基于动态故障树的AFDX网络性能可靠性分析

孙利娜[1] 黄 宁[1,2] 张 朔[1]
(北京航空航天大学可靠性与系统工程学院 北京 100191)[1]
(北京航空航天大学可靠性与环境工程技术重点实验室 北京 100191)[2]

摘 要 AFDX网络是现代飞机集成的基础,其性能可靠性是飞机高可靠运行的保证。当前的研究虽然进行了性能评估或预测,但并没有针对网络故障所具有的相互影响、传播、依赖等特点深入研究,更缺乏对性能可靠性进行评估的方法。提出一种基于业务的动态故障树建模方法,对AFDX网络的数据传输是否及时、完整及传输次序、到达源端是否正确等性能可靠性问题的故障原因及故障模式进行了分析和建模,给出了一种量化计算方法。分析思路和方法对AFDX网络设计、动态故障树建模、可靠性分析和评估都有较好的意义和借鉴作用。

关键词 AFDX网络,性能可靠性,业务,动态故障树
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.10.009

Performance Reliability Analysis of AFDX Network Based on Dynamic Fault Tree

SUN Li-na[1] HUANG Ning[1,2] ZHANG Shuo[1]
(School of Reliability and Systems Engineering, Beihang University, Beijing 100191, China)[1]
(Key Laboratory of Science & Technology on Reliability & Environmental Engineering, Beihang University, Beijing 100191, China)[2]

Abstract AFDX network is the foundation of modern aircraft integration, and its performance reliability ensures the high reliability of aircraft operations. The current study analyzes the reliability issues from the perspective of performance evaluation and prediction, but fails to delve into the features such as interacting, communication and dependency of network fault. This paper proposed a dynamic fault tree modeling method based on practical application. It analyzes and models the causes of failure and failure modes of AFDX network's data transmission. A quantitative calculation method was given. The analysis and method in this paper are of great significance and provide a reference to AFDX network design, dynamic fault tree modeling, reliability analysis and evaluation.

Keywords AFDX network, Performance reliability, Application, DFT

AFDX网络以以太网为基础,采用全双工通信原理,引入虚链路、冗余网络机制,达到数据传输确定性、及时性、容错性等要求。目前其已成为大型飞机的主干通信网络,国际先进的大型飞机如空客A380、波音787等均选用AFDX作为机载主干通信网络。

随着AFDX网络成为机载主干通信网络,其网络性能表现也受到了广泛的关注。时延是网络性能的重要体现,相关学者们基于网络演算法[1-7]以及网络模拟的方法[8-10],对不同情况、不同考虑因素下AFDX网络的传输时延进行了有效的分析和估计。网络时延问题是网络故障的一种体现,这些分析目前还没有深入到对造成AFDX时延的故障原因及故障模式的探究。数据完整性也是AFDX网络性能关注的重要方面,文献[13,14]用故障树的建模方法分析了AFDX网络中的数据是否能够完整地到达,对故障原因及故障模式进行了探究,但其建模是从单个帧的角度考虑,这样的考虑显然是不合适的。除此之外,网络传输次序及到达源端是否正确也是AFDX网络必须关注的性能问题,文献[15,16]已对这方面进行了较为详细的说明,但目前还少有学者对这两方面的网络性能可靠性问题进行建模分析。

故障树分析方法可以通过设定不同的顶事件多方面考察网络的性能可靠性,同时可以分析影响网络性能可靠性的故障原因。针对具有动态逻辑的复杂时序故障,1992年,J. B. Dugan教授首次提出了动态故障树分析方法(DFT)[17],该方法被广泛应用于系统的可靠性分析。AFDX是一个系统,其网络传输具有故障模式的相互影响、依赖、传播等特点,对于这些复杂的、动态的故障原因,可以利用DFT方法进行建模和可靠性分析,但AFDX网络又有其作为网络属性的独特性。网络功能的完成本质是搭载在网络上不同业务的实现,例如通信网中的短信业务、通话业务等。而业务是以数据传输的方式体现的,DFT对系统进行自上而下的演绎分析,其实质上是一种自顶向下地对系统进行由大到小层级式的分析与建模。但是数据传输并不是自顶向下的,用传统的对系统自上而下解剖式的建模方式对AFDX网络系统进行建模分析显然是不合适的。基于这些考虑,本文在DFT模型的基础上提出了一种基于业务的动态故障树建模方法,并根据此建模方法对AFDX网络的数据传输是否完整、及时以及数据帧次序、到达的源端是否正确等性能可靠性进行建模分析;最后选取一个模型进行了定量计算和验证。

