本课题来源于工信部的民用飞机专项科研《航空发动机电子控制系统适航审定关键技术》中的子课题《航空发动机电子控制器软件和硬件适航审定技术研究》，针对大型客机涡扇发动机电子控制系统软件的适航审定问题，开展相关的基础技术研究。

2017年5月，C919大客机的首次试飞顺利完成，我国民用航空事业进入新的历史阶段。2010年年底，民航局受理了C919飞机型号合格证申请，开展C919飞机型号合格审定，制定了66份的审定计划，规划4000余份用于证明符合特定适航标准的技术报告计划和近1500项的实验验证计划。截至2018年12月，已完成近300项验证试验的试验目击审查，批准500余份的验证试验大纲和80余份的试验报告。按照计划，审查组还要完成包括审定试飞在内的、证明飞机设计符合适航要求的大量工程技术审查工作，根据研制进度和取证的工作量，预计2020年底取得C919飞机型号合格证。

为确保航空飞行器的安全性，飞行器的设计维护、人员培训和飞机操作等各个方面都要达到足够的安全与完整性。航空电子设备属于安全关键项目，要使用航空电子设备实现功能，其设计与制造的安全与完整性要达到适航要求，否则有可能危害人员或设备的安全。为了确保飞机系统的设计和制造符合要求的目标，不同的国家成立了不同的机构负责安全关键系统的适航审查。飞行批准认证机构包括欧洲航空安全局(EASA)和美国联邦航空局(FAA)等。我国的则是民航管理局（）。当飞机系统首次开发或升级时，飞行认证机构必须在系统设计获准飞行前进行适航审查并认证。只有符合预先定义的设计和操作限制，该型号的飞行器才能用于飞行。航空电子设备由硬件和软件两部分组成，对于硬件来说其安全性和完整性通常有着定量要求。而对于软件来说，很难通过统计测试和操作经验等方法来定量地展示其安全和可靠性水平。因此，适航软件的标准通过确保控制开发过程的质量，来确保软件的可靠性。在民用航空领域，DO178C是机载软件批准的主要标准。DO178C文件的目的是“为机载系统和设备提供软件生产指南，使这些系统和设备在满足适航要求的安全可靠性水平上履行其预期功能”。DO178C定义了航空业界关于机载软件批准的共识。开发方通过提交生命周期数据来获得适航认证，这些生命周期数据表明软件开发是否按照DO178C标准指定的过程和要求执行。

绪论第2页

1. 目前Do178C审定工作 特别是在配置管理方面存在的困难问题，还有目前

2.软件配置管理过程是CMMI。。，多么重要。。。 在Do178C标准中也作出了明确规定，并。。。

对于scm过程的审定也非常重要，（国外对适航审定中配置管理的研究主要是。模型驱动建模，建立UML文件，对人员要求高、难度大，需要各方协调；还有？？？。。。）而且国内未对此进行专门的研究。所以得出结论

1. 配置管理过程在DO178C过程中所起的作用，以及目前对适航审定中Do178C的研究成果。

国内航空发动机研制相对国外具有较大差距，研发、适航审定经验不足，给航空发动机适航审定带来很大困难。审计机载软件给认证机构和航空航天公司带来问题。问题摘要如下:

一、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（标准不一定能够看出工业实践中的安全管理证据，而只对工业实践中需要被采用的信息作出要求，因此单纯从标准无法指导实际研发和审定工作的具体的方法、证据形式等内容），这也

研发方提供的审定材料存在哪些问题，可能给局方进行审定造成很大的困难，虽然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

二、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（而且这种审查方式需要耗费大量的时间、人力，工作效率低、周期长、成本高、质量控制难以把握。时间短、任务重）

传统适航审定，审定人员 提交审定材料 进行人工审查，审查标准 评审人员对标准文件的理解和评审人员的日常经验和阅历，不同评审人员在进行相同的评审活动时可能得出的结论有差异，甚至得出相反的结论（软件标准不同的解释），这将导致评审结果的不确定性，有争议性。

软件配置管理阶段。

软件配置管理（SCM——Software Configuration Mangement）是ISO9001和CMM Level2中的重要组成元素,它在软件产品开发的生命周期中,提供了结构化、有序化、产品化的管理软件工程方法,是软件开发和维护的基础。

