Probability risk analysis and control of aeroengine control system failures

Han BAO*, Hongfu ZUO

(College of Civil Aviation, Nanjing University of Aeronautics and Astronautics,
Nanjing 210016, P.R.China)

*Corresponding author's e-mail: baohan@nuaa.edu.cn

Abstract: While aeronautical technology has been developing continuously in recent years, aviation accidents can never be completely eliminated. According to statistics, the actual risk of engine control system is often higher than risk expected in the design stage, which does harm to aviation safety. Therefore, a probability risk assessment method of engine control system is proposed, in which bottom faults, loss of thrust control (LOTC) events and serious consequence of aircraft are all evaluated. At last, the validity and practicability of this method are verified by the example of the failure risk analysis and control of VSV actuator in CFM56-7B engine. This paper provides a reference for risk management of engine control system in the stage of continued airworthiness.

1.Introduction

Engine control system is the core subsystem of the engine. For one thing, the loss of its function may cause the aircraft-level function failure and serious consequences, such as engine off in flight, total thrust loss and so on. For another thing, the control system is a nonlinear multivariable complex system and has high failure rate [1].

Due to the uncertain factors in the standard setting or the standard conformity, design, manufacture and operation environment, the actual operation risk of the engine control system is often higher than that expected, and the traditional deterministic methods have a large deviation in the risk analysis [2].

In order to overcome the shortcomings of the traditional safety life method and further improve the safety of the key components of the engine, Shah A R and other scholars proposed the PRA (probability risk analysis) method [3]. Under this framework, DARWIN (Design Assessment of Reliability with Inspection) was proposed by Southwest Research Institute in conjunction with GE and other engine manufacturers, which predicted probabilistic risk of engine based on failure mechanism [3]. Subsequently, the FAA issued Advisory Circulars 39-8 and proposed a risk assessment method based on component failure statistics, Weibull analysis and Monte Carlo simulation for aeroengines[4]. Although the above two PRA methods provide a reference, the risk assessment of engine control system has not been effectively carried out, due to the complexity of the system and the limitation of operating data

In recent years, the continuous optimization of risk models, the improvement of computational efficiency, and the construction of aviation basic database provide opportunities for the PRA method to identify and analyze the actual risks of complex systems [5]. Combining with the actual operation data of the control system, this paper takes the LOTC events as the bridge of risk assessment of the control system, establishes the failure risk assessment model of the engine control system from the bottom failures to unsafe outcomes. At last, risk analysis and control process are both demonstrated and verified by an actual case.

2.Procedure of risk assessment for engine control system failures

The key components of aeroengine control system include electronic engine controllers (EEC), hydraulic mechanical unit (HMU), actuators and sensors. And the main failure risks also come from these four parts[9].

A LOTC event is the top-level failure event of engine control system, which is defined to be one wherein: the engine cannot be modulated between idle and 90% of maximum rated power (at any flight condition) via normal throttle movement, or the engine cannot meet the operability requirements of Part 33, or the engine thrust oscillates in an unacceptable manner. LOTC rate is an important mark to assess engine safety[7]. While it is difficult to directly estimate the impact of an individual failure on the safety of the whole aircraft, LOTC events can be used as a bridge for risk analysis with the help of the safety analysis during the design phase.

Therefore, the analysis process is illustrated schematically in figure 1. Fault modeling is used to analyze risk of bottom failures developing into LOTC event, and event chain modeling is used to assess the risk of LOTC events developing into unsafe outcomes at aircraft level. After comparing the actual individual risk and fleet risk with airworthiness requirements, corresponding corrective measures should be taken if necessary.

