基于航电系统架构模型的安全性分析工具的设计与实现

徐文华 张育平
(南京航空航天大学计算机科学与技术学院 南京 211100)

摘 要 航电系统作为安全关键系统,必须对其进行共模分析和区域安全性分析,以满足系统的隔离性需求。随着航电系统综合化程度的提高,传统的共模分析和区域安全性分析方法主要依赖于分析人员对系统的理解程度,无法确保隔离性需求的完整性。同时由于安全性分析人员与系统设计人员对系统的理解不同而导致系统需求难以追溯,尤其在设计方案频繁变更的情况下,会出现安全性分析结果不准确、不一致的情况。针对上述问题,设计并实现了一种基于航电系统架构模型的安全性分析工具,通过采用物理架构中数据信号路径追溯的方法自动完成故障树建模,并基于此故障树完成共模分析和区域安全性分析,得出共模检查单和区域隔离性需求。以某飞机驾驶舱显示系统为案例的实验结果表明,该工具能对 SysML 语言描述的航电系统架构模型进行故障树自动建模,并能对需要隔离的系统组件进行标记,确保了共模分析和区域安全性分析结果的完整性。

关键词 航电系统架构,系统建模语言(SysML),共模分析,区域安全性分析,故障树建模
中图法分类号 TP302 **文献标识码** A

Design and Implementation of Safety Analysis Tool Based on Avionics System Architecture Model

XU Wen-hua ZHANG Yu-ping
(School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, China)

Abstract Common mode analysis and zone safety analysis need to be conducted to the safety critical avionics system in order to form new separation requirements. As the avionics system is becoming more and more integrated, the traditional common mode analysis and zone safety analysis methods can't ensure the completeness of the separation requirements as they mainly rely on how well the analyzers understand the system. Meanwhile, the requirements of the system are hard to be traced due to the differences between the understanding of the safety analyzers to the system and that of the system designers, especially when the design changes frequently, safety analysis results are always inaccurate and inconsistent. Aiming at the above problems, a safety analysis tool based on avionics system architecture model was designed and implemented. Fault tree auto-modeling was conducted through tracing the data signal path in physical architecture. Then common mode analysis and zone safety analysis were conducted based on the generated fault tree, getting a common mode checklist and some zone separation requirements. The results of the case study on one cockpit display system indicate that the tool is able to conduct auto fault tree modeling based on the avionics system architecture model described in SysML, and also can mark the components need to be isolated, ensuring the completeness of the results of common mode analysis and zone safety analysis.

Keywords Avionics system architecture model, SysML, Common mode analysis, Zone safety analysis, Fault tree modeling

1 引言

航空电子的发展经历了分立式、联合式、综合式以及先进综合式[1]几个阶段。为了增强传统航空电子系统的功能,提高其性能,降低飞机生命周期费用,同时解决系统软硬件的升级移植问题,美国航电委员会提出了综合模块化航空电子(IMA)的概念。综合化航电系统将进行信号和数据处理的航电设备计算功能集中在多功能处理器中,集成到航电设备架中,并利用高带宽光纤总线进行内部互连[2]。综合化航空电子系统本质上是一个开放的分布式实时计算环境,通过综合,达到硬件通用化、功能软件化、软件运行环境标准化,最终实现系统的高度综合以及信息的高度共享[3]。然而,综合化航电系统中功能依赖关系信号交联复杂,故障传播致因关系难以确定,因此需要对其进行安全性分析。

故障树分析是一种逻辑性强、表达直观的系统安全性分析方法。它以一种图形化的表达方式,将系统故障形成的原因从总体到部分按照树形结构自顶向下逐层细化,并通过与门、或门、表决门等逻辑门连接,由结构函数给出其数学描述。通过求解故障树顶事件的最小割集和失效概率,可以确定可能造成系统故障的各种因素、因素之间的逻辑关系及其发生概率[4]。航电系统为安全关键系统,因此在假设故障独立的前提下构建故障树进行分析后,还需要对航电系统进行共模分析和区域安全性分析[5]。

为了提高航电系统的安全性,航电系统普遍采用了冗余

本文受国家 973 计划资助项目(2014CB744901,2014CB744903,2014CB744904,2014CB744905)资助。
徐文华(1992-),女,硕士生,主要研究方向为软件工程与开发技术,E-mail:xstraw@126.com;张育平(1959-),男,副教授,主要研究方向为软件工程与数据库技术。

