aerospace

MDPI

Article

Analysis and Evaluation of Fault Propagation Behavior in Integrated Avionics Systems Considering Cascading Failures

Lei Dong [1,2], Bo Peng [1,3], Xi Chen [1,2,*] and Jiachen Liu [1,4]

[1] Key Laboratory of Civil Aircraft Airworthiness Technology, Civil Aviation University of China, Tianjin 300300, China; l-dong@cauc.edu.cn (L.D.); 2022122025@cauc.edu.cn (B.P.); 2021095005@cauc.edu.cn (J.L.)
[2] Science and Technology Innovation Research Institute, Civil Aviation University of China, Tianjin 300300, China
[3] Sino-European Institute of Aviation Engineering, Civil Aviation University of China, Tianjin 300300, China
[4] College of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China
* Correspondence: chen_x@cauc.edu.cn

Abstract: As the synthesis, modularization, and integration of avionics systems increase, the interconnections between systems and equipment within subsystems become increasingly complex, posing risks to the safety and reliability of the integrated avionics system. To address the risk of fault propagation due to functional cascade failures in integrated avionics systems, this paper proposes a discrete dynamic fault propagation analysis method, which was applied to an all-electric braking system to assess its feasibility. First, the architectural features of the Distributed Integrated Modular Avionics system are summarized. Subsequently, the constructed system layer model is described, establishing the function–resource hierarchical architecture. Subsequently, the behavior of cascading failure propagation in discrete dynamic systems is analyzed by integrating the cascading failure analysis method from SAE ARP 4761A and considering the coupling characteristics between system properties and functions comprehensively. This approach facilitates the development of a cascading failure propagation model for DIMA based on discrete dynamic systems. Finally, by using the all-electric braking system under DIMA architecture as a case study, key Core Processing Modules and failure-prone functions are identified. The findings reveal that within this system, CPM2 and CPM6 are particularly susceptible to failure propagation, and the automatic brake function is notably vulnerable. Data show that the system's failure rate escalates markedly after 2×10^4 h of operation. Performing maintenance before reaching this threshold can further mitigate risks. This practice aligns with current international aircraft maintenance time regulations. The method proposed in this paper can be applied early in the allocation of DIMA resources to enhance security and support DIMA design.

Keywords: integrated avionics systems; fault propagation; cascade failure; discrete dynamic systems; aircraft all-electric braking systems

Citation: Dong, L.; Peng, B.; Chen, X.; Liu, J. Analysis and Evaluation of Fault Propagation Behavior in Integrated Avionics Systems Considering Cascading Failures. *Aerospace* **2024**, *11*, 608. https://doi.org/10.3390/aerospace11080608

Academic Editors: Roberto Sabatini and Alessandro Gardi

Received: 11 June 2024
Revised: 13 July 2024
Accepted: 21 July 2024
Published: 25 July 2024

1. Introduction

One of the most significant current developments in avionics system architecture is Distributed Integrated Modular Avionics (DIMA). In contrast to the traditional integrated modular avionics approach, DIMA eschews the design concept of centralizing all computing resources in a single cabinet and instead distributes them across various parts of the aircraft. This approach not only enhances flexibility, but also increases the sophistication of the design. The literature [1,2] reports that the Distributed Integrated Modular Avionics system has been successfully implemented in A380 and B787 aircraft. Additionally, references [3,4] detail the architectural characteristics of DIMA. The open system architecture of DIMA not only provides opportunities for innovation, but has also been advocated by scientific and technological research projects under the EU FP7 [5,6], covering typical

avionics systems such as the braking and power systems. The literature [7–9] details the performance requirements and highlights the current technical limitations of typical avionics systems under the DIMA architecture. It can therefore be concluded that aircraft systems under the DIMA architecture are expected to become the dominant trend in future aircraft system design.

The current approaches to fault propagation analysis for DIMA fall into two categories: manual analysis [10–12] and intelligent diagnostic analysis [13]. In manual analysis, decisions are primarily based on the analyst's experience and subjective judgment, while intelligent diagnostic analysis relies on the monitoring of fault information and the training of fault models. This automation enhances the analysis and assessment of fault propagation behavior. Wu Yuqian and colleagues [14] highlight that avionics functional integration often presents cascading failure challenges in typical avionics systems. Consequently, the high degree of coupling between the Core Processing Modules (CPM) in DIMA architecture must be considered, underscoring the importance of establishing a cascading failure propagation model. Cascading failures [15,16], which occur due to positive feedback loops and escalate over time, typically initiate with the failure of a single node or subsystem. The failure of a single node leads to load redistribution to the remaining nodes, thereby increasing the likelihood of further system failures. This can lead to a vicious cycle, often described as a snowball effect. The process of analyzing cascade failures is outlined in SAE ARP 4761A. It begins by determining the initial conditions, continues by delineating the cascade's range of influence, and concludes with an analysis of the outcomes. Motter et al. [17] proposed a dynamic model for describing cascade failures, now widely used in complex network robustness analysis. Zheng et al. [18–20] developed a cascade failure model by incorporating the congestion effect, which assesses node load in a congested complex system and elucidates the cascading relationships among nodes. Zheng Jianfeng [21] utilized statistical physics, operations research, and computer simulations to explore traffic distribution, congestion, and cascading failure behaviors in typical complex networks, focusing on a discrete time and state. It is proposed that the time scales of cascading failures be considered in studies of typical complex network systems. Xiang Chenyang [22] applied Floyd's algorithm to analyze system coupling correlations and established a structural model of fault propagation for an all-electric brake system. Based on this, the probability of fault path propagation and the system edge median were combined to develop a model that quantifies the system's fault propagation intensity and identifies the most critical fault propagation path.

However, studies addressing the impact of cascading failures on avionics systems from a discrete time dynamic perspective are lacking. Event-based modeling of discrete systems effectively captures the dynamics of fault occurrence and propagation, offering a more natural and accurate description of fault behavior. In discrete systems, state changes typically occur at specific, discrete intervals, aligning closely with the characteristics of fault propagation. This suggests that fault occurrences and their effects are sudden and well-defined, as opposed to being gradual and continuous. Consequently, discrete systems are more apt for describing and analyzing fault propagation behaviors compared to continuous systems. However, it is essential that avionics systems are analyzed on a time scale due to their dynamic nature.

In light of the aforementioned circumstances, we proposed the development of a cascade failure propagation model based on a discrete time dynamic system. This model will facilitate the study of failure propagation behavior in aircraft avionics systems under the DIMA architecture. The model development will adhere to the cascade failure analysis method described in SAE ARP 4761A. The fundamental concept involves utilizing the conditional failure probability between modules to depict the cascade relationship among DIMA modules. The probability that a DIMA module is in a failure state at a specific point in time is considered a state variable of the discrete dynamic system.

