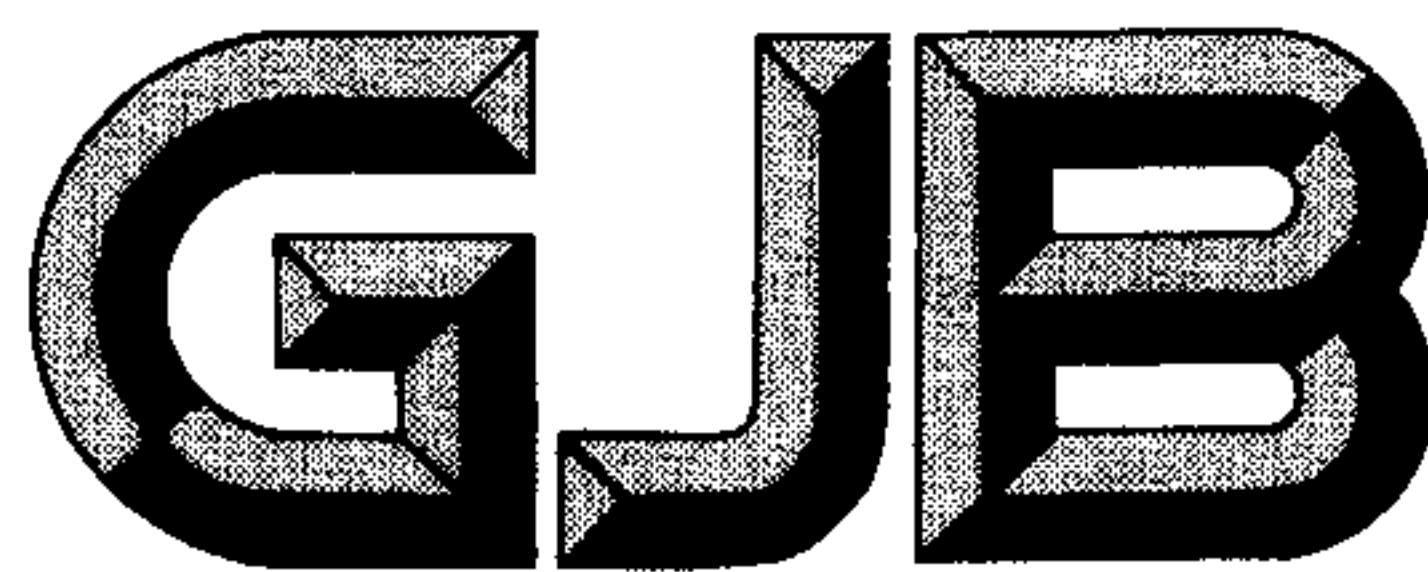




中华人民共和国国家军用标准

FL 0112

GJB 2786A—2009
代替 GJB 437—1988、GJB 2786—1996
和 GJB 2255—1994

军用软件开发通用要求

General requirements for military software development

2009—05—25 发布

2009—08—01 实施

中国人民解放军总装备部 批准

目 次

前言.....III

1 范围.....1

2 引用文件.....1

3 术语、定义和缩略语.....1

3.1 术语和定义.....1

3.2 缩略语.....2

4 一般要求.....3

4.1 软件开发过程.....3

4.2 软件开发的一般要求.....4

5 详细要求.....5

5.1 概述.....5

5.2 项目策划和监控.....5

5.3 软件开发环境建立.....6

5.4 系统需求分析.....6

5.5 系统设计.....7

5.6 软件需求分析.....7

5.7 软件设计.....7

5.8 软件实现和单元测试.....8

5.9 单元集成和测试.....8

5.10 CSCI 合格性测试.....9

5.11 CSCI/HWCI 集成和测试.....9

5.12 系统合格性测试.....10

5.13 软件使用准备.....10

5.14 软件移交准备.....11

5.15 软件验收支持.....12

5.16 软件配置管理.....13

5.17 软件产品评价.....13

5.18 软件质量保证.....13

5.19 纠正措施.....14

5.20 联合评审.....14

5.21 测量和分析.....15

5.22 风险管理.....15

5.23 保密性有关活动.....15

5.24 分承制方管理.....15

5.25 与软件独立验证和确认 (IV&V) 机构的联系.....15

5.26 与相关开发方的协调.....15

5.27 项目过程的改进.....15

附录 A (资料性附录) 活动与多个构建版的映射.....16

附录 B (规范性附录) 采用可重用软件产品对本标准的解释.....17

附录 C (资料性附录) 一个系统或 CSCI 按多个构建版开发时各项活动的实施建议.....20

附录 D (规范性附录) 问题报告的类别及严重性等级.....23

附录 E (规范性附录) 软件产品评价.....24

附录 F (资料性附录) 可供选用的测度.....29

附录 G (资料性附录) 关于项目策略、剪裁和构建版策划的指南.....30

参考文献.....37

前 言

本标准代替 GJB 437-1988《军用软件开发规范》、GJB 2786-1996《武器系统软件开发》和 GJB 2255-1994《军用软件产品》。

与 GJB 2786-1996 相比，本次修订主要有如下变化：

- a) 标准名称改为“军用软件开发通用要求”；
- b) 增加了使用和开发可重用软件产品、系统合格性测试、软件验收支持、软件质量保证、测量和分析以及保密性有关活动、与相关开发方的协调和项目过程的改进等方面的要求；
- c) 修改完善了项目策划和监控、系统需求分析、系统设计、CSCI/HWCI 集成与测试、软件使用准备、联合评审、风险管理、与软件独立验证和确认机构的联系等方面的内容；
- d) 删除了原标准中的附录 A“对软件编码标准的要求”（补充件），附录 D“缩略语表”（参考件），将标准中出现的缩略语在第 3 章给出；
- e) 增加了附录 A～附录 C、附录 F～附录 G。

本标准附录 B、附录 D 和附录 E 是规范性附录，附录 A、附录 C、附录 F 和附录 G 是资料性附录。本标准由总装备部电子信息基础部提出。

