绪论素材

课题来源及研究背景 课题研究背景和意义

许多标准要求对每个安全关键系统进行安全评估。安全评估与风险评估[1]有一些相似之处，并且使用类似的方法执行，生成系统开发人员必须遵守的安全需求和约束的列表。执行安全评估是开发安全关键系统的必要和关键元素

除了开发与安全相关的需求外，标准通常还有其他与认证相关的需求。这些要求不一定在软件中实现，而是表示必须提交给认证机构的关于软件的信息。例如，适航标准要求开发人员提交关于系统中使用的COTS软件的信息。此外，它要求开发人员指定系统中使用的与时间相关的函数，如过滤器。因此，能够轻松地收集关于软件的此类信息是非常重要的。

作为证据管理的一部分，从业者还必须评估证据的充分性。充分性通常是根据收集到的信息的可信度来评估的，这些信息用于支持关于系统安全[9]的特定声明。充分性可以定性地(例如，通过置信水平)估计，也可以定量地(例如，通过数字充分性程度)估计。

通常还需要可追溯性链接来捕获用作安全证据的人工制品之间的关系。例如，测试用例与派生测试用例的需求之间存在关系。由于这些关系的存在，一项证据的改变可能会影响到其他证据，可能导致这些证据不再充分。例如，如果系统需求被修改了，那么相关的测试用例可能必须被更新。因此，系统供应商必须在证据体系中跟踪各种关系，以便能够分析变更的影响。这种分析的目的是识别变更的潜在后果，或者是评估为了完成变更[10]需要抱怨什么。

尽管安全标准为管理安全证据提供了一些指导，但它们是通用的，通常是包含数百页和数千个需求的大型文档。例如，IEC 61508——最广泛使用的安全标准之一——被组织成8本小册子(部分)，正文超过450页。对于大多数安全标准，都需要进行一定程度的解释，以使其适应应用环境。这意味着系统供应商必须根据标准的指导来决定哪种类型的证据最适合给定的场景，以及应该如何对其进行结构化、评估和管理。因此，标准并不一定反映安全证据管理中的工业实践，而只提供可能被采用的实践的一般信息。这意味着这些标准不允许某人知道是否使用了某些实践，或者确定它们的使用频率。

**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（这不就是我的思路？）**

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。

适当的可跟踪性是大型系统开发中的关键，对于安全关键系统的开发更是如此。例如，适航DO-178B标准[4]要求跨越开发生命周期的可追溯性。事实上，它要求至少软件设计可以追溯到所有D级或更高级别软件的原始高级需求。因此，能够跟踪设计元素到需求是很重要的。

为什么变更管理能够代表了配置管理的关键技术？

由于变更管理中，必然涉及到了基线管理、标识配置、所以建立变更管理的模型。基线的建立是基于变更的，而进行标识配置是为了基线管理和变更管理服务。

包含了配置标识活动以及基线管理活动的，以变更管理为中心的配置管理模型。能够反映配置管理过程的关键技术环节

国内外研究现状：

1.Do178c相关研究

### 1.2.1 DO-178C标准相关研究

在安全关键的基于计算机的系统中，包括软件密集的系统中，出现故障可能会导致灾难性的后果。这些系统通常要经过安全认证，也被称为安全保证，以确保系统不会对人、财产或环境造成过度伤害。安全认证是一个严格的过程，通常由一个独立的许可或监管机构进行，以确保一个系统已经满足其声明的安全特性，并且该系统能够以安全的方式交付其预期的服务。在认证过程中需要满足的安全标准通常以安全标准的形式规定

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[[[1]](#endnote-1)][[[2]](#endnote-2)][[[3]](#endnote-3)]，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[[[4]](#endnote-4)]。文献[[[5]](#endnote-5)]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）[[[6]](#endnote-6)]。《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。

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[[[7]](#endnote-7)]。对标准的研究

文献[[[8]](#endnote-8)]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。 结构覆盖分析

