

# 面向驾驶舱显示系统需求的形式化建模与分析

战芸娇<sup>1</sup>, 魏 欧<sup>1</sup>, 胡 军<sup>1</sup>, 王立松<sup>1</sup>, 谷青范<sup>2</sup>

(1. 南京航空航天大学 计算机科学与技术学院, 江苏 南京 211106;

2. 中国航空无线电电子研究所, 上海 200000)

**摘 要:** 在实际的工程项目中, 需求错误普遍发生, 对系统的安全有着很大的影响。对复杂的系统需求进行建模分析与检测, 找出其中的错误仍然面临着很大的挑战。驾驶舱显示系统负责显示飞机的状态信息, 并直接为飞行员提供飞行导引。保证驾驶舱显示系统需求的完整、一致和准确是飞机正常和安全运行的重要基础和保障。对此, 提出了一种针对复杂系统需求的一致性和完备性描述方法, 帮助检测需求中存在的错误。其中, 根据四变量模型和表格符号表示以驾驶舱显示系统为例建立需求模型; 在建立的需求模型的基础上, 为需求模型提供精确的语义; 最后, 使用 T-VEC 工具对需求模型进行检测。通过使用该方法对驾驶舱显示系统需求文档进行一致性和完备性检测, 找出了需求模型中的潜在错误。

**关键词:** 驾驶舱显示系统; 需求工程; 一致性和完备性检测; 四变量模型; 表格符号; 形式化方法; T-VEC 工具

中图分类号: V241.8; TP311.5

文献标识码: A

文章编号: 1673-629X(2018)03-0020-06

doi: 10.3969/j.issn.1673-629X.2018.03.005

## Formal Modeling and Analysis of Cockpit Display System Requirements

ZHAN Yun-jiao<sup>1</sup>, WEI Ou<sup>1</sup>, HU Jun<sup>1</sup>, WANG Li-song<sup>1</sup>, GU Qing-fan<sup>2</sup>

(1. School of Computer Science and Technology, Nanjing University of

Aeronautics and Astronautics, Nanjing, 211106, China;

2. China Aviation Radio Electronics Research Institute, Shanghai 200000, China)

**Abstract:** In the actual project, the requirements for errors generally occur, which produce a great influence on the security of the system. It is still a challenge to identify the errors by modeling analysis and testing for the complex system requirements. The cockpit display system is responsible for displaying the status information of the aircraft and providing flight guides directly to the pilot, so it is an important foundation and guarantee for the normal and consistent operation of the cockpit to show the complete, consistent and accurate requirements of the aircraft. For this, we present a consistency and completeness description method for complex system requirements to help detect errors in requirements. According to the four-variable model and the table symbol, the demand model is established with the cockpit display system as an example, based on which the requirements semantics are provided for the demand model. Finally, the requirements model is tested by the tool of T-VEC. By using this method to verify the consistency and completeness of the cockpit display system requirements document, the potential errors in the requirements model are found out.

**Key words:** cockpit display system; requirement engineering; consistency and completeness checking; four-variable model; table symbol; formal methods; T-VEC tool

## 1 概 述

需求分析是软件开发流程中的第一步, 也是最重要的一步。在航空航天领域等实际的安全关键系统中, 由于需求的复杂性、缺乏统一的需求模型、需求描

述的结构混乱和语言歧义等原因<sup>[1]</sup>, 往往造成需求中存在大量的不一致和不完备。相关研究表明, 在系统维护阶段修改所发现的需求错误所需要的工作量, 大约是更改需求分析阶段发现的错误所需的工作量的 200 倍<sup>[2]</sup>。因此, 减少需求中的错误至关重要, 不仅能

收稿日期: 2017-04-06

修回日期: 2017-08-10

网络出版时间: 2017-12-05

基金项目: 国家“973”重点基础研究发展计划项目(2014CB744901); 国家自然科学基金(61170043)

作者简介: 战芸娇(1993-), 女, 硕士研究生, CCF 会员(72613G), 研究方向为形式化方法、需求分析; 魏 欧, 博士, 副教授, 研究方向为形式化方法、软件自动验证; 胡 军, 博士, 副教授, 研究方向为软件工程、形式化方法和软件自动验证; 王立松, 副教授, 研究方向为系统软件。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20171205.0903.018.html>

够保证系统的安全性,也可以减少系统开发的成本。

驾驶舱显示系统<sup>[3]</sup> (cockpit display system) 是驾驶员和飞机进行信息交互重要的机载系统。通过将传统的飞行仪表信息进行数字化综合处理,驾驶舱显示系统采用多种显示器按需展现各种不同数据,如主飞行显示器、导航显示器等,增强了驾驶员的态势感知能力,简化了对飞机的操纵导航,使得驾驶员能够专注于最为相关的信息,降低飞行成本。