本标准起草单位：总装备部电子信息基础部标准化研究中心、航天科工集团 706 所、航天科技集团软件评测中心、总参三部计算中心站、总参 61 所、空军装备研究院总体所、总装武器装备论证研究中心。

本标准主要起草人：王 纬、潘 华、石 柱、杨宝明、刘新建、胡兢玉、胡九川、周宏建、叶东升、刘远有、梁 敏。

军用软件开发通用要求

1 范围

本标准规定了军用软件开发的通用要求,包括软件开发的基本活动、支持活动和管理活动等方面的要求。

本标准适用于需方和开发方获取、开发及维护军用软件(含固件中的软件)。本标准中所涉及的“系统”有两类:一类是硬件-软件系统(例如一个雷达系统),对于这种系统,本标准只适用于系统中的软件元素;一类是软件系统(例如一个地理信息系统),对这类系统,本标准适用于其整个系统。

2 引用文件

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,其后的任何修改单(不包含勘误的内容)或修订版本都不适用于本标准,但提倡使用本标准的各方探讨使用其最新版本的可能性。凡不注日期或版次的引用文件,其最新版本适用于本标准。

GB/T 11457 软件工程术语

GJB 438B-2009 军用软件开发文档适用要求

3 术语、定义和缩略语

3.1 术语和定义

GB/T 11457 确立的以及下列术语和定义适用于本标准。

3.1.1 行为设计 behavioral design

按用户观点,对整个系统或计算机软件配置项将如何运转的设计,它只考虑满足用户需求而不考虑系统或计算机软件配置项的内部实现。这种设计与体系结构设计不同,后者要标识系统或计算机软件配置项的内部成分,并有这些成分的详细设计。

3.1.2 构建版 build

软件的一个版本,它满足最终软件将满足的全部需求的一个规定的子集。

3.1.3 计算机软件配置项 computer software configuration item

满足最终使用要求并由需方指定进行单独配置管理的软件集合。计算机软件配置项的选择基于对下列因素的权衡:软件功能、规模、宿主机或目标计算机、开发方、保障方案、重用计划、关键性、接口考虑、需要单独编写文档和控制、以及其他因素。

3.1.4 测度 measure (noun)

通过执行一次测量赋予实体属性的数或类别。

3.1.5 测量 measurement

使用一组度量,把标度值(可以是数或类别)赋予实体的某个属性。

注:使用类别时,测量可以是定性的。如软件产品的一些重要属性,例如源程序语言(Ada, C, COBOL 等)就是定性的类型。

3.1.6 度量 metric

定义的测量方法和测量标度。

注1:度量可以是内部的或外部的,可以是直接的或间接的。

注2:度量包括把定性数据进行分类的方法。

3.1.7 合格性测试 qualification testing

为了向需方证明 CSCI 或系统满足其规定的需求而进行的测试。

3.1.8 再工程 reengineering

为了以一种新的形式重组一个现有系统而对其进行检查和改造的过程。再工程可包括逆向工程(分析一个系统并在更高的抽象层次上产生其表示,如从代码产生设计),重构(在同一个抽象层次上把系统从一种表示形式转换到另一种表示形式),重编文档(分析一个系统并产生用户文档和支持文档),正向工程(使用从现有系统导出的软件产品,结合新的需求,以产生新的系统),重定目标(对系统进行转换,以便将其安装到不同的目标系统上)和翻译(将源码从一种语言转换到另一种语言或者从一种语言的某个版本转换到另一个版本)。

3.1.9 可重用软件产品 reusable software product

为一种用途开发但还具有其他用途的软件产品,或者专门为了用于多个项目或一个项目的多种任务而开发的软件产品。例如商业现货软件产品、需方提供的软件产品、重用库中的软件产品和开发方现有的软件产品。每一次使用可以包括这些软件产品的全部或部分,也可以包括它的修改部分。