软件配置管理

目前国内几乎没有对于适航软件审定中配置管理过程的专门研究， 只有两种情况研究。1.参与适航软件的研发，设计了配置管理系统

2.进行了适航配置管理的思考，但只是提出 思路与分析，未给出可用于实践操作

在适航软件的开发实践中，对于配置管理过程的实施主要是应用CMMI（软件能力成熟度模型集成）中配置管理过程的研究成果（配置管理是CMMI二级的一个过程域），在实际的项目中按照配置管理人员对于Do178C标准的理解进行软件配置管理计划的制订以保证配置管理过程相关目标的完成，这也导致了审定方进行审定时 得到的证据难以使用，审定难度大。 无法提供足够的证据，不能通过审定。

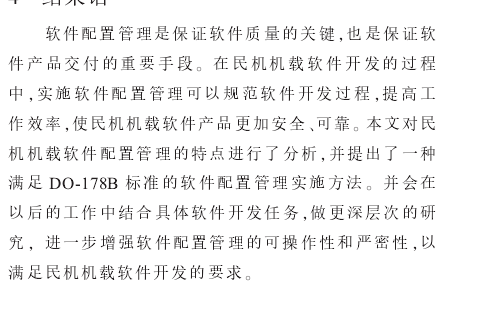
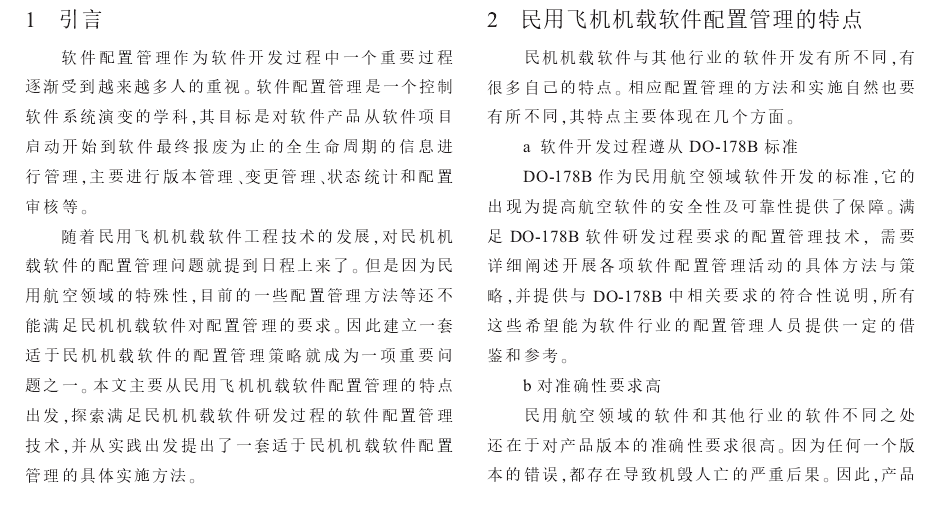
综上所述，对配置管理 过程的相关目标进行研究，规范研发方提供证据的信息与格式要求，提出审定方审定证据数据的方法，确定开发过程符合配置管理过程目标，是满足DO178c标准进行审定的一部分，也是保证适航安全关键软件符合安全标准的重要部分 ，提出审定方法，半自动化审定的方法，能够提高审定人员工作的效率，并且为审定工作的**可**查性提供可观测到的依据。

软件过程管理对航空软件产品的安全性和可靠性发挥着至关重要的作用，而配置管理 技术作为软件过程中的一个重要环节，无疑又是重中之重

软件配置管理技术主要解决的是软件开发过程 中的资源管理问题［4］。它作为软件过程管理中的

一项重要内容，在 DO － 178B 中具有明确的目标与 要求。

软件配置管理过程



二、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

特别是在我国，Do178C标准还处于学习和研究阶段，在软件开发的工业实践中，没有一套成熟的系统，无论研制方还是审定方，都是依靠专家的经验对安全关键软件 是否达到适航标准 人工进行审查啊，而专家审查 也存在着 无审查分类、记录等信息，容易出问题， 在与国外对接时，国外对我国的标准不认可，影响我国民用大飞机的进一步发展，与走出国门。