The rest of this paper is organized as follows. Section 2 establishes the hierarchical architecture of DIMA. Section 3 constructs a cascade failure propagation model using a

discrete time dynamic system. Section 4 validates the proposed method via an illustrative analysis of an aircraft's all-electric brake system. Section 5 analyzes and discusses the experimental data and proposes a method for improvement. Section 6 summarizes this paper.

2. DIMA Hierarchical Architecture Construction and Cascade Effect Analysis

2.1. DIMA's Layered Architecture

DIMA represents the latest advancement in modern avionics system architecture. It is designed for enhanced flexibility compared to traditional modular avionics systems, emphasizing the versatility, extensibility, and adaptability of system modules. In this open system architecture, functions from aircraft electromechanical, avionics, and other systems increasingly integrate and intersect. For avionics systems with stringent real-time requirements, achieving low-latency, low-jitter, and deterministic data transmission is essential, while also considering functional implementation. The adoption of DIMA technology provides robust computational support to enhance the real-time performance of avionics systems. Based on this, the layered architecture of DIMA is outlined in Figure 1, reflecting its distinctive architectural features.

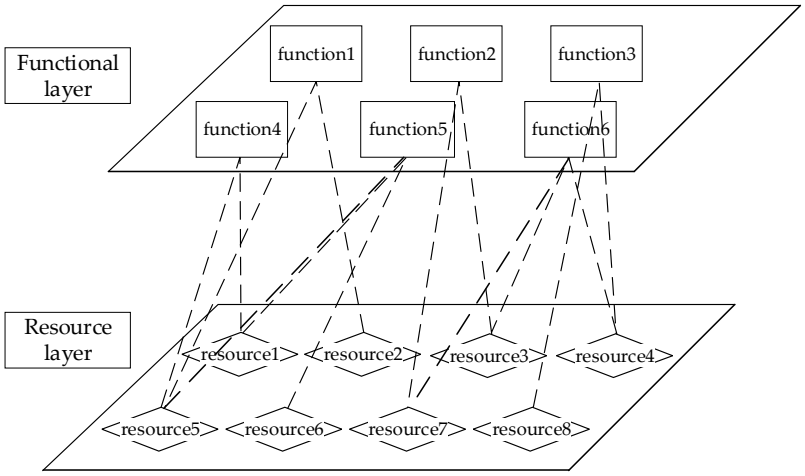

Figure 1. Layered architecture of DIMA.

In the context of distributed and integrated avionics systems, a layered architectural design is employed, which includes the system's functional and resource layers. From this architectural perspective, the functional layer consists of related subsystem functions, serving to simplify the system. In contrast, the resource layer utilizes its robust public computing resources to ensure the rapid loading of control algorithms and the output of control commands. Resource scheduling is based on mapping rules and activities linking the functional and resource layers. This primarily involves the correspondence between functions and resources, as well as between signals and links.

a. Functional Layer

The system design should serve as a starting point, referring to the design criteria of a typical avionics system [23,24], which involves requirements for resources, interfaces, performance, and security. Based on the characteristics of the DIMA platform, the core functions of a typical avionics system need to be structured. Furthermore, the correspondence between the functional and resource layers refines the core functions and guides the analysis of future interactions within avionics systems at the resource layer.

b. Resource Layer

To realize the above functions, core processing modules in the resource layer must be employed to provide the necessary computational power for functional algorithms or the

control cycles of a typical avionics system. These processing modules deploy functionality as required by the application. To facilitate hierarchical modeling and correlation analysis in avionics systems, it is recommended that only one functional application is run per region, without spare modules. Furthermore, establishing correspondence between the functional and resource layers requires considering the correlations among different CPMs, as various functions may share the same CPM.

2.2. Avionics System Cascade Effect Analysis Process

The document SAE ARP 4761A emphasizes that cascade effects within and between systems are crucial when analyzing the propagation of failures in aircraft avionics systems. Cascade Effect Analysis (CEA) is a bottom-up qualitative analysis methodology that evaluates an initial condition (e.g., a failure condition, a failure mode, or a combination of failure modes) and captures the overall effect of that initial condition on the aircraft. This involves an iterative process that identifies both the direct and the indirect effects propagated due to system dependencies. All systems, whether directly or indirectly connected to the system affected by the initial condition, are considered. Cascading effects analysis supports any analysis requiring identification of multi-system effects at an aircraft level or for a specific initial condition. The effects of each initial condition are fed back to the source analysis.

Cascade effects analysis is conducted under an initial condition, which may include a failure condition, a failure mode, or a combination of failure modes. Figure 2 provides a summary of the cascade effects analysis steps and their sequence, with the term 'system' replaced by 'device' or 'module' in each activity to adapt to lower-level activities.

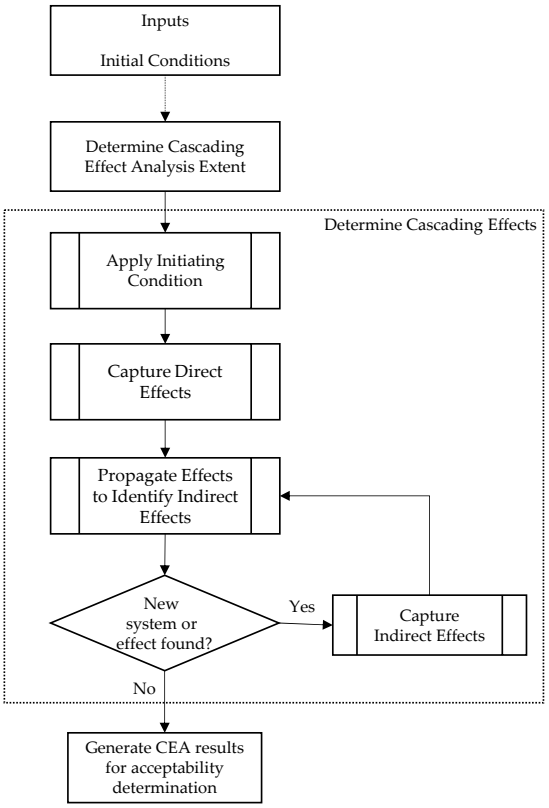

Figure 2. Steps in analyzing cascade effects.

Once the system architecture and initial conditions are established, the scope of cascading failures is initially determined. The sphere of influence is determined by identifying systems either directly affected by, or indirectly connected through, the initial condition. This step focuses on identifying and documenting the interaction pathways between initial and potential system interfaces. The cascading effects of the aircraft are identified through

an iterative process, culminating in the output of the cascading effects analysis results. The output should include the initial conditions, the range of analyzed effects, a list of systems associated with the initial conditions and their effects, and the assumptions used in the analysis, each tailored to the specific cascade effect.

