**中图分类号：TP311.5**

**论文编号：10006SY1306227**



硕 士 学 位 论 文

**面向DO-178C的软件过程目标满足性论证支撑技术研究**

作者姓名 杨 阳

学科专业 软件工程

指导教师 刘 超 教授

培养院系 计算机学院

**Research on the Technology for Supporting Objectives Conformity Argument Based on DO-178C**

A Dissertation Submitted for the Degree of Master

**Candidate： Yang** **Yang**

**Supervisor：** **Prof. Liu Chao**

School of Computer Science & Engineering

Beihang University, Beijing, China

**中图分类号：TP311.5**

**论文编号：10006SY1306227**

硕 士 学 位 论 文

面向DO-178C的软件过程目标满足性论证支撑技术研究

作者姓名 杨 阳 申请学位级别 工学硕士

指导教师姓名 刘 超 职 称 教授

学科专业 软件工程 研究方向 适航软件安全性验证

学习时间自 2013 年 9 月 5 日 起至 2015 年 12 月 21 日止

论文提交日期 2015年 12 月 24 日 论文答辩日期 2015 年 12 月 21 日

学位授予单位 北京航空航天大学 学位授予日期 2016 年 1 月 8 日

关于学位论文的独创性声明

本人郑重声明：所呈交的论文是本人在指导教师指导下独立进行研究工作所取得的成果，论文中有关资料和数据是实事求是的。尽我所知，除文中已经加以标注和致谢外，本论文不包含其他人已经发表或撰写的研究成果，也不包含本人或他人为获得北京航空航天大学或其它教育机构的学位或学历证书而使用过的材料。与我一同工作的同志对研究所做的任何贡献均已在论文中作出了明确的说明。

若有不实之处，本人愿意承担相关法律责任。

学位论文作者签名：        日期： 年 月 日

学位论文使用授权书

本人完全同意北京航空航天大学有权使用本学位论文（包括但不限于其印刷版和电子版），使用方式包括但不限于：保留学位论文，按规定向国家有关部门（机构）送交学位论文，以学术交流为目的赠送和交换学位论文，允许学位论文被查阅、借阅和复印，将学位论文的全部或部分内容编入有关数据库进行检索，采用影印、缩印或其他复制手段保存学位论文。

保密学位论文在解密后的使用授权同上。

学位论文作者签名： 日期： 年 月 日

指导教师签名： 日期： 年 月 日

# 摘 要

机载软件需要符合适航审定标准，通过局方的适航审定，才能投入使用。DO-178C是一种广泛使用的适航审定标准。为了论证机载软件是否符合适航审定标准，使用比较广泛的一种方法是基于证据的目标满足性论证。

目标结构化表示法（Goal Structing Notation，GSN）是目前一种主要的基于证据的目标满足性论证方法。但是，在使用GSN建立基于证据的论证模型来论证适航软件是否满足DO-178C标准时，发现存在如下问题：现有GSN表示符号需要扩展以便完成目标满足性论证模型的构建；目标论证间存在相似性或重复现象，造成构建论证模型时，存在大量繁琐的重复性工作；特别是当针对不同项目构建论证模型时，如果总是从头开始构建，必然存在大量重复工作。

为了解决上面提出的问题，本文提出目标满足性论证模式，并提出了依据DO-178C提取项目无关的目标满足性论证模式的方法，建立了DO-178C标准中软件验证过程的目标满足性论证模式，并据此提出了论证模式实例化方法，以构建项目相关的目标满足性论证模型。

用户依据本文提出的方法就可以建立项目相关目标满足性论证模型，并且论证模型满足DO-178C标准规定。本文归纳总结出DO-178C标准中目标间的相似性，并加以利用，使得一个目标满足性论证模式能够表达多个DO-178C的目标。此外，本文建立的目标满足性论证模式有效抽取项目无关的论证结构，提高了论证模型的复用性。不同的项目，可能会实例化出相似的但不完全相同的论证结构。

本文开发了目标满足性论证建模工具来支持本文提出的方法。工具提供了GSNEdit编辑器来编辑目标满足性论证模型，GSNModelEdit编辑器来编辑目标满足性论证模式，模型管理模块支持用户实现从目标满足性论证模式向目标满足性论证模型的转化。

最后，在建模工具的支持下，运用本文提出的目标满足性论证模式概念，运用了基于模式的实例化方法建立一组针对某机载操作系统项目的目标满足性论证模型，验证了本文提出的方法的可行性，以及工具的有效性。

**关键词**：目标满足性论证模型，DO-178C，目标结构化表示法，论证模式

# Abstract

Airborne software can be executed in the system, only when the aircraft certification authority approve software in compliance with certification standards.DO-178C“Software Considerations in Airborne Systems and Equipment Certification”is a widely used certification standard. Generally people use objectives compliance argument based on evidence to prove if the software is comply with certification standards or not.

Tim Kelly proposed GSN（Goal Structing Notation）. It is a popular method which can express objectives compliance argument based on evidence. However, when GSN is used to construct objectives compliance argument for airborne software, the problems exist as follows: We need to extend GSN expressions for objectives compliance argument model. The objectives have repeating argument, which would increase the amount of work for constructing argument model. When people construct arugment model for different projects, they always construct them from the first step, this method make people do much repetitive work.

We propose objectives compliance argument pattern as solution for the above problems. We also propose methods to extract objectives compliance argument pattern based on DO-178C standard in software verification process. And based on these, we propose instantiation method to construct objectives compliance argument model based on standard and projects.

The methods we proposed in this paper can solve the problem that it is difficult to construct objectives compliance argument model which are related to specific projects, user can construct accurate objectives compliance argument model based on methods we proposed in this paper. We also summarized and took advantage of the similarity in objectives of DO-178C, so one objectives compliance argument pattern can stand for several objectives in DO-178C. And the pattern also extracts the argument structure which is related to standard, this can improve the reusability for argument.

In this paper, we carried out a tool which can construct both objectives compliance argument pattern and objectives compliance argument model. The tool provides an editor called GSNEdit, the editor can edit objectives compliance argument model. The tool also provides an editor called GSNModelEdit, the editor can edit objectives compliance argument pattern. The tool provides a model management module to support prople transform the objectives compliance argument pattern to objectives compliance argument model.

Finally, we integrate the methods for constructing objectives compliance argument pattern and objectives compliance argument model. Through the tool we developed, we used our methods in a real program which is an airborne operating system, which proves the feasibility of the methods and the effectiveness of the tool.

**Key words**: Objectives conformity argument model, DO-178C, GSN (Goal Structing Notation), Argument pattern

# 目 录

[第一章 绪论 1](#_Toc438763662)

[1.1 选题背景和意义 1](#_Toc438763663)

[1.2 国内外研究现状 2](#_Toc438763664)

[1.2.1 DO-178C标准相关研究 2](#_Toc438763665)

[1.2.2 安全案例相关研究 3](#_Toc438763666)

[1.2.3 GSN相关研究 4](#_Toc438763667)

[1.2.4 使用GSN表达的安全案例模式相关研究 4](#_Toc438763668)

[1.3 研究目标及主要研究内容 5](#_Toc438763669)

[1.3.1 建立基于DO-178C标准的目标满足性论证模式 5](#_Toc438763670)

[1.3.2 实例化目标满足性论证模式 5](#_Toc438763671)

[1.3.3 目标满足性论证建模工具的设计和实现 6](#_Toc438763672)

[1.4 论文组织结构 6](#_Toc438763673)

[第二章 适航软件基于标准的目标论证技术综述 8](#_Toc438763674)

[2.1 DO-178C系列标准 8](#_Toc438763675)

[2.1.1 DO-178C标准 8](#_Toc438763676)

[2.1.2 DO-178C标准相关标准 9](#_Toc438763677)

[2.1.3 DO-178C标准相关研究 9](#_Toc438763678)

[2.2 安全案例及GSN 10](#_Toc438763679)

[2.2.1 安全案例 10](#_Toc438763680)

[2.2.2 目标结构化表示法GSN（Goal Structuring Notation） 11](#_Toc438763681)

[2.2.3 安全案例模式Safety Case Pattern 12](#_Toc438763682)

[2.3 GMF（Graphical Modeling Framework）框架 14](#_Toc438763683)

[2.4 小结 14](#_Toc438763684)

[第三章 基于DO-178C的目标满足性论证模式抽取方法研究 16](#_Toc438763685)

[3.1 研究目标与方法 16](#_Toc438763686)

[3.2 GSN扩展符号 16](#_Toc438763687)

[3.3 目标满足性论证模式的建模方法 17](#_Toc438763688)

[3.4 评审分析目标满足性论证模式 19](#_Toc438763689)

[3.4.1 评审和分析的目标满足性论证结构 19](#_Toc438763690)

[3.4.2 评审和分析的目标满足性论证模式 29](#_Toc438763691)

[3.5 软件测试目标满足性论证模式 31](#_Toc438763692)

[3.5.1 软件测试目标满足性论证结构 31](#_Toc438763693)

[3.5.2 软件测试目标满足性论证模式 37](#_Toc438763694)

[3.6 测试需求覆盖率目标满足性论证模式 39](#_Toc438763695)

[3.6.1 测试需求覆盖率目标满足性论证结构 40](#_Toc438763696)

[3.6.2 测试需求覆盖率目标满足性论证模式 42](#_Toc438763697)

[3.7 结构测试覆盖率目标满足性论证模式 44](#_Toc438763698)

[3.7.1 结构测试覆盖率目标满足性论证结构建立 44](#_Toc438763699)

[3.7.2 结构测试覆盖率目标满足性论证模式 48](#_Toc438763700)

[3.8 小结 49](#_Toc438763701)

[第四章 建立基于DO-178C的目标满足性论证模型方法研究 51](#_Toc438763702)

[4.1 建立目标满足性论证模型方法分析 51](#_Toc438763703)

[4.2 目标满足性论证模式实例化 51](#_Toc438763704)

[4.2.1目标满足性论证模式实例化方法 51](#_Toc438763705)

[4.2.2目标满足性论证模型示例 53](#_Toc438763706)

[4.3 目标满足性论证模型文本表达方法 54](#_Toc438763707)

[4.4 小结 55](#_Toc438763708)

[第五章 目标满足性论证建模工具的设计与实现 56](#_Toc438763709)

[5.1 工具需求分析与整体设计 56](#_Toc438763710)

[5.2 GSNEdit编辑器 57](#_Toc438763711)

[5.2.1 GSNEdit工具体系结构设计 57](#_Toc438763712)

[5.2.2 GSNEdit工具元模型设计 57](#_Toc438763713)

[5.2.3 GSNEdit工具实现 59](#_Toc438763714)

[5.3 GSNModelEdit编辑器 60](#_Toc438763715)

[5.3.1 GSNModelEdit工具体系结构设计 60](#_Toc438763716)

[5.3.2 GSNModelEdit工具元模型设计 60](#_Toc438763717)

[5.3.3 GSNModelEdit工具实现 62](#_Toc438763718)

[5.4 模型管理实现 62](#_Toc438763719)

[5.4.1 模型转换模块设计与实现 63](#_Toc438763720)

[5.4.2 模型验证模块设计与实现 64](#_Toc438763721)

[5.5 小结 65](#_Toc438763722)

[第六章 实验分析 67](#_Toc438763723)

[6.1 实验目的 67](#_Toc438763724)

[6.2 实验方案设计 67](#_Toc438763725)

[6.3 实验项目背景 68](#_Toc438763726)

[6.4 目标满足性论证模式-目标满足性论证模型间的转换 68](#_Toc438763727)

[6.4.1 目标满足性论证模型（原型） 69](#_Toc438763728)

[6.4.2 建立并实例化目标满足性论证模式 70](#_Toc438763729)

[6.4.3 转化为目标满足性论证模型 71](#_Toc438763730)

[6.4.4 实验结果对比 73](#_Toc438763731)

[6.5 模型验证 74](#_Toc438763732)

[6.5.1 描述属性不为空 74](#_Toc438763733)

[6.5.2 论证符号不能与自身建立连接 75](#_Toc438763734)

[6.6 小结 75](#_Toc438763735)

[总结与展望 76](#_Toc438763736)

[参考文献 78](#_Toc438763739)

[攻读硕士学位期间取得的学术成果 81](#_Toc438763740)

[致 谢 82](#_Toc438763741)

# 图 目

[图 1 简化的DO-178C主要论证结构 10](#_Toc438763742)

[图 2 安全案例 10](#_Toc438763743)

[图 3 安全案例模式示例 13](#_Toc438763744)

[图 4 GMF工作流 14](#_Toc438763745)

[图 5 目标满足性论证模式建模流程 18](#_Toc438763746)

[图 6 软件高层需求评审分析的目标满足性论证结构 22](#_Toc438763747)

[图 7 软件低层需求评审分析的目标满足性论证结构 24](#_Toc438763748)

[图 8 软件体系结构评审分析的目标满足性论证结构 26](#_Toc438763749)

[图 9 软件源代码评审分析的目标满足性论证结构（1） 28](#_Toc438763750)

[图 10 软件源代码评审分析的目标满足性论证结构（2） 29](#_Toc438763751)

[图 11 评审和分析目标满足性论证模式1 31](#_Toc438763752)

[图 12 高层需求-可运行代码符合性目标满足性论证结构 34](#_Toc438763753)

[图 13 高层需求-可运行代码健壮性目标满足性论证结构 36](#_Toc438763754)

[图 14 低层需求-可运行代码符合性目标满足性论证结构 37](#_Toc438763755)

[图 15 低层需求-可运行代码健壮性目标满足性论证结构 37](#_Toc438763756)

[图 16 软件测试目标满足性论证模式（1） 38](#_Toc438763757)

[图 17 软件测试目标满足性论证模式（2） 39](#_Toc438763758)

[图 18 测试高层需求组覆盖率目标满足性论证结构 42](#_Toc438763759)

[图 19 测试低层需求组覆盖率目标满足性论证结构 43](#_Toc438763760)

[图 20 测试需求覆盖率目标满足性论证模式 43](#_Toc438763761)

[图 21 MC/DC覆盖率目标满足性论证结构 46](#_Toc438763762)

[图 22 判定覆盖率目标满足性论证结构 47](#_Toc438763763)

[图 23 语句覆盖率目标满足性论证结构 48](#_Toc438763764)

[图 24 结构测试覆盖率目标满足性论证模式 49](#_Toc438763765)

[图 25 目标满足性论证模型建立流程 51](#_Toc438763766)

[图 26 项目相关目标满足性论证模型 54](#_Toc438763767)

[图 27 工具构件图 56](#_Toc438763768)

[图 28 GSNEdit工具构件图 58](#_Toc438763769)

[图 29 GSNEdit工具元模型 58](#_Toc438763770)

[图 30 GSNEdit工具元模型（类图） 59](#_Toc438763771)

[图 31 GSNEdit工具界面 59](#_Toc438763772)

[图 32 GSNModelEdit工具构件图 60](#_Toc438763773)

[图 33 GSNModelEdit工具元模型 61](#_Toc438763774)

[图 34 GSNModelEdit工具元模型（类图） 61](#_Toc438763775)

[图 35 GSNModelEdit工具界面 62](#_Toc438763776)

[图 36 第一组实验流程图 68](#_Toc438763777)

[图 37 测试低层需求覆盖率目标满足性论证模型（原型） 69](#_Toc438763778)

[图 38 语句覆盖率目标满足性论证模型（原型） 69](#_Toc438763779)

[图 39 目标满足性论证模型（原型） 69](#_Toc438763780)

[图 40 实例化的测试需求覆盖率目标满足性论证模式 70](#_Toc438763781)

[图 41 实例化的语句覆盖率目标满足性论证模式 71](#_Toc438763782)

[图 42 实例化的目标满足性论证模式 71](#_Toc438763783)

[图 43 测试低层需求覆盖率目标满足性论证模型 72](#_Toc438763784)

[图 44 语句覆盖率目标满足性论证模型 72](#_Toc438763785)

[图 45 目标满足性论证模型 73](#_Toc438763786)

[图 46 name属性不能为空 75](#_Toc438763787)

[图 47 论证符号不能关联自身 75](#_Toc438763788)

# 表 目

[表 1 失效的等级划分 8](#_Toc438763789)

[表 2 GSN图形符号含义 11](#_Toc438763790)

[表 3 GSN连接符号含义 12](#_Toc438763791)

[表 4 基于模式的GSN扩展符号含义 12](#_Toc438763792)

[表 5 基于模式的实体抽象扩展符号含义 13](#_Toc438763793)

[表 6 GSN扩展符号含义 16](#_Toc438763794)

[表 7 软件高层需求评审分析目标解读 20](#_Toc438763795)

[表 8 软件高层需求评审分析证据结构 22](#_Toc438763796)

[表 9 软件体系结构评审分析目标解读 24](#_Toc438763797)

[表 10 软件源代码评审分析目标解读 27](#_Toc438763798)

[表 11 高层需求-可运行代码符合性目标解读 32](#_Toc438763799)

[表 12 高层需求-可运行代码符合性证据结构 33](#_Toc438763800)

[表 13 高层需求-可运行代码健壮性目标解读 34](#_Toc438763801)

[表 14 测试高层需求覆盖率目标解读 40](#_Toc438763802)

[表 15 测试高层需求覆盖率证据结构 41](#_Toc438763803)

[表 16 MC/DC覆盖率目标解读 45](#_Toc438763804)

[表 17 MC/DC覆盖率证据结构 46](#_Toc438763805)

[表 18 元模型间转换对应关系 63](#_Toc438763806)

[表 19 ETL语言编写的Egoal2Goal转换规则 63](#_Toc438763807)

[表 20 EVL语言编写的HasName约束 64](#_Toc438763808)

[表 21 低层需求覆盖率模型论证结果对比 73](#_Toc438763809)

[表 22 语句覆盖率模型论证结果对比 73](#_Toc438763810)

[表 23 所有模型论证结果对比 74](#_Toc438763811)

# 第一章 绪论

## 1.1 选题背景和意义

机载软件是安全关键性软件（Safety Critical Software），需要符合适航审定标准并通过局方的适航审定才能投入使用。因此，论证机载软件是否符合适航审定标准成为一项值得关注的问题。

目前，针对机载软件的适航审定，应用最广泛的是美国航空无线电委员会发布的《机载系统和设备合格审定中的软件考虑》RTCA DO-178C[[[1]](#endnote-2)]以及其它与之相关的标准：DO-278A[[[2]](#endnote-3)]（空中交通管制的软件完整性考虑），DO-248C[[[3]](#endnote-4)]（DO-178C和DO-278A的补充文档），DO-330[[[4]](#endnote-5)]（软件工具鉴定考虑），DO-331[[[5]](#endnote-6)]（对DO-178C和DO-278A的基于模型开发验证的补充文档），DO-332[[[6]](#endnote-7)]（对DO-178C和DO-278A的面向对象方法及其相关技术的补充文档），DO-333[[[7]](#endnote-8)]（对DO-178C和DO-278A的形式化方法的补充文档），上述文件形成了DO-178C标准体系。

目前有多种论证机载软件满足DO-178C标准的方法，使用比较广泛的是基于证据的目标满足性论证，即针对DO-178C标准中规定的目标和相关要求，构建相应的目标满足性论证模型，并通过对软件开发过程及其制品数据的分析，提取论证模型中所需证据，并据此来论证软件开发过程及其最终产品是否满足标准中的各项目标，即符合标准中规定的各项目标和相关目标。这种基于证据的论证方法不仅适用于标准满足性的论证，同样也适用于软件安全性论证。

为了能够使用结构化的表达方式表示基于证据的论证模型，目前存在表达方式-CAE。此外，还有一种广泛使用的表达方法，是由英国约克大学的Tim Kelly教授及其团队提出的目标结构化表示法（Goal Structing Notation，GSN)[[[8]](#endnote-9)]。这种表示方法用于表示基于证据的论证模型。但是，使用GSN符号建立基于证据的模型来论证适航软件是否满足DO-178C标准时，存在如下问题：

1. 基于模式的GSN扩展符号表达目标满足性论证模型时，部分论证结构缺少合适的符号表示。

2. DO-178C标准中，相同阶段不同目标有时会执行相似的活动，得到相似的输出。在进行基于证据的建模方案时，往往忽略了目标与目标之间这一潜在的关联，从而将时间和精力浪费在重复进行相似论证的过程中。

3. 针对不同项目建立基于证据的论证模型时，应当避免重新阅读DO-178C标准和重新建立论证模型。但是，目前尚缺少一种有效的方案，将DO-178C中项目无关的论证结构提取出来，在建立不同项目的论证模型时，有效利用项目无关的论证结构，提高论证结构的复用性。

为了解决上述三个问题，本文提出了提取目标满足性论证模式的方法并提出了目标满足性论证模式；并据此提出实例化的方法，最终建立项目相关的论证模型。

这种方法是一种层次化的方案。用户在本文提出的目标满足性论证模式的基础上，采用本文提出的实例化方法，可以建立项目相关的目标满足性论证模型。

本文提出的目标满足性论证模式，找出目标间的潜在关联，可以表达具有相似论证结构的两个或多个目标。利用目标之间的关联，提高了目标满足性论证结构的复用性。

本文提出的实例化方法，能够通过实例化目标满足性模式，建立目标满足性论证模型。因此，不同的项目可以依据相同的目标满足性论证模式，通过对模式中相关参量或选择项的实例化，为该项目建立针对相应目标的目标满足性论证模型。利用了项目无关的论证结构，提高了目标满足性论证模型的复用性。

## 1.2 国内外研究现状

### 1.2.1 DO-178C标准相关研究

DO-178C标准针对9个软件过程提出了71个安全目标，以保证航空软件以规范的方式进行开发，并以规范的方式排除软件缺陷，修复代码漏洞，从过程上保证软件最终达到所需的安全性[1]。

DO-178C标准对依据安全评估确定不同安全等级的软件，提出了不同的目标。软件一共分为5个安全等级，其中A级软件需要满足所有的71个目标，即A级软件对安全性的要求最高。B，C，D级软件需要满足的目标数量依次递减，E级软件由于实际上不会影响飞机的安全性，因此没有安全性方面的具体要求。

美国NASA的研究员C. Michael Holloway从事DO-178C标准的相关研究[[[9]](#endnote-10)][[[10]](#endnote-11)][[[11]](#endnote-12)]，他利用担保案例（assurance case）来表示如何根据DO-178C标准中提出的各项安全目标论证DO-178C标准的总目标。其中，DO-178C标准的总目标是：适航软件具有必需的安全性保证，并符合适航要求。在文献[9]中，作者对不同等级的软件建立了相应的担保案例，说明不同等级的软件如何根据DO-178C标准中的各个安全目标来论证其总目标。

国内，也有一些针对DO-178B/C标准的研究。胡宁对比了DO-178B与DO-178C标准的相同和不同之处，并分析了DO-178C试图关注的重点[[[12]](#endnote-13)]。文献[[[13]](#endnote-14)]中，介绍了如何进行DO-178B中规定的结构覆盖分析活动，及其在实际项目中的应用情况。

在标准领域，为了帮助实现DO-178C标准的认证，美国联邦航空管理局（FAA）提出了软件审批指南（Software Approval Guidelines）[[[14]](#endnote-15)]。《软件审批指南》为适航审定部门提供帮助，以确定如何审定适航软件是否符合DO-178C标准。它对DO-178C中规定的活动，以及输出有了进一步详细的解释，提出了其中需要关注的要点，为建立目标满足性论证模式提供了重要的指导。

### 1.2.2 安全案例相关研究

担保案例（assurance case）是指一系列可以编辑的目标、论证过程以及证据组成的层次化论证结构。同时，论证过程和证据用来支撑该目标，论证定义的系统会满足该论证结构的总目标[[[15]](#endnote-16)]。安全案例（safety case）属于担保案例的一种，就是说安全案例是指通过一系列可以编辑的目标、论证过程以及证据，来论证所定义的系统满足特定的安全性需求。当前比较常用的安全目标论证手段是基于证据的安全论证[[[16]](#endnote-17)]。

关于安全案例的研究有很多，[Fuping Zeng](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Fuping%20Zeng.QT.&newsearch=true)提出了基于安全案例的软件安全性认证框架[[[17]](#endnote-18)]。这个框架包括了安全目标获取，论证结构的组成以及证据的选择。并应用于工程化项目中说明该框架的有效性。关于安全案例相关概念的解释，文献[[[18]](#endnote-19)]指出：安全案例是推理系统为什么安全的论证过程；描述性的安全案例是反映实际安全案例的镜像；安全案例报告用来细化安全论证的概念。上述三种概念看似相似，其实是不能够混淆的，为了理解安全案例，必须对它们的概念有清晰的认识。

此外，针对GSN在证据需求描述中存在的问题，Rajwinder K. Panesar-Walawege提出使用证据模型来描述安全证据类型和结果，目的在于提高证据需求的可重用性[[[19]](#endnote-20)]。关于证据追溯性方面的研究，文献[[[20]](#endnote-21)]总结了目前的追溯性存在的七个领域，并指出工业界和学术界应该联合起来解决追溯性的问题。文献[[[21]](#endnote-22)]为评估安全证据的有效性提出了一套方法，按照这种方法提出的步骤来判断安全证据是否有效。此外，文献[[[22]](#endnote-23)]提出了基于证据是软件过程数据还是软件产品数据，将证据进行分类的方法。

### 1.2.3 GSN相关研究

GSN[8]是一种表达担保案例（assurance case）的图形化符号。该方法是由英国约克大学的Tim Kelly教授首次提出。目前，已经广泛应用到描述安全案例的领域中，得到了大家的认可。关于GSN的研究已很多，文献[[[23]](#endnote-24)]定义了GSN的元模型，为模型化GSN提供了基础。文献[[[24]](#endnote-25)]提出了对GSN模型的扩展方法，主要有两种，第一种是从论证模式方向上的扩展。主要包括了连接线上的扩展，提出了“或”关系的表示方法，以及一个父目标分解为多个同类子目标的表示方法。同时也定义了实例化目标的表现形式；第二种是从模块化方向上的扩展，包括引用其他论证结构的表现形式，引用其他论证结构中其他目标的表现形式，引用其他解决方案的表现形式，引用其它上下文结构的表现形式等。除此之外，文中还提出了建立GSN的方法，主要分为两种，自顶向下的方法，以及自底向上的方法。

文献[[[25]](#endnote-26)]提出了当系统发生的变更对建立的安全案例产生影响时，定义一种安全案例的扩展符号，使其能够表示这种变更的方法。以方便实现对安全案例的管理。

### 1.2.4 使用GSN表达的安全案例模式相关研究

安全案例模式（Safety case Patterns）[[[26]](#endnote-27)]是Tim Kelly于1998年提出的，他指出，可以复用成功的安全案例的论证结构。因此，定义了安全案例模式的表示方法。同时，也说到了安全案例的优势，就是通过建立一系列安全案例模式，可以在一定情况下提高论证模型的复用性。同时，当这些模式积累到一定数量时，可以改进安全案例的建立方法。

经过Tim Kelly在安全案例模式领域的不懈研究，他和他的团队在2007年提出了面向先进控制软件的安全案例模式[[[27]](#endnote-28)]。文中总结了用于自适应系统的14种论证模式。通过这14种模式，来构建论证结构，进而支持对总目标的论证。这项工作为建立先进控制软件的安全案例做出了很大的贡献，为建立先进控制软件的安全案例提供了有效指导。

参数化的论证结构为安全案例模式带来了很高的灵活性。同时，也带来了一些潜在的问题，例如没有对参数化的表达形式进行精确的定义，这可能会引发一致性问题。为了解决这一问题，文献[[[28]](#endnote-29)]定义了精确的参数化表达形式，包括了参数的变量，参数的取值范围等。并提供了类型检查机制，可以自动检查参数的一致性，有效的解决了上面提出的问题。

## 1.3 研究目标及主要研究内容

本论文研究的主要目标是：（1）基于DO-178C标准，提出建立目标满足性论证模式的方法，并总结提出软件验证过程的五种目标满足性论证模式；（2）设计实例化目标满足性论证模式的方法，建立项目相关的目标满足性论证模型；（3）设计实现目标满足性论证建模工具，能够构建目标满足性论证模式以及目标满足性论证模型，并实现模式与模型之间的转换。

### 1.3.1 建立基于DO-178C标准的目标满足性论证模式

需要说明的是，基于DO-178C标准的目标满足性论证模型是指：总目标是DO-178C标准中规定的目标，并以软件生命周期过程中产生的数据作为证据来建立的项目相关的论证结构。并且该结构最终使用GSN表示。基于DO-178C标准的目标满足性论证模式是可以复用并通过实例化，并表达多个目标满足性论证模型的表达方式。

