## 一、安全证据管理技术概述

目前国际上保证安全证据结构的技术，可以分为基于论证方法管理、基于模型管理、基于文本模板管理三种类型。

1. 基于论证的证据结构管理。论证是一种向相关方证明系统安全性达到了目标要求的方法，结构化的论证需要有直接的证据支持，人们为此提出了构建证据的具体技术，技术又可以分为基于图形构建证据结构和使用基于文本构建证据结构。

基于图形技术构建证据结构，对论据和论证证据进行表示。在[PS3, PS5, PS8, PS9, PS10])中使用了GSN技术，它可以用来显式地记录参数的元素和结构以及参数与证据的关系。在GSN中，论证的声明被记录为目标，证据项被记录在解决方案中。[PS20, PS22, PS72, PS78]) 使用了CAE技术，它提倡一种类似于GSN的三层方法，包括在一个论证中断言的一个顶级声明、对支持一个声明的参数的描述，以及对支持一个声明或论证的证据的引用。 [PS23, PS38, PS58, PS, PS])使用了BBN,它在一个有向非循环图中引入一个结构来表示它们之间的条件依赖关系。SSG [PS]是一种线性图，它将安全规范表示为节点，将证据及其关系表示为边。

基于结构化文本对论据和论证证据进行表示的方法。（PS18540）使用 了Trust cases技术，Trust cases指的是为安全声明、参数和证据归纳出结构化的文本格式，并使用参考文档的方式进行展示说明。[PS185]中，使用了结构化HTML标签来链接和构造各种作为安全证据的人工制品。[PS80]，为普通文本规定某种结构，显式的表示论点的关键部分;规定大纲格式构造参数和证据，使用数学中的几何证明结构给出陈述和理由;使用LISP编程语言的语法结构的特点，使用简短的名称和括号作为证据和参数。

2. 基于模型的证据管理是指使用模型描述安全证据结构，确定证据的规格与要求。

[PS]使用模型驱动的方法，为do - 178标准构建了UML概要文件，用于软件产品的开发和审定。

-[PS99]使用的是数据建模，在大型安全案例中，使用实体关系图来构造数据内容。

-[PS]利用了过程模型，对于产生证据数据的活动与过程，进行研究和建模，并使用基于树的结构进行展示。

3.文本模板(3%): 使用模板来提供预定义的表，以及以预定义文本格式构造证据的约束。

- [PS50]，使用了ACRuDA模板，该模板被用来 根据预先定义的安全案例结构构造证据。

- [PS19]提出了 Template Add-ons，它为预定义的一组文档提供模板，这些文档将在不同的系统开发和安全保证阶段生成。它还就文档化、半形式化描述以及验证和验证过程所需的方法提供了建议。

## 二、对证据进行评估的技术概述：共四种

目前国际上对证据进行评估的技术，大致可以分为

1.定性评估(%):是指使用非数值方法评估证据的技术。 PS,PS,PS,PS,PS,PS使用了论证，论证是定性评价中最广泛使用的方法。可以基于不受限制的自然语言、(半)结构化的自然语言或图形化的论证结构，如GSN。图形论证结构通常具有易于理解、检查和导航的优点。

- [PS，研究基于活动的质量模型，它使用质量矩阵来评估是否符合IEC62304标准。

- [PS]提出了，Evidence-confidence conversion process ，该过程通过评审过程评估安全证据，从而确定对系统安全的信任程度。。

2，检查列表(%):我们将这类技术分类为“待办事项列表”，其中包含一组需要在检查证据时回答或检查的指导问题。

-[PS]设计核对表，核对表根据系统设计的具体情况来评估证据。

-[PS]，基于目标/问题/度量框架[](GQM)。定义了用于评估产品和过程证据的顶级目标、为实现这些目标而需要回答的问题，以及提供可度量参考的度量标准，以便执行分析。

-[PS]以论证为基础的核对表，将核对表与论证相结合来评估证据。

-[PS]则采用了基于分类的问卷调查，问卷包含了305个涉及到软件安全风险分类和评估过程中安全属性和人工制品的问题。

,3.定量评估(%):使用数值方法评估证据的技术。

- [PS41,PS,PS,PS,PS])BBNs技术，它利用条件概率分布来评估存在不确定性的证据。该技术与BBN证据结构结合使用(第4.2节)。这是文献中最常用的证据评估定量技术。