1 网络性能可靠性

目前针对AFDX网络性能可靠性的考察主要是考察AFDX网络在数据传输过程中完整传输、及时传输、次序传

到稿日期:2015-07-15 返修日期:2015-09-20
孙利娜(1992—),女,硕士生,主要研究方向为网络可靠性;黄 宁(1968—),女,博士,教授,博士生导师,主要研究方向为网络可靠性、软件测试、可靠性;张 朔(1990—),男,硕士生,主要研究方向为网络可靠性。

输、正确传输等的能力。相应地，其性能可靠性为数据完整可靠性、及时可靠性、次序可靠性、源可靠性[16]。

数据完整可靠性：在规定条件下和规定时间内，服务数据无错误传输的能力。

及时可靠性：在规定条件下和规定时间内，从发送端发送的数据包及时被接收端接收的能力。

次序可靠性：在规定条件下和规定时间内，虚拟链路的端系统保持其接受和发送数据次序的能力。

源可靠性：数据被正确的源端接收到的能力。

2 AFDX 网络 DFT 建模

传统的故障树分析法是一种基于静态逻辑或静态故障机理的分析方法，系统规模不断扩展和复杂，系统功能联系日趋紧密，系统的故障模式和故障影响并不仅仅呈现静态关系。针对这些问题，美国 J. B. Dugan 教授利用 Markov 理论和组合数学方法的优势建立了动态故障树模型，于 1992 年在分析空间站及空中交通控制等复杂系统中首次应用[17]，随后该方法被不断推广。一般称至少含有一个动态逻辑门的故障树为动态故障树，动态故障树中的动态逻辑门主要有功能相关门、优先与门、顺序相关门、冷备件门、温备件门、热备件门。

AFDX 作为一个系统，其网络拓扑结构复杂，软硬件故障交互，故障模式具有传播、依赖等特点。相较于静态故障树，DFT 可以对其故障进行合理的建模，并对网络的可靠性进行分析。但 AFDX 网络又有其作为网络属性的独特性。网络功能的完成本质是搭载在网络上不同业务的实现，例如通信网中的短信业务、通话业务等。而业务是以数据传输的方式体现的，DFT 建模方法是对系统进行自上而下的演绎分析，其实质上是一种自顶向下地对系统进行由大到小层级式的分析与建模。但是数据传输并不是自顶向下的，基于此，本文在 DFT 建模的基础上提出了一种基于业务的故障树建模，下面给出建模的方法流程。

