Article citation info:
TU J, CHENG R, TAO Q. Reliability Analysis Method of safety-critical avionics system based on Dynamic Fault Tree under Fuzzy Uncertainty. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2015; 17 (1): 156–163.

Jiliang TU
Ruofa CHENG
Qiuxiang TAO

RELIABILITY ANALYSIS METHOD OF SAFETY-CRITICAL AVIONICS SYSTEM BASED ON DYNAMIC FAULT TREE UNDER FUZZY UNCERTAINTY

SPOSÓB ANALIZY NIEZAWODNOŚCI KRYTYCZNYCH DLA BEZPIECZEŃSTWA SYSTEMÓW ELEKTRONIKI LOTNICZEJ OPARTY NA METODZIE DYNAMICZNEGO DRZEWA BŁĘDÓW W WARUNKACH ROZMYTEJ NIEPEWNOŚCI

A safety-critical avionics system has to qualify the performance related requirements and the safety-related requirements simultaneously. This paper presents a comprehensive study on the reliability analysis method for safety-critical avionics system by using dynamic fault tree approach based on Markov chain. The reliability models were constructed applying dynamic fault tree (DFT) modeling method according to deeply analysis of the typical failure modes, causes and influence of the safety-critical avionics system by considering the aspect of repairable feature and redundancy. Taking into account the both failure phenomenon of safety-critical avionics system and many uncertainties exist in the fault status and fault reasons, fuzzy sets theory is introduced into dynamic fault tree method. Specifically, it adopts expert elicitation and fuzzy set theory to evaluate the failure rates of the basic events for safety-critical avionics system. Furthermore, the fuzzy dynamic fault tree analysis method for safety-critical avionics system based on the consecutive parameter Markov chain is proposed. The modularization design was utilized to divide the dynamic fault trees into static and dynamic sub-trees. The static tree was solved by binary decision diagram (BDD) and the dynamic tree was solved by Markov chain method. The results show that the proposed method is more flexible and adaptive than conventional fault tree analysis for fault diagnosis and reliability estimation of safety-critical avionics system.

Keywords: *safety-critical avionics system, dynamic fault tree, Markov chain, Fuzzy Uncertainty.*

Krytyczne dla bezpieczeństwa układy elektroniki lotniczej (awioniki) muszą jednocześnie spełniać zarówno wymogi eksploatacyjne jak i wymagania związane z bezpieczeństwem. W niniejszej pracy przedstawiono kompleksowe opracowanie dotyczące metody analizy niezawodności krytycznych dla bezpieczeństwa systemów awioniki wykorzystującej opartą na łańcuchu Markowa metodę dynamicznego drzewa błędów. Modele niezawodności konstruowano z zastosowaniem metody dynamicznego drzewa błędów zgodnie z przeprowadzoną dokładną analizą typowych przyczyn uszkodzeń oraz czynników wpływających na systemy elektroniki lotniczej, z uwzględnieniem aspektu naprawialności i nadmiarowości. Biorąc pod uwagę, że zarówno ze zjawiskiem uszkodzenia krytycznego dla bezpieczeństwa systemu awioniki jak i ze stanem awarii i przyczynami błędów wiąże się wiele niepewności, metodę dynamicznego drzewa błędów poszerzono o teorię zbiorów rozmytych. W szczególności, zaproponowana metoda wykorzystuje ocenę ekspercką oraz teorię zbiorów rozmytych do oceny intensywności uszkodzeń dla podstawowych zdarzeń zachodzących w krytycznych dla bezpieczeństwa systemach elektroniki lotniczej. Ponadto zaproponowano metodę analizy krytycznych dla bezpieczeństwa systemów awioniki wykorzystującą teorię rozmytych dynamicznych drzew błędów opartą na markowowskim łańcuchu następujących po sobie parametrów. Budowę modułową wykorzystano do podziału dynamicznych drzew błędów na poddrzewa statyczne i dynamiczne. Drzewa statyczne rozwiązywano za pomocą binarnego schematu decyzyjnego (BDD) a drzewa dynamiczne – metodą łańcuchów Markowa. Wyniki pokazują, że proponowana metoda diagnozowania błędów i oceny niezawodności krytycznych dla bezpieczeństwa systemów elektroniki lotniczej jest bardziej elastyczna i łatwiejsza do adaptacji niż konwencjonalna analiza drzewa błędów.

Słowa kluczowe: *krytyczne dla bezpieczeństwa układy elektroniki lotniczej, dynamiczne drzewo błędów, łańcuch Markowa, niepewność rozmyta.*

1. Introduction

Over the past several decades, reliability has been a critical issue in many embedded applications in aerospace, aircraft, road vehicles, railways, nuclear systems, and implanted devices because the failure of a safety-critical system may cause catastrophic damage or loss of life [19].With the increased concerns on reliability in safety-critical system, the requirements to improve system efficiency and reliability have become even more stringent. Modern safety-critical systems for avionics(SCAS) utilize not only an increasing amount of sophisticated software but also a software embedded hardware to process the large amount of data needed to control avionic systems and monitor their current status [4, 15]. Avionics safety is considered at the system level and has no important implications when considered separately with regard to software and hardware [14]. For fast technology innovation, the performance of key equipment in the safety-critical systems for avionics has been greatly improved with the wide application of high technology on one hand, but, on the other hand, its complexity of technology and structure increasing significantly raise challenges in system reliability analysis and evaluation. These challenges are displayed as follows [6, 16, 22]. (1) Lack of sufficient fault data: Obtain-

