ISSN 1673-9418 CODEN JKYTA8
Journal of Frontiers of Computer Science and Technology
1673-9418/2000/00(00)-0000-00
doi: 10.3778/j.issn.1673-9418.

E-mail: fcst@vip.163.com
http://www.ceaj.org
Tel: +86-10-89056056

目标符合性论证中成本优化的证据收集方法

李璇，吴际+，刘超 ，杨海燕

北京航空航天大学 计算机学院，北京 100191

Evidence Collection Approach for Cost Optimization in Objectives Conformity Argument

LI Xuan, WU Ji+, LIU Chao,Yang Hai Yan

Department of Computer Science and Technology,BeiHang University,Beijing 100191,China

+ Corresponding author: Phn: +86-1352118276, E-mail: wujizeze@foxmail.com

LI Xuan,WU Ji,LIU Chao,YANG Hai Yan. Evidence Collection Approach for Cost Optimization in Objectives Conformity Argument. Journal of Frontiers of Computer Science and Technology, 2017, 0(0): 1-000.

Abstract: Objectives confirmity argument for standards is important issues in the field of airworthiness certification.In order to demonstrate that the objectives confirmation reaches the desired value, it is necessary to collect evidence further in the process of confirmity argument. However, due to the lack of effective methods to delineate the scope of evidence collection, evidence collection is usually costly and inefficient. Therefore, it is necessary to avoid collecting any evidence of inefficient and high collection costs to ensure that the total cost of evidence collection is lower when the objective compliance statement reaches the desired value. In this paper, an evidence collection approach based on dynamic programming is proposed to clarify the evidence and collection efforts. To evaluate the effectiveness of our approach, one case study,which of mul-ti-branch coverage,is conducted.

Key words: objectives conformity ; evidence; cost of evidence collection; collection efforts

摘 要: 面向标准的目标符合性论证是适航认证领域的重要研究内容。在论证过程中，为表明目标符合性论证结果满足期望要求，有必要进一步收集证据。然而，由于缺少有效的方法帮助划定证据收集范围，导致证据收集的结果往往是高成本低效力的。因此，必须避免收集任何低效力且高收集成本的证据，以确保在目标符合性论证结果满足期望要求时证据收集总成本较低。文中针对定量评估的论证方法，提出了一种成本优化的证据收集方案，以便于明确需收集的证据项及收集力度。通过一个覆盖多分支情况的案例，评估了方案的

有效性。

关键词: 目标符合性;证据;证据收集成本;收集力度
文献标志码：A 中图分类号：****

1 引言

证据定义为用于符合性论证的数据[1],即论证过程的输入。证据收集成本用于描述将该证据“能证明目标满足符合性要求”的置信度从 x 提升到 x+Δx 所花费的绝对成本。其中,Δx理解为证据收集力度。

在实际案例中，证据信息主要通过申请者从大量文档、源文件和测试日志等收集获得。依赖人主观判断的证据收集通常是耗时和易出错的[2][3]，这主要归因于以下 2 方面：1)收集者对目标的证据需求没有建立准确的认知，而收集大量无效的信息作为证据。2)论证结构中复杂的论证关系和论证方法使得收集者难以判断证据效力，可能消耗大量成本在低效力证据收集上或在同效力证据项中错误选择了高收集成本的证据。

在避免收集无效证据的问题上,Rajwinder 提出了一种基于 UML 的模型驱动方法[4][11]以获得安全标准下所需要的证据；文献[5]提出了一种基于 Systematic Literature Review (SLR)的安全证据收集、组织和论证的方法。但对于如何从已知有效的证据集中确定下一步待收集的证据和收集力度，以保证高效低成本的完成目标符合性从不满足期望值到满足期望值的提升，尤其对采用定量评估方法的目标符合性论证来说，仍缺少有效的方法。

结合上述问题，本文的目标是结合目标符合性论证结构和过程信息，为证据收集者提供一种成本优化的证据收集方法，以保证目标符合性能够从不满足期望值提升到满足期望值。结合上述目标，本文基于动态规划[6]的思想，提出了一种基于成本分配模型的证据收集方案。考虑到论证方法中定量评估[7]较定性评估[8]引入了置信度的概念和复杂计算，以及定量评估中 BNNs[9]和 D-S 证据理论[10]方法在数学层次上的关系，本文针对采用 D-S 证据理论和事件概率论证方法的目标符合性论证展开，更具有实际意义和拓展性。

本文第 2 节介绍了相关背景知识。第 3 节介绍了基于成本分配模型的证据收集方案的相关细节。第 4 节以案例的形式描述方案的实际应用过程，说明本文方案的有效性。第 5 节介绍了相关研究工作。第 6 节对本文工作进行总结并指出进一步的研究方向。

2 背景

2.1 论证模式

论证模式描述了证据对目标的向上论证关系，特别指出，子目标在用于论证父目标符合性时，被视为具有依赖的证据，这类证据不同于普通证据能够直接论证目标符合性，它们需要同其它子目标以“与”、“或”的方式来联合论证目标符合性。

