软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(11):3412−3434 [doi: 10.13328/j.cnki.jos.005291]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

支持软件过程可信评估的可信证据*

王德鑫[1,2,3], 王 青[1,2,3]

[1](中国科学院 软件研究所 互联网软件技术实验室,北京 100190)

[2](中国科学院大学,北京 100190)

[3](计算机科学国家重点实验室(中国科学院 软件研究所),北京 100190)

通讯作者: 王德鑫, E-mail: wangdexin@itechs.iscas.ac.cn; 王青, E-mail: wq@itechs.iscas.ac.cn

摘 要: 近年来,软件可信一直是人们争论的焦点.一种比较共识的观点认为,软件可信是软件行为符合预期的程度.质量形成于过程,显然,建立质量信心的证据也散布于过程.软件开发过程中,主体、行为和各种保障手段则是建立软件可信的基本依据.基于证据的决策和管理是现代质量理论的核心,基于证据、数据驱动的软件工程都是试图从客观数据的角度去解决问题.在国家自然科学基金等计划的支持下,从过程保障的角度提出了软件过程可信度模型,其中,证据作为建立软件可信、支持可信评估的基础要素,是模型非常重要且基础的组成部分.主要研究该模型中的证据体系,遵循完整性、必要性、兼容性和可持续性这 4 项原则,基于过程管理的基本要素,通过调研以及与 CMMI 等软件过程参考模型的对接来提炼、定义和质证模型中的可信证据,使证据具备良好的公信力和可比性;同时,增加了部分目前其他模型都没有涉及的证据来刻画对软件过程的可信增强,从而建立了一个从可信实体、可信行为、可信制品这 3 个目标进行可信保障、并覆盖软件过程全生命周期的证据体系.该证据体系科学、客观并具有良好的公信力,结合可信度模型的其他部分,可以实现基于证据的、自底向上的软件过程可信评估,可供软件组织广泛采用.

关键词: 软件可信;过程可信;证据采信

中图法分类号: TP311

中文引用格式: 王德鑫,王青.支持软件过程可信评估的可信证据.软件学报,2018,29(11):3412−3434. http://www.jos.org.cn/1000-9825/5291.htm

英文引用格式: Wang DX, Wang Q. Trustworthiness evidence supporting evaluation of software process trustworthiness. Ruan Jian Xue Bao/Journal of Software, 2018,29(11):3412−3434 (in Chinese). http://www.jos.org.cn/1000-9825/5291.htm

Trustworthiness Evidence Supporting Evaluation of Software Process Trustworthiness

WANG De-Xin[1,2,3], WANG Qing[1,2,3]

[1](Laboratory for Internet Software Technologies, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[2](University of Chinese Academy of Sciences, Beijing 100190, China,)

[3](State Key Laboratory of Computer Science (Institute of Software, The Chinese Academy of Sciences), Beijing 100190, China)

Abstract: In recent years, software trustworthiness has been a focus of interest for researchers. A more consensus view is that software trustworthiness is the degree of how software behavior is accordant with people's expectation. The quality is formed in the process. Obviously, the evidences that build the confidence of software quality are presented in software process too. The process subjects, behaviors and the various methods to guarantee the quality of process products provide the basic evidences to establish the software trustworthiness. Evidence-based decision-making and management is the core of the modern theories of quality. Thus, both

* 基金项目: 国家自然科学基金(91318301, 91218302, 61432001)
Foundation item: National Natural Science Foundation of China (91318301, 91218302, 61432001)
收稿时间: 2017-01-29; 修改时间: 2017-03-20; 采用时间: 2017-04-12; jos 在线出版时间: 2017-07-12
CNKI 网络优先出版: 2017-07-12 15:35:11, http://kns.cnki.net/kcms/detail/11.2560.TP.20170712.1535.011.html

evidence-based and data-driving software engineering approaches have tried to address the problem from the perspective of objective data. Under the support of national natural science foundation of China, this study presents a software process trustworthiness model for building the confidence from the view of software processes. As the important and fundamental part in the model, evidence is used to transfer the trust chain bottom-up and to support the evaluation of trustworthiness of software process. Focusing on evidence system in the model, this study complies with four principles including integrity, necessity, compatibility and sustainability. According to the basic requirements of process management, it investigates CMMI and other software process reference models to refine and cross-examination the evidences, create some new evidence to adapt open source software development and extend some evidence to enhance the trustworthiness of process. The study develops an evidence system with high credibility, objectiveness and comparability. The presented evidence system can establish the trustworthiness from three dimensions: process subjects, process behaviors and process products. It also covers the whole lifecycle of software development. Combined with other parts of the trustworthiness model, it can support the evidence-based, bottom-up trustworthiness evaluation of software process. The presented model can be widely applied in software industry.

Key words: software trustworthiness; process trustworthiness; credibility for evidence

信息时代,软件应用领域不断扩展,软件产品的规模不断扩大,复杂度也越来越高.人们对软件需求越来越多的同时,对软件质量的容忍度却越来越低.现代质量管理理论强调质量形成于过程,所以,软件是否有可信的质量这个问题日渐困扰着人们.从基本的可信机理讲,软件可信性是主体和客体之间的信任关系,其基本问题主要表现为在特定应用场景下,基于各种手段来进行度量、评估、判定与演化过程,也就是说,需要有证据让用户相信,软件可以满足用户的需要.而这些证据散布于软件开发的整个生命周期,所以软件是否可信不能仅依赖于对最终产品的测试,对软件可信的评估和确认需要软件开发过程中各类相关证据的支持.

针对软件过程的研究,国际上已有 30 多年的历史,在我国也从 21 世纪初开始,有 10 多年的发展历史.目前,国际上与软件过程有关的标准和模型有 ISO 9000[1]和 CMMI[2]系列模型.其中,ISO 9000 是一个面向各个行业的质量管理标准;CMMI 是面向软件相关开发领域的过程成熟度模型,主要针对过程应该做什么的问题.但如何保证过程的行为和制品满足预期的要求,应该采集哪些过程中的证据才能对软件是否可信地满足客户/用户需求做出评价,是已有标准/模型都没有解决的问题.

在国内,近年来软件的可信性也越来越受重视,国家也发布了“可信软件基础研究”重大研究计划.本研究团队在国家自然科学基金和国家高技术研究发展计划(863 计划)的支持下,提出了基于证据的软件过程可信度模型及评估方法[3]以及基于过程可信性度量和改进软件可信性的方法[4].目前,《软件过程及制品可信度评估》标准的制定工作已经在国家标准化管理委员会立项.本文的工作主要是标准前期的技术研究.

我们的研究参考 TSM[5]的 44 个可信原则、CMMI[2]等业界广泛采用的软件过程模型,从现代质量管理的基本元素出发,提出了软件过程可信度模型,从可信实体、可信行为、可信制品这 3 个可信保障目标出发,保障软件过程以及过程制品的可信性.该模型结合软件过程的实践活动特点,建立了 6 类并覆盖整个软件过程生命周期的 36 个过程可信原则以及 1 个覆盖软件生命周期的制品可信原则.

本文的主要工作聚焦于软件过程可信度模型中,支持 36 个过程可信原则的证据的设计和采信.目标是基于软件开发过程中数据所形成的证据,对软件过程和制品的可信程度进行量化、客观、系统的评估.

“采信”一词借鉴于法律界对证据的采信规则,即法院在已经提供的一系列证据中,认定、采用具有证明力和可信度的证据时必需遵循的规则.任何证据只有经过质证,才有可能作为裁判依据.我们通过调研以及和现有公共模型的对接来质证,提炼和定义本模型中的可信证据,使其具备良好的公信力和可比性.

本标准/模型的目的是:从软件过程及制品可信的角度,建立系统化的证据模型,指导软件开发过程中采集合适的证据,支持证据驱动下的软件可信性评价.

本文第 1 节讨论相关研究.第 2 节介绍软件过程可信度模型的相关背景,包括可信原则和可信证据的联系.第 3 节介绍可信证据的含义,包括证据的组成、级别和证据类型.第 4 节重点介绍可信证据的采信质证,包括可信原则与 CMMI 过程域的对应关系、可信证据的设计与制定以及 CMMI 模型未涉及的过程可信证据,并单独介绍高级别的可信证据.第 5 节列举不同等级的可信证据与 CMMI 模型过程域的映射关系.第 6 节讨论和总结

本研究的结论,并提出未来研究工作的展望.

1 相关研究

软件可信的研究主要涉及软件的安全性、可维护性、可靠性等,包括特定领域条件下软件产品的度量和评价技术,以及利用形式化方法和模型验证技术增强软件某一特征的可信度[6],可信计算机国家评估标准(TCSEC)[7]把安全性作为软件可信的唯一标准;Parnas 等人[8]认为,软件可信是利用软件工程技术减少软件失效的能力,包括增强测试、回访和检测技术;而通用标准(CC)[9]提出评价软件安全性的完整框架,并将其作为可信评价的标准来执行.近年来,业界对软件可信的研究主要涉及软件众包和云服务的可信评价体系,以及在实际应用环境下如何保证和改进软件可信.Anurag 等人[10]研究了众包软件开发的可信度,提出了影响众包可信度的因素和风险.Catia 等人[11]实现了一种定位和环境感知系统的可信评价,采用了众包和传感器数据,映射城镇和建筑物的位置关系.Mohammed[12]提出了一种 Cloud Advisor 框架,提供一种基于云提供商的历史数据度量可信度大小.基于云服务的复杂性,Wu 等人[13]提出了一种可信度评价框架,实现可定制的决策支持.基于健康社区中用户共享的知识信息经常出现错误和缺失,Subhabrata 等人[14]提出一种自动化方法,建立用户生成的健康信息的可信度,挖掘医学专家库信息,判断社区用户的可信性.应用该方法能提取社区中关于药品副作用的知识,识别能提供有价值信息的可信用户.在电子商务领域,Neeraj 等人[15]提出了一种动态的声誉计算方法,区别于一般的声誉体系对商家可信度的计算模式,减少失信商家对消费者的危害.基于 FISCAN 在安检设备领域的实践,Li 等人[16]提出一种由软件产品线(SPL)构建的软件可靠性系统体系(srSoS),能够减少因复杂性增大或突发情况而导致的系统可信度问题,在机场安检项目中证明该体系的有效性.在开放的服务市场,软件服务的可信度很难判断,并且大部分服务的选择和协商都不考虑服务的可信程度,Lahiru[17]定义了服务的可信性,通过证据监控和集成量化可信度,在软件服务规范中描述可信的定义,并在服务的选择和协商过程中使用这些定义,从而改进服务的选择和协商过程.代码的缺陷容易导致泄密的产生,为了管理全球数千开发者的代码,Intel 公司[18]开发了一种创新的安全技术,能够允许开发者控制敏感代码和数据的安全性,通过创建应用程序的可信领域来保护软件关键信息,这项技术已经在企业管理、视频会议、金融交易中使用并取得良好的效果.

