基于模型驱动的航电系统安全性分析技术研究

谷青范[1] 王国庆[1,2] 张丽花[1,2] 翟 鸣[1]

(中国航空无线电电子研究所 上海 200233)[1] (西北工业大学计算机学院 西安 710072)[2]

摘 要 针对综合化航空电子系统安全性分析存在的失效模式完备性和动态失效问题以及数据一致性问题,将航电系统分为3个层次:应用操作层、功能层和资源层,采用形式化方法分别对每个层次进行建模,利用模型转换技术实现3个层次之间的语义转换,确保语义的一致性。利用Event-B语言对系统应用操作和功能层建模,实现对应用操作模式完备性的检查,利用AltaRica语言能够对系统的异常行为建模,实现对系统动态失效问题的分析。以飞机自动飞行控制系统为例,利用Event-B建模工具Rodin实现对应用操作模式的分析,借助基于AltaRica语言的SimFia工具对其安全性进行分析,结果验证了所提方法的有效性和实用性。

关键词 模型驱动方法,航空电子系统,安全性分析

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.3.025

Research on Model Based Safety Analysis Technology for Avionics System

GU Qing-fan[1] WANG Guo-qing[1,2] ZHANG Li-hua[1,2] ZHAI Ming[1]

(China National Aeronautical Radio Electronics Research Institute, Shanghai 200233, China)[1]

(School of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an 710072, China)[2]

Abstract This paper introduced a new model based method for safety analysis to address the problem of failure modes integrity, dynamic failure and data consistency currently encountered in safety assessments for integrated avionics system. The method models integrated avionics system hierarchically with layers of application operation, function and resource. It simplifies a large part of the analysis, the development of fault trees, and can guarantee the consistency of results. Event-B language is used to model application layer to check the integrity of operations modes and AltaRica is used to model dysfunction of system to solve the problem of dynamic failure. The efficiency and practice of the method are illustrated by analyzing safety of auto pilot system through Rodin tool which is used for analyzing operational modes of application and Simfia tool which is used for safety analysis.

Keywords Model based method, Avionics system, Safety analysis

1 引言

综合化航空电子系统的综合体现在系统资源、功能综合和任务合成3个方面,资源综合的对象主要是具有并发、共享特性的部件(硬件、软件),即多道资源。多道资源综合指的是能够通过时分多路、空分多路等方式来实现资源的共享和重用,从而减少资源配置,提高资源的效能。资源综合的表现形式有物理空间综合(共享相同位置)、电气综合(共享电源)、逻辑综合(共享地址空间)等。资源综合的主要特征是基于模块化的功能设计,随着硬件计算能力的提高,越来越多的功能通过嵌入式软件来实现,使得相同的硬件平台能够加载多重功能模块,如显示处理功能、飞行管理数据处理功能。功能综合的主要特征是利用不同子系统/功能之间的动态协作(信息共享/控制信号交换)提高系统执行任务(应用)的能力,降低机组人员的工作负载,例如通过将导航功能和飞行控制功能综合后形成自动驾驶功能,通过将无线电高度表、GPS、惯性导航(INS)的信息进行融合,能够获得更精确的飞机位置信息。功能综合的同时,又需要增加一部分功能(如信息融合)来利用综合的收益。随着综合化程度增加,飞行员的工作角色从飞行管理者向任务管理者转变,而随着飞行操作需求的增加,为了提高任务执行能力,需要将一些任务通过自动控制系统来执行。任务合成就是基于当前系统能力状态和探测到的外部环境参数完成一部分决策的自动化,从而减轻飞行员的工作负荷。综合化在带来上述收益的同时,也增加了系统复杂性,如功能交联、软件与硬件交互、系统与飞行员交互增加,使得系统故障在综合、融合和合成过程中的蔓延、混沌和不确定性对系统安全性产生很大的影响。传统的安全性分析方法(如FTA、FMEA)主要依赖于工程经验,并且与系统设计不是同步进行的,随着系统复杂程度的提高,很难列举出系统所有的失效模式和影响,同时由于系统设计的迭代,很难保证失

到稿日期:2014-04-23 返修日期:2014-08-01 本文受航空基金(20125552053),国家重点基础研究计划(973)(2014CB744900)资助。

