Model-based System Reliability Analysis by using Monte Carlo Methods

Li Dong, Zhong Lu, Mengdie Li
College of Civil Aviation
Nanjing University of Aeronautics and Astronautics
Nanjing, China
luzhong@nuaa.edu.cn, dong_li@nuaa.edu.cn
lmd1998@126.com

Jia Zhou
Department of Aircraft Maintenance
China Eastern Airlines Jiangsu Limited
Nanjing, China
zhou_jia81@126.com

***Abstract*—With the increasement of integrity and complexity of aircraft systems, it is difficult to evaluate the impacts of the component failure modes on the systems. In this paper, a method for system reliability analysis of large and complex systems with multiple failure modes is proposed by combining the Monte Carlo (MC) method and model-based technology. The MATLAB/Simulink language is used to create the nominal model. And the model extension is obtained by injecting failure modes based on the nominal model. The extended system model is used to observe and analyze the behaviors and performances of the complex systems in the presence of different faults. Performance metrics are used to evaluate system effects caused by component failures. A procedure for system reliability evaluation based on the MC method is given, which can be applied to the reliability evaluation of a system. The method proposed is insensitive to the dimensionality of problems and can be used to the reliability evaluation of large and complex systems. The system response with fault injection can be analyzed to determine the effect of component failures or their combinations in system reliability analysis, which can avoid the dependence on the subjective judgment and experience of analysts. Furthermore, it can help improve the systems development. A case study is given to illustrate our proposed method.**

Keywords- Reliability Evaluation; Model-based Technology; Nominal Model; Monte Carlo method; Failure Injection

I. INTRODUCTION

System reliability analysis techniques have been well developed and are widely used in the design of complex systems [1-5]. Based on data from different sources, the reliability engineers traditionally perform system reliability analysis, which includes informal design models and various other documents. While these analyses are highly subjective and dependent on the skill of the practitioner [6]. In particular, increasing functionality and complexity of aircraft systems often take much effort for the reliability analysts to gather system details and evaluate system reliability. So using accurate formal models of the large and complex systems may help reduce errors and conduct a more thorough reliability analysis.

Model-based technology is gradually applied to the field of safety and reliability analysis of the system when Joshi et al [6] proposed a model-based approach to perform safety analysis in 2005. Compared with traditional analysis process, the model-based method used in the process of safety and reliability analysis can address some of the issues arising owing to the manual and informal and accomplish automation of parts of the analysis process and consistent analyses [7]. Model-based technology has been increasingly accepted by the regulators in the last decade, particularly in the aviation section. For instance, Bozzano et al. [8] examined the informal process employed in AIR6110 Wheel Brake System by using a thorough, formal methodology. The European Union applied model-based technology to aviation engineering project named ISAAC in Europe [9]. Based on the model-based technology, researchers and engineers proposed different methods for system safety and reliability analysis. Li et al. [10] proposed an approach for complex systems by linking function modeling using formal language and fault propagation. Matthias et al. [11] proposed a method for probabilistic model-based analysis for synchronous parallel system and presented function models, which can be used for reliability evaluation of the safety and reliability of a system in the early design phase. Alejandro et al. [12] proposed an integrated methodology for the reliability analysis of fault-tolerant systems based on model-based technology and used Markov chains to model stochastic process when failures occur.

In this study, a method for system reliability analysis of complex systems is proposed by combining the Monte Carlo (MC) method and model-based technology. The MATLAB/Simulink language is used to create nominal (non-failure) models of research systems, which is the primary step in this method. Then, we extend a nominal model via injecting failure modes, failure condition descriptions and additional data about the system to the nominal model. The extended system model can be used to observe and analyze the behaviors and performances of a system in the presence of faults. A procedure for the system reliability evaluation based on the MC method is given in this study. In particular, this method proposed is introduced to improve and guide the system design process.

The paper is structured as follows. In Section II, the nominal system modeling and extension is introduced. In Section III, the reliability evaluation based on the nominal model extension is shown. In Section IV, a case study for the lateral-directional flight control system (FCS) of a fighter aircraft is given to illustrate the method proposed. In Section V, concluding remarks are presented.

