ICS 35.080
L 77

中华人民共和国国家标准

GB/T 14394—2008
代替 GB/T 14394—1993

计算机软件可靠性和可维护性管理

Computer software reliability and maintainability management

2008-07-18 发布　　2008-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准代替 GB/T 14394—1993《计算机软件可靠性和可维护性管理》。

本标准与 GB/T 14394—1993 的主要差别是：GB/T 14394—1993 依据 GB/T 8566—1988《计算机软件开发规范》划分软件生存周期，按阶段描述软件可靠性和可维护性要求；本标准依据 GB/T 8566—2007《信息技术　软件生存周期过程》划分软件生存周期，按过程和活动描述软件可靠性和可维护性要求。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准起草单位：中国电子技术标准化研究所、山东省计算中心。

本标准主要起草人：韩红强、王纬、李刚、周鸣乐、王英龙。

本标准所代替标准的历次版本发布情况为：

——GB/T 14394—1993。

计算机软件可靠性和可维护性管理

1 范围

本标准规定了软件产品在其生存周期内如何选择适当的软件可靠性和可维护性管理要素，并指导软件可靠性大纲和可维护性大纲的制定和实施。

本标准适用于软件产品生存周期的基本过程。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 8566—2007 信息技术 软件生存周期过程

GB/T 11457—2006 信息技术 软件工程术语

GB/T 16260.1—2006 软件工程 产品质量 第1部分：质量模型 (ISO/IEC 9126-1:2001, IDT)

3 术语和定义

GB/T 11457—2006 中界定的以及下列术语和定义适用于本标准。

3.1

软件可靠性大纲 software reliability program

描述为保证软件满足规定的可靠性要求所采取的技术和管理方法的文档，典型地描述要做的工作、所需要的资源、使用的方法、采用的过程、要满足的进度表和项目组织方法。

3.2

软件可维护性大纲 software maintainability program

描述为保证软件满足规定的可维护性要求所采取的技术和管理方法的文档，典型地描述要做的工作、所需要的资源、使用的方法、采用的过程、要满足的进度表和项目组织方法。

3.3

软件 FRACAS software failure reporting analysis and corrective action system

软件失效报告、分析和纠正措施系统(FRACAS)是一个闭环控制系统，它将软件的失效加以记录、报告，找出失效原因，采取纠正措施。

4 软件生存周期

4.1 在软件生存周期基本过程中的可靠性和可维护性管理要求

本标准依照 GB/T 8566—2007 将软件生存周期划分为五个基本过程，提出了在这五个基本过程中进行软件可靠性和可维护性管理的要求。表1给出了本标准的活动与 GB/T 8566—2007 软件生存周期过程和活动的映射关系。

表 1　从本标准活动到 GB/T 8566—2007 软件生存周期过程和活动的映射

软件可靠性与可维护性管理	GB/T 8566—2007 软件生存周期	
	过程	活动
获取	获取	——启动 ——招标的准备 ——合同的准备和更新 ——对供方的监督 ——验收和完成
供应	供应	——启动 ——投标准备 ——签订合同 ——策划 ——执行和控制 ——评审和评价 ——交付和完成
概念	开发	——过程实现 ——系统需求分析 ——系统体系结构设计
需求	开发	——软件需求分析
设计	开发	——软件体系结构设计 ——软件详细设计
实现	开发	——软件编码和测试
测试	开发	——软件集成 ——软件合格性测试 ——系统集成 ——系统合格性测试
安装和检验	开发	——软件安装 ——软件验收支持
运作	运作	——过程实现 ——运行测试 ——系统运行 ——用户支持
维护	维护	——过程实现 ——问题和修改分析 ——修改实现 ——维护评审/验收 ——迁移 ——软件退役

4.1.1　在获取过程中的可靠性和可维护性管理要求

需方确定需要获取的软件产品的可靠性和可维护性要求，确保要求是合理的、可行的、可验证的，并有相应的资源保证，进而在制定标书、选择供方过程中加以体现，并且依照要求管理获取过程，最终验收软件产品的可靠性和可维护性是否达到预期要求。

4.1.2　在供应过程中的可靠性和可维护性管理要求

供方在投标书中对可靠性和可维护性进行说明以答复需方要求，并反映在可行性研究报告、合同

中，通过评定后确定为管理和保证软件产品的可靠性和可维护性所需的过程、规程和资源，确保在软件开发过程中及时、适当地处理可靠性和可维护性要求，直到软件产品满足要求并交付给需方。

