面向DO-178C的襟缝翼控制系统需求的形式化描述

战芸娇 魏 欧 胡 军

(南京航空航天大学计算机科学与技术学院 南京 211106)

摘 要 DO-178C是对机载软件适航认证标准DO-178B的改进和补充,用于对民用飞机机载系统和设备软件质量控制提供指导。SCR(Software Cost Reduction)方法作为一种形式化方法,基于四变量模型,可以对复杂和大型的嵌入式系统进行需求描述。文中基于DO-178C,使用SCR方法对原飞机系统中的襟缝翼控制系统的需求文档进行形式化的需求描述,针对襟缝翼控制系统中的襟翼电机转速控制模块进行详细的案例分析,判断其是否满足DO-178C的相关验证指标。通过分析和验证,提出了SCR方法中的一些应用技巧。该工作可为SCR方法在机载软件系统中的应用提供依据。

关键词 DO-178C,SCR方法,四变量模型,机载软件,T-VEC

中图法分类号 TP311 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.04.033

Formal Description of Requirement of Slats and Flaps Control System for DO-178C Case

ZHAN Yun-jiao WEI Ou HU Jun

(College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China)

Abstract DO-178C is an improvement and supplement for airborne software airworthiness certification standard DO-178B, and it is used to provide guidance for software quality control of civil aircraft airborne systems and equipments. SCR(Software Cost Reduction), as a formal method, can be applied to the description of complex and large-scale embedded systems based on four-variable model. Based on the DO-178C, this paper used the SCR method to formalize the requirement specification of the flap slat control system in the original aircraft system, and carried on the detailed case for the flap motor speed control module in the flap slat control system. Through analysis, whether the DO-178C meets the relevant validation indicators can be determined . Through analyzing and validating, some application techniques of SCR method were proposed. This work will provide the basis for the application of SCR method in airborne software system.

Keywords DO-178C, SCR method, Four-variable model, Airborne software, T-VEC

1 引言

随着嵌入式软件系统在航空航天领域的广泛应用,由机载软件故障导致的灾难性事故也屡屡发生。事故的每一次发生都会造成生命和财产等的巨大损失,影响重大。机载软件[1]通常都具有规模庞大、数据关联复杂、安全级别要求高等特点,其需求存在可维护性差、相同操作描述不一致、不可验证信息较多和低层次与高层次需求不平衡等问题。美国航空无线电委员会(Radio Technical Commission for Aeronautics, RTCA)提出的航空适航认证指标DO-178C对机载软件的安全性提出了严格要求,其中规定了软件制品在开发过程中的需求分析阶段应达到的安全标准。保证软件系统在需求分析阶段的正确性及安全性是机载软件开发的重要课题。

通常,创建需求说明的方法有以下几种:1)列举所有的需求,这种方法将需求定义得很模糊,无法检验出需求间的联系与冲突;2)基于UML模型或伪代码的方法,此方法会造成重要信息的丢失,过多地限制了内部事件的顺序,导致需求过于完备;3)创建场景或测试用例的方式,这种方法的最大问题就是无法穷尽所有的场景或用例,不能保证需求的正确性。针对机载系统这种安全关键性系统,以上方法均不能保证需求的正确性。与传统的需求描述方法相比,基于形式化方法[2]的需求描述在软件开发的需求分析阶段可对变量及变量之间的关系进行形式化的描述,更易于发现需求中的错误;使用变量间的逻辑关系来表达需求之间的关系,便于进行需求中的一致性和完备性检查,可极大地提高需求的正确性和可靠性。

目前,学术界已经提出了许多用于需求描述的形式化方法,并在机载软件的分析中进行了实践。Leveson等[3]提供了一种针对过程控制系统的需求规范撰写语言——RSML(Requirements State Machine Language),并将该语言运用到了飞机防碰撞系统上。Parnas[4]首次提出了四变量模型,其

到稿日期:2017-02-20 返修日期:2017-05-01 本文受国家自然科学基金项目(61170043),国家重点基础研究发展计划(973)项目(2014CB744904),航空科学基金项目(20155552047)资助。

战芸娇(1993-),女,硕士生,CCF会员,主要研究领域为形式化方法、需求分析;魏 欧(1974-),男,博士,副教授,主要研究领域为形式化方法、软件自动验证,E-mail:owei@nuaa.edu.cn(通信作者);胡 军(1973-),男,博士,副教授,主要研究领域为形式化方法、机载系统安全性。

通过描述系统不同层次的需求文档和规范之间的关系，指明了文档需要包含的必要信息。Galloway 等[5]在 Parnas 的四变量模型的基础上，提出了两种对四变量模型进行改进的方法，完善了四变量模型对安全关键系统需求的描述，从而使其适用于航空航天领域中的安全关键性系统。

SCR 方法[6]最初是由 NRL 的研究员在为美国海军 A-7 飞机的作战飞机程序创建需求文档的过程中发展起来的，随着其优势的不断体现，逐渐被更多的工业组织（如贝尔实验室[7]、格鲁曼（美国安全公司）[8]、安大略省电力公司[9-10]等）使用。SCR 方法是一种用于描述需求的形式化方法，其基于四变量模型，使用表格的形式来表示系统需求中涉及的各类变量和变量之间的关系。表格化的抽象表示可以消除自然语言二义性的影响，清晰地反映相关变量之间的关系，便于检查变量取值的完备性。但 SCR 方法过于通用，缺少针对具体机载系统的指导。因此，本文基于 DO-178C，使用 SCR 方法对襟缝翼控制系统中的一个模块进行需求描述，以检验其是否满足标准中规定的目标并提供证据支持；最后通过实践总结了 SCR 方法的使用方法和应用技巧，展示了 SCR 方法在机载软件系统中的实用性。