谷青范(1974—),男,博士,副教授,主要研究方向为系统安全性、计算机理论、航空电子技术,E-mail:gu_qingfan@careri.com;王国庆(1956—),男,博士,教授,博士生导师,主要研究方向为航空电子技术、复杂系统、计算机技术等;张丽花(1981—),女,博士生,主要研究方向为航空电子技术、安全性分析、数据挖掘等;翟 鸣(1979—),男,博士,主要研究方向为人机功效、飞行管理设计、数据融合等。

效模式同系统架构的一致性。针对上述问题，考虑到安全性是航电系统的一个基本属性，提出将系统设计过程与安全性分析过程集成，在模型层上确保数据描述的一致性，并利用分层建模的方法实现对综合化航空电子系统的安全性分析。

2 基于模型驱动的安全性分析方法

SAE ARP4754A 阐述了航空系统开发的全生命周期过程，ARP4761[1]描述了在飞机级与系统级进行安全性评估的过程。在最初阶段，依据飞机级初步危害性评估的数据，开始进行系统级的功能危害性评估；在项目联合设计阶段，飞机级的功能失效状态信息可能非常有限，这就需要使用历史数据和工程经验进行初始的系统级安全性评估，其结果反馈给客户再进行新一轮的飞机级的安全性评估。

系统安全性评估是一个随着系统设计的推进需要不断更新的迭代过程，上一次安全性评估的结果作为安全性需求输入给系统设计过程，系统设计可能依据这些需求进行变更，当确认已完成的设计满足所有确定的安全性需求时，安全性评估过程结束，如图 1 所示。

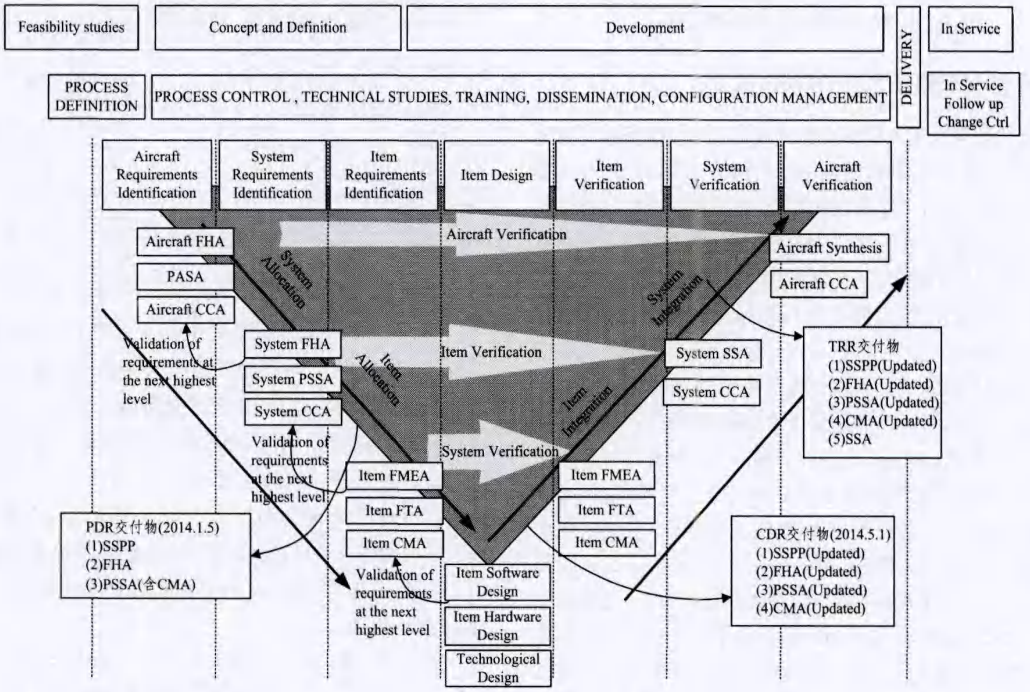

图 1 航空系统设计与安全性分析过程(引用自 ARP4754A Figure 5)

在上述安全性评估过程中，系统功能危害分析(FHA)主要是基于工程经验的方法来判断系统功能失效对飞机、机组成员和飞机的影响，初步系统安全性分析(PSSA)从完整性角度来分析功能失效模式和状态影响。由于 PSSA 是建立在对系统架构设计理解的基础上的，一方面需要考虑资源综合引起的共模分析(CMA)，另一方面还需要考虑功能综合引起的功能交互行为的安全性(如故障传播)。现有的安全性分析方法主要存在以下几种问题：

