Research Article

Classification and Control of Key Factors Affecting the Failure of Aviation Piston Turbocharger Systems Using Model-Based System Safety Analysis

Mengyao Bao,1 Shuiting Ding,2 and Guo Li3

1Civil Aviation Management Institute of China, Beijing 100102, China
2Civil Aviation University of China, Tianjin 300300, China
3Beihang University, Beijing 100083, China

Correspondence should be addressed to Guo Li; 09869@buaa.edu.cn

Received 2 May 2021; Revised 26 July 2021; Accepted 24 August 2021; Published 17 September 2021

A survey conducted by the US National Transportation Safety Board (NTSB) reported that most of the general aviation piston engine accidents could be attributed to turbocharger malfunction-induced engine power failure [1–3]. Therefore, the NTSB has recommended that the US Federal Aviation Administration (FAA) pay particular attention to the issue of turbocharger-induced power reduction and power loss in general aviation piston engines [1, 4–7]. Generally, turbocharger failure is caused by inherent lag characteristics and positive feedback characteristics associated with the pneumatic connection between the turbocharger and the engine [6, 8, 9]. That is, a strong, complex matching connection and closed-loop characteristics occur between the two, resulting in mutual coupling of failure forms. Consequently, it is difficult for traditional analytical methods to decompose and identify the failure modes [10, 11]. It is therefore more difficult to formulate and execute accurate and targeted safety control strategies to ensure turbocharger safety.

In recent years, model-based system safety analysis methods have been developed to overcome the limitations of traditional analytical methods in handling complex coupling engineering problems [13–19]. Model-based safety analysis refers to the introduction of a complex system model that is specifically targeted at an object of study in the failure mode analysis [12, 20–24], that is, the utilization
of an established model to test the system through simulation at each stage of failure mode analysis, in order to verify whether the system can operate according to the functional requirements. In the process, since the failure mode analysis and the system verification test share the same model, model-based safety analysis can reflect the matching and coupling characteristics between systems and effectively address the issue of failure mode identification. The key to model-based system safety analysis is the combination of the model-based development process with the field of safety analysis, which has received increasing amounts of attention since its inception. In 2005, Joshi and Heimdahl [20] from the University of Minnesota and Miller and Whalen from the Rockwell Collins Advanced Technology Centre jointly introduced the model-based development process into the system safety assessment process. In 2006, Joshi et al. [12] further explained the basic idea of the model-based system safety assessment process and analysis methods in a National Aeronautics and Space Administration (NASA) report and compared the model-based system safety assessment process with the traditional process, as shown in Figure 1. The processes show that the model-based system safety assessment process continues to use the traditional process but at the same time incorporates other methods based on the analysis model. In 2007, Joshi and Heimdahl [21] further explained system behaviour modelling. In 2010, Feller [22] clarified the role of model-based system safety analysis in improving system-level safety. Chaudemar et al. [23] introduced this idea into unmanned aerial vehicle (UAV) control systems. Gudemann and Ortmeier [24, 25] further introduced a failure mode probability model into the qualitative model-based system safety analysis and attempted to carry out quantitative model testing on it. The aforementioned analyses have all shown that they can better utilize the system information in the design process to match the development process with the safety assessment process and effectively avoid the uncertain factors of design and safety evaluation transformation, thereby reducing the analytical errors caused by human subjective judgement. At present [26], Advisory Circular No. 20-115D (AC20-115D) issued by the FAA has officially confirmed that RTCA, Inc. document 331 (DO-331) model-based analysis and verification can be used for the airworthiness certification of airborne systems and equipment development.

Therefore, in connection with the complex matching and coupling safety issues of aviation piston engine turbochargers, this study introduces a model-based method for safety analysis of turbocharging systems. To identify the key factors affecting failure, the column profile coordinates of correspondence analysis with the numerical deviation of the key factors are used. The corresponding safety control strategy of each key factor is then proposed and assessed by failure probability. The result of this study provides a new approach to determining the influence factors and potential inducements of the failure issues in the actual operation of aviation piston engine turbocharging systems, with the ultimate goal of ensuring safety of general aircraft.

2. Summary of the Model-Based Safety Assessment Process and Key Technologies for the Turbocharging System

Model-based design refers to a method of design relying on mathematical models and simulations. The established model can test and verify the system through simulation at any stage of the development process, thereby ensuring that the system can operate normally according to the requirements of the functional design. Regarding the difficulty in identifying the mutually coupled failure modes caused by the complex matching connection between the turbocharger and the engine, the model can be an effective tool in the system safety analysis and design process, overcoming the limitations of traditional safety analysis methods. The model-based development process is introduced into the system safety assessment process to form a model-based turbocharging system safety assessment process and analysis method.

Figure 2 gives a schematic diagram of a typical model-based safety assessment process for the engine and its systems.

Compared with the general system safety assessment process, on the basis of the original V-model assessment process, there are interactions between the system model, system safety analysis, and design process involved in the introduced model development process, such that testing, analysis, and verification are carried out at every stage in the development process. Therefore, in connection with the characteristics of the model-based system safety assessment process, the key components in the corresponding system safety analysis methods are as follows: (1) establishment of the system model, (2) description method for the work boundaries and safety boundaries of the failure modes, (3) classification method for the key influencing factors acting on the failure modes, and (4) proposal and verification of the safety control strategies. Detailed discussions of these components are presented in the subsequent sections according to the aforementioned order.