襟缝翼控制系统[11]是控制飞机飞行时襟翼和缝翼运动的重要组件，为飞机在起飞、降落及空中飞行阶段提供升力。主要通过驾驶舱操作杆来设置襟翼和缝翼的目标状态，并通过闭环反馈控制器控制襟翼和缝翼的运动，使之达到目标状态。该系统的正确工作与否将直接影响飞机飞行时的安全，因此保证它的正确工作尤为重要。

本文使用 SCR 方法，针对 DO-178C 中关于高级需求分析的检验指标，在原有的以自然语言描述的需求文档的基础上，对襟缝翼控制系统中的襟翼电机转速控制模块进行需求描述。通过使用表格的形式描述需求并在 T-VEC 工具中建模，来对错误进行检查和验证分析。

本文第 2 节介绍了 DO-178C 和相关方法的基础知识；第 3 节给出了使用 SCR 方法进行需求描述的模式和步骤；第 4 节按照第 3 节提出的模式和步骤对襟缝翼控制系统中的襟翼电机转速控制模块进行了案例分析；第 5 节针对 DO-178C 中关于需求的标准，对 T-VEC 检验后的需求进行了验证与分析；最后总结了 SCR 方法的使用技巧。

2　背景知识

2.1　DO-178C

DO-178C 是对机载软件适用标准 DO-178 的第三次改版。其中，最重要的修改内容是针对许多新的软件研制技术或研制方法对原文档进行了改进和补充，包括面向对象技术、形式化方法、基于模型的开发和验证等，保持了该标准的稳定性和可扩展性。

适航标准 DO-178B 认为需求是软件质量的源头，并在相关技术说明中指明了软件高级需求和低级需求应该满足准确性、一致性和可验证性等。高级需求是指从系统需求、安全相关的需求及系统设计结构开发出的，与软件的功能、行为及安全等相关的需求。本文将针对系统高级需求进行分析。

2.2　SCR 方法

SCR 方法是一种基于四变量模型[12]的通用形式化方法。其将系统建模成一个由输入计算输出的黑盒子。监控变量（monitor variables）代表影响系统行为的输入环境量，受控变量（control variables）代表由系统控制的输出环境量；由输入变量（input variables）和输出变量（output variables）来描述系统内部软硬件之间的交互。另外，SCR 方法[13]中的中间变量（term）是需求说明中的一类辅助变量；一个模式类（mode classes）是系统状态集合到模式的一种划分；事件（events）是变量取值的改变。

在 SCR 需求说明中，使用表格来定义变量和变量取值的变化。每一类变量都定义在对应类别的表格中。条件表[14]描述了控制变量或中间变量作为监控变量和条件的函数的取值。条件标志着系统状态表达式取值的真假。事件表描述了控制变量或者中间变量作为监控变量和事件的函数的取值。当系统中的变量取值发生改变时，表明一个事件发生。@T(c) WHEN d[15]代表一个条件事件，当 d 发生时，c 变为真，且在此之前，c 为假，@F(c)代表 c 为假，DUR(c)代表条件 c 为真所持续的时间。

在 SCR 需求说明[15]中，通常使用以下前缀来代表变量类别："m"代表监控变量；"c"代表控制变量；"i"代表输入变量；"o"代表输出变量；"t"代表中间变量；"mc"代表模式类。

2.3　T-VEC 工具

美国 T-VEC 技术公司[16]参与了 DO-178C 标准的制定，提供了基于需求的测试和验证工具。T-VEC 是针对 SCR 需求分析方法，对系统的需求阶段和设计阶段进行测试验证和仿真的工具，具有集成的工作环境。自 1989 年以来，它被广泛应用于飞机的安全关键性系统、实时系统和许多嵌入式系统，并得到了 FAA 的认证。

本文主要关注 T-VEC 对表格式需求进行测试验证的测试向量生成工具。此工具从 SCR 需求分析中直接抽取测试输入、期待的测试输出和每个测试与相关需求间的映射关系。通过对需求进行编译，T-VEC 编译器也可以检查出需求中的语法错误和语义错误。

3　SCR 方法的应用过程

本节将简单介绍使用 SCR 方法对襟缝翼控制系统进行需求描述所遵循的方法步骤。

基于 DO-178C，图 1 描述了使用 SCR 方法创建需求描述过程的说明框架[15]。

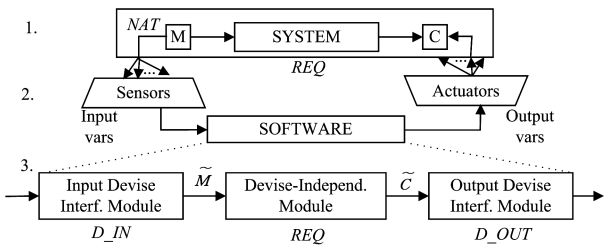

图 1　创建需求说明的 4 个步骤

Fig. 1　Four steps of creating requirement description

该框架将需求描述过程分为系统需求说明（System Re-

quirements Specification)、系统设计说明(System Design Specification)、软件需求说明(Software Requirements Specification)和通过增加对硬件故障的处理行为来扩展系统需求说明4个层次,层次间存在一定的关联关系。需求说明的过程遵循信息隐藏原则,将需求中不可能同时改变的部分分配在不同的组件中,使得每个需求的变化都只在单一的组件中发生而不会影响其他相关组件。