设计方案，其基本思想是两个分离且独立的分系统同时发生故障的可能性远低于一个单独的分系统。然而，随着装备复杂程度的提高，冗余系统的独立性往往被不经意间造成的依赖关系所破坏，因此需要对航电系统进行共模分析（Common Mode Analysis，CMA）。CMA 针对影响一个以上冗余通道的故障进行分析，识别独立冗余系统中可能存在的相关性及相互关系，从而查找导致共模故障发生的原因。另外，综合化航电系统的综合集成设计也使得其系统/组件之间在结构上和功能上的相互关联性和影响力很强，区域安全性问题更为突出。区域安全性分析 ZSA（Zone Safety Analysis，ZSA）从复杂系统各组成部分之间的相互干涉关系入手，找出区域内的危险因素，为制定安全性准则提供了重要依据。然而，传统的共模分析和区域安全性分析方法主要依赖于工程师对系统的理解程度，该方法十分主观。另外，手工建树耗时耗力，特别是系统设计的迭代对故障树建模和分析结果的更新造成了严重的负担。由于安全性分析与系统设计并不是同步进行的，因此很难保证失效模式同系统架构的一致性[6]。

针对上述问题，本文面向广泛应用于工程实践的 SysML 语言描述的航电系统物理架构，设计并实现了一种基于航电系统架构模型的安全性分析工具。由于传统安全性分析方法存在严重依赖工程师对系统的理解程度，更新效率低下以及数据不一致等问题，本文提出：安全性分析数据应与设计模型数据保持一致，故障树建模和分析工作自动完成。基于航电系统架构模型的安全性分析工具并基于模型驱动的思想，通过向系统建模语言（System Modeling Language，SysML）描述的航电系统架构模型添加安全性属性来扩展此模型，从而自动生成故障树并进行共模分析和区域安全性分析。该工具的开发统一了系统设计和故障树分析过程，使得对系统模型进行一键分析成为可能。最后利用所开发的工具针对某飞机驾驶舱显示系统架构模型自动生成故障树进行安全性分析，并将此故障树与传统手工方法构建的故障树进行了比对，验证了所开发的工具的有效性。

2 航电系统架构模型

在航电系统架构设计过程中，通常从逻辑架构和物理架构两个角度描述和设计航电系统架构。

2.1 航电系统逻辑架构模型

逻辑架构模型规定了系统由哪些逻辑元素组成，以及这些逻辑元素之间的数据流和流向关系。图 1 为某采用 IMA 架构[7,8]的飞机驾驶舱显示系统所对应的逻辑架构图。图中驻留在通用处理模块（General Process Module，GPM）上的显示系统产生用于显示的源数据，其经过交换机（Switch）进行网络传输，送至显示单元设备（Head Down Display，HDD）。其中，交换机网络采用 A、B 通道进行传输备份。航电系统逻辑架构模型支持生成接口控制文档（Interface Control Document，ICD）。ICD 定义和描述了组成航空电子系统的各分子系统和电子设备之间接口信号的组成、功能、技术特性及使用说明[9]，它的设计是航空电子系统设计的重要组成部分。

