基于模型的安全性分析及其在航空发动机软件系统上的应用

Application of Model Based Safety Analysis in Aero Engine Software System

魏钱锌 朱宇 阚鑫禹 曹志涛/中国航发研究院

安全性是武器装备研制、生产、使用和保障的第一要求。基于模型的安全性分析（MBSA）是传统安全性分析的进一步发展。航空发动机的设计人员与安全分析人员通过使用相同的系统模型，可避免因系统理解不一致而产生的设计分析协调问题，有助于提高安全性分析的完整性、连续性与可追溯性。

安全性是产品的一种固有属性，是保障武器装备使用效能的重要因素。我国自20世纪90年代起，先后颁布了一系列安全性工程技术和管理规定，逐步在飞机、火箭、导弹等大型武器装备系统的研制中推行安全性工程技术，促进了我国武器装备安全性工作的迅速发展。近年来，随着计算机科学与集成电路技术的日益盛行，传统的机械控制越来越多地被嵌入式软件控制所替代。对于航空航天领域，由于设计对象高度的系统集成化与深度的软硬件结合，如何进行有效的分析与验证，使严苛的安全需求得到保证已成为关注的焦点。

传统安全性分析方法及其局限性

传统安全性分析方法

系统安全性分析过程是传统安全科学的重要分支，基于系统安全理论的安全性分析方法自20世纪五六十年代诞生以来，一直用于战略战术武器、飞机、核电站等复杂系统的安全分析。基于系统安全的通用标准与行业标准体系日趋成熟且不断更新改进，其在军用产品领域主要的标准包括美军标MIL-STD-882E、英国军工标准Def Stan 00-56、电子电器产品安全性标准IEC61508等。国内军工领域的主要安全性标准为GJB 900A。此外，在一些特定领域也有各自制定的标准，例如，航空领域系统设计过程中常用的SAE ARP 4754A和SAE ARP 4761等，最初是为民用机载系统准备，但同样适用于飞机其他系统，例如发动机系统及其子系统。以发动机系统为例，基于SAE ARP 4761的安全性分析流程如图1所示。

