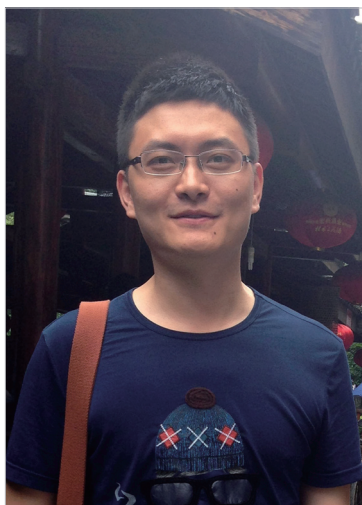


# 基于模型的系统工程在航电系统设计中的应用研究<sup>\*</sup>

## Study on Application of Model-Based System Engineering in Avionics System Design

中航工业第一飞机设计研究院 葛立敏 刘远恒 王 扬



葛立敏

硕士,工程师,主要研究方向为航空电子系统设计。

传统设计流程的每个阶段都是基于文档描述的形式,通过大量的、各种不同的文档传递信息。随着系统规模和复杂度的不断增加,文档的数量和种类成倍增加,而且在整个过程中主要依赖于人,人的经验和质量意识影响系统设计的结果。现代飞机的航电系统功能越来越复杂,综合化程度不断提高,给传统设计带来了

基于模型的系统工程设计方法,就是在模型的基础上,采用科学的指导方法,帮助和引导系统设计人员始终围绕着需求,逐步深入了解、明确系统的过程。该设计方法有效地解决了传统设计中的不足和弊端,完成了由经验研发向需求研发的转变。

DOI:10.16080/j.issn1671-833x.2015.08.060

新的挑战<sup>[1]</sup>。表现为:

(1) 在需求阶段的投入不足。其详细的需求分析没有科学的指导方法,系统设计的需求会存在很多隐患,而需求的捕获、分析及定义对于开发一个成功的系统至关重要。

(2) 前期需求缺少验证的手段,在后续设计和实现阶段发现大量需求存在的问题,耗费大量人力、物力和时间,直接影响系统开发的成败。

(3) 设计文件基于文字形式描述,信息传递差、标准化程度低,容易产生二义性,难以表述各种活动。

(4) 更改难度大。所有信息都包含在不同的文档中,要确保所有需要更改的内容都得到更改,将是个艰难的工程。

(5) 方案设计、详细设计、开发、

仿真和验证,整个过程之间缺少有效的需求追踪关系。

### 基于模型的系统工程设计方法

现代飞机航电系统这样复杂的任务不可能靠一个人来完成,因为没人能精通整个系统所涉及的全部专业知识,也没人能有足够的时间来完成数量惊人的技术协调工作。这就需要有一套科学的方法将人员、物质、资金等组织起来,有条理、高效率地完成工程任务。

系统工程设计方法分析与设计过程的目标是将用户需求转化为设计说明,即能够指导系统实现的一套解决办法。简单地讲,系统工程就是开发解决问题的系统的思想方法,按

<sup>\*</sup> 国家重大专项资助项目(2012ZX01041-006),国家航空科学基金项目(2013ZC31003,2013ZC31005)资助。

照这样的方法和步骤就可以帮助人们了解一个系统,对复杂的系统就不会感到无从下手,从而用流程和方法来保证系统设计的质量<sup>[2]</sup>。

基于模型的系统工程采用通用的系统建模语言 SysML<sup>[3]</sup>对系统进行建模分析。基于模型的系统工程设计流程如图 1 所示分为两大阶段,即黑盒分析和白盒分析过程。简而言之,黑盒分析过程明确系统要干什么,白盒分析过程确定如何实现。

## 需求分析

### 1 需求定义

基于模型的系统工程设计方法是基于需求分析和设计的指导方法,而非进行需求捕获的方法。采用 DOORS 工具对需要进行管理,可根据需要定义需求属性。

基于模型的系统工程设计方法只针对 ARP4754 中描述的功能性需求进行建模。功能性需求是系统需求的核心,先有功能性需求才会提出对应的性能需求、操作需求和接口需求等<sup>[4]</sup>。

