计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20151055
54(3):654-668,2017

面向 DO-178C 软件测试过程的目标符合性论证模式

杨 阳[1] 吴 际[1] 苑春春[1] 刘 超[1] 杨海燕[1] 邢 亮[2]
[1](北京航空航天大学计算机学院 北京 100191)
[2](中航工业西安航空计算技术研究所 西安 710068)
(yyangbuaa@sina.com)

Objectives Conformity Argument Patterns for Software Testing Process in DO-178C

Yang Yang[1], Wu Ji[1], Yuan Chunchun[1], Liu Chao[1], Yang Haiyan[1], and Xing Liang[2]
[1](*School of Computer Science and Engineering, Beihang University, Beijing* 100191)
[2](*Xi'an Aeronautics Computing Technique Research Institute, Aviation Industry Corporation of China, Xi'an* 710068)

Abstract Safety-critical software has been widely used in many fields. As the specific requirement of safety-critical software is preventing catastrophes, this kind of software must comply with its relevant safety standards. But now it does not have any effective ways to construct objectives conformity argument model for standards. By analyzing the features of objectives of software testing process in DO-178C, an objective conformity argument pattern description framework based on GSN is proposed, and these patterns are described through four fields: the problems that we need to solve, the specification for the solution, the approach to use them and the effect after using them. At the same time, some extensions for safety case patterns are proposed to describe the objectives conformity argument patterns. On this basis, three objectives conformity argument patterns based on software testing process in DO-178C are proposed, which are code-requirement conformity argument pattern, test coverage of requirements argument pattern and test coverage of structure argument pattern. At the same time, the instantiated method to build the objectives conformity argument structure for a specific program based on these patterns is proposed. People can construct objectives conformity argument structure for objectives of software testing process in DO-178C effectively through the proposed way. At last, one case study, which is an embedded real-time operating system, indicates that the objectives conformity argument patterns proposed here are useful and effective.

Key words safety-critical software; airworthiness certification; DO-178C; GSN; argument patterns

摘 要 安全关键软件已广泛应用于众多领域.鉴于其对防范灾害风险方面的特殊要求,必须符合相关领域的安全性标准.但是目前对于如何建立面向标准的目标符合性论证模型,尚缺乏有效的方法.针对DO-178C标准中关于软件测试过程目标的特征描述,提出了一个基于GSN的目标论证模式描述框架,分别从解决问题、解决方案、应用方法和产生效果4个方面对目标论证模式进行描述;同时使用一种扩展的安全案例模式描述方式,用以描述面向标准的目标符合性论证模式.在此基础上,提出了3种面向DO-178C软件测试过程的目标符合性论证模式,分别是代码-需求符合性论证模式、需求测试覆盖率论证模式、结构测试覆盖率论证模式,并提出基于这些模式建立针对特定项目的目标符合性论证结构的实例化方法,为建立面向DO-178C软件测试过程的目标符合性论证结构提供了有效指导.通过一个机载嵌入式实时操作系统的案例,说明了提出的目标符合性论证模式的可用性和有效性.

收稿日期:2015-12-09;**修回日期**:2016-11-04
通信作者:吴际(wuji@buaa.edu.cn)

关键词　安全关键性软件;适航认证;DO-178C;GSN;论证模式

中图法分类号　TP311

安全关键软件(safety critical software)正在越来越广泛地应用于航空、航天、高铁、汽车、能源、通信、医疗、金融、工业控制等众多领域.这类软件必须符合各自领域中规定的安全性相关标准,比如在航空领域,机载软件必须符合最新的适航审定标准 DO-178C[1]以及一系列相关标准,并通过局方的适航审定,才能投入使用.DO-178C 针对不同安全等级的软件分别提出了一系列目标,比如 A 级软件必需满足全部 71 个目标,其中针对 A 级软件的单元测试,要求必需满足语句覆盖、分支覆盖和 MC/DC 覆盖等测试充分性准则.机载软件的开发方需要依据软件开发过程中产生的各种数据和信息,提供必要证据,通过有效的论证过程说明其符合安全性标准中规定的目标.

但是,目前在建立面向标准的目标符合性论证结构方面还存在 3 个基本问题:

1) 建立面向特定项目的论证结构涉及的因素多且建立过程复杂.安全性相关标准中对产品开发过程及其制品以及相关影响因素的监控等均有严格的要求,明确规定了必须满足的一系列目标,包括蕴含的相关子目标和具体要求.为了对特定的安全关键软件或系统的标准符合性进行有效论证,需要将其开发过程(包括各种相关活动及其采用的方法、准则、策略以及实际执行结果中可提取的安全性相关证据等)与相关标准的具体目标和要求之间建立起明确的关联.因此,需要依据相关标准,建立针对具体项目的安全性论证结构,以支持其安全论证体系的建设、安全性相关证据的采集和分析以及安全性目标的论证.然而,如何从标准中提取出必需满足的各个目标及其相关子目标和具体要求,以建立安全性论证结构,以及如何建立其与具体项目过程及其所产生的相关证据之间的关联,目前尚没有有效的方法.

2) 对于不同的软件项目,由于其产品特点和开发过程等方面的差异,其论证结构之间亦存在差异,致使项目相关的论证结构难以重用.但是,由于在相关标准的约束下这些论证结构之间显然存在高度的相似性,因此有必要提炼共性特征,以方便论证结构的快速建立.例如提炼具有共性的论证结构模式,并据此自动生成针对项目的特定论证结构实例.

3) 事实上,安全性相关标准中规定的各种目标之间存在一定关联,其符合性论证结构之间也存在一定的相似性,因此可以进一步提炼面向不同目标的论证结构模式.

本文以 DO-178C 规定的软件测试过程目标为研究对象,参考安全案例模式(safety case pattern)[2],将可重用的结构模式引入到目标符合性论证结构设计中,提出了 3 种针对软件测试过程目标符合性论证结构的论证模式,以及通过对论证模式的实例化建立面向项目的论证结构的方法.并以某实际项目为应用案例,说明本文提出的目标符合性论证模式的可重用性和有效性.这种基于模式的目标符合性论证方法,对于其他面向标准的目标符合性论证同样具有参考价值,适用于针对 DO-178C 等安全性相关标准的目标符合性论证结构的建立.

1　适航软件论证研究现状

1.1　DO-178C 标准

DO-178C[1]依据软件失效带来的危害等级,将软件分为 A,B,C,D,E 五个级别.其中 A 级软件对安全性要求最高,E 级软件则不需要满足 DO-178C 标准中规定的目标.DO-178C 规定了不同安全等级的机载软件在软件开发过程中必须符合的目标和相关要求,在机载软件的安全性认证中已被广泛采用.NASA 的研究员 Holloway[3-4]对于 DO-178C 中提出的总目标与软件开发过程中需要达到的各个目标之间的证明与被证明关系进行了分析,并通过对这些目标的分类,利用 GSN(goal structuring notation)[5]清楚地展示了针对不同安全等级的软件,其过程目标与总目标之间的结构关系.国内也有针对 DO-178B/C 的研究,文献[6]将 DO-178B 标准与 DO-178C 标准进行比较,分析了 DO-178C 在软件开发过程中新增或者变更的内容;文献[7]提出了满足 DO-178B 中结构覆盖率分析的解决方案,并在实际的项目中应用.

在基于 DO-178C 的认证方面,软件审批指南(software approval guidelines)[8]为基于 DO-178C 的认证提供了指导,该指南指出在执行基于 DO-178C 标准的认证时应该考虑的因素,并得到了广泛认可.

1.2　软件的标准符合性论证方法

标准符合性论证指的是通过建立一种规范的论证结构来支持对项目实施过程是否符合标准的论证.论证结构中通常包括待论证的标准目标、结构化的论证过程以及用来论证目标的数据或证据.

为了论证软件是否符合标准中规定的目标(如

软件测试过程需满足的目标),可以使用不同的论证方法.例如基于检查单的论证、基于 GQM[9](goal question metric)模型的论证、基于 GSN[5]模型的论证等.

基于检查单的论证是在工程实践中常用的方法[10].这种方法将标准中规定目标的具体要求以检查单的形式列举出来,通过人工检查来确认被论证的软件是否符合检查单中规定的各项要求.这种论证方法不仅工作量大,更重要的是通用的检查单中无法体现具体项目的特点和差异,且无法建立目标与证据之间的关联,论证结果常会受到论证人的主观判断的影响.

GQM 是一种层次化的论证方法,以表格的形式表达,分为目标、问题和度量 3 层.首先确立目标,然后将目标分解成若干问题,并针对每个问题采用量化的度量来进行论证.然而,这种固定的 3 层结构对复杂目标的分层细化难度很大,因此无法支持针对 DO-178C 这类标准的严谨论证.此外,在度量层,只考察了预定的度量数据,而不考虑各种复杂数据或证据之间的关系,以及开发人员能力等复杂的影响因素.因此,GQM 也具有明显的局限性.

