applied sciences

MDPI

Article

A Novel Risk Assessment and Analysis Method for Correlation in a Complex System Based on Multi-Dimensional Theory

Zeyong Jiang, Tingdi Zhao, Shihai Wang * and Fuchun Ren

School of Reliability and Systems Engineering, Beihang University, Beijing 100191, China; jiangzeyong@buaa.edu.cn (Z.J.); ztd@buaa.edu.cn (T.Z.); renfuchun@126.com (F.R.)

* Correspondence: wangshihai@buaa.edu.cn

Received: 3 April 2020; Accepted: 20 April 2020; Published: 25 April 2020

Abstract: With the rapid development of high integrations in large complex systems, such as aircraft, satellite, and railway systems, due to the increasingly complex coupling relationship between components within the system, local disturbances or faults may cause global effects on the system by fault propagation. Therefore, there are new challenges in safety analysis and risk assessment for complex systems. Aiming at analyzing and evaluating the inherent risks of the complex system with coupling correlation characteristics objectively, this paper proposes a novel risk assessment and analysis method for correlation in complex system based on multi-dimensional theory. Firstly, the formal description and coupling degree analysis method of the hierarchical structure of complex systems is established. Moreover, considering the three safety risk factors of fault propagation probability, potential severity, and fault propagation time, a multi-dimensional safety risk theory is proposed, in order to evaluate the risk of each element within the system effecting on the overall system. Furthermore, critical safety elements are identified based on Pareto rules, As Low As Reasonably Practicable (ALARP) principles, and safety risk entropy to support the preventive measures. Finally, an application of an avionics system is provided to demonstrate the effectiveness of the proposed method.

Keywords: safety; coupling correlation; risk assessment; multi-dimensional theory

1. Introduction

In recent years, due to the complex correlation of components in complex systems, local faults may have a great effect on the overall system by fault propagation [1–3]. Therefore, the safety and risk analysis of such complex systems has attracted more and more attention. Safety analysis and risk assessment aims to eliminate and control various hazards through the design system and take preventive measures to prevent accidents that will cause personal injury, equipment damage, and task failure during system operation. With the development of science and technology, a series of analysis methods for evaluating system failures and risk events have been developed, especially in high-risk fields such as aerospace, chemical, nuclear, and other industrial fields [4,5]. However, there are still a number of safety problems in these methods caused by the coupling and correlation characteristics in complex systems.

Traditional safety modeling and analysis methods are mainly based on the logical process of induction and deduction to carry out system safety analysis. From the local characteristics of the system or the direct relationship between internal components, these methods are used to find the root cause of safety problems and carry out safety work such as analysis, verification, assurance, etc. Typical analysis methods are Fault Tree Analysis (FTA) [6], Event Tree Analysis (ETA) [7,8], Failure Mode and Effects Analysis (FMEA) [9–11], Hazard and Operability Analysis (HAZOP), Probability Risk Assessment (PRA) [12,13], etc. These methods have applications in nuclear power, chemical, and even aerospace. Zhou, X. [14] proposed a modified FMEA based on Dempster–Shafer evidence theory to analyze safety of aircraft turbine rotor blades. Rhee, Seung J. [15] used a Monte Carlo simulation and cost-based FMEA to account for the uncertainties in: detection time, fixing time, occurrence, delay time, down time, and model complex scenarios. Hyeon-ae Jang [16] proposed a time-dependent probabilistic approach of FMEA to evaluate safety of automotive-manufacturing. Liu, Yang [17] proposed an FTA-based method for risk decision-making in emergency response and applied it in H1N1 infectious diseases. Cheraghi, M. [18] proposed a fuzzy multi-attribute HAZOP technique and Analytic Hierarchy Process (AHP) to determine the weight of risk factors and to prioritize the hazards.

Moreover, with the development of the accident theory, a large number of modern methods for safety analysis, such as Markov process, Analysis and Design Language (AADL), Petri nets, Bayesian networks, etc., have also been invented. Feng, Q. [19] proposed the staged Bayesian failure model for girth welds of a pipeline, using the tree-type accident theory and Bayesian survival analysis method. Zhao, C. [20] applied the continuous-time Markov chains to analyze reliability of the reconfigurable integrated modular avionics. Singh, P. [21] applied Petri nets to estimate performability to ensure system dependability requirements and did the performance analysis of safety critical and control systems that helps to estimate the risk. Baouya, A. [22] presented AADL based on model-driven specification and probabilistic model checking to automatically analyze safety-based availability before synthesizing the embedded software product. John McDermid's team at the University of York in the United Kingdom proposed the theory and analysis techniques of safety case [23–26] to confirm that the system reaches an acceptable level of safety by establishing a correlation between safety requirements and safety evidence. The Functional Resonance Accident Model (FRAM) [27,28] was proposed by Erik Hollnagel, based on the principle of stochastic resonance in the system. However, the above safety analysis methods mainly focused on a qualitative description and the study of coupling mechanisms, and lack the quantitative analysis and evaluations of coupling and correlation relationships between components in the system.

Internationally, aviation criteria ARP 4754 (A) [29,30] recommended by the American Society of Automotive Engineers defines safety as a state where the risk is lower than the border risk. The domestic GJB 900A defines safety as the ability of a product not to cause personal injury or death, system damage, major property damage, or damage human health and the environment. For the measurement of risk, risk model of probability and severity is the most widely used, such as the civil aviation standard ARP 4761 [31], the US military standard MIL-STD-882E [32], the national military standard GJB 900A, etc., FTA, FMEA, ETA, and other reliability and safety analysis methods all use the models to evaluate risks. However, with the further understanding of the concept of risk, people have more research and cognition of the elements involved in risk. Mazzuchi T A. [33] developed a relationship for the probability of wire failure as a function of influencing factors in an aircraft environment in order to analyze wire failure in aircraft. Cour-Harbo A L. [34] presented a method for quantifying the probability of fatalities resulting from an uncontrolled descent of an unmanned aircraft conducting a beyond visual line-of-sight (BVLOS) flight so as to solve the major challenges to make a realistic and effective risk assessment of conducting operation of BVLOS. Li L. [35] proposed a new risk assessment method based on the cloud model, aiming to make an effective risk assessment method for subway operation by considering five aspects. Fayaz, M. [36] proposed an integrated risk index model based on hierarchical fuzzy logic for underground risk assessment to avoid occurrence of accidents due to underground facilities. Duan, Y. [37] presented a novel network security risk assessment approach by combining subjective and objective weights under uncertainty to effectively evaluate computer network security. Most of the above risk assessment methods focus on the analysis of accident probability and severity, and lack of multi-dimensional safety risk assessment methods by taking time factor related fault into consideration.

In view of the above considerations, this paper proposes a novel risk assessment and analysis method for correlation in complex system based on multi-dimensional theory, aiming at analyzing and evaluating the risk of complex system considering the coupling correlation, so as to identify the critical risk elements. Firstly, the formal description and coupling correlation analysis method of the hierarchical structure of complex systems based on the typical task-function-resource model is proposed, aiming to achieve a formal description of the coupling correlation between components within complex systems, providing the foundation for and analysis and evaluation of risk. Moreover, considering the three safety risk factors of propagation probability, potential severity, and propagation time, a multi-dimensional safety risk theory is proposed, in order to evaluate the risk of each element in the system effecting on the overall system from multiple perspectives. Furthermore, critical safety elements are identified based on Pareto rules, ALARP principles, and safety risk entropy to support the preventive measures.

The remainder of the paper is organized as follows. Section 2 describes the hierarchical model of complex systems and coupling correlation between elements in system. In Section 3, multi-dimensional safety risk theory and assessment are proposed. Section 4 introduces an application of avionics system. Section 5 presents the conclusions.

2. Coupling Correlation of Complex System

In a general sense, the adjective "complex" describes a system or component that by design or function or both is difficult to understand and verify [38]. Complex system is any system featuring a large number of interacting components that is often difficult to understand, and hard to solve [39,40]. Compared with simple systems, complex systems are usually characterized by more components and a high degree of coupling [41,42]. In the real world, there are a large number of systems that show the characteristics of complexity, such as ecosystem, social organization system, complex social technology system, complex electromechanical system, and complex equipment system [43–45]. The complex system concerned in this paper is mainly located in the complex engineering technology system, that is, a kind of complex system with engineering technology characteristics.

Coupling correlations refer to all kinds of association relationships between various elements in the system due to task and function requirements, such as resource reuse, information transfer, data sharing, etc. The strength of the coupling correlation can be quantified by the degree of coupling. For complex systems, the internal coupling correlations are more complicated. The complex coupling correlations increase the risk of fault propagation in the system. The establishment of a system model based on the coupling correlation is the basis for analyzing and quantifying the risk of system for fault propagation.

2.1. Hierarchical Model and Description of Complex Systems

2.1.1. Hierarchical Model

Generally, a system is built on the background of specific task requirements, that is, the use case scenarios of the system are planned in advance through requirements analysis. These planned use case scenarios can be defined as the task view or task layer of the system. Then, based on the system task planning, the necessary functional decomposition is needed, namely, what basic functions need to be established in order to achieve a specific task. Therefore, this paper defines such decomposed functions as the functional view or function layer of the system. However, the tasks and functions are in the design of the system logic layer. The final implementation still needs the support of the physical layer such as typical computing, storages, communication resources, etc. In other words, the configuration and mapping relationships from logic layer to the physical layer in the system require to be clarified and completed. This paper defines these general physical resources as the resource view or resource layer of the system.

In summary, when analyzing from the perspective of hierarchical decomposition, a hierarchical system model based on the task-function-resource layer can be established [46–48]. Then, the coupling relationships between the elements in the task-function-resource layer and between the layers can be considered. Based on the topology modeling theory, a topology model with elements as nodes and correlation relationships as connections can be formed. Finally, combined with hierarchical decomposition and coupling analysis, a complex system hierarchy model based on task-function-resource architecture is synthesized, as shown in Figure 1 and different colors and shapes are applied to present the elements in different layers for distinguishing. It is based on the assumption that the number of tasks, functions, and resources is unchanged during the time and the correlation relationships in systems are constant during the time.

