第一章

## 第二章 相关理论和关键技术

### Do178C标准相关理论（）

Do178c 的

这部分相对简单，因为抄了改就行 具体内容包括：

本节首先介绍适航领域软件相关的标准，以及标准中规定的与普通软件开发不同的软件生命周期和相应的软件生命周期数据，然后介绍标准中与软件需求跟踪相关的内容。

### DO-178B/C标准介绍

20世纪70年代末，计算机软件应用在飞机设备和系统中使用越来越多，因此为了保证这些应用能够满足适航局的审定要求，美国航空无线电技术委员会制定了相应软件规则，用来支持以软件为基础的设备和系统的合格审定[1]。自此之后，DO-178系列《机载系统和设备合格审定中的软件考虑》产生，并不断补充扩展，经历了DO-178、DO-178A、DO-178B，现在已经发展到DO-178C。其中DO-178B标准是相对稳定的，其制定汲取了多方面共同意见，包括飞行制造商、设备供应商、工具开发商和适航认证机构等，在使用的19年过程中没有发现严重的问题。由于在实际开发软件的过程中，方法会因项目的不同而不同，因此DO-178B标准是面向过程和目标的，即尽可能的不涉及到实际的技术，但是，DO-178B在一些方面，“面向目标”的原则贯彻的不够彻底，因此对DO-178B做了一些修正，于是出现了DO-178C。

DO-178B/C规定的软件生命周期过程包括：软件计划、软件开发以及软件综合过程，三个过程结构图如图4所示。其中软件计划过程规定了五个计划和三个标准。五个计划包括软件审定、开发、验证、构型管理以及质量保证等计划，三个标准包括软件需求、设计以及编码等标准。与开发和设计人员关系最密切的软件开发过程由软件需求、设计、编码和集成等四个过程组成。软件综合过程包括软件验证、构型管理、质量保证以及审定联络等四个子过程，并且综合过程在软件全生命周期中起作用。

在整个软件生命周期中，软件开发过程是主线，软件综合过程与软件开发过程同时执行，并且软件综合过程执行在软件开发过程的各个子过程上，具体的关系如图5所示。虽然标准中对软件生命周期过程规定较多，但是标准并没有强制所有软件活动必须按照规定活动严格执行，只需要在软件生命周期中描述清楚所有过程和活动的先后顺序和执行关系，并定义过程之间的迁移准则即可[2]。



图4 DO-178B/C生命周期过程结构图



图5 DO-178B/C软件生命周期方阵图

在整个软件生命周期过程中，产生了大量的软件生命周期数据，这些软件生命周期数据供审定局方来验证软件的研制开发已经满足了标准中的相应目标。DO-178B/C中列举了20种软件生命周期数据，其中包括软件计划过程中的五个计划数据和三个标准数据，软件开发过程中的软件需求数据、设计描述数据、源代码数据、可执行目标代码数据和软件验证用例和规程，以及软件综合过程中的软件验证结果、环境构型索引、软件构型索引、软件构型管理记录、问题报告、质量保证记录以及软件完结总数。其中本文将使用到的数据包括软件需求数据和源代码数据。

DO-178B/C根据软件失效条件将软件分为不同的等级，不同等级的软件需要满足不同数量的目标。标准对于每个过程都制定了相应的需要完成的目标，目标是审定方审定软件是否满足适航要求的最终依据。

DO-178B/C三个基本要素为上述介绍的过程、软件生命周期数据和目标，三者的关系如图6所示。



图6 DO-178B/C中基本要素的相互关系

## GSN图像论证方式

## 适航领域 变更管理和配置管理相关技术研究 适航审定技术

配置管理的流程相关的研究：

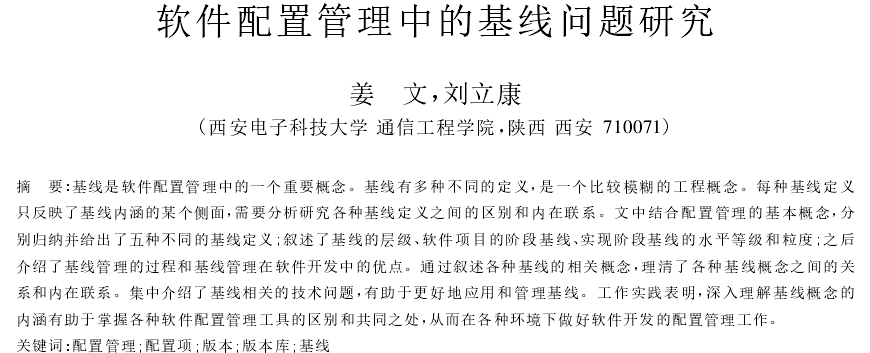
1.软件配置管理系统的优化研究与设计 张薇 进行了管理优化流程的分析，适用于普通项目

