A Novel Model-Based Method for Automatic Generation of FMEA

Juan Zhang
School of reliability and system engineering
Beihang University
100191 Beijing, China
zhangjuan198804@163.com

Guoqi Li
School of reliability and system engineering
Beihang University
100191 Beijing, China
gqli@buaa.edu.cn

***Abstract*—FMEA is a popular safety analysis method for embedded software and its automatic generation is a hot topic recently. In this paper, a novel model-based method for automatic generation of FMEA is presented, which is hopeful to overcome the shortages of exit automatic generation methods. The methodology and procedures of the method are described in detail.**

Keywords- FMEA; embedded software; safety analysis; model-based development

I. INTRODUCTION

FMEA (Failure Mode and Effect Analysis) is a method to analyze all probably failure modes for each components of a system and confirm all possible impacts on the system. This method was first developed in US military industry. As an important analysis technology of current reliability area, FMEA is applied to both software and hardware systems.

For the problems of how to avoid uncertainty of artificial analysis in FMEA procedure, how to improve the accuracy and efficiency by apply FMEA, this paper presents a new technology on improving the efficiency of FMEA analysis procedures based on model. The technical method in information extraction for analyzed objects, analysis and management for analyzed data and other aspects are superior to software products in the past. Therefore, there are significant effects to find system flows, to improve reliability of system and to reduce the failure of the software products.

A. Background of FMEA

FMEA can evaluate and analyze all possible risks in order to eliminate or reduce these risks to an acceptable level with existing technologies [1].

Simple FMEA technology has its own flaws and shortcomings. This paper describes inadequacies of FMEA from two aspects:

a) Cause-effect relationship is not adequately represented in current FMEA models. Sometimes certain faults do not always lead to ultimately failure effects.

b) FMEAs intrinsically contain extensive amounts of information. An FMEA identifies a product's functions, how the product can fail to perform those functions, potential causes of those failures, and the immediate and downstream effects. Hundreds of pages of information can be accumulated for the simplest of products. Storing, retrieving, and searching the FMEA document for particular information can be time consuming and tedious.

Procedures of FMEA are shown in Fig.1:

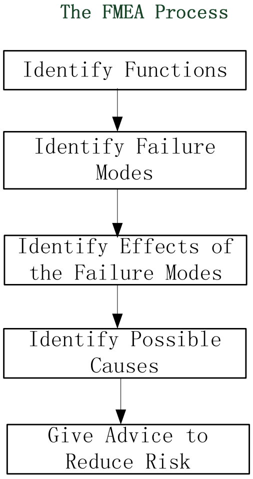

Figure 1. FMEA Process

FMEA Process is cockamamie, subjective, and error rate is relatively high if we simple rely on humans' collation and analysis. Model-base safety analysis is a solution for the problem.

B. Model-Based Safety Analysis

Model-based method is a tool or thinking of modern scientific understanding with providing ideas and impressions. It not only condition of access to knowledge, but an important part of human cognitive structures. Model-based method can reveal model prototype, characteristic and its essence, is a specific form of logical method. As we all known, in software development engineering, model-based development method is praised highly and has been widely used, especially in the field of safety critical systems development, it is currently one of the mainstream and the most advanced technology.

Model plays an important role in model-based development process. However, there are a variety of modeling technologies, which can build model for different aspects. Different parts of the system are considered to solve problems in design and analysis. Model is a form of description on structure information and behavior for a real system, is a kind of quantitative abstraction for system characteristic and variation pattern as a means or tool for people to know things. Specifically, there are three types of models currently:

Published by Atlantis Press, Paris, France.

- Physical model is an objective entity cannot transfer with person’s will. For example, flight models of aircraft development, ship models of ship manufacturing.
- Mathematical model, which come from some similar functions or structure, is a mathematical means to reproduce the functional or structural characteristics of prototype.
- Simulation model, is mathematical model based on system, can be achieved with simulation languages into computer.

In this paper, following FMEA aided method which can help to improve the effectiveness of process of FMEA is completed on the basis of model simulation and the application of the model–based development methods. Complete, consistent analysis, model checking to model and so on can ensure the correctness of the final code in the development process. From the point of the technology, Simulink is a package to realize dynamic system modeling and simulation as a part of extension of MATLAB. It is no doubt that it is an effective means for people to create simulation model. Simulink provides an interactive graphical environment and customizable modules library for people to design, simulate, implement and test for models. The main support tool of Simulink for embedded system development is Stateflow, which is based on the theory of hierarchical state machine, and is mainstream technology for embedded software logical modeling. Modeling and simulation technologies of Simulink can support this model-based development. What’s more, SCADE technology of Esterel [2], SpecTRM technology in software engineering can also support these similar development activities. On the other hand, in the FMEA process, being analyzed objects point of view should be considered. Model development, model simulation, model verification and model confluence analysis can be finished in MATLAB/Simulink. Models for analysis established in Simulink can associated with the data source of FMEA process. Bridging tool between FMEA aided software and MATLAB/Simulink can automatically enter models and simulation results of Simulink environment into FMEA aided software, modeling and simulation results will directly determine the results of FMEA process.

