

国家 863 重点项目

“高可信软件生产工具与集成环境”技术文档



软件可信性证据框架规范

Software Trustworthiness Evidence Framework Specification
(TRUSTIE-STE V 2.0)

2009 年 5 月 30 日

发布声明

牵头单位：北京航空航天大学计算机学院

参研单位：国防科技大学计算机学院

北京大学信息科学技术学院

中国科学院软件研究所

中创软件公司

南京大学计算机学院

执笔人：刘旭东、孙海龙、谢冰、刘超、杨叶

版本号：2.0

发布时间：2009年5月30日

审核人：王怀民、李宣东

版权声明

本技术规范得到国家 863 重点项目“高可信软件生产工具及集成环境”第一课题“可信的国家软件资源共享与协同生产环境”的资助，版权归“可信的国家软件资源共享与协同生产环境”课题组所有。

本规范在以下条件下可以自由传播：

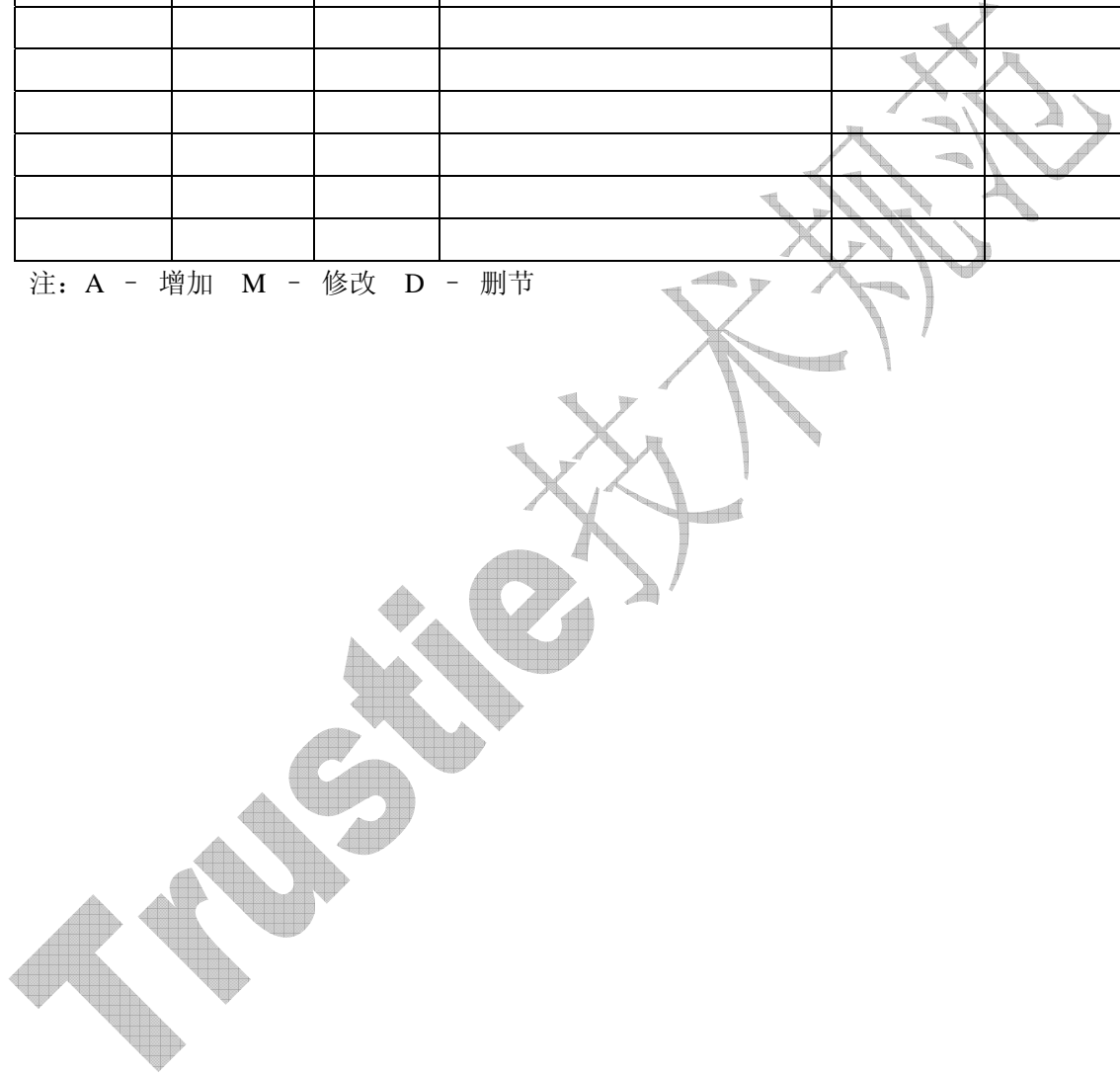
- (1) 保持本规范的完整性（包括发布声明）；
- (2) 未经课题组许可，任何人不得以本规范盈利。