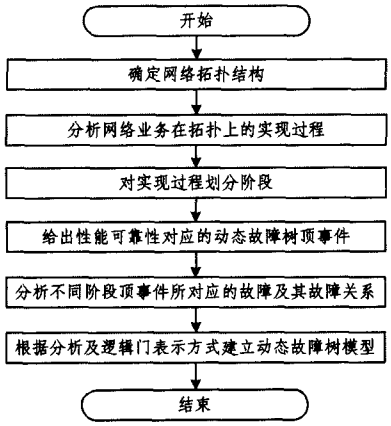

图 1 基于业务的动态故障树建模

2.1 确定网络拓扑结构

AFDX 网络存在多种物理拓扑结构，有单个端系统的自发自收、冗余拓扑结构、级联结构及复杂拓扑结构，本文在此选择冗余拓扑结构，如图 2 所示。

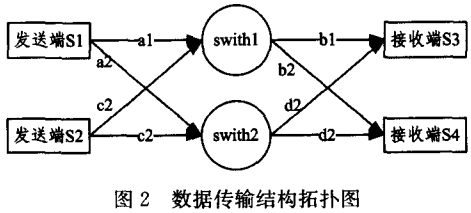

图 2 数据传输结构拓扑图

2.2 业务实现过程分析

上述拓扑结构 AFDX 网络的业务实现过程中，总共有 4 类业务，4 类业务在 AFDX 网络的实现途径分别如下。

第一类业务：S1-冗余双网-S3；

第二类业务：S1-冗余双网-S4；

第三类业务：S2-冗余双网-S3；

第四类业务：S3-冗余双网-S4。

在此我们选取第一类业务进行分析，在 S1 发送端，数据帧经过不同报头的添加并复制后得到传输所需的冗余帧；冗余帧经过冗余双网 A 和 B 中链路和交换机的转发传输到达接收端 S3；接收端 S3 通过完整性检查和冗余管理获取有效帧，并经过接收端的去报头处理获取有效字段。

2.3 实现过程划分阶段

业务的实现过程是以数据处理和传输的方式体现的，数据的处理及传输主要集中在发送端、冗余双网、接收端。故将业务实现过程依次划分为发送端 S1 传输、AB 双网传输、S3 接收端传输。

2.4 性能可靠性动态故障树顶事件

AFDX 网络性能可靠性分为数据完整可靠性、及时可靠性、次序可靠性和源可靠性；依据这 4 个方面可以确定故障树依次对应的 4 个顶事件，分别为 AFDX 网络传输数据丢帧、AFDX 网络传输数据有误、AFDX 网络数据传输发生延时、AFDX 网络传输源端有误。

2.5 故障分析及动态故障树建模

2.5.1 AFDX 网络丢帧动态故障树

数据丢帧故障树按照数据传输流程分 3 个阶段进行考虑：发送端 ES、AB 网以及接收端 ES。AB 双网的传输主要由 2 个交换机和 4 条链路完成。其中，任意阶段发生丢帧均会造成整网数据传输发生丢帧。

同时，3 个阶段的数据传输又有一定的联系。在相关协议中，到达接收端的帧要经过完整性检查后，采用“先到先得”的冗余管理算法获取有效帧。

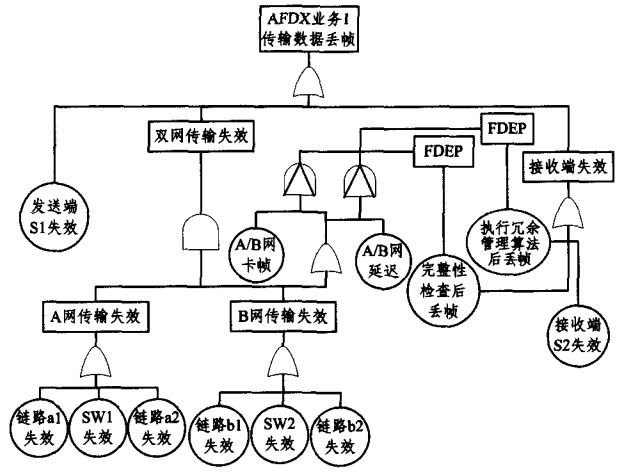

图 3 AFDX 网络传输丢帧动态故障树

传输过程中，如果一个传输网络先发生了卡帧，另一个网络在卡帧之后由于某一比特错误发生了丢帧，那么整个网络经过完整性检查就会发生丢帧现象。在网络传输过程中，传输的每一组帧都会编上序号，在冗余管理过程中，如果一个传输网络先发生丢帧，另一个传输网络的冗余帧发生了延时，并在发生丢帧的传输网络中下一个帧到来之后到达，那么冗余管理机制就会获取先到达的帧，而冗余帧因次序小于获取的帧，按照冗余管理算法将会被丢弃，对于整个网络而言就发生了丢帧现象。这两种失效关系都对事件的发生顺序有要求，需要用优先与门来表示。按照上述分析，可以建立如图 3 所示的动态故障树。