(1)依赖工程经验和对系统的理解，对于复杂的综合化系统难以满足完备性要求。

(2)仅能分析单个失效的影响分析。

(3)仅从构成、逻辑路径分析，无法评估动态失效的影响。

(4)复杂系统的共模分析难以实现(independency，Fail Safe)。

其根本原因在于系统设计与安全性分析数据不能统一表示，使得系统设计不能展示其安全性属性，安全性分析结果不能直接反馈到系统设计模型中。

针对上述问题，需要对系统设计和安全性分析采用一致的形式化模型，并扩展现有的系统设计/分析工具，使其支持基于接口的失效模式生成，自动产生功能失效影响要素，即基于模型驱动的安全性分析方法(MBSA，见图 2)[2]。

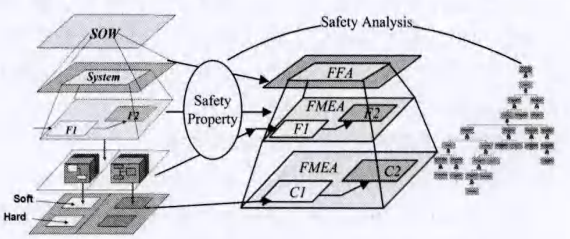

图 2 基于模型驱动的安全性分析方法(MBSA)

MBSA 方法可以支持两种主要情况：一种是设计人员在一定的抽象层次上进行系统功能的形式化建模(如 UML-B)，在此模型基础上，安全性分析人员通过形式化验证方式增加系统安全性属性；另外一种情况是在开始阶段，系统设计模型还没有形成，首先进行架构的安全性评估，需要安全性分析人员利用组件构建顶层模型，利用组件的失效模式自动合成系统的失效模式和生成影响要素(安全属性)。MBSA 方法的执行流程描述如图 3 所示[7]。

其中，组件库为设计模式，可以直接应用于系统建模中，规则库是基于组件的形式化安全性属性，能够被建模工具直接使用，并将其作为行为属性添加到系统设计模型中。从图 3 可以看出，系统设计工程师和安全性工程师通过形式化模型实现二者在语义上的一致。

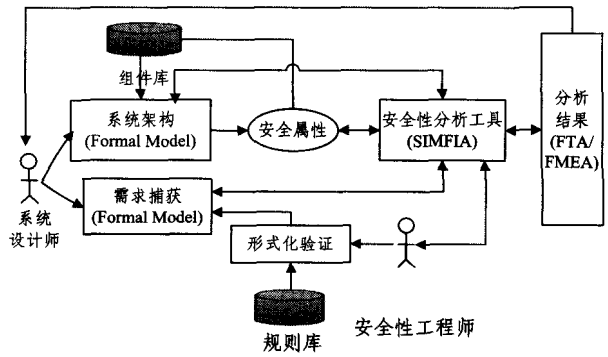

图 3　基于模型驱动的安全性分析流程

3　综合化航空电子系统 MBSA 实现

综合化航空电子系统安全性分析的目标是确保系统功能执行能够"正确无误"地满足应用操作需求。考虑到综合化分为任务、功能和资源 3 个层次的综合，在进行安全性分析时关键是确保资源能够"正确无误"地支持功能层的需求，而功能综合层具有确定的能够"正确无误"执行任务层的操作需求，从系统工程角度来看，也就是要求系统实现、设计和需求保持一致性和完整性。目前基于 UML/SysML 的系统设计建模方法已成为实际的工业标准，而安全性建模方法如 FTA、Markov 链、随机 Petri 网属于低级建模语言，对于系统设计来说，一方面比较难以理解，另一方面难以实现完整建模和数据维护。进一步地考虑到复杂航电系统的开发过程(包括安全性分析过程)是一个迭代的过程，我们采用 Event-B 形式化语言对系统设计进行建模，采用 AltaRica 语言进行安全性描述，其中 Event-B 既能够支持逐步迭代的设计方法，又能够和 UML/SysML 相结合(如 UML-B)，而 AltaRica 语言能够支持分层的安全性分析。利用 AltaRica[4] 模型能够生成导致功能故障的失效事件序列，这样就可以实现从资源层到操作层的故障传播分析，并且已在空客和波音公司得到了应用(Cecilia OCAS 工具对 Falcon 7X 的飞控系统进行安全性建模分析)。下面用 AltaRica[4,6] 和 Event-B[8] 语言来对综合化航空电子系统的 3 个层次进行建模[10]。