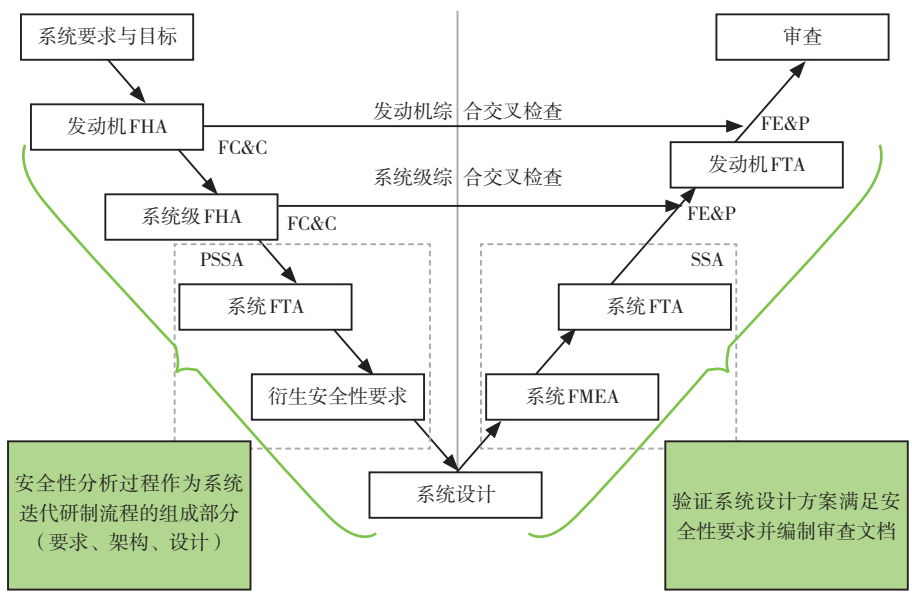

图1 基于SAE ARP 4761的安全性分析流程

完整的安全性分析流程包括安全性要求的定义与系统安全性要求的验证，其流程结构符合基于系统工程研制方法的V形结构。系统安全性分析方法按照研制流程分为功能危险分析（FHA）、初步系统安全性分析（PSSA）及系统安全性分析（SSA）三个阶段。FHA在设计研制阶段的早期进行，用来识别整机的功能失效情况及功能故障、衰退和功能丧失可能带来的风险；PSSA以FHA的结果为输入，通过安全性分析手段，如故障树（FTA）等，确定与分系统设计有关的危险及部件之间的功能关系导致的危险及影响，并得到衍生的安全性要求。SSA是在PSSA的基础上完成的，用以完成系统级安全性的综合评价。

局限性

在使用基于传统安全性分析方法进行安全关键系统分析时，由于设计对象高度的系统集成化以及深度的软硬件结合，传统的安全性分析方法出现了诸多弊端。

首先是系统分析结果的一致性。传统的安全性分析需要分析人员在全面了解系统的前提下才能开展安全性分析工作，而在实际分析中，安全性分析人员往往需要投入大量的时间收集系统架构信息与系统行为，然后根据对系统的理解构建安全性分析所需要的模型，如FTA等。这种分析的准确性严重依赖于分析人员的技术能力，且高度主观、易错，因此衍生出了大量的一致性验证工作。

其次是分析结果的重用性。一般而言，不同的研制阶段会进行不同程度的安全性分析，随着研制进度的推进，每一次系统的细化都要进行安全性分析的迭代，系统、部件设计的改变往往会导致整体安全性分析结论的变化，例如，系统失效模式与影响分析（FMEA）的变化，从而产生大量重复性工作。

MBSA流程及其优势

基于模型的安全性分析（MBSA）是在传统安全性分析的基础上引入了模型的理念，其核心在于通过计算机实现一部分重复性的安全性分析工作。在基于模型的研发过程中，很多研制过程活动，例如，仿真、验证、测试与代码生成等，都依赖于一个形式化的系统模型，模型可以用来做各种分析，例如，完整性与一致性分析、模型检查、定理证明等。