GSN[11]是一种结构化的表示论证组织形式的方法,其主要论证结构为:总目标、可分层细化的子目标及其分解策略、子目标对应的证据.基于 GSN 的论证指的是针对每个待论证的目标,建立对应的 GSN 结构,并根据采集到的证据进行目标论证的方法.GSN 是一种多层的论证结构,可以根据标准对目标的定义和相关要求,将目标分解为若干个子目标,并可以准确描述目标的分解策略等,为目标论证提供必要依据和指导.此外,图形化的表达方式使得复杂的论证结构更加直观,易于理解.在 GSN 基础上,GSN 提出者通过文献[11]从论证模式和模块化表示 2 个方向进行扩展,使得 GSN 的适用范围更加广阔.

除了 GSN 提出者的研究团队,其他的研究团队针对 GSN 模型也从不同的侧重点进行了扩展.Takai 等人[12]提出在安全案例发生变更时,针对变更的表示方法,并通过案例说明了该方法的有效性.Matsuno 等人[13]提出了基于 GSN 的安全案例模式的一种参数化表达方法,这种方法可以支持一致性检查,避免使用安全案例模式进行参数实例化时出现的一致性错误.

1.3 安全案例和安全案例模式

安全案例用来论证在特定的上下文中,系统是否具有足够安全的保证[2].安全案例是一种论证结构,由论证目标、结构化的论证过程以及证据组成.依据证据,通过结构化的论证过程来论证预期的目标是否成立.目前,通常使用 GSN 来表示安全案例.

安全案例模式(safety case pattern)[2]的概念是由 Kelly 和 McDermid 在 1998 年提出的.安全案例模式使用 GSN 表示,并对 GSN 的符号进行了一定的扩展.安全案例模式将可复用的论证结构这个概念引入了安全案例中.在此基础上,Alexander 等人[14]依据建立安全案例的经验,在 2007 年发表 1 份报告,针对先进控制软件总结了 14 种安全案例模式,并且使用了参数化的表示方法来描述安全案例模式,为建立该类型软件的安全案例提供了指导.

2 基于 GSN 的目标论证模式框架

本文提出一种基于 GSN 的目标论证模式描述框架,分别从模式的解决问题、解决方案、应用方法和产生效果 4 个方面对目标论证模式进行描述,并提出了一种扩展的安全案例模式描述方式,用于在解决方案中详细定义面向标准的目标符合性论证模式.该描述方式针对安全案例模式进行扩展,下面对安全案例模式的主要结构和本文扩展的部分进行介绍.

安全案例模式的主要结构如下.

1) 主要论证元素:目标(矩形框表示)、策略(平行四边形表示)、证据(圆形表示);辅助论证元素:上下文(圆角矩形框表示)、假设(右下角有大写字母 A 的椭圆形框)、论证(右下角有大写字母 J 的椭圆形框);关联关系:实心箭头建立主要论证元素之间的关联、空心箭头建立主要论证元素和辅助论证元素的关联.

2) 在目标和策略中引入模式变量(以下简称变量),用{变量名}表示,并在其关联的上下文中对变量进行进一步解释说明,包括对其值域的定义,表达方式为

变量名:{值,…}.

这些变量可以指代目标论证所针对的软件(项目)、待论证的性质或要求、相关的活动或制品、候选策略、环境约束等.此外,定义 $\#(Y)$ 为集合 Y 中元素的数量.

3) 扩展的关联关系.在关联关系上增加了对实例化数量的约束,用"带实心圆点的实心箭头+实例化后的目标数量"表示;目标间"或"的关联关系,用"实心箭头+菱形"表示.

本文扩展的部分如下.

1) 目标关联的上下文中定义目标约束条件. 含义为:在进行论证模式实例化时,只有约束条件成立时,对应的目标才会存在.

2) 证据关联的上下文中必须定义对证据结构的要求,只有提供的证据元素符合结构的要求时,才能保证最终建立的论证结构成立,可以进行论证推导.

3) 建立与标准的关联. 在各类节点中,用"(标准中相关条目编号或章节号)"方式注释其与标准中相关条目的关联性,方便检查核对论证结构与标准的对应关系.

4) 添加含有字母 T 的矩形框,用于目标下方. 表示该目标成立,不需要用证据证明.

为了清晰地区分出图 1～8 定义的各种元素,图 1～8 各个元素的标识符均使用大一号的字号;标准的关联性注释使用带下划线的字;所有变量名均使用斜体字. 上述扩展元素的标识方式,参见第 3 节.

此外,本文使用的复合目标,该符号源于文献[11]对 GSN 的扩展. 复合目标(类似文件夹的图形表示符号,并在其中填写名称),其本身是一个独立的论证结构. 引入复合目标,是为了提取可重用的论证结构,避免在多个目标论证中对其进行重复定义. 同时,通过对复合目标的引用,可以简化复杂的论证结构.

3　面向 DO-178C 软件测试过程的论证模式

通过对 DO-178C 标准中关于软件测试过程目标和相关要求的分析,本文提出了针对此类过程的 3 种典型的论证模式,实现了其目标符合性论证结构的可重用性. 这种可重用性主要体现在 2 个层面:

1) 这种模式可以表示面向标准(即独立于特定项目)的目标符合性论证结构;

2) 这种模式可以表示针对 1 个项目中多个同类目标的符合性论证结构.

3.1　代码-需求符合性论证模式

3.1.1　解决问题

DO-178C 规定的基于需求的测试活动的主要目标是测试可运行目标代码与需求之间是否符合、是否健壮. 本节中提出的模式为建立目标代码与高

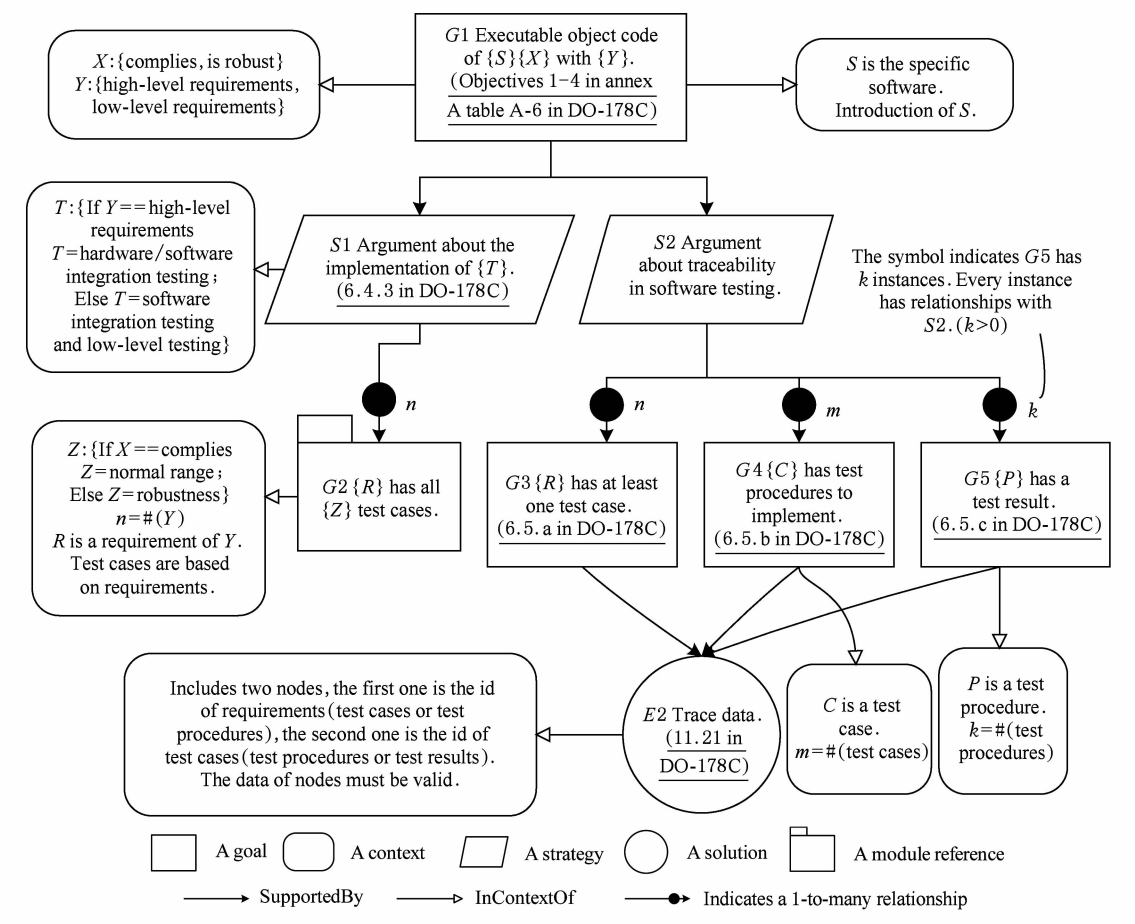


Fig. 1　Code-requirement conformity argument pattern 1

图 1　代码-需求符合性模式 1

层需求和低层需求之间的符合性与健壮性目标(DO-178C 附录 A 中表 A-6 的目标 1～4)的论证结构提供具体指导,并可通过实例化该论证模式,进一步建立针对具体项目的论证结构.

3.1.2 解决方案

解决方案如图 1 和图 2 所示.

