

# ISO9001 与软件工程质量体系

新慧俐 (北京中国科技大学研究生院 100039)

**摘要:**本文在总括介绍了ISO9000质量管理与质量保证系列标准的基础上,对我国软件开发企业适用ISO9001标准进行了研究。

**关键词:**软件工程管理 ISO9000 ISO9001 质量体系 软件开发

## 一、研究背景

软件工程技术的研究与软件工程管理的研究长期以来一直处在一个严重不平衡的状态。软件开发企业的管理水平远远落后于技术水平,软件工程管理和质量保证在长时间内都未能引起人们的足够重视,软件大部分的质量问题都出在管理上。

近年来,国内外对软件工程管理的研究状况大致以两方面为主:(1)各国软件工程师根据本国软件实践经验对软件工程管理进行的总结和研究,其中以美国软件工程研究提出的功能成熟度模型(CMM: Capability Maturity Model)和美、日对软件的全面质量管理的研究为代表;(2)自ISO9000系列国际标准发布以来,就软件企业适用与实施ISO9000系列的研究。

目前,我国软件开发企业在技术上与国外先进的软件开发技术水平差距不大,但在软件产品开发过程依赖技术人员的个人能力,没有系统的项目管理和配置管理,缺乏软件质量保证。

基于上述背景,作者认为:在我国软件行业面临从小型化软件开发到大型化、规模化、商业化的软件开发的发展趋势,为了适应这一趋势对软件开发过程进行控制和提高软件产品质量是极为重要的。而研究ISO9000系列标准对我国软件开发的适用,是迅速提高软件开发企业的软件工程管理水平的有效途径。

## 二、ISO 9000 系列标准的概况

ISO 9000系列标准是有关质量管理和质量保证的标准,包括ISO8402, ISO9000, ISO9001, ISO9002, ISO9003, ISO9004等对质量管理和质量保证的定义、指南或具体模式。本文以适用软件开发企业的ISO9001标准为主要研究对象。

ISO9000起源于硬件产品的质量控制,但同样适用

与软件开发企业(ISO9000-3是对软件产品的质量体系的补充性指南)。ISO9000系列的作用体现为企业内部的管理职能和企业外部的保证职能。

ISO9001从20个方面描述质量体系要素,并通过这些质量体系要素的实施,建立一个文件化、控制化、进行审核与监控、有效的、不断提高的质量体系。这20个方面的质量体系要素是(编号与ISO9001编号一致):

- |                     |                 |            |
|---------------------|-----------------|------------|
| 4.1 管理职责            | 4.2 质量体系        | 4.3 合同评审   |
| 4.4 设计控制            | 4.5 文档控制        | 4.6 采购     |
| 4.7 需方提供产品的控制       | 4.8 产品标识可追溯性    | 4.9 过程控制   |
| 4.10 检验和测试          | 4.11 检验和测试设备的控制 | 4.12 检验和测试 |
| 4.13 不合格产品的控制       | 4.14 纠正和预防措施    |            |
| 4.15 搬运、储存、包装、保管和交付 |                 |            |
| 4.17 内部质量审核         | 4.18 培训         | 4.19 服务    |
| 4.20 统计技术           |                 |            |

上述20个方面相互结合,从三个方面反映了企业质量体系的组织结构。

(1)总体管理要求:包括4.1, 4.2,是对质量体系的建立、控制与评审的结构性的说明;

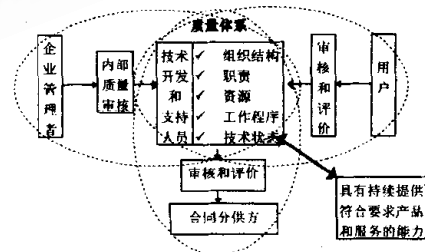


图1 质量体系结构图

(2)专项工业的要求:包括4.3, 4.4, 4.6, 4.7, 4.9, 4.10, 4.11, 4.15, 4.19, 4.20,它们相互联系,每一项工作

要么是其他一些专项工作的输入,要么是另一些专项工作的输出:

(3)支持性要求:包括 4.5, 4.8, 4.12, 4.13, 4.14, 4.16, 4.17, 4.18, 为质量体系要素中专项工作及其他支持性工作一项或多项提供必要的支持。

通过上述这 20 个要素的相互作用而建立的质量体系,充分反映了企业内部对内部质量审核机制和企业外部用户的审核与评价机制;同时也反映了质量体系通过合同分供方的控制,保证外部提供产品的质量。图 1 是对质量体系这几个方面相互关系的综合反映。

