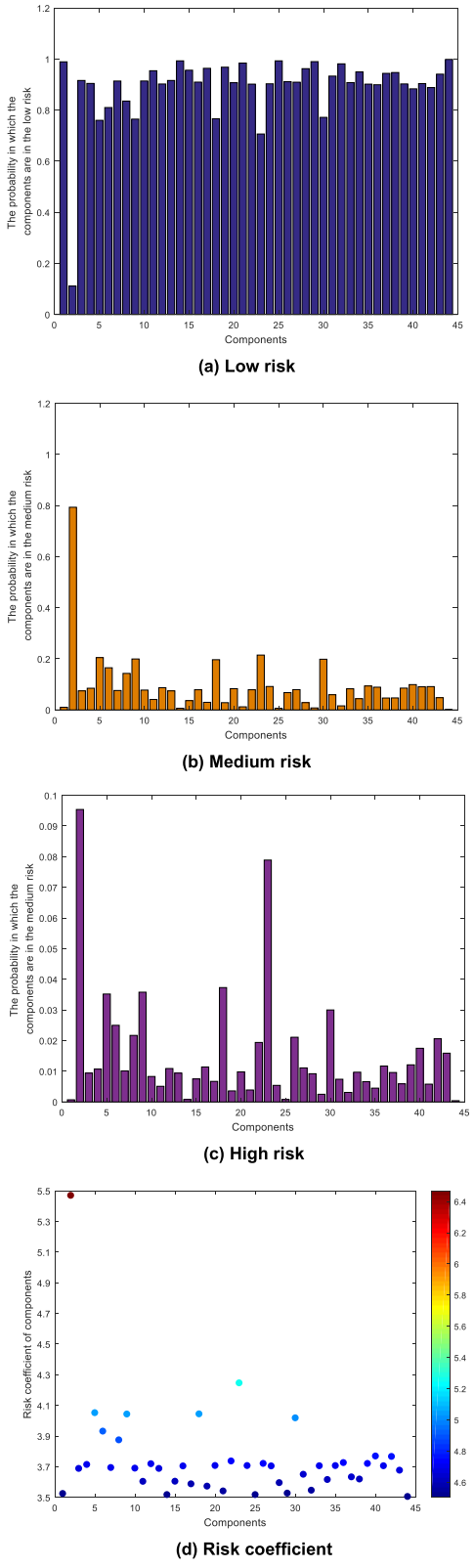


FIGURE 6. Risk coefficient of components.