软件配置管理（SCM——Software Configuration Mangement）是ISO9001和CMM Level2中的重要组成元素,它在软件产品开发的生命周期中,提供了结构化、有序化、产品化的管理软件工程方法,是软件开发和维护的基础。

目前国内几乎没有对于适航软件审定中配置管理过程的专门研究，在适航软件的开发实践中，对于配置管理过程的实施主要是应用CMMI（软件能力成熟度模型集成）中配置管理过程的研究成果（配置管理是CMMI二级的一个过程域），在实际的项目中按照配置管理人员对于Do178C标准的理解进行软件配置管理计划的制订以保证配置管理过程相关目标的完 成，这也导致了审定方进行审定时 得到的证据难以使用，审定难度大。 无法提供足够的证据，不能通过审定。

综上所述，对配置管理 过程的相关目标进行研究，规范研发方提供证据的信息与格式要求，提出审定方审定证据数据的方法，确定开发过程符合配置管理过程目标，是满足DO178c标准进行审定的一部分，也是保证适航安全关键软件符合安全标准的重要部分 ，提出审定方法，半自动化审定的方法，能够提高审定人员工作的效率，并且为审定工作的**可**查性提供可观测到的依据。

——————————————————————————————————————————————————————————————————————

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（标准不一定能够看出工业实践中的安全管理证据，而只对工业实践中需要被采用的信息作出要求，因此单纯从标准无法指导实际研发和审定工作的具体的方法、证据形式等内容），这也

**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目标和相关目标。**

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。

***遵守规范的标准往往是常态在民用航空领域[16],特别是关于机载软件的审批和认证(6、19)。***

***在说明性认证中，开发人员通过满足一组过程目标来证明软件系统是可接受的安全的，这些过程目标是安全标准所要求的符合性。满足这些目标的方法通常在规定的标准中被严格定义，留给开发人员很少的空间来为遵从性应用替代方法，这可能更适合他们的软件产品和过程。规定性软件标准的一个基本限制在于，好的工具、技术和方法并不一定导致达到特定级别的完整性。规定的技术与系统故障率之间的相关性是不可行的[16,20]。另一方面，在基于目标的认证中，标准要求提交一份论证，说明从测试、分析和评审中产生的证据如何满足有关软件功能安全性的要求。尽管有明确的安全论证和证据的优点，但是对于创建符合这些标准中设定的目标(即缺乏足够的有效的论证实例或生成证据的样本方法)的保证论证的指导是否足够，仍然存在一些担忧。许多研究已经考虑并比较了这两种软件安全保证方法[21-23]，强调了每种方法的优点和局限性，以及它们可能如何组合成[24]。***

配置管理和变更管理的关系

***认证是指“确保产品或流程具有某些规定的属性，然后将其记录在证书中”的过程。担保可以定义为对感兴趣的属性[8]的合理信心。（compliance with prescriptive standards tend to be the norm in the civil aerospace domain [16–18],）***

***而安全的概念和保证情况下[9 - 11]是大量使用基于目标标准在关键领域,如国防(12、13)铁路[14]和石油和天然气[15],遵守规范的标准往往是常态在民用航空领域[16],特别是关于机载软件的审批和认证(6、19)。在说明性认证中，开发人员通过满足一组过程目标来证明软件系统是可接受的安全的，这些过程目标是安全标准所要求的符合性。满足这些目标的方法通常在规定的标准中被严格定义，留给开发人员很少的空间来为遵从性应用替代方法，这可能更适合他们的软件产品和过程。规定性软件标准的一个基本限制在于，好的工具、技术和方法并不一定导致达到特定级别的完整性。规定的技术与系统故障率之间的相关性是不可行的[16,20]。另一方面，在基于目标的认证中，标准要求提交一份论证，说明从测试、分析和评审中产生的证据如何满足有关软件功能安全性的要求。尽管有明确的安全论证和证据的优点，但是对于创建符合这些标准中设定的目标(即缺乏足够的有效的论证实例或生成证据的样本方法)的保证论证的指导是否足够，仍然存在一些担忧。许多研究已经考虑并比较了这两种软件安全保证方法[21-23]，强调了每种方法的优点和局限性，以及它们可能如何组合成[24]。***