### 2 系统需求分析

将系统的涉众需求归纳为初步系统需求,把 DOORS 中的需求导入建模工具 Rhapsody 中。建模过程中的所有活动都以需求作为驱动。

#### 2.1 系统用例图

USE CASE 图看似简单,但却是非常困难和重要的一个阶段。用例图包括 3 部分信息:边界、用例(功能块)和参与者,如图 2 所示。初步系统需求往往是非常庞大的,而且信息比较杂乱,如何有效地从中提取系统的相关需求变得尤为重要。用例图提供了一种科学的指导方法:(1)一定要站在系统的角度来抽象系统要完成的功能。刚开始只关注系统要完成的功能,根据功能对需求进行整理,明确系统边界。(2)现代飞机航电系统提供的功能非常繁杂,避免一开始就陷入需求的细节。要对关键功能需求进行抽象,根据功能的相关性抽象几个大的功能块,功能块之间尽可能独立。(3)分析完系统的边界和系统的功能块,紧接着考虑每个用例分别给“谁”提供信息,又需要

“谁”参与,定义系统的参与者。

整个分析过程就是对系统需求的充分理解,随着对系统认识的深入必然对需求有所更改,进一步更新完善系统需求。

#### 2.2 用例图需求追踪

建立需求追踪矩阵,再次确认用例分析过程中没有遗漏主要功能项,特别是分析中更改、完善的需求。

## 系统功能分析

完成系统用例图后,按用例进行分工,针对每一个用例进行系统功能分析。功能分析只关注系统的功能,不考虑系统的架构和实现方式。把系统当作一个黑盒,通过活动图、时序图、端口和接口、状态机运行多个视角分析系统,形成一个反复迭代、逐步深入的过程。用模型的方式更直观地展示系统的功能,最为关键的就是通过模型的运行,能够尽早地验证、确认功能需求<sup>[5]</sup>。

采用这样的功能分析方法,能够进一步明确系统的功能需求,帮助思考以下几点:(1)是否正确理解系统的功能需求;(2)功能需求是否存在冲突、重复、二义性和错误;(3)是否有遗漏的功能需求。

### 1 黑盒活动图

黑盒活动图的目的是识别系统的所有功能和主要的功能流,关注系统内在功能和可能发生的交互;规定系统的业务流程,功能之间的逻辑关系,隐含了功能之间的依存关系;动态有交互地展现系统的功能需求,如图 3 所示。

(1)建模过程是站在系统的角度看待系统的活动,要注意区分系统使用流程和系统活动之间的区别。(2)建立活动图时,先关注互相独立的关键功能,把问题先分解最后再整体考虑。(3)建立活动图的过程中对系统的认识越来越深入,会考虑到系统功能的很多细节,包括对外部参与者的输入、输出。活动图中涵盖定

