Failure Propagation Model Based for System Safety Analysis

Hongli Wang, Tingdi Zhao, Fuchun Ren and Nuo Zhao

ABSTRACT

The traditional safety analysis methods focus more on the critical single equipment or the critical part. It is difficult to master the causal logic relationship between the failures, thereby limiting effectiveness of the methods. This paper establishes the system failure model based on the ideology of model-based system safety analysis, and identifies and analyzes the failure modes. We make the modeling and the analysis in view of the failure model. Finally, failure propagation model is analyzed for an application example. The results show the practicability of the method by analyzing. The achievements of this study provide the basis for the safety of system design, and have the important theoretical value and practical significance.

INSTRUCTION

The development of complex system is being more and more integrated, leading to the complexity of its structure, function, and communication. As a result, the system safety has become the key to the development of complex system. However, the complexity, dynamic and hybridity of the system are increasing dramatically, and bring about a challenge for safety analysis of the system.

To be satisfied with the requirements, system safety analysis methods have witnessed continuous development. The existing safety analysis methods mainly divided into three categories: 1) event-based safety analysis method; 2) state-based safety analysis method; 3) safety analysis method based on failure propagation model. Even-based safety analysis method is taken the anomalies such as component fault and
function failure as studying object. And analyze causal relationship of these events in a particular system, such as Fault Tree Analysis (FTA) [1], Failure Mode and Effect Analysis (FMEA) [2] and Hazard and Operability Analysis (HAZOP). However, these methods are mostly from the summary of engineering practice, and low degree of automation cannot meet the demand of large-scale complex system. State-based safety analysis method focuses on the behavior of system itself, such as Stochastic Petri Net (SPN) [3], Logic validation. System state and migration relations between states are abstracted, and establish mathematical model. However, it is difficult to solve because model is too complex, and this limits the application of this method in a great extent.

And safety analysis method based on failure propagation model can be regarded as a fusion of two above thoughts. All possible failure behaviors of system components are analyzed, and also can get the corresponding propagation path. Thus this method can be used to quantitative and qualitative analysis for system safety analysis under the model of the system structure, such as Model Based Safety Analysis (MBSA) [4]. Compared with the above two methods, safety analysis method based on failure propagation model is more to fit the needs of a new generation of complex system.

Based on the deep understanding of model-based system safety analysis method ideology, stratification characteristics and message interaction characteristics in integrated complex system, we establish system failure model and identify and analyze failure modes in this paper. Finally, the paper presents a case of application on Integrated Modular Avionics system to demonstrate the validity of the approach.

SAFETY ANALYSIS METHOD BASED ON FAILURE PROPAGATION MODEL

Failure propagation model method is appeared in the 90s, which is a method considering failure propagation and effect. It is the basis of FTA, FMEA, and functional hazard analysis. This method analyzes all possible deviation factors of each component in the framework of system structure and behavior, to solve the deviation transmission path, and then obtains qualitative and quantitative safety analysis result. This section introduces two typical safety analysis methods based on failure propagation model, namely Failure Propagation and Transformation Notation (FPTN) and Hierarchically Performed Hazard Origin and Propagation Studies (HiP-HOPS).

(1) FPTN: Failure Propagation and Transformation Notation is put forward by Fenelon in 1992 and it is a new safety analysis method [5][6]. This method focuses on how failure propagates in the system and the system how to change type of failure or eliminate malfunction. FPTN is a kind of hierarchical graphical symbol semantic system that can describe and research failure behavior of complex system. It will system be seen as a set of modules. And these modules are not clear limitation, may be a few lines of code and also may be overall system. Failure mode is connected between modules and modules. But it is with great regret that the method is currently only as a compact description language, and used for summing up traditional method analyzed fault information.

(2) HiP-HOPS: Hierarchically Performed Hazard Origin and Propagation Studies is integration of functional hazard analysis, FMEA and FTA, it synthetically assesses hierarchical description complex system [7][8]. Hip-HOPS is a kind of method based on component interface. It argues to obtain all propagation paths of system out-put.
failure from system model, by studying the failure, by studying logical relations of each component from input failure, internal failure to the output [9]. HiP-HOPS makes system components modularized, and considers module output failure by connection relation between modules and internal characteristics of modules [10].

CASE STUDY

This section takes Integrated Modular Avionics (IMA) [11] for example to illustrate the application of the proposed method. Firstly we make IMA system layer and then hierarchically modeling based on ideas of hierarchical modeling. In reference with ASAAC [12], IMA system is managed by a three-layer model: Aircraft Level (AL), Integration Area Level (IAL) and Resource Element Level (REL). This three level hierarchy is illustrated in Figure 2. One of three-layer namely aircraft hydraulic power braking system is chosen as an example to elaborate using HiP-HOPS method introduced above and with combination of SIMULINK and special tool of HiP-HOPS.

![ASaac Three-Layer System Management Model](image)

Figure 1. ASAAC three-layer system management model.