MBSA流程

目前对于MBSA具体应该怎样开展，在技术上有了一定的研究基础，但是由于不同研究者采用的技术不同，所采用的流程也不太相同。英国约克大学利萨戈[1]等人研究了每

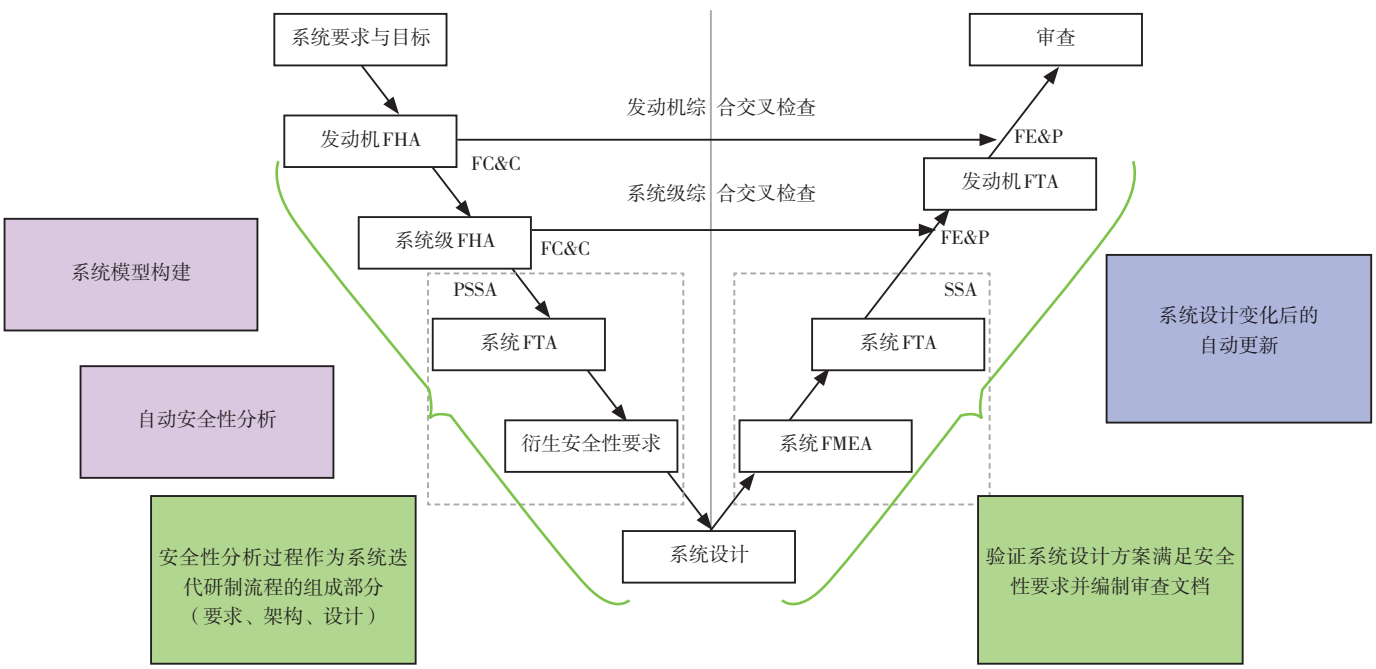

图2 加入MBSA方案的安全性分析流程

种MBSA技术的有效性并进行了对比分析。其中比较有代表性的是美国兰利研究中心的一份报告，该报告在传统安全性分析流程中加入了特定的分析理念，扩展总结了基于模型的安全性分析流程[2-3]，如图2所示。

为了支持基于模型的安全性评估，传统的V形结构需要进行相应的修改，以确保安全性分析工作能够围绕统一的系统模型展开。这些模型既可用于系统设计也能用于安全性分析，模型也是系统研制过程中的核心产物。比较典型的MBSA流程包含了形式化定义、名义系统建模、故障建模、模型扩展及安全性分析等流程。

形式化定义 安全性需求即是需要验证的系统安全性属性，例如航空发动机不能发生不可恢复的空中停车、转子叶片不能断裂等。定义安全性需求是所有安全性分析工作的第一步。基于MBSA流程的安全性需求的确定与传统的安全性分析确定需求的方法相同。为了支持自动分析，安全性需求需要通过形式化的符号表示出来。目前学术界提出了许多描述方法，例如时序逻辑语言CTL/LTL，同样也可以在构建系统模型的建模语言中直接确定安全性要求[4]。

名义系统建模 名义系统模型是指系统研发工程师和安全性工程师共同使用的明确的系统模型。名义模型中的系统行为用形式化语言表示，目前可采用的形式化配置语言种类繁多，支持图形或者文本等多种描述。例如，Matlab综合仿真环境Simulink/Stateflow，安全关键系统综合验证平台SCADE及相应支持语言——时序文本语言Lustre，基于AltaRica的分析验证平台Cecilia OCAS、Simfia等。

故障建模 故障模型包含的信息主要包括各种系统部件（包括数字控制器与机械系统）的故障方式。它定义了通用失效模式的行为，例如不确定、翻转、死锁等。故障模型同时也说明了故障的触发条件与失效时间，以及更复杂的故障行为，例如故障传播、条件故障（从属故障）等。借助于系统模型，可以构造不同类型的数字故障、机械故障、时间故障等。当前的MBSA技术中利用Simulink/Stateflow或SCADE来描述故障行为的研究较多。

模型扩展 将故障模型加入到名义系统模型中，描述系统在各种故障条件下的行为，得到的模型称作扩展系统模型。目前有两种方式将故障信息加入到系统模型中：第一种方式是构建一个独立于系统模型的故障模型，自动将两种模型合并用于分析，但这种建模方式在描述连续系统时存在一定的局限性，并且对系统信息的需求较大；第二种建模思路是直接构建失效情况下的行为，例如失效传播与转化符号（FPTN）、分层危险起因与传播研究（HiP-HOPS）等失效逻辑建模方法。在名义系统模型中加入了故障信息后，即得到了待验证的扩展模型。