Trustie 技术规范

变更记录

变更版本	日期	A/M/D	原因与修改情况描述	修订人	审核人
V1.0	2009.5.4	M	第 5 章 软件开发阶段证据项 修改	孙海龙	刘旭东
V1.1	2009.5.30	M	根据 09 年 5 月长沙讨论修改	刘旭东	

注：A - 增加 M - 修改 D - 删节



目 录

第 1 章	引言.....	1
1.1	背景.....	1
1.2	概述.....	1
第 2 章	范围与引用.....	3
2.1	范围.....	3
2.2	引用.....	3
第 3 章	软件可信性证据框架.....	4
第 4 章	软件可信性证据项.....	5
4.1	开发阶段证据项.....	5
4.2	提交阶段证据项.....	6
4.3	使用阶段证据项.....	7

第1章 引言

1.1 背景

软件可信分级评估是国家 863 计划重点项目“高可信软件生产工具与集成环境”中的一项重要研究内容。针对这一问题，“可信的国家软件资源共享与协同生产环境”课题组特别开展了软件可信分级规范的研究和制定工作，以推动该软件可信分级评估的标准化。该项工作由北京航空航天大学牵头负责，由国防科技大学、北京大学、中国科学院软件所、中创软件中间件有限公司等单位共同参与。在软件可信分级规范的研究和制定中，经过广泛深入的研究和探讨，课题组认为软件可信性证据是软件可信分级中的重要内容，是软件可信等级评估的依据。为规范化软件可信性证据的相关内容，特别开展了《软件可信性证据框架规范》的制定工作。

软件可信性证据框架的规范化工作是和可信分级规范工作协同开展的，从 2008 年 1 月份以来，工作组成员进行了大量的研究和广泛的交流讨论工作。2008 年 11 月 27 日在北京大学由南京大学李宣东教授主持召开了由北大、北航、中科院等多家单位代表参加的软件可信证据框架研讨会，确定了涵盖软件开发、软件实体提交和软件应用等三阶段证据的软件可信证据框架，并在项目各课题组范围内进行了意见征询和问卷调查。2009 年 1 月 5 日，以上单位的研究人员代表在北京就调查问卷结果进行了深入的讨论，就可信性证据达成了共识，形成了本参考规范 1.0 版。2009 年 5 月，课题组在长沙软件可信分级和可信证据框架再一次进行了讨论，在此基础上至，形成了本参考规范 2.0 版。

本规范起草的主要成员包括：南京大学李宣东、北京航空航天大学刘旭东、郎波、刘超、孙海龙，北京大学谢冰，中国科学院软件所杨叶。

1.2 概述

软件可信性证据是指与软件相关的能够反映其某种可信属性的度量值、文档或其他信息，它是软件可信分级评估（如图 1 所示）的重要组成部分之一，为软件可信等级评定提供直接的依据。