2.5.2 AFDX 网络传输发生时延动态故障树

在 AFDX 网络传输过程中，时延主要来自两个方面：1）网络中相关器件失效造成数据处理时间增多，2）网络配置不当造成的数据传输时延的增大。在发送端，系统配置不当主要是来自于对虚链路（VL）的配置和缓冲区的配置，其次是端系统器件失效造成的处理数据时间变长；在双网传输过程中，时延主要来自于资源竞争或者信道拥塞，以及交换机数据处理，交换机数据处理时延又主要来自于交换机配置不当和硬件失效；在接收端系统时延主要来自于缓冲区配置不当、最大偏移时间设置过大以及硬件失效。按照上述分析可以建立如图 4 所示的动态故障树。

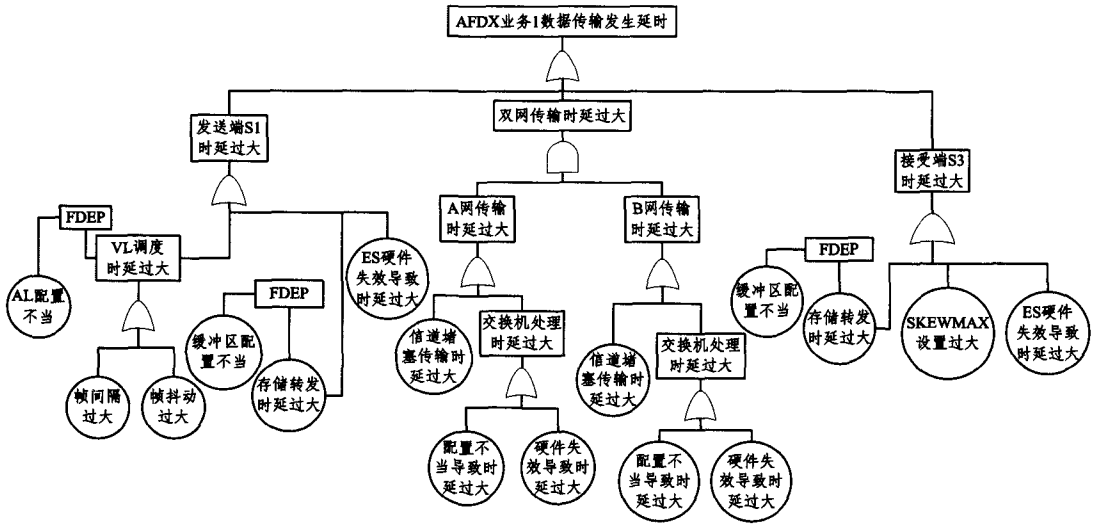

图 4　AFDX 网络传输时延动态故障树

2.5.3 AFDX 网络传输次序有误故障树

数据帧次序是对于 VL 而言的，AFDX 网络对每个 VL 上的数据帧添加序列号。对于发送端，系统启动配置、序列号的初始化、帧添加序列号、帧存储等过程均可能致使序列号出现错误从而导致次序有误。

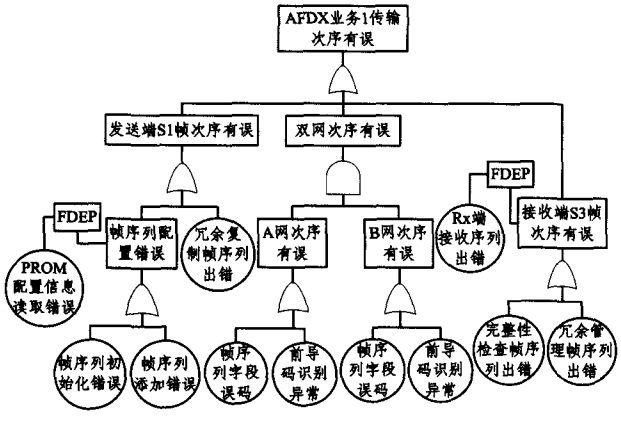

图 5　AFDX 网络传输次序有误动态故障树

在 A、B 双网冗余传输过程都出现帧序列号误码将导致接收端的次序有误。对于接收端系统，接收到传输来的序列号错误的帧、数据帧存储、冗余管理和完整性检查的功能失效都会导致数据帧的传输次序有误。经过分析，可以建立如图 5 所示的动态故障树模型。