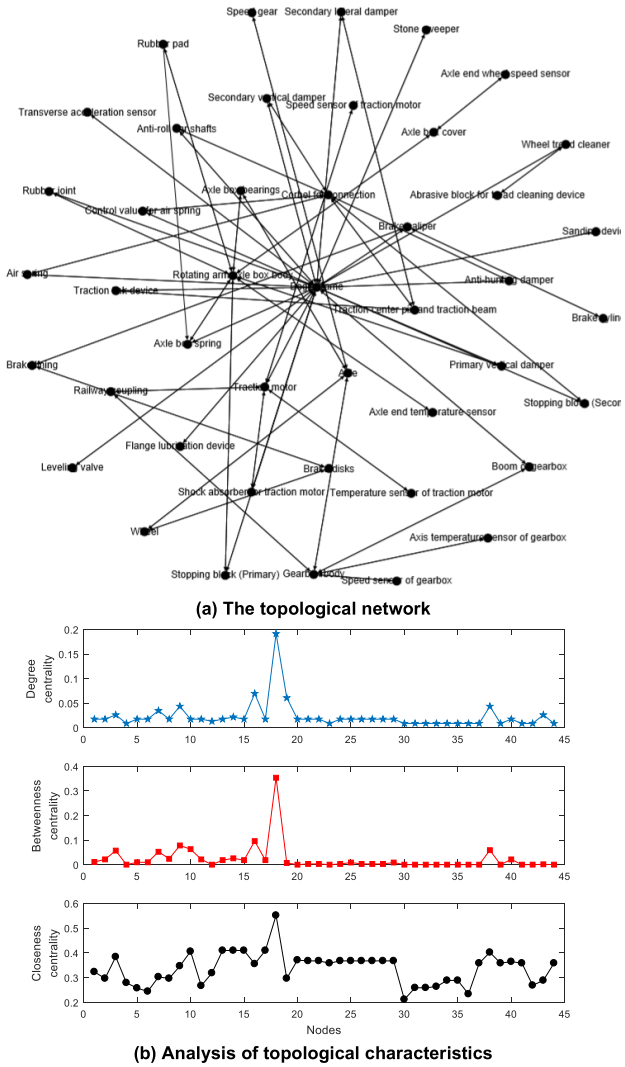


FIGURE 7. The topological network of the bogie system.

TABLE 3. Fault propagation paths of the bogie system.

Spreading steps	Failed node	Propagation intensity	Fault path
$k=0$	v_2	$PI_{v_2}(k=0)=0.0331$	v_2
$k=1$	v_3	$PI_{v_3,e_{23}}(k=1)=0.0005$	$v_2 \to v_3$
	v_5	$PI_{v_4,e_{24}}(k=1)=0.0207$	$v_2 \to v_5$
$k=2$	v_4	$PI_{v_4,e_{34}}(k=2)=7.1589\times10^{-9}<10^{-8}$ stop	$v_2 \to v_3$
	v_{18}	$PI_{v_{18},e_{5,18}}(k=2)=9.9887\times10^{-10}<10^{-8}$	$v_2 \to v_5 \to v_6$
	v_6	stop	
		$PI_{v_5,e_{56}}(k=2)=0.0001$	
$k=3$	v_7	$PI_{v_7,e_{67}}(k=3)=5.2312\times10^{-9}<10^{-8}$	$v_2 \to v_3$ $v_2 \to v_5 \to v_6$

Only fault path $v_2 \to v_5 \to v_6$ occurs in status 2. Both $v_2 \to v_3$ and $v_2 \to v_5 \to v_6$ occur simultaneously in status 3. An important observation is that the greater the number of fault nodes is, the greater the impact on system safety and reliability.

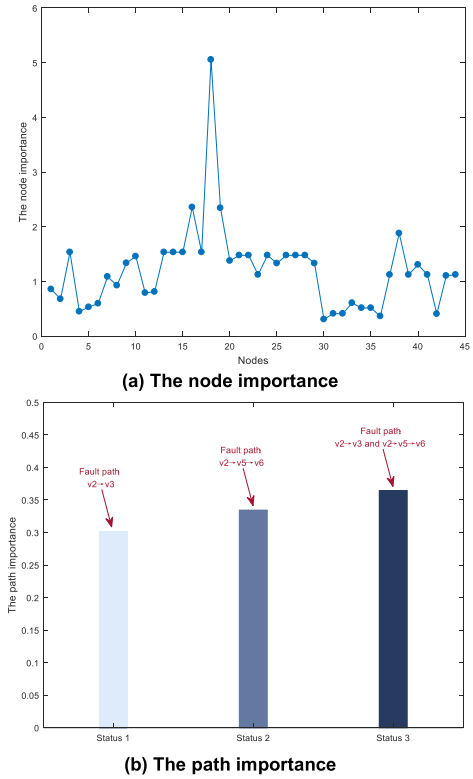


FIGURE 8. Parameters of the system risk measurement.

Through a combination of parameters in Fig. 8 and Eq. (19), the system risk measurement is determined to be $SR_{Status1}(t=12)=0.5072$ for status 1, $SR_{Status2}(t=12)=0.4925$ for status 2 and $SR_{Status3}(t=12)=0.0003$ for status 3. The system risk measurement considers not only the major impact of fault paths on system safety but also the possibility of a system failure state. The results indicate that the system risk of status 3 is lower than that of the other two situations and that the system risk is highest if the system is in status 1.