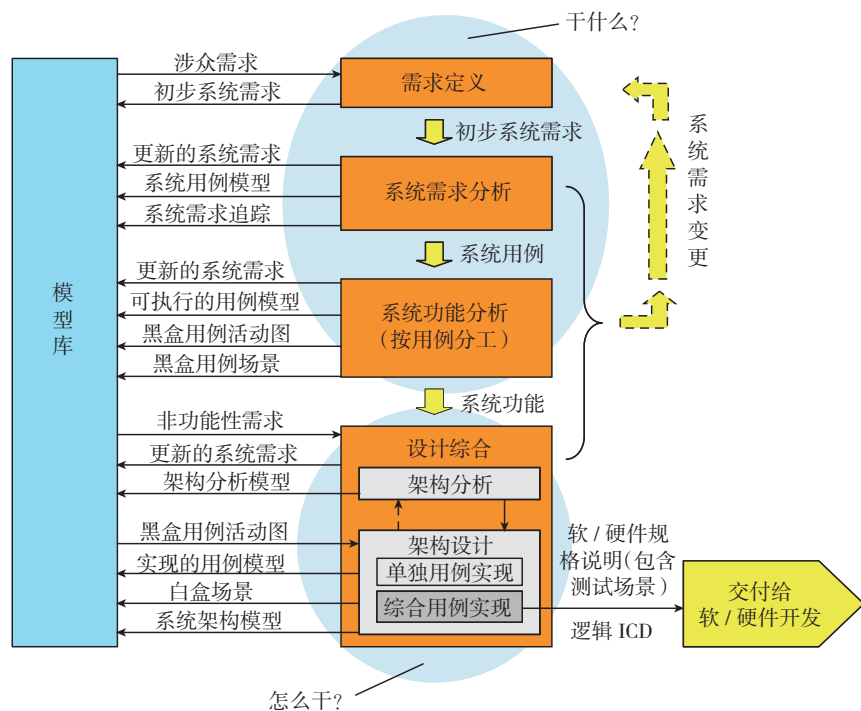


图1 基于模型的系统工程设计流程

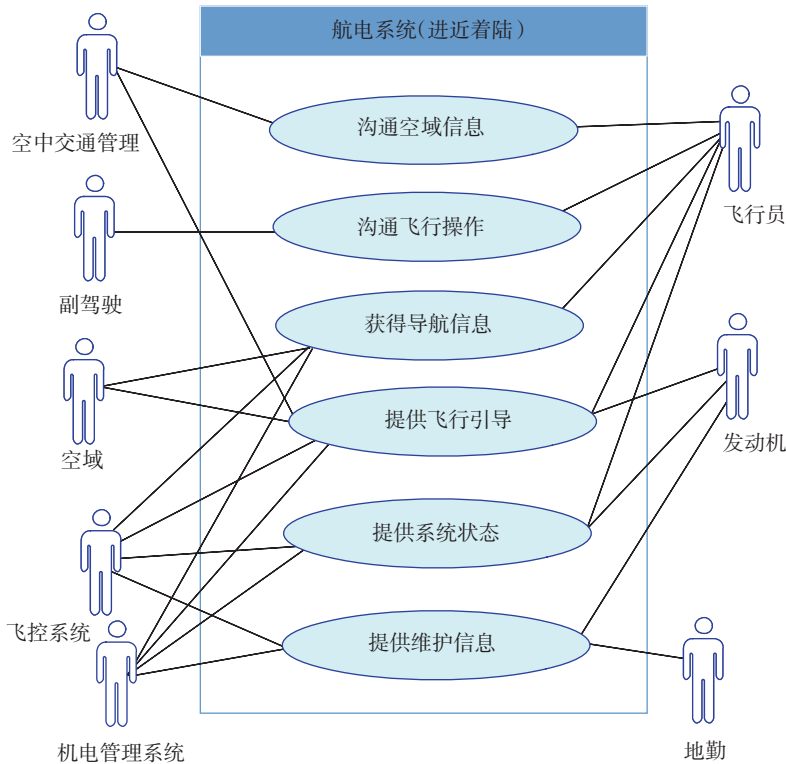


图2 航电系统进近阶段用例图

义所有的外部参与者。(4)活动图建模过程中避免使用含糊的描述,明确指出系统需要输入的具体参数,引出系统的端口和接口。

## 2 黑盒顺序图

在活动图的基础上考虑系统运行的场景,将注意力集中于每一个场景,而不是整个系统。让设计者的关注点更加集中,再次明确系统功能的动态过程以及与外部参与者的交互。顺序图相比活动图并没有增加新的内容,而是将活动图中的活动转换为序图中的行为。但因其独特的展现方式能更有效地揭示系统与外界参与者之间的交互内容,更加凸显系统的时序性,有时也称为时序图。

(1)在活动图的基础上建立系统的多个不同场景,场景中必须涵盖活动图中所有活动。

(2)顺序图中重点关注系统外部交互,明确系统与外部交互的具体内容,用于后续生产端口和接口(系统级逻辑 ICD)。活动图中的每个参与者标识“actor pin”都会对应一个

事件“event”。

(3)顺序图是在活动图的基础上,且信息都来源于活动图,切忌把顺序图建成活动图的翻版。顺序图并非换了种方式来描述活动图,而是要帮

助设计人员认知系统。每个顺序图对应一种特定的场景,使用多个顺序图尽可能遍历系统的所有运行场景。

(4)顺序图中的行为和活动图中的活动的描述必须一致,不能出现遗漏和增加。

## 3 创建系统端口接口

顺序图中包含了系统之间通信的具体数据,明确了每个数据的使用场景。创建系统的 IBD 图(内部块图),确定系统之间的端口。

系统之间的接口包括了与所有外部参与者的数据。与人员(飞行员和地勤)之间的接口即是系统的显示控制需求,与外部系统之间的接口就是系统之间的逻辑 ICD (接口控制文件)。为系统设计文件 ICD (接口文件)和 POP (飞行员操作程序)提供依据,可以保证所有的设计文件是有追溯的,这正是系统设计思想的核心。