受传统制造业的启发,研究者提出了面向过程的方法,比如可信软件方法学(TSM)[5]、CMMI[2]以及国际标准 ISO9126[19],关注提高软件开发过程的质量,提高软件的可信性.TSM 是美国国家安全局和其他 3 家机构提出的,用来定义软件可信,提供评价软件可信度的一系列方法.其中,TSM 提出广义上能被接受的 44 个可信原则,提供了开发过程中检测评估软件可信性的指导方法.本文的研究正是基于 TSM 的 44 个可信原则开展的.CMMI 是被业界广泛采用的软件过程管理框架,用软件开发过程的知识技术解决软件管理流程.CMMI 定义了过程管理、项目管理、支持过程和工程过程 4 类供 22 个软件过程域,在每个过程域定义了一组过程实践来支持过程域的实现,并强调通过持续的过程改进来提高产品的质量.CMMI 作为描述和评估软件过程的集成化框架,强调改进软件过程能力,帮助企业对软件工程产品开发过程进行管理和改进,增强开发能力,从而按时地、不超预算地开发出高质量的软件.由于 CMMI 为改进一个组织的各种过程提供了单一的集成化框架,消除了各个模型的不一致性,减少了模型间的重复,增加了透明度,能够总体上改进软件开发组织的质量和效率.

我们对嵌入式软件系统领域的案例[3]进行研究发现,对于一个采用 CMMI ML3~5 进行过程改进的组织,依然有部分可信原则达不到 2 级的要求.这是因为 CMMI 强调过程的可管理性,在大多数 CMMI 的评估中,只观察是否有证据以及是否有弱项,而对证据本身的要求以及证据表现的性能并不关注.比如在开发支持,CMMI 关注足够的资源支持开发活动,但评估时不会强调工具的覆盖范围.但在可信度模型中,则对工具的支持程度有不同的等级要求,以对应不同的可信要求.这也使得很多同样成熟度级别的组织,其过程能力差距其实很大.本模型强调管理的可信性,从实体、行为、制品这 3 个保障目标定义并明确了过程实践应该提供的证据,使得基于本模型的评估更加客观,也具有更好的可比性.此外,本可信度模型在建立可信度要求时,允许用户根据所开发产品的可信要求和失效风险确定过程应该达到的可信等级,而 CMMI 只是依据过程的成熟程度来确定其目标等级,与产品本身的特点无关.也就是说,CMMI 本身并不关注组织的过程应该达到什么等级,CMMI ML5 级的企

业可以只开发普通的民生软件,无需达到较高的可信级别.而开发航空航天软件的企业也可以只达到低级别.

国内近年也开展大量软件可信保障方面的研究,国家自然科学基金委专门部署了软件可信研究的重大计划,国家高技术研究发展计划(863 计划)也部署可信软件开发环境方面的重点课题.吕建院士领导的由南京大学、北京大学、中国科学院软件研究所、国防科技大学以及上海交通大学等研究机构组成的团队,在软件可信的理论方法方面开展了卓有成效的研究.其他很多研究者也开展了大量相关研究,比如,陈火旺等人[20]认为,软件系统的可信性质是指该系统需要满足的关键性质;当软件一旦违背这些关键性质会造成不可容忍的损失时,称这些关键性质为高可信(high confidence)性质;同时,他还强调了形式化方法、需求分析、设计和测试技术以及过程技术在开发和保障高可信软件系统中的重要作用.蔡斯博等人[21]提出了一种支持软件资源可信评估的框架,该框架中包括证据收集、证据信任管理和可信评估等技术.Tan 等人[22]针对软件可信性度量进行了基于属性的研究,他认为,软件的行为及其产生的结果可以用一组属性来表示,软件的可信性也可以通过一组属性以及用户在这组属性上的预期来共同定义.刘旭东等人[23]提出了软件过程可信度框架,认为过程可信可以作为产品可信的重要指证.陈仪香等人[24]提出了一种软件可信的度量模型及分级评价方法,通过航天软件的可信属性来研究软件的可信度和定量分析评价.该航天嵌入式软件可信性度量模型及分级评价方法能够有效评价航天嵌入式软件的可信性,并发现软件产品研制过程中需要加强的部分.陈仪香领导的研究团队基于多维度可信的 4 种度量标准[25]提出了一种新的可信度量模型,给出了一种多项式时间复杂度的组合算法,用于评估基于排序的权重向量.在可信计算方面,林闯等人[26]提出了一种可量化的多目标指标体系,将可信属性分为不同等级,以此建立可信分析模型和服务状态转换模型,在大规模网络环境下,实现多目标优化问题的解决.在开源软件的可信研究领域,王怀民等人[27]提出了一种分层的软件可信分级模型.该模型定义了软件可信属性模型与软件可信等级,建立了软件可信证据参考模型,描述了可信属性、可信等级、可信证据以及可信评价指标之间的内在联系.该软件可信分级模型为建立软件可信评估机制提供了一种有效的方法.在此基础上,王怀民[28]还提出了一种包含生命周期模型、证据模型和演化模型的可信软件模型,基于该模型,设计并应用了可信软件工具和应用环境 TRUSTIE,能够支持国内外开发团队的众包协作.建立软件可信属性模型的基本思想是:以 ISO9126[19]软件质量模型为基础,由可用性、可靠性、安全性、实时性、可维护性和可生存性构成.在我们的可信证据体系[3]中,属于制品可信原则的范畴.基于制品可信原则,我们建立了 108 类制品可信证据,这些可信证据覆盖软件的全生命周期的制品,包括需求、设计、源代码、测试和产品共 5 个阶段,主要源自学术界和产业界目前已经较为广泛采用的度量.制品可信原则和可信证据在本文中不作重点阐述,本文我们主要关注开源软件在开发过程中数据所形成的过程可信证据,提出开源软件的过程可信原则和对应的过程可信证据.

本研究小组从 2005 年开始软件质量管理和保障技术的研究,本文的研究希望从软件过程证据指标的采信过程,保障最终软件产品的可信程度.我们基于国际主流的软件过程模型 CMMI,综合现代软件开发模式的变革等新特征,研究提出了支持 36 个过程可信原则的 133 个可信证据.

2 软件过程可信度模型

本研究团队在国家自然科学基金和国家高技术研究发展计划(863 计划)的支持下,提出了软件过程可信度模型[3],该模型由 36 个过程可信原则和 1 个制品可信原则构成,覆盖软件全生命周期.

其中,软件过程可信原则及保障目标如图 1 所示.

可信原则表示可信的通用要求,依据过程管理人、机、料、法、环这 5 要素,我们以可信保障目标为导向,确定了 6 类可信原则,每类称为一个可信过程域,即实体安全、开发支持、可管理、文档化、可验证和可追溯.每个原则由不同的过程实践活动来实现,这些实践活动被实现的程度,代表了其行为或者结果可信的程度.比如:是否选择了合适的开发工具和方法、工作环境适应开发要求的程度、评审的效力和符合性等.这些实践或者属于软件生命周期的某个阶段的活动,或者是共性支撑活动,跨越整个生命周期.

其中,过程实践即是可信证据的来源.可信原则和可信证据的关系如图 2 所示.

可见,证据是软件过程可信度模型的基本元素,证据结果可以评估可信原则达到的程度,也可以进一步评价

依据本模型的软件过程到达的可信程度.

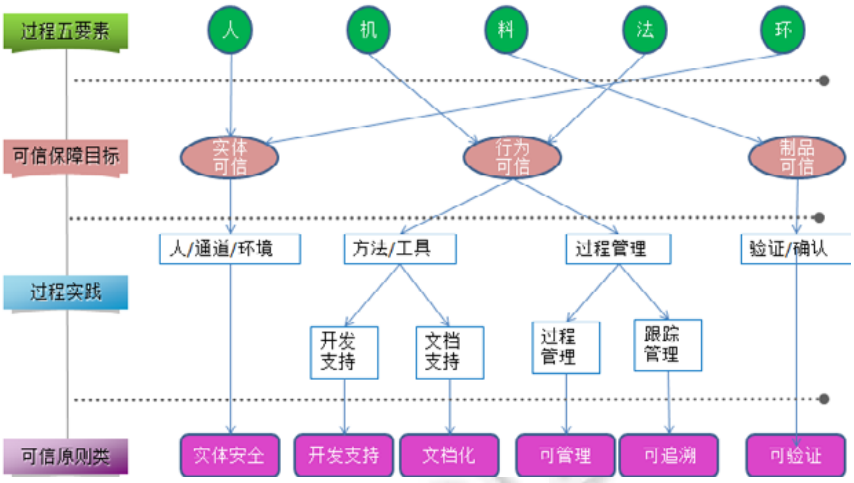

Fig.1 Software process trustworthiness principles and guarantee goals

图 1 软件过程可信原则及保障目标

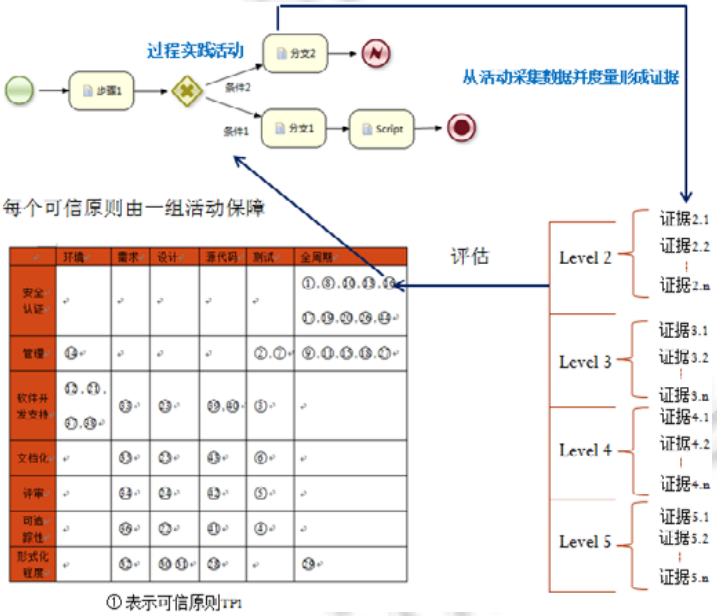

Fig.2 Diagram of trustworthiness principles and evidences

图 2 可信原则和可信证据的关系图

3 可信证据

可信原则由一组可信证据支持,是支持可信原则评估的基础.可信证据既要充分支持对可信原则,进而支持对整个过程的可信评估,也要考虑证据的必要性以及获取证据的成本问题,任何可信性的满足都是以成本为代价的.在本模型中,我们遵循以下原则提炼和定义可信证据,旨在建立一个科学、客观并可广泛采用的证据体系.