首先，本文在现有GSN模式的基础上扩展了目标满足性论证模式中需要表示的几种约束条件的表示符号，及其表示的含义。

接下来，本文提出了基于DO-178C标准目标满足性论证模式的构建方法。基于提出的构建方法，建立了针对软件验证过程的、项目无关的目标满足性论证结构。并从中抽取了5种模式，表达了DO-178C软件验证过程的36个目标。涉及到了评审分析软件高层需求，评审分析软件低层需求，评审分析软件体系结构，评审分析软件源代码，测试高层需求-可运行代码符合性，测试高层需求-可运行代码健壮性，测试低层需求-可运行代码符合性，测试低层需求-可运行代码健壮性，测试高层需求覆盖率，测试低层需求覆盖率，MC/DC覆盖率，判定覆盖率，语句覆盖率，额外代码论证。

### 1.3.2 实例化目标满足性论证模式

本文提出了实例化目标满足性论证模式的方法，通过实例化目标满足性论证模式，可以建立目标满足性论证模型。实例化目标满足性论证模式可以分为两个层面：确定需要论证的目标；依据项目中可以提供的实际信息，实例化目标满足性论证模式。

此外，在提出实例化目标满足性论证模式的基础上，为了保证建立的目标满足性论证模型的灵活性，本文提出实例化目标满足性论证模式时，可以依据项目的实际情况，对模式中的目标，策略或者其他论证结构进行修改。

为了保证实例化后的目标满足性论证模型的正确性，本文提出了验证目标满足性论证模式实例化完成的依据，以此保证从目标满足性论证模式向目标满足性论证模型的正确转化。

### 1.3.3 目标满足性论证建模工具的设计和实现

本文实现了三个模块:

模块一，实现了目标满足性论证模式的编辑器。能够编辑本文扩展后的GSN图形符号，用户可以使用该编辑器建立本文提出的目标满足性论证模式，并对建立的目标满足性论证模式就进行修改、删除等操作。同时也可以编辑前文中提到的安全案例模式。

模块二，实现了目标满足性论证模型的编辑器。能够编辑目标满足性论证模型，并对建立的目标满足性论证模型进行修改、删除等操作。同时也可以编辑通用的GSN模型。

模块三，实现了从实例化的目标满足性论证模式向目标满足性论证模型的自动转换。还有两种验证规则：验证GSN符号及GSN扩展符号中的name属性不能为空；符号不能与自身关联。

实现本工具过程中，利用GMF+EMF+GEF框架技术实现编辑器；此外，使用Epsilon Transformation Language（ETL）[[[29]](#endnote-30)]语言设计模型转换规则，并使用Epsilon Validation Language（EVL）[[[30]](#endnote-31)]语言定义模型验证规则。

## 1.4 论文组织结构

本文内容组织与安排如下：

第一章 绪论：主要介绍本文研究的选题背景与研究意义，国内外研究现状，并对本文的研究目标和主要研究内容进行阐述。

第二章 适航软件基于标准的目标论证技术综述：主要对DO-178C标准以及其相关标准进行介绍，并介绍了与本研究工作直接相关的GSN表示符号，面向模式的GSN表示符号的定义和使用方法，最后介绍了工具设计中涉及的建模技术。

第三章 基于DO-178C的目标满足性论证模式抽取方法研究：提出了为论证目标满足性论证模式对GSN表示符号的扩展方案。分析并提出了抽取目标满足性论证模式的方法。在此基础上，基于DO-178C软件验证过程中规定的目标，提出了5种目标满足性论证模式。

第四章 构建基于DO-178C的目标满足性论证模型方法研究：基于第三章的提出的目标满足性论证模式，提出实例化方法建立目标满足性论证模型，并用案例说明实例化方法的可行性，并提出了目标满足性论证模型的文本表示方法。

第五章 目标满足性论证建模工具的实现：主要介绍GSNEdit编辑器，GSNModelEdit编辑器以及模型管理工具的体系结构、功能与实现方式。

第六章 实验分析：通过两组实验，利用实际的项目工程数据，验证上述研究工作的有效性。

最后，对本论文研究工作进行总结与展望。

# 第二章 适航软件基于标准的目标论证技术综述

## 2.1 DO-178C系列标准

### 2.1.1 DO-178C标准

DO-178C标准[1]将软件生命周期定义为软件计划过程，软件开发过程，软件验证过程，软件配置管理过程，软件质量保证过程，软件联络审定过程。其中，软件开发过程可以分为：软件需求过程，软件设计过程，软件编码过程，软件集成过程。软件验证过程可以分为：验证软件需求输出的过程，验证软件设计输出的过程，验证软件编码集成过程输出的过程，测试软件集成过程输出的过程，验证验证过程输出的过程。这些过程中一共包含了71个安全目标。

DO-178C标准中，将失效分为五个等级，如表1所示。

表 1 失效的等级划分

|  |  |
| --- | --- |
| **分类** | **定义** |
| 灾难性的 | 阻止继续安全飞行和着陆的失效。 |
| 危险的 | 降低航空器的性能和机组人员克服不利操纵状态的能力的失效。 |
| 较重的 | 可能降低航空器的性能和机组人员克服不利操纵状态的能力的失效。 |
| 较轻的 | 不会严重降低航空器安全性及有关机组的活动在他们的能力内能很好完成的失效。 |
| 无影响的 | 不影响航空器的工作性能或不增加机组工作量的失效。 |

DO-178C标准依据失效等级将软件分为5个等级：A、B、C、D、E。

A级软件是指：软件的异常行为会导致航空器的灾难性失效。

B级软件是指：软件的异常行为会导致航空器的危险性失效。

C级软件是指：软件的异常行为会导致航空器的较重失效。

D级软件是指：软件的异常行为会导致航空器的较轻失效。

E级软件是指：软件的异常行为对航空器没有影响。并指出，如果适航审定时定义某软件属于E级软件，那么将不需要满足DO-178C的任何目标。

不同级别的软件需要满足的目标不同，依据DO-178C标准的定义，A级软件需要满足的目标总数是71个，B级软件需要满足的目标总数是69个，C级软件需要满足的目标总数是62个，D级软件需要满足的目标总数是26个。

除了定义不同级别的软件需要执行的目标外，DO-178C标准还定义了为实现该目标，需要执行的活动以及执行活动产生的输出。DO-178C中规定的这些具体要求为构建目标满足性论证模型中的子目标，证据提供了重要参考。

### 2.1.2 DO-178C标准相关标准

除了DO-178C标准外，RTCA在2011年还发布了6部标准，和DO-178C标准关系紧密。分别是DO-278A[2]DO-248C[3]，DO-330[4]，DO-331[5]，DO-332[6]，DO-333[7]。其中DO-333标准提出使用形式化的方法定义或实现DO-178C标准中规定的活动。该标准提出，使用形式化的方法可以消除描述软件需求的二义性，保证工程师之间的交流不存在二义性，保证了描述的一致性。通过形式化的方法执行软件开发过程的部分活动，作为一种可以采用的方法。

此外，为了帮助执行DO-178C标准的适航审定，FAA发布了软件审定指南（Software Approval Guidelines）[14]，该指南为验证软件是否满足DO-178C标准提供了有效的帮助。在软件评审阶段，指出软件评审活动的目标，以及不同阶段的评审活动需要强调的要点，并详细地说明了评审活动的输出数据结构，为建立目标满足性论证模型提供了有效指导。

### 2.1.3 DO-178C标准相关研究

除了DO-178C标准及其相关的系列标准，还存在一些关于DO-178C标准的研究。NASA的研究员C. Michael Holloway对DO-178C进行了较长时间的研究，他指出“DO-178C标准做出了假设，如果软件满足DO-178C标准中规定的目标，就可以认为软件是安全的”[9]。并且提出了不同安全等级的软件，论证DO-178C总目标“适航软件具有必需的安全性保证，并符合适航要求”的论证结构。他提出的论证结构主要分为两部分：主要论证模块，支撑论证模块。

图1是文献[9]提出的针对一个D级软件的主要论证结构。该论证结构中省略了上下文、假设等元素。在图1中，论证元素右下角的编号是每个元素的唯一编号。右上角添加的小矩形表示该元素存在辅助论证结构支撑论证该论点。图1中，目标1.1表示了DO-178C的总目标，作者分析了DO-178C标准中D级软件需要满足的目标，并将这些目标分为两类，分别是目标3.1，目标3.2，因此，建立了图1所示的论证结构。

国内关于DO-178C标准的研究集中于分析DO-178C标准相对于DO-178B标准的新特性[[[31]](#endnote-32)][[[32]](#endnote-33)]。除此之外，文献[[[33]](#endnote-34)]对DO-178C标准进行了深入解读，定义了DO-178C标准中规定目标在执行过程中需要注意的地方，以及目标具体执行的活动。并且对DO-178C中的一些特征进行了总结，如追溯性，一致性等，对建立目标满足性论证模型起到了很大的帮助。

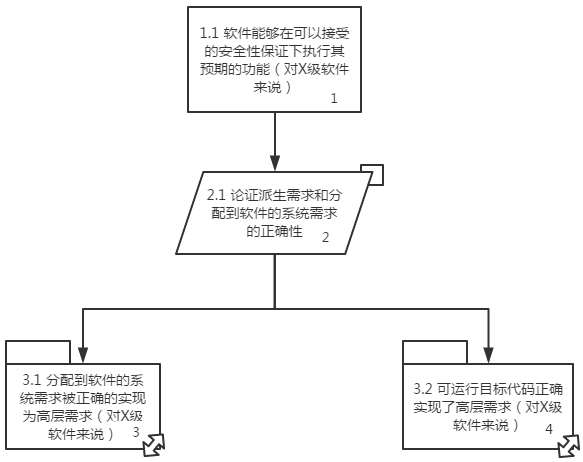


图 1 简化的DO-178C主要论证结构

## 2.2 安全案例及GSN

### 2.2.1 安全案例

验证系统及其开发过程是否符合相应的安全标准要求评估人员验证一系列安全目标是否得到满足[[[34]](#endnote-35)]。目前，基于证据的安全论证过程是一种被广泛采用的论证过程。为了能够系统化地构建基于证据的安全论证过程，Tim Kelly提出了使用安全案例（Safety Case）来描述证据到安全目标的推理过程。一个安全案例包括三个基本要素：安全目标，安全证据，安全论证结构。其关系是：评估人员使用安全证据对安全目标进行论证[[[35]](#endnote-36)]。安全案例的结构关系如图2所示。

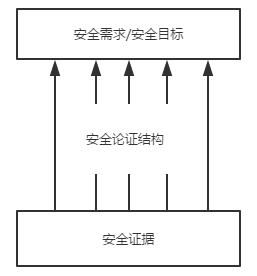


图 2 安全案例

安全目标（Safety Objective）描述了系统及其开发过程中应当满足的安全相关要求，也可以叫做安全需求。安全证据（Safety Evidence）是一类制品或者数据信息，这类信息能够为论证系统是否满足安全目标提供证据和支撑[34]。

### 2.2.2 目标结构化表示法GSN（Goal Structuring Notation）

GSN[8]由英国约克大学的Tim Kelly教授首次提出。GSN可以层次化的描述安全目标的论证结构[8]。GSN标准[24]中定义了GSN图形符号及其含义。表2给出了GSN基本的节点类图符（包括辅助论证符号和主论证符号），并解释了其含义。表3给出了GSN的基本连接图符，并解释了其含义。

表 2 GSN图形符号含义

|  |  |
| --- | --- |
| Goal | **目标**  用矩形表示，代表了安全论证中的目标（也可以是子目标） |
| Strategy | **策略**  用平行四边形代表，描述了目标到其分解的子目标的推理的本质，或者推理的规则 |
|  | **解决方案**  用圆形来表示，代表了某个证据或者某几个证据项的引用 |
| Context | **上下文**  用圆角矩形来表示，代表了上下文。这个可以作为一个引用来表示上下文相关的信息，也可以是一个论述 |
| J | **说明**  在椭圆形下方有一个大写字母J表示论证的某个目标对象是可信的 | |
| A | **假设**  在椭圆形下方有一个大写字母A表示一个可能的外部条件，这很有可能作为说明策略的合理性的依据 | |

**表2 GSN图形符号含义（续）**

|  |  |
| --- | --- |
|  | **未开发的实体**  表示该论证过程尚未开发出来，这个可以应用与目标，也可以应用于策略 |
|  | **尚未开发的目标**  代表了一个目标在开发过程中尚未开发出来 |

表 3 GSN连接符号含义

|  |  |
| --- | --- |
|  | **推理**  实心箭头表示一种推理关系，用来表示目标，解决方案，策略之间的关系 |
|  | **支撑论证**  空心箭头表示一种上下文附属关系 |

使用GSN建立安全案例时，使用上面的符号就可以完全实现需要表达的信息。其中，目标、策略、解决方案是主论证符号。上下文、说明、假设是辅助论证符号，未开发的实体的使用方法如表2的“未开发实体”表示符号所示。此外，实心箭头连接主论证符号，空心箭头表达辅助论证符号和主论证符号之间的关系。

### 2.2.3 安全案例模式Safety Case Pattern

安全案例模式（Safety case Pattern）[26]是Tim Kelly提出的，安全案例模式可以复用成功的安全案例的论证结构[26]。安全案例模式提取出了论证过程中可以复用的部分，为了能够使用GSN表达安全案例模式，需要对现有的GSN符号进行扩展。依据GSN标准的定义，扩展的GSN符号及其含义如表4所示。

表 4 基于模式的GSN扩展符号含义

|  |  |
| --- | --- |
|  | **n元推理**  n表示存在0-n个实例化后的子目标，是由其父目标分解而成 |
|  | **选择推理**  空心的圆表示对应的子目标可能支撑父目标，也可能不支撑 |

为了表示抽象化的实体，GSN进行了实体抽象化扩展，如表5所示。

表 5 基于模式的实体抽象扩展符号含义

|  |  |
| --- | --- |
|  | **未实例化的实体**  这个符号表示与其关联的实体还未进行实例化 |
|  | **待分解实例化的实体**  这个符号表示与其关联的实体还需要分解，并且没有进行实例化 |

为了能够完整表示安全案例模式，对符号内的文本信息的表达方式也需要进行一定的规定，文献[27]对这种扩展做出了详细的定义。图3为其中一个安全案例模式示例。

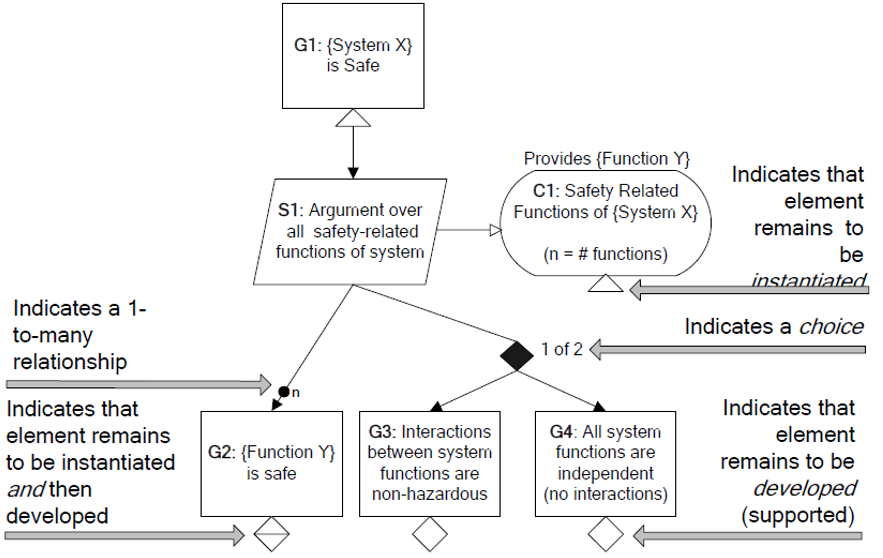


图 3 安全案例模式示例

图3所示的安全案例模式示例是文献[27]中一个安全案例模式。其中大括号{}中定义的是需要实例化的变量，例如G1中的System X；G1通过策略S1分解为子目标G2，G3，G4。G1至G2的n元推理关系表示目标G1可以分解为n个实例化后的G2子目标，其中n=Function的个数，实例化G2目标需要把具体的功能X赋值到变量Function Y中。C1对需要进行实例化的变量进行解释说明。目标G2还需要进行分解，并且此时没有实例化。S1和G3，G4之间的关联符号表示，当G3，G4两个目标中的一个目标成立就满足论证结构的定义，并且目标G3，G4不需要进行实例化，但是需要进一步进行分解。

## 2.3 GMF（Graphical Modeling Framework）框架

GMF是基于EMF[[[36]](#endnote-37)]和GEF[[[37]](#endnote-38)]建立的图形化编辑器的开发环境和运行时的框架[[[38]](#endnote-39)]。IBM为其撰写了红皮书[[[39]](#endnote-40)],并提供了案例帮助大家学习和使用。GMF框架主要包括两个部分，运行时环境和图形化开发环境[[[40]](#endnote-41)]。图形化开发环境采用MVC架构，帮助人们构建图形编辑器。

图4是文献[40]中给出的GMF的工作流。从图中我们可以看出，要创建一个GMF项目，首先需要定义领域模型，领域模型使用ecore文件表示。接下来定义图形化模型，该模型主要定义了图形编辑器的画布中可以绘制的基本图符。然后定义工具模型，该模型定义了工具栏中图符及表现形式。最后定义匹配模型，即建立上述三个模型之间的映射关系。建立完成后，就可以自动生成图形编辑器。但是这种图形编辑器的功能还不健全，需要添加或者修改代码来实现模型的验证，定义图符形状（GMF默认只有矩形和椭圆形两种形状）等功能，最终完成图形编辑工具的实现。

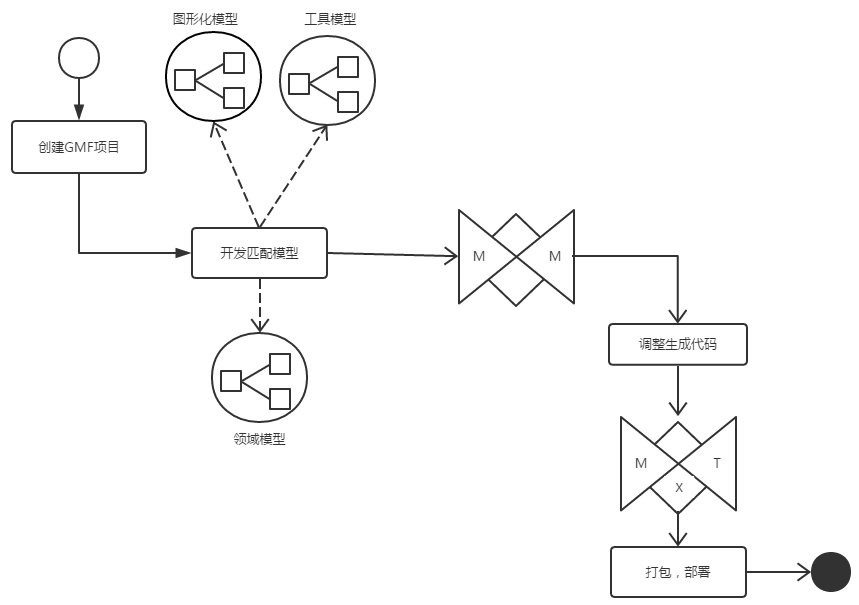


图 4 GMF工作流

## 2.4 小结

本章首先调研了DO-178C标准及其相关标准的内容，重点介绍了DO-178C标准中的内容，并说明了DO-178C标准目前的研究现状。

对GSN进行了重点介绍，包括GSN的基本表示符号及其含义。接下来介绍了安全案例模式（Safety Case Pattern）的含义，表示安全案例模式（Safety Case Pattern）的GSN扩展符号及其含义。

针对本文开发的目标满足性论证建模工具拟采用的模型化开发框架，本章概要地介绍了GMF的主要组成部分，以及建立图形编辑器时使用GMF框架的主要操作流程。

# 第三章 基于DO-178C的目标满足性论证模式抽取方法研究

本章首先对GSN图符进行了扩展，能够表达本文定义的目标满足性论证模式。接下来提出了建立目标满足性论证模式的方法，由于篇幅限制，以软件验证过程为例，给出DO-178C软件验证过程目标的5种目标满足性论证模式。

## 3.1 研究目标与方法

本研究提出了目标满足性论证模式概念，抽取论证模型中可重用的部分，使用一项目标满足性论证模式表达两个或多个目标满足性论证模型。同时，同一个目标满足性论证模式可以实例化为不同项目的目标满足性论证模型。从这两个层面提高了目标满足性论证模型的重用性。

同时为了表达目标满足性论证模式，本文在原有基于模式的GSN符号中扩展了特定的符号。

## 3.2 GSN扩展符号

GSN是表达基于证据的安全论证结构的一种表示方法。为了能够准确地定义目标满足性论证模式，本研究对GSN的表达符号进行了扩展。扩展的表达符号见表6。在目标满足性论证模式中，主论证符号为证据，目标和策略，其余符号均为辅助论证符号。

表 6 GSN扩展符号含义

| **表达符号** | **名称** | **含义** |
| --- | --- | --- |
| D:\实验室项目\2015后半年总体方案\GSEdit代码+说明\工具使用图片\YConstraint.gif | 其他约束条件 | 目标或者策略的辅助论证符号。  含义：其支撑的目标或者策略存在的前提条件。如果该约束条件为假，则其支撑的论证结构或目标不成立。 |
| D:\实验室项目\2015后半年总体方案\GSEdit代码+说明\工具使用图片\YConstraintForSolution.gif | 证据约束条件 | 证据的辅助论证符号。  含义：目标满足性论证模式中证据的结构。实例化时，待论证的软件提供的证据必须满足证据约束条件。 |

**表 6 GSN扩展符号含义（续）**

| **表达符号** | **名称** | **含义** |
| --- | --- | --- |
| D:\实验室项目\2015后半年总体方案\GSEdit代码+说明\工具使用图片\YConstraintForValue.gif | 变量约束条件 | 主论证结构中变量的辅助论证符号。  含义：如果主论证结构中的变量类型为枚举类型，该符号定义了枚举类型变量的可能取值。 |
| D:\实验室项目\2015后半年总体方案\GSEdit代码+说明\工具使用图片\Reference.gif | 关联标准章节 | 目标，策略或证据的辅助论证符号。  含义：当目标，策略或证据的描述与DO-178C标准的章节关联，该符号描述出具体关联的章节号。 |
| D:\实验室项目\2015后半年总体方案\GSEdit代码+说明\工具使用图片\MConstraintForGoal.gif | 目标约束条件 | 可选目标的辅助论证符号。  含义：目标约束条件是其对应的可选目标成立的前提假设。与可选目标配套使用。 |
| D:\实验室项目\2015后半年总体方案\GSEdit代码+说明\工具使用图片\AlternativeGoal.gif | 可选目标 | 主论证符号“目标”的一种。  含义：当其对应的目标约束条件成立时，该目标需要满足。与目标约束条件配套使用。 |

约束条件的书写格式定义如下：

赋值语句：变量名={可能取值1，可能取值2，可能取值3，…}

复合句：IF （判断语句） 赋值语句； ELSE 赋值语句

判断语句：变量名=={取值}

## 3.3 目标满足性论证模式的建模方法

为了能够帮助建立可以复用的基于DO-178C标准的目标满足性论证模式，本研究提出了一种基于DO-178C标准的目标满足性论证模式构建方法。采用该方法所构建的目标满足性论证模式，按照DO-178C的标准要求构建，为下一步构建含有项目特性的目标满足性论证模型提供了相应实例化的接口。本节将具体介绍目标满足性论证模式的建模方法。

目标满足性论证模式的建模流程如图5所示。

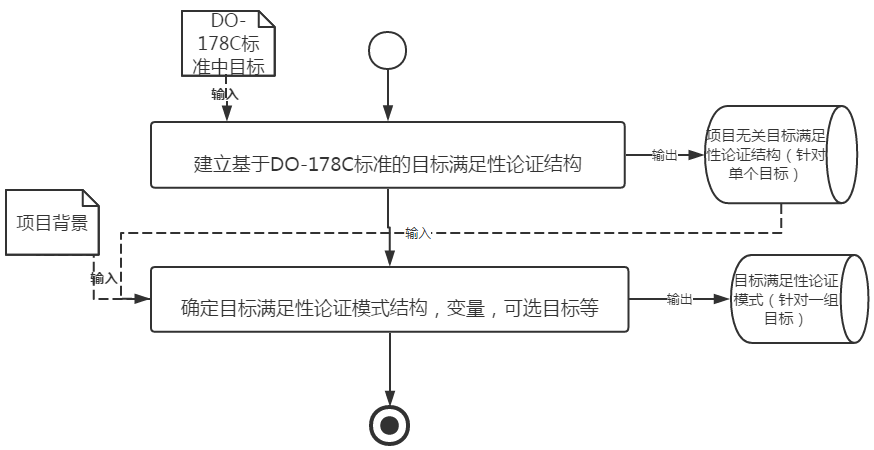


图 5 目标满足性论证模式建模流程

第一步，基于对DO-178C标准中规定的各项目标的分析和理解，建立基于DO-178C标准的项目无关目标满足性论证结构。针对每个目标，依据标准中对该目标的定义和描述，以及对需要执行的活动及其输入和输出的说明。确定建立论证结构的基本步骤如下所述：

1. 确定目标及其支持活动：针对需要论证的目标，确定该论证对应DO-178C标准中需要执行的活动。

2. 基于活动确定子目标：针对目标中定义需要执行的每项活动，依据活动的具体内容，及该活动与其余活动间的关联关系，将活动分为几种类型，最终确定目标论证结构中的子目标和分解策略，同时添加关联标准章节等辅助论证符号支撑相应子目标的论证。

3. 基于目标输入及相关要求确定必需的证据：参考目标中规定的输出，及其相关联的数据，依据标准的描述，确定哪些输出为目标满足性论证结构的证据。同时依据标准中对输出数据的描述，结合需要论证的子目标，定义证据的约束条件，同时确定证据之间的关联。有的子目标不能直接使用目标规定的输出进行论证，这时依据目标的实际情况确定其需要的证据数据，参考标准中对该数据的描述，以及需要论证的子目标对证据的结构要求，确定证据的约束条件。

第二步，这一过程主要是依据第一步建立的目标满足性论证结构，确立目标满足性论证模式的结构，基于同类目标特征以及项目特征确定论证模式中的变量，可选目标，约束条件等要素。建立目标满足性论证模式的基本步骤如下所述：

1. 基于同类目标特征分析引入可实例化变量，确定关联关系：依据标准对目标的定义和描述，以及执行的活动，找出该目标与其他目标之间的关联（规定执行的活动一致或相似），把具有相似论证结构的目标用同一种论证结构表达出来。并将其中的可变内容抽取出来，确定其为变量或者可选目标，并定义变量的取值范围或者可选目标的目标约束条件，并按照3.2节中的定义符号表示。

2. 添加其他约束条件：如果建立的论证结构需要某项约束条件，确定该约束条件为其他约束条件，并按照3.2节中的定义符号表示。并作为辅助论证添加其与论证结构的关联。

3. 依据项目确定变量，可选目标：结合实际项目的特点，找到其与标准之间的不同之处，找到这些不同之处在第一步中建立的项目无关的目标满足性论证结构的中具体描述，确定为变量，或可选目标。并定义变量的取值范围，或可选目标的约束条件，并将最终建立的模型按照3.2节定义的GSN扩展符号表达出来。此时建立的模型为基于DO-178C的目标满足性论证模式。

## 3.4 评审分析目标满足性论证模式

本节以RTCA DO-178C标准的软件验证过程中评审分析需要实现的目标为实例，说明提取构建该类目标满足性论证模式的过程。

### 3.4.1 评审和分析的目标满足性论证结构

RTCA DO-178C标准的6.3中要求，软件需求阶段输出的高层需求，软件设计阶段输出的低层需求和软件体系架构，软件编码阶段输出的源代码都要通过评审和分析活动进行验证。

DO-178C标准将需求分为两大类：系统需求和软件需求。系统需求定义了系统应当为用户提供的服务以及需要满足的一系列条件；软件需求定义了软件应当为当前用户提供的服务以及需要满足的条件。

DO-178C标准将软件需求分为两类，分别是高层需求和低层需求。高层需求是指实现系统需求，系统的软件部分需要提供的功能和所要满足的条件；低层需求是指直接由源代码实现的软件需求。