3. Cascading Failure Propagation Modelling for DIMA

3.1. DIMA Network Topology

Understanding the role of network topology [25,26] significantly facilitates the study of complex system problems. In the DIMA model, a network topology graph represents the cascade relationships within the avionics system. The graph consists of nodes and directed edges. Nodes represent the system's constituent modules, and directed edges depict the cascade relationships between these nodes. The overall performance of an avionics system depends on the operational status of each module. System performance can be described, analyzed, and evaluated across multiple dimensions. Among these dimensions, the network connectivity index is commonly used to gauge the system's overall performance. This index reflects the system's connectivity. Within the proposed modeling framework, this index can be replaced with other performance indicators to assess various system dimensions [27]. Depending on the nature of the dependencies between modules, various relational networks can be formed [28], including star, ring, bus, tree, mesh, and hybrid structures, as shown in Figure 3.

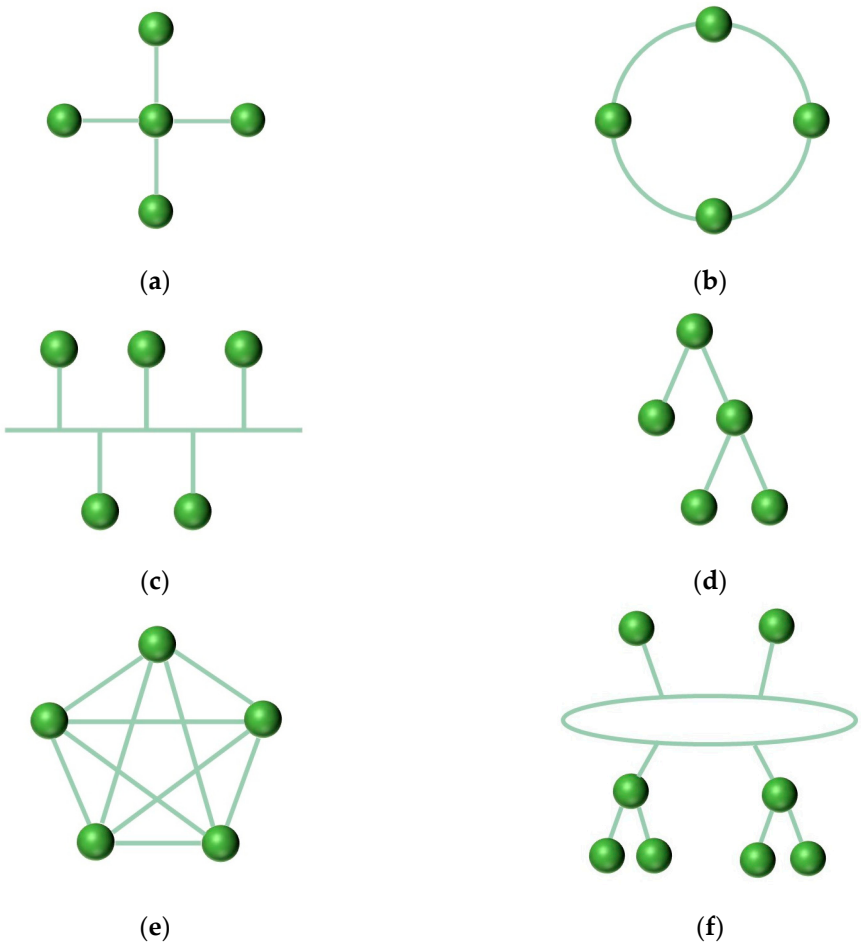

Figure 3. Network topology. (**a**) Star topology; (**b**) ring topology; (**c**) bus topology; (**d**) tree topology; (**e**) mesh topology; (**f**) hybrid topology.

Most network topologies in DIMA are mesh structures. Concurrently, the network topology method quantitatively characterizes the association strength between two sys-

tem modules based on failure condition probabilities, easily integrating with module failure probabilities.

3.2. Failure Analysis of DIMA Module Based on Discrete Dynamic System

DIMA involves the evolution of certain quantities over time, where the state of the system evolves in discrete time steps, i.e., discrete dynamic systems. These quantities are referred to as state variables. When modelling DIMA as a discrete dynamic system, a set of sequences of system states over time can be determined. The state changes of the system conform to certain rules, which enable future states to be determined from a given initial state. A scalar between 0 and 1 is employed as the state variable of the system, which represents the probability that the module x will be in a faulty state at a given point in time.

The probability in question may be defined as the state variable $x(t)$ of a system node, where $t \in T$ and T denotes a discrete time set.

For the sake of convenience, the setting of $T = 0, 1, 2, \cdots$ in the model can be accomplished through the use of different time scales, contingent upon the specific requirements of the model in question. When there are n nodes $x_1, x_2, \cdots, x_n$ in the system, the state variable of the system is recorded as $X(t)$ at time t, where $X(t) = (x_1(t), x_2(t), \cdots\cdots, x_n(t))^{\mathrm{T}}$, $t \in T$.

In light of the aforementioned definition, the approximate model of the DIMA discrete time dynamic system can be described as follows:

$$\begin{cases} X(t+1) = f(X(t), t) \\ t = 0, 1, 2, \cdots\cdots \end{cases}, \tag{1}$$

where $X(0)$ is the initial setting and f is a nonlinear mapping.

At a defined time t, the events at node $x_i \in \{x_1, x_2, \cdots\cdots, x_n\}$ in the system can be classified into the following types: failure events $F_{x_i}(t)$, direct failure events $D_{x_i}(t)$, cascading failure events $C_{x_i}(t)$, and cascading failure events $C_{x_i}^{x_j}$ due to the failure of node x_j. For a failure event $F_{x_i}(t)$, the union of two failure events, $D_{x_i}(t)$ and $C_{x_i}(t)$, is considered. The cause of direct failure event $D_{x_i}(t)$ is mainly the failure of a system node due to causal factors. Furthermore, the cascade failure event C_{x_i} is a concatenation of the cascade failure sub-events $C_{x_i}^{x_j}$. The cascade failure sub-event $C_{x_i}^{x_j}$ is a failure of the upstream node x_j, which leads to a cascade failure of node x_i. The mechanism and probability of cascade failure events are discussed in the following sections. Consequently, the probability of $F_{x_i}(t)$ occurring can be expressed as:

$$P(F_{x_i}(t)) = P(D_{x_i}(t) \cup C_{x_i}(t)),\ t = 0, 1, 2, \cdots. \tag{2}$$

As events $D_{x_i}(t)$ and $C_{x_i}(t)$ are independent of one another, they can be obtained.

$$P(F_{x_i}(t)) = P(D_{x_i}(t)) + P(C_{x_i}(t)) - P(D_{x_i}(t))P(C_{x_i}(t)),\ t = 1, 2, 3, \cdots. \tag{3}$$

In accordance with the definition of the state variables of the system presented in the preceding section, it can be demonstrated that

$$x_i(t) = P(F_{x_i}(t)). \tag{4}$$

Subsequently, if only DIMA is deemed to have failed at the initial stage, then $P(D_{x_i}(t)) = 0, t = 1, 2, 3, \cdots$. Furthermore, it can be demonstrated that

$$P(F_{x_i}(t)) = P(C_{x_i}(t)), t = 1, 2, 3, \cdots. \tag{5}$$

3.3. Construction of DIMA Cascade Failure Propagation Model Based on Discrete Dynamic System

In order to construct a DIMA cascading failure propagation model $X(t)$ based on discrete dynamical systems, it is necessary to assess and determine the probability $P(D_{x_i}(t))$

of direct failure of module x_i in DIMA at a given point in time. This is done by considering the type of failure and the type of facility.

