A METHOD FOR AUTOMATIC GENERATING SAFETY ANALYSIS BASED ON AVIATION PISTON ENGINE MODEL

Guo Li[1,2], Yida Teng[1], Zilu Wang[1], Tongge Xu[1] & Shuiting Ding[1,3]

[1] Beihang University, Beijing, China
[2] Tianmushan Laboratory, Hangzhou, China
[3] Civil Aviation University of China, Tianjin, China

Abstract

Safety results based on traditional safety analysis generated by manual qualitative means such as FTA are limited in response to complex systems. Therefore, a safety analysis based on engine design model is proposed in this paper, which can generate safety results of complex coupling systems automatically, comprehensively and efficiently.

Keywords: Safety analysis, model-based safety analysis, FTA, FMEA

1. Introduction

General aviation (GA) is currently facing various safety challenges with the highest civil aviation accidents and fatalities[1]. For general aviation categories, aviation piston aircraft provide an important public transportation connection throughout general aviation due to the relatively low acquisition cost[2]. Aero-engines are critical components that ensure the propulsion of aircraft and the engine safety required to be attended to. In addition, reports from the National Transportation Safety Board shown that structural failures of aviation piston engines are associated with aviation safety events[3]. Notably, factors affecting engine safety are coupled with each other in many cases, resulting in a series of events ending in engine in-flight failures[4]. In other words, safety is influenced by the complexity and interactions of aviation piston engine systems. Therefore, with the increasing complexity of engines, comprehensively identifying the single and coupled factors that potentially contribute to engine failure is essential.

Safety analysis is an essential approach to ensure the level of safety. With the significant increase in the complexity of the engine safety analysis process due to the complexity of the system, the traditionally safety analysis methods have revealed some limitations. Specifically, guidance documents that provide the system safety assessment include SAE ARP 4761 and SAE ARP 4754A[5][6]. As stated in the documents, the safety requirements are assigned top-down during the Preliminary System Safety Assessment (PSSA), which is an iterative stage of interaction between the design and the safety process. Fault Tree Analysis (FTA) is the main method used in this phase. After the design is finalized, a bottom-up implementation of validation is required, which is evaluated through Failure Mode and Effects Analysis (FMEA). Currently the most commonly used in engineering practice to generate FTA and FMEA is still based on manually. However, there are difficulties in identifying comprehensive and effective FMEAs and FTAs by manually as the complexity of the system increases, manifested by the increase in the number of systems and in the coupling correlation between the systems. Difficulties are reflected in the fact that manual fault trees are based on system description documents, and considerable knowledge is required for the analyst to understand the interdependencies between system components and functions. Thus, the analysis is error-prone, costly, and may not necessarily be complete. In addition, the efficiency, completeness, accuracy, and traceability of the implementation of safety analysis are also the issues that required to be investigated.

Model-based safety analysis method (MBSA) is an effective method to overcome the limitations of manual-based analysis through a model-based approach[7]. The method is gradually recognized by industry and bureau in the airworthiness validation process[8]. Significantly, MBSA is a methodology rather than a specific analytical method or analytical process. Differences in technical characteristics are contained in different methods and tools. However, incorporating the MBSE is the ideal MBSA. Therefore, the safety analysis should

be carried out on the basis of a design model, resulting in improved traceability. At present, MBSA is mainly widely used on airplanes and airborne systems[9][10][11], and the research on aviation engines is relatively limited. Therefore, the implementation of model-based system safety analysis in conjunction with the actual aviation engine design model is required to be investigated. In addition, extracting classical safety analysis results based on the model for different failure states, including the fault tree FTA and the failure state and effect analysis table FMEA, is another difficult issue to investigate.

Therefore, an innovative approach to engine system safety analysis is proposed in this paper. Specifically, an engine system model is first constructed, and model expansion is performed for the corresponding component fault modes to generate a safety model in conjunction with formal safety requirements. Further, FMEAs and FTAs are automatically and comprehensively generated through model simulation to better assist in the implementation of the system safety assessment in the ARPs. Finally, the proposed engine model-based safety analysis method is implemented using an actual aviation piston engine as case study, and the safety results including FMEA and FTA are obtained. The innovation of this paper is to introduce the engine modeling language and method into MBSA to achieve automatic and comprehensive generation of FTA and FMEA. More coupled faults can be identified, and the workload of safety analysis is simplified with better reusability of the analysis process and results.

The paper is structured as follows. Section 2 introduces the modified model-based safety analysis method based on the engine model and constructs the safety model. Section 3 presents the automatic generation of safety results, including FMEA and FTA, based on the safety model. Section 4 demonstrates the proposed method by a simplified single-cylinder aviation piston engine as case. Section 5 summarizes the conclusion.