3.1　形式化建模语言 AltaRica 和 Event-B

AltaRica 语言是由 LaBRI (Laboratoire Bordelais de Recherche en Informatique)开发的用于实现对系统功能和异常行为的建模，每个系统功能组件由一个 Node 表示，每个 Node 的定义包含 3 个部分。

第一个部分是对 Node 参数的不同类别进行定义，包括 state，flow 和 event，其中 state 表示当前功能节点状态(失效或正常)的内部变量；flow 表示节点的输入/输出，state 和 flow 的数据类型可以是 integer，enumeration 和 boolean；event是引起 Node 由一个内部状态变迁到另一个内部状态的事件，利用 event 可以对飞行员行为或失效发生以及对某个输入条件的确定性响应行为进行建模。

第二个部分描述自动变迁，首先利用 init 定义初始状态的值，变迁可以用一个三元组 $g \xrightarrow{evt} e$ 进行表示，其中 g 是变迁发生的门限条件，evt 是事件名称，e 是变迁的结果，其中门限是关于 state 和 flow 的布尔逻辑算子，它定义了事件 evt 发生的条件。事件发生的结果 e 是关于状态变量的值列表。因此，变迁部分描述了功能或失效状态是如何传播的。最后，可以通过向事件添加发生的概率规则，实现对事件发生概率特征的刻画。需要注意的是 Dirac(X)概率规则建模的是在 X 时间单位内对于输入条件的确定性响应，因此由 Dirac(0)用于建模立即发生的事件，只要引起变迁发生的条件满足，就即刻引起变迁的发生。

第三个部分是断言集合，断言是一个原子等式或由多个 case 构造而成的结构化等式。断言建立了组件 state 和 flow 之间的固有关系，描述了组件的输出如何由其输入和当前的功能模式所确定。在 SimFia 工具中，一个组件或节点用一个块图(block)表示，并且一个 block 可以嵌套另外一个 block，每个 block 有输入、输出接口(分别用◦和 • 表示，见图 4)。

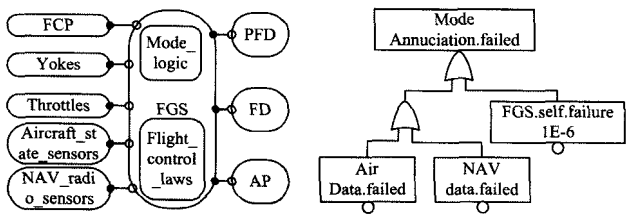

图 4　基于 AltaRica 的 FGS 安全性模型与故障树

Event-B 扩展了 B 形式化方法[9,11]，用于实现对复杂系统的设计，它是基于经典逻辑[12]和集合理论利用证据的方法来对系统的属性进行验证，比较适合应用于机载系统安全性架构的验证。根据 Event-B，每个不连续转换系统可以通过两种组件进行建模：machine 和 context 组件。一个 context 组件包含所有常量、集合和与这些常量、集合有关的公理，其刻画了系统的静态特征；相反，machine 组件表示系统的行为或动态方面，其随着 context 的增加而不断进行扩展，一个 machine 组件包括：

variables 或 state variables：具有相应的类型(enumerated，integer 或 free sets)，在使用前需要初始化；

invariants：与 state variables 相关联，表示其必须满足的约束条件或属性；

events：表示与系统有关的操作或变迁，通常一个事件包含一个"guard"(门限，表示事件发生的条件)和"action" 部分(可以是确定或非确定，表示事件发生的结果或影响)。

3.2　应用操作层建模

综合化航空电子系统应用操作层体现的是系统与外部环境的交互，即飞行员根据指令或所处环境选择执行相应的操作(任务)，应用操作层模型包含系统状态(用 machine 组件表示)、外部环境条件(含人为因素，用 context 组件表示)，基于 Event-B 构建应用操作模式与任务合成模式。下面以飞机自动飞行控制系统(AFCS)的应用为例进行说明[3](见图 5)，飞行员根据外部环境(如飞行高度超过 400 英尺才能使用自动驾驶仪)和飞行阶段选择人工驾驶(MP)或自动驾驶(AP)，其中 MP 进一步分解为接收飞行员指令，并产生作动器动作，AP 是执行自动驾驶功能，需要进一步从通信、导航系统获取精确的飞机姿态、位置信息，飞机控制模型计算，并产生精确的控制指令，这就要求 AFCS 采用分层的逻辑控制架构，并根据外部环境与自动驾驶系统的交互定义系统边界。根据 SAE ARP4761，对于 AFCS 的安全性分析需要考虑从飞机发动、起飞到降落的整个过程的功能危害及失效条件，首先需要在应用操作层考虑操作模式的失效对系统的影响分析。

