



中华人民共和国国家标准

GB/T 19000.3—2001
idt ISO 9000-3:1997

质量管理和质量保证标准 第3部分：GB/T 19001—1994 在计算机软件开发、供应、安装 和维护中的使用指南

Quality management and quality assurance standards—
Part 3: Guidelines for the application of GB/T 19001—1994
to the development, supply, installation
and maintenance of computer software

2001-02-13 发布

2001-10-01 实施



国家质量技术监督局 发布

中华人民共和国
国家标准
质量管理和质量保证标准
第3部分:GB/T 19001—1994
在计算机软件开发、供应、安装
和维护中的使用指南
GB/T 19000.3—2001

*

中国标准出版社出版
北京复兴门外三里河北街16号
邮政编码:100045

电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷
新华书店北京发行所发行 各地新华书店经营

*

开本 880×1230 1/16 印张 2¼ 字数 57 千字
2001年6月第一版 2001年6月第一次印刷
印数 1—10 000

*

书号:155066·1-17647 定价 16.00 元

网址 www.bzcbs.com

*

科目 570—494

版权专有 侵权必究
举报电话:(010)68533533

前 言

本标准等同采用国际标准 ISO 9000-3:1997《质量管理和质量保证标准——第3部分:ISO 9001:1994 在计算机软件开发、供应、安装和维护中的使用指南》。

本标准是 GB/T 19000 族标准的组成部分,并与其保持一致。

本标准对 GB/T 19000.3—1994(idt ISO 9000-3:1993)做了技术性修订,主要技术内容变化如下:

1) 编辑格式

老版本是按照软件生存周期的模式,将质量体系要求分成三部分,即:质量体系——框架、质量体系——生存周期活动、质量体系——支持活动,分成 23 项质量要求;修订后按照 GB/T 19001—1994 的 20 个要素编辑。

2) 在内容上进行了较大的调整和补充

主要表现在软件的设计和开发活动大部分通过 4.4 条“设计控制”要素来实现,另外在 4.3.2 条增加了软件的知识产权保护和许可制度,在 4.4.2 条中增加了防病毒控制等等。

本标准的附录 A 为标准的附录,附录 B 为提示的附录。

本标准自实施之日起代替 GB/T 19000.3—1994。

本标准由中国标准研究中心提出。

本标准由全国质量管理和质量保证标准化技术委员会归口。

本标准由中国标准研究中心负责起草。

本标准主要起草单位:中国标准研究中心、航天总公司二院 204 所、北京航空航天大学、亚信科技(中国)有限公司、信息产业部四所。

本标准主要起草人:咸奎桐、王伟、蔡开元、刘江鹰、刘辉。

本标准首次发布是 1994 年,2000 年第一次修订。

ISO 前言

国际标准化组织(ISO)是由各国标准化团体(ISO 成员团体)组成的世界性的联合会,制定国际标准的工作通常由 ISO 的技术委员会完成,各成员团体若对某技术委员会已确立的标准项目感兴趣,均有权参加该委员会的工作。与 ISO 保持联系的各国际组织(官方的或非官方的)也可参加有关工作。在电工技术标准化方面,ISO 与国际电工委员会(IEC)保持密切合作关系。

由技术委员会正式通过的国际标准草案提交各成员国表决,国际标准需取得至少 75% 参加表决的成员团体的同意才能正式通过。

国际标准 ISO 9000-3 由 ISO/TC 176/SC 2 质量管理 and 质量保证技术委员会质量体系分委员会制定的。

本版本对第一版(ISO 9000-3:1991)做了技术性修订,以取代第一版。

ISO 9000 的总标题是:质量管理和质量保证标准,由以下部分组成:

- 第 1 部分:选择和使用指南;
- 第 2 部分:ISO 9001、ISO 9002 和 ISO 9003 的实施通用指南;
- 第 3 部分:ISO 9001:1994 在计算机软件开发、供应、安装和维护中的使用指南;
- 第 4 部分:可信性大纲管理指南。

本标准的附录 A 和附录 B 仅供参考。

引 言

本标准是为承担计算机软件设计、开发、安装和维护等业务的供方使用 GB/T 19001—1994 提供指南,该软件可以:

- a) 作为对外签定商务合同的一部分;
- b) 作为市售产品;
- c) 支持供方的业务过程;
- d) 作为嵌入硬件产品中的软件。

本标准指出需要涉及的问题,而与供方采用的技术、生存周期模型、开发过程、活动顺序或组织结构无关。

当组织的活动范围包括计算机软件开发以外的其他领域时,该组织的质量体系中计算机软件要素与其他领域的要素之间的关系应明确说明,以形成一个完整的质量体系。

本标准是为使用 GB/T 19001—1994 提供指南,在引用 GB/T 19001—1994 原文的地方加上了方框,以便于识别。

本标准自始至终用“应”(shall)表示对双方或多方均具有约束力的规定;用“希望或愿意”(will)表示一方的目的声明或意向;用“最好”、“建议”、“宜”(should)表示在诸多可能性中的一种推荐建议;用“可以”(may)指明在本标准限制下允许的作法。

目 次

前言	Ⅲ
ISO 前言	Ⅳ
引言	V
1 范围	1
2 引用标准	1
3 定义	1
4 质量体系要求	2
4.1 管理职责	2
4.2 质量体系	3
4.3 合同评审	4
4.4 设计控制	6
4.5 文件和资料控制	11
4.6 采购	12
4.7 顾客提供产品的控制	13
4.8 产品标识和可追溯性	13
4.9 过程控制	14
4.10 检验和试验	15
4.11 检验、测量和试验设备的控制	18
4.12 检验和试验状态	18
4.13 不合格品的控制	19
4.14 纠正和预防措施	19
4.15 搬运、贮存、包装、防护和交付	20
4.16 质量记录的控制	21
4.17 内部质量审核	22
4.18 培训	22
4.19 服务	22
4.20 统计技术	23
附录 A(标准的附录) 参考文献	25
附录 B(提示的附录) 与 ISO/IEC 12207:1995 的对照索引表	25

中华人民共和国国家标准

质量管理和质量保证标准
第3部分:GB/T 19001—1994
在计算机软件开发、供应、安装
和维护中的使用指南

GB/T 19000.3—2001
idt ISO 9000-3:1997

代替 GB/T 19000.3—1994

Quality management and quality assurance standards—
Part 3: Guidelines for the application of GB/T 19001—1994
to the development, supply, installation
and maintenance of computer software

1 范围

本标准是为承担计算机软件开发、供应、安装和维护的组织使用 GB/T 19001—1994 提供指南,本标准并未增加或改变 GB/T 19001—1994 的要求。

本标准不用作质量体系认证和(或)注册的评定准则。

2 引用标准

下列标准中所包含的条文,通过在本标准中引用而构成为本标准的条文。本标准出版时,所示版本均为有效。所有标准都会被修订,使用本标准各方应探讨使用下列标准的最新版本的可能性。

GB/T 6583—1994 质量管理和质量保证 术语(idt ISO 8402:1994)

GB/T 19001—1994 质量体系 设计、开发、生产、安装和服务的质量保证模式
(idt ISO 9001:1994)

3 定义

本标准采用 GB/T 6583 的定义及下述定义。

3.1 产品 product

活动或过程的结果。

注1:产品可以包括服务、硬件、流程性材料、软件或它们的组合。

注2:产品可以有形的(如组件或流程性材料),也可以是无形的(如知识或概念)或是它们的组合。

注3:本标准中“产品”这一术语,仅适用于期望提供的产品,而不是影响环境的非期望的“副产品”,这不同于 GB/T 6583 中的定义。

[GB/T 19001—1994]

3.2 投标 tender

供方应邀作出提供满足合同要求产品的报盘。

[GB/T 19001—1994]

3.3 合同 contract

供方和顾客之间以任何方式传递的、双方同意的要求。

[GB/T 19001—1994]

3.4 基线 baseline

经正式批准的某个配置项的一个版本,该版本在其生存周期内的某一特定时间被正式标明和确定,不论何种介质的载体。

[ISO/IEC 12207:1995]

3.5 开发 development

一个软件的生存周期过程,它由下列活动组成:软件产品的需求分析、设计、编码、集成、测试、安装和验收支持。

3.6 生存周期模型 life cycle model

从确定需求开始的到停止使用终止,系统的整个生存周期,包含与软件产品的开发、运行和维护有关的过程、活动和任务的框架。

[ISO/IEC 12207:1995]