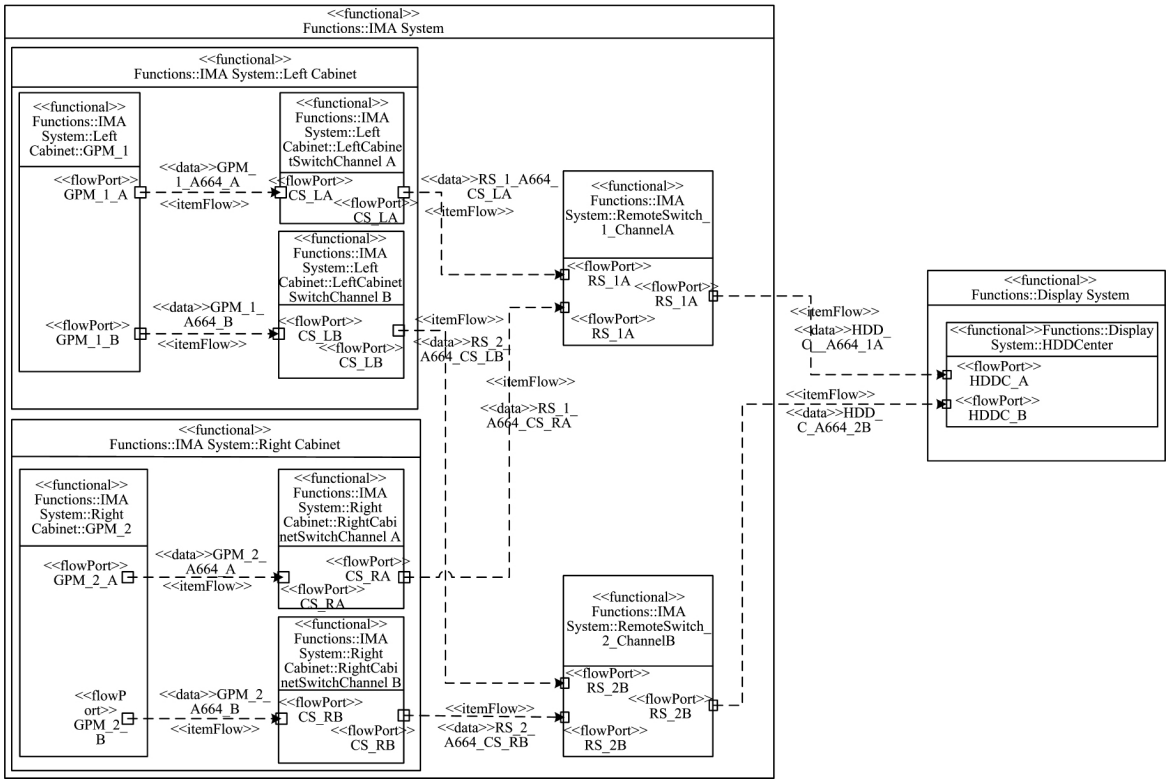


图 1 某飞机驾驶舱显示系统逻辑架构图

2.2 航电系统物理架构模型

物理架构模型规定了组成系统的物理元素、这些物理元素之间的关系以及它们的部署策略。图 2 为上述飞机驾驶舱显示系统所对应的物理架构图。由于物理架构清晰地定义了底层硬件以及硬件之间的实际交联关系，因此我们主要基于航电系统物理架构进行安全性分析，以快速有效地找到故障发生的根本原因。在工程实践中，Enterprise Architect（EA）以其对 SysML 系统工程建模的有力支持而被用作航电系统架构的建模环境。因此，本文对面向 EA 环境中建立的航电系统物理架构模型进行安全性分析。

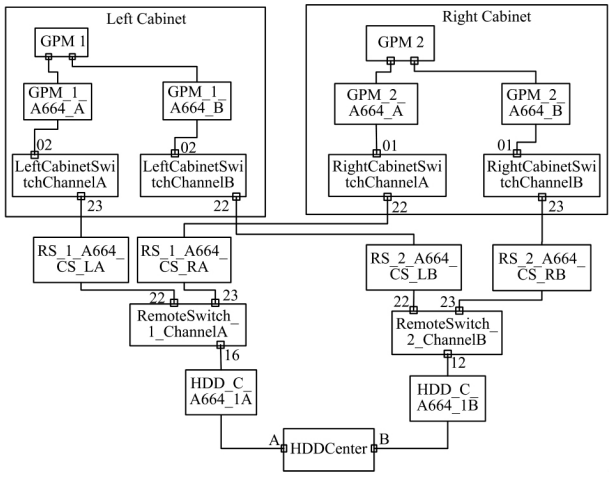


图 2　某飞机驾驶舱显示系统物理架构图

3　基于航电系统架构模型的安全性分析

为了避免单点失效，冗余设计方案在航电系统中得到了普遍的应用。然而，冗余设计的独立性经常被交联复杂的依赖关系破坏，而本文采用数据信号路径追溯方法自动完成的故障树建模是在假设故障独立的前提下进行的，因此对该架构的安全性分析除了需要对故障树进行基本的定性和定量分析外，还需要对其进行共模分析和区域安全性分析。

3.1　故障树定性分析[10]

为了找出导致顶事件发生的所有可能的故障模式，以便改进设计或指导故障诊断，需要对故障树进行定性分析。一般来说，定性分析的方法是寻找故障树的最小割集。

假设故障树中有 n 个底事件 $X_1, X_2, \cdots, X_n$，C 为某些底事件的集合，当其中全部底事件都发生时，顶事件才发生，则称 C 为故障树的一个割集。若 C 是一个割集，而任意去掉其中一个底事件后就不是割集了，这样的割集被称为最小割集。

对于故障树的最小割集的求解，通常采用下行法。即根据故障树的实际结构，从顶事件开始，顺次将逻辑门的输出事件置换成输入事件。遇到与门就将其输入事件排在同一行，遇到或门就将其输入事件各自排成一行，直到全部换成底事件为止，即可求得全部割集。再应用集合运算规则将它们简化，可得到故障树的全部最小割集。

