基于模型的 FMEA分析方法研究

Model-Based FMEA Analysis Method Research

卢波 高亚辉 姜成平 刘明 朱静 尹明明 / 中国航发动控所

针对当前全权限数字式电子控制（FADEC）系统研制过程中安全性评估工作不充分和不准确的问题，中国航发动控所创新团队开展了基于模型仿真的“失效模式和影响分析”（FMEA）工作，实现了故障模式对系统功能、性能影响的定性、定量和动态化分析，显著提高了复杂系统安全性评估的准确性和效率，降低了数控系统的研发成本，缩短了研制周期。

全权限数字式电子控制（FADEC）系统是关系到飞行安全的关键系统，适航标准对控制系统的安全性也做出了明确的要求。例如，美国和欧洲的适航标准规定申请人必须通过设计和验证来表明控制系统的安全性符合要求，可能对发动机产生危险性影响的单个元件的一次性失效必须在安全性分析中说明；我国的《航空发动机适航规定》（CCAR–33R2）中规定，在全勤构型中，对于失去推力或功率控制（LOTC/LOPC）事件相关的电子和电气的失效，发动机控制系统必须能容忍单点故障，并且申请人必须完成发动机控制系统的安全评估。

目前，FADEC系统的安全性评估主要采用传统的人工安全性评估流程和分析方法进行——通过非形式化设计模型和需求文件来人工进行安全性分析工作，如故障树分析（FTA）等。然而，这种分析非常主观，很大程度依赖分析人员的个人经验。安全性分析人员由于受专业领域和认知水平的限制，很难准确评估最小设计单元失效对系统行为的影响，分析结果也无法做到完整、准确。

中国航发动控所创新团队针对传统航空发动机控制系统研制过程中安全性评估流程与分析方法的局限性，在基于模型的系统工程（MBSE）方法论的指导下，开展了FADEC系统的多学科联合仿真建模研究；在此基础上，开展部件故障建模，基于故障注入开展故障影响分析和安全性仿真，实现故障模式对系统功能、性能影响的定量和动态化分析，将安全性评估工作从人工保证转为工具保证，从而显著提高了复杂系统安全性评估的准确性和效率。

FADEC系统的模型化

基于模型的FADEC系统安全性评估与分析的首要问题是解决FADEC系统的模型化。航空发动机数控系统主要由电子、液压、软件和传感器等组成，航空发动机各部件涉及的领域和专业各不相同，且均使用各自领域内的专业建模工具。航空发动机FADEC系统全数字仿真模型主要包括发动机模型、电子控制器模型、控制软件模型、液压模型、传感器模型等，各模型都使用不同的建模方法、不同的建模工具、不同的求解器形成各自的动态仿真模型。

发动机模型主要采用部件级建模方法，先对发动机各个部件进行独立模块建模，然后根据部件间的物理联系将各模块装配在一起，构成满足共同工作条件的动态数学模型。

电子控制器模型主要由电子控制器硬件电路模型组成，为了设计精确的控制参数、进行高精度的性能仿真以及实现故障注入，必须建立电子控制器电路的结构模型，一般采用Saber系统仿真软件来建立。

控制软件模型是控制逻辑和控制规律的载体，用来按照既定的逻辑和计划对发动机进行控制，控制软件模型可以采用C语言编程实现，也可使用MATLAB中的可视化仿真工具Simulink等图形化建模方法实现。

液压模型是对燃油泵、液压机械组件（HMU）和执行机构的统一建模，可模拟不同状态下燃油与作动子系统的工作过程，具有燃油计量模拟、燃油分配模拟和作动反馈模拟等功能。为了提高仿真精度、实现故障注入，同样必须采用结构化建模方法，常用的建模与仿真工

具为AMESim软件。

传感器模型的目标是模拟传感器工作时的静态和动态特性，同时其输入/输出接口应与发动机模型、电子控制器模型相匹配。常用的传感器建模工具为Saber或Simulink。

通过对以上FADEC系统各部件的常规建模工具与方法的分析可知，如果想要完成基于模型的系统安全性评估，首先就要解决这些多源异构模型的数据互联、仿真协同调度，以及故障注入等关键技术，即FADEC系统各部件的多学科联合仿真技术。

多学科联合仿真平台的建立

通过对本项目的不断探索与实践，创新团队采用总线集成式方案解决多源异构模型的数据互联、仿真协调调度。总线集成式方案是将各学科模型挂接在第三方虚拟总线上，由总线进行数据交互和仿真调度管理。CosiMate协同仿真计算平台是一种开放架构的协同仿真总线，可进行多点集成和不同仿真工具间的数据通信和传递，同时能对跨越各种网络环境的模型进行仿真，优化中央处理器（CPU）的利用率，提升仿真计算的效率。基于CosiMate的FADEC系统多学科联合仿真原理如图1所示。

实现故障注入的手段主要是各部件模型必须采用结构化建模方法且建模层级要追溯到最小元器件单元，通过对部件的详细建模，采用基于时间触发或事件触发的方式实现故障模式的注入，从而通过失效模式遍历仿真获得元器件失效对系统级的影响域分析，实现基于模型的安全性分析。