3.1 系统需求说明

在使用SCR方法创建系统说明的过程中,首先识别出与系统相关的环境量,即与外部环境相关的监控变量和受控变量,然后通过定义在监控变量与受控变量上的 NAT 和 REQ 关系来描述系统的需求行为。NAT 关系描述了法律、系统环境等施加在环境量上的约束,REQ 描述了建立在监控变量与受控变量之间且系统必须执行的行为。分析时,首先就系统在理想情况下的行为定义 REQ 关系;然后针对每个受控变量,指明时间约束或可能的容错处理。

3.2 系统设计说明

在该过程中需要完成对输入设备和输出设备的描述,以及对输入变量与监控变量之间、输出变量与受控变量之间的关系的描述。识别和记录估量监控变量值的输入变量和设置控制变量值的输出变量的方法。通常,硬件装置寄存器或控制器负责对这些值进行读写,其中,输入设备负责将读取的值定义为输入变量,输出设备负责将书写的值定义为输出变量。

3.3 软件需求说明

系统需求说明和系统设计说明是软件需求说明的基础。软件需求说明分为3个模块,分别是两个设备依赖模块:输入设备接口模块(D_IN)和输出设备接口模块(D_OUT);一个设备独立模块:功能驱动模块(REQ)。在本步骤中对设备依赖模块的需求行为即 D_IN 和 D_OUT 进行说明。

3.4 故障处理

图1中,$\widetilde{R}EQ$ 关系指明了监控量估计值 $\widetilde{M}$ 和受控量估计值 $\widetilde{C}$ 之间的关系。通常情况下,$\widetilde{R}EQ$ 是扩展的 REQ,$\widetilde{R}EQ$ 不仅描述了如 REQ 描述的理想情况下的系统行为,还增添了对许多外部非理想状态下的系统行为的处理,如硬件故障、传感器失效等。将可能发生变化的情况添加到相应变量的事件表或条件表中,使得所创建的需求描述具有灵活性和实用性。

4 对襟缝翼控制单元的案例分析

本节将采用第3节中说明的方法步骤,针对襟缝翼控制单元中的襟翼电机转速控制模块的需求进行描述。由于是对自然语言叙述的原文档进行改写,因此没有全部补充原需求中缺失的信息。4.1节对襟翼电机转速控制模块进行简单介绍;4.2节对模块需求说明进行了描述;4.3节对模块的设计说明进行了描述;4.4节描述了模块的软件需求说明;4.5节增加了对变量的故障处理和时间约束等。

4.1 模块介绍

襟翼电机转速控制模块是襟缝翼系统的重要功能模块,主要实现襟翼电机转速的闭环控制。模块的原理是根据襟翼电机转速设定值和襟翼电机转速传感器反馈信号,解算襟翼电机驱动电压输出及襟翼制动指令。如图2所示,模块对襟翼转速设置、襟翼转速反馈、襟翼禁用等输入信息进行处理,解算出襟翼电机驱动和襟翼制动指令信息,使得襟翼电机转速达到设定值,从而控制襟翼的偏转。

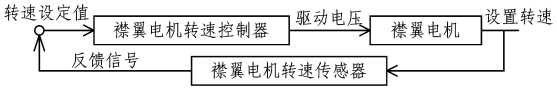

图2 襟翼电机转速控制原理图

Fig. 2 Schematic diagram of flap motor speed control

4.2 模块需求说明

模块需求说明主要依照SCR方法的原则和思想,识别出模块的监控变量、受控变量和需求描述中需要阐明的中间变量,并对监控变量与控制变量之间的 REQ 关系进行描述。针对每个变量,首先确定其所属的类型,然后在对应类别的变量表中描述其名称、标识符、类型、初始值及用途。其中,初始值是使用SCR方法描述变量时新增加的变量属性,可以描述变量取值的状态变化。本文将所有变量的初始值设为0,在具体应用中以系统启动时的变量取值为准。

4.2.1 模块中的受控变量分析

在襟翼电机转速控制模块中,包括两个输出到外部的量,通过输出驱动电压来改变襟翼电机的转速,进一步改变襟翼的偏转角度;通过输出制动指令来实现对襟翼电机的制动或解除。它们都是输出到模块之外由模块控制的量,因此被识别为受控变量。用变量襟翼电机驱动(*cg_fFlapMotorDrive*)来表示实际中输出的具体电压值,用襟翼制动指令(*cg_bFlapBrake*)表示是否对襟翼进行制动。模块受控变量如表1所列。

表1 襟翼电机转速控制中的受控变量

Table 1 Controlled variables of flap motor speed control

名称	标识	类型	初始值	用途
襟翼电机驱动	*cg_fFlapMotorDrive*	模拟量	0	襟翼电机驱动电压输出
襟翼制动指令	*cg_bFlapBrake*	布尔量	0	襟翼制动有效(1)、解除(0)

