Research Article

Safety Analysis of Integrated Modular Avionics System Based on FTGPN Method

Haiyun Yang¹,¹ Youchao Sun¹,¹ Longbiao Li,¹ Yundong Guo,¹ Siyu Su,¹
and Qijun Huangfu²

¹College of Civil Aviation, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China

²Nanjing Glaway Software Co., Ltd., Nanjing 210013, China

Correspondence should be addressed to Youchao Sun; sunyc@nuaa.edu.cn

Received 27 May 2020; Revised 5 August 2020; Accepted 18 August 2020; Published 1 September 2020

Academic Editor: Feng Qu

Copyright © 2020 Haiyun Yang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Compared with federated avionic architecture, the integrated modular avionic (IMA) system architecture in the aircraft can provide more sophisticated and powerful avionic functionality, and meanwhile, it becomes structurally dynamic, variably interconnected, and highly complex. The traditional approach such as fault tree analysis (FTA) becomes neither convenient nor sufficient in making safety analysis of the IMA system. In order to overcome the limitations, the approach that FTA combines with generalized stochastic petri net (GSPN) is proposed. First, FTA is used to establish the static model for the top level of the IMA system, while GSPN is used to build a dynamic model for each cell system. Finally, the combination model is generated, which is called the FTGPN model. Moreover, the FTGPN model is made safety analysis with the PIPE2 tool. According to the simulation result, corresponding measures are taken to meet the safety requirements of the IMA system.

1. Introduction

IMA system is evolving to provide more functionality with lesser parts, weight, and cost, while it is also meeting all the reliability and safety constraints [1–4]. To cope efficiently with the high level of complexity, a novel and structured development methodology is required [5–7]. As known to all, FTA is widely used for safety analysis of the system, but it has some limitations. One of such limitation is that it can only evaluate the safety of static systems. However, the IMA system gives rise to a variety of dynamic failure characteristics such as functional dependencies between events and priorities of failure events [8].

Model-Based safety analysis (MBSA) utilizes software automation and integrates with design models to simplify the safety analysis of complex systems [9]. Among these MBSA methods, the HiP-HOPS focuses on the automatic construction of predictive system failure analyses [10–17]. Meanwhile, the languages such as Architecture Analysis and Design Language (AADL) and AltaRica are used, auto-

matically analyzing potential failures in a system model. AADL provides a standardized textual and graphical notation for describing software and hardware system architectures and their functional interfaces [18, 19]. Therefore, the IMA system is proposed to model based on AADL [20–26]. However, its disadvantage is that it cannot directly perform safety analysis and needs to be converted to other safety analysis methods such as Petri net and HiP-HOPS [16, 17]. In addition, AltaRica [27] is high-level modelling language dedicated to safety analysis. Based on the AltaRica, there is a commercial tool called Simfia, which is the modelling platform for Airbus A380.

The two methods that GSPN and Fault tree driven Markov processes (FTDMP) are compared in [28]. Then, it points out that GSPN is at a higher level in modelling formalism and shows a superior modelling capacity compared to FTDMP. A conceptual framework, which incorporates the Semi-Markov Process (SMP) based complex behavior to HiP-HOPS for modelling of complex system is proposed in [29]. Although the quantitative analysis results obtained

FIGURE 1: IMA system.

through this SMP [30, 31] is much more precise than the results from GSPN analysis, the safety model in GSPN is more intuitive. Moreover, in order to reduce the computation for GSPN analysis, many mature simulation software tools such as GreatSPN [32] and PIPE2 [33, 34] are developed.

The hybrid method that GSPN is used with these cell systems and the FTA process is applied to the upper-level system is validated effectively [35]. Then, it gained a clear view of the relationship between the failure of subsystems and the failure of the system. However, it also lacks the further safety evaluation for the whole system. In addition, GSPN in some works [36–43] have been used to build a safety model for a single dynamic system. But the model cannot illustrate its interactions with other systems.

Within this broader context, the smaller novelties include:

- (1) According to the working principle, the IMA system is simplified in order to make the safety model more easily
- (2) The proposed FTGPN method not only builds static safety analysis for the top level of the IMA system but also establishes the dynamic safety model for cell systems
- (3) FTGPN model for the IMA system is simulated with PIPE2 tool and corresponding parameters can be adjusted to meet the safety requirements easily

FTGPN method solves the problem of being unable to conduct a comprehensive and accurate safety model for complex IMA system. Moreover, FTGPN provides an effective safety analysis method for the IMA system.

The section of this paper is organized as follows:

Section 2 introduces some preliminary knowledge mainly about the IMA system and the FTGPN method. Section 3 establishes the FTGPN model with FTA and GSPN for the IMA system. Section 4 makes the safety analysis for the FTGPN model. Section 5 depicts the capabilities and limitations of the FTGPN. Section 6 draws the conclusions.

2. Preliminary

In this section, the first IMA system is introduced. Then, an interview of the GSPN is given.