(1) 证据的完整性:该原则的目标是保证证据体系可以支撑所有的可信要求,并覆盖软件开发过程的全周期.我们在第 2 节介绍了软件过程可信度模型的结构和基本元素的关系,在前期工作中[3]详细介绍了

可信度模型中可信原则的设计思想和构成.可以看到,我们建立的 6 类可信过程域可以覆盖对可信实体、可信行为、可信制品这 3 类可信保障目标的支持,每个可信域中,可信原则的设计则覆盖了软件开发的全生命周期.每个可信原则由一组可信证据支持,所以这些可信证据的集合是可以完整覆盖全部可信保障目标以及全生命周期的.

(2) 证据的必要性:该原则的目标是保证证据体系建立在较小甚至最小的成本代价上.我们在证据的质证设计中强调证据的来源以及必要性,亦即支撑对应可信原则的最小证据要求.大部分的证据来源于 CMMI 模型[2]的实践要求,因为 CMMI 模型是软件领域最为广泛采用的过程参考模型.另外,在 CMMI 模型中很多过程域都有关联性,我们在 CMMI 实践中和评估中也发现许多证据同时出现在不同的过程域中,增加了评估的工作量和评估结果产生冲突的可能性.因此,我们在设计本模型证据体系时特别关注了关联证据的融合问题,以期减少证据的重复和冗余,并缓解证据间的冲突.

(3) 证据的兼容性:该原则的目标是保证可信度模型与软件领域其他过程模型的兼容性,目的也是旨在减少软件企业在模型采用时的成本.目前,在软件领域主要采用的模型有 CMMI、ISO 9000[1]、ISO 15504[29]等.CMMI 模型从 V1.2 版就开始考虑和 ISO 15504 的融合,而且两个模型的绝大多数实践要求都是一样的.ISO 9000 是应用于所有行业的质量标准,其中并不关注软件领域的具体实践.所以,我们在模型证据体系的设计时主要考虑和 CMMI 模型的兼容.另有实体安全类中的 4 个原则扩充了 CMMI 模型在实体资源的实践要求,明确了对可信实体保障的实践和证据要求.此外,我们还增加了对开源支持可信原则的证据要求.

(4) 证据的可持续性:该原则的目标是保证证据所刻画实践的可信能力,能随着软件过程的改进而提高,以支持持续的改进.我们设计了 5 个级别的证据能力,分别支持可信原则达到的可信程度,表达对活动不同的可信要求:Level 1.表示未达到要求的最低可信级别;Level 2.表示满足基本的有管理的要求;Level 3.表示该证据刻画的实践在管理制度化方面应达到统一的要求和执行;Level 4.表示该证据刻画的实践在量化管理方面的要求和执行;Level 5.表示在持续改进方面的实践要求和执行.部分类型的证据可以通过其能力的提升来支持高级别的可信要求.所有原则下的证据都分在二级至五级的证据级别中,一级没有要求的证据,所有达不到最低级别要求的证据即表明其在一级的能力程度上.此外,并不要求所有的级别中都必须有证据.图 2 表示了可信原则(TP)、实现原则的实践以及证据之间的关系,右边表示的是一个可信原则对应的可信证据结构,其中,证据等级表示该证据从该级开始要求,其满足程度可以不断提高,最高等级大于等于起始级别.

基于以上 4 个原则,本可信度模型建立了软件过程可信的基本要求和支撑证据.此外,本模型的工作作为国家标准的研究工作,模型本身保持开放的结构,以支持吸纳业界相关的经验和成果,使模型本身也保持持续的改进和优化.

基于本模型,我们在软件开发过程中采集相应的数据,并进行度量,即可获得需要的证据,并进一步对软件过程的行为和制品的可信性进行评估.根据证据的实际数据度量得到的证据,表征该证据所刻画的过程行为/实体达到的可信程度.这些基础的证据可以实现量化评估软件的可信性,避免评估人员主观定性判断带来的可信性度量和评估结果不准确不可靠等问题.

下面将基于以上原则,介绍本模型的证据体系.

3.1 可信证据的级别

在模型中,可信证据由相关的度量支撑,表示为定义 1.

定义 1. *Evident*=⟨*Metric*,*T-Level*,*Evident-Type*⟩.

其中,*T-Level* 表示该证据满足的可信级别,从最低 1 级到最高 5 级共分 5 个级别.如前所述,本模型从可信实体、可信行为、可信制品这 3 类目标来保障软件过程和产品的可信性.其中,可信实体和行为均为过程的特征,我们定义为过程证据,主要度量过程的实体和行为是否可信,支持前 36 个可信原则;另一类是制品可信证据,主要度量过程的结果,即制品是否可信,支持第 37 条可信原则.

Evident-Type∈{*Process-Evident*,*Artifact-Evident*},证据类型不同,其度量 *Metric* 的定义不同,本文主要讨论过程证据的相关内容.

过程可信证据对应于 *Process-Evident* 类型,其对应的证据度量定义为定义 2.

定义 2. *Metric*=〈*MName*,*MType*,*Lower-Limit*,*Upper-Limit*,*Performance*〉:*MName* 表示度量元及其表述;*MType* 表示该度量的数据类型;*Lower-Limit* 是该度量适用的最低可信级别,也表示该证据所属的级别;*Upper-Limit* 是该度量可以满足的最高可信级别,当度量值达到最高级别后,亦表示其满足更高级别的可信要求;*Performance* 是该度量的实际值,介于 *Lower-Limit* 和 *Upper-Limit* 之间.

每个证据度量的结果反映了该证据可支持的可信级别,以可信证据“人员对可信知识了解程度”为例:

该证据是一个等级类型的证据,分为 4 级:(1) 不了解;(2) 一般了解;(3) 有专门的培训;(4) 有专业的职业认证资格.该证据支持的可信级别见表 1.我们用 Level 2~Level 5 分别表示该证据从 2 级~5 级的可信等级要求,在下文表格中我们也采用同样的方式表示.

例如,如果要到可信 2 级,该证据对应的程度应该到“2”,亦即一般了解即可;若希望到可信 4 级,则需要有专业的职业认证资格.此外,由于该证据的最高级别 *Upper-Limit* 为 4,当达到 4 级的程度时,也满足可信 5 级的要求.

Table 1 Five levels of trustworthiness requirements of “Degree of People’s Understanding to Trustworthiness”

表 1 可信证据“人员对可信知识了解程度”的 5 级可信要求

可信过程域	可信原则	对应可信证据	证据类型	Level 2	Level 3	Level 4	Level 5
实体安全	安全政策	人员对可信知识了解程度	等级型	2	3	4	

3.2 证据的数据类型

在模型中,过程可信证据的数据类型 *MType* 共有 4 种:布尔型(用字母“B”表示)、等级型(用字母“L”表示)、数值型(用字母“N”表示)和百分比型(用字母“P”表示).

- 布尔型的可信证据

该证据的度量值为“0”或“1”:“0”表示未满足证据要求,“1”表示满足该证据要求.以可信原则“管理制度化”的第 1 个证据 2.1“是否建立管理规程”为例,详见后文表 5.该证据可以表示为

〈是否建立管理规程,B,2,2,Y/N〉.

表明该证据属于 2 级证据,起始和最高级别都是 2 级,实际上对布尔型证据,其起始级别和最高级别相同.

对于布尔型证据,其可信级别的判定如下:

$$T\text{-}Level=\begin{cases}Metric.Lower\text{-}Limit, & \text{if } Metric.Performance=\text{Y}\\ 1, & \text{if } Metric.Performance=\text{N}\end{cases}.$$

对于 2 级布尔型证据,如果满足(Y),则该证据对于 3~5 级的评估也是满足的.同样,3 级、4 级的布尔型证据也支持其高级别的可信评估.

- 等级型的可信证据

它的可信度量值分为若干等级,每一级有具体的满足条件,表 1 即是一个等级型证据,可以表示为

〈人员对可信知识了解程度,L,2,4,1/2/3/4〉.

该证据也是一个二级证据,最高级别为 4 级,度量值可以是 1 到 4 之间的数字.

对于等级型证据,其可信级别的判定如下:

$$T\text{-}Level=\begin{cases}Metric.Performance, & \text{if } Metric.Performance\geqslant Metric.Lower\text{-}Limit\\ 1, & \text{if } Metric.performance<Metric.Lower\text{-}Limit\end{cases}.$$

同样,当等级型证据的度量值达到最高级别(*Upper-Limit*)时,它也支持其更高级别的可信评估.比如表 1 的证据,当 *Performance* 为 4 时,该证据满足 4 级和 5 级的可信要求.

- 数值型的可信证据

数值型证据的度量值是连续或者离散的数值,根据数值的范围划分为不同的区间(interval),表明可信的等

级.以可信证据“代码评审人员的经验”为例,该证据的具体形式见表 2.

Table 2 Trustworthiness evidence of “Experience of Code Reviewer”

表 2 可信证据“代码评审人员的经验”

可信过程域	可信原则	对应可信证据	证据类型	Level 2	Level 3	Level 4	Level 5
可验证	源代码评审	代码评审人员的经验	N	平均≥1 年	2 年≤平均<3 年	平均≥3 年	–

该证据可以表示为

〈代码评审人员的经验,N,2,4,Years〉.

对于数值型证据,其可信级别的判定如下:

$$T\text{-}Level=\begin{cases}Metric.Performance\text{对应的区间级别}, & \text{when } Metric.Performance \text{ fall in Interval}\\ 1, & \text{if } Metric.performance < Minimum\end{cases}.$$

对应上例,如果代码评审人员的平均经验达到 2 年半时间,则表示满足可信等级 3 级的要求;如果代码评审人员的平均经验不到 1 年,则该证据只达到 1 级.

- 百分比型的可信证据

它的可信度量值为百分比,每一级由两个百分比包含的区间表示,以可信证据“遵从测试标准”为例,见表 3.

Table 3 Trustworthiness evidence of “Compliance with Test Standards”

表 3 可信证据“遵从测试标准”

可信过程域	可信原则	对应可信证据	证据类型	Level 2	Level 3	Level 4	Level 5
可验证	测试评审	遵从测试标准	P	60%	80%	90%	95%

该证据可以表示为

〈遵从测试标准,P,2,5,%〉.