ing enough failure data is time-consuming, and may be impossible for highly reliable systems. Some component state of safety-critical systems for avionics is get worsening rather than instantaneous failure in the early life cycle, so it is very difficult to obtain mass original parameters (such as the failure rate, repair rate) of the equipment which need lots of case studies in practice due to some reasons. One reason is the imprecise knowledge in an early stage of new product design. The other factor is the changes of the environmental conditions which may cause that the historical fault data can not represent the future failure behaviors. (2) Failure dependency of components: safety-critical systems for avionics adopts many redundancy units and fault tolerance techniques to improve its reliability, the failure or malfunction of software can be due to interactions with hardware. Additionally, software and hardware domains have mutual influence on each other during aviation system development and the system equipment can not carry out the necessary maintenance during operation. So, the behaviors of components in the system and their interactions, such as failure priority, sequentially dependent failures, functional dependent failures, and dynamic redundancy management, should be taken into consideration. (3) High levels of fuzzy uncertainty: it is usually operated in the harsh environment for a long-term and is greatly affected by the measurement error, human, and operational malfunctions that may lead to hazardous incidents of safety-critical systems for avionics. It is difficult to give a precise estimation of reliability characteristic values, especially for the system with very low failure rates or new parts, For example, it is common for experts to say that 'there is a low possibility that the component A fails' rather than the probability of failure of the component A is '1.2E−5'.These terms can be quantified with the use of membership functions of the corresponding fuzzy sets.

Fault tree analysis (FTA) is a systematic approach to estimate safety and reliability of a complex system, qualitatively as well as quantitatively. It is a logical and diagrammatic method for evaluating the possibility of an accident resulting from combinations of failure events. However, in traditional FTA, the failure probabilities of the basic events (BEs) are expressed by exact values, has been found to be inadequate to deal with these challenges mentioned above. And this makes quantitative analysis of a fault tree of a system questionable by conventional methods [3]. In order to handle subjective factors and nonlinear characteristics, inherent in the importance identification for a fault tree in the reliability analysis, many conscientious researchers have taken the fuzzy uncertain situations into consideration. Fuzzy set theory has been proven to be effective on solving problems where there are no sharp boundaries and precise values, while it is also efficient. The pioneering work on fuzzy fault tree analysis (fuzzy FTA) belongs to Tanaka et al. [4–5], who treated imprecise probabilities of basic events as trapezoidal fuzzy numbers and defined an index function analogous to the importance measure for ranking the effectiveness of each basic event. Since then, there have been a number of approaches where the technology of fuzzy sets was used to evaluate system reliability. For example, Ding et al. proposed a membership function of fuzzy numbers to represent a sub-system state to assess the reliability of multi-state weighted k-out-of-n systems [22].In Gargama and Chaturvedi, the membership functions of fuzzy numbers are used to represent linguistic variables and a defuzzification technique has been used to generate a crisp score for prioritize failure modes to overcome the limitation of the traditional FMEA[5,15].However, these approaches use the static fault tree to model the system fault behaviors and cannot cope with challenge (2). Dynamic fault tree analysis has been introduced [1, 6, 7, 13], which takes into account not only the combination of failure events but also the order in which they occur. Rongxing Duan [17] analysed the dependability of data communication systems with on-demand and active failure modes using dynamic fault tree and solved it to get some reliability results by equivalent Bayesian network (BN) model. However, this is an approximate solution and requires huge memory resources to obtain the joint probability distribution accurately. Furthermore, the reliability parameters by dynamic fault tree are mapped into equivalent BN calculation is complex. Some innovative algorithm has been introduced to reduce the dimension of conditional probability tables by an order of magnitude. However, this method cannot perform probability updating. Montaniet et al. proposed a translation of the dynamic fault tree into a dynamic Bayesian network (DBN) [16]. The DBN model is essentially applicable to Markov processes and the result of the calculation gives the approximated probabilities, but the method can not solve the differential equation. In order to solve a larger dynamic fault tree, a Markov state transition method was proposed for the reliability analysis of dynamic fault tree in [18]. They converted dynamic logic gates to Markov chain and calculated the reliability results by a standard formula of DFT based on the consecutive parameter Markov chain [21]. Markov state transition method can clearly describe the dynamic characteristics of system reliability and describe each state change process in reliability analysis under fault condition [2].

On the basis of the discussed notions, we attempted to conceptualize and articulate the design process of safety-Critical avionics system for achieving both performance-and reliability-related requirements by utilizing the fuzzy set and dynamic fault tree. A reliability analysis method is proposed in this paper, it pays special attention to meet the above three challenges. We adopt expert elicitation and fuzzy set theory to deal with insufficient fault data and uncertainty problem by treating the failure rates as fuzzy numbers without the need to engage basic event failure probability distribution. The reliability models were constructed applying dynamic fault tree (DFT) modeling method according to deeply analysis the typical failure modes, causes and influence of the safety-Critical avionics system. In addition, the modularization design was utilized to divide the dynamic fault trees into static and dynamic sub-trees. The dynamic fault tree model can capture the dynamic behaviors of safety-Critical avionics system failure mechanisms. The static tree was solved with binary decision diagram (BDD) and the dynamic tree was solved with Markov chain method in order to avoid the aforementioned problems.

The purpose of this study is to involve dynamic analysis into the traditional static methods using fuzzy set and dynamic fault tree for the SCAS reliability analysis, as well make Markov models more efficient for the users. After the introduction, the rest of the paper is organized as follows. Section 2 provides a brief introduction on SCAS and its dynamic fault tree model. Section 3 describes estimation of failure rates for the basic events. Section 4 presents a novel dynamic fault tree solution in which the modularization design was utilized to divide the dynamic fault trees into static and dynamic sub-trees. The outcomes of the research and future research recommendations are presented in the final section.

