Feasibility Analysis of Reliability Analysis Methods Applying in Air Traffic Control System

Zhuojia Wang*, Xin Jiang and Jian Tang
Avionics Research Department, Commercial Aircraft Corporation of China, Beijing, China
Email: wangzhuojia@buaa.edu.cn

Abstract. Air traffic control system plays a vital role of air traffic management system, of which reliability determines the service quality and supply level of air transportation. The structure of air traffic control system is considered, and an expression of reliability analysis is applied. A mount of methods including traditional reliability analysis and network system reliability analysis are introduced to demonstrate whether they are feasibility for reliability analysis of air traffic control system. This work can be used as reference and basic for air traffic control system, which is meaningful for ATM safety operation, system selection and response repair.

Keywords. Air traffic control system, Software and hardware integration model, Reliability analysis method.

1. Introduction
The Air Traffic Control (ATC) system is a strategic infrastructure for the country to implement airspace management, ensure flight safety, and achieve efficient and orderly operation of air transportation. It is an important part of the national air defense system. The air traffic control automation system, as the core technical equipment in the modern ATC system, integrates the information processing, information display and command functions of various kinds of equipment such as communication, navigation and monitoring, and is the support unit of the ATC system. Therefore, the reliability of the air traffic control automation system is an important part of the air traffic management safety management. Assessing the reliability of an air traffic control automation system is the basis for the transport service capability and assurance assessment of the entire air traffic control system.

In recent years, the flight volume of civil aviation has increased year by year. The number of aircraft movements in China has exceeded 10 million for the first time in 2017, and the annual growth rate has exceeded 1 million. The control pressure of the control system will become larger and larger in the future. At the same time, the reliability of the existing air traffic control automation system has become one of the bottlenecks of the industry. The potential safety risks caused by the failure of the control system in civil aviation operation are becoming more and more important.

In April 2017, the Hong Kong International Airport Air Traffic Control System was unable to identify the target due to the lack of eight flight signage information, resulting in an inbound flight that could not be released for about 15 minutes. In September 2017, the Sydney airport air traffic control system caused computer software failure due to radar failure, causing domestic flights to stop and land for 4 hours, dozens of flights cancelled, and flight delays to Sydney for one day.

In November 2017, a radio failure occurred in the Sapporo control system in Japan, causing 10 airports in Hokkaido and surrounding areas in northeastern Japan to stop taking off and land for more than 90 minutes. The flights scheduled to fly to the area were delayed to take off or return, and 20
flights were cancelled. Therefore, there is an urgent need to carry out technical research on the reliability guarantee of air traffic control automation systems.

The current research field of reliability analysis has made great progress. The evaluation method brings together a large number of concepts, models and algorithms, but the reliability analysis of the air traffic control automation system is still insufficient.

Traditional system reliability analysis studies generally involve the air traffic control system subsystem or its software system, and it is difficult for each analysis method to extend the analysis of the entire system. The specific performance is that the description ability of the topology special relationship is limited, and it is difficult to analyze the influence of the fault propagation. The air traffic control automation system is a typical software and hardware integrated network information system, which has the characteristics of software and hardware synthesis, complex structure and complex function association. The comprehensive hardware and software features are embodied in a two-layer structure, including hardware levels such as monitoring processors and control seats, and software levels such as situation monitoring and air-to-air command; the system structure involves system equipment such as communication, navigation, surveillance, and meteorology; While the various services of the system work together, the faults will also propagate with different interactions between software and hardware.

In contrast, the networked method is more suitable for studying the air traffic control automation system because of its flexible expansion and convenient relationship. However, in the field of air traffic management systems, the research of networked systems is mostly the information network of traffic networks rather than air traffic control automation systems. In the study of traffic network, there are related researches from system structure and microscopic features [1-2] to route topology network [3-4]. Although the research content of traffic network and air traffic control automation information system is different, the related research of fault propagation [5-8], multi-layer network modeling [9], fault repair, etc. [10] has certain similarities and can be used as a reference basis.