## 4 黑盒状态机

状态机表达了系统基于状态变迁的行为逻辑。随着系统的建模分析,设计人员对系统的认识越来越明确、深入。在这种情况下,设计人员

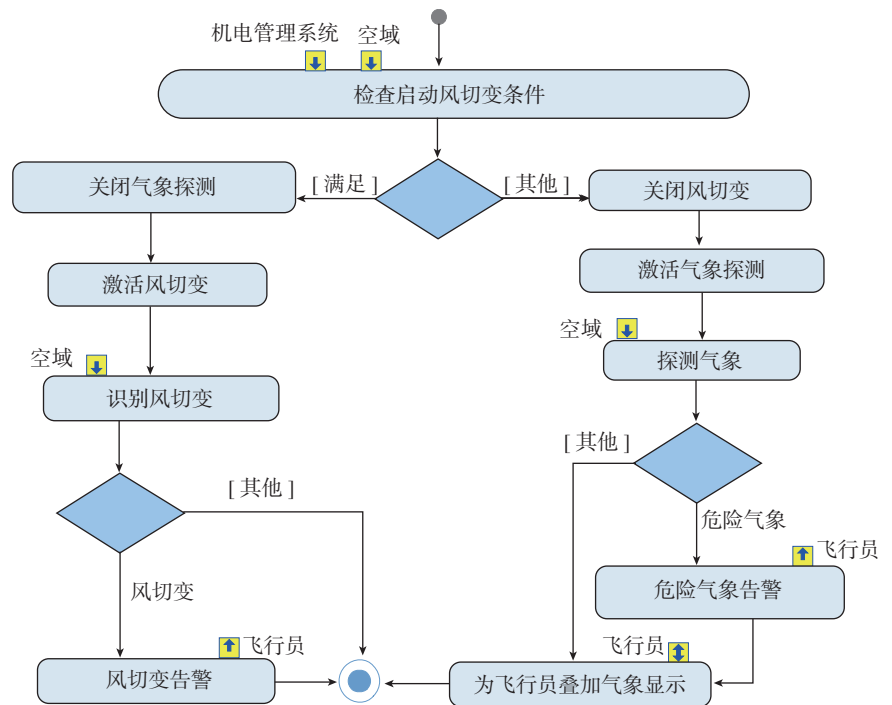


图3 气象探测黑盒活动图

就能够全面考虑系统运行的行为。

状态机的组成包括：有限的系统状态；状态之间的变迁；状态内系统的活动。活动图和顺序图中已经分析了系统的活动，状态机中包括了二者的所有信息，但缺少系统何时运行、触发的事件和条件等信息。在状态机中设计者重点思考系统运行状态之间的变迁事件和条件。之前的模型中只要通过“语义”能把系统的分支情况表述清楚即可，但状态机中必须符合“语法”来描述分支条件，故要对系统中的条件建立属性。

### 5 运行状态机

状态机模型中包含了系统的所有信息。为了更有效地验证系统模型，将状态机生成可执行模型。通过模型的运行来检验系统运行，再次思考模型是否合理，是否能够明确表达系统需求，以及系统需求的描述是否与模型一致。

如图4所示，通过状态机模型的执行和仿真系统内部的运行活动，可以更直观地检查系统行为。在执行状态机模型时，多考虑系统异常情况，可能发现系统新的需求和新的活动。模型的执行就是检验系统模型，

明确系统的功能性需求。在模型执行过程中会暴露出一些问题，设计人员必须再次完善系统功能性需求，一次次地迭代，直至验证系统功能性需求描述正确，系统模型确认无误。

### 6 关联需求

经过模型的执行和验证，得到有效的系统黑盒模型；紧接着要建立模型和系统需求之间的“satisfy（满足）”追踪关系，确保系统的功能性需求都在模型中体现，模型中涉及的系统功能都有相应的需求项描述；再次思考系统模型和需求之间的关系，确保分析过程的正确性。