### 三、ISO9001 对我国软件开发企业的适用

#### 1. 我国软件开发企业的特点

目前,我国软件开发企业在总体上有以下几个突出的特点:从软件产品的特点上讲,(1)软件产品以用户软件为主,行业化、系统化明显。如银行、税务等大型企业作为计算机用户,为其开发的用户软件适用于整个行业,这一市场是我国软件市场的主流。(2)软件开发企业自行开发的商业软件,市场不充分,商业化不足。从质量上这些软件产品大多数很难和国外的同类先进水平的软件相比,使得商业化市场主要被国外的软件开发公司占据。从企业结构上看,(1)我国软件开发企业以中、小型企业为主,软件开发的组织方式以项目设计组为主;(2)过分重视技术的重要性,而忽视软件管理,使软件开发处于无序或依赖于开发人员的个人水平,管理问题是产生软件产品质量的主要问题。

基于上述特点,在研究我国软件开发企业如何实施 ISO9001 的方面,我们侧重:(1)引进软件机构的开发组织方式,以建立系统化、规范化、全员化的质量体系为根本目标;(2)以专用软件的开发为主要适用范围;(3)结合我国有关软件工程开发和管理的国家标准,并恰当地予以应用。

#### 2. ISO9001 对我国软件开发企业的适用

(1)管理职责。管理职责是质量体系的核心部分,它明确了有关质量体系的质量方针、质量目标、组织结构、岗位职责及资源。

针对软件工程的实施,一个有效的质量体系组织结构应包括:质量管理委员会、软件开发部门、支持部门,分别对企业的质量管理、软件开发及技术与管理支持活动进行规范和控制。由于在实践中往往一个软件公司可能同时开发几个不同的软件项目,分别组成几个软件项目

小组。我们认为,软件项目小组也应由管理、开发、支持三个方面的人员组成,独立工作,相互监督。

(2)质量体系。ISO9001 要求质量体系是文件化的。因此要求质量体系文件能够对质量体系进行全面描述,反映质量方针和质量目标,以及该组织的全部质量活动或有选择的质量活动的内容与程序。ISO9001 下的质量体系文件由三个层次的文件组成:

①质量手册。

②书面的质量体系程序。这两个层次文件均按照 ISO9001 标准进行编写,是对企业质量管理与质量认证的指南。

③其他的质量文件—包括详细的作业文件。三级文件除管理规范或其他保证质量的统一规定外,应充分反映具体软件工程项目的自身特点和要求,是具体的工程指南。编制三级文件时可以参照国家标准《GB8567 计算机软件产品开发文件编制指南》要求。

(3)合同评审。对软件工程来讲,合同评审的核心问题是如何确定在用户规定的限制条件及己方的现有条件下对完成被开发系统软件的把握性。

一般来说,软件系统合同的签订应包括三个阶段:①可行性研究与计划阶段;②投标阶段即需求分析阶段;③合同的评审阶段。

软件产品的合同评审应把握软件产品的自身特点,注意以下几个方面的问题:①需方要求明确并已形成文件;②识别可能出现的意外或风险;③恰当保护有关的专利信息;④解决所有与招标不一致的需求;⑤公司有满足并接受合同要求;⑥双方对软件质量的评定标准与要求;⑦规定合同分供方的工作责任;⑧统一双方对术语的理解;⑨对合同评审的结论应进行记录。特别强调的是需求说明书的制定是本部分工作的重点,也是整个软件开发质量保证的前提(应明确规定需方变更需求的条件和方法)。

(4)设计控制。设计是软件工程的核心,而设计控制的核心是设计结果符合需求或规定要求。对本部分在软件工程中的应用,我们认为可以结合国家标准《GB8566: 计算机软件开发规范》的软件生存周期模型中规定的概要设计、详细设计及实现阶段的活动予以规范。设计活动进行控制是保证软件产品质量的最重要的环节。

软件生存周期的观点从横向对设计程序进行了规定:

①软件的概要设计,确定软件系统的事务处理流程、

软件的总体结构及全局数据结构、输入/输出及安全性控制的全局性规划等;

②软件的详细设计,确定程序模块、存储数据结构、输入/输出数据等详细策划;

③编码与实现,生成源程序代码;