4.2.2 模块中的监控变量分析

本节描述外部环境中影响该模块行为而需要被监视的变量。控制襟翼电机转速的方式有两种,即主控制器控制和闭环反馈控制,模块需要根据所处的控制方式发出不同指令,因此,设置监控变量襟翼主控开关(*mg_dFlapMDCtrl*);该模块有3种模式,即手动模式、自动模式和禁用模式,因此,设置监控变量襟翼手动开关(*mg_bFlapMCommand*)、襟翼禁用(*mg_bFlapInhibit*)和襟翼手动指令(*mg_bFlapMCommand*)来表示模式状态。为了确定襟翼将来的运动状态,需要了解襟翼此时的转速值和襟翼转速的设定值,并计算二者的偏差,对转速进行调整,因此,模块需要监视襟翼转速设置(*mg_fFlapMotorSet*)和襟翼转速反馈(*mg_fFlapMotorFeedback*)两个监控变量的值。对于受控变量襟翼电机驱动的取值,需要参考前一时刻的值,因此定义监控变量襟翼电机驱动(*mg_fFlapMotorDrive*)。另外,在模块所涉及的用于计算电机驱动电压的增量PI控制算法中,需要襟翼电机转速控制器比例系数和襟翼电机转速控制器积分时间(ms)两个参数,表示为监控变量襟翼转速P参数(*mgf_*

FlapProportion）和襟翼转速 *I* 参数（*mgf_FlapIntegral*）。

表 2 列出了襟翼电机转速控制监控变量。

表 2　襟翼电机转速控制中的监控变量

Table 2　Monitored variables of flap motor speed control

名称	标识	类型	初始值	用途
襟翼转速设置	*mg_fFlapMotorSet*	模拟量	0	襟翼电机转速设定值
襟翼转速反馈	*mg_fFlapMotorFeedback*	模拟量	0	襟翼电机转速传感器测量值
襟翼禁用	*mg_bFlapInhibit*	布尔量	0	襟翼强制停止运动
襟翼手动开关	*mg_bFlapManual*	布尔量	0	襟翼手动开关开启标志，0 表示自动，1 表示手动
襟翼手动指令	*mg_bFlapMCommand*	离散量	0	襟翼手动状态输出指令，−1 表示角度减小，0 表示停止，1 表示角度增大
襟翼主控开关	*mg_dFlapMDCtrl*	布尔量	0	襟翼电机转速控制回路故障，主控制器直接控制电机驱动
襟翼转速 P 参数	*mg_fFlapProportion*	模拟量	0	襟翼电机转速控制器比例系数
襟翼转速 I 参数	*mg_fFlapIntegral*	模拟量	0	襟翼电机转速控制器积分时间（ms）
襟翼电机驱动	*mg_fFlapMotorDrive*	模拟量	0	根据监控到的范围确定输出电压值

在对模块的监控和受控变量的属性进行识别时，不可避免地会加入对变量的自然约束（NAT）。例如，在对襟翼的转速进行设置并驱动电压输出时，转速和电压等需要满足一定的范围，不可过小或超出实际应用的范围。在需求说明中，要随时保持监控变量与受控变量的一致性，如当受控变量襟翼电机驱动电压值发生改变时，相应的监控变量襟翼电机驱动电压值也需要做出更改。在 SCR 方法中，通常认为监控变量的值在与相应监控变量有关的控制变量的变化之后改变。

4.2.3　模块中的中间变量分析

在 SCR 方法中引入中间变量，可以使得需求描述更加简明。在襟翼电机转速控制模块中，襟翼电机转速的设定值和襟翼电机转速的反馈值之间的偏差（*te*(*t*)）不被模块监控，也不受模块控制，却影响着模块对襟翼运动的处理，因此将其设置为中间变量。同理，添加了中间变量襟翼手动开关（*tg_bFlapManual*）、襟翼手动指令（*tg_bFlapMCommand*）、B 项机驱动电压（*tB_FlapMotorV*）。表 3 列出了襟翼电机转速控制模块所监视的中间变量。

表 3　襟翼电机转速控制中的中间变量表

Table 3　Term variables of flap motor speed control

名称	标识	类型	初始值	用途
襟翼手动开关	*tg_bFlapManual*	布尔量	0	襟翼手动开关开启标志，0 表示自动，1 表示手动
襟翼手动指令	*tg_bFlapMCommand*	离散量	0	襟翼手动状态输出指令，−1 表示角度减小，0 表示停止，1 表示角度增大
偏差	*te*(*t*)	模拟量	0	襟翼转速设置和襟翼转速反馈的偏差
B 项机驱动电压	*tB_FlapMotorV*	模拟量	0	B 项机驱动电压取值

4.2.4　监控与受控变量之间的 *REQ* 关系分析

在 SCR 方法中，通常将受控变量看作监控变量与中间变量的函数，列出监控变量与中间变量在不同的取值情况下受控变量的值，表示为条件表、事件表和模式表。原文档中指出，当襟翼禁用为无效且襟翼转速设置不为 0 时，襟翼制动指令（*cg_bFlapBrake*）被设置为无效；当襟翼转速设置为 0 并保持 2 s 后，设置襟翼制动指令（*cg_bFlapBrake*）为有效。其描述的是监控变量取值的改变导致受控变量的变化，因此使用事件表来表示这一过程。使用规范的 SCR 表格表示方法将其转化为襟翼制动指令事件表，如表 4 所列，其中 0 代表襟翼制动指令无效，1 代表襟翼制动指令有效。