In the event that a single node x_j is associated with x_i, the probability of node failure due to cascade is $P(C_{x_i}(t+1))$. The following equation is therefore valid:

$$P(C_{x_i}(t+1)) = P(C_{x_i}^{x_j}|F_{x_j})P(F_{x_j}(t)), \tag{6}$$

where $P(F_{x_j}(t))$ denotes the probability that node x_j associated with node x_i fails at moment t. C_{x_i} denotes the cascading failure event at node x_i, and $C_{x_i}^{x_j}$ denotes the cascading failure event at node x_i due to node x_j. Given that x_j is the only node associated with x_i, the following relationships are to be established:

$$C_{x_i} = C_{x_i}^{x_j} \text{ and } P(C_{x_i}|F_{x_j}) = P(C_{x_i}^{x_j}|F_{x_j})$$

where $P(C_{x_i}^{x_j}|F_{x_j})$ denotes the association between nodes x_i and x_j. The cascade failure event $C_{x_i}^{x_j}$ of node x_i is initiated by the failure F_{x_j} of node x_j.

In the event that multiple nodes within a network are associated with node x_i, for example, nodes x_j and x_k collectively influence node x_i, the following applies:

$$C_{x_i} = C_{x_i}^{x_j} \cup C_{x_i}^{x_k}, \tag{7}$$

where $C_{x_i}^{x_j}$ denotes a cascading failure event of node x_i due to node x_j and $C_{x_i}^{x_k}$ denotes a cascading failure event of node x_i due to node x_k.The failure of node x_j occurs subsequent to the event $C_{x_i}^{x_j}$, which disables node x_i. Concurrently, the failure of node x_k occurs at the same time as event $C_{x_i}^{x_k}$, which also disables node x_i. In other words, whenever one of node x_j and node x_k fails, node x_i is affected. Therefore, it can be obtained:

$$P(C_{x_i}) = P(C_{x_i}^{x_j}) + P(C_{x_i}^{x_k}) - P(C_{x_i}^{x_j})P(C_{x_i}^{x_k}) = 1 - (1 - P(C_{x_i}^{x_j}))(1 - P(C_{x_i}^{x_k})). \tag{8}$$

In consideration of the values of $P(C_{x_i}^{x_j}) = P(C_{x_i}^{x_j}|F_{x_j})P(F_{x_j})$ and $P(C_{x_i}^{x_k}) = P(C_{x_i}^{x_k}|F_{x_k})$ $P(F_{x_k})$, and the occurrence of state transfer at discrete time t, the probability of cascade failure for node x_i is as follows:

$$P(C_{x_i}(t+1)) = 1 - (1 - P(C_{x_i}^{x_j}|F_{x_j})P(F_{x_j}(t)))(1 - P(C_{x_i}^{x_k}|F_{x_k})P(F_{x_k}(t))). \tag{9}$$

In a similar manner, if there are m nodes $\{x_1, x_2, \cdots\cdots, x_m\}$ associated with node x_i,

$$C_{x_i} = \bigcup_{j=1}^{m} C_{x_i}^{x_j}, \tag{10}$$

$$P(C_{x_i}(t+1)) = 1 - \prod_{j=1}^{m} (1 - P(C_{x_i}^{x_j}|F_{x_j})P(F_{x_j}(t))). \tag{11}$$

For any node x_j connected to x_i, the conditional probability of failure $P(C_{x_i}^{x_j}|F_{x_j})$ indicates that the cascading failure event $C_{x_i}^{x_j}$ of node x_i is triggered by the failure F_{x_j} of node x_j. The conditional probability of failure $P(C_{x_i}^{x_j}|F_{x_j})$ is known to have a value between 0 and 1. The closer the value of $P(C_{x_i}^{x_j}|F_{x_j})$ is to 1, the stronger the correlation between the nodes. This implies that the failure of the upstream node is more likely to be transmitted to the associated node x_i, which will result in the failure of the associated node x_i. When $P(C_{x_i}^{x_j}|F_{x_j}) = 1$, it signifies that the two nodes are fully correlated, and the failure of the upstream node x_j will lead to the failure of the downstream associated node x_i. Conversely, when $P(C_{x_i}^{x_j}|F_{x_j}) = 0$, it indicates that both parties are uncorrelated and independent of

each other. The conditional probability of failure, denoted by $P(C_{x_i}^{x_j}|F_{x_j})$, represents the strength of association between two nodes, x_i and x_j.

The actual operational scenarios of DIMA may be more complex; for instance, $P(C_{x_i}^{x_j}|F_{x_j})$ may vary with time or events. However, the objective of this paper is to propose a generalized model to study the risk propagation of DIMA cascade failures and to address the issues mentioned earlier. Therefore, the focus of this paper does not involve the determination of conditional probabilities. For the purposes of this paper, it is convenient to set the conditional failure probability as a known fixed value that does not vary with time. This is consistent with the majority of international studies [29,30]. The conditional probability of failure between DIMA modules can then be calculated based on the correlation relationship between the modules and the strength of the correlation. To illustrate, consider a system comprising n nodes, where nodes x_i and x_j are linked. The probability that the failure of node x_j leads to the failure of node x_i is denoted by $P(C_{x_i}^{x_j}|F_{x_j})$. This probability may be abbreviated as follows:

$$p_{ij} = P(C_{x_i}^{x_j}|F_{x_j}). \tag{12}$$

This yields p_{ij}, which characterizes the effect of node x_j on node x_i in terms of probabilities. If a system has n nodes, there are n^2 associations, i.e., there are n^2 conditional probabilities. Consequently, a $n \times n$ cascade matrix, $\boldsymbol{P}_M = (p_{ij})_{n\times n}$, can be obtained as follows:

$$\boldsymbol{P}_M = (p_{ij})_{n\times n} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & \vdots & & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{bmatrix}. \tag{13}$$

If DIMA contains n modules at a given moment t, the state variables of its discrete dynamical system correspond to $X(t) = (x_1(t), x_2(t), \cdots, x_n(t))^{\mathrm{T}}$. At the subsequent moment $t+1$, the propagation of faults is considered, but the occurrence of direct fault events is not taken into account. The nonlinear mapping $f(X(t))$ is as follows:

$$\begin{aligned} f(X(t)) &= f\begin{pmatrix} x_1(t) \\ x_2(t) \\ \vdots \\ x_n(t) \end{pmatrix} \\ &= \begin{pmatrix} 1-\prod_{j=1}^{n}(1-p_{1j}x_j(t)) \\ 1-\prod_{j=1}^{n}(1-p_{2j}x_j(t)) \\ \vdots \\ 1-\prod_{j=1}^{n}(1-p_{nj}x_j(t)) \end{pmatrix} \\ &= \begin{pmatrix} x_1(t+1) \\ x_2(t+1) \\ \vdots \\ x_n(t+1) \end{pmatrix} \\ &= X(t+1), t = 0, 1, \cdots \end{aligned} \tag{14}$$

where $X(0)$ is the initial value of the system state variable. In order to simulate the failure modes of DIMA, it is possible to set different initial values according to the type of failure in question. Similarly, when evaluating the module cascade characteristics, the initial values can be changed as needed. In conclusion, the DIMA cascade failure propagation model based on a discrete dynamic system has been established.