机载软件<sup>[4-5]</sup> 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。在显示系统广泛应用的同时,在实际中也时常发生由于显示系统错误而引起安全事故。例如,2005年8月1日,马来西亚航空公司的一架波音777-200ER从珀斯飞回吉隆坡,期间主飞行显示器(PFD)的速度显示区域发生显示了飞机同时接近高速极限值和低速极限值的冲突信息,致使飞行员立即解除自动驾驶并紧急降落在珀斯<sup>[6]</sup>。这些事故都造成了生命、财产等的重大损失,影响巨大。对于驾驶舱显示系统而言,为保障驾驶员能够对飞机飞行中的状况做出正确的判断、避免事故的发生,在开发早期发现需求中存在的错误,可以减少需求错误对系统造成的影响,提高系统的安全性。因此,对驾驶舱显示系统的需求进行严格的定义和分析以及错误检测显得尤为重要。

针对驾驶舱显示系统这样特定应用的系统需求,需要判定其是否满足一致性和完备性。从广义上来说,一致性保证需求中不存在矛盾的信息,完备性保证需求中必须包含那些对于系统正常工作、保证系统安全所必要的信息。因此,应检测需求中是否存在以下问题:

(1) 检测出需求中未定义的显示情况,即完备性问题。目的是避免显示器上出现需求中没有定义的某种显示信息。

(2) 检测出需求中出现的显示不确定性问题,即一致性问题。目的是避免显示器上出现矛盾的信息显示。

(3) 检测出需求中缺失的并且影响系统安全的信息,如数据的时间边界、数据的有效性等。

T-VEC工具是对复杂系统的需求阶段进行错误检测与验证,并对设计阶段进行仿真的工具。1989年以来,其广泛应用在飞机领域的安全关键性系统、实时系统和许多嵌入式系统中。文中主要利用T-VEC的测试向量生成工具,对表格式需求进行测试验证。通过对变量和条件等相关需求模型的输入,对需求进行编译,以检测需求中的各种错误和特性。

针对以上问题,为了找到驾驶舱显示系统这样的安全关键系统需求中的错误,就需要一套完整的方法来对需求进行一致性和完备性检测工作。文中以四变量模型为基础,提出了具体的建立驾驶舱显示系统的需求模型的方法,包括对需求描述方式和严格的语义,支持需求的一致性和完备性的T-VEC检测工具。

## 2 四变量模型

四变量模型<sup>[7-9]</sup> (four-variable model) 是由Parnas提出来的用以指明需求的方法,如图1所示。

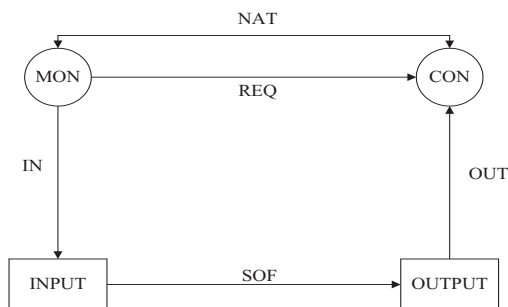


图1 四变量模型

四变量模型中的变量是时间连续型函数,分为四类变量:

(1) 监督变量(monitored variables, MON): 系统需要观测的外部环境量;

(2) 受控变量(controlled variables, CON): 受系统控制的环境量;

(3) 输入变量(input variables, INPUT): 由传感器等输入设备将监督变量转换而来的变量;

(4) 输出变量(output variables, OUTPUT): 发送到输出设备上的、改变受控变量的变量。

例如,监督变量可以是飞机在飞行中的飞行高度和飞行速度,受控变量可以是显示仪表盘上飞行高度和飞行速度值的显示;相应的输入输出变量可以是软件读入的、写出的ARINC-429总线上的数据。

在这些变量上,定义了4种数学关系:

(1) NAT: 施加在环境量上的自然限制,例如飞机的最大爬升率;

(2) REQ: 定义了系统需求,指明受控变量与监督变量的关系。系统需求REQ是可行的,当且仅当REQ中考虑了NAT中的所有环境限制条件。

(3) IN: 描述了监督变量和输入变量之间的关系。IN模拟了输入硬件接口,如传感器和模数转换器;

(4) OUT: 描述输出变量和受控变量之间的关系。OUT模拟了输出硬件接口,如数模转换器和作动器。

## 3 驾驶舱显示系统的需求模型

结合驾驶舱显示系统的特点,利用四变量模型框

架找出需求中的变量和关系,再利用表格符号的形式将需求中的关系表示出来,建立需求模型。

### 3.1 需求的组成

对系统进行准确的描述从而形成需求,意味着需要确定系统、子系统和组件的行为(并无必要知道行为是如何具体实现的)。Parnas 最初提出的四变量模型是用来准确描述系统需求、并形成相应需求文档的方法。