3. Establishment and Verification of the System Simulation Model

Regarding the failure of a piston engine turbocharger, the key is in the complex matching connection that exists between the turbocharger and the engine itself, as well as the coupling of failure modes. Therefore, a system simulation model based on the whole engine is established first to accurately reflect the system pattern, serving as the foundation for the subsequent analysis of the key influencing factors of failures. In this paper, the Rotax 914 aviation piston engine [27] equipped with a new type of two-stage turbocharger is selected and the GT-Power software is used to construct the system simulation model. To overcome the crudity of zero dimensional models and complexity of multidimensional models, a quasi-dimensional model is introduced and three subsystems with corresponding models are considered, namely, the working process model inside the cylinder, air intake and exhaust system model, and
Figure 1: Comparison of the traditional system safety assessment process and the model-based system safety assessment process [12].

Figure 2: Model-based safety assessment process for the engine and its systems.
4 International Journal of Aerospace Engineering

The turbocharger system model. For the working process model, the Wiebe combustion function is used and the Woschni semi-empirical formula is applied in the heat transfer model. For the turbocharger system model, the modelling process includes four parts: turbocharger parameter determination, dynamical model analysis, matching principle between the compressor and turbine, and calculation of the characteristic parameter of the compressor and turbine. To simplify the analysis, the friction and scavenging models are ignored. Besides, it should be pointed out that, for this new turbocharging system, the two-stage compressors are arranged “back to back” and coaxially driven by one turbine, as shown in Figure 3. So, it is dramatically different from the traditional two-stage turbocharging system. The engine performance parameter table comparing the two is provided in Table 1. The details of this new turbocharging system are given in Reference [28].

To verify the accuracy of the model, data from a characteristic experiment are used for comparison with the calculation results of the simulation model. In the experiment, the ambient temperature was 20°C, and the ambient pressure was 100.7 kPa. The calculated operating points were at rotational speeds of 3,000 to 5,500 r/min, with operating points at intervals of 500 r/min, plus an additional operating point of 5,800 r/min. Comparisons of the simulation data and experimental data of the output power and torque changes of the engine are given in Figure 4. Here, it should be pointed out that the torque output is from the output shaft after gearbox. Generally, the simulated values of the model and the experimental values fit fairly well within the allowable range. Therefore, the simulation model reasonably reflects the characteristics of the actual system and can be used for subsequent analysis.

4. Safety Boundary Description Method for the Failure Modes

4.1. Safety Boundaries of the Failure Modes. Generally, as a kind of constraint on the failure mode (i.e., the top event), the safety boundary is the maximum allowable range for the parameters at which the object of study can safely work. In a mathematical model, the safety boundary can be reflected as a parameterized expression of the functional characteristic value or safety feasible region in a situation where the failure mode (i.e., the top event) does not occur.

In this paper, the object of analysis is the safety issue of matching the turbocharging system of the two-stage aviation piston engine with the whole machine; therefore, the influence of the turbocharging system on the safety of the entire engine in the context of engine is a key factor of consideration. In actual analysis, according to the model-based turbocharging system safety assessment process, the safety of the engine subsystems must also be studied from the perspective of the entire system. Therefore, there are two levels of safety requirements in the FHA stage, namely, engine level and turbocharging system level. The safety requirements involved at each level can be characterized through the engine system safety boundaries and the turbocharging system safety boundaries; that is, the maximum allowable range of the working parameters required in a safe working state is first analyzed from the safety boundaries of engine operation, after which the safety boundary requirements for the turbocharging system are issued accordingly, in order to ensure matching. In the PSSA stage, however, it is necessary to further apply the work boundaries and safety boundaries of the turbocharging system and apply the model to analyze the influencing factors that may play a role in the failure modes identified in the FHA stage.

Figure 5 shows the schematic diagram of engine-level FHA safety boundaries, where the possible safe operating conditions and working range of the engine are drawn using the $P_e - n$ coordinate system. The possible safe working area of the engine is restricted to an area enclosed by the maximum power (external characteristic power line) that the engine can deliver, the minimum stable rotational speed $n_{min}$ of the engine (safety boundary line on the left), the maximum working rotational speed $n_{max}$ of the engine (safety boundary line on the right), and the abscissa axis. The safety design of the engine required in this study is determined according to the operating manual of the Rotax 914 engine.

The safety requirements for the two-stage turbocharging engine involved in this study are determined by the engine-level FHA safe operating boundaries. Note that the matching problem of the two-stage turbocharging system leads to many safety problems for the engine. For example, if the turbocharging pressure ratio $\pi_c$ selected is too low, the predetermined turbocharged engine power will not be reached, and the engine exhaust temperature will be too high. On the other hand, if the turbocharging pressure ratio $\pi_c$ selected is too high, the maximum explosion pressure of the engine and the rotational speed of the turbocharger will be excessively high. In addition, since the flow rate $G_f$ and the turbocharging pressure ratio $\pi_c$ are coupled, an inappropriate selection of flow rate will lead to poor match quality between the turbocharger and the engine. More importantly, determining the turbine flow capacity will be impossible, resulting in conditions far from the design values. The schematic diagram of turbocharging system-level FHA safety boundaries is given in Figure 6. The working range of the turbocharging system is the area enclosed by the minimum stable rotational speed $n_{min}$ (left), the rated rotational speed $n_e$ of the engine (right), the maximum allowable temperature $T_{max}$ of the turbine (uppermost), the compressor surge line (upper left), the maximum rotational speed $n_{Cmax}$ allowed by the turbocharger (upper right), and the abscissa axis.

After the safety boundaries (or safe working area) are determined, the failure modes of the turbocharging system can be further reflected through the safety boundaries. Generally, the failure of the turbocharging system may be defined as a single-failure mode or a coupling-failure mode. The schematic diagram of failure modes for the turbocharging system expressed through the safe working area and its safety boundaries is given in Figure 7. Typical single-failure mode and coupling-failure mode can be summarized as follows.
Figure 3: Schematic diagram of the two-stage turbocharging system.