表 4　襟翼制动指令事件

Table 4　Flap brake command event

Event	*cg_bFlapBrake*
@*T*(*mg_bFlapInhibit*=0)	0
Dur(*mg_fFlapMotorSet* > 0)s	1

襟翼电机驱动电压的输出范围，须根据襟翼当前实际转速的不同取值来判断。为表示取不同转速值时电压的输出范围，将襟翼转速值的条件转换成符号表示的谓词逻辑表达式，其转化成的襟翼电机驱动条件如表 5 所列。表中最后一行表明，当监控变量襟翼电机驱动的绝对值小于 1.5 V，即电压较小时，将襟翼电机驱动近似为 0 V。

表 5　襟翼电机驱动条件

Table 5　Flap motor drive condition

Condition	*cg_fFlapMotorDrive*/V
mg_fFlapMotorFeedback	[0,28]
mg_fFlapMotorFeedback−200r/min	[−28,0]
mg_fFlapMotorFeedback	[−28,28]
|*mg_fFlapMotorDrive*|<1.5	0

事件的改变往往不只影响一个受控变量的变化。例如：原文档中襟翼手动开关和襟翼手动指令的不同组合会同时影响襟翼电机驱动和襟翼制动指令的取值。将其转换成如表 6 所列的联合事件表，表中含有中间变量襟翼手动开关。

表 6　襟翼电机驱动与襟翼制动指令事件表

Table 6　Flap motor drive and flap brake command event

Event	*cg_fFlapMotorDrive*/V	*cg_bFlapBrake*
@*T*(*mg_bFlapManual*=1 *mg_bFlapMCommand*=0)	0	1
@*T*(*mg_bFlapManual*=1 *mg_bFlapMCommand*=1)	14	0
@*T*(*mg_bFlapManual*=1 *mg_bFlapMCommand*=−1)	−14	0
@*T*(*mg_bFlapInhibit*=1 *tg_bFlapManual*=0)	0	1

4.3　模块设计的说明

该小节重点描述了襟翼电机转速控制模块中与硬件设备相关的输出变量、输入变量、输出变量与受控变量之间的对应关系以及输入变量与监控变量之间的对应关系。其间，忽略了一些设备接口的细节信息，如硬件设备的存储方式、映射方式等。

4.3.1 模块中的输出变量分析

输出变量通过模块内的硬件设备输出，与受控变量对应。表 7 列出了模块中涉及的输出变量。

表 7 襟翼电机转速控制中的输出变量

Table 7 Output variables of flap motor speed control

名称	标识	类型	初始值	用途
襟翼电机驱动	*og_fFlapMotorDrive*	模拟量	0	襟翼电机驱动电压输出
襟翼制动指令	*og_bFlapBrake*	布尔量	0	襟翼制动有效、解除

输出变量与受控变量通常是一对一的关系，襟翼电机转速控制模块就符合这种情况，即输出变量襟翼电机驱动电压经过硬件设备的滤波处理后形成受控变量襟翼电机驱动。

4.3.2 模块中的输入变量分析

输入变量通过与模块相关的硬件设备输入，并与监控变量对应。为了得到襟翼转速反馈数值，在模块中安装襟翼电机转速传感器来测量襟翼的反馈转速，传感器的输出用模块输入变量襟翼转速反馈(*ig_fFlapMotorFeedback*)表示。模块需要对襟翼所处的控制方式和模块所处的模式进行判断，在模块中添加硬件设备的手动开关和主控开关。手动开关的状态用输入变量襟翼手动开关(*ig_bFlapManual*)表示。主控开关的状态用输入变量襟翼主控开关(*ig_dFlapMDCtrl*)表示。

对于硬件设备来说，设备故障的发生是不可避免的。因此，对硬件设备添加故障描述，对襟翼电机转速传感器、襟翼手动开关、襟翼主控开关的故障用输入变量襟翼电机转速传感器故障(*ig_fFlapMotorMal*)、襟翼手动开关故障(*ig_bFlapManualMal*)、襟翼主控开关故障(*ig_dFlapMDCtrlMal*)表示。表 8 列出了在监控变量的基础上添加的输入变量。

表 8 襟翼电机转速控制的输入变量

Table 8 Input variables of flap motor speed control

名称	标识	类型	初始值	用途
襟翼电机转速传感器故障	*ig_fFlapMotorMal*	布尔量	0	用于判断襟翼电机转速传感器是否发生故障，0 代表没有故障，1 代表发生故障
襟翼手动开关故障	*ig_bFlapManualMal*	布尔量	0	用于判断襟翼手动开关是否发生故障，0 代表没有故障，1 代表发生故障
襟翼主控开关故障	*ig_dFlapMDCtrlMal*	布尔量	0	用于判断襟翼主控开关是否发生故障，0 代表没有故障，1 代表发生故障

由于监控变量是在忽略可能发生故障的理想状态下定义的，因此输入变量中的故障变量不对应监控变量。其余的 8 个输入变量各自对应一个监控变量。

4.4 模块的软件需求说明

软件需求说明主要是对设备依赖模块 *D_IN* 和 *D_OUT* 之间的关系进行说明。*D_IN* 关系指明了怎样使用输入变量来估计监控变量的值。在襟翼电机转速控制模块中，除襟翼电机转速反馈的值需经过滤波处理后进入模块进行处理外，其他的输入变量与对应的监控变量之间都是直接对应的关系。*D_OUT* 关系指明了用受控变量的估计值来驱动输出设备的方法。在襟翼电机转速控制模块中，情况比较简单，输出变量与对应的受控变量之间也都是直接对应的关系。