在适航认证领域,目标或直接受普通证据论证，或至少存在两个子目标，存在子目标的目标不受普通证据直接论证，因为普通证据总能对应论证到该父目标的某一子目标项上。结合上述分析，论证结构主要包括四种基本论证模式，如图 1 所示。

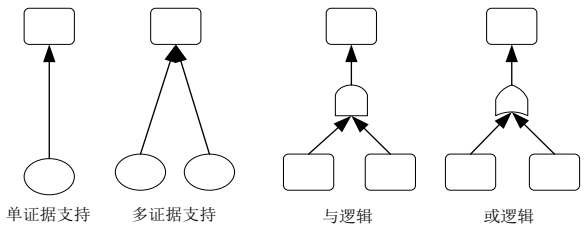


Fig 1 Four basic demonstration modes

图 1 四种基本论证模式

其中，“单证据支持”表示目标符合性仅受单一普通证据论证，体现为 1:1 的论证关系；“多证据支持”表示目标符合性受多条普通证据论证,体现为 1:n 的论证关系；“与逻辑”定性描述为所有子目标符合性均满足是判断目标符合性满足的充分条件，体现为 A&B→C 的论证关系；“或逻辑”定性描述为所有子目标符合性均满足是判断目标符合性满足的充分条件，体现为 A|B→C 的论证关系。文中将上述四种论证模式用一组统一描述规则定义如下：

定义 1 $AM =< Object, ESet, ArguType >$

$Eset = \{Evi_1, Evi_2, \cdots, Evi_n\}$

其中，Object 表示被论证目标；Eset 表示论证目标 Object 的证据集合；ArguType 表示 Eset 对 Object 的向上论证关系，null 表示 ESet 为普通证据集合，依据 ESet 中证据数量表现为单证据支持或多证据支持，and/or 表示 ESet 为 Object 的子目标集，论证模式分别表现为“与逻辑”和“或逻辑”。

无法用上述四种论证模式直观表达的论证关系称为复杂论证模式。

2.2 D-S 证据理论

D-S 证据理论作为一种不确定推理方法，主要特点是：满足比贝叶斯概率论更弱的条件；具有直接表达“不确定”的能力。本文对于“单证据支持”和“多证据支持”论证模式采用了 D-S 证据理论论证上级目标的符合性，主要涉及的领域概念如下：

⑴ 识别框架Θ

对于识别框架Θ，总存在以下假设，就是在框架Θ中存在且仅存在一种可能性是该判决问题的答案，即在Θ中存在着唯一的真值。

⑵ mass 函数（也称为基本可信度分配）

设识别框架Θ，如果$m: 2^{\Theta} \to [0,1]$(2^{Θ}为Θ的幂集)满足：$m(\emptyset) = 0, \sum_{A \subset \Theta}(A) = 1$，则称 m 为识别框架Θ上的基本可信度分配，$\forall A \subset \Theta$, m(A)为 A 的基本可信数，反映了对 A 本身的可信度大小。

⑶ 信度函数 Bel

设识别框架Θ，$m: 2^{\Theta} \to [0,1]$为识别框架Θ上的基本可信度分配，则称由$Bel(A) = \sum_{B \in A} m(B)$，$\forall A \subset \Theta$定义的函数$Bel: 2^{\Theta} \to [0,1]$为识别框架$\Theta$上的信度函数，反映了证据对 A 本身可信度的总支持度。

⑷ m 个 mass 函数的 Dempster 合成规则

对于$\forall A \subset \Theta$,识别框架Θ的有限个 mass 函数m_1，$m_2 \cdots m_n$的 Dempster 合成规则为：

$$(m_1 \oplus m_2 \oplus \cdots \oplus m_n)(A) = \frac{\sum_{A_1 \cap A_2 \cap \cdots \cap A_n = A} m_1(A_1) \cdot m_2(A_2) \cdots m_n(A_n)}{K}$$

$$K = 1 - \sum_{A_1 \cap A_2 \cap \cdots \cap A_n = \emptyset} m_1(A_1) \cdot (A_2) \cdots m_n(A_n)$$

2.3 事件概率

对于相互独立事件 A 和 B，A 与 B 均发生 A∩B 的概率为 P(AB)=P(A)P(B),A 与 B 至少一件事件发生 A∪B 的概率为 P(A+B)=P(A) + P(B) – P(A)P(B) = 1 – P($\overline{A}$)P($\overline{B}$)。

本文对于“与逻辑”和“或逻辑”论证模式分别采用了交事件和合事件论证上级目标的符合性。

2.4 证据收集成本

依据工程经验可知，证据收集成本与置信度的相关性可描述为同类证据同样将置信度提升差值Δt时，起始基准较小的证据所花费的成本会低于另一项，即置信度 v 从 0 提升到 0.3 花费的成本必定小于/等于 v 从 0.6 到 0.9 花费的成本，甚至有可能随着起始基准的增加使得成本指数性增长。考虑到证据优化方案关注于提升证据置信度所花费的绝对