DO-178C标准定义的软件体系架构，即实现软件需求的软件架构，在软件设计阶段产生。

源代码指的是使用高级语言编写的代码，是机器可读的语言，是依据软件低层需求以及软件体系架构编写的。

DO-178C标准附录A的表3、表4和表5中，定义了评审和分析软件需求阶段，软件设计阶段，软件编码阶段输出的相关目标。下面将依据不同软件生命周期阶段，及阶段中各种输出，分别分析基于DO-178C标准的目标满足性论证结构。

#### 3.4.1.1 软件高层需求评审和分析的目标满足性论证结构：

DO-178C对高层需求的评审和分析活动需要满足的目标在DO-178C附录A的表3中有详细的说明，包括7个目标，分别是：

1. 高层需求要符合（comply）系统需求的定义。

2. 高层需求是精确（accuracy）和一致的（consistency）。

3. 高层需求和目标计算机兼容（compatibility）。

4. 高层需求可验证（verifiability）。

5. 高层需求符合（conformance）标准。

6. 高层需求和系统需求间是可追溯（traceability）的。

7. 高层需求阶段提出的算法是精确（accuracy）的。

表7对这7个目标依据标准进行了详细的解读，确定了不同目标的论证结构（包含证据）。

表 7 软件高层需求评审分析目标解读

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 目标1 | DO-178C标准规定了其需要执行的活动为标准中的6.3.1.a节。6.3.1.a节内容，论述了两个要求：可追溯到系统需求的高层需求需要实现的要求，以及派生高层需求需要实现的要求。基于此，本文认为可以将这一目标分解为两个目标，分别以可追溯高层需求，派生高层需求为特征，即所有和软件有关的系统需求都被高层需求实现；定义的派生高层需求需要正确阐述其存在的原因。并且这两个目标可以通过软件验证结果论证。 |

**表 7 软件高层需求评审分析目标解读（续）**

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 目标2 | DO-178C标准规定了其需要执行的活动为标准中的6.3.1.b节。6.3.1.b节内容，论述了每个高层需求需要达到的特性以及对需求间关系的要求。基于此，本文认为可以将其这一目标分为两个目标：所有的高层需求都是精确，无二义性并且详细的；所有的高层需求之间不会相互冲突。并且这两个目标可以通过软件验证结果论证。 |
| 目标3 | DO-178C标准规定了其需要执行的活动为标准中的6.3.1.c节。6.3.1.c节内容，论述了高层需求和目标计算机之间没有冲突的要求。基于此，本文认为可以将这一目标分解为一个目标：高层需求和目标机的软件、硬件间不存在冲突。并且这一目标可以通过软件验证结果论证。 |
| 目标4 | DO-178C规定了其需要执行的活动为标准中的6.3.1.d节。6.3.1.d节内容，论述为每个高层需求都可以被验证。基于此，本文认为针对目标4存在能够直接论证其正确性的证据，因此，认为其已经不需要进一步分解；并且这一目标可以通过软件验证结果论证。 |
| 目标5 | DO-178C规定了其需要执行的活动为标准中的6.3.1.e节。6.3.1.e节内容，论述为软件需求过程遵守需求标准，并且所有冲突的地方都正确解释。基于此，本文认为可以将这一目标分解为一个目标：所有和标准有冲突的地方都正确解释，这个目标包含了6.3.1.e节内容。并且这一目标可以通过软件验证结果论证。 |
| 目标6 | DO-178C规定了其需要执行的活动为标准中的6.3.1.f节。6.3.1.f节内容，论述内容为追溯性，即所有软件相关的系统需求都可以追溯到高层需求。基于此，本文认为针对目标6存在能够直接论证其正确性的证据。因此，认为其已经不需要进一步分解；并且这一目标可以通过追溯数据论证。 |
| 目标7 | DO-178C规定了其需要执行的活动为标准中的6.3.1.g节。6.3.1.g节内容，论述为提出的算法必须是精确的。基于此，本文认为针对目标7存在能够直接论证其正确性的证据。因此，认为其已经不需要进一步分解；并且这一目标可以通过软件验证结果论证。 |

通过表7可知，软件验证结果可以作为证据论证目标1、2、3、4、5、7。此外，追溯数据可以作为证据论证目标6。标准中对软件验证结果和追溯数据进行定义，在本论证过程中只选取和论证目标相关的项。具体证据的组成结构如表8所示。

表 8 软件高层需求评审分析证据结构

|  |  |
| --- | --- |
| **证据** | **证据结构** |
| 软件验证结果 | 配置项（软件版本），评审/分析过程，评审/分析结果。 |
| 追溯数据 | 软件高层需求和软件相关系统需求间的关联。 |

通过上述分析，建立的高层需求评审分析的目标满足性论证结构如图6所示：

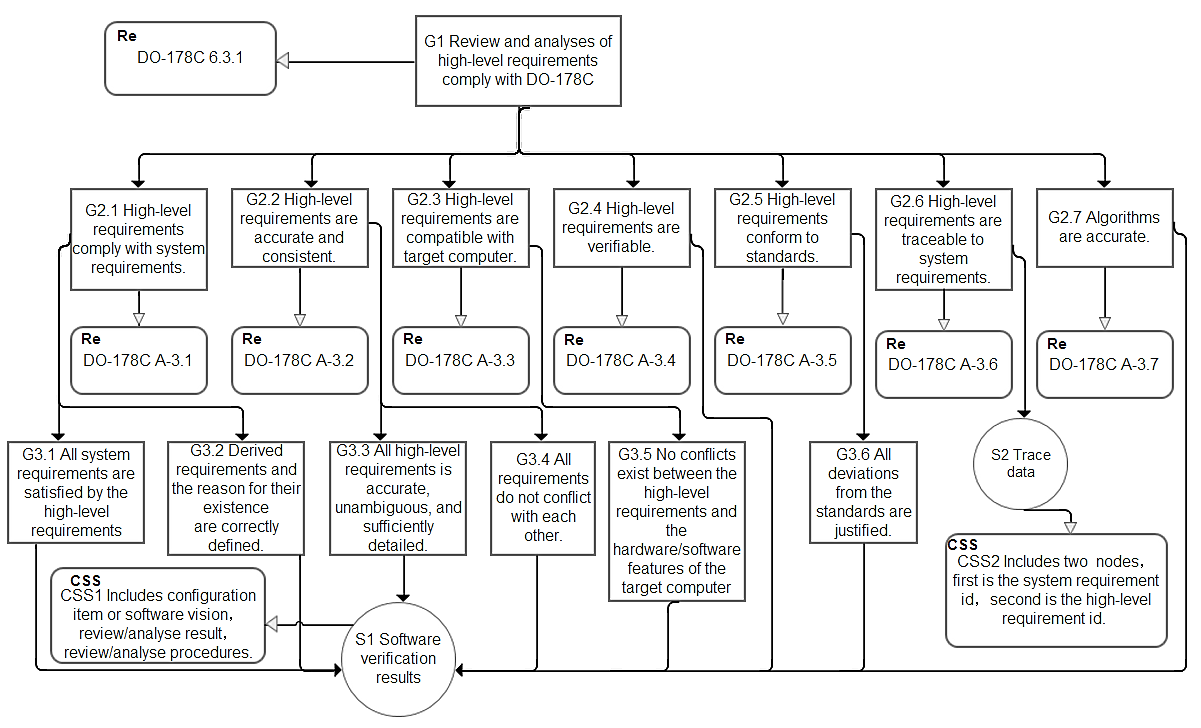


图 6 软件高层需求评审分析的目标满足性论证结构

图6中，论证结构的论证对象是软件需求阶段的输出-高层需求，确定总目标为G1，评审分析高层需求符合DO-178C标准（reviews and analyses of high-level requirements comply with DO-178C）。

G1总共包含了七个子目标（G2.1、G2.2、G2.3、G2.4、G2.5、G2.6、G2.7）（即本节的目标1-7），这7个目标参考了标准中附录A表3，在图6中写在关联标准章节符号里（圆角矩形带有Re标签，3.2节中详细介绍）。并且依据表7的目标解读，确定了目标G2.1分解为G3.1、G3.2（表7中目标1及目标1解读），目标G2.2分解为G3.3、G3.4（表7中目标2及目标2解读），目标G2.3分解为G3.5（表7中目标3及目标3解读），目标G2.5分解为G3.6（表7中目标5及目标5解读）；目标G2.4（表7中目标4及目标4解读），G2.6（表7中目标6及目标6解读），G2.7（表7中目标7及目标7解读）不必分解；同时确定目标G3.1、G3.2、G3.3、G3.4、G3.5、G3.6、G2.4、G2.7由证据软件验证结果直接论证，目标G2.6由证据追溯数据直接论证。同时参照表8，,证据结构定义在CSS1（表8软件验证结果证据结构），CSS2（表8软件追溯数据证据结构）中。

#### 3.4.1.2 软件低层需求评审和分析的目标满足性论证结构

DO-178C对低层需求的评审和分析活动需要满足的目标在附录A的表4中有详细的说明，包括7个目标，分别是：

1. 低层需求要符合（comply）高层需求的定义。

2. 低层需求是精确（accuracy），一致的（consistency）。

3. 低层需求和目标计算机兼容（compatibility）。

4. 低层需求可验证（verifiability）。

5. 低层需求符合（conformance）标准。

6. 低层需求和高层需求间是可追溯（traceability）的。

7. 低层需求阶段提出的算法是精确（accuracy）的。

对这7个目标的解读与软件高层需求评审和分析的目标满足性论证结构的表7，表8有很大的相似性，此处不再赘述，最终建立的低层需求评审分析的目标满足性论证结构如图7所示，图7中各个目标的分解情况与图6有很大的相似性，此处不再赘述。

#### 3.4.1.3 软件体系结构评审和分析的目标满足性论证结构

DO-178C对软件体系结构的评审和分析活动需要满足的目标在附录A的表4中有详细的说明，包括6个目标，分别是：

1. 软件体系结构和高层需求兼容（compatibility）。

2. 软件体系结构一致（consistency）。

3. 软件体系结构和目标计算机兼容（compatibility）。

4. 软件体系结构可验证（verifiability）。

5. 软件体系结构符合（conformance）标准。

6. 确认（confirm）软件的分区完整性。

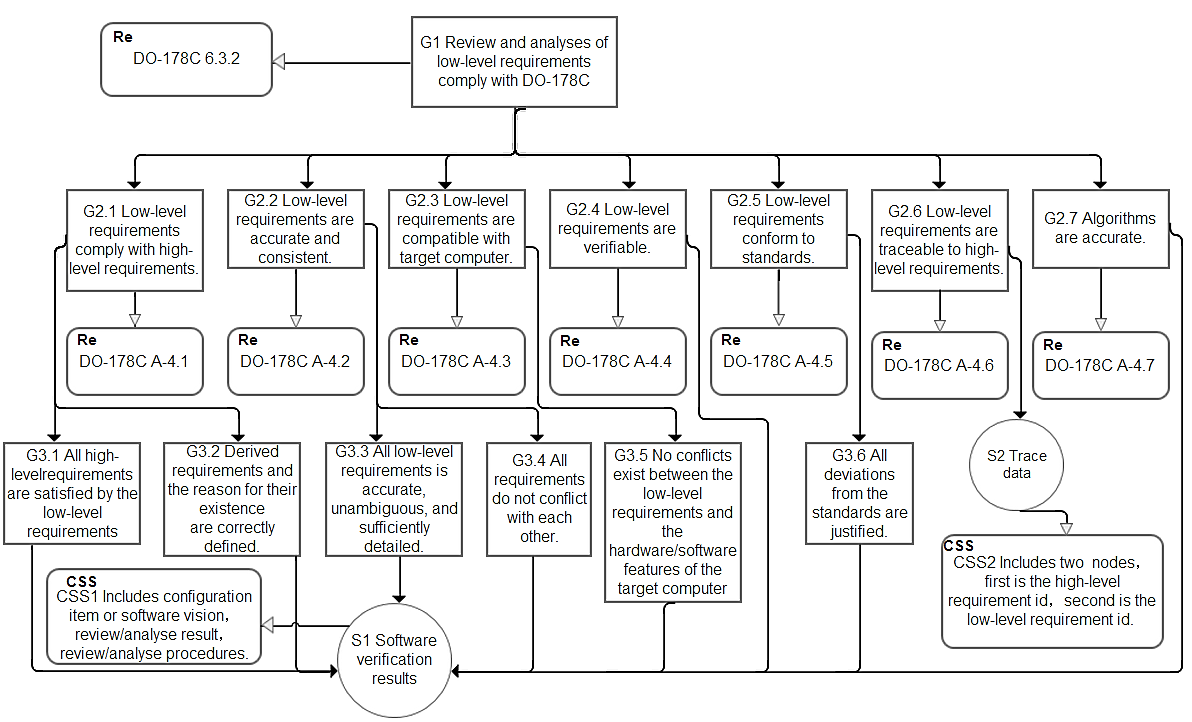


图 7 软件低层需求评审分析的目标满足性论证结构

表9对这6个目标依据标准进行了详细的解读，确定了不同目标的论证结构。

通过表9可知，软件验证结果可以作为证据论证所有目标。标准中对软件验证结果进行定义，在本论证过程中只选取和论证目标相关的项。证据的组成结构如表8中软件验证结果所在行所示。

表 9 软件体系结构评审分析目标解读

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 目标1 | DO-178C标准规定了其需要执行的活动为标准中的6.3.3.a节。6.3.3.a节内容，论述了软件高层需求和软件体系结构间的兼容关系。基于此，本文认为可以将这一目标分解为一个目标：软件体系结构和高层需求之间没有冲突。并且这一目标可以通过软件验证结果论证。 |
| 目标2 | DO-178C标准规定了其需要执行的活动为标准中的6.3.3.b节。6.3.3.b节内容，论述了软件体系结构各个构件间必须保持关系正确，并且构件间的关系存在于数据流和控制流中。基于此，本文认为可以将其这一目标分为两个目标：软件体系结构中构件间的数据流保持一致；软件体系结构中构件间的控制流合理正确。并且这两个目标可以通过软件验证结果论证。 |

表 9 软件体系结构评审分析目标解读（续）

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 目标3 | DO-178C标准规定了其需要执行的活动为标准中的6.3.3.c节。6.3.3.c节内容，论述了软件体系结构和目标计算机之间没有冲突的要求，并强调了软件特定4种操作（初始化，异步，同步，中断）下必须保持兼容性。基于此，本文认为可以将这一目标分解为五个目标：软件体系结构在初始化时不会和目标机产生冲突，软件体系结构在异步操作时不会与目标机冲突，软件体系结构在同步操作时不会与目标机冲突，软件体系结构在中断时不会与目标机冲突，软件体系结构不会在其他情况下与目标机冲突。并且这五个目标可以通过软件验证结果论证。 |
| 目标4 | DO-178C规定了其需要执行的活动为标准中的6.3.3.d节。6.3.3.d节内容，论述为软件体系结构可以被验证。基于此，本文认为针对目标4存在能够直接论证其正确性的证据，因此，认为其已经不需要进一步分解；并且这一目标可以通过软件验证结果论证。 |
| 目标5 | DO-178C规定了其需要执行的活动为标准中的6.3.3.e节。6.3.3.e节内容，论述为软件设计过程遵守软件设计标准，并且所有冲突的地方都正确解释。基于此，本文认为可以将这一目标分解为一个目标：所有和标准有冲突的地方都正确解释。这个目标包含了6.3.3.e节内容；并且这一目标可以通过软件验证结果论证。 |
| 目标6 | DO-178C规定了其需要执行的活动为标准中的6.3.3.f节。6.3.3.f节内容，论述内容为不存在分区违规。基于此，本文认为可以将这一目标分解为一个目标：不存在分区违规。并且这一目标可以通过软件验证结果论证。 |

通过上述分析，建立的软件体系结构评审分析的目标满足性论证结构如图8所示：

图8中，论证结构的论证对象是软件设计阶段的一项输出-软件体系结构，确定总目标为G1，评审分析软件体系结构符合DO-178C标准（reviews and analyses of software architecture comply with DO-178C）。

G1总共包含了六个子目标（G2.1、G2.2、G2.3、G2.4、G2.5、G2.6）（即本节的目标1-6），这6个目标参考了标准中附录A表4，在图8中写在关联标准章节符号里（圆角矩形带有Re标签，3.2节中详细介绍）。并且依据表9的目标解读，确定了目标G2.1分解为G3.1（表9中目标1及目标1解读），目标G2.2分解为G3.2、G3.3（表9中目标2及目标2解读），目标G2.3分解为G3.4、G3.5、G3.6、G3.7、G3.8（表9中目标3及目标3解读），目标G2.5分解为G3.9（表9中目标5及目标5解读）；目标G2.6分解为G3.10（表9中目标6及目标6解读）；G2.4（表9中目标4及目标4解读）不必分解；同时确定了目标G3.1、G3.2、G3.3、G3.4、G3.5、G3.6、G3.7、G3.8、G3.9、G3.10、G2.4由证据软件验证结果直接论证。同时参照表8中“软件验证结果”所在行，证据结构定义在CSS1（表8软件验证结果证据结构）中。

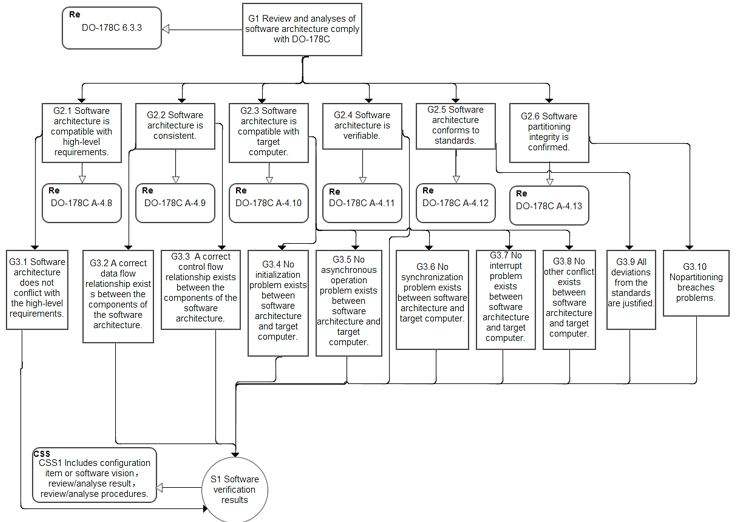


图 8 软件体系结构评审分析的目标满足性论证结构

#### 3.4.1.4 软件源代码评审分析的目标满足性论证结构

DO-178C对软件源代码的评审和分析活动需要满足的目标在附录A的表5中有详细的说明，包括6个目标，分别是：

1. 软件源代码要符合（comply）低层需求。

2. 软件源代码要符合（comply）软件体系结构。

3. 软件源代码可验证（verifiability）。

4. 软件源代码符合（conformance）标准。

5. 软件源代码可以追溯（traceability）到低层需求。

6. 软件源代码是精确（accuracy），一致的（consistency）。

表10对这6个目标依据标准进行了详细的解读，确定了不同目标的论证结构。

通过表10可知，软件验证结果可以作为证据论证目标1、2、3、4、6。此外，追溯数据可以作为证据论证目标5。标准中对软件验证结果和追溯数据进行定义，在本论证过程中只选取和论证目标相关的项。证据软件验证结果的组成结构如表8中“软件验证结果”所在行所示。追溯数据的证据结构为软件源代码和软件低层需求间的关联。

表 10 软件源代码评审分析目标解读

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 目标1 | DO-178C标准规定了其需要执行的活动为标准中的6.3.4.a节。6.3.4.a节内容，论述了软件源代码和软件低层需求的兼容关系，表现为两点：所有的低层需求都被源代码的实现要求，源代码没有不符合低层需求的要求。基于此，本文认为可以将这一目标分解为两个目标，所有的低层需求都被精确完整的实现；源代码没有实现未编写的功能。并且这两个目标可以通过软件验证结果论证。 |
| 目标2 | DO-178C标准规定了其需要执行的活动为标准中的6.3.4.b节。6.3.4.b节内容，论述了软件源代码和软件体系结构的兼容关系。基于此，本文认为可以将其这一目标分为两个目标：软件源代码与软件体系结构中定义的数据流一致；软件源代码与软件体系结构中定义的控制流一致。并且这两个目标可以通过软件验证结果论证。 |
| 目标3 | DO-178C规定了其需要执行的活动为标准中的6.3.4.c节。6.3.4.c节内容，论述为软件源代码可以被验证。基于此，本文认为针对目标3存在能够直接论证其正确性的证据，因此，认为其已经不需要进一步分解；并且这一目标可以通过软件验证结果论证。 |
| 目标4 | DO-178C规定了其需要执行的活动为标准中的6.3.4.d节。6.3.4.d节内容，论述为软件编码过程遵守软件编码标准，并且所有冲突的地方都正确解释。基于此，本文认为可以将这一目标分解为一个目标：所有和标准有冲突的地方都正确解释。这个目标包含了6.3.4.d节内容；并且这一目标可以通过软件验证结果论证。 |
| 目标5 | DO-178C规定了其需要执行的活动为标准中的6.3.4.e节。6.3.4.e节内容，论述内容为追溯性。基于此，本文认为针对目标5存在能够直接论证其正确性的证据。因此，认为其已经不需要进一步分解；并且这一目标可以通过追溯数据论证。 |

表 10 软件源代码评审分析目标解读（续）

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 目标6 | DO-178C规定了其需要执行的活动为标准中的6.3.4.f节。6.3.4.f节内容，论述内容为软件源代码的正确性和一致性要求，定义了十种软件编码过程中需要注意的问题。基于此，本文认为可以将这一目标分解为十一个目标：源代码的栈使用情况合理；源代码中内存使用情况合理；源代码中定点算数溢出解决；浮点运算正确；资源争夺限制合理；异常处理合理；不存在使用未初始化变量；缓存管理合理；不存在未使用变量；不存在由于任务或者中断冲突造成的数据损坏；考虑硬件影响情况下的最坏运行时间合理。并且这些目标可以通过软件验证结果论证。 |

通过上述分析，建立的软件源代码评审分析的目标满足性论证结构如图9，图10所示：

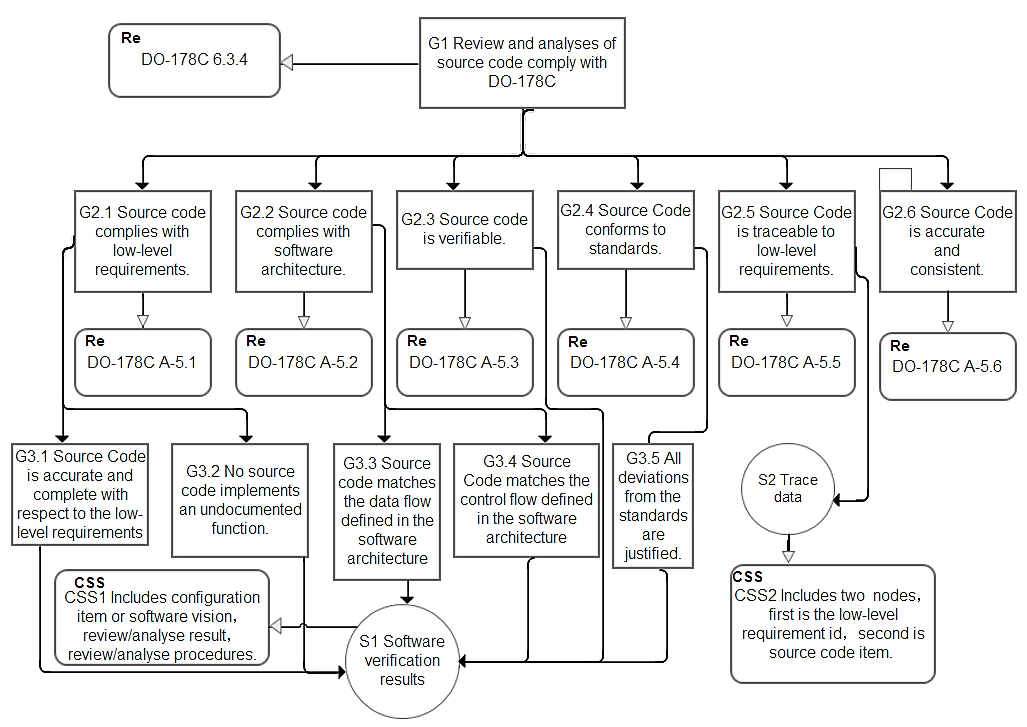


图 9 软件源代码评审分析的目标满足性论证结构（1）

图9中，论证结构的论证对象是软件编码阶段的输出-软件源代码，确定总目标为G1，评审分析软件源代码符合DO-178C标准（reviews and analyses of source code comply with DO-178C）。

G1总共包含了六个子目标（G2.1、G2.2、G2.3、G2.4、G2.5、G2.6）（即本节的目标1-6），这6个目标参考了标准中附录A表5，在图9中写在关联标准章节符号里（圆角矩形带有Re标签，3.2节中详细介绍）。并且依据表10的目标解读，确定了图9中目标G2.1分解为G3.1、G3.2（表10中目标1及目标1解读），目标G2.2分解为G3.3、G3.4（表10中目标2及目标2解读），目标G2.4分解为G3.5（表10中目标4及目标4解读），目标G2.6分解为G3.9（表9中目标5及目标5解读）；目标G2.6（篇幅限制，在图9中使用文件夹符号表示，具体结构在图10中描述）分解为图10中的（G3.1-G3.11）（表10中目标6及目标6解读）；G2.3（表9中目标3及目标3解读）不必分解；同时确定了图9的目标G3.1、G3.2、G3.3、G3.4、G3.5和图10的G3.1- G3.11由证据软件验证结果直接论证。同时参照表8中“软件验证结果”所在行，,证据结构定义在CSS1（表8软件验证结果证据结构）中。目标G2.5由追溯数据直接论证，证据结构在本节中有定义，在CSS2中描述。

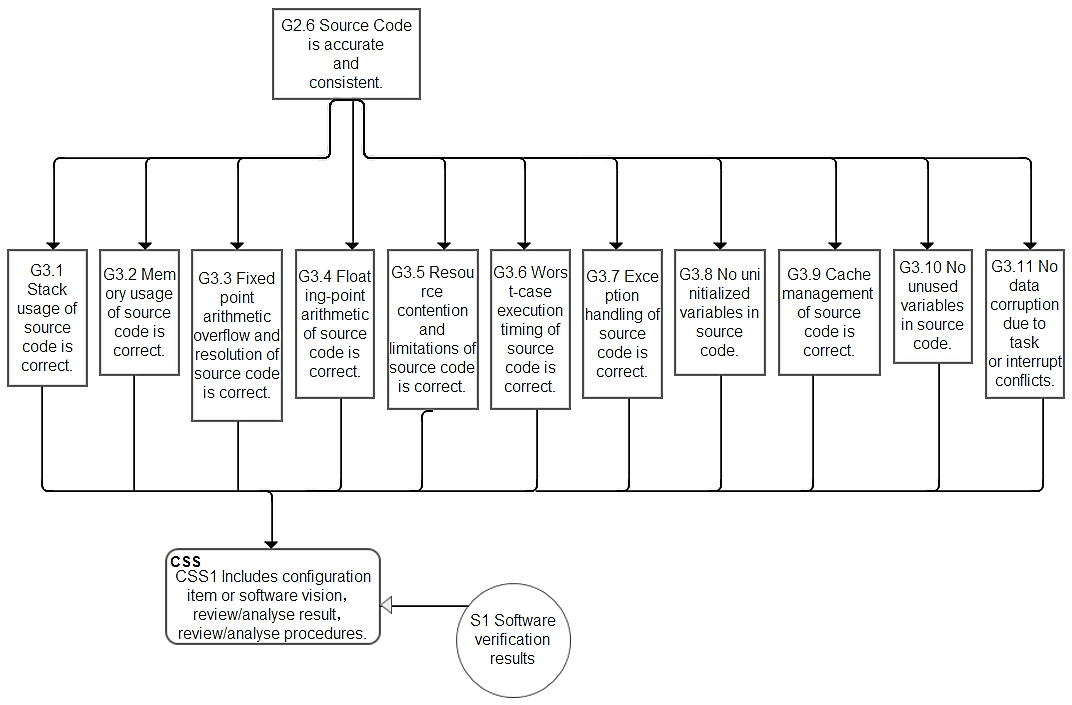


图 10 软件源代码评审分析的目标满足性论证结构（2）

### 3.4.2 评审和分析的目标满足性论证模式

通过3.4.1节中提出的DO-178C标准中不同阶段软件验证实现的目标，以及执行的活动，可以发现这几种论证结构相似，因此，本文抽取出一种项目无关目标满足性论证模式，表达出通用的论证结构，最终通过实例化方法满足不同目标的论证。