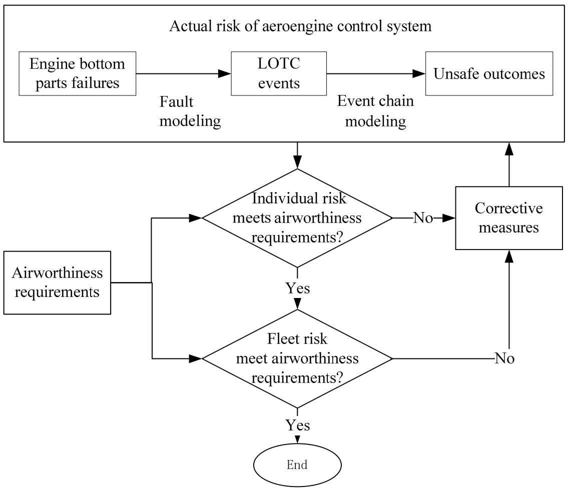
Actual risk of aeroengine control system
Engine bottom parts failures
LOTC events
Unsafe outcomes
Fault modeling
Event chain modeling
Individual risk meets airworthiness requirements?
No
Corrective measures
Airworthiness requirements
Yes
Fleet risk meet airworthiness requirements?
No
Yes
End

Figure 1. Process of engine control system failure risk assessment

3.Fault modeling of engine control system

The actual risk developing from the bottom failures of engine control system to LOTC events is determined by fault modeling, which mainly considers two aspects: the failure probability of a single component and the probability of a single failure developing into a LOTC event.

1）Failure probability of a single component ($\lambda(t)$)

According to statistics from NASA, the two-parameter Weibull distribution is the most valuable distribution function in aeroengine failure analysis[8].The density function of known two parameter Weibull distribution is

$$f(t) = \frac{m}{\eta}(t / \eta)^{m-1}e^{-(t / \eta)^m}, t \geq 0, m, \eta > 0 \tag{1}$$

Where: m is shape parameter; η is scale parameter, concerning that some actual failure data are right censored life data which are replaced by preventive maintenance, m and η can be solved iteratively by numerical method based on the transcendental equation.

In the case that failure rate distributions is known, the operation time T and inspection interval τ

should be considered[9].Therefore, in the next inspection cycle [T, $T+\tau$], the component failure probability $\lambda(t)$ can be expressed as

$$\lambda(t) = 1 - (R_{T+\tau} / R_T) = 1 - \frac{e^{-[(t+\tau)/\eta]^m}}{e^{-(t/\eta)^m}} \tag{2}$$

2）Conditional probability of a single failure developing into a LOTC event (μ)

The conditional probability of a single failure (failure A, for example) developing into a LOTC event can be transformed into the probability of related failures occurring during the exposure time of the failure A. The minimum combination of basic events that results in LOTC events can be found through the fault tree of LOTC events[10].And other failures in the minimum cutset are the related failure of failure A.

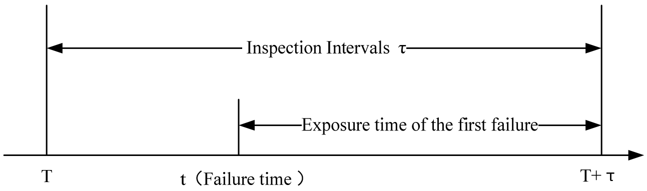

Figure 2. Diagram of failure exposure time

As shown in figure 2，if the first failure occur at t during [T, $T+\tau$]，the exposure time of this failure is $T+\tau$-t. So, the expected time of failure exposure be expressed by

$$E(T+\tau+t) = \int_T^{T+\tau} \frac{m}{\eta}(t/\eta)^{m-1} e^{-(t/\eta)^m} \cdot (T+\tau-t)dt \tag{3}$$

Then combine the average failure ratio of the related failure λ_1， i=1,2...， so, the expression of conditional probability is

$$\mu = E(T+\tau-t) \cdot \prod_1^i \lambda_i \tag{4}$$

4.Event chain modeling of engine control system

Event chain modeling is mainly used to establish the overall process from LOTC events to unsafe outcomes. Control system LOTC is regarded as the primary event of the event chain. By establishing event tree or event sequence diagram model, the serious unsafe consequences such as aircraft disintegration and crash are deduced from LOTC events and through a series of intermediate events.