Table 1: Comparison of engine power when using different turbochargers.

| Engine speed (r/min) | Throttle position 40% | Throttle position 60% | Engine power (kW) | Throttle position 80% | Throttle position 100% | Throttle position 115% |
|----------------------|------------------------|-----------------------|-------------------|------------------------|------------------------|------------------------|
|                      | Two-stage | One-stage | Two-stage | One-stage | Two-stage | One-stage | Two-stage | One-stage |
|----------------------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| 3000                 | 25.48     | 25.29     | 27.47     | 27.77     | 31.44     | 31.75     | 30.28     | 30.59     |
| 4000                 | 31.77     | 31.91     | 39.72     | 39.70     | 43.53     | 43.51     | 47.67     | 47.65     |
| 4500                 | 34.09     | 34.23     | 45.35     | 45.50     | 50.32     | 50.30     | 55.45     | 55.60     |
| 5000                 | 37.07     | 37.05     | 50.15     | 50.14     | 57.28     | 57.26     | 63.40     | 63.39     |
| 5500                 | 37.57     | 37.55     | 54.13     | 54.11     | 63.24     | 63.22     | 69.03     | 69.02     |

Figure 4: Comparison of the simulated and experimental data of power and torque.
4.2. Determining the Boundaries of the Failure Modes. After the work boundary and safety boundary of the failure modes are determined, whether the system has failed can be judged by the containment relationship between the safety boundary and the work boundary. With reference to the requirements of ARP4761 [29], it is necessary to identify all possible failure modes that affect system functions in the FHA stage and to analyze the causes of the failure modes identified in the FHA stage within PSSA. This means that the failure mode is used as the top event, the influencing factors that may play a role in the failure mode are decomposed and parameterized, and safety protection measures are derived.

The relationship between failure and the boundaries in the model-based system safety analysis method is shown in Figure 8. For example, $E_0, E_1, E_2$, and $E_3$ represent the state points on the work boundary of the turbocharging system in operation under different work conditions. If point $E_0$, representing the working state of the turbocharging system, operates within the safe working area to point $E_1$, the turbocharging system manifests normal operation. If point $E_1$ moves from the safe working area to point $E_2$ on the safety boundary, the turbocharging system still manifests normal operation, but there are potential safety hazards. If point $E_2$ moves from the safety boundary to point $E_3$ in the unsafe area, the turbocharging system can no longer operate normally, exhibiting a single-failure mode or even a coupling-failure mode. Turbocharger failures can be judged by the containment relationship between the work boundary and the safety boundary. If the work boundary point during system operation exceeds the safety boundary, entering the unsafe area, then the system is considered to fail. If the system operates in the safe area or on the safety boundary, then the system is considered to be normal. Therefore, safety of the system can be ensured by controlling the actual work boundary in turbocharging system operation within a range that does not exceed the safety boundary.

5. Classification of the Key Influencing Factors for Failure Based on the Correspondence Analysis Method

For the turbocharging system involved in this paper, an improved correspondence analysis method is used to probe the coupling relationship and degree of closeness between the failure modes and key influencing factors in that system, in order to identify the key factors.

5.1. Analysis Principles and Processes of the Improved Correspondence Analysis. Correspondence analysis is a recently developed statistical analysis technique with multivariate-dependent variables, and its essence is
For surrogate model construction and data type normalization, the details are given in Reference [5]. The present study only focuses on the classification of the key influencing factors. That is, when the order of magnitude of the sample points is large, the safety margins of the work boundaries become the variable points (column points), and the criticality of these key influencing factors regarding the safety of the turbocharging system is determined according to the relationship between the key influencing factors (independent variables) and the safety margins of the work boundaries (dependent variables). Generally, the specific implementation process includes surrogate model construction based on the response surface methodology, data type normalization, and classification of the key influencing factors.

For surrogate model construction and data type normalization, the details are given in Reference [5]. The present study only focuses on the classification of the key influencing factors. That is, when the order of magnitude of the sample points is large, the safety margins of the work boundaries become the variable points (column points), and the criticality of these key influencing factors regarding the safety of the turbocharging system is determined according to the relationship between the key influencing factors (independent variables) and the safety margins of the work boundaries (dependent variables). Generally, the specific implementation process includes surrogate model construction based on the response surface methodology, data type normalization, and classification of the key influencing factors.

5.2. Realization of the Classification of Key Influencing Factors for the Turbocharging System

5.2.1. Determination of the Working Range. This particular piston aviation engine equipped with a turbocharging system is mainly used for a certain type of UAV. The flight envelope requirements for that type of UAV at full altitude are given in Table 2. The typical operating conditions at flight altitudes of 7-10 km are extracted for additional analysis. The calculation sample points in connection with different altitudes are shown in Table 3.

5.2.2. Selection of the Variable Points (Influencing Factors). This paper focuses on the operating conditions of an engine with a turbocharging system during high-altitude or high-speed cruise (long-term working state of the engine), which includes altitudes of 7-10 km, throttle valve openings of 70%-100%, and engine rotational speeds of 4,200-5,500 r/min. In a situation where the control system is not taken into consideration, the settings of the key influencing factors can be represented by a group of controllable design parameters. These parameters include the throttle position $e_1$, the diameter of the wastegate $e_2$, the altitude $e_3$, the rotational speed of the engine $e_4$, and the diameter of the exhaust pipe $e_5$. In addition, the work boundaries for this type of turbocharging system include turbine inlet temperature, rotational speed, compressor pressure ratio, and maximum explosion pressure.