对于百分比型证据,其可信级别的判定如下:

$$T\text{-}Level=\begin{cases}1, \text{ if } Metric.Performance < Metric.Lower\text{-}Limit\text{要求的}Minimum\\ 2, \text{ if 2级要求的}Minimum \leqslant Metric.Performance < \text{3级要求的}Minimum\\ 3, \text{ if 3级要求的}Minimum \leqslant Metric.Performance < \text{4级要求的}Minimum \text{ and } Metric.Upper\text{-}Limit > 3\\ 4, \text{ if 4级要求的}Minimum \leqslant Metric.Performance < \text{5级要求的}Minimum \text{ and } Metric.Upper\text{-}Limit > 4\\ 5, \text{ if 5级要求的}Minimum \leqslant Metric.Performance\end{cases}.$$

对应上例,如果测试满足的标准与计划中所有测试标准的比值大于等于 90%且小于 95%,则可信等级满足 4 级要求;如果小于 60%,则只达到 1 级;若大于等于 95%,则满足 5 级.

这里,我们只是举一个例子来说明某个百分比型的可信证据如何确定其可信级别,并非所有这类证据都采用该百分比区间来评价可信级别.一些同行的研究,如陈仪香教授[24]的研究中,提出采用近似黄金分割的比例区间划分可信等级的方式划分软件可信分级,比如认为“低于 70 分的属性个数不超过 3 个且没有低于 45 分的属性”可以认为达到可信 3 级.可以借鉴用于某些多属性数据综合的等级划分,特别是我们模型中制品可信的证据度量.

4 证据的采信质证

证据的采信质证是本模型建立的证据是否具有公信力和客观性的关键.由于 CMMI 模型是目前世界范围内软件企业最广泛的过程模型,CMMI 作为描述和评估软件过程的集成化框架,强调改进软件过程能力,帮助企业对软件工程产品开发过程进行管理和改进,增强开发能力,从而按时地、不超预算地开发出高质量的软件.由于 CMMI 为改进一个组织的各种过程提供了单一的集成化框架,消除各个模型的不一致性,减少模型间的重复,增加透明度,能够总体上改进软件开发组织的质量和效率.但 CMMI 是一个参考模型,主要解决应该做什么的问题.我们在实践中发现很多企业并不知道应该采集什么数据来客观地证明过程实践的有效性,所以很多采用

CMMI 的企业,其过程能力的差异非常大.所以我们在证据的采信质证中,主要参考 CMMI 模型中对过程实践的要求,设计出对应的证据及度量体系,这样不仅质证了本模型证据的采信性,也支持了采用 CMMI 模型组织在采集证据时的客观、公信和可对比能力的建设.

证据来自于过程的实践活动,本模型证据的采信质证过程分 4 步.

(1) 建立可信原则与 CMMI 模型过程域的对应关系;

(2) 从 CMMI 对应的过程域关联的实践中建立过程证据;

(3) 没有 CMMI 对应的可信原则,从文献调研和我们的研究实践中建立过程证据;

(4) 通过调查实证的方法,收集业界对初步建立的可信证据的反馈意见,修正和改进证据体系.

本文的工作主要介绍前 3 步,第 4 步的工作是迭代循环的步骤,我们已经开展过 2 轮先导性调研,但本文限于篇幅,不涉及这部分内容.

4.1 可信原则与CMMI过程域

CMMI 模型[2]共有 22 个过程域(process area,简称 PA),分为 5 个成熟度等级,表 4 详细标注了每个过程域的名称和成熟度等级.CMMI 强调过程管理的制度化和过程的稳定性,希望通过过程的改进不断使得过程稳定,并且在控制下持续改善能力.随着成熟能力的提高,过程量化控制的能力越强.我们研究工作的目标并不在于强调过程的稳定可控,而是过程管理的可信性.稳定的过程在度量分析的能力上具备更好的可信程度,但并不意味在所有的可信要求上都具备更好的可信程度.

Table 4 Twenty-Two process areas of CMMI model

表 4 CMMI 模型的 22 个过程域

等级	过程域(process area)PA
5. 优化级	OPM(organizational performance management:组织性能管理) CAR(causal analysis and resolution:原因分析与解决方案)
4. 量化级	OPP(organizational process performance:组织过程绩效) QPM(quantitative project management:项目定量管理)
3. 定义级	RD(requirement development:需求开发) TS(technical solution:技术解决方案) PI(product integration:产品集成) VER(verification:验证) VAL(validation:确认) OPF(organizational process focus:组织过程焦点) OPD(organizational process definition:组织过程定义) OT(organizational training:组织培训) IPM(integrated project management:集成化项目管理) RSKM(risk management:风险管理) DAR(decision analysis and resolution:决策分析与解决方案)
2. 管理级	REQM(requirement management:需求管理) PP(project planning:项目规划) PMC(project monitoring and control:项目监控) SAM(supplier agreement management:供应商协议管理) MA(measurement and analysis:度量分析) PPQA(Process and Product Quality Assurance:过程和产品质量保证) CM(configuration management:配置管理)
1. 初始级	–

为了叙述简便,下文所有的 22 个过程域 PA 均采用英文首字母简写的方式表示.

可信原则与 CMMI 过程域的对应关系如图 3 所示.

在图 3 中,实心圆点表示可信原则与过程域 PA 存在主要对应关系;而空心圆点表示该可信原则应该涵盖的过程域 PA,但实际并未与其存在主要对应关系.

从图 3 可以看出,只有开源支持这个可信原则在 CMMI 过程域中没有对应,但开源支持在现在软件开发中普遍需要.对于该原则的证据设计,我们将在后面章节介绍.

No	TP \ CMMI PA	OPD	OPF	OPM	OPP	OT	IPM	PMC	PP	QPM	REQM	RSKM	SAM	PI	RD	TS	VAL	VER	CAR	CM	DAR	MA	PPQA
1	安全政策	●				●																	
2	安全管理策略	●				●																	
3	安全环境	●																		●			
4	信息安全工具支持	●																					
5	开发环境工具	●																					
6	重用支持													●	●	●							
7	开源支持																						
8	采购支持												●										
9	需求分析工具														●								
10	设计工具															●		●					
11	源代码分析工具																	●					
12	测试工具																●	●					
13	知识共享	●	●			●																	
14	管理制度化	●		○		●	○		○	○											○		
15	环境完整性	●																					
16	风险管理											●											
17	计划						●		●														
18	度量与分析	●			●					●									●			●	
19	配置管理																			●			
20	过程审计																						●
21	需求分析文档化													●	●					●			
22	设计文档化													●		●				●			
23	源代码文档化													●		●				●			
24	测试文档化													●	●					●			
25	形式化验证要求																●						
26	形式化需求验证																●						
27	需求分析评审																	●					
28	设计评审																	●					
29	形式化设计验证																●						
30	形式化代码验证																●						
31	源代码评审																	●					
32	测试评审																	●					
33	需求可跟踪性							●			●												
34	设计可跟踪性							●			●												
35	源代码可跟踪性							●			●												
36	测试可跟踪性							●			●												

Fig.3 Corresponding relations between trustworthiness principles and process areas of CMMI

图 3 可信原则与 CMMI 过程域的对应关系

4.2 可信证据的设计与制定

可信证据的目的是为其支撑的可信原则提供证据支持.所以,我们的方法是基于可信原则对应的 CMMI 过程域,研究这些过程域下面的实践要求,抽取支持该原则的可信证据.

以“管理制度化”为例,该原则的目标是软件过程应该建立对过程活动管理的程序和要求,包括计划、执行和决策等活动,并要求根据建立的程序要求,由有资格的实体(人员)对软件工程环境、软件工具、软件开发活动进行维护和监督.

由图 3 可见,该可信原则对应的主要 CMMI 过程域是 OPD 和 OT,应该涵盖的过程域有 PP,IPM,QPM,OPM 和 DAR.

基于此,我们为“管理制度化”设计的证据见表 5,包括 4 个 2 级证据和 1 个 3 级证据.

Table 5 Trustworthiness principle of “Management Institutionalization” and the corresponding trustworthiness evidences

表 5 可信原则“管理制度化”和对应可信证据的具体形式

	证据	数据类型	Level 2	Level 3	Level 4	Level 5
2 级证据	2.1. 是否建立管理规程	B	Y	–	–	–
	2.2. 能否明确职责和权限	B	Y	–	–	–
	2.3. 是否开展了培训	B	Y	–	–	–
	2.4. 管理规程的覆盖范围	L	2. 建立项目估算、计划的基本程序	3. 建立了 CMMI ML3 所有 PA 的管理规程	4. 建立了量化管理过程的规程	5. 建立改进组织业务性能的管理规程
3 级证据	3.1. 建立决策过程的管理规程	B	–	Y	–	–

该可信证据和主要对应的 CMMI 过程域实践(SP)的关系见表 6.

Table 6 Corresponding relations between the corresponding evidences with “Management Institutionalization” and the practices of CMMI process areas

表 6 可信原则“管理制度化”对应的可信证据与 CMMI 过程域实践的关系

	CMMIPA	SG1							SG2		
		SP1.1	SP1.2	SP1.3	SP1.4	SP1.5	SP1.6	SP1.7	SP2.1	SP2.2	SP2.3
管理制度化	OPD	建立标准过程	建立生命周期模型	建立裁剪指南	建立度量库	建立资产库	建立工作环境标准	建立团队合作指南	–		
	证据	2.1,2.4,3.1	2.4	2.4	2.4	2.4	2.4	2.2			
	OT	建立培训战略需求	确定组织培训需求	建立培训计划	建立培训能力	–			开展培训	建立培训记录	评价培训效果
	证据								2.3	2.3	2.3

另外,我们选取“度量与分析”可信原则,包含 2 级到 5 级各个级别的可信证据,属于典型的可信原则.该可信原则的目标是对软件过程和制品进行了合适的度量和分析,以准确地理解过程和制品的状态,及时了解过程的偏差,以采取合理的纠正措施.

由图 3 可见,该可信原则对应的主要 CMMI 过程域是 OPD,OPP,QPM,CAR 和 MA.

我们为“度量与分析”设计的证据见表 7,包括 4 个 2 级证据、2 个 3 级证据、2 个 4 级证据以及 1 个 5 级证据.

Table 7 Trustworthiness principle of “Measurement and Analysis” and the corresponding trustworthiness evidences

表 7 可信原则“度量与分析”和对应可信证据的具体形式

	证据	数据类型	Level 2	Level 3	Level 4	Level 5
2 级证据	2.1. 是否建立和度量目标	B	Y	–	–	–
	2.2. 是否建立了相关的度量元、数据采集,以及度量和存储方法	B	Y	–	–	–
	2.3. 度量体系覆盖的程度	L	2. 有度量	3. 在组织级别建立了度量体系	4. 建立了关键过程的性能基线和量化管理的方法	5. 建立原因分析和改进效果评价的度量方法
	2.4. 项目开展度量分析的程度	L	2. 部分项目有度量	3. 全部项目按组织要求进行了度量	–	–
3 级证据	3.1. 度量分析结果在组织级别进行保存和分析	B	–	Y	–	–
	3.2. 有工具支持度量数据的采集、分析和存储	B	–	Y	–	–
4 级证据	4.1. 选择的关键过程控制属性在统计意义上稳定	B	–	–	Y	–
	4.2. 对过程异常进行了分析和改进	B	–	–	Y	–
5 级证据	5.1. 通过量化方法分析过程和产品持续改进的机会	B	–	–	–	Y

该可信证据和主要对应的 CMMI 过程域实践的关系见表 8.

