An Integrated Safety and Formal Analysis for Aircraft Landing System Based on SysML

Yuan Yuan, Jian Jiao* and Mengwei Wei
School of Reliability and Systems Engineering, Beihang University, Beijing, China

*Corresponding author email: jiaojian@buaa.edu.cn

Abstract. The integration and interaction of multiple factors in large-scale system such as aircraft is the main reason of safety problem. For example, the aircraft can be affected by a variety of interactive factors due to changes in pilot conditions, avionics equipment and environmental state during flight. Aiming at the process of carrier aircraft landing, this paper proposes a formal modeling method based on System Modeling Language (SysML) to describe and analyze the safety of system. Firstly, the method based on SysML is detailed to model the structural and behavioural aspects, relying on the analysis of mission and/or behavior process. Then, the integrated method of SysML and Simulink, using the TGG method, is adopted to facilitate the analysis of the behavior processes. Finally, the attitude control during the aircraft landing process is taken as an example to assess the deviation and the dangerous time variation of the system in different disturbance degrees, which will help to make a better safety strategy.

1. Introduction
Advanced large-scale equipment system, such as aircraft, satellite and modern ship, are getting more complex and emerging more new risks due to the integrating of different functions and the interactions of factors between systems. Aircraft flight is a typical complex process where various technical factors, including flight dynamics, control guidance and information communication, etc., can affect its safety. In terms of aviation safety simulation, NASA established an aviation safety simulation model [1]. Zhu et al. [2] proposed the reliability and safety evaluation techniques of aircraft systems based on AltaRica language through graphical interactive simulation. In reference [3], Kim presented a sensitivity analysis and technology evaluation for the civil aircraft in the conceptual design stage. Chen et al. [4] developed an improved formal analysis approach to estimate the safety of the airborne equipment. At present, most of the researches are focused on the flight process of civil aircraft. Compared with civil aircraft, the influencing factors and the mission process of the carrier aircraft during flight are more complex [5]. In reference [6], the aircraft landing control based on fuzzy modeling networks is presented, to improve the performance of conventional automatic landing systems.

During several years of researching, the safety analysis of landing control under certain conditions has been improved. However, there are still some shortcomings in the research on the construction of the normalized, reusable models. Although there have been some attempts to resolve this question, Wei et al. [7] analyzed the potential combinations of failures in flight control system by using SPIN, Dai et al. [8] proposed a method to evaluate landing safety, combining with support vector machine (SVM) and rough set theory (RST), more detailed practical methods are needed.

Aimed at the above problems, an integrated method of large-scale system process modeling and safety analysis is proposed. In addition, the dynamic simulation of entity is combined with the formal
modeling of SysML. Through the simulation, the risk evaluation during the aircraft landing process can be executed so that some suggestions can be provided for the system safety assessment.

2. An Integrated Method of System Process Modeling and Safety Analysis

The integrated method of large-scale system process modeling and safety analysis is shown in Figure 1, where the main process is divided into 4 stages. Firstly, the mission and/or behavior process of system are analyzed and the system is decomposed to identify the hierarchical structure of entities and their behavior process. Secondly, the formal conceptual models are established to define the structural and behavioral characteristics of system in SysML, considering general task and feature of behavior phases. Furthermore, the conceptual model based on SysML is transformed to the entity model in Simulink platform. Finally, the safety of the system is analyzed through simulation using these conceptual and entity models.

Figure 1. The main process of the integrated method

In the analysis of the system mission process, the influence of system components and system behavior, especially their interactions, are mainly considered. The behavior process in the system is divided into object dimension and process dimension. The object dimension describes the structure of the system. The process dimension decomposes the task process of the system. The classified objects and their behavior will be modeled formally in stage 2 to support simulation and safety analysis. The state change modelling and the quantitative safety evaluation can be performed based on the SysML and simulation, respectively. In order to measure the level of safety state, the safety state indicators need to be defined. Based on the simulation of the dynamic change of system state in the Simulink models, the risk of system behavior and mission can be evaluated.

