A Fault Diagnosis Model for Embedded Software Based on FMEA/FTA and Bayesian Network

Shunkun YANG
Department of System Engineering
Beihang University
Beijng, China

Minyan LU, Bin LIU, Bonan HAO
Department of System Engineering
Beihang University
Beijng, China

***Abstract*—Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) are two effective fault analysis technologies and the integration of them is also applied widely in many industry domains.But when they are used for fault diagnosis ,the ability of inference is not very enough and especially they are not suitable to use the fault related symptoms to do some posterior inference. To solve this problem, this paper combines FMEA and FTA based on Bayesian Network (BN) to form a fault diagnosis analysis model. Case study shows that this model has a good FMEA /FTA fusion ability and posterior inference ability for embedded software fault diagnosis.**

Keywords- Fault diagnosis; Bayesian network; FMEA; FTA

I. INTRODUCTION

Software fault diagnosis is a complex process. With the software system becoming huger and the program structure more complex, to identify the cause of failure becomes increasingly difficult. So software fault diagnosis has been paid more and more attention. Over the last decades, there have been a lot of substantial work on software fault diagnosis and many new methods and technologies have been emerging, including Intelligent Fault Diagnosis, Program Slice-based Software Fault Diagnosis, Combining-Test based Software Fault Diagnosis, Control Flow-based Fault Diagnosis, Genetic Algorithm based Software Fault Diagnosis, Information Fusion Technology and Dempster-Shafer theory, etc [1].

As two effective methods for fault related analysis, FTA and FMEA are often used to help identify the possible fault module leading to the final failure and to narrow the scope of fault location. In recent years there have seen many interests in the use of combined FMEA/FTA to address problems in software fault diagnosis [1][4]. TFT [6] is a method to integrate FMEA and FTA which including two ways: Forward (First FMEA then FTA) and Backward (First FTA then FMEA). BFA [7] is also a creative technology to combine FMEA and FTA. BFA connects the two methodologies allowing an analyst to "bounce" between top-down and bottom-up, from FT diagram to FM table and back, changing the presentation and the direction of the analysis for convenience of analysis at any point in the process. Meanwhile methods of constructing BN from FTA [3][4][9] or constructing BN from FMEA [2] have been studied well and applied in some projects.

BN is somewhat similar to FMEA and FTA on the aspect of inference mechanism and system state, and can be constructed from FMEA or FTA [2][3][4][8][9], but at the same time BN has stronger description ability. Through representing the probabilistic relationship between random events, BN can get more useful conclusion to be the theory evidence for fault diagnosis inference. So BN can be used as the central component to combining FMEA and FTA to form an integrated fault diagnosis analysis model, which can be constructed from FMEA/FTA and dynamicly adjust the diagnosis strategy to improve the efficiency and accuracy of fault diagnosis. There are also a lot of fault diagnosis methods based on BN [7]. But none of these methods mentioned above maximize the advantages and minimize the shortcomings of FMEA/FTA/BN at the same time. FBF discussed in this paper, to our knowledge is the first applications of combining FMEA and FTA based on BN for embedded software fault diagnosis.

II. FMEA-BN-FTA FAULT DIAGNOSIS MODEL (FBF)

FBF is a three-view analysis model for fault diagnosis, which can realize the transformation between FTA, BN and FMEA. Through a transfer component, both FMEA and FTA can be transformed to BN, and given some condition BN can also be transformed to FMEA or FTA.

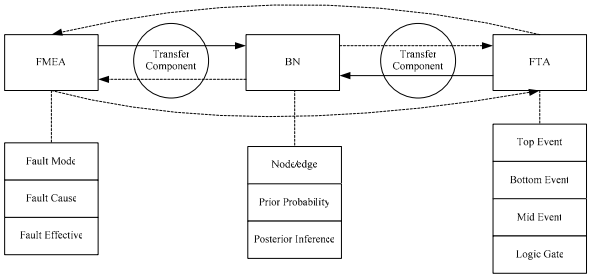

Figure 1. FBF Diagnosis Model

FBF can support the traditional “Forward FMEA/FTA”, “Backward FTA/FMEA” and the iterative process between them just like BFA [6].In essence, FBF is a method for fault information fusion. It can use FMEA to consider the possible fault modes as far as possible, use FTA to consider the possible combination of fault modes, and use the BN to conduce quantitative failure diagnosis based on the given priori probability and the specific posterior evidence.