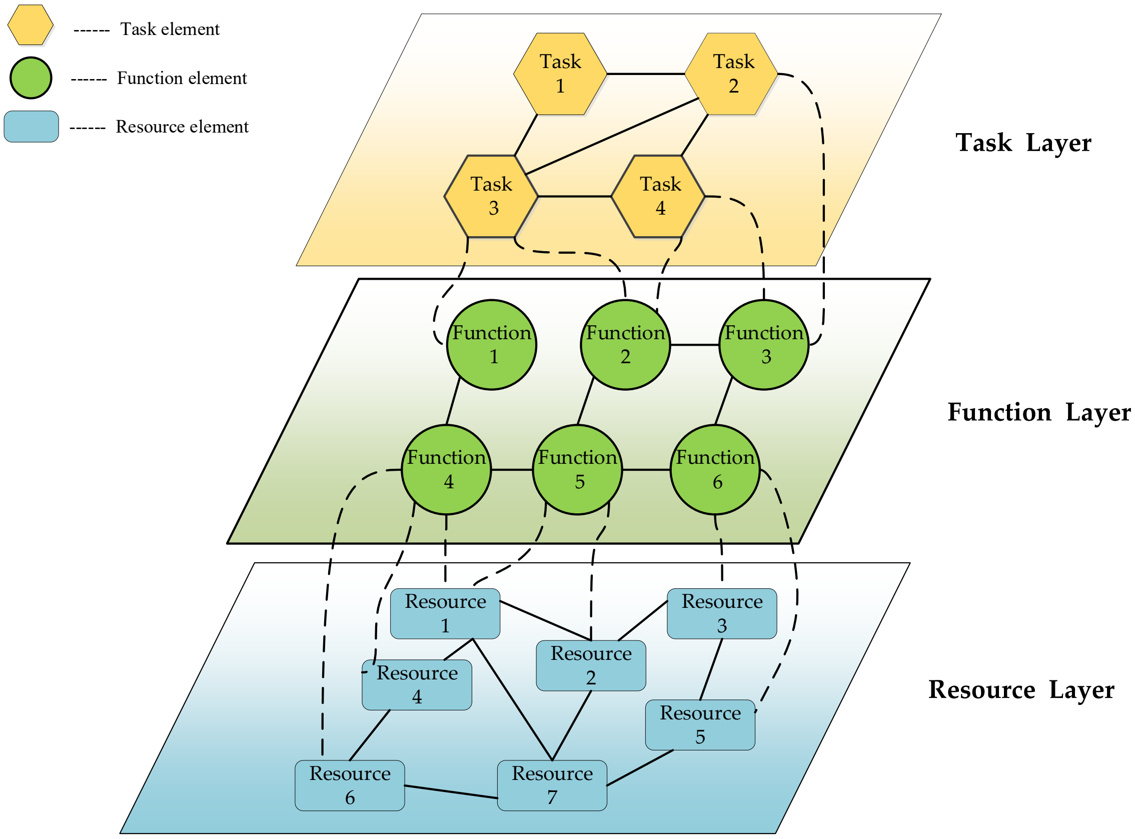


Figure 1. Typical task-function-resource architecture of complex systems. The straight lines represent the coupling correlation of elements in the same layer, and dashed lines represent coupling correlation across layers of elements in the different layers. Lines (connections) are bi-directional.

It is assumed that the destructive event of the system only originates from the fault of the element of resource layer, and the element of function layer exists as the use of the element of resource layer and the role of the caller. Therefore, in this paper, based on the fault propagation problem introduced by resource layer, the fault of the resource element is the fault trigger point, and the function element provides the propagation medium.

2.1.2. Formal Description of Hierarchical Model

For the task-function-resource hierarchy architecture of the system, from the perspective of the element set, the system's task element set, function element set, and resource element set can be defined separately. The task element t_i is a task unit established by the system requirement analysis. It is supported by a series of basic function elements. The task element set T can be expressed as a set of several task elements: $T = \{t_1, t_2, \ldots, t_k\}$. Similarly, the function element f_i is the basic function unit that supports the task implementation in the system. It is supported by a series of basic resource elements. The function element set F can be expressed as a set of several functional elements: $F = \{f_1, f_2, \ldots, f_m\}$. The resource element r_i is a physical or logical unit that supports the realization of function in the system. The system resource element set R can be represented as a set of several resource elements: $R = \{r_1, r_2, \ldots, r_n\}$.

Through the analysis of the system hierarchy architecture, in order to describe specific relational information, adjacency matrix can be used for the most direct formal record, that is, the mapping correlation matrix between task-function elements can be expressed as shown in Matrix (1).

$$M^{tf} = (M^{tf}_{ij})_{k\times m} = \begin{array}{c} \\ t_1 \\ t_2 \\ \vdots \\ t_k \end{array} \begin{array}{c} \begin{array}{cccc} f_1 & f_2 & \cdots & f_m \end{array} \\ \begin{bmatrix} M^{tf}_{11} & M^{tf}_{12} & \cdots & M^{tf}_{1m} \\ M^{tf}_{21} & M^{tf}_{22} & & M^{tf}_{2m} \\ \vdots & & \ddots & \vdots \\ M^{tf}_{k1} & M^{tf}_{k2} & \cdots & M^{tf}_{km} \end{bmatrix} \end{array} \tag{1}$$

where $M^{tf}_{ij} = 1$ means there is a direct correlation between task element t_i and function element f_j; $M^{tf}_{ij} = 0$ means no direct correlation.

Similarly, the function-resource element mapping correlation matrix can be expressed shown as Matrix (2).

$$M^{fr} = (M^{fr}_{ij})_{m\times n} = \begin{array}{c} \\ f_1 \\ f_2 \\ \vdots \\ f_m \end{array} \begin{array}{c} \begin{array}{cccc} r_1 & r_2 & \cdots & r_n \end{array} \\ \begin{bmatrix} M^{fr}_{11} & M^{fr}_{12} & \cdots & M^{fr}_{1n} \\ M^{fr}_{21} & M^{fr}_{22} & & M^{fr}_{2n} \\ \vdots & & \ddots & \vdots \\ M^{fr}_{m1} & M^{fr}_{m2} & \cdots & M^{fr}_{mn} \end{bmatrix} \end{array} \tag{2}$$

where $M^{fr}_{ij} = 1$ means there is a direct correlation between function element f_i and resource element r_j; $M^{fr}_{ij} = 0$ means no direct correlation.

If requiring to further record the cross-layer correlation relationship between task and resource elements, we can define and obtain it by matrix operation $M^{tr} = M^{tf} \times M^{fr}$ shown in Matrix (3). However, in general, the practical significance of this cross-layer correlation is not obvious. It is the focus on the system design to clarify the software-hardware configuration mapping relationships from functions to resources. Therefore, this paper will focus on correlations from functions to resources.

$$M^{tr} = M^{tf} \times M^{fr} = \begin{array}{c} \\ t_1 \\ \vdots \\ t_n \end{array} \begin{array}{c} \begin{array}{ccc} r_1 & \cdots & r_n \end{array} \\ \begin{bmatrix} M^{tf}_{11} \times M^{fr}_{11} + \ldots M^{tf}_{1m} \times M^{fr}_{m1} & \cdots & M^{tf}_{11} \times M^{fr}_{11} + \ldots M^{tf}_{1\mathrm{m}} \times M^{fr}_{mn} \\ \vdots & \ddots & \vdots \\ M^{tf}_{\mathrm{k1}} \times M^{fr}_{\mathrm{k1}} + \ldots M^{tf}_{\mathrm{km}} \times M^{fr}_{mn} & \ldots & M^{tf}_{\mathrm{k1}} \times M^{fr}_{\mathrm{k2}} + \ldots M^{tf}_{\mathrm{km}} \times M^{fr}_{mn} \end{bmatrix} \end{array} \tag{3}$$

where $M^{tr}_{ij} \geq 1$ means there is a direct correlation between task element t_i and resource element r_j. $M^{tr}_{ij} = 0$ means no direct correlation.

2.2. Analysis of Coupling Degree

As the physical layer within the system, the form of coupling between the resource layer is also the most obvious: on the one hand, this coupling may result from the functional/logical coupling generated by each resource element serving the same function; on the other hand, it may also cause direct material or information transfer between resource elements, thus introducing specific coupling relationships. Both of the above two coupling forms can be defined as direct coupling. In contrast, a more complex form of indirect association between groups of coupled resource elements is generated due to the addition of the resource-sharing form. This form of coupling can be defined as indirect/cascading coupling. In order to quantitatively describe the direct and indirect coupling relationships within the system hierarchy, this study takes the resource layer as an example to define and distinguish the two coupling concepts.

1. Direct coupling degree matrix

The direct coupling degree is used to characterize the direct coupling relationship between elements. It represents the situation where there are direct information interactions, material exchanges or being occupied by the same other layer elements in the layer. The direct coupling degree matrix C^d is represented in Matrix (4):

$$C^d = (C^d_{ij})_{n\times n} = \begin{array}{c} \\ r_1 \\ r_2 \\ \vdots \\ r_n \end{array} \begin{array}{c} \begin{array}{cccc} r_1 & r_2 & \cdots & r_n \end{array} \\ \begin{bmatrix} C^d_{11} & C^d_{12} & \cdots & C^d_{1n} \\ C^d_{21} & C^d_{22} & & C^d_{2n} \\ & \vdots & \ddots & \vdots \\ C^d_{n1} & C^d_{n2} & \cdots & C^d_{nn} \end{bmatrix} \end{array} \tag{4}$$

where $C^d_{ij} = 0$ means no direct correlation; $C^d_{ij} = 1$ means correlation degree between resource element r_i and resource element r_j is 1, that, is, the fault propagation from resource element r_i to resource element r_j only needs 1 step.

2. Indirect coupling degree matrix

According to the fault propagation theory and cascading failure theory, the fault of a single element will not only affect the element itself, but also cause a cascading effect by the correlation between elements, causing the fault propagation and diffusion, and the more serious situation may affect the normal operation of the whole system. Thus, simply establishing the concept of direct coupling degree is insufficient to assess the potential risk introduced by multiple coupling correlation of elements. In contrast, the indirect coupling degree is more efficient to reflect the degree of such risk.

The indirect coupling degree matrix C^c_{ij} characterizes the indirect coupling relationships between elements, which is an extension of the direct coupling degree. It can be represented by the indirect coupling degree matrix C^c as presented in Matrix (5).

$$C^c = (C^c_{ij})_{n\times n} = \begin{array}{c} \\ r_1 \\ r_2 \\ \vdots \\ r_n \end{array} \begin{array}{c} \begin{array}{cccc} r_1 & r_2 & \cdots & r_n \end{array} \\ \begin{bmatrix} C^c_{11} & C^c_{12} & \cdots & C^c_{1n} \\ C^c_{21} & C^c_{22} & & C^c_{2n} \\ & \vdots & \ddots & \vdots \\ C^c_{n1} & C^c_{n2} & \cdots & C^c_{nn} \end{bmatrix} \end{array} \tag{5}$$

Based on the direct coupling degree matrix C^d, the shortest fault propagation path order is calculated based on the Floyd algorithm, and that means the indirect coupling degree matrix C^c is generated. Among them, the element C^c_{ij} in the matrix is a natural number. When $C^c_{ij} = 0$, it means no indirect coupling relationship. When $C^c_{ij} = n$, it means that coupling correlation degree between resource element r_i and resource element r_j is n, indicating that fault propagation from resource element r_i to resource element r_j needs n steps.