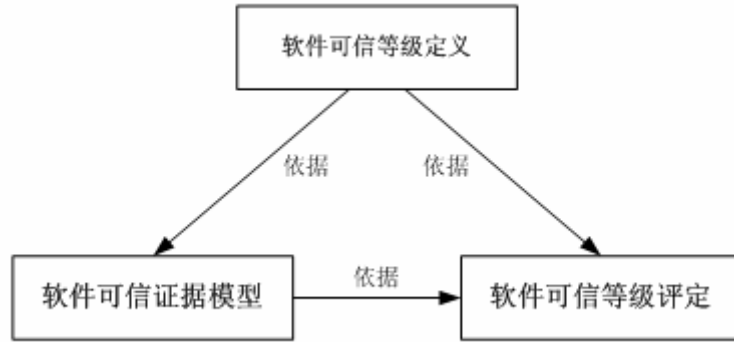


图 1 软件可信分级评估模型

软件可信评估是确定软件可信级别的过程。软件可信评估中，需要针对特定类型的软件，基于用户对该类软件可信性的期望，并依据可信分级的定义，确定该类软件可信性证据模型，利用一定的方法和技术获取软件可信性证据并对可信性证据进行度量，最后依据可信分级定义并依据可信性证据确定软件可信级别。因此，软件可信性证据是进行软件可信分级的基础和前提。

可信性证据可以经过查证确定属实，并能够用来证明软件资源质量真实情况，必须具备以下三个特征：

(1)客观性，即证据是不以人们的意志为转移的客观存在的事实。这是证据的本质特征。

(2)关联性，或称相关性，是指证据和需要证明的质量可信度间有一定的关系或联系。

(3)可获得性，是指证据是可以依照确定的程序收集、审查、判断、获得和检验的。

第2章 范围与引用

2.1 范围

本规范规定了用于评估软件可信性的软件可信性证据所包含的内容、形式及约束条件等，这些证据是软件可信性评估的依据。

本规范适用于软件制品的可信分级，也适用于有需要的组织和个体对目标软件进行可信评估和改进，软件的可信等级取决于所提交的可信性证据。

2.2 引用

下列文件中的有关条款通过引用而成为本标准的条款。凡注日期或版次的引用文件，其后的任何修改（不包括勘误的内容）或修订版都不适用于本标准，但提倡使用本标准的各方探讨使用其最新版本的可能性。凡不注明日期或版次的引用文件，其最新版本适用于本标准。

TRUSTIE 课题组,《软件可信分级参考规范(**TRUSTIE-STC V 2.0**)》 V2.0, 2009 年 6 月。

第3章 软件可信性证据框架

软件资源质量及可信评估证据框架是该机制的核心，这里称其为可信证据框架。软件的可信性是由软件生命周期各个阶段的各种因素所共同决定的，因此这里从软件生命周期的角度定义软件的可信证据框架（如图 2 所示），将可信证据分为开发阶段的证据、提交阶段的证据以及应用阶段的证据。

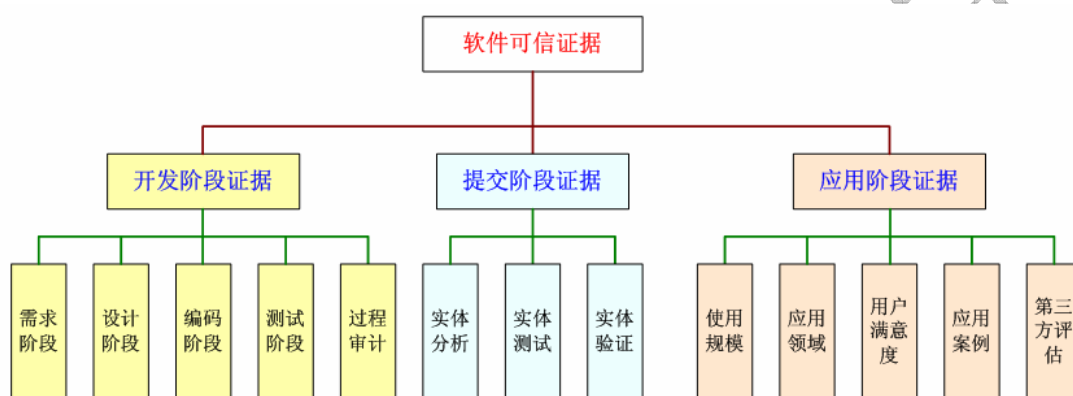


图 2 软件可信证据框架

(1) 开发阶段的证据

软件在开发过程中如何通过规范化的设计、生产和管理流程得到符合设定目标的软件实体的证据。具体包括软件开发中的需求管理、软件设计、软件开发、软件测试与过程审计等阶段的相关信息。