符合标准要求的。安全证据的一些通用示例，包括测试结果、系统规范、人员能力和源代码。对于一个实际的大型系统，实践者需要在系统的分析、开发、验证、维护、运行和演进过程中收集和管理大量的安全证据。必须对这些庞大的信息进行结构化，以显示其如何满足安全标准的要求。如果证据结构不合理，其纯粹的数量和复杂性可能危及高水平安全目标[8]的实现的可靠性。安全证据的结构可以是图形化的(例如，使用模型)，也可以是文本化的。

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。

主要是针对开发方的。 依赖于实际项目，不同的项目要重新设计。

对于已有的目前我国适航文档证据的实际情况，实用性不强

是对标准呢所有的目标的 研究 ，给出

都没有给审定方提供可以应用于审定实践的具体流程

国内外研究现状：

——————————————————————————————————————————————

国内外审定方法方面的研究

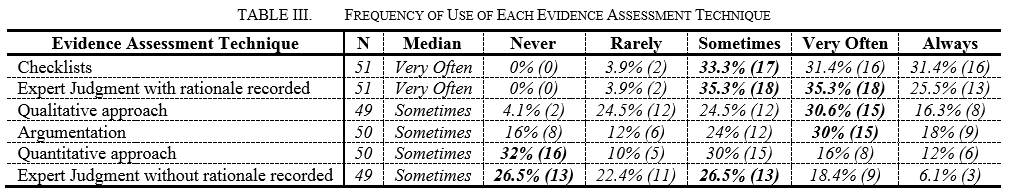
模型驱动研发过程 有论文 ？？？ 文本管理进行证据管理 有18 们描述了需要一个跨越这些不同市场的共同认证框架，以改进安全批准的相互承认协议，通过可重用的审定框架，降低审定的成本

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

在国外，工业上使用清单（检验表）最多（evidence的调查显示）

**工业上 对证据进行评估的 方法What Techniques Are Used For Assessing Evidence In Practice**

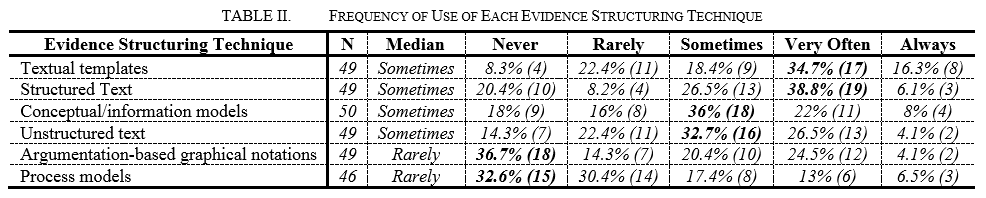
专家审查（面向审查）、有记录与无记录。 定性分析方法（面向？），**定量分析方法（面向开发）** 以及**论证**的方法（双向的）？



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

在实践中对证据结构是怎么提供和保证的

What Techniques Are Used For Structuring Evidence In Practice?