By researching various scenarios and consulting specialists, we developed a system safety threshold. If $SS \in [0, 0.25)$, the system is safe; if $SS \in [0.25, 0.75)$, the system is in a medium unsafe level; and if $SS \in [0.75, 1]$, the system is seriously unsafe. Table 4 presents the results

TABLE 4. System safety assessment.

Status	Credibility: Safety level α_{safe}	Credibility: Medium unsafe level $\alpha_{M-unsafe}$	Credibility: Serious unsafe level $\alpha_{S-unsafe}$	The expected utility of system safety $y_{statusi}, i=1,2,3$	
1	0.0333	0.7434	0.2233	0.5554	
2	0.0244	0.8404	0.1352	0.5950	y=0.3835
3	0.9999	0.00003	0.00002	0.00004	

of the system safety assessment using the proposed method. System safety is 0.3835, which indicates that the bogie system is at a medium unsafe level. Therefore, the managers should adjust the corresponding operation plan to ensure safe train operation. Furthermore, we also obtain the system safety in different statuses. These indicators provide theoretical support for maintenance personnel to quickly find the source of failure and to formulate a maintenance strategy in time.

B. ANALYSIS AND DISCUSSION

To demonstrate the approach proposed in Section 3, the above analysis results are compared with the statistical results based on fault data and the other existing methods.

1) DISCUSSION OF SYSTEM SAFETY

In China, there are usually multiple trains on the same line. For example, there are 44 trains a day from Beijing to Shanghai. Thus, 44 high-speed trains run on this line. To reduce the coincidence of evaluation results, we compare the system safety of 20 high-speed trains that run on the same line. According to Fig. 9, a broken blue line indicates the bogie system safety with 20 trains obtained using the proposed method, and the three columns represent the probabilities that the bogie system is at the safe level, medium unsafe level and seriously unsafe level according to the statistical analysis based on fault data. The statistical results show that bogie systems of these 20 trains are all in the medium unsafe state, and the proposed method indicates that 95% of bogie systems are also at the medium unsafe level. However, notably, the bogie system of train 18 is in the serious unsafe state according to the proposed method. This is because the potential fault propagation is considered when system safety is evaluated.

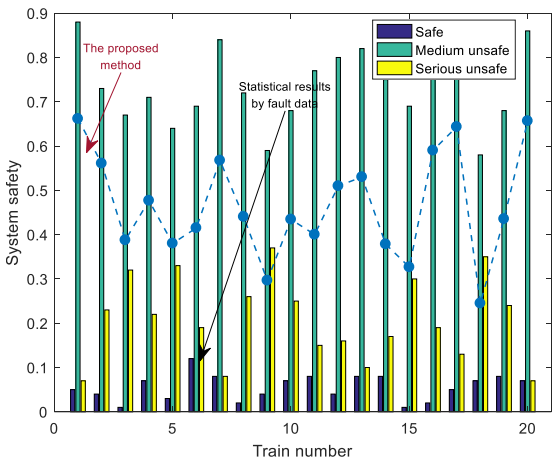


FIGURE 9. Bogie system safety of 20 trains.

To illuminate the practicability of the proposed method, three common approaches (i.e., ETA, Petri net analysis and Bayesian analysis) are also used to evaluate bogie system safety when node v_2 fails at 12 million kilometers. From Table 5, the values of system safety index calculated using the four methods are also different. The result based on

TABLE 5. Comparison of safety assessment methods.

Methods	Bogie system safety	
	Safety index	Safety level
The proposed method	0.3835	Medium unsafe
ETA	0.6752	Unsafe
Petri net	0.5289	Medium unsafe
Bayesian	0.5986	Unsafe

Petri net analysis is consistent with the proposed method. ETA and the Bayesian approach show that the bogie system is unsafe. The realization of these three methods requires a lot of expert experience. For example, establishment of ETA, Bayesian analysis and Petri net analysis requires expert guidance. In addition, the relationship between the calculated results of the safety index and the safety level also needs to be determined by experts. However, the proposed method evaluates the system security from the point of view of fault data and topology and could reduce the influence of subjective factors to a certain extent.