2. Construction of SCAS Dynamic fault tree

SCAS is a complex system consists of many key components, such as Vehicle Management system (VMS), Crew Station (CS), Mission&System Management (MSM), Local Path Generation (LPG), Scene & Obstacle Following (SOF), Among them VMS are responsible for the aircraft fuselage control. In addition, it also performs the most important task such as common System management& control. CS can provide necessary flight information for pilot, MSM implements resource sharing by the users of a real-time computer system. In order to improve the reliability of SCAS, it adopts redundancy technique to ensure higher reliability. For example, the hardware redundancy technique is adopted in designing VMS, CS, MSM, LPG and SOF. High coupling degree together with complicated logic relationships exists between these modules. So, the behaviors of components in these modules and their interactions, such as failure priority, sequentially dependent failures, functional-dependent failures, and dynamic

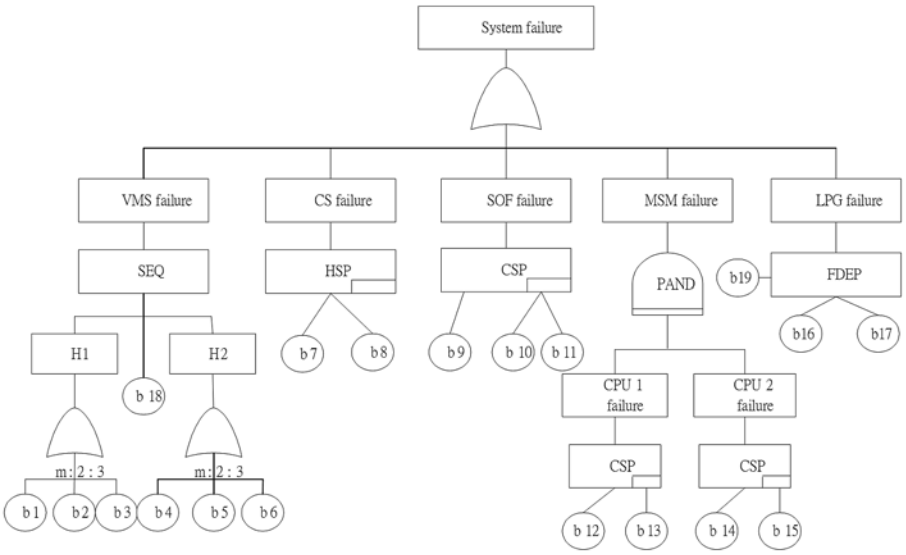

Fig. 1. DFT of SCAS

redundancy management, should be taken into consideration. Obviously, traditional static fault tree is unsuitable to model these dynamic fault behaviors. So, we use the dynamic fault tree model to capture the dynamic behavior of system failure mechanisms such as sequence-dependent events, spares and dynamic redundancy management, and priorities of failure events. A DFT is a stochastic technique for the reliability analysis, suitable to model systems characterized by time-dependent logics. By adding new gates to static (regular) Fault Trees, Dynamic Fault Trees aim to take into account dependencies among events (which typically exist in systems with spare components).

By analysis on the structure and principle of avionics system, we can found that (1) SCAS consists of five function modules, shown as "or" gate, for each module, when a hardware failure or a main software and backup software fault, then the system fault is announced. (2) There are two processing unit in the VMS and MSM subsystem, especially , in the VMS , H1 is a master component, another group of H2 as a spare unit, each set of equipment containing 3 monomer, if 3 channel main system components in the 2 failure, the main system fault is announced; in MSM subsystem, It simply detects the failure order and fails just in one case (failure occurs if CPU1 fails before CPU2,but CPU2 may fail before CPU1 without producing a failure). (3)The CS is 2:1 Parallel structure subsystem and SOF is 3:1 cold spare module, Only after all the equipment failure, then announced the subsystem fault;(4) in the LPG module, b19 is the path interface unit, b16 and b17 delegate 2 channel in path generation subsystem, only b19 or b16,b17 all failure, the LPG subsystem become failure. Based on the above analysis, the control failure of avionic system is adopt as the top event, then the DFT of SCAS is established in Figure 1.

3. A Basic event failure possibility evaluation

The motivation of this section is how to obtain basic event failure probabilities of SCAS when basic events do not have probability distributions of their lifetime to failures. Therefore, we develop a fuzzy reliability algorithm to assess basic event failure probabilities through qualitative linguistic value processing without the need to engage basic event failure probability distribution.

3.1. Linguistic value and membership function

A basic event failure possibility distribution is a set of qualitative linguistic terms used to scale the failure likelihood of the basic events of fault trees of SCAS. Based on the range of the component failure data collected from avionic system operating experiences. In this paper, the component failure rate is defined by seven linguistic values, that is, very high(VH), high(H), reasonably high(RH),moderate(M), reasonably low(RL), low(L), and very low(VL).For example, very low failure possibility can be used to represent components which are rigid and very unlikely to be failure even once. This set of qualitative linguistic values(UH) can be expressed as[8]:

$$UH = \{h_i \,|\, i = 1,2,...,7\} = \{VL, L, RL, M, RH, H, VH\}$$

The fuzzy sets represent qualitative basic event failure possibilities defined in the [0, 1] universe of discourse. Seven membership functions of triangular fuzzy numbers have been developed in Purba et al. [9] to represent those seven basic event failure possibilities, the shapes of the membership functions to mathematically represent linguistic variables are shown in Figure 2. These membership functions are mathematically given in follows:

$$\mu_{VL}(x) = (0.00, 0.04, 0.08), \mu_{L}(x) = (0.07, 0.13, 0.19), \mu_{RL}(x) = (0.17, 0.27, 0.37),$$
$$\mu_{M}(x) = (0.35, 0.50, 0.65), \mu_{RH}(x) = (0.63, 0.73, 0.83), \mu_{H}(x) = (0.81, 0.87, 0.93),$$
$$\mu_{VH}(x) = (0.92, 0.96, 1.00)$$