文本型的模板 结构化的文本 审定指南 审查单

元模型或信息模型 偶尔使用 有一个研究

非结构化的文本 偶尔使用 不用这个

过程模型 有不少研究 极少用于实践 ，过程模型多用于交流。

本文将过程模型与结构化证据（通过文本结构化）同时考虑了目标（过程目标和大目标） 的论证（通过GSN方法），构建了配置管理过程的审查模型。

基于图形符号论证 不知道有没有论文 有 evidence20 还有杨阳的。

另外还有一些其他。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

国外： 国内：审定技术？

论文1 ：

论文2：

论文:3

DO178c才配置管理研究、变更管理

国内：国外：

论文1：

论文2：

论文3：

What Types Of Information And Artefacts Are Used As Evidence For Demonstrating Compliance With Safety Standards? Figure 4 shows the 16 process-based evidence types provided as options in the questionnaire in the vertical axis, and the percentage and number (in brackets) of respondents who selected each type in the horizontal axis. V&V plan was the most recognized process-based evidence type. The second most selected type was Development plan, followed by Safety management plan and Configuration management plan. Only four process-based evidence types were selected by less than 50% of the respondents: Operator competence specification, Communication plan, Reused component historical service data, and Development and V&V staff competence specification. As for the product information category, shown in Figure 5, we identified that Requirements specification was the most selected product-based evidence type. The second most selected type was Test results, followed by Test case specification and Design specification. The least identified evidence type in the product information was Theorem proving results. Other product evidence types selected in low percentages were Model checking, Object code, System historical service data, and Accidents specification. These four types were selected by less than 50% of the respondents. Since the Testing results evidence type is a very broad category, we decomposed it into 16 finergrained types, shown in Figure 6. As indicated in Figure 6, we identified that System testing was the most selected type in this category, followed by Functional testing, Normal range testing, and Acceptance testing. The least selected testing type was Non-operational testing. All the other testing types were selected by more than 50% of the respondents. We did not find any new evidence types mentioned in the others sections by the participants.

哪些类型的信息和人工制品被用作证明符合安全标准的证据?图4显示了垂直轴上问卷中作为选项提供的16种基于过程的证据类型，以及在水平轴上选择每种类型的受访者的百分比和数量(括号内)。V&V计划是公认的基于过程的证据类型。其次是验证计划、开发计划，其次是安全管理计划和配置管理计划。只有不到50%的受访者选择了四种基于流程的证据类型:操作员能力规范、通信计划、重用组件历史服务数据、开发和V&V员工能力规范。对于产品信息类别，如图5所示，我们确定需求规范是最被选择的基于产品的证据类型。第二大选择类型是测试结果，其次是测试用例规范和设计规范。产品信息中最难识别的证据类型是定理证明结果。其他低百分比选择的产品证据类型包括模型检查、目标代码、系统历史服务数据和事故规范。这四种类型被少于50%的受访者选择。由于测试结果证据类型是一个非常广泛的类别，所以我们将它分解为16个更细粒度的类型，如图6所示。如图6所示，我们确定系统测试是这个类别中选择最多的类型，其次是功能测试、正常范围测试和验收测试。最少选择的测试类型是非操作测试。所有其他测试类型都是由超过50%的受访者选择的。我们没有发现参与者在其他部分提到的任何新的证据类型。

表II显示了使用不同证据结构技术的频率，表示每种技术的响应总数(N)、它们的中值和模式(粗体)。除了流程模型(如SPEM)和基于参数的图形表示法(如GSN)之外，实践中使用的技术的中值有时是。流程模型和基于参数的图形符号是惟一一种模式永远不会出现的技术，而文本模板和结构化文本具有最高的模式(通常)。文本模板也是报告使用频率最高的技术，也是报告使用频率最高的技术(91.7%)。

**相关理论和技术：**

* 1. Do178C基础理论

1.2（配置管理过程、） 标准介绍

2.安全审定的方法理论   
（不在这里写）

基于。。。。

基于。。。。

***在说明性认证中，开发人员通过满足一组过程目标来证明软件系统是可接受的安全的，这些过程目标是安全标准所要求的符合性。满足这些目标的方法通常在规定的标准中被严格定义，留给开发人员很少的空间来为遵从性应用替代方法，这可能更适合他们的软件产品和过程。规定性软件标准的一个基本限制在于，好的工具、技术和方法并不一定导致达到特定级别的完整性。规定的技术与系统故障率之间的相关性是不可行的[16,20]。另一方面，在基于目标的认证中，标准要求提交一份论证，说明从测试、分析和评审中产生的证据如何满足有关软件功能安全性的要求。尽管有明确的安全论证和证据的优点，但是对于创建符合这些标准中设定的目标(即缺乏足够的有效的论证实例或生成证据的样本方法)的保证论证的指导是否足够，仍然存在一些担忧。许多研究已经考虑并比较了这两种软件安全保证方法[21-23]，强调了每种方法的优点和局限性，以及它们可能如何组合成[24]。***

**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目标和相关目标。**

3.需求追踪技术：文本相似度技术，wordvec，选择排序

文本相似度技术

Towards a Model-Based Evolutionary Chain of Evidence for Compliance with Safety Standards