2.1. Integrated Modular Avionics. IMA architectures provide a general platform for hosting avionics in the aircraft. IMA platform includes the shared processing system, shared data network, and shared I/O system. The shared platform is an efficient means for implementing avionic functionality since it greatly reduces the electronic box and wire count in the aircraft. Therefore, the IMA system enables a great reduction in the size, weight, and power for a suite of avionic systems.

The IMA architecture is shown in Figure 1 [44]. The ARINC-653 standard is a common implementation of software partitioning [45]. It can guarantee each application's memory space and temporal execution environment so that they will not be affected by other applications.

The shared network replaces many dedicated communication lines with a shared backbone network. A common network implementation today is defined by the ARINC-664p7 standard [46]. ARINC-664p7 also includes the concept of partitioning through the use of Virtual Links (VLs) to ensure that communications from one application cannot affect the contents or impact the temporal characteristics of the message delivery (not-to-exceed data latency is guaranteed).

FIGURE 2: The simplified topology of the IMA system.

The shared Input/Output (I/O) system acts as a gateway to transfer I/O between many separate sources and the shared network. This makes the I/O available to all network-connected devices without having to run dedicated wiring in the aircraft. Since many sources of data are concentrated onto a common network, these devices are typically referred to as “Remote Data Concentrators (RDCs)” [47].

In order to model the IMA system, the simplified topology of the IMA system is attained and shown in Figure 2. These include the RDC, the General Processing Module (GPM), and the shared communication data network using the ARINC664 standard. The terminal AFDX has two independent communication interfaces, which are channels A and B, respectively. The software and hardware of the operating system for each GPM are the same while the software applications of the GPM are different [2].

The IMA system works as a converter and all communication signals are processed in the system. First, the non-ARINC664 signal is converted to the ARINC664 signal. Second, the signal goes through RDC. Third, it is transmitted to the GPM through channel A or B. After the signal is being processed, it is output through channel A or B from GPM. Finally, the signal is changed to the corresponding non-ARINC664 signal at RDC. This whole process is the simplified work theory of the IMA system. The following sections will make a safety analysis for the IMA system based on its simplified structure.

2.2. Overview of GSPN. GSPN is consisted by places (circular), transitions (rectangular bars), directed arcs, and tokens (black bullets). The directed arcs connect input places to transitions or transitions to input places. The places “P” represent the state or condition of a component. The transition “T” describes the change in state from input to output place. However, the direction of the flow of tokens is determined by the directed arcs. Each arc has a multiplicity, which depicts the token migration capacity of the arc. The transition can

FIGURE 3: A simple GSPN.

only fire if the input place has an equal number of tokens or more as the arc multiplicity [48–50].

In stochastic petri net (SPN), if a transition is fired, the token waits until the firing delay ends, the migration of tokens takes place from initial to final place, and the number of tokens migrating depends upon the input and output functions. Then, SPN was extended to GSPN. Besides SPN features, two new features are added which are immediate transition firing and inhibitor arcs (used to disable the transition when a token is present in input places) [51, 52]. The definitions of the GSPN are introduced as follows.

A GSPN is a 6-tuple $(P, T, F, W, M_0, \lambda)$ where:

(1) $P = \{p_1, p_2, \dots, p_m\}$ is a finite set of places, $n \geq 0$

(2) $T = T_1 \cap T_2$ presented all the transitions

$T_1 = \{t_1, t_2, \dots, t_m\}$ is a finite set of timed transitions which is associated with a random delay time between enabling and firing;

$T_2 = \{t_{m+1}, t_{m+2}, \dots, t_n\}$ is a finite set of immediate transitions which can be fired randomly and the delay is zero.

(3) $F \subseteq (P \times T) \cap (T \times P)$ is a set of arcs

There exist inhibitor arcs that can only form places to transitions and make the enable conditions to be disenabled.

(4) W is a weight function of arcs

(5) $M_0 : P \rightarrow \{0, 1, 2, 3, \dots\}$ is initial marking where $(P \times T) = \varphi \cap (T \times P) = \varphi$

(6) $\lambda = \{\lambda_1, \lambda_2, \dots, \lambda_n\}$ is a set of the firing rates corresponding to the timed transitions

M_i is from M_0 . For example, as shown in Figure 3, M is represented by $\{P1, P2, P3\}$. M_0 is $\{1, 0, 0\}$. A new marking $M_1\{0, 1, 0\}$ is reached when timed transitions $T1$ is enabled. M_1 marking is Vanishing state because the immediate transition $T2$ is enabled at once. Meanwhile, the Tangible state $M_2\{0, 0, 1\}$ is reached. M_0 , M_1 , and M_2 are the reachability sets for the simple system. M_0 and M_2 are Tangible states, while M_1 is Vanishing state. That is Vanishing state can change to a new Tangible state immediately.

3. Proposed FTGPN Method

Traditional safety analysis methods (such as fault trees, reliability block diagrams, binary decision diagrams, and Markov process models) cannot effectively simulate the dynamic behaviour of the system. However, GSPN is suitable for modelling the dynamic behaviour of the system [50].