注:可重用软件产品可以是任何软件产品(例如需求、体系结构等),而不只限于软件本身。

3.1.10 软件 software

与计算机系统的操作有关的计算机程序、规程和可能相关的文档。

注:本标准中软件只限于计算机程序和计算机数据库。

3.1.11 软件开发 software development

产生软件产品的一组活动。可包括新开发、修改、重用、再工程、维护或者任何会产生软件产品的其他活动。

3.1.12 软件开发文件 software development file

与特定软件开发有关的资料库。其内容一般包括(直接或通过引用)有关需求分析、设计和实现的考虑、理由和约束条件;开发方内部的测试信息;以及进度和状态信息。

注:软件开发文件不是一个特定文档,通常为由多个电子文件组成的文件夹。

3.1.13 软件产品 software product

作为定义、维护或实施软件过程的一部分而生成的任何制品,包括过程说明、计划、规程、计算机程序和相关的文档等,无论是否打算将它们交付给顾客或者最终用户。软件产品在开发过程中也称软件工作产品。

3.1.14 软件保障 software support

为确保软件安装后能继续按既定要求运行而且在系统的运行中能起既定作用而发生的一系列活动。软件保障包括软件维护、用户支持和有关的活动。

3.1.15 软件移交 software transition

使软件开发的从一个组织转交给另一个组织的一系列活动。一般说,前一个组织实施软件开发,而后一个组织实施软件保障。

3.1.16 软件单元 software unit

计算机软件配置项(CSCI)设计中的一个元素;例如,CSCI的一个主要构成部分、这种构成部分的一个部件、一个类、对象、模块、函数、子程序或者数据库。软件单元可以出现在层次结构的不同层上,并可以由其他软件单元组成。设计中的软件单元与实现它们的代码和数据实体(子程序、过程、数据库、数据文件等)之间,或与包含这些实体的计算机文件之间并不一定有一一对应的关系。

3.2 缩略语

CASE—computer-aided software engineering 计算机辅助软件工程;

COM—computer operation manual 计算机操作手册;

CPM—computer programming manual 计算机编程手册;

CSCI—computer software configuration item 计算机软件配置项;

DBDD—database design description 数据库设计说明;
 FSM—firmware support manual 固件保障手册;
 HWCI—hardware configuration item 硬件配置项;
 IDD—interface design description 接口设计说明;
 IRS—interface requirement specification 接口需求规格说明;
 IV&V—independent verification and validation 独立验证和确认;
 OCD—operational concept description 运行方案说明;
 SCMP—software configuration management plan 软件配置管理计划;
 SCMR—software configuration management report 软件配置管理报告;
 SCOM—software center operator manual 软件中心操作员手册;
 SDD—software design description 软件设计说明;
 SDF—software development file 软件开发文件;
 SDP—software development plan 软件开发计划;
 SDTD—software development task description 软件研制任务书;
 SDSR—software development summary report 软件研制总结报告;
 SIOM—software input/output manual 软件输入/输出手册;
 SIP—software installation plan 软件安装计划;
 SOW—statement of work 工作说明;
 SPS—software product specification 软件产品规格说明;
 SQAP—software quality assurance plan 软件质量保证计划;
 SQAR—software quality assurance report 软件质量保证报告;
 SRS—software requirement specification 软件需求规格说明;
 SSDD—system/subsystem design description 系统/子系统设计说明;
 SSS—system/subsystem specification 系统/子系统规格说明;
 STD—software test description 软件测试说明;
 STP—software test plan 软件测试计划;
 STR—software test report 软件测试报告;
 STrP—software transition plan 软件移交计划;
 SUM—software user manual 软件用户手册;
 SVD—software version description 软件版本说明。

4 一般要求

4.1 软件开发过程

开发方应建立一个与合同要求一致的软件开发过程。软件开发过程可包括下列活动:

- a) 项目策划和监控(5.2);
- b) 软件开发环境建立(5.3);
- c) 系统需求分析(5.4);
- d) 系统设计(5.5);
- e) 软件需求分析(5.6);
- f) 软件设计(5.7);
- g) 软件实现和单元测试(5.8);
- h) 单元集成和测试(5.9);
- i) CSCI 合格性测试(5.10);

- j) CSCI/HWCI 集成和测试(5.11);
- k) 系统合格性测试(5.12);
- l) 软件使用准备(5.13);
- m) 软件移交准备(5.14);
- n) 软件验收支持(5.15);
- o) 软件配置管理(5.16);
- p) 软件产品评价(5.17);
- q) 软件质量保证(5.18);
- r) 纠正措施(5.19);
- s) 联合评审(5.20);
- t) 测量与分析(5.21);
- u) 风险管理(5.22);
- v) 保密性有关活动(5.23);
- w) 分承制方管理(5.24);
- x) 与软件独立验证和确认(IV&V)机构的联系(5.25);
- y) 与相关开发方的协调(5.26);
- z) 项目过程的改进(5.27)。

其中 c)~n) 为软件开发的基本活动, o)~t) 为软件开发的支持活动, 其他为软件开发管理活动。

这些活动可以重叠或迭代应用, 对不同的软件元素可以应用不同的活动, 并且不必按上面列出的次序执行。针对具体软件, 可对这些活动进行剪裁。软件开发过程应在软件开发计划中描述。