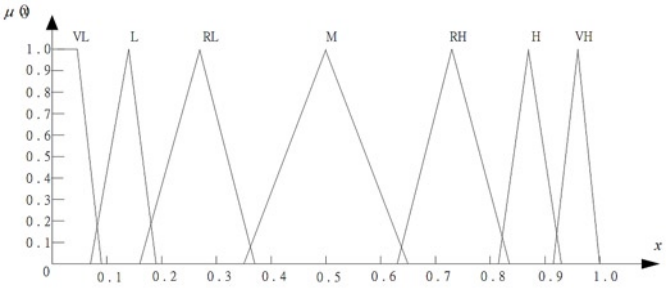

Fig. 2. The event membership functions

3.2. Fuzzification module and defuzzification module

In real-world applications, the avionic experts may have different levels of expertise, background and working experience. Hence, they may demonstrate different perceptions about the same events and subjectively provide different assessment. To eliminate bias coming from an expert and reflect their differences of assessment, different justification weights from 0 to 1 may be assigned to every expert. So, it is necessary to combine or aggregate these opinions into a single one. There are many methods to aggregate fuzzy numbers. In this paper, we adopt simple linear weighting as formula (1), which consider the weight of individual value, can be implemented in this method as well [9].

$$M_B = \begin{bmatrix} \mu_{b1}(x) \\ \mu_{b2}(x) \\ ... \\ \mu_{bl}(x) \end{bmatrix} = \begin{bmatrix} \mu_{UH}(x)^{(e_1 b_1)}, \mu_{UH}(x)^{(e_2 b_1)}, ..., \mu_{UH}(x)^{(e_n b_1)} \\ \mu_{UH}(x)^{(e_1 b_2)}, \mu_{UH}(x)^{(e_2 b_2)}, ..., \mu_{UH}(x)^{(e_n b_n)} \\ ..... \\ \mu_{UH}(x)^{(e_1 b_l)}, \mu_{UH}(x)^{(e_2 b_l)}, ..., \mu_{UH}(x)^{(e_n b_l)} \end{bmatrix} \bullet \begin{bmatrix} w_1 \\ w_2 \\ ... \\ w_n \end{bmatrix} \quad (1)$$

where $\mu_{bl}(x)$ is the final membership function for basic event b_l, $\mu_{UH}(x)^{(e_i b_j)}$ is the ith membership function given by expert e_i to

basic event b_j, w_i is the weight given to expert e_i, n is the number of experts, and l is the number of basic events.

A failure possibility score (FPS) is a single numerical value, which is decoded from a membership function, to represent the experts' belief of the most likely score indicating that an event may occur. This step is usually called defuzzification. There are several defuzzification techniques [10]: area defuzzification technique, the left and right fuzzy ranking defuzzification technique, the centroid defuzzification technique, the area between the centroid point and the original point defuzzification technique, and the centroid based Euclidean distance defuzzification technique. Among the diversity of the methods, an area defuzzification technique(ADT) is used to map the fuzzy numbers into FPS because it has the lowest relative errors and has the closest match with the real data. More specifically, the method returns a numeric value computed as follows [10]:

$$FPS = d(\mu_{bi}(x)) = x_1 y_0 + \int_{x_2}^{d} \mu_{bi}^{R}(x) \tag{2}$$

where y_0 is the centroid point of the real fuzzy number $\mu_{bl}(x)$ on the vertical axis, x1 is the intersection point between the line y_0 and the left membership function $\mu_{bl}^{L}(x)$ on the horizontal axis, and x2 is the intersection point between the line y_0 and the right membership function $\mu_{bl}^{R}(x)$ on the horizontal axis. If it is a triangular fuzzy number $\mu_{bi}(x) = (a,b,c)$, then its FPS is calculated using formula (3):

$$FPS = \frac{1}{18}(4a + b + c) \tag{3}$$

3.3. Basic event failure probability generation

The event fuzzy possibility score is then converted into the corresponding fuzzy failure rate, which is similar to the failure rate. Based on the logarithmic function proposed by Onisawa [19], which utilizes the concept of error possibility and likely fault rate, the fuzzy failure rate(FFR) can be obtained by (4):

$$FFR = \begin{cases} \dfrac{1}{10^{2.301*[(1-FPS)/FPS]^{1/3}}}, FPS \neq 0 \\ 0, \quad FPS = 0 \end{cases} \tag{4}$$

Table 1. Basic events' FPS and FFR

Basic events	Final membership functions	FPS	FFR
b1	(0.43, 0.57, 0.70)	0.165952	1.14E−4
b2	(0.43, 0.57, 0.70)	0.165952	1.14E−4
b3	(0.47, 0.60, 0.73)	0.178095	1.48E−4
b4	(0.43, 0.57, 0.70)	0.165952	1.14E−4
b5	(0.43, 0.57, 0.70)	0.165952	1.14E−4
b6	(0.43, 0.57, 0.70)	0.165952	1.14E−4
b7	(0.92, 0.96, 1.00)	0.313333	1.03E−03
b8	(0.92, 0.96, 1.00)	0.313333	1.03E−03
b9	(0.94,0.97,1.00)	0.318333	1.24 E−03
b10	(0.94,0.97,1.00)	0.318333	1.24 E−03
b11	(0.92, 0.96, 1.00)	0.313333	1.03E−03
b12	(0.55, 0.66, 0.78)	0.20238	2.32E−4
b13	(0.58,0.68,0.79)	0.2106	2.6E−4
b14	(0.43, 0.57, 0.70)	0.165952	1.14E−4
b15	(0.47, 0.60, 0.73)	0.178095	1.48E−4
b16	(0.22, 0.34, 0.45)	0.092857	1.21E−5
b17	(0.18, 0.28, 0.38)	0.077381	5.54E−6
b18	(0.32, 0.47, 0.61)	0.131905	4.87E−5
b19	(0.14, 0.23, 0.32)	0.061905	2.02E−6

Table 1 shows the fuzzy failure rates of the basic events for the SCAS.