4.1.3 在开发过程中的可靠性和可维护性管理要求

开发者负责实施在软件产品的需求分析、设计、编码、集成、测试以及有关的安装和验收等活动中可靠性和可维护性要求。

4.1.3.1 在概念活动中的可靠性和可维护性管理要求

进行软件可行性分析，制定初步软件开发计划，提出软件可靠性和可维护性分解目标、要求及经费。

4.1.3.2 在需求活动中的可靠性和可维护性管理要求

分析和确定软件可靠性和可维护性的具体设计目标，确保与研制任务书或合同中相应要求的可追踪性，制定实施计划，制定各实施阶段的基本准则，确定各实施阶段的验证方法。

4.1.3.3 在设计活动中的可靠性和可维护性管理要求

进行软件可靠性和可维护性分析和设计，编写相应的设计说明，明确对编码、测试阶段的具体要求，组织设计评审，并验证可靠性和可维护性目标的实施和与需求活动中所提相应要求的可追踪性。

4.1.3.4 在实现活动中的可靠性和可维护性管理要求

按照规定的规则，在软件编码过程中依据需求和设计活动中相应的规定实现可靠性和可维护性要求，进行单元测试，做好后续测试工作的准备，评价或审查代码以验证相应要求的实现。

4.1.3.5 在测试活动中的可靠性和可维护性管理要求

在单元和集成测试阶段，验证相应可靠性和可维护性要求的实现，进行重用软件的可靠性和可维护性管理。

在软件配置项测试和系统集成测试阶段，建立适当的软件可靠性测试环境，组织分析测试和测量的数据，验证软件可靠性和可维护性的实现，进行风险分析，决定交付时机。

4.1.3.6 在安装和验收活动中的可靠性和可维护性管理要求

采取联合评审、审核、软件合格性测试和系统合格性测试等手段对可靠性和可维护性进行最终验证和评定。

4.1.4 在运作过程和维护过程中的可靠性和可维护性管理要求

在软件运作过程和维护过程中，应分析和提高软件可靠性：

a) 制定并实施软件可靠性数据采集规程；

b) 实施软件 FRACAS；

c) 测量可靠性，分析现场可靠性是否达到要求；

d) 跟踪用户满意程度；

e) 用可靠性测量数据指导产品和工程过程的改进；

f) 软件产品维护时执行适当的维护规程并参照 4.1.3 实施适用的管理活动。

4.2 在软件生存周期基本过程中的可靠性和可维护性测量

在软件生存周期的各个基本过程中，应进行与可靠性和可维护性有关的测量。软件可靠性测量包括对成熟性、容错性、易恢复性、可靠性的依从性等要素进行的测量，软件可维护性测量包括对易分析性、易改变性、稳定性、易测试性、维护性的依从性等要素进行的测量。具体测量方法的选择应参照 GB/T 16260.1—2006，考虑软件所处的阶段、测量的内容、测量的角度和其活动而定，其目的在于帮助明确要求，分析达到目标要求的程度，从而更有效地管理，以保证在软件生存周期特定过程的可靠性与可维护性问题能得到及时解决。

5 软件可靠性大纲和可维护性大纲

根据合同或协议书中对软件可靠性和可维护性的要求编制大纲，大纲的制定和修改应按质量保证有关标准规定的程序进行评审和审批；软件可靠性大纲和可维护性大纲应纳入软件开发计划，一并综合

实施；软件可靠性大纲和可维护性大纲的实施应由主管机构和软件开发项目各层次负责人分工负责。

5.1 制定大纲应考虑的主要因素

编制大纲，应考虑如下因素：

a） 所处的生存周期过程；

b） 软件生存周期各过程所包含的与可靠性和可维护性相关的要素；

c） 规定的可靠性和可维护性目标；

d） 实现可靠性和可维护性所采取的方法；

e） 实现可靠性和可维护性所进行的活动；

f） 拟采用的开发技术和类似软件的历史状况；

g） 时间进度、经费与其他资源，存储空间与运行时间，程序设计语言，软件运行的软、硬件环境等各种限制条件。

5.2 大纲应包括的主要活动

以下条款给出了软件可靠性大纲和可维护性大纲要素，并对这些要素的应用及任务进行了描述。

5.2.1 制定大纲目标

在需求分析阶段，应建立软件产品的可靠性大纲和可维护性大纲目标，该两项大纲的目标应确保满足合同要求。大纲目标由一系列与每项大纲要素有关的任务组成，应明确每项任务的责任，并提供一个任务实施初步日程表，当情况变化或出现偏差时大纲应根据需要加以修改。