FIGURE 4: FTGPN is illustrated with a simple example.

Therefore, the FTGPN approach is developed to combine fault trees and GSPN in a new way. And FTGPN is used to make safety analysis for the IMA system in this paper.

3.1. Brief Description of FTGPN. FTGPN is depicted clearly with a simple example in Figure 4. The failure of component Z1 is represented by “Z1”, while the failure of component Z2 is represented by “Z2”. Fault tree uses λ_{z1} and μ_{z1} as the failure and repair rates of component Z1 for quantitative analysis. If the component Z1 has failed, the FTGPN would use a GSPN model to represent the failure behaviour of Z1.

FTGPN approach is applied in the following steps. First, the fault tree is used to clearly identify the cell systems’ sequence with the deductive logic and establish the top level of the system. Second, the GSPN model for each cell systems is built. Third, the GSPN of cell systems are constructed according to the architecture of the fault tree. Finally, the FTGPN model for the whole system is formed and it can be made the safety analysis with the PIPE2 tool. And how to establish the FTGPN model for the IMA system will be introduced in detail in the following sections.

3.2. FTA Modelling. Generally, in order to ensure that the FTGPN model is correct and effective for application, some restrictions need to be made. It is assumed that the following conditions are true:

Assumption 1. Each component of the system has only two states, which are failed and operational.

FIGURE 5: The FTA model of the IMA system.

Assumption 2. Each component in the system fails independently, and no more than two components will fail at the same time.

Assumption 3. The maintenance equipment is sufficient, and the component is repaired in time after failed, and the repaired component is new as before.

Assumption 4. The failure rate of component is λ .

Assumption 5. The repair rate of component is μ .

Figure 5 shows the fault tree analysis for the architecture of the IMA system. The failure of RDC is represented by B. Meanwhile channel A of ARINC664 network is C1 and channel B of ARINC664 network is C2. Then, both of them lead to the failure of ARINC664 network represented as C. In addition, CPU is D, memory is E, RTOS is H, and the software of end system is G. Therefore, that one of them is failure will lead to the failure of GPM represented as M. Moreover, the relationship among the RDC, the ARINC664 network, and the GPM is combined with “OR”.

3.3. FTGPN Modelling. Based on the module theory, the GSPN model for GPM and ARINC664 network are established firstly. Finally, the top level of the FTGPN model for the IMA system is synthesized.

3.3.1. GPM Model. The GSPN of GPM model is illustrated in Figure 6, and model descriptions are presented in Tables 1 and 2. The working process for GPM is as follows. It is operational normally at first. After a random time, CPU changes from P_{dw} to the P_{df} and the marks in P_{mw} is empty (the number of marks in P_{mn} is 1, and it is used to prohibit the failure of other components in GPM), then the immediate transition T_{mf} is triggered, and the GPM changes from P_{mw} to P_{mf} . A random time later, it is assumed that the CPU in the GPM is repaired, and it changes from P_{df} to P_{dw} (the marks of P_{df} and P_{mn} disappear). Then, the CPU changes from P_{mf} to P_{mw} , and it indicates that CPU is operational.

3.3.2. ARINC664 Network Model. The GSPN model of the ARINC664 network is depicted in Figure 7, and the model descriptions are presented in Tables 3 and 4. The working

FIGURE 6: The GSPN model of GPM.

TABLE 1: Places in the GSPN model for GPM.

Name	Operational meaning
P_{mw}	GPM is operational
P_{mf}	GPM is failed
P_{dw}	CPU is operational
P_{df}	CPU is failed
P_{ew}	Memory is operational
P_{ef}	Memory is failed
P_{hw}	RTOS is operational
P_{hf}	RTOS is failed
P_{gw}	Software is operational
P_{gf}	Software is failed
P_{mn}	Number of components in failed state

TABLE 2: Transitions in GSPN model for GPM.

Name	Operational meaning	Trigger rate (1/h)
T_{mr}	GPM goes from failed to operational	—
T_{mf}	GPM goes from operational to failed	—
T_{dr}	CPU goes from failed to operational	0.001
T_{df}	CPU goes from operational to failed	2×10^{-5}
T_{er}	Memory goes from failed to operational	0.002
T_{ef}	Memory goes from operational to failed	2×10^{-5}
T_{hr}	RTOS goes from failed to operational	0.0011
T_{hf}	RTOS goes from operational to failed	5×10^{-5}
T_{gr}	Software goes from failed to operational	0.0011
T_{gf}	Software goes from operational to failed	5×10^{-5}

process for the ARINC664 network is as follows. It is operational normally at first. After a random time, ARINC664 network channel A changes from P_{clw} to P_{clf} , and the number of marks in P_{cw} becomes 1, then the number of marks in P_{cn} is 1. When the number of marks in P_{cw} becomes 0 and the number of marks in P_{cn} becomes 2, the immediate transition T_{cf} is triggered, and the ARINC664 network changes to P_{cf} . A random time later, ARINC664 network channel A changes from P_{clf} to P_{clw} , and the ARINC664 network system recovers to P_{cw} .