The basic process of the Floyd algorithm is to start from the direct coupling matrix C^d and recursively update n times. Each update process introduces a new transition node to compare whether the path optimization can be achieved, until all nodes are introduced. Meanwhile, by using Floyd algorithm, the shortest path matrix C^r is obtained, where C^r_{ij} represents the next resource element that fault propagation from resource element r_i to resource element r_j should go through. Then, the order of the resource elements which the shortest path of fault propagation from resource element r_i to resource element r_j should go through can be deduced in turn.

2.3. Related Factors of Risk

2.3.1. Potential Severity

Further, when a risk quantification is required in view of coupling correlations, a potential severity matrix S_p can be established as Matrix (6):

$$S_p = \left(S_p\right)_{n\times n} = \begin{array}{c c} & \begin{array}{cccc} r_1 & r_2 & \cdots & r_n \end{array} \\ \begin{array}{c} r_1 \\ r_2 \\ \vdots \\ r_n \end{array} & \left[\begin{array}{cccc} S_{11} & S_{12} & \cdots & S_{1n} \\ S_{21} & S_{22} & & S_{2n} \\ \vdots & & \ddots & \vdots \\ S_{n1} & S_{n2} & \cdots & S_{nn} \end{array}\right] \end{array} \tag{6}$$

The potential severity between resource elements will decrease non-linearly with the indirect coupling degree (such as the impact of radio waves, noise, etc.), that is, due to the natural elasticity and robustness of the system, the more propagation steps a potential fault needs, the lower its effect will be. Therefore, a function relationship between the potential severity and the indirect coupling degree is required to be established. According to the characteristics of the membership relationship between the two factors in the shape of the graph. The typical mapping relationship function is divided into normal type, Γ type, and Cauchy type [49–51], and each type is divided into smaller-type, middle-type, and larger-type [52,53]. Because the degree of propagation effect decreases nonlinearly with the coupling degree, a typical smaller-type of Cauchy type membership function [54,55] $S_p(C^c)$ is used for fitting in this paper shown in Equation (7).

$$S_p(C^c) = \begin{cases} \frac{1}{1+a(C^c-c)^2}, \ C^c > c \\ 1, \ C^c \le c \end{cases} \tag{7}$$

where C^c represents the coupling degree (positive integer) which can be obtained from the indirect coupling degree matrix. S_p is the potential severity; a and c are constant, and need to be further quantified.

Moreover, the factor of safety critical degree $SCG = \{g_1, g_2, \ldots, g_n\}$ of resource elements requires to be considered. In other words, there is difference in the fault effect strength in different resource elements. Therefore, the SCG factor needs to be added to the potential severity matrix, $S = S_p \times SCG$ forming updated potential severity matrix S.

2.3.2. Propagation Probability and Propagation Time

Ideally, the original data should be determined by experimental statistics. However, in the case of insufficient experimental data, the expected data can be obtained by simulation complex system or modified by referring to expert experience. For example, for the direct propagation probability and direct propagation time, from the perspective of related faults, based on the analysis of the fault effect mechanism between elements, fault correlation effect (simulation) test work can be carried out. Based on the test data, the frequency and average time of fault propagation are calculated and counted as the expected values of the direct propagation probability matrix C_d^P and the direct propagation time matrix C_d^T. In the paper, fault injection [56,57] is applied in the simulation system for a large number of times (usually 10,000) to record and obtain average propagation probability and propagation time [58,59]. In general, if the sample size is large enough, then the average value can be regarded as the actual value [60–62].

If fault propagation from resource element r_i to resource element r_j needs n steps (can be obtain from the shortest path matrix), the probability of each propagation step is $p_1, p_2, \ldots, p_n$ (can be obtained from the direct propagation probability matrix C_d^P). Indirect propagation probability $C_{c(ij)}^P$ that fault in element r_i to element r_j can be calculated by Equation (8) and then indirect propagation probability matrix C_c^P is formed.

$$C_{c(ij)}^P = \prod_{m=1}^{n} p_m \tag{8}$$

Similarly, if the fault propagation from resource element r_i to resource element r_j needs n steps (it can be obtained from the shortest path matrix), and the time of each propagation step is $t_1, t_2, \ldots,$ t_n (it can be obtain from the direct propagation time matrix C_d^T), indirect propagation time $C_{c(ij)}^T$ that fault propagation takes from element r_i to element r_j can be calculated by Equation (9). Then indirect propagation time matrix C_c^T is formed.

$$C_{c(ij)}^T = \sum_{m=1}^{n} p_m \tag{9}$$

3. Multi-Dimensional Safety Risk Theory

3.1. Multi-Dimensional Safety Risk Model

Generally, the safety risk of a system is measured in two dimensions, which is to quantify the safety risk from two dimensions: the probability of a dangerous event and the severity of the potential effect as shown in Equation (10). However, it is incomprehensive to fully characterize the safety risk characteristics of the system by analyzing and evaluating safety risks from only two dimensions. Therefore, this paper takes another dimension (propagation time) into consideration and proposes a new theory to quantify safety risk from three dimensions: probability, severity and time, and compare the effect weight and correlation of each element, in order to analyze and evaluate the safety risk comprehensively. Combined with the risk concept of Terje Aven [63], the multi-dimensional safety risk model can be formalized as presented in Equation (11).

$$R = f(P, S) \tag{10}$$

where P is the probability of a dangerous event, S is the severity of the potential effect.

$$R = f(P, S, T) \tag{11}$$

where P is the fault propagation probability, S is the potential severity, and T is the fault propagation time.

3.2. Calculation of Multi-Dimensional Safety Risk Model

Traditional risk assessment often adopts qualitative/semi-quantitative methods. The basic rule is to classify risk factors into different levels qualitatively based on experience, and then refer to the risk assessment model for semi-quantitative risk assessment. The core reason for using the qualitative/semi-quantitative risk assessment method is that the risk factors have different dimensional units, and the resulting risk values can be considered as the normalized result after empirical classification. In GJB 900A [64], the probability and severity are classified into five levels and four levels, respectively, and based on expert scoring method [65,66], different probability levels and severity levels corresponding to different risk values are shown in Table 1.

Table 1. Risk index matrix based on GJB 900A.

Probability Level	**Severity Level**			
	1	**2**	**3**	**4**
1	1	3	7	13
2	2	5	9	16
3	4	6	11	18
4	8	10	14	19
5	12	15	17	20

Therefore, risk value in Table 1 mapping to the two-dimensional space, then Euclidean distance between the risk assessment point $R(P, S)$ as shown in Figure 2 and the space origin is introduced to calculate risk evaluation values as shown in Equation (12). a, b is the preference correction factors.

$$R = \sqrt[2]{(a * P)^2 + (b * S)^2} \tag{12}$$

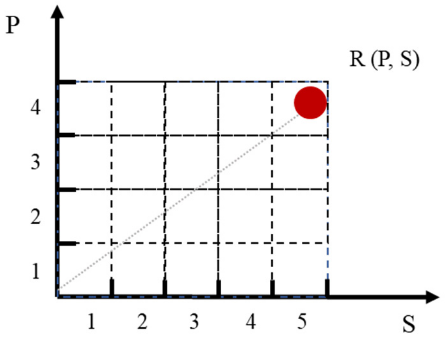


Figure 2. Traditional risk model space of risk factors.

According to Table 1, $R = f(P, S)$, $1 = f(1, 1)$, $2 = f(2, 1)$, $3 = f(4, 1)$ . . . , and based on Equation (12), 'regress' function in MATLAB is applied to implement multiple linear regression fitting, obtaining $a = 2.2$, $b = 3.3$.

Similarly, based on the multi-dimensional safety risk theory, this paper uses a five-level risk factor level method based on expert experience [67]. In other words, the degree from light to heavy is level 1 to level 5. Similarly, based on GJB 900A and expert scoring method, different risk values corresponding to different propagation probability, severity and propagation time are obtained as shown in Table 2. Therefore, the actual parameter values of the safety risk factor propagation probability P, potential severity S, and propagation time T can be quantified into risk factor level.

Table 2. Risk index of multi-dimensional safety risk model.

Risk	**Probability Level**	**Severity Level**	**Propagation Time**
1	1	1	1
1	2	1	1
1	1	1	2
1	1	2	1
1	3	1	1
2	2	1	2
. . .	. . .	. . .	. . .
13	3	3	3
. . .	. . .	. . .	. . .
25	5	5	5

Based on multi-dimensional safety risk model, the risk factors P, S, T are mapped to the three-dimensional space shown as Figure 3. The improved Euclidean distance between the risk assessment point $R(p,s,t)$ and the space origin is introduced to calculate risk evaluation values as shown in Equation (13).

$$R = \sqrt[2]{[a * f_1(p)]^2 + [b * f_2(s)]^2 + [c * f_3(t)]^2} \tag{13}$$

where $f_1(p)$, $f_2(s)$, $f_3(t)$ are risk factor levels, which actual parameter values of risk factors P, S, T are classified into, respectively; a, b, c is the preference correction factors. Based on Table 2 and Equation (13), 'regress' function in MATLAB is applied to implement multiple linear regression fitting, obtaining a = 2.2, b = 3.3, c = 2.7.

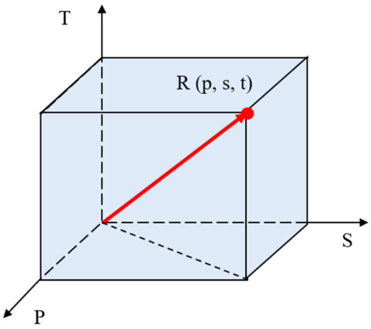


Figure 3. The three-dimensional model space of risk factors.

In addition, total safety risk value R_N of the system and safety risk ratio η_i of element i is calculated as shown in Equations (14) and (15).

$$R_N = \sum_{i=1}^{n} R_i \tag{14}$$

$$\eta_i = \frac{R_i}{R_N} \times 100\% \tag{15}$$

3.3. Evaluation of Multi-Dimensional Safety Risk Model

1. Pareto rule

The safety risk ratio characterizes the extent to which each element in the system contributes to the total safety risk value of the system, and from this, the critical safety factor in the system can be intuitively identified. According to Pareto rule [68,69], when distinguishing safety-critical links, it can be considered that 80% of accidents are originated from 20% of dangerous sources. Therefore, the value of the safety risk ratio η_i is sorted in descending order, and the first 20% of the values of η_i are defined as safety-critical elements, and the last 80% are defined as general safety elements.