大纲目标应定量和定性地建立，并说明验证所需的判据和条件。

a） 大纲制定和实施所需的组织机构和职责；

b） 定量、定性的可靠性和可维护性目标[如：可靠度 R(T)、失效发生率 ROCOF，等等]；

c） 各项任务实施进度表；

d） 确保软件产品可靠性、可维护性的要素；

e） 可靠性和可维护性验证所用的判据；

f） 软件版本控制、配置管理要求；

g） 软件工程标准化要求；

h） 评审的时间表、对象、准则；

i） 测试实施；

j） 文档编制要求；

k） 培训及支持保证。

5.2.2 分析运行环境

在可行性研究与计划和需求分析阶段应分析运行环境，并在概要设计和详细设计阶段进行必要的修改，同时要注意运行环境的变化会对软件可靠性和可维护性的影响。

下列运行环境和最终使用条件应该分析：

a） 运行的系统及体系结构；

b） 运行和维护方式；

c） 负载；

d） 运行和维护环境(如电磁辐射和感应)；

e） 运输和安装条件；

f） 操作和维护人员要求；

g） 新版本的发行和升级；

h） 恢复的规程和要求；

i） 终端和通信媒体类型。

5.2.3 软件可靠性和可维护性要求的可行性论证

在可行性研究与计划阶段，应对软件的可靠性和可维护性要求进行可行性论证，对于合同中提出的软件可靠性和可维护性要求应根据软件符合规定标准和规范的能力进行评审和论证。这个论证是整个产品研究的一部分，其目的是：

a） 确定设计工作的起点；

b） 估计可靠性和可维护性特性对技术选择、设计配置以及产品性能的影响。

应该考虑：

a） 软件的功能需求；

b） 新软件的市场潜力；

c） 现有软件的技术状况；

d） 生存周期费用；

e） 开发新软件与改造现有软件所付出的劳动的比较；

f） 类似软件产品可靠性和可维护性状况。

5.2.4 选定或制定规范和准则

在需求分析阶段，应选定适当的软件规范和准则。若没有适当的软件规范和准则可遵循，则应自行制定。其内容包括：

a） 确保软件可靠性和可维护性所必须的软件工程规范；

b） 制定软件开发必须遵循的技术准则；

c） 制定软件的支持和维护要求；

d） 制定质量保证计划中的可靠性和可维护性要求；

e） 必要时制定外购、分包和重用原有软件的可靠性和可维护性控制规范；

f） 确保软件可靠性和可维护性所必须的软件工程管理及人员规范。

5.2.5 软件可靠性和可维护性分析

在软件开发过程中各个阶段进行有关的软件可靠性和可维护性分析并编写分析报告应考虑：

a） 可靠性和可维护性目标分配；

b） 软件使用需求量过载情况；

c） 软件开发过程管理及相关产品配置管理情况；

d） 软件质量保证计划中的可靠性和可维护性保证手段；

e） 软件开发技术对于可靠性和可维护性的保障；

f） 软件系统所涉及业务对于可靠性和可维护性的要求；

g） 可靠性和可维护性对软件产品其他要素的影响和关系；

h） 软件设计中的实现情况；

i） 可靠性和可维护性预测；

j） 故障模式、影响及危害度分析；

k） 根源分析；

l） 关键模块分析；

m） 故障定位和隔离技术的应用；

n） 测试环境、测试数据、测试用例和测试覆盖情况；

o） 软件安全性及安全保障分析；

p） 维护实施简易性。

5.2.6 评审

在软件开发各阶段都要求进行评审，评审管理要求按 GB/T 8566－2007 进行，其中与软件可靠性和可维护性有关的具体评审要求如下：

5.2.6.1 概念评审

a) 可靠性和可维护性要求；
b) 可靠性和可维护性的实现可行性；
c) 可靠性和可维护性对于软件产品整体的影响和关系；
d) 可靠性和可维护性对于软件产品相关业务的意义。

5.2.6.2 需求评审

a) 可靠性和可维护性目标；
b) 实施计划；
c) 功能降级使用方式下，软件产品最低功能保证的规格说明；
d) 选用或制定的规范和准则；
e) 验证方法。

5.2.6.3 设计评审

a) 可靠性和可维护性目标分配；
b) 可靠性和可维护性设计方案；
c) 设计分析，关键成分的时序，估计的运行时间，错误恢复及相关性能要求；
d) 测试原理、要求、文档和工具。