美国NASA的研究员C. Michael Holloway从事DO-178C标准的相关研究[[[9]](#endnote-9)][[[10]](#endnote-10)][[[11]](#endnote-11)]，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。（理论上论证）

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）[[[12]](#endnote-12)]。《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。

对于开发安全关键系统，存在许多与安全相关的和认证标准。在实践中进行安全评估，根据标准进行系统认证需要提交关于软件的信息。适航标准RTCA DO-178B是商业和军事航空航天项目事实上的软件标准。

在本研究中，从RTCA DO-中提取了安全相关概念的列表

然后给出一个UML概要文件来支持对它们进行建模。然后，给出了从UML模型中生成与认证相关的信息的方法。通过开发飞机导航控制器子系统的实例说明了这种新方法

在本研究中，我们分析了航空工业中实际与安全相关的适航标准[4]，从中提取出安全工程师和软件工程师都感兴趣的一系列与安全相关的概念

2.变更管理的流程研究

3.审定的证据研究

本论文旨在探讨实务人员如何处理关键电脑系统的安全证明管理。目前关于该活动在业界如何执行的信息非常有限。

结论:(1)V&V在安全保障中发挥着重要作用;(2)行业将明显受益于更多的工具支持来收集和操纵安全证据;(3)未来安全证据管理的研究需要更加重视工业应用

4.审定的方法研究

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。

国外。。。。 国内。。。。 配置管理研制过程 Do178C流程研究

配置管理的软件

许多安全关键飞机功能是软件实现的。机载软件必须经过审计，并在部署之前批准的航天CERTI网络阳离子当局。审计过程非常耗时，其结果是不可预知的，因为关键性和机载软件的复杂性。为了保证机载软件工程是系统监管，是审计，CERTI网络阳离子当局强制要求符合安全标准，详细说明产业最佳实践。

选择建模的方法，实际情况，国外的研发审定工作1.目前证据管理的情况 2.国外成立的专门进行研发审定的研究、统一工作的传统，其中，1论文提到了一种安全UML，该UML的目的是， 作为一项基于标准的工作，某种程度上以后的相关工作人员都应参照此项的情况，

考虑这两点因素，本人此次建模参考安全UML标准，特别是n.n章对各个对象间关系的分类、精简与总结

软件质量评估的方法，主要是针对研发方的，对于审定方的，间“证据”论文，（大多都没有太强的实用性）

同时在数据项的选择上，设定为可粗可细，（不归这里管），选取了实际工作中最关键的相关的要素，结合标准规定的数据项要素， 在软件的实际设计开发过程中，为能够适应不同格式标准情况的生命周期数据，可以选择审定项的细致程度，当然可由该工具审定的结果也根据生命周期数据情况的不同而不同。对于无法标准化或由于复杂程度只能有专家进行分析的部分，展现为易于得到的文本以利于审查人员管理证据

那个网站研究的内容 及文章的摘要。

相关技术

1. 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-1)
2. 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-2)
3. 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-3)
4. 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-4)
5. 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-5)
6. Order F A A.8110.49[J]. Software approval guidelines,2003 [↑](#endnote-ref-6)
7. 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-7)
8. 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-8)
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-9)
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-10)
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-11)
12. Order F A A.8110.49[J]. Software approval guidelines,2003

    以前的工作也承认使用文本模板文档来构造证据[18]，尽管它没有指出它的总体频率。另一项调查[20]报告说，使用基于论证的图形符号，如GSN和CAE，来构建索赔、论证和证据，是最流行的，但我们的结果注意到实践中的差异。基本上，这些图形符号是最流行的用于论证的符号，这意味着基于论证的图形符号在实践中得到了广泛的应用。虽然在构建和管理证据的模型的使用方面有很好的结果已经在[18]中报道过，但是这种方法似乎还没有在工业中被广泛使用。尽管如此，这是有意义的使用，因为使用模型预知结构最近已经提出。工业也可能已经使用了一些证据结构技术几十年，而没有考虑采用其他技术或意识到它们。有关工作的范围(就受访者来自的国家而言)可能也是与我们的调查结果不同的一个可能的解释。