(1) System model description

The Wheel Brake System is mainly used to provide safe retardation of the aircraft during taxiing and landing phases, and in the event of a rejected take-off. The wheel brakes also prevent unintended air-craft motion when parked, and may be used to provide differential braking for aircraft directional control. A secondary function of the wheel brake system is to stop main gear wheel rotation upon gear retraction. If braking system fails during take-off and landing glide phases, it is not allowed that the consequences are plane flies off the runway or collision with other plane. Thus, it must be analyzed and assessed its safety to ensure the acceptable risk of brake system in the development stage of the airplane [13].
Based on description of S18 aircraft hydraulic brake system in ARP4761, we get system model diagram by further simplification, as shown in the Figure 2. This system contains only related components of the brake hydraulic power generation and control, regardless of brake actuator. In this diagram, component A represents that controller is used to receive the pedal signal and produces hydraulic control signal. B, C are hydraulic generator, both are used to create hydraulic pressure. B and C will take action when the commonly used hydraulic device fails. D is the hydraulic alternative valve, and used to select appropriate hydraulic device. E and F are the hydraulic matching valve, which output given value hydraulic pressure after receive controller signal and hydraulic signal. G is emergency hydraulic device, directly receives pedal signal and creates hydraulic pressure after detecting standby hydraulic fail. H is an integrator, H itself does not happen fail. P is sensor of pedal signal. S1 and S2 express sensor. S1 is used to monitor normal brake signal of brake, S2 is used to monitor standby brake signal. The following analyzes braking system by HiP-HOPS method.

(2) Functional failure analysis

Functional failure analysis for model is to determine system functional failure and the influences on aircraft and personnel, and evaluates its severity. The system is only used to provide a hydraulic power in this paper. We adopt principle of failure silently, namely system has always been in failure condition and without any output once system fails to work. The system functional failure analysis is as shown in Table 1.

| Function          | Failure state          | The influences on the aircraft and personnel                                                                 | Degree of influence |
|-------------------|------------------------|----------------------------------------------------------------------------------------------------------------|---------------------|
| Provide the brake power | Braking system complete loss braking power | Aircraft: the aircraft speed can't control, leads to plane overshot the runway and even damage in the stage of take-off and landing  
Crew: may cause death due to plane damage  
Passengers: may cause most of passengers death due to plane damage | I                   |
Table II. Local failure behavior of model.

| Component name | Internal failure | Input failure | Output failure | Logical relationship |
|----------------|------------------|---------------|----------------|----------------------|
| A              | a_failure        | o_A.In1       | o_A.Out1       | o_A.Out1 = o_A.In1 or a_failure |
|                |                  | o_A.In2       | o_A.Out2       | o_A.Out2 = o_A.In1 and o_A.In2 or a_failure |
| B              | b_failure        | None          | o_B.Out1       | o_B.Out1 = b_failure |
| C              | c_failure        | None          | o_C.Out1       | o_C.Out1 = c_failure |
| D              | d_failure        | o_D.In1       | o_D.Out1       | o_D.Out1 = o_D.In1 or o_D.In2 or d_failure |
|                |                  | o_D.In2       | o_D.Out2       | o_D.Out2 = o_D.In2 or d_failure |
|                |                  | o_D.In3       |                | o_D.In3 or d_failure |
| E              | e_failure        | o_E.In1       | o_E.Out1       | o_E.Out1 = o_E.In1 or o_E.In2 or e_failure |
| F              | f_failure        | o_F.In1       | o_F.Out1       | o_F.Out1 = o_F.In1 or o_F.In2 or f_failure |
| G              | g_failure        | o_G.In1       | o_G.Out1       | o_G.Out1 = o_G.In1 or o_G.In2 or g_failure |
| H              | None             | o_H.In2       | o_H.Out1       | o_H.Out1 = o_H.In1 and o_H.In2 and o_H.In3 |
| S1             | s1_failure       | None          | o_S1.Out1      | o_S1.Out1 = s1_failure |
| S2             | s2_failure       | None          | o_S2.Out1      | o_S2.Out1 = s2_failure |
| P              | p_failure        | None          | o_P.Out1       | o_P.Out1 = p_failure |

(3) Failure analysis for components

Failure analysis for components mainly study local failure behavior of system. To explore failure mode of each components and transmission logic from input failure, internal failure to output, and local failure of each components is written in system command. For the convenience of analysis, assume that each component only has one internal failure mode and this internal failure can cause component without output. Local failure behaviors of hydraulic braking system components are as shown in Table 2. After completing definition of local failure behavior, the local failure behavior of components is written in the model by SAM tool and complete failure injection.

Write all local failure and set up system output failure, then we make failure analysis for model. In this case tool can’t perform analysis because the system contains a closed loop. We modify model and introduce additional alternative valve D1. The output of the sensor S1 is as the activation signal of D1, and makes corresponding modification for local failure behaviors, as shown in Figure 3 and Table 3.
Figure 3. The modified model diagram.