2.5.4 AFDX 网络传输源端有误故障树

在 AFDX 网络传输过程中，一系列的帧都要求按照要求传输到正确的源端口，即数据要被正确的源端口接收才是有效的。在发送端，CPU 主要为传输到 AFDX 网络的数据帧添加 UDP 报头，然后判断数据帧的长度，根据长度确定是否分片，分片后为数据添加 IP 报头，然后通过 DPROM 将数据传输到 FPGA 模块，FPGA 模块为数据添加以太网报头，数据帧进入链路层，经过调度并添加序列号，此后帧进入冗余管理单元，经过冗余复制后发送，经过冗余双网的传输到达接收端[18]。接收端与发送端类似，恰好是发送端的逆过程。如果发送端是包装的过程，接收端就是解包的过程。经过分析，建立如图 6 所示的动态故障树模型。

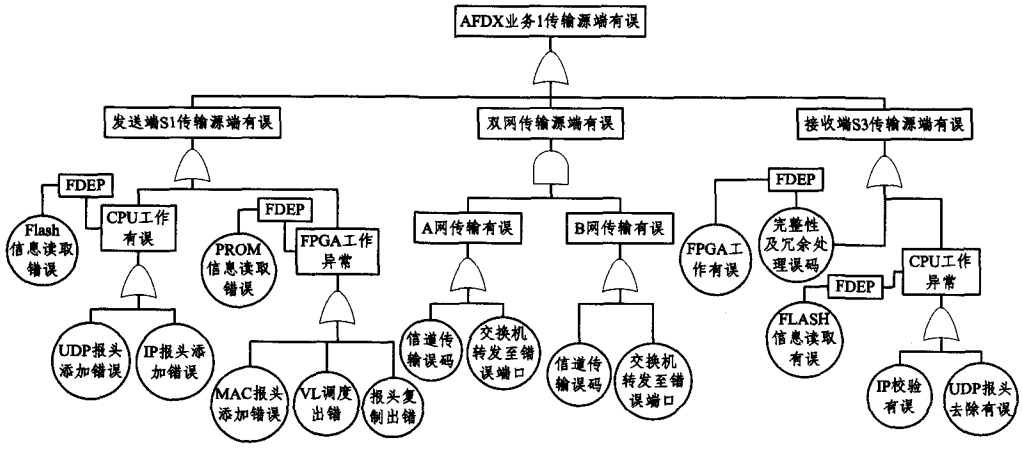

图 6　AFDX 网络传输源端有误动态故障树

3 AFDX 网络动态故障树定量计算

上述建模过程给出了 AFDX 动态故障树的 4 个模型，为了说明模型的合理性和价值，在此选取一个模型进行定量分析。选取 AFDX 网络丢帧动态故障树模型，在该动态故障树中，基本事件都服从指数分布，参考相关技术报告及文献[13]中的数量级，假设基本事件的近似失效率如表 1 所列。

表 1　基本事件失效率

基本事件	序号	失效率
发送端/接收端 ES 失效	1	1.10E−10
链路 a1/a2/b1/b2 失效	2	5.00E−11
交换机 SW1/SW2 失效	3	3.71E−9
A/B 网卡帧	4	4.52E−8
A/B 网延迟	5	3.63E−8
完整性检查丢帧	6	7.60E−8
冗余管理丢帧	7	8.40E−8

具体求解动态故障树的过程中，可以将动态子树模块化，转化成马尔科夫链的方式求解，然后按照传统静态故障树的方法定量求解整个动态故障树的相关参数。

在可靠性分析中，串联模型可靠度的数学公式为：

$$R(t)=\prod_{i=1}^{n}R_i=\prod_{i=1}^{n}e^{-\int_0^1\lambda_i(t)dt}$$

其中，各个单元均服从指数分布，且系统的寿命也服从指数分布，系统的故障率 λ_s 为系统中各单元的故障率 λ_i 之和。可表示为 $\lambda_s=\sum_{i=1}^{n}\lambda_i$。