3.7 阶段 phase

规定的工作部分。

注:阶段并不针对任何特定的生存周期模型。

3.8 回归测试 regression testing

为了确定纠正缺陷所作的更改未引起派生缺陷所进行的测试。

3.9 复制 replication

将软件产品从一个载体拷贝到另一载体。

3.10 软件 software

见软件产品(3.11)

注:本标准中的术语“软件”只限于计算机软件。

3.11 软件产品 software product

整套的计算机程序、规程以及可能的与其相关的文档和数据。

[ISO/IEC 12207:1995]

注:软件产品可以是指定用于交付的产品、另一产品的组成部分或在开发过程中使用的产品。

3.12 软件项 software item

软件产品的任何可标识的部分。

4 质量体系要求

4.1 管理职责

4.1.1 质量方针

负有执行职责的供方管理者,应规定质量方针,包括质量目标和对质量的承诺,并形成文件,质量方针应体现供方组织的目标以及顾客的期望和需求。供方应确保其各级人员都理解质量方针,并坚持贯彻执行。

没有与软件有关的进一步指南。

4.1.2 组织

4.1.2.1 职责和权限

对从事与质量有关工作的管理、执行和验证的人员,特别是对需要独立行使权力开展以下工作的人员,应规定其职责、权限和相互关系,并形成文件:

- a) 采取措施,防止出现与产品、过程和质量体系有关的不合格;
- b) 确认和记录与产品、过程和质量体系有关的问题;
- c) 通过规定的渠道,采取、推荐或提出解决办法;
- d) 验证解决办法的实施效果;
- e) 控制不合格品的进一步加工、交付或安装,直至缺陷或不满足要求的情况得到纠正。

没有与软件有关的进一步指南。

4.1.2.2 资源

对管理、执行工作和验证活动(包括内部质量审核),供方应确定资源要求并提供充分的资源,包括委派经过培训的人员(见 4.18)。

没有与软件有关的进一步指南。

注:进一步的信息见 ISO/IEC 12207:1995 的 7.2 条。

4.1.2.3 管理者代表

负有执行职责的供方管理者,应在自己的管理层中指定一名成员为管理者代表,不论其在其他方面职责如何,应明确权限,以便:

- a) 确保按照本标准的要求建立、实施和保持质量体系;
- b) 向供方管理者报告质量体系的运行情况,以供评审和作为质量体系改进的基础。

注 5: 管理者代表的职责还可包括就供方质量体系有关事宜与外部各方的联络工作。

没有与软件有关的进一步指南。

注:进一步的信息见 ISO/IEC 12207:1995 的 6.3.1.6 条。

4.1.3 管理评审

负有执行职责的供方管理者,应按规定时间的间隔对质量体系进行评审,确保持续的适宜性和有效性,以满足本标准的要求和供方规定的质量方针和目标(见 4.1.1)。评审记录应予以保存(见 4.16)。

没有与软件有关的进一步指南。

注:进一步的信息见 ISO/IEC 12207:1995 的 7.1.4 条。

4.2 质量体系

4.2.1 总则

供方应建立质量体系,形成文件并加以保持,作为确保产品符合规定要求的一种手段,供方应编制覆盖本标准的质量手册,质量手册应包括或引用质量体系程序,并概述质量体系文件的结构。

注 6: ISO 10013 提供了质量手册的编制指南。

没有与软件有关的进一步指南。

4.2.2 质量体系程序

供方应:

- a) 编制与本标准要求和供方规定的质量方针相一致的形成文件的程序;
- b) 有效地实施质量体系及其形成文件的程序。

基于本标准的目的,作为质量体系一部分的质量体系程序,其范围和详略程度应取决于工作的复杂程度、所用的方法,以及开展这项活动涉及的人员所需的技能和培训。

注 7: 形成文件的程序可以引用规定某项活动如何进行的作业指导书。

没有与软件有关的进一步指南。

4.2.3 质量策划

供方应对如何满足质量要求作出规定,并形成文件。质量策划应与供方质量体系的所有其他要求相一致,并形成适于供方操作的文件。为满足产品、项目或合同规定的要求,供方应适当考虑下述活动:

- a) 编制质量计划;
- b) 确定和配备必要的控制手段、过程、设备(包括检验和试验设备)工艺装备、资源和技能,以达到所要求的质量;
- c) 确保设计、生产过程、安装、服务、检验和试验程序和有关文件的相容性;
- d) 必要时,更新质量控制,检验和试验技术,包括研制新的测试设备;
- e) 确定所有测量要求,包括超出现有水平,但在足够时限内能开发的测量能力;
- f) 确定在产品形成适当阶段的合适的验证;
- g) 对所有特性和要求,包括含有主观因素的特性和要求,明确接收标准;
- h) 确定和准备质量记录(见 4.16)

注 8: 4.2.3a)提及的质量计划可以采取引用相应的形成文件的程序的方式,这些程序构成供方质量体系的一个部分。

适当时,质量计划应描述下列内容:

- a) 可行时,用可测量的方式表达的质量要求;
- b) 软件开发过程中采用的生存周期模型;
- c) 规定每一项目阶段启动和结束的准则;
- d) 明确要执行的评审、测试以及其他验证和确认活动的类型;
- e) 明确要执行的配置管理程序;
- f) 针对下列各项制定详细计划(包括进度安排、程序、资源和批准)及具体职责和权限:
 - 配置管理;
 - 开发产品的验证和确认;
 - 采购产品的验证和确认;
 - 顾客提供产品的验证;
 - 不合格品的控制和纠正措施;
 - 确保在质量计划中规定的各项活动得到执行。

质量计划提供将质量体系应用于特定的项目、产品或合同剪裁方法。

适当时,质量计划可以包括或引用通用的程序和(或)项目/产品/合同特定的程序。质量计划应根据开发进展情况加以更新,当每个阶段开始时,与该阶段有关的事项都应完全确定。

质量计划应由所有与计划实施相关的组织的评审并取得一致意见。

描述质量计划的文件可以是独立的文件(加以质量计划标题)或作为另一文件的一部分,或由几个文件组成。

质量计划可以包括或引用单元测试、集成测试、系统测试和验收测试的计划,测试策划和测试环境的指南是检验和试验的一部分。

注: GB/T 19015 提供了质量计划的指南,GB/T 19017 提供了配置管理指南,进一步的信息见 ISO/IEC 12207:1995 的 6.2~6.5 条。

4.3 合同评审

4.3.1 总则

供方应建立并保持合同评审和协调合同评审活动的形成文件的程序。

软件可以作为合同的一部分、作为进入市场销售的产品、作为硬件产品中嵌入的软件或作为供方业务过程的支撑软件而开发。合同评审适用于所有这些情况。

4.3.2 评审

在投标或接受合同或订单(对要求的说明)之前,供方应对标书、合同或订单进行评审,以确保:

- a) 各项要求都有明确规定并形成文件;在以口头方式接到订单,而对要求没有书面说明的情况下,供方应确保订单的要求在其被接受之前得到同意;
- b) 任何与投标不一致的合同或订单的要求已经得到解决;
- c) 供方具有满足合同或订单要求的能力。

在供方对软件标书、合同或订单评审期间,还可能涉及到下述有关事项:

a) 与顾客有关的事项:

- 采用的名词术语由有关各方协商一致;
- 顾客具有履行合同义务的能力和资源;
- 经过协商一致的顾客接受或拒收产品的准则;
- 顾客在提供资料和有关设施方面的职责;
- 在联合开发或分承包工作中,顾客参与的程度;
- 为监督合同进展而进行联合评审的安排;
- 在开发和(或)维护期间处理顾客需求更改方面协商一致的程序;
- 顾客指定的生存周期过程;
- 验收后发现的问题的处理,包括顾客的投诉和索赔;
- 任何保证期后消除不合格的职责;
- 当供方认为有必要向后续版本升级时顾客承担的义务,或者供方维护以往版本的义务;
- 推广应用和有关的用户培训。

b) 技术事项:

- 满足需求的可行性;
- 需采用的软件开发标准和规程;
- 明确需由顾客提供的设施、工具、软件和资料,确定评审它们适用性的方法,并形成文件;
- 操作系统或硬件平台;
- 对与软件产品的接口进行控制的协议;
- 复制和分发要求。

c) 管理事项:

- 明确可能的事故或风险,并评估它们对后续活动的影响;
- 供方关于分承包工作的职责;
- 进度、技术评审和交付的时间安排;
- 安装、维护和支持要求;
- 技术、人力和财力资源的及时可得性。

d) 法规、安全和保密事项:

- 按合同使用的信息可能会涉及知识产权、许可证协议、保密性和这些信息的保护等问题;
- 产品母版的保护,以及顾客查阅或验证该母版的权力;
- 需由各方协商同意的向顾客透露信息的程度;
- 担保条款的规定;
- 与合同有关的责任/赔偿。

注:进一步的信息见 ISO/IEC 13207:1995 的 5.2.1 条、5.2.6 条和 6.4.2.1 条。

4.3.3 合同的修订

供方应确定如何进行合同修订,并正确传递到供方组织内的有关职能部门。

没有与软件有关的进一步指南。

注:进一步的信息见 ISO/IEC 12207:1995 的 5.1.3.5 条和 5.2.3.2 条。

4.3.4 记录

应保存合同评审的记录(见 4.16)。

注 9: 供方应与顾客建立有关合同事宜的联络渠道和接口。

没有与软件有关的进一步指南。

4.4 设计控制

4.4.1 总则

供方应建立并保持产品设计控制和验证形成文件的程序,以确保满足规定的要求。

本条对需求分析、概要设计、详细设计和编码等开发活动提供指导。本条也包括对开发策划的指导。

软件开发项目应根据一个或多个生存周期模型进行组织。过程、活动和任务应根据采用的生存周期模型的性质加以计划和实施。所采用的生存周期模型可以调整以适合特定项目的需要,本标准主张在应用时不限定生存周期模型。

生存周期模型明确一套过程,并规定何时和如何引用这些过程。本标准所描述的这些过程顺序并非推荐按此顺序执行。

开发过程是将需求转换为软件产品的过程,为防止错误的导入,这一过程应以规范的方式进行,这种方法减少了以验证和确认过程作为发现问题的唯一方法的依赖性,因此,供方应建立并保持形成文件的程序,以保证软件产品的开发符合规定的要求,并按开发计划和(或)质量计划进行。

应当考虑设计活动所固有的下述方面:

- a) 设计方法:应系统地使用设计方法,应考虑这种方法对任务、产品或项目类型的适合性,以及方法与所采用的工具的兼容性;
- b) 利用过去的经验:利用从过去的实践吸取的经验教训,供方通过应用从先前项目、度量分析和过去项目评审取得的经验教训,应避免同样的或类似的问题重复出现;
- c) 后续过程:软件产品应尽可能设计得便于测试、安装、维护和使用;
- d) 保密和安全:设计应特别考虑可测试性或确认。对于失效将给人员、财产或环境造成危害的产品,这种软件的设计应确保规定特殊设计要求,详细说明期望避免出现的潜在失效条件,和系统对潜在的失效状态应作出的反应。

对于编码,应规定和遵守有关的规则,比如编程语言的用法,一致的命名规则,编码规则和适当的注释规则。这类规则应形成文档并加以控制。

供方可以使用工具、设施和技术,以使本标准中的质量体系指南产生预期的效果。这些工具、设施和技术可有效地用于管理目的,也可以有效地用于产品开发和(或)服务。不管这些工具和技术是内部开发的或购买的,供方均应评价它们是否适合于使用目的。在产品实现中使用的工具,比如分析工具和设计工具、编译程序、汇编程序等应经批准,并在使用之前应按配置管理控制的适当级别配置。这种工具和技术的使用范围应形成文档,并在适当的时候评审它们的使用情况,以确定是否对它们进行改进和(或)升级。

在开始使用这种工具和技术时,或任何改进和(或)升级之后,可能需要对人员进行培训。

4.4.2 设计和开发策划

供方应对每项设计和开发活动编制计划,计划应阐明或列出应开展的活动,并规定实施这些活动的职责。设计和开发活动应委派给具备一定资格的人员去完成,并为其配备充分的资源。计划应随设计的进展加以修改。

对于软件产品,开发策划应确定需求分析、设计、编码、集成、测试、安装和软件产品的验收支持等各项活动。开发策划应形成开发计划文档。

开发计划应经评审和批准。开发计划可以有其他名称,比如软件开发计划或软件项目计划。

开发计划在考虑合同的全部要求情况下,可以确定项目如何进行管理、需要的进度评审,向管理者、顾客和其他有关方报告的类型和频次。

适当时,开发计划应描述下述事项:

- a) 项目的定义,包括对其目标的说明以及参考的顾客或供方的任何有关项目;
- b) 项目作为一个整体的输入和输出的定义;
- c) 项目资源的组织,包括工作小组的结构、职责、分承包方的使用以及需使用的物质资源;
- d) 个人或小组之间的组织接口和技术接口,例如:
 - 子项目小组;
 - 分承包方;
 - 用户;
 - 顾客代表;
 - 质量保证代表。
- e) 明确或引用以下内容:
 - 需进行的开发活动;
 - 每项活动所要求的输入;
 - 每项活动所要求的输出;
 - 需进行的管理和支持活动。
- f) 对与开发有关的可能风险、假设、依存关系和问题的分析;
- g) 进度安排,需明确:
 - 项目的各个阶段;
 - 需进行的工作(每项任务的定义、输入和输出);
 - 相关的资源和时间要求;
 - 相关的依存关系;
 - 里程碑。
- h) 明确下列事项:
 - 标准、规则、惯例和约定;
 - 开发用的工具和技术,包括对这类工具和技术的约束条件和配置控制;
 - 配置管理惯例;
 - 控制不合格品的方法;
 - 用于支持开发的非交付软件的控制方法;
 - 归档备份和恢复的程序,包括应急计划;
 - 病毒防护控制方法;
- i) 明确有关计划(包括系统级计划)如:
 - 质量计划;
 - 风险管理计划;
 - 配置管理计划;

- 集成计划；
- 测试计划；
- 安装计划；
- 移植计划；
- 培训计划；
- 维护计划；
- 重用计划。

开发计划和任何有关的这些计划可以是独立的文档,或是另一文档的一部分或由若干文档组成。

注:进一步的信息见 ISO/IEC 12207:1995 的 5.2.4 条。

4.4.3 组织和技术接口

应规定参与设计过程的不同部门之间在组织上和技术上的接口,将必要的信息形成文件,予以传递并定期评审。

应在供方或分供方的开发计划中清楚地确定承担软件产品的每一方的职责范围、在所有各方之间传递技术信息的方式。供方可以要求分承包方提交开发计划,以供评审。

在确定接口时,除了顾客和供方之外,应注意考虑到需要参与设计、安装、维护和培训活动的各方。他们可包括分承包方、上级管理机关、相关开发项目和辅助工作人员。特别是,可能需要最终用户和中间运行职能部门的参与,以保证得到适当的能力和培训,达到承诺的服务水平。

根据合同顾客可能有某种职责。特别需要注意的事包括需要顾客与供方合作以及时提供所有必要信息,并协调行动事宜。在有顾客代表的地方,顾客代表可以代表产品的最终使用者和执行管理者,有权处理合同事项,包括但不限于下列事项:

- a) 确定顾客对供方的要求;
- b) 回答供方的询问;
- c) 认可供方的建议;
- d) 与供方达成协议;
- e) 保证顾客的组织遵守与供方达成的协议;
- f) 确定验收准则和程序;
- g) 处理顾客提供的不适合使用的软件项、数据、设施和工具;
- h) 确定顾客的职责。

相互协商一致后,供方和顾客的联合评审可以安排为定期的或在发生重要的项目事件时进行,适当时,联合评审覆盖下述方面:

- a) 供方担负的软件开发工作的进展;
- b) 业已协商同意由顾客承担的活动的进展;
- c) 开发的产品是否符合顾客同意的需求规格说明;
- d) 开发中涉及的系统最终用户的活动的进展,比如系统转换和培训;
- e) 验证结果;
- f) 验收测试结果。

注:进一步的信息见 ISO/IEC 12207:1995 的 5.2.6.1 和 6.6.2 条。

4.4.4 设计输入

供方应确定与产品有关的设计输入要求,包括适用的法令和法规要求,形成文件,并评审其是否适当。对不完善的、含糊的或矛盾的要求,应会同提出者一起解决。

设计输入应考虑合同评审活动的结果。

需求规格说明应由顾客提供。然而,在相互协商一致时,供方也可提供需求规格说明。在这种情况下,适当时,供方应:

- a) 建立形成文件的程序来制定需求规格说明书,包括:
 - 商定需求和授权更改的方法,特别是在反复制定的需求期间;
 - 如采用原型或演示,对原型或演示的评价的方法;
 - 记录和审查双方讨论的结果;

b) 与顾客密切合作制定需求规格说明书,并且采取措施,力求避免误解,例如:提供术语定义,解释需求的背景等;