Compliance with safety standards can greatly increase the development cost and time of critical systems. Major problems arise when evolutions to a system entail reconstruction of the body of safety evidence. When changes occur in the development or certification processes, identification of the new evidence to provide, the evidence that is no longer adequate, or the evidence that can be reused poses some challenges. Therefore, practitioners need support to identify how a chain of evidence evolves as a result of the changes. Otherwise, execution of the above activities can be very costly, and it can even result in abandonment of certification efforts. This paper outlines a solution to deal with these challenges. The solution is based on the use of model-driven engineering technology, which has already been applied for safety certification but not from an evolutionary chain of evidence-based perspective. The paper also sets the background for developing the solution, describes real situations in which the solution can help industry, and discusses possible challenges for developing it. The solution will be developed as part of OPENCOSS, a research project on cross-domain evolutionary certification.

遵守安全标准可以大大增加关键系统的开发成本和时间。当系统的演化需要重构安全证据体时，就会出现主要的问题。当开发或认证过程中发生更改时，要提供的新证据的标识、不再充分的证据或可重用的证据会带来一些挑战。因此，实践者需要支持来确定证据链是如何随着变更而演变的。否则，执行上述活动可能会非常昂贵，甚至可能导致放弃认证工作。本文概述了应对这些挑战的解决方案。该解决方案基于使用模型驱动的工程技术，该技术已经应用于安全认证，但不是从基于证据的进化链的角度。本文还设置了解决方案开发的背景，描述了解决方案可以帮助行业的实际情况，并讨论了开发该解决方案可能面临的挑战。该解决方案将作为OPENCOSS的一部分开发，OPENCOSS是一个跨领域演进认证的研究项目。

**通过模型驱动技术，确定证据材料的变更和演变的方法。**

# On the Use of Goal Models and Business Process Models for Elicitation of System Requirements

Goal modelling and business process modelling are two techniques that can be used for elicitation of system requirements of an information system. In general, goal-based approaches aim at supporting the objectives that an organization needs to achieve, whereas business process-based approaches aim at supporting the activity of an organization. Consequently, it could be assumed that these two types of approaches represent completely different perspectives for elicitation of system requirements. In this paper we argue that a correspondence exists between the perspectives and that they can be considered equivalent in some operational aspects. Therefore, the use of a perspective also implies support for the other. This argument is based on the definition of a set of guidelines that shows how a goal model can be derived from a business process model. As a result, we discuss when selection of one of the perspectives or their combination would be more suitable for requirements elicitation

**目标建模和业务流程建模**是两种可用于获取信息系统的系统需求的技术。通常，基于目标的方法旨在支持组织需要实现的目标，而基于业务流程的方法旨在支持组织的活动。因此，可以假设这两种类型的方法代表了对系统需求提取的完全不同的观点。在本文中，我们认为这些透视图之间存在对应关系，并且在某些操作方面可以认为它们是等价的。因此，使用透视图也意味着支持另一个透视图。此参数基于一组指导原则的定义，这些指导原则显示了如何从业务流程模型派生出目标模型。因此，我们讨论了什么时候选择一个透视图或者它们的组合更适合于需求捕获。.

**基于目标建模和基于流程建模在获取软件需求时的特点和选择。**

**使用该方法的思路进行分析并提出方法，但该方法是用于软件需求的**

Supporting the verification of compliance to safety standards via model-driven engineering: Approach, tool-support and empirical validation

* Many safety–critical systems are subject to safety certification as a way to provide assurance that these systems cannot unduly harm people, property or the environment.

许多安全关键系统都要经过安全认证，以确保这些系统不会过度伤害人、财产或环境。

* Creating the requisite evidence for certification can be a challenging task due to the sheer size of the textual standards based on which certification is performed and the amenability of these standards to subjective interpretation.

创建认证所需的证据可能是一项具有挑战性的任务，因为执行认证所依据的文本标准的绝对规模，以及这些标准对主观解释的适应性。

* Objective
* This paper proposes a novel approach to aid suppliers in creating the evidence necessary for certification according to standards.

本文提出了一种新的方法来帮助供应商根据标准创建认证所需的证据。

* The approach is based on Model-Driven Engineering (MDE) and addresses the challenges of using certification standards while providing assistance with compliance.