成本，故而成本分布应依据证据置信度从当前值 v 提升Δt 所需的绝对成本 f(Δt,v)给出，实际使用中可借助 matlab 等依据实际工程数据拟合获得成本分布函数。

3 基于成本分配模型的证据收集方案

成本分配模型描述了提升顶级父目标符合性到期望值时所花费的最低证据收集总成本及对应的证据收集方案。

定义 2 $\mathrm{CTDModel} =< \mathrm{MinCost}, \mathrm{TraceList}, \mathrm{HisValue}, \mathrm{ReqValue} >$

$\mathrm{TraceList} = \{list_1, list_2, \ldots, list_m\}$

其中,MinCost 表示顶级父目标从 HisValue 提升到 ReqValue 花费的最小成本 ,TraceList 表示最小成本下的证据收集链集合。

成本分配模型的构建过程涉及到两个模型、一项指南和三个规则。“两个模型” 分别为目标符合性论证模型和目标符合性与成本关联模型，“一项指南” 为原生复杂论证模式转换指南，“三个规则” 为目标符合性提升范围划定规则、关联模型遍历规则和证据收集链构建规则。

目标符合性论证模型分别对适航领域存在的四种基本论证模式构建了对应的目标符合性论证公式，是目标符合性与成本关联模型构建要素之一。

目标符合性与成本关联模型定位于描述深度为 2 的论证结构下的顶级目标符合性成本关联关系，是成本分配模型实施过程的基本要素。

复杂论证模式转换指南能够保证上述两个面向四种基本论证模式的模型即使在存在复杂论证模式的情况下也能成功构建。

目标符合性提升范围划定规则用于为目标符合性与成本关联模型建立过程规避掉无效用的计算。

关联模型遍历规则描述了为论证结构中各目标建立关联模型时应遵循的构建顺序。

证据收集链构建规则描述了如何从顶级目标的关联模型中回溯获得最终的证据收集方案。

上述各模型与规则的作用关系如图 2 所示：

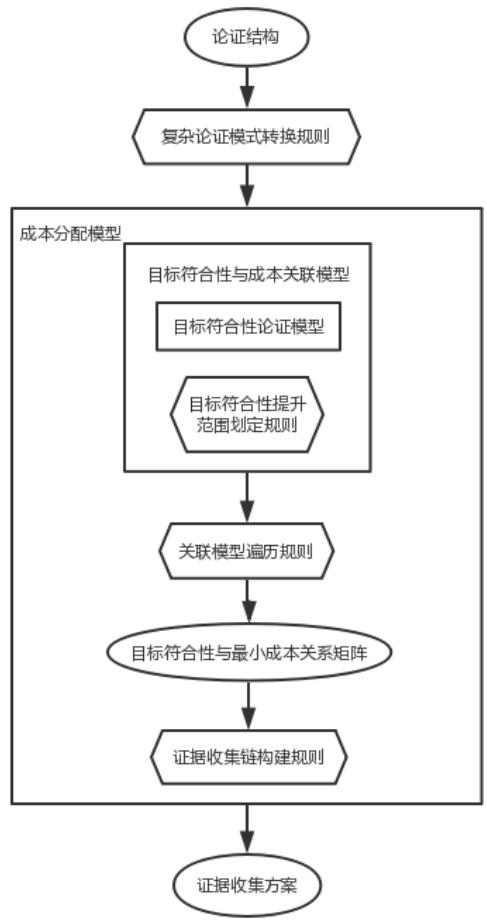


Fig.2 The relationship between model and rule

图 2 模型与规则作用关系图

3.1 目标符合性论证模型

目标符合性论证模型的定义如下：

定义 3 $\mathrm{AU}(\mathrm{CPSet}, \mathrm{ArguType})$

$\mathrm{CPSet} = \{cp_1, cp_2, \cdots, cp_n\}$

其中，CPSet 为证据 “能证明目标满足符合性要求” 的置信度 ,ArguType 为目标符合性论证方法。

当论证方法 ArguType 为 D-S 证据理论时，构

建识别框架Θ={valid,unvalid,uncertain},其中 valid 表示目标通过符合性认证这一断言成立的可信度，unvalid 表示目标通过符合性认证这一断言不成立的可信度，uncertain 表示不确定程度，则有

$$AU(CPSet,D\text{-}S)=(m_1 \oplus m_2 \oplus \cdots \oplus m_n)(valid) \quad (1)$$

当论证方法 ArguType 为事件概率中的交事件时，目标通过符合性认证这一断言成立的充分条件是各证据项均通过符合性认证，则有：

$$AU(CPSet, and)=\prod_{i=1}^{n} cp_i \quad (2)$$

当论证方法 ArguType 为事件概率中的合事件时，目标通过符合性认证这一断言成立的充分条件是存在证据项通过符合性认证，则有：

$$AU(CPSet, or) = 1 - \prod_{i=1}^{n}(1 - cp_i) \quad (3)$$

3.2 目标符合性与成本关联模型

关联模型以成本为目标函数，表示目标符合性程度每提升 *x* 所花费的证据收集成本。

定义 3 $CTCPModel =< DP, MinCost, Etuple, HisValue, ReqValue >$

$ETuple = \{Tuple_1, Tuple_2, \ldots, Tuple_n\}$

其中，DP 表示一种动态规划方案，是形成该关联模型的核心组件。HisValue 表示目标符合性当前值，ReqValue 表示目标符合性期望值，MinCost 表示将目标符合性从 HisValue 提升到 ReqValue 的最小成本，ETuple 表示收集成本为 MinCost 时的直接证据的收集方案，如下方式：