A/B 网络传输失效由 3 个基本事件通过或门表示，或门在可靠性模型中表示的是一种串联关系，那么 A 网络失效率可以表示为：

$\lambda_A=\lambda_{a1}+\lambda_{SW1}+\lambda_{a2}=1.371\times10^{-10}$

同时，$\lambda_B=1.371\times10^{-10}$。

假设动态故障树中的动态子模块为 M1，如图 7 所示，将其转化为马尔科夫状态转移链。

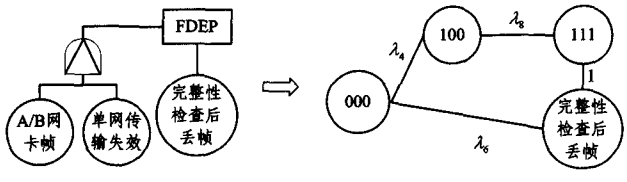

图 7　动态子树 Markov 转移图

其中 000 依次表示动态子模块中 3 个基本事件从左到右依次处于完好状态或没有发生状态，0 变为 1 表示该基本事件失效或发生。

文献[19]给出了一种求解马尔科夫链的简单方法，通过推导不同链长的马尔科夫链的失效公式，根据不同链长的公式求解失效链路的失效概率，最后对所有链路的失效概率求和，从而求出整个马尔科夫链的失效概率。

故障树中单网传输失效率为：

$\lambda_8=\lambda_A+\lambda_B=2.742\times10^{-10}$

上述马尔科夫链中链路为 3 的失效链路的失效概率为：

$$P_1(t)=\lambda_4\lambda_8\left[\frac{-e^{-\lambda_4 t}}{\lambda_4(1-\lambda_4)(\lambda_8-\lambda_4)}+\frac{-e^{-\lambda_8 t}}{\lambda_8(1-\lambda_8)(\lambda_4-\lambda_8)}+\frac{-e^{-t}}{(\lambda_8-1)(\lambda_4-1)}+\frac{1}{\lambda_4\lambda_8}\right]$$

链路为 1 的失效概率为：

$P_2(t)=1-e^{-\lambda_6 t}$

所以整个动态子模块的失效概率为：

$F_1(t)=P_1(t)+P_2(t)$

类似地可以求得另一功能相关门动态子模块 M2 的失效概率为 $F_2(t)$。

将动态故障树模块化，如图 8 所示。

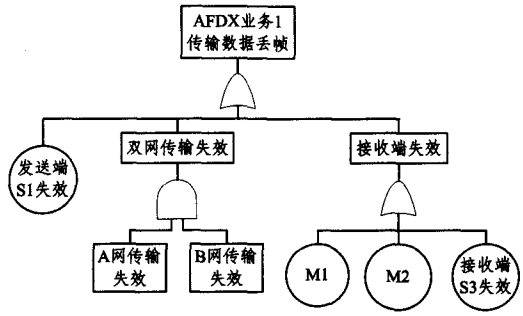

图 8　动态故障树模块化图

根据上述分析，类似地处理其余动态子模块，通过设定不同的时间节点，可以定量计算顶事件发生的概率，结果如表 2 所列。

表 2　顶事件不可靠度

时间(t)	不可靠度(Unreliability)
1000	1.60534213E−004
2000	3.21042655E−004
3000	4.81525330E−004
4000	6.41982241E−004
5000	8.02413395E−004
6000	9.62818793E−004
7000	1.12319844E−003
8000	1.28355234E−003
9000	1.44388050E−003
10000	1.60418292E−003