II. NOMINAL SYSTEM MODELING AND EXTENSION

In this section, a method for system reliability analysis by combining the MC method and model-based technology is

978-1-7281-0860-5/19/$31.00 ©2019 IEEE

introduced. Figure 1 shows the procedure of our proposed method. The part of improving and guiding the system design process is presented in section IV.

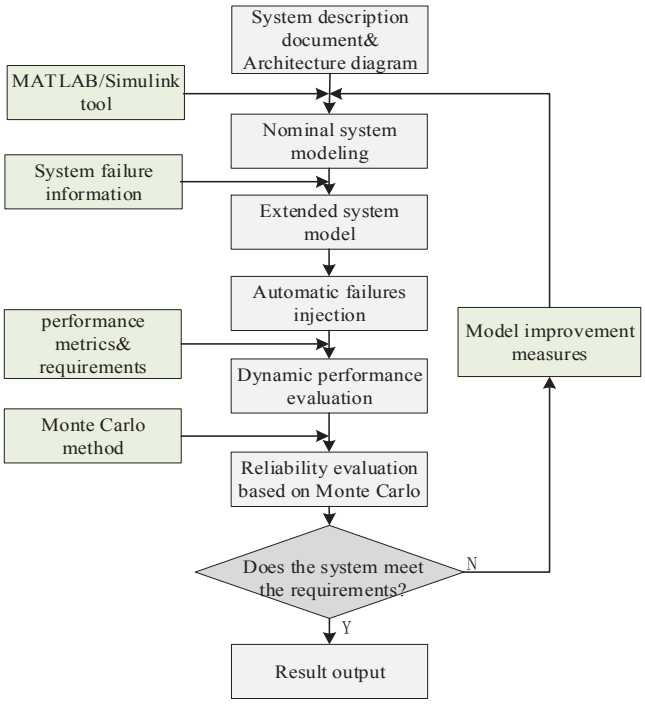

Figure 1. The procedure of the method proposed in this study.

A. Nominal system modeling

The creation of a nominal system model is the first step in automating safety analysis [6]. We can use modeling languages supporting graphical or textual representation to model behaviors of the system with no-fault. The MATLAB/Simulink language, developed by The Math Works [13], has become the standard formalism for modeling and implementing control software in areas like avionics, transportation, and process automation. Joshi et al. [14] used Simulink tool to create the nominal model of the wheel brake system described in Aerospace Recommended Practice (ARP) 4761 document. Alejandro et al. [12] modeled a lateral-directional FCS by using MATLAB/Simulink tool. In this study, the graphical tool named Simulink is also used to establish the nominal model of a system.

B. Model extension and automatic failures injection

After a model used to describe the nominal behaviors of the system is created, we will focus on analyzing the system performance in the presence of various failures. We can specify and evaluate different component failure modes by extending the original model with failure modes. In order to evaluate the possible behaviors of the system in the presence of failures, we also use the Simulink tool to extend a nominal model by injecting a number of (candidate) component failures. An example is given in Figure 2, which illustrates the process of model extension. Figure 2 shows that the selection and injection of three fault modes (omission, random, and delay). Omission failure mode means the system output is equal to zero; random failure mode means the system output is a random number that varies over time within a certain range; delay failure mode means the system output delays for a period of time.

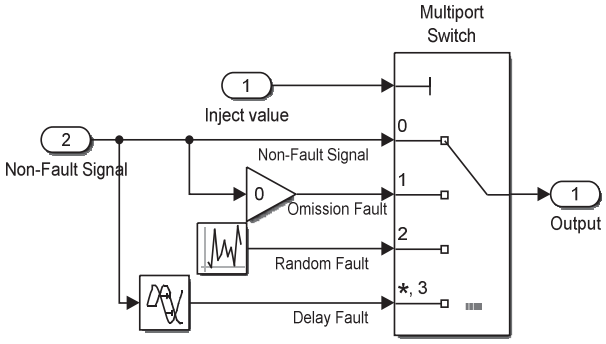

Figure 2. Three simple failure modes in Simulink.

The automatic failures injection based on the extended system model can be implemented with MATLAB/Simulink tool. The procedure of the automatic failures injection is presented in Figure 3. According to system performance requirements, we can evaluate and analyze the system behaviors under different failures.