This paper first introduces the structure and characteristics of the air traffic control automation system; then introduces a description method of the reliability of the reaction system; finally, the software and hardware reliability analysis methods are combined to analyze their respective usability, and how to describe the software and hardware integration of the system characteristic.

2. Introduction to Air Traffic Control Automotive System

The modern air traffic control automation system uses the information technology to provide the control personnel with the control and command functions of flight planning, flight dynamic monitoring and flight interval deployment. It is the key to ensure the safe and orderly flight, and directly determines the transportation service capability of the air traffic control system. And the level of protection.

The air traffic control automation system is a type of system with relatively stable reliability. Due to the strict requirements of the air traffic control system for all-day work and high stability requirements, software and hardware have been tested separately and in the whole process from system design to on-site commissioning, but this does not mean air traffic control automation. The system no longer requires analysis of reliability. On the one hand, the system is dynamically changing during use, and this dynamic change is most reflected in the increase in device functionality.

After these new software and hardware are added to the system, the upgraded system lacks a large-scale continuous test of the overall time due to the requirement that the production operation does not stop, and thus may cause a failure due to the conflict. On the other hand, in the daily operation, there may be a phenomenon of human supervision and maintenance negligence, and unexpected events other than expected. These human causes and emergencies are likely to cause failures and have a large impact.
The reliability of the air traffic control automation system refers to the ability of the air traffic control automation system to complete the specified functions within a certain period of time under certain conditions of use. In order to establish its reliability index system, it is necessary to establish a reliability assessment dimension based on the function and structure of the system. This paper divides the reliability dimension into three dimensions: system dimension, state dimension and business dimension. Figure 1 shows the reliability dimension division of the air traffic control automation system.

In the system dimension, the system is divided into three levels: system layer, subsystem layer and equipment layer according to the system structure and function. The layer-by-layer decomposition and reliability analysis are layer-by-layer decomposition corresponding to the system reliability index requirements.

The state dimension describes the degree of failure of different systems and the impact of the reliability indicators. Reliability analysis is divided into five levels: disaster failure, severe fault, critical fault, mild fault and normal work according to the degree of hazard of the system. Among them, normal work can be subdivided into supporting full-load work and only supporting normal work.

The service dimension mainly describes the impact of different fault types and user types corresponding to the reliability indicators. The physical layer pays attention to the system structure function, which is mainly the connectivity of the system structure network; the configuration layer pays attention to the system component performance, which is mainly the reliability of the system function performance; the service layer pays attention to the support business dynamics, mainly for the system to actually perform the specified function reliability.

This representation method can modify the content of the state dimension to make appropriate changes, which itself can reflect the current system availability and can reflect the service capabilities that the system can currently support. If the content for the state dimension is modified to various metrics, expressed as the ability to support full-load work to support low-load work, the representation structure can be used for system selection and performance evaluation.

3. Overview of Reliability Analysis Methods
As a command center system to ensure safe, efficient and smooth operation of air traffic, the air traffic control automation system has always been a hot issue for the air traffic control academic community. The early research work mainly used traditional reliability engineering theory to analyze and evaluate some reliability technologies and subsystems around reliability parameter indicators. However, traditional research methods are not enough to solve the current software and hardware synthesis, topological structure, and functions. Incompatibility analysis of a wide range of air traffic control systems. In the past ten years, with the development of the theory of network reliability and cascading
failure, the research on the invulnerability of the air traffic control automation system has ushered in a new opportunity.

3.1. Research Based on Traditional Reliability Theory
The reliability analysis of the initial air traffic control system is carried out around the analysis and evaluation of the system engineering aging parameters. Common reliability indicators include Mean Time to Failure (MTTF), Mean Time Between Malfunction (MTBM), and Mean Time Between Maintain (MTBM). Accurate calculation of the above parameters is highly complex and is not suitable for use in large-scale, complex network systems. The simulation method estimates such parameters, such as sample-based Monte Carlo simulation [11] and NHPP model using statistical probability knowledge to estimate reliability indicators [12], can’t reflect the special topological relationship of hardware and software coupling in the air traffic control system.