安全性分析 对模型开展安全性分析是MBSA的关键环节。传统的安全性分析是通过模拟手段完成，即所谓的仿真方法，除此之外，计算机领域形式化方法的研究使模型检查、定理证明等新型分析方法在模型的分析中广泛普及。

采用仿真策略的安全性分析方法就是通过给所构建的模型施加激励信号或者外部数据，演绎系统正常或失效的动作与场景，判断系统安全性要求是否都得到了满足。采用仿真方法进行安全性分析的优势是原理简单易于实现。但仿真往往只能证明系统在预期条件下做了预期的事，并不能证明系统是否会做预期以外的事，因此仿真存在非完备性的缺点。目前MBSA研究领域采用仿真方法开展安全性分析的研究不多，在工程中更倾向于采用形式化方法（Formal Method）验证安全性需求是否被满足。

形式化方法最初是用在软件工程领域，主要目的是通过精确的数学语言来描述系统的结构和运行过程，它是设计与编写程序的出发点，也是验证程序是否正确的最重要依据。在模型建立完成之后，形式化方法可以被分为两类：一是模型检查，二是定理证明。在这两类方法中，模型检查方法相对成熟[5]，它是将原始设计表述成特定的模型，将要验证的性质用时态逻辑语言描述，通过遍历模型状态空间检验需求是否满足。模型检查的优点是分析过程全自动且无须人机交互，当判断性质不能满足时可以给出反例以定位设计错误。目前存在许多成熟的模型检查工具，例如贝尔实验室的软件与协议验证工具SPIN、卡耐基梅隆大学的符号模型验证工具SMV及其升级版本NuSMV。由于模型检查有着检测效率高且能够判断预期之外的故障是否发生的优势，因此基于模型检查的MBSA是目前进行模型安全性分析的主流。

MBSA的优势

基于以上分析，相较于传统安

全性分析方法，MBSA具有以下优点。

首先，系统设计人员与安全分析人员能够使用相同的系统模型，从而避免了由于系统理解不一致而产生的设计分析协调问题，有助于提高安全分析的完整性、连续性与可追溯性。

其次，基于模型开展安全性分析，可以利用现有的自动分析算法（形式化验证方法）通过计算机实现自动的安全性分析，在精准、高效、完备的基础上，也尽可能地减少安全分析人员的重复性工作，降低设计成本，同时也提高安全分析的质量。

MBSA应用于航空发动机软件开发

必要性与可行性分析

航空发动机作为复杂程度极高的关键系统，其安全性关系到发动机乃至飞机的使用寿命，甚至威胁到乘客及飞行员的人身安全。世界各国适航当局以确保安全为目的，颁布了各类适航规章、审定规范。我国借鉴美国联邦航空局（FAA）颁布的FAR33《航空发动机适航标准》颁布了中国民用航空规章CCAR33《航空发动机适航规定》，CCAR33的第33.75条款是专门针对发动机及其子系统安全性要求提出的，明确指出申请人必须对发动机及其控制系统进行安全性分析，以确保航空发动机的安全水平[6]。但当前国际上通常使用的分析方法仍是将民用飞机系统安全性分析方法直接运用到航空发动机上，导致航空发动机的安全性分析仍具有高度的主观性，因此，将MBSA应用到航空发动机上是十分必要的。

基于模型的航空发动机安全性分析，可以提供统一的系统模型，解决了因缺少统一架构模型导致无法进行完备的安全性分析的难题，并使得安全性分析随着研制模型的不断迭代而更具有连续性、一致性与可追溯性。因此，将MBSA应用于航空发动机是可行的。

分析框架

现阶段MBSA的应用主要集中在机载系统，且现有研究仍处于底层部分软件系统，鲜见在航空发动机整机系统上的应用。在航空发动机软件开发领域，已有基于模型开发的研究案例，即利用较为成熟的SCADE平台，将成熟的Simulink模型转换成SCADE模型，在SCADE平台中进行模型验证并生成代码，最后进行集成验证[7]。因此，在航空发动机软件系统率先进行MBSA的应用是现实可行的。目前工程研究人员广泛采