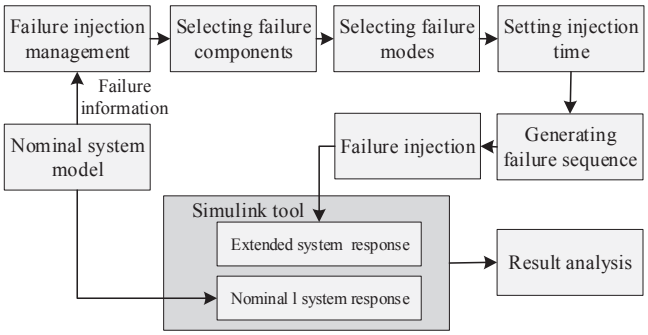

Figure 3. Automatic failure injection procedure in MATLAB/Simulink tool.

III. RELIABILITY EVALUATION BASED ON THE NOMINAL MODEL EXTENSION

A. Performance metrics and requirements definition

Performance metrics are a set of system-related properties, which can be used for quantifying how well a system performs the design functions. The performance metrics used to analyze a system rely on the type of the system and engineers' focus. For instance, the property such as roll angle or roll rate related to flight control may be significant in the flight control system. If the evaluated system is an aircraft power system, the average power consumption and the current peak may be performance metrics. According to these properties within a system, we can evaluate the system nominal model and the extended system model.

Performance requirements represent the values that the performance metrics are allowed to take on the normal systems. We can evaluate the system state by observing whether the values of performance metrics are within performance requirements. The range of performance requirements relies on the evaluated system. Once the values of performance metrics exceed the range of performance requirements, we would think the systems have failed.

B. *Reliability evaluation based on the nominal model extension by using the MC method*

MC methods [15] are a broad class of computational algorithms, which is an application of the laws of probability and statistics to the natural sciences and widely applied in solving real problems in many engineering fields [16]. Furthermore, the MC method is insensitive to the dimensionality of problems and has strong applicability to solve problems [17]. Therefore, it plays an irreplaceable role in reliability analysis of large and complex systems.

In this study, we propose a reliability evaluation method based on the MC simulation for the created system models in Simulink. This method takes advantage of the MC method and can be used for the reliability evaluation of aircraft systems. The procedure of this method is presented in Figure 4.

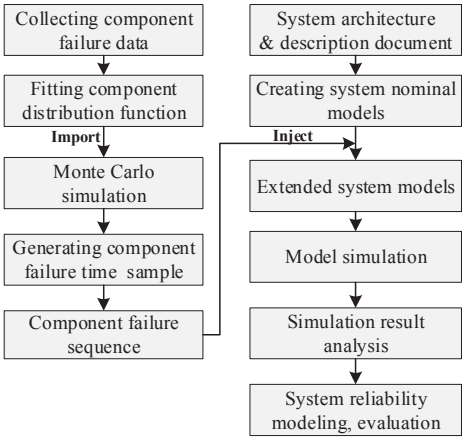

Figure 4. The procedure of reliability evaluation based on the MC method.

This method proposed can be used to simulate various failure scenarios of a system at any time via generating different component failure sequences and setting failure injection time. Based on different distribution functions corresponding to the failure modes of components, we can utilize MC method to produce randomly a group of samples, which are used to simulate failure time corresponding to all failure modes within a system. In a failure sequence, we assume that any component only fails once and the smallest sample among all failure modes of the same component is taken as the lifetime of this component. So, we can get a group of component lifetime samples that correspond to different components within a system, and the values of these samples will be used to determine the order of components within a failure sequence. We can implement failures injection based on a failure sequence. After simulating different failure sequences, we can get a group of system lifetime samples. Based on these system lifetime samples, we can model and evaluate the system reliability.

IV. CASE EXAMPLE: LATERAL-DIRECTIONAL FLIGHT CONTROL SYSTEM

To illustrate the approach in the paper, a case study for the lateral-directional FCS of a fighter aircraft described in the literature [12] [18] is presented in this section. The architecture of the research system consists of two primary flight computers (PFC1/2) that receive flight data from triple redundant inertial measurement units (IMU1/2/3), rudder position sensors (RPS1/2/3), left aileron position sensors (LAPS1/2/3), right aileron position sensors (RAPS1/2/3) and pilot input. Both PFCs calculate the flight control laws for the control surface actuation subsystems (LAAS1/2, RAAS1/2, RAS1/2) based on the received data. The control surfaces of the aircraft are actuated by the actuation subsystems. The fighter aircraft in this study utilizes fly-by-wire technology.