4.5 故障处理及时间约束

在实际系统中，故障的发生是不可避免的，因此在系统设计的过程中，一定要考虑系统的容错能力，添加系统满足的对硬件设备故障的处理要求和时间约束。

4.5.1 处理模块中的硬件故障

襟翼电机转速传感器、襟翼手动开关、襟翼主控开关分别有输入变量对应它们的故障情况，当其中有变量值为真时，表示对应的硬件设备发生故障。当襟翼手动开关发生故障时，将不能判断此时的襟翼电机转速控制模块是处于手动模式还是自动模式，此时，出于对系统安全的考虑，将模块强制设置成手动模式。为此，将表 6 转换成表 9。

表 9 襟翼电机驱动与襟翼制动指令事件

Table 9 Flap motor drive and flap brake command events

Event	*cg_fFlapMotorDrive*/V	*cg_bFlapBrake*
$@T((mg\_bFlapManual=1 ig\_bFlapManual=1) mg\_bFlapMCommand=0)$	0	1
$@T((mg\_bFlapManual=1 ig\_bFlapManual=1) mg\_bFlapMCommand=1)$	14	0
$@T((mg\_bFlapManual=1 \vee ig\_bFlapManual=1) \wedge mg\_bFlapMCommand=-1)$	−14	0
$@T(mg\_bFlapInhibit=1 tg\_bFlapManual=0)$	0	1

在表中对应事件襟翼手动开关有效的后面添加条件襟翼手动开关发生的故障，构成或关系，表示在襟翼手动开关设置为手动模式或者襟翼手动开关故障的事件发生时，对应襟翼电机驱动，襟翼制动指令的设置可能会发生。

襟翼主控开关(*g_dFlapMDCtrl*)的打开或关闭决定着襟翼处于主控模式或非主控模式。当襟翼电机转速控制回路故障(*mg_bFlapFault*)发生时，襟翼主控开关打开；故障消除时，主控关闭。表 10 列出了模式之间的迁移关系。

表 10 襟翼主控开关模式

Table 10 Flap master switch mode

g_dFlapMDCtrl	触发事件	*g_dFlapMDCtrl_OUT*
off	$@T(ig\_bFlapFaultMal=1)$	*on*
on	$@T(ig\_bFlapFaultMal=0)$	*off*

4.5.2 处理模块中变量的时间约束

变量的时间约束在系统中是十分常见的。为了更完整地表示模块行为，在襟翼电机转速控制模块的每个控制变量上都添加了相应的时间约束。理想化的模块描述中没有对变量

的时间约束。表 11 给出了在表 5 中添加对控制变量襟翼电机驱动的时间约束，表明当监控变量襟翼转速反馈的条件值或者襟翼电机驱动的值发生变化时，对应襟翼电机驱动的电压值要在 300 ms 之内做出改变，区间中的 0 代表做出改变的最小时间值，300 代表做出改变的最大时间值。

表 11　襟翼电机驱动条件

Table 11　Flap motor drive condition

Condition	*cg_fFlapMotorDrive*/V
mg_fFlapMotorFeedback	[0,28]
mg_fFlapMotorFeedback−200 r/min	[−28,0]
mg_fFlapMotorFeedback	[−28,28]
|*mg_fFlapMotorDrive*|<1.5	0
Timing constraint/ms	[0,300]

5　需求验证与分析

本节主要针对第 4 节中的需求描述，分析 T-VEC 工具与 DO-178C 标准中高级需求的符合性。

使用 T-VEC 验证有以下好处：1）可以对需求说明中一些简单的关键字拼写错误、语法表达错误进行检查和定位，节省了很多人为检查的时间，且准确性更高；2）对于大型和复杂的系统，通常很难保证需求的一致性，使用 T-VEC 运行需求可以发现需求说明中上下文出现的冲突，帮助工程师发现系统行为和使用场景等中的问题并重新确立；3）系统的很多错误常发生在边界，T-VEC 可以在定义的数据量的最大值、最小值边界处生成测试向量，在需求阶段测试系统的稳定性，确定安全性，发现错误，从而减少后续更正的工作量。

使用 T-VEC 对襟翼电机转速控制模块的需求进行验证与分析主要分为以下几方面：1）编译输入的需求模型，对变量定义、事件表等进行语法错误检查，以验证需求模型的正确性，从而发现模型中的错误。由于篇幅有限，此处只列出部分问题：第一，襟翼制动指令事件表中的变量组合不完备。在表 1 监控变量襟翼禁用和襟翼转速设置 2 种变量组合时应该有 4 种情况，而表中只有 1 种情况组合。第二，未对变量设置初始值。原文档中对变量做简要描述时未对变量设置初始值，这是很严重的一项缺失，编译需求模型时报错。2）查看工程状态报告，根据报告中的测试向量、测试路径（DCP）情况等进行进一步检验。3）查看覆盖率分析，确认覆盖分析能通过，验证需求模型的完备性。针对本文的例子，产生 21 条 DPC 即能满足要求。4）生成测试向量，由测试向量中的输入、输出及关联的需求来验证需求的一致性和正确性。验证结果如表 12 所列，表中第 1 行和第 3 行分别表明：在襟翼主控开关关闭且无故障发生时，襟翼主控开关仍保持关闭模式；当襟翼主控开关关闭且发生故障时，襟翼主控开关打开，襟翼处于主控模式，从而验证了模式转换的正确性和一致性。这些均符合 DO-178B 中利用形式化方法对系统高级需求的准确性和一致性以及系统需求符合性的验证。