3. The Conceptual Modeling Based on SysML

SysML is a standard system modeling language, which is reusable, supporting the specifying, analyzing, designing and verifying of complex industrial systems [9]. The SysML provides a toolkit of 9 diagrams that can be used to realize a number of views of the model [10]. In most cases, it is not necessary to use all the diagrams to model a system. The structural and behavioral aspects are the most two distinct aspects of the model, by which the model can be fully specified in the SysML. In the case of process modeling, we can use the block definition diagram(BDD) to illustrate the structural aspect and use the use case diagram (UCD), the activity diagram(AD) and state machine diagram(stmD) to illustrate the behavioral aspect.

In general, the mission process of a system is the interactive process of human and machine combining with the influence of environment. Hence, the system structural hierarchy can be classified into three dimensions, i.e. system operator, equipment, and environment, as shown in Figure 2. Based on the BDD structure, the hierarchical relationships among these factors are clarified, as well as the unique attributes of each factor to support the further modeling of behavior.

In order to ensure the streamline operation and management of the system, the behavioral aspect of system usually can be divided into several activity stages. The decomposition steps of the system process are shown in Figure 2. Firstly, the process is divided into several main sub-processes in the UCD. Then in the AD, the specific sub-processes are represented as a combination of a set of basic
actions from the perspective of different objects. The logical relationship between the actions, as well as signals passed between two actions are modeled in AD. Moreover, combining with the process decomposition, the description of the object state change and the transition event can be represented explicitly. After defining the different safety state, the stmD is used to analyze and model the possible states change of the different objects, as well as the safety of system.

System behavior process

Subprocess 1

Action 1

Subprocess 2

Action 2

Subprocess n

Action n

Figure 2. The decomposition steps of the system process

4. The entity Modeling of Landing Process

4.1. The Integrated Method of SysML and Simulink

The SysML emphasizes the visual modeling of system and its behavior rather than the quantitative modeling and simulation based on mathematical model, while the latter is an indispensable part in system analysis. To address the quantitative modeling and simulation, the platform of Simulink is a widely used tool. Therefore, this paper adopts an integration method of SysML and Simulink, based on Triple Graph Grammars (TGG), to model and simulate the behavior process.

Figure 3. The integration example of SysML and Simulink

The TGG specific transformation rules mainly include the transformation of object, parameter and control. An example of the transformation between the source model (AD) and the target model in Simulink is shown in Figure 3. In step 1, the rule indicates the parameter and the same value type between the srcObj1 and trgObj1. In step 2, the action node is transformed into the subsystem block in Simulink according to the tggLink2. Furthermore, the control node in AD is corresponding to different operators in Simulink. At last, the returned value of the parameter can be translated to the source model. Referring to the above transformation rules, the transformation of other SysML models can be achieved to realize the modeling of the dynamic behavior process of system entity.

4.2. The Aircraft Landing System Modeling

The adjustment or maintenance of aircraft flight status is generally realized through feedback control. This paper mainly considers the effect of man-machine-environment during landing, so the manual control model is analyzed and built. Since the flying speed of general aircraft is less than Mach 0.2 and the influence of air compressibility can be ignored, so the aerodynamic characteristics of the aircraft are generally considered to be linear. And there is little lateral movement when close to the ship. Therefore, it is generally assumed that the aircraft only moves longitudinally and the dynamic characteristics of the aircraft can be expressed by the linear small disturbance state equation:
\[
\begin{align*}
\frac{dx}{dt} &= Ax + Bu \\
y &= Cx + Du
\end{align*}
\]

Where, \( x \) is a state variable; \( u \) and \( y \) are input and output variables respectively; \( A, B, C, D \) are vectors with appropriate dimensions. The equation (1) expresses the basic principles followed by the different parameters relevant to the aircraft and supports the construction and calculation of the aircraft dynamic simulation model, as shown in Figure 4 where the ideal elevator control values are input to the aircraft state equation. After calculation, the output of the aircraft speed (VT), attack angle (alpha), pitch angle (theta), pitch angle speed (q), and the aircraft altitude (h) are selected to display.

**Figure 4.** The flight dynamics simulation model

In the personnel control model, the cascade proportional-integral-derivative (PID) control is used to realize the function of controlling flight attitude. As shown in Figure 5, the pitch attitude maintenance function of the elevator passage is selected as an example to show the control principle. The basic control equations based on PID are expressed as equation (2) and (3).

\[
m(t) = K_p e(t) + K_i \int_0^t e(t) dt + K_d \frac{de(t)}{dt}
\]

\[
e(t) = a(t) - c(t)
\]

\( m(t) \): the output of PID; \( e(t) \): the error signal; \( a(t) \): the actual flight altitude; \( c(t) \): the expected flight altitude; \( K_p \): the gain of controller; \( T_i \): the constant of integration time; \( T_d \): the constant of differential time.