3.3.3. FTGPN Model. The FTGPN model of the IMA system is shown in Figure 8, and the model descriptions are presented in Tables 5 and 6. The working process for the IMA system is as follows. The IMA system works normally at first. After a random time, the transition T_{bf} is triggered and the IMA system changes to P_{af} . A random time later, the RDC

recovers to operational, and the transition T_{br} is triggered next. Meanwhile, the mark of P_{af} disappears, and the IMA system recovers to operational. Finally, according to top level of FTA model for the IMA system, the GSPN models for the cell systems such as GPM and ARINC664 network are combined to the FTGPN model. Additionally, the safety analysis is made for the IMA system in the following sections.

4. Results and Discussion

The tool PIPE2 [33, 34] is used to make analysis for the FTGPN model of the IMA system. PIPE2 is an open-source tool that supports creating and analyzing Petri nets and has an easy-to-use graphical user interface that allows a user to establish stochastic petri net models. Additionally, the analysis environment in this tool includes different modules such as steady-state analysis, reachability/coverability graph analysis, and GSPN analysis [37].

FIGURE 7: The GSPN model of ARINC664 network.

TABLE 3: Places in GSPN model for ARINC664 network.

Place	Operational meaning
P_{cw}	ARINC664 network is operational
P_{cf}	ARINC664 network is failed
P_{c1w}	ARINC664 network channel A is operational
P_{c1f}	ARINC664 network channel A is failed
P_{c2w}	ARINC664 network channel B is operational
P_{c2f}	ARINC664 network channel B is failed
P_{cn}	Number of channels in failed state

First, the FTGPN model is established in PIPE2 as shown in Figure 8. Then, the analysis results in Tables 7 and 8 can be obtained through GSPN analysis. As depicted in Table 7, the IMA system's operational states are $M0$, $M5$, and $M6$, and the number of tokens in P_{af} is 0. Moreover, the total value of $M0$, $M5$, and $M6$ is 0.89213. It equals to the probability of P_{af} when the number of tokens is 0 ($\mu = 0$) in Table 8. Therefore, the conclusion is that the probability of the IMA system in operational state is 0.89213.

Figure 9 illustrates the reachability graph of the FTGPN model for the IMA system. Each of the graph node acts as one of the IMA system states, and the initial state is node $S0$. It is known that $S0 = \{0, 0, 0, 0, 1, 0, 1, 0, 0, 2, 0, 1, 0, 1, 0, 1, 0, 0, 1\}$, which is represented by the number of tokens in each place. Also, $S0$ is corresponding to $M0$ in Table 7. In addition, the Tangible state is presented in red color, while the blue color is for Vanishing state. Therefore, the marking of the Tangible state is corresponding to the marking in Table 7.

As shown in Figure 9, the states are changed by firing the transitions. For instance, state $S0(M0)$ is fired by transition T_{c1f} and then becomes $S6(M6)$. Meanwhile, state $S0(M0)$ is fired by transition T_{c2f} and then becomes $S5(M5)$. These

TABLE 4: Transitions in GSPN model for ARINC664 network.

Transition	Operational meaning	Trigger rate (1/h)
T_{cf}	ARINC664 network goes from operational to failed	—
T_{cr}	ARINC664 network goes from failed to operational	—
T_{c1f}	ARINC664 network channel A goes from operational to failed	2×10^{-5}
T_{c1r}	ARINC664 network channel A goes from failed to operational	0.001
T_{c2f}	ARINC664 network channel B goes from operational to failed	2×10^{-5}
T_{c2r}	ARINC664 network channel B goes from failed to operational	0.001

can all be referred to in Table 7. The number of marks is changing in the corresponding transitions such as P_{c1f} , P_{c1w} , P_{c2f} , and P_{c2w} . Meanwhile, $S7(M1)$, $S8(M2)$, $S9(M3)$, and $S10(M4)$ can be found in the corresponding states in Table 7. The states in Table 7 match with the Tangible state with red color one by one in Figure 9. Although the results can be attained manually from Figure 7, the whole reachability graph for a complex system is got fast and accurate with the PIP2 tool.

In addition, every small part of the reachability graph is a closed loop. For instance, first, $S6(M6)$ is fired by transition T_{df} and becomes $S18$. Second, $S18$ is fired by transition T_{mf} and becomes $S27$. Third, $S27$ is fired by transition T_{dr} and becomes $S29$. Finally, $S29$ is fired by transition T_{mr} and returns to $S6(M6)$. The whole process is a circle which is depicted in purple color in Figure 9. And the reachability graph is composed of many circles. These indicate all the Tangible states and Vanishing states for the IMA system. Moreover, according to the reachability graph, further research for quantitative analysis can be made in the future.

The different initial random firings have been implemented for the simulation of the FTGPN model. The token distribution has been updated by 100, 500, and 1000 random firings, which are shown in Figure 10.