4 分析

上述计算选取了一个模型，该模型将发送端传输和接收端传输两个重要业务的实现过程考虑在内，同时又添加了文献[13]中没有分析到的动态逻辑故障，模型更为合理和全面，也清楚地体现了不同阶段与 AFDX 网络性能可靠性相关的具体故障原因和故障模式等。从计算结果可以看出，10000 小时之内，AFDX 业务 1 传输数据帧丢失的概率数量级都在 10^{-3} 之内，符合飞机重要系统高可靠性的预期。同时失效概率随着时间的推移而增大，在 7000 小时时，顶事件的失效概率提高了一个数量级。以上分析的过程和结果可以作为后续对 AFDX 相关业务实现可靠性评价的指导和参考。

结束语　作为机载主干通信网络的 AFDX 网络的性能可靠性是飞机高可靠性的基础和保证，本文综合考虑 AFDX 网络性能可靠性故障模式的动态逻辑时序特性和 AFDX 网络特有的网络特征，在动态故障树建模的基础上，提出了一种基于业务的动态故障树建模方法。在此方法上，通过对数据完整传输、及时传输、次序传输、正确传输的分析，多方面考察 AFDX 网络的性能可靠性，对其进行了分析建模，并给出了定量分析，该建模的方法和思路对工程实践有较好的指导意义。需要说明的是，文中对于业务的分析和建模，目前还没有考虑

（下转第 62 页）

Proceedings of the 13th International Conference on System Sciences (ICSS). Honolulu, HI, 1980

[14] Baker J, Thornton J. Software engineering challenges in bioinformatics[C]// International Conference on Software Engineering. 2004:12-15

[15] Xie Xiao-yuan, Ho J, Murphy C, et al. Improving the quality of computational science software by using metamorphic relations to test machine learning applications[J]. Department of Computer Science Columbia University, 2009, 12(1):1-80

[16] Ho J W K, Lin M W, Adelstein S, et al. Erratum: customising an antibody leukocyte capture microarray for systemic lupus erythematosus: beyond biomarker discovery[J]. Proteomics-Clinical Applications, 2010, 4(6/7):679-679

[17] Ho J W K, Stefani M, Remedios C G, et al. Differential variability analysis of gene expression and its application to human diseases[J]. Bioinformatics, 2008, 24:390-398

[18] Xie Xiao-yuan, Ho J W K, Murphy C, et al. Testing and validating machine learning classifiers by metamorphic testing[J]. Journal of Systems and Software, 2011, 84(4):544-558

[19] Xie Xiao-yuan, Ho J, Murphy C, et al. Application of metamorphic testing to supervised classifiers[C]// International Conference on Quality Software. IEEE, 2010:135-144

[20] Jones J A, Harrold M J, Stasko J. Visualization of test information to assist fault localization[C]// ICSE 2002. 2002:467-477

[21] Jia Y, Harman M. A Custimizable, Runtime-Optimized Higher Order Mutation Testing Tool for the Full C Language[C]// Practice and Research Techniques. 2008:94-98

[22] Ma Y S, Offutt J, Kwon Y R. MuJava: An Automated Class Mutation System[J]. Journal of Software Testing, Verification and Reliability, 2005, 15(2):97-133

[23] Chen T Y, Kuo F C, Liu Ying, et al. Metamorphic Testing and Testing with Special Values[C]// Acis International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. 2004:128-134

[24] Dong Guo-wei. Metamorphic testing techniques for error detection efficiency[D]. Southeast University, 2009

[25] Chen T Y, Tse T H, Zhou Zhi-quan. Semi-proving: an integrated method based on global symbolic evaluation and metamorphic testing[C]// ACM Sigsoft Software Engineering Notes, 2002, 27(4):191-195

[26] Hutchins M, Foster H, Goradia T, et al. Experiments of the effectiveness of dataflow-and controlflow-based test adequacy criteria[C]// International Conference on Software Engineering. IEEE Computer Society Press, 1994:191-200

(上接第 56 页)

到多业务交叉传输实现的情况，这方面将是我们后续研究的一个深入点。

参 考 文 献

[1] Charara H, Scharbarg J, Ermont J, et al. Methods for bounding end-to-end delays on an AFDX network[C]// 18th Euromicro Conference on Real-Time Systems. IEEE, 2006:193-202