基于此方法,本模型初步建立了 133 个可信证据(包括“开源支持”可信原则以及所对应的可信证据),与主对应 CMMI 过程域 PA 的关系如图 3 所示.

Table 8 Corresponding relations between the corresponding evidences with “Measurement and Analysis” and the practices of CMMI process areas

表 8 可信原则“度量与分析”对应的可信证据与 CMMI 过程域实践的关系

	CMMIPA	SG1					SG2				SG3		
		SP1.1	SP1.2	SP1.3	SP1.4	SP1.5	SP2.1	SP2.2	SP2.3	SP2.4	SP3.1	SP3.2	SP3.3
度量与分析	MA	建立度量目标	建立度量方法	建立数据采集和存储方法	建立分析过程	–	获得数据	分析数据	存储数据和结果	沟通问题	–		
	证据	2.1	2.2, 2.3	2.2,2.3, 3.1,3.2	2.2, 2.3		2.4	2.4	2.4	–			
	OPP	建立质量和过程性能目标	选择过程	建立过程性能度量	分析和建立性能基线	建立过程性能模型	–				–		
	证据	2.3	2.3	2.3	4.1	4.1							
	QPM	建立项目控制目标	组合项目过程	选择要控制的属性	选择度量技术	–	监控所选过程性能	管理项目性能	分析异常原因	–	–		
	证据	2.3	2.3	2.3	2.3		2.4,4.1	4.1	4.2				
	CAR	选择分析目标	分析原因	–			实现改进建议	评价改进效果	记录数据	–	–		
	证据	2.3	5.1				2.4	5.1	2.2				
	OPM	维护业务目标	分析过程性能数据	识别改进机会	–		收集和分析改进	确认改进	选择部署	–	计划改进	管理改进	评价改进效果
	证据	2.3	2.4	5.1			–	–	–		–	–	5.1

4.3 CMMI模型未涉及的过程可信证据

我们提出软件过程可信度模型,是对 CMMI 模型在可信方面的增强[4].可信度模型在可信实体、可信行为和可信制品这 3 个维度上保障软件产品的可信性.其中,CMMI 模型主要关注过程行为方面的成熟能力,可信制品由最后一个可信原则“制品可信”来保障,不在本文介绍的范围.

可信实体的保障则是由“实体安全可信”域的 4 个可信原则来保障.CMMI 模型虽然也包括软件开发实体(实践者)的活动以及工作环境的建立,比如 OPD 中对过程和环境的要求,以及 OT 要求的培训,但关注的主要焦点是工程师的技能是否可以胜任工作、以及人员培训、沟通、协同和承诺等,不能完全覆盖本模型对实体可信的全部要求.

此外,开源软件是当前软件开发组织中最常用到的资源,在 CMMI 模型中也没有专门的关注.

本节主要介绍这几个可信原则的可信证据.

4.3.1 实体安全可信

实体安全可信过程域的目标是保证软件开发主体、权限以及环境、信息通道等实体的可信控制,即通过建立合适的机制,保证软件开发过程的实体遵守可信的安全和管理规范,亦即在可信的环境下,由可信的人员,操作可信的资源开发软件产品.实体安全可信过程域共有 4 个可信原则,全部贯穿软件开发全生命周期,分别是:

- 安全政策:建立有关实体安全相关的政策,并贯彻到所有相关的人员.
- 安全管理策略:建立生命周期活动中与安全相关的管理策略,比如相关活动的执行需要由至少 2 个或 2 个以上有资格的开发人员的认同和参与,聘用人员入职前的背景调查等.

- 安全环境:软件工程环境应该包括一个明确的机制来保证生命周期的活动不会被未授权的方法截获.
- 信息安全工具支持:根据清晰定义的安全策略,所有确定的软件生活周期活动应该有相应的工具支持管理和控制.

实体安全可信域的证据设计见表 9.

Table 9 Evidence design table for trusted domain of “Entity Security”

表 9 实体安全可信域的证据设计表

TP		证据	数据类型	Level 2	Level 3	Level 4	Level 5
安全政策	2 级证据	2.1. 是否建立安全政策	B	Y	–	–	–
		2.2. 人员是否了解安全相关政策	B	Y	–	–	–
	3 级证据	3.1. 是否开展了培训	B	–	Y	–	–
安全管理策略	2 级证据	2.1. 人员入职前是否做过背景调查	B	Y	–	–	–
		2.2. 人员对可信知识了解程度	L	2. 一般了解	3. 有专门的培训	4. 有专业的职业认证资格	–
		2.3. 信息安全管理的程度	L	2. 建立了规程	3. 建立专门的信息安全体系	4. 通过信息安全体系审核	–
		2.4. 项目遵循安全要求的程度	L	2. 遵照执行,但少数有弱项	3. 遵照执行,但多数有弱项	4. 遵照执行,没有弱项	–
	3 级证据	3.1. 是否开展了安全管理相关的培训	B	–	Y	–	–
		3.2. 是否有共享监控机制	B	–	Y	–	–
安全环境	2 级证据	2.1. 是否建立安全工作环境标准	B	Y	–	–	–
		2.2. 是否建立软件过程和资产访问权限和环境	B	Y	–	–	–
		2.3. 网络服务安全性	L	2. 少部分保护	3. 大部分保护	4. 全部保护	–
信息安全工具支持	2 级证据	2.1. 自动化工具对权限控制的支持程度	L	2. 少部分支持	3. 大部分支持	4. 全部支持	–
	3 级证据	3.1. 组织结构对权限支持	B	–	Y	–	–

其中,部分证据与 CMMI 过程实践的对应关系见表 10.

Table 10 Corresponding relations between the trusted domain of “Entity Security” and the practices of CMMI process areas

表 10 实体安全可信域与 CMMI 过程域实践的关系

TP	CMMIPA	SG1							SG2			SG3	
		SP1.1	SP1.2	SP1.3	SP1.4	SP1.5	SP1.6	SP1.7	SP2.1	SP2.2	SP2.3	SP3.1	SP3.2
安全政策	OPD	建立标准过程	建立生命周期模型	建立裁剪指南	建立度量库	建立资产库	建立工作环境标准	建立团队合作指南	–			–	
	证据	2.1	–	–	–	–	–	–					
	OT	建立培训战略需求	确定组织培训需求	建立培训计划	建立培训能力	–			开展培训	建立培训记录	评价培训效果	–	
	证据	–	–	–	–				3.1	3.1	2.2		

Table 10 Corresponding relations between the trusted domain of “Entity Security” and the practices of CMMI process areas (Continued)

表 10 实体安全可信域与 CMMI 过程域实践的关系(续)

TP	CMMIPA	SG1							SG2			SG3	
		SP1.1	SP1.2	SP1.3	SP1.4	SP1.5	SP1.6	SP1.7	SP2.1	SP2.2	SP2.3	SP3.1	SP3.2
安全管理策略	OPD	建立标准过程	建立生命周期模型	建立裁剪指南	建立度量库	建立资产库	建立工作环境标准	建立团队合作指南	–			–	
	证据	2.3	–	–	–	–	–	–					
	OT	建立培训战略需求	确定组织培训需求	建立培训计划	建立培训能力	–			开展培训	建立培训记录	评价培训效果	–	
	证据	–	–	–	–				3.1	3.1	2.2		
安全环境	OPD	建立标准过程	建立生命周期模型	建立裁剪指南	建立度量库	建立资产库	建立工作环境标准	建立团队合作指南	–			–	
	证据	–	–	–	–	–	2.1	–					
	CM	识别配置项	建立配置管理系统	建立和发布基线	–				跟踪变更	控制配置项	–	建立配置管理记录	配置审计
	证据		2.2						2.2	2.2		2.2	2.2
信息安全工具支持	OPD	建立标准过程	建立生命周期模型	建立裁剪指南	建立度量库	建立资产库	建立工作环境标准	建立团队合作指南	–			–	
	证据	–	–	–	–	–	2.1	–					

4.3.2 开源支持

开源改变了软件的开发模式,通过聚集群体智慧的力量打破组织边界,使得创造出更高质量、更安全、更易用的软件成为可能,更重要的是改变了软件的使用方式——从“使用许可”为主的商业模式变成以支持、咨询等面向服务为主的商业模式,在全球向服务经济转型的过程中扮演着日益重要的角色.

经过 30 年的发展,开源软件从已经成功应用于商业、金融、医疗、电子政务、制造、零售、通讯、交通等关乎国计民生的各重要行业,并日益增长.95%的全球 2 000 强企业广泛采用了开源软件的产品和服务.欧盟 FLOSS 项目的《开源对欧盟软件通信产业竞争力和创新的影响》调查报告指出,商业、金融以及通讯传媒是开源软件应用最为广泛的领域,在被调查的欧盟企业中,使用率均超过了 75%,使用开源软件的公共组织更是超过 80%;即使在信息化比较薄弱的医疗领域,也几乎达到了 6 成的使用率.据 Optaros Inc 的调查报告,美国的企业正在积极从使用传统商业软件转向开源软件,在调查的 512 家企业中,87%已经开始使用开源软件,中大型企业更加倾向于选择开软件:被调查的企业中,年收入超过 5 千万美元的企业有 156 家,全部都在使用开源软件.而且,使用的类别并不局限于操作系统(如 Linux),越来越多的关键业务应用软件也在转向开源.

近年来,随着云计算、大数据、移动互联网的迅猛发展,开源软件的地位和作用也不断攀升,给全球 IT 领带来全局性的持续转变,并在 IT 创新和社会基础设施建设方面发挥着愈加重要的引领作用.在使用开源软件的企业中,已经有 45%的企业将开源软件作为其核心关键业务系统的部署和运营环境,开源数据库、Web 服务器和 Linux 服务器是企业使用最为广泛的开源软件,有三分之二都在用 Apache,Tomcat 或者 Linux.以 Android(Linux)智能终端开源操作系统、OpenStack 开源云平台、Hadoop 大数据开源平台等为代表的开源软件在全球蓬勃发展,有关统计显示,全球 90%以上的云计算运行在开源软件基础架构上.

可见,开源支持对软件可信的意义非常重大.我们为该可信原则设计了 4 个 2 级证据、1 个 3 级证据,详见

表 11.