该方法基于模型驱动工程(MDE)，解决了在提供遵从性帮助的同时使用认证标准的挑战。

* Method

方法

* Given a safety standard, a conceptual model is built that provides a succinct and explicit interpretation of the standard.

给出了一个安全标准，建立了一个概念模型，该模型对标准进行了简洁而明确的解释。

* This model is then used to create a UML profile that helps system suppliers in relating the concepts of the safety standard to those of the application domain, in turn enabling the suppliers to demonstrate how their system development artifacts comply with the standard.

然后使用这个模型来创建一个UML概要文件，该概要文件帮助系统供应商将安全标准的概念与应用程序领域的概念联系起来，从而使供应商能够演示他们的系统开发构件如何符合标准。

* Results

结果

* We provide a generalizable and tool-supported solution to support the verification of compliance to safety standards.

我们提供一个通用的和工具支持的解决方案，以支持验证是否符合安全标准。

* Empirical validation of the work is presented via an industrial case study that shows how the concepts of a sub-sea production control system can be aligned with the evidence requirements of the IEC61508 standard.

通过一个工业案例研究对工作进行了实证验证，该案例研究显示了海底生产控制系统的概念如何能够符合IEC61508标准的证据要求。

* A subsequent survey examines the perceptions of practitioners about the solution.

随后的调查调查了从业者对解决方案的看法。

建立符合标准的元模型，概念模型，该模型对标准进行了简洁而明确的解释, , 然后使用这个模型来创建一个UML概要文件，该概要文件帮助系统供应商将安全标准的概念与应用程序领域的概念联系起来，从而使供应商能够演示他们的系统开发构件如何符合标准。

**1是面向开发方的，**

**2是对开发人员的培训、学习和开发影响要求很高**

**3.是面向多种安全标准的，为给Do178C 标准的实际审定给出具体化的建议**

Challenges for an Open and Evolutionary Approach to Safety Assurance and Certification of Safety-Critical Systems

* Abstract— Safety assurance and certification are amongst the most expensive and time-consuming tasks in the development of safety-critical embedded systems.

摘要-安全保证和认证是嵌入式系统开发中最昂贵和最耗时的任务之一。

* The increasing complexity and size of this kind of systems combined with the growing market demand requires the industry to implement a coherent reuse strategy.

这种系统的复杂性和规模不断增加，加上市场需求的不断增长，要求行业实现一致的重用策略。

* A major problem arises as typically a safetycritical product and accompanying safety evidence is monolithic, based on the whole product, and evolutions to the product become costly and time consuming because they entail regenerating the entire evidence-set.

一个主要的问题出现了，因为典型的安全关键产品和伴随的安全证据是基于整个产品的整体的，并且产品的演进会变得昂贵和耗时，因为它们需要重新生成整个证据集。

* Another key difficulty appears when trying to reuse products from one application domain in another, because they are constrained by different standards and the full safety assurance certification process is applied as for a new product, thus reducing the return on investment of such reuse decision.

当试图在另一个应用程序域中重用来自一个应用程序域的产品时，还会出现另一个关键的困难，因为它们受到不同标准的约束，并且对新产品应用完整的安全保证认证流程，从而降低了此类重用决策的投资回报。

* This paper describes the current state on safety assurance and certification of embedded systems in the avionics, railway and automotive domains and then proposes some future directions for work in the area.

介绍了航空电子、铁路、汽车等领域嵌入式系统安全保障与认证的现状，并提出了该领域未来的发展方向。

* In particular, we describe the need for a common certification framework that spans these different markets to improve mutual recognition agreement of safety approvals.

特别地，我们描述了需要一个跨越这些不同市场的共同认证框架，以改进安全批准的相互承认协议。

* We then discuss the need for new strategies focused on a compositional and evolutionary certification approach with the capability to reuse safety arguments, safety evidence, and context information about system components, in a way that makes certification more cost-effective, precise, and scalable.

然后，我们将讨论新策略的需求，重点放在具有重用安全参数、安全证据和关于系统组件的上下文信息的能力的组合和演进认证方法上，从而使认证更具成本效益、更精确和可伸缩性

**目的：夸越不同领域标准的安全关键系统的共同认证框架，**

**介绍了各领域安全保障与认真的现状，提出了未来发展的方向。**

**为提出具体的解决办法。**