    在整个软件过程中，要求认证机构对开发、验证和支持活动进行审计。审计被称为参与阶段(SOI)审计。每个审核都位于生命周期中的战略点，以减少最终认证审核失败的风险。早期发现潜在的认证失败对于确保软件过程不会朝着错误的方向发展至关重要。审计失败通常要求在重复审计之前必须对人工制品进行重新加工。审计之间的典型时间间隔为4至6个月。因此，在执行SOI审核之前，软件和安全工程师必须了解软件过程是否符合认证要求。在航空航天软件项目中，通常的做法是收集项目生命周期中发现的缺陷的度量标准，并将这些缺陷与一个公分母联系起来(例如，每行代码中发现的缺陷数量)。通过将这些缺陷度量标准与认证机构的需求相关联，可以生成指标来确定软件为下一次SOI审计做好准备

    在这项工作中，我们主要关注两组涉众，即认证作者—ity审核员和开发团队。审核员可以使用项目生命周期历史上的数据趋势来识别软件问题和可能的误导信息。航空航天公司内的开发团队也可以使用这些数据来评估软件项目是否符合认证目标。

    Certiﬁcation refers to the ‘‘process of assuring that a product or process has certain stated properties, which are then recorded in a certiﬁcate’’ [7]. Assurance can be deﬁned as justiﬁed conﬁdence in a property of interest [8].

    DO178B指南根据软件的安全临界性(即软件组件如何对系统危害作出贡献)区分了不同级别的保证。在系统安全评估过程中，软件的安全性是根据与软件组件相关的故障条件在系统级确定的。这些安全状况可分为五类:“灾难性”、“危险/严重-主要”、“主要”、“轻微”和“无影响”[25,26]。然后DO178B指南定义了五个不同的保证级别，它们与上述故障条件的分类相关(级别A到E，其中级别A是最高的，因此需要最严格的流程)。每一层的软件保证都与一组目标相关联，这些目标大多与基本的生命周期过程有关，例如计划、开发和验证活动(图1)。

    57个目标必须得到满足。另一方面，要达到软件“A”级，其中错误的软件行为可能会导致灾难性的失败，必须满足9个额外的目标——其中一些目标是通过独立的[27]实现的。

    为证明符合DO178B，申请人须向核证机关提交下列生命周期数据:

    它们还应该使所有软件生命周期数据，例如与开发、验证和规划相关的数据，都可以由认证机构进行评审。特别地，情景应用程序应该提供

    证据表明，PSAC已经达到了合规要求。情景应用程序应该提供系统(例如体系结构和安全特性)和软件(例如功能和分区策略)的概述。它还应该提供一个基于系统安全评估的潜在软件对系统危害的贡献的总结，以及这与分配的保证级别之间的关系。然后，sa引用生成的软件生命周期数据，以满足与分配的保证级别相关联的目标。

    在认证过程中，航空航天企业对软件生命周期数据存在公开问题的情况并不鲜见。这是可以接受的，只要任何剩余的问题不危及飞机安全。所有已知的问题都必须在SOI审核期间向认证机构声明和解释。每个问题都必须提交一个分类，以确定飞机[29]的潜在安全风险。在整个软件生命周期中设置了四种不同的SOI审计。这些审核通常持续五天，并在软件生命周期的以下阶段进行:

    [逐句翻译](javascript:;)

    [相似例句](javascript:;)