3.2　故障树定量分析[10]

定量分析主要是通过系统各单元（底事件）的失效概率求出系统的失效概率。利用最小割集可以求出顶事件发生的概率。假设故障树有 n 个最小割集 $K_i(1\leqslant i\leqslant n)$，系统故障事件表示为

$$T=K_1+K_2+\cdots+K_n \tag{1}$$

其中，每个最小割集 K_i 是底事件 $X_i(1\leqslant i\leqslant m, m$ 为底事件数目）的积事件，即

$$K_i=\bigcap_{i\in K} x_i \tag{2}$$

则顶事件发生概率

$$\begin{aligned}P(T)&=P(K_1+K_2+\cdots K_n)\\&=P(\bigcup_{j=1}^{n}K_j)\\&=\sum_{i=1}^{n}P(K_i)-\sum_{i<j=2}^{n}P(K_iK_j)+\sum_{i<j<k=3}^{n}P(K_iK_jK_k)+\\&\quad\cdots+(-1)^{n-1}P(K_1K_2K_3\cdots K_n)\end{aligned} \tag{3}$$

3.3　共模分析

依据 ARP4761，CMA 过程基于分析设计以及可能破坏该设计内功能冗余度或独立性的元件实施。通过应用检查单来进行本分析。凡要求的冗余度或独立性遭到破坏时，则要求证明对该损害的可接受性或消除这种损害。共模分析的过程可综述如下[11]：

1）建立特定检查单大纲。本文依据 ARP4761 中通用共模类型、来源和失效/差错检查单的示例，建立检查单，包括原理和设计、制造、安装/综合和试验、使用、维修、试验、校准、环境 8 项。

2）确定 CMA 要求。由于冗余设计在故障树中通过“与”门来体现，因此对于来自 FTA 的 CMA 要求，应识别故障树中的每一“与”门事件，以确保哪种失效组合是独立的。只有冗余系统/组件同时发生故障，系统才有可能发生故障，因此，冗余系统/组件必定在同一割集中。本文针对“与”门事件的每一最小割集中的所有基本事件进行分析，以验证最小割集中是否存在共模故障，从而导致系统独立性遭到破坏。

3）对步骤 2）中指定的检查项对照检查单进行检查。本文为每个检查项提供了 N/A、有待分析、已派生设计改进需求和明显功能原理/项目开发独立 4 个选择，用户可根据实际情况选择或进行详细说明。

3.4　区域安全性分析

从历史上看，仅在系统原理简图的基础上进行系统安全性分析并不能充分认识可能大大削弱组件之间独立性的系统硬件物理安装的关系。因此，定义区域性安全性分析这种分析方法，使其考虑到飞机上各个系统/组件的安装关系以及机上安装非常邻近的各系统/组件之间的相互干扰。本文将对冗余系统/组件的区域安全性分析分为两方面内容。一方面，冗余系统/组件之间应该物理隔离或满足一定的物理隔离要求；另一方面，通过定义危险区域列表，要求冗余系统/组件不能处于同一个危险区域，以降低备份设备之间被区域内相同的危险因子影响的概率。故障树中基本事件的区域属性即其所对应的系统/组件所处区域。

3.4.1　系统/组件隔离检查

系统/组件隔离检查指检查冗余系统/组件之间是否满足给定的物理隔离要求。用户输入最小隔离距离，本文在比较“与”门事件的所有最小割集的基本事件对之间的实际距离与最小隔离距离后，输出基本事件对之间的距离以及该距离是否满足隔离距离的要求，从而得出系统/组件之间的隔离性需求。这里采用“保守距离”来估算实际距离，隔离距离检查过程如图 3 所示。假设所有的系统/组件的形状均为正方体，两个正方体的中心和边长分别为 (x_1, y_1, z_1)、(x_2, y_2, z_2)、r_1、r_2，则“保守距离”

$$d=\sqrt{(x_1-x_2)^2+(y_1-y_2)^2+(z_1-z_2)^2}-\sqrt{3}r_1/2-\sqrt{3}r_2/2 \tag{4}$$

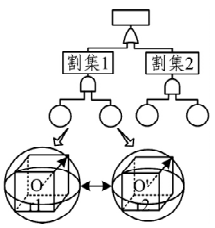


图 3　系统/组件隔离检查过程

3.4.2 危险区域隔离检查

危险区域隔离检查指检查冗余系统/组件是否处于同一个危险区域。危险区域隔离检查要求用户输入危险区域列表，并且危险区域之间必须相互隔离。在计算“与”门事件的所有最小割集的基本事件与所有危险区域的实际距离后，输出该系统/组件是否满足危险区域隔离要求，从而得出系统/组件与危险区域之间的隔离性需求。这里同样采用“保守距离”来估算实际距离，危险区域隔离检查过程如图 4 所示。