首先确定模式论证结构的总目标，依据模式的表达范围定义总目标的可变部分，确定其为变量，并定义变量的取值范围。

接下来找到论证结构中总目标分解后，共同存在的论证子目标，将他们添加到目标满足性论证模式中。

在这些论证结构中，对于总目标，下属的所有相似的论证目标，将其可变部分定义为变量，并确定其取值范围，并将其作为子目标添加到目标满足性论证模式中；而对于总目标下属的特有的论证目标，将其定义为可选子目标，并依据情况，为其添加目标约束条件。

按照每个论证结构的层次，逐一查看各层中的每个子目标，采用上述方法建立对应的子论证结构模式，直到子目标均处理完成后，将各相关证据添加到最底层子目标之下，并添加证据的约束规则。

将此时建立的论证结构中涉及项目相关的变量，可选目标，可选目标约束条件提取出来，使用模式中变量和可选目标的符号表示，最终建立目标满足性论证模式。

变量的定义表达方式以及目标约束条件等项目的表达方式在3.2节有详细的介绍。

**模式一**

本文将3.4.1节中提出的软件高层需求评审和分析的目标满足性论证结构，软件低层需求评审和分析的目标满足性论证结构，软件源代码评审和分析的目标满足性论证结构融合，建立如图11所示的论证模式。能够实现DO-178C附录A中的目标A-3.1-A-3.7，A-4.1-A-4.7，A-5.1-A-5.6。

在图11所示模式中，总目标为G1，三种不同论证结构都需要实现的目标是G2.1，G2.2，G2.4，G2.5，G2.6，G3.1，G3.5，G3.6，G3.7，其余目标只有当其目标约束条件满足时才保留，这些目标约束条件已经标注在图11中。对应的证据S1，S2以及证据约束条件也标注在图中。

**模式二**

由于软件体系结构目标满足性论证结构和图11描述的三种论证结构差异比较大，因此将建立单独的目标满足性论证结构表达。由于该论证结构中所有目标所有类型的软件都要实现，因此，不存在变量以及可选目标，最终建立的论证模式如图8所示，此处不再赘述。

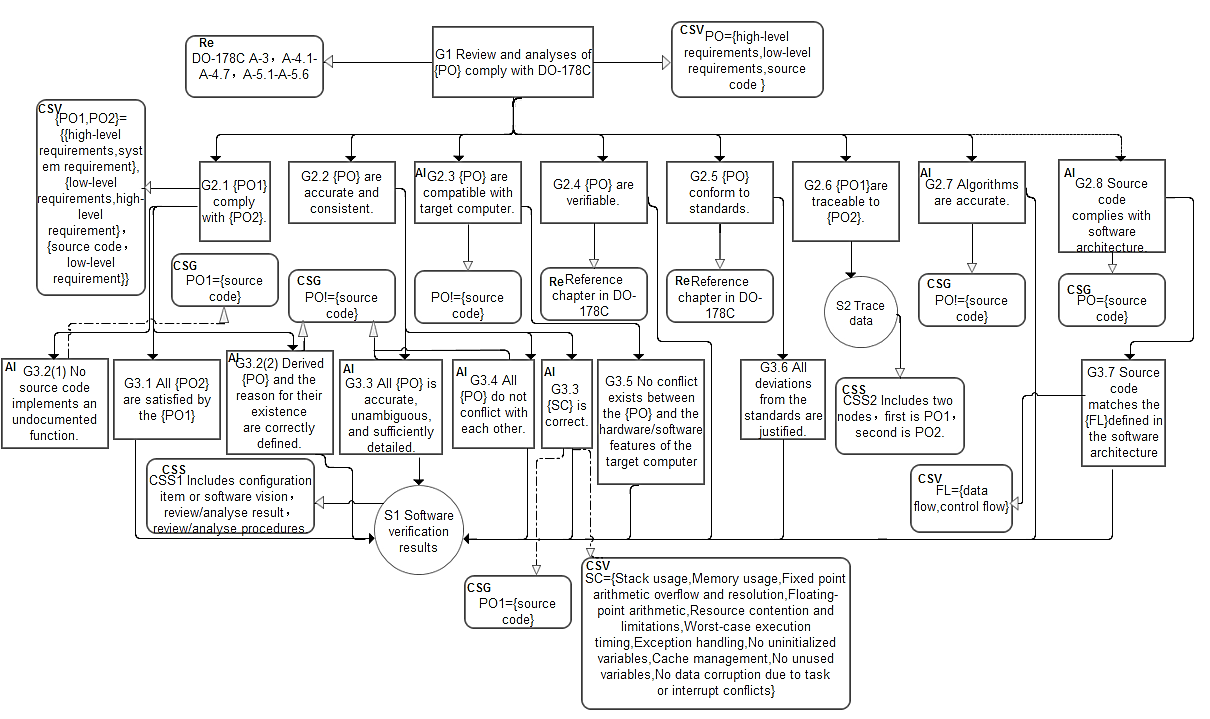


图 11 评审和分析目标满足性论证模式1

## 3.5 软件测试目标满足性论证模式

本节以RTCA DO-178C标准的软件测试过程与需求相关的目标为实例，说明提取项目无关目标满足性论证结构的过程。

DO-178C对软件测试过程中针对高层需求和低层需求需要满足的目标在附录A的表6中有详细的说明，主要包括4个目标，分别是：

1. 可运行代码符合（comply）高层需求。

2. 可运行代码满足对高层需求的健壮性（robust）。

3. 可运行代码符合（comply）低层需求。

4. 可运行代码满足对低层需求的健壮性（robust）。

下面将分别阐述这4个目标的论证结构，并依据论证结构提出软件测试过程目标满足性论证模式。

### 3.5.1 软件测试目标满足性论证结构

依据DO-178C标准对软件测试的定义，知道DO-178C标准规定的软件测试是基于需求的测试。软件测试活动包括三类，软件/硬件集成测试，软件集成测试和低层测试。软件/硬件集成测试为了验证软件在目标机环境下是否能够正确操作，软件集成测试为了验证软件需求和构件间的内部关系，低层测试为了验证低层需求的实现情况。

执行这三种测试活动后，需要进行基于需求的测试覆盖率分析，以及软件的结构覆盖率分析。最终测试活动结束。

本节主要论证软件测试过程中针对高层需求和低层需求需要满足的目标的论证过程。下面将分别建立这四个目标的目标满足性论证结构。

#### 3.5.1.1 高层需求-可运行代码符合性目标满足性论证结构

表11对目标（可运行代码符合（comply）高层需求）依据标准进行了详细的解读，确定了目标的具体论证结构。

表 11 高层需求-可运行代码符合性目标解读

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 总目标 | DO-178C标准规定了其需要执行的活动为标准中的6.4.2,6.4.2.1,6.4.3和6.5节。6.4.2节内容，论述了基于需求的测试用例选择的原则（必须包括正常测试用例和异常测试用例）。6.4.2.1节内容，论述了正常范围测试用例的选择。6.4.3节内容，论述了基于需求的测试方法，本目标中只需要关注软件/硬件集成测试的方法。6.5节内容，论述了追溯性，即测试用例和需求的追溯性，测试用例和测试程序的追溯性，测试程序和测试结果的追溯性。基于此，本文认为可以将这一目标分解为两类目标。第一类目标：论证所有的需求都执行测试高层需求的测试活动（软件/硬件集成测试），并且正常测试用例按标准要求完成测试。第二类目标：论证整个软件测试活动是可追溯的。 |
| 第一类目标 | DO-178C标准规定了其需要执行的活动为标准中的6.4.2,6.4.2.1,6.4.3节。在执行软件/硬件集成测试中，依据6.4.2.1节内容，论述了正常范围测试用例的选择，如边界类测试用例，状态转换测试用例以及针对逻辑表达式的测试用例。基于此，本文认为可以将其这一目标分为三个目标：包含实现了等价类，边界类测试用例；对状态转换功能，实现了正常操作下所有状态转换的测试用例；对于使用逻辑表达式表示的需求，包含了验证所有变量的测试用例。并且这三个目标可以通过测试用例数据论证。 |

**表 11 高层需求-可运行代码符合性目标解读（续）**

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 第二类目标 | DO-178C标准规定了其需要执行的活动为标准中的6.5节。6.5节内容，论述了需求，测试用例，测试程序，测试结果之间的追溯性要求。基于此，本文认为可以将这一目标分解为三个目标：所有高层需求都存在至少一个测试用例测试；所有测试用例都有测试程序实现；所有测试程序都有测试结果，并且测试结果为真。并且这三个目标可以通过追溯数据论证。 |

通过表11可知，测试用例可以作为证据论证第一类目标。追溯数据可以作为证据论证第二类目标。标准中对测试用例和追溯数据进行定义，在本论证过程中只选取和论证目标相关的项。具体证据的组成结构如表12所示。

表 12 高层需求-可运行代码符合性证据结构

|  |  |
| --- | --- |
| **证据** | **证据结构** |
| 测试用例 | 测试目标，输入，测试条件，预期结果，软件版本，需求类型，测试方法，测试用例唯一编号。 |
| 追溯数据 | 软件需求和测试用例间的关联，测试用例和测试程序间的关联，测试程序和测试结果间的关联。 |

通过上述分析，建立的高层需求-可运行代码符合性目标满足性论证结构如图12所示：

图12中，总目标G1为DO-178C标准中目标A-6.1。依据表11的目标解读，确定两种分解策略S1、S2（表11中总目标及总目标解读），第一类目标为G2.1，进一步分解为G3.1、G3.2、G3.3（表11中第一类目标及第一类目标解读）；第二类目标分解为G2.2、G2.3、G2.4（表11中第二类目标及第二类目标解读）；并最终通过证据E1（测试用例），E2（追溯数据）论证子目标是否成立。并且确定了目标G3.1、G3.2、G3.3由证据测试用例直接论证，目标G2.2、G2.3、G2.4由追溯数据直接论证。对于证据E1，E2的约束条件通过CSS1，CSS2定义出来。CSS1参照（表12测试用例证据结构），CSS2参照（表12追溯数据证据结构）。

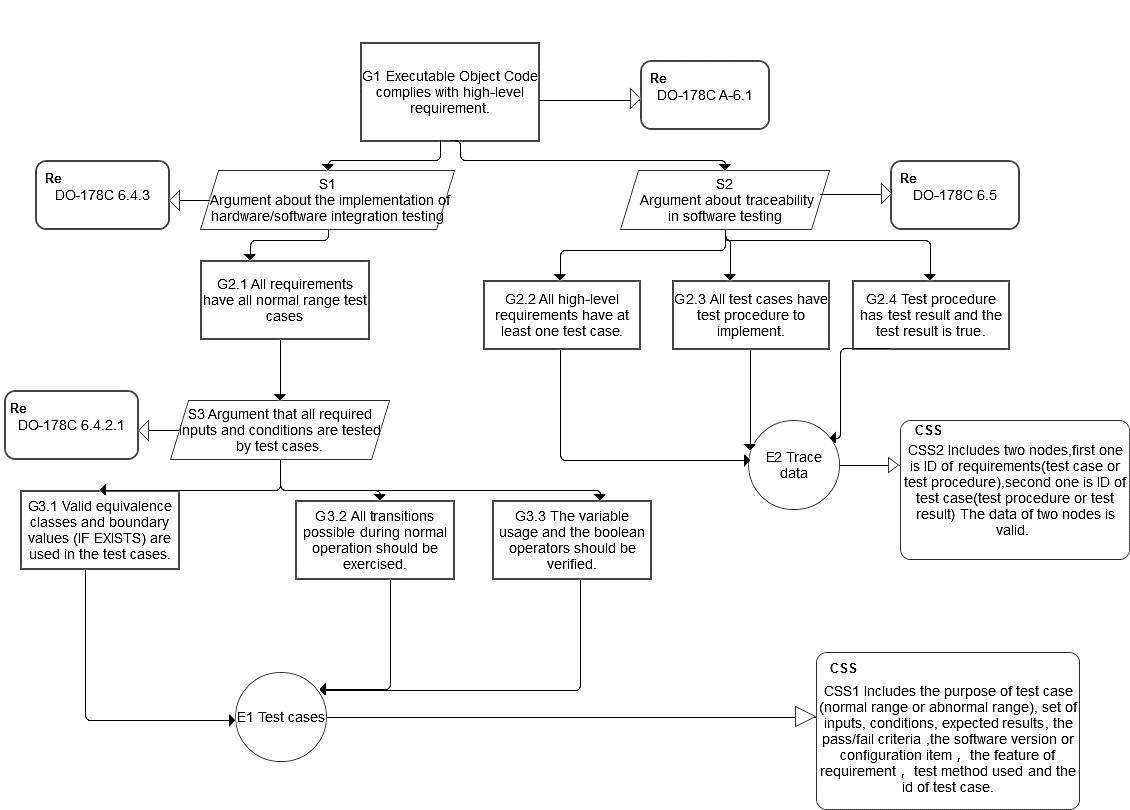


图 12 高层需求-可运行代码符合性目标满足性论证结构

#### 3.5.1.2 高层需求-可运行代码健壮性目标满足性论证结构

表13对目标（可运行代码满足对高层需求的健壮性（robust））依据标准进行了详细的解读，确定了目标的具体论证结构。

表 13 高层需求-可运行代码健壮性目标解读

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 总目标 | DO-178C标准规定了其需要执行的活动为标准中的6.4.2,6.4.2.2,6.4.3和6.5节。6.4.2节内容，论述了基于需求的测试用例选择的原则（必须包括正常测试用例和异常测试用例）。6.4.2.2节内容，论述了异常范围测试用例的选择。6.4.3节内容，论述了基于需求的测试方法，本目标中只需要关注软件/硬件集成测试的方法。6.5节内容，论述了追溯性，即测试用例和需求的追溯性，测试用例和测试程序的追溯性，测试程序和测试结果的追溯性。基于此，本文认为可以将这一目标分解为两类目标。第一类目标：论证所有的需求都执行测试高层需求的测试活动，并且健壮性测试用例按标准要求完成测试（软件/硬件集成测试）。第二类目标：论证整个软件测试活动是可追溯的。 |

表 13 高层需求-可运行代码健壮性目标解读（续）

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 第一类目标 | DO-178C标准规定了其需要执行的活动为标准中的6.4.2,6.4.2.2,6.4.3节。在执行软件/硬件集成测试中，依据6.4.2.2节内容，论述了异常测试用例的选择，如边界类测试用例，失效模式测试用例，超出响应时间测试用例等7种。基于此，本文认为可以将其这一目标分为七个目标：包括实现了等价类，边界类测试用例；异常情况下测试系统初始化功测试用例；测试可能的失效模式测试用例；测试超出循环量测试用例；测试超出响应时间帧测试用例；测试系统时间相关功能算数溢出保护机制测试用例；测试不允许发生的状态转换的测试用例。并且这七个目标可以通过测试用例数据论证。 |
| 第二类目标 | DO-178C标准规定了其需要执行的活动为标准中的6.5节。6.5节内容，论述了需求，测试用例，测试程序，测试结果之间的追溯性要求。基于此，本文认为可以将这一目标分解为三个目标：所有高层需求都存在至少一个测试用例测试；所有测试用例都有测试程序实现；所有测试程序都有测试结果，并且测试结果为真。并且这三个目标可以通过追溯数据论证。 |

通过表13可知，测试用例可以作为证据论证第一类目标。追溯数据可以作为证据论证第二类目标。标准中对测试用例和追溯数据进行定义，在本论证过程中只选取和论证目标相关的项。具体证据的组成结构如表12所示。

通过上述分析，建立的高层需求-可运行代码健壮性目标满足性论证结构如图13所示：

图13中，总目标G1为DO-178C标准中目标A-6.2。依据表13的目标解读，确定两种分解策略S1、S2（表13中总目标及总目标解读），第一类目标为G2.1，进一步分解为G3.1-G3.7（表13中第一类目标及第一类目标解读）；第二类目标分解为G2.2、G2.3、G2.4（表13中第二类目标及第二类目标解读）；并最终通过证据E1（测试用例），E2（追溯数据）论证子目标是否成立。对于证据E1，E2的约束条件通过CSS1，CSS2定义出来。同时确定了目标G3.1-G3.7由证据测试用例直接论证，目标G2.2、G2.3、G2.4由证据追溯数据直接论证。同时参照表12，,证据结构定义在CSS1（表12测试用例证据结构），CSS2（表12追溯数据证据结构）中。

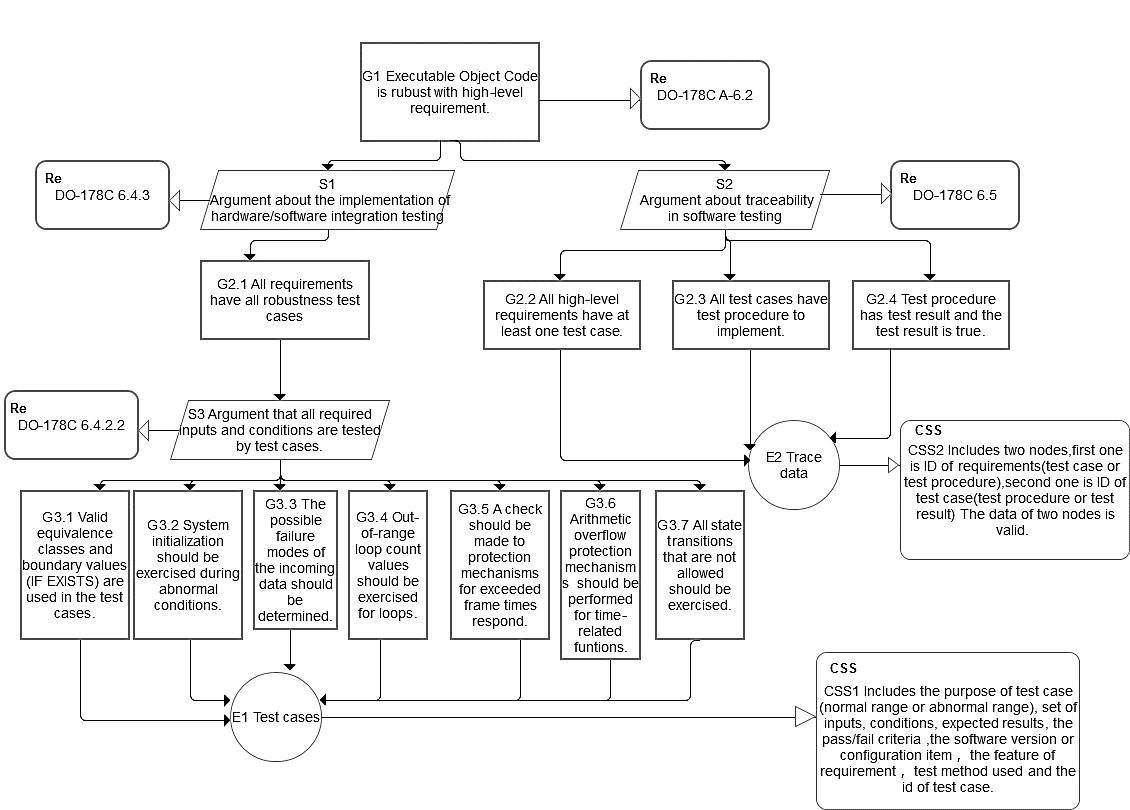


图 13 高层需求-可运行代码健壮性目标满足性论证结构

#### 3.5.1.3 低层需求-可运行代码符合性目标满足性论证结构

本目标（可运行代码符合（comply）低层需求）的解读与软件高层需求-可运行代码符合性目标满足性论证结构的表11，表12有很大的相似性，此处不再赘述，最终建立的低层需求-可运行代码符合性目标满足性论证结构如图14所示，图14中各个目标的分解情况与图12有很大的相似性，此处不再赘述。

#### 3.5.1.4 低层需求-可运行代码健壮性目标满足性论证结构

本目标（可运行代码满足对低层需求的健壮性（robust））的解读与高层需求-可运行代码健壮性目标满足性论证结构的表13，表12有很大的相似性，此处不再赘述，最终建立的低层需求-可运行代码健壮性目标满足性论证结构如图15所示，图15中各个目标的分解情况与图13有很大的相似性，此处不再赘述。

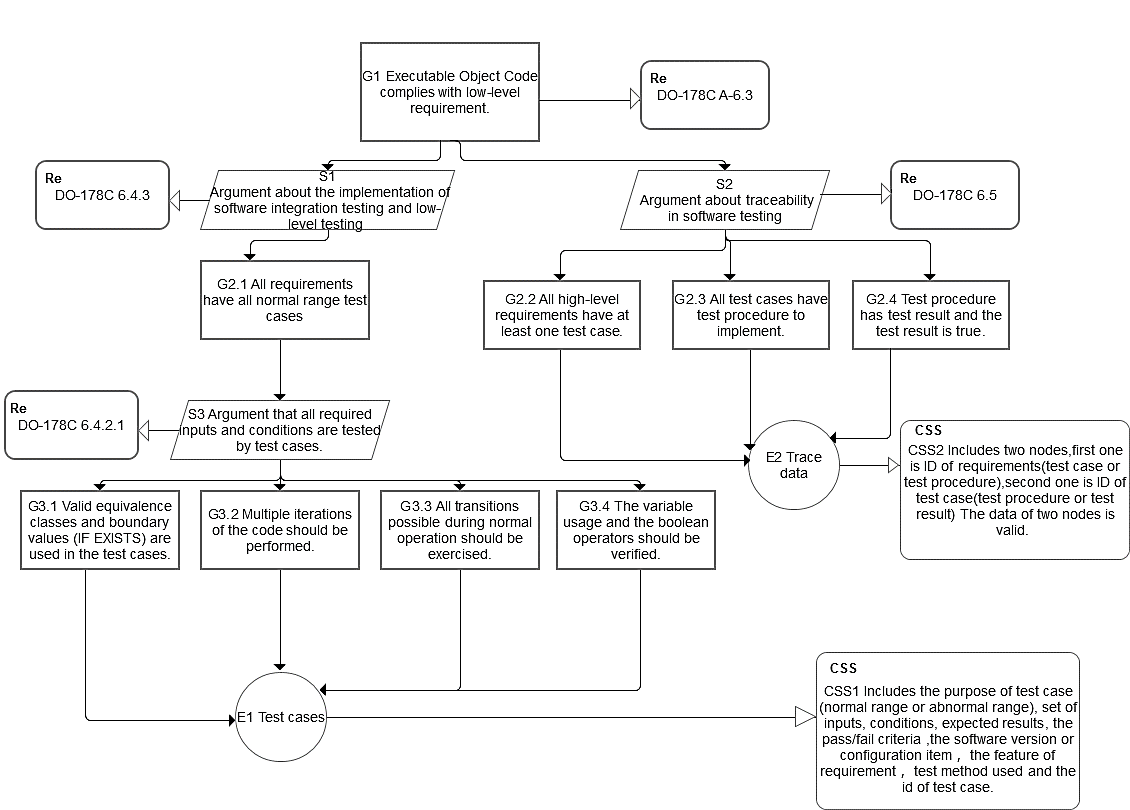


图 14 低层需求-可运行代码符合性目标满足性论证结构

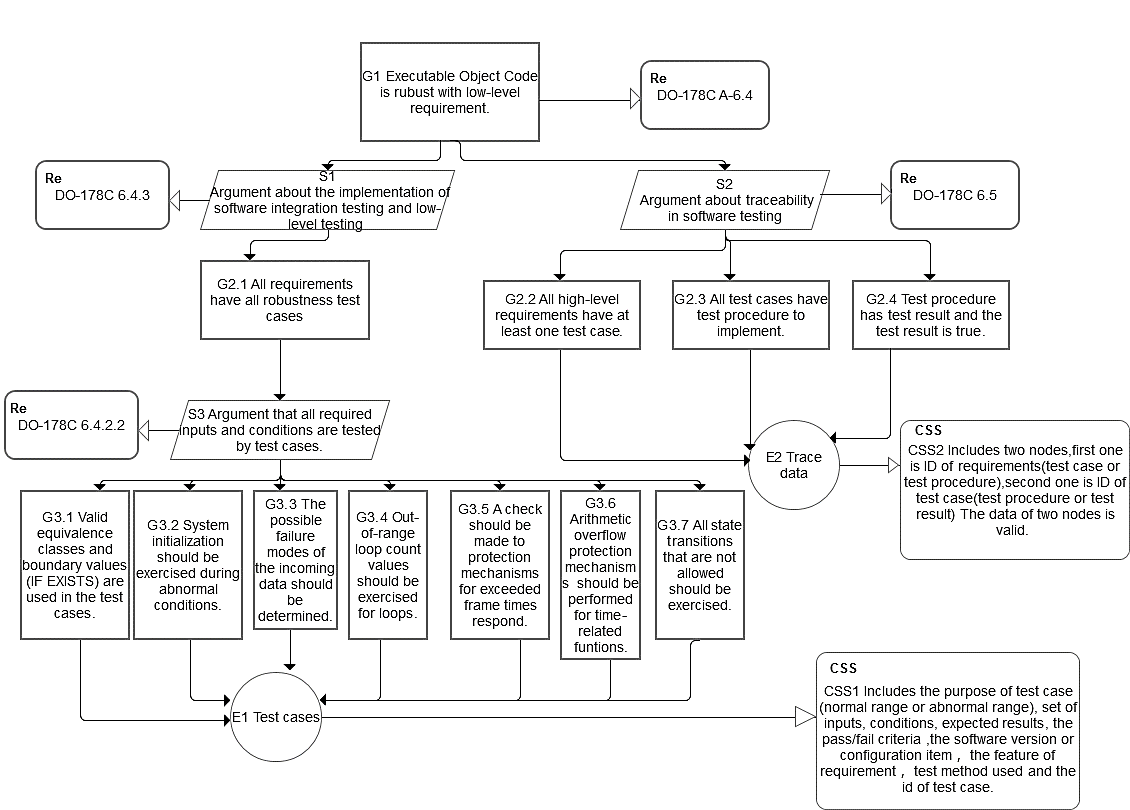


图 15 低层需求-可运行代码健壮性目标满足性论证结构

### 3.5.2 软件测试目标满足性论证模式

通过3.5.1节中归纳的DO-178C标准中对应软件测试实现的目标，以及执行的活动，可以发现这几种论证结构相似。因此，本文抽取出一种项目无关目标满足性论证模式，表达出通用的论证结构。接下来，这个论证模式将涉及特定项目的信息抽取出来，建立软件测试目标满足性论证模式。最终通过实例化方法可以满足不同项目不同目标的论证。

本文中软件测试目标满足性论证模式如图16，17所示：

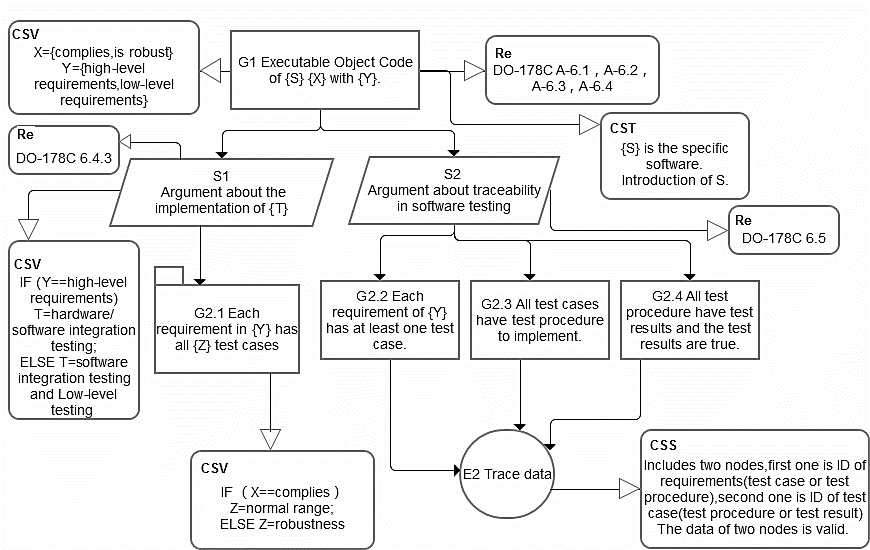


图 16 软件测试目标满足性论证模式（1）

本文将3.5.1节中提出的高层需求-可运行代码符合性，高层需求-可运行代码健壮性，低层需求-可运行代码符合性，低层需求-可运行代码健壮性四个论证结构融合，抽取出图16，17所示论证模式。能够实现DO-178C附录A中的目标A-6.1，A-6.2，A-6.3，A-6.4。