4. Reliability analysis method for SCAS

With the help of dynamic gates, sequence-dependent failure behavior of SCAS can be specified using dynamic FTs that are compact and easily understood. With the increase in the number of basic elements, there is problem state space explosion [12]. To reduce state space and minimize the computational time, an improved modularization method was utilized to divide the dynamic fault trees into static and dynamic sub-trees in this paper [11]. The static tree was solved with binary decision diagram (BDD) and the dynamic tree was solved with Markov chain method, the reliability parameters of the global integrated system is calculated at last.

4.1. Analysis of static fault tree based on BDD

In the Figure 1, SCAS is comprised of five components. It is obviously that the relation five subsystem is OR gates which also combine input events, but any one is sufficient to cause the output, so we can calculate the reliability degree by use the BDD (binary decision diagram) method. BDD is a kind of simplified Boolean expression method in which has two types of endpoints, respectively is 0 and 1. In BDD, 0 represented no failure state, 1 representative failure state. Figure 3 shows the conversion of Static fault tree of SCAS into BDD, among them, S1 denote VMS subsystem, S2 denote CS subsystem, S3 denote SOF subsystem, S4 denote MSM, S5 denote LPG subsystem.

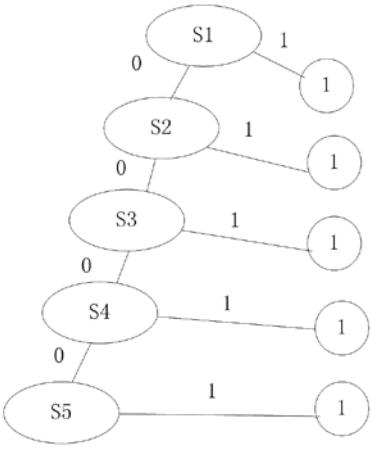

Fig. 3. BDD decomposition process of SCAS

So the structure function of fault tree for the SCAS failure accident can be obtained as follows:

$$\Phi(S) = S_1 \cup S_2\overline{S_1} \cup S_3\overline{S_2}\,\overline{S_1} \cup S_4\overline{S_3}\,\overline{S_2}\,\overline{S_1} \cup S_5\overline{S_4}\,\overline{S_3}\,\overline{S_2}\,\overline{S_1} = S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5 \tag{5}$$

When $\Phi(S) = 1$, it is denote the system failed , when $\Phi(S) = 0$ that the system failure did not occur. The system product of structure func-

tion is disjoint after BDD decomposition, so the FTA probability calculation is very simple. The probability of system failure is:

$$P(X_s) = P(\Phi(S=1) = P(S_1) + P(S_2\overline{S_1}) + P(S_3\overline{S_2S_1}) + P(S_4\overline{S_3S_2S_1}) + P(S_5\overline{S_4S_3S_2S_1}) \quad (6)$$

4.2. Analysis of dynamic fault tree based on Markov chain

Dynamic fault tree (DFT) of SCAS main introduces four basic (dynamic) gates: the priority AND (PAND), the sequence enforcing (SEQ), the standby or spare (SPARE), and the functional dependency (FDEP). SPARE gates are dynamic gates modeling one or more principal components that can be substituted by one or more backups (spares) varing with the state of spare gate, it can divide into cool spare gate, hot spare gate, warm spare gate. The following example illustrates how the five functions of this system subsystem is transformed into a Markov chain, the detailed algorithm of converting a fault tree into a Markov model was proposed in [2].

4.2.1. Mapping Dynamic Fault Tree into Markov chain

In subsystem of VMS, A SEQ gate forces its inputs to fail in a particular order: when a SEQ gate is found, it never happens that the failure sequence takes place in different orders. While the SEQ gate allows the events to occur only by pre-assigned order and states that a different failure sequence can never take place. Suppose the failure rate of H1 is λ_1, H2 is λ_2, b18 is λ_{b18}, the Markov state transfer chain of VMS subsystem is shown in Figure 4. It is assumed that each device failure events is independent in this paper, the failure probability of VMS subsystem is $P(VMS) = P(H_1)P(b_{18})P(H_2)$.

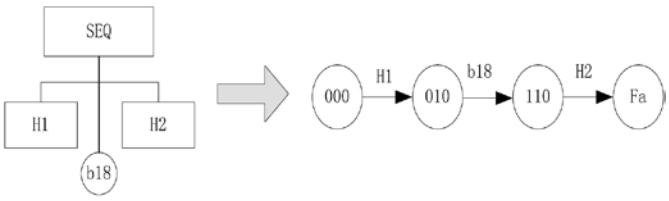

Fig. 4. The Markov chain of SEQ gate

In subsystem of CS, spare gate will have one active component (say b7) and remaining spare components (say b8). When there is no demand, it will be in standby state or may be in failed state due to on-shelf failure. It can also be unavailable due to test or maintenance state as per the scheduled activity when there is a demand for it. On the princple of hot spare gate, we can get the Markov chain of CS subsystem in Figure 5. The Failure probability of VMS subsystem is: $P(CS) = 2P(b_7)P(b_8)$.