A. *Nominal system modeling and model extension*

Basing on the lateral-directional FCS architecture and other design information, we can use the Simulink tool to create the nominal model of the research system. We assume that the roll command curve is 0.2 rad, 0.1Hz square wave. Figure 5 shows the response curves of the system model.

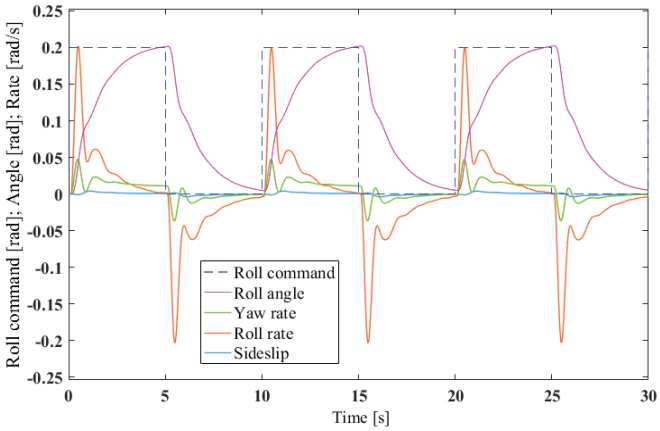

Figure 5. System performance curves.

In the lateral-directional FCS example, we consider some common failure modes of the different hardware components. We create an extended system model by injecting a number of component failures to the original model. Description corresponding to the failure modes is given in Table I.

TABLE I. FAILURE MODES DESCRIPTIONS OF THE DIFFERENT COMPONENTS

Component	Failure mode	Description	Failure rate(/h)
PFC-1/2	Omission	Output set to zero	2E-8
	Random	Random output	1E-8
	Stuck	Output stuck at last correct value	1E-8
	Delayed	Output delayed 0.2s	1E-8
LAAS-1/2, RAAS-1/2, RAS-1/2	Omission	Output set to zero	8E-7
	Stuck	Output stuck at last correct value	8E-7
LA, RA, RU	Omission	Output set to zero	1E-8
	Trailing	Output command by the aircraft dynamics	1E-8
LAPS-1/2/3, RAPS-1/2/3, RPS-1/2/3	Omission	Output set to zero	4E-7
	Gain change	Output scaled by a factor	3E-7
	Biased	Output biased by a factor	3E-7
IMU-1/2/3	Omission	Output set to zero	4E-7
	Gain change	Output scaled by a factor	3E-7
	Biased	Output biased by a factor	3E-7

After extending the nominal model with the failures, we can implement these failure modes in Simulink for simulating different failure scenarios, which can be accomplished by operating block interface “Failure Injection” in the extended system model. To illustrate how a normal system model is

extended and how to inject failures to an extended system model, we will show how to create an extended block of the system in the case study. The complete extended system model will be created by connecting all the extended blocks. Figure 6 shows an extended block that can be used to compute roll control law. Figure 7 shows the internal connection of this extended block in Simulink. There are four failure modes including Omission (The Multiport Switch input 1 is passed to the output), Random (The Multiport Switch input 2 is passed to the output), Stuck (the Multiport Switch input 3 is passed to the output) and Delayed (The Multiport Switch input 4 is passed to the output).

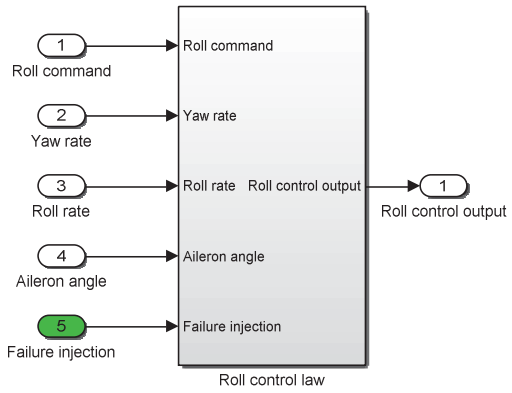

Figure 6. An extended block in Simulink.