(2) 提交阶段的证据

关注软件提交之后自身可信特性的相关可信证据，主要通过分析、测试和验证工具获得。在软件分析证据方面，主要包括对 C、C++ 以及 JAVA 语言编写的软件进行死锁检测、内存泄漏检测、风格缺陷检测以及其他一般缺陷检测等相关信息。在软件测试方面，包括测试充分度、缺陷残留情况以及软件测试过程及其执行情况等相关的信息。

(3) 应用阶段的证据

关注软件应用广泛程度、用户的评价反馈以及软件提供者的信誉。具体包括使用规模、应用领域、用户满意度、应用案例以及第三方评测论证等信息。

第4章 软件可信性证据项

本章详细阐明了在软件可信性证据框架中所包含的软件开发、提交和应用三个阶段的各个证据项，主要包括证据项的名称、衡量的方法以及约束条件等。软件可信性评估人员基于随同软件提交的各个证据项，对软件的可信性等级进行客观评定。

4.1 开发阶段证据项

分类	证据名称	数据类型	支撑附件	说明
开发阶段	过程管理规范	字符串（300 字符）	软件资源过程管理文档	1) 本证据项取值为本软件资源开发阶段所采用的过程管理规范名称； 2) 所采用的过程管理规范可以是 ISO9000 或 CMMI 等被业界普遍认同的标准或规范，也可以是开发单位自主制定的特定规范。 3) 本软件资源过程管理文档作为附件一并提交
	需求变更数	整型	需求变更记录文档	1) 本证据项取值为软件资源开发阶段需求项增加、删除和修改的总数 2) 需求变更记录作为附件一并提交。
	需求评审结论	字符串（100 字符）	需求评审报告	1) 本证据项取值为需求评审结论简述 2) 需求评审报告作为附件一并提交
	设计方法	字符串（100 字符）		1) 软件资源设计方法的描述
	设计评审结论	字符串（100 字符）	设计评审报告	1) 本证据项取值为设计评审结论简述 2) 设计评审报告作为附件一并提交
	编码规范	字符串（100 字符）	编码规范文档	1) 本证据项取值为编码规范简要说明 2) 编码规范涵盖编码风格规范和异常处理规范 3) 编码规范文档作为附件一并提交。
	测试缺陷趋势	{ 开始时间: 时间型; 结束时间: 时间型; 缺陷密度: 浮点型; }		1) 本证据项取值为的一组描述测试缺陷密度变化趋势的数据，按时间顺序，每个数据为一个三元组，包括开始时间、结束时间和测试缺陷密度。 2) 测试缺陷密度定义为：该时间段内测试发现代码缺陷总数与被测软件实体代码行数的比值。

	缺陷清除率	浮点型		1) 缺陷清除率定义为：软件资源开发阶段已清除的缺陷总数占应清除的缺陷总数的百分比。
--	-------	-----	--	--

4.2 提交阶段证据项

分类	证据名称	数据类型	支撑附件	说明
测试结果	测试类型与结果	{ 测试类型：字符串（20 字符）； 测试结果：字符串（100 字符）； }	测试报告	1) 本证据项取值为的一组关于测试类型及其测试结果的文字描述，包括测试类型描述和对应测试结果描述 2) 测试类型包括功能测试、性能测试、可靠性测试、安全性测试等； 3) 测试结果是对所进行的测试内容和测试结论的简短描述。如功能测试的测试结果可包括对功能测试的覆盖率和正确率的描述。 4) 该证据项源自于软件测试报告，测试报告作为附件一并提交。
	残留缺陷数	整型	测试报告	1) 该证据项是对残留缺陷数的统计值。 2) 残留缺陷列表作为附件一并提交，残留缺陷附件与测试报告可以是同一附件。
测试需求	测试准则	字符串（100字符）	测试报告	1) 该证据项是对测试要求及其依据的简单描述。如：对于安全软件，依据行业标准，必须通过单元测试且语句覆盖和分支覆盖需达到100%等。 2) 该证据项源自于软件测试报告，测试报告作为附件一并提交。
	测试需求	字符串（100字符）	测试报告	1) 该证据项是对测试需求的简单描述。如需通过测试来确认的质量特性。 2) 该证据项源自于软件测试报告，测试报告作为附件一并提交。
测试过程	测试方法	字符串（100字符）	测试报告	1) 该证据项是对所采用测试方法的简单描述 2) 该证据项源自于软件测试报告，测试报告作为附件一并提交。 3) 面向功能组件结构的测试方法：白盒测试、黑箱测试、灰盒测试 4) 面向验证符合设计标准的测试方法：功能测试、性能测试、边界测试、使用界面测试、可用性测试、安全型测试、试用版测试 5) 面向检验覆盖面的测试方法：单元测试、系统测试或集成测试、压力测试、随机任意性测试、全程测试、回归测试、自动化测试
	测试	字符串（100字符）	测试报告	1) 该证据项是对测试组织和测试人员及其测