4.2 软件开发的一般要求

4.2.1 软件开发方法

对软件开发的全部活动, 开发方应采用文档化的系统方法。这些方法应在软件开发计划中给予描述或引用。

4.2.2 软件产品标准

开发方应使用表述需求、设计、编码、测试用例、测试规程和测试结果等的标准。这些标准应在软件开发计划中给予描述或引用。

4.2.3 可重用软件产品

4.2.3.1 采用可重用软件产品

开发方应标识和评价为满足合同要求而使用的可重用软件产品, 并应按照软件开发计划的要求确定可重用软件产品的选择范围和评价准则。只要切实可行, 就应采用满足准则的可重用软件产品。所采用的可重用软件产品还应满足合同中规定的有关权限的要求。

关于采用可重用软件产品需考虑的评价准则以及为采用可重用软件产品而对本标准所作的解释见附录 B。

4.2.3.2 开发可重用软件产品

在履行合同期间, 开发方应评估开发可重用软件产品的可行性、成本及可能产生的效益, 并向需方说明费效比且与项目目标相一致的情况。

合同中也可以要求开发方专门开发可重用软件产品。

4.2.4 关键需求的处理

4.2.4.1 安全性保证

开发方应将其失效可能导致危险的系统状态(如导致意外死亡、伤害、财产损失或危害环境的状态)的 CSCI 或其中的部分标识为安全关键的。如果有这种软件, 开发方应制定安全性保证策略(包括测试和分析), 以排除或最大限度地降低在这种软件的需求、设计、实现和操作规程中潜在的危险。该策略

应包括软件安全性大纲，并纳入系统安全性大纲(若已有)中。开发方应在软件开发计划中记录该策略，实施该策略，并提供实施该策略的证据。实施该策略的证据应作为所要求的软件产品的一部分。

4.2.4.2 保密性保证

开发方应将其失效可能导致破坏系统保密性的 CSCI 或其中的部分标识为保密关键的。如果有这种软件，开发方应制定保密性保证策略，以排除或最大限度地降低这种软件的需求、设计、实现和操作规程所引起的破坏系统保密性的可能性。开发方应在软件开发计划中记录该策略，实施该策略，并提供实施该策略的证据。实施该策略的证据应作为所要求的软件产品的一部分。

4.2.4.3 其他关键需求的保证

如果一个系统依赖于软件来满足在合同和系统规格说明中认为是关键的其他需求，如可靠性，那么开发方应标识其失效可能导致违背这些关键需求的 CSCI 或其中的部分；制定策略，用来保证使所标识软件的需求、设计、实现和操作规程不会发生这种违背或使其可能性最小；开发方应在软件开发计划中记录该策略，实施该策略，并提供实施该策略的证据。实施该策略的证据应作为所要求的软件产品的一部分。

4.2.5 计算机硬件资源的利用

开发方应分析合同中关于计算机硬件资源利用方面的要求(如允许使用的最大处理器能力、内存容量、输入/输出设备能力、辅存设备能力和通信/网络设备能力)。开发方应在各 CSCI 之间分配计算机硬件资源，在合同期间监督这些资源的利用。必要时，为满足合同要求，应重新分配或标明需要的附加资源。

4.2.6 决策理由的记录

开发方应记录在软件需求分析、设计、实现和测试中作出重要决策的理由，这些记录对保障机构有用。决策理由应包括所考虑的折中情况、分析方法和决策所用的准则。这些理由应记录在文档、代码注释或其他将移交给保障机构的媒体中。

“重要决策”的含意应在软件开发计划中加以描述，作出这些决策的理由应在软件开发计划中指出。

4.2.7 便于需方评审

为了对合同所要求的软件产品及各项活动进行评审，开发方应为需方或其授权代表访问有关设施(如软件工程环境等)提供方便。

5 详细要求

5.1 概述

软件开发过程包括 5.2~5.27 规定的 26 项活动，活动描述的顺序并不表示活动执行的顺序。活动执行的顺序依赖于所选择的生存周期模型。

本标准要求软件开发方参与软件所在系统层面的活动。若所在系统是硬件-软件系统(例如一个雷达系统)，则“参与”指参加；若所在系统是软件系统(例如一个地理信息系统)，则“参与”是指负责。如果软件是按多个构建版开发的，那么某些活动可能在每个构建版中都要执行，另一些活动可能只在一些选定的构建版中执行，并且这些活动和软件产品在若干构建版或所有构建版完成之前不可能是完成的。附录 A 提供了活动如何应用到多个构建版的例子。只含单个构建版的项目将完成该项目有关软件所要求的所有活动。如果一个系统或 CSCI 按多个构建版开发，各项活动的实施建议参见附录 C。

5.2 项目策划和监控

5.2.1 软件开发策划

开发方应为实施本标准所要求的活动和合同中其他有关软件需求所要求的各项活动制定计划。该策划应与系统级策划一致，策划应以项目估计为基础，并应包括 GJB 438B-2009 中软件开发计划(SDP)规定的全部适用项。