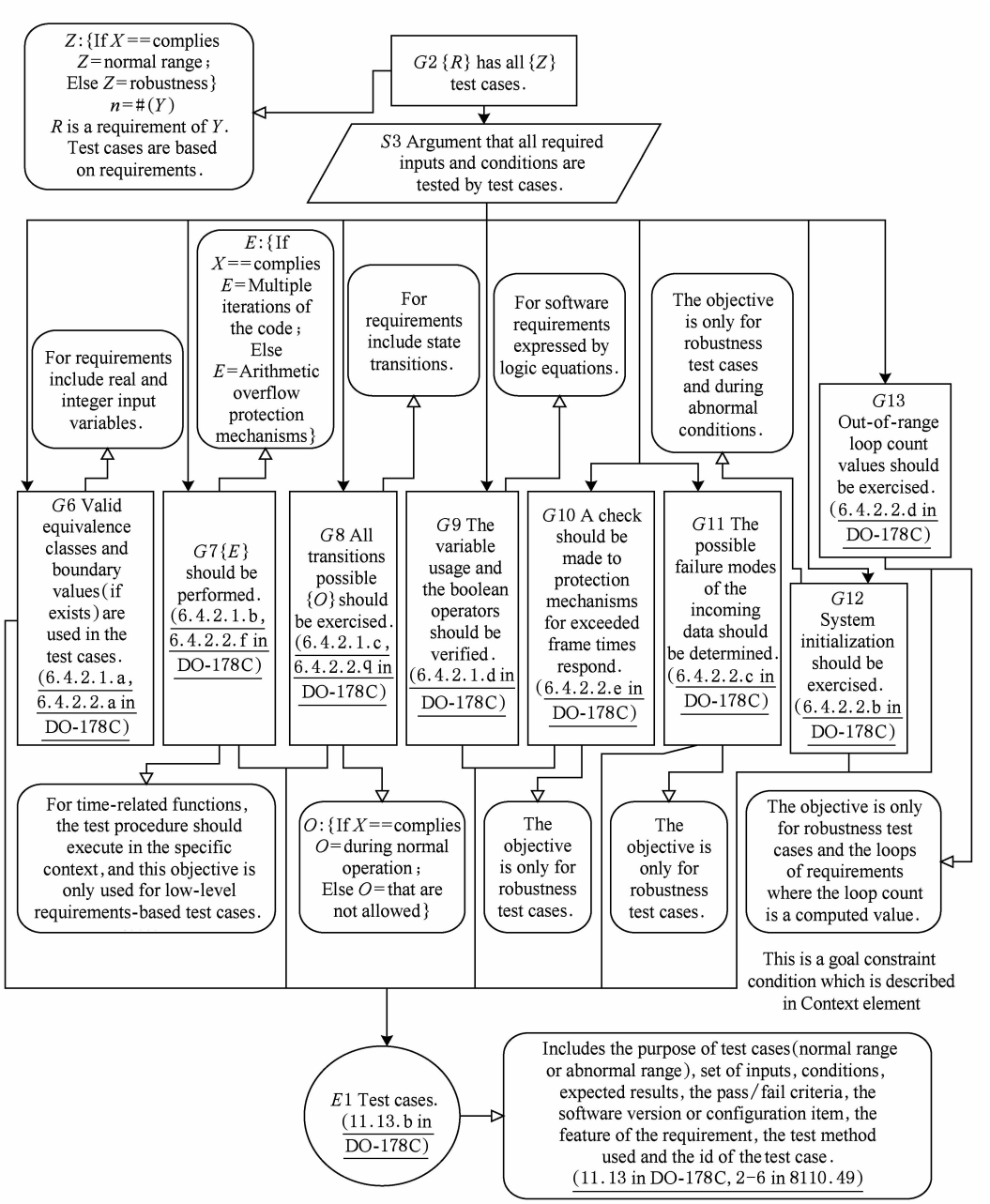


Fig. 2 Code-requirement conformity argument pattern 2

图 2 代码-需求符合性模式 2

图 1 描述了 DO-178C 规定的基于需求的测试活动的主要目标,包括测试可运行目标代码与需求之间符合性(compliance)和健壮性(robustness).图 2 是对复合目标 $G2$ 的定义.在该模式定义中:

1) 目标 $G1$ 中引用的模式变量 S 指代软件名称,在实例化时可直接使用具体的软件名称替代;X 的取值是其上下文描述中定义的 complies 或 is robust;Y 的取值是 high-level requirements(高层需求)或 low-level requirements(低层需求).

2) 在上下文元素中分别定义了其对应的目标或策略的约束条件.例如对策略 $S1$,当 $G1$ 针对的是 Y = high-level requirements 时,要求论证 T = hardware/software integration testing(硬件/软件集成测试)的实现;否则,当 Y = low-level requirements

时,则应论证 T=software integration testing and low-level test(软件集成测试以及低层测试).类似地,对目标 $G2$,如果 $G1$ 针对的是 X=complies,则 $G2$ 中的 Z=normal range(测试正常范围),否则 Z=robustness(测试鲁棒性).而对于目标 $G8$,则规定只有当需求中包括状态转换的内容时,其才需要存在.

3) 针对证据的上下文描述中给出了对证据结构的要求.例如对于证据 $E1$,其上下文描述中定义了测试用例中应该包含哪些元素,只有提供的证据元素符合上下文描述中对证据结构提出的要求时,才能保证最终建立的论证结构是成立的,可以进行论证推导.

图 1 和图 2 所示的模式表达了 DO-178C 标准附录 A 中表 A-6 的目标 1～4 的论证结构,分别用于论证可运行目标代码与高层需求或低层需求之间的符合性及健壮性.针对总目标 $G1$(可运行目标代码和需求之间的符合性或健壮性)的论证,被分成 2 个论证结构,即测试用例的选择符合标准定义的规则($S1$→$G2$)以及对整个测试活动中追溯性的检验($S2$→{$G3$,$G4$,$G5$}).论证 1 结构依据 $S1$ 进行分解论证,$S1$ 说明编写的测试用例所属测试类型,分解到 $G2$ 目标,描述了针对各项具体需求编写覆盖正常范围(或健壮性)的测试用例集,并通过扩展的关联关系说明在实例化论证模式时,要求实现 n 个目标 $G2$,其中 n 为需求的总数量(n=♯(Y)),即变量 R 将实例化为一项具体需求,并且对应每一项需求都将实例化出一个 $G2$ 的实例.在图 2 中,将 $G2$ 按照策略 $S3$ 向下分解,通过 $G6$～$G13$ 将不同类型的需求(时间相关的需求、涉及到状态转换的需求、包含整型实型的需求),在不同条件下(正常范围内的测试或者健壮性测试)需要选择的测试用例的目标分别表示出来,并且每个目标的约束条件都以其上下文描述的形式给出定义,最终这些目标用证据 $E1$ 论证目标是否实现.论证 2 结构依据 $S2$ 进行分解论证,判断需求、测试用例、测试程序、测试结果之间是否存在追溯性.其中,目标 $G3$ 表达每个需求都至少存在一个测试用例,目标 $G4$ 表达每个测试用例都由测试程序实现,目标 $G5$ 表达每个测试程序都有测试结果,最终用证据 $E2$ 论证这些目标是否实现.此外,对证据 $E1$,$E2$ 的结构要求定义在其对应的上下文描述中.

3.1.3　应用方法

实例化模式的方法分为 5 步:

1) 结合项目真实情况实例化论证模式中的模式变量,即将其赋值,并将模式中定义模式变量可能取值的上下文描述矩形框删除.

2) 结合项目实际情况判断是否满足上下文描述中定义的约束条件,删除不符合约束条件的子目标及其约束条件,并且在保留的子目标中,将对应的约束条件保留,并以假设(右下角有大写字母 A 的椭圆形框)的形式作为辅助论证结构来支撑对应的子目标,其含义是:当这个假设成立时,对应的子目标才可以进行是否成立的论证.

3) 项目中实际的证据结构必须满足模式中规定的证据结构,否则无法进行目标符合性论证.

4) 依据项目实际情况,可以对现有的目标进行进一步的分解,或者添加原来模式中没有但是项目中必需的子目标项,提供对应证据,并给出对证据结构的要求,以上下文描述的形式与对应证据相关联.

5) 检查最终实例化目标论证结构,最终建立的论证结构中,不能包括未实例化的模式变量;除证据结构要求的上下文描述项,不能包含其他约束条件上下文描述项;如果没有达到上述条件,则重复上述步骤继续实例化.

本文以 1 个简化的嵌入式实时操作系统(本文中称作操作系统 A)的论证目标 DO-178C 附录 A 中表 A-6 的目标 1 为例,采用上述方法,通过实例化上述论证模式,建立了该项目中针对该目标的论证结构,如图 3 所示.

图 3 中,首先对 $G1$ 进行实例化,说明论证的总目标是操作系统 A 中可运行目标代码和高层需求之间的符合性,并在其上下文描述对 A 进行说明.依据策略 $S1$,$S2$ 将总目标 $G1$ 向下分解.