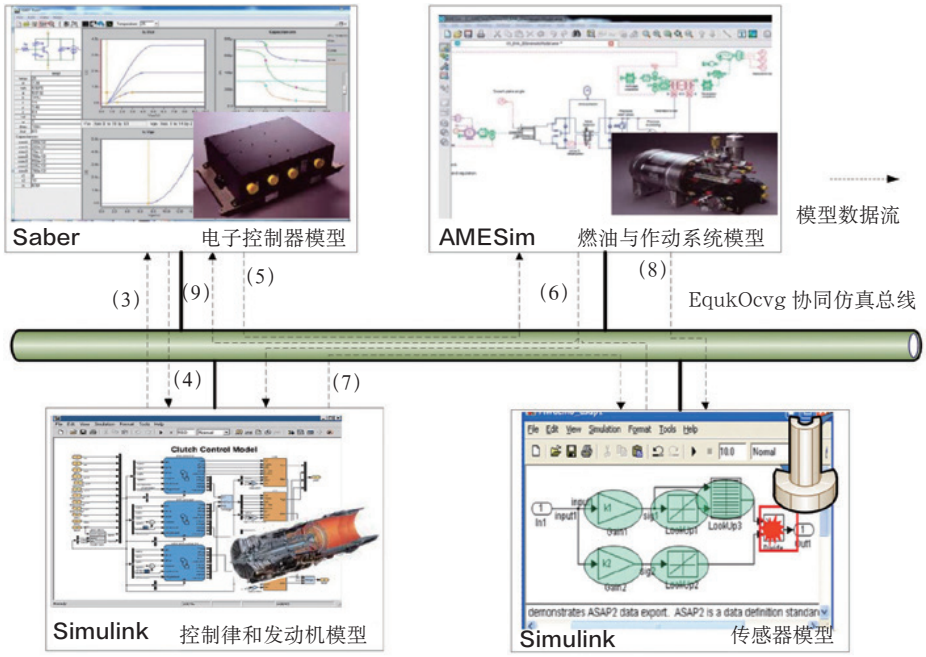

图1 基于CosiMate的FADEC系统多学科联合仿真

基于多学科联合仿真的FMEA技术实施路径

在完成上述基础工作之后，创新团队制定了基于多学科联合仿真的FMEA技术实施路径，如图2所示。

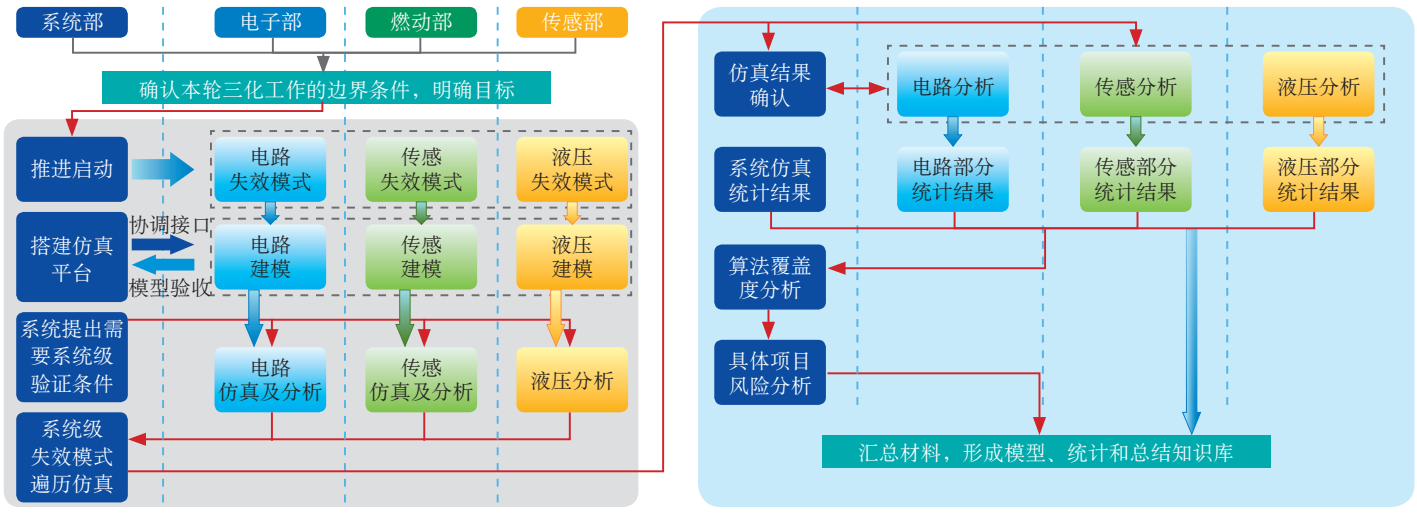

图2 基于多学科联合仿真的FMEA技术实施路径

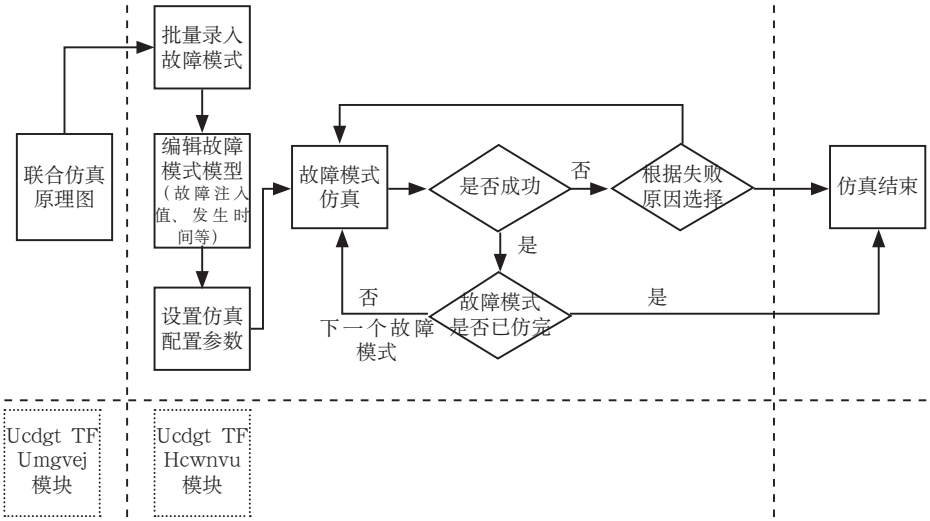

图3 实现故障自动遍历仿真的过程

首先，由系统工程师完成多学科联合仿真的方案设计，然后协同各部件专业完成数据流和模型接口的定义。

其次，各部件专业在已达成共识的各自约束条件下完成各部件的详细建模。各部件模型需要实现部件的功能、性能、失效模式等仿真。开展故障失效影响分析的前提是识别和定义故障模式，并建立对应的故障模型，故障模式根据部件的最小单元进行划分，每个最小单元有几种失效模式，进行遍历性建模，各部件建模人员需要对各自模型的准确性负责。

然后，由系统工程师对各部件模型进行综合，开展联合仿真调试。确认各自模型综合出的系统模型涌现性符合预期，然后根据各部件的最小单元失效模式进行遍历仿真，分析元器件级的失效对系统级的影响，系统级现有的故障检测与处理方法是否满足预期。

最后，通过建立自动比对测试平台实现对各元器件失效模式的遍历性仿真结果的确认，获取FMEA分析结果。由系统工程师根据结果分析故障覆盖度和项目风险，完成FMEA分析报告。

基于多学科联合仿真的FMEA自动化技术

由于FADEC系统本身的复杂程度较高，在具体实施过程中，基于多学科联合仿真的安全性评估工作量非常大，需要修改故障用例、配置用例、仿真和结果分析测试等，故障用例库也非常庞大，如果全部由人工来实现，效率非常低。因此，在工具链的基础上，创新团队通过二次开发，实现了基于MATLAB、Saber、AMESim等仿真软件的FADEC系统多学科全自动批次联合仿真技术。