The graph in Figure 10 shows that the three lines almost coincide. The highest point is P_{cw} , and the average number of tokens is close to 2, while the lowest points are P_{bf} , P_{bw} , and P_{cf} . The value of P_{bw} is not our expectation. Therefore, corresponding countermeasures should be developed to increase its value and make it get to 1. Obviously, the simulation for the FTGPN model allows users to analyze the failure behavior of IMA systems in a more intuitive way. In fact, the above simulations are used to explain the application to the FTGPN model of the IMA system. However, it does not correspond to the real case in the aircraft. For example, there is no repair for the IMA system when the FTGPN model is based on the flight. Although the FTGPN method for modelling the IMA system is verified effectively, further quantitative analysis should be made in the future.

FIGURE 8: FTGPN model of the IMA system.

TABLE 5: Places in GSPN model for RDC and IMA system.

Place	Operational meaning
P_{bw}	RDC is operational
P_{bf}	RDC is failed
P_{af}	IMA system is failed

TABLE 6: Transitions in the GSPN model for RDC.

Transition	Operational meaning	Trigger rate (1/h)
T_{bf}	RDC goes from operational to failed	2.0×10^{-5}
T_{br}	RDC goes from failed to operational	0.001

5. Capabilities and Limitations of the FTGPN

Some of the capabilities and limitations (limitation in making accurate quantitative analysis for the IMA system) of the FTGPN are discussed in this section.

5.1. Capabilities of the FTGPN. The FTGPN offers the following capabilities.

- (1) First, the architecture of the IMA system is simplified according to the work theory. And this is a very important step to build the FTA model for the top level of the system

- (2) The FTGPN method establishes the top level of the IMA system with FTA in the static model, while the cell systems are built with GSPN in a dynamic model. In addition, the dependency and interactions among the IMA system are depicted intuitively by the FTGPN model
- (3) PIPE2 tool is chosen to make a simulation for the FTGPN model of the IMA system. The results are not only the Tangible states but also the probability of the IMA system in operational. In addition, the

TABLE 7: GSPN steady-state analysis results set of Tangible states.

	M0	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14
P_{af}	0	1	1	1	1	0	0	1	1	1	1	1	1	1	1
P_{bf}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P_{bw}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P_{c1f}	0	0	0	0	0	0	1	0	1	0	1	0	1	0	1
P_{c1w}	1	1	1	1	1	1	0	1	0	1	0	1	0	1	0
P_{c2f}	0	0	0	0	0	1	0	1	0	1	0	1	0	1	0
P_{c2w}	1	1	1	1	1	0	1	0	1	0	1	0	1	0	1
P_{cf}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P_{cn}	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1
P_{cw}	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1
P_{df}	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1
P_{dw}	1	1	1	1	0	1	1	1	1	1	1	1	1	0	0
P_{ef}	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0
P_{ew}	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1
P_{gf}	0	0	1	1	0	0	0	0	0	1	1	0	0	0	0
P_{gw}	1	1	0	0	1	1	1	1	1	0	0	1	1	1	1
P_{hf}	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0
P_{hw}	1	0	1	1	1	1	1	0	0	1	1	1	1	1	1
P_{mf}	0	1	1	1	1	0	0	1	1	1	1	1	1	1	1
P_{mn}	0	1	1	1	1	0	0	1	1	1	1	1	1	1	1
P_{mw}	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0

TABLE 8: Token probability density.

	P_{af}	P_{bf}	P_{bw}	P_{c1f}	P_{c1w}	P_{c2f}	P_{c2w}
$\mu = 0$	0.89213	1	1	0.98077	0.01923	0.98077	0.01923
$\mu = 1$	0.10787	0	0	0.01923	0.98077	0.01923	0.98077
$\mu = 2$	0	0	0	0	0	0	0
	P_{cf}	P_{cn}	P_{cw}	P_{df}	P_{dw}	P_{ef}	P_{ew}
$\mu = 0$	1	0.96154	0	0.98216	0.01784	0.99108	0.00892
$\mu = 1$	0	0.03846	0.03846	0.01784	0.98216	0.00892	0.99108
$\mu = 2$	0	0	0.96154	0	0	0	0
	P_{gf}	P_{gw}	P_{hf}	P_{hw}	P_{mf}	P_{mn}	P_{mw}
$\mu = 0$	0.95945	0.04055	0.95945	0.04055	0.89213	0.89213	0.10787
$\mu = 1$	0.04055	0.95945	0.04055	0.95945	0.10787	0.10787	0.89213
$\mu = 2$	0	0	0	0	0	0	0

reachability graph which depicts all the states can be attained automatically. Moreover, the number of tokens is illustrated clearly in each place. Therefore, the corresponding measures can be taken according to the simulation

5.2. *Limitations of the FTGPN.* The FTGPN has the following limitations. All will be resolved in our future works.