\[
\Delta d_p^{(i)} = \sqrt{\left([F_{j2}(i) - F_{j1}(i)]^2 + ([F_{j1}(i) - F_{j1}(i)]^2}\right)^2, \quad j = 1, 2, \ldots, p \tag{1}
\]

where $F_{j1}$ and $F_{j2}$ are the first and second coordinate vectors of $F$ before the column point changes, respectively, and $F_{j1}(i)$ and $F_{j2}(i)$ are the first and second coordinate vectors of $F$ after the column point changes, respectively.
5.2.3. Generation and Verification of the Surrogate Model. The initial simulation conditions for the controllable design parameters are given according to the operating conditions of the turbocharging system, as shown in Table 4. For the described five controllable design parameters within the range considered (operating boundaries in the turbocharging system design), the central composite-faced (CCF) design is applied to generate 36 sample points. A second-order response surface surrogate model is constructed by calculating the key influencing factors and the values of various work boundary points in the system model output. To ensure the accuracy of the surrogate model, the relative errors between the surrogate model and the simulation model are determined, as shown in Figure 10. The errors generated by using the surrogate model for analysis are generally less than 8% and can be acceptable in the following study of this paper.

5.2.4. Determination of the Safety Margins. According to the principle of data type normalization, each variable point in the original matrix X is transformed into the safety margin of each corresponding work boundary, i.e., the variable points in data matrix Y, which are the safety margin of the turbine inlet temperature ($Y_1$), the safety margin of rotational speed of the turbocharger rotor ($Y_2$), the compressor surge margin ($Y_3$), and the safety margin of the maximum explosion pressure ($Y_4$).

5.3. Result Analysis and Determination of the Key Influencing Factors. Correspondence analysis is directly carried out on the sample points in data matrix Y, and the results are shown in Figure 11. When there are too many sample points, it is difficult to intuitively observe the degree of importance of each key influencing factor in the sample points to the variable points, and classification cannot be achieved. Therefore, the key influencing factor classification method given in Section 3 is used for processing. First, based on direct correspondence analysis, the column profile coordinate $F$ corresponding to each variable point is extracted. Each controllable design parameter in the set of sample points is changed one by one in the same proportion. In the analysis, the throttle position $e_1$, the diameter of the wastegate $e_2$, the altitude $e_3$, the rotational speed of the engine $e_4$, and the diameter of the exhaust pipe $e_5$ are increased one by one by 5%, 10%, 20%, and 30%, respectively. The new column profile coordinate $F(i)$ generated for each variable point is projected onto the same two-dimensional plane, as shown in Figure 12. Therefore, when the numerical value of each key influencing factor is changed, sorting can be carried out according to the size of the distance in the relative change in the position of the initial column point corresponding to each column point on the two-dimensional scatter plot. A greater change in the distance means a more critical key influencing factor and vice versa.

Based on the results from Figure 12, the deviation distances for the initial column points generated by the changes in each key influencing factor are determined, as shown in Figure 13, where sorting is carried out. Changes in the diameter of the wastegate $e_2$ have the greatest effect on the safety margin of each work boundary. According to the deviation distance, this parameter affects the safety margin of each work boundary in the following order from most to least impact: safety margin of the turbine inlet temperature ($Y_1$), compressor surge margin ($Y_3$), safety margin of the rotational speed of the turbocharger rotor ($Y_2$), and safety margin of the maximum explosion pressure ($Y_4$). In addition, the rotational speed of the engine $e_4$ also has a relatively strong effect on the safety margins of the work boundaries, and its impacts on the work boundaries are $Y_1 > Y_2 > Y_3 > Y_4$. The throttle position $e_1$, the altitude $e_3$, and the diameter of the exhaust pipe $e_5$ have relatively weak effects on the safety margin of each work boundary. Therefore, these parameters are not regarded as key influencing factors.
Since the effects of the diameter of the wastegate $e_2$ on the safety margin of each work boundary have been determined to be the most critical, it should be considered first when it comes to control. Note that for turbocharge piston engines in general, the wastegate diameter is a key adjustment parameter and should be given special attention. Therefore, the analytical conclusions of this paper are in line with the consensus of turbocharged piston engine control, which once again suggests reliability of the proposed method.

6. Safety Control Strategies and Verification for the Key Influencing Factors

The classification analysis of the key influencing factors in the turbocharging system shows that changes in the key influencing factors all play a primary role in the deviation of the safety margins of the work boundaries (column points) or the sample point clusters (row points), and the degree of influence is often greater than those of the general influencing factors. Therefore, to ensure that when abnormal situations emerge in the operation of this system, the sample point clusters do not deviate or deviate as little as possible from their normal positions, the controllable key influencing factors in the design should be controlled first.

Since the diameter of the wastegate $e_2$ is the most critical influencing factor in the complex matching connection between the turbocharging system and the engine, by regulating $e_2$ (or the diameter of the wastegate), the fuel gas flow through the turbine is regulated. This changes the rotational speed of the turbocharger rotor and the output power of the turbine, thus changing the compressor flow and turbocharging ratio. The turbocharging pressure can reach the target...
value of the pressure stabilization chamber, thereby achieving a good match between the turbocharger and the engine.

The safety control strategies of the turbocharging system will be studied in this section. Additionally, according to the method described in Section 5, the influencing factors of the two-stage turbocharging system after the safety control strategy implementation will also be reclassified and analyzed.

6.1. Determination of the Safety Control Strategies of the Turbocharging System. In regard to the regulation measures for the turbocharger, the simplest and most commonly used measure at present is bypass venting at the turbine end, where the wastegate driven by the motor through the actuator is its core component. Therefore, a wastegate control model is added to the original model to analyze the safety control strategies, as shown in Figure 14.