No matter for the development of FMEA aided software or to analysis simulation models in MATLAB/Simulink. It is likely that safety requirements such as complete, consistent, and error free should be achieved because these activities have complete system architectures and accuracy models for corresponding failure mode.

C. Current Methods and Their Disadvantages for Automatic Generation of FMEA

As introduced above, even for a simple product, FMEA process is time-consuming and easy to go wrong if only rely on peoples’ analysis. A variety of analysis documents are confusing and not convenient for people to retrieve and research. So, some FMEA aided software developed to reduce the pressures of FMEA processes, meanwhile, their limitations also are shown inevitably [3].

For example, Jun Sheng FMEA knowledge system [4] allows PDCA cycle mechanism of Know How library, the idea of which is to accumulate FMEA knowledge library in daily works. Besides product process, FMEA with certain relevance, compatibility and convenience also provided to help FMEA method introduced into other aspects. A failure cause may lead to a variety of failure modes, and a failure mode can be resulted from more than a failure cause. There are similar relationships between failure modes and failure effects. FMEA Facilitator can support FMEA process, a one-to-many relationship is defined between failure modes and effects, even though a many-to-many relationship exists in reality. Consequently, repeat Effects will occasionally appear on the Effects table, if the same effect is associated with more than one failure mode. The database could be more “efficient” if repeat entries were eliminated with many-to-many relationships. However, the additional bulk of the database accommodates the standard thought processes of human beings performing an FMEA, which more than justifies the electronic cost of additional storage space. For this reason, all relationships in the FMEA database are defined as one-to-many. There are others similar FMEA aided software, they have different emphasis according to the different characteristics of FMEA process. But most of them are not developed based on model, they cannot meet the requirements of complete and error free very well. In fact, the lack of precise models of the system architecture and its failure modes often forces the safety analysts to devote much of their effort to gathering architectural details about the system behavior, and safety and quality cannot be guaranteed. Traditional software development lacks enough adaptability as well as cannot keep away from risks in the development process. Some FMEA aided software tools are achieved by application of model-drive development method. These methods allow analysis and verification for system at early stage and help to ensure properties of the system quality which determined by system architecture. Thus, appropriate architecture description languages became the most important aspect of the research in design and development of based on model-driven. Common architecture description language mainly contains UML (unified modeling language), ADL (architecture description language). UML focuses on describing the software architecture of system, the method of multi-models and multi-analysis may create inconsistence among these models. Darwin, Wright, Aesop, Unicon, Rapide, and other AADL are common software description languages. But it is hard to satisfy co-design for hardware and software, real-time response, resource-constrained and other specific needs for them. AADL is considered to be the foundation of design and implementation of embedded real-time systems based on model-driven, which can meet the way of single model supporting a number of analyses with put system design, analysis, verification, generation of automatic code and other key steps into a framework. It has a broad application prospect. However, implementation model of AADL involves building, development, scheduling, communication, modes change and many others, these is difficult for people to master, and AADL formal semantics need to be further developed. For how to ensure effectiveness and usefulness of modeling and analysis tools, how to satisfy the needs of reality systems when AADL applied to real industrial systems, especially in large scale system design, further studies are needed, which makes the application of AADL not widely than expected [5].

FMEA process under this condition has strong subjectivity because it mainly dependent on user's analysis experience and FMEA technology. Technology method below will make up deficiencies and shortages of this, which based on user demands, put the growing model-based method into FMEA process.

II. Idea and Framework of the New Method

FMEA software is committed to solve current shortcoming and limitations by provide new ideas and methods for users. The highlight advantages of this method on the framework, formal requirements and automatic verification. They can support extensions and automatic checking to model.

Compare to past FMEA aided software, this approach focus on the application of database. The functions data statistics and analysis would help to analysis and Graphic represent for entry data, which supporting screen and retrieve for needed results. All of these are benefit for user to understand current state of reliability more intuitively and comprehensively.