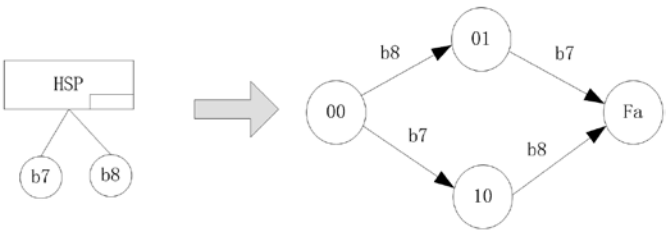

Fig. 5. The Markov chain of HSP gate

In subsystem of SOF, the process of analysis is similar to subsystem VSM. In Figure 6,but because of the failure rate of cold spare gate is 0, and each section of chain transfer in Markov state points on the self transition probability is different. The failure probability of SOF subsystem is $P(SOF) = P(b_9)P(b_{10})P(b_{11})$.

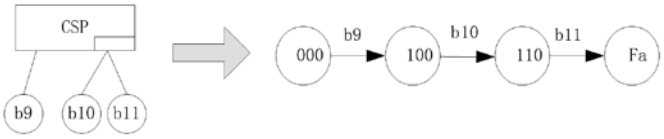

Fig. 6. The Markov chain of CSP gate

In subsystem of MSM, consider PAND gate having two active components, CPU1and CPU2. Active component is the one which is in working condition during normal operation of the system. Active components can be either in success state or failure state. The PAND gate reaches a failure state if all of its input components have failed in a pre-assigned order (usually from left to right).When the first component failed followed by the second component, it is identified as failure and simultaneous downtime is taken into account. Especially, both the components have failed simultaneously but second component has failed first hence it is not considered as failure. The Markov chain of MSM As shown in Figure 7.The failure probability of SOF subsystem is:

$$P(MSM) = 3P(b_{12})P(b_{13})P(b_{14})P(b_{15})$$

In subsystem of LPG, The FDEP gate's output is a 'dummy' output as it is not taken into account during the calculation of the system's failure probability. When the trigger event (b19) occurs, it will lead to the occurrence of the dependent event (say b16 and b17) associated with the gate. During the down time of the trigger event, the dependent events will be virtually in failed state though they are functioning. we can get the markov chain of LPG subsystem in Figure 8. The failure probability of VMS subsystem can be derived as:

$$P(LPG) = P(b_{19}) + 2P(b_{16})P(b_{17}) + P(b_{16})P(b_{19}) + P(b_{17})P(b_{19})$$

In the above diagram, 0 represents the bottom events is normal, and 1 represents the bottom event failure. Fa represent the system failure state, the circles represent the state of a system.

4.2.2. Reliability calculation of *n* order Markov chain

For the complicated system state more, can imagine will transfer graph is decomposed into a plurality of state transfer chain state, according to the different chain length, respectively, deduces the formula. In the application of these formulas only apply, and then integrated for each chain results, we can get the reliability index of the whole system. The nth order Markov chain transfer process is illustrated as Figure 9.

The core of Markov method is to decide the state transferring probability matrix. Suppose each equipment state transfer rate obeys exponential distribution. If the process is a random continuous state space, then state i and state j fixed on arbitrary, so the transfer rate from state i to state j as follows:

$$q_{ij} = p_{ij}'(0) = \lim_{\Delta t \to 0} \frac{p_{ij}(\Delta t) - p_{ij}(0)}{\Delta t} = \lim_{\Delta t \to 0} \frac{p_{ij}(\Delta t) - \delta_{ij}}{\Delta t}, \delta_{ij} = \lim_{t \to 0} p_{ij}(t) = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases} \quad (7)$$

Then the transfer rate matrix A which the chain length with N with respect to the state transfer process as follows:

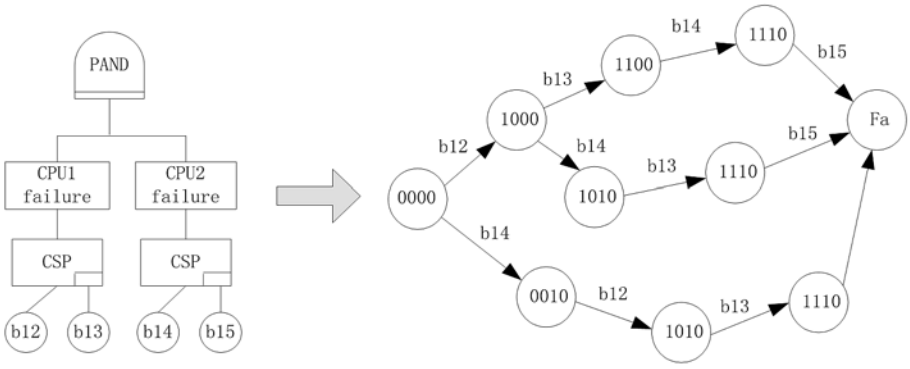

Fig. 7. The Markov chain of PAND gate

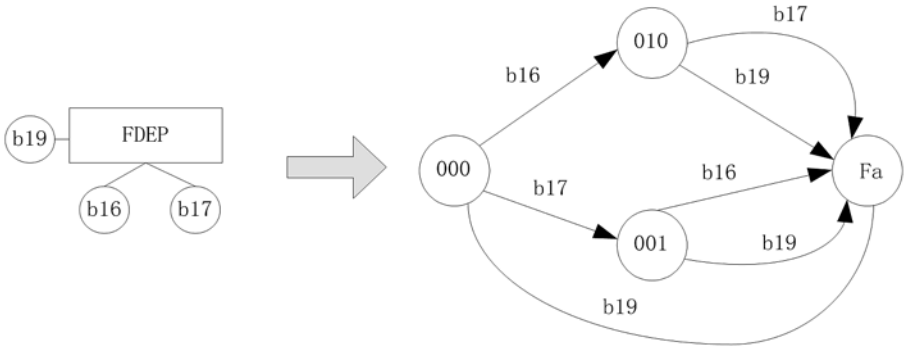

Fig. 8. The Markov chain of FDEP gate

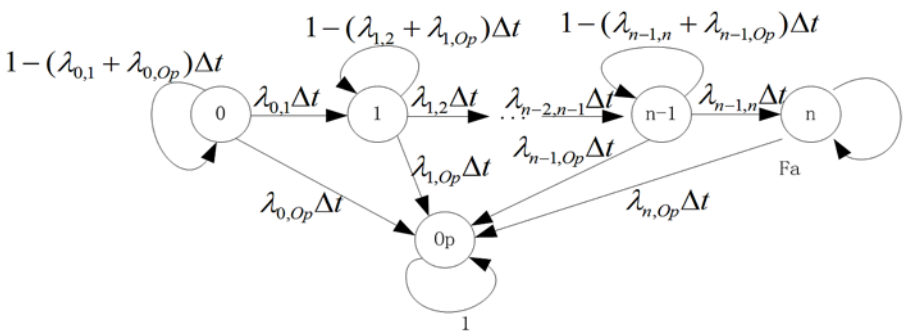

Fig. 9. The nth order Markov chain of transfer process

$$A=\begin{pmatrix} -\lambda_{0,1}-\lambda_{0,Op} & \lambda_{0,1} & 0 & 0 & \dots & 0 & 0 & \lambda_{0,Op} \\ 0 & -\lambda_{1,2} & -\lambda_{1,Op} & \lambda_{1,2} & 0 & \dots & 0 & \lambda_{1,Op} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & -\lambda_{n-1,n}-\lambda_{n-1,Op} & \lambda_{n-1,n} & \lambda_{n-1,Op} \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix}$$

According to theory of Markov processes, the state transition probability matrix equation is defined as:

$$\begin{cases} P' = AP \\ P(0) = E \end{cases},$$

P is the Column vector of each state probability, P' is the Derivatives of the Column vector P.

For solving the matrix equation, Laplace solution is be used in this paper. Suppose $L[P'(t)] = L[P(t)A]$,then $sP(s) - P(0) = P(s)A$, $P(s) = P(0)[sE - A]^{-1} = [sE - A]^{-1}$. Both sides of equation to take the inverse transform and according to the Heaviside expansion, then the failure probability P(t) of the chain can derived as:

$$P(t) = \prod_{i=1}^{n} \lambda_{i-1,i} \left(\prod_{i=1}^{n} \frac{1}{\lambda_{i-1,i}} - \sum_{i=1}^{n} \frac{e^{-\lambda_{i-1,i}t}}{\lambda_{i-1,i} \prod\limits_{\substack{j=1 \\ j \neq i}}^{n} (\lambda_{j-1,j} - \lambda_{i-1,i})} \right) \tag{8}$$

According to the dynamic fault tree shown in Figure 1 and the basic failure data shown in Table 1, we can map the dynamic fault tree into a Markov chain with different chain length using the proposed method in this paper. Once the structure of DFT is known and all the probability tables are filled, it is straight forward to compute the failure probability of each subsystem in SCAS using the formula 8 during the work time. Then the dynamic fault tree failure probability can be obtained by adding each chain probability. Table 2 shows the unreliability of each subsystem for SCAS in the 1000 hours time using proposed methods for the dynamic fault tree solution.

According to Table 2, the LPG subsystem has the maximum Failure probability, which means that they are the most unreliable components. So, when SCAS fails, we should diagnose them firstly to locate the failure of SCAS Furthermore, proper measures should be allocated for these components to improve their reliability at the stage of product design in order to decrease the failure probability of SCAS. For example, high reliability components or redundancy structure could be adopted.

Table 2. Failure probability of different subsystem and the whole system

Subsystem name	Failure probability
VMS	8.7482E-10
CS	3.743e-8
SOF	9.4364e-13
MSM	7.5324E-5
LPG	0.1229
SCAS	0.12298

5. Conclusions

This paper introduces a method for reliability assessment of complex avionics system. In order to simplify the complex reliability problems, conventional approaches make many assumptions to make it to a simple mathematical model. In real-world applications, when

quantitative historical failure data are scarce or are not available at all, linguistic values are often used by decision makers to assess system reliability. This study has proposed a fuzzy reliability algorithm to handle qualitative data in order to assess basic events of fault trees through qualitative data processing. Those data are described in terms of failure possibilities and represented by fuzzy numbers, to characterize basic event failure likelihood. In terms of the challenge of failure dependency, we use a dynamic fault tree to describe the dynamical behavior of avionic wireless communication system failure mechanisms. Furthermore, the modularization design was utilized to divide the dynamic fault trees into static and dynamic sub-tree in order to avoid the state space explosion problem and huge memory resources. In this work all the basic dynamic gates (PAND, SEQ, SPARE, and FDEP) have been implemented with Markov chain approach. By using the formula of dynamic reliability of fault tree is given in this paper, the process can avoid directly solving differential equations, the convenience brought to the engineering application of dynamic fault tree.

As it can be seen from the result, the LPG sub-system has the most contribution to the top event probability. So, we should improve their reliability at the stage of product design in order to decrease the failure probability of SCAS by several approaches. The proposed method makes use of the advantages of the dynamic fault tree for model, fuzzy set theory for handling uncertainty, and Markov chain for state clearly ability, which is especially suitable for reliability evaluation and fault diagnosis of the Safety-Critical avionics System.