6.2. Analysis of the Role of Safety Control Strategies. In order to determine the degree of importance of other influencing factors after the safety control strategy is used, under the premise that types of influencing factors \( e_1-e_5 \), initial simulation conditions, and work boundaries of the turbocharging system \( Y_1-Y_4 \) are unchanged, classification of the influencing factors is achieved as follows. First, the response surface method is used to extract the surrogate model for the two-stage turbocharged engine system model after the safety control strategy is used. \( N \) sample points are randomly generated, and various corresponding work boundary values are generated through the surrogate model and then transformed into the safety margin of each work boundary required by the variable points in the correspondence analysis. Finally, correspondence analysis is carried out with the sample points and the variable points.

![Figure 12](image-url)

**Figure 12:** Relative position deviations generated in the safety margin of the work boundary with increase in the key influencing factors.
Classification involves first extracting the column profile coordinate $F$ corresponding to each variable point on the basis of the aforementioned correspondence analysis and then increasing the influencing factors $e_1$ to $e_5$ by $+5\%$, $+10\%$, $+20\%$, and $+30\%$ one by one in the same proportion, respectively. The new column profile coordinate $F^{(i)}$ generated for...

| Influencing factor | $Y_1$ | $Y_2$ | $Y_3$ | $Y_4$ |
|-------------------|-------|-------|-------|-------|
| $e_1$             | 0.0000| 0.0000| 0.0000| 0.0000|
| $e_2$             | 0.0005| 0.0005| 0.0005| 0.0005|
| $e_3$             | 0.0010| 0.0010| 0.0010| 0.0010|
| $e_4$             | 0.0015| 0.0015| 0.0015| 0.0015|
| $e_5$             | 0.0020| 0.0020| 0.0020| 0.0020|

Figure 13: Relative deviations in the safety margins generated by changes in the influencing factors.

Figure 14: Safety control strategy with added wastegate control.
each variable point is projected onto the same two-dimensional plane. Figure 15 shows the results after the increases.

As the degree of deviation of each influencing factor continues to increase, deviations generated by \( e_3 \) and \( e_4 \) have greater effects on the safety margin of each work boundary, but the effects of \( e_1 \) and \( e_5 \) are not significant. Using the +30% change as an example, the change in the distance between the relative positions of each column point on the two-dimensional scatter plot before and after the safety control strategy is used is given in Figure 16, where the deviation distances of the initial column points due to the change in each influencing factor can be further sorted to complete the reclassification.

Figure 16 shows that \( e_3 \) has the greatest influence on the safety margin of each work boundary, making itself the most critical influencing factor in the new round. Because the effects on the safety margins of \( Y_1 \) and \( Y_3 \) are comparatively strong, \( e_3 \) is still a key influencing factor. Therefore, \( e_3 \) and \( e_4 \) are determined to be the key factors in the new round. If the turbocharging system still cannot satisfy the system safety requirements after the safety control strategy is executed on \( e_2 \), it is necessary to propose a corresponding safety control strategy for \( e_3 \) in the subsequent safety analysis.

6.3. Verification Method for the Safety Analysis of the Turbocharging System. In the analysis described in the previous section, the two-stage turbocharged engine model is used as the object of analysis, and the classification and positioning of the influencing factors in terms of their effects on the failure modes are realized by introducing the improved correspondence analysis method. This determines the key
influencing factors in the PSSA stage and ultimately yields the safety control strategy for the turbocharging system. However, whether the safety strategy can improve the safety level and quantification of the improvement is unknown. Therefore, in the SSA stage, to determine whether the analyzed turbocharging system model reaches the acceptable design safety level after the safety control strategy is used, the safety of this system is verified through the Monte Carlo method in this section. The Monte Carlo method is used to assess the failure probability of each failure mode, and the differences in the system failure modes and probabilities before and after using the safety control strategy are compared to explore the effectiveness of the safety control strategy.

6.3.1. Monte Carlo-Based Verification Method for Safety Analysis of the Turbocharging System. From Section 4, the safety boundary is a constraint for the operation of the turbocharging system, i.e., the maximum allowable range of parameters under safe operating conditions, which is composed of the compressor surge line \( \text{Surge line} \), the line for the maximum temperature allowed by the turbine \( T_{\text{rmax}} \), the line for the maximum rotational speed allowed by the turbocharger \( n_{\text{TCmax}} \), the line for the minimum stable rotational speed of the engine \( n_{\text{min}} \), and the line for the rated rotational speed of the engine \( n_{e} \), as shown in Figure 17.

![Figure 16: Comparison of the changes in the distance between the relative positions of each column point before and after using the safety control strategy.](image)

![Figure 17: Relationship between the system operating state and safety boundary.](image)

In system safety analysis, every safety boundary in Figure 17 can constrain a failure mode. Therefore, one can set the safety boundaries representing the constraints of the failure modes as \( y_{sm}(m = 1, 2, \cdots, n) \) and the work boundaries representing the system operating state as \( y_{om}(m = 1, 2, \cdots, n) \), where in connection with every safety boundary \( y_{sm} \) and work boundary \( y_{om} \), \( G(E) \) is the system limit state function corresponding to the safety margin of the work boundary for determining the failure mode. The
safety margin of each work boundary can be expressed through a group of system limit state functions:

\[ G(E) = \frac{y_{sm} - y_{om}}{y_{sm}}. \]  

(2)

When \( G(E) < 0 \), the system is operating outside the safety boundary; that is, when operating in the unsafe area, the system is in an unsafe working state. When \( G(E) = 0 \) or \( G(E) > 0 \), the system is operating on the safety boundary or within the safe area and is in a safe working state. In addition, from the perspective of safety, it is usually better to have a greater safety margin, but increasing the safety margin requires sacrificing some performance and economic benefits. Although decreasing the safety margin can reduce costs, it may result in greater economic losses, which requires search of a better safety margin interval within the safety margin range. However, due to the inconsistent forms of expression of the safety margin in the existing research, the application of the margin is in the qualitative description stage. Therefore, equation (3) shows that when the working state of the system is safe, the value range of \( G(E) \) is \([0, 1]\). When \( G(E) = 1 \), the system is operating far from the limiting value of the safety boundary, and the system safety allowance is at its maximum. When \( G(E) = 0 \), the system is operating on the safety boundary, the system safety allowance is at its minimum, and potential safety hazards may exist. Therefore, to comprehensively consider safety, power performance, and economic requirements of the system, it is assumed that if the safety margin of the work boundary for the system under analysis is between 0.05 and 0.5 and the frequency of occurrence is concentrated in a better state of system operation, then a certain allowance exists in the work boundary and the safety boundary of system operation at this time, and the working state is safe.

