Model-based System Safety Assessment of Aircraft Power Plant

Yan Li\textsuperscript{a}, Qi Gong\textsuperscript{b}, Duo Su\textsuperscript{b}, a*

\textsuperscript{a}Beihang University, Beijing, 100191, P.R.China
\textsuperscript{b}Aero-Polytechnology Establishment, 100028, Beijing, P.R.China

Abstract

The aircraft power plant becomes even harder since the complexity and integrity of system function, and the traditional system safety analysis, influenced by the personal skills and experience of analysis, may cause error and system failure condition and effects. The paper presents a new approach called Model-based Safety Analysis (MBSA) for complex system, and the process of MBSA is studied by linking function modeling using formal language and fault propagation based on Altarica, and the given method can be introduced to aircraft power plant system in order to unify the process the system development and system safety assessment, and versatility and feasibility of the approach are demonstrated with the case study of aircraft power plant.

\textcopyright{} 2013 Published by Elsevier Ltd. Selection and peer-review under responsibility of ENAC.

Keywords: safety assessment; complex system; MBSA; formal modeling; power plant

1. Introduction

The power plant system is the heart of aircraft, which is complex and critical system. Due to technical difficulty as well as dynamic loading and environment, the safety assessment of power plant system is becoming challenge.

The regulations associated with system safety show it is of importance to unify the process between system design and safety analysis, making it more efficient to ensure that the systems meet their safety requirements during safety design, analysis and assessment for complex system. For instance, the regulation of SAE ARP4754A requires comprehensive analysis stem from different system model[1], on the one hand safety requirements are obtained through safety assessment, and on the other hand the safety requirements should be transmitted to system engineering in order to reduce and control risk through a

*Yan Li. Ph.D. Tel.: +86-10-84380188.
E-mail address: liyan_cape@126.com.
deductive and iterative approach. Therefore, in order to steer automated integration process by a study of system safety analysis, it is capital to combine system process and safety assessment.

Since different functions of power plant system becomes high relevant and coupling, traditional process of safety assessment (e.g. FMEA FTA) relying on manual iteration used by safety engineering is lower efficient, and any change associated system design would make the classical safety analysis of complex system increasingly more difficult to complete, so the analysis of safety critical systems confronts with a situation in which, on the one hand complexity of systems causes a shift towards integration, while on the other hand safety concerns push for a re-thinking of the presently established safety assessment processes.

According the difficulties of system safety analysis proposed in the paper, the presented approach is MBSA [2-3], which makes contributions to automate safety analysis and conquers the drawback of traditional safety analysis, in addition objectives of MBSA can support continuous safety iteration during the whole process of design phase. MBSA has been applied to Dassault and Airbus 380, which reflects possible hazard origins during the system design phase, so the method can developed to reduce and control potential hazard used an integrity safety model for enhance the safety level of complex system. Significant works addressed the studies, the reference [4] proposes an integrated safety prognosis model considering the randomness, complexity and uncertainty of fault propagation, and the reference [5] proposes a method which can automatically identify the combinations of failures from FMEA results report, making it practical for system designer and safety engineering to study and act on the results.

Therefore, the paper proposes a new approach called MBSA for complex system, and the proposed method can unify the process between system design and safety assessment, and complete the automated iteration process of system safety analysis during the whole life. The given method is applied to a real system to access the safety state of aircraft power plant system, which identifies the hazard and controls the risk.

### Nomenclature

- **FMEA**: Failure mode and effect analysis
- **MBSA**: Model-based safety analysis
- **FHA**: Function Hazard Analysis
- **FTA**: Fault Tree Analysis
- **AADL**: Architecture Analysis & Design Language
- **DBD**: Dysfunctional Behavior Data
- **PSSA**: Preliminary System Safety Assessment
- **SSA**: System Safety Assessment

### 2. The technique of safety analysis based on model

#### 2.1. Process overview of Model-Based safety Assessment

The safety assessment proposed SAE ARP4754A for V process requires to involve aircraft, system and equipments level, and the whole work should be completed manually, however the efficiency is lower with the system larger and complexity, so it should improve the traditional process of safety assessment aiming at automated safety integration, and the improve V process is show as Fig 1.
In addition, AC25.1309-1A of FAA suggest that the work of system safety assessment should be performed based on model[6], so it is necessary to focus on the approach of automated safety analysis.

The method proposed in Fig.2 is a deductive and iterative process which can reflect the system safety requirements from system design model and it can be mainly automated safety analysis using multidisciplinary tools and formal language which includes the following process:

1) Identification of the dysfunctional behavior with FMEA which is automatically generated by SysML.
2) Construction of a model integrating functional and dysfunctional behaviors with the formal language (e.g. AltaRica) based on risk engineering aiming at the simulation of fault scenario.
3) Analysis and quantification of dysfunctional behavior and the impact on safety requirements with a Semi formal language such as Architecture Analysis & Design Language (AADL).

At the beginning of the approach, the knowledge expressing the architecture and the function behavior of the system should be established, the dysfunctional behaviors are stored in the Dysfunctional Behavior Data(DBD), then the model of fault propagation is set up by designers, and the DBD is developed through the iterative process, finally real time safety analysis is performed by AADL.

Therefore, the key techniques of system safety based on function model are formal modelling and safety synthesis, and the difficulties of the techniques will be described in detail.