Since then, system reliability research has been based on models describing system structure and operational processes, studying the time-dependent parameters of system reliability, and designing other evaluation indicators [13]. The most direct modeling idea is to establish a relational model based on logical relationships such as system series and parallel or GO method. However, the logic block diagram description does not reflect fault propagation between modules. Focusing on the idea of hierarchical analysis, some studies first define the air traffic control system as a combination of basic components, and then use the fault tree model for analysis [14-15]. Similarly, in the risk of upgrading the air traffic control automation system, Li Dongbin and others from the Civil Aviation Institute of China also applied an event tree based analysis method [16]. However, such research is extremely demanding for the construction of model relationships. It is not only difficult to express some special structural relationships in the system, but also requires accurate structural models as a prerequisite for analysis.

Modeling based on state changes is based on Petri nets and Markov chains. Lucio F.V. used the fluid stochastic Petri net (FSPN) to model the ADS-B-based empty pipe system and conducted risk analysis on various safety factors such as airspace, aircraft, and navigation [17]. Wang Xinglong et al. used the Markov chain model and combined operational fault data to predict and analyze the software running state of the air traffic control automation system [18]. For large-scale systems, the Petri net model is difficult to express the interaction between hardware and software. The Markov chain model is difficult to analyze due to too many states, and it needs to ensure that the state transition probability is constant, and only applies to the ideal situation.

At the traditional evaluation level, the research objects are usually single, and most of them focus on subsystems or hardware devices. For example, for the reliability assessment of the air traffic control automation system subsystem, Li Qian of Sichuan University adopted the fuzzy neural network. Such research has tended to be a preliminary trend in networked research or hierarchical research, but has not yet involved a specific model of networking.

In summary, although the traditional reliability analysis theory has limited applicability, it can be used as the basis for reliability analysis of unit components. With the continuous expansion of the management scale and analysis level of the ATC automation system, the research object can’t stay in the local system and independent factors [19]. The traditional reliability assessment methods have their own shortcomings in the three problems of software and hardware coupling analysis, special topology performance and fault propagation law analysis. In order to study the overall reliability of the air traffic control automation system, it is necessary to combine the network analysis mode to make up for the above shortcomings.

3.2. Research Based on Networked Theoretical Methods
The concept of network reliability was proposed by Lee in 1955 for communication network problems. Based on graph theory and equipment physical failure, the analysis and evaluation model was built, and the research content of network reliability was divided into two categories: connectivity and performance [20]. In the 1970s, the network system studied was mainly a homogenous
telecommunication network or computer network, mainly studying the information forwarding function of small-scale networks. The reliability analysis content is mainly the connectivity of the network and the simple performance of the communication network congestion and delay. The analysis object is the communication hardware device.

In recent years, with the continuous construction and expansion of network systems in various fields, the development of various types of software, and the comprehensive use of hardware and software, the functions that the system is given are far more than the basic information forwarding. The focus of network reliability research also extends from structural connectivity reliability to operational reliability. Among them, network analysis represented by complex network theory [21-22] has become a research branch. Because it is good for reflecting the heterogeneous topology of large-scale integrated networks, it scientifically reveals the essential features and dynamic laws of topologies. Not only can structural availability be analyzed, for example, Albert et al. [23] used two methods of destruction to test the damage of ER random networks and BA scale-free networks, and analyzed the invulnerability of network structures in different damage modes. Moreover, the functional availability can also be analyzed. Taking the power network function research as an example: the functional reliability of Lucas Cuadra et al. [24] is introduced into the knowledge parameters of the telecommunications field, and the networked model is used to analyze the functional use reliability of the power network system.

At the same time, in the face of fault analysis in the network, more attention is paid to the study of the propagation impact of faults, in which the effects of multi-layered dependent networks and cascade faults are the main research contents. Multi-layer networks can abundantly represent the structural level of the system. Sergey V. Buldyrev et al. [25] based on this idea, established a two-layer reliability model for the coupling of the transmission network and power information network of the Italian power system, and analyzed the level. Joint failure effect. Cascading failure is the main form of fault propagation research. Dwivedi A. et al. [26-27] analyzed the brittleness of cascade failure caused by power system faults for the load capacity problem in the network model.