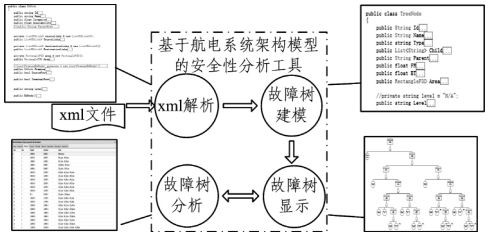


图 4 危险区域隔离检查过程

4 基于航电系统架构模型的安全性分析工具

本文开发了一种基于航电系统架构模型的安全性分析工具，开发环境为 Visual Studio 2010。为了统一表示系统设计与安全性分析数据，故构建故障模型，并基于表示这两种模型的数据结构文件自动生成故障树并对其进行分析，其功能架构如图 5 所示。基于航电系统架构模型的安全性分析工具以从 EA 环境导出的 xml 文件作为输入，主要包括 xml 解析、故障树建模、故障树显示和故障树分析 4 个功能模块，能通过屏幕和文件两种形式输出生成的故障树和安全性分析结果。

本工具首先基于物理架构模型和故障模型自动生成故障树，这个过程就是将这两个模型转化为故障树图形化结构的过程。在 EA 环境中，我们通常采用模块图来定义航电系统物理架构，利用“Block”元素来表示系统/设备，“Port”元素表示硬件设备的端口，而连接关系则通过 EA 提供的“模块元素关系”来表示。由此，航电系统架构模型中的元素被转化为模块和连接两类。

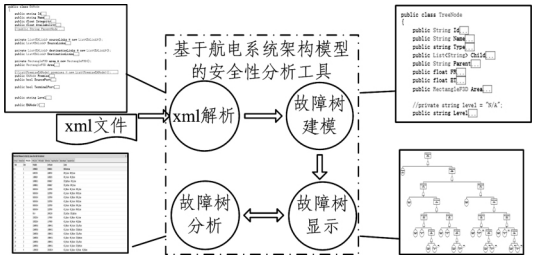
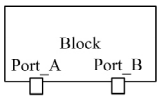
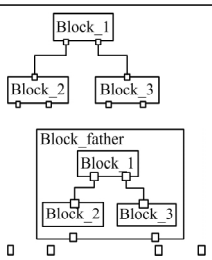


图 5 基于航电系统架构模型的安全性分析工具功能架构图

物理架构模型到故障树图形化结构的转化过程如表 1 所列。其中，Level 属性表示了该模块所对应的系统/设备处于哪一层级。本文将航电系统物理架构中的模块分为外场可更换单元（Line Replaceable Unit，LRU）和外场可更换模块（Line Replaceable Module，LRM）两种层级。LRU 具有实现某种功能的能力，是完成这种特定功能的软硬件综合独立体。它拥有标准的形式、功能、外观尺寸和安装接口。LRM 驻留在 LRU 中，不存在外观尺寸属性。由于区域安全性检查是对实际物理设备所处区域是否满足隔离要求进行检查，所以只对 LRU 模块进行。

表 1 物理架构模型和故障模型到故障树图形化结构的转化过程

SysML 模型 （xml 文件）	Xml 解析 （EANode 类）	故障树建模 （TreeNode 类）	故障树显示 （BasicNode，BasicLink 类…）
模块 	Id：唯一的标识符 Name：名称 Integrity：完整性 Availability：可用性 Level：LRU，LRM Area：所处区域 ……	Id：唯一的标识符 Type：类型 Name：名称 Integrity：完整性 Availability：可用性 Level：LRU，LRM Area：所处区域 ……	Id：唯一的标识符 Name：名称 Integrity：完整性 Availability：可用性 Level：LRU，LRM Area：所处区域 其他外观属性： Shape：形状 Size：大小 …… 其他计算属性： Probability：概率 ……
关系 	Parent：源链接 Child：目标链接 Premise：所驻留的模块	Parent：源链接 Child：目标链接	SourceLinks：源链接 DestinationLinks：目标链接

4.1 故障模型构建

在解析 xml 文件之前，首先需要构建故障模型。故障模型包含失效模式和失效率两方面内容。在 EA 环境中，TaggedValue 类能很方便地描述这个模型。TaggedValue 类主要包含 name 和 value 两个成员，分别对应故障模型中的失效模式和失效概率。