定义 4 $Tuple_i =< Evi_i, HisValue, ReqValue >$

DP 是以成本最低为目标的动态规划方案，其规划过程需要论证模式、论证方法、证据成本、目标符合性当前值和目标符合性期望值的支持。

定义 5 DP=<AM,AU,FSet,CPSet,HisValue, ReqValue>

FSet=$\{f_1, f_2, \ldots, f_n\}$,CPSet=$\{c_1, c_2, \ldots, c_n\}$

其中，AM 表示目标的论证模式，AU 表示目标符合性论证函数，FSet 表示证据成本集合,CPSet 表示证据符合性程度当前值集合。

假设对目标 g 建立符合性与成本的关联模型，其中目标 g 符合性受 n 个证据$e_1, e_2, \ldots, e_n$,论证，每个证据的初始符合性程度记为$c_i, i = 1,2, \ldots, n$,则 DP 动态规划方案执行步骤描述如下：

输入：AM,AU,FSet,CPSet,HistValue,ReqValue

输出：C(g,k,k')表示目标 g 符合性从k'提升到 k 所产生的最小成本；ETuple 表示最小成本下的证据提升分配方案；

约束条件: AU($\{t_1 + c_1, t_2 + c_2, \ldots, t_n + c_n\}$ ArguType) = ReqValue

步骤：

①k = ReqValue, k'= HisValue

②若 AM.ArguType=null,n=1,即论证模式为“单证据支持”，则:

C(g,k, k') = $f_1(t_1, c_1)$，ETuple=$\{<e_1, t_1, cp_1>\}$

③若 AM.ArguType=null 或 AM.ArguType=and, 即论证模式为“多证据支持”或“与逻辑”，则:

C(g,k,k') = E_g[k] [n], $E_g[k][1] = f_1(t_1, c_1)$

ETuple=$\{<e_1, t_1, c_1>, <e_2, t_2, c_2>, \ldots, <e_n, t_n, c_n>\}$

$E_g[k][i] = \min(E_g[k][i-1], \min(p_g(t_1, t_2, \ldots, t_i))$ $p_g(t_1, t_2, \ldots, t_i) = \sum_j^i f_j(t_j, c_j), cp_j + 0.01 \le k_j \le 1$

其中，$E_g[k][i]$表示最多提升目标 g 的前 i 个证据使得 A 符合性达到 k 的最低成本；$p_g(t_1, t_2, \ldots, t_i)$表示目标 g 的前 i 个证据提升到$t_i$所花费的成本。

④若 AM.ArguType=or 即论证模式为“或逻辑”：

$C(g, k, k') = \min(f_i(t_i, c_i))$ $ETuple = \{< e_i, t_i, c_i >\}$

上述动态规划方案，依据论证模型作为优化过程中的约束条件，使得输出结果总能保证目标符合性达到期望值。该关联模型的建立，将论证结构中各目标符合性的提升成本从未知转为已知，使得后续成本分配模型的得以展开。

3.3 复杂论证模式转换指南

目标符合性与成本关联模型应用场景建立在图 1 所描述的四种基本论证模式上。在论证结构中，可能会存在复杂论证模式，这类论证模式无法直接支持目标符合性与成本关联模型的建立。因此，本节给出一种转换指南指导复杂论证模式到基本论证模式的转换。转换的前提是保证论证结构转换前后的一致性，转换后论证模式应为四种基本论证模式的简单相加。