In the future work, we will focus on the common cause failures to optimize the dynamic fault tree model, more experimentation using various uncertainly data sets coming from other fault tree analysis would be advantageous to gain a better assessment of the performance of the model and the linguistic analysis. Furthermore, the underlying model can be further refined and enriched by admitting various classes of fuzzy sets (membership functions).

Acknowledgments

Authors gratefully acknowledge the financial support provided by the National Natural Science Foundation of China (Grant No. 51167013) and research fund for the doctoral program of higher education of NCHU, Jiang Xi, China (Project No.EA201304348). At the same time, the authors sincerely thank the reviewers for their insightful comments.

References

1. Antoine B. Rauzy, Sequence Algebra. Sequence decision diagrams and dynamic fault trees. Reliability Engineering and System Safety 2011; 96(2): 785–792.
2. Christopher C. Drovandi, Anthony N. Pettitt, Robert D. Henderson. Marginal reversible jump Markov chain Monte Carlo with application to motor unit number estimation. Computational Statistics & Data Analysis 2014; 72(3): 128-146.
3. Daqing Wang, Peng Zhang, Liqiong Chen. Fuzzy fault tree analysis for fire and explosion of crude oil tanks. Journal of Loss Prevention in the Process Industries 2013; 26(1): 1390-1398.
4. Jafarian E, Rezvani MA. Application of fuzzy fault tree analysis for evaluation of railway safety risks: an evaluation of root causes for passenger train derailment. Proceedings of the Institution of Mechanical Engineers F: Journal of Rail and Rapid Transit 2012; 226(1): 14-25.
5. Gargama, H. Chaturvedi, S.K.Criticality Assessment models for failure mode effects and criticality analysis using fuzzy logic. IEEE Transactions on Reliability 2011; 60(1): 102-110.
6. HUANG Hongzhong, TONG Xin, ZUO Mingjian. Posbist fault tree analysis of coherent systems. Reliability Engineering and System Safety 2004; 84(2): 141-148.
7. J. B. Dugan, S. J. Bavuso, and M. A. Boyd. Dynamic fault-tree models for fault-tolerant computer systems. IEEE Transactions on Reliability 1992; 41(3): 363-377.
8. Julwan Hendry Purba. A fuzzy-based reliability approach to evaluate basic events of fault tree analysis for nuclear power plant probabilistic safety assessment. Annals of Nuclear Energy 2014; 70(2): 28-30.
9. Julwan Hendry Purba, Jie Lu, Guangquan Zhang. A fuzzy reliability assessment of basic events of fault trees through qualitative data processing. Fuzzy Sets and Systems 2014; 243(1): 50–69.
10. J.H. Purba, J. Lu, G. Zhang, and D. Ruan. An area defuzzification technique to assess nuclear event reliability data from failure possibilities. International Journal of Computational Intelligence and Applications 2012; 11(4): 1-16.
11. K.DurgaRao, V.Gopika, V.V.S.SanyasiRao. Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. Reliability Engineering and System Safety 2009; 94(1): 872-883.
12. L. Meshkat, J. B. Dugan, and J. D. Andrews. Dependability analysis of systems with on-demand and active failure modes using dynamic fault trees. IEEE Transactions on Reliability 2002; 51(2): 240-251, 2002.
13. LI Yanfeng, HUANG Hongzhong, LIU Yu. A new fault tree analysis method: Fuzzy dynamic fault tree analysis. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2012; 14(3): 208-214.
14. Mohsen Naderpour, Jie Lu, Guangquan Zhang. An abnormal situation modeling method to assist operators in safety-critical systems. Reliability Engineering and System Safety 2014; 119(2): 67-89.
15. Ningcong Xiao, Hong-Zhong Huang, Yanfeng Li. Multiple failure modes analysis and weighted risk priority number evaluation in FMEA. Engineering Failure Analysis 2011; 18(1): 1162-1170.
16. Peter Popov. Bayesian reliability assessment of legacy safety-critical systems upgraded with fault-tolerant off-the-shelf software. Reliability Engineering and System Safety 2013; 117(5): 98-113.
17. Rongxing Duan, Jinghui Fan. Reliability Evaluation of Data Communication System based on Dynamic Fault Tree under Epistemic Uncertainty. Mathematical Problems in Engineering 2014; 35(2): 134-142
18. S. Montani, L. Portinale, A. Bobbio, and D. Codetta-Raiteri. A tool for reliability analysis of dynamic fault trees through conversion into dynamic Bayesian networks. Reliability Engineering and System Safety 2008; 93(7): 922-932.
19. T. Onisawa. An approach to human reliability in man-machine systems using error possibility. Fuzzy Sets and Systems 1988; 27(2): 87-103.
20. Wonkeun Youn, Baeck-jun Yi. Software and hardware certification of safety-critical avionic systems: A comparison study. Computer Standards & Interfaces 2014; 36(3): 889-898.

21. Xinglong Wang, Weixiang Liu. Research on air traffic control automatic system software reliability based on Markov chain.Physics Procedia, 2012; 24(3): 1601-1606.
22. YANG Jianping, HUANG Hongzhong, LIU Yu. Evidential networks for fault tree analysis with imprecise knowledge. International Journal of Turbo & Jet Engines 2012; 29(2): 111-122.
23. Yi Ding, Zuo M.J. Lisnianski A,Wei Li. A Framework for Reliability Approximation of Multi-State Weighted -out-of- Systems. IEEE Transactions on Reliability 2010; 59(3): 297-308.

Jiliang TU
Ruofa CHENG
Qiuxiang TAO
School of Information Engineering, Nanchang Hangkong University
Nanchang Jiangxi, 330063, China
Email: tjl1980@nchu.edu.cn or 395229630@qq.com