From the perspective of the overall research, the research object of networked reliability analysis gradually presents the trend of multi-layer heterogeneous networks integrated with software and hardware, and the analysis level is no longer limited to a single level of hardware devices or a certain function. In the software system alone, that is, the multi-level structure inside the demand research, related work such as: Zhao Haohua et al. [28] introduced the social network analysis method into the structural complexity analysis of the software network, and qualitatively analyzed the structure of the software network. In the study of the overall reliability of the system, it is necessary to address different levels of the internal, and has preliminary research and exploration.

4. Networked Modeling and Description of Air Traffic Control Automation System

According to the structure of the air traffic control automation system, a multi-layer network model suitable for system expansion and analysis of the integrated software and hardware network model should be constructed. Focus on the establishment of a networked model of air traffic control automation information system. The model is divided into two levels of software and hardware, describing the operation mode of the system in the heterogeneous network model.
When the node and the edge are defined hierarchically as shown in figure 2, the hardware device and the function software are respectively network nodes in the respective layers, and the properties and functional categories of each layer node are distinguished. For example, in the hardware layer, a pure hardware node and a hardware-software integrated node are distinguished; in the software layer, an operating system class node and an application system class node are distinguished. According to the coupling relationship between software and hardware, the affiliation relationship establishes the coupling edge between different layer nodes; according to the physical connection relationship between the hardware and software nodes in the same layer, the functional affiliation, the connection between the same layer nodes is established.

When defining the information flow, different information interaction behaviors exist between different nodes, and the direction and weight of the edge are set according to the instruction class relationship and the information interaction class relationship. For example, the node corresponding to the surveillance radar can acquire information and send information to other nodes. The forwarding node in the physical communication network is responsible for forwarding information, and the software operation node sends specific instructions to the application class node. There are also instruction class relationships and information interaction class relationships between different layer nodes. The instruction class relationship and the information interaction class relationship will respectively correspond to the one-way and two-way edge establishment. At the same time, according to the application characteristics and flow information of the interaction, the weights of the inter-layer coupling edges are set.

Describe the operation of the system in the model, based on the function settings of the above nodes and connected edges. In the model, the information is collected and generated by the end information collecting device (surveillance radar, ADS-B receiving device, etc.), and then sent to the neighboring device to the required processing server device; the information is transmitted across layers through the software and hardware coupling relationship. It is delivered to the terminal display node in the information network; at the same time, in the software network, information such as related instructions is transmitted to the hardware network through the layers to complete the final operations. Through the flow of information through generation, forwarding, processing, handover, and implementation, the operation of the system is finally expressed as various dynamic behaviors in the model, describing various modes of system operation.

5. Conclusion
The air traffic control automation system is the core technical equipment for ensuring the air traffic control. Assessing its reliability will help to grasp the system performance in practice and clarify the ability of the system to be extended and extended, which will help guide the selection and replacement of equipment. After clarifying the characteristics of hardware and software integration and complex
relationship of the ATC automation system, the reliability representation method suitable for evaluation is analyzed. Aiming at the traditional analysis methods and network analysis methods, the characteristics of system hardware and software, fault propagation characteristics and complex structure are compared and analyzed. Finally, the coupling modeling is introduced.