## 设计综合

设计综合分为架构分析和架构设计两部分。架构分析过程中定义关键系统功能，确定候选解决方案，通过权衡分析合并解决方案，形成系统架构。架构设计过程将系统的功能分配到架构中，分析过程类似于系统功能分析，本文不做详细描述；最后进行用例合并，完成模型交付。

## 结束语

通过建模分析，得到基于模型的

系统工程设计成果。

(1)通过对系统建模，无歧义且有效地描述系统的各种活动，避免了文字描述中容易出现理解偏差，解决了文字描述复杂系统的缺陷，便于后期更改、维护和升级。

(2)标准化的模型设计，有利于信息传递，并且提高了沟通交流的效率。

(3)设计活动的追溯性。系统模型的建立涵盖系统的整个生命周期过程，包括需求、功能分析、设计、验证和确认，是一个统一整体的过程，可以提供一个完整的、一致的并可追溯的系统设计，确保所有的系统活动都是有依据的，是一个面向需求的设计过程。

(4)系统生命周期中包含着许多信息的传递和转换过程，模型更便于知识的存储，使得信息的获取以及再利用都更加方便有效。

(5)通过模型多角度地分析系统，分析更改的影响，并支持在早期通过状态机的运行来验证和确认系统需求，从而可以降低风险，避免了通过物理样件的试验来发现系统功能性需求问题，提高设计效率和设计质量。

(6)为后续系统设计过程提供设计输入，例如为系统设计文件ICD和POP提供依据，因此就可以保证所有的设计文件是有追溯的，是经过一系列科学分析的结果。

综上所述，基于模型的系统工程设计方法，就是在模型的基础上，采用科学的指导方法，帮助和引导系统设计人员始终围绕着需求逐步深入了解、明确系统的过程。该设计方法有效地解决了传统设计中的不足和弊端，完成了由经验研发向需求研发的转变。

本文共有参考文献5篇，因篇幅有限，未能一一列出，读者如有需要，请向本刊编辑部索取。

(责编 小城 谷雨)

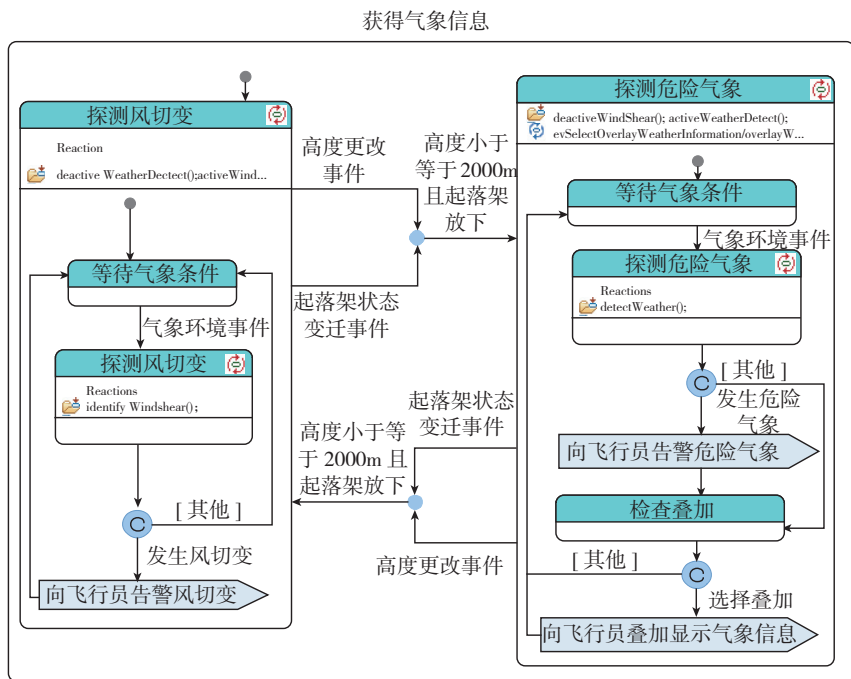


图4 气象探测黑盒状态机