As shown in Fig.2, the idea of this paper is to create models in MATLAB/Simulink as the knowledge sources of FMEA process. To perform system-level safety analysis, we must also consider the environment in which the system runs, which usually involves mechanical components. By combining models containing the digital components (software and hardware) with models of the mechanical components, we create a model of the nominal system behavior. This model can then be augmented with fault models for the digital and mechanical systems to create the Extended System Model [6]. We can simulate extended models and system models to get the results compared, which are important source for FMEA analysis.

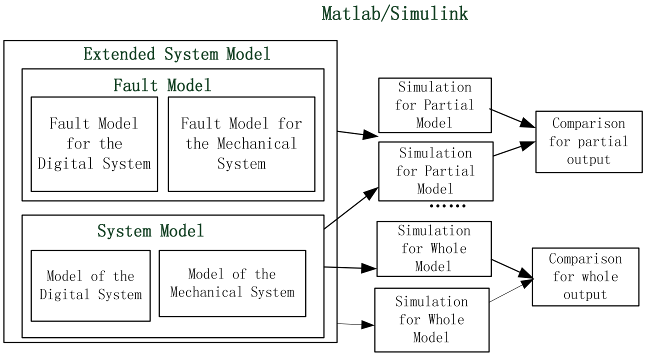
Matlab/Simulink
Extended System Model
Fault Model
Fault Model for the Digital System
Fault Model for the Mechanical System
System Model
Model of the Digital System
Model of the Mechanical System
Simulation for Partial Model
Simulation for Partial Model
......
Simulation for Whole Model
Simulation for Whole Model
Comparison for partial output
Comparison for whole output

Figure 2. Acquire Knowledge from MATLAB/Simulink

Model-based method has been fully used here, which can be seen from the chart above, appropriate fault models established in MATLAB/Simulink, then bridging tools between MATLAB//Simulink and software tool will be automatically entered fault models into FMEA aided software. By the means of simulation in Simulink to determine Failure Modes and Failure Effects and so on, but at this point we not very sure about the Failure Models, our aim is to find out the reasons of fault occurred and to take corresponding improvement measures to enhance the reliability of the system. For the current analysis of the possible causes, we can return to MATLAB/Simulink to modify and refine the models. Continuous improvement and simulation should bring us desired model. These improvement measures should be helpful to give some advice to reality system to reduce risks. Therefore, costing too much and difficult practical operation in engineering practice can be avoided.

According to FMEA process characteristics, the functions of this technical method described in the following:

To do FMEA, no matter for hardware or software, the procedures are the same [1]:

- Identification of systems and functions. Functions are purpose of products. It is necessary to understand the function of product being analyzed. This can help to analysis and judge for FMEA process.
- Identification of Failure Modes. Failure modes are the form of the failure happen.
- Determination of Effects of Failure modes. Certain failure modes will bring certain effects on system, but not all of failure modes will cause the final failure occurs. A failure mode may produce one or more failures. A failure effect may be caused by multiple failure modes. Therefore, determination of effects of failure modes is the important step in FMEA process.
- Identification of possible causes. Each occurrence of a failure mode is caused by a specific reason. A failure mode may correspond to more than one failure causes, a failure cause may also bring a variety of failure mode occurs. We need to determine the possible causes of failure modes to take some measure to improve system reliability.

Documentation and risk reduction. All processes of FMEA are just for taking measures to reduce risks.

From Fig.3, process (1) realizes the acquisition of Knowledge for failure modes. Bridging tools between MATLAB/Simulink and FMEA aided software help to convert faults models established in Simulink into FMEA aided software. By identifying and judgment in FMEA software, failure model will be displayed as failure modes. We also need to establish a system model in the MATLAB/Simulink, then doing partial model simulation for them (2). At the same time partial simulate the extended system with fault models (3). These activities are to compare the both partial outputs (4). Transferred to the FMEA aided software to determine local effects (class). Similarly, comparing the results of the whole model simulations of the system model (6) and the extended system model (7) we can get more outputs (8), then the final compared results can determine the final effects (class) of failure modes. We can modify the current system models according to possible failure causes and some advices including digital system models and mechanical system models. Improved model may meet the reliability requirements or have other failures. It is need for us return to the above procedure (2-9) to establish another round of comparison of simulation outputs to determine these. For Improved models do not meet reliability requirements, we need a new round of simulation for that to get compared outputs and advices from FMEA process to modify the model repeatedly (11). We should clear that models will meet the reliability requirements though our modified, which proved the improvement advices given before are correct and effective in FMEA process (13). At last, system reliability we expected can be achieved through this continuous improvement.