针对驾驶舱显示系统中输入变量对显示信息的影响——一组输入变量取值情况对同一显示造成的影响不同,且这些变量之间存在依赖关系,对输入变量进行分类。在驾驶舱显示系统上所显示的信息包括两类:一类是数值、文本或图形信息,另一类是数值、文本或图形的样式信息(如颜色和字体)。将驾驶舱显示系统需求的输入变量分为显性变量(explicit variables)和隐性变量(implicit variables)。显性变量:参数(输入变量)的值直接决定了显示器上数值、文本或图形信息的显示;隐性变量:参数的值仅仅影响数值、文本或图形的显示样式。其中,显性变量和隐性变量对系统安全造成的影响有所不同,显性变量失效直接造成显示器上相关区域的读数/文本、图形信息为空,飞行员无法从显示器上得知任何有关飞机的状态信息,而隐性变量仅仅影响了显示器上显示信息的样式;隐性变量在显示器上的显示依赖于显性变量的有效性/取值情况,只有在显性变量有效且取特定值情况下,隐性变量的取值情况才会对显示信息造成影响。

另外,为了更好地利用四变量模型准确描述驾驶舱显示系统需求,以使用表格符号对需求中的关系进行表示,需要提供两种额外的结构:条件(condition)和事件(events)。条件是定义在系统输入和输出上的谓词;当两个或多个隐性变量之间的大小关系发生变化,就表示一个事件发生。

图 2 是结合显示系统的体系结构<sup>[10]</sup>,参考四变量模型,描述驾驶舱显示系统需求的结构概念图。其中,传感器(sensor)采集外部环境的监督变量(monitor variables),将其转换成系统可识别的输入变量,并传递给显示系统控制单元;子系统(subsystem)采集来自系统内部的监督变量——飞机系统自身的状态信息,如:FADEC 采集引擎参数和控制引擎,通过转换传递给显示系统控制单元;cockpit display controller unit 表示处理从传感器和其他子系统传递而来的参数的处理单元,一方面,它将处理后的显示信息指令传递给显示单元,另一方面,将产生的指令反馈给自身(如图中黑色箭头所示),作为系统内部其他功能的控制条件;cockpit display unit 表示显示单元,接收来自处理单元处理后产生的显示信息指令,并在显示器上给予特定的

显示。

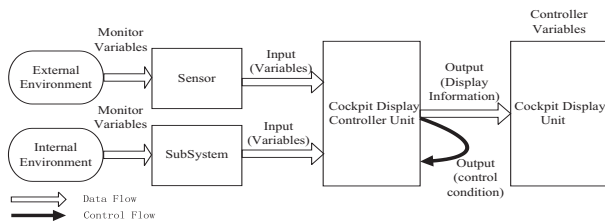


图 2 驾驶舱显示系统需求结构概念图

### 3.2 需求的表格符号表示

系统开发工程师发现:利用表格表示需求<sup>[11]</sup>,不仅有利于开发人员对系统的理解和开发,还能将大量的需求信息准确地表示出来<sup>[12]</sup>。因此,在利用四变量模型找出系统需求中存在的各个组件和变量的基础上,利用表格符号<sup>[13]</sup>来表示需求中变量之间的关系。鉴于驾驶舱显示系统内部各个组件的功能不同,分别定义不同的表格予以表示:对于传感器和子系统,这两种组件都是将监督变量(来自内部环境和外部环境)转换成显示系统控制单元可识别的量,因此,定义输入映射表(mapping table of input)作为监督变量和输入变量的对应关系;对于显示单元,它接收来自显示控制单元的输变量(显示指令),并控制显示单元的受控变量的显示,因此,定义输出映射表(mapping table of output)作为输出变量和受控变量的对应关系;对于驾驶舱显示系统控制单元到显示单元的特殊性——在不同的显示逻辑下,将从传感器和其他子系统传递而来的参数,在显示单元上予以相应的显示——定义三种表格:映射表(mapping table)、事件表(event table)和条件表(condition table)。这三种表格都对应了四变量模型中的 SOF,而且,这里的显示控制单元的输变量是与受控变量有关的,每一个表格中的输出变量(输出变量组)都唯一对应一个受控变量。映射表:与受控变量相关的输出变量的取值情况由输入变量的取值情况确定;事件表:与受控变量相关的输出变量的取值情况取决于输入变量的取值情况和所发生的事件;条件表:与受控变量相关的输出变量的取值情况取决于输入变量的取值情况和当前的条件。除此之外,还需要定义输入变量表格(input table)和输出变量表格(output table),确定输入和输出变量的类型、取值范围,不仅有利于查看系统中所有的输入和输出变量,还方便后续对需求的一致性和完备性检测工作。

## 4 需求模型的语义

上一节,通过参考四变量模型,利用表格符号,将用自然语言描述的需求转换成表格符号表示的需求,建立需求模型。接下来,需要为需求模型提供精确的语义<sup>[14]</sup>。这里的需求模型,对于 SOF,定义了输出根