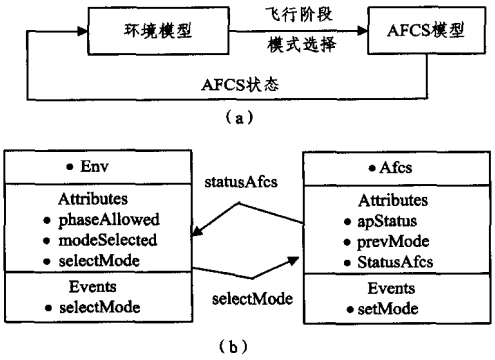

图 5　自动飞行控制系统应用操作示例

将 AFCS 中的模式转换用 Event-B 中的 event 表示，利用 Event-B 建模工具 Rodin 将其操作模式建模如下：

```
MACHINE
    MComp 〉
VARIABLES
    phaseAllowed Physical Unit:Inferred Physical Unit:〉
    modeSelected Physical Unit:Inferred Physical Unit:〉
    prevMode Physical Unit:Inferred Physical Unit:〉
    statusAfcs Physical Unit:Inferred Physical Unit:〉
INVARIANTS
    inv1:phaseAllowed ∈ BOOL theorem 〉
    inv2:statusAfcs ∈ BOOL theorem 〉
    inv3:modeSelected ∈N not theorem 〉
    inv4:prevMode ∈ N not theorem 〉
    inv5:(prevMode ≠ modeSelected) ∨ (prevMode=2 ∧ modeSe-
        lected=0) not theorem 〉
    inv6:phaseAllowed=TRUE⇒statusAfcs=TRUE not theorem 〉
  EVENTS
    INITIALISATION: not extended ordinary〉
    END
    selectMode: not extended ordinary standard〉
    ANY
        selectVal 〉
    WHERE
        grd1:MComp=env not theorem 〉
        grd2:phaseAllowed=TRUE not theorem 〉
        grd3:modeSelected=0 not theorem 〉
        grd4:preMode=0 not theorem 〉
    THEN
        act1:MComp := afcs 〉
        act2:modeSelected :=selectVal 〉
    END
    setMode:not extended ordinary standard〉
    ANY
        setVal〉
    WHERE
        grd1:MComp=afcs not theorem 〉
        grd2:preMode ≠ modeSelected theorem 〉
        grd3:phaseAllowed=FALSE not theorem 〉
    THEN
        act1:Mcomp := env 〉
        act2:statusAfcs := FALSE 〉
        act3:modeSelected := setVal 〉
        act4:preMode := modeSelected 〉
      END
END
```

其中 inv5 定义了 AFCS 模式转换处理逻辑，而 inv6 描述了理想情况。通过上述建模方式，可以枚举出所有飞行员操作模式，通过定义 INVARIANTS 属性描述操作限制，通过 Proof Obligations 来进行模型验证约束条件是否满足和一致。操作模式分析的结果作为设计约束传递到 AFCS 的实现上，接下来就可以独立地对 AFCS 进行功能层的建模。

3.3　功能层建模

Event-B 支持 refine 的方式对系统进行迭代设计，利用状态图实现对功能内部建模，通过接口实现功能之间交互的建模，对于正常交互行为的建模这里不再赘述，对于异常交互的行为我们可以利用 AltaRica 进行建模。图 6 是 AFCS 中 FGS 的功能架构与利用 SimFia 对其安全性建立的模型。