1) 实例化策略 $S1$ 的论证结构,编写高层需求的测试用例属于软件/硬件集成测试.实例化图 1 中的目标 $G2$,该软件存在 9 项高层需求,实例化为图 3 中的目标 $G2.1$～$G2.9$.$G2.1$ 描述了操作系统 A 中任务挂起需求的测试用例要求,按照本模式中的定义,这个需求属于状态转换需求,对应于图 2 中的 $G8$,除此之外,该需求不满足这一层级其他目标的约束条件,因此对于这个目标来说,实例化时将删除模式中的目标 $G6$,$G7$,$G9$,$G10$,$G11$,$G12$,$G13$,只保留 $G8$,并将 $G8$ 中的约束条件转换为图 3 中目标 $G3.1$ 相关联的假设(右下方有大写字母 A 的椭圆形),保留模式中的 $G8$ 被实例化为图 3 中 $G3.1$,来测试正常操作下所有状态转换.依据操作系统 A 的特点可以知道,当任务处于就绪态或者休眠态,并且任务中没有锁(锁机制是操作系统中保持数据一致

性的一种机制,文献[15]介绍了操作系统中锁的实现原理)时可以挂起,因此在该模式的基础上,还需要添加目标 $G4.1$ 和目标 $G4.2$,并通过证据 $E1$ 证明是否符合目标.

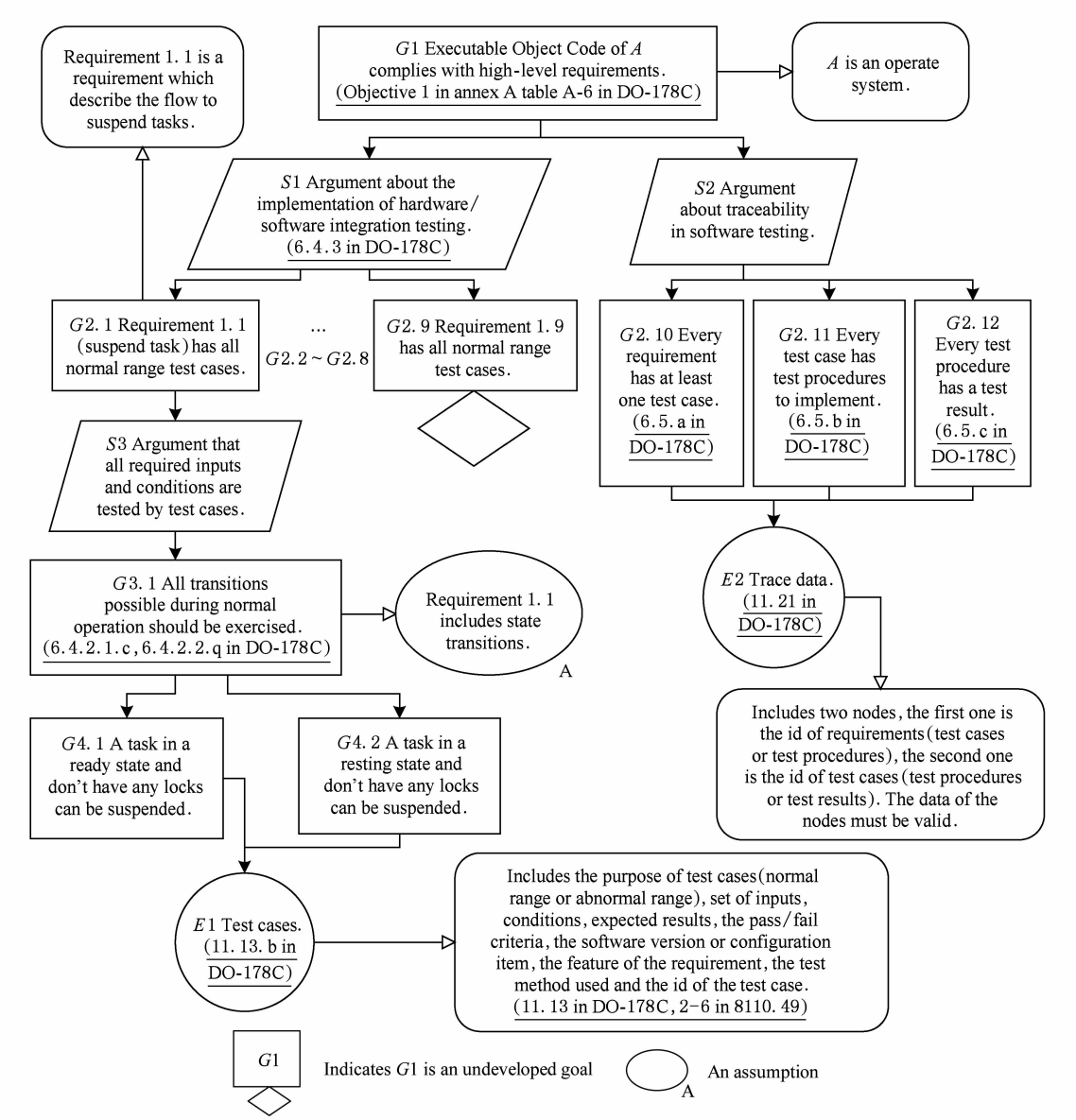


Fig. 3 An example of code-high-level requirement conformity argument structure

图 3 代码-高层需求符合性论证结构示例

由于篇幅限制,本文没有将 $G2.2$~$G2.9$ 的所有目标列举出来,使用省略号表示,此外 $G2.9$ 目标下的菱形框表示这个目标需要进一步分解.

2) 实例化策略 $S2$ 的论证结构. 图 1 中的目标 $G3$ 要求每个需求都要存在至少一个测试用例. 为了节省篇幅,图 3 没有将每个具体需求的编号逐一展示,而使用"Every requirement has"(每个需求都要实现)这样的句型表示. 图 1 中的目标 $G4$ 和 $G5$ 实例化情况类似. 因此,图 1 中的 $G3$,$G4$,$G5$ 目标分别对应于图 3 的 $G2.10$,$G2.11$,$G2.12$,并通过证据 $E2$ 证明是否符合目标.

3.1.4 产生效果

建立代码-需求符合性论证模式,有助于为不同项目实现 DO-178C 附录 A 中表 A-6 的目标 1~4 的论证结构提供便利. 论证模式包含了 DO-178C 针对这些目标规定的需要执行的所有活动,即在该模式中标注了标准中规定的所有相关活动,因此最终建立的论证模型符合标准规定,并可通过规范的步骤实例化,从而最终建立简明的论证结构.

此外,模式中为不同活动的执行规定了约束条件,因此,可以依据项目的实际情况决定是否执行该活动,对标准中规定的活动是否执行提供了指导,在

保证符合标准的前提下最大程度地提高了效率,避免执行不必要的活动.

3.2　需求测试覆盖率论证模式

3.2.1　解决问题

DO-178C 规定的基于需求的测试活动需要验证需求的测试覆盖率.本节中提出的模式为建立需求测试覆盖率目标(DO-178C 附录 A 中表 A-7 的目标 3～4)的论证结构提供具体指导,并可通过实例化该论证模式,进一步建立针对具体项目的论证结构.

3.2.2　解决方案

解决方案如图 4 所示:

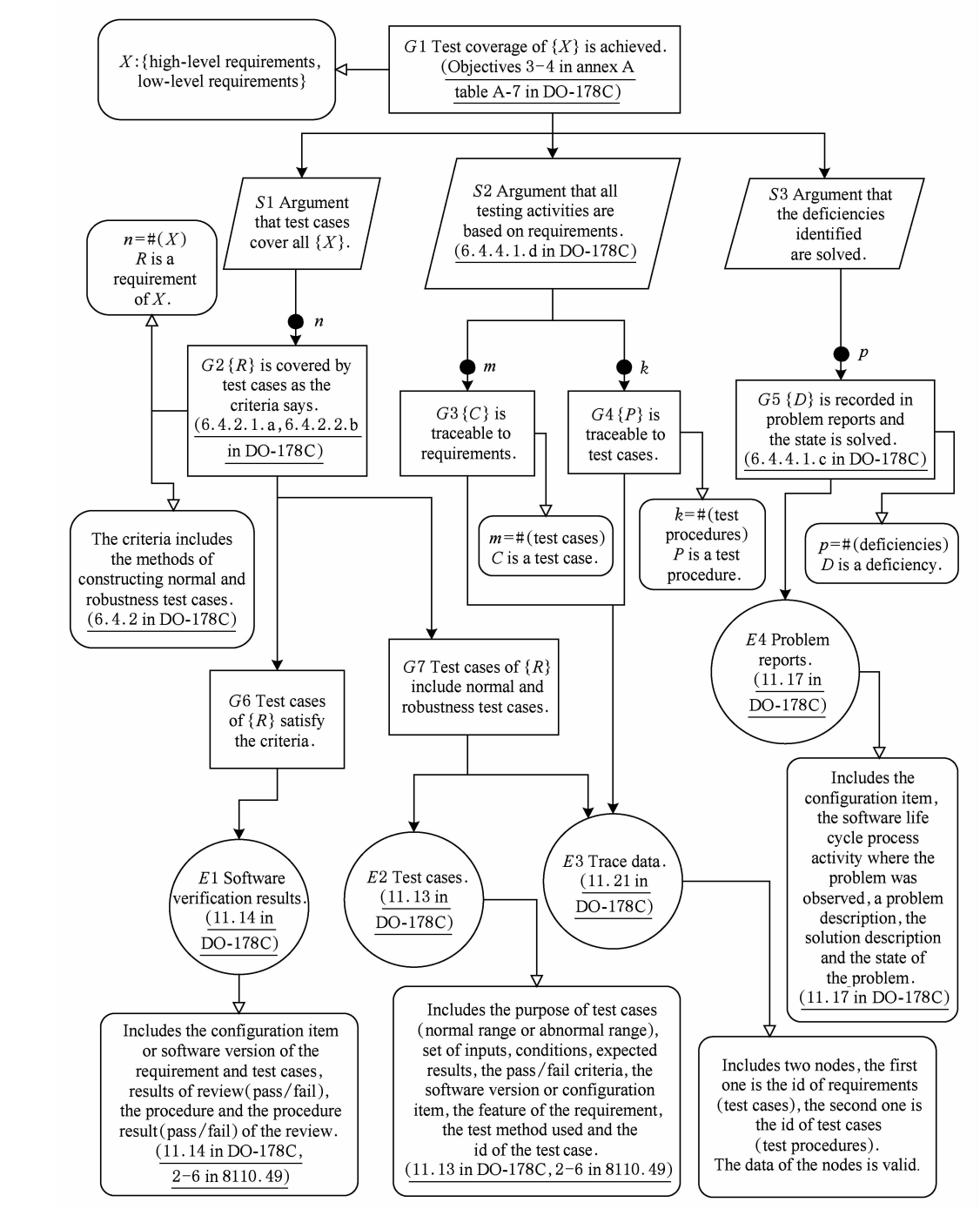


Fig. 4　Test coverage of requirements argument pattern

图 4　需求测试覆盖率论证模式

图 4 描述了针对 DO-178C 附录 A 中表 A-7 的目标 3～4 的论证模式,分别用于论证高层需求和低层需求的测试覆盖率.论证目标 G1,分成 3 个子论证结构,即论证测试用例覆盖了所有需求,论证所有

的测试活动都是基于需求的,论证整个覆盖率分析所执行活动的过程中发现的缺陷都记录并且解决了.论证 1 结构依据 $S1$ 进一步分解为目标 $G2$,$G2$ 又分解为目标 $G6$ 和 $G7$.$G6$ 验证基于需求的测试用例是否满足规定的正常以及健壮性测试准则,用验证结果 $E1$ 论证该目标是否实现.$G7$ 说明每个需求都存在正常和健壮性测试用例,用测试用例 $E2$ 和追溯数据 $E3$ 论证该目标是否实现.论证 2 结构依据 $S2$ 分解为 $G3$ 和 $G4$,分别说明每个测试用例可以追溯到需求和必须存在测试程序可以追溯到测试用例.通过这 2 个目标来说明所有测试活动都是基于需求的,用追溯数据 $E3$ 论证该目标是否实现.论证 3 结构依据 $S3$ 分解为 $G5$,说明所有发现的缺陷都被记录并解决,用问题报告 $E4$ 论证该目标是否实现.其中对证据 $E1$,$E2$,$E3$,$E4$ 的结构要求定义在其对应的上下文中.

3.2.3 应用方法

实例化的步骤与 3.1.3 节应用方法中的 1,3,4,5 一致,因为本模式中不存在需要删除的子目标,也不能删除任何子目标.即便在需求测试覆盖率分

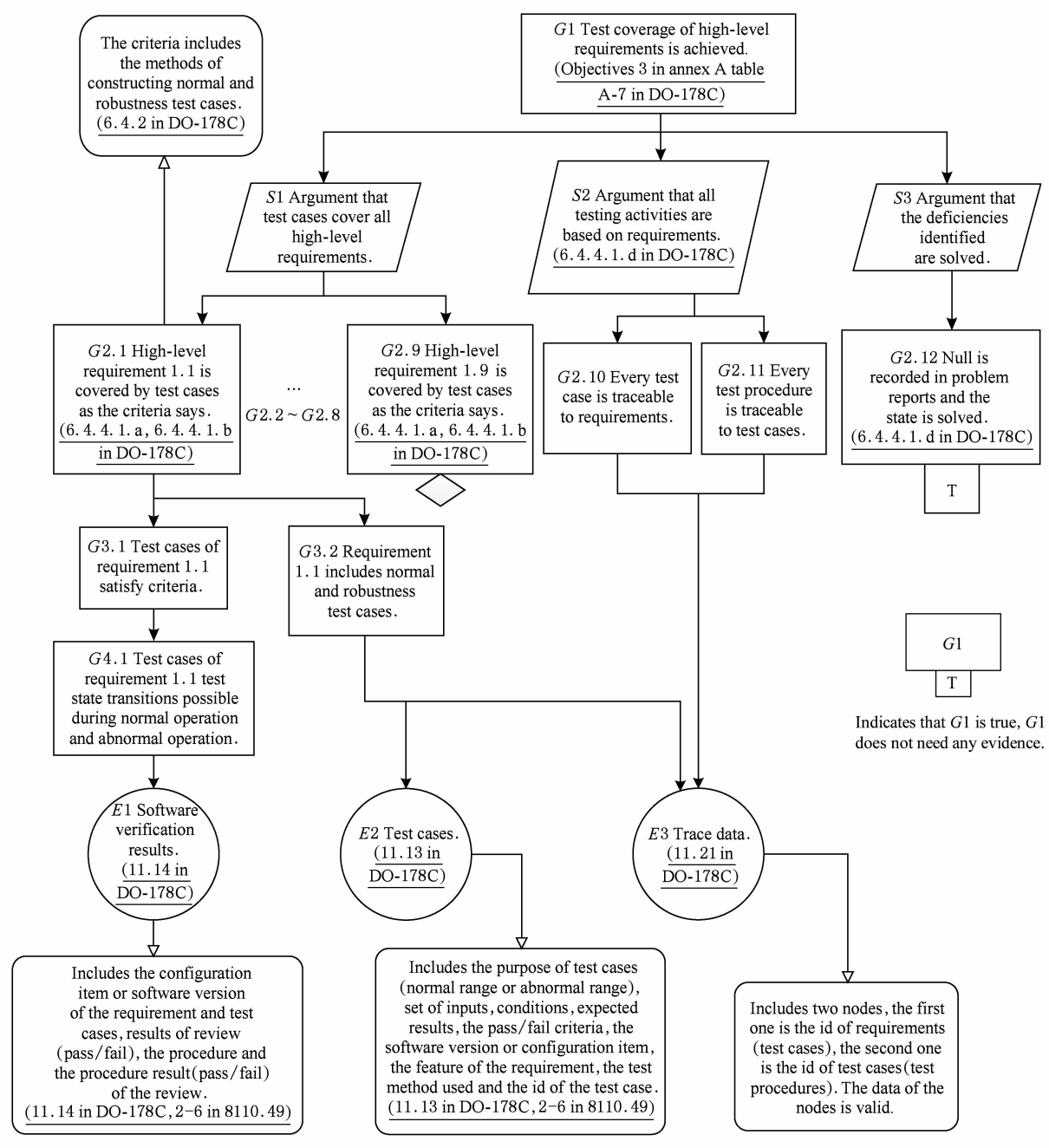


Fig. 5 An example of test coverage of requirements argument structure

图 5 需求测试覆盖率论证结构示例

析过程中没有发现错误,$G5$ 中的模式变量 D 可以用 null 表示,但是 $G5$ 是 DO-178C 中规定必须执行的活动,因此不能删除.

同样以操作系统 A 为例,采用上述方法实例化论证模式建立了针对 DO-178C 附录 A 中表 A-7 的目标 3 的论证结构,如图 5 所示.

图 5 中,先对 $G1$ 进行实例化,说明论证的总目标是高层需求的测试覆盖率符合标准.依据模式中定义的策略 $S1$,$S2$,$S3$ 将总目标 $G1$ 向下分解:

1) 实例化策略 $S1$ 的论证结构.即论证测试用例覆盖了所有的高层需求,实例化图 4 中的目标 $G2$,得到图 5 中的目标 $G2.1$～$G2.9$,其中 $G2.1$ 描述了操作系统 A 中任务挂起需求需要被测试用例覆盖,$G3.1$ 说明该测试用例要满足标准中的准则.依据 DO-178C 中对建立测试用例准则的描述,针对该需求需要建立正常操作以及异常操作下所有可能产生的状态转换的测试用例,因此添加目标 $G4.1$ 来说明,判定是否建立了这样的测试用例集,并通过证据 $E1$ 来验证.除此之外,还需要说明需求包含正常测试用例以及健壮性测试用例,在目标 $G3.2$ 中说明,并通过证据 $E2$ 和 $E3$ 证明是否符合这项目标.

同样篇幅限制,本文没有将 $G2.2$～$G2.9$ 的所有目标列举出来,使用省略号表示.