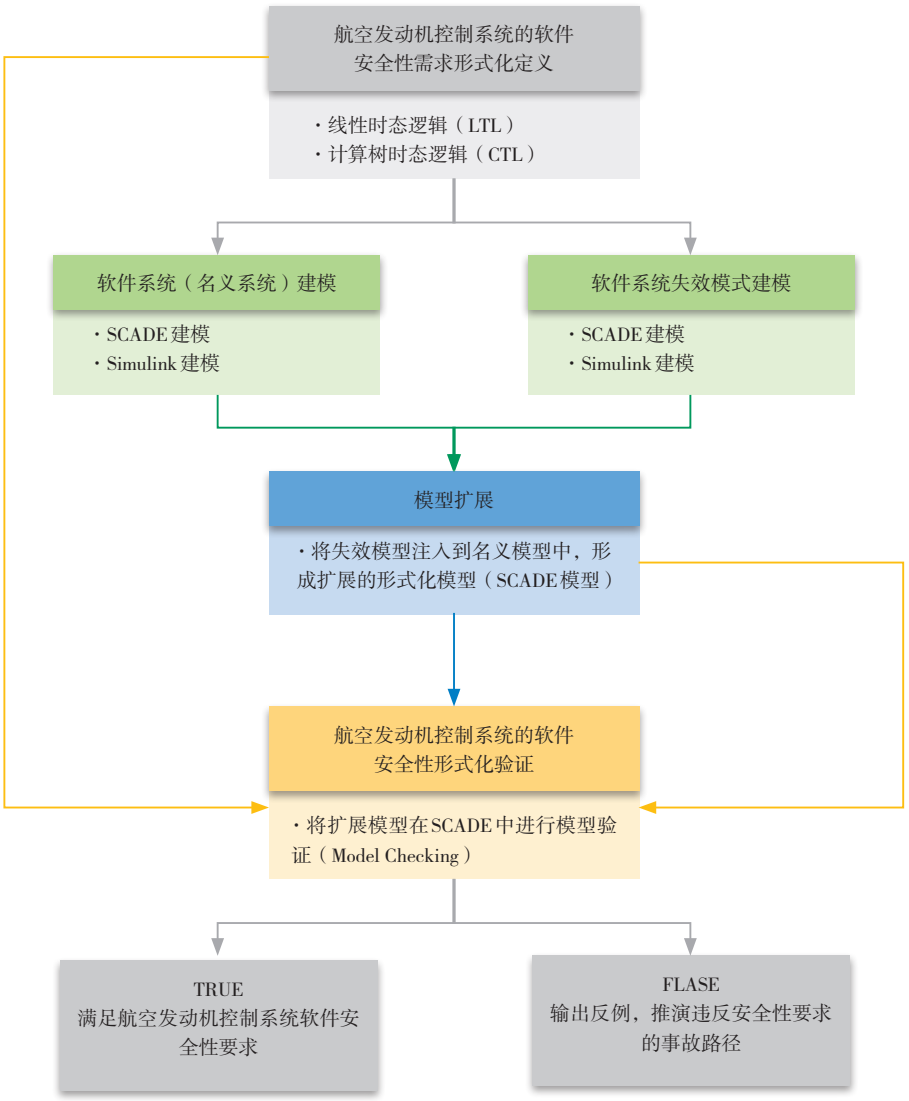

图3 基于模型的航空发动机软件系统安全性分析框架

用的模型构建及分析工具是Simulink与SCADE。SCADE专注于高安全性系统和嵌入式软件的集成开发，提供了多种接口，支持跨平台的联合开发。在与Simulink的联合开发方面，SCADE提供了Simulink Gateway和Simulink Wrapper，支持两者交互式开发。其中，SCADE Simulink Gateway包括Simulink Translator和Stateflow Importer两个模块，能将Simulink模型转换成SCADE模型。Simulink Wrapper可将SCADE模型集成到Simulink模型中并在Simulink环境下进行联合仿真。目前，GE公司、罗罗公司、普惠公司都用SCADE作为MBD的开发环境。