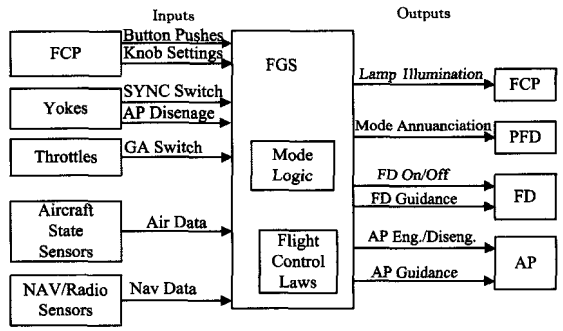

图 6　FGS 功能架构

对分解后的每个分系统进行功能建模，确立功能组织的失效模式（如着陆功能失效、指示功能失效等）。通过将一个 block 转换为 AltaRica Node，一个 function 转换为 AltaRica Component，将 sysML 模型转换为 AltaRica 模型（可以通过工具 SimFia 自动转换），然后在部件层次将 AltaRica 模型自动转换为故障树（见图 4），故障传播在 AltaRica 中通过 Component 的输入/输出来实现。

最后，通过故障树可以计算出功能失效概率。注意：这里仅阐述了系统开发的一次迭代过程，在实际中，可以根据需要对模型进行修改，这些修改通过模型可以自动反映到最终的结果中。

3.4　资源层建模

利用 AltaRica 模型对 AFCS 的应用操作层、功能层和资源层进行统一描述，形成如下层次架构（见图 7），操作层同功能层进行交互，功能层根据操作性的模式操作指令进行相应功能的执行。

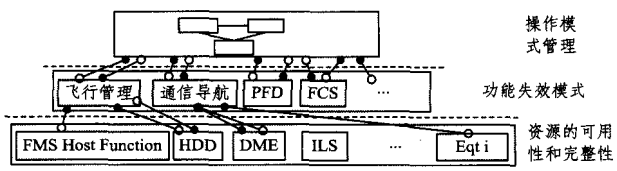

图 7　基于 AltaRica 的航电系统架构

航空电子系统的资源综合实现体现在电气/集成电路/可编程电子、SoC(System on-a-Chip)、SoS(System of System)以及结构综合（如多电控制结构）[5]。综合化资源的安全性分析包括资源的完整性和可用性两个方面，其中完整性包含了支撑多个功能间的共模情况。对于资源层建模，需要遵循如下步骤：

（下转第 143 页）

结束语 本文提出了一种针对 DNS Query Flood 攻击的检测方法，其利用域名解析的成功率计算出信息熵值，根据信息熵值的变化情况来判断 DNS 服务器是否出现异常。在判断 DNS 服务器出现异常的情况下，利用了滑动窗口进一步判断源 IP 地址的信息熵的变化情况，从而判断 DNS 服务器是否受到了攻击，并通过实验验证了该检测方法的有效性。这两种基于信息熵的方法结合起来使用可以有效准确地检测到攻击，提高检测的准确率，在某种程度上降低了漏报率；同时这种方法不需要设置阈值，这就避免了因经验不足而设置错误阈值的情况。

参 考 文 献

[1] Mockapetris P. Domain Names-Concepts and Facilities [S]. RFC1034. 1987

[2] Eastlake D. Domain Name System Security Extensions [S]. RFC2535. 1999

[3] 宗兆伟，黎峰，翟征德. 基于统计分析和流量控制的 DNS 分布式拒绝服务攻击的检测及防御[C]//2009 年计算机网络与通信学术会议论文集. 2009：206-213

[4] 黄宸，郑康峰，卢天亮，等. 基于信息熵的应用层 DDoS 攻击检测方法[C]//第十七届全国青年通信学术年会论文集. 第二卷，2012：467-472

[5] 李锦玲. 应用层分布式拒绝服务攻击的异常检测算法研究[D]. 郑州：解放军信息工程大学，2013

[6] 张小妹，赵荣彩，单征，等. 基于 DNS 的拒绝服务攻击研究与防范[J]. 计算机工程与设计，2008，29(1)：21-23

[7] 王佳佳. DDoS 攻击检测技术的研究[D]. 扬州：扬州大学，2008

[8] 刘永杰. 异常流量识别系统及其关进技术研究[D]. 南京：南京邮电大学，2013

[9] 徐川. 应用层 DDoS 攻击检测算法研究及实现[D]. 重庆：重庆大学，2012

[10] 尚波涛，祝跃飞，陈嘉勇. 一种应用层分布式拒绝服务攻击快速检测方法[J]. 信息工程大学学报，2012(5)：601-607

(上接第 127 页)