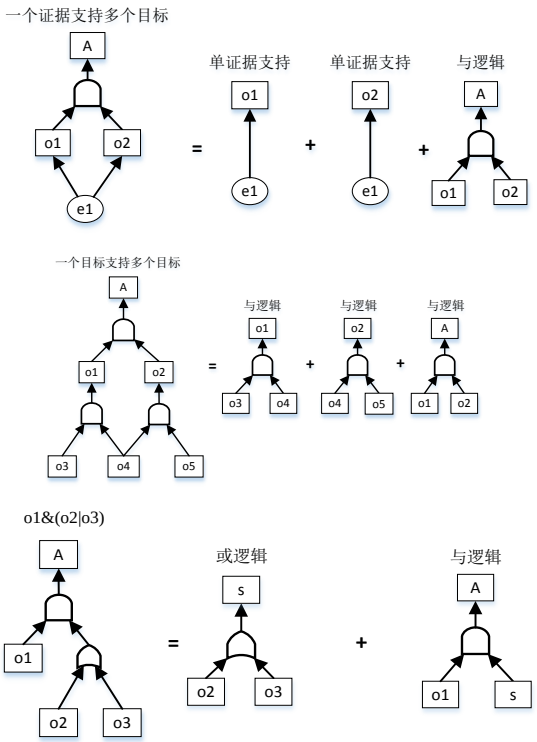
这里复杂论证模式指具有以下三种任意一种的表现形式：

⑴一个证据支持多个目标，表现为证据$\xrightarrow{1:n}$目标；

⑵一个目标支持多个目标，表现为目标$\xrightarrow{1:n}$目标；

⑶在同一目标→目标的论证维度下，无法用单一的“与逻辑”或“或逻辑”表示论证关系，表现为 A&(B|C)→D 或者 A|(B&C)→D。

针对上述三种表现形式，建立转换指南如下。



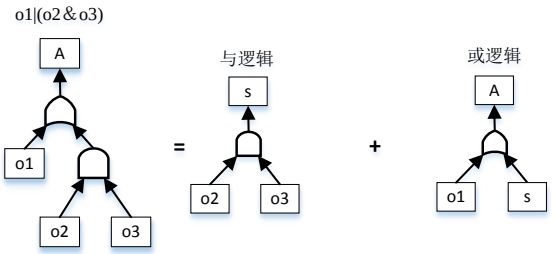


Fig 3 Conversion Guide

图 3 转换指南

3.4 目标符合性提升范围划定规则

目标符合性提升范围U_g=[a,b]定义了顶级父目标符合性达到期望值时目标 g 自身符合性允许的取值区间。其中，a 表示目标 g 的符合性至少要提升到 a 才使得顶级父目标符合性可能达到期望值，b 表示目标 g 的符合性提升到 b 时使得顶级父目标符合性必定达到期望值。

通过为目标 g 设定提升范围，可以为后续目标符合性与成本关联模型建立过程规避掉无效用的计算，因为提升目标 g 的置信度到 b 肯定比 b+ε的成本要低，而目标 g 的置信度<a 时获得的搜索组合无法使顶级目标置信度达到期望值。

目标符合性提升范围由父目标符合性的提升范围、目标符合性当前值及目标与父目标间的论证模式确定。依据上述要素，将影响性质划分为三类：

第一类目标：该类目标必使得顶级目标“通过符合性审查”的置信度小于期望值。

第二类目标：非第一类和第三类的目标。

第三类目标：该类目标必使得顶级目标“通过符合性审查”的置信度大于期望值。

设目标 g 的符合性当前取值为 HV，其父目标 r 的提升范围为U_p= [L,H]，则目标符合性提升范围U_g的划定规则如表 1 所示。

Table 1 Lifting range U_g=[a,b] delineation rules

表 1 提升范围U_g=[a,b] 划定规则

论证模式	目标类别	U_g=[a,b]
或逻辑	第 2 类	[HV+0.01,s], AU<{s, c_2, … , c_n},or> = H
与逻辑	第 1 类	[k,s], AU({s, c_2 … c_n}, and) = H
与逻辑	第 2 类	[HV+0.01,s],AU<{s, c_2, … , c_n},and>= H

3.5 关联模型遍历规则

建立父目标的符合性与成本关联模型的前提是其 1 级子目标均建立了成本关联模型。在面向完整论证结构时，只有位于论证结构最底层的普通证据的成本分布是给定的，各级目标的成本均需要通过建立目标符合性与成本关联模型获得。

结合上述分析，将论证结构看作一棵论证树，其中顶级父目标为树的根节点，各级子目标按照论证层次作为树中的各级节点，普通证据为树的叶节点，定义关联模型遍历规则如下：

⑴ 后根遍历论证树的各目标子树。

⑵ 访问根节点，即顶级目标。

3.6 证据收集链构建规则

证据收集链是组成证据收集方案的基本单位，其具有以下性质：

⑴假设以父目标构建一棵树，则其证据收集链即为以链首为根节点的 n 棵子树，子树叶节点构成该链首项的证据收集集合，所有子树的叶节点构成该父目标的证据收集集合。

⑵证据收集链的总数表示了所需要提升的 1 级子目标数。

证据收集链的构建过程，即是基于广度遍历的关联模型搜索过程。定义证据收集链构建规则如下：

⑴初始化 n 条证据收集链，n 表示顶级父目标关联模型下 Etuple 集中提升力度>0 的项的总数，上述 n 项即为链首。

⑵建立一棵以顶级父目标为根节点的树，其子节点即为上述 n 项目标。

⑶广度遍历树，若节点为目标，则获得该目标关联模型下 Etuple 集中提升力度>0 的 m 项，拓展为该节点的子节点；若节点为普通证据，不做处理。

⑷当遍历结束时，证据提升链构建完成。

4 案例分析

为了说明方案的有效性，案例全覆盖了文中提到的各分支情况，包括四种基本论证模式、复杂论证模式、不同类别的目标，能够很好的诠释本文提出的方案在案例中的实施过程。案例分析的目标是说明方案的有效性：1)方案能够覆盖标准符合性审查中的普遍论证模式 2)依据方案能够获得满足约束条件的证据收集建议。

选取 RTCA DO-178C[17]中的目标“High-level requirements comply with system requirements.” 作为顶级目标，其对应的目标符合性论证结构如图 4 所示，数据信息如表 2 所示。

A: High-level requirements comply with system requirements.

o1: All system requirements are satisfied by the high level requirements.

o2: Derived requirements and the reason for their existence are correctly defined.

o3: There is no derived requirements at all.

e1: Software Verification Results about the functional requirements compliance.

e2: Software Verification Results about the performance requirements compliance.

e3: Software Verification Results about the safety-related requirements compliance.

e4: Software Verification Results about the derived requirements compliance.

e5: Software Verification Results about the derived requirements recorded.

e6: Software Verification Results about the derived requirements recorded.