4. Validation of Cascade Failure Propagation Models for All-Electric Brake Systems under DIMA Architecture

The mapping relationship between the all-electric brake system and the resource layer is detailed based on the existing model of the all-electric brake system under the DIMA architecture [31], as illustrated in Table 1.

Table 1. Function-resource mapping relationship of all-electric brake system.

Functional Layer	CPM1	CPM2	CPM3	CPM4	CPM5	CPM6	CPM7	CPM8	CPM9
Information Display								√	√
Crew alarm					√	√	√		
Automatic braking	√	√	√			√			
Manual brake	√	√		√					
Ground stop brakes		√		√					
Air braking		√							√

The function–resource mapping relationship of the all-electric brake system, detailed in Table 1, facilitates the derivation of the network topology diagram, as illustrated in Figure 4. The system model includes nine CPM modules and thirteen directed edges, where the cascade relationships between CPMs are represented by these edges. In the figure, straight lines represent bidirectional edges. For interrelated modules x_i and x_j, the probability of module x_i failure caused by module x_j failure is $P(C_{x_i}^{x_j}|F_{x_j})$. Based on the aforementioned assumptions, the conditional probability $P(C_{x_i}^{x_j}|F_{x_j})$ of a cascade failure between CPMs is set to

$$P(C_{x_i}^{x_j}|F_{x_j}) = P_0 = \frac{1}{N}, \tag{15}$$

where N denotes the number of directed edges in the fault model. In order to facilitate the numerical calculation, P_0 is set to $1/N$, in order to make the results more intuitive. Meanwhile, the average failure probability of each CPM of the system at a certain moment T_n is defined as the failure risk of the all-electric brake system. This can be reasonably assumed to be $T_{n+1} - T_n = 10^3$ h under the actual operating conditions of the all-electric brake system, as stated in the paper [32].

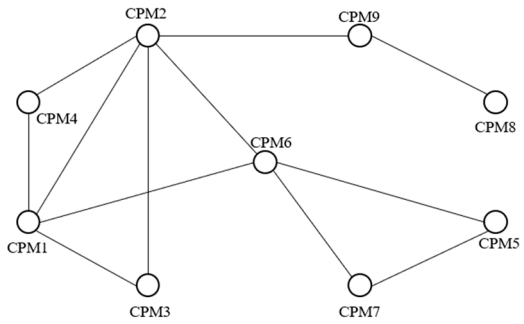

Figure 4. Topology of an all-electric brake system.

In this context, the probability of failure of the all-electric brake system $M_G(t)$ can be expressed as

$$M_G(t) = \frac{\sum_{i=1}^{N} P(F_{x_i}(t))}{N}. \tag{16}$$

Subsequently, the failure probability $P(F_{x_i}(t))$ of each CPM in the aforementioned equation is weighted according to its importance. Alternatively, a new performance evaluation function based on failure probability may be proposed. However, evaluating the performance of the all-electric brake system is not the focus of this study. Therefore, the failure modeling of the all-electric brake system utilizes the two aforementioned metrics to

approximately describe the changes in overall system performance. Two types of failure modes are considered. The first is an initial CPM failure, which leads to the system module being affected by cascading failures but not by direct external failure events. This is represented by

$$P(D_i(t)) = 0,\ t = 1, 2, \cdots. \tag{17}$$

Failure mode 2 is characterized by the continued impact of an external direct fault event on the all-electric brake system following the cascading failure propagation, which is represented by the following parameter:

$$P(D_i(t)) > 0,\ t \geq 1. \tag{18}$$

To identify the cascading fault propagation capabilities of each CPM in an all-electric brake system, only fault mode 1 was considered. It was assumed that, under the initial fault event, only one CPM would fail while the other CPMs would remain operational. A series of numerical experiments were conducted for each CPM, with the aim of recording the system's state changes over the first 5×10^4 h. The initial fault occurrence in CPM1 served as a case study to document the state variables of the all-electric brake system at various times.

When $T = 0$, it is known that

$$P(F_1(0)) = P(D_1(0)) = 1. \tag{19}$$

That is to say, CPM1 fails at the initial moment, and in the following time, no external direct failure event D_i occurs in the system, and it is affected only by the cascading failure event C_i. Therefore, $P(F_i(t)) = P(C_i(t))$, $t \geq 1$. Transitioning from the initial to the subsequent moment, as illustrated in Figure 4, it becomes evident that the risk of failure in CPM1 is transferred to CPM2, CPM3, CPM4, and CPM6. To illustrate this point, consider CPM2; from Equations (10) and (6), it is evident that

$$\begin{aligned} P(F_2(1)) &= P(C_2(1)) \\ &= P(C_2^1(1) \cup C_2^3(1) \cup C_2^4(1) \cup C_2^6(1) \cup C_2^9(1)) \\ &= P(C_2^1(1)) \\ &= P(C_2^1|F_1)P(F_1(0)) \\ &= \frac{1}{13} \times 1 \\ &= 0.077 \end{aligned} \quad . \tag{20}$$

Consequently, the probability of failure for each CPM at various moments can be calculated. Currently, the international standard requires aircraft maintenance after 24,000 flight hours. Therefore, to ensure comprehensive fault analysis, the simulation period should exceed this duration. Accordingly, we selected 50,000 flight hours for our simulation research. As illustrated in Figure 5, the cascade failure propagation model for the all-electric brake system under the DIMA architecture is displayed, covering 5×10^4 h of operation starting from the initial failure of CPM1. In the figure, the color of each CPM changes according to the probability of failure. The color shifts from blue to red, signifying a change in the failure probability of a CPM from 0 to 1. Table 2 lists the specific values of the system state variables at ten-moment intervals under the initial failure state of the CPM1 node. As shown in the accompanying image and table data, the state variable of CPM1 consistently equals 1, indicating a complete failure, consistent with the initial failure condition of CPM1. The failure probabilities of CPM2, CPM3, CPM4, and CPM6, directly linked to CPM1, increase more rapidly than that of CPM8, which has a weaker connection to CPM1.