2. Modified model-based safety analysis based on aviation piston engine model

The safety analysis process proposed in this paper is shown in Figure 1. First, a system model of an aviation piston engine is developed, which is composed of thermodynamics, aerodynamics, and mechanical dynamic and the coupling relationship between degrees. Secondly, the system model is extended by defining the corresponding fault models of the components, and a formal characterization of the safety requirements is proposed to realize the construction of the safety model. Finally, the generation of safety results including FTA and FMEA is achieved by simulating the safety model with automated procedures.

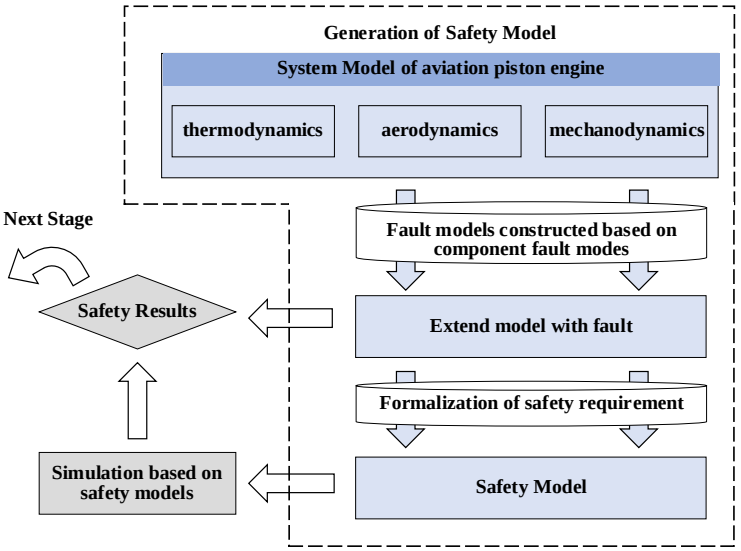


Figure 1. Process of modified model-based safety analysis based on aviation piston engine model

2.1 System model of aviation piston engine

A four-stroke compression ignition aviation piston engine is researched in this paper and a one-dimensional numerical model of total engine is developed.

At this stage, the thermodynamics, aerodynamics, mechanical dynamics and the relationships between parameters in the model vary with the crankshaft angle. The model is developed in MATLAB environment and consists of the following modules: intake manifolds and valves, cylinder, injector, exhaust manifolds and valve, and crankshaft as shown in Figure 2.

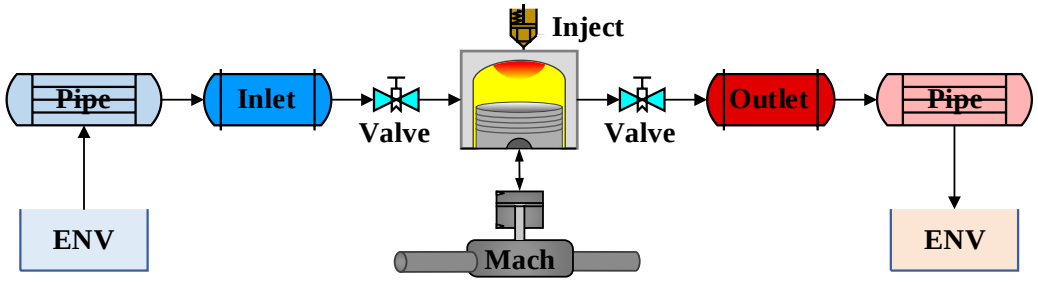


Figure 2. Schematic of the simplified aviation piston engine

Filling and emptying method is adopted in the aerodynamic module. Algebraic and differential equations are employed to characterize the associated system behavior. The fluid is modeled as an ideal gas while the specific internal energy and enthalpy are both functions of temperature and fluid composition. Brief description of each degree is given below, with more detailed explanation in [12].

The aerodynamic is modeled by the ideal gas equation as follows,

$$pV = mRT \tag{1}$$

where p is the pressure, V is the volume, m is the fluid mass, R is the gas constant and T is the temperature.

Fluid mass and energy are calculated through the continuity and the energy dynamic equation,

$$\frac{d(\rho V)}{dt} = (M_i - M_0) \tag{2}$$

$$\frac{d(\rho UV)}{dt} = \left(M_i H_i - M_0 H_0 + M_f H_f + \phi - P\right) \tag{3}$$

where ρ is the gas density, U is the gas specific internal energy, M_i and M_o are the mass flow rate at the inlet and outlet section, H_i and H_0 are the specific enthalpy at the inlet and outlet, M_f and H_f are respectively the fuel mass flow rate and lower heating value, Φ is the heat flow and P is the mechanical power.