2. ALARP principle

As a project risk criterion generally adopted by domestic and foreign institutions, the principle of ALARP (As Low As Reasonably Practicable) [70,71] sets two risk "boundaries" based on the value of safety risk and related experience: intolerable boundary and negligible boundary [70], meanwhile forming three risk region and level: serious risk region, ALARP region and negligible region, and the top extreme of the principle is "accident", and the bottom extreme is "safety". ALARP rule is shown as Figure 4. The values of the regions and boundaries of ALARP principle are all relative, and there is no standard of definition [72,73]. In practice, expert evaluation method considering potential severity, propagation probability, and propagation time can be applied to determine final values of the boundaries [70,74,75]. Meanwhile, alternative values of the boundaries are also obtained. Finally, compared and analyzed results of final values and alternative values of boundaries, final results can be determined. ALARP region means risk value in this region is reasonably acceptable. Therefore, according to the ALARP principle, this paper classifies risk value of each element into different regions, in order to make further research to propose preventive measurements, so as to reduce the risk level and improve system safety.

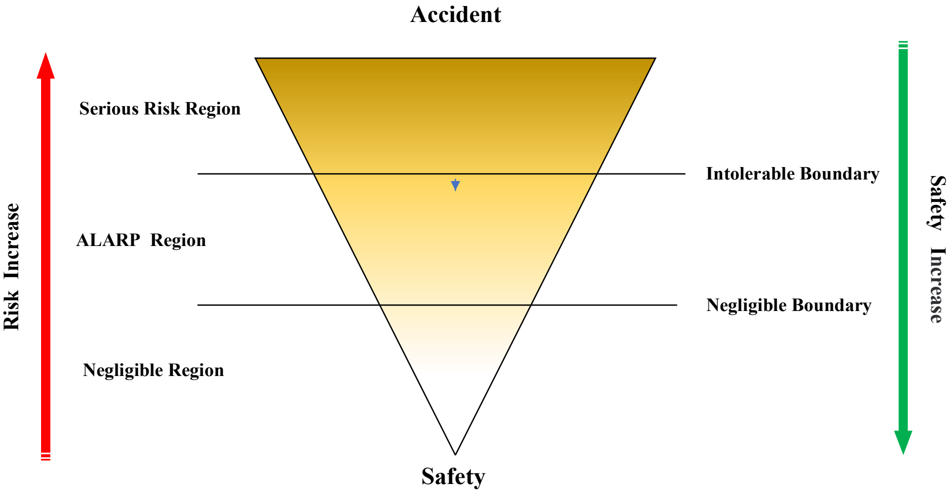


Figure 4. As Low As Reasonably Practicable (ALARP) model.

3. Safety risk entropy

The essence of entropy [76,77] is considered as a measure of the degree of disorder in the system. Currently, there are three typical definitions: Clausius entropy, Boltzmann entropy, Shannon entropy. Therefore, in this paper, safety risk entropy is defined as the measure of all random factors in system safety risk. Through the previous system's safety risk analysis, it was found that the randomness mainly derives from the probabilistic characteristics of each step of the fault propagation process. Therefore, according to the definition of Shannon entropy, it is assumed that the fault propagation from resource element r_i to resource element r_j requires n steps, and the probability of fault propagation for each step is $p_1, p_2, \ldots, p_n$ (based on the direct propagation matrix C_d^P). Then, based on Shannon entropy, H_{ij} means the effect of safety risk entropy that from resource element resource r_i to the resource element r_j, as shown in Equation (16). In other words, H_{ij} represents the uncertainty risk of fault propagation from resource element r_i to resource element r_j. Moreover, total safety risk entropy H_i of resource element r_i, which effects the overall system calculated in Equation (17). The higher the safety risk entropy value is, the greater the uncertainty risk caused by the fault in this element effects on the system is.

$$H_{ij} = -\sum_{m=1}^{n} p_m \ln p_m \tag{16}$$

$$H_i = \sum_{j=1}^{n} H_{ij} \tag{17}$$

According to comprehensive analysis on results of Pareto rule, ALARP principle and safety risk entropy, aimed at the serious risk region and critical risk factors, the coupling correlations are further researched to propose preventive measurements, so as to reduce the risk level and improve system safety.

4. Case Study and Discussion

4.1. Coupling Correlation of Complex System

4.1.1. Hierarchical Model and Description

1. Hierarchical model

Integrated modular avionics (IMA) [78,79] is a shared set of flexible, reusable, and interoperable hardware and software resources. When integrated, these resources can form a platform that provides service, designed and verified to a defined set of safety and performance requirements, to host applications performing aircraft functions [80]. Based on ASAAC criterion [81], IMA system is managed by a three-layer model: Aircraft Level (AL), Integration Area Level (IAL) and Resource Element Level (REL). This three-level hierarchy of IMA is typical task-function-resource model.

On the basis of the initial design plan of a certain aircraft, this integrated modular avionics (IMA) system contains three functions: navigation, communication, and integrated management; nine system resources: GPM (Graphics Processing Module), GPM, DPM (Data Processing Module), DPM, SPM (Signal Processing Module), SPM, PCM (Power Conversion Module), PCM, NSM (Network Support Module). The IMA system task-function-resource mapping relationship and details of function-resource mapping relationship are shown in Figure 5 and Table 3.

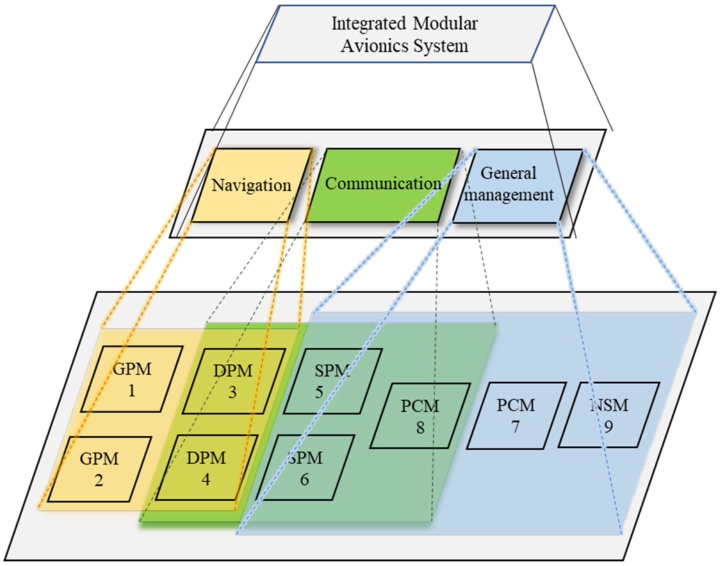


Figure 5. Task-function-resource model of the Integrated modular avionics (IMA) system. GPM, Graphics Processing Module; DPM, Data Processing Module; SPM, Signal Processing Module; PCM, Power Conversion Module; NSM, Network Support Module.

Table 3. Details of function-resource mapping relationship of the IMA system.

Function Layer	**Resource Layer/Resource Serial Number**				
	GPM	**DPM**	**SPM**	**PCM**	**NSM**
navigation	1, 2	3, 4	/	/	/
communication	/	3, 4	5, 6	8	/
integrated management	/		5, 6	7, 8	9

It is generally considered that in the IMA system, the top-level system functional entities are unique, and it can be considered that there is only one element in the IMA system task set $T = \{t_1\}$, which is aimed to complete the management of the entire IMA system to support the operation of the system. Therefore, it can be ignored. Then, function element set $F = \{f_1, f_2, f_3\}$; resource element set $R = \{r_1, r_2, \ldots, r_9\}$.

The safety critical grade *SCG* of the resource elements is divided into 3 levels (larger numbers indicate higher *SCG*), and based on experience set $SCG_{1\times 9} = \{1, 2, 3, 3, 2, 1, 2, 2, 3\}$.

2. Coupling degree Matrix

Function-resource element mapping coupling matrix M^{fr} is presented in Matrix (18).

$$M^{fr} = (M_{ij}^{fr})_{3\times 9} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{18}$$

4.1.2. Coupling Degree and Related Factors

1. Direct coupling degree matrix

Direct coupling relationship caused by different resource elements serving same function can be presented by direct coupling degree matrix C^d shown in Matrix (19).

$$C^d = (C_{ij}^d)_{9\times 9} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \tag{19}$$

2. Indirect coupling degree

Based on Floyd algorithm, fault propagation path order is calculated referring to direct coupling matrix C^d, and then, the indirect coupling degree matrix C^c and the shortest path matrix C^r of fault propagation are generated as shown in Matrix (20) and Matrix (21), respectively.

C_{ij}^r represents the next element that the fault propagation from element i to element j should pass. For instance, fault propagation from element 1 to element 9, according to $C_{19}^r = 3$, it can be inferred that fault in element 1 will propagate to element 3 first. Then, according to $C_{39}^r = 5$, it can be inferred that fault will propagate from element 3 to element 5 second. Finally, according to $C_{59}^r = 9$, it can be seen that fault will propagate from element 5 to element 9. Therefore, the fault propagation path from element 1 to element 9 is formed: $1 \rightarrow 3 \rightarrow 5 \rightarrow 9$. So, other fault propagation paths can be deduced by analogy.

$$C^c = (C_{ij}^c)_{9\times 9} = \begin{bmatrix} 0 & 1 & 1 & 1 & 2 & 2 & 3 & 2 & 3 \\ 1 & 0 & 1 & 1 & 2 & 2 & 3 & 2 & 3 \\ 1 & 1 & 0 & 1 & 1 & 1 & 2 & 1 & 2 \\ 1 & 1 & 1 & 0 & 1 & 1 & 2 & 1 & 2 \\ 2 & 2 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 2 & 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 3 & 3 & 2 & 2 & 1 & 1 & 0 & 1 & 1 \\ 2 & 2 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 3 & 3 & 2 & 2 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \tag{20}$$

$$C^r = (C^r_{ij})_{9\times9} = \begin{bmatrix} 1 & 2 & 3 & 4 & 3 & 3 & 3 & 3 & 3 \\ 1 & 2 & 3 & 4 & 3 & 3 & 3 & 3 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 & 5 & 8 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 5 & 8 & 5 \\ 3 & 3 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 3 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 5 & 5 & 5 & 5 & 6 & 7 & 8 & 9 \\ 3 & 3 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 5 & 5 & 5 & 5 & 6 & 7 & 8 & 9 \end{bmatrix} \tag{21}$$

3. Potential severity

The potential severity effect is greatest when there is a direct coupling correlation relationship between the elements (the coupling degree is 1), so the corresponding potential severity value is set to 1. In addition, when the coupling degree is 5 or above, the degree of effect is the smallest, and the corresponding potential severity value is set to 0.1. Based on Equation (7), $S_p(1) = \frac{1}{1+a(1-c)^2} = 1$, $S_p(5) = \frac{1}{1+a(5-c)^2} = 0.1$, as shown in equation set (22), and then solving equation set (22), obtaining $c = 1$, $a = 0.56$. Then, based on Equation (7), obtaining $S_p(2) = 0.64$,$S_p(3) = 0.31$,$S_p(4) = 0.17$. Therefore, potential severity matrix S_p is shown as Matrix (23).