注 1：软件开发计划涵盖本标准所要求的全部活动。为了有利于提高信息的可利用性，计划的一些部分可以分开单

独装订或维护。例如,软件质量保证和软件配置管理可分别编制计划(对于需要定型的软件产品,常常要求分别编制)。

注2:关于项目策划的进一步要求,参见 GJB 5000A-2008 中 6.4 项目策划过程域。

5.2.2 CSCI 测试策划

开发方应制定 CSCI 合格性测试计划。该计划应包括 GJB 438B-2009 中软件测试计划(STP)规定的全部适用项。

5.2.3 系统测试策划

开发方应参与制定系统合格性测试计划。对软件系统而言,该计划应包括 GJB 438B-2009 中软件测试计划(STP)规定的所有适用项。

5.2.4 软件安装策划

开发方应制定在合同规定的用户现场进行软件安装和培训的计划。该计划应包括 GJB 438B-2009 中软件安装计划(SIP)规定的全部适用项。

5.2.5 软件移交策划

开发方应指明保障机构为完成合同规定的保障工作所需的全部软件开发资源。开发方应制定软件移交计划,以标识这些资源并说明向保障机构移交应交付项目所遵循的方法。该计划应包括 GJB 438B-2009 中软件移交计划(STrP)规定的全部适用项。

5.2.6 计划的跟踪和修订

在需方认可了 5.2.1~5.2.5 中的计划后,开发方应根据计划进行相关活动。开发方的管理者应按照软件开发计划规定的时间间隔检查软件开发过程。在发现显著偏离计划要求时应采取纠正措施,以保证整个过程遵守合同并贯彻该计划。除了开发方内部的安排和有关人员配备的信息以外,对这些计划的修订都应得到需方的认可。

注:关于项目监控的进一步要求,参见 GJB 5000A-2008 中 6.3 项目监控过程域。

5.3 软件开发环境建立

5.3.1 软件工程环境

开发方应建立、控制和维护软件工程环境(包括测试环境)。开发方应确保该环境的各组成部分都能执行其预定的功能。

5.3.2 软件开发资料库

开发方应建立、控制和维护一个软件开发资料库,用来管理软件、文档、其他中间的和最终的软件产品,以及相关的用以促进软件的有序开发和后续保障的工具和方法。该库有利于软件的有序开发和后续保障,也有利于为组织积累资产。该库可以是软件工程环境的组成部分。在合同期内,开发方应维护软件开发资料库。

5.3.3 软件开发文件

开发方应为每个软件单元(或一组逻辑上相关的软件单元)和每个 CSCI 建立、控制并维护软件开发文件(SDF)。适用时,为 CSCI 的逻辑组、子系统和整个系统建立、控制和维护软件开发文件(SDF)。开发方应将有关软件开发的信息记录在相应的 SDF 中,并应在合同期内维护这些软件开发文件(SDF)。

5.3.4 非交付软件

开发方在交付软件的开发中可以使用非交付软件,但应保证交付软件在交付给需方后的运行和保障中不依赖于这些非交付软件,或能确保需方拥有或者可以得到同样的软件。开发方应确保用于项目的全部非交付软件执行其预定的功能。

5.4 系统需求分析

5.4.1 用户要求分析

开发方应参与分析需方提供的用户要求,以了解用户需要。用户要求可以采取如下形式:

- a) 用户需要说明;

- b) 调研报告;
- c) 问题/更改报告;
- d) 对原型的反馈;
- e) 访谈记录;
- f) 其他形式的用户输入或反馈。

5.4.2 运行方案

开发方应参与定义和记录系统运行方案,其结果应包括 GJB 438B-2009 中运行方案说明(OCD)规定的全部适用项。

5.4.3 系统需求

开发方应参与定义和记录系统要满足的需求以及保证每项需求得以满足所使用的方法。这些需求包括所要求的状态和方式、能力、外部接口、内部接口、内部数据、适应性、安全性、保密性、环境、计算机资源、质量因素、设计和构造的约束、合格性、需求可追踪性等方面。其结果应包括 GJB 438B-2009 中系统/子系统规格说明(SSS)规定的全部适用项。有关系统接口的需求可以包含在系统/子系统规格说明(SSS)中,也可以包含在接口需求规格说明(IRS)中。

注:如果一个系统由若干个子系统组成,那么 5.4.3 中的活动与 5.5 中的活动将迭代地执行,以定义系统需求、设计该系统并标识其子系统、定义这些子系统需求、设计这些子系统并标识其部件等等。

5.5 系统设计

5.5.1 系统级设计决策

开发方应参与定义和记录系统级设计决策(即关于系统的行为设计和其他影响系统部件选择与设计的决策),其结果应包括 GJB 438B-2009 中系统/子系统设计说明(SSDD)内有关系统级设计部分中全部适用项。有关接口设计可以包含在 SSDD 中,也可以包含在接口设计说明(IDD)中;有关数据库的设计可以包含在 SSDD 中,也可以包含在数据库设计说明(DBDD)中。