In the thermodynamic, a single zone actual cycle approach is adopted to assess in-cylinder phenomena. The flow through the inlet and exhaust valves is determined by Equation 4 for compressible gas through a flow valve restriction,

$$\frac{dm}{dt} = C_D \frac{A_R p_i}{(RT_i)^{0.5}} \left(\frac{p_0}{p_i}\right)^{\frac{1}{k}} \left\{\frac{2k}{k-1}\left[1 - \left(\frac{p_0}{p_i}\right)^{\frac{k-1}{k}}\right]\right\}^{0.5} \tag{4}$$

In the case of choked flow, the equation adopted as follows,

$$\frac{dm}{dt} = C_D \frac{A_R p_i}{(RT_i)^{0.5}} k^{\frac{1}{2}} \left(\frac{2}{k+1}\right)^{\frac{k+1}{2(k-1)}} \tag{5}$$

where p_i and T_i are the pressure and temperature at the inlet valves, p_0 is the exhaust manifold pressure, A_R is the valve open area and k is the ratio of specific heats.

The mechanical dynamic coupled with thermodynamic by determining the displacement of the piston from the top dead by the crank angle value through the following equation,

$$x = r\left[1 + \frac{1}{r} - \left(\frac{l^2}{r^2} - \sin^2\theta\right)^{\frac{1}{2}} - \cos\theta\right] \tag{6}$$

where r is the crank radius and l is the connecting rod length. From the x values, the volume V of Equation 2 and Equation 3 is possible to calculate. The air compression process is determined by Equation 3 for each crank angle step variation ($d\theta$). Classical Woschni correlation was adopted as the heat transfer model. Combustion model imposed the combustion burn rate using a three-term Wiebe function. The effective power would be extracted from the simulation results by a specific function when the simulation convergence satisfied the criteria.

2.2 Extend model with fault

The ability to simulate both normal system behavior and system failure is a requirement of the model-based safety analysis approach. Therefore, faults are required to be modeled. Specifically, fault model structures that could be extended with system model and incorporate the physical characteristics of the engine are the first considerations for modeling. In addition, the faults required to be modeled in the simplest way, with ensuring fault simulation and safety analysis. A stable and efficient traversal of fault combinations could be achieved even for large system models containing a considerable number of components by ensuring the principle.

Therefore, the modeling of faults is achieved by developing a fault expansion model. Specifically, an expanded model includes at least modes 0, 1, and 2, i.e., there are at least three states: normal, slight fault, and severe fault, as shown in Table 1. The equations for reflecting faults and the corresponding fault logic combined with engine modeling language features can be supplemented, which is the component fault extension. Specifically, faults affect components with different fault variables. Fault variables could be categorized into minor and severe variables based on the degree of impact, and the classification of different fault modes can be established through the condition accordingly. Specifically, the example of clogged injector nozzles corresponding to the engine is illustrated as shown in Figure 3.

Table 1. Fault modes definition for fault modeling

Mode	**0**	**1**	**2**
Implication	Normal	Minor fault	Severe fault

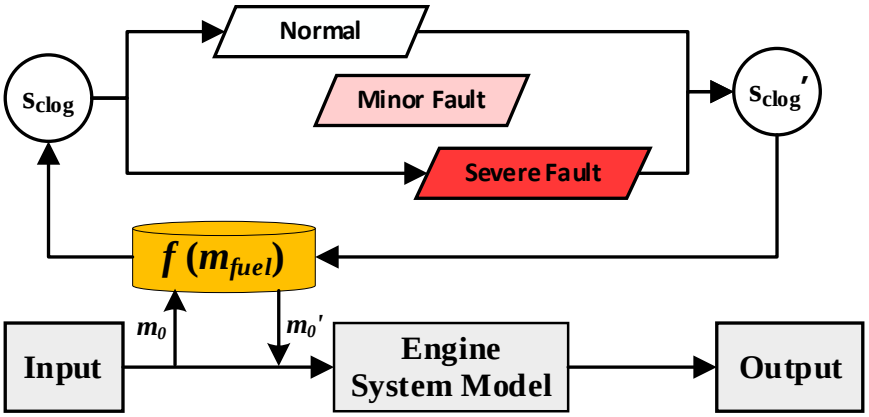


Figure 3. Schematic of system model extension with injector nozzle clogging fault as illustration

The lower portion of Figure 3 represents the engine system model, where the "Inputs" block determines the boundary inputs for the injected mass; m_{fuel} represents the value of injected mass. The upper part of Figure 3 contains a fault model that represents a fault with three modes. The fault injection is used as a variable represented by f(m_{fuel}) to regulate the variation in fuel injection. The different modes represent the quantity of variation that affects the fuel injection. The other fault categories listed in Table 2 are linked in the same way to the corresponding engine system model input variables. The subscripts n and f for each variable represent before and after the fault, respectively. Noteworthily, the method flow is the main focus in this paper. Therefore, minor and severe failures of components are assumed to represent deviations from normal values of 5% and 10%, respectively. That is, the values of K mode in Table 2 are 0, 5% and 10% when mode is 0,1,2. In practice, the deviation values of each component required to be set according to the actual situation, nevertheless the method in this paper is still applicable.

