A Failure Propagation Analysis Method Based on $3 \times 3$ Hierarchical Model

Shujie Pang and Jian Jiao*

School of Reliability and Systems Engineering, Beihang University, Beijing, China

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

Abstract. In recent years, with the increasing complexity of equipment, system design and safety analysis for the equipment are becoming more and more difficult. In this paper, we make a more comprehensive analysis of the hierarchical relationship of the system from the vertical and horizontal angles and put forward the $3 \times 3$ Hierarchical Model. Then, we propose a failure propagation analysis method based on $3 \times 3$ Hierarchical Model. At the same time, SysML is used to build the models, which is convenient for different people to learn and modify the models. Finally, a hydraulic transmission system is taken as an example to illustrate the feasibility of the method.

Keywords: Safety analysis, $3 \times 3$ hierarchical model, failure propagation analysis, SysML.

1. Introduction

To ensure the safety and reliability of the system, the safety analysis should run through the whole life cycle of the system. Therefore, we should carry out the corresponding safety analysis from the early design stage. In this paper, we mainly study the hierarchical design method and failure analysis method of the system.

With the increasing complexity of the system, the system design needs to be divided into hierarchies and carried out in an orderly manner. The design work based on conceptual information in system design began in 1966. With the continuous development of system design, there are two main modeling frameworks in the industrial field: function-structure and function-behaviour-structure. In addition, there are other methods derived from them, such as task-function-resource, mission-capability-resource, function-behaviour-structure-state, etc. The existing methods can describe the design requirements of each hierarchy of the system. However, there is a lack of consideration in the modeling of the whole life cycle of the system.

At present, there are many failure propagation analysis methods. The state of art methods include the Systems-Theoretic Process Analysis (STPA), Functional Resonance Analysis (FRAM), Hierarchical Performed Hazard Origin and Propagation Studies (HIP-HOPS), Functional Failure Identification and Propagation (FFIP), etc. The STPA [1] establishes models under the framework of system structure and behaviour but lacks analysis of system function. The FRAM [2] involves the analysis of functions, but it is mainly used for social technology system and safety accident analysis. The HIP-HOPS method [3] uses if-FMEA to analyze the failure logic, and uses tables and words to describe failure causes, which leads to the described results are ambiguous. FFIP method [4] is a graphical modeling method, which is suitable for the early design stage of the system, so its scope of application is limited. Therefore, the shortcomings of current failure propagation analysis methods can be summarized into three aspects: (i) the analysis of system structure, function and behaviour are not comprehensive; (ii) there is ambiguity
due to the description of natural language; (iii) there is a lack of analysis methods suitable for the whole life cycle of the system.

To sum up, aiming at the shortcomings of the current hierarchical design method and failure analysis method, we have conducted the following research. Firstly, we analyzed the hierarchical relationship of the system from a two-dimensional perspective and proposed the $3 \times 3$ Hierarchical Model. Then, we proposed a failure propagation analysis method based on the $3 \times 3$ Hierarchical Model. Moreover, we took a hydraulic transmission subsystem as an example, used the above method to analyze the failure propagation path. At the same time, we used SysML to describe the models, which not only avoided the ambiguity caused by natural language, but also facilitates different people to learn and modify these models.

2. $3 \times 3$ Hierarchical Model

In this part, we make a comprehensive analysis of the hierarchical relationship of the system from a two-dimensional perspective: vertical direction and horizontal direction. Then, we put forward the $3 \times 3$ Hierarchical Model, as shown in Figure 1. The advantage of the $3 \times 3$ Hierarchical Model is to help the system build a unified model. With the advance of system life cycle, different hierarchies can be selected for analysis.

![Figure 1. The $3 \times 3$ hierarchical model.](image)

The system model can be built in both vertical and horizontal directions. Vertically, it can be divided into three layers: system-subsystem-component. Horizontally, the three layers can be divided into other three layers: function-behaviour-structure. So, the model is called $3 \times 3$ Hierarchical Model. Among them, function refers to an attribute that can meet a certain demand. Behaviour is the characteristic of variables in a system over time. Structure is a collection of interrelated system elements organized according to certain laws.

When studying the system hierarchical relationship, we first make a horizontal analysis from the system. The function of system layer is the beginning of design. It is the description of the tasks that the system finally needs to complete. Due to the realization of function needs to rely on the implementation of
behaviour, the next hierarchy is the behaviour layer. Behaviour needs a specific structure to complete. For the system layer, the system is composed of subsystems, which expand vertically to the subsystem layer. The subsystem layer can also be analyzed according to the function-behaviour-structure. The subsystem is composed of various components. Therefore, the structure layer of the subsystem can be extended vertically downward to the function-behaviour-structure of the components.