B. *System reliability evaluation*

According to the literature [12], the aircraft state variables, which include sideslip, the axis roll rate, the axis yaw rate and the axis roll angle, are chosen as performance metrics of the research system in this study. The performance requirements are defined as

$$\begin{aligned}\Omega_1 &= \left\{\beta(t) \in \mathrm{IR} / \| \beta(t) - \beta_r(t) \|_\infty \le r_\beta \right\} \\ \Omega_2 &= \left\{ p_b(t) \in \mathrm{IR} / \| p_b(t) - p_{b_r}(t) \|_\infty \le r_{p_b} \right\} \\ \Omega_3 &= \left\{ r_b(t) \in \mathrm{IR} / \| r_b(t) - r_{b_r}(t) \|_\infty \le r_{r_b} \right\} \\ \Omega_4 &= \left\{ \phi(t) \in \mathrm{IR} / \| \phi(t) - \phi_r(t) \|_\infty \le r_\phi \right\}\end{aligned} \quad (1)$$

Where Ω_1, Ω_2, Ω_3 and Ω_4 denote performance requirements associated with the performance metrics $\beta(t)$, $p_b(t)$, $r_b(t)$ and $\phi(t)$ respectively; $\beta_r(t)$, $p_{b_r}(t)$, $r_{b_r}(t)$ and $\phi_r(t)$ denote reference aircraft state variable values of $\beta(t)$, $p_b(t)$, $r_b(t)$ and $\phi(t)$ respectively; $r_\beta = 0.15\mathrm{rad}$; $r_{p_b} = 0.45\mathrm{rad/s}$; $r_{r_b} = 0.45\mathrm{rad/s}$; $r_\phi = 0.15\mathrm{rad}$.

Here, we consider that the aircraft is in a cruising phase with velocity 178m/s and pitch angle 0.216rad. To evaluate system performance and reliability, the behaviors of the system with single failure modes can be firstly analyzed by setting the length of the failure sequence to 1 in MATLAB/Simulink. Table I shows single failure modes that cause a system failure. We utilize the Markov method to compute the probability of these failures at the end of the maintenance period T=500h of the aircraft and the calculated probability values are also given in Table II.

With the increasing number of failures, we will face the problem of state-space explosion when the Markov method is used to compute the system probability. In this study, we use the reliability evaluation based on the MC method to compute system unreliability. According to the proposed method based on the MC simulation, we can get a group of samples of the system lifetime. Figure 8 shows the 2000 system lifetime samples via the MC simulation and model-based technology.

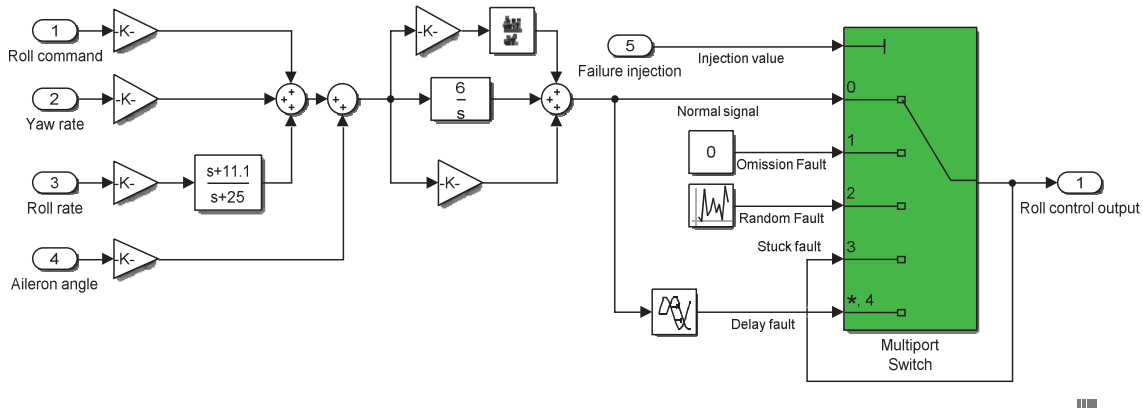

Figure 7. The internal connection of the extended block in Simulink.

In order to evaluate the system lifetime samples distribution, we linearly fit these samples via several common distribution functions. Figure 9 shows the linear fitting process for system lifetime samples. We can find the samples are subject to the Weibull distribution.