Fig. 10 plots the system safety with the different running kilometers. The system is not always in safe status or in an unsafe status. In the initial stage, due to defects in design, raw materials and manufacturing, system safety has great changes. As the operating mileage increases, the system has a safe status. Due to the implementation of the maintenance plan, if a failure is observed, measures are taken to ensure the safe operation of the bogie system. This is consistent with the Bathtub curve.

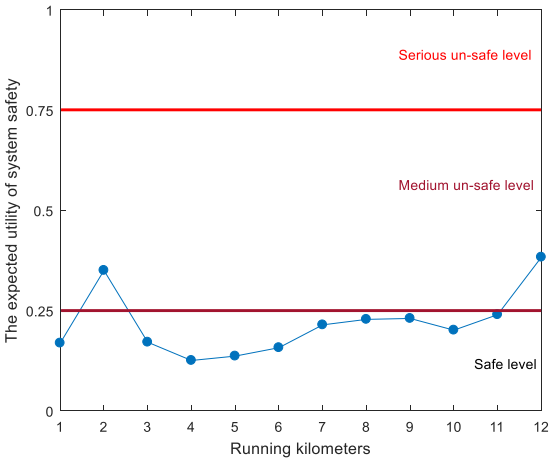
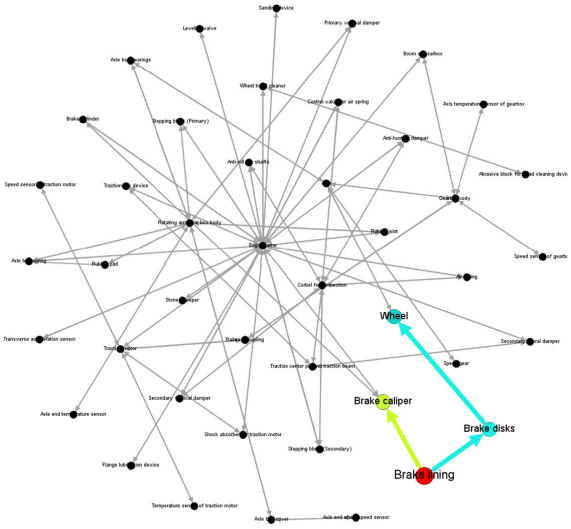


FIGURE 10. System safety with different running kilometers.

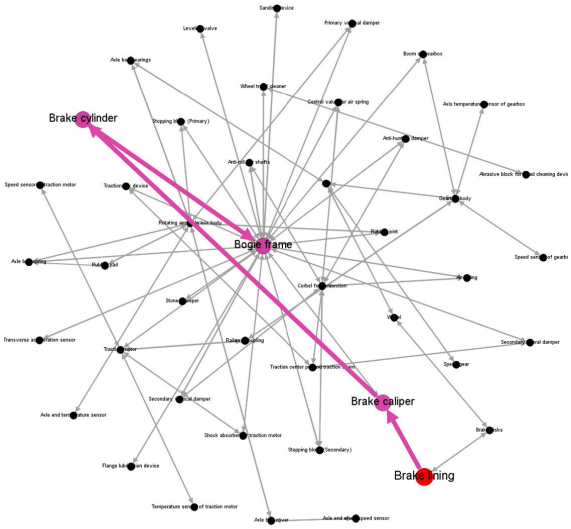
2) ANALYSIS OF FAULT PROPAGATION

In previous safety assessment methods, expert experience is usually used to analyze the propagation relationship among faults. To reduce the influence of subjective factors, we propose a fault propagation model based on the system topological network and fault data.