    （技术方法）软件度量为评估和监视软件产品和过程的成本、进度和质量提供了强大的方法。度量对于安全关键软件的认证尤其重要，特别是与问题报告和测试覆盖率相关的度量。尽管几个软件项目监视和测量过程的可用性(如实际软件和系统测量(PSM)[31],目标问题度量(GQM)[32],六西格玛[33]和构造,有效成本模型(COCOMO II)[34]),很少有研究已经发表在如何将这些方法应用于软-器皿认证流程。Basili等人讨论了如何使用GQM方法为安全关键软件[35]的开发提供早期生命周期可见性。这是通过一组“准备情况评估问题”来实现的，这些问题应该根据预定义的度量和模型来回答。Habli和Kelly使用类似的方法来评估安全关键的软件过程，方法是将安全案例中的验证证据与生成此证据的过程联系起来。然后，将这些过程中的弱点用作可分配给安全证据的信心水平的指标。同样，Murdoch等人报道了一些关于PSM应用于生成支持安全过程管理的措施的结果[37,38]。其中一些措施与安全认证有关，例如根据认证数据要求完成认证。然而，这些研究都没有提供实证结果来验证这些测量技术对软件安全认证过程产生的工业数据的有效性。

    目前审计机载软件的方法给认证机构和航空航天公司带来了一系列问题。这些问题的摘要如下:

    问题一：审计人员只审核软件过程的快照。与花费在整个软件工程生命周期上的时间相比，权威机构在审计上花费的时间很短。审计人员很难在进行审计的时间内找出复杂的问题。

    问题2软件安全标准有不同的解释。软件和安全工程师在努力满足标准要求的过程中，可能会对软件进行过多或过少的设计。（To this end, they may be over- spending to achieve certiﬁcation credit or under-spending and risking an audit failure.）为此，他们可能会为了获得认证信用而过度支出，或者支出不足，并有审计失败的风险。航空公司可以向核证机关征求意见，但为了保持其独立性，当局只能提供有限的意见。

    问题3:公司可能有欺诈行为:这种情况非常罕见，但并非闻所未闻。软件公司可能试图在SOI审计中就其软件过程的状态误导当局。这可能是由于财务或时间的因素，迫使公司作出错误的声明，以避免项目时间表[39]的延误。通常，这将在审计时表现出来，这时公司可能意识到项目还没有准备好进行SOI审计。

    问题4:缺乏确定软件状态的客观标准:为了评估认证要求的实现情况，认证机构必须了解正在开发的软件的技术方面，例如在开发过程中提出的安全问题。这通常是通过审查项目的技术报告来实现的，有时是在SOI审计的短时间内。对审计人员来说，吸收软件项目的技术细节并进行客观的评估是一项具有挑战性的任务，特别是当他们负责审计来自不同公司的多个软件项目时。

    5 .一再犯同样的错误:许多公司进入SOI审计，犯了他们以前犯过的同样的错误，主要是由于对当局旨在评估的认证目标理解不足。这可能是由于缺乏经验(可能是由于人员流动)或缺乏严格的质量控制在这些公司。新技术的引进也可能造成这一问题。同样，对于第一次开发机载软件的公司来说，这个问题也是一个问题的来源。

    上述问题部分来自于对有经验的独立软件审核员的采访。内部意见的重点是审计过程的效率以及认证机构和开发团队之间关系的透明度。

    当然，上述问题构成了审计过程中遇到的问题的子集。不同的国家、公司和项目的发展实践可能有所不同。例如，其他问题包括在不同的项目之间不适当地重用认证证据，或者不成熟地部署新技术。然而，上述五个问题似乎是软件安全审核员所面临的最常见的困难。

    为此目的，如果认证机构拥有基于预定义标准的度量标准，在审计开始之前反映软件项目的状态，那么它们可以更好地为SOI审计做好准备，特别是从技术角度。如果在项目开发过程中定期提供这些度量标准，认证机构可以使用项目生命周期历史上数据的趋势来识别任何误导信息。例如，一个迹象可能是在SOI审计时进度图中的突然改进。此外，如果度量数据在不同的软件项目之间被标准化，那么它还可以用来比较一个项目的质量和进度，以及之前已经成功通过SOI审核的其他项目。同样，航空航天公司内部的质量保证部门也可以使用这些指标来确定软件对认证目标的准备情况。根据这些标准，可以向航空航天公司提供重点培训，以改进其内部能力和其认证材料的质量。 [↑](#endnote-ref-12)