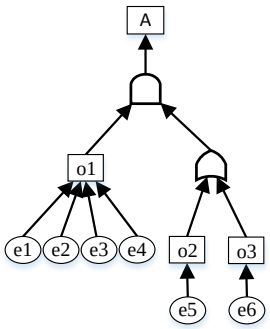


Fig 4 Argument structure

图 4 论证结构关系图

其中证据 e1,e2,e3,e4 到目标 o1 表现为多证据支持论证模式；证据 e5 到目标 o2 表现为单证据支持论证模式；证据 e6 到目标 o3 表现为单证据支持论证模式；目标 o1,o2,o3 到目标 A 表现为复杂论证模式。

Table 2 Basic data information

表 2 基本数据信息表

证据置信度	目标置信度	证据成本分布
e1=(0.6,0.3,0.1)	o1=(0.96,0.03,0.01)	$f_{e1}(\Delta t,p) = e^{20p\Delta t}$
e2=(0.5,0.2,0.3)	o2=(0.9,0.04,0.08)	$f_{e2}(\Delta t,p)=e^{5\Delta t}/\sqrt{1-p}$
e3=(0.7,0.1,0.2)	o3=(0.3,0.65,0.05)	$f_{e3}(\Delta t,p) = 30pe^{5\Delta t}$
e4=(0.7,0.05,0.25)	A=(0.89,0.06,0.05)	$f_{e4}(\Delta t,p)=20e^{0.1p+\Delta t}$
e5=(0.9,0.04,0.06)		$f_{e5}(\Delta t,p) = 3^{50p\Delta t}$
e6=(0.3,0.65,0.05)		$f_{e6}(\Delta t,p) =3^{50p\Delta t}$

其中，证据置信度与证据成本分布由申请人或专家提供，目标置信度通过上文中的目标符合性论证模型获得。在这里，本文问题重心定位为“目标符合性论证中成本优化的证据收集方法”,故前提条件中的证据置信度和证据成本分布均为仿真数据，真实数据由申请人或专家提供。

通过建立目标符合性与成本关联模型，获得目标 o1、o2 和 o3 的目标符合性与最小成本的对应关系如图 5 所示，其中 x 轴表示目标符合性取值，y 轴表示最小成本，(x,y) 表示将目标符合性从当前值提升到 x 所需的最小成本，数据标注描述了最小成本下的证据收集方案 Etuple。

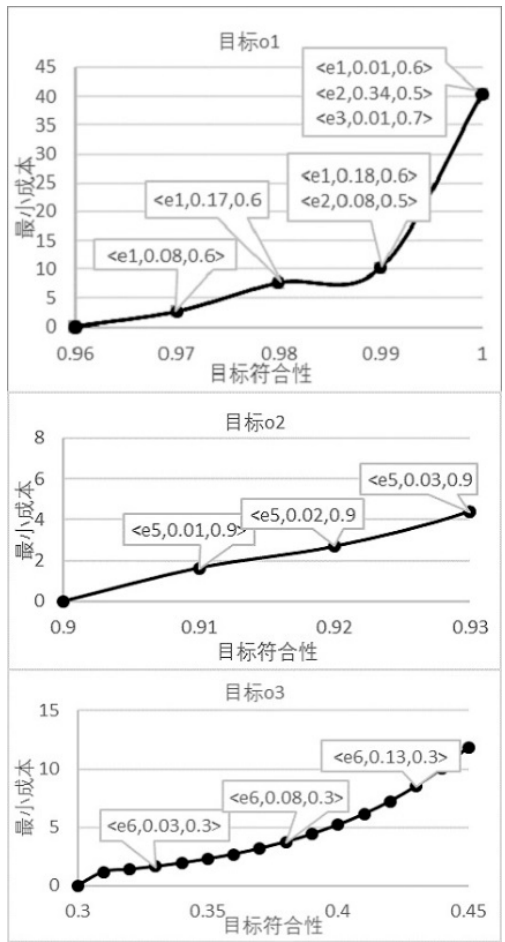


Fig 5 The relationship between object conformance and minimum cost

图 5 目标符合性与最小成本对应关系图

最后，对顶级父目标 A 建立关联模型，获得目标 A 符合性从 0.89 提升到 0.94 的最小成本为 19.67，对应的直接收集方案为 提升目标 o1 符合性到 0.97，提升目标 o2 符合性到 0.95，提升目标 o3 符合性到 0.4。依据证据收集链构建规则，获得最终的证据收集方案为表 3 所示。