The conditional probability in the event chain is approximated by the cyclic ratio of the fault. The cyclic ratio is defined as the ratio of flight cycles for damage to propagate from initial condition to condition A1, divided by retirement life. The higher the cyclic ratio is, the faster the damage develops, and the possibility of developing from the current state to the next state is also higher. Table 1 is about conditional probability which is made by FAA and Boeing company[11]. When conditional probability is not very clear, generally, it will be assumed to be 1 conservatively.

Table 1. Conditional probability

Cycle ratio，%	PA1
0～10	1
11～30	0.75
31～50	0.5
51～70	0.1
71～90	0.01
91～100	0.005

There are many criteria to measure the unsafe outcomes. In quantitative analysis, FAA proposes to show the severity of unsafe consequences through injury rate (IR) [11],which is shown in Table 2.

Table 2. Injury ratio

	Crash All	Controlled Crash	Uncontrolled Crash	CFIT[a]	CFIT-Off CFIT	CFIT-On Airport	In-flight Breakup	Runway Departure	Overrun	Lateral Departure	Mid-Air Collision
All Transports	0.67	0.43	0.92	0.69	0.83	0.065	0.99	0.0084	0.019	0.0098	0.72
Prop-Turboprop	0.61	0.30	0.60	0.72				0.0045	0.0004	0.0074	0.78
Large	0.76	0.77	1.05	0.66		0.096		0.0092	0.024	0.0071	0.64
Regional	0.64	0.34	0.91					0.013	0.014	0.0095	
Business	0.71	0.40	0.87	0.74		0.079		0.021	0.024	0.017	1.35

[a]CFIT is abbreviation of Controlled Flight Into Terrain.

5.Risk modeling of engine control system

At the period of transport airplane continuous operation，the risk types can be divided into individual risk and fleet risk, which are used to ensure the safety level of each aircraft and whole fleet are both acceptable.

Individual risk is the highest probability of fatal injury to exposed crew per flight hour when potential unsafe conditions have been identified and corrective actions have not been taken，which is used to determine the existence of unsafe condition and guide the decision-making of corrective measures when the individual aircraft operates in high risk condition.

Fleet risk is the number of times an event is expected to occur in the affected engine fleet when potential unsafe conditions have been identified and corrective measures have not been taken. It is used to predict the fleet risk which haven't taken the corrective measures and to determine the existence of unsafe state and guide the decision of corrective actions.

（1）Individual risk

According to the failure model and event chain model, the individual risk (R_I) of the engine control system failure can be expressed as

$$R_\mathrm{I} = \lambda(t) \cdot \mu \cdot \sum(CP_i \cdot IR_i), i = 1,2\ldots \quad (5)$$

Where: $\lambda(t)$ is the probability of the single failure having occurred before the next checking, see equation (2); μ is the probability of related failures occur and lead to LOTC events during the period of known failures, see equation (4); $\mathrm{CP_i}$ is conditional probability that LOTC events develop to the serious consequence i; $\mathrm{IR_i}$ is the damage probability of the serious consequence i.

（2）Fleet risk

According to the failure model and event chain model, the fleet risk of the engine control system failure can be expressed as

$$R_\mathrm{Fleet} = \mathrm{n} \cdot \sum(CP_i \cdot IR_i), i = 1,2\ldots \quad (6)$$

Where: CP_i and IR_i have the same definition as equation (5); n is the predicted number of engines containing failures in the engine fleet for remaining life. n can be expressed as

$$\mathrm{n} = \sum_{i=1}^{N} \frac{F(T+\tau) - F(T)}{1 - F(T)}, i = 1,2 \ldots \quad (7)$$

F(t) is cumulative distribution function, according to equation (1), it can be expressed as

$$F(t) = 1 - \exp(-(\frac{t}{\eta})^m), t \geq 0, m, \eta > 0 \quad (8)$$

（3）Risk criteria

calculation results of actual risk need to be compared with airworthiness standards to determine whether corresponding risk control measures need to be taken. According to the request of

AC-21-AA-2013-19, the target value of the actual risk level in the continuous airworthiness phase is the maximum risk level in aircraft design phase. For engine control system, the individual risk level caused by engine control system failure must be lower than 1x10^{-7}/FH. At the same time, the fleet risk level caused by engine control system failure must be lower than 0.02[13]. When the actual risk exceeds the airworthiness requirements, corrective or improvement measures must be taken, including changes of inspection interval, replacement in advance and issue of airworthiness directive (AD) when important inspection and design changes are involved.