2) 实例化策略 $S2$ 的论证结构.图 4 模式中 $G3$ 目标要求每个测试用例都可以追溯到需求.为了节省篇幅,实例化时图 5 没有将每个具体的测试用例的编号逐一展示,而使用"Every test case is"(每个测试用例都要实现)这个句型表示.图 4 中的目标 $G4$ 实例化时情况类似.因此,图 4 中 $G3$,$G4$ 目标分别对应于图 5 的 $G2.10$,$G2.11$,并通过证据 $E3$ 论证是否符合目标.

3) 实例化策略 $S3$ 的论证结构.在本例中由于没有在论证需求的测试覆盖率所执行的活动过程中发现错误,因此在子目标 $G2.12$ 下添加含有内容 T 的矩形框,表示其自动成立,不需要通过证据证明.

3.2.4　产生效果

建立需求测试覆盖率论证模式,有助于对不同项目实现 DO-178C 附录 A 中表 A-7 的目标 3～4 的论证结构提供便利.论证模式包含了 DO-178C 针对这些目标规定的需要执行的所有活动,即在该模式中标注了标准中规定的所有相关活动,并且在标准规定的基础上,对实现这些活动的途径进行了扩展,因此最终建立的论证模型不仅符合标准规定,而且具有可行性,并可通过规范的步骤实例化,从而最终建立简明的论证结构.需要注意的是,本模式中所有的子目标都必须包含并进行论证,否则将不满足

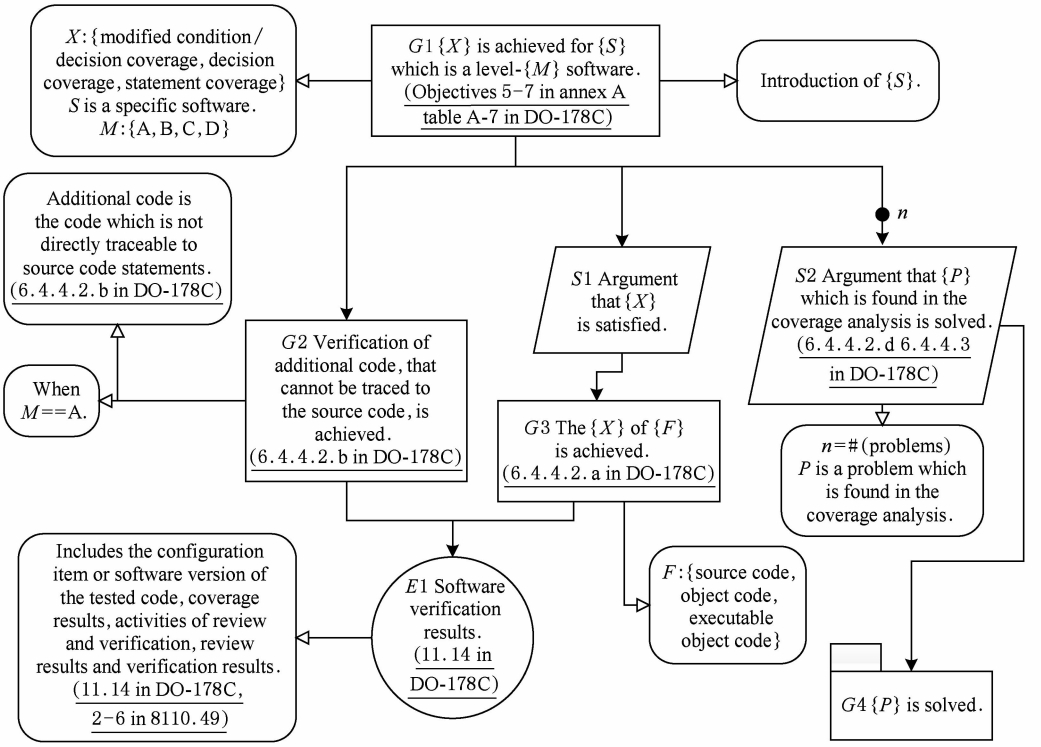


Fig. 6　Test coverage of structure argument pattern 1

图 6　结构测试覆盖率论证模式 1

标准的规定.

3.3 结构测试覆盖率论证模式

3.3.1 解决问题

DO-178C 规定的基于需求的测试活动需要验证结构测试覆盖率. 本节中提出的模式为结构测试覆盖率目标(DO-178C 附录 A 中表 A-7 的目标 5～7)的论证结构提供具体指导,并可通过实例化该论证模式,进一步建立针对具体项目的论证结构.

3.3.2 解决方案

图 6 和图 7 描述的是针对 DO-178C 附录 A 中表 A-7 的目标 5～7 的论证模式,分别用于语句覆盖率、分支覆盖率以及 MC/DC 覆盖率. 论证目标 $G1$ 分成 3 个论证结构:1)当待论证软件是 A 级软件时,需要验证额外代码[1](即由编译器、链接器或者其他方式生成的不能直接追溯到源代码语句的代码);2)论证代码的结构化覆盖率;3)论证整个覆盖率分析过程所执行的活动中发现的缺陷都记录并且解决. 论证 1 结构的论证目标是 $G2$(与 DO-178C 附录 A 中表 A-7 的目标 9 一致),需要验证额外代码,用验证结果 $E1$ 论证该目标是否实现. 论证 2 结构依据 $S1$ 进行分解论证,$G3$ 说明结构覆盖率达到了规定的要求,也要用验证结果 $E1$ 论证该目标是否实现. 论证 3 结构依据 $S2$ 进行分解论证,$G4$ 说明所有的问题都被记录并解决,并依据问题的不同,提出

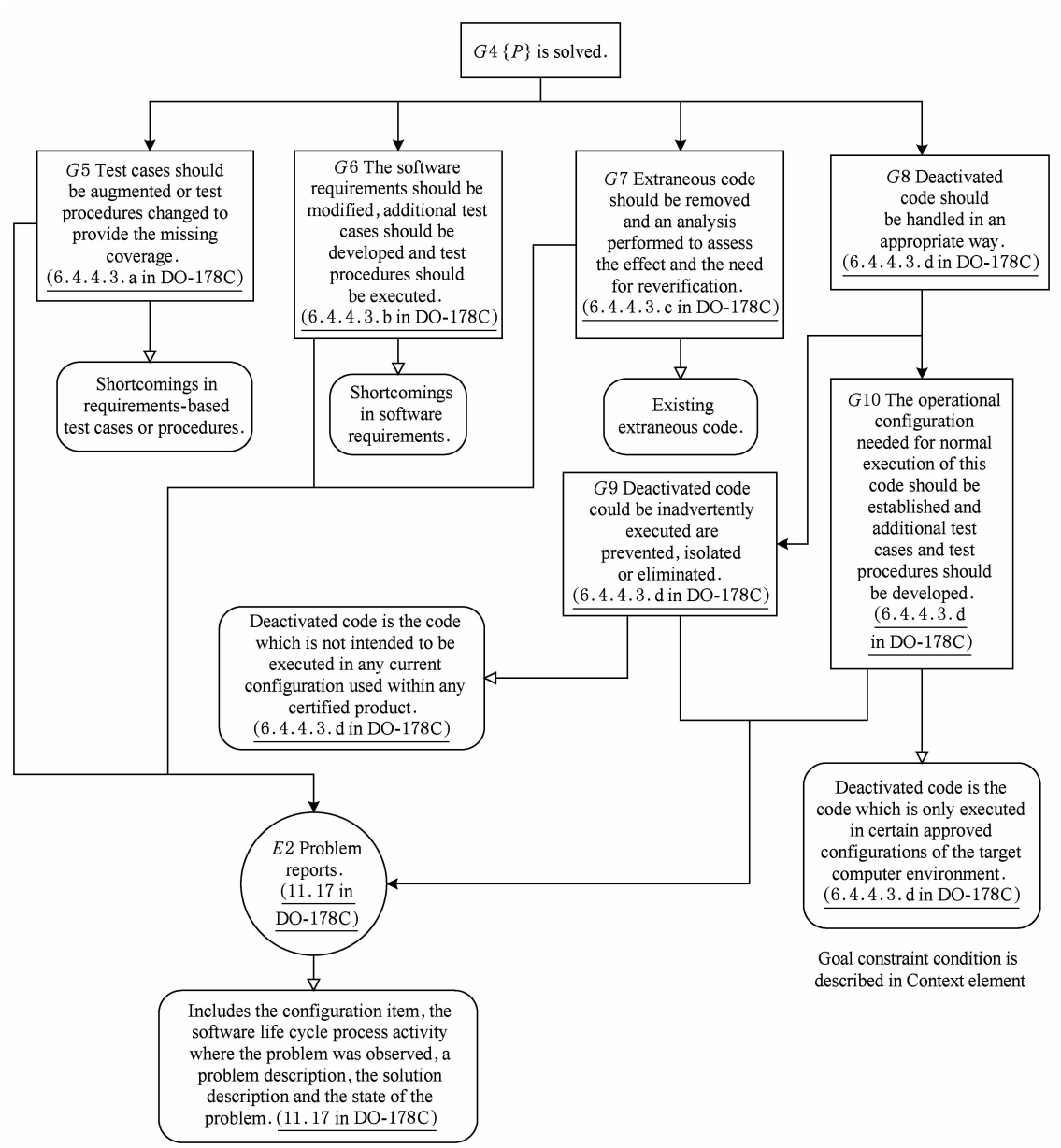


Fig. 7 Test coverage of structure argument pattern 2

图 7 结构测试覆盖率论证模式 2

需要满足的不同的要求 $G5$,$G6$,$G7$,$G8$(如图 7 所示),并在对应的上下文描述中说明其约束条件,其中 $G8$ 依据不同的停用代码使用情况,分解成目标 $G9$,$G10$,并在目标 $G9$,$G10$ 的上下文描述中说明其约束条件.最终用问题报告 $E2$ 论证该目标是否实现.其中对证据 $E1$,$E2$ 的结构要求定义在其对应的上下文中.