During the simulation, the pitch angle in the outer ring of the control loop is controlled based on the altitude deviation, and the pitch angle rate is adjusted according to the pitch angle deviation. Furthermore, the deviation of the pitch angle rate is processed to obtain the desired value of the elevator operating to the aircraft. The difference between the actual flight altitude and the expected can be expressed in equation (3), which is defined as the error signal. Then, the specific value of the output
of PID is calculated through equation (2). Combined with the above equations and Figure 5, we can know the altitude deviation \( e(t) \) is used to calculate the pitch angle, and then the pitch angle rate. The output \( m(t) \) provides the desired value of the elevator operating to the aircraft. The integration and transformation of the conceptual model to the entity model is completed referred to the method proposed in Section 4.1, and the attitude control model based on Simulink is shown in Figure 6.

![Figure 6. The flight attitude control model in Simulink](image)

5. Safety Analysis of Landing Control Process

In this paper, the aircraft attitude control during the landing is chosen to illustrate the safety analysis. According to the conceptual modeling method in Section 3, the structural and behavioral characteristics can be modeled in SysML. Taking the behavioral modeling as an example, the attitude control activity is presented in AD, as shown in Figure 7.

The main actions in the AD include aircraft manipulation, optical guidance, adjusting the elevator, etc., where aircraft manipulation and optical guidance are parallel actions. The execution of subsequent actions are determined by the value of the flow input, in the decision node i.e. “Aircraft manipulation”. The information interactions between different objects of aircraft attitude adjustment can be clearly presented, through the connection relationship between the different action nodes.

![Figure 7. The AD of attitude control](image)

In this example, the initial flight speed is 102m/s, the initial glide height is 240m, and the ideal glide angle is -3°. The parameter variables in the small perturbation equation of state are as follows:

\[
A = \begin{bmatrix}
-0.0555 & -6.6382 & -16.5890 & -9.6783 & 0 \\
-0.0020 & -0.7187 & 1.0000 & -0.0156 & 0 \\
0.0003 & -1.0945 & -0.9745 & 0.0039 & 0 \\
0 & 0 & 0.9950 & 0 & 0 \\
0 & -102.0900 & 0 & 102.0900 & 0
\end{bmatrix}, \quad B = \begin{bmatrix}
-0.5653 \\
-0.1303 \\
-4.0098 \\
0 \\
0
\end{bmatrix}
\]
The landing process of aircraft can be affected by the many factors including personnel control deviation, wake, and the landing conditions of the aircraft carrier. The disturbance can be divided into three specific conditions, such as H1, H2 and H3, with increasing influence, whose effects on aircraft altitude control are introduced into the control system through the AWGN module (additive white Gaussian noise). Deviation adjustment in the aircraft attitude control actions can directly affect the aircraft actual path, which is related to the safety of aircraft landing. The classification of the deviation grade is shown in Table 1. The actual deviation of vertical altitude is chosen to determine the safety condition of aircraft, and divided into three categories, namely, the normal state (vertical deviation within 3 m), critical state (vertical deviation between 3 m and 5 m) and dangerous state (vertical deviation beyond 5 m). The safety state evolution of the system can be simulated after defining the safety state levels and safety state indicator.

Table 1. Classification of track deviation

| Deviation type               | Ideal value (m) | allowable value (m) |
|------------------------------|-----------------|---------------------|
| Horizontal position deviation| -6.1—6.1        | -12.2-12.2          |
| Vertical deviation           | -3—3            | -5—5                |
| Transverse center deviation  | -1.52—1.52      | -3.05—3.05          |

The change of the actual track height and the time change of dangerous state under different disturbance degrees are shown in Figure 8 and Figure 9. The green line in Figure 8 represents the ideal path height curve. The H1, H2, and H3 curves respectively represent the actual path height changes of the aircraft under slight disturbance, moderate disturbance and severe disturbance. The change of aircraft altitude is also shown in Figure 8, where the initial position is 60 meters higher than the specified glide altitude. Firstly, the pilot controls the aircraft to reach the required glide altitude (about 240m). After flying at a fixed altitude for 14 seconds and confirming the state, the aircraft enters the slide path at the 20th second. However, as the disturbance level increases, it can be clearly seen that the deviation between H3 and the ideal path height curve is greater than H2 and greater than H1, indicating that the aircraft altitude deviation during the landing will become larger due to the increase of disturbance of external conditions.