据输入或者输入、条件(事件)的改变而发生的变化;描述了从表格中导出的表格函数(table function)—表格符号的形式化表示。这些表格函数不仅定义了从输入到输出或者输入、条件(事件)到输出的映射关系,还定义了监督变量和输入变量、输出变量和受控变量的映射关系。定义一个七元组  $(MV, CV, D, C, E, F, VS)$  来表示该需求模型,其中  $D$  表示数据项,包含输入和输出变量,  $D = \{IP, OP\}$ , 输入变量分为显性变量和隐性变量,即  $IP = \{EX\_IP, IM\_IP\}$ 。

为了阐述形式化模型,有关元组的定义如下:

(1)七元组元素:模型中的监督变量、输入、输出和受控变量,以及条件、事件、输入输出的取值范围。定义以下集合:

$MV$ :非空的不相交的监督变量集合,  $MV = \{mv_1, mv_2, \dots, mv_l\}$ ,  $mv_1, mv_2, \dots, mv_l$  称为监督变量;

$CV$ :非空的不相交的受控变量集合,  $CV = \{cv_1, cv_2, \dots, cv_k\}$ ,  $cv_1, cv_2, \dots, cv_k$  称为受控变量;

$IP$ :非空的不相交的输入变量集合,  $IP = \{ip_1, ip_2, \dots, ip_l\}$ ,  $ip_1, ip_2, \dots, ip_l$  称为输入;

$OP$ :非空的不相交的输出变量集合,  $OP = \{op_1, op_2, \dots, op_m\}$ ,  $op_1, op_2, \dots, op_m$  称为输出;

$VS$ :表示输入输出变量的所有取值范围。假设  $r$  代表输入或者输出变量,那么其取值范围为  $VS(r)$ ;

$C$ :条件,条件是定义在输入或输出上的谓词。条件,如真、假或者逻辑表达式  $r \odot r'$  或  $r \odot a$ , 其中  $r, r'$  表示输入、输出变量,  $a$  表示常数值,  $\odot \in \{=, <, >, \neq, \geq, \leq\}$  表示关系操作符;

$E$ :事件,两个或多个隐性变量值大小关系的变化,用  $e$  表示,如隐性变量值的改变表示一个事件  $e: (im\_ip_i - im\_ip'_i = v) \wedge (im\_ip_i - im\_ip'_i = v')_{now}$ , 其中  $im\_ip_i - im\_ip'_i = v$  表示上一时刻  $im\_ip_i - im\_ip'_i$  的差值为  $v$ , 而  $(im\_ip_i - im\_ip'_i = v')_{now}$  表示当前时刻输入变量  $im\_ip_i - im\_ip'_i$  的差值为  $v'$ , 此时,  $v - v'$  增大减小的大小情况便是一个事件;

$F$ :系统功能,在第3节中,所有的组件的功能都可以用表格表示,这些表格都描述成表格函数  $f_i$ 。

(2)输入映射表:该表格描述了所有的监督变量到所有的输入变量的映射关系  $f_{MI}: MV \rightarrow IP$ , 准确地定义  $\rho_{MI} = \{(mv_i, ip_i) \in MV \times IP\}, i = 1, 2, \dots, n$ ,  $\rho_{MI}$  必须满足:

(a)对于任意的监督变量都存在唯一( $\exists!$ )的输入变量与其对应,  $\forall mv_i \exists! ip_i: ip_i = f_{MI}(mv_i)$ ;

(b)对于任意的输入变量只存在唯一的监督变量与其对应。

(3)输出映射表:该表格描述了所有的输出变量到所有的受控变量的映射关系  $f_{OC}: OP \rightarrow CV$ , 准确地

定义  $\rho_{OC} = \{((op_i, \dots, op_j), cv_i) \in OP \times CV\}; i, j = 1, 2, \dots, n$ , 关系  $\rho_{OC}$  必须满足:

(a)对于任意的输出变量都存在唯一( $\exists!$ )的受控变量与其对应,  $\forall op_i \exists! cv_i: cv_i = f_{MI}(op_i)$ ;

(b)同一个受控变量可能对应多个输出变量。

(4)受控变量  $CV$  映射表:在输入变量取值不同情况下,相对应的输出变量取值情况。准确地定义  $\rho_i = \{(\cup IP_{i,k}, \cup OP_{i,k}) \in \cup VS(IP_i) \times \cup VS(OP_i)\}, k = 1, 2, \dots, n$ 。其中  $\cup VS(IP_i)$  作为与受控变量  $cv$  相关的所有输入组成的输入变量组取值情况的集合,  $\cup VS(OP_i)$  作为与  $cv$  相关的所有输出组成的输出变量组取值情况的集合,  $IP_{i,k}$  表示单个输入变量  $IP_i$  的取值。关系  $\rho_i$  必须满足以下属性:

(a)所有输入变量的任意取值组合情况  $\bigcup_{k=1}^s IP_{i,k}$  都包含在表格中,即对于所有的  $k$ ,  $(IP_{i,k} \in VS(IP_i)) \wedge (\bigcup_{k=1}^s IP_{i,k} = VS(IP_i))$ ;