A. Construct BN from FTA

BN can be constructed from any FT and the construction algorithm [3][4] has been used widely. Two main factor of BN

978-1-4244-4905-7/09/$25.00©2009 IEEE

is Node and Connection Strength, which can be corresponded to the Event and Logic Gate in FTA. The events in FT are represented as nodes in BN. If the same event appears many times in FT, only one node needs to be represented in BN. Any logic relationship in FT can be realized by conditional probabilities table (CPT) in BN. Every prior probability in FT can be assigned to node in BN directly.

B. Construct BN from FMEA

BN can also be constructed from FMEA. CFE (Cause Failure Effect)[2] is a kind of BN whose structure is constructed by the relationship between Fault Cause, Fault Mode, and Fault Effective to represent the causality and hierarchy. The effective of the fault mode in low level is the fault mode in high level. And the fault mode itself is the fault cause in the high level. According to this iterative relationship, every low level analysis result can be included to the high level analysis.

C. BN Combination

The BNs constructed from FMEA and FTA may be different in most cases. To some extent, FTA and FMEA are often treated as initial fault knowledge sources. BN can be constructed from scratch and it can also be constructed from these existed FTA and FMEA, if possible, which can greatly improve the efficiency of BN construction. There must be some information redundancy and overlapping in different BNs constructed from FMEA and FTA. These BNs should be merged to form a new BN and the information should be reserved as far as possible. Markov Based Bayesian Combination (MBBC) and Extended Relational Data Theory Based Bayesian Combination (ERDTBBC)[10] can be used to merge the different BN. The following question is how to get the new Conditional Probability Tables (CPT). If only the dependency sequence is changed, CPT can be derived from BN using Bayesian formula. If two BNs with different structure or different parameter, we can use MBBC to complete the structure combination first, and get the normalized probability based on Correlation Superposition [9].

D. BN Aggregation

BN's structure and representation may be too complicated when it is used for some special diagnosis inference. For example, a complicated software fault diagnosis includes many systems, subsystems, modules and variables. If we want to pay more attention to the relationship between subsystems and modules, and don't care about the internal information of these modules and probabilistic relation between trivial variables, then this complicated BN structure could certainty affect the inference efficiency.

So the combined BN should be modified adaptively to support the BN's modular packaging- Aggregation. Some closely related nodes, which have loose relation outside, could be aggregated as a big node just as an abstract part of BN. Because BN can be represented by a chain graph[10] equivalently, we can first transfer BN to chain graph in which undirected edge indicating equivalence relations and directed edge indicating Causal relationship. The same class of nodes can be treated as one big node, and the corresponding parameter should be modified to complete the aggregation of BN.

E. Reverse Construction

Although BN can use CPT to indicate the logic relation such as "and", "or" etc, but it is less intuitive than FT in logic representation. So sometimes we need to transform BN meeting some assumption to FT to intuitively represent the logic relation and calculate the minimal cut sets using FTA tool.

Occasionally BN should also be transformed to FMEA because sometimes we want to replenish the FMEA after the BN has been modified with other new information. Because basic FMEA doesn't have any conditional probabilities information, so it should be expanded to support the Object-Oriented transformation from BN to FMEA which could reserve the total quantitative information as far as possible.

F. Fault Diagnosis Inference

Though we can transfer BN to FMEA and FTA, but the core of FBF to fault diagnosis inference is still by BN constructed from FMEA and FTA.

Definition1: Fault Inference based on Bayesian network means computing the conditional probability for some nodes (fault event) given information (evidence) on other nodes.

The essence of this diagnosis inference is to reason the probabilistic of the fault event and corresponding causes through some symptoms got by testing or other means. This is easy when all available evidence is on variables that are ancestors of the node(s) of interest. But when evidence is available on a descendant of the node(s) of interest, we have to perform inference opposite the direction of the edges. To this end, we should employ Bayesian Theorem:

$$P(A|B)=P(B|A)P(A)/P(B). \quad (1)$$

Definition2: The Most Likely Combination -The combination of some special value of nodes in BN, which can get the biggest conditional probability given the evidence.

The practical strategy of diagnosis inference is: First give the CPT according to experience based on the logic relation represented by FTA; Then determine the value of some nodes according to the posterior evidence; Randomly give the value of other nodes and calculate the probability of these nodes without any evidence according to the conditional probabilities relation; Determine the next round of variable value to be calculated according to the probability of every node; Repeat this until n times(n big enough), the final result is the updated CPT.

On the other side, Conditional Event Algebra[9] can be used to expand the ability of BN to represent the logic relation between conditional event(A|X)and(B|Y).