6.Case study

Taking the actuator of adjustable stator vane (VSV) of Boeing 737 CFM56-7B engine as an example, the actual risk of engine control system failure is analyzed as follow.

6.1 Risk assessment

The actual service lives of VSV actuators of CFM56-7B engine fleet in a certain airline is collected in Table 3 and the preventive replacement data are marked by '*'.

Table 3. Life data of VSV actuators of an engine fleet

No.	Life(FH)	No.	Life(FH)	No.	Life(FH)
1	14000	6	18000*	11	9600
2	17000	7	15200	12	17200
3	17200	8	14600	13	16200
4	9200	9	18000*	14	15400
5	17400	10	15800	15	7900

With Weibull parameter maximum likelihood method based on censored data, the parameters of Weibull distribution can be calculated, m = 8.136, η= 16467. Put them into the equation (2), this failure probability of VSV actuator before next inspection can be expressed as

$$\lambda(t) = 1 - \frac{e^{-[(T+\tau)/16467]^{8.136}}}{e^{-(T/16467)^{8.136}}}$$

The fault tree of the engine control system LOTC shows that VSV actuator failure will directly lead to abnormal opening of VSV, and then lead to abnormal control of VSV, that resulting in thrust oscillation and the crew has to shut down the engine. And eventually LOTC events will happen. In other words, the failure of VSV actuator will inevitably result in LOTC events, that means conditional probability μ =1.

According to the conditional probability in table 1 and injury ratio in table 2, event tree can be established, as shown in figure 3.

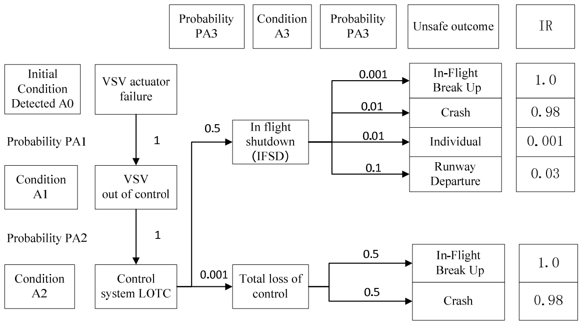

Figure 3. Event tree of engine control system LOTC

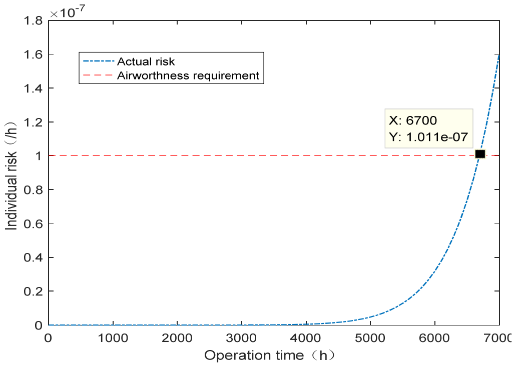

Figure 4. Individual risk（inspection interval is 250h）

Then, it can be calculated as $\sum(CP_i \cdot IR_i) = 0.007$.

Through searching for the airline's aircraft maintenance plan and related engineering instructions, it is known that the airline regularly inspects the fleet's VSV actuators, lubricates and cleans them as necessary. The inspection interval is 250FH. The individual risk of VSV actuator failure is a function of operation time T. It can be expressed as

$$R_{\mathrm{I}} = 0.007 - \frac{0.007e^{-[(T+250)/16467]^{8.136}}}{e^{-(T/16467)^{8.136}}}$$

The fleet risk can be expressed as

$$R_{\mathrm{Fleet}} = 0.07 \cdot \sum^{N} \frac{F(T+250) - F(T)}{1 - F(T)}$$

With the increase of operation time, the risk level caused by the failure of VSV actuators increases gradually. As shown in figure 4, the individual risk increases rapidly after 4000FH. Comparing with the airworthiness risk standard 1x10-7/FH, the actual operational risk exceeds the airworthiness safety requirement when the operation time reaches about 6700FH.