(b)所有输出变量的可能取值组合情况  $\bigcup_{k=1}^t OP_{i,k}$  都包含在表格中,即对于所有的  $k$ ,  $(OP_{i,k} \in VS(OP_i)) \wedge (\bigcup_{k=1}^t OP_{i,k} = VS(OP_i))$ ;

(c)在所有输入变量的任意取值组合情况  $\bigcup_{k=1}^s IP_{i,k}$  确定的情况下,在所有输出变量内,存在唯一的取值组合情况  $\bigcup_{k=1}^t OP_{i,k}$  与其对应;

(d)在所有输出变量的任意取值组合情况  $\bigcup_{k=1}^t OP_{i,k}$  确定的情况下,在所有输入变量内,存在唯一的取值组合情况  $\bigcup_{k=1}^s IP_{i,k}$  与其对应。

为了明确具体的输出和输入之间的关系,用表格函数  $f_i$  替换关系  $\rho_i$ , 其中属性(a)、(b)、(c)保证了  $f_i$  是一个函数,属性(c)、(d)保证了  $f_i$  是双射:

$$OP_i = f_i(IP_i) = \begin{cases} OP_{i,1}, & \text{if}(IP_i = IP_{i,1}) \\ OP_{i,2}, & \text{if}(IP_i = IP_{i,2}) \\ \vdots \\ OP_{i,n}, & \text{if}(IP_i = IP_{i,n}) \end{cases} \quad (1)$$

(5)受控变量  $CV$  条件表:在输入变量取值不同的情况下,输出变量的取值情况。准确地定义  $\rho_i = \{((\cup IP_{i,k}, c_{i,j}), \cup OP_{i,k}) \in (\cup VS(IP_i) \times \{C_{i,1}, C_{i,2}\}) \times \cup VS(OP_i)\}, k = 1, 2, \dots, n; j = 1, 2$ 。其中  $C_i$  是与受控变量相关的条件,  $c_{i,j}$  表示保证条件  $C_i$  的真假情况。关系  $\rho_i$  必须满足以下属性:

(a)所有输入变量的任意取值组合情况  $\bigcup_{k=1}^s IP_{i,k}$  都包含在表格中,即对于所有的  $k$ ,  $(IP_{i,k} \in VS(IP_i)) \wedge (\bigcup_{k=1}^s IP_{i,k} = VS(IP_i))$ ;

(b)表格中,在所有输入变量取值组合确定的情况下一 $\bigcup_{k=1}^s IP_{i,k}$ ,条件 $C_i$ 取值确定的情况下一 $c_{i,j}$ ,与其对应的所有输出变量取值集合 $\bigcup_{k=1}^t OP_{i,k}$ 必须唯一确定;

(c)表格中,特定条件下,在所有输出变量的任意取值组合情况 $\bigcup_{k=1}^t OP_{i,k}$ 确定的情况下,在所有输入变量内,存在唯一的取值组合情况 $\bigcup_{k=1}^s IP_{i,k}$ 与其对应;

(d)表格中,在所有输入变量取值确定的情况下,其对应的条件 $C_i$ 的所有取值情况 $c_{i,j}$ 都包含在表格内,因为 $C_i$ 只可以取布尔值,所以对于任意的 $i:c_{i,1}=T \wedge c_{i,2}=F$ ;

(e)所有输出变量的可能取值组合情况 $\bigcup_{k=1}^t OP_{i,k}$ 都包含在表格中,即对于所有的 $k$ , $(OP_{i,k} \in VS(OP_i)) \wedge (\bigcup_{k=1}^t OP_{i,k} = VS(OP_i))$ 。

用表格函数 $f_i$ 替换关系 $\rho_i$ ,其中属性(a)、(c)、(d)、(e)保证 $f_i$ 是一个函数,属性(b)、(c)保证 $f_i$ 是双射:

$$OP_i = f_i (IP_i, C_i) = \begin{cases} OP_{i,1}, \text{if}(IP_i = IP_{i,1} \wedge C_i = c_{i,1}) \\ OP_{i,2}, \text{if}(IP_i = IP_{i,2} \wedge C_i = c_{i,2}) \\ \vdots \\ OP_{i,n}, \text{if}(IP_i = IP_{i,n} \wedge C_i = c_{i,n}) \end{cases} \quad (2)$$

(6)受控变量 CV 事件表:在发生事件的情况下,输入变量取值如何影响与受控变量相关的输出变量的取值。由于事件表同条件表类似,只是将条件替换为事件,因此不再赘述。