图16所示模式中，总目标为G1，将整个论证过程分为S1，S2两个子论证过程，S1论证每个需求都被测试用例完整测试，S2论证整个测试活动是可追溯的，其中S1的具体论证过程在图17中。S2的论证过程分为3个子目标分别论证了需求和测试用例，测试用例和测试程序以及测试程序和测试结果间的追溯性。S2的论证过程对应证据E2，证据约束条件标注在图中。

图17中，S1的论证过程分为8个子目标，这8个子目标均为可选目标，其对应的约束条件标注在图中，通过证据E1论证，E1的约束条件标注在表中。

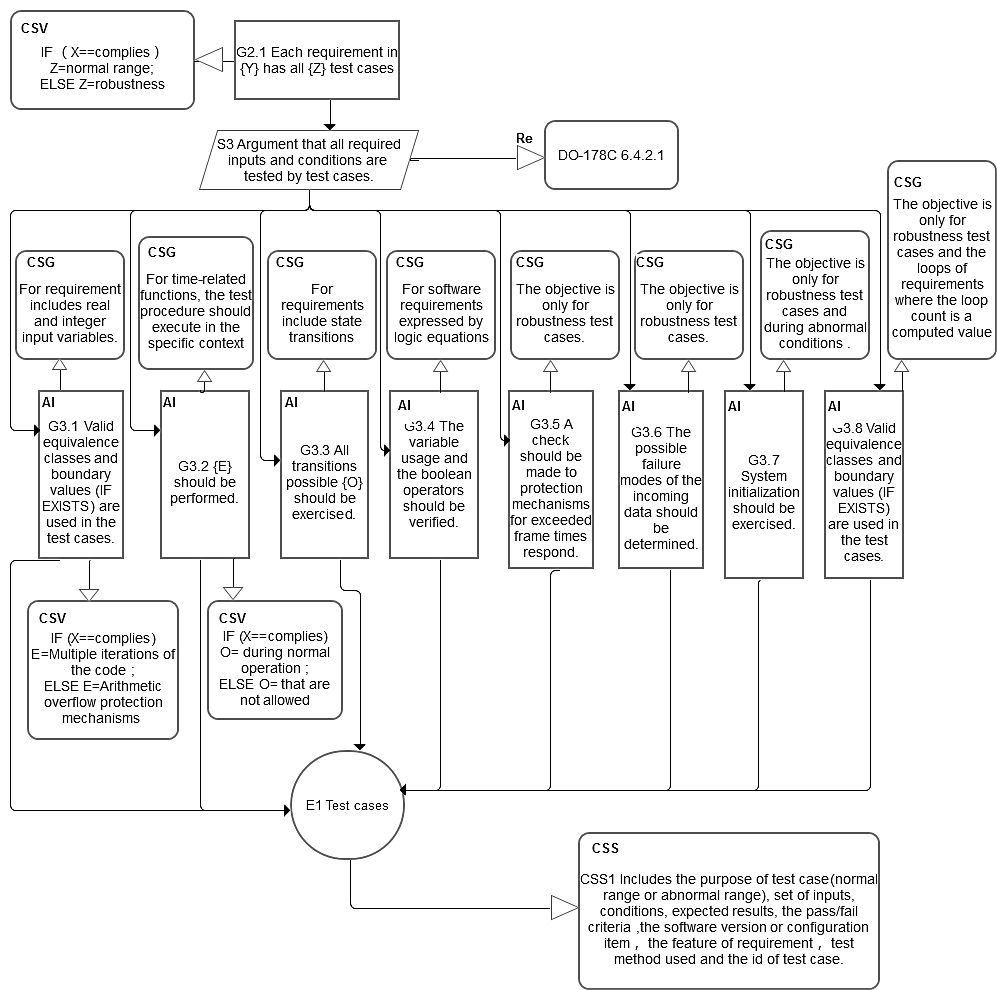


图 17 软件测试目标满足性论证模式（2）

## 3.6 测试需求覆盖率目标满足性论证模式

本文针对RTCA DO-178C标准的测试需求覆盖率分析提取项目无关目标满足性论证结构。

DO-178C对软件测试活动的需求覆盖率目标在附录A的表7中有详细的说明，主要包括2个目标，分别是：

1. 测试的高层需求覆盖率达到标准（achieve）。

2. 测试的低层需求覆盖率达到标准（achieve）。

下面将分别阐述这2个目标的论证结构，并依据论证结构提出测试需求覆盖率目标满足性论证模式。

### 3.6.1 测试需求覆盖率目标满足性论证结构

3.5.1节中提到测试活动结束后，需要进行基于测试的需求覆盖率分析，本节主要论证需求覆盖率分析阶段需要实现的目标。

依据DO-178C标准对测试需求覆盖率分析的描述，可以知道执行测试需求覆盖率分析的目标是检查是否需要添加额外的测试用例（测试用例必须是基于需求的）。

本小节主要论证执行测试需求覆盖率分析活动时需要实现的目标的论证过程。下面将分别建立这2个目标的目标满足性论证结构。

#### 3.6.1.1 测试高层需求覆盖率目标满足性论证结构

表14对目标（测试的高层需求覆盖率达到标准（achieve））依据标准进行了详细的解读，确定了目标的具体论证结构。

表 14 测试高层需求覆盖率目标解读

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 总目标 | DO-178C标准规定了其需要执行的活动为标准中的6.4.4.1节。6.4.4.1节内容，论述了四项要求，分别是存在追溯数据保证每个需求都有测试用例测试；测试用例满足测试用例设计时正常测试和健壮性测试准则；所有分析过程中发现的异常都解决；追溯性，即所有测试用例，测试程序都可以追溯到需求。基于此，本文认为可以将这一目标分解为三类目标。第一类目标：测试用例覆盖了所有需求。第二类目标：所有的测试活动都是基于需求的。第三类目标：整个覆盖率分析过程中发现的缺陷都记录并解决。 |
| 第一类目标 | DO-178C标准规定了其需要执行的活动为标准中的6.4.4.1.a，6.4.4.1.b节。6.4.4.1.a以及6.4.4.1.b节内容，论述了每个需求都有测试用例，并且测试用例也满足了正常测试和健壮性测试的规则。基于此，本文认为可以将其这一目标分为两个目标：基于需求的测试用例满足规定的正常以及健壮性测试用例；所有需求都存在正常以及健壮性测试用例。第一个子目标通过软件验证结果论证，第二个子目标通过测试用例和追溯数据来论证。 |

表 14 测试高层需求覆盖率目标解读（续）

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 第二类目标 | DO-178C标准规定了其需要执行的活动为标准中的6.4.4.1.d节。6.4.4.1.d节内容，论述了需求，测试用例，测试程序之间的追溯性要求。基于此，本文认为可以将这一目标分解为两个目标：所有测试用例都可追溯到需求；所有测试程序都可以追溯到测试用例。并且这两个目标可以通过追溯数据论证。 |
| 第三类目标 | DO-178C标准规定了其需要执行的活动为标准中的6.4.4.1.c节。6.4.4.1.c节内容，论述了所有分析过程中发现的缺陷都要解决。基于此，本文认为可以将这一目标分解为一个目标：所有发现的缺陷都被记录下来并解决了。并且这个目标可以通过问题报告论证。 |

通过表14可知，软件验证结果，测试用例，追溯数据可以作为证据论证第一类目标。追溯数据可以作为证据论证第二类目标。问题报告可以作为证据论证第三类目标。标准中对上述证据进行定义，在本论证过程中只选取和论证目标相关的项。具体证据的组成结构如表15所示。

表 15 测试高层需求覆盖率证据结构

|  |  |
| --- | --- |
| **证据** | **证据结构** |
| 软件验证结果 | 需求和测试用例的配置项或版本信息，评审结果，评审过程描述。 |
| 测试用例 | 测试目标（正常或异常测试），输入集合，测试条件，预期结果，需求版本，使用测试方法以及测试用例唯一编号。 |
| 追溯数据 | 软件需求和测试用例间的关联，测试用例和测试程序间的关联。 |
| 问题报告 | 软件配置项，问题发现时软件所处生命周期，问题描述，解决方案描述以及当前问题状态。 |

通过上述分析，建立的测试高层需求覆盖率目标满足性论证结构如图18所示：

图18中，总目标G1为DO-178C标准中目标A-7.3。依据表14的目标解读，确定三种分解策略S1、S2、S3（表14中总目标及总目标解读），第一类目标为G2.1，进一步分解为G3.1、G3.2（表14中第一类目标及第一类目标解读）；第二类目标分解为G2.2、G2.3（表14中第二类目标及第二类目标解读）；第三类目标分解为G2.4（表14中第三类目标及第三类目标解读）。并最终通过证据E1（软件验证结果），E2（测试用例），E3（追溯数据），E4（问题报告）论证子目标是否成立。同时参照表15，,证据结构定义在CSS中。

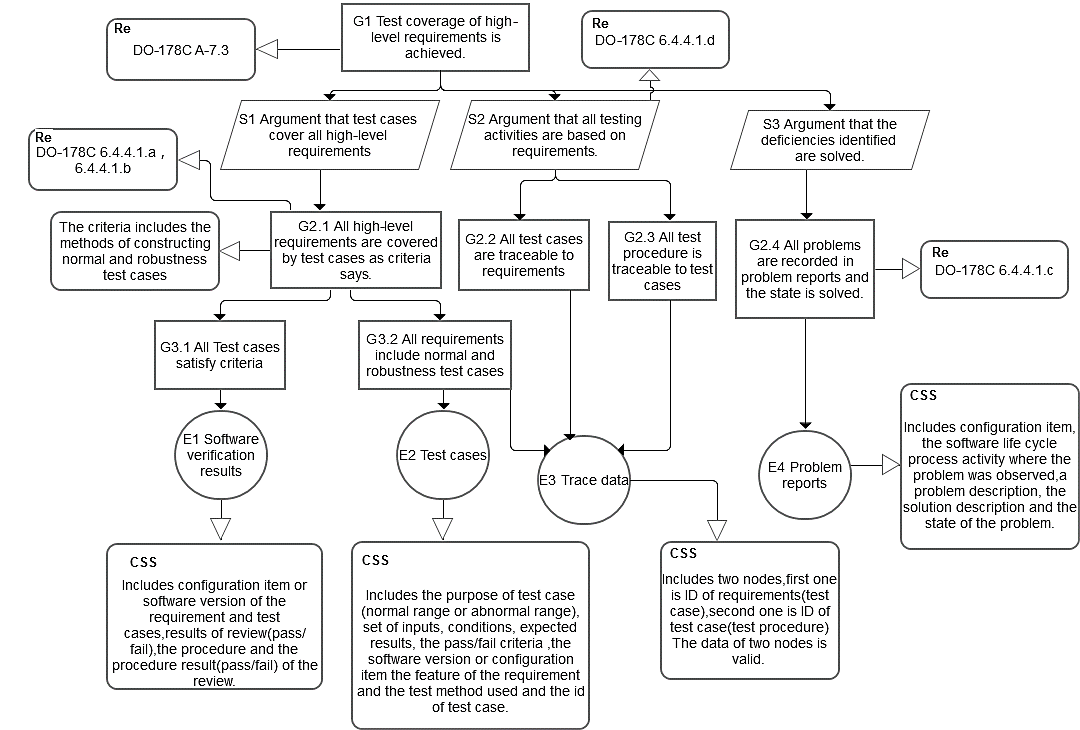


图 18 测试高层需求组覆盖率目标满足性论证结构

#### 3.6.1.2 测试低层需求覆盖率目标满足性论证结构

本目标（测试的低层需求覆盖率达到标准（achieve））的解读与测试高层需求覆盖率目标满足性论证结构的表14，表15有很大的相似性，此处不再赘述，最终建立的测试低层需求覆盖率目标满足性论证结构如图19所示，图19中各个目标的分解情况与图18有很大的相似性，此处不再赘述。

### 3.6.2 测试需求覆盖率目标满足性论证模式

通过3.6.1节中提出的DO-178C标准中软件测试需求覆盖率分析实现的目标，以及执行的活动，可以发现这2种论证结构相似，因此，本文抽取出一种项目无关目标满足性论证模式，表达出通用的论证结构。此外，这个论证模式将涉及特定项目的信息抽取出来，建立测试需求覆盖率目标满足性论证模式。因此，最终通过实例化方法可以满足不同项目不同目标的论证。

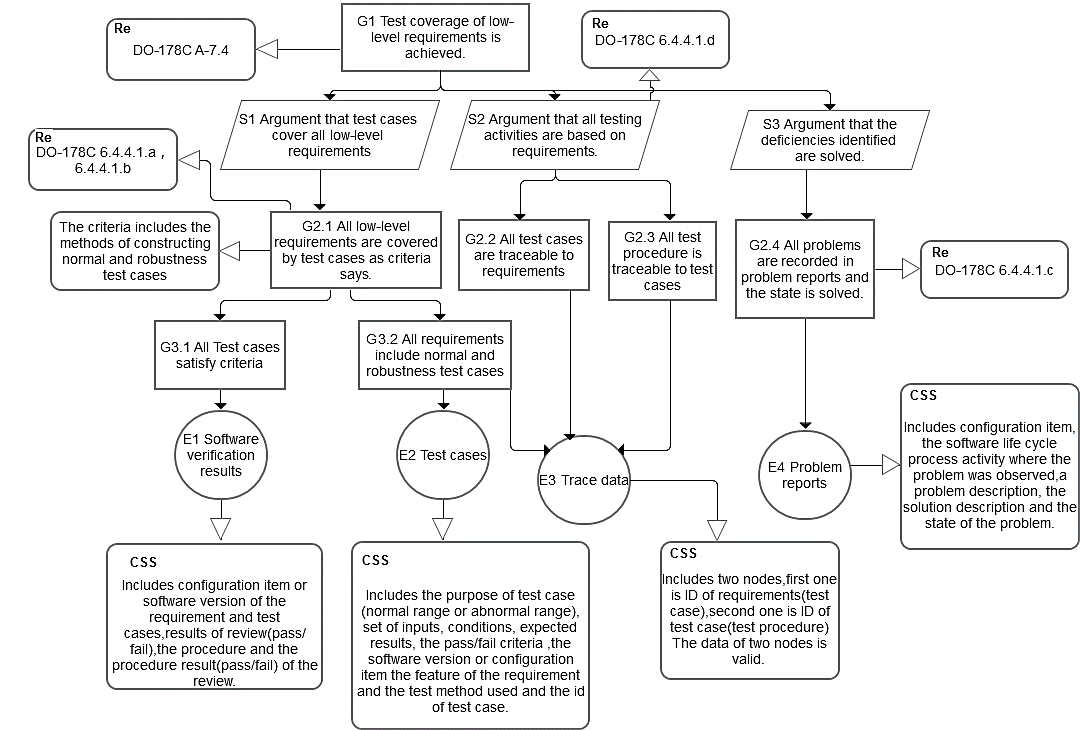


图 19 测试低层需求组覆盖率目标满足性论证结构

本文中测试需求覆盖率目标满足性论证模式如图20所示：

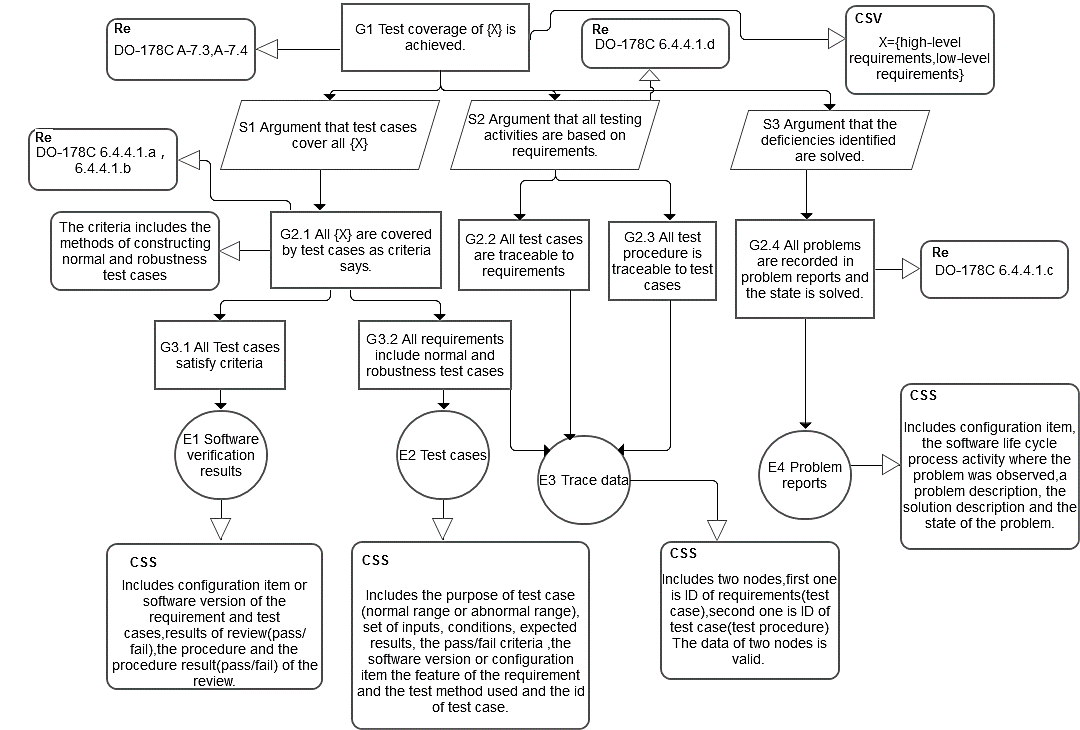


图 20 测试需求覆盖率目标满足性论证模式

本文将3.6.1节中提出的测试高层需求覆盖率目标满足性论证结构，测试低层需求覆盖率目标满足性论证结构2个论证结构融合，抽取出图20所示论证模式。能够实现DO-178C附录A中的目标A-7.3，A-7.4。

图20所示模式中，总目标为G1，将整个论证过程分为S1，S2，S3三个子论证过程，S1论证测试用例覆盖了所有需求，S2论证所有测试活动都是基于需求的，S3论证整个覆盖率分析过程中发现的缺陷都记录并解决了。第一类论证结构分解为G3.1和G3.2两个子目标，通过软件验证结果和测试用例，追溯数据分别论证；第二类论证结构分解为G2.2，G2.3，通过追溯数据论证。第三类论证结构分解为G2.4，由问题报告论证。证据的约束条件在证据约束条件符号里表示。

## 3.7 结构测试覆盖率目标满足性论证模式

本文针对RTCA DO-178C标准的结构覆盖率分析提取项目无关目标满足性论证结构。

DO-178C对软件测试活动的结构覆盖率目标在附录A的表7中有详细的说明，主要包括4个目标，分别是：

1. 测试的MC/DC覆盖率达到标准（achieve）。

2. 测试的判定覆盖率达到标准（achieve）。

3. 测试的语句覆盖率达到标准（achieve）。

4. 验证额外代码达到标准（achieve）。

下面将分别阐述这4个目标的论证结构，并依据论证结构提出测试需求覆盖率目标满足性论证模式。

### 3.7.1 结构测试覆盖率目标满足性论证结构建立

3.5.1节中提到测试活动结束后，需要进行覆盖率分析，首先进行需求覆盖率分析，论证结构在3.6节阐述。接下来进行结构覆盖率分析，本节主要论证结构覆盖率分析阶段需要实现的目标。

依据DO-178C标准对结构覆盖率分析的定义，其中语句覆盖率，分支覆盖率以及MC/DC覆盖率的定义和标准定义一致，此处不再赘述。需要指出的是，标准中的多余代码指的是：不能够追溯到源代码的目标代码或者可运行目标代码。标准指出这类代码可能不会立刻直接在代码级别显示出副作用，因此需要额外的验证手段。

本小节主要论证执行结构覆盖率分析活动时需要实现的目标的论证过程。下面将分别建立这4个目标的目标满足性论证结构。

#### 3.7.1.1 MC/DC覆盖率目标满足性论证结构

表16对目标（测试的MC/DC覆盖率达到标准（achieve））依据标准进行了详细的解读，确定了目标的具体论证结构。

通过表16可知，软件验证结果，可以作为证据论证第一类目标、第二类目标。问题报告可以作为证据论证第三类目标。标准中对上述证据进行定义，在本论证过程中只选取和论证目标相关的项。具体证据的组成结构如表17所示。

表 16 MC/DC覆盖率目标解读

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 总目标 | DO-178C标准规定了其需要执行的活动为标准中的6.4.4.2.a，6.4.4.2.b，6.4.4.2.d，6.4.4.3节。6.4.4.2.a节内容，论述了软件结构覆盖率要符合软件要求。6.4.4.2.b节内容，论述了软件结构覆盖率分析的对象是源代码，目标代码或可运行目标代码，并且强调A级软件需要验证额外代码的要求。6.4.4.2.d节，6.4.4.3节内容，论述了结构覆盖率分析发现的缺陷的解决方案要求。基于此，本文认为可以将这一目标分解为三类目标。第一类目标：验证额外代码。第二类目标：代码的MC/DC覆盖率达到要求。第三类目标：整个覆盖率分析过程中发现的缺陷都记录并解决了。 |
| 第一类目标 | DO-178C标准规定了其需要执行的活动为标准中的6.4.4.2.b节。6.4.4.2.b节内容，论述了A级软件需要验证额外代码（不能追溯到源代码的代码）。基于此，本文认为针对第一类存在能够直接论证其正确性的证据，因此，认为其已经不需要进一步分解；并且这一目标可以通过软件验证结果论证。 |
| 第二类目标 | DO-178C标准规定了其需要执行的活动为标准中的6.4.4.2.a、6.4.4.2.b节。6.4.4.2.a节内容，论述了对软件的结构覆盖率要求。6.4.4.2.b内容，论证了结构覆盖率分析的对象可以是源代码，目标代码或可运行目标代码。基于此，本文认为可以将这一目标分解为一个目标：源代码（目标代码或可运行目标代码）的MC/DC覆盖达到要求。并且这个目标可以通过软件验证结果论证。 |

表 16 MC/DC覆盖率目标解读（续）

|  |  |
| --- | --- |
| **目标** | **目标解读** |
| 第三类目标 | DO-178C标准规定了其需要执行的活动为标准中的6.4.4.2.d，6.4.4.3节。6.4.4.2.d，6.4.4.3节内容，论述了所有分析过程中发现的缺陷都要解决并提出不同缺陷的解决方案。基于此，本文认为可以将这一目标分解为四个目标：基于需求的测试用例或测试程序有缺陷时，对测试用例或测试程序进行修改；当软件需求有缺陷时，修改软件需求，添加测试用例测试该需求；存在额外代码时需移除该代码；存在停用代码时，如果停用代码永不使用，需要保证其永不被调用；如果停用代码在特定环境下运行，测试该代码在该环境下运行。并且这四个目标可以通过问题报告论证。 |

表 17 MC/DC覆盖率证据结构

|  |  |
| --- | --- |
| **证据** | **证据结构** |
| 软件验证结果 | 需求和测试用例的版本信息，评审结果，评审过程描述，覆盖率分析结果。 |
| 问题报告 | 软件配置项，问题发现时软件所处生命周期，问题描述，解决方案描述以及当前问题状态。 |

通过上述分析，建立的MC/DC覆盖率目标满足性论证结构如图21所示：

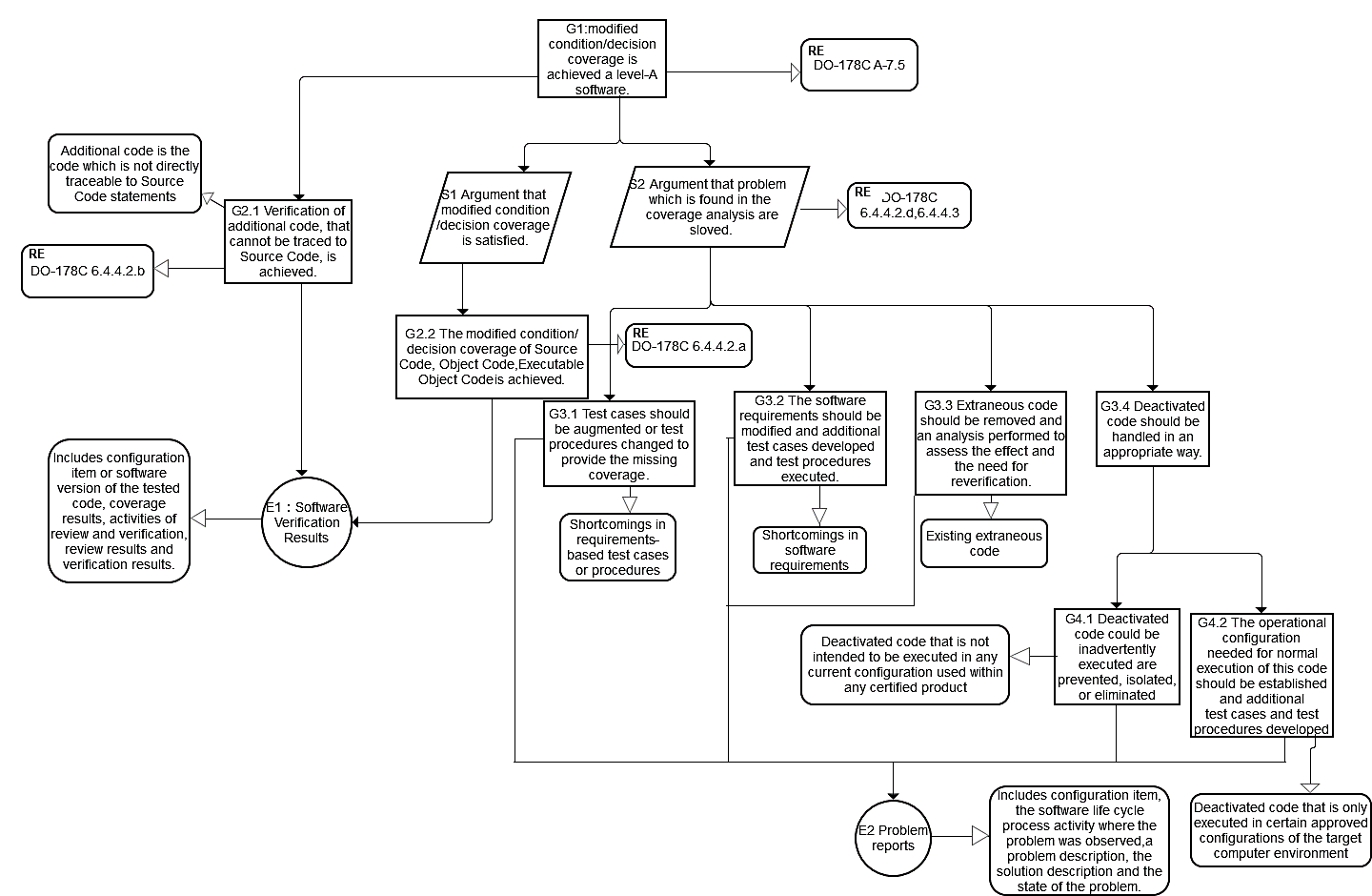


图 21 MC/DC覆盖率目标满足性论证结构

图21中，总目标G1为DO-178C标准中目标A-7.5。依据表16的目标解读，确定三种分解策略G2.1、S2、S3（表16中总目标及总目标解读），第一类目标为G2.1（表16中第一类目标及第一类目标解读）；第二类目标分解为G2.2（表16中第二类目标及第二类目标解读）；第三类目标分解为G3.1-G3.4，并且G3.4分解为G4.1、G4.2（表16中第三类目标及第三类目标解读）。并最终通过证据E1（软件验证结果），E2（问题报告）论证子目标是否成立。同时参照表17，,证据的详细结构定义在不同证据的证据约束条件（CSS）中。

#### 3.7.1.2 判定覆盖率目标满足性论证结构

本目标（测试的判定覆盖率达到标准（achieve））的解读与MC/DC覆盖率目标满足性论证结构的表16，表17有很大的相似性，此处不再赘述，最终建立的判定覆盖率目标满足性论证结构如图22所示，图22中各个目标的分解情况与图21有很大的相似性，此处不再赘述。