The Maximum Likelihood Estimate (MLE) method [19] is used to estimate distribution parameters. Therefore, we can get a Weibull distribution function with the shape parameter equal to 1.387 and the scale parameter equal to 4.614×10^5, which is given in Equation (2). And the 95% confidence intervals for the estimates of the shape parameter and the scale parameter are $[1.342, 1.434]$ and $[4.463\times10^5, 4.771\times10^5]$ respectively.

$$f(t) = \frac{1.387}{(4.614\times10^5)^{1.387}} t^{0.387} e^{-\left(\frac{t}{4.614\times10^5}\right)^{1.387}}, t > 0 \quad (2)$$

Where t denote the system lifetime, $f(t)$ is the value of probability density function. The curve of t and $f(t)$ is presented in Fig 8.

TABLE II. SINGLE POINTS OF FAILURE AND CORRESPONDING PROBABILITY OF TIME 500H

NO.	Single points of failure	Failure rates (10E-8/h)	System state	Probability (T=500h)
1	PFC-1: omission	2	Failed	9.946E-06
2	PFC-1: random	1	Failed	4.973E-06
3	PFC-1: stuck	1	Failed	4.973E-06
4	PFC-1: delayed	1	Failed	4.973E-06
5	PFC-2: omission	2	Failed	9.946E-06
6	PFC-2: random	1	Failed	4.973E-06
7	PFC-2: stuck	1	Failed	4.973E-06
8	PFC-2: delayed	1	Failed	4.973E-06
9	Left aileron: trailing	1	Failed	4.973E-06
10	Right aileron: trailing	1	Failed	4.973E-06
11	Rudder: trailing	1	Failed	4.973E-06

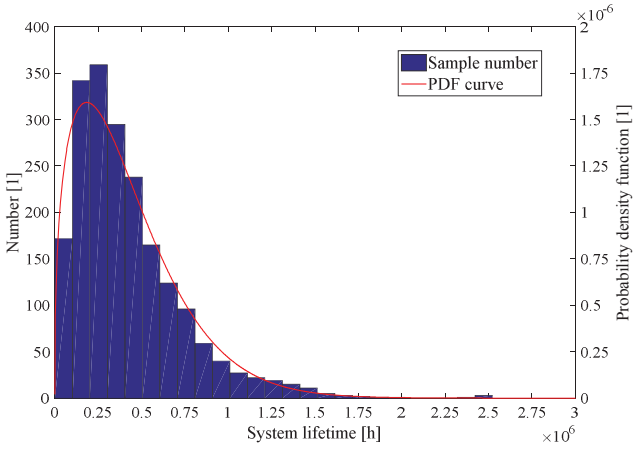

Figure 8. The fitted distribution curve and system lifetime samples based on the MC method and model-based technology.

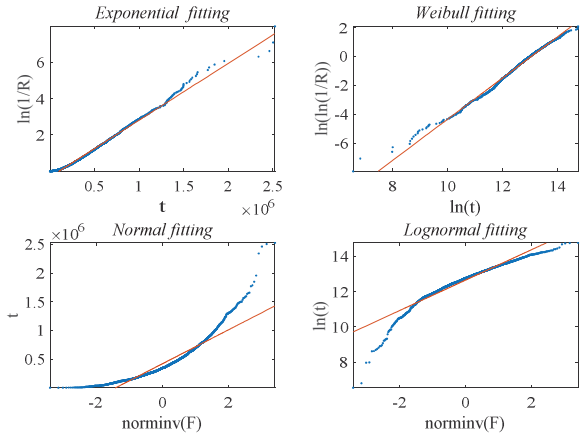

Figure 9. The linear fitting process for a group of samples.

Furthermore, we can also get the unreliability function $F(t)$ the failure rate $\lambda(t)$ function of the system, which can be used to evaluate the system performance and reliability at any time.

C. Enhanced system architecture

In the design process of the mechanical system, we often require the system must be single fault-tolerant. In this case study, there are 11 single points of failure within the lateral-directional flight control system. For failures in the left aileron, right aileron and rudder, we cannot solve them by using redundancy technology since the aileron and rudder in this case study are non-redundant. However, propulsion controlled aircraft (PCA) developed by NASA can be used to compensate for these failures [20]. So, we mainly focus on failures within the PFCs in this section.