表 12　测试向量输出结果

Table 12　Output results of test vector

test	*vector*	*g_dFlapMDCtrl_OUT*	*g_dFlapMDCtrl*	*mg_bFlapFault*
1	1,2	*off*=0	*off*=0	*False*=0
2	3,4	*on*=1	*on*=1	*True*=1
3	5,6	*on*=1	*off*=0	*True*=1
4	7,8	*off*=0	*on*=1	*False*=0

另外，基于 SCR 方法的准确性原则，原文档中所使用的“保持 2s”的含义不清，即保持 2s 是否应该包括 2s 指代不明，本文中指包括 2s。在对偏差的计算中，原文档中只提到了襟翼转速设置与襟翼转速反馈的差值，没有表明是前者减后者还是后者减前者，本文认为是前者减后者。SCR 方法中遵循信息隐藏的原则，即隐藏组件的内部实现细节，只暴露组件间的接口信息，符合 DO-178B 中高级需求与目标机兼容的要求。

6　方法总结

本文使用 SCR 方法对自然语言描述的需求文档进行改写。针对 SCR 方法过于通用、具体应用细节不清楚的问题，将如何从原文档中识别出监控变量、受控变量及中间变量，区分控制变量取值变化的事件和条件等总结如下。

6.1　监控变量与受控变量的识别

对监控变量进行识别时，首先检索所有的输入变量，找到与外部环境相关输入到模块中的变量，如温度、湿度、风速等，确认这一类为监控变量，并根据对应的输入变量的类型、精度、初始值等来确定监控变量的信息。然后，对剩下的输入变量进行检索，找到其他模块输入到该模块中的变量，如在襟缝翼系统中，将翼面位置控制模块的输出变量襟翼电机转速设定值作为襟翼电机转速控制模块的输入变量。将这类输入变量作为所分析模块的监控变量，变量的初始值、类型、精度等信息由前一模块的输出来确定，这是因为前一模块的输出未受到任何干扰，更能代表理想状态下模块的监控变量值。最后，根据剩余的输入变量，分析其与模块行为的相关程度，如果相关程度不大，且在模块的处理过程中并不十分需要可以考虑删去这些变量；对于那些模块处理过程必且原输入变量没有涉及的变量，可考虑将其添加到监控变量中。

受控变量的识别与监控变量类似。首先，对所有的输出变量进行检索，找到输出到外部环境中的变量，如控制温度、高度等，并根据对应输出变量的类型、精度等来确定受控变量的信息。然后，对剩下的输出变量进行检索，找到将要作为输入变量输入到其他模块的输出变量，如在襟缝翼系统中，襟翼电机转速控制模块的输出变量襟翼电机驱动将作为输出接口数据转换模块的输入变量，将这类变量作为所分析模块的受控变量，变量的取值、类型、精度则与原输出变量保持一致。最后，根据模块的处理过程，分析出那些受模块控制而未体现在原输出变量中的变量，并将其添加到受控变量中；而对于那些并不完全由该模块控制或不相关的变量，则将其删除。

6.2　中间变量的识别

与其他具体的变量不同，中间变量是 SCR 方法中为方便分析系统行为、简化表格表述而引入的一类变量。在本文所述转化中，需将模块的处理过程抽象成公式的表达形式，在逻辑描述中除了常涉及的那 4 类变量外，还有一些不属于那 4 类变量中的任何一类，或者是由某些变量计算得来的中间值，此时就需将那些变量识别为中间变量。如：在襟翼电机转速控制模块中，为了方便描述模块的功能，将由监控变量襟翼转速设置和襟翼转速反馈计算得来的中间变量偏差作为中间变量；在模块处理过程中涉及的 B 项机驱动电压不属于 4 类变量中的任何一类，但在计算中对其有需要，因此将它也识别为中间变量。

6.3 事件与条件的区分

在 SCR 方法中，如何区分控制变量改变的事件与条件是一项重要内容。事件代表了系统某些性质取值的改变，条件刻画的是系统状态表达式取值的真假。为此，在自然语言描述的处理过程中，当存在“当…时”或“如果…时”这类表述时，将其作为事件进行处理。如：原文档中出现“当襟翼转速反馈大于或等于 200 r/min 时”，将其当作事件填写到事件表中。在剩下的处理过程中，若语句最后判定变量的真假取值，则将其作为条件进行处理。如：在原文档中出现“襟翼制动指令为有效”，则将其当作条件填写到条件表中。另外，在原文档中常将最后的取值设定在区间内，这种情况下将其控制条件作为条件进行处理。还有一些特殊情况需要在特定的情况下分析。

6.4 需求中变量间的对应关系原则

在 SCR 方法中，监控变量对应输入变量，控制变量对应输出变量，这种关系并不一定是一一对应的。如：在襟翼电机转速控制模块中，硬件故障输入变量不对应任何的监控变量。因为在系统的需求说明阶段讨论的是系统在理想状态下的正常行为，暂时忽略模块的硬件故障，所以故障变量在需求分析的后期引入，不对应监控变量。在另外一些情况下，监控与输入变量、受控与输出变量之间可能有复杂的转化关系，如需要对几个控制器输出的控制变量进行分析和综合以得到受控变量。大部分监控与输入变量、受控与输出变量之间存在一一对应关系。