Table 2. Description of the aviation piston engine faults

Component	**Fault Form**	**Mode**	**Variable**	**Expression**
Intake manifold	Pipe roughness	0/1/2	Roughness	$f_{intake,f} = K_{mode} \times f_{intake,n}$
Intake valve	Open time error	0/1/2	Opening time	$A_{intake,f} = K_{mode} \times A_{intake,n}$
Injector	Clogged nozzles	0/1/2	Inject mass	$m_{fuel,f} = K_{mode} \times m_{fuel,n}$
Cylinder	Over-temperature	0/1/2	Cool temperature	$T_{cool,f} = K_{mode} \times T_{cool,n}$
Exhaust valve	Open time error	0/1/2	Opening time	$A_{exhaust,f} = K_{mode} \times A_{exhaust,n}$
Exhaust manifold	Pipe roughness	0/1/2	Roughness	$f_{exhaust,f} = K_{mode} \times f_{exhaust,n}$
Crankshaft	Deformation	0/1/2	Stroke	$L_{stroke,f} = K_{mode} \times L_{stroke,n}$

2.3 Safety model

Safety criteria required to be specified to evaluate the state of the system after modeling the engine system model and the component fault expansion model. Specifically, the criteria that define normal operation and system failure are specified by safety analysts based on the characteristics of the system proper as well as the requirements during the security assessment process. Therefore, certain determination criteria are required to be developed and applied in the system model to indicate exactly the state of the system, i.e., normal or failed, and to signal the corresponding outputs. For engine systems, the system state is usually calculated by comparing the difference between the actual output power supplied to the aircraft and the actual power required.

In order to accomplish automated model-based analysis, not only do the criteria require to be judged, but also the criteria require to be formally expressed. The formalization of a safety criteria for a system is actually the equivalent of converting natural language, which is understandable by humans, into machine language, which could be processed by machines. Specifically, on the one hand, formal judgment criteria have to map to specific structures or variables in the target system model in order to be understood by the system. On the other hand, the model requires to be able to simulate the target system in different fault states, which is the purpose of safety modeling. Thus, for an aviation piston engine, a machine language description of the labeling judged by the effective output power of the engine as,

$$\mathrm{G(E)} = \frac{Power_{engine,1} - Power_{engine,0}}{Power_{engine,0}} \tag{7}$$

where *G(E)* is system limit state function, $Power_{engine,0}$ is the normal power required by aircraft, $Power_{engine,1}$ is the power after safety model simulation. Engine failure is considered to occur when *G(E)* deviates by 10%, thus defining 5% as a minor failure and 20% as a severe failure condition. Ultimately, the construction of the safety model is completed based on the engine system model and the extended fault model, combined with the formal expression of the safety requirements.

3. Automatic generation of FTA and FMEA based on safety models

Model-based safety analysis could be primarily employed to assist FMEA and FTA in classical analyses. Therefore, this section first presents the automatic generation of FMEAs by simulating different failure modes of different components sequentially. Then, the automated assistance of model-based safety analysis for fault trees is introduced.

3.1 Generation of FMEAs based on safety model

FMEA analyzes the events underlying a fault during the system safety analysis to determine whether the function or component satisfies the safety requirements. Therefore, the FMEA generation can be automated by iteratively simulating the safety model and determining the system state accordingly, after determining and formalizing the fault effects. The process is shown in Figure 4.

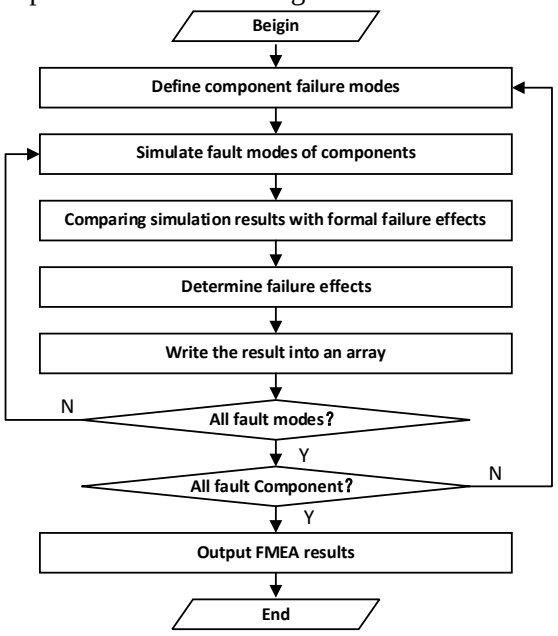


Figure 4. FMEA generation process based on safety models

Figure 4 illustrates the algorithmic logic for automatic FMEA generation. Firstly, different components and different fault mode combinations are defined. Secondly, the safety model simulation values for the current component with the current fault mode are simulated. The simulation results are compared with the formal failure effects to determine the failure state. Finally, the component name, component fault mode and component fault mode effects are written into the FMEA. All fault modes of all components are traversed in this process. The automatic generation of FMEA results can accurately reflect the real fault situation of the system. Moreover, the model-based FMEA could accurately reflect the parameter boundaries of possible fault effects in the case of component parameter varies. Programmed data-based determination methods can partially eliminate the subjectivity of manual analysis.