In order to remove all single points of failure in PFCs in the case study, we proposed an enhanced dual unit architecture in PFCs, which is presented in Figure 10. The main difference between the initial PFC and the enhanced PFC is that the former only consists of a command unit, and the latter consists of a command unit and a monitor unit. The command unit mainly accepts data from sensors and pilot command and calculates the aircraft control laws based on flight control algorithms. The monitor unit mainly checks whether the orders from the command unit are executed correctly. The aircraft control laws calculated by the monitor unit are used to compare with the command unit, but not for output. Two units within the enhanced PFC are similar in composition and separated by a center partition.

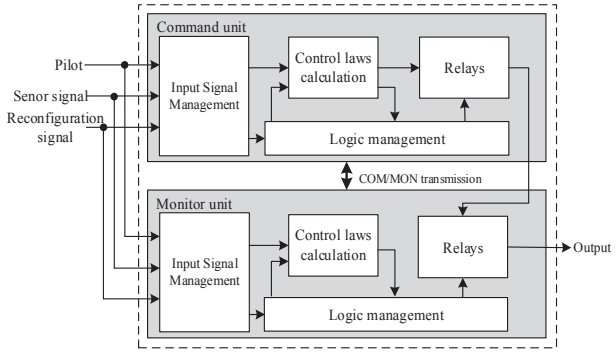

Figure 10. Enhanced architecture in PFCs.

The two units within a PFC will check whether the calculations of the control laws are consistent with each other. Once the monitor unit (the command unit) checks the control laws of two units disagree, this PFC will be shut down, which means the PFC is failed and its control laws cannot be output. When any PFC fails, reconfiguration signals from two units within the failed PFC will be sent to the remaining PFC. the remaining PFC will change the control laws for making up for the failed PFC.

For the improved lateral-directional flight control system, we carry out failures injection automatically in Simulink and evaluate system performance and reliability when the aircraft is in the assumed flight phase. Table III shows the single points of failure in the improved system and corresponding probability values at the end of the maintenance period T=500h.

D. Result discussions

Through Table II, III, we can see that the number of single points of failure within the system decrease from 11 to 3 via improving the architecture of the PFCs.

Based on the proposed method in this study and MLE method, we analyze and evaluate the enhanced system architecture and can get a new Weibull distribution function

with the shape parameter equal to 1.415 and the scale parameter equal to 5.365×10^5 . The cumulative density function curves of distributions of the original system and the enhanced system are presented in Fig 11. It is obvious that the improved lateral-directional FCS architecture is more reliable compared with the original lateral-directional FCS architecture.

TABLE III. SINGLE POINTS OF FAILURE AND CORRESPONDING PROBABILITY OF TIME 500H

NO.	Single points of failure	Failure rates (10E-8/h)	System state	Probability (*T*=500h)
1	Left aileron: trailing	1	Failed	4.973E-06
2	Right aileron: trailing	1	Failed	4.973E-06
3	Rudder: trailing	1	Failed	4.973E-06

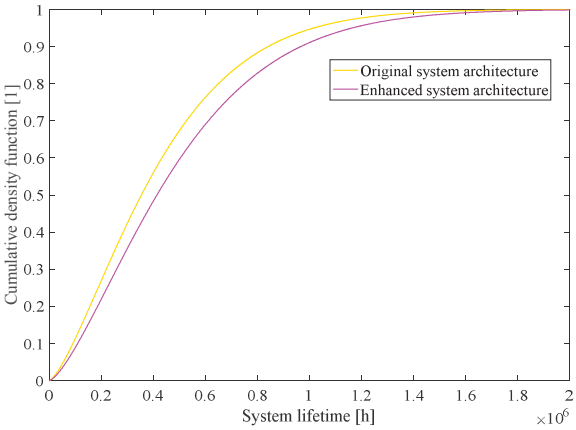

Figure 11. The cumulative density function curves of distributions of the original system and the enhanced system.

V. CONCLUSIONS

A method for system reliability evaluation of large and complex systems with multiple failure modes is proposed by combining MC method and model-based technology. The system nominal model and the extended model are created in MATLAB/Simulink. Based on the extended system model, we can observe and analyze the behaviors and performances of a system in the presence of different component failures. The procedure of the automatic failures injection is given in this study, which can be used to carry out the quantitative system evaluation in Simulink. The procedure for the system reliability evaluation based on the MC method is proposed in this study, which can be applied to the system reliability modeling and avoid the state explosion problem.