④对软件设计工作进行评审、验证和确认。

(5)文档控制。现代软件工程项目中包括许多不同类型的文档,其中包括来自供方内部的主要技术与管理文档和来自外部的文档。上述文档在使用过程中都会不断地修订,产生多种版本。对它们进行配置管理,在有效标识的基础上,在软件生存周期内控制文档的批准、发布、更改、记录并报告文档配置的状态和更改要求、验证配置项的完全性和正确性及系统的一致性。

(6)采购。本部分是针对软件开发企业从分包商处购买外购品(软件或硬件)时,应注意的问题。对分包商提供的外购品,比如说转包软件,应确认以下二个问题:①分包商开发转包软件的标准与内部软件开发需求的标准基本一致;②分包商开发的转包软件质量达到或满足软件需求。

基于上述目的,供方除了应对合同分供方进行评定外,在采购前对采购文件与需求规定是否一致进行确认;在采购过程中对采购产品进行验证也就同样的重要。

(7)需方提供产品的控制。需方可能向供方提供的产品包括:①软件:部分软件系统或软件开发工具;②文档:如需求规格说明、系统设计说明等;③数据:系统的支持数据或测试数据等;④硬件:设备、工具或与软件系统进行连接的硬件系统。

供方在确定本部分工作时应注意:一是在需求分析阶段,向需方索要其提供的软件产品的相关文档,并对上述文档的可读性与可理解性进行评估;二是在接受需方提供的软件产品后,在待开发系统中使用之前,供方应对其进行测试;三是在对该需方提供的软件产品进行使用的过程中,应对其进行标识;任何有关该软件产品的程序或文档的遗失、损坏或不适用予以记录并及时向需方报告;四是在整个软件系统的运行和维护阶段,考虑到对需方提供产品部分的支持。

(8)产品标识可追溯性。合理的标识方法是良好的配置管理的基础。软件工程实施过程中,产品的标识应当包括对被开发软件系统程序的标识、文档的标识、硬件设备的标识。

软件产品及其文档的标识符应包括:①配置项所属

系统的名称代码及开发过程的代码;②配置项来源的代码(需方、软件转包商、供方);③描述配置项形式的符号(软件程序、文档、硬件);④配置项目条款名称代码;⑤版本号;⑥修订号;⑦检测状态确认符号。

可追溯性的控制是通过有效的产品标识来完成的。软件产品的可追溯性应当从配置的可追溯性和功能的可追溯性两方面理解。前者即为有效的配置管理,后者应通过采用结构化的软件开发方法(如瀑布型方法等)达到功能的正向及反向可追溯性。

(9)过程控制。软件生存周期过程按照国际标准化组织 ISO12207 的划分,包括:获取、供应、操作、维护、开发五个基本过程和支持与组织过程,这七个过程是按照具体实施人为中心建立的。应当提起注意的是,获取过程按软件开发企业的质量体系中应表现为对采购的控制。确定软件开发生存周期过程对软件工程管理是非常重要的。具体过程的确立应根据具体软件工程项目的复杂程度和重要程度确定。过程确立的目的在于帮助软件开发人员明确工作程序、确定工作职责,对软件项目开发计划主要路径上的过程作出标识,并频繁地监督它们的实施。

(10)检验和测试。“测试”在软件工程中是指:用人工或自动的方法来执行和评价系统或系统组成成分的过程,以验证它是否满足规定的需求,或识别出期望的结果和真正结果之间是否存在差异。测试的目的在于发现软件的错误而不是证明程序无错。

一个软件产品是否合格,在其软件开发生存周期过程中应完成三类不同层次的测试:即单元测试、组装测试和确认测试。

(11)检验、测量和试验设备的控制。软件工程的测试工具可能包括:供方自行开发或通用的或某个项目专用的软件测试工具,它们的质量和水平直接关系到被开发软件系统的质量。ISO9001 对设备的校准,在此应理解对上述软件测试工具的检查、测试和确认,保证其处于良好的使用状态。

对软件测试工具的控制可以通过区分测试工具的种类和来源(外购或自行开发)来确定不同的控制手段。如外购的软件测试工具应满足采购产品的验证或需方提供产品的验证的要求;自行开发的软件测试工具需要确定设计、实现和研制测试工具的计划并使该计划与整个目标项目的标准和程序相一致等。