Table 3 Evidence collection

表 3 证据收集方案

可收集证据项	收集力度Δt	效力

e1	0.08(0.6To0.68)	o1 的符合性从 0.96 到 0.97
e5	0.05(0.9To0.95)	o2 的符合性从 0.9 到 0.93
e6	0.1(0.3To0.4)	o3 的符合性从 0.3 到 0.4

在实际收集过程中，可围绕提高证据的完备率或证据可信度展开。其中，证据的完备率表明了其支持目标通过符合性审查的能力，而证据收集方式的差异将会影响证据的可信度。举例来说，支持软件版本质量满足目标“最新版本的测试失效数大于5”的要求的证据是”最新版本的测试失效数为 2”，假设该证据的置信度(0.7,0.1,0.2),若要提升置信度到（0.9,0,0.1），则可以考虑从 1)测试覆盖率 2)RTOS4A 复杂度 3)测试成本 4)测试方法等方面加以提升。

案例中覆盖了“基于证据的目标符合性评审”中会涉及到的四种论证模式，能够适用于符合性论证中的大多论证结构。同时，针对复杂的论证模式，给出了转换指南以指导完成复杂论证模式到基本论证模式的转换。说明目标符合性提升方案能够适用于多种论证场景。

将案例返回的证据优化方案作为验证信息，代入 e1=(0.68,0.3,0.02)，e2=(0.5,0.2,0.3)，e3=(0.5,0.2,0.3)，e5=(0.7,0.1,0.2)，e6=(0.4,0.6,0)到目标 A 的符合性论证中获得 A(0.941,0.052,0.007)，由于 0.941>0.94，说明目标符合性提升方案能够保证目标 A 的符合性达到期望值 0.94。

为验证证据收集方案划定的证据项是否满足高效低成本的要求，对目标 o1 的证据 e1,e2,e3,e4 在收集力度Δt =0.08 的效力和成本进行分析，得到表 4。

Table 4 The effectiveness of evidence and cost under the same collection effort

表 4 同收集力度下的证据效力和成本

可收集证据项	收集力度Δt	效力	成本
e1	0.08	o1 的符合性从 0.96 到 0.97	2.62
e2		o1 的符合性从 0.96 到 0.969	77.2
e3		o1 的符合性从 0.96 到 0.973	1146.56
e4		o1 的符合性从 0.96 到 0.973	23.24

依据表 4 可知，在同等收集力度，证据 e1 不仅效力不低于其它证据，且成本最低，说明了证据收集方案结果的合理性。

依据案例中各提供的各证据绝对成本分布函数绘制成本分布趋势如图 6 所示。

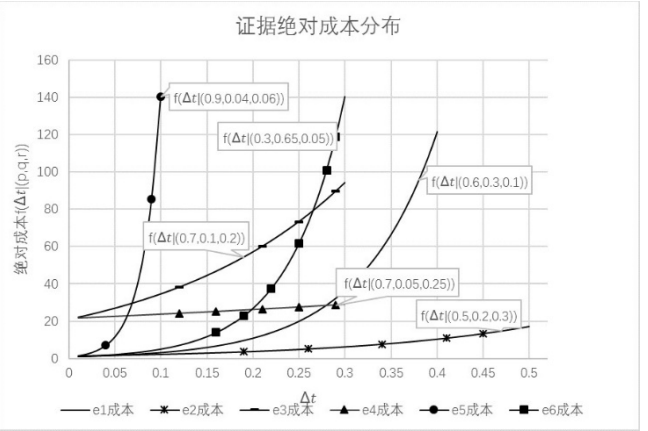


Fig 6 Evidence cost distribution

图 6 证据成本分布图

依据表 3 中的证据收集方案，观察图 6 中可知，各证据的收集力度Δt均控制在绝对成本 f(Δt,v)呈较低成本阶段，说明本文提出的以最低成本为目标提升方案是有效的。

5 相关工作

虽然目前存在与证据收集相关的研究和方法，但主要集中在如何避免收集无效证据和如何简化人工证据收集过程。

OMG(Object Management Group)在 2008 年提出的 SVBR(Semantic Business Vocabulary and Rules)[12] 和在 2011 年提出的 SACM(Structured Assurance

Case Model)[13],前者主要解决安全目标描述时自然语言表达的不一致性和二义性来描述安全目标,后者主要帮助构建和管理证据，但两者均缺少对证据收集过程的描述。

文献[5]提出了一种基于 SLRs 的安全证据收集、管理与评估的方法，但并未展开如何合理的组织证据来提高论证过程的相关研究。文献[14][15]设计了用于证据收集的工具。