构建故障模型后，需要将系统设计与安全性分析数据导出到 xml 文件中。EA 工具提供了这项功能，可方便地进行这项操作。

4.2 xml 文件解析

解析 xml 文件的过程就是将 xml 文件中的信息转化为 EANode 列表的过程。本过程采用用于 XML 的语言集成查询（Linq to XML）技术，依据 xml 元素的不同类型提取所需信息，并将其存储到 EANode 列表中，完成 xml 文件解析的过程。

4.3 故障树建模

故障树建模的过程就是将 EANode 列表转化为 TreeNode 列表的过程。在故障树建模时，首先需要进行故障注入。

故障注入即将故障模型注入到物理架构模型中。物理架构模型定义了模块和模块间的转移关系，故障模型则定义了与该模块相关的安全性分析数据，故障注入的过程就是基于这两个模型，确定元素的故障模式、故障概率以及故障转移方式的过程。本文采用的是数据信号路径追溯的故障树建模方法，即从终端对象的故障模式开始，根据数据传播的路径逆推出可能造成这种故障的原因，由此完成故障注入的过程。故障树建模的基本单元可以描述为：对于某模块，其功能故障的原因必为其本身故障或数据流输入故障。根据模块间的数据流流向、驻留关系以及模块的故障模式，对此故障树基本单元进行适应性修改和扩展后即可完成故障树建模。

4.4 故障树显示

故障树显示模块主要实现 3 项功能：1）依据来自故障树建模的故障树数据，图形化呈现故障树；2）提供用户接口，支持对故障树进行人工修改和编辑；3）提供用户控制界面，实现故障树定量计算、计算数据输出等控制操作。本功能模块所用到的类库主要为 Northwoods. go. diagram，故障树呈现的数据结构主要继承于该类库，并添加了一些属性和行为来定制故障树的呈现形式。对故障树的编辑则主要通过调用、重写或重载上述类库中的函数来完成。通过读取故障树分析模块的分析结果，并将其绑定在界面上，即可完成计算结果输出功能。

4.5 故障树分析

本功能模块主要用于实现故障树的定量计算，并进行共模分析和区域安全性分析。通过对开源故障树分析工具 XFTA 计算算法的深度优先调用，获得故障树的各中间事件概率值和最小割集。XFTA 采取符合 OPENPSA 标准的 xml 文件为输入，提供 XFTA. dll 以及接口函数供用户调用。因此，在对故障树进行计算之前，先将故障树文件转化为符合 OPENPSA 标准的 xml 文件。实现故障树的定量计算后，针对“与”门事件的最小割集进行共模分析和区域安全性分析。

5 案例分析

为了验证所开发的基于航电系统架构模型的安全性分析工具的有效性，现对如图 2 所示的某飞机座舱显示系统，利用上述工具进行故障树自动建模和分析。

5.1 故障模型构建

对图 2 所示的某飞机座舱显示系统物理架构模型中的每个模块建立相应的故障模型，即对每个模块建立相应的 taggedValue，定义该模块的失效模式和失效概率。模块 HDDCenter 对应的故障模型如图 6 所示。其中，LossOfFunction 定义了丧失类及丧失概率，StationLine，WaterLine，ButtockLine 和 VolumeBudgeted 定义了该模块所处位置和体积。

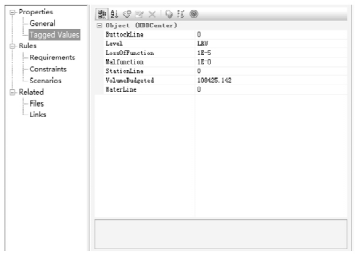


图 6 模块 HDDCenter 对应的故障模型

5.2 故障树建模

基于 EA 环境中导出的 xml 文件，采用数据信号路径追溯的方法完成故障树建模，生成的故障树如图 7 所示。顶事件为 HDDCenterOutputLoss，表示显示系统输出丧失，它连接的或门连接了 HDDCenterLoss 和 HDDCenterInputLoss 两个事件，分别表示 HDDCenter 丧失和 HDDCenter 的输入丧失，以此类推。其中，LeftCabinet 和 RightCabinet 的丧失会导致驻留在其中的所有设备/子系统发生丧失，因此故障树中会出现重复事件，以 repeat 标注。