注:设计决策一般由开发方自行处理,除非已通过合同正式转换成了需求。开发方负责全部需求的实现,并通过合格性测试(见 5.10, 5.12)来证明该工作已完成。设计决策作为开发方所要实现的内部“需求”,适用时也可要求分承制方执行,通过开发方内部测试来确认,但不必向需方证明其完成。

5.5.2 系统体系结构设计

开发方应参与定义和记录系统的体系结构设计(标识系统部件,包括硬件、软件、人工操作项及其接口,以及它们之间的执行的方案)以及系统部件与系统需求之间的可追踪性。其结果应包括 GJB 438B-2009 中系统/子系统设计说明(SSDD)内有关体系结构设计和可追踪性方面全部适用项。一般情况下,其结果还应包括 GJB 438B-2009 中软件研制任务书(SDTD)规定的全部适用项。有关接口设计可以包含在 SSDD 中,也可以包含在接口设计说明(IDD)中。

5.6 软件需求分析

开发方应定义和记录每个 CSCI 要满足的软件需求、保证每项需求得以满足所使用的方法以及 CSCI 需求与系统需求之间的可追踪性。软件需求包括要求的状态和方式、能力、外部接口、内部接口、内部数据、适应性、安全性、保密性、环境、计算机资源、质量因素、设计和实现约束、合格性、需求可追踪性等方面。软件需求分析的结果应包括 GJB 438B-2009 中软件需求规格说明(SRS)规定的全部适用项。有关 CSCI 接口的需求可以包含在软件需求规格说明(SRS)中,也可以包含在接口需求规格说明(IRS)中。

5.7 软件设计

5.7.1 CSCI 级设计决策

开发方应定义和记录 CSCI 级设计决策(即关于 CSCI 行为设计的决策和其他对组成 CSCI 的软件单元的选择和设计有影响的决策),其结果应包括 GJB 438B-2009 中软件设计说明(SDD)内有关 CSCI 级设计方面的全部适用项。有关接口的设计可以包含在 SDD 中,也可以包含在接口设计说明(IDD)中;

有关数据库的设计可以包含在 SDD 中,也可以包含在数据库设计说明(DBDD)中。

5.7.2 CSCI 体系结构设计

开发方应定义和记录每个 CSCI 的体系结构设计(标识组成该 CSCI 的软件单元及接口,它们之间的执行的方案)和软件单元与 CSCI 需求之间的可追踪性,其结果应包括 GJB 438B-2009 中软件设计说明(SDD)内有关体系结构设计和可追踪性方面的全部适用项。有关接口的设计可以包含在 SDD 中,也可以包含在接口设计说明(IDD)中。

注:软件单元可以由其他软件单元组成,并可以组织成为表示 CSCI 体系结构所需的多个层次。例如,一个 CSCI 可以分成三个软件单元,而其中每个软件单元又可以分成另一些软件单元,等等。

5.7.3 CSCI 详细设计

开发方应编写和记录每个软件单元的说明,包括每个软件单元的设计决策和约束、接口和数据库的详细设计说明,其详细程度应达到能够根据说明进行软件实现,其结果应包括 GJB 438B-2009 中软件设计说明(SDD)内有关详细设计方面全部适用项。有关接口的设计可以包含在 SDD 中,也可以包含在接口设计说明(IDD)中;本身是数据库的软件单元或者是访问或操作数据库的软件单元的设计可以包含在 SDD 中,也可以包含在数据库设计说明(DBDD)中。

5.8 软件实现和单元测试

5.8.1 软件实现

开发方应开发和记录与 CSCI 设计中每个软件单元相对应的程序。适用时,这项工作应包含下列活动:对计算机指令和数据定义进行编码,建立数据库,将数据值填入数据库和其他数据文件中,以及其他为实现设计所需的活动。对于需交付的软件,开发方如要采用非合同规定的程序设计语言,应经需方批准。

注 1:设计中的软件单元与实现它们的代码和数据实体(子程序、过程、数据库、数据文件等)或包含这些实体的计算机文件之间并不一定存在一一对应关系。

注 2:关于软件单元测试的进一步要求,参见 GJB/Z 141-2004 第 5 章和第 9 章。

5.8.2 单元测试的准备

开发方应为与每个软件单元相对应的软件制定测试计划(包括规定测试需求和进度)、准备测试用例(按照输入、预期的结果和评价准则进行描述)、测试规程和测试数据。测试用例应覆盖该单元详细设计的所有方面。开发方应在相应的软件开发文件(SDF)中记录这些信息。

5.8.3 单元测试的执行

开发方应测试与每一个软件单元相对应的程序,测试应按照单元测试计划、用例和规程进行。

5.8.4 修改和回归测试

开发方应根据单元测试的结果对软件进行必要的修改,并进行全部必要的回归测试,以及根据需要更新软件开发文件(SDF)和其他软件产品。

5.8.5 分析和记录单元测试结果

开发方应分析单元测试的结果,并应在相应的软件开发文件(SDF)中记录该测试和分析的结果。

5.9 单元集成和测试

5.9.1 单元集成与测试和准备

开发方应为进行单元集成和测试制定计划,包括规定测试需求、测试策略和进度安排,并准备测试用例(按照输入、预期结果和评价准则进行描述)、测试规程和测试数据。测试用例应覆盖 CSCI 级设计决策和 CSCI 体系结构设计的所有方面。开发方应将这方面的信息记录在相应的软件开发文件(SDF)中。