The following section details the cascade failure propagation model of the all-electric braking system under DIMA architecture over a 5×10^4 h operation period, starting with an initial failure in module 6, as depicted in Figure 6. Table 3 lists the specific values of

the system state variables at each of the ten moments following the initial failure of the CPM6 node. As shown in the accompanying image and table data, the state variable of CPM6 consistently registers as 1, indicating a complete failure, consistent with the initial condition. Similarly, this failure probability affects CPM1, CPM2, CPM5, and CPM7, which are directly linked to CPM6. The failure probabilities of CPM3 and CPM4 increase more rapidly due to their direct links to CPM1 and CPM2. Consequently, the failure probabilities of systems indirectly associated with CPM6 and CPM4 escalate more quickly. Additionally, the high indirect correlation with CPM6 leads to a faster increase in its failure rate over time. In contrast, CPM8, with its weaker correlation to CPM1, exhibits a slower increase in failure probability.

Subsequently, using Equation (14), the initial moment of failure was simulated for each of the nine CPMs, with system state changes recorded over a 5×10^4 h period. As shown in Figure 7, the curves depict how the probability of failure for the system's CPMs increases over time. Subsequently, using Equation (16), the failure risk of the all-electric brake system, denoted as $M_G(t)$, can be calculated.

Figure 8 illustrates the risk of failure of the all-electric brake system under different initial conditions. As can be seen from the figure, the fault risk $M_G(t)$ grows most rapidly at the initial failure of CPM2, followed by the initial failure of CPM6. In contrast, the risk of failure $M_G(t)$ grows most slowly when CPM8 has an initial failure.

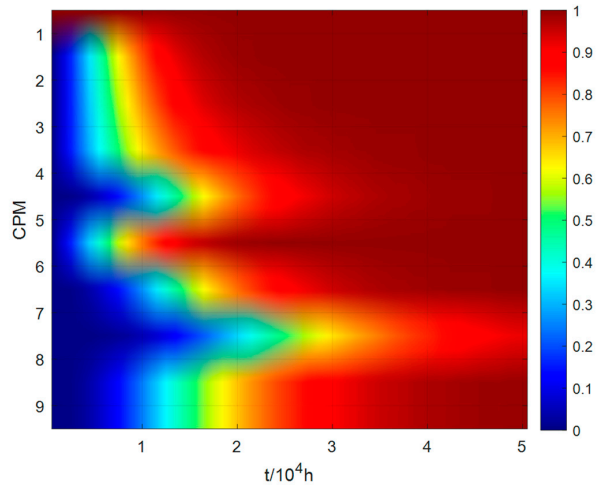

Figure 5. State diagram of all-electric brake system CPM1 at initial failure.

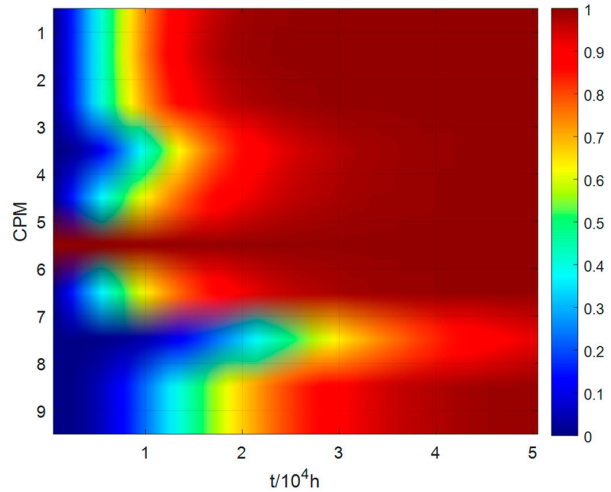

Figure 6. State diagram of the all-electric brake system CPM6 at initial failure.

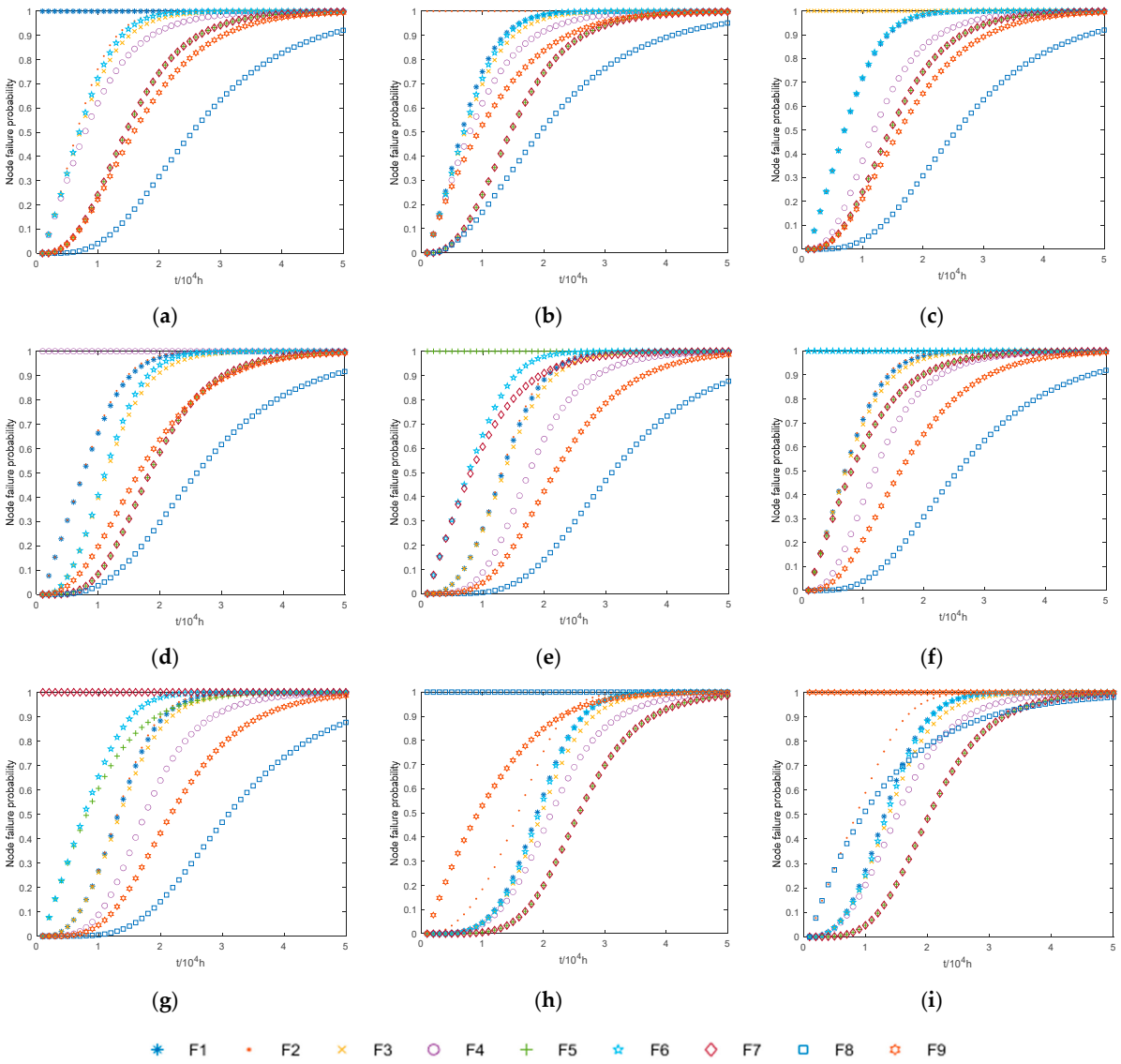

Figure 7. CPM failure rate of all-electric brake system under different initial condition. (**a**) CPM1 initial fault; (**b**) CPM2 initial fault; (**c**) CPM3 initial fault; (**d**) CPM4 initial fault; (**e**) CPM5 initial fault; (**f**) CPM6 initial fault; (**g**) CPM7 initial fault; (**h**) CPM8 initial fault; (**i**) CPM9 initial fault.