5 案例分析

引擎指示和机组警告系统<sup>[15]</sup> (engine-indicating

and crew-alerting system, EICAS) 是为飞机机组显示提供飞机引擎和其他系统运转情况的综合显示系统。

EICAS 通常包含多种引擎参数显示仪表,如引擎转速、引擎温度、燃料流速和燃料量、油压等。被 EICAS 系统监督的其他飞机系统包括液压、气动、电力、除冰系统、飞行操作系统等。EICAS 是驾驶舱显示系统的重要组成部分,以软件驱动的电子系统取代了原有的模拟仪表装置,其大部分显示区域用作导航和定位显示。机组警告系统 (CAS) 用来取代旧式系统中的信号指示面板,CAS 不再单单以亮起指示灯来显示系统故障,而是在 EICAS 的指示区域显示一系列的信息来告知机组人员系统故障。

表 1 是驾驶舱显示系统中 EICAS 需求的一部分 (由于篇幅原因,并没有将完整的需求文档内容进行展示,展示的是用表格符号表示后的需求)。它是关于引擎推力模式显示的条件表:在飞机飞行的不同阶段,飞机引擎的推力模式不同,EICAS 系统通过接收从其他相关子系统传递来的参数,根据参数的取值情况确定并显示当前引擎推力的模式。其中,ipFADECEngineNormalTOSelected 代表引擎正常全推力起飞模式是否被选中的参数,当参数取值为 True 时代表被选中(下同);ipFADECEngineFlexTOSelected 代表非全推力起飞模式是否被选中的参数;ipFADECEngineNormalCLBSelected 代表飞机是否处于全推力爬升模式的参数;ipFADECEngineCruiseSelected 代表飞机引擎是否以巡航模式运作的参数;ipFADECEngineGASelectd 代表飞机引擎是否以复飞模式运作的参数;ipFADECEngineMCTSelected 代表飞机引擎是否以最大连续推力模式运作的参数;ipFADECEngineTO1DerateSelected 代表飞机是否以减推力模式 1 起飞的参数;ipFADECEngineTO2DerateSelected 代表飞机是否以减推力模式 2 起飞的参数;条件 Reduced thrust

表 1 引擎推力模式 cvThrustMode 条件表

参数		Value( OR )							
Input	ipFADECEngineNormalTOSelected	T	F	F	F	F	F	F	F
	ipFADECEngineFlexTOSelected	F	T	F	F	F	F	F	F
	ipFADECEngineNormalCLBSelected	F	F	F	F	T	F	F	F
	ipFADECEngineCruiseSelected	F	F	F	F	F	F	T	F
	ipFADECEngineGASelectd	F	F	F	F	F	F	F	T
	ipFADECEngineMCTSelected	F	F	F	F	F	T	F	F
	ipFADECEngineTO1DerateSelected	F	F	T	F	F	F	F	F
	ipFADECEngineTO2DerateSelected	F	F	F	T	F	F	F	F
Condition	Reduced thrust takeoff	T							
Output	opText_cvThrustMode	TO	FLEX-TO	D-TO1	D-TO2	CLB	CON	CRZ	G/A
	opFont_cvThrustMode	Small							
	opColor_cvThrustMode	Green 100							

takeoff 代表减推力起飞模式是否被选择;输出项的模式文本显示 opText\_cvThrustMode 取值:TO(正常全推力起飞)、FLEX-TO(非全推力起飞)、D-TO1(减推力模式1起飞)、D-TO2(减推力模式2起飞)、CLB(全推力爬升模式)、CON(连续最大推力飞行模式)、CRZ

$$\begin{aligned} (op_i, cv_i) &= f_i(ip_1, ip_2, \dots, ip_8, c_i) = \\ \left\{ \begin{array}{ll} \text{'TO'} & \text{if}(ip_1 = T \wedge ip_2 = F \wedge ip_3 = F \wedge ip_4 = F \wedge ip_5 = F \wedge ip_6 = F \wedge ip_7 = F \wedge ip_8 = F) \wedge RTT = T \\ \text{'FLEX-TO'} & \text{if}(ip_1 = F \wedge ip_2 = T \wedge ip_3 = F \wedge ip_4 = F \wedge ip_5 = F \wedge ip_6 = F \wedge ip_7 = F \wedge ip_8 = F) \wedge RTT = T \\ \text{'D-TO1'} & \text{if}(ip_1 = F \wedge ip_2 = F \wedge ip_3 = T \wedge ip_4 = F \wedge ip_5 = F \wedge ip_6 = F \wedge ip_7 = F \wedge ip_8 = F) \wedge RTT = T \\ \text{'D-TO2'} & \text{if}(ip_1 = F \wedge ip_2 = F \wedge ip_3 = F \wedge ip_4 = T \wedge ip_5 = F \wedge ip_6 = F \wedge ip_7 = F \wedge ip_8 = F) \wedge RTT = T \\ \text{'CLB'} & \text{if}(ip_1 = F \wedge ip_2 = F \wedge ip_3 = F \wedge ip_4 = F \wedge ip_5 = T \wedge ip_6 = F \wedge ip_7 = F \wedge ip_8 = F) \wedge RTT = T \\ \text{'CON'} & \text{if}(ip_1 = F \wedge ip_2 = F \wedge ip_3 = F \wedge ip_4 = F \wedge ip_5 = F \wedge ip_6 = T \wedge ip_7 = F \wedge ip_8 = F) \wedge RTT = T \\ \text{'CRZ'} & \text{if}(ip_1 = F \wedge ip_2 = F \wedge ip_3 = F \wedge ip_4 = F \wedge ip_5 = F \wedge ip_6 = F \wedge ip_7 = T \wedge ip_8 = F) \wedge RTT = T \\ \text{'G/A'} & \text{if}(ip_1 = F \wedge ip_2 = F \wedge ip_3 = F \wedge ip_4 = F \wedge ip_5 = F \wedge ip_6 = F \wedge ip_7 = F \wedge ip_8 = T) \wedge RTT = T \end{array} \right. \quad (3) \end{aligned}$$