根据梳理的失效模式列表，结合仿真模型，实现故障的批次注入。以电子控制器的故障自动注入为例，SaberRD软件的故障仿真模块能实现故障模式批量录入、批量设置、故障模式定时触发、多个故障模式并发、故障自动遍历仿真的功能。基于SaberRD的故障仿真模块实现故障自动遍历仿真的过程如图3所示。

在实现故障自动注入后的仿真过程中，跨工具进行数据抽取与交互将各工具的实施运行结果传递到MATLAB中，再通过二次开发，实时扫描数据并进行非覆盖性批次存储，再结合标称模型和故障模型各截面数据的自动分析判断，实现仿真结果报表的自动生成。

实施效果

创新团队通过研究，实现了基于模型的故障模式与效应仿真分析，并实现了过程自动化以及并行仿真等提高仿真效率的关键技术。随后，创新团队将相关成果在涡扇发动机数控系统的温度电路进行技术应用与验证。结果表明，通过基于模型的故障模式与效应仿真分析，使得温度电路96个故障模式和效应的扫描分析的时间从人工80h缩短为6h，效率提升了13倍，另外通过多电脑集群并行仿真技术，效率还可进一步提升N倍（N表示参与并行计算的计算资源节点数量）。基于多学科联合仿真进行控制系统安全性评估，发现了系统潜在安全性风险，为故障检测手段改进优化提供了理论依据，对提高系统的故障检测率具有重要意义。

结束语

相比较于现有的安全性分析方法，创新团队实施的方法不仅可以开展失效影响的定量化、显形化分析，而且通过自动化技术降低人工成本，显著提高效率和准确度，对系统安全性的提高具有重要的现实意义。另外，该项成果还可直接向其他项目和安全性评估等领域进行应用推广。 航空动力

（卢波，中国航发动控所，工程师，从事控制系统总体设计、FADEC系统多学科联合仿真工作）