# 国内外研究现状。

## 1.1安全证据管理方法研究

对证据结构提供保证的方法包括 模型驱动、基于文本结构、模板化文本、基于流程等。

抄。。。。。。。。。

审查单、专家、

•在 opencsoo的调查中，大多数合作伙伴建议使用模型来构建认证文档。某某人在。。。里使用模型驱动的方法，达到了。。。。。。的目的。

17. Kelly, T. P.: Can Process-Based and Product-Based Approaches to Software Safety

Certification be Reconciled? In: Improvements in Systems Safety. Springer (2008)

研究了哪些基于过程的证据与基于软件产品的证据的性质，研究哪种证据更适合用来证明软件的安全性，结论是两种证据都是必要的而且是相关的。

Research-based prototypes have been developed for specification of certificates associated   to  source  code  [34],  V&V  activities  [38],  and  the  activities  of  the development  process  [41],  and (2) expert  judgement-based  quantification  of confidence on evidence [35].

基于原型的研究

用于(1)与源代码[34]、证据与整机活动[38]、开发流程[41]活动相关的用于认证的规范，而且 对基于专家判断的证据[35] 的置信度进行了量化。（https://www.researchgate.net/publication/266089534\_ModelME\_Technical\_Report\_MODUS\_A\_Goal-Based\_Approach\_for\_Quantitative\_Assessment\_of\_Technical\_Systems）

* Within   OMG,   there   are   two   initiatives   aimed   at standardizing the notion of and the concepts related to assurance evidence [22] and arguments  [24].

在OMG中，有两个计划旨在标准化与保证证据[22]和参数[24]相关的概念和概念。

。

二、证据管理方面的研究

本节回顾一些现有的研究和工具，这些研究和工具涉及安全证据、安全管理和安全演变。

17. Kelly, T. P.: Can Process-Based and Product-Based Approaches to Software Safety

Certification be Reconciled? In: Improvements in Systems Safety. Springer (2008)

安全证据 可以分为 基于过程的证据与基于软件产品的证据。

研究了哪些基于过程的证据与基于软件产品的证据的性质，研究哪种证据更适合用来证明软件的安全性，结论是两种证据都是必要的而且是相关的。 并说明了基于Do178的实践中存在的特点以及需要。

DO178c是一种基于过程证据进行认证的标准。

34. Programatica project: <http://programatica.cs.pdx.edu/index.html>(Accessed May 15, 2012)

34. Programatica project: <http://programatica.cs.pdx.edu/index.html>(Accessed May 15, 2012)

Sherriff, M., Williams, L.: DevCOP. In: ISSRE 2006

41 Open-DO initiative: <http://www.open-do.org/>(Accessed May 15, 2012)

Research-based prototypes have been developed for (1) specification of certificates associated   to  source  code  [34],  V&V 软件验证 activities  [38],  and  the  activities  of  the development  process  [41],  and (2) expert  judgement-based  quantification  of confidence on evidence [35].

已经开发了基于研究的原型，用于(1)与源代码[34]、验证活动[38]、开发流程[41]的活动相关的证书规范，以及(2)

基于专家判断的证据[35]置信度量化。

1.2现有的一些直接或间接处理证据管理的商业工具包括:

•atego Workbench[3]，支持软件开发工作产品的可跟踪性、影响分析和版本控制。

Parasoft Concerto [33], 支持需求、用例和缺陷管理，以及这些数据间的可跟踪性和影响分析。

## 安全关键软件配置管理概述

模型驱动 审定与研发的结合。

抄哪个。

## 1.3 安全关键软件审定方法概述

## 来源于evidence 和审定指南。

对安全关键软件审定的方法

0.Openss介绍

一、Opens 的项目介绍

写几个

三、审定方法

专家、 审查单、 文本模板 、结构文本 、

四、配置管理方面的研究

大多是构建追溯矩阵 针对开发文档

Content-based 针对前期文档也记性了

但都是基于开发的，国外的审定，没有 都只关注追溯性的配置项，而对于 过程数据，对于已经研发完成、得到了生命周期数据，需要进行审定的情况，并没有 考虑

问题，是否有作假等 不能用于审定

而对于审定如何执行， 某论文进行了调查。

而美国则是由审定指南，主要由专家 进行检查单的方法进行审定

When comparing the evidence assessment techniques, the main difference that we have identified is that the importance of Checklists in practice is High while in literature is Low. A possible reason is that the checklists used in industry correspond to well-established, widely-accepted means for evidence assessment, thus research on new checklists might not be very important. When performing the SLR, we did not consider expert judgement as a technique for evidence assessment unless the result or rationale was recorded with or based on another technique. Since the results of the survey show that the importance of this technique in practice is High, and as mentioned above, we think that studying how experts assess safety evidence and thus system safety is a relevant area for future research. TABLE

TABLE II shows the frequency of use of different evidence structuring techniques, indicating the total number of responses (N) for each technique, their median, and their mode (in bold). Except Process models such as SPEM and Argumentation-based graphical notation such as the GSN, the median of the techniques as used in practice is Sometimes. Process models and Argumentation-based graphical notations are the only techniques whose mode is Never, whereas Textual templates and Structured text have the highest modes (Very Often). Textual templates is also the technique most frequently reported as being used Always, as well as the technique reported as used by the highest number of respondents (91.7%). Therefore, the results suggest a generalised and frequent use of Textual templates for structuring evidence. TABLE

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%)。因此，研究结果表明，使用文本模板构建证据是普遍且频繁的。

[逐句翻译](javascript:;)

[相似例句](javascript:;)

Previous work has also acknowledged the use of textual templates documentations for structuring evidence [18], although it did not indicate its overall frequency. Another survey [20] reports the use of Argumentation-based graphical notations such as GSN and CAE for structuring claims, arguments, and evidence as most popular, but our results note differences in the practice. Basically, the fact that these graphical notations are the most popular ones for argumentation does mean that Argumentation-based graphical notations are widely used in practice. Although promising results in the use of models for structuring and managing evidence have been reported in [18], it seems that such approaches are not extensively used in industry yet. Nonetheless, this makes sense to use because the use of models for evidence structuring has been proposed recently. Industry might also have been using some evidence structuring techniques for decades, without considering to adopt other techniques or being aware of them. The scope of the related work (in terms of the countries from which the respondents are) might be a possible explanation for the differences with the results of our survey too. A

以前的工作也承认使用文本模板文档来构造证据[18]，尽管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)来组织索赔、论证和证据是最流行的，但我们的结果注意到了实践中的差异。基本上，这些图形符号是论证中最常用的符号，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。尽管[18]中已经报道了在使用模型构建和管理证据方面的有希望的结果，但是这种方法似乎还没有在工业上得到广泛应用。尽管如此，这还是有意义的，因为最近有人提出了使用模型来构建证据。业界可能几十年来一直在使用一些证据结构技术，而没有考虑采用其他技术或意识到这些技术

The percentage and number (in brackets) of responses for ways to check the degree of evidence completeness is shown in Figure 7. Most of the respondents indicated that the degree of completeness for the evidence is checked manually (e.g., using paper-based checklists). A majority of the respondents (79%; 41 respondents) also noted that they provide, check or request details about how the change of a piece of evidence has affected other pieces of evidence. When asked about how they analyse the effect of the change of a piece of evidence on other pieces, 46% of the respondents noted manual checks according to some predefined process. Approximately the same percentage of respondents replied that the effect is checked manually although without following any predefined process. One respondent mentioned the use of modular software safety cases [32]. Figure 8 shows the frequency of the evidence change effect techniques.

用于检查证据完整性程度的方法的响应的百分比和数量(在括号中)如图7所示。大多数受访者表示，证据的完整性程度是手工检查的(例如，使用基于纸张的清单)。大部分受访者(79%;41名被访者)亦指出，他们提供、核对或要求提供有关更改一项证据如何影响其他证据的详情。当被问及他们如何分析一块证据的变化对其他证据的影响时，46%的受访者表示会根据一些预先设定的流程进行手工检查。大约相同比例的受访者回答说，效果是手动检查的，尽管没有遵循任何预定义的过程。一名受访者提到使用模块化软件安全案例[32]。图8显示了证据更改效果技术的频率。