因此，本文尝试提出基于SCADE平台对航空发动机控制系统的软件部分应用MBSA的框架，如图3所示，试图为航空发动机安全性分析与验证提供一种全新的思路。

首先提出航空发动机控制系统的软件安全性需求，包含三个来源：一是航空发动机FHA的结论；二是对航空发动机不同层级（整机级、系统级、部件级）FTA及FMEA的结论；三是前一研制阶段模型检查得到的结论。以上分析结果是以直白的文字语言表达的，例如，航空发动机控制系统的软件部分不能发生进程死锁，需要将其应用时态逻辑进行形式化表达，使其能够作为模型检查的输入语言。通常，时态逻辑按照对系统时间的假设分为线性时态逻辑（LTL）和计算树逻辑(CTL)，由于两种时态逻辑的描述方式与描述能力存在差异，需要依据安全性需求的特点选择合适的时态逻辑。得到安全性需求的形式化表达后，应用SCADE或Simulink进行航空发动机名义系统建模，来描述控制系统正常工作情况下的系统行为。安全分析人员在得到航空发动机名义系统模型后，再应用SCADE或Simulink将失效模式进行建模，并注入到名义模型中，相当于对名义系统内的正常行为添加行为偏差，获得扩展的系统模型。将该扩展模型在SCADE平台中进行模型检查，通过自动遍历系统所有状态，验证是否存在进程死锁的可能，若平台输出TRUE则说明满足控制系统软件安全性要求，若输出FLASE则模型检查将输出反例，即一次或多次故障的行为轨迹，进而可以帮助航空发动机安全性分析人员推演进程死锁的事故路径。

关键技术

虽然将MBSA应用于航空发动机上是必要且可行的，但需要克服一些关键技术难题以求得进一步发展。

一是如何建立高保真模型。MBSA的核心是模型，模型的精确程度将决定着安全性分析的精确程度。航空发动机包含大量的热、气动、结构、强度等参数，如何使航空发动机名义模型与失效模型最大程度地接近发动机实际状态，对提高安全性分析的准确性具有重要意义。

二是如何转换安全性分析结论。现有基于模型的形式化验证的结论通常是用计算机语言描述的，语义难以理解且不能作为工程中安全性审查的结论。如何能将形式化验证的结果自动的转换为传统安全性验证结论（如FTA、FMEA等），找到模型检查与传统安全性分析工作的桥接，对完善MBSA流程具有重要意义。

结束语

MBSA作为当前国际安全性领域的研究热点，利用模型分析不仅可以提高安全性分析的准确性和效率，也为开展基于模型的各项智能化技术提供了良好的接口。对于航空发动机这一复杂关键系统，借助已有的研究经验对MBSA框架下的各项技术进行深入的应用研究，不仅能够为航空发动机安全性分析提供研究基础和技术积累，同时也将对提高航空发动机的安全性、可靠性带来巨大的工程价值。 航空动力

（魏钱锌，中国航发研究院，工程师，主要从事航空发动机智能制造前沿技术研究）

参考文献

[1] Lisagor O, Sun L, Kelly T. The Illusion of Method: Challenges of Model-Based Safety Assessment: 28th International System Safety Conference[C]. IEEE, 2010.

[2] Joshi A, Miller S P, Whalen M, et al. A proposal for Model-Based Safety Analysis:Digital Avionics Systems Conference[C]. IEEE, 2005.

[3] Joshi A, Whalen M, et al. Model-Based Safety Analysis Final Report[R]. NASA,2005.

[4] Halbwachs N, Caspi P, Raymond P, et al. The Synchronous Data Flow Programming Language Lustre[J]. Proceedings of the IEEE, 1991, 79(9) : 1305-1320.

[5] Clarke E M, Grumberg O, Peled D. Model Checking[M]. MIT Press, 1999.

[6] 中国民用航空总局. 航空发动机适航标准：CCAR-33-R2 [S]. 北京：中国民用航空总局, 2011: 1-2.

[7] 周彰毅. 基于SCADE的航空发动机FADEC软件开发[J]. 测控技术, 2018 (1): 110-115.