- (1) The simplified IMA system is used in this paper. However, it is known that simplifying the complex

(2) It takes much time to establish the FTGPN model. In addition, it is very easy to make mistakes in building model manually. Therefore, a software

which can generate the model automatically should be developed

- (3) Comparing with the existing approaches [12, 29–32], the FTGPN method is better in establishing the safety model clearly and directly. However, quantitative analysis for FTGPN is not accurate. Therefore, the quantitative analysis of the FTGPN should be optimized and verified with the Aircraft fuel distribution system. Making optimization for quantitative analysis is my further work
- (4) In this paper, the PIPE2 tool is chosen to make the simulation. Because of the limitations of the tool, the safety analysis is inadequate. Therefore, the functions for the tool should be extended especially in quantitative analysis

6. Conclusion

FTGPN model is proposed for dynamic safety analysis of the IMA system. First, FTA is introduced to make a static model for the top level of the IMA system, and then GSPN is employed to construct a dynamic model for cell systems. It represents an advancement model for safety analysis and allows faster, automatic analysis of dynamic systems using GSPN. The FTGPN model has combined the advanced features of FTA with GSPN. The integration for the two safety analysis methods is a potential tool to make the safety analysis for the complex and interactive IMA system.

The conclusions of this paper are as follows:

- (1) The complex IMA system is simplified properly which makes the rest work such as establishing the FTGPN model more easily
- (2) The FTGPN method for combining the FTA and GSPN and applying in the IMA system not only shows the relationship between cell systems but also simulates the dynamic interactions in each cell system
- (3) PIPE2 is used to simulate the FTGPN model of the IMA system. All the parameters that we need are shown to us obviously. Then, we can adjust them to meet the safety requirements conveniently

However, for the large system including thousands of components, it is difficult to build the FTGPN model. It is better to develop a tool that can establish the FTGPN model and make safety analysis for it automatically.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no competing interests.

Acknowledgments

This paper is supported by the Research Program supported by the National Natural Science Foundation of China (U1333119), the National defense basic scientific research program of China (JCKY2013605B002), and the Civil Aircraft Special Foundation of Ministry of Industry and Information Technology (MJ-2017-J-91).

References

- [1] D. Rajaram, Y. Cai, I. Chakraborty, and D. N. Mavris, "Integrated sizing and optimization of aircraft and subsystem architectures in early design," *Journal of Aircraft*, vol. 55, no. 5, pp. 1942–1954, 2018.
- [2] C. H. Fleming and N. G. Leveson, "Improving hazard analysis and certification of integrated modular avionics," *Journal of Aerospace Information System*, vol. 11, no. 6, pp. 397–411, 2014.
- [3] T. Ishimatsu, N. G. Leveson, J. P. Thomas et al., "Hazard analysis of complex spacecraft using systems-theoretic process analysis," *Journal of Spacecraft and Rockets*, vol. 51, no. 2, pp. 509–522, 2014.
- [4] Z. Jiang, T. Zhao, S. Wang, and F. Ren, "A novel risk assessment and analysis method for correlation in a complex system based on multi-dimensional theory," *Applied Science*, vol. 10, article 3007, 2020.
- [5] R. P. Collinson, *Introduction to Avionics System*, Springer Science & Business Media, 2017.
- [6] C. R. Spizer, *Digital Avionic Handbook*, 3rd edition, pp. 22–258, CRC Press., 2015.
- [7] J. B. Itier, "A380 integrated modular avionics," in *Proceedings of the ARTIST2 Meeting on Integrated Modular Avionics*, pp. 72–75, Roma, Italy, 2007.
- [8] J. Anjali and W. Michael, *Model-based safety analysis final report*, NASA/CR-2006-21395, NASA Contractor Report, 2006.
- [9] Y. Papadopoulos, M. Walker, D. Parker et al., "A synthesis of logic and bio-inspired techniques in the design of dependable systems," *Annual Reviews in Control*, vol. 41, pp. 170–182, 2016.
- [10] Y. Papadopoulos and J. A. McDermid, "Hierarchically performed hazard origin and propagation studies," in *Computer Safety, Reliability and Security. SAFECOMP 1999*, M. Felici and K. Kanoun, Eds., vol. 1698 of Lecture Notes in Computer Science, pp. 139–152, Springer, Berlin, Heidelberg, 1999.
- [11] Y. Papadopoulos, M. Walker, D. Parker et al., "Engineering failure analysis and design optimisation with HiP-HOPS," *Engineering Failure Analysis*, vol. 18, no. 2, pp. 590–608, 2011.
- [12] S. Kabir, M. Walker, and Y. Papadopoulos, "Dynamic system safety analysis in HiP-HOPS with petri nets and bayesian networks," *Safety Science*, vol. 105, pp. 55–70, 2018.
- [13] M. Bozzano and Y. Papadopoulos, "A model-based extension to HiP-HOPS for dynamic fault propagation studies," in *Model-Based Safety and Assessment. IMBSA 2017*, M. Bozzano and Y. Papadopoulos, Eds., vol. 10437 of Lecture Notes in Computer Science, pp. 163–178, Springer, Cham, 2017.
- [14] Z. Mian, L. Bottaci, Y. Papadopoulos, and M. Biehl, "System dependability modelling and analysis using AADL and HiP-HOPS," in *Proceedings of the 14th IFAC Symposium on*