3.2 Generation of FTAs based on safety model

Fault tree is an important safety analysis method in traditional safety assessment systems. Fault tree, after logical simplification, is essentially the smallest cut set of bottom events that could lead to the top event. The model-based safety analysis method could simulate the model fault combination state space, so as to obtain the cut set of the bottom event. Then, the minimum cut-set can be obtained by simplifying according to the principle of repeated cut-set removal. The generation method of the minimum cut set is shown in Figure 5.

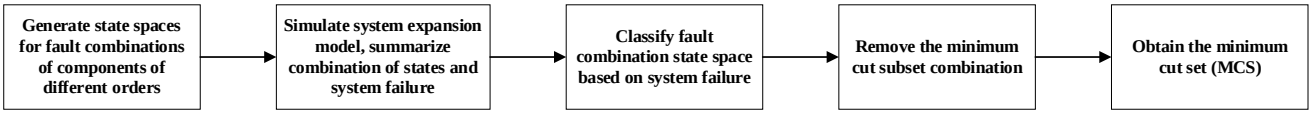


Figure 5. Minimum cut set generation method

3.2.1 Definition of minimum cut set

Minimal Cut Set (MCS) refers to the set of all minimal cuts of a system. A cut is a combination of component fault modes that cause a system failure. System failure is defined as a single specific system failure that generally corresponds to the top event of the fault tree. Top event implementation depends on the system failure mode definition as well as the analysis scenario. In addition, component failure modes generally correspond to fault tree bottom events. A cut is labeled as a minimum cut if the cut contains only component fault modes that are merely sufficient to cause system failure[13]. Minimum cuts may consist of one, two, three, or more component faults and are called first-order, second-order, third-order, and multi-order minimum cuts, respectively. Generally, at most, only third-order minimum cuts are considered, since the probability of occurrence of higher-order minimum cuts is very small and negligible. The assumption of independence between component failures is still adopted in this paper.

In this section, a maximum of three orders of cuts are considered, as well as components in a total of three fault modes including normal and two degrees of fault. The number of fault mode combinations is calculated as,

$$N_{all} = 2^{nr_1} \times 3^{nr_2} \tag{8}$$

n_{ri} represents the sum of the number of components in the system considering i failures, where i=1,2, and N_{all} represents the number of all combinations that fail. In addition, the all combinations of zero-order, one-order, two-order and three order could be represent as,

$$N_{0123} = 1 + N_1 + N_2 + N_3 \tag{9}$$

Where N_i is the i-order of component fault modes as,

$$N_1 = 2nr_2 \tag{10}$$

$$N_2 = 2^2 C_{nr_2}^2 \tag{11}$$

$$N_3 = 2^3 C_{nr_2}^3 \tag{12}$$

For the simplest simplified single cylinder four stroke piston engine system used as an example, which consists of 7 components, assuming that all components have two fault modes, the number of first-order combinations is 14, the number of second-order combinations is 84, and the number of third-order combinations is 280. The quantity would be even larger if the actual engine system consists of at least hundreds of engine components, and multiple fault modes are considered for each component. Therefore, it can be seen that the state space of system fault combination is very large, and manual decomposition alone is not enough.

3.2.2 Minimum cut set generation

Specifically, the generation process of first-order, second-order, and third-order fault combinations is shown

in Figure 6. Figure 6 depicts the generation process of the fault combination state space and the simulation of the system model based on the generated fault combination.