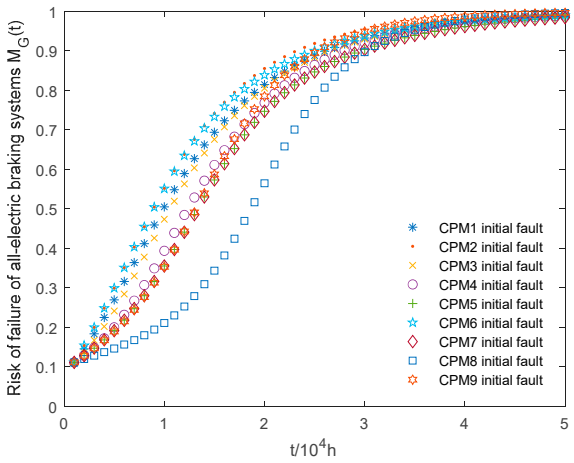

Figure 8. Failure risk of the all-electric brake system under different initial faults.

Table 2. State variable of the all-electric brake system under initial failure condition of node 1.

Module	$X(t = 0)$	$X(t = 10^4$ h)	$X(t = 2 \times 10^4$ h)	$X(t = 3 \times 10^4$ h)	$X(t = 4 \times 10^4$ h)	$X(t = 5 \times 10^4$ h)
CPM1	1.000	1.000	1.000	1.000	1.000	1.000
CPM2	0.000	0.760	0.990	0.999	1.000	1.000
CPM3	0.000	0.698	0.968	0.997	1.000	1.000
CPM4	0.000	0.620	0.917	0.983	0.997	0.999
CPM5	0.000	0.240	0.745	0.942	0.988	0.998
CPM6	0.000	0.722	0.986	0.999	1.000	1.000
CPM7	0.000	0.240	0.745	0.942	0.988	0.998
CPM8	0.000	0.040	0.317	0.634	0.827	0.921
CPM9	0.000	0.222	0.664	0.895	0.974	0.994

Table 3. State variable of the all-electric brake system under initial failure condition of node 6.

Module	$X(t = 0)$	$X(t = 10^4$ h)	$X(t = 2 \times 10^4$ h)	$X(t = 3 \times 10^4$ h)	$X(t = 4 \times 10^4$ h)	$X(t = 5 \times 10^4$ h)
CPM1	0.000	0.714	0.981	0.999	1.000	1.000
CPM2	0.000	0.725	0.986	0.999	1.000	1.000
CPM3	0.000	0.694	0.967	0.997	0.999	1.000
CPM4	0.000	0.370	0.847	0.969	0.994	0.999
CPM5	0.000	0.603	0.903	0.979	0.996	0.999
CPM6	1.000	1.000	1.000	1.000	1.000	1.000
CPM7	0.000	0.603	0.903	0.980	0.996	0.999
CPM8	0.000	0.038	0.308	0.626	0.823	0.919
CPM9	0.000	0.211	0.653	0.891	0.972	0.994

5. Discussion

In the all-electric brake system, it was observed that CPM2 and CPM6 have the highest risk of fault propagation, whereas CPM8 has the lowest. The uncertainty associated with CPM2 and CPM6 is higher, and their failures significantly impact the system. According to Table 1, CPM2 and CPM6 are mapped to the automatic brake function within the functional layer of the all-electric brake system. Consequently, this mapping results in a higher probability of failure for the automatic brake function in the actual system. Therefore, enhancing the safety and reliability of the automatic brake function to the greatest extent is imperative in the design of the all-electric brake system. This enhancement can be achieved by implementing multimode redundancy for CPM2 and CPM6, along with conducting common cause and mode analyses. An analysis of Figure 8 indicates that the failure risk of the aircraft's all-electric braking system escalates notably when the flight duration approaches 2×10^4 h. Therefore, it is essential to inspect and maintain this system prior to reaching this flight duration to ensure the aircraft's safe operation. These measures effectively reduce the failure probability of the all-electric brake system, thereby enhancing civil aircraft safety.

6. Conclusions and Future Works

This paper integrates the architectural features of an avionics system under the DIMA architecture to construct a hierarchical model from the system's function and resource layers. This model establishes a function–resource hierarchy that lays the foundation for analyzing the impact of failure propagation. A general model was proposed to examine the risk propagation in DIMA cascade failures, utilizing the cascading failure analysis method from SAE ARP 4761A to study fault propagation in discrete dynamic systems. DIMA module failure events were defined, with conditional probabilities of inter-node failures used to depict cascade relationships. A cascade failure propagation model was constructed for avionics systems under the DIMA architecture using discrete dynamic systems to represent cascade relationships over time. The state variables of the all-electric brake system under the DIMA architecture were calculated following the initial failure of each CPM module, and subsequently, the failure risk under various initial conditions was assessed. Key nodes of failure propagation and system vulnerability were identified in the all-electric brake system, and the validity and accuracy of the proposed method were confirmed. This study

confirmed that within the system, CPM2 and CPM6 are particularly vulnerable to failure propagation, and the automatic brake function exhibits notable susceptibility. Analysis indicates that the system's failure rate increases significantly after two hours of operation, underscoring the necessity of maintenance prior to this threshold to reduce risks. This maintenance strategy is in line with current international aircraft maintenance regulations, affirming its relevance and applicability. Furthermore, the method developed in this paper can apply in the early stages of DIMA resource allocation, thereby enhancing security and aiding in the design of DIMA systems. These findings not only validate the proposed method, but also suggest its potential for broader application in similar contexts.

With the continuous development of avionics systems, the architecture is evolving from a purely integrated framework to a hybrid architecture that combines both integrated and federate architectures. In the future, this method should be refined to suit avionics systems within such a hybrid architecture.