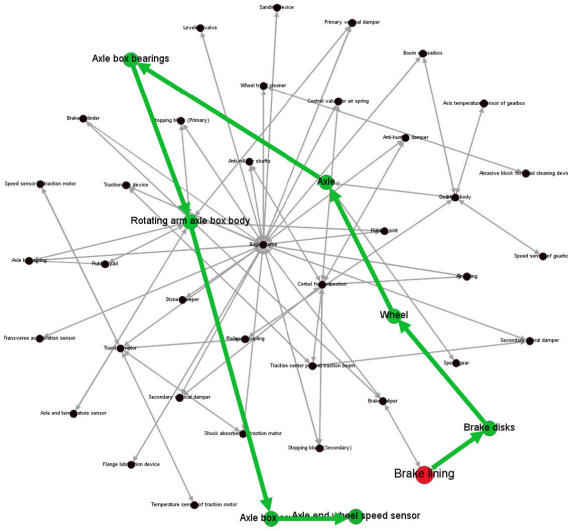
Fig. 11 analyzes the fault paths with three approaches. The fault path obtained from the event tree is $v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_{18}$. However, the analysis of a large number of fault



(a) The proposed method



(b) ETA method



(c) Petri net method

FIGURE 11. Failure propagation path of a bogie system.

data reveals that node v_{18} rarely fails and that its probability of failure is only 0.2%. In other words, fault propagation of other nodes rarely affects node v_{18}. In fact, due to the core position of node v_{18} in the bogie system, once it fails, it will have a fatal impact on the safety of the bogie system. Hence, in design and manufacturing, we usually improve the reliability of node v_{18}.

The failure path $v_2 \rightarrow v_5 \rightarrow v_6 \rightarrow v_7 \rightarrow v_8 \rightarrow v_{16} \rightarrow v_{14} \rightarrow v_{33}$ is obtained with the Petri net method. However, through field investigation and fault data analysis, we find that a component failure in the bogie system usually does not affect more than three other components because in order to ensure the system safety, redundant components or the reliability of key components is usually increased in the design process.

Compared with the two others approaches, the advantage of the proposed model is that it gives all possible fault propagation paths and their occurrence probability. In addition, the analysis results of fault paths are in good agreement with those of statistical analysis, due to the considered system topology and fault data.

3) RISK ANALYSIS OF COMPONENTS

The basic unit of mechatronics systems is the components, while the unique properties of these systems emerge from the interactions between components. Thus, risk analysis of components is critical for holistic system safety assessment.

In early research, it was generally believed that components with high failure rates have higher risk and have great influences on the system safety. In Fig. 12, the node with the highest probability of failure is v_2, and the failure probability of bogie frame v_{18} is 0.0202. However, according to fault data and practical experience, bogie system safety is greatly affected by the failure of node v_{18}. Although node v_2 has a high probability of failure, its impact on system safety after failure is relatively lower than that of node v_{18}.

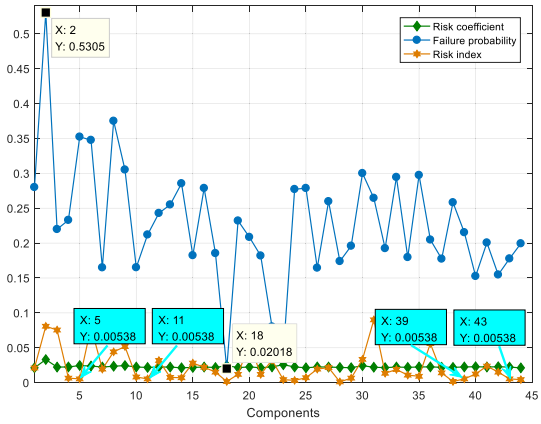


FIGURE 12. Component risk.

In traditional risk analysis, it is generally believed that the risk index of a component is the product of the fault severity and fault frequency. From Fig. 12, it can be observed that

the risk indexes of nodes v_5, v_{11}, v_{39} and v_{43} are the same. In other words, these nodes have the same degree of risk. However, in practice, the risk degree of components with different structural locations and attributes is often different.

Therefore, in order to overcome the shortcomings of common methods in practice, we propose a risk coefficient of components based on fault data to replace the existing component indicators and participate in system safety assessment.