- Information Control Problems in Manufacturing*, pp. 1447–1652, Bucharest, Romania, 2012.
- [15] Y. Papadopoulos, *Safety-Directed System Monitoring Using Safety Cases*, [Ph.D. thesis], University of York, 2000.
 - [16] Z. Mian, L. Bottaci, Y. Papadopoulos, and N. Mahmud, “Model transformation for analyzing dependability of AADL model by using HiP-HOPS,” *Journal of Systems and Software*, vol. 151, pp. 258–282, 2019.
 - [17] Z. Mian, Y. Gao, X. Shi, and C. Tang, “Semantic mapping for model transformation between AADL2 and HiP-HOPS,” in *2019 4th International Conference on System Reliability and Safety (ICSRS)*, pp. 539–543, Rome, Italy, 2019.
 - [18] A. E. Rugina, *Dependability modelling and evaluation-from AADL to stochastic petri nets in systèmes informatiques*, [Ph. D. thesis], Institute National Polytechnique de Toulouse, Toulouse, 2007.
 - [19] A. E. Rugina, K. Kanoun, and M. Kaâniche, “A system dependability Modeling framework using AADL and GSPNs,” in *Architecting Dependable Systems IV*, R. Lemos, C. Gacek, and A. Romanovsky, Eds., vol. 4615 of Lecture Notes in Computer Science, pp. 14–38, Springer, Berlin, Heidelberg, 2007.
 - [20] A. E. Rugina, K. Kanoun, and M. Kaâniche, “The ADAPT tool: from AADL architectural models to stochastic petri nets through model transformation,” in *2008 Seventh European Dependable Computing Conference*, Kaunas, Lithuania, 2008.
 - [21] R. B. Han and S. H. Wang, “Transformation rules from AADL to improved colored GSPN for integrated modular avionics,” in *2016 11th International Conference on Reliability, Maintainability and Safety (ICRMS)*, Hangzhou, China, 2016.
 - [22] B. Liu, Z. Quan, and S. Wang, “IMA reconfiguration modelling and reliability analysis based on AADL,” in *The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent*, Hong Kong, China, 2014.
 - [23] T. Robati, A. E. Kouhen, A. Gherbi, S. Hamadou, and J. Mullins, “An extension for AADL to model mixed-criticality avionic systems deployed on IMA architectures with TTEthernet,” in *1st Architecture Centric Virtual Integration Workshop (ACVI)*, Valencia, Spain, 2014.
 - [24] Y. Wu, W. Wang, Z. Yu, and B. Liu, “Study of Ima software dynamic reconfiguration based on AADL,” *Information Technology Journal*, vol. 12, no. 22, pp. 6627–6630, 2013.
 - [25] J. Delange and P. Feiler, “Architecture fault modeling with the AADL error-model annex,” in *2014 40th EUROMICRO Conference on Software Engineering and Advanced Applications*, Verona, Italy, 2014.
 - [26] P. Wang, C. X. Zhao, and F. Yan, “Research on the reliability analysis of the integrated modular avionics system based on the AADL error model,” *International Journal of Aerospace Engineering*, vol. 2018, Article ID 9358461, 11 pages, 2018.
 - [27] T. Prosvirnova, M. Batteux, P. A. Brameret et al., “The altarica 3.0 project for model-based safety assessment,” in *Proceedings of 4th IFAC Workshop on Dependable Control of Discrete Systems, DCDS 2013*, York, Great Britain, September 2013.
 - [28] M. Talebberrouane, F. Khan, and Z. Lounis, “Availability analysis of safety critical systems using advanced fault tree and stochastic petri net formalisms,” *Journal of Loss Prevention in the Process Industries*, vol. 44, pp. 193–203, 2016.
 - [29] S. Kabir, K. Aslansefat, I. Sorokos, Y. Papadopoulos, and Y. Gheraibia, “A conceptual framework to incorporate complex basic events in HiP-HOPS,” in *Model-Based Safety and Assessment. IMBSA 2019*, Y. Papadopoulos, K. Aslansefat, P. Katsaros, and M. Bozzano, Eds., vol. 11842 of Lecture Notes in Computer Science, pp. 109–124, Springer, Cham, 2019.
 - [30] S. Kabir, K. Aslansefat, I. Sorokos, Y. Papadopoulos, and S. Konur, “A hybrid modular approach for dynamic fault tree analysis,” *IEEE Access*, vol. 8, pp. 97175–97188, 2020.
 - [31] K. Aslansefat and G. R. Latif-Shabgahi, “A hierarchical approach for dynamic fault trees solution through semi-Markov process,” *IEEE Transactions on Reliability*, vol. 2019, pp. 1–18, 2019.
 - [32] E. G. Amparore, M. Beccuti, and S. Donatelli, “(Stochastic) model checking in Great SPNApplication and Theory of Petri Nets and Concurrency. PETRI NETS 2014,” vol. 8489 of Lecture Notes in Computer Science, Springer, Cham, 2014.
 - [33] P. Bonet, C. M. Llad, and R. Puigianer, “PIPE v2.5: a petri net tool for performance modelling,” in *In Proceedings of 23rd Latin American conference informatics*, Costa Rica, 2007.
 - [34] N. J. Dingle, W. J. Knottenbelt, and T. Suto, “PIPE2: a tool for the performance evaluation of generalised stochastic petri nets,” *ACM SIGMETRICS Performance Evaluation Review*, vol. 36, no. 4, pp. 34–39, 2009.
 - [35] Y. Lu, Y. W. Dong, X. M. Wei, and M. Xiao, “A hybrid method of redundancy system reliability analysis based on AADL models,” in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, Lisbon, Portugal, 2018.
 - [36] J. P. Fan and T. D. Zhao, “Dispatch reliability of civil aviation simulation based on generalized stochastic petri nets (GSPN),” in *2014 10th International Conference on Reliability, Maintainability and Safety (ICRMS)*, Guangzhou, China, 2014.
 - [37] L. M. Almutairi and S. Shetty, “Generalized stochastic petri net model based security risk assessment of software defined networks,” in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, pp. 545–550, Baltimore, MD, USA, 2017.
 - [38] D. Jana and N. Chakraborty, “Generalized stochastic petri nets (GSPN) for analysis of microgrid under uncertainties,” in *2018 20th National Power Systems Conference (NPSC)*, Tiruchirappalli, India, 2018.
 - [39] M. Garoui, “Modeling and analysis of vehicles platoon safety in a dynamic environment based on GSPN,” in *Enterprise, Business-Process and Information Systems Modeling. BPMDS 2016, EMMSAD 2016*, R. Schmidt, W. Guédria, I. Bider, and S. Guerreiro, Eds., vol. 248 of Lecture Notes in Business Information Processing, pp. 465–478, Springer, Cham, 2016.
 - [40] S. Kabir, M. Walker, and Y. Papadopoulos, “Quantitative evaluation of Pandora temporal fault trees via petri nets,” *IFAC-Papers Online*, vol. 48, no. 21, pp. 458–463, 2015.
 - [41] M. A. Marsan, G. Balbo, G. Conte, S. Donatelli, and G. Franceschinis, “Modelling with generalized stochastic petri nets,” *ACM SIGMETRICS Performance Evaluation Review*, vol. 26, no. 2, 1998.
 - [42] Y. Chu, Z. Yuan, and J. Chen, “Research on dynamic reliability of a jet pipe servo valve based on generalized stochastic petri nets,” *International Journal of Aerospace Engineering*, vol. 2015, 8 pages, 2015.
 - [43] S. Tigane, L. Kahloul, S. Benharzallah, S. Baair, and S. Bourekkache, “Reconfigurable GSPNs: a modeling formalism of evolvable discrete-event systems,” *Science of Computer Programming*, vol. 183, article 102302, 2019.
 - [44] C. Watkins, “Integrated modular avionics: managing the allocation of shared intersystem resources,” in *2006 IEEE/AIAA*