- c) 取得顾客对需求规格说明书的认可。

适当时,可采用交谈、调查、研究、提供原形、演示和分析等任何适当的方法来制定需求规格说明书。

需求规格说明书可以以系统说明书形式提供并协商一致。在这种情况下,应有适当的程序以确保将系统要求正确地分配到硬件、软件以及适当的接口说明书中。

需求规格说明书在接受合同时可以不完全确定,在项目进行期间可继续制定,当需求规格说明书更改时,合同可以修订。对需求规格说明书的更改应加以控制。

需求应包括为满足顾客认可的要求所必需的所有方面。需求规格说明书可能需要考虑运行环境。需求可以包括但不限于下述特性:功能性、可靠性、易用性、效率、维护性和可移植性(见 GB/T 16260)。可以规定子特性,例如:保密性。也可以规定安全性和法定的义务。

如果软件产品需要与其他软件或硬件产品接口,在需求规格说明书中尽可能地用直接规定或用参见文件的方式规定待开发的软件产品和其他软件或硬件产品之间的接口。

需求应以在产品验收时可以确认的条款表示。

注:进一步的信息见 ISO/IEC 12207:1995 的 5.3.2~5.3.4 条。

4.4.5 设计输出

设计输出应形成文件,并以能够对照设计输入要求进行验证和确认的形式来表达。

设计输出应:

- a) 满足设计输入的要求;
- b) 包含或引用验收准则;
- c) 标出与产品安全和正常工作关系重大的设计特性(如操作、贮存、搬运、维修和处置的要求)。

设计输出文件在发放前应予以评审。

应根据所选择的方法确定所要求的设计输出并形成文档,这种文档应是正确的、完整的并符合需求。设计输出可以包括:

- 概要设计说明书;
- 详细设计说明书;
- 源代码;
- 用户指南。

注:进一步的信息见 ISO/IEC 12207:1995 的 5.3.5~5.3.7 条。

4.4.6 设计评审

在设计的适当阶段,应有计划地对设计结果进行正式的评审,并形成文件。每次设计评审的参加者应包括与被评审的设计阶段有关的所有职能部门的代表,需要时也应包括其他专家。这些评审记录应予以保存(见 4.16)。

供方应对所有软件开发项目的评审过程制定计划并加以实施,评审过程有关活动的正式程度和严格程度应适合于产品的复杂程度以及与软件产品规定的使用相关的风险程度。供方应建立形成文件的

程序来处理在这些活动期间发现的过程和产品中的缺陷或不合格之处。

设计评审应考虑设计活动的内在因素,例如:可行性、保密性和安全性、编程规则和可测试性。

评审结果以及确保符合规定要求所需的进一步活动,当它们完成时应加以记录和检查。

开发期间的大多设计评审要加以计划安排,但也可能有一些未经安排的设计评审。

形成文件的设计评审程序应阐明下述内容:

- a) 评审什么,何时评审以及评审类型;
- b) 在每种评审类型中应涉及什么职能部门,如果需要召开评审会议,应由谁主持;
- c) 必须产生的记录,例如:会议记录、讨论的议题、要解决的问题、措施和措施状态。

在设计评审程序中还可以阐明以下内容:

- a) 为保证符合性,对规则、惯例和约定的应用进行监督的方法,如同行评审、走查、代码审查;
- b) 在评审之前必须做什么,如制定目标、会议议程、所需的文档和评审人员的分工;
- c) 在评审期间必须做什么,包括需采用的技术和所有参加人员的行为准则;
- d) 评审通过的准则;
- e) 需采用什么跟踪方法以确保评审中发现的问题得以解决。

合同中有规定时,供方应与顾客协作召开设计评审会议,双方应对评审结果协商一致。

建议只有当所有已知的缺陷都得到满意的解决,或者继续进行的风险已知时,才能继续进行进一步的设计活动。

注:进一步的信息见 ISO/IEC 12207:1995 的 5.3.4.2、5.3.5.6、5.3.6.7 和 6.6.3 条。

4.4.7 设计验证

在设计的适当阶段,应进行设计验证,以确保设计阶段的输出满足该设计阶段输入的要求。设计验证应予以记录(见 4.16)。

注 10:除实施设计评审(见 4.4.6)之外,设计验证还可以包括以下活动:

- 变换方法进行计算;
- 可能时,将新设计与已证实的类似设计进行比较;
- 进行试验和证实;
- 对发放前的设计阶段文件进行评审。

在开发过程的适当阶段,应进行设计验证。设计验证可由设计输出评审、原型和仿真的演示或测试组成。验证也可以针对其他开发活动的输出进行。这些验证活动应根据质量计划或形成文件的程序予以计划和进行,以保证过程输出满足过程输入要求。

验证结果和为保证满足设计阶段输入的要求所需要的任何进一步的措施应予以记录,并且当措施完成时进行检查。

只有经验证的设计输出才应提交验收和后续使用。对任何发现的问题都应进行恰当地说明和解决。

注:进一步的信息见 ISO/IEC 12207:1995 的 5.3.4.2、5.3.5.6、5.3.5.7、5.3.7.5、5.3.9 和 6.4 条。

4.4.8 设计确认

应进行设计确认,以确保产品符合规定的使用者需要和/或要求。

注

- 11 设计确认在成功的设计验证(见 4.4.7)之后进行;
- 12 确认通常在规定的操作条件下进行;
- 13 确认通常针对最终产品进行,但产品完成前的各阶段也可能需要进行;
- 14 如果有不同的预期用途,也可以进行多次确认。

在产品提交顾客验收之前,例如:在最终检验和试验期间,供方应根据其规定的预期用途确认产品。

在软件开发过程中,为确保满足规定的要求,重要的是对确认结果和需要进一步采取的措施应加以记录,并且当措施完成时进行检查。只有经确认的产品才能提交验收或后续使用。

注:进一步的信息见 ISO/IEC 12207:1995 的 5.3.1 和 6.5 条。

4.4.9 设计更改

所有的设计更改和修改在实施之前都应由授权人员加以确定,形成文件,并评审和批准。

供方应建立和保持实施任何设计更改的控制程序,这种更改可能在产品开发生存周期的任何时候发生,该程序是为了:

- a) 将更改形成文档并证实它是合理的;
- b) 评价更改的后果;
- c) 批准或不批准更改;
- d) 实施并验证更改。

在软件开发环境中,设计更改的控制通常在配置管理范畴中阐明。

注:进一步的信息见 ISO/IEC 12207:1995 的 5.5.2、5.5.3 和 6.2.3 条。

4.5 文件和资料控制

4.5.1 总则

供方应建立并保持形成文件的程序,以控制与本标准要求有关的所有文件和资料,包括适当范围的外来文件,如标准和顾客提供的图样。

注 15: 文件和资料可以呈任何介质形式,如硬拷贝或电子介质。

配置管理程序可以用来实施文件和资料控制。在建立的文件和资料的控制程序中,供方应确定那些需遵守控制程序的文件和资料,包括外来的文件和资料,例如标准和顾客提供的资料。

文件和资料控制程序应适用于相关的文件和资料,包括下述种类:

- a) 合同文件,包括需求规格说明书;
- b) 在软件生存周期中应用的描述质量体系的程序文件;
- c) 描述供方活动的策划和进展以及供方与顾客合作的计划文件;
- d) 描述或者与某一具体软件产品有关的产品文档和资料。

注:进一步的信息见 ISO/IEC 12207:1995 的 6.1 条。

4.5.2 文件和资料的批准和发布

文件和资料在发布前应由授权人员审批其适用性,应制定并可随时得到识别文件现行修订状态的控制清单或相当的文件控制程序,以防止使用失效和/或作废的文件。

这种控制应确保:

- a) 在对质量体系的有效运行起重要作用的各个场所,都能得到相应文件的有效版本;
- b) 从所有发放或使用场所及时撤出失效和/或作废的文件,或以其他方式确保防止误用;
- c) 为法律和/或积累知识的目的所保留的任何已作废的文件,都应进行适当标识。

在用电子手段实现文件控制的地方,对其适当的批准、存取、分发、媒体和归档程序应予以特别注意。

4.5.3 文件和资料的更改

除非有专门指定,文件和资料的更改应由文件的原审批部门/组织进行审批,若指定其他部门/组织审批时,该部门/组织应获得审批所需依据的有关背景资料。

可行时,应在文件或相应附件上指明更改的性质。

没有与软件有关的进一步指南。