The operation condition of VSV actuators in this engine fleet is showed in Table 4.

Table 4. Operation time of VSV actuator of this engine fleet

No.	1-4	4-8	8-12	12-17	18-20
Operation time （FH）	3000	3500	5500	6500	9500

Table 4 shows that there are three VSV actuators (No. 18-20) operating more than 6700FH in the current engine fleet, so some corrective measures are necessary.

In addition, we can calculate the fleet risk R_{fleet} of the VSV actuator of engine fleet, which is 6.44×10^{-5}. Obviously, it’s lower than airworthiness requirement, 0.02.

6.2 Risk control

The risk level is controlled by optimizing the inspection interval τ of the VSV actuator when the operation time T is fixed. The 5 curves in Figure 5 indicate that the inspection intervals are 100h, 150h, 200H, 250h and 300h respectively, and the actual risk increases with the increase of operation time. If the operation time is limited to 7000h, the intersections of the vertical line and the five straight lines in Figure 5 represent the risk levels corresponding to different inspection intervals when the operation time is 7000h, respectively. It can be found that only when the inspection interval is less than 150h, the risk level meets the requirements.

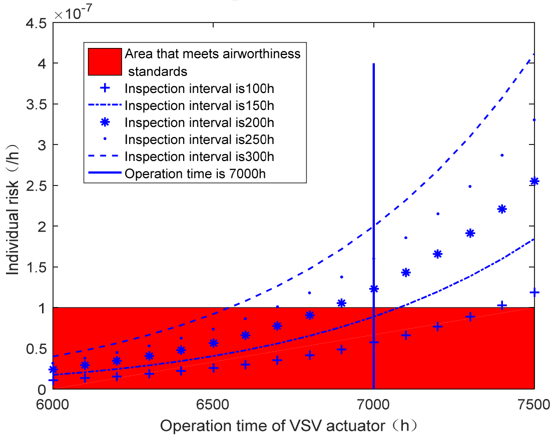

Figure 5. Risk with different inspection intervals

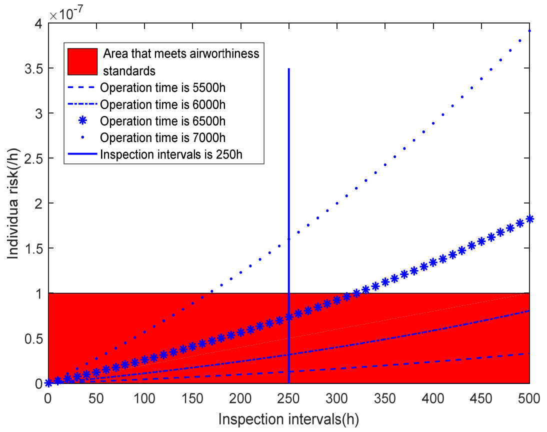

Figure 6. Risk with different operation times

When the inspection interval τ is determined, the actual use time T of the VSV actuator can be controlled by replacing or cleaning ahead of time to control the risk level. The 4 curves in Figure 10 indicate the use time is 5500h, 6000h, 6500h and 7000h respectively. The actual risk increases with the increase of inspection interval. If the current inspection interval remains unchanged for 250 hours, the risk level meets the requirement only when the operation time is controlled within 6500 hours.

According to the above risk judgment, the following four risk control plans are proposed as follow.