25TH Digital Avionics Systems Conference, Portland, OR, USA, 2006.

- [45] A. R. I. N. C. Electronic Engineering Committee, *ARINC653: Avionics Application Software Standard Interface*, Aeronautical Radio, Inc, Annapolis, MD, 2006.
- [46] ARINC Electronic Engineering Committee, "ARINC 664p7: Aircraft Data Network, Part 7," in *Avionics full duplex switched ethernet (AFDX) network*, Aeronautical Radio, Inc, Annapolis, MD, 2005.
- [47] C. B. Watkins and R. Walter, "Comparing two industry game changers: integrated modular avionics and the iPhone," in *2009 IEEE/AIAA 28th Digital Avionics Systems Conference*, Orlando, FL, USA, 2009.
- [48] R. David and H. Alla, *Discrete, Continuous, and Hybrid Petri Nets*, Springer, Berlin Heidelberg, 2005.
- [49] T. Murata, "Petri nets: properties, analysis and applications," *Proceedings of the IEEE*, vol. 77, no. 4, pp. 541–580, 1989.
- [50] R. Li and S. Reveliotis, "Performance optimization for a class of generalized stochastic petri nets," *Event Dynamic Systems*, vol. 25, no. 3, pp. 387–417, 2014.
- [51] M. Z. Kamil, M. Taleb-Berrouane, F. Khan, and S. Ahmed, "Dynamic domino effect risk assessment using petri-nets," *Process Safety and Environmental Protection*, vol. 124, no. 2019, pp. 308–316, 2019.
- [52] P. J. Haas, "Stochastic petri nets: modelling, stability, simulation," in *Proceedings of the 2004 Winter Simulation Conference*, vol. 1, pp. 101–112, 2004.