V. CONCLUSION

In this paper, a novel method for assessing the safety of mechatronics systems is proposed for PS. The method considers not only the properties of components based on historical data but also the influence of system topology and fault propagation mechanisms on system safety. Instead of only fusing multiple safety indicators from a macroscopic perspective, the proposed method obtains a comprehensive measure of system safety by integrating information from component properties to fault propagation through the whole system. Indeed, this method offers a flexible and effective means of assessing system safety with respect to PS, i.e., in the case that a failure or a local fault has occurred. A practical example of a bogie system is examined to demonstrate the implementation and effectiveness of the proposed method. The results demonstrate that the PS-oriented framework for evaluating the safety of mechatronics systems may be widely applied in engineering.

Although the effectiveness of the proposed method has been verified in the bogie system, its validity and capability in handling more practical and complicated problems must be further tested. In other words, more case studies are needed to verify and revise the proposed method. In addition, system safety is affected by many factors, including humans and the environment. Therefore, further studies regarding how to calculate system safety by considering more factors must be conducted in the future.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their constructive comments and suggestions, which helped us to improve the paper.

REFERENCES

[1] M. Tomasikova, M. Tropp, T. Gajdosik, L. Krzywonos, and F. Brumercik, "Analysis of transport mechatronic system properties," *Procedia Eng.*, vol. 192, pp. 881–886, 2017.

[2] C. K. Pang, T. S. Ng, F. L. Lewis, and T. H. Lee, "Managing complex mechatronics R&D: A systems design approach," *IEEE Trans, Syst., Man, Cybern. A, Syst., Humans*, vol. 42, no. 1, pp. 57–67, Jan. 2012.

[3] D. Meinel, Paryanto, and J. Franke, "Methodology towards computer-aided testing of complex mechatronic systems: A case study about assembling a train system," *Procedia CIRP*, vol. 41, pp. 247–251, Jun. 2016.

[4] S. Lin, Y. Wang, L. Jia, and H. Zhang, "Reliability assessment of complex electromechanical systems: A network perspective," *Qual. Rel. Eng. Int.*, vol. 34, no. 5, pp. 772–790, Jul. 2018.

[5] P. Singh and L. K. Singh, "Design of safety critical and control systems of nuclear power plants using Petri nets," *Nucl. Eng. Technol.*, vol. 51, no. 5, pp. 1289–1296, Aug. 2019.

[6] V. Chabridon, M. Balesdent, J.-M. Bourinet, J. Morio, and N. Gayton, "Evaluation of failure probability under parameter epistemic uncertainty: Application to aerospace system reliability assessment," *Aerosp. Sci. Technol.*, vol. 69, pp. 526–537, Oct. 2017.

[7] Z. Ye, Z. Cai, F. Zhou, J. Zhao, and P. Zhang, "Reliability analysis for series manufacturing system with imperfect inspection considering the interaction between quality and degradation," *Rel. Eng. Syst. Saf.*, vol. 189, pp. 345–356, Sep. 2019.

[8] Z. Zhao, Q. Quan, and K.-Y. Cai, "A profust reliability based approach to prognostics and health management," *IEEE Trans. Rel.*, vol. 63, no. 1, pp. 26–41, Mar. 2014.

[9] F.-J. Zhao, Z.-J. Zhou, C.-H. Hu, L.-L. Chang, Z.-G. Zhou, and G.-L. Li, "A new evidential reasoning-based method for online safety assessment of complex systems," *IEEE Trans. Syst. Man Cybern, Syst.*, vol. 48, no. 6, pp. 954–966, Jun. 2018.

[10] M. Carvalho, J. Milho, J. Ambrosio, and N. Ramos, "Railway occupant passive safety improvement by optimal design," *Int. J. Crashworthiness*, vol. 22, no. 6, pp. 624–634, Nov. 2017.

[11] M. Althoff and A. Mergel, "Comparison of Markov chain abstraction and Monte Carlo simulation for the safety assessment of autonomous cars," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1237–1247, Dec. 2011.