Author Contributions: Conceptualization, L.D. and B.P.; methodology, B.P. and J.L.; software, B.P.; validation, L.D., B.P. and X.C.; formal analysis, X.C.; investigation, B.P.; resources, J.L.; data curation, X.C.; writing—original draft preparation, B.P.; writing—review and editing, B.P.; visualization, L.D.; supervision, X.C.; project administration, L.D.; funding acquisition, L.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key Research and Development Program of China Grant 2021YFB1600602, the Fundamental Research Funds for the Central Universities under Grant 3122022044 and the Fundamental Research Funds for the Central Universities under Grant 3122024037.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Xuan, Z.; Xiong, H.; Feng, H. Hybrid partition-and network-level scheduling design for distributed integrated modular avionics systems. *Chin. J. Aeronaut.* **2020**, *33*, 308–323.
2. Zhang, W.; Liu, J.; Cheng, L.; Filho, R.S.; Gao, F. A survey of optimal hardware and software mapping for distributed integrated modular avionics systems. *Appl. Sci.* **2020**, *10*, 2675. [CrossRef]
3. Wang, G.; Gu, Q.; Wang, M.; Zhang, L. Research on new generation integrated avionics system architecture technology. *J. Aeronaut.* **2014**, *35*, 1473–1486.
4. Chu, J.; Zhao, T.; Jiao, J.; Chen, Z. Optimal design of configuration scheme for integrated modular avionics systems with functional redundancy requirements. *IEEE Syst. J.* **2020**, *15*, 2665–2676. [CrossRef]
5. Fuchsen, R. IMA NextGen: A new technology for the Scarlett program. *IEEE Aerosp. Electron. Syst. Mag.* **2010**, *10*, 10–16. [CrossRef]
6. Yan, F.; Xing, P.; Zhao, C.; Wang, P. Reliability modelling and analysis of DIMA systems based on the joint k/n (G) model. *J. Aeronaut.* **2018**, *39*, 185–193.
7. Bernard, S.; Garcia, J.-P. *Braking Systems with New IMA Generation*; SAE International: Warrendale, PA, USA, 2011.
8. He, Y.; Liu, Y.; Zhao, Y.; He, W. Research on aircraft brake control architecture based on new generation modular avionics system. *Aircr. Des.* **2015**, *35*, 41–45.
9. Bennett, J.; Mecrow, B.; Atkinson, D.; Atkinson, G. Safety-critical design of electromechanical actuation systems in commercial aircraft. *IET Electr. Power Appl.* **2011**, *5*, 37–47. [CrossRef]
10. Qiao, G.; Liu, G.; Shi, Z.; Wang, Y.; Ma, S.; Lim, T.C. A review of electromechanical actuators for More/All Electric aircraft systems. *Proc. Inst. Mech. Eng. Part C J. Eng. Mech. Eng. Sci.* **2018**, *232*, 4128–4151. [CrossRef]
11. Wang, Z.; Li, Z.; Li, W. Research of Aircraft Electric Brake Control System. In Proceedings of the 3rd International Symposium on Mechatronics and Industrial Informatics (ISMII 2017), Haikou, China, 27–29 October 2017; pp. 198–200.
12. SAE. *Information on Electric Brakes: SAE AIR5937*; SAE International: Warrendale, PA, USA, 2019.
13. Xiang, L.; Ma, R. Power-on self-test of aircraft electromechanical actuation systems with all-electric brakes. *J. Aeronaut.* **2016**, *37*, 3832–3842.
14. Wu, Y.; Xiao, G.; Wang, M. Cascading failure analysis method of avionics based on operational process state. *IEEE Access* **2020**, *8*, 148425–148444. [CrossRef]
15. Lei, W. Study on Robust Enhancement Strategy for Complex Networks with Adjustable Weights under Cascading Faults. Master's Thesis, Central South University, Changsha, China, 2022.

16. Jin, Y.; Zhang, Q.; Chen, Y.; Lu, Z.; Zu, T. Cascading failures modeling of electronic circuits with degradation using impedance network. *Reliab. Eng. Syst. Saf.* **2023**, *233*, 109101. [CrossRef]
17. Zheng, J.-F.; Yang, L.-X.; Gao, Z.-Y.; Fu, B.-B. Cascading failures in congested scale-free networks. *Int. J. Mod. Phys. C* **2010**, *21*, 991–999. [CrossRef]
18. Wu, Y.; Yao, K.; Su, W. Dirichlet problem of Poisson's equation on SG-4. *Chin. Ann. Math.* **2019**, *40*, 27–34.
19. Wu, Y.; Yao, K.; Zhang, X. The Hadamard fractional calculus of a fractal function. *Fractals* **2018**, *26*, 1850025. [CrossRef]
20. Wang, J.-W.; Rong, L.-L. Vulnerability of effective attack on edges in scale-free networks due to cascading failures. *Int. J. Mod. Phys. C* **2009**, *20*, 1291–1298. [CrossRef]
21. Zheng, J. Modeling of Complex Networks and Study of Dynamic Processes on Typical Networks. Ph.D. Thesis, Beijing Jiaotong University, Beijing, China, 2010.
22. Xiang, C. Application of Harmony-SE Method in Design and Analysis of All-Electric Brake System. Master's Thesis, Civil Aviation University of China, Tianjin, China, 2021.
23. SAE. *Information on Brake-By-Wire (BBW) Brake Control Systems: SAE AIR5372A*; SAE International: Warrendale, PA, USA, 2019.
24. SAE. *Braking System Dynamics: SAE AIR1064D*; SAE International: Warrendale, PA, USA, 2016.
25. Wu, Y.; Chen, Z.; Zhao, X.; Gong, H.; Su, X.; Chen, Y. Propagation model of cascading failure based on discrete dynamical system. *Reliab. Eng. Syst. Saf.* **2021**, *209*, 107424. [CrossRef]
26. Tudoroiu, A. Study of Different Network Topologies Using Cisco Packet Tracer. *Sci. Bull. Electr. Eng. Fac.* **2023**, *23*, 31–33. [CrossRef]
27. Dueñas-Osorio, L.; Craig, J.I.; Goodno, B.J. Seismic response of critical interdependent networks. *Earthq. Eng. Struct. Dyn.* **2007**, *36*, 285–306. [CrossRef]
28. Santra, S.; Acharjya, P.P. A study and analysis on computer network topology for data communication. *Int. J. Emerg. Technol. Adv. Eng.* **2013**, *3*, 522–525.
29. Deng, J. Research on Requirements Modeling and Validation of Integrated Modular Avionics System. Master's Thesis, Nanjing University of Aeronautics and Astronautics, Nanjing, China, 2017.
30. Xing, P. Dynamic Reconfiguration Strategy and Reliability Model Analysis of Integrated Avionics System. Master's Thesis, Civil Aviation University of China, Tianjin, China, 2019.
31. Yan, F.; Xiang, C.; Dong, L.; Wang, P. Analysis and evaluation of fault propagation behavior of aircraft all-electric braking system under DIMA architecture. *J. Aeronaut.* **2021**, *42*, 445–461.
32. Zhu, H.; Huang, J.; Zhao, L. Slipping Analysis on the Braking Process of a Commercial Aircraft with the Electric Brake Actuator. In Proceedings of the International Conference on Mechanical System Dynamics, Beijing, China, 1–5 September 2023; pp. 4179–4190.