	人员			<p>试能力等级的描述；</p> <p>2) 该证据项源自于软件测试报告，测试报告作为附件一并提交。</p>
	测试工具	字符串（100字符）	测试报告	<p>1) 该证据项是对采用的测试工具的描述。</p> <p>2) 该证据项源自于软件测试报告，测试报告作为附件一并提交。</p>
	测试环境	字符串（100字符）	测试报告	<p>1) 该证据项是对各种测试环境的描述。</p> <p>2) 该证据项源自于软件测试报告，测试报告作为附件一并提交。</p>
	测试过程记录	字符串（200字符）	测试记录	<p>1) 该证据项是对测试过程追踪和记录的描述。</p> <p>2) 该证据项源自于软件测试记录，测试记录作为附件一并提交。</p>
分析证据	死锁检测	整型	分析报告	<p>1) 本证据项取值为未处理的死锁缺陷数量；</p> <p>2) 死锁缺陷包括同步类缺陷，如死锁；继承类缺陷，如方法重载缺陷；数据流缺陷，如空指针引用等。</p> <p>3) 若有所采用的分析工具生动生成的分析报告，作为附件一并提交</p>
	内存泄漏检测	整型	分析报告	<p>1) 本证据项取值为未处理的内存泄漏缺陷数量；</p> <p>2) 若有所采用的分析工具生动生成的分析报告，作为附件一并提交</p>
	代码风格缺陷检测	整型	分析报告	<p>1) 本证据项取值为未处理的代码风格缺陷个数；</p> <p>2) 若有所采用的分析工具生动生成的分析报告，作为附件一并提交</p>

4.3 使用阶段证据项

分类	证据名称	数据类型	支撑附件	说明
使用阶段	使用规模	整型 或 浮点型	用户使用报告	<p>1) 本证据项取值为资源被不同系统使用的次数或行业占有率。同一目标系统的多个拷贝只计算1次。可以通过用户合同、下载用户、下载次数等确定。</p> <p>2) 若有用户提供的具体使用情况报告，作为附件一并提交</p>
	应用领域	字符串（20字符）		<p>1) 本证据项取值为资源被使用的应用领域名称。应用领域将与相应的可信评估方法有关。此证据可由资源发布者或使用者填写。</p>

	用户满意度	枚举型[很好、较好、中、较差、很差]	用户满意度详细说明	<ol style="list-style-type: none"> 1) 本证据项取值为用户满意度枚举值，可由资源发布者或使用者填写。 2) 若用用户提供的更具体的满意度说明，作为附件一并提交。
	应用案例	字符串（100 字符）	详细应用情况介绍	<ol style="list-style-type: none"> 1) 本证据项是对应用案例的简短描述，可由资源发布者或使用者填写。应用案例应能够反映资源的质量特性，以便可信评估。 2) 若有更为详细应用情况介绍，作为附件一并提交。
	第三方评测论证情况	字符串（100 字符）	第三方评测报告	<ol style="list-style-type: none"> 1) 本证据项是对权威或专业第三方对本软件资源评价信息的简短描述，如关于奖励情况、评测情况、网上排名或被应用次数等的描述。 2) 与第三方评测相关的原始文档（获奖证书、评测报告等），作为附件一并提交。