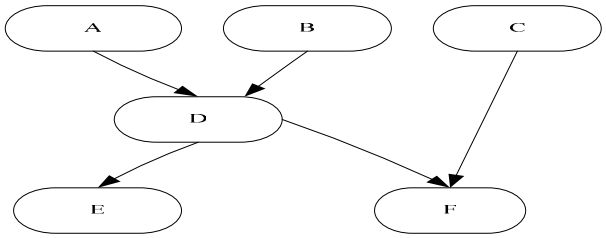

Figure 2. One Bayesian diagnosis network

For the BN showed in Fig.2, We can get the probability of P(D|EF)through Bayesian inference based on statistic data, but the probability of "(D|EF)∧(C|F)" or "(D|EF)∨(C|F)" can not be inferred . At this point, GNW Conditional Algebra can be used to calculate the corresponding conditional logic probability:

$$P((DEF)\vee(CF))=P((DEF\vee CF)\wedge(DEF\vee CF\vee EF))/P(DEF\vee CF\vee EF)$$
$$P((DEF)\wedge(CF))=P((CDEF)\wedge(DEF\vee CF\vee EF))/P(DEF\vee CF\vee EF)$$

III. CASE STUDY

One software system often suffered a random failure: no output or incorrect output. From the pre-observation we can know that one specific pointer location is random modified non-expectedly. From this point, we carried out the further diagnosis. First we use FTA/FMEA reverse integrated method to set up the initial FTA (Fig. 3) and FMEA (Table 1) of some part.

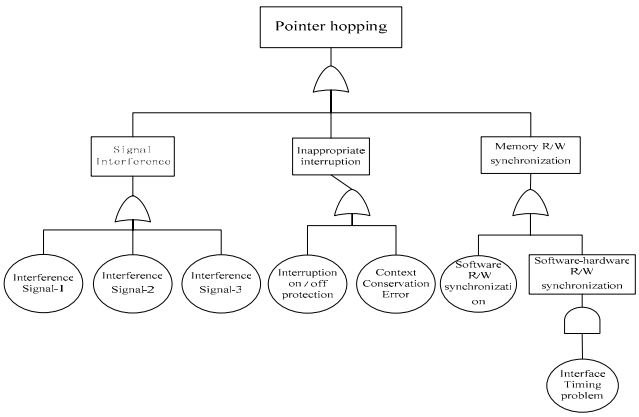

Figure 3. "Pointer Hopping"Fault Tree

TABLE I. "SIGNAL INTERFERENCE" FMEA

Mode	Fault Cause	Fault Effectives	others
Interference Signal-1(F1)	Wrong Signal-1 (C1)	Protected. No Effect(E1)	…
	Signal-1Transfer Error(C2)		
Interference Signal-2(F2)	Misidentification Interference Signal 2 as 1 (C3)	Maybe affect the memory R/W and some output variable.(E2)	…
	Wrong Signal-2 (C4)		
	Signal-2Transfer Error (C5)		
Interference Signal-3(F3)	Other Interference Signal(C6)	Maybe affect the memory R/W and some output variable.(E2)	…

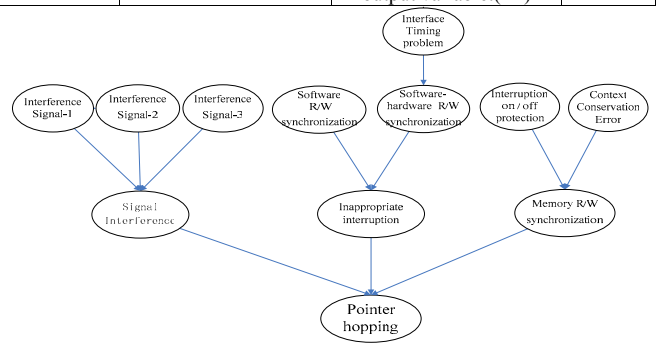

Figure 4. "Pointer Hopping"FT converting to BN1

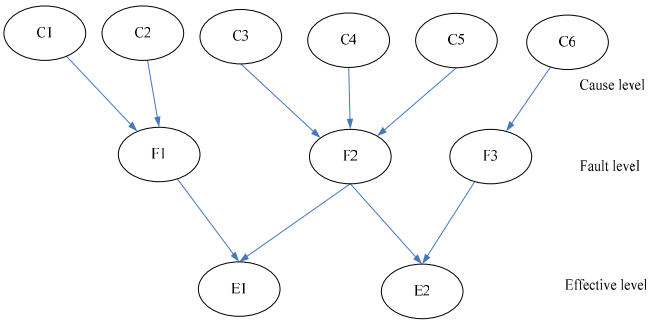

Figure 5. "Signal Interference" FMEA converting to BN2

From "Pointer Hopping" FT, we can construct the corresponding BN1, and from "Signal Interference" FMEA we can construct BN2. BN1 and BN2 can combined to form a new BN3 after some irrelevant part has been cut. We can carry out the diagnosis based on the final BN3.