Table 5. Risk control plans

No.	Plans	Meet airworthiness requirement?	Cost （Equivalent inspection times）
1	θ=7000，τ=150	Yes	557
2	θ=7000（when T<6500，τ=300; 6500<T<7000, τ=100）	Yes	357
3	θ=7000（when T=6000，τ=500; 6000<T<7000，τ=150）	Yes	280
4	θ=6500，τ=250	Yes	380

According to the calculation, the risks of the four schemes are all controlled within the airworthiness standard. Take an engine life span of 70 thousand hours as an example. It is known that the replacement cost of the VSV actuator is 10 times as much as the inspection cost. The costs of the four plans are as shown in table 5, in which we can see plan 3 is the best solution. The actual risk level of plan 3 is shown in figure 7, which is always lower than airworthiness risk standard and has lowest cost at the same time.

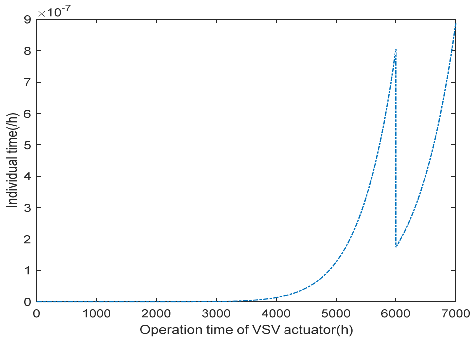

Figure 7. Individual risk with corrective actions

Since all engine control system events can be converted into LOTC events, other related failures can learn from the risk analysis process in this case.

7.Conclusion

This paper focuses on the problem that actual risk of engine control system is higher than expected，analyzes the control system failure mode, and establishes the control system failure model, event chain model and risk model based on PRA. Taking the failure of VSV actuator of CFM56-7B engine as an example to assess the actual risk and analyze the influence of the runtime and inspection interval. The model has a certain generality, which can provide a quantitative reference for the Bureau in assessing the risk of unsafe incidents, and also provide a quantitative basis for the airlines to make use and maintenance plans.

References

[1] Vittal S, Hajela P,Jos hi A .（2004）Review of app roaches to gas turbine life management. In: Aiaa/issmo Multidisciplinary Analysis and Optimization Conference. New York. 876-886.

[2] Aircraft Airworthiness Certification Department. (2013) AC-21-AA-2013-19 Requirements for Continuous Airworthiness System for Type Certificate Holders. http://www.caac.gov.cn/XXGK/XXGK/GFXWJ/201511/t20151102_8377.html.

[3] Atluri, S. N. (1992) Probabilistic evaluation of uncertainties and risks in aerospace components.

Nasa Sti/recon Technical Report N, 94.

[4] Federal Aviation Administration AIR-100. (2003) AC-39-8 Continued Airworthiness Assessment of Powerplant and Auxiliary Power Unit Installations of Transport Category Airplanes. https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/22951.

[5] Ding S T, Zhang G. (2011) Review of probabilistic risk assessment on aero-engine airworthiness. Journal of Aerospace Power, 26(7):1441-1451.

[6] Li N X. (2017) FADEC system safety analysis method based on bayesian network. Nanjing University of Aeronautics and Astronautics. Nanjing.

[7] SAE. (2006) ARP5107B Guidelines for time-limited-dispatch（TLD）analysis for electronic engine control systems. https://www.sae.org/standards/content/arp5107b.

[8] Cole G K. (1998) Practical issues relating to statistical failure analysis of aero gas turbines. Proceedings of the Institution of Mechanical Engineers Part G Journal of Aerospace Engineering,212(3):167-176.

[9] Dai S A，Wang Y，Cai J. (2016) Research on an quantitative risk assessment method for hidden failure of civil aircraft. Journal of Ordnance Equipment Engineering,37(6):162-165.

[10] Jing G X, Jia Z W, Duan Z W. (2004) Application of Minimum Cutset in System Safety Analysis. China Safety Science Journal,14(5):99-102.

[11] Violette M G, Safarian P, Han N, et al. (2015) Transport Airplane Risk Analysis. Journal of Aircraft, 52(2):395-402

[12] Federal Aviation Administration. (2012) 8110.107A Monitor safety/analyze data. https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentid/1020373.

[13] Federal Aviation Administration. (2011) PS-ANM-25-05 Transport airplane risk assessment methodology handbook. https://www.faa.gov/documentlibrary/media/order/faa_order_8100_18.pdf.