(1)识别资源的功能块/功能块要素。这里功能块的定义为资源(硬件、软件)中能够影响到资源功能安全的最小元素，一个功能块可由许多功能块组成(功能综合)，组成功能块的部分成为功能要素。例如，一个用于控制容器燃油容量的安全阀门可以分解为图 8 所示的功能块。

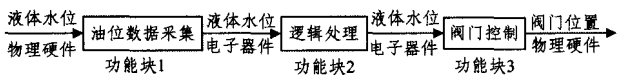

图 8 安全阀门-功能块分解示例

(2)将(1)中的功能块/功能块要素映射到子系统/子系统要素。子系统/子系统要素是一个物理实体的概念，是功能块/功能块要素的实现。一个子系统可以包括多个其它子系统，构成子系统的部分称为子系统要素，其失效会影响整个资源的失效，例如上例中构成安全阀门的每个子系统(水位传感器、可编程逻辑电路和阀门)失效都会影响到安全阀门的功能失效。对于子系统/子系统要素，其安全性分析需要考虑架构方面的约束和失效概率方面的要求。

(3)通过对资源的功能块、子系统分解，我们可以采用基于 Event-B 和 AltaRica 进行建模分析，这里不再赘述。

结束语 本文针对综合化航空电子系统安全性分析存在的失效模式完备性和动态失效问题以及数据一致性问题，提出了基于模型驱动的安全性分析方法，分别从应用操作层、功能层和资源层对航电系统建模，借助形式化工具能够实现 3 个层次上的语义一致性，从而从源头解决系统设计与安全性工作的相互分离的现象。本文的工作主要有如下 3 点：

(1)对综合化航空电子系统特征和安全性分析流程进行了分析，提出了现有工程实践中存在的问题；

(2)提出了基于模型的安全性分析流程和方法，实现了系统设计与安全性设计的集成；

(3)提出应用操作、功能和资源层分别建模的方法，并以航电系统安全性分析实例对提出的方法进行了验证。

参 考 文 献

[1] Society of Automotive Engineers. ARP-4761：Aerospace Recommended Practice：Guidelines and Methods for Conducting the Safety Assessment[C]//Process on Civil Airborne Systems and Equipment. 1996

[2] Papadopoulos Y, McDermid J A. Hierarchically Performed Hazard Origin and Propagation Studies[C]//Proceedings of SAFECOMP '99, 18th International Conference on Computer Safety, Reliability and Security. 1999

[3] Joshi A, Miller S P, Heimdahl M P E. Mode Confusion Analysis of a Flight Guidance System Using Formal Methods[C]//Proceedings of the 22st Digital Avionics Systems Conference (DASC'03). Indianapolis, Indiana, Oct. 2003：12-16

[4] Description A[OL]. [2012-01-19]. http://www.lix.polytechnique.fr/rauzy/

[5] IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems[S]. http://zh.wikipedia.org/wiki/IEC-61508, 1998

[6] Adeline R, et al. Toward a Methodology for The AltaRica Modelling of Multi-Physical Systems[C]//European Conference on Safety and Reliability (ESREL). Taylor & Francis：Rhodes, Greece, 2010

[7] Liu S, McDermid J A. A Model-Oriented Approach to Safety Analysis Using Fault Trees and a Support System[J]. Journal of Systems and Software, 1996, 35(2)：151-164

[8] Dotti F L, Iliasov A, Ribeiro L, et al. Modal Systems：Specification, Refinement and Realization[C]//Proceedings of the 11th International Conference on Formal Engineering Methods：Formal Methods and Software Engineering(ICFEM'09). 2009：601-619

[9] Chaudemar J-C, Bensana E, Castel C. Christel Seguin AltaRica and Event-B Models for Operational Safety Analysis：Unmanned Aerial Vehicle Case Study[OL]. [2014-03-19]. http://www.lix.polytechnique.fr/rauzy/altarica/AltaRica.html/

[10] Troubitsyna E, Laibinis L. Fault Tolerance in a Layered Architecture：a General Specification Pattern in B[C]//Proc. of the 2nd Int. Conference on SEFM. Beijing, IEEE, 2004：346-355

[11] Abrial J R. The B-book：Assigning Program to Meanings[M]. CUP, 1996

[12] Gallier J H. Logic for Computer Science：Foundations of Automatic Theorem Proving[M]. Publications Dover, 1986