5.9.2 单元集成和测试和执行

开发方应执行单元集成和测试,测试应按照单元集成测试计划、用例和规程进行。

5.9.3 修改和回归测试

开发方应根据单元集成和测试的结果对软件进行全部必要的修改,并进行所有必要的回归测试,以

及根据需要更新必要的软件开发文件(SDF)和其他软件产品。

5.9.4 分析和记录单元集成和测试的结果

开发方应分析单元集成和测试的结果,并将测试和分析结果记录在相应的软件开发文件(SDF)中。

注 1: 单元集成和测试是指将两个或两个以上的软件单元所对应的软件集成起来,并测试集成后的软件,以确保它能按设计要求工作,并将这项工作持续到每个 CSCI 中的所有软件都被集成和测试为止。这种测试的最后一步是开发方内部的 CSCI 测试。因为软件单元可以由其他软件单元组成,所以有些软件单元的集成与测试工作可以在单元测试期间进行。5.9 的要求并不是要重复这些活动。

注 2: 关于单元集成测试进一步要求,参见 GJB/Z 141-2004 中第 6 章、第 7 章和第 9 章。

5.10 CSCI 合格性测试

5.10.1 CSCI 合格性测试的独立性

负责进行 CSCI 合格性测试的人员不应是从事该 CSCI 详细设计和实现的人员,但不排除进行 CSCI 详细设计及实现的人员为该测试过程作贡献,例如,提供一些依赖于该 CSCI 内部实现知识的测试用例。

5.10.2 在目标计算机系统中进行测试

CSCI 合格性测试应在目标计算机系统或在需方批准的替代系统上进行。

5.10.3 CSCI 合格性测试的准备

开发方应按照 CSCI 合格性测试策划结果定义和记录用于 CSCI 合格性测试的测试准备、测试用例、测试规程,以及测试用例与 CSCI 需求之间的可追踪性。其结果应包括 GJB 438B-2009 中软件测试说明(STD)规定全部适用项。开发方应准备执行测试用例所需的测试数据,并事先把 CSCI 合格性测试的时间和地点通知需方。

5.10.4 CSCI 合格性测试的预演

如果 CSCI 合格性测试要由需方见证,开发方应对测试用例和规程进行预演,以确保它们完备与准确,并确保该软件已经为见证测试做好了准备。开发方应在相应的软件开发文件(SDF)中记录这些活动的结果,并相应地更新 CSCI 测试用例和规程。

5.10.5 CSCI 合格性测试的执行

开发方应对每个 CSCI 执行 CSCI 合格性测试。测试应按照 CSCI 测试的计划、用例和规程进行。

5.10.6 修改与回归测试

开发方应根据 CSCI 合格性测试的结果对该软件作必要的修改,进行必要的回归测试;回归测试前应通知需方;还应根据需要更新软件开发文件(SDF)和其他软件产品。

5.10.7 分析并记录 CSCI 合格性测试的结果

开发方应分析和记录 CSCI 合格性测试的结果,其内容应包括 GJB 438B-2009 中软件测试报告(STR)规定的全部适用项。

注 1: 执行 CSCI 合格性测试是为了向需方证明 CSCI 的需求已经得到满足。该测试覆盖软件需求规格说明(SRS)和相关的接口需求规格说明(IRS)中对该 CSCI 的需求。

注 2: 关于 CSCI 合格性测试的进一步要求,参见 GJB/Z 141-2004 中第 7 章“配置项测试”和第 9 章“回归测试”。

5.11 CSCI/HWCI 集成和测试

5.11.1 CSCI/HWCI 集成和测试的准备

开发方应参与制定和记录用于执行 CSCI/HWCI 集成和测试的测试计划,包括规定测试需求、测试策略和进度安排,并参与开发和记录测试用例(按照输入、预期结果及评价准则进行描述)、测试规程和测试数据。测试用例应覆盖系统级设计决策和系统体系结构设计的各个方面。开发方应将软件有关的信息记录在相应的软件开发文件(SDF)中。

5.11.2 CSCI/HWCI 集成和测试的执行

开发方应参与 CSCI/HWCI 的集成和测试。测试应按 CSCI/HWCI 测试的计划、用例和规程进行。

5.11.3 修改和回归测试

开发方应根据 CSCI/HWCI 集成和测试的结果对软件进行必要的修正,并参与全部必要的回归测试。需要时,修改相应的软件开发文件(SDF)和其他软件产品。

5.11.4 分析和记录 CSCI/HWCI 集成和测试的结果

开发方应参与 CSCI/HWCI 集成和测试结果的分析。与软件有关的分析与测试结果应记录在相应的软件开发文件(SDF)中。

注 1: CSCI/HWCI 集成和测试是指将 CSCI 与接口连接的 HWCI 和 CSCI 集成起来,并测试其组合结果,以确定它们能否按设计要求工作,持续执行这个过程直到该系统中所有的 CSCI 和 HWCI 都被集成和测试完成。这种测试的最后一个阶段就是开发方内部的系统测试。