$$\begin{cases} \frac{1}{1+a(1-c)^2} = 1 \\ \frac{1}{1+a(5-c)^2} = 0.1 \end{cases} \tag{22}$$

$$S = (S_p)_{9\times9} = \begin{bmatrix} 0.00 & 1.00 & 1.00 & 1.00 & 0.64 & 0.64 & 0.31 & 0.64 & 0.31 \\ 1.00 & 0.00 & 1.00 & 1.00 & 0.64 & 0.64 & 0.31 & 0.64 & 0.31 \\ 1.00 & 1.00 & 0.00 & 1.00 & 1.00 & 1.00 & 0.64 & 1.00 & 0.64 \\ 1.00 & 1.00 & 1.00 & 0.00 & 1.00 & 1.00 & 0.64 & 1.00 & 0.64 \\ 0.64 & 0.64 & 1.00 & 1.00 & 0.00 & 1.00 & 1.00 & 1.00 & 1.00 \\ 0.64 & 0.64 & 1.00 & 1.00 & 1.00 & 0.00 & 1.00 & 1.00 & 1.00 \\ 0.31 & 0.31 & 0.64 & 0.64 & 1.00 & 1.00 & 0.00 & 1.00 & 1.00 \\ 0.64 & 0.64 & 1.00 & 1.00 & 1.00 & 1.00 & 1.00 & 0.00 & 1.00 \\ 0.31 & 0.31 & 0.64 & 0.64 & 1.00 & 1.00 & 1.00 & 1.00 & 0.00 \end{bmatrix} \tag{23}$$

In addition, considering the safety critical grade of the resource elements $SCG_{1\times9} = \{1, 2, 3, 3, 2, 1, 2, 2, 3\}$, and based on Equation (7), the final potential severity matrix S is presented as Matrix (24).

$$S = S_{9\times9} = \begin{bmatrix} 0.00 & 2.00 & 3.00 & 3.00 & 1.28 & 0.64 & 0.62 & 1.28 & 0.93 \\ 1.00 & 0.00 & 3.00 & 3.00 & 1.28 & 0.64 & 0.62 & 1.28 & 0.93 \\ 1.00 & 2.00 & 0.00 & 3.00 & 2.00 & 1.00 & 1.28 & 2.00 & 1.92 \\ 1.00 & 2.00 & 3.00 & 0.00 & 2.00 & 1.00 & 1.28 & 2.00 & 1.92 \\ 0.64 & 1.28 & 3.00 & 3.00 & 0.00 & 1.00 & 2.00 & 2.00 & 3.00 \\ 0.64 & 1.28 & 3.00 & 3.00 & 2.00 & 0.00 & 2.00 & 2.00 & 3.00 \\ 0.31 & 0.62 & 1.92 & 1.92 & 2.00 & 1.00 & 0.00 & 2.00 & 3.00 \\ 0.64 & 1.28 & 3.00 & 3.00 & 2.00 & 1.00 & 2.00 & 0.00 & 3.00 \\ 0.31 & 0.62 & 1.92 & 1.92 & 2.00 & 1.00 & 2.00 & 2.00 & 0.00 \end{bmatrix} \tag{24}$$

4. Propagation probability

Fault injection is applied in simulation of the IMA system for 10,000 times, and the direct propagation probability matrix C_d^P and the direct propagation time matrix C_d^T are obtained as shown in Matrix (25) and Matrix (26).

$$C_d^p = (C_d^p)_{9\times 9} = \begin{bmatrix} 0.0 & 1.0 & 0.8 & 0.9 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 \\ 1.0 & 0.0 & 0.8 & 1.0 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 \\ 0.8 & 0.8 & 0.0 & 1.0 & 0.8 & 0.7 & 0.0 & 0.9 & 0.0 \\ 0.9 & 1.0 & 1.0 & 0.0 & 0.8 & 0.8 & 0.0 & 0.7 & 0.0 \\ 0.0 & 0.0 & 0.8 & 0.8 & 0.0 & 1.0 & 0.9 & 0.7 & 0.9 \\ 0.0 & 0.0 & 0.7 & 0.8 & 1.0 & 0.0 & 0.7 & 0.8 & 0.9 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.9 & 0.7 & 0.0 & 0.8 & 1.0 \\ 0.0 & 0.0 & 0.9 & 0.7 & 0.7 & 0.8 & 0.8 & 0.0 & 1.0 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.9 & 0.9 & 1.0 & 1.0 & 0.0 \end{bmatrix} \tag{25}$$

$$C_d^T = (C_d^T)_{9\times 9} = \begin{bmatrix} 0.0 & 0.5 & 0.7 & 0.6 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 \\ 0.5 & 0.0 & 0.8 & 0.4 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 \\ 0.7 & 0.8 & 0.0 & 0.6 & 0.7 & 0.7 & 0.0 & 0.9 & 0.0 \\ 0.6 & 0.4 & 0.6 & 0.0 & 0.8 & 0.7 & 0.0 & 0.8 & 0.0 \\ 0.0 & 0.0 & 0.7 & 0.8 & 0.0 & 0.5 & 0.6 & 0.7 & 0.4 \\ 0.0 & 0.0 & 0.7 & 0.7 & 0.5 & 0.0 & 0.7 & 0.5 & 0.6 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.6 & 0.7 & 0.0 & 0.6 & 0.5 \\ 0.0 & 0.0 & 0.9 & 0.8 & 0.7 & 0.5 & 0.6 & 0.0 & 0.8 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.4 & 0.6 & 0.5 & 0.8 & 0.0 \end{bmatrix} \tag{26}$$

where the unit in C_d^P and C_d^T is percentage (%) and second (s), respectively.

Based on direct propagation probability matrix C_d^P, referring to propagation path, indirect propagation probability is calculated by Equation (8). For example, fault propagation path from element 1 to element 9 is 1 → 3 → 5 → 9. The propagation probability from element 1 to element 3, and element 3 to element 5, and element 5 to element 9 is 0.8, 0.8, 0.9, respectively, based on $C_{19}^P = 0.8$, $C_{39}^P = 0.8$, $C_{59}^P = 0.9$ in the direct propagation probability C_d^P. Then, fault propagation probability from element 1 to element 9 is 0.8 × 0.8 × 0.9 = 0.576. Similarly, whole indirect propagation probability matrix C_c^P is formed as shown in Matrix (27).

$$C_c^p = (C_c^p)_{9\times 9} = \begin{bmatrix} 0.00 & 1.00 & 0.80 & 0.90 & 0.64 & 0.56 & 0.576 & 0.72 & 0.576 \\ 1.00 & 0.00 & 0.80 & 1.00 & 0.64 & 0.56 & 0.576 & 0.72 & 0.576 \\ 0.80 & 0.80 & 0.00 & 1.00 & 0.80 & 0.70 & 0.72 & 0.90 & 0.72 \\ 0.90 & 1.00 & 1.00 & 0.00 & 0.80 & 0.80 & 0.72 & 0.70 & 0.72 \\ 0.64 & 0.64 & 0.80 & 0.80 & 0.00 & 1.00 & 0.90 & 0.70 & 0.90 \\ 0.56 & 0.56 & 0.70 & 0.80 & 1.00 & 0.00 & 0.70 & 0.80 & 0.90 \\ 0.576 & 0.576 & 0.72 & 0.72 & 0.90 & 0.70 & 0.00 & 0.80 & 1.00 \\ 0.72 & 0.72 & 0.90 & 0.70 & 0.70 & 0.80 & 0.80 & 0.00 & 1.00 \\ 0.576 & 0.576 & 0.72 & 0.72 & 0.90 & 0.90 & 1.00 & 1.00 & 0.00 \end{bmatrix} \tag{27}$$

5. Propagation time

Similarly, based on direct propagation time C_d^T, referring to propagation path, indirect propagation time is calculated by Equation (9). For instance, fault propagation path from element 1 to element 9 is 1 → 3 → 5 → 9. The fault propagation time from element 1 to element 3, and element 3 to element 5, and element 5 to element 9 is 0.7, 0.7, 0.4, respectively, based on $C_{19}^T = 0.7$(s), $C_{39}^T = 0.7$(s), $C_{59}^T = 0.4$(s) in the direct propagation time C_d^T. Then propagation time from element 1 to element 9 is 0.7 + 0.7 + 0.4 = 1.8(s). Similarly, the whole indirect propagation time matrix C_c^T is formed as shown in Matrix (28).

$$C_c^T = (C_c^T)_{9\times 9} = \begin{bmatrix} 0.0 & 0.5 & 0.7 & 0.6 & 1.4 & 1.4 & 2.0 & 1.6 & 1.8 \\ 0.5 & 0.0 & 0.8 & 0.4 & 1.5 & 1.5 & 2.1 & 1.7 & 1.9 \\ 0.7 & 0.8 & 0.0 & 0.6 & 0.7 & 0.7 & 1.3 & 0.9 & 1.1 \\ 0.6 & 0.4 & 0.6 & 0.0 & 0.8 & 0.7 & 1.4 & 0.8 & 1.2 \\ 1.4 & 1.5 & 0.7 & 0.8 & 0.0 & 0.5 & 0.6 & 0.7 & 0.4 \\ 1.4 & 1.5 & 0.7 & 0.7 & 0.5 & 0.0 & 0.7 & 0.5 & 0.6 \\ 2.0 & 2.1 & 1.3 & 1.4 & 0.6 & 0.7 & 0.0 & 0.6 & 0.5 \\ 1.6 & 1.7 & 0.9 & 0.8 & 0.7 & 0.5 & 0.6 & 0.0 & 0.8 \\ 1.8 & 1.9 & 1.1 & 1.2 & 0.4 & 0.6 & 0.5 & 0.8 & 0.0 \end{bmatrix} \tag{28}$$

4.2. Risk Assessment

1. Classification of risk factors

Considering numerical ranges within the indirect propagation probability matrix C_c^P, the potential severity matrix S, and the indirect propagation time matrix C_c^T, qualitative risk factor level rules are given (from light to heavy, respectively 1 to 5), as shown in Table 4 based on experience.

Table 4. Classification level of risk factor.