In addition, to further quantitatively analyze the failure probability of the system, the Monte Carlo method is used to simulate the failure probability \( p_j \) of any failure mode, which can be expressed as

\[ p_j = P\{G(E) < 0\} = \int_{D_j} f(E) dE. \]  

(3)

Then, the system safety index \( \beta \) can be expressed as

\[ \beta = \Phi^{-1} \left( 1 - p_j \right), \]  

(4)

where \( E = \{e_1, e_2, \ldots, e_n\}^T \) is a random variable of \( n \) dimensions, i.e., the vector of the influencing factor; \( f(E) = f(e_1, e_2, \ldots, e_n) \) is the joint probability density function of basic random variables; \( G(E) \) is the group of system limit state functions; \( D_j \) is the failure area corresponding to \( G(E) \); and \( \Phi(.) \) is the cumulative probability under standard normal distribution.

Therefore, the failure probability expressed using the Monte Carlo method is written as

\[ p_{\wedge} = \frac{1}{N} \sum_{i=1}^{N} I[G(E_{i})], \]  

(5)

where \( N \) is the number of samples and ‘\( \wedge \)’ is the sample value. Moreover, when \( G(E_{i}) < 0 \), \( I[G(E_{i})] = 1 \); when \( G(E_{i}) \geq 0 \), \( I[G(E_{i})] = 0 \).

In the subsequent analysis, the failure probabilities of the turbocharging system before and after the safety strategy is used can be obtained by equation (3).

6.3.2. Probability Distribution Characteristics of the Influencing Factors. For the turbocharging system, the input variables are influencing factors that are considered to play a more important role in the work boundary changes of the system, i.e., the influencing factors determined in the analysis in Section 5.2, including \( e_1 \) to \( e_5 \), whereas the output variables are the functions for judging the limit states of the system failure modes, i.e., the system limit state functions determined in the analysis in Section 5.2, including \( Y_1 \) to \( Y_8 \). The probability distribution characteristics and related parameters of each influencing factor involved in the sample points are shown in Table 5, where the parameter values are derived from expert experience or statistical data. Note that the distribution functions for the input variables (influencing factors) and the determination of related parameters directly decide the results of safety analysis. In an actual analysis, since there are many factors that affect system safety, the corresponding statistical characteristics would be more complicated.

6.3.3. Analysis of Impact of the Safety Control Strategy on the Failure Probability of the Turbocharging System. The input variables are randomly sampled, and calculation is carried out by using the two-stage turbocharged engine model. Probability distribution characteristics and related parameters of each system limit state function are obtained from the statistical results. Figures 18–21 show the probability distributions of the safety margin for the turbine inlet temperature, the safety margin for the turbine inlet temperature, the safety margin for the rotational speed of the turbocharger rotor, the compressor surge margin, and the safety margin for the maximum explosion pressure before and after the safety control strategy is used, respectively. Overall, the distribution of each safety margin is more scattered before the safety control strategy is used and is more concentrated after, with the safety margin distribution mostly concentrated within \([0.02, 0.2]\). For example, the distribution interval for the safety margin of the rotational speed of the turbocharger rotor is changed from \([-0.4, 0.8]\) to \([-0.2, 0.5]\). Note that the frequency of occurrence for the safety margin distribution is clearly reduced when \( G(E) < 0 \), which illustrates that the safety level of the rotational speed of the turbocharger rotor is improved after the control strategy is used and that the system operating state is good. The other three aspects all exhibit similar trends. Besides, it should be noted that the internal lubrication of the turbocharger is also very...
important for the failure of the turbocharger. However, it is not considered here because it is associated with different and more complex engine-level system models, which will be studied in more depth in future research.

To further analyze the effect of the safety control strategy on the failure probability of each failure mode, the changes in the failure probabilities of each failure mode before and after the safety control strategy is used are given in Figure 22. After the safety control strategy is used, the failure probability of the system limit state function \( G(E) \) corresponding to the safety margin of each work boundary is lower, where the largest decrease occurs in the failure probability of the failure mode for excess revolution of the turbocharger rotor. This illustrates that after the safety control strategy is used on the wastegate, the effect on the rotational speed of the turbocharger rotor is the most significant. When some of the exhaust is discharged through the wastegate, the exhaust flow through the turbine and the exhaust back pressure decrease, thereby preventing overshooting the rotational speed of the turbocharger. If a change is generated in the degree of opening of the corresponding wastegate, changing the exhaust volume and air pressure of the turbine achieves a different rotational speed of the turbocharger rotor, thereby affecting the turbocharging pressure of the compressor intake, and therefore, the effect on the compressor surge margin is more significant. Since the connection between the turbocharger and the engine is pneumatic, the lag in the response of the compressor makes the effect of the maximum explosion pressure of the engine weaker than those of the rotational speed of the turbocharger rotor and the compressor surge margin. The positive feedback characteristics reflected will ultimately be embodied in the probability changes in the safety margin of the turbine inlet temperature. Therefore, the above analysis shows that the safety control strategy used for the turbocharging system can improve the safety level, but the degree of the improvement in the safety level of different parameters is not the same.