[2] Mifdaoui A, Frances F, Fraboul C. Real-time guarantees on Full-Duplex Switched Ethernet for military applications[OL]. http://oatao.univ-toulouse.fr/2160

[3] Zeng X, Song D. The Research on End-to-End Delay Calculation Method for Real-Time Network AFDX[C]// International Conference on Computational Intelligence and Software Engineering. 2010:1-4

[4] Zhao Yong-ku, Wang Hong-chun, Tang Lai-sheng, et al. Analysis Method of End-to-End Delays on an AFDX Avionic Network [J]. Electronics Optics & Control. 2013, 20(4):81-83(in Chinese)
赵永库，王红春，唐来胜. AFDX 网络端到端时延分析方法[J]. 电光与控制，2013，20(4)：81-83

[5] Wu Z T, Huang N, Wang X W, et al. Analysis of end-to-end delay on AFDX based on stochastic network calculus[J]. Systems Engineering and Electronics, 2013, 35(1):168-172(in Chinese)
伍志韬，黄宁，王学望，等. 基于随机型网络演算的 AFDX 端端时延分析方法[J]. 系统工程与电子技术，2013，35(1)：168-172

[6] Scharbarg J, Ridouard F, Fraboul C. A Probabilistic Analysis of End-To-End Delays on an AFDX Avionic Network[J]. IEEE Transactions on Industrial Informatics. 2009, 5(1):38-49

[7] Georges J P, Rondeau E, Divoux T. Evaluation of switched Ethernet in an industrial context by using the Network Calculus[C]// IEEE International Workshop on Factory Communication Systems. 2002:19-26

[8] Zhang J, Li D, Wu Y. Modelling and performance analysis of AFDX based on Petri Net[C]// International Conference on Future Computer and Communication. IEEE, 2010:V2-566-V2-570

[9] Wang C, Li J, Hu F. Fault tree synthesis for an avionic network [C]// International Conference on Transportation, Mechanical, and Electrical Engineering. IEEE, 2011:155-159

[10] Wang Chen-hu. Reliability Model and Performancy Analysis of AFDX Avionics Networks[D]. Shanghai: Shanghai Jiao Tong University. 2012(in Chinese)
王臣虎. AFDX 航空网络的可靠性建模与性能分析[D]. 上海：上海交通大学，2012

[11] Huang N, Wu Z T. Survey of network reliability evaluation models and algorithms[J]. Systems Engineering and Electronics, 2013, 35(12):2651-2660(in Chinese)
黄宁，伍志韬. 网络可靠性评估模型与算法综述[J]. 系统工程与电子技术，2013，35(12)：2651-2660

[12] Li S, Wang X W, Kang R. Investigation on Reliability Parameters of Avionics Full Duplex Switched Ethernet (AFDX) for Integrity Requirements[J]. Journal of Xi'an Jiaotong University, 2013, 47(3):126-131(in Chinese)
李硕，王学望，康锐. 面向完整性要求的航空电子全双工交换式以太网可靠性评价参数研究[J]. 西安交通大学学报，2013，47(3)：126-131

[13] Dugan J B, Bavuso S J, Boyd M A. Dynamic fault-tree models for fault-tolerant computer systems[J]. IEEE Transactions on Reliability. 1992, 41(3):363-377

[14] Du Y J. Research on avionics full duplex switched Ethernet[J]. Computer Engineering, 2009, 35(11):77-79(in Chinese)
杜亚娟. 航空全双工交换式以太网探究[J]. 计算机工程，2009，35(11)：77-79

[15] Zhu Zheng-fu, Li Chang-fu, He En-shan. The dynamic fault tree analysis method based on Markov chain[J]. Acta Armamentarii, 2008, 29(9):1104-1107(in Chinese)
朱正福，李长福，何恩山，等. 基于马尔可夫链的动态故障树分析方法[J]. 兵工学报，2008，29(9)：1104-1107