2.2. Formal modeling of system fault scenario

The formal modelling language Altarica developed at LaBRI and Dassault to describe both functional and dysfunctional behavior of complex system, currently the platform SimFia associated with Altarica for assessment and validation of safety critical systems is becoming the importance tool for EASA.
Altarica supports the automated modelling and analysis of system safety based on functional model, and it allows representing the failure propagation. The language is carried out by the tool CeciliaTMOCAS and SimFia of Dassault and APSYS respectively which provides a graphical interface to design models and allow analyzing them by different ways such as simulation, automatic generation of minimal cuts or sequences. An Altarica model is a network of interconnected components so called "node" which is atomic or composed of interconnected sub-nodes, and each node has a finite number of states:

1) Flow variables. They are the inputs and outputs of the node used to link the node and its environment (other nodes).

2) State variables. These internal variables memorizes current or previous functioning mode (e.g. failure mode). In the formal modelling with Altarica, these variables (flow and state) belong to finite domains of values (Boolean or enumerated).

3) Events. They label changes of value of state variables. They model the occurrences of fault, human actions or a reaction to a change of one input value.

The node dynamic is defined by:

1) Initiation. This is used to assign initial value to state variables.

2) Transitions. The described how the state variables are modified and they have the following format: \( G(s, v) \rightarrow E \rightarrow s' \)

Where \( G(s, v) \) is a Boolean condition on the state variables \( s \) and input variables \( v \), \( E \) is the event and \( s' \) is the effect of transition on the state variables. If condition \( G \) is true, then the event \( E \) can be triggered and state variable are modified as described in \( s' \).

2.3. Automated safety synthesis

To enable model-based safety assessment, the fault model which is described by formal language is composed with the nominal system model to describe the behavior of the system in the presence of fault scenario. We call this the Extended System Model (similar to the FSAP/NuSMV-SA documentation). There are two approaches to adding fault information to the system model. First, it is possible to embed the fault behavior directly into the system model. The second option is to develop the fault model as a separate entity from the system model and automatically merge these two models for analysis. We will investigate both these approaches later in the report.

Once we have the extended system model, the safety analysis involves verifying whether safety requirements hold in the presence of the faults defined in the fault model. The safety or system engineer can perform exploratory analysis by simulating faults on specific components and observing the behavior of the system. For more rigorous analyses, it is possible to use formal verification tools to determine whether safety properties of interest hold.

3. Application

3.1. Illustration of Power plant Functions

The approach proposed in the paper is applied to power plant system, and overview is given in Fig.2
The power plant system is composed of engine, nacelle and power plant components in airframe, and the main function is as follows:

1) Providing the normal thrust for aircraft;
2) Providing the reverse thrust for aircraft;
3) Providing the information of engines parameters;
4) Providing crew alerting information of engines;
5) Providing the power resource for variable frequency generator;
6) Providing bleed for environment control system;
7) Providing uncontained rotor protection of engines.

3.2. Power plant system FHA

According the outputs of power plant FHA, safety requirements of power plant system are given in Table1(Partial):

| Reference | Failure Condition | Safety Objective | Flight Phase |
|-----------|------------------|-----------------|--------------|
| 71-F1-02  | Uncontrolled high thrust | <5e-10 | T, F4, L,T |
| 71-F1-05  | Unprotected overspeed | <1e-9 | F1-F4, L |
| 71-F1-06  | Loss of normal thrust for two engines | <1e-9 | T(V>V1), GA |
| 71-F1-07  | Loss of thrust control for two engines | <1e-9 | T(V>V1), F1-F4, L |
| 71-F1-09  | Thrust Loss of one engine and N1 too slow on the other engine | <1e-9 | T(V>V1), F1-F4,L |
| 71-F2-09  | Uncommented open of one thrust reverser | <3e-10 | T, F1-F4, L |
3.3. Formal modeling of power plant system

The system dysfunctional behavior is modeling based on formal language Altarica, and the formal model of uncontrolled high thrust is illustrated in Fig.3.

![Diagram of formal model of uncontrolled high thrust](image)

Fig.3. Formal model of uncontrolled high thrust

3.4. Automated FTA generation

According the formal model of power plant with Altarica data flow based on risk engineering, then fault propagation can be modelled, finally the FTA is generated autonomicly. In this paper, the FTA result is shown in Fig.4.
The process of safety design, analysis and assessment is performed automatically in the unified formal model through the application of power plant system, and the potential hazards are identified, and the method proposed in the paper can developed to reduce and control possible hazard origins, enhancing the safety level of power plant system, therefore illustration of power plant system demonstrates the applicability and versatility of the proposed approach.

Acknowledgements

We would like to thank COMAC (Commercial Aircraft Corporation of China) for funding this work, in particular Ning Cui and Zongbao Guo for their useful comments and for supporting development of ideas in this paper.
References

[1] SAE ARP 4754 A. Guidelines for development of civil aircraft systems. 2010, REV. A.
[2] M. Bozzano, A. Villaflorita. Improving system reliability via model checking: the fasp/nusmv-sa safety analysis platform. In Proceedings of SAFECOMP 2003, p. 49-62.
[3] M. Bozzano. An integrated methodology for design and safety analysis of complex system. In Proceedings of ESREL 2003:237-245, Balkema Publishers.
[4] Jinqiu Hu, Laibin Zhang, Lin Ma. An integrated safety prognosis model for complex system based on dynamic Bayesian network and ant colony algorithm. Expert System with Applications, 2011, 38(2):1431-1446.
[5] C.J. Price, N.S. Taylor. Automated multiple failure FMEA. Reliability Engineering and System Safety, 2002, 76(1): 1-10.
[6] AC25.1309. System Design and Analysis. Advisory Circular, 2002.
[7] Pierre David, Vincent Idasiak. Reliability study of complex physical systems using SysML. Reliability Engineering and System Safety, 2010, 95(5): 431-450.
[8] Boiteau M, Dutuit Y, Rauzy A, Signoret J-P. The AltaRica data-flow languages in use: modeling of production availability of a multi-state system. Reliability Engineering and System Safety, 2006, 91(8):747-755.