[12] Z. Chen, Z. Li, C. Huang, G. Zhang, and H. Yu, "Safety assessment method of bridge crane based on cluster analysis and neural network," *Procedia Comput. Sci.*, vol. 131, pp. 477–484, 2018.

[13] R. Yu and M. Abdel-Aty, "Utilizing support vector machine in real-time crash risk evaluation," *Accident Anal. Prevention*, vol. 51, pp. 252–259, Mar. 2013.

[14] G. Li, Z. Zhou, C. Hu, L. Chang, Z. Zhou, and F. Zhao, "A new safety assessment model for complex system based on the conditional generalized minimum variance and the belief rule base," *Saf. Sci.*, vol. 93, pp. 108–120, Mar. 2017.

[15] J. Yang, H.-Z. Huang, L.-P. He, S.-P. Zhu, and D. Wen, "Risk evaluation in failure mode and effects analysis of aircraft turbine rotor blades using Dempster–Shafer evidence theory under uncertainty," *Eng. Failure Anal.*, vol. 18, no. 8, pp. 2084–2092, Dec. 2011.

[16] J. Dunjó, V. Fthenakis, J. A. Vílchez, and J. Arnaldos, "Hazard and operability (HAZOP) analysis. A literature review," *J. Hazardous Mater.*, vol. 173, nos. 1–3, pp. 19–32, Jan. 2010.

[17] A. L. Dakwat and E. Villani, "System safety assessment based on STPA and model checking," *Saf. Sci.*, vol. 109, pp. 130–143, Nov. 2018.

[18] R. Fattahi and M. Khalilzadeh, "Risk evaluation using a novel hybrid method based on FMEA, extended MULTIMOORA, and AHP methods under fuzzy environment," *Saf. Sci.*, vol. 102, pp. 290–300, Feb. 2018.

[19] S. Kabir, "An overview of fault tree analysis and its application in model based dependability analysis," *Expert Syst. Appl.*, vol. 77, pp. 114–135, Jul. 2017.

[20] N. Ramzali, M. R. M. Lavasani, and J. Ghodousi, "Safety barriers analysis of offshore drilling system by employing fuzzy event tree analysis," *Saf. Sci.*, vol. 78, pp. 49–59, Oct. 2015.

[21] Q. Shi, M. Abdel-Aty, and R. Yu, "Multi-level Bayesian safety analysis with unprocessed Automatic Vehicle Identification data for an urban expressway," *Accident Anal. Prevention*, vol. 88, pp. 68–76, Mar. 2016.

[22] D. Wu and W. Zheng, "Formal model-based quantitative safety analysis using timed coloured Petri nets," *Rel. Eng. Syst. Saf.*, vol. 176, pp. 62–79, Aug. 2018.

[23] Y.-H. Lin, Y.-F. Li, and E. Zio, "A reliability assessment framework for systems with degradation dependency by combining binary decision diagrams and Monte Carlo simulation," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 46, no. 11, pp. 1556–1564, Nov. 2016.

[24] P. Gonçalves, J. Sobral, and L. Ferreira, "Unmanned aerial vehicle safety assessment modelling through Petri nets," *Rel. Eng. Syst. Saf.*, vol. 167, pp. 383–393, Nov. 2017.

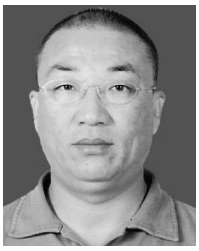
[25] S. Fu, X. Yan, D. Zhang, C. Li, and E. Zio, "Framework for the quantitative assessment of the risk of leakage from LNG-fueled vessels by an event tree-CFD," *J. Loss Prevention Process Industries*, vol. 43, pp. 42–52, Sep. 2016.

[26] M. Yazdi, S. Daneshvar, and H. Setareh, "An extension to fuzzy developed failure mode and effects analysis (FDFMEA) application for aircraft landing system," *Saf. Sci.*, vol. 98, pp. 113–123, Oct. 2017.