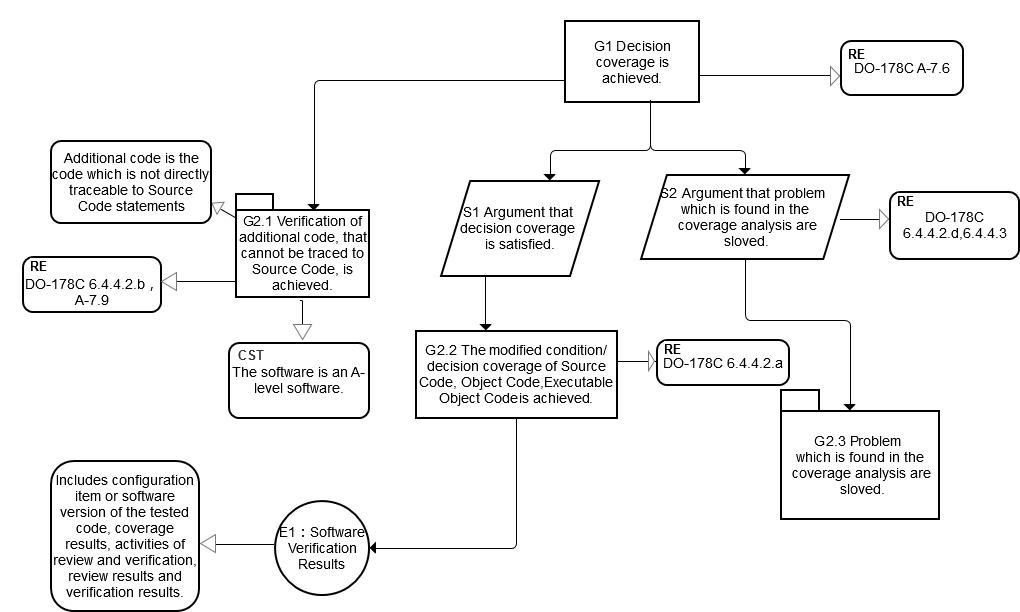


图 22 判定覆盖率目标满足性论证结构

#### 3.7.1.3 语句覆盖率目标满足性论证结构

本目标（测试的语句覆盖率达到标准（achieve））的解读与MC/DC覆盖率目标满足性论证结构的表16，表17有很大的相似性，此处不再赘述，最终建立的判定覆盖率目标满足性论证结构如图23所示，图23中各个目标的分解情况与图21有很大的相似性，此处不再赘述。

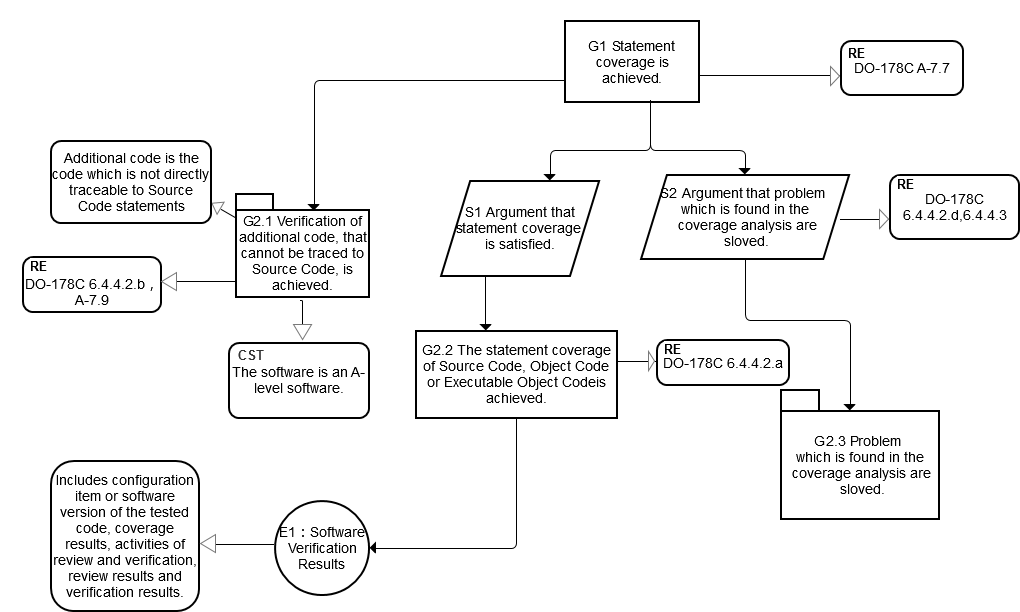


图 23 语句覆盖率目标满足性论证结构

#### 3.7.1.4 额外代码目标满足性论证结构

需要说明的是，建立MC/DC覆盖率目标满足性论证结构中子目标G2.1即为本目标，因此，具体论证过程在MC/DC覆盖率目标满足性论证结构中完整展示，此处不再赘述。

### 3.7.2 结构测试覆盖率目标满足性论证模式

通过3.7.1节中提出的DO-178C标准中结构测试覆盖率分析实现的目标，以及执行的活动，可以发现这几种论证结构相似，因此，本文抽取出一种项目无关目标满足性论证模式，表达出通用的论证结构。此外，这个论证模式将涉及特定项目的信息抽取出来，建立结构测试覆盖率目标满足性论证模式。因此，最终通过实例化方法可以满足不同项目不同目标的论证。

本文将本文3.7.1节中提出的MC/DC覆盖率目标满足性论证结构，判定覆盖率目标满足性论证结构，语句覆盖率目标满足性论证结构3个论证结构融合，抽取出图24所示论证模式。能够实现DO-178C附录A中的目标A-7.5、A-7.6、A-7.7。

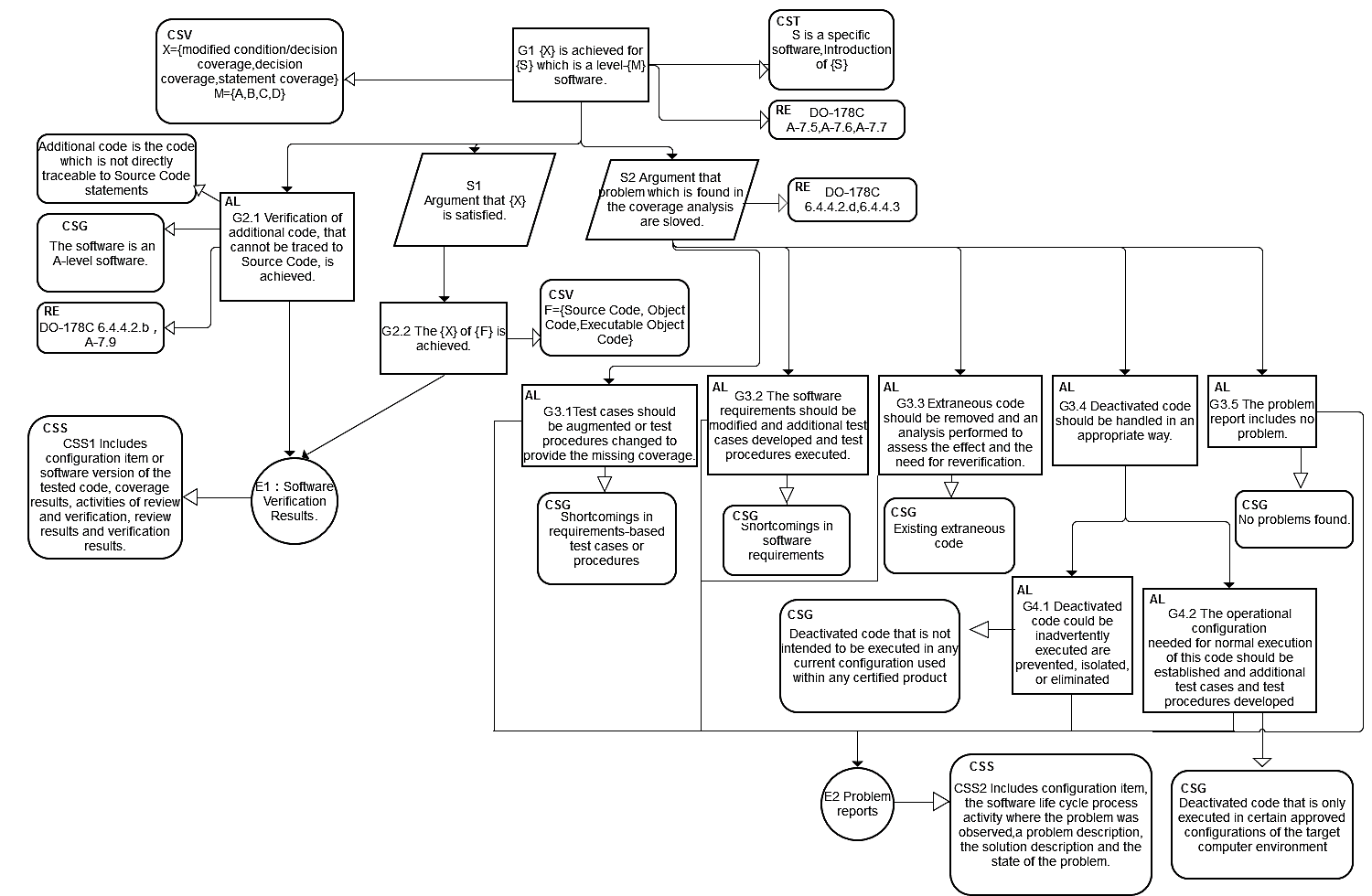


图 24 结构测试覆盖率目标满足性论证模式

图24所示模式中，总目标为G1，将整个论证过程分为三个子论证过程，G2.1论证额外代码（只有A级软件需要满足此要求），S1论证代码的结构化覆盖率，S2论证整个覆盖率分析过程中发现的缺陷都记录并解决了。第一类论证结构分解为G2.1，通过软件验证结果论证；第二类论证结构分解为G2.2，通过软件验证结果论证，第三类论证结构分解为G3.1、G3.2、G3.3、G3.4、G3.5，这5个目标为可选目标，对应的目标约束条件定义在其辅助论证结构中，最终由问题报告论证。证据的约束条件在证据约束条件符号里表示。

## 3.8 小结

本章主要描述了建立目标满足性论证模式的方法。首先提出了对GSN的表示符号扩展方法，为描述目标满足性论证模式做准备。

接下来，给出了抽取目标满足性论证模式的具体方法。

接下来本文提出了五种基于DO-178C标准的论证模式，分别是评审分析目标满足性论证模式一，评审分析目标满足性论证模式二，软件测试目标满足性论证模式，测试需求覆盖率目标满足性论证模式，结构测试覆盖率目标满足性论证模式。并给出了建立这五种模式的具体过程。首先基于DO-178C标准抽取不同目标的论证结构，其次，找出他们的共同之处，将具有相似论证结构的目标融合在一种论证模式中，并找出项目相关特征，通过本章给出的方法进行抽取，最终建立目标满足性论证模式。

# 第四章 建立基于DO-178C的目标满足性论证模型方法研究

## 4.1 建立目标满足性论证模型方法分析

本文建立了基于DO-178C标准的目标满足性论证模式，这是一种项目无关的论证模式，为建立项目相关的目标满足性论证模型提供了基础和基本框架。本章将描述建立目标满足性论证模型的具体方法，并提出目标满足性论证模型向文本形式转换的设想。

通过提出的目标满足性论证模型，可以将其转换为文本表达方式。为实现基于证据的论证过程建立文本表达的形式，为未来进行的论证工作做准备。

基于目标满足性论证模式，我们提出了建立目标满足性论证模型的方法，具体流程如图25所示：

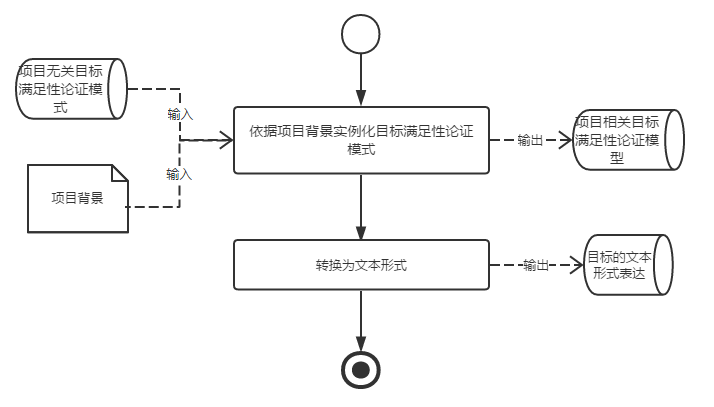


图 25 目标满足性论证模型建立流程

如图25所示，首先依据建立的目标满足性论证模式，以及项目的具体特征，实例化目标满足性论证模式，建立项目相关目标满足性论证模型。第二步，将建立完成的项目相关目标满足性论证模型转换为文本表达方式，最终建立目标满足性论证的文本表示。

通过分层的方法建立项目相关的目标满足性论证模型有助于将特定项目的论证模型和安全标准分离，提高目标满足性论证模型的复用性。

## 4.2 目标满足性论证模式实例化

### 4.2.1目标满足性论证模式实例化方法

通过第三章建立的目标满足性论证模式，结合项目背景，本文提出了实例化目标满足性论证模式的具体方法，分为下面几步：

1. 采用自顶向下实例化的分析方法，从总目标到子目标（策略）逐层进行实例化。对目标（策略）实例化的具体方法为：

1.1结合项目真实情况实例化目标（策略）中的变量，将变量赋值。对于定义变量约束条件的变量，其实例化范围为变量约束条件中的取值。对于没有定义变量约束条件的变量，其变量的实例化参考论证模式中上下文符号里的提示或其他约束条件，结合项目实际情况进行实例化。实例化完成后，将变量约束条件删除。

1.2结合项目真实情况判断支撑目标的目标约束条件是否成立，调整论证结构。结合项目真实情况情况判断目标约束条件的真假；当目标约束条件为真时，保留其对应的可选目标并转换为一般目标，将目标约束条件中的内容转换为假设的表示符号（GSN标准表示符号）保留在最终建立的目标满足性论证模式中。当目标约束条件为假时，删除约束条件以及其对应的可选目标，同时删除该可选目标关联的论证结构。

1.3按照支撑子目标的其他约束条件修改目标满足性论证模型，完成后，删除其他约束条件。

1.4 将关联标准章节符号转化为上下文符号（GSN标准表示符号）。

2. 结合项目真实情况，如果存在下面情况中的一项或几项：1）现有证据不能直接论证对应子目标；2）子目标需要进一步分解；3）需要添加多项子目标才能论证对应的子目标；4）存在多种证据论证某一子目标；那么可以依据项目真实情况添加或者修改子目标（策略或证据），完善目标满足性论证模型。需要注意的是，如果添加了证据数据，必须添加其对应的证据约束条件。

3. 自顶向下实例化所有目标后，项目中用来论证的证据结构必须包含目标满足性论证模式在证据约束条件中定义的项，否则不能进行下一步推理论证。如果证据数据和实际数据不完全一致，保证实际数据包含证据数据约束条件的所有项，同时修改该证据数据为实际数据的名称。将证据对应的证据约束条件转化为上下文。

4. 检查实例化后的目标满足性论证模型。最终建立的目标满足性论证模型，结构上不能包含变量约束条件，其他约束条件，目标约束条件，可选目标和证据约束条件。内容上不能包含没有实例化的变量，自己添加的子目标中的语句不能包含疑问句，或者可能，也许，如果等含有不确定含义的词语。如果没有满足上面提出的要求，则返回1,2,3步，继续进行实例化，直到满足4的要求为止。

### 4.2.2目标满足性论证模型示例

为了能够更加具体的描述目标满足性论证模式实例化为目标满足性论证模型的过程，通过对本文中3.7.2节提出的结构测试覆盖率目标满足性论证模式进行实例化，说明4.2.1节中的具体步骤。

以某机载操作系统为例，该操作系统定义为DO-178C中的A级软件，论证DO-178C标准中的目标A-7.7：测试的语句覆盖率达到标准。接下来具体描述实例化本文3.7.2节中图24的过程：

1. 图24中建立的模式中总目标G1包含的变量有：X,S,M。为了论证本目标，X的取值为statement coverage（语句覆盖率）；S的取值为OS，OS为此操作系统的简称；M的取值为A，此软件为A级软件； 删除辅助论证G1的变量约束条件和其他约束条件。

2. G1可以分解为三种子论证结构。先实例化第一种子论证结构，G2.1。G2.1是可选目标，此软件满足目标约束条件“M==A”，因此，此时将目标约束条件转换为假设（GSN标准符号），将可选目标转换为一般目标。

3. 实例化第二种子论证结构，S1。S1中的变量X即为G1中定义的X，将X赋值为statement coverage，S1分解为子目标G2.2。G2.2中包含两个变量：X,F。其中X值为statement coverage，此案例中语句覆盖率是针对可运行目标代码的，因此将F取值为Executable Object Code，删除辅助论证G2.2的变量约束条件。

4. 实例化第三种子论证结构，S2中不存在约束和变量，因此，保留不变化。

5. 第一个论证结构，第二个论证结构均不存在第三层子目标。因此，继续实例化第三个子论证结构的子目标。实例化子目标G3.1，G3.2，G3.3，G3.4，G3.5，这5个子目标均为可选目标。本例在分析语句分析覆盖率时不满足前4个子目标提出的目标约束条件，因此，将这四个子目标及对应的目标约束条件删除。符合子目标G3.5的目标约束条件，因此，此时将G3.5的目标约束条件转换为G3.5的假设（GSN标准符号），将G3.5转换为一般目标。

6. 模式中除证据结构及其辅助论证结构外，所有的结构都完成实例化。依据项目实际情况，项目提供的证据数据能够直接论证最底层子目标，不需要添加额外的论证结构。因此，接下来，确定项目中作为证据的数据项满足目标满足性论证模式中对证据的约束条件，将证据约束条件转化为上下文。到此，论证模式的实例化工作完成。

7. 检查实例化完成后的目标满足性论证模型，不存在变量，可选目标，以及各类约束条件。因此，此时，基于DO-178C标准目标A-7.7的项目相关目标满足性论证模型建立完成。

建立的项目相关目标满足性论证模型如图26所示：

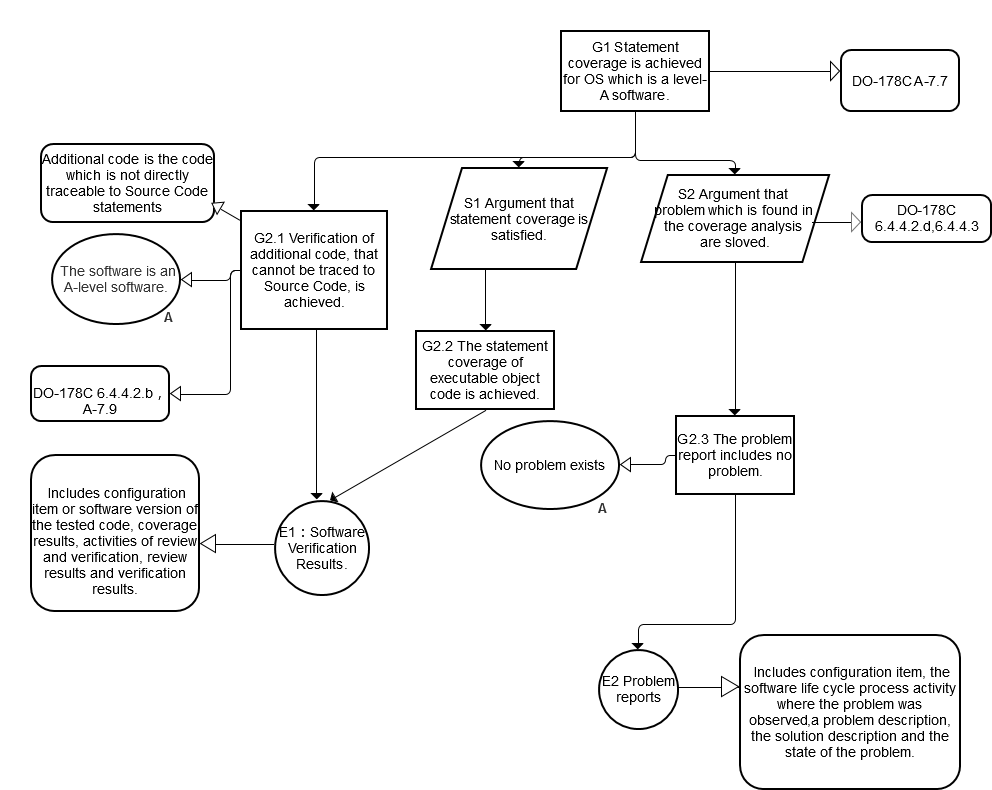


图 26 项目相关目标满足性论证模型

图26中，依据本文4.2.1节中提出的实例化方法实施，最终建立的论证结构分为三部分G2.1，G2.2，G2.3。由E1（软件验证过程），E2（问题报告）支撑论证。最终建立的论证模型不存在约束条件，不存在变量，只保留了GSN中规定的基本符号。实现了从目标满足性论证模式向目标满足性论证模型的转换。

## 4.3 目标满足性论证模型文本表达方法

为了能够将使用GSN结构表达的目标满足性论证模型使用文本的形式表达出来，本文使用了从目标满足性论证模型向文本形式表达的方法。

本文将定义遍历GSN模型的算法，遍历GSN模型，最终得出目标满足性论证模型的文本形式。

为了实现遍历算法，定义如下数据结构：

GSN图形中目标节点的数据结构是：xxx的标识号（xxx\_id），所属类型（主要论证符号或辅助论证符号），与其相关联的主要论证符号的标识号，与其相关联的辅助论证符号的标识号，节点信息描述。

定义好数据结构后，实现的算法流程为：

1. 遍历所有节点，找到最底层子目标，即与证据结构相连的主要论证目标节点。

2. 将每个最底层子目标中的属性“节点信息描述”使用and符号连接起来，最终得出了目标满足性论证模型。

文本表示的语义是：当所有子目标都成立时，总目标成立；如果有任一子目标不成立，则总目标不成立。

本文以图26为例，通过本文的遍历算法，首先找到最底层子目标G2.1。G2.1的文本表示为“Verification of additional code, that cannot be traced to Source Code, is achieved.”下划线部分为最底层子目标的文本描述。

用同样的方法遍历最底层子目标G2.2，G2.3，得到的文本表示分别为：The statement coverage of executable object code is achieved；The problem report includes no problem.

最终得到的文本表达方式是：Verification of additional code, that cannot be traced to Source Code, is achieved **AND** The statement coverage of executable object code is achieved **AND** The problem report includes no problem.

## 4.4 小结

本章研究的主要成果是：提出了实例化目标满足性论证模式为目标满足性论证模型的方法，并通过案例来说明具体实例化的过程。这种表达方式分离了安全标准和项目相关论证模型，提高了安全标准论证模型的可重用性。此外，提出了从目标满足性论证模型向文本表示方法的转换方法，通过转换的文本，可以明白最终论证的逻辑结构，为进行基于证据的论证做好准备工作。

# 第五章 目标满足性论证建模工具的设计与实现

本章首先对建模工具进行需求分析，其次分别介绍目标满足性论证模型编辑工具和目标满足性论证模式编辑工具的设计与实现，包括体系结构，元模型和主要功能点。然后介绍从目标满足性论证模式转换为目标满足性论证模型的工具设计和实现，以及从目标满足性论证模型转换为文本表示形式的实现方案；最后介绍模型验证模块的设计实现。

## 5.1 工具需求分析与整体设计

本章设计并实现目标满足性论证模型编辑工具（GSNEdit）以及目标满足性模式编辑工具（GSNModelEdit）。以支持对目标满足性论证模式以及目标满足性论证模型的编辑与修改。此外，支持对建立的论证模式以及模型的自动化检验，以及从目标满足性论证模式向目标满足性论证模型的自动转换。

工具的构件图如图27所示：

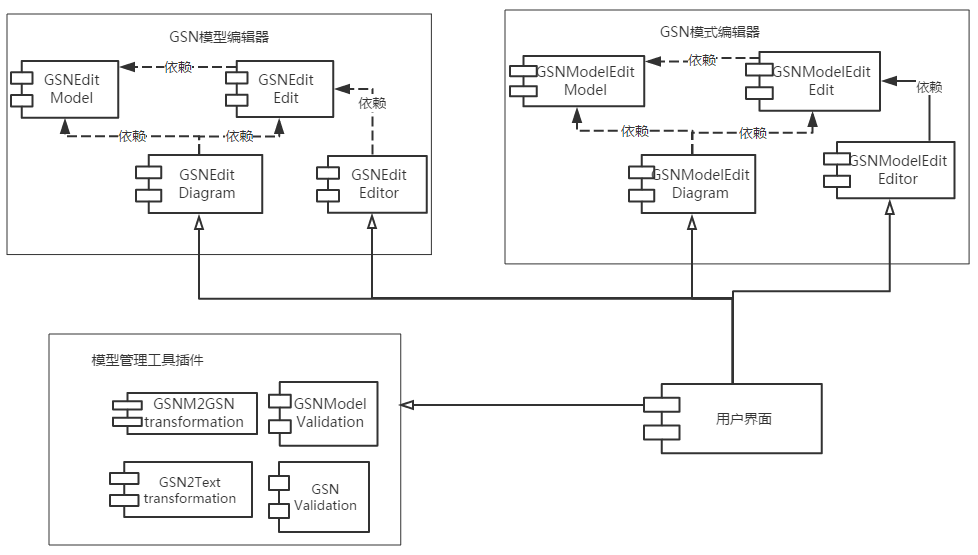


图 27 工具构件图

如图27所示，工具由三部分插件构成，包括GSN模型编辑器（GSNModelEdit）插件，GSN模式编辑器（GSNEdit）插件，以及模型管理工具插件。其中GSNEdit插件实现了基于GSN的目标满足性论证模型的编辑，GSNEdit Model包括了GSNEdit工具的元模型，是构建整个编辑工具的基础。GSNEdit Edit构件包含了能够进入模型的类，GSNEdit Editor构件负责产生模型编辑器的用户视图，GSNEdit diagram构件负责管理模型中信息和图形的映射。

GSNModelEdit工具插件的构建和GSNEdit类似，此处不再赘述。

第三部分，模型管理插件实现的功能是：实现从GSNModelEdit编辑的目标满足性论证模式向可以使用GSNEdit编辑的目标满足性论证模型的转换；以及对使用GSNModelEdit和GSNEdit工具编辑的模型的检验。

## 5.2 GSNEdit编辑器

### 5.2.1 GSNEdit工具体系结构设计

本文建立的GSNEdit工具最终展示层为GSNEdit Editor。最终建立的编辑器使用了MVC框架。其中GSNEdit编辑器包括两个用户视图，模型视图以及图形视图。其中模型视图是构建的是目标满足性论证模型的模型数据，图形视图构建的是图形表示的目标满足性论证模型。使用MVC框架具体表现为：

1. MVC中Model部分对应GSNEdit编辑器的模型视图。

2. MVC中View部分对应GSNEdit编辑器的图形视图。

3. MVC中Controller部分对应GSNEdit编辑器中GSNEdit Diagram构件。

GSNEdit工具的构件图如图28所示：

如图28所示，用户通过模型视图或图形视图建立GSN表示的目标满足性论证模型，当图形发生变更时，可以通过GSNEdit Diagram进行管理。如果用户修改图形，对应的模型数据也会修改，反之亦然。

### 5.2.2 GSNEdit工具元模型设计

GSNEdit工具的元模型是建立GSNEdit工具最基础的部分，本文建立的GSNEdit元模型如图29，30所示：

GSNEdit编辑器可以编辑目标满足性论证模型。主要包括两类图形，目标论证表示符号和连接线。其中目标论证表示符号包括两种：主论证结构表示符号（AbstractShape1），包括目标（Goal），策略（Strategy），解决方案（Solution）；辅助论证表示符号（AbstractShape2），包括上下文（Context），假设（Assumption），论证（Justifycation）。连接线也分为两种：主论证连接线（AbstractConnection1），包括“被解决为”（isSlovedBy）；辅助论证连接线（AbstractConnection2），包括“作为上下文”（InContextOf）。并且主论证连接结构的源节点，目标节点都为主论证表示符号；辅助论证连接结构的源节点是主论证表示符号，目标节点是辅助论证表示符号。图29是工具的元模型图。