其中,  $ip_1, ip_2, \dots, ip_8$  表示输入变量;RTT 表示条件 Reduced Thrust Takeoff;  $op_1, op_2, op_3$  表示输出变量。

根据第4节中定义的表格所要满足的属性,利用 T-VEC 工具对函数  $f_i$  进行检测(为了简便,用  $IP_{i,k}$ ,  $IP_{i,j}$  分别表示输入变量集合  $\{ip_1, ip_2, \dots, ip_8\}$  内所有输入变量的一种取值情况;用  $OP_{i,k}$ ,  $OP_{i,j}$  分别表示输出变量集合  $\{op_1, op_2, op_3\}$  内所有输出变量的一种取值情况;用  $c_{1,1}$  表示条件为真),发现对于任意的  $OP_{i,k}$ ,  $OP_{i,j}$ ,  $k, j \in [1, 2, \dots, 8]$ ,  $k \neq j$ , 其相应逻辑表达式为  $IP_{i,k} \wedge c_{1,1} \rightarrow OP_{i,k}$ ,  $IP_{i,j} \wedge c_{1,1} \rightarrow OP_{i,j}$ , 且  $((IP_{i,k} == IP_{i,j}) \wedge (c_{1,1} \wedge c_{1,1})) \neq \text{True}$ , 将对应的变量和变化关系输入到 T-VEC 中进行检测,编译通过,并没有错误报出,说明引擎推力模式显示的条件表满足输出的一致性。然而,将输入变量取值情况  $\bigcup_{i=1}^8 IP_{i,k} \neq \text{VS}(IP_i)$ ,  $k = 1, 2$  输入到 T-VEC 工具中, T-VEC 给出了警告,表示还存在未考虑的输入变量取值组合情况,无法通过测试向量的生成;且在条件中,表函数也只考虑了  $RTT = \text{True}$  的情况,并未考虑  $RTT = \text{False}$  的情况,因此引擎推力模式显示的条件表不满足输入的完备性。

## 6 结束语

需求的一致性和完备性对于系统的安全性起着至关重要的作用。找出需求中存在的错误,避免其对系统造成的不良影响,可以提高系统的安全性。传统的人工方法对需求进行检查和评审,不仅费时费力,而且容易忽略需求中存在的错误。利用 Parnas 提出的四变量模型作为指导框架确定驾驶舱显示系统的需求组成和关系,并用表格符号将需求进行表示,建立需求模型;运用形式化方法为需求模型定义精确的语义,并利用 T-VEC 工具进行检测。通过这一系列的工作,不

(巡航模式)、G/A(复飞模式), opFont\_cvThrustMode 为输出模式文本的字体, opColor\_cvThrustMode 为输出模式文本的颜色。

该条件表所表示的函数如下所示:

仅可以准确地描述需求,而且找出了需求中存在的错误。

在将来的工作中,计划开发出一个支持 T-VEC 工具到符号化模型检测语言 NuSMV 的自动化工具,支持需求的安全性检测,找出需求中存在的安全错误,从而产生高质量的需求。这样的高质量需求,可以减少需求错误对系统的影响,提高系统的安全性。同时,自动化工具也减少了系统开发的成本。

## 参考文献:

- [1] VERAS P C, VILLANI E, AMBROSIO A M, et al. Errors on space software requirements: a field study and application scenarios[C]//IEEE international symposium on software reliability engineering. [s. l.]:IEEE,2010.
- [2] BOEHM B W. Software engineering economics[J]. IEEE Transactions on Software Engineering, 1984, 10(1):4-21.
- [3] ZHOU Y, ZHUANG D, ZHANG L, et al. Study on ergonomics evaluation method of the cockpit display system[C]//IEEE international conference on computer-aided industrial design & conceptual design. [s. l.]:IEEE,2010.
- [4] GALLOWAY A, IWU F, MCDERMID J, et al. On the formal development of safety-critical software[M]//Verified software: theories, tools, experiments. Berlin: Springer-Verlag, 2005:362-373.
- [5] 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.
- [6] 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):150-156.
- [7] PARNAS D L, MADEY J. Functional documents for computer systems[J]. Science of Computer Programming, 1995, 25(1):41-61.
- [8] PARNAS D L. From requirements to architecture[C]//New