3. The Failure Propagation Analysis Method Based on 3 × 3 Hierarchical Model

In this part, we proposed a new safety analysis method. The method mainly includes six steps (as shown in Figure 2), they are determining analysis objectives and safety requirements, establishing hierarchical model, establishing function model, establishing behaviour model, failure logic reasoning and failure propagation path analysis. The analysis process of the whole framework needs to select the appropriate hierarchy vertically according to the purpose of the analysis. The specific analysis process is carried out in strict accordance with the horizontal three hierarchies of structure-function-behaviour. In addition, the purpose of this method is to analyze the failure propagation path of the system, so this method is named the Failure Propagation Analysis Method Based on 3 × 3 Hierarchical Model (the 3 × 3 Analysis Model for short).

![Figure 2. The 3 × 3 analysis model.](image)

- **Determine analysis objectives and safety requirements**
  Firstly, determine the analysis object and the analysis purpose according to the life cycle stage of the system. Next, select the appropriate system hierarchy. Then, analyze the possible risk factors and determine the safety requirements of the system.

- **Establish hierarchical model**
  In this step, the hierarchical structure of the model is systematically established. The model can describe the interaction between the internal structures of the system.

- **Establish function model**
  According to the hierarchical model, the functional model of the system can be established. Function model is a collection of functions that must be included in the system, reflects the transfer relationship of functions between components. It describes the information and data flow between component functions.

- **Establish behaviour model**
The behaviour model describes the time-varying characteristics of variables in the system. It uses the changing relationship between process variables to describe the behaviour state of components.

- **Failure logic reasoning**
  Failure logic refers to the specific form of behaviour deviation caused by the system. Failure logic describes the changes of variable relationship which can lead to component failure.

- **Failure propagation path analysis**
  By traversing the causality defined in the failure logic of each component, the failure propagation path in the whole system can be inferred and analyzed.

4. Case Study

Taking a hydraulic transmission system as an example, the specific implementation process of the above proposed method is described. According to the $3 \times 3$ Analysis Method, we establish model and analyze the failure propagation of hydraulic transmission system. In this paper, we describe the model with SysML which can improve the comprehensiveness, consistency and traceability of design.

The main source of risk factors of hydraulic transmission subsystem is component failure. The safety requirement is to ensure the load moves when needed to realize the hydraulic transmission function. Firstly, we divide the analysis object into two hierarchies: hydraulic transmission subsystem hierarchy and component hierarchy. The component layer includes four categories: power components, control components, execution components and auxiliary components. Then, we mark the function of each component and the output variables.

In this paper, we use the block definition diagram in SysML to establish the hierarchical model and the function model of $3 \times 3$ analysis method. In this way, the structure, function and data flow can be shown at the same time, making the functional design of components clearer. The hierarchical model and functional model of hydraulic transmission subsystem are shown in Figure 3.

![Figure 3. The hierarchical model and function model of hydraulic transmission subsystem.](image)

Then, we establish the behaviour model using the sequence diagram in SysML to describe the information transfer relationship between modules, as shown in Figure 4. Figure 4 depicts the behaviour of the hydraulic transmission subsystem under normal conditions.
Next, the failure logic is deduced. The state machine diagram of SysML can show different states of components and the transformation relationship between states. This paper uses the state machine diagram to represent the failure logic. Figure 5 describes the normal state and failure states of the hydraulic pump.

Finally, the failure propagation path is analyzed. The fault tree is used to represent the failure propagation path of the hydraulic transmission subsystem, as shown in Figure 6.
5. Conclusion
In this paper, we proposed the 3 × 3 Hierarchical Model by decomposing the system horizontally and vertically, which considered of the design and modeling of each stage of the system. Then, we proposed a failure propagation analysis method which made up for the shortcomings of the existing methods. In addition, we used SysML to build the system models, which improved the consistency and traceability of the model. Finally, we used the method to analyze the failure propagation path of the hydraulic transmission subsystem and obtained the fault tree.

References
[1] D A Longji; V Emilia. System safety assessment based on STPA and model checking. Safety Sci 2018, 109, 130-143.
[2] V Salehi; B Veitch; D Smith. Modeling complex socio-technical systems using the FRAM: A literature review. Human Factors and Ergonomics in Manufacturing & Service Industries 2021, 31, 118-142.
[3] S Sharvia; S Kabir; M Walker; Y Papadopoulos. Model-based dependability analysis. Software Quality Assurance 2016, 251-278.
[4] S J, Pang; J Jiao. Simulation and Risk Assessment of Sand Mixing Equipment Based on Function Failure Propagation. In 2020 4th International Conference on Modelling, Simulation and Applied Mathematics (MSAM 2021), Wuhan, China, 2021