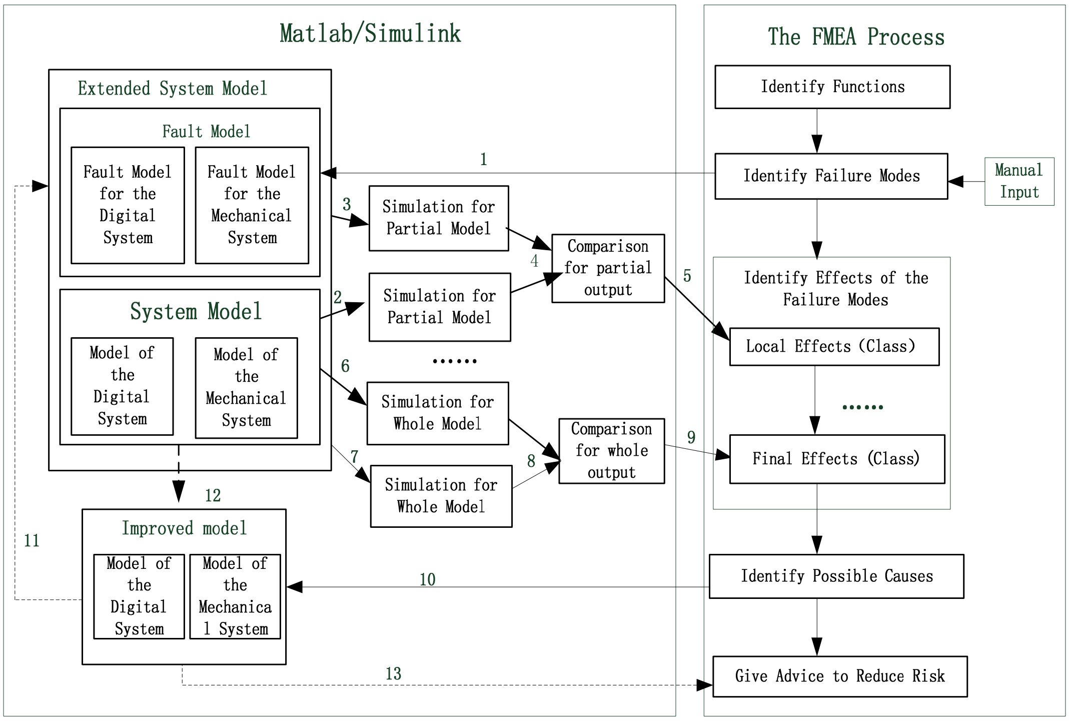
Matlab/Simulink
Extended System Model
Fault Model
Fault Model for the Digital System
Fault Model for the Mechanical System
System Model
Model of the Digital System
Model of the Mechanical System
Simulation for Partial Model
Simulation for Partial Model
Simulation for Whole Model
Simulation for Whole Model
Comparison for partial output
Comparison for whole output
Improved model
Model of the Digital System
Model of the Mechanica l System
1
2
3
4
5
6
7
8
9
10
11
12
13
The FMEA Process
Identify Functions
Identify Failure Modes
Manual Input
Identify Effects of the Failure Modes
Local Effects (Class)
Final Effects (Class)
Identify Possible Causes
Give Advice to Reduce Risk

Figure 3. Function of the New Method

These activities ensure the quality of FMEA process, have real significance, and also improve the efficiency of the FMEA process.

III. Conclusion

This paper focus on a new technology aimed at improving the efficiency of FMEA process. Meet the current model-based methods, obtaining knowledge from models and then to analysis and manage them according to FMEA process. There are new functions and expression methods in aspects of data entering, retrieve, statistic, screening and analysis, which make FMEA analysis process more convenient, effective and accurate.

References

[1] D.H. Stamatis, "Failure mode and effect analysis: FMEA from theory to execution". Serie "Failure mode and effect analysis: FMEA from theory to execution". 2003: Asq Press.

[2] A. Joshi and M. Heimdahl, "Model-based safety analysis of Simulink models using SCADE design verifier". Computer Safety, Reliability, and Security, 2005: p. 122-135.

[3] H. Pentti and H. Atte, "Failure mode and effects analysis of software-based automation systems". STUK-Y TO-TR-19 0, August, 2002. 2(00): p. 2.

[4] R. Wirth, B. Berthold, A. Krämer, and G. Peter, "Knowledge-based support of system analysis for the analysis of failure modes and effects". Engineering Applications of Artificial Intelligence, 1996. 9(3): p. 219-229.

[5] M. Hecht, A. Lam, R. Howes, C. Vogl, S. Lake, and UT City. "Automated Generation of Failure Modes and Effects Analyses from AADL Architectural and Error Models". in Proc. 2010 Systems and

[6] A. Joshi, M. Whalen, and P.E. Heimdahl, "Model-based safety analysis final report". NASA 2005.