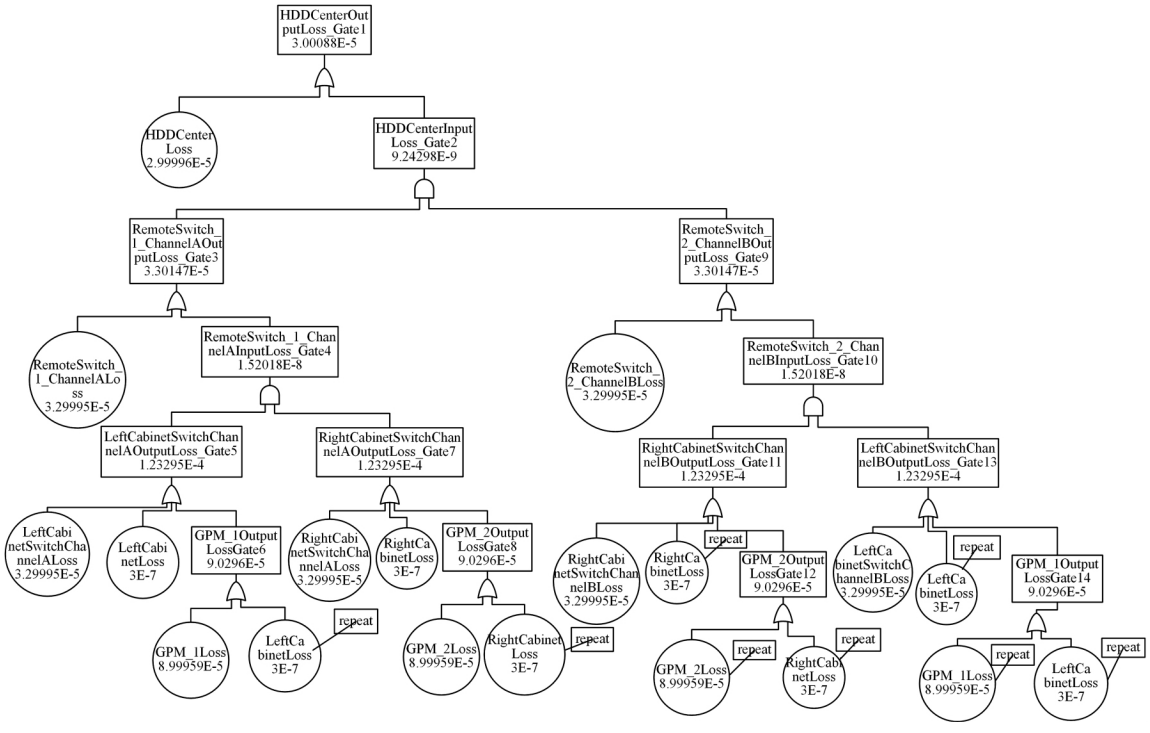


图 7 丧失类故障树

5.3 故障树分析

首先调用 XFTA 提供的接口函数对此故障树进行计算，对应每一个中间事件分别生成最小割集文件和顶事件概率文件。该工具对应每一个中间事件读取这两个文件，并将概率

显示在故障树中，将最小割集显示在表中。HDDCenterOutputLoss_Gate1 对应的最小割集如图 8 所示。传统手工建树结果与图 7 类似，然而其高度依赖于工程经验，耗时耗力。本工具则能针对架构模型自动生成故障树，故障树与架构模型相对应，确保了在此基础上进行安全性分析的结果的完整性。因此，无论是从用时长短还是有效性上，该工具都明显优于传统手工建树方法。

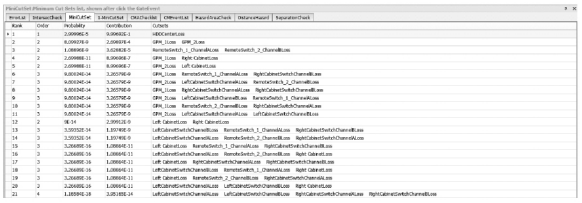


图 8　HDDCenterOutputLoss_Gate1 对应的最小割集

5.3.1　共模分析

对故障树中所有的“与”门事件进行共模分析，依据 ARP4761 列出检查清单，结果如图 9 所示。

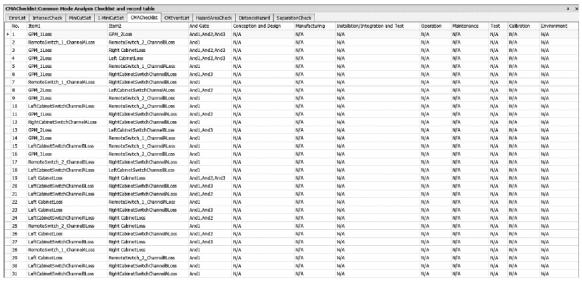


图 9　共模检查结果

5.3.2　区域安全性分析

输入最小隔离距离为 10m，系统/组件隔离检查结果如图 10 所示。由于本例将所有模块的位置均设为 0，因此所有的模块均相交，不符合最小隔离需求。由此得出系统/组件之间的隔离性需求为表中的系统/组件对之间的距离均大于 10m。