### Table 5: Probability distribution characteristics and related parameters of influencing factors (normalized).

| Influencing factor                  | Distribution type | Expectation | Variance |
|-------------------------------------|-------------------|-------------|----------|
| Throttle position, \( e_1 \)       | Normal distribution | 1           | 0.5      |
| Diameter of the wastegate, \( e_2 \) | Normal distribution | 2           | 0.5      |
| Altitude, \( e_3 \)                | Normal distribution | 0.6         | 0.3      |
| Rotational speed of the engine, \( e_4 \) | Normal distribution | 0.6         | 0.3      |
| Diameter of the exhaust pipe, \( e_5 \) | Normal distribution | 2           | 0.5      |

**Figure 18:** Probability distribution of the safety margin for the turbine inlet temperature \( Y_1 \).
Figure 19: Probability distribution of the safety margin for the rotational speed $Y_2$.

Figure 20: Probability distribution of the compressor surge margin $Y_3$. 
7. Conclusion

Starting from the general aircraft safety problems caused by the failure of the aviation piston engine turbocharging system and limitations of traditional safety analysis methods regarding complex matching and coupling safety problems, this paper incorporates a model-based system safety analysis method into the safety analysis of a turbocharging system, with the goal of forging a whole set of analytical processes and methods that accurately identify the key influencing factors of the failures. Safety control strategies are accordingly proposed and verified. The research results are summarized as follows.

1. The model-based system safety processes and methods can handle the complex coupling failure problems of turbocharging. The key components include establishment of the system model, description method for the work boundaries and safety boundaries of the failure modes, classification method for the key influencing factors of the failure modes, and proposal and verification of safety control strategies.

2. On the basis of the established two-stage turbocharged engine model, the response surface method is used first to abstract the surrogate model from the analysis model and to determine the relationship between the influencing factors (controllable design parameters) and the work boundaries. The surrogate model is randomly sampled to generate the basic data required for correspondence analysis and to improve the correspondence analysis method, forming a classification method based on changes in the column profile coordinate $F$ with the numerical deviations of the influencing factors. This determines the degree of criticality of these influencing factors to the safety of the turbocharging system and realizes
eventual classification of the key influencing factors. The results show that the diameter of the wastegate $e_2$ is the most important factor affecting the safety margin of each work boundary.

(3) By adjusting the diameter of the wastegate $e_2$ in the safety control strategy, the distribution of the safety margin can be more concentrated and the failure probability is decreased. After implementation of the safety control strategy, the distribution interval of the safety margin for the turbine inlet temperature, rotational speed, compressor surge margin, and maximum explosion pressure is decreased from $[-0.06, 0.32], [-0.4, 0.8], [-0.8, 1.3]$, and $[-0.24, 0.9]$ to $[-0.02, 0.18], [-0.2, 0.5], [-0.35, 1.2]$, and $[-0.1, 0.58]$, respectively.

**Nomenclature**

$D_f$: The failure area corresponding to $G(E)$

$d_f$: The distance before and after a change in the column point

$E$: Random variable of $n$ dimensions, $E = \{e_1, e_2, \ldots, e_i\}$

$e$: Key influencing factors

$e_1$: Opening of the throttle valve

$e_2$: Diameter of the wastegate

$e_3$: Altitude

$e_4$: Rotational speed of the engine

$e_5$: Diameter of the exhaust pipe

$F_{11}$: First vectors of the row profile coordinates $F$

$F_{12}$: Second vectors of the row profile coordinates $F$

$f(E)$: Column profile coordinates

$G(E)$: A group of system limit state functions

$G_c$: Flow rate

$P_c$: Power

$P_f$: Failure probability

$PC1$: The first dimension of the two-dimensional scatter plot for correspondence analysis

$PC2$: The second dimension of the two-dimensional scatter plot for correspondence analysis

$X$: Variable points in the original matrix, $X = (x_{ij})_{nxp}$

$x$: Value of the $j^{th}$ index in the $i^{th}$ sample

$Y$: Postindex normalization data matrix, $Y = (y_{ij})_{npc}$

$y_{omi}$: Safety boundaries representing the constraints of failure modes

$y_{omi}$: Work boundaries representing the system operating state

$\beta$: System safety index

$\tau$: Turbocharging pressure ratio

$\varphi$: Cumulative probability under standard normal distribution

FHA: Functional hazard analysis

FTA: Fault tree analysis

SSA: System safety assessment

PSSA: Preliminary system safety assessment

FMEA: Failure mode and effect analysis

UAV: Unmanned aerial vehicle.

**Data Availability**

The analysis data used to support the findings of this study are included within the article.

**Conflicts of Interest**

The authors declare that they have no conflicts of interest.

**Acknowledgments**

This work was supported by the Innovation Team of Complex System Safety and Airworthiness of Aeroengine from the Co-Innovation Center for Advanced Aeroengine of China. Funding was provided by the National Natural Science Foundation of China and the Civil Aviation Administration of China (No. U1833109).

**References**

[1] D. Hersman, *National Transportation Safety Board, National Transportation Safety Board*, Washington, DC, USA, 2009.

[2] G. A. Gordon, “FAA will study accidents of turbocharged aircraft,” *Business & Commercial Aviation*, vol. 75, no. 2, p. 18, 1994.

[3] P. Katz, “Turbocharger trouble,” *Plane & Pilot*, vol. 44, no. 9, pp. 78–80, 2008.

[4] "Emergency procedures for turbocharger failures sought," *Air Safety Week*, vol. 22, no. 21, p. 5, 2008.