Risk Factor Level	C_c^P	S	C_c^T/s
1	(0, 0.3)	(0, 0.6)	(2, +∞)
2	(0.3, 0.5)	(0.6, 1.2)	(1.5, 2)
3	(0.5, 0.7)	(1.2, 1.8)	(1, 1.5)
4	(0.7, 0.9)	(1.8, 2.4)	(0.5, 1)
5	(0.9, 1)	(2.4, +∞)	(0, 0.5)

2. Calculation of multi-dimensional safety risk

Based on Table 2, the safety risk factors P, S, T are converted into uniform safety risk level. Equation (13) is used to calculate multi-dimensional safety risk value, as shown in Matrix (29). Total risk value that element i effect on the overall system is calculated as shown in Matrix (30).

$$P = R_{9\times 9} = \begin{bmatrix} 0.00 & 21.85 & 21.59 & 21.59 & 14.39 & 12.36 & 10.78 & 14.30 & 10.78 \\ 18.62 & 0.00 & 21.59 & 23.99 & 14.39 & 12.36 & 9.72 & 14.30 & 10.78 \\ 15.42 & 19.19 & 0.00 & 22.58 & 19.19 & 14.27 & 15.53 & 19.19 & 17.81 \\ 15.42 & 21.85 & 22.58 & 0.00 & 19.19 & 15.42 & 15.53 & 18.29 & 17.81 \\ 12.36 & 14.39 & 21.59 & 21.59 & 0.00 & 18.62 & 19.19 & 18.29 & 23.06 \\ 12.36 & 14.39 & 20.80 & 21.59 & 21.85 & 0.0 & 18.29 & 20.83 & 21.59 \\ 9.14 & 9.72 & 17.81 & 17.81 & 19.19 & 14.27 & 0.0 & 19.19 & 23.9 \\ 12.25 & 14.30 & 21.59 & 20.80 & 18.29 & 17.41 & 19.19 & 0.0 & 22.58 \\ 9.14 & 10.78 & 17.81 & 17.81 & 20.83 & 15.42 & 21.85 & 20.29 & 0.0 \end{bmatrix} \tag{29}$$

$$R_i = [127.66, 125.76, 142.18, 143.08, 149.11, 151.71, 134.13, 144.42, 136.95] \tag{30}$$

System total safety risk assessment value $R_N = 1255$, and based on Equation (15), safety risk ratio is shown in Matrix (31).

$$\eta_i = [10.17, 10.02, 11.33, 11.40, 11.88, 12.09, 10.69, 11.51, 10.91] \tag{31}$$

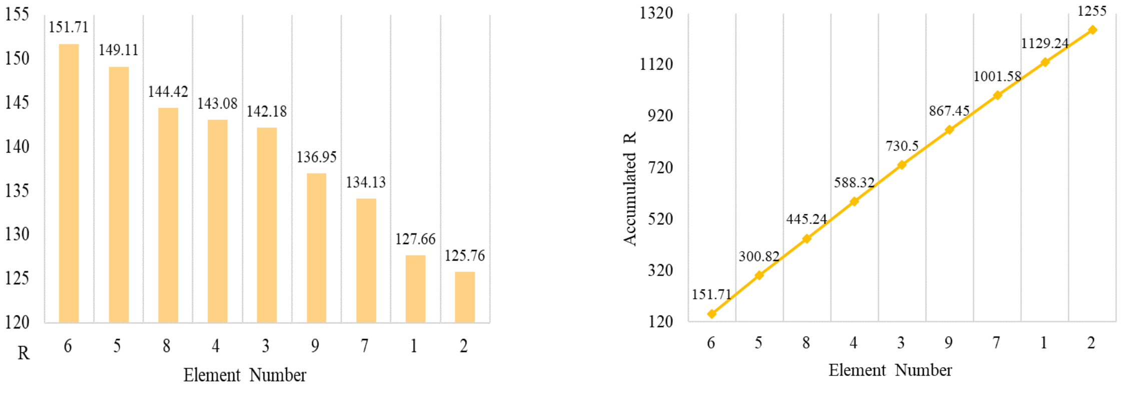
3. Results of risk

- Pareto rule

The results of R_i and η_i are sorted in descending order as shown in Table 5. Then Pareto chart is presented as Figures 6 and 7.

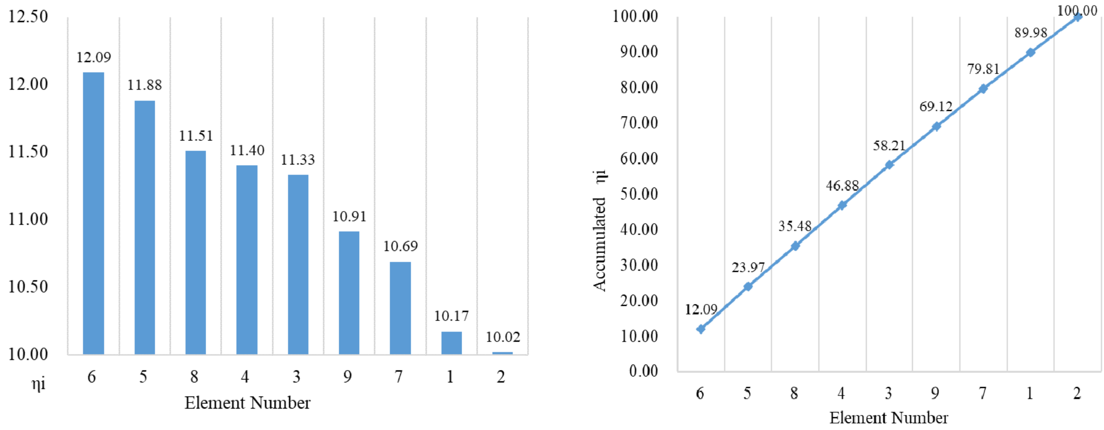
Table 5. Results of Pareto rule.

Rank	Element Number	R_i	η_i	Accumulated Value
1	6	151.71	12.09	12.09%
2	5	149.11	11.88	23.97%
3	8	146.42	11.51	35.48%
4	4	146.08	11.40	46.88%
5	3	143.18	11.33	58.21%
6	9	133.95	10.91	69.12%
7	7	131.13	10.69	79.81%
8	1	127.66	10.17	89.98%
9	2	125.76	10.02	100.00%



(**a**) (**b**)

Figure 6. Chart of Pareto rule of the risk value R. (**a**) the risk value R of the single element in descending order; (**b**) the accumulated risk value R.



(**a**) (**b**)

Figure 7. Chart of Pareto rule of η_i. (**a**) the safety risk ratio η_i of the single element in descending order; (**b**) the accumulated the safety risk ratio η_i.

- ALARP principle

Under the ALARP principle, two risk "boundaries" are set based on expert experience: the intolerable boundary and the negligible boundary are 145 and 130, respectively, and the alternative values of the boundaries are 140 and 130, respectively. On the condition of alternative values, element 3, 4, 5, 6, 8 are all in the serious risk region. According to Pareto rule, when distinguishing safety-critical links, it can be considered that 80% of accidents are originated from 20% of dangerous sources, but the accumulated risk value of the elements in the serious risk region is well over 20%, which is a violation of the Pareto rule. Therefore, value of the boundaries 145, 130 are determined. The risk level of each element is presented in Figure 8.

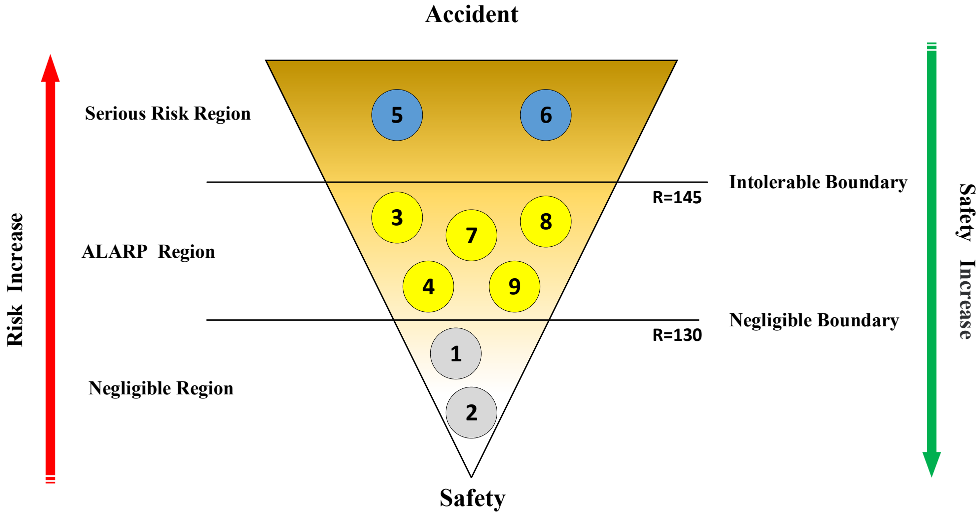


Figure 8. Results of ALARP model chart.

- Safety risk entropy

Based on Equation (16), entropy matrix H is presented as Matrix (32).

$$H = H_{9\times 9} = \begin{bmatrix} 0.00 & 0.00 & 0.17 & 0.09 & 0.35 & 0.42 & 0.45 & 0.27 & 0.45 \\ 1.00 & 0.00 & 0.17 & 0.00 & 0.35 & 0.42 & 0.45 & 0.27 & 0.45 \\ 0.17 & 0.17 & 0.00 & 0.00 & 0.17 & 0.24 & 0.27 & 0.09 & 0.27 \\ 0.09 & 0.00 & 0.00 & 0.00 & 0.17 & 0.17 & 0.27 & 0.24 & 0.27 \\ 0.35 & 0.35 & 0.17 & 0.17 & 0.00 & 0.00 & 0.09 & 0.24 & 0.09 \\ 0.42 & 0.42 & 0.24 & 0.17 & 0.00 & 0.00 & 0.24 & 0.17 & 0.09 \\ 0.45 & 0.45 & 0.27 & 0.27 & 0.09 & 0.24 & 0.00 & 0.17 & 0.00 \\ 0.27 & 0.27 & 0.09 & 0.24 & 0.24 & 0.17 & 0.17 & 0.00 & 0.00 \\ 0.45 & 0.45 & 0.27 & 0.27 & 0.09 & 0.09 & 0.00 & 0.00 & 0.00 \end{bmatrix} \tag{32}$$

Based on Equation (17), total safety risk entropy H_i of element i which effects on the overall system is calculated as shown in Matrix (33). The safety risk entropy of the single element in descending order and the accumulated the safety risk entropy are presented in Figure 9.

$$H_i = [2.24, 2.14, 1.43, 1.25, 1.51, 1.81, 1.97, 1.49, 1.64] \tag{33}$$

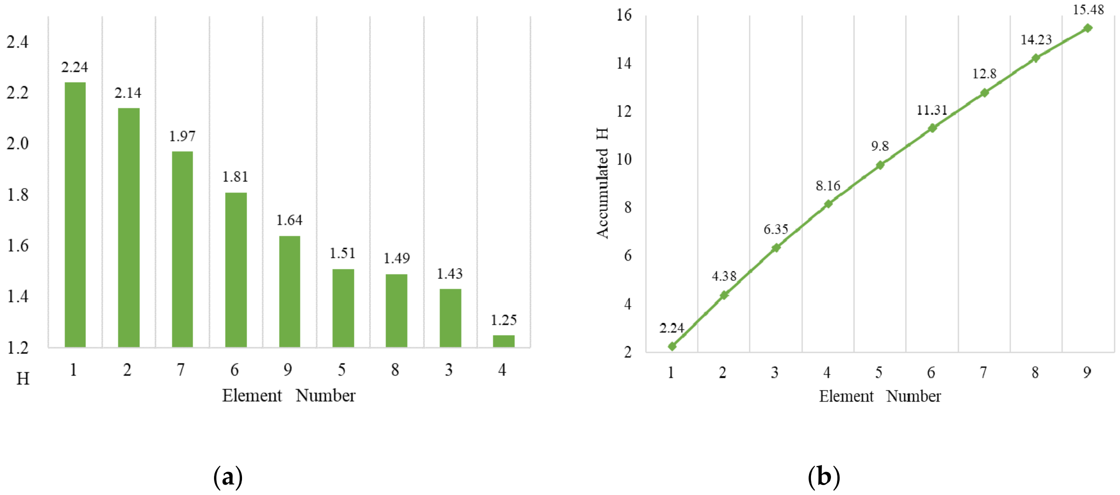


Figure 9. Chart of results of safety risk entropy *H*. (**a**) the safety risk entropy of the single element in descending order; (**b**) the accumulated the safety risk entropy.