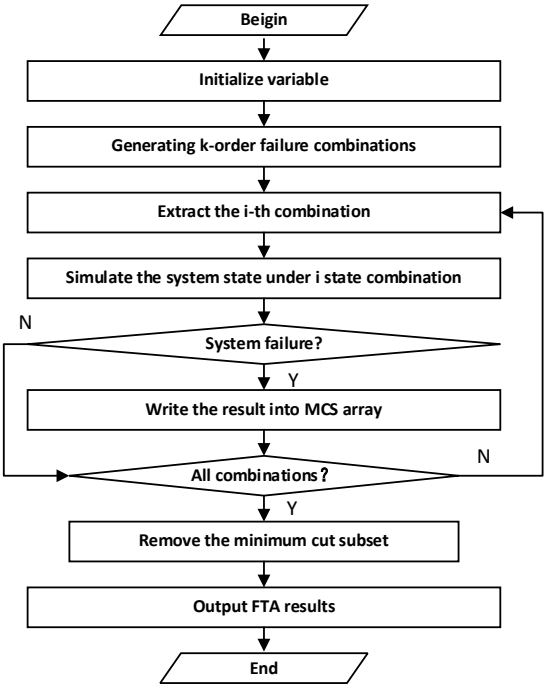


Figure 6. Minimum cut set generation

The final output of the entire process is the MCS represented in array form with the minimum number of cuts, and the corresponding system failure mode. As shown in the figure, the state value is initialized first. Secondly, generate all fault combinations corresponding to *k*-order failures, and count the number of combinations. Then, put all first-order to third-order combinations into the safety model and simulate the safety model. Based on the simulation results, the model will automatically determine whether the system is failure. Finally, the failure combinations are summarized in the state space that will cause system failure into the MCS according to the system failure form. Notably, the MCS is not an accurate MCS at this time, and it is necessary to remove the subset of the MCS.

3.2.3 Removal of minimum cut set

Specifically, by identifying whether higher-order combinations contain fault components and corresponding modes in lower order combinations as,

$$if\ N_{2i} \ni N_{3i}, then\ N'_3 = N_3 - N_{3i} \tag{13}$$

$$if\ N_{1i} \ni N_{2i}, then\ N'_2 = N_2 - N_{2i} \tag{14}$$

The meaning of first equation is that if both the third-order failure combination and the second-order failure combination can cause the same failure situation, the corresponding third-order failure combination will be merged into the corresponding second-order combination and the original third-order combination will be removed. Similar processes can be extended to second-order and first-order combinations.

In addition, the MCS set and the minimum number of cuts is required to alter accordingly. Finally, after removing the minimum cut subset, the resulting combination is the minimum cut set that causes the system to fail in a certain failure form.

4. Case Study

This section employs a simplified single cylinder four stroke aviation piston engine system as a case to establish a numerical simulation model for engine safety. Moreover, safety analysis is conducted based on numerical simulation, and the analysis output is presented in the form of classic safety analysis results, including FMEA and FTA.

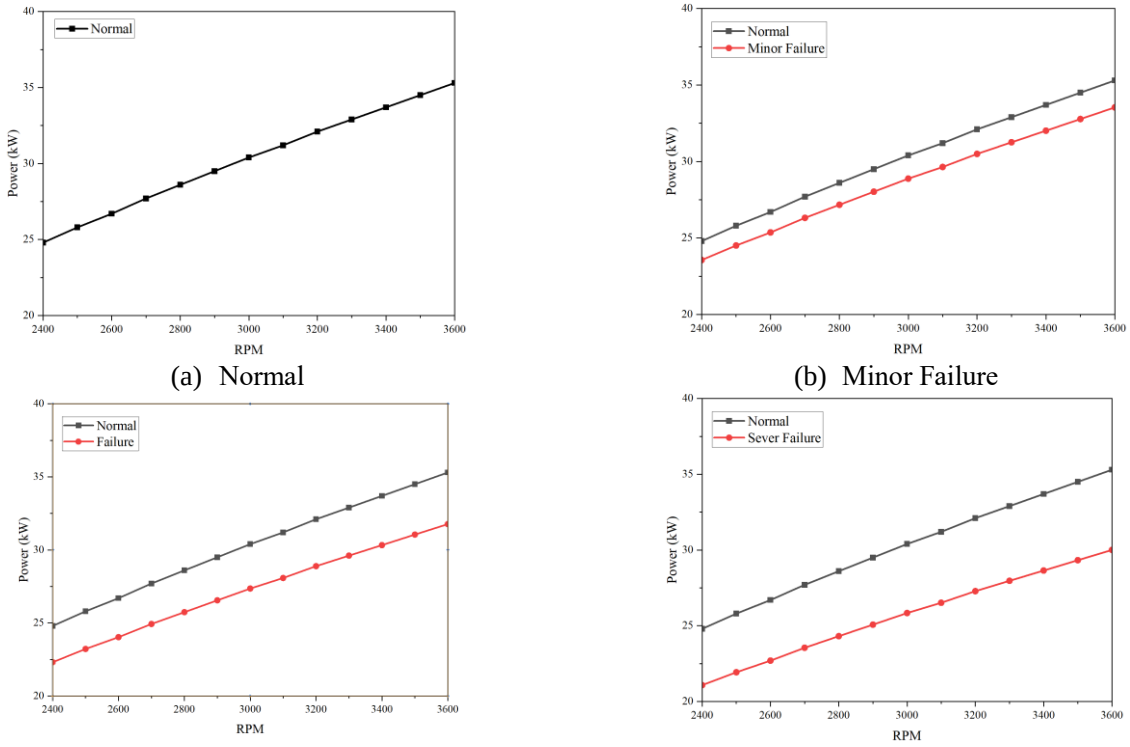
4.1 Construction of engine safety model

A simplified 35kw four-stroke compression-ignition aviation piston engine is considered in this paper which consisted by inlet manifold, inlet valve, cylinder, injector, exhaust valve, exhaust manifold, crank mechanism, and other function blocks. The main parameters required for piston engine modeling are shown in Table 3.