TABLE II. CPT FOR "SIGNAL INTERFERENCE" NODE

F3	Yes		No	
F2	Yes	No	Yes	No
Signal Interference=Yes	0.9	0.05	0.05	0
Signal Interference=No	0.1	0.95	0.95	1

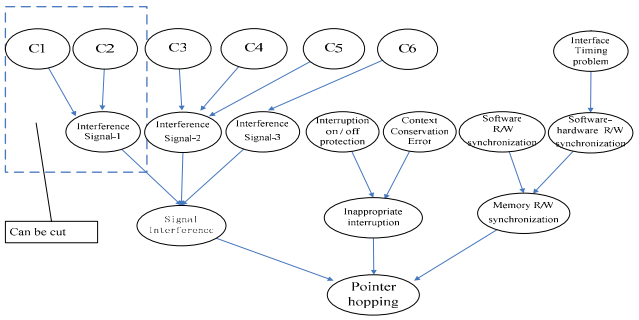

Figure 6. BN3 combined and aggregated from BN1 and BN2

First set every leaf node the prior probability, 0.05 for example. Specify the CPT for other node based on the logic relationship from FTA and specify the CPT for the node transferred from FMEA based on experience. CPT from FTA can be automated transferred. In fig 6, only CPT for node "F2" and "F3" should be given as table 2, for example. And we assume that the logic relationship between the leaf nodes of F2 is "or". P (F3| ¬ C6) = 0.5, P (F3|C6) = 0.05. The CPT for node "F3" is the same as the node "Memory R/W synchronization". The prior probability of other nodes can be calculated automatically.

Now because "Pointer hopping" has been set as evidence, the probability of it should be set as 100%. P(Inappropriate Interruption)=0.53, P(Signal Interference)=0.49 and P(Memory R/W Synchronization)=0.02. The Most Likely Combination is "Interruption on / off protection"=error and "Context protect"=error. If both of them are excluded, the new evidence can be specified and BN can be updated automate. Now P(Signal Interference)=0.96, is the biggest and the possible clause is C3, C4 or C5. P(C3)= P(C4)= P(C5)=0.27. We can continue to analyze C3, C4 and C5 based on this iterative process until the more refined final failure clause is found.

IV. Related Works

In (Andrea Bobbio et al., 1999)[11] the authors showed that any FT can be easily mapped into a BN and that basic inference techniques on the latter may be used to obtain classical parameters computed using the former.

In (Gregory Mocko et al., 2002)[13] Bayesian formula is used in conjunction with information extracted from FMEA, FTA, component reliability, and prior system knowledge to construct the Component-Indication Joint Probability Matrix (CIJPM). But this process is not reversible.

In (Karsten Pickard et al., 2005)[15], by integrating the procedures of the FMEA and FTA into a combined procedure, the mFMEA (multiple Failure Mode and Effects Analysis), an inclusive reliability analysis of complex, mechatronical systems, is made possible.

In (Martin S. Feather et al., 2004)[17] the author shows a unified approach that combines fault trees with explicit treatment of risk mitigations (a generalization of the notion of a "detection" seen in FMECA analyses). Fault trees capture the causal relationships by which failure mechanisms may combine to lead to failure modes. Risk mitigations encompass options to prevent risks, detect risks, and alleviate risks.

In (David Marquez et al., 2008)[18] a Hybrid Bayesian Network (HBN) framework is presented to analyze dynamic fault trees. No exact expression for the posterior marginal is needed and no conditional probability tables need to be completed. Sensitivity analysis, uncertainty, diagnosis, common cause failure analysis, can all be easily performed within this framework.

There are also a lot of fault diagnosis methods based on FMEA, FTA and BN [7][14]. But none of these methods mentioned above maximize the advantages and minimize the shortcomings of FMEA/FTA/BN at the same time. Most of these methods are only consider the combination of two methods, for example FMEA/FTA, FMEA/BN or FTA/BN, except CIJPM (Gregory Mocko et al., 2002)[13] .The main difference between it and FBF discussed in this paper is FBF set BN as the core component to connect FMEA and FTA and at the same time either of the two components can be transformed to another through BN, while CIJPM is not reversible. Also, to our knowledge FBF is the first application of combining FMEA and FTA based on BN for embedded software fault diagnosis.