综上,在动态多文档文摘领域,动态流行排序思想值得研究,是一种有效的动态多文档文摘方法。

4 结束语

在认真研究国内外多文档文摘领域最新发展的基础上,创新性地对动态内容的演化关系进行了差异性分析。考虑到文摘句的信息新颖度和信息显著度对文摘的重要性,运用流行排序思想整合信息新颖度和信息显著度对句子集合中所有句子进行排序,根据排序值抽取句子形成文摘。同时融入对句子历史信息特征的惩罚和时间特征的奖励后,还能实现对文档集所含信息动态演化性的建模,使文摘具有动态性,对于推动动态多文档文摘领域的发展起到了一定的作用。下一步将是研究如何与其他模型更好地融合,使动态文摘具有更好的显著性和新颖性。

参考文献:

[1] NENKOVA A, MASKEY S, LIU Y. Automatic summarization [C]//Proceedings of the 49th annual meeting of the association for computational linguistics. Stroudsburg, PA, USA: Association for Computational Linguistics, 2001.

[2] ALLAN J, JIN H, RAJMAN M, et al. Topic-based novelty detection[R]. Baltimore: Center for Language and Speech Processing, Johns Hopkins University, 1999.

[3] TRIPATHY A, AGRAWAL A, RATH S K. Classification of sentimental reviews using machine learning techniques [C]//Proceedings of 3rd international conference on recent trends in computing. [s. l.]: [s. n.], 2015: 821-829.

[4] ALLAN J, PAPKA R, LAVRENKO V. On-line new event detection and tracking [C]//Proceedings of the 21st annual international ACM SIGIR conference on research and development in information retrieval. New York, NY, USA: ACM, 1998: 37-45.

[5] GILLICK D, FAVRE B. A scalable global model for summariza-

tion [C]//Proceedings of the workshop on integer linear programming for natural language processing. [s. l.]: [s. n.], 2009: 10-18.

[6] 张瑾, 许洪波. 基于动态内容的文摘方法研究 [C]//全国信息检索与内容安全学术会议. 出版地不详: 出版者不详, 2007.

[7] XIE X, LIU Y, LE W, et al. S-looper: automatic summarization for multipath string loops [C]//International symposium on software testing and analysis. New York, NY, USA: ACM, 2015: 188-198.

[8] SEUNG H, LEE D D. The manifold ways of perception [J]. Science, 2000, 290 (5500): 2268-2269.

[9] 陈惠勇. 流形概念的起源与发展 [J]. 太原理工大学学报: 社会科学版, 2007, 25 (3): 53-57.

[10] 徐蓉, 姜峰, 姚鸿勋. 流形学习概述 [J]. 智能系统学报, 2006, 1 (1): 44-51.

[11] NASTASE V. Topic-driven multi-document summarization with encyclopedic knowledge and spreading activation [C]//Conference on empirical methods in natural language processing. Stroudsburg, PA, USA: Association for Computational Linguistics, 2008: 763-772.

[12] SILVEIRA S B, BRANCO A. Extracting multi-document summaries with a double clustering approach [M]//Natural language processing and information systems. Berlin: Springer, 2012: 70-81.

[13] LIN C Y, HOVY E. Automatic evaluation of summaries using n-gram cooccurrence statistics [C]//Proceedings of the 2003 conference of the North American chapter of the association for computational linguistics on human language technology. Stroudsburg, PA, USA: Association for Computational Linguistics, 2003: 71-78.

[14] FERREIRA R, CABRAL L D S, FREITAS F, et al. A multi-document summarization system based on statistics and linguistic treatment [J]. Expert Systems with Applications, 2014, 41 (13): 5780-5787.

(上接第25页)

trends in software methodologies, tools and techniques. [s. l.]: IOS Press, 2010: 3-36.

[9] 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.

[10] MOIR I, SEABRIDGE A, JUKES M. Civil avionics systems [M]. [s. l.]: John Wiley & Sons, 2013.

[11] PARNAS D L. Tabular representation of relations [D]. Canada: Telecommunications Research Institute of Ontario McMaster University, 1997.

[12] HEITMEYER C L, JEFFORDS R D, LABAW B G. Automated consistency checking of requirements specifications [J]. ACM Transactions on Software Engineering & Methodology, 1996, 5 (3): 231-261.

[13] 张鹏, 刘磊, 刘华斌, 等. Tabular 表达式的指称语义研究 [J]. 软件学报, 2014, 25 (6): 1212-1224.

[14] HATTON L. What is a formal method (and what is an informal method)? [C]//Proceedings of the 12th annual conference on computer assurance 1997. [s. l.]: IEEE, 1997: 125-126.

[15] WELLS A T, RODRIGUES C C. Commercial aviation safety [M]. [s. l.]: McGraw-Hill Professional, 2011.