Figure 8. The actual track altitude change under different disturbance degrees

As shown in Figure 9, when the disturbance type is H1, referred to Table 1, the aircraft has a vertical deviation beyond 5 meters during 0-5 seconds and 44-61 seconds, which is in a dangerous state; the vertical deviation is between 3 and 5 meters during 20-43 seconds and 62-68 seconds, located in critical state. Compared with H1, the time of the aircraft in dangerous state increases 9.9% in H2.
Similarly, the time in dangerous state increases 11.4% in H3 than H1, where the critical state time in H3 is about 1 seconds longer than H2. According to the data, the duration of the aircraft in the dangerous state increases significantly with the increase of the degree of external disturbance. Combined with the aircraft attitude control, we can speculate, when the disturbance is slight (H1), the pilot can ensure the aircraft deviation in a small range by adjusting the operation, and the aircraft is in a safe state at most time. However, when the disturbance is large (H3), the pilot's operation becomes difficult, the time when the aircraft is in a dangerous state is obviously increased as well as the safety risk. Therefore, how to avoid the impact of external interference during the aircraft landing and enhance the system's ability to resist interference will become an important way to improve the safety of system.

![Figure 9. The dangerous state time change](image)

6. Conclusion

This paper proposed a formal modeling and safety analysis method based on the SysML. The SysML was used to formally describe the system behavior process, and the integration of SysML and Simulink was adopted to support the simulation based on mathematical model. Furthermore, the entity model was built to simulate the aircraft landing system and support safety analysis. The "aircraft attitude control" is taken as a case study to demonstrate and verify the proposed method and models. This work provides a feasible method to address the formal modeling and safety analysis for complex processes, and also provides valid ideas and suggestions for system safety analysis. However, the presented methodology has some limits, i.e., the interaction of human, machine and environment is not fully considered, and the safety assessment method based on observation indicators needs a further optimization to support a more complete safety analysis.

References

[1] Houser S 2001 *Aviation Safety Simulation Model* (NASA/CR-2001-211022)
[2] Zhu Y, Zhang J, Gong Q, et al. 2011 *Proc. Int. Conf. on Reliability, Maintainability and Safety*, Reliability and safety assessment with AltaRica for complex aircraft systems, DOI: 10.1109/ICRMS.2011.5979336
[3] Kim, Yun, Hwang 2019 Sensitivity Analysis and Technology Evaluation for a Roadable Personal Air Vehicle at the Conceptual Design Stage. *Applied Sciences*, 9(19):4121
[4] Chen L, Jiao J, Wei Q, et al. 2017 An improved formal failure analysis approach for safety-critical system based on MBSA. *Eng Fail Anal*, 82:713-725
[5] Jiao J, Wei M, Yuan Y, et al. 2020 Risk Quantification and Analysis of Coupled Factors Based on the DEMATEL Model and a Bayesian Network. *Applied Sciences*, 10(1):317
[6] Juang J, Chio J 2005 Fuzzy modelling control for aircraft automatic landing system. *Int J Syst Sci*, 36(2):77-87
[7] Wei Q, Jiao J, Zhao T 2017 Flight control system failure modeling and verification based on SPIN. *Eng Fail Anal*, 82:501-513

[8] Dai Y, Tian J, Rong H, et al. 2015 Hybrid safety analysis method based on SVM and RST: An application to carrier landing of aircraft. *Safety Sci*, 80:56-65

[9] Bougain S, Gerhard D 2017 Integrating Environmental Impacts with SysML in MBSE Methods. *Procedia CIRP*, 61:715-720

[10] Zhou S, Jiao J, Sun Q 2014 *Proc. Int. Conf. on Reliability, Maintainability and Safety*, A safety modeling method based on SysML, DOI: 10.1109/ICRMS.2014.7107390