5.2.6.4 测试评审

a) 针对可靠性和可维护性的测试目标；
b) 测试方法；
c) 测试用例；
d) 测试工具；
e) 测试通过标准；
f) 测试报告。

5.2.6.5 安装和验收评审

a) 软件可靠性和可维护性验证和确认方法；
b) 软件可靠性和可维护性测试(计划、规程、用例和设施)；
c) 验证与确认时所用的其他准则。

5.2.6.6 软件用户手册评审

a) 软件产品可靠性和可维护性对于运行环境的要求；
b) 软件产品可靠性和可维护性的管理手段；
c) 软件产品可靠性和可维护性的异常处理；
d) 运作和维护过程中实施软件 FRACAS 的考虑，以及可靠性数据采集规程的考虑。

5.2.7 文档和数据

根据合同要求和数据管理目标，确定文档和数据要求的范围。

大纲应建立一个报告事件及其结果的系统。该系统应提供数据可追踪性，并建立相应文档，文档应写明具体数据的采集条件、所作的设想，并注明对数据应用的限制。为保证关键事件得到明确认识，该系统应提供充分的数据，并且系统的输出应适合接受者的需要和分发的要求。

应监视以下关键事项：

a) 大纲目标的建立；
b) 可靠性和可维护性目标分配；
c) 模块一览表的制定；
d) 测试；
e) 故障发生；

f） 缺陷和错误的检查；

g） 维护活动；

h） 恢复活动；

i） 数据分析；

j） 采取的纠正措施和结果。

5.2.8 培训

要求及时制定培训计划，培训计划应与软件开发计划、维护要求、运行支持策略协调一致。培训对象包括软件开发人员、维护人员、质量控制人员、管理人员、操作人员，针对不同对象进行不同类型、不同级别的培训。培训内容为：

a） 一般知识或专门技术；

b） 软件系统所涉及业务；

c） 软件的复杂性；

d） 操作要求；

e） 需用的时间和资源；

f） 需用的设施和工具。

5.2.9 维护保障要求

对维护保障要求应进行说明并制定计划。需考虑下列因素：

a） 维护和后勤保障策略；

b） 技术保障职能；

c） 维护保障任务；

d） 配置管理；

e） 操作和修改规程；

f） 突发事件和分析；

g） 数据采集和现场跟踪；

h） 软件系统使用情况跟踪及维护；

i） 文档。

5.3 示例

表 2 说明了大纲的各项活动同软件生存周期各过程的基本关系，它为适当地选择相关大纲任务提供一个示例。

表 3 说明了大纲的各项活动同软件生存周期开发过程各阶段的基本关系，它为适当地选择相关大纲任务提供一个示例。

表 2 软件生存周期过程与软件可靠性大纲和软件可维护性大纲要素对应关系

生存周期过程	5.2.1 制定大纲目标	5.2.2 分析运行环境	5.2.3 软件可靠性和可维护性要求的可行性论证	5.2.4 选定或制定规范和准则	5.2.5 软件可靠性和可维护性分析	5.2.6 评审	5.2.7 文档和数据	5.2.8 培训	5.2.9 维护保障要求
获取过程	√	√	√	√		√			
供应过程				√	√	√			
开发过程	√	√	√	√	√	√	√	√	√
运作过程						√	√	√	
维护过程						√	√	√	√
注：“√”表示该阶段所需考虑的有关任务条款。									

表 3　软件开发过程与软件可靠性大纲和软件可维护性大纲要素对应关系

生存周期过程	5.2.1 制定大纲目标	5.2.2 分析运行环境	5.2.3 软件可靠性和可维护性要求的可行性论证	5.2.4 选定或制定规范和准则	5.2.5 软件可靠性和可维护性分析	5.2.6 评审	5.2.7 文档和数据	5.2.8 培训	5.2.9 维护保障要求
概念		√	√		√		√		
需求	√	√		√	√	√	√		√
设计				√	√	√	√	√	√
实现					√	√	√		√
测试					√	√	√	√	√
安装和检验					√	√	√	√	√
注：“√”表示该阶段所需考虑的有关任务条款。									

5.4　剪裁

大纲内容可根据软件类别、规模和关键程度作适当剪裁。剪裁原则是：所制定大纲能使软件开发以最佳费用效益实现规定的可靠性和可维护性要求。

参 考 文 献

[1] GB/T 5271.1—2000 信息技术 词汇 第1部分:基本术语(eqv ISO/IEC 2382-1:1993).

[2] GB/T 5271.20—1994 信息技术词汇 20部分 系统开发(eqv ISO/IEC 2382-20:1990).

[3] 龚庆祥等. 型号可靠性工程手册[M]. 北京:国防工业出版社,2007.