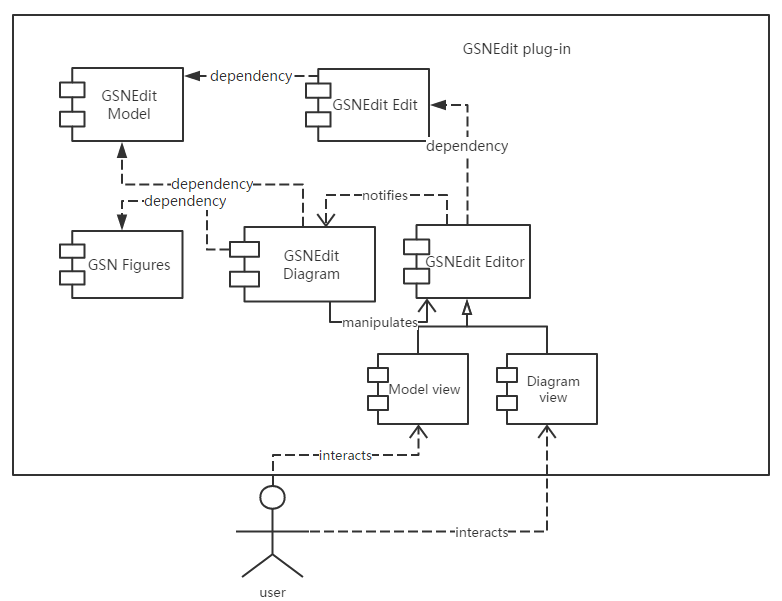


图 28 GSNEdit工具构件图

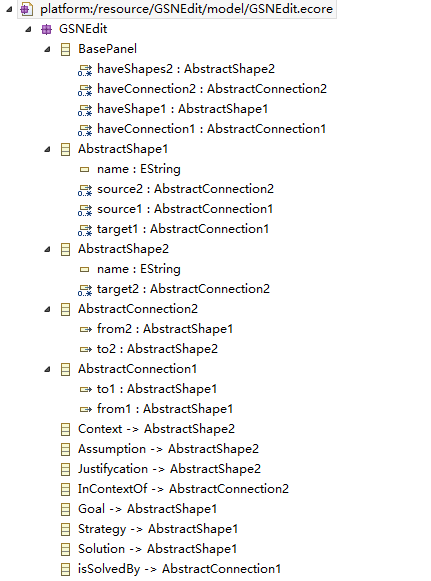


图 29 GSNEdit工具元模型

图30为元模型对应的类图表示。

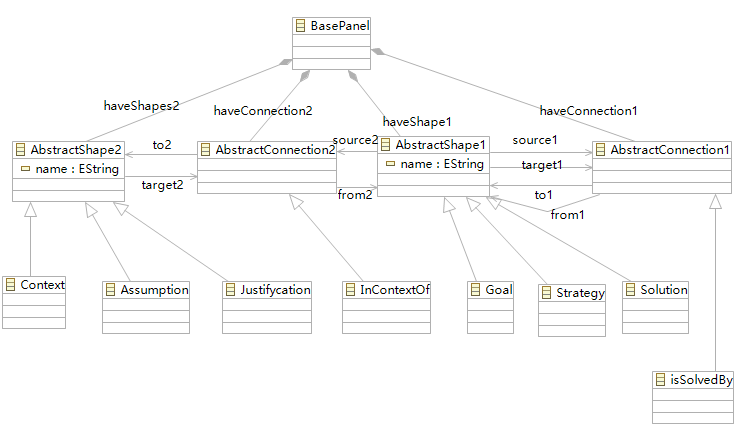


图 30 GSNEdit工具元模型（类图）

### 5.2.3 GSNEdit工具实现

本文使用GMF，EMF以及GEF框架，构建GSNEdit工具元模型。定义了GSNEdit画布中每种图形的符号，定义工具栏中每种图形的小图标。此外定义了从元模型，到画布中图形的符号，以及工具栏中的小图标之间的映射关系。最终设计并实现GSNEdit工具。最终建立的GSNEdit编辑器能够编辑目标满足性论证模型，并以模型和视图两种格式存储。其中模型文件可以使用xml解析器解析。工具支持目标满足性论证模型的修改和删除，同时用户可以自己改变显示图形的大小，移动图形位置，修改连接线位置。图31所示为GSNEdit工具界面：

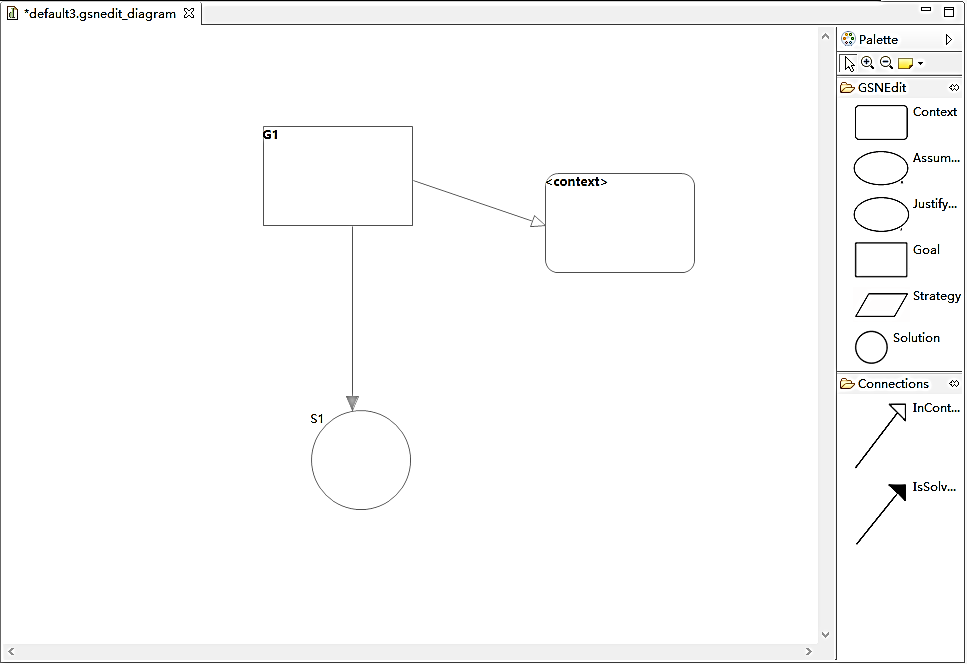


图 31 GSNEdit工具界面

## 5.3 GSNModelEdit编辑器

### 5.3.1 GSNModelEdit工具体系结构设计

本文建立的GSNModelEdit工具最终展示层为GSNModelEdit Editor。最终建立的编辑器使用了MVC框架，其中GSNModelEdit编辑器包括两个用户视图，模型视图以及图形视图。其中模型视图是构建的是模型表示的目标满足性论证模式，图形视图构建的是图形表示的目标满足性论证模式。使用MVC框架具体表现为：

1. MVC中Model部分对应GSNModelEdit Editor的模型视图。

2. MVC中View部分对应GSNModelEdit Editor的图形视图。

3. MVC中Controller部分对应GSNModelEdit编辑器中GSNModelEdit Diagram构件。

GSNModelEdit工具的构件图如图32所示：

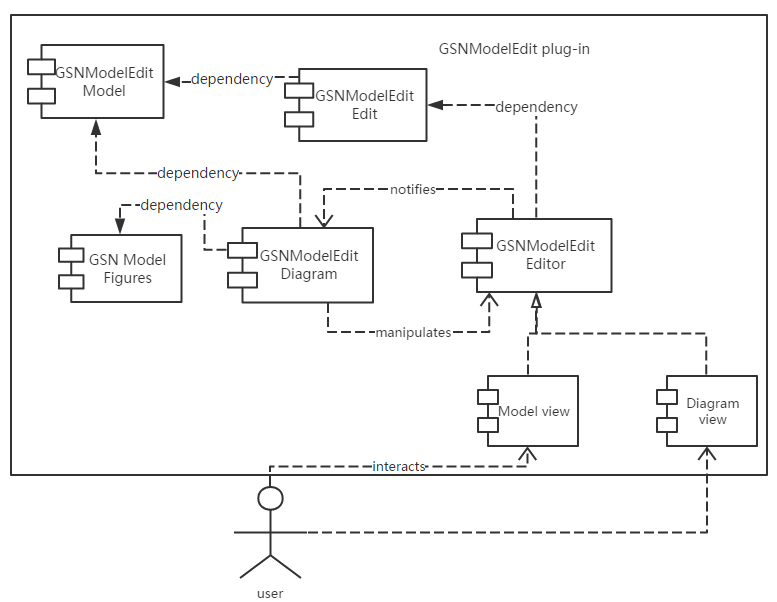


图 32 GSNModelEdit工具构件图

如图32所示，用户通过模型视图或图形视图建立GSN表示的目标满足性论证模式。当图形发生变更时，可以通过GSNModelEdit Diagram进行管理，如果用户修改图形，对应的模型数据也会修改，反之亦然。

### 5.3.2 GSNModelEdit工具元模型设计

GSNModelEdit工具的元模型是建立GSNModelEdit工具最基础的部分，本文建立的GSNModelEdit元模型如图33，34所示：

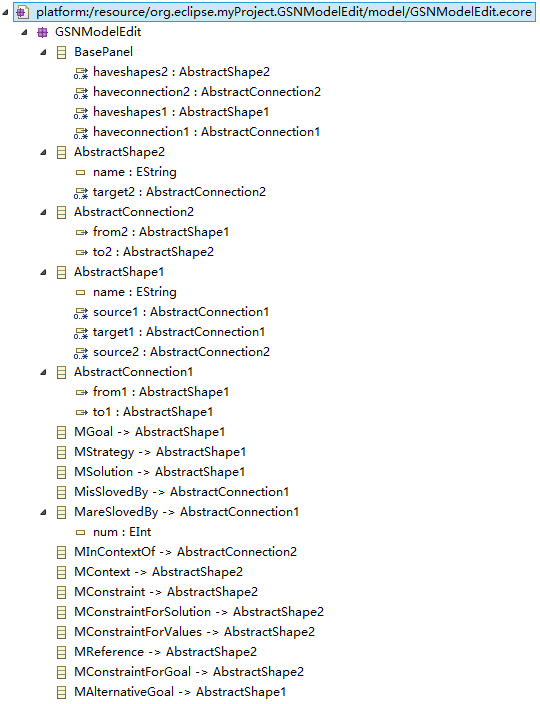


图 33 GSNModelEdit工具元模型

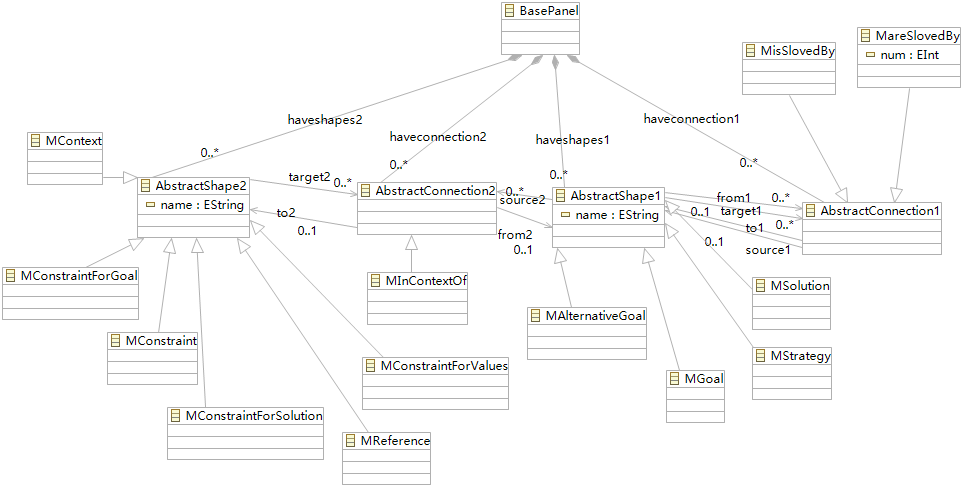


图 34 GSNModelEdit工具元模型（类图）

GSNModelEdit编辑器可以编辑目标满足性论证模式。主要包括两类图形，目标论证模式表示符号和连接线。其中目标论证表示符号包括两种：主论证结构表示符号（AbstractShape1），包括目标（MGoal），策略（MStrategy），解决方案（MSolution），可选目标（MAlternativeGoal）；辅助论证表示符号（AbstractShape2），包括上下文（MContext），其它约束条件（MConstraint），解决方案约束条件（MConstraintForSolution），变量约束条件（MConstraintForValues），目标约束条件（MConstraintForGoal），关联标准章节（MReference）。连接线也分为两种：主论证连接结构（AbstractConnection1），包括“被解决为”（MisSlovedBy），“被几种同类目标共同解决为”（MareSlovedBy）；辅助论证连接结构（AbstractConnection2），包括“作为上下文”（MInContextOf）。并且主论证连接结构的源节点，目标节点都为主论证表示符号；辅助论证连接结构的源节点是主论证表示符号，目标节点是辅助论证表示符号。

### 5.3.3 GSNModelEdit工具实现

本文使用GMF，EMF以及GEF框架，构建GSNModelEdit工具元模型。定义了GSNModelEdit画布中每种图形的符号，定义工具栏中每种图形的小图标。此外定义了从元模型，到画布中图形的符号，以及工具栏中的小图标之间的映射关系。最终设计并实现GSNModelEdit工具。最终建立的GSNModelEdit编辑器能够编辑目标满足性论证模式，并以模型和视图两种格式存储。其中模型文件可以使用xml解析器解析。工具支持目标满足性论证模式的修改和删除，同时用户可以自己改变显示图形的大小，移动图形位置，修改连接线位置。图35所示为GSNModelEdit工具界面：

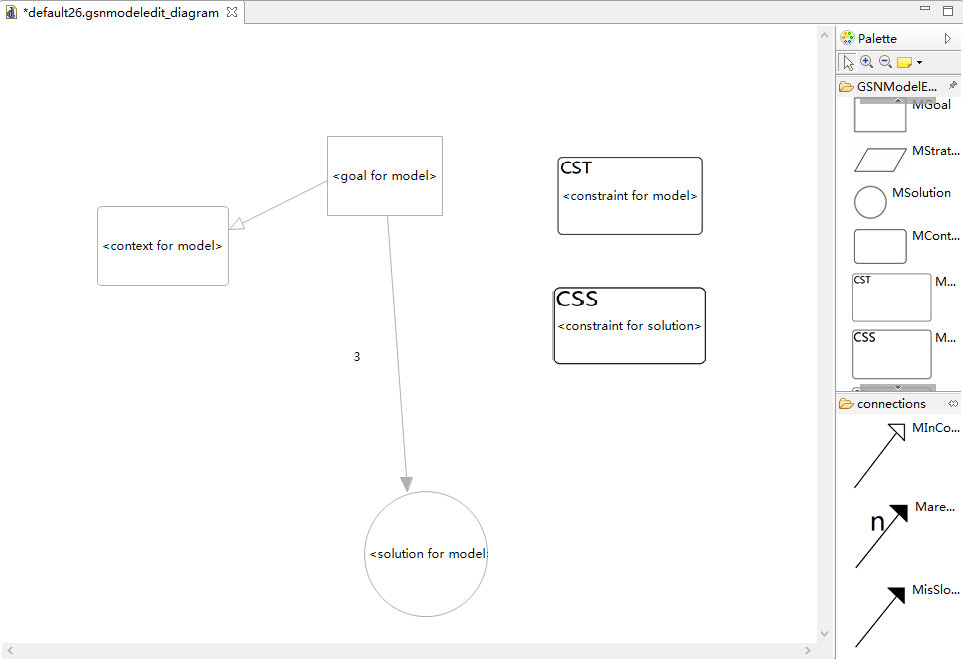


图 35 GSNModelEdit工具界面

## 5.4 模型管理实现

本文中模型管理模块主要实现的功能有两个：实现从实例化后的目标满足性论证模式向目标满足性论证模型的自动转换，目标满足性论证模型的文本化转换；对建立的目标满足性论证模式和目标满足性论证模型进行检验。下面分别对这两个模块进行解释：

### 5.4.1 模型转换模块设计与实现

本文设计从实例化后的目标满足性论证模式向目标满足性论证模型转换的规则并实现转换。用户可以在GSNModelEidt编辑器上编写目标满足性论证模式，同时依据项目实际情况实例化模式中的变量，删除不需要的可选目标，再通过本模块就可以将该模式转换为目标满足性论证模型。本文实现的转换是基于元模型的转换，具体转换的元模型对应关系如表18所示：

表 18 元模型间转换对应关系

|  |  |
| --- | --- |
| Initialized GSNModelEdit Metamodel | GSNEdit MetaModel |
| MGoal | Goal |
| Mstrategy | Strategy |
| Msolution | Solution |
| Mcontext | Context |
| MconstraintForGoal | Assumption |
| MinContextOf | InContextOf |
| MisSlovedBy | IsSlovedBy |
| AlternativeGoal | Goal |
| Reference | Context |
| ConstraintForSolution | Context |

本文通过使用Epsilon Transformation Language（ETL）语言实现元模型到元模型的转换。表19所示为实现将GSNModelEdit 中的Mgoal元素转换为GSNEdit中的Goal元素的使用ETL语言编写的转换规则：

表 19 ETL语言编写的Egoal2Goal转换规则

|  |
| --- |
| pre  {  //创建全局变量作为整个画布的根元素 |

表 19 ETL语言编写的Egoal2Goal转换规则（续）

|  |
| --- |
| var c:= **new** GSNEdit!BasePanel;  }  //转换GSN模式中的目标元素为GSN模型中的目标元素  rule MGoal2Goal  transform s:GSNModelEdit!MGoal  to t : GSNEdit!Goal  {  t.name:=s.name;  c.haveShape1.add(t);  } |

表19提出了ETL描述的转换规则Mgoal2Goal，首先定义模型转换名称，接下来定义目标转换规则的源元模型，目标元模型。定义了具体的属性转换。接下来定义关联转换，源元模型的关联关系对应目标元模型的关联关系。转换完成。

本文使用ETL语言实现了表18中描述的元模型间的转换。

此外，依据本文第4章的4.3节列出的目标满足性论证模型向文本的转换算法，使用ETL语言以及XML解析器将GSNEdit编辑器中编辑的目标满足性论证模型转换为文本的表现形式。转换方法与上述类似，此处不再赘述。

### 5.4.2 模型验证模块设计与实现

本文设计对使用的GSNEdit工具与GSNModelEdit工具建立的模型实现验证的模块。主要实现了两种验证：1.每个论证表示符号的name属性不能为空。2.每个目标都不能与自身存在关联关系。下面分别描述这两种验证的实现方法：

#### 5.4.2.1 论证表示符号的name属性不为空

为了实现这种约束，本文使用Epsilon Validation Language（EVL）描述验证规则。当用户建立一个新的论证表示符号时，name属性都有一个默认的值，用户可以自己修改，但是修改的值不能为空。表20描述了使用EVL描述的方法：

表 20 EVL语言编写的HasName约束

|  |
| --- |
| context AbstractShape1 //定义约束应用与主论证符号中  { |

表 20 EVL语言编写的HasName约束（续）

|  |
| --- |
| constraint HasName  {  check : self.name.isDefined()  message : 'Unnamed ' + self.eClass().name + ' not allowed'  fix  {  title:'Give an identifier to '+self.eClass.name  do  {  var target := UserInput.prompt('Type an name: ');  var target := UserInput.prompt('Type an name: ');  if(target.isDefined)  {  self.name:=target;  }  }  }  }  } |

如表20所示，定义的约束名为HasName，定义了检查方法，以及如果为空时，系统的修复方法。即显示提示信息要求输入name信息，并将输入的信息定义为name属性。

#### 5.4.2.2 论证表示符号不能与自身关联

由于目标满足性论证模式以及目标满足性论证模型本身的含义，要求每个模式或者模型中的论证表示符号都和自身没有关联关系。因此，本文定义约束关系，使得每个论证表示符号都不能建立与自身的关联。

具体的设计方法是：将建立的编辑器中的映射模型中，为关联关系添加约束条件self <> oppositeEnd，使得其不能与自身关联。

## 5.5 小结

本章描述了目标满足性论证建模工具的设计与实现。主要包含三部分，分别是GSNEdit编辑器的设计实现，GSNModelEdit编辑器的设计与实现，模型管理模块的设计与实现。其中模型管理主要包括了两部分，分别是实现从实例化的目标满足性论证模式向目标满足性论证模型的转换，目标满足性论证模型的文本化转换，以及对目标满足性论证模型以及目标满足性论证模式的验证。通过本工具，可以实现目标满足性论证模式的建立，以及从实例化的目标满足性论证模式向目标满足性论证模型的自动转换。

# 第六章 实验分析

## 6.1 实验目的

本章是在第五章开发的集成工具-目标满足性论证建模工具的支持下，建立第三章提出的目标满足性论证模式，并依据第四章提出的目标满足性论证模式的实例化方法对某航空系统软件建立基于目标满足性论证模式实例化方法的目标满足性论证模型，验证其是否能够建立满足DO-178C标准。本章实验包括如下两方面目标：

（1）验证工具有效性：验证是否能够建立目标满足性论证模式并进行实例化，并验证是否能够正确转化为目标满足性论证模型，验证模型验证模块是否能够正确运行。

（2）验证方法可行性：通过该航空系统的案例研究，验证本文提出的目标满足性论证模式在工程实践中的可行性。

## 6.2 实验方案设计

本章主要进行两组实验，第一组实验验证GSNModelEdit编辑器以及GSNEdit编辑器是否能够正确编辑目标满足性论证模式以及目标满足性论证模型，并实现从目标满足性论证模式向目标满足性论证模型的转化。第二组实验验证第五章提出的模型验证模块能够正确实现，即name属性不能为空，以及论证表示符号不能与自身相关联。

第一组实验的流程如图36所示。首先在GSNEdit工具中建立项目原有的目标满足性论证模型。接下来将本文第三章提出的目标满足性论证模式在GSNModelEdit中编辑。然后，结合项目实际情况应用本文第四章中提出的实例化方法，利用GSNModelEdit工具实例化目标满足性论证模型。接下来利用本工具实现从GSNModelEdit工具中建立的模式向GSNEdit工具中表达的模型的自动转化。最后将基于模式的目标满足性论证模型和原有模型进行对比，找出异同。

第二组实验的流程如下：

1. 验证GSNModelEdit和GSNEdit工具建立的模型的name属性为空时，系统是否报错。

2. 验证GSNModelEdit和GSNEdit工具建立的模型视图中图符试图建立与自身的关联，系统是否允许。

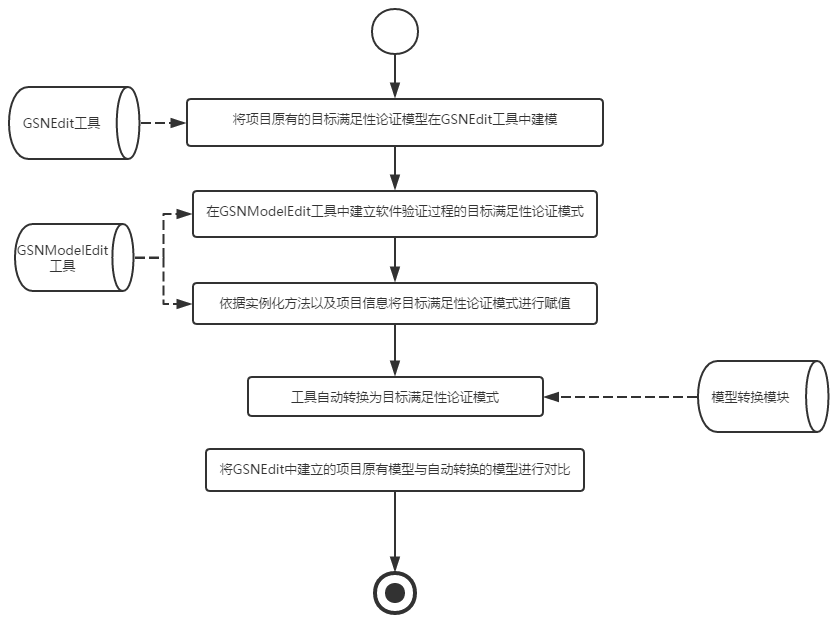


图 36 第一组实验流程图

## 6.3 实验项目背景

该航空系统软件包括近5000个源代码函数，2万份覆盖率分析报告。

本实验收集的数据包括软件测试过程的下列制品信息：

（1）单元测试数据：包括单元测试结果和单元测试覆盖率分析报告。

（2）配置项测试数据：包括配置项测试程序信息和测试日志信息。

单元测试报告反映了单元测试结果，单元测试覆盖率结果。与源代码中的函数相关联。配置项测试文件包括配置项测试用例，包括了正常测试用例和异常测试用例的测试结果，测试点总数，相关联的低层需求。

此外，还包括软件验证结果和问题报告单。软件验证结果包含对软件测试用例设计的评审结果和额外代码的评审结果。问题报告单包括发现问题时所处的过程、问题描述、问题解决方案以及问题目前所处状态。

## 6.4 目标满足性论证模式-目标满足性论证模型间的转换

### 6.4.1 目标满足性论证模型（原型）

本项目未采用模式之前建立的目标满足性论证模型如图37，图38，图39所示：

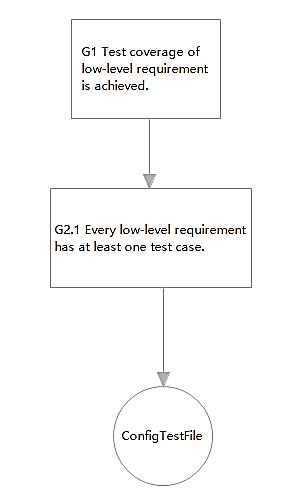


图 37 测试低层需求覆盖率目标满足性论证模型（原型）

图37描述的是对DO-178C中A-7.4目标的实现，计算低层需求覆盖率即每个低层需求都存在至少一个测试用例测试。当低层需求覆盖率达到项目要求时，该目标实现。

图38描述的是对DO-178C中的A-7.7目标的实现。当该软件的语句覆盖率达到项目要求时，该目标实现。

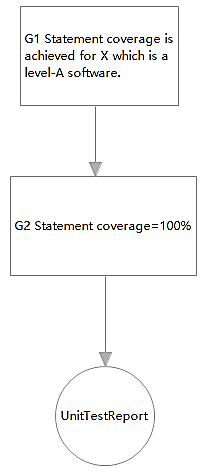


图 38 语句覆盖率目标满足性论证模型（原型）

除上述模型外，本文构建了MC/DC覆盖率和分支覆盖率的目标满足性论证模型。篇幅限制，不再赘述。最终建立的所有目标满足性论证模型（原型）如图39所示：

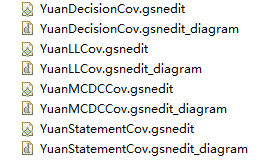


图 39 目标满足性论证模型（原型）

如图39所示，分别包含了论证模型的模型文件和视图文件。

### 6.4.2 建立并实例化目标满足性论证模式

利用GSNModelEdit，基于本文第三章提出的目标满足性论证模式中的测试需求覆盖率目标满足性论证模式和结构测试覆盖率目标满足性论证模式，如图20和图24所示。依据项目的实际情况，最终实例化的目标满足性论证模型如图40，图41和图42所示：

图40中，在实例化模式时，变量X为low-level requirements。并且在本项目中，没有在配置项执行活动中发现异常，因此，将论证结构S3删除。在本项目中，论证结构S2中需要的证据数据在配置项测试文件中。因此，最终论证G2.2和G2.3的证据为配置项测试文件，并修改配置项测试文件的解决方案约束条件，添加追溯数据约束项。除此之外，论证结构的其他元素与本文提出的目标满足性论证模式中的结构一致。

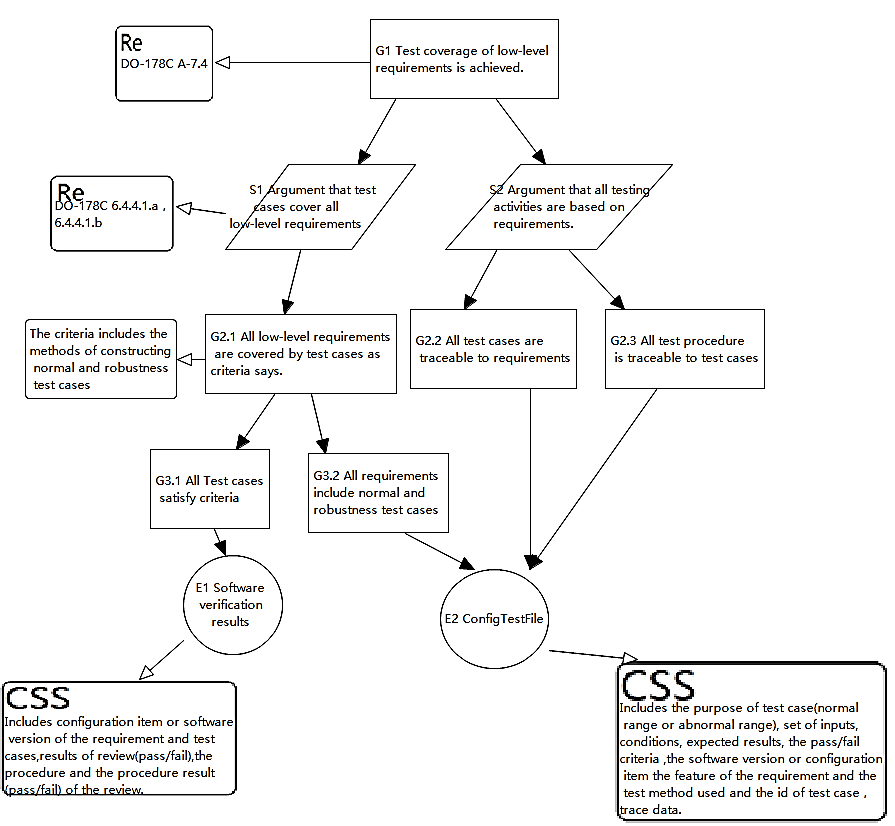


图 40 实例化的测试需求覆盖率目标满足性论证模式

在图41中，实例化变量X为statement coverage，项目中软件代号为X。由于该软件为A级软件，因此必须保留可选目标G2.1及其约束条件。论证G2.1的项目制品数据和规定数据一致。本项目中语句覆盖率的测试对象是可运行目标代码，因此将变量F实例化为Executable Object Code。论证该目标的证据存在于单元测试文件中，因此，添加证据E3，并添加E3的约束条件CSS3。在论证过程中，依据实际情况，由于存在额外代码，因此论证结构S3中保留目标G3.3，删除其余可选目标及其约束条件。G3.3可由问题报告单论证，与模式中定义一致。