2.软件配置管理在软件开发平台中的应用\_裴树军 分析研究了配置管理过程 中遇到的问题，基于CMMI 实施配置管理的有效方法。

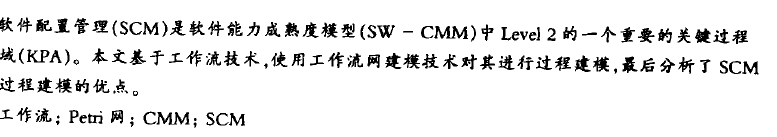
3.软件配置管理理论与实践\_赵文杰 基于两级配置管理的模型的具体实施方案 面向开发 组织及配置管理和项目级配置管理

4.基于DO-178B的软件配置管理技术研究 对基于Do178B的配置管理中各个流程在实践中需满足的基本情况 等进行了介绍

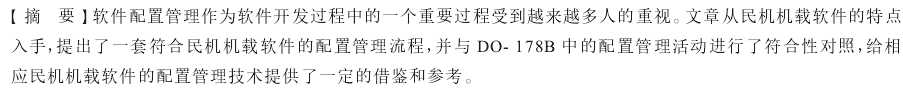
5



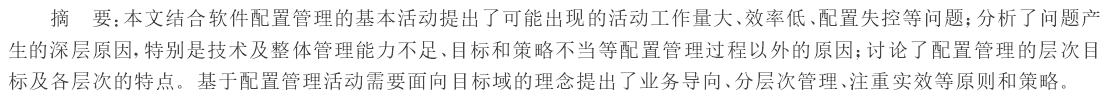
6.基于工作流技术的软件配置管理过程建模\_王槐彬



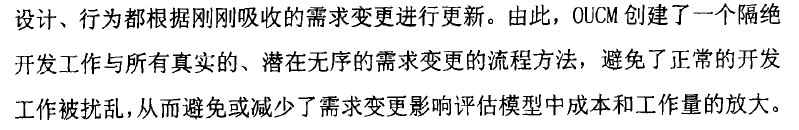
7.民机机载软件配置管理技术研究\_杨娟



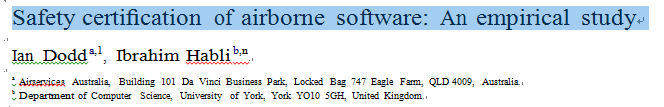
8.软件配置管理的问题\_目的\_层次和策略\_严晓光



9.软件需求变更管理的研究与实践\_赵海英



Safety certiﬁcation of airborne software: An empirical study



通过GQM方法软件 metric 控制 问题报告数量，提前解决问题。 数据交给 审定部门保存 ，审定部门参与多

适航审定的主要方法包括

## 需求追踪技术（内容从他们那里找）

文本相似度技术

Wordvec

选择排序

1. **对软件配置管理流程建模技术**

安全UML建模

6.基于工作流建模，建模优点

模型驱动的建模（Do178c标准）

**B.软件配置管理在Do178C的理论研究 以及应用 国内**

4. 178实践

7.民用符合178c的流程

8.do178c层次、策略等

**C对配置管理流程的研究**

1.普通项目管理优化流程的分析

9.需求变更管理的流程方法。

**D.其他问题的研究**

5.基线，

2. 基于CMMI 实施配置管理在开发中的问题和方法

3基于两级配置管理的模型的具体实施方案

## **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[[[1]](#endnote-1)][[[2]](#endnote-2)]。除此之外，文献[[[3]](#endnote-3)]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。

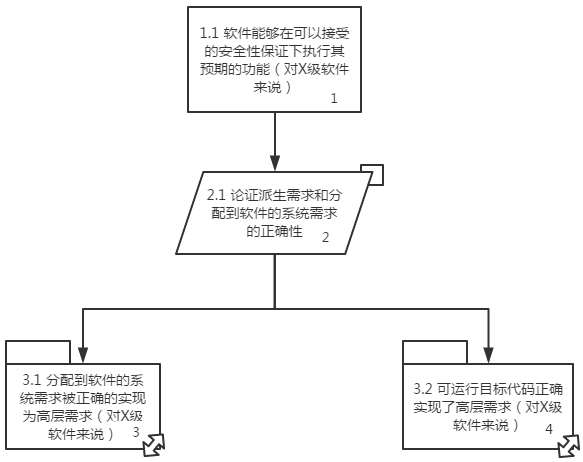


图 1 简化的DO-178C主要论证结构

## 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[][][]，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[]。文献[]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）[]。《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. 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-1)
2. 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-2)
3. 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-3)