- [PS]，提出了结合了定量评估和正式论证结构Modus方法。该方法基于定量推理，使用目标模型、专家启发式和概率模拟来评估安全案例的总体目标。

-[PS96]使用了Evidence Volume Approach证据量法，该方法允许内部专家对描述每一证据相对重要性的证据分配加权因子。然后为加权证据选择一个聚合函数来计算一个称为证据量的卷，根据这个卷选择结果(接受或拒绝)。

4 基于逻辑的评估(6%):使用逻辑公式的技术，以阐明和验证证据项及其关系的属性。例如一阶逻辑语句。基于逻辑的技术最适合于检查证据信息的格式良好性和一致性约束。例如，。。。使用OCL[23] 确保特定系统生成的证据项之间存在一致的链接，

## 三、软件配置管理 安全保证技术相关研究。

目前对软件配置管理的研究主要关注软件文档制品中的配置项的标识和跟踪。通过对比软件开发文档制品，对配置项进行追溯与管理（包括不同的软件开发文档制品中相同需求的追溯性） ，通过比较软件开发文档制品和代码制品，验证软件开发文档工件的需求是否被正确的编写成了代码；通过对代码制品进行比较，对状态修改、软件版本和依赖性进行管理，对功能或物理特性的变化进行控制。

[10-12]使用跟踪矩阵管理软件配置管理的文档构件。跟踪矩阵中的每个需求都由惟一ID标识，并位于第一行。文档构件的类型位于列中，与需求映射的配置项的索引放在矩阵的内容字段中。可跟踪性矩阵可用于跟踪不同文档构件中具有相同需求的配置项。

[13-14]应用信息检索技术实现了可追溯矩阵的自动生成。通过处理软件文档构件中的简单链接，使用可跟踪矩阵的优势在于易于读取和使用。

,[15] 提出通过使用依赖关系,跟踪关系，和文档制品的结构化信息。推断新文档产品之间的追踪关系

【content-based】（）提出了基于内容的配置管理系统，该系统生成“关联链接”，用来管理软件研究文档构件中高度抽象的非功能需求。关联链接由相关的两个配置项和配置项间需要遵循的规则组成，用于对软件研发文档制品进行配置管理

我国也有许多对配置管理过程的研究

软件配置管理的问题\_目的\_层次和策略\_严晓光

结合软件配置管理可能出现的活动工作量大、效率低、配置失控等问题，深入分析了问题出现的原因，讨论了配置管理的层次目标及各层次的特点，提出了业务导向、分层次管理、注重实效等原则和策略。

姜文软件配置管理中的基线问题研究 分别归纳并给出了五种不同的基线定义，叙述了基线的层级、软件项目的阶段基线、实现阶段基线的水平等级和粒度，集中介绍了基线相关的技术问题

软件需求变更管理的研究与实践\_赵海英 提出了一种oucm，oucm创建了一个隔绝开发工作的，潜在无序的需求变更的流程方法，避免了正常开发工作被扰乱，减少不当需求变更引起的成本和工作量。

以上研究主要针对于配置管理中的某一方面进行专门研究，

这两个研究则面向配置管理的整个流程。

张薇 软件配置管理系统的优化研究与设计 对配置管理的流程进行了优化设计，提出了比较普遍全面的流程

王槐彬 基于工作流技术的软件配置管理过程建模\_

基于工作流技术，使用工作交流网建模技术对配置管理进行过程建模，并析了配置管理建模的优点。

以上的研究都是针对软件配置管理本身，没有特别的对适航软件中的SCM，或结合DO178标准进行研究。为设计到安全保证和证据管理的内容。

这两个，

则对我国机载软件开发 结合Do178标准，进行了流程、和各项活动具体方法与策略的研究。

民机机载软件配置管理技术研究\_杨娟

从结合民用机载软件的特点，提出了符合机载软件要求的配置管理流程，并与DO178B中的配置管理活动进行了符合性对照。

基于DO-178B的软件配置管理技术研究 毛佳、胡林平

以DO － 178B 为指导，详细阐述了开展各项软件配置管理活动的具体方法与策略。为提高数据控制的有效性，以满足DO － 178B 的A 级软件研发过程为例，说明了如何按照DO － 178B 中的两种控制类型对软件生命周期数据进行分类，最后，提供了符合DO － 178B 要求的说明