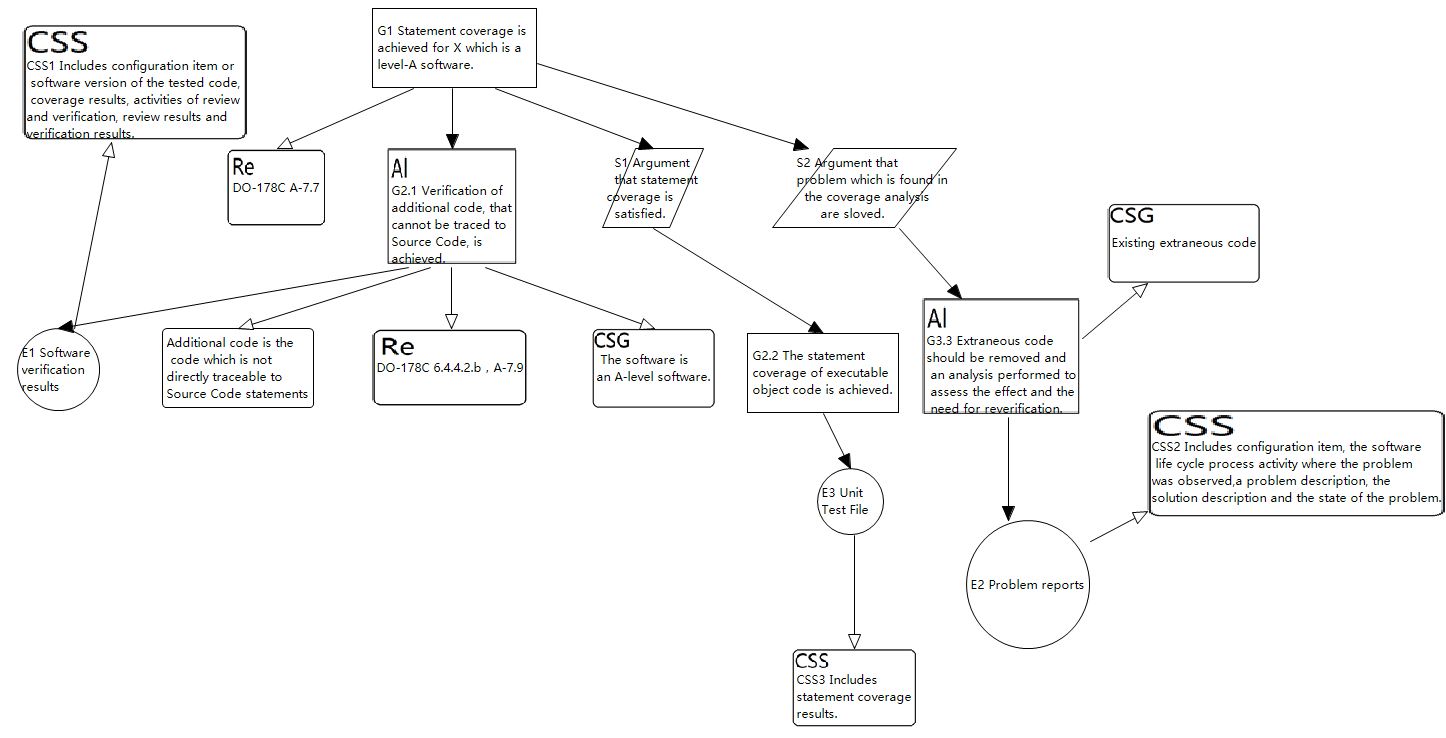


图 41 实例化的语句覆盖率目标满足性论证模式

此外，还建立了实例化分支覆盖率目标满足性论证模式以及MC/DC覆盖率目标满足性论证模式。篇幅限制，不再赘述。最终建立的全部模式如图42所示。包含了实例化的目标满足性论证模式的模型文件和视图文件。

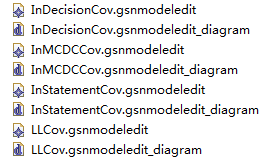


图 42 实例化的目标满足性论证模式

### 6.4.3 转化为目标满足性论证模型

通过第五章建立的模型转换模块，最终转换目标满足性论证模型如图43，44和45所示。

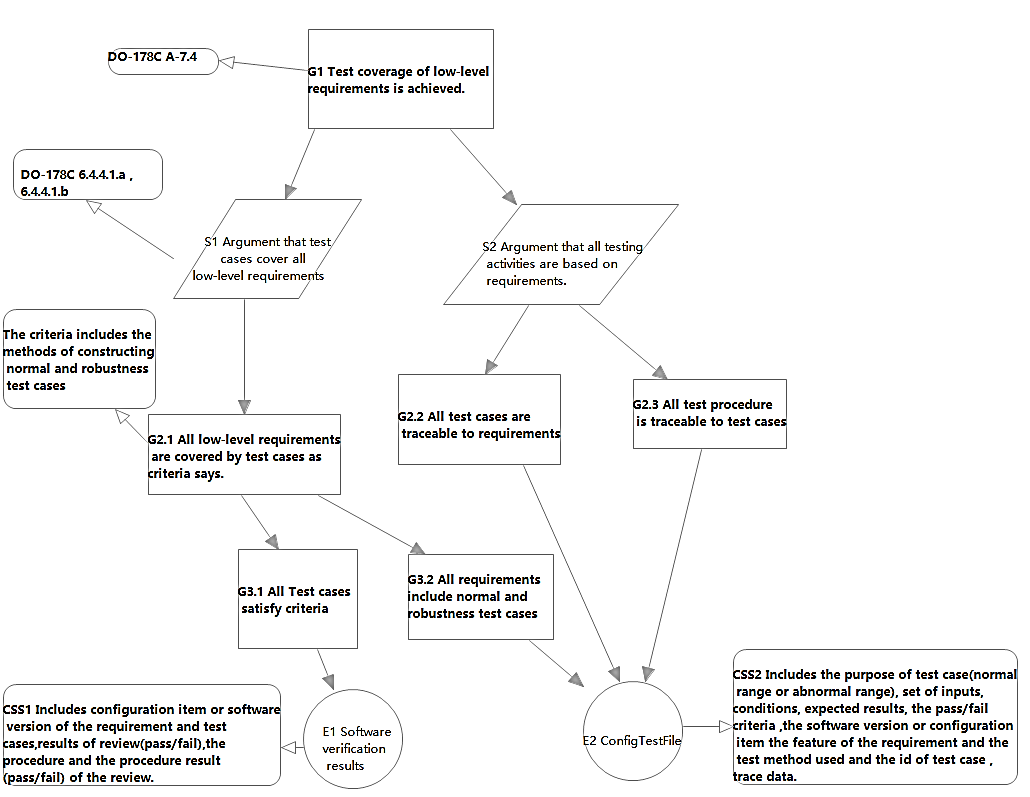


图 43 测试低层需求覆盖率目标满足性论证模型

依据第五章5.4.1节定义的元模型间转换的对应关系，最终建立的测试低层需求覆盖率和语句覆盖率的目标满足性论证模型分别如图43和图44所示。

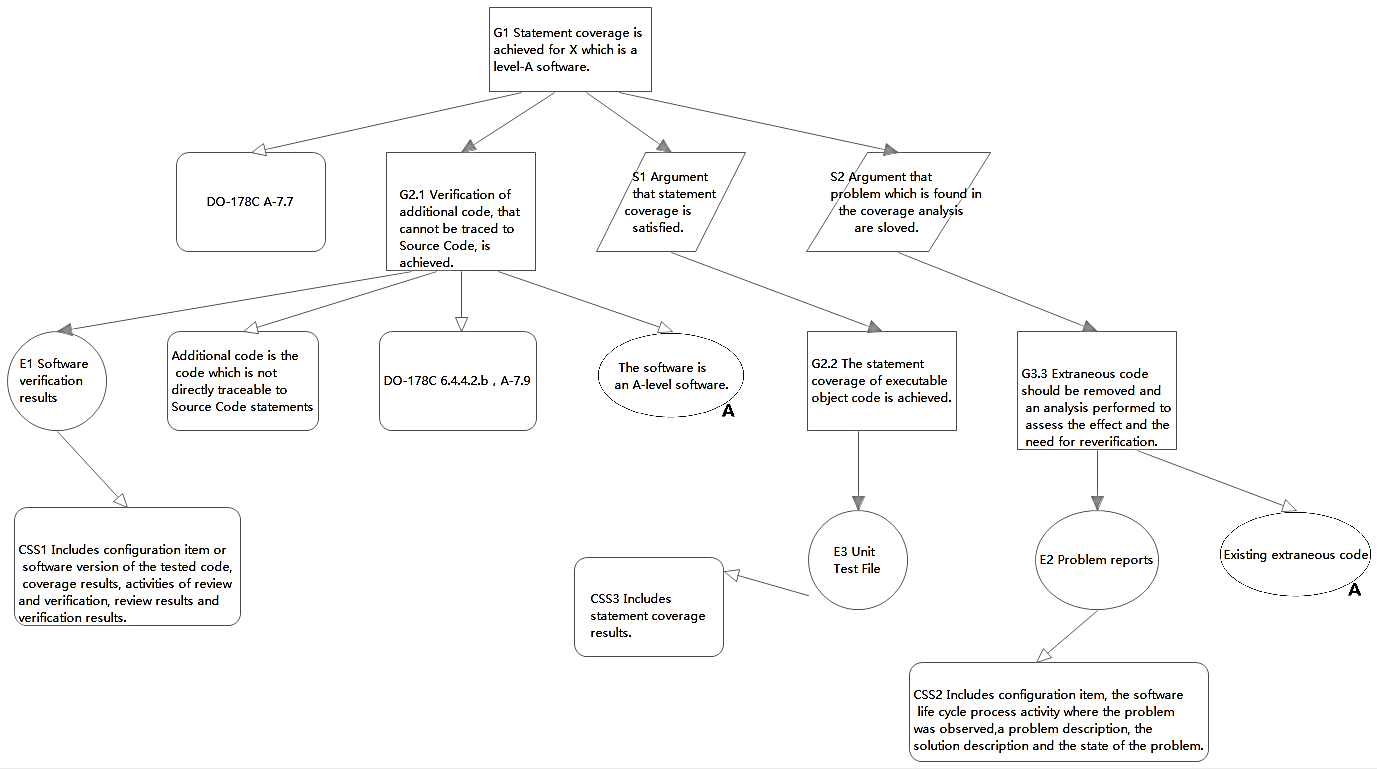


图 44 语句覆盖率目标满足性论证模型

此外，还建立了分支覆盖率目标满足性论证模型以及MC/DC覆盖率目标满足性论证模型。篇幅限制，不再赘述。最终建立的所有目标满足性论证模型如图45所示。包含了目标满足性论证模型的模型文件和视图文件。

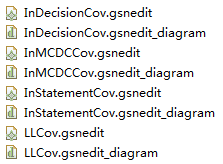


图 45 目标满足性论证模型

### 6.4.4 实验结果对比

本章6.4.1节和6.4.3节中建立的目标满足性论证模型的对比结果如表21，表22和表23所示：

表 21 低层需求覆盖率模型论证结果对比

|  |  |  |
| --- | --- | --- |
| **元素数量** | **目标满足性论证模型（原型）** | **基于模式的目标满足性论证模型** |
| 总目标 | 1 | 1 |
| 论证分支 | 1 | 2 |
| 论证层数 | 2 | 3 |
| 子目标 | 1 | 5 |
| 策略 | 0 | 2 |
| 证据 | 1 | 2 |
| 假设 | 0 | 0 |
| 上下文 | 0 | 5 |

表 22 语句覆盖率模型论证结果对比

|  |  |  |
| --- | --- | --- |
| **元素数量** | **目标满足性论证模型（原型）** | **基于模式的目标满足性论证模型** |
| 总目标 | 1 | 1 |
| 论证分支 | 1 | 2 |
| 论证层数 | 2 | 3 |
| 子目标 | 1 | 3 |

表 22 语句覆盖率模型论证结果对比（续）

|  |  |  |
| --- | --- | --- |
| 策略 | 0 | 2 |
| 证据 | 1 | 3 |
| 假设 | 0 | 2 |
| 上下文 | 0 | 6 |

表 23 所有模型论证结果对比

|  |  |  |
| --- | --- | --- |
| **元素数量** | **目标满足性论证模型（原型）** | **基于模式的目标满足性论证模型** |
| 总目标 | 4 | 4 |
| 论证分支 | 4 | 11 |
| 论证层数 | 8 | 12 |
| 子目标 | 4 | 14 |
| 策略 | 0 | 8 |
| 证据 | 2 | 4 |
| 假设 | 0 | 6 |
| 上下文 | 0 | 22 |

通过表21，表22，表23的对比可以看出，基于模式的目标满足性论证模型的论证结构更加复杂，原型目标满足性论证模型相对简单。基于模式的目标满足性论证模型建立的论证结构每个分支的分解参照标准中的规定，建立的论证模型得到了合作方认可。据此，本文提出的目标满足性论证模式及依据其建立的目标满足性论证模型的方法是可行的。同时，工具能够表达目标满足性论证模型，目标满足性论证模式，在实现转换后实现的模型和预期模型一致，说明了GSNEdit，GSNModelEdit以及模型转换模块工具的有效性。

## 6.5 模型验证

本组实验目标是验证工具的模型验证模块实现的正确性。具体的实验结果如下所述：

### 6.5.1 描述属性不为空

本节主要验证当描述属性为空时，系统的处理情况。当验证模型中的name属性为空时，系统将会提示错误。最终效果如图46所示。

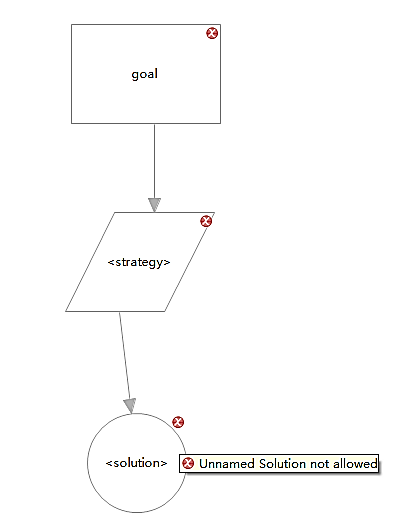


图 46 name属性不能为空

### 6.5.2 论证符号不能与自身建立连接

本节主要验证，论证符号视图与自身建立连接时，系统的处理情况。当用户试图使论证符号与自身建立连接时，系统会禁止执行操作，操作失败。最终效果如图47所示：

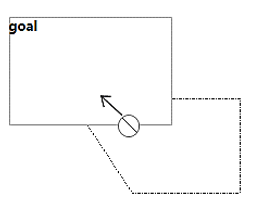


图 47 论证符号不能关联自身

## 6.6 小结

本章主要检验了本文第三章第四章提出的方法的可行性，以及本文建立的工具的有效性。

本章设计的第一组实验，依据第三章内容建立了低层需求覆盖率目标满足性论证模式和结构测试覆盖率目标满足性论证模式。并依据项目背景，以及第四章提出的实例化方法，建立了低层需求覆盖率的目标满足性论证模型，结构覆盖率目标满足性论证模型。并与原来建立的目标满足性论证模型的对比，验证本文提出方法的可行性，以及工具的有效性。

本章设计的第二组实验，验证了本文实现的模型验证模块工具的有效性。

# 总结与展望

## 工作总结

本文以基于DO-178C的适航软件的安全性论证为背景，针对现有适航软件安全论证过程中存在的问题：建立的基于标准的目标满足性论证模型存在相似性，没有在建立论证结构中有效利用；建立目标满足性论证模型时没有抽取出目标满足性论证结构的项目无关的部分，导致目前的目标满足性论证模型复用性不高。

本文以GSN表达方式为基础，为解决上述问题提出了解决方案，具体包括以下几项工作：

1. 对DO-178C标准及其相关标准的主要内容进行介绍。解释了GSN表示符号的含义，使用GSN表达的安全案例模式的符号含义，使用方式。对GMF框架技术进行了介绍。

2. 基于现有的安全案例模式中的符号，为构建目标满足性论证模式对GSN进行了扩展，同时提出了构建基于DO-178C标准的目标满足性论证模式的方法，并对DO-178C软件验证过程中的目标构建了5项目标满足性论证模式。

3. 基于构建的目标满足性论证模式，提出了实例化目标满足性论证模式的方法。并通过案例解释该方法的使用方法。

4. 实现目标满足性论证建模工具，该工具中的模型编辑器采用了GMF框架技术。最终实现的工具能够构建目标满足性论证模型，目标满足性论证模式，同时实现目标满足性论证模式向目标满足性论证模型的转换。

5. 本文通过两组实验，使用真实的实验案例说明目标满足性论证论证模式，以及目标满足性论证模型方法的可行性。同时说明本文实现的工具的有效性。

## 工作展望

尽管在本文提出目标满足性论证模式的过程中进行了大量的分析和研究工作，但是仍然存在着诸多需要进一步深入研究的内容：

1. 本文只提取了DO-178C标准中软件验证过程的目标满足性论证模式，没有对DO-178C标准中其他开发过程的目标进行分析。

2. 本文侧重研究构建目标满足性论证结构，关于证据结构的构建方面的研究工作比较少，未来会在证据构建工作上进一步完善。

# 参考文献

# 攻读硕士学位期间取得的学术成果

[1] 杨阳，苑春春，刘超，吴际，杨海燕，邢亮 .面向DO-178C软件测试过程的目标符合性论证模式 [A] . 第14届全国软件与应用学术年会[C], 2015

[2] 刘超，杨阳，杨海燕，任健. 一种面向DO-178C软件测试过程的目标验证及证据模型提取方法[P] 中国专利, 201510419701.3. 2015-07-16

# 致 谢

整个研究生生涯中，我十分庆幸能够遇到我的老师，刘超老师。刘老师从做人和科研方面都给了我很多的指导。在编写小论文期间，刘老师给了我很多的指导，也给我的研究带来了很多启发。在我的大论文编写过程中，也给了我非常大的帮助，我能够有今天的成果，和刘老师对我的帮助是分不开的。此外，刘老师在做人方面也教会了我很多，他和蔼可亲，宽厚待人的性格也深受实验室同学的喜爱，是一位良师益友。在这里，我要向老师表达深深的谢意。

在这里，还需要感谢我的另一位指导老师，吴际老师。吴老师在我的学术研究中帮助了我非常多，吴老师对我提出的很多问题都有深入独到的见解，为我打开了学术研究的视野，在编写大论文和小论文时，也给了我很多的关心和帮助，我十分感激吴老师。同时，吴老师的多才多艺也令人惊叹，让我十分敬佩。

此外，还要感谢任健老师和苑春春师兄，他们将我带入了我的研究领域的大门，给了我很多珍贵的研究资料，并且每次有问题都会十分耐心的解答，在我缺乏自信时，也会给我鼓励，所以，在这里要表达我对他们深深的谢意。

另外一位帮助我很多的是林欢师兄，林欢师兄对我的研究领域有很深的了解，从开题开始林欢师兄就给了我很多有价值的参考价值的建议，同时也给了我很大的帮助，十分感谢林欢师兄给我的帮助。

还要感谢杨海燕老师，在生活上给了我们很多帮助，并且总是能够给我们很多无私的帮助，让我很感激。感谢实验室同届小伙伴郑培真，张莹，袁斯骏，在研究生期间收获了真诚的友谊，相互鼓励，一同进步。感谢邓志丹师兄，吴雪师姐，孙磊师兄，张曼师姐，王飞师姐让我感受到实验室的温暖，给了我很多帮助。此外，要感谢实验室的孙艺，李苓，邓明丽师妹，赵晶鑫，鲍力师弟在我研究生期间对我工作的支持。希望大家在未来的工作学习中，都能一切顺利。

最后，感谢我的父母。他们对我无私的爱支撑我度过每一天，不论遇到什么事都无条件的支持我，真诚的向你们说，爸妈，辛苦了，谢谢你们。

1. RTCA DO-178C, Software Consideration in Airborne Systems and Equipment Certification [S]. Washington DC: RTCA Inc, 2011 [↑](#endnote-ref-2)
2. RTCA DO-278A, “Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems,” December 2011 [↑](#endnote-ref-3)
3. RTCA DO-248C, “Supporting Information for DO-178C and DO-278A,” December 2011 [↑](#endnote-ref-4)
4. RTCA DO-330, “Software Tool Qualification Considerations,” December 2011 [↑](#endnote-ref-5)
5. RTCA DO-331, “Model-Based Development and Verification Supplement to DO-178C and DO-278A,” December 2011 [↑](#endnote-ref-6)
6. RTCA DO-332, “Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A,” December 2011 [↑](#endnote-ref-7)
7. RTCA DO-333, “Formal Methods Supplement to DO-178C and DO-278A,” December 2011 [↑](#endnote-ref-8)
8. Tim Kelly, Rob Weaver, “The Goal Structuring Notation – A Safety Argument Notation”, Dependable Systems and Networks 2004 on Assurance Cases, 2004 [↑](#endnote-ref-9)
9. Holloway, C. Michael: "Explicate '78: Uncovering the Implicit Assurance Case in DO-178C", 23rd Safety-critical Systems Symposium, 2-5 February 2015, Bristol, UK [↑](#endnote-ref-10)
10. Holloway, C. M: "Towards Understanding the DO-178C / ED-12C Assurance Case", Proceedings of the IET 7th International Conference on System Safety, October 2012, Edinburgh, Scotland [↑](#endnote-ref-11)
11. Holloway, C. Michael: "Making the Implicit Explicit: Towards an Assurance Case for DO-178C", Proceedings of the 31st International System Safety Conference, 12-16 August 2013, Boston, Massachusetts [↑](#endnote-ref-12)
12. 胡宁. 从DO-178 C的新变化透视软件适航关注点[J]. 航空计算技术, 2014, 第4期(4):94-98 [↑](#endnote-ref-13)
13. 张军才, 王娟, 潘卫. 基于DO-178B的结构覆盖分析研究[J]. 航空计算技术, 2011, 41(4) [↑](#endnote-ref-14)
14. Order F A A.8110.49[J]. Software approval guidelines,2003 [↑](#endnote-ref-15)
15. SACM, Structured Assurance Case Metamodel[S]. Massachusetts: OMG, 2013 [↑](#endnote-ref-16)
16. Rajwinder K. Panesar-Walawege. Using Model-Driven Engineering to Support the Certification of Safety-Critical Systems[D]. Norway: University of Oslo, 2012 [↑](#endnote-ref-17)
17. Fuping Zeng; Minyan Lu; Deming Zhong, "Software Safety Certification Framework Based on Safety Case," in Computer Science & Service System (CSSS), 2012 International Conference on , vol., no., pp.566-569, 11-13 Aug. 2012 [↑](#endnote-ref-18)
18. Habli, I.; Kelly, T., "Safety Case Depictions vs. Safety Cases - Would the Real Safety Case Please Stand Up?," in System Safety, 2007 2nd Institution of Engineering and Technology International Conference on , vol., no., pp.245-248, 22-24 Oct. 2007 [↑](#endnote-ref-19)
19. Rajwinder K. Panesar-Walawege. Using Model-Driven Engineering to Support the Certification of Safety-Critical Systems[D]. Norway: University of Oslo, 2012 [↑](#endnote-ref-20)
20. Cleland-Huang J, Gotel O, Hayes J H, et al. Software traceability: Trends and future directions[C]//Proc. of the 36th International Conference on Software Engineering (ICSE), Hyderabad, India. 2014 [↑](#endnote-ref-21)
21. Hawkins R, Kelly T. A structured approach to selecting and justifying software safety evidence[C]//System Safety 2010, 5th IET International Conference on. IET, 2010: 1-6 [↑](#endnote-ref-22)
22. Nair, S.; de la Vara, J.L.; Sabetzadeh, M.; Briand, L., "Classification, Structuring, and Assessment of Evidence for Safety -- A Systematic Literature Review," Software Testing, Verification and Validation (ICST), 2013 IEEE Sixth International Conference on , vol., no., pp.94,103, 18-22 March 2013 [↑](#endnote-ref-23)
23. GSN元模型 http://www.goalstructuringnotation.info/gsn-metamodel [↑](#endnote-ref-24)
24. GSN, Goal Structuring Notation Standard[S]. York: GSN Working Group, 2011 [↑](#endnote-ref-25)
25. Takai, T.; Kido, H., "A Supplemental Notation of GSN Aiming for Dealing with Changes of Assurance Cases," Software Reliability Engineering Workshops (ISSREW), 2014 IEEE International Symposium on , vol., no [↑](#endnote-ref-26)
26. Kelly T, Mcdermid J. Safety Case Patterns -- Reusing Successful Arguments[C]// Understanding Patterns and Their Application to Systems Engineering (Digest No. 1998/308), IEE Colloquium on. IET, 1998:3/1 - 3/9 [↑](#endnote-ref-27)
27. Robert Alexander, Tim Kelly, Zeshan Kurd, and John McDermid. Safety cases for advanced control software: Safety case patterns. Technical report, Department of Computer Science, University of York, 2007 [↑](#endnote-ref-28)
28. Matsuno, Y.; Taguchi, K., "Parameterised Argument Structure for GSN Patterns," Quality Software (QSIC), 2011 11th International Conference on , vol., no., pp.96,101, 13-14 July 2011 [↑](#endnote-ref-29)
29. Kolovos D., Paige R., Polack F.,. The Epsilon Transformation Language, in Proc. 1st In-ternational Conference on Model Transformation, ICMT'08, Zurich, Switzerland, July 2008 [↑](#endnote-ref-30)
30. Kolovos D., Paige R., Polack F., Detecting and Repairing Inconsistencies Accross Hetero-geneous Models, in Proc. 1st IEEE International Conference on Software Testing, Verifi-cation and Validation, ICST 08, Lillehammer, Norway, April 2008 [↑](#endnote-ref-31)
31. 马媛. 机载设备软件取证指南DO-178C新特性研究[J]. 信息系统工程, 2013, 07期(7):144-145 [↑](#endnote-ref-32)
32. 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 [↑](#endnote-ref-33)
33. 蔡喁，郑征．机载软件适航标准DO-178B/C研究[M]．上海：上海交通大学出版社，2013 [↑](#endnote-ref-34)
34. S. Niar, J. de la Vara, A. Melzi, G. Taglaferri, and F. Belmonte. Safety Evidence Traceability: Problem Analysis and Model[A]. Requirement Engineering: Foundation for Software Quality[C]. 2014: 309-324 [↑](#endnote-ref-35)
35. R. Weaver, G. Despotou, T. Kelly, and J. McDermid. Combining Software Evidence: Arguments and Assurance[A]. England: SIGSOFT Software, 2004: 152-160 [↑](#endnote-ref-36)
36. EMF Project http://www.eclipse.org/modeling/emf/ [↑](#endnote-ref-37)
37. GEF Project http://www.eclipse.org/gef/ [↑](#endnote-ref-38)
38. GMF Project http://www.eclipse.org/modeling/gmp/ [↑](#endnote-ref-39)
39. IBM Redbook: Eclipse Development Using the Graphical Editing Framework and the Eclipse Modeling Framework, www.redbooks.ibm.com/abstracts/sg246302.html [↑](#endnote-ref-40)
40. Richard C. Gronback. ECLIPSE MODELING PROJECT-A Domain-Specific Language Toolkit[M]. USA: Pearson Education, Inc,2008 [↑](#endnote-ref-41)