References
[1] Li D B, Liu Y M and Xu J W 2016 Risk assessment on the transition program for air traffic control automation system upgrade *Matec Web of Conferences* **63** 04041
[2] Hossain M M and Alam S 2017 A complex network approach towards modeling and analysis of the Australian Airport Network *Journal of Air Transport Management* **60** 1-9
[3] Cai K Q, Zhang J and Du W B 2012 Analysis of the Chinese air route network as a complex network *Chinese Physics B* **21** (2) 596-602
[4] Du W B, Liang B Y and Hong C 2017 Analysis of the Chinese provincial air transportation network *Physica A Statistical Mechanics & Its Applications* **465** 579-586
[5] Lordan O, Sallan J M and Simo P 2014 Robustness of the air transport network *Transportation Research Part E* **68** (68) 155-163
[6] Lordan O, Sallan J M and Simo P 2014 Study of the topology and robustness of airline route networks from the complex network approach: a survey and research agenda *Journal of Transport Geography* **37** 112-120
[7] Xiao M, Zhang J and Cai K 2016 ATCEM: a synthetic model for evaluating air traffic complexity *Journal of Advanced Transportation* **50** (3) 315-325
[8] Zhao J, Li D and Sanhedrai H 2016 Spatio-temporal propagation of cascading overload failures in spatially embedded networks *Nature Communications* **7** p 10094
[9] Du W B, Zhou X L and Lordan O 2016 Analysis of the Chinese airline network as multi-layer networks *Transportation Research Part E* **89** 108-116
[10] Tokadli G, Marzuoli A and Boidot E 2016 Resilience of the national airspace system: A case study of the fire at the Chicago ARTCC *Proceedings of Digital Avionics Systems Conference* *IEEE* 1-10
[11] Margellos K and Lygeros J 2013 Toward 4-D trajectory management in air traffic control: A study based on monte carlo simulation and reachability analysis *IEEE Transactions on Control Systems Technology* **21** (5) 1820-1833
[12] Li Q and Pham H 2017 NHPP software reliability model considering the uncertainty of operating environments with imperfect debugging and testing coverage *Applied Mathematical Modelling* **51**
[13] Zhao Y and Rozier K Y 2014 Probabilistic model checking for comparative analysis of automated air traffic control systems *2014* 690-695
[14] Andrews J W, Welch J D and Erzberger H 2005 Safety analysis for advanced separation concepts *Air Traffic Control Quarterly* **14** (1) 5-24
[15] Tu J, Cheng R and Tao Q 2015 Reliability analysis method of safety-critical avionics system based on dynamic fault tree under fuzzy uncertainty *Eksplotacja I Niezawodnosc-Maintenance and Reliability* **17** (1)156-163
[16] Vismari L F and Junior J B C 2011 A safety assessment methodology applied to CNS/ATM-based air traffic control system *Reliability Engineering & System Safety* **96** (7) 727-738
[17] Li D B, Liu Y M and Xu J W 2016 Risk assessment on the transition program for air traffic control automation system upgrade *Matec Web of Conference* **63** 04041
[18] Wang X and Liu W 2012 Research on air traffic control automatic system software reliability based on markov chain *Physics Procedia* **24** 1601-1606
[19] De Jong H H and Preti F 2008 A framework of indicators for the potential influence of air navigation services on air traffic safety in Europe *Journal of Risk & Reliability* **222** (1) 57-78
[20] Ball M O, Colbourn C J and Provan S J 1995 Network Reliability *Network Models* **673-762**
[21] Newman M E, Forrest S and Balthrop J 2002 Email networks and the spread of computer viruses Physical Review E Statistical Nonlinear & Soft Matter Physics 66 (3 Pt 2A) 035101
[22] Guimerà R, Mossa S and Turtschi A 2005 The worldwide air transportation network: Anomalous centrality, community structure, and cities’ global roles Proceedings of the National Academy of Sciences of the United States of America 102 (22) 7794-7799
[23] Albert R, Jeong H and Barabasi A L 2000 The Internet’s Achilles’ Heel: Error And Attack Tolerance Of Complex Networks (Amsterdam: Elsevier B.V.)
[24] Cuadra L, Salcedo-Sanz S and Ser J D 2015 A critical review of robustness in power grids using complex networks concepts Energies 8 (9) 9211-9265
[25] Buldyrev S V, Parshani R and Paul G 2010 Catastrophic cascade of failures in interdependent networks Nature 464 (7291) 1025-8
[26] Dwivedi A and Yu X 2013 A maximum-flow-based complex network approach for power system vulnerability analysis IEEE Transactions on Industrial Informatics 9 (1) 81-88
[27] Dwivedi A, Yu X and Sokolowski P 2009 Identifying vulnerable lines in a power network using complex network theory Proceedings of IEEE International Symposium on Industrial Electronic 18-23
[28] Zhang H H, Feng W J and Wu L J 2010 The static structural complexity metrics for large-scale software system Applied Mechanics & Material 44-47 3548-3552