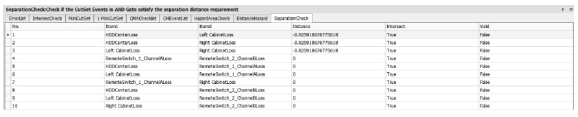


图 10　系统/组件隔离检查结果

以两个极端大小的危险区域为例。输入危险区域为位于(0,0,0)处的边长为 10000 米的立方体，危险区域检查结果如图 11 所示。

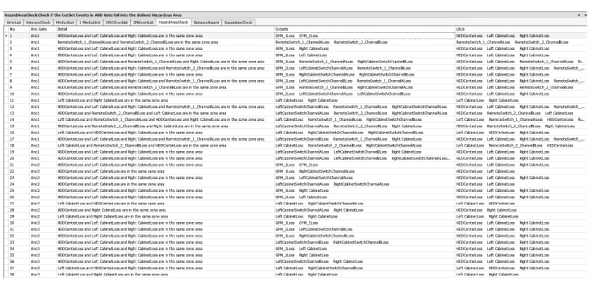


图 11　危险区域隔离检查结果

由于危险区域很大，因此所有的模块均落在这个区域内。修改危险区域为位于(10,0,0)处的边长为 0 的立方体，危险区域检查结果列表为空。这是由于危险区域位置与模块的位置不同且体积为 0，因此所有的模块均不在这个区域内。

结束语　本文首先介绍了基于航电系统架构模型的安全性分析方法(主要包括故障树的定性、定量分析)，以及所提出的基于最小割集的共模分析和区域安全性分析方法；随后对所开发工具的的功能模块进行了介绍；最后利用某飞机座舱显示系统的案例说明了该工具的有效性。该工具在建立航电系统架构模型的同时建立故障模型，使得系统设计能够明确展示其安全性属性，能够完成故障树的自动建模和分析，大大简化了人工建立和更新故障树的繁琐步骤，降低了出错的概率。最后，共模分析和区域性安全分析能够对航电系统中的冗余设计方案提供有力保证。因此，基于航电系统架构模型的安全性分析工具是有效的，为航电系统的故障树自动建模分析问题提供了一种新的、更高效的解决方案。本文考虑了失效和错误两种失效状态，没有考虑到具体的失效模式，下一步工作将把每个设备/组件的失效模式和影响纳入考虑，构建能够描述详细失效模式的故障树并对其进行分析。

参 考 文 献

[1] Wang G. Integration technology for avionics system[C]// 2012 IEEE/AIAA 31st Digital Avionics Systems Conference (DASC). IEEE, 2012: 7C6-1-7C6-9

[2] Moir I, Seabridge A G, Jukes M. Military avionics systems[M]. John Wiley & Sons Inc, 2006

[3] 许文平. 综合化航空电子资源融合机制研究[D]. 南京：南京航空航天大学, 2012

[4] Ruijters E, Stoelinga M. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools[J]. Computer Science Review, 2015, 15: 29-62

[5] Moir I, Seabridge A, Jukes M. Civil avionics systems[M]. John Wiley & Sons, 2013

[6] 谷青范，王国庆，张丽花，等. 基于模型驱动的航电系统安全性分析技术研究[J]. 计算机科学, 2015, 42(3): 124-127

[7] Schenkelberg R H. Low cost integrated modular avionics (IMA) [C]// Proceedings of the IEEE 1996 National Aerospace and Electronics Conference, 1996 (NAECON 1996). IEEE, 1996, 1: 48-55

[8] RTCA (Firme). Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations[M]. RTCA, 2005

[9] 杨洋，严俊，谷青范. 航空电子系统接口控制文档工具的设计与实现[J]. 航空电子技术, 2014(1): 24-29

[10] Vesely W E, Goldberg F F, Roberts N H, et al. Fault tree handbook[R]. Nuclear Regulatory Commission. Washington DC, 1981

[11] Society of Automotive Engineers, ARP-4761: Aerospace Recommended Practice: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, 12th edition[R]. SAE, 400 Commonwealth Drive Warrendale PA United States, 1996