V. Discussion and Conclusions

This paper introduces the problem of how to diagnosis embedded software fault. We have presented a model FBF to combine FMEA, FTA and BN, and we also have shown that our method provides substantially better analyzing and information fusion ability regarding quantitative analysis than both FMEA and FTA, or their combination. Especially our algorithm achieves significant improvements over these other approaches especially when there are some evidences or fault symptoms and therefore can dynamic adjust the diagnosis strategy to make the software diagnosis process more reasonable.

There are many interesting directions in which we can extend our work. Ongoing and future research that we are pursuing is to construct an expert system based on this diagnosis model, and combining some advanced bug detection method and automated test environment to set up an automated diagnosis system for embedded software.

Acknowledgment

Some of the experiments were performed using MSBN, a BN software developed by Microsoft.

Thank the anonymous reviewers for their useful comments. The work was supported by CDSTB 2132007B002.

References

[1] X. He, S.K. Yang, and B. Liu. "Embedded Software Fault Diagnosis based on FMEA/FTA." Computer Measurement & Control,2008.09.

[2] X.M. Shi, and H.W. Wang. "FMEA Model of Complex System Based on Bayesian Networks,"ORDNANCE INDUSTRY AUTOMATION, 2004 Vol.2.

[3] G.Y. Wan, Z.J. Ma, and Q.W. Hu, "The Fault Tree Analysis Based on Bayesian Networks, System Engineering Theory and Practice, 2004

[4] J.C. Li, N.Q. Hu, G.J.Qin, and S.S.Wen. "Application and Construction of Basesian Networks Based on Fault Trees." Computer Engineering and Application, 2003, 24.

[5] C.F. GAN, H.B. CAO, and Y.H. HUANG, "CAI Jinyan. FMECA and FTA Based Fault Diagnosis and Fault Prognosis," Systems Engineering and Electronics, 2002, Vol.124, No.11.

[6] Z. Bluvband, R. Polak, and P. Grabov, "Bouncing Failure Analysis (BFA)," The Unified FTA-FMEA Methodology, IEEE RAMS 2005.

[7] Z. Bluvband, P. Grabov, and O. Nakar,"Expanded FMEA," RAMS Symposium, LA, 2004.

[8] K.W. Przytula, and D. Thompson, "Construction of Bayesian Networks for Diagnostics," IEEE 2000.

[9] A. Bobbio, L. Portinale, M. Minichino and E.Ciancamerl. "Improving the analysis of dependable systems by mapping fault trees into Bayesian networks," Reliability Engineering & System Safety, March 2001, Vol.71, Issue. 3, , pp.249-260.

[10] W.Y. Liu, W.H. Li, and K. Yue, “Intelligent Data Analysis.” Beijing: Science Press. 2007.

[11] A. Bobbio , L.G. Portinale, M. Minichino, and E. Ciancamerla. “Comparing Fault Trees and Bayesian Networks for Dependability Analysis.” SAFECOMP’99, LNCS 1698, 1999, pp.310-322.

[12] I. Ruiz, E. Paniagua, J. Albert, and J. Sanabria. “State Analysis: an Alternative Approach to FMEA, FTA and Markov Analysis.” 2000 Proceedings Annual Reliability and Maintanability Symposium.

[13] G. Mocko, and R. Paasch. “INCORPORATING UNCERTAINTY IN DIAGNOSTIC ANALYSIS OF MECHANICAL SYSTEMS.” ASME 2002.

[14] C.H. Yang, C.A. Zhu., and X.J. Hu, “Inference Method for Fault Diagnosis of Complex Systems Based on Bayesian network.” IEEE 2008.

[15] K. Pickard, and P. Müller, “Bernd Bertsche. Multiple Failure Mode and Effects Analysis – An Approach to Risk Assessment of Multiple Failures with FMEA.” IEEE2005.

[16] B.H. Lee. “Using Bayes Belief Networks In Industrial FMEA Modeling And Analysis.” IEEE 2001.

[17] S. M. Feather. “Towards a Unified Approach to the Representation of, and Reasoning with, Probabilistic Risk Information about Software and its System Interface.” Proceedings of the 15th International Symposium on Software Reliability Engineering (ISSRE’04).

[18] D. Marquez, M. Neil and N. Fenton. “Solving Dynamic Fault Trees using a New Hybrid Bayesian Network Inference Algorithm.” IEEE 2008.

[19] I. Canova Calori, and T. Stålhane. “FMEA and BBN for robustness analysis in web-based applications.” European Safety and Reliability Conference 2007.

[20] K.J. Yusuke, Y. Kitamura and R. Mizoguchi. “Ontology-Based Transformation Extended Functional Model To Fmea. International Conference On Engineering Design Iced 05 Melbourne,” August,2005.