为了遵循信息隐藏的原则，不直接使用输出变量的值来表示受控变量。直接用输出变量暴露了系统使用的特定硬件输出装置的信息，这不利于系统出现问题时的更改，也使得系统设计不够灵活。采用该措施的另一个原因是：便于开发。可以先确定系统的非设备依赖关系 *REQ*，然后建立系统的设备依赖关系 *D_IN*，对 *D_OUT* 关系进行解释说明，*D_IN* 关系和 *D_OUT* 关系并不对 *REQ* 关系进行更改。

结束语 本文针对 SCR 方法过于通用及缺少对具体的机载系统进行分析的问题，提出了使用 SCR 方法对襟缝翼控制系统中的襟翼电机转速控制模块进行需求描述以满足需求的一致性、完备性、正确性等特性的方法。通过案例分析，总结了将自然语言的需求描述转化为 SCR 描述的方法。在 SCR 方法中变量使用符号表示，变量间的关系通过逻辑描述，需求使用表格来表示，使得需求中的错误易于发现，便于检查需求的一致性、完备性与正确性。由于本文的需求描述是基于原自然语言文档进行改写的，因此对原文档中缺少的内容没有完全补充。接下来，将利用 T_VEC 工具将基于 SCR 的需求描述转化为 NuSMV，以进行形式化验证。

参 考 文 献

[1] CHEN X, WANG H, MU M. Software requirement development method research for DO-178B request[J]. Computer Engineering & Design, 2012, 33(7): 2673-2677. (in Chinese)
陈鑫，王辉，牟明. 满足 DO-178B 要求的软件需求开发方法[J]. 计算机工程与设计，2012，33(7)：2673-2677.

[2] ZHANG X, LI T, WANG X, et al. Formal Analysis to Non-Functional Requirements of Trustworthy Software[J]. Journal of Software, 2015, 26(10): 2545-2566. (in Chinese)
张璇，李彤，王旭，等. 可信软件非功能需求形式化表示与可满足分析[J]. 软件学报，2015，26(10)：2545-2566.

[3] LEVESON N G, HEIMDAHL M P E, HILDRETH H, et al. Requirements Specification for Process-Control Systems[J]. IEEE Transactions on Software Engineering, 1994, 20(9): 684-707.

[4] PARNAS D L, MADEY J. Functional documents for computer Systems[J]. Science of Computer Programming, 1995, 25(1): 41-61.

[5] GALLOWAY A, IWU F, MCDERMID J, et al. On the Formal Development of Safety-Critical Software[C]// First IFIP TC 2/WG 2.3 Conference(VSTTE 2005). Zurich, Switzerland, 2005: 10-13.

[6] HU J, SHI J J, CHENG Z, et al. System Safety Modeling and Analysis Method Based on Four-variable Model[J]. Computer Science, 2016, 43(11): 193-199. (in Chinese)
胡军，石娇洁，程桢，等. 一种基于四变量模型的系统安全性建模与分析方法[J]. 计算机科学，2016，43(11)：193-199.

[7] HESTER S D, PARNAS D L, UTTER D F. Using Documentation as a Software Design Medium[J]. Bell Labs Technical Journal, 1981, 60(8): 1941-1977.

[8] PARNAS D L, MADEY J, ASMIS G J K. Assessment of safety-critical software in nuclear power plants[J]. Nuclear Safety, 1991, 32(2): 189-198.

[9] FAULK S, BRACKETT J, WARD P, et al. The Core method for real-time requirements[J]. IEEE Software, 1992, 9(5): 22-33.

[10] FAULK S, FINNERAN L, KIRBY J J, et al. Experience applying the CoRE method to the Lockheed C-130J software requirements[C]// Ninth Conference on Computer Assuranace, Compass 94 Safety, Reliability, Fault Tolerance, Concurrency & Real Time. IEEE, 1994: 3-8.

[11] CHEN G Y, HUANG Z Q, CHEN Z, et al. Safety Analysis of Slat and Flap Control Unit for DO-333[J]. Computer Science, 2016, 43(5): 150-156. (in Chinese)
陈光颖，黄志球，陈哲，等. 面向 DO-333 的襟缝翼控制单元安全性分析[J]. 计算机科学，2016，43(5)：150-161.

[12] PARNAS D L. From Requirements to Architecture[J]. Frontiers in Artificial Intelligence & Applications, 2010, 217: 3-36.

[13] LEVESON N G, HEIMDAHL M P E, REESE J D. Designing Specification Languages for Process Control Systems: Lessons Learned and Steps to the Future[C]// European Software Engineering Conference. ACM. 1999: 127-145.

[14] BABER R L, PARNAS D L, VILKOMIR S A, et al. Disciplined Methods of Software Specification: A Case Study[C]// International Conference on Information Technology: Coding and Computing. IEEE, 2008: 428-437.

[15] HEITMEYER C, BHARADWAJ R. Applying the SCR Requirements Method to the Light Control Case Study[J]. Journal of Universal Computer Science, 2000, 6: 2000.

[16] ZHENG J, HUANG Z Q, XU B F. Current progress and prospects of airworthiness certification standards in airborne software[J]. Computer Engineering & Design, 2012, 33(1): 204-208. (in Chinese)
郑军，黄志球，徐丙凤. 机载软件适航认证标准新进展及展望[J]. 计算机工程与设计，2012，33(1)：204-208.