Table 11 Evidence design table for trusted domain of “Open Source Supporting”

表 11 可信原则“开源支持”的证据设计表

	证据	数据类型	Level 2	Level 3	Level 4	Level 5
2 级证据	2.1. 是否对选择开源软件进行过调研	B	Y	–	–	–
	2.2. 对采用开源软件的成本估算	B	Y	–	–	–
	2.3. 开源软件的提供方持续的技术支持	L	2. 没有	3. 一般	4. 强	–
	2.4. 开源软件的质量评价	L	2. 一般	3. 好	4. 很好	–
3 级证据	3.1. 采用开源软件的风险评估	B	–	Y	–	–

在设计可信原则“开源支持”的过程中,2 级证据“2.4 开源软件的质量评价”为等级型证据,从 2 级开始设计了该证据各个可信等级的评价要求.如何判断质量可以参考很多同行,比如国防科技大学王怀民教授[27]的成果,王怀民教授将软件可信级别定义为未知级、可用级、证实级、实用级、评估级和证明级,不同的级别表征软件不同的质量.可用级对应 Level 2,证实级对应 Level 3,实用级以上对应 Level 4.我们未对评估级和证明级做进一步 Level 等级的划分,是因为开源软件本身几乎不可能做评估和证明,而如果采用系统需要高级别,可以在采用系统进行相关验证.

4.4 高级别可信证据

根据我们提出的软件过程可信度评价方法[3],可信原则满足的可信程度取决于其下属的可信证据所表征的可信级别.基于对可信原则满足程度的评估,我们可以进一步评估整个软件过程实现的可信度水平.对软件过程的可信度评估遵循木桶原理,即所有适用的原则必须达到要求的可信级别.因此,在满足 2 级和 3 级可信证据的基础上,为了提高整个软件项目的可信水平,需要关注 4 级和 5 级可信证据在实际中的表现.在模型中,我们共设计了 8 个高级别可信证据,共 5 个 4 级证据和 3 个 5 级证据,这些高等级可信证据的具体内容如下所述.

可管理可信过程域共有 2 个 4 级证据和 1 个 5 级证据涉及度量与分析可信原则,分别是:

- 选择的关键过程控制属性在统计意义上稳定.该证据类型是布尔型,可信等级 4 级及以上为“1”.
- 对过程异常进行了分析和改进.该证据类型是布尔型,可信等级 4 级及以上为“1”.
- 通过量化方法分析过程和产品持续改进的机会.该证据类型是布尔型,可信等级 5 级为“1”.

可验证可信过程域共有 3 个 4 级证据和 1 个 5 级证据,涉及的可信原则有形式化需求验证、形式化设计验证以及形式化代码验证,分别是:

- 是否有形式化需求规约.该证据类型是布尔型,可信等级 4 级及以上为“1”.
- 是否有形式化设计验证.该证据类型是布尔型,可信等级 4 级及以上为“1”.
- 是否有形式化设计规约.该证据类型是布尔型,可信等级 4 级及以上为“1”.
- 是否有形式化代码验证.该证据类型是布尔型,可信等级 5 级为“1”.

可追溯可信过程域共有 1 个 5 级证据,涉及源代码可跟踪性可信原则,即

- 设计到源代码的可追踪程度.该证据类型是布尔型,可信等级 5 级为“1”.

4.5 可信证据集合

最终,我们得到按照可信关键域表示的过程可信证据等级详细的分布情况,见表 12.在 36 个可信原则对应的 133 个过程可信证据中,包括 114 个与 CMMI 模型兼容的可信证据、14 个对 CMMI 模型扩展可信增强的证据以及 5 个支持可信原则“开源支持”的可信证据.

图 4 是不同开发阶段下 6 类可信关键域的证据分布,气泡中的数字表示各类可信关键域对应各个阶段的可信证据数量,其中,可信关键域和阶段的定义来源于我们对软件过程可信度模型的研究[3].由图 4 可见,我们定义的可信证据能够涵盖软件开发的各个环节,在开发支持、文档化、可验证和可追溯 4 类可信关键域,主要关注从软件需求到测试阶段的开发实践中的可信证据,在实体安全域和可管理域,建立了对软件工程环境和全生命周期的可信要求,能够满足软件可信度评价体系对可信证据完整性的要求.

Table 12 Process evidences grade distribution according to trusted critical domain

表 12 按可信关键域分类表示过程证据等级分布

可信关键域	TP	证据等级					可信关键域	TP	证据等级				
		2 级	3 级	4 级	5 级	总计			2 级	3 级	4 级	5 级	总计
实体安全	安全政策	2	1	0	0	3	文档化	需求分析文档化	2	0	0	0	2
	安全管理策略	4	2	0	0	6		设计文档化	2	0	0	0	2
	安全环境	3	0	0	0	3		源代码文档化	2	0	0	0	2
	信息安全工具支持	1	1	0	0	2		测试文档化	5	0	0	0	5
开发支持	开发环境工具	1	2	0	0	3	可验证	形式化验证要求	2	0	0	0	2
	重用支持	4	1	0	0	5		形式化需求验证	2	0	1	0	3
	开源支持	4	1	0	0	5		需求分析评审	4	0	0	0	4
	采购支持	3	0	0	0	3		设计评审	3	0	0	0	3
	需求分析工具	3	0	0	0	3		形式化设计验证	1	0	2	0	3
	设计工具	2	0	0	0	2		形式化代码验证	1	0	0	1	2
	源代码分析工具	3	0	0	0	3		源代码评审	3	0	0	0	3
	测试工具	5	4	0	0	9		测试评审	4	0	0	0	4
可管理	知识共享	2	2	0	0	4	可追溯	需求可跟踪性	1	0	0	0	1
	管理制度化	4	1	0	0	5		设计可跟踪性	2	0	0	0	2
	环境完整性	1	2	0	0	3		源代码可跟踪性	3	0	0	1	4
	风险管理	1	3	0	0	4		测试可跟踪性	3	0	0	0	3
	计划	6	0	0	0	6							
	度量与分析	4	2	2	1	9							
	配置管理	6	0	0	0	6							
	过程审计	4	0	0	0	4							

Fig.4 Distribution of trustworthiness evidences under trusted critical domain and development phase

图 4 可信关键域和阶段维度下的过程可信证据分布

5 可信证据与 CMMI 模型过程域的映射关系

基于上述工作,我们建立了对应 6 类 36 个过程可信原则的 133 个可信证据.图 5 给出了每个 CMMI 过程域对应的可信证据的数量.

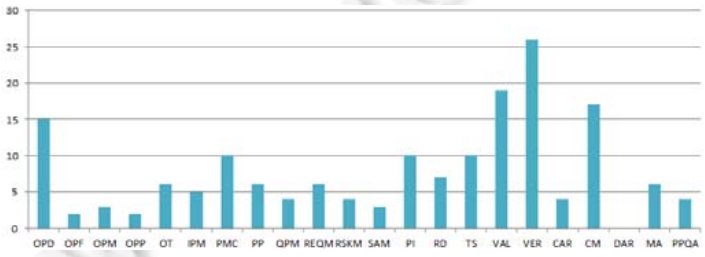

Fig.5 Distribution of trustworthiness evidences under 22 process areas of CMMI

图 5 22 个 CMMI 过程域对应的可信证据的分布

由图 5 可见,DAR 没有 1 个可信证据与其存在主对应关系.但根据图 3 显示,“管理制度化”可信原则应该涵盖的过程域包括 DAR,我们设计的过程可信模型完全涵盖了所有 22 个 CMMI 过程域 PA.

图 6 显示全部可信证据在 4 个可信级别上的分布情况.在下文,我们按照从低可信等级到高可信等级,分别对过程可信证据的分布构成进行详细阐述.

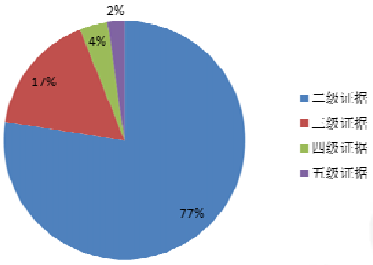

Fig.6 Distribution of all trustworthiness evidences under 4 evidences grades

图 6 全部可信证据在 4 个可信级别上的分布

5.1 2级证据

如前所述,2 级证据表示从可信度 2 级就开始要求的证据,其中等级型、数值型和百分比型证据在高级别要求等级或者度量值相应提高,直到最高等级.

如图 6 所示,本模型共建立 103 个 2 级证据,占全部证据的 77%,覆盖全部可信原则.2 级证据在 CMMI 各个过程域的分布如图 7 所示.

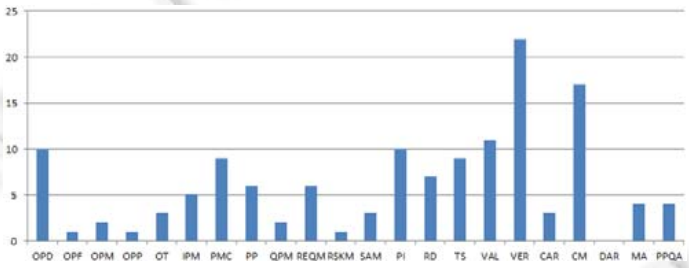

Fig.7 Distribution of trustworthiness evidences of Level 2 under 22 process areas of CMMI

图 7 22 个 CMMI 过程域对应的 2 级证据分布

2 级证据中最高级别为 2 级~5 级的证据分布如图 8 所示.从图 8 我们可以看到,有 57%的 2 级证据延伸到高级别,在高级别起证据要求的数据集性能也是提高的.

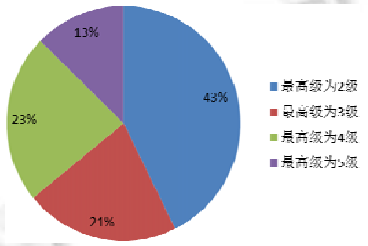

Fig.8 Distribution of trustworthiness evidences of Level 2 with the highest level from Level 2 to Level 5

图 8 2 级证据中最高级别为 2 级~5 级的证据分布

5.2 3级证据

3 级证据表示从可信度 3 级开始要求的证据,其中,等级型、数值型和百分比型证据在高级别要求等级或者度量值相应提高,直到最高等级.

如图 6 所示,本模型共建立 22 个 3 级证据,占全部证据的 17%,分布在 12 个可信原则中.3 级证据在 CMMI 各个过程域的分布如图 9 所示.3 级证据中最高级别为 3 级~5 级的证据分布如图 10 所示.