基于上述相关研究，能够有效地帮助收集者收集与目标符合论证相关的有效证据，但忽略了有效证据间也存在论证效力和收集成本的差异。

本文从证据论证效力和收集成本出发，提出了一种新的证据收集角度来提升目标符合性论证结果，解决当前证据收集研究领域的局限性。

6 结束语

本文针对 D-S 证据理论和事件概率的目标符合性论证，提出了一种基于成本分配模型的证据收集方案，指导提升目标符合性到期望值的过程，以保证证据收集的成本较低。分析目标符合性论证结构，针对四种基本论证模式建立目标符合性关联模型，并为复杂论证模式建立转换指南以拓宽模型的适用性。在关联模型建立阶段，约束了目标符合性取值范围，有效地规避了无效用计算。在以后的研究中，将在关联模型的目标遍历规则中依据划分的目标类别构造遍历优先级，来代替当前平等的后根遍历算法以提高计算效率。此外，针对 BNNs 条件概率和主观逻辑与本方案采用论证方法具有相通性，可拓展方案到适用于上述两种论证方法中。

References:

[1] R. Weaver, G. Despotou, T. Kelly, J. McDermid, “Combining software evidence – arguments and assurance”, Workshop on Realising Evidence-Based Software Engineering, REBSE 2005.

[2] P. Rodriguez-Dapena, “Software safety certification: A multidomain problem”, IEEE Softw 16(4): 31-38, 1999.

[3] M.L. Squair, “Issues in the application of software safety standards”, in Austrailian Workshop on Safety Critical Systems and Software, 2005

[4] R. K. Panesar-Walawege, M. Sabetzadeh, and L. Briand, “A Model Driven Engineering Approach to Support the Verification of Compliance to Safety Standards,” in Software Reliability Engineering (ISSRE), 2011 IEEE 22nd International Symposium on, Nov 2011, pp. 30–39.

[5] Nair S, Vara J L D L, Sabetzadeh M, et al. Classification,Stru-cturing, and Assessment of Evidence for Safety -- A Systematic Literature Review[C]// IEEE Sixth International Conference on Software Testing, Verification and Validation. IEEE, 2013:94-103.

[6] Sahni S. Data structures, algorithms and applications in C++[J]. 2005.

[7]Darimont R, van Lamsweerde A. Formal refinement patterns for goal-driven requirements elaboration. In: Proc. of the 4th ACM Symp. on the Foundations of Software Engineering. San Francisco, 1996. 179−190. http://ing.de.soft1.googlepages.com/RefinementPatterns.pdf

[8] Aiello M, Giorgini P. Applying the Tropos methodology for analysing Web services requirements and reasoning about qualities of services. CEPIS Upgrade the European Journal of The Informatics Professional, 2004,5(4):20−26.

[9] M. Bouissou, F. Martin, A. Ourghanlian, “Assessment of a safety-critical system including software: a bayesian belief network for evidence sources”, In: Annual Reliability and Maintainability Symposium, 1999.

[10] G. Shafer, A Mathematical Theory of Evidence, Princeton Univ.Press, Princeton, NJ, 1979.

[11] D. Falessi, M. Sabetzadeh, L. Briand, E. Turella, T. Coq, and R. K. Panesar-Walawege, “Planning for Safety Evidence Collection: A ToolSupported Approach Based on Modeling of Standards Compliance Information,” IEEE Software, vol. pp, no. 99, 2011.

[12] “Semantics of Business Vocabulary and Business Rules (SBVR), version 1.0,” 2008.

[13] “Structured Assurance Case Metaodel (SACM), version 1.0,” 2013.

[14] OPENCOSS. Accessed Nov 18, 2014. [Online]. Available: http://www.opencoss-project.eu/

[15] iFast. Accessed Nov 18, 2014. [Online]. Available: http://www.artemisifest.eu/home.

[16] “Software Consideration in Airborne Systems and Equipment Certification: RTCA DO-178C,” Dec 2011.

[17] DO R. 178C[J]. Software Considerations in Airborne Systems and Equipment Certification, 2011.

1 寸数字照片
须为证件照，不能提供生活照，不能低于 300 像素

LI Xuan was born in 1993.She is an M.S. candidate at BeiHang University. Her research interest is software engineering.

李璇（1993-），女，山东菏泽人，北京航空航天大学硕士研究生，主要研究领域为软件工程。

1 寸数字照片
须为证件照，不能提供生活照，不能低于 300 像素

WU Ji was born in 1974.He is an associate professor at BeiHang University.His research interests include Software security and reliability and embedded software design and verification.

吴际(1974–)，男，安徽合肥人，北京航空航天大学副教授，主要研究领域为软件安全性与可靠性、嵌入式软件设计与验证。

1 寸数字照片
须为证件照，不能提供生活照，不能低于 300 像素

LIU Chao was born in 1958. He is a professor at BeiHang University.His research interests include Software testing, object-oriented technology and software development environment..

刘超(1958–)，男，北京人，北京航空航天大学教授，主要研究领域为软件测试、面向对象技术、软件开发环境。

1 寸数字照片
须为证件照，不能提供生活照，不能低于 300 像素

YANG Hai Yan was born in 1974.She is lecturer at BeiHang University. Her research interest is software engineering.

杨海燕(1974–)，女，重庆人，北京航空航天大学讲师，主要研究领域为软件工程。