Table 3. Engine model parameters for analysis

Parameter	Characteristic values(units)
Bore/mm	100
Stroke/mm	100
Connecting rod length/mm	220
Displaced volume/L	0.785
Compression ratio	16.5:1
Injection volume/mg/cycle	80

Fault components and corresponding fault modes adopted to construct the fault extension model are shown in Table 2, and the extension formula is also provided in the table. In addition, the variation of aviation piston engine power is a comprehensive reflection of overall performance and an important basis for evaluating engine safety. It is worth noting that the method proposed in this article could also be used to analyze other safety standards, such as maximum pressure. Therefore, this paper selects power as the safety evaluation index for the engine for method explanation. Power can be obtained through the overall engine model. Figure 7 shows the power and speed under normal conditions and different failure forms.



(a) Normal (b) Minor Failure

(c) Failure (d) Sever Failure

Figure 7. Engine power under different system state

4.2 Safety results from safety model

4.2.1 FMEA

After determining the fault effects of the corresponding components of the engine and formalizing the failure forms, FMEA results could be automatically generated based on the FMEA simulation process. By iteratively simulating the FMEA model, the system state is determined based on the satisfaction of simulation results and preset conditions. The process requires a large amount of computation, however detailed information would be provided correspondingly.

After running the program, the output FMEA results are shown in Table 4.

Table 4. FMEA results

No.	Component	Fault mode	Fault effect	Failure effect	Failure formal
1	Intake manifold	0	0%	0%	Normal
		1	5%	0.08%	Minor Failure
		2	10%	0.21%	Minor Failure

		0	0%	0%	Normal
2	Intake valve	1	5%	6.42%	Failure
		2	10%	17.16%	Severe Failure
		0	0%	0%	Normal
3	Injector	1	5%	4.85%	Minor Failure
		2	10%	9.92%	Failure
		0	0%	0%	Normal
4	Cylinder	1	5%	0.13%	Minor Failure
		2	10%	0.27%	Minor Failure
		0	0%	0%	Normal
5	Exhaust valve	1	5%	6.36%	Failure
		2	10%	17.89%	Severe Failure
		0	0%	0%	Normal
6	Exhaust manifold	1	5%	0.17%	Minor Failure
		2	10%	0.21%	Minor Failure
		0	0%	0%	Normal
7	Crankshaft	1	5%	2.08%	Minor Failure
		2	10%	13.08%	Severe Failure

It can be seen from the table that the automatically generated FMEA results can accurately reflect the actual failure situation of the system, and can reflect in detail the different system failure states that may correspond to different components fault modes. In this article, two different fault modes of components are presented, which can further refine the forms of component faults and better determine the parameter boundaries of possible system failure effects. Overall, the programmatic model-based judgment method has great potential to solve subjectivity problem of manual analysis.

4.2.2 FTA

Due to space limitations, this paper only considers the generation of FTA in the case of failure, i.e., considering the case of power offset of 10%. For minor and severe failures, similar process could be developed. In this case, the number of considered engine fault components is 7. The fault modes for each component are two types. Table 5 shows the combination state space containing first-order to third-order generated based on the fault modes of system model components.

Table 5. Combinations of fault modes

No.	Component 1	Mode 1	Component 2	Mode 2	Component 3	Mode 3
1	1	1				
2	2	1				
3	3	1				
……	……	……				
7	7	1				
8	1	2				
9	2	2				
10	3	2				
……	……	……				
14	7	2				
15	1	1	2	1		
16	1	1	3	1		
……	……	……	……	……		
99	1	1	2	1	3	
100	1	1	2	1	4	
……	……	……	……	……	……	……
378	5	2	6	2	7	2

Furthermore, on the basis of formalizing system failure, system failure results caused by considering component faults could be obtained through simulation. The results are shown in Table 6.