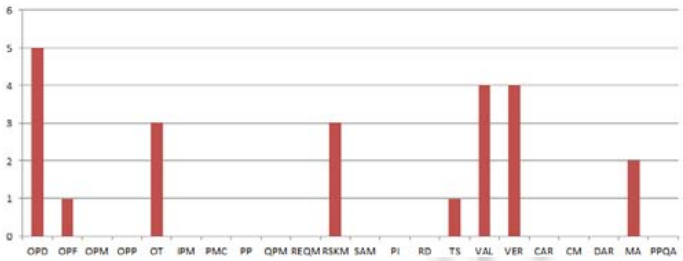

Fig.9 Distribution of trustworthiness evidences of Level 3 under 22 process areas of CMMI

图 9 22 个 CMMI 过程域对应的 3 级证据分布

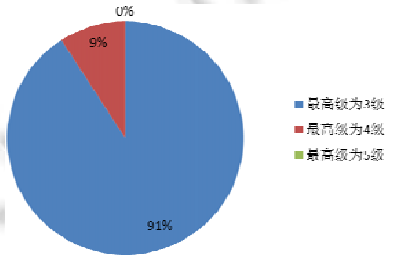

Fig.10 Distribution of trustworthiness evidences of Level 3 with the highest level from Level 3 to Level 5

图 10 3 级证据中最高级别为 3 级~5 级的证据分布

5.3 4级和5级证据

4 级证据表示从可信度 4 级开始要求的证据,其中等级型、数值型和百分比型证据在高级别要求等级或者度量值相应提高,直到最高等级.5 级证据表示从可信度 5 级才开始要求的证据,是最高级别的可信证据.

本模型共建立 5 个 4 级证据,占全部证据的 4%,分布在 3 个可信原则中;共建立 3 个 5 级证据,占全部证据的 2%,分布在 3 个可信原则中.本模型 4 级和 5 级证据在 CMMI 各个过程域的分布如图 11 所示.可以看到,由于 5 级证据“通过量化方法分析过程和产品持续改进的机会”对应 OPM 和 CAR 两个 CMMI 过程域,因此出现 3 个 5 级证据对应 4 个 CMMI 过程域的情况.

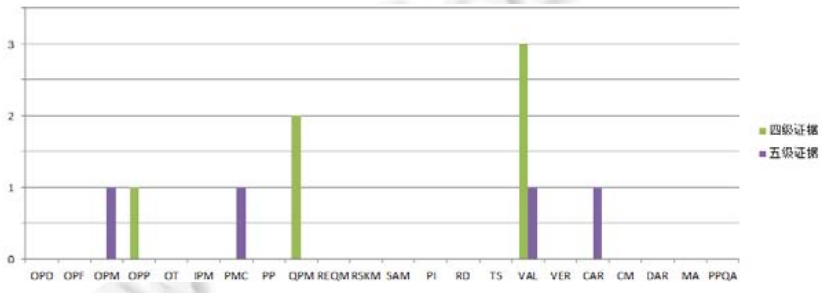

Fig.11 Distribution of trustworthiness evidences of Level 4 and Level 5 under 22 process areas of CMMI

图 11 22 个 CMMI 过程域对应的 4 级和 5 级证据分布

5.4 CMMI成熟度级别对应的可信证据

本节我们从CMMI成熟度级别的角度分析可信证据的分布.图12是CMMI成熟度2级中7个过程域上可信证据的数量和对应的可信域的情况.由图12可见,CMMI成熟度2级一共对应了52个可信证据,覆盖除可验证外的5个可信域,除了配置管理CM之外,其他6个过程域都只对应一个可信域.图13给出了这些证据所属级别,其中,49个是2级证据,占94%;另外还包括2个3级证据和1个5级证据.这说明我们的可信度模型并不限于CMMI的分级模型,在某些可信原则上,综合考虑其能力的持续改进.

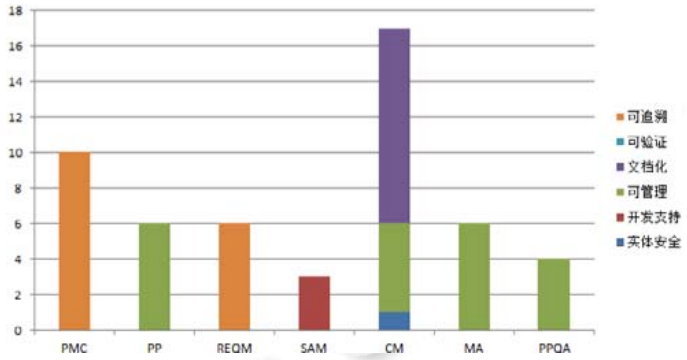

Fig.12 Distribution of trustworthiness evidences in trusted domains under CMMI process areas of Level 2

图12 CMMI成熟度2级过程域上的证据可信域分布

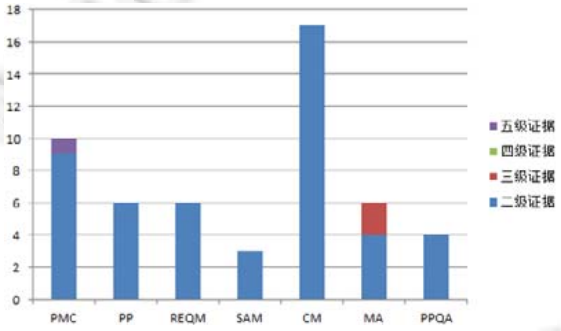

Fig.13 Distribution of trustworthiness evidences in process grades under CMMI process areas of Level 2

图13 CMMI成熟度2级过程域上的证据等级分布

图14和图15是CMMI成熟度3级中,11个过程域上的可信证据分布和对应的可信域情况.

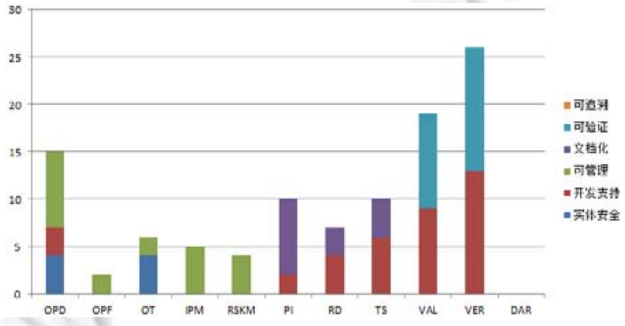

Fig.14 Distribution of trustworthiness evidences in trusted domains under CMMI process areas of Level 3

图14 CMMI成熟度3级过程域上的证据可信域分布

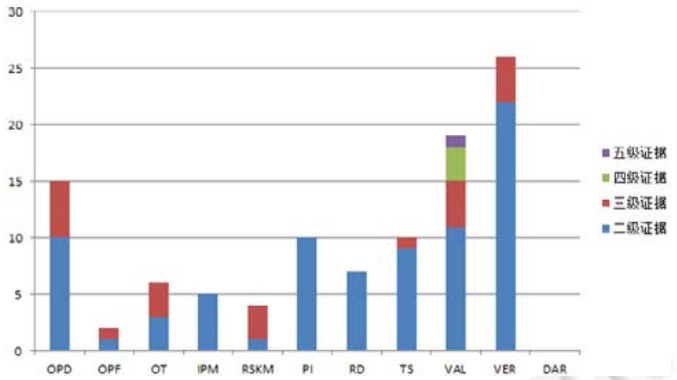

Fig.15 Distribution of trustworthiness evidences in process grades under CMMI process areas of Level 3

图 15 CMMI 成熟度 3 级过程域上的证据等级分布

由图 14 可见,CMMI 3 级过程域上对应的可信证据覆盖了全部可信域,而且大部分过程域都对应到 2 个以上可信域.由图 15 可见,CMMI 成熟度 3 级对应的证据共 104 个,其中有 76%是 2 级证据,20%是 3 级证据,4%是 4 级和 5 级证据.

图 16 和图 17 对应 4 级和 5 级 CMMI 过程域 PA,包括 OPP,QPM,OPM 以及 CAR.

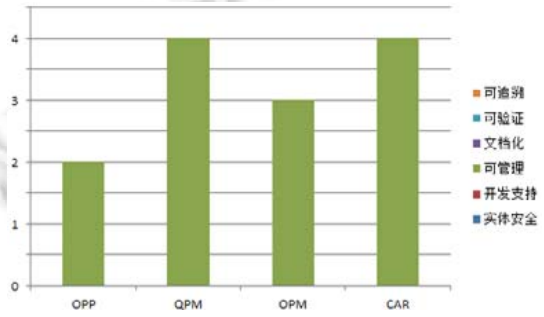

Fig.16 Distribution of trustworthiness evidences in trusted domains under CMMI process areas of Level 4 and Level 5

图 16 CMMI 成熟度 4 级和 5 级过程域上的证据可信域分布

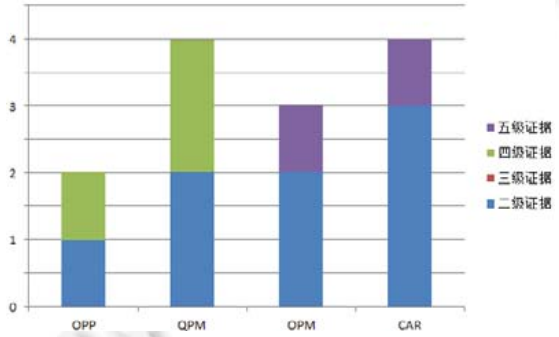

Fig.17 Distribution of trustworthiness evidences in process grades under CMMI process areas of Level 4 and Level 5

图 17 CMMI 成熟度 4 级和 5 级过程域上的证据等级分布

由图 16 可见,4 级和 5 级 CMMI 过程域 PA 全部与可管理可信关键域对应.上文已提到,对软件过程的可信度评估遵循木桶原理,即所有适用的原则必须达到要求的可信级别.因此,为了提高整个软件项目的可信水平,需要关注可管理领域的相关可信证据.而从图 17 可以看出,对应于 CMMI 高级别的过程域,仍然有 61%的可信证据是 2 级证据,这些证据的持续提高,支持了高级别过程域的实现.这也说明了本模型的证据在设计上考虑了过程持续水平渐进的客观情况.

以上分析可见,我们的证据采信质证过程是有效的,采用的证据可以比较全面地反映软件过程的客观实践,证据数据可以证明过程在实体、行为方面的可信程度.基于这些证据,我们可以进行软件过程可信性的评估.

6 总结与讨论

6.1 有效性威胁

本研究模型中,对标的过程证据主要基于 CMMI V1.3[2]和文献调研,我们在对标过程中主要考虑这些证据是否能从标准化的度量体系中证明其存在的准确性和权威性.但证据应用的广泛性尚需进一步验证,证据中采用的可信等级和对应的度量值可能有一定的局限性,这也是本研究目前最主要的弱点.此外,关于证据的裁剪性指南,还需要进一步制定和完善.本文介绍的研究成果已经申请国家标准立项,本文工作主要从技术角度说明证据采用的可行性.下一步,我们将协同其他研究机构、软件企业和评测机构一同讨论和验证本模型证据的有效性,改进和完善标准中的证据,以保证这些证据的客观、公平以及实用性和适用性.