4.3. Discussion

1. According to the sorting results in Figure 6, Figure 7, and Pareto Rule, elements 5 and 6 can be defined as the safety-critical elements; and elements 1, 2, 3, 4, 7, 8, and 9 are defined as safety-general elements.
2. Based on Figure 8, element 5 and 6 are in the serious risk region; elements 3, 4, 7, 8, and 9 are in the ALARP region; and elements 1 and 2 are in the negligible region.
3. From Figure 9, elements 1 and 2 have higher uncertainty; elements 6, 7, and 9 have moderate uncertainty; and elements 3, 4, 5, 8 are with lower uncertainty.
4. In summary, elements 5 and 6 are the safety-critical elements and located in a serious risk region, which has a serious effect on the overall system. Simultaneously, it has a certain degree of uncertainty. Therefore, corresponding measures must be taken to ensure the safety of elements 5 and 6 in order to decrease the system risk. In other words, more attention must be paid to Signal Processing Module in this avionics system. Elements 3, 4, 7, 8, and 9 are in the ALARP region and have lower uncertainty. This means that the risk caused by these elements in the region are acceptable. As a consequence, Data Processing Module, Power Conversion Module, and Network Support Module should be given due attention if the conditions permit. Although elements 1 and 2 have higher uncertainty, they are located in the negligible region. Consequently, Graphics Processing Module can be ignored under limited conditions. If the conditions permit, in view of the higher uncertainty of elements 1 and 2 (Graphics Processing Module), by increasing the reliability of elements 1 and 2 and ensuring the reliability of the element's correlation with other elements, such as ensuring the reliability of the data transmission channel between elements 1 and 2 and other elements, and the reliability of the information transmission bus, etc. Based on these measures, the fault propagation from elements 1 and 2 to other elements can be reduced, so as to reduce risk to overall systems of high uncertainty of elements 1 and 2.

5. Conclusions

While aiming to address the insufficiency of traditional safety risk analysis and risk assessment technology to solve coupling problems between components in complex systems, this study proposed a novel risk assessment and analysis method for correlation in complex systems based on multi-dimensional theory. Firstly, a matrix-based hierarchical model for the complex system is presented and correlation relationships between elements in the system were established. Furthermore, based on correlation relationship, the multi-dimensional theory and model are proposed in order to evaluate risk more objectively. Moreover, based on the Pareto rule, ALARP principle, and safety risk entropy, the critical risk elements are identified, which provides a theoretical basis for putting forward preventive measures, so as to ensure and improve system safety. Compared with the current methods and technologies, the method proposed in this paper mainly reflects the advantages of two aspects. On the one hand, the hierarchical model is modeled in a matrix manner, and the association relationship of each element in the complex system is quickly and accurately analyzed, which reduces the skill requirements of analysts. On the other hand, it provides a feasible and multi-faceted analysis method for the risk assessment of systems in view of fault propagation, which is the core judgment criterion for identifying critical risk factors and of great significance for ensuring system safety.

Author Contributions: Conceptualization, Z.J. and T.Z.; methodology, Z.J., S.W., and F.R.; formal analysis, Z.J. and F.R.; writing—original draft preparation, Z.J.; writing—review and editing, Z.J. and S.W.; project administration, T.Z.; funding acquisition, T.Z. and S.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Foundation of No.61400020404.

Conflicts of Interest: The authors declare that there are no conflicts of interest.

References

1. Zhu, Z.; Feng, Y.; Lu, C.; Fei, C. Efficient Driving Plan and Validation of Aircraft NLG Emergency Extension System via Mixture of Reliability Models and Test Bench. *Appl. Sci.* **2019**, *9*, 3578. [CrossRef]
2. Song, S.; Ko, T.K.; Choi, Y.; Lee, S. A Novel Fault Diagnosis Method for High-Temperature Superconducting Field Coil of Superconducting Rotating Machine. *Appl. Sci.* **2019**, *10*, 223. [CrossRef]
3. Xiao, D.; Ding, J.; Li, X.; Huang, L. Gear Fault Diagnosis Based on Kurtosis Criterion VMD and SOM Neural Network. *Appl. Sci.* **2019**, *9*, 5424. [CrossRef]
4. Chu, J.; Zhao, T.; Jiao, J.; Chen, Z.; Ren, F. Reliability Modelling and Evaluation for LTD System Based on Load-Sharing Model. *Appl. Sci.* **2019**, *9*, 5528. [CrossRef]
5. Jiao, J.; Wei, M.; Yuan, Y.; Zhao, T. Risk Quantification and Analysis of Coupled Factors Based on the DEMATEL Model and a Bayesian Network. *Appl. Sci.* **2020**, *10*, 317. [CrossRef]
6. Vesely, W.E.; Goldberg, F.F.; Roberts, N.H.; Haasl, D.F. *Fault Tree Handbook*; Nuclear Regulatory Commission: Washington, DC, USA, 1981.
7. Papazoglou, I.A. Functional Block Diagrams and Automated Construction of Event Trees. *Reliab. Eng. Syst. Saf.* **1998**, *61*, 185–214. [CrossRef]
8. Andrews, J.D.; Dunnett, S.J. Event-Tree Analysis Using Binary Decision Diagrams. *IEEE Trans. Reliab.* **2000**, *49*, 230–238. [CrossRef]
9. Amzen, H.E. Failure Mode and Effect Analysis: A Powerful Engineering Tool for Component and System Optimization. In Proceedings of the Fifth Reliability and Maintainability Conference, New York, NY, USA, 18–20 July 1966; pp. 355–371.
10. Teng, S.; Ho, S.Y. Failure Mode and Effects Analysis: An Integrated Approach for Product Design and Process Control. *Int. J. Qual. Reliab. Manag.* **1996**, *13*, 8–26. [CrossRef]
11. Mahdiyar, A.; Jahed Armaghani, D.; Koopialipoor, M.; Hedayat, A.; Abdullah, A.; Yahya, K. Practical Risk Assessment of Ground Vibrations Resulting from Blasting, Using Gene Expression Programming and Monte Carlo Simulation Techniques. *Appl. Sci.* **2020**, *10*, 472. [CrossRef]
12. Schuëller, G.I. Impact of probability risk assessment on containment. *Nucl. Eng. Des.* **1984**, *80*, 203–216. [CrossRef]
13. Li, J. The Application of Probability Risk Assessment to the Safety Management in a Nuclear Power Plant. *J. Chin. Peoples Armed Police Force Acad.* **2010**, *26*, 43–46.
14. Zhou, X.; Tang, Y. Modeling and Fusing the Uncertainty of FMEA Experts Using an Entropy-Like Measure with an Application in Fault Evaluation of Aircraft Turbine Rotor Blades. *Entropy* **2018**, *20*, 864. [CrossRef]
15. Rhee, S.J.; Ishii, K. Using cost based FMEA to enhance reliability and serviceability. *Adv. Eng. Inform.* **2003**, *17*, 179–188. [CrossRef]
16. Jang, H.A.; Min, S. Time-Dependent Probabilistic Model for Hierarchical Structure in Failure Mode and Effect Analysis. *Appl. Sci.* **2019**, *9*, 4265. [CrossRef]
17. Liu, Y.; Yan, Z.P.; Yuan, Y.; Li, H. A FTA-based method for risk decision-making in emergency response. *Comput. Oper. Res.* **2014**, *42*, 49–57. [CrossRef]