3.3.3　应用方法

实例化的步骤与 3.1.3 节应用方法中的 1,2,3,4,5 一致.如果在结构测试覆盖率分析过程中没有发现错误,那么 $G4$ 中的变量 P 使用 null 表示,由于 $G4$ 是 DO-178C 中规定必须执行的活动,因此 $G4$ 不能删除.

需要特别指出的是,如果规定的项目不是 A 级软件,应删除子目标 $G2$,否则不删除.

以操作系统 S 为例,采用上述方法实例化论证模式,最终建立了其针对 DO-178C 附录 A 中表 A-7 的目标 7 的论证结构,如图 8 所示:

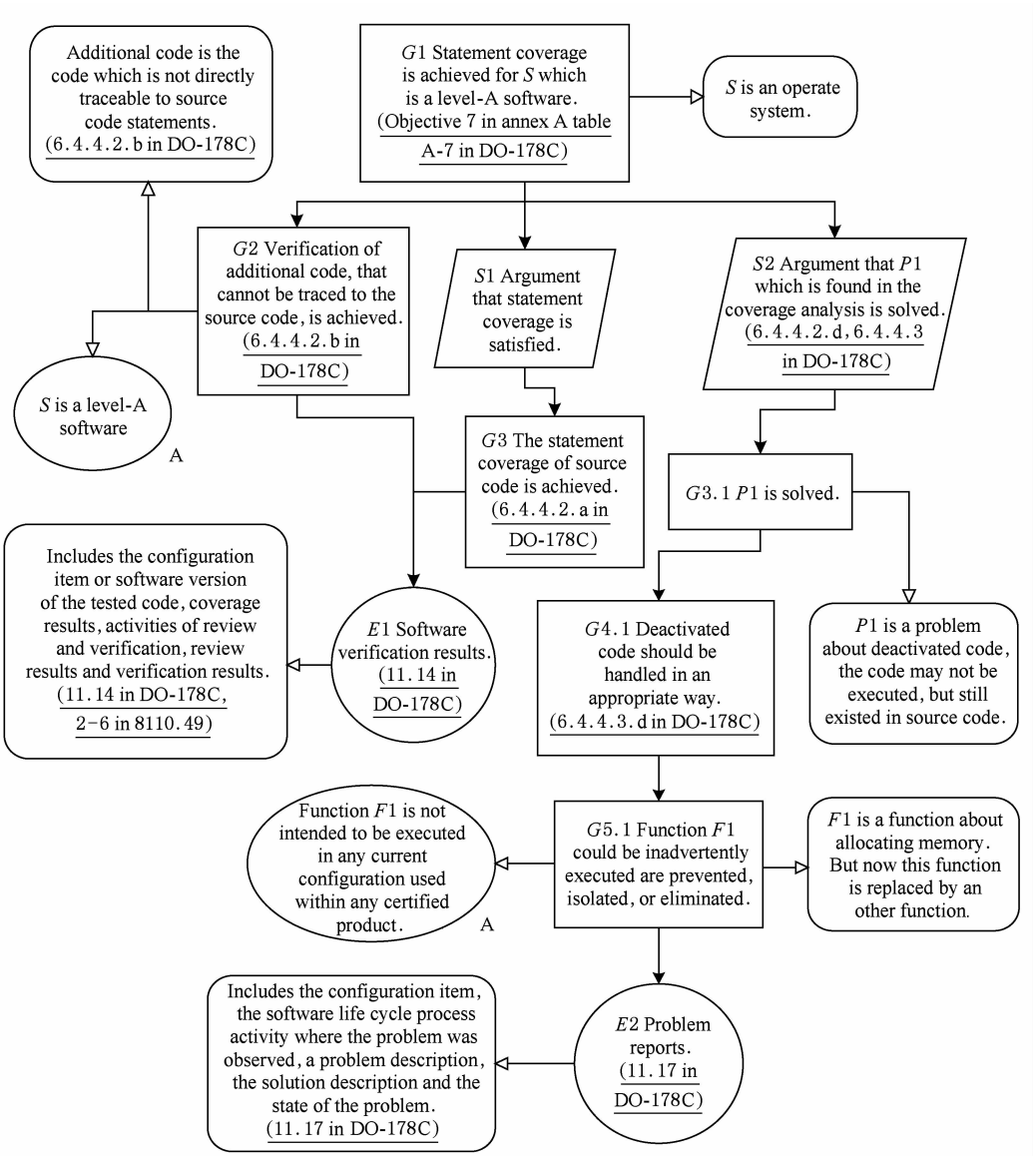


Fig. 8　An example of test coverage of structure argument structure

图 8　结构测试覆盖率论证结构示例

图 8 中,先对 $G1$ 进行实例化,说明论证的总目标是 A 级软件 S 的语句覆盖率符合标准.依据模式中定义的策略 $S1$,$S2$ 和目标 $G2$,将总目标 $G1$ 向下分解.

1) 实例化目标 $G2$ 的论证结构.描述 A 级软件必须对额外代码进行验证,通过证据 $E1$ 证明是否符合这项目标.

2) 实例化策略 $S1$ 的论证结构.在本例中,计算软件的语句覆盖率,依据实际情况,需要论证源代码语句覆盖率(目标 $G3$),并通过证据 $E1$ 来证明是否符合这项目标.

3) 实例化策略 $S2$ 的论证结构.在本例中,由于在结构覆盖率分析过程中发现存在停用代码的问题,因此需将图 6 中的 $G4$ 实例化为图 8 中的 $G3.1$,在进一步向下分解时,删除图 7 模式中其他不符合的目标 $G5$,$G6$ 和 $G7$.停用代码 $F1$ 由于已经被其他代码取代因而不会再被调用,因此图 8 中 $G5.1$ 对应于图 7 中的 $G9$,并将图 7 中 $G9$ 的约束条件以假设的形式添加到图 8 中的目标 $G5.1$ 中,即保证该代码在任何情况下都不能被调用.并通过证据 $E2$ 证明是否符合这项目标.

3.3.4 产生效果

建立结构测试覆盖率论证模式,有助于对不同项目实现 DO-178C 附录 A 中表 A-7 的目标 5～7 的论证结构提供便利.论证模式包含了 DO-178C 针对这些目标规定的所有需要执行的活动,即在该模式中标注了标准中规定的所有相关活动,并且列举出了不同等级软件需要实现的不同目标,因此最终建立的论证模型符合标准规定,并可通过规范的步骤实例化.在实例化的过程中,对于前 2 个论证结构(图 6 中的 $G2$ 和 $S1$),不同的项目之间区别不大,但是对最后一个论证结构(图 6 中的 $S2$),则需依据项目的实际情况进行实例化,不同的项目之间存在差别.

3.4 论证模式关联

本文提出了上述 3 种针对 DO-178C 软件测试过程目标的论证模式.依据 DO-178C 中对软件测试活动的定义,软件测试活动分为执行不同类型的测试、进行需求测试覆盖率分析和进行结构测试覆盖率分析这 3 种,主要实现的目标是 DO-178C 中附录 A 中表 A-6 以及表 A-7 中包含的目标.本文提出的 3 种模式可以实现 DO-178C 规定的软件测试过程中的 9 个目标.同时,这 3 种模式在软件测试过程目标的论证中缺一不可、相辅相成.

4 方法对比分析

4.1 描述内容对比

以 3.1.3 节提到的机载操作系统 A 为例,本节分别使用本文提出的目标符合性论证模式以及 GQM 方法进行论证,建立论证结构,并对论证效果进行对比.

图 9 所示为论证操作系统 A 是否满足 DO-178C 附录 A 中表 A-7 的目标 7 的 GQM 论证结构.对其中的每个问题,都对应着 1 个度量来回答该问题.

通过图 9 建立的模型,论证人员可以找到度量中提到的数据来评估该操作系统是否满足目标.

基于本文提出的目标符合性论证模式建立的 DO-178C 附录 A 中表 A-7 的目标 7 的论证结构如图 8 所示.将这 2 种方法进行对比,可以发现图 9 建立的模型相对简单,因此只能粗略地列举需要论证的目标和所需的度量,难以根据需要逐层细化复杂论证结构,比如在图 9 中:

1) 论证的过程只能分为 3 层,因此描述的论证结构过于简单,难以进一步细化复杂的论证问题.例如问题 3:是否所有存在问题都已经解决,没有明确说明对于不同类型的问题,什么样的处理方式才是合适的.