Table 6. Preliminary results of system failure simulation

No.	Component 1	Mode 1	Component 2	Mode 2	Component 3	Mode 3	Failure
1	1	1					0
2	2	1					1

3	3	1					0
……	……	……	……	……	……	……	……
7	7	1					0
8	1	2					0
9	2	2					1
10	3	2					1
……	……	……	……	……	……	……	……
14	7	2					1
15	1	1	2	1			0
16	1	1	2	2			1
……	……	……	……	……	……	……	……
99	1	1	2	1	3	1	0
100	1	1	2	1	4	1	0
……	……	……	……	……	……	……	……
378	5	2	6	2	7	2	1

Furthermore, according to the simplification principle outlined in section 3.2.3, eliminate non minimum cut failure combinations. The minimum cut set for the failure event of engine power failure can be automatically obtained, as shown in Table 7. Results show that a total of 16 minimum cut sets were obtained, including 6 first-order failure combinations and 10 second-order failures. Therefore, safety control could be applied to different identified failure combinations based on the obtained results. Especially, the control of fault combinations that were not previously identified by human intervention could improve system safety.

Table 7. Minimal cut set

Component 1	Mode 1	Component 2	Mode 2	Component 3	Mode 3	Failure
2	1	0	0	0	0	1
2	2	0	0	0	0	1
3	2	0	0	0	0	1
1	1	3	1	0	0	1
……	……	……	……	……	……	……

5. Conclusion

In this paper, a method for automatic generation of FMEA and FTA based on engine model is proposed. The method includes generating an engine system model, then expanding with the component faults and constructing a safety model by expressing the safety requirements through a formalized method. Finally, the FMEA and FTA methods are automatically generated by simulating the safety model.

The demonstration of the procedure of this method is performed by a case study of a single-cylinder aero-piston engine system. Compared with the traditional safety analysis, multi-order coupled faults of different components could be considered based on this method, and the identified fault tree results are more complete. In addition, the analytical process based on this method shows a reduced workload. Specifically, this method is integrated with the engine design process by directly extending the design-stage model with faulty components. Secondly, the automatic generation of safety results could be realized by automatic simulation and programming of the model. As a result, the main safety effort is focused on extended modeling of faulty components, reducing the requirement for the total amount of work and capacity of safety analysts. Finally, the reuse of safety results generated by the present method is relatively well. Specifically, only the corresponding model refinement is required to be updated for more complex engine models without reconstructing the fault tree as in the case of traditional safety analysis methods since the model-based characteristic of the proposed method. Therefore, it is reasonable to believe that the present method could be extended to more detailed engine models and possibly utilized as a comparison between different engine configurations.

Acknowledgements

The work was funded by the National Natural Science Foundation of China and Civil Aviation Administration of China [Grant U2233213]. The work was supported by the Innovation Team of Complex System Safety and Airworthiness of Aero-Engine from the Co-Innovation Center for Advanced Aero-engine of China.

Copyright Statement

References

[1] Boyd DD. A review of General Aviation Safety (1984-2017). *Aerospace Medicine and Human Performance*, Vol. 88(7)(2017): pp.657-664.

[2] General Aviation Manufacturers Association. General aviation's contribution to the U.S. economy. Washington DC, USA, 2006.

[3] Douglas DB. Causes and risk factors for fatal accidents in non-commercial twin engine piston general aviation aircraft. *Accident Analysis & Prevention*, Vol.77 (2015): pp.113-119.

[4] Leveson N. Engineering a Safer World: Systems Thinking Applied to Safety. Cambridge, USA: MIT Press, 2011: pp.21-56.

[5] Society of Automotive Engineers International. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment. Technical Report No. ARP 4761. Warrendale, USA: Society of Automotive Engineers, 1996: pp.4-6.

[6] Society of Automotive Engineers International. Certification considerations for highly-integrated or complex aircraft systems. Technical Report No. ARP 4754. Warrendale, USA: Society of Automotive Engineers, 1996: pp.1-12.

[7] Joshi A, Miller SP, and Whalen MW. A proposal for model-based safety analysis. *Proceedings of the 24th Digital Avionics Systems Conference*. New York: Springer Verlag, 2005: pp.393-405.

[8] Bozzano M, Villafiorita A, and Akerlund O. ESACS: an integrated methodology for design and safety analysis of complex systems. *Proceedings of ESREL*. Balkema Publisher, 2003: pp.237-245.

[9] US Department of Transportation Federal Aviation Administration. Airborne software assurance. Technical Report No. Advisory Circular 20-115C. Washington, America: Federal Aviation Administration, 2013:1-3.

[10] Mhenni F, Choley JY, and Nguyen N. Flight Control System Modeling with SysML to Support Validation, Qualification and Certification. *IFAC Papers OnLine*, Vol. 49(3) (2016): pp.453-458.

[11] Sirgabsou Y, Baron C, and Pahun L. Model-driven engineering to ensure automotive embedded software safety. Methodological proposal and case study. *Computers in Industry*, Vol. 138(2022): 103636.

[12] Heywood JB. Internal Combustion Engine Fundamentals. New York, USA: McGraw-Hill, 2018: pp.156-273.

[13] Schallert C. Integrated safety and reliability analysis methods for aircraft system development using multi-domain object-oriented models, 2016.