18. Cheraghi, M.; Eslami Baladeh, A.; Khakzad, N. A fuzzy multi-attribute HAZOP technique (FMA-HAZOP): Application to gas wellhead facilities. *Saf. Sci.* **2019**, *114*, 12–22. [CrossRef]
19. Feng, Q.; Sha, S.; Dai, L. Bayesian Survival Analysis Model for Girth Weld Failure Prediction. *Appl. Sci.* **2019**, *9*, 1150. [CrossRef]
20. Zhao, C.; Wang, P.; Yan, F. Reliability Analysis of the Reconfigurable Integrated Modular Avionics Using the Continuous-Time Markov Chains. *Int. J. Aerosp. Eng.* **2018**, *2018*, 5213249. [CrossRef]
21. Singh, P.; Singh, L. Verification of safety critical and control systems of Nuclear Power Plants using Petri nets. *Ann. Nucl. Energy* **2019**, *132*, 584–592. [CrossRef]
22. Baouya, A.; Ait Mohamed, O.; Bennouar, D.; Ouchani, S. Safety analysis of train control system based on model-driven design methodology. *Comput. Ind.* **2019**, *105*, 1–16. [CrossRef]
23. Wilson, S.P.; Kelly, T.P.; McDermid, J. Safety Case Development: Current Practice, Future Prospects. In *Safety and Reliability of Software Based Systems*; Springer: London, UK, 1997; pp. 135–156.
24. Kelly, T.P. Arguing Safety—A Systematic Approach to Safety Case Management . Ph.D. Thesis, Department of Computer Science University of York, York, UK, September 1998.
25. Alexander, R.; Kelly, T.P.; Kurd, Z.; McDermid, J.A. Safety Cases for Advanced Control Software: Safety Case Patterns. Ph.D. Thesis, Department of Computer Science University of York, York, UK, 2007.
26. Iwu, F.; Galloway, A.; McDermid, J.; Toyn, I. Integrating Safety and Formal Analyses Using UML and PFS. *Reliab. Eng. Syst. Saf.* **2007**, *92*, 156–170. [CrossRef]
27. Hollnagel, E.; Goteman, O. The Functional Resonance Accident Model. *Proc. Cogn. Syst. Eng. Process Plant* **2004**, *2004*, 155–161.
28. Hollnagel, E. *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems*; Ashgate Publishing, Ltd.: Farnham, UK, 2012.
29. SAE. *ARP 4754 Certification Considerations for Highly-Integrated or Complex Aircraft Systems*; SAE: Warrendale, PA, USA, 1996.
30. SAE. *ARP 4754A Guidelines for Development of Civil Aircraft and Systems*; SAE: Warrendale, PA, USA, 2010.
31. SAE. *ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*; SAE: Warrendale, PA, USA, 1996.
32. *MIL-STD-882E Department of Defence Standard Practice: System Safety*; Defense Acquisition University: Fort Belvoir, VA, USA, 2011.
33. Mazzuchi, T.A.; Linzey, W.G.; Bruning, A. A paired comparison experiment for gathering expert judgment for an aircraft wiring risk assessment. *Reliab. Eng. Syst. Saf.* **2008**, *93*, 722–731. [CrossRef]
34. Cour-Harbo, A.L. Quantifying risk of ground impact fatalities of power line inspection BVLOS flight with small unmanned aircraft. In Proceedings of the 2017 International Conference on Unmanned Aircraft Systems, Miami, FL, USA, 13–16 June 2017.
35. Li, L.; Wu, Y.; Guo, G.; Shi, J. Research on risk assessment method of subway operation based on cloud model. In Proceedings of the 2016 35th Chinese Control Conference (CCC), Chengdu, China, 27–29 July 2016.
36. Fayaz, M.; Ullah, I.; Park, D.; Kim, K.; Kim, D. An Integrated Risk Index Model Based on Hierarchical Fuzzy Logic for Underground Risk Assessment. *Appl. Sci.* **2017**, *7*, 1037. [CrossRef]
37. Duan, Y.; Cai, Y.; Wang, Z.; Deng, X. A Novel Network Security Risk Assessment Approach by Combining Subjective and Objective Weights under Uncertainty. *Appl. Sci.* **2018**, *8*, 428. [CrossRef]
38. Weng, G.; Bhalla, U.S.; Iyengar, R. Complexity in biological signaling systems. *Science* **1999**, *284*, 92–96. [CrossRef]
39. Rind, D. Complexity and climate. *Science* **1999**, *284*, 105–107. [CrossRef]
40. Chan, S. *Complex Adaptive Systems, in: Research Seminar in Engineering Systems*; MIT Press: Cambridge, MA, USA, 2001; pp. 1–9.
41. Ladyman, J.; Lambert, J.; Wiesner, K. What is a complex system? *Eur. J. Philos. Sci.* **2013**, *3*, 33–67. [CrossRef]
42. Dietz, T.; Klamroth, K.; Kraus, K.; Ruzika, S.; Schäfer, L.E.; Schulze, B.; Stiglmayr, M.; Wiecek, M.M. Introducing multiobjective complex systems. *Eur. J. Oper. Res.* **2020**, *280*, 581–596. [CrossRef]
43. Mokshin, A.V.; Mokshin, V.V.; Sharnin, L.M. Adaptive genetic algorithms used to analyze behavior of complex system. *Commun. Nonlinear Sci.* **2019**, *71*, 174–186. [CrossRef]
44. Nair, A.; Reckien, D.; van Maarseveen, M.F.A.M. A generalised fuzzy cognitive mapping approach for modelling complex systems. *Appl. Soft Comput.* **2019**, *84*, 105754. [CrossRef]

45. Chaabane, S.; Trentesaux, D. Coping with disruptions in complex systems: A framework. *IFAC-PapersOnLine* **2019**, *52*, 2413–2418. [CrossRef]
46. Chen, L.; Jiao, J.; Wei, Q.; Zhao, T. An improved formal failure analysis approach for safety-critical system based on MBSA. *Eng. Fail. Anal.* **2017**, *82*, 713–725. [CrossRef]
47. Wei, Q.X. A Research of Formal Verification of System Safety based on Model Checking. Master's Thesis, Beihang University, Beijing, China, 2017.
48. Wang, H.; Zhao, T.; Ren, F.; Jiang, Z. Integrated modular avionics system safety analysis based on model checking. In Proceedings of the 2017 Annual Reliability and Maintainability Symposium (RAMS), Orlando, FL, USA, 23–26 January 2017.
49. Medasani, S.; Kim, J.; Krishnapuram, R. An overview of membership function generation techniques for pattern recognition. *Int. J. Approx. Reason.* **1998**, *19*, 391–417. [CrossRef]
50. Dombi, J. Membership function as an evaluation. *Fuzzy Sets Syst.* **1990**, *35*, 1–21. [CrossRef]
51. Rakus-Andersson, E. The new approach to the construction of parametric membership functions for fuzzy sets with unequal supports. *Procedia Comput. Sci.* **2017**, *112*, 2057–2065. [CrossRef]
52. Liu, K.; Li, J.; Yang, L. The measure and improvement of fuzzy decision in membership function determination method. *Shaanxi Inst. Technol.* **2005**, *21*, 68–71.
53. Yadav, H.B.; Yadav, D.K. Construction of Membership Function for Software Metrics. *Procedia Comput. Sci.* **2015**, *46*, 933–940. [CrossRef]
54. Wang, X.L. The Measure and Improvement of Fuzzy Decision in Membership Function Determination Method. Ph.D. Thesis, Nanjing University of Aeronautics and Astronautics, Nanjing, China, 2016.
55. Hasuike, T.; Katagiri, H.; Tsubaki, H. An Interactive Algorithm to Construct an Appropriate Nonlinear Membership Function Using Information Theory and Statistical Method. *Procedia Comput. Sci.* **2015**, *61*, 32–37. [CrossRef]
56. Zhang, R.P. Research on Fault Samples Selection and Fault Injection Method for Flight Control Systems. Master's Thesis, Nanjing University of Aeronautics and Astronautics, Nanjing, China, 2017.
57. Eslami, M.; Ghavami, B.; Raji, M.; Mahani, A. A survey on fault injection methods of digital integrated circuits. *Integration* **2020**, *71*, 154–163. [CrossRef]
58. Azimi, S.; Du, B.; Sterpone, L. Evaluation of transient errors in GPGPUs for safety critical applications: An effective simulation-based fault injection environment. *J. Syst. Architect.* **2017**, *75*, 95–106. [CrossRef]
59. Kirbiš, G.; Selčan, D.; Kramberger, I. Software Reliability Validation and Verification Using Fault Injection Techniques on a Fault Tolerant Processor. *IFAC-PapersOnLine* **2015**, *48*, 252–257. [CrossRef]
60. Zhang, R.; Xiao, L.; Li, J.; Cao, X.; Qi, C.; Li, J.; Wang, M. A fast fault injection platform of multiple SEUs for SRAM-based FPGAs. *Microelectron. Reliab.* **2018**, *82*, 147–152. [CrossRef]
61. Kim, M.C.; Seo, J.; Jung, W.; Choi, J.G.; Kang, H.G.; Lee, S.J. Evaluation of effectiveness of fault-tolerant techniques in a digital instrumentation and control system with a fault injection experiment. *Nucl. Eng. Technol.* **2019**, *51*, 692–701. [CrossRef]
62. Xu, G.X. Research of Software-Implemented Fault Injection and Reliability Evaluation Methods in Distributed Real-Time System. Doctoral Thesis, Chongqing University, Chongqing, China, 2011.
63. Steen, R.; Aven, T. A Risk Perspective Suitable for Resilience Engineering. *Saf. Sci.* **2011**, *49*, 292–297. [CrossRef]
64. COSTIND. *GJB 900A-2012, General Requirements for Materiel Safety Program*; COSTIND: Beijing, China, 2012.
65. Tang, K.H.D.; Md Dawal, S.Z.; Olugu, E.U. Integrating fuzzy expert system and scoring system for safety performance evaluation of offshore oil and gas platforms in Malaysia. *J. Loss Prevent. Proc. Ind.* **2018**, *56*, 32–45. [CrossRef]
66. Campagne, C.S.; Roche, P.; Gosselin, F.; Tschanz, L.; Tatoni, T. Expert-based ecosystem services capacity matrices: Dealing with scoring variability. *Ecol. Indic.* **2017**, *79*, 63–72. [CrossRef]
67. Hokstad, P.; Utne, I.B.; Vatn, J. *Risk and Interdependencies in Critical Infrastructures*; Springer: Lund, Sweden, 2012.
68. Tsai, S.B.; Xue, Y.Z. Models for forecasting growth trends in renewable energy. *Renew. Sustain. Energy Rev.* **2017**, *77*, 1069–1078. [CrossRef]
69. Jure, M.; Janez, K.; Tomaz, B. Methodology for Searching Representative Elements. *Appl. Sci.* **2019**, *9*, 3482–3497.
70. Melchers, R.E. On the ALARP Approach to Risk Management. *Reliab. Eng. Syst. Saf.* **2001**, *71*, 201–208. [CrossRef]

71. Martin, C.J.; Whitby, M. Application of ALARP to extremity doses for hospital workers. *J. Radiol. Prot.* **2003**, *23*, 405–421. [CrossRef] [PubMed]
72. Andrew Hopkins. Risk-management and rule-compliance: Decision-making in hazardous industries. *Saf. Sci.* **2011**, *49*, 110–120. [CrossRef]
73. Seminatore, A.A.; Ghelardoni, L.; Ceccarelli, A.; Falai, L.; Schultheis, M.; Malinowsky, B. ALARP (A Railway Automatic Track Warning System Based on Distributed Personal Mobile Terminals). *Procedia Soc. Behav. Sci.* **2012**, *48*, 2081–2090. [CrossRef]
74. Van Coile, R.; Jomaas, G.; Bisby, L. Defining ALARP for fire safety engineering design via the Life Quality Index. *Fire Saf. J.* **2019**, *107*, 1–14. [CrossRef]
75. Sørskår, L.I.K.; Selvik, J.T.; Abrahamsen, E.B. On the use of the vision zero principle and the ALARP principle for production loss in the oil and gas industry. *Reliab. Eng. Syst. Saf.* **2019**, *191*, 106541. [CrossRef]
76. An Institution of Civil Engineers. *Risk Analysis and Management for Projects (RAMP)*; ICE Publishing: London, UK, 2009.
77. Lorenc, A.; Kuźnar, M. An Intelligent System to Predict Risk and Costs of Cargo Thefts in Road Transport. *Int. J. Eng. Technol. Innov.* **2018**, *8*, 284–293.
78. Watkins, C.B. Integrated Modular Avionics: Managing the allocation of shared intersystem resources. In Proceedings of the 2006 IEEE/AIAA 25th Digital Avionics Systems Conference, Portland, OR, USA, 15–18 October 2006; pp. 1–12.
79. Prisaznuk, P.J. Integrated modular avionics. In Proceedings of the IEEE 1992 National Aerospace and Electronics Conference (NAECON 1992), Dayton, OH, USA, USA, 18–22 May 1992; pp. 39–45.
80. *Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations*; Radio Technical Commission for Aeronautics DO-297; RTCA: Washington, DC, USA, 2005.
81. *STANAG 4626, Final Draft of Proposed Standards for Software*; ASAAC, NATO: Brussels, Belgium, 2004.