Table III. LOCAL Failure behaviors after model modification.

| Component | Internal failure | Input failure | Output failure | Logical relationship          |
|-----------|------------------|---------------|----------------|------------------------------|
| B         | b_failure        | None          | o_B.Out1       | o_B.Out1 = b_failure         |
| C         | c_failure        | None          | o_C.Out1       | o_C.Out1 = c_failure         |
| D         | d_failure        | o_D.In1       | o_D.Out1       | o_D.Out1 = o_D.In1 or d_failure |
| D1        | d1_failure       | o_D1.In1      | o_D1.In2       | o_D1.In1 = o_D1.In1 or d1_failure |
| E         | e_failure        | o_E.In1       | o_E.Out1       | o_E.Out1 = o_E.In1 or o_E.In2 or e_failure |
| F         | f_failure        | o_F.In1       | o_F.Out1       | o_F.Out1 = o_F.In1 or o_F.In2 or f_failure |
| S1        | s1_failure       | None          | o_S1.Out1      | o_S1.Out1 = s1_failure       |

(4) Model analysis

If input is correct after completing local failure injection, then makes analysis and generate corresponding fault tree, cut set and FMEA. Each component is actually a tree in failure analysis of components, and system whole fault tree is actually stitching by component fault tree. Tool generates fault tree, cut set and FMEA, in which fault tree as shown in Figure 4. Due to lack of necessary failure probability, this paper only makes qualitative analysis and gets 27 minimum cut sets as shown in Table 4.
As seen in Table 4, the failure of component P will directly cause the system without output, namely P failure is a single point of failure. Thus it needs to be paid attention to P single point of failure in the subsequent design, and takes the redundancy measures to reduce the effects of P on the whole system. We can adopt redundancy measures and introduce the backup mechanism to make the system fails.
after all pedal signal sensors are failure. This will reduce the input failure probability that the pedal signal of controller occurs, thus to improve the overall system safety.

CONCLUSION

This paper establishes system failure model based on the ideology of model based system safety analysis, and identifies and analyzes the failure modes. We make the modeling and the analysis in view of the failure model. Finally, the paper presents a case of application on Integrated Modular Avionics system to demonstrate the validity of the approach. The achievements of this study provide the basis for the safety of system design, and have the important theoretical value and practical significance.

The article shows the possibility to establish a failure propagation model and identify its potential hazards. However, the system is carried on more simplification and it has a gap in actual system. The future research, which focuses on how to describe multifaceted variability and couplings, will make this approach more powerful and more applicable value in engineering.

The authors would like to thank the support by a grant from the Major State Basic Research Development Program of China (973 Program) (No.2014CB744904).

REFERENCES

1. Khana, F.I., Husaina, T. 2001. “Risk assessment and safety evaluation using probabilistic fault tree analysis, human and ecological risk assessment,” *An International Journal*, 7(7): 1909-1927.
2. Stamatis, D.H. 2003. “Failure mode and effect analysis: FMEA from theory to execution,” ASQ Quality Press.
3. Marsan, M.A., Balbo, G., Conte, G., et al. 1994. “Modelling with Generalized Stochastic Petri Nets,” *John Wiley & Sons, Inc*, 1994, 26(2): 58-60.
4. Papadopoulos, Y., McDermid, J.A. 1999. “A new method for safety analysis and the mechanical synthesis of fault trees in complex systems,” Proceedings of ICSSEA 99, 12th International Conference on Software and Systems Engineering and their Applications 4(13): 1-9.
5. Fenelon, P., McDermid, J.A. 1992. “Integrated techniques for software safety analysis,” IEEE computing and control deviation colloquium on hazard analysis digest, London, 1992: 2/1-216.
6. Fenelon, P., McDermid, J.A. 1993. “An integrated toolset for software safety analysis,” *Journal of Systems and Software*, 21(3): 279-290.
7. Sharvia, S., Papadopoulos, Y. 2011. “Integrated application of compositional and behavioral safety analysis,” Dependable Computer Systems Advances in Intelligent and Soft Computing 97: 179-192.
8. Papadopoulos, Y., McDermid J.A. 1999. “Hierarchically performed hazard origin and propagation studies,” 18th International Conference on Computer Safety, Reliability and Security SAFECOMP99. Toulouse France: 139-152.
9. Oleg, L. 2010. “Failure logic modelling: A pragmatic approach,” University of York.
10. Aizpurua, J.I., Muxika, E. 2013. “Model-based design of dependable systems: Limitations and evolution of analysis and verification approaches,” *International Journal on Advances in Security*, 6(12): 12-31.
11. Prisaznuk, P.J. 1992. “Integrated modular avionics,” Aerospace and Electronics Conference, 1992. NAECON 1992, Proceedings of the IEEE 1992 National. IEEE: 39-45.
12. STANAG 4626, 2004. “Final draft of proposed standards for software,” ASAAC.
13. SAE ARP4761. 1996. “Guideline and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment,” SAE.