6.2 与现有模型和标准的关系

CMMI 模型[2]是软件企业最广泛采用的过程模型,本文研究工作提取的大部分证据都和 CMMI 要求的实践有关.但 CMMI 关注的是软件开发应该执行的活动,在 CMMI 相关的评估中,也只是验证这个活动执行没有.但执行这些活动应该留下什么证据、哪些证据是合理充分的,需要依据评估师的专业经验去判断.CMMI 将过程域分成 5 个等级,虽然在模型的解释中强调了一些低级别的过程对高级别的支持,但如何支持以及如何评估这些过程达到了高级别的要求,一直是困扰实践者和评估者的问题.ISO 15504[29](软件过程改进和能力确定)是一个和 CMMI 类似并兼容的模型,特别是和 CMMI 的连续模型非常接近.事实上,CMMI 的一些工作一直在考虑和 ISO 15504 的兼容,但该标准在国际上的采用并不多.ISO 9126[19]是一个软件质量标准,给出软件质量的 6 种属性和 20 多个指标,主要关注的是软件产品的质量.我们提出的可信度模型中,支持制品可信原则的证据将和 ISO 9126 有关,本文的过程证据与该标准基本无关.

本模型主要关注软件开发活动中应该留下的证据,并且规范化了这些证据,模型建立的证据覆盖了软件过程的全生命周期,从实体、行为和制品这 3 个维度进行可信保障,同时还建立了证据级别以支持证据所表现的能力和过程可信度的提升.这使得软件组织采用本模型更方便,并可在收集证据、进行评估等方面更加明确和有效.

此外,CMMI 模型是美国卡内基梅隆大学领导研究并制定的,在我国有很多企业采用,但我国迄今为止,但没有一个适用于软件企业的国家标准,这也是我们积极开展本工作的动力.

6.3 未来的研究工作展望

在本文的研究成果基础上,未来我们还将针对以下几项内容进行进一步的工作.

(1) 证据支撑度量指标的完善和优化.软件过程及其制品已经存在大量的度量,事实上,没有绝对适用的度量,大多数组织都是根据自身的特点、成熟能力和过程工程师的知识水平选择偏好的度量.下一步,我们将在更大的范围征求意见和反馈,尽可能建立可以广泛接受的证据度量.

(2) 基于开放式软件的可信度模型和度量体系,对软件的质量属性和可信提出了更高的挑战.目前,虽然我们考虑了开源支持,但对开放环境下软件过程和质量的证据要求、可采集性等还有诸多问题要研究和解决.在保障开放/开源软件可信要求的前提下,如何满足不断发展的开放/开源软件可信性需求的变化,及时调整模型的可信原则和证据体系,使之适应开放/开源的软件开发过程,并支持对开放/开

源环境下的软件可信性进行评估,将是下一步非常有挑战的工作.

总之,信息技术使得社会对软件的需求急剧增长,软件越来越复杂、越来越庞大;而同时,人们对软件质量的要求却越来越高,对质量问题的容忍度越来越低.人们不仅希望软件好用,还希望它安全、可靠、不泄露隐私,要求的质量属性越来越多,可信赖地使用软件已经成为软件社会的重要诉求.所以,系统地建立软件可信的证据,并贯彻到软件开发的生命周期,不仅可以支持软件的相关利益方建立软件的可信信心,还可以帮助开发者改进其过程,以达到可信的要求.

References:

[1] Int'l Standards Organization. ISO 9000. 2015.

[2] CMMI for development, Version 1.3. 2010. http://cmmiinstitute.com/resources/cmmi-development-version-13

[3] Wang DX, Wang Q, He J. Evidence-Based software process trustworthiness model and evaluation method. Ruan Jian Xue Bao/Journal of Software, Ruan Jian Xue Bao/Journal of Software, 2017,28(7):1713−1731 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5102.htm [doi: 10.13328/j.cnki.jos.005102]

[4] Yang Y, Wang Q, Li MS. Process trustworthiness as a capability indicator for measuring and improving software trustworthiness. In: Wang Q, *et al*., eds. Proc. of the ICSP 2009. Heidelberg: Springer-Verlag. 2009. 389−401.

[5] Goertzel KM, Winograd T, McKinley HL, Oh L, Colon M, McGibbon T, Fedchak E, Vienneau R. Software security assurance: A state-of-the-art-report. Technical Report, Herndon, 2007.

[6] Amoroso E, Taylor C, Watson J, Weiss J. A process-oriented methodology for assessing and improving software trustworthiness. In: Proc. of the 2nd ACM Conf. on Computer and Communications Security. Virginia, 1994. 39−50.

[7] Department of Defense, National Computer Security Center. Trusted Computer System Evaluation Criteria. 1985.

[8] Parnas DL, Van Schouwen AJ, Kwan SP. Evaluation of safety-critical software. Communications of the ACM, 1990,33(6): 636−648.

[9] Common criteria portal. http://www.commoncriteriaportal.org/

[10] Dwarakanath A, Shrikanth NC, Abhinav K, Kass A. Trustworthiness in enterprise crowdsourcing: A taxonomy & evidence from data. In: Proc. of the ICSE 2016. Companion, 2016. 41−50.

[11] Prandi C, Mirri S, Salomoni P. Trustworthiness assessment in mapping urban accessibility via sensing and crowdsourcing. In: Proc. of the URB-IOT 2014. 2014. 108−110.

[12] Almanea MIM. Cloud advisor—A framework towards assessing the trustworthiness and transparency of cloud providers. In: Proc. of the 2014 IEEE/ACM 7th Int'l Conf. on Utility and Cloud Computing (UCC 2014). 2014. 1018−1019.

[13] Wu ZP, Zhou Y. Customized cloud service trustworthiness evaluation and comparison using fuzzy neural networks. In: Proc. of the IEEE 40th Annual Computer Software and Applications Conf. (COMPSAC 2016). 2016. 433−442.

[14] Mukherjee S, Weikum G, Danescu-Niculescu-Mizil C. People on drugs: Credibility of user statements in health communities. In: Proc. of the 20th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining (KDD 2014). 2014. 65−74.

[15] Sharma NK, Gaur V, Muttoo SK. A dynamic reputation system with built-in attack resilience to safeguard buyers in e-market. ACM SIGSOFT Software Engineering Notes, 2012,37(4):1−19.

[16] Li D, Yang Y. Enhance value by building trustworthy software-reliant system of systems from software product lines. In: Proc. of the 3rd Int'l Workshop on Product LinE Approaches in Software Engineering (PLEASE 2012). 2012. 13−16.

[17] Gallege LS. TruSSCom: Proposal for trustworthy service representation, selection and negotiation for integrating software systems. In: Proc. of the 2013 Companion Publication for Conf. on Systems, Programming, & Applications: Software for Humanity (SPLASH 2013). 2013. 33−36.

[18] Hoekstra M, Lal R, Pappachan P, Rozas C, Phegade V, Cuvillo JD. Using innovative instructions to create trustworthy software solutions. In: Proc. of the 2nd Int'l Workshop on Hardware and Architectural Support for Security and Privacy (HASP 2013). 2013.

[19] Int'l Standards Organization. ISO 9126. 2001.

[20] Chen HW, Wang J, Dong W. High confidence software engineering technologies. Chinese Journal of Electronics, 2003,31(S1): 1933−1938 (in Chinese with English abstract).

[21] Cai SB, Zou YZ, Shao LS, Xie B, Shao WZ. Framework supporting software assets evaluation on trustworthiness. Ruan Jian Xue Bao/Journal of Software, 2010,21(2):359−372 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3786.htm [doi: 10.3724/SP.J.1001.2010.03786]

[22] Tan T, He M, Yang Y, Wang Q, Li MS. An analysis to understand software trustworthiness. In: Proc. of the 2008 Int'l Symp. on Trusted Computing. 2008. 2366−2371.

[23] Zeng J, Sun HL, Liu XD, Deng T, Huai JP. Dynamic evolution mechanism for trustworthy software based on service composition. Ruan Jian Xue Bao/Journal of Software, 2010,21(2):261−276 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3735.htm [doi: 10.3724/SP.J.1001.2010.03735]

[24] Wang J, Chen YX, Gu B, Guo XY, Wang BH, Jin SY, Xu J, Zhang JY. An approach to measuring and grading software trust for spacecraft software. Scientia Sinica Technologica, 2015,45(2):221−228 (in Chinese with English abstract).

[25] Tao H, Chen YX. A new metric model for trustworthiness of softwares. Telecommunication Systems, 2012,51(2):95−105.

[26] Lin C, Xue C. Multi-Objective evaluation and optimization on trustworthy computing. Science China Information Sciences, 2016, 59(10):No.108102.

[27] Lang B, Liu XD, Wang HM, Xie B, Mao XG. A classification model for software trustworthiness. Journal of Frontiers of Computer Science and Technology, 2010,4(3):231−239 (in Chinese with English abstract).

[28] Wang HM. TRUSTIE: Towards software production based on crowd wisdom. In: Proc. of the 20th Int'l Systems and Software Product Line Conf. (SPLC 2016). 2016. 22−23.

[29] ISO/IEC 15504. 2015. https://en.wikipedia.org/wiki/ISO/IEC_15504

附中文参考文献:

[3] 王德鑫,王青,贺劼.基于证据的软件过程可信度模型及评价方法.软件学报,2017,28(7):1713−1731. http://www.jos.org.cn/1000-9825/5102.htm [doi: 10.13328/j.cnki.jos.005102]

[20] 陈火旺,王戟,董威.高可信软件工程技术.电子学报,2003,31(S1):1933−1938.

[21] 蔡斯博,邹艳珍,邵凌霜,谢冰,邵维忠.一种支持软件资源可信评估的框架.软件学报,2010,21(2):359−372. http://www.jos.org.cn/1000-9825/3786.htm [doi: 10.3724/SP.J.1001.2010.03786]

[23] 曾晋,孙海龙,刘旭东,邓婷,怀进鹏.基于服务组合的可信软件动态演化机制.软件学报,2010,21(2):261−276. http://www.jos.org.cn/1000-9825/3735.htm [doi: 10.3724/SP.J.1001.2010.03735]

[24] 王婧,陈仪香,顾斌,郭向英,王保华,金晟毅,徐建,张居阳.航天嵌入式软件可信性度量方法及应用研究.中国科学:技术科学,2015, 45(2):221−228.

[27] 郎波,刘旭东,王怀民,谢冰,毛晓光.一种软件可信分级模型.计算机科学与探索,2010,4(3):231−239.

王德鑫(1985－),男,山东青岛人,博士,工程师,主要研究领域为可信软件,需求协商,开源社区知识共享.

王青(1964－),女,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为软件过程方法与技术,经验软件工程.