(12)检验和试验状态。确定检验和测试状态的目的在于确定产品的开发过程。

软件工程中,检验是指在软件工程中一般针对如软件需求说明书、软件概要设计书、软件详细设计书、软件测试计划等文档。检验状态则应标明这些文档资料是否已经送审,以及在相应的技术评审中是否无错、存在小的可立即被更正的错误、存在重大错误需更改后重新评审等状态。测试在软件工程中针对模块的单元测试、组装测试和确认测试。一个软件的程序编码处在什么样的测试阶段以及在本阶段中的测试结果反映了它的测试状态。

(13)不合格产品的控制。软件工程中不合格品是指那些不符合要求或经检验和测试不能达到要求的程序代码或文档资料。它可能包括:未经测试的模块、经评审发现有错误的设计、被用户发现有问题的系统等。

软件缺陷可能会出现于开发期或运行过程中。如果在软件开发期发现软件缺陷,应通过确定合格/不合格的评定标准,并对评定为缺陷软件产品进行标识,作出修改或重新开发等处理意见。只有最终通过了软件全部软件测试的产品方可交付需方。如果软件缺陷是在交付需方后的软件运行过程中发现的,应执行软件的维护程序。

(14)纠正和预防措施。软件工程中,纠正和预防措施是指在测试阶段和维护阶段中软件开发人员发现了可导致产品不合格的问题时应采取的措施。

软件工程中发现产品不合格的来源大致包括:①来自软件开发/支持人员或软件用户的投诉;②软件测试结果;③在软件维护阶段对软件进行功能扩充或性能改进的过程。

软件开发企业应确定故障分析和故障反馈的标准,以保证对发现的问题进行及时的纠正,对可能产生的问题进行预防。

(15)搬运、储存、包装、保管和交付。本部分在软件工程中主要实施的是对储存、保管和交付的要求。

软件产品的储存是通过建立软件配置管理库来实现的,它包含了主要的项目文档和所有的程序代码。并有专人负责对软件配置管理库的写入;一般的软件开发人员在软件被送入配置管理库冻结之后,只有权读出而无权写入。

磁盘文件的保存,软件配置管理库的管理人员应注意定期对软件进行备份,并通过软件比较工具确定新、旧版本的软件。防止计算机病毒及其他人为的破坏行为。

交付是指供方将开发好的经过确认的软件产品交付需方,并根据需方要求进行系统安装与调试的过程。

(16)质量记录的控制。质量记录是提供满足质量要

求的程度的客观证据或一个质量体系要素运行效果的证据。对质量记录予以控制的目的在于证实、追溯、预防和纠正。

(17)内部质量审核。内部质量审核应包括对质量体系、产品质量和过程质量三个方面的审核。并由独立于被评审对象的质量保证人员对评审。其中产品质量审核按对完成的软件质量的要求进行。审核依据是对特定软件产品的检验和测试结果以及产品度量的结果。过程质量审核根据过程的要求进行,适用于软件生存周期全过程。审核的依据是过程度量的结果。

证审的目的包括:①有效性的确认;②改进过程的实施;③是否满足标准及程序文件的要求。

(18)培训。由于计算机技术处于一个日新月异的阶段,对进行软件开发和管理的人员进行特定领域知识的培训是非常必要的。

(19)服务。软件产品的服务以售后服务为主。包括:①软件的安装与调试;②软件系统使用的培训;③软件运行中的维护。其中软件运行中的维护是重点。

软件系统的维护包括三个方面的内容:一是对被开发的软件系统错误的更改;二是由需求变更引起的系统更改;三是增加系统功能。

(20)统计技术。软件工程的统计技术主要是指针对软件产品的某项特性进行的软件度量,包括产品度量和过程度量两个方面。软件的产品度量主要是针对于软件程序和文档的功能性、可靠性、易用性、高效性、可维护性和可移植性进行量化评价。软件的过程度量主要是针对软件开发过程和交付过程是否达到规定的阶段要求和质量目标进行量化评价。

#### 主要参考资料

- [1] ISO8402 - 1994 质量管理和质量保证—术语
- [2] ISO9000 - 3:1991 质量管理和质量保证标准 第三部分:ISO9001 在软件开发、支持和维护中应用指南
- [3] ISO9001:1994 质量体系—设计、开发、生产、安装和服务的质量保证模式
- [4] Darrel Ince; ISO 9001 and Software Quality Assurance, McGraw - Hill International (UK) Limited, 1994
- [5] Charles H. Schmauch; ISO 9000 for Software Developers, ASQC Quality Press, 1994

(来稿时间:1997年4月)