Compared with traditional reliability analysis techniques such as FTA, the method proposed in this study is insensitive to the dimensionality of problems and can be used for the reliability evaluation of complex aircraft systems. Moreover, the precise system formal model created in the process may help reduce errors and conduct a more thorough reliability analysis. Another advantage of the proposed method is that it can help promote the system design process in the system design phase.

REFERENCES

[1] L. A. Gavrilov, N. S. Gavrilova, "The Reliability Theory of Aging and Longevity," Journal of Theoretical Biology, vol. 213, no. 4, pp. 527-545, 2001.

[2] A. Birolin, "Reliability Engineering: theory and Practice, Seventh Edition," Berlin: Spring, 2007.

[3] M. Finkelstein, "Failure rate modelling for reliability and risk," Springer London, 2008.

[4] B. K. Lad, M. S. Kulkarni, K. B. Misra, "Optimal Reliability Design of a System," IEEE Transactions on Reliability, vol. 22, no. 5, pp. 255-258, 2009.

[5] X. Du, W. Chen, "Collaborative Reliability Analysis under the Framework of Multidisciplinary Systems Design," Optimization & Engineering, vol. 6, no. 1, pp. 63-84, 2005.

[6] A. Joshi, S. P. Miller, M. Whalen, "A PROPOSAL FOR MODEL-BASED SAFETY ANALYSIS," Digital Avionics Systems Conference. IEEE, 2005.

[7] A. Joshi, M. P. E. Heimdahl, "Behavioral Fault Modeling for Model-based Safety Analysis," IEEE High Assurance Systems Engineering Symposium. IEEE, 2007.

[8] M. Bozzano, A. Cimatti, A. F. Pires, et al., "Formal Design and Safety Analysis of AIR6110 Wheel Brake System," International Conference on Computer Aided Verification. Springer, Cham, 2015.

[9] O. Aaker. P. Bieber, "ISAAC, a framework for integrated safety analyses of functional, geometrical and human aspects," Proceedings of the Electronic Reciprocal Transfer System, pp. 145-162, 2006.

[10] Y. Li, Q. Gong, D. Su, "Model-based System Safety Assessment of Aircraft Power Plant," Procedia Engineering, vol. 80, pp. 85-92, 2014.

[11] Güdemann, Matthias, and F. Ortmeier, "Probabilistic Model-Based Safety Analysis," Electronic Proceedings in Theoretical Computer Science 28.Proc. QAPL 2010(2010):114-128.

[12] D. D Alejandro, J. G. Kassakian, J. E. Schindall, and J. J. Zinchuk, "An integrated methodology for the dynamic performance and reliability evaluation of fault-tolerant systems," Reliability Engineering and System Safety, vol. 93, no. 11, pp. 1628-1649, 2008.

[13] G. Sybille, P. Brunelle, L. H. Hoang, et al., "Theory and applications of power system blockset, a MATLAB/Simulink-based simulation tool for power systems," Power Engineering Society Winter Meeting. IEEE, 2000.

[14] A. Joshi, M. P. E. Heimdahl, "Model-Based Safety Analysis of Simulink Models Using SCADE Design Verifier," 2005.

[15] R. Y. Rubinstein, "Simulation and the Monte Carlo Method," Simulation and the Monte Carlo method, 2008.

[16] E. R. Jose, W. C. Coit, "A Monte-Carlo simulation approach for approximating multi-state two-terminal reliability," Reliability Engineering & System Safety, vol. 87, no. 2, pp. 253-264, 2005.

[17] E. Zio, W. Marella, L. Podofillini, "A Monte Carlo simulation approach to the availability assessment of multi-state systems with operational dependencies," Reliability Engineering and System Safety, vol. 92, no. 7, pp. 871-882, 2007.

[18] D. T. Mcruer, T. T. Myers, P. M. Thompson, "Literal singular-value-based flight control system design techniques," Journal of Guidance, Control, and Dynamics, vol. 12, no. 6, pp. 913-919, 1989.

[19] A. John, "R. A. Fisher and the making of maximum likelihood 1912-1922," Statistical Science, vol. 12, no. 3, pp. 162-176, 1997.

[20] T. Tucker, "Touchdown: The Development of Propulsion Controlled Aircraft at NASA Dryden," NASA, no. 16, 1999.