2) 针对论证目标,对应的度量数据难以进一步细化定义,因此可能存在歧义.对数据的理解不同会直接影响论证的结果.例如,需要语句覆盖率的运算结果,但是没有说明语句覆盖率的来源及其必需包含的内容.

Goal	Purpose Issue Object(Process) Viewpoint	Achieve Statement coverage Software verification process From the certification authorities
Question1		What is the current statement coverage?
Metrics1		Statement coverage = Tested statement/ All statement
Question2		Is the statement coverage achieved?
Metrics2		Statement coverage Subjective evaluation of certification authorities
Question3		All problems are solved or not?
Metrics3		Problem reports

Fig. 9 The GQM model of objective 7 in table A-7

图 9 表 A-7 目标 7 的 GQM 论证结构

对于图 9 中存在的上述问题,在图 8 建立的论证结构中都得到了解决.依据本文提出的方法建立论证结构,对论证目标及其上下文的约束和证据及其数据结构约束等都有更加完整明确的规定和清晰的表达方式.

4.2 成本对比

此外,本文提出的基于模式的目标符合性论证方法可以显著提高论证结构的可重用性,有效地降低面向标准的目标论证结构的建立成本,即工作量.假设建立 1 个论证结构的成本为 1.由于建立 1 个 GSN 论证结构与建立 1 种相应的论证模式的成本是大体相当的,亦可视为 1,因为其主要工作量主要

是对标准的理解和论证要素的提取.由于实例化论证模式相对简单,绝大多数步骤仅仅是对模式变量值的选择等,因此其成本可以忽略不计.

以另一个机载嵌入式实时操作系统 B 为例,表 1 展示了直接使用 GSN 建立论证结构,以及使用本文提出的模式建立论证结构来论证 DO-178C 软件测试过程目标的成本.

Table 1　The Cost of Constructing Argument Structure

表 1　2 种方法建立论证结构的成本

Objectives	GSN(Cost)	Objectives Conformity Argument Structure based on Patterns(Cost)
A-6.1	12	1
A-6.2	12	
A-6.3	156	
A-6.4	156	
A-7.3	4	1
A-7.4	4	
A-7.5	4	1
A-7.6	4	
A-7.7	4	

在操作系统 B 中,高层需求共有 708 项,低层需求共有 3 207 项.依据高层需求,整个系统分为 4 个子系统.依据低层需求,整个系统分为 52 个模块.在建立 DO-178C 附录 A 中表 A-6 的目标 1～2 的论证结构时,需要为每个子系统的每种特征(包含时间相关需求的子集、包含状态转换需求的子集、包含其他需求的子集)分别建立论证结构,用以分别判断其对应的测试用例是否符合 DO-178C 标准中规定的测试用例设计准则,因此,需要为每个目标分别建立 12 个论证结构.同理,在建立 DO-178C 附录 A 中表 A-6 的目标 3～4 的论证结构时,针对 52 个模块,需要为每个目标分别建立 156 个论证结构.因此,对论证 DO-178C 附录 A 中表 A-6 的目标 1～2,直接建立 GSN 论证结构的成本均为 12.对论证 DO-178C 附录 A 中表 A-6 的目标 3～4,直接建立 GSN 论证结构的成本均为 156.然而,建立上述 4 个目标的论证结构,如采用本文提出的第 1 种论证模式,通过实例化来建立上述论证结构,则其成本则近似为 1.

同样,由于有 4 个子系统,所以,针对论证目标 DO-178C 附录 A 中表 A-7 的目标 3～4 和 DO-178C 附录 A 中表 A-7 的目标 5～7,直接建立 GSN 论证结构的成本均为 4,合计 20.而采用本文提出的方法,则仅需要分别实例化第 2 种和第 3 种论证模式,因此,基于模式建立论证结构的成本均为 1,合计为 2.

通过本案例可以看出,本文提出的模式能够应用于目标论证结构的建立和实例化工作中,并且能够有效的降低建立论证结构的成本,提高了效率.

5　结束语

本文提出一种基于论证模式的标准符合性论证方法,并重点针对 DO-178C 对软件测试过程提出的主要目标和要求,提出了 3 种对应的目标符合性论证模式,以及基于这些模式建立面向特定软件项目的目标符合性论证结构的实例化方法.本文提出的 3 种论证模式覆盖了软件测试过程涉及到的主要目标.在第 4 节中,以 1 个机载操作系统软件项目为案例,说明了利用本文提出的模式建立论证结构的有效性.接下来,我们的工作重点是如何将这种基于论证模式的目标符合性论证方法进一步应用于 DO-178C 的其他过程目标论证以及其他安全性标准的目标论证工作中.

参　考　文　献

[1] RTCA. DO-178C software considerations in airborne systems and equipment certification [S]. Washington: RTCA Inc, 2011

[2] Kelly T, McDermid J. Safety case patterns—Reusing successful arguments [C] //Proc of IEE Colloquium on Understanding Patterns & Their Application to Systems Engineering. London: IET, 1998

[3] Holloway C M. Explicate'78: Discovering the implicit assurance case in DO-178C [C] //Proc of the 23rd Safety-Critical Systems Symp. North Charleston, South Carolina, USA: CreateSpace Independent Publishing Platform, 2015: 205-225

[4] Holloway C M. Towards understanding the DO-178C/ED-12C assurance case [C] //Proc of the 7th IET Int Conf on System Safety, Incorporating the Cyber Security Conf. London: IET, 2012: 1-6

[5] Spriggs J. GSN—The Goal Structuring Notation: A Structured Approach to Presenting Arguments [M]. Berlin: Springer, 2012

[6] Hu Ning. Study on airworthiness concerns of changes of DO-178C [J]. Aeronautical Computing Technique, 2014, 44(4): 94-98 (in Chinese)

(胡宁. 从 DO-178C 的新变化透视软件适航关注点[J]. 航空计算技术, 2014, 44(4): 94-98)

[7] Zhang Juncai, Wang Juan, Pan Wei, et al. Research on structural coverage analysis based on DO-178B [J]. Aeronautical Computing Technique, 2011, 41(4): 67-69 (in Chinese)
(张军才, 王娟, 潘卫, 等. 基于 DO-178B 的结构覆盖分析研究[J]. 航空计算技术, 2011, 41(4): 67-69)

[8] Federal Aviation Administration (FAA). Order 8110.49 Software Approval Guidelines [S]. Washington: Federal Aviation Administration (FAA), 2003

[9] Basili V R, Caldiera G, Rombach H D. The goal question metric approach [J]. Encyclopedia of Software Engineering, 1994, 2: 528-532

[10] Object Management Group (OMG). Kernel and Language for Software Engineering Methods (Essence), Version 1.1 [S]. Needham, MA: Object Management Group (OMG), 2015

[11] Goal Structuring Notation Working Group. GSN Community Standard, Version 1 [S]. York: Origin Consulting (York) Limited, 2011

[12] Takai T, Kido H. A supplemental notation of GSN aiming for dealing with changes of assurance cases [C] //Proc of 2014 IEEE Int Symp on Software Reliability Engineering Workshops. Piscataway, NJ: IEEE, 2014: 461-466

[13] Matsuno Y, Taguchi K. Parameterised argument structure for GSN patterns [C] //Proc of the 11th Int Conf on Quality Software. Piscataway, NJ: IEEE, 2011: 96-101

[14] Alexander R, Kelly T, Kurd Z, et al. Safety cases for advanced control software: Safety case patterns, FA8655-07-1-3025 [R]. York: Department of Computer Science, University of York, 2007

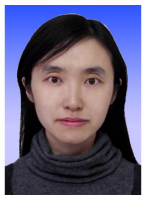
[15] quainzk. The implementation of lock in operating system [EB/OL]. [2016-05-08]. http://blog.sina.com.cn/s/blog_75f0b54d0100r7af.html (in Chinese)
(quainzk. 操作系统中锁的实现原理[EB/OL]. [2016-05-08]. http://blog.sina.com.cn/s/blog_75f0b54d0100r7af.html)

Yang Yang, born in 1991. Master. Her main research interests include safety certification and software engineering.

Wu Ji, born in 1974. Associate professor and PhD in Beihang University. Member of CCF. His main research interests include software safety, software engineering, software testing and requirement engineering.

Yuan Chunchun, born in 1985. PhD candidate in Beihang University. His main research interests include software engineering, software safety and software reliability (yccnankai@buaa.edu.cn).

Liu Chao, born in 1958. Professor and PhD supervisor in Beihang University. Senior member of CCF. His main research interests include software engineering, software safety and software testing (liuchao@buaa.edu.cn).



Yang Haiyan, born in 1974. Master and lecturer in Beihang University. Her main research interests include software engineering, software testing, software safety and requirement engineering (yhy@buaa.edu.cn).

Xing Liang, born in 1983. Engineer in Xi'an Aeronautics Computing Technique Research Institute, Aviation Industry Corporation of China. His main research interests include safety certification and software engineering (lionxing@163.com).