[5] M. Bao, S. Ding, and G. Li, “Identification of key factors affecting the failure of aviation piston engine turbochargers based on an improved correspondence analysis-polar angle-based classification,” *Chinese Journal of Aeronautics*, vol. 34, no. 5, pp. 466–484, 2021.

[6] W. E. Williams, *A Summary of Unmanned Aircraft Accident/Incident Data: Human Factors Implications*, Federal Aviation Administration, Oklahoma City, OK, USA, 2004.

[7] M. T. DeGarmo, *Issues Concerning Integration of Unmanned Aerial Vehicles in Civil Airspace*, The MITRE Corporation, Center for Advanced Aviation System Development, McLean, VA, USA, 2004.

[8] M. T. DeGarmo, *Issues Concerning Integration of Unmanned Aerial Vehicles in Civil Airspace*, Federal Aviation Administration, 2004.

[9] Y. Zhou, L. Shao, C. Zhang et al., “Numerical and experimental investigation on dynamic performance of bump foil journal bearing based on journal orbit,” *Chinese Journal of Aeronautics*, vol. 34, no. 2, pp. 586–600, 2021.

[10] K. Xu, M. Zhu, and Z. Fan, “FMEA of turbocharged diesel engine system using fuzzy inferencing,” *SAE Transactions*, vol. 109, no. 3, pp. 529–535, 2000.

[11] K. Xu, L. C. Tang, M. Xie, S. L. Ho, and M. L. Zhu, “Fuzzy assessment of FMEA for engine systems,” *Reliability Engineering & System Safety*, vol. 75, no. 1, pp. 17–29, 2002.

[12] A. Joshi, M. W. Whalen, and M. P. Heimdahl, *Model-Based Safety Analysis Final Report*, NASA Techreport, 2006.

[13] M. Whalen, D. Cofer, S. Miller, B. H. Krogh, and W. Storm, “Integration of formal analysis into a model-based software development process,” in *Formal Methods for Industrial Critical Systems*, pp. 68–84, Springer, 2007.
[14] G. Berry, “Synchronous design and verification of critical embedded systems using SCADE and Esterel,” in Formal Methods for Industrial Critical Systems, p. 2, Springer, 2007.
[15] M. G. Hinchey and J. P. Bowen, Industrial strength formal methods in practice, Springer, London, UK, 1999.
[16] D. Jackson, B. Tannenbaum, and W. Jachimczyk, ”Adoption, impact, and vision of model-based design,” in Modeling and Simulation for Military Applications, pp. 1–10, Orlando, FL, USA, 2006.
[17] M. Baleani, A. Ferrari, L. Mangeruca et al., “Correct-by-Construction Transformations across Design Environments for Model-Based Embedded Software Development,” in Design, Automation and Test in Europe, pp. 1044–1049, Munich, Germany, 2005.
[18] M. Ahmadian, Z. J. Nazari, N. Nakhaee, and Z. Kostic, ”Model based design and SDR,” 2nd IEE/EURASIP Conference on DSPenabledRadio, 2005, pp. 1–8, London, UK, 2005.
[19] S. P. Miller, A. C. Tribble, M. Whalen, and M. P. E. Heimdahl, ”Proving the shalls,” International Journal on Software Tools for Technology, vol. 8, no. 4-5, pp. 303–319, 2006.
[20] A. Joshi, S. P. Miller, M. Whalen, and M. P. E. Heimdahl, ”A proposal for model-based safety analysis,” in 24th Digital Avionics Systems Conference, pp. 1–13, Washington, DC, USA, 2005.
[21] A. Joshi and M. Heimdahl, ”Behavioral fault modeling for model-based safety analysis,” in 10th IEEE High Assurance Systems Engineering Symposium (HASE’07), pp. 199–208, Plano, TX, USA, 2007.
[22] P. H. Feiler, ”Model-based validation of safety-critical embedded systems,” in 2010 IEEE Aerospace Conference, pp. 1–10, Big Sky, MT, USA, 2010.
[23] J. C. Chaudemar, E. Bensana, and C. Seguin, ”Model Based Safety Analysis for an Unmanned Aerial System,” in DRHE 2010 - Dependable Robots in Human Environments, pp. 16–17, Toulouse, France, 2010.
[24] M. Güdemann and F. Ortmeier, ”Probabilistic model-based safety analysis,” Electronic Proceedings in Theoretical Computer Science, vol. 28, pp. 114–128, 2010.
[25] N. Tanaka, H. Yomiya, and K. Ogawa, ”A method to support the accountability of safety cases by integrating safety analysis and model-based design,” in Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops, pp. 23–35, Springer, 2020.
[26] AC 20-115C, Airborne Software Assurance, Federal Aviation Administration, 2013.
[27] BRP-Rotax GmbH&Co KG, Operation Manual for Rotax Engine Type 914 F, BRP-Rotax GmbH&Co KG, Gunskirchen, Austria, 2007.
[28] Y. Zhou, F. Du, S. Ding, and X. Liu, ”A two-stage turbocharge with low pneumatics inertance and fast response,” US Patent ZL201410790321.6, 2012.
[29] ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, Society of Automotive Engineers, 1996.
[30] G. Michael, International Encyclopedia of the Social & Behavioral Sciences: Correspondence Analysis, Elsevier, Barcelona, Spain, 2nd edition, 2015.
[31] M. J. Greenacre, Correspondence Analysis in Practice, Chapman & Hall/CRC, London, UK, 2nd edition, 2007.
[32] N. Sourial, C. Wolfson, B. Zhu et al., ”Correspondence analysis is a useful tool to uncover the relationships among categorical variables,” Journal of Clinical Epidemiology, vol. 63, no. 6, pp. 638–646, 2010.