[27] N. Khakzad, F. Khan, and P. Amyotte, "Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches," *Rel. Eng. Syst. Saf.*, vol. 96, no. 8, pp. 925–932, Aug. 2011.

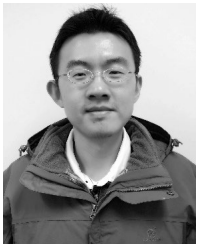
[28] J. H. Purba, "A fuzzy-based reliability approach to evaluate basic events of fault tree analysis for nuclear power plant probabilistic safety assessment," *Ann. Nucl. Energy*, vol. 70, pp. 21–29, Aug. 2014.
[29] S. Faghih-Roohi, M. Xie, and K. M. Ng, "Accident risk assessment in marine transportation via Markov modelling and Markov Chain Monte Carlo simulation," *Ocean Eng.*, vol. 91, pp. 363–370, Nov. 2014.
[30] H.-C. Liu, J.-X. You, X.-Y. You, and M.-M. Shan, "A novel approach for failure mode and effects analysis using combination weighting and fuzzy VIKOR method," *Appl. Soft Comput.*, vol. 28, pp. 579–588, Mar. 2015.
[31] S. Lin, Y. Wang, and L. Jia, "System reliability assessment based on failure propagation processes," *Complexity*, vol. 2018, pp. 1–19, Jun. 2018.
[32] W. Jiang, C. Xie, M. Zhuang, and Y. Tang, "Failure mode and effects analysis based on a novel fuzzy evidential method," *Appl. Soft Comput.*, vol. 57, pp. 672–683, Aug. 2017.
[33] P. Smets and R. Kennes, "The transferable belief model," *Artif. Intell.*, vol. 66, no. 2, pp. 191–234, Feb. 1994.
[34] Y. Zhou, W. Su, L. Ding, H. Luo, and P. E. D. Love, "Predicting safety risks in deep foundation pits in subway infrastructure projects: Support vector machine approach," *J. Comput. Civil Eng.*, vol. 31, no. 5, Sep. 2017, Art. no. 04017052.
[35] D. Chen, L. Lü, M.-S. Shang, Y.-C. Zhang, and T. Zhou, "Identifying influential nodes in complex networks," *Phys. A, Statist. Mech. Appl.*, vol. 391, pp. 1777–1787, Feb. 2012.
[36] T. Xia, Y. Dong, L. Xiao, S. Du, E. Pan, and L. Xi, "Recent advances in prognostics and health management for advanced manufacturing paradigms," *Rel. Eng. Syst. Saf.*, vol. 178, pp. 255–268, Oct. 2018.
[37] S. Lin, Y. Wang, L. Jia, H. Zhang, and Y. Li, "Intuitionistic mechanism for weak components identification method of complex electromechanical system," *J. Intell. Fuzzy Syst.*, vol. 34, no. 1, pp. 583–598, Jan. 2018.

SHUAI LIN received the Ph.D. degree and Postdoctoral Program in safety science and engineering from Beijing Jiaotong University, Beijing, China, in 2018 and 2019, respectively. She is currently a Postdoctoral Researcher with the Antai College of Economics & Management, Shanghai Jiao Tong University, Shanghai, China. Her research interest includes reliability and safety of complex electromechanical systems.



LIMIN JIA received the Ph.D. degree from the China Academy of Railway Sciences, Beijing, China, in 1991. He is currently with the State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University. His current research interests include safety science and engineering, control science and engineering, and transportation engineering.

YANHUI WANG received the Ph.D. degree in safety engineering from the Beijing University of Science and Technology, Beijing, China, in 2005. He is currently with the State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University. His research interest includes the intelligent transportation systems.



HENGRUN ZHANG received the master's degrees from Shanghai Jiao Tong University, Shanghai, China, in 2015, and George Mason University, Fairfax, VA, USA, in 2018. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Volgenau School of Engineering, George Mason University, Fairfax, VA, USA. His research interests include machine learning and data mining, as well as network communication.