注 2: CSCI/HWCI 集成的每一步结果都是一个层次的系统,每一步集成后的测试相当于整个系统的一个中间层次的局部系统的测试。关于 CSCI/HWCI 集成测试的进一步要求,参见 GJB/Z 141-2004 中第 8 章“系统测试”和第 9 章“回归测试”。

5.12 系统合格性测试

5.12.1 系统合格性测试的独立性

负责系统合格性测试的人员不应是从事该系统中软件的设计或实现的人员,但不排除这些人员对系统合格性测试作贡献,例如,提供一些依赖于系统内部实现知识的测试用例。

5.12.2 在目标计算机系统中进行测试

开发方的系统合格性测试应在目标计算机系统中或在经需方批准的替代系统上进行。

5.12.3 系统合格性测试的准备

开发方应按照系统合格性测试策划结果,参与编写并记录测试准备、测试用例和测试规程,参与确定并记录测试用例与系统需求之间的可追踪性。对于软件系统,其结果应包括 GJB 438B-2009 中软件测试说明(STD)规定的全部适用项。开发方应参与为执行测试用例所需测试数据的准备,并事先将系统合格性测试的时间和地点通知需方。

5.12.4 系统合格性测试的预演

若要由需方见证系统合格性测试,开发方应参与系统测试用例和规程的预演,以确保它们完备与准确,并确保系统已为见证测试做好准备。开发方应将这项活动中与软件有关的结果记录在相应的软件开发文件(SDF)中,并应参与对系统测试用例与规程作相应的更新。

5.12.5 系统合格性测试的执行

开发方应参与系统合格性测试。这种参与应按照系统测试的计划、用例和规程进行。

5.12.6 修改和回归测试

开发方应根据系统合格性测试的结果对软件进行必要的修改,并事先通知需方将进行的回归测试,开发方应参与全部必要的回归测试,根据需要修改软件开发文件(SDF)和其他软件产品。

5.12.7 分析并记录系统合格性测试的结果

开发方应参与系统合格性测试结果的分析 and 记录。对于软件系统,其内容应包括 GJB 438B-2009 中软件测试报告(STR)规定的全部适用项。

注 1: 执行系统合格性测试的目的是为了向需方表明系统需求已经得到满足。这种测试覆盖系统/子系统规格说明(SSS)和相关联的接口需求规格说明(IRS)中的系统需求。

注 2: 关于系统测试的进一步要求,参见 GJB/Z 141-2004 中第 8 章和第 9 章。

5.13 软件使用准备

5.13.1 可执行软件的准备

开发方应为每个用户现场准备可执行的软件,包括在目标计算机上安装和运行该软件所需的所有批处理文件、命令文件、数据文件或其他软件文件。其结果应包括 GJB 438B-2009 中软件产品规格说明(SPS)内有关可执行软件方面的全部适用项。

注: 若只要求交付可执行软件(源文件和相关的支持性信息延迟到以后构建版交付),需方可对 SPS 文档进行剪裁,

删去其中除可执行软件方面的所有内容。

5.13.2 为用户现场准备版本说明

开发方应标识和记录为每个用户现场准备的软件的准确版本。其内容应包括 GJB 438B-2009 中软件版本说明(SVD)规定的全部适用项。

5.13.3 用户手册的准备

5.13.3.1 软件用户手册

开发方应标识和记录软件的直接用户(既要操作该软件又要应用其结果的人员)所需的信息,这些信息应包括 GJB 438B-2009 中软件用户手册(SUM)规定的全部适用项。

5.13.3.2 软件输入/输出手册

对于依靠其他人在计算机中心或者在集中式或网络式的软件装置上操作该软件的用户,开发方应标识和记录用户应向计算机提交的输入和从计算机获得的输出。这种信息应包括 GJB 438B-2009 中软件输入/输出手册(SIOM)规定的全部适用项。

5.13.3.3 软件中心操作员手册

开发方应标识和记录在计算机中心或者在集中式或网络式的软件装置上操作该软件的人员所需要的信息,使之能为其他人所用。这种信息应包括 GJB 438B-2009 中软件中心操作员手册(SCOM)规定的全部适用项。

5.13.3.4 计算机操作手册

开发方应标识和记录为操作运行该软件的计算机所需的信息。这些信息应包括 GJB 438B-2009 中计算机操作手册(COM)规定的全部适用项。

注:只有少数的系统才需要 5.13.3 列出的全部 4 种手册。需方应确定对一个特定的系统而言哪些手册是适用的,哪些是需要编制的,所有这些手册都允许用含有所需信息的商用手册或其他手册来替代。5.13.3 所列的各种手册一般都是与软件开发工作并行开发,以备 CSCI 测试时使用。

5.13.4 在用户现场的安装

开发方应:

- a) 在合同规定的用户现场安装和检测可执行的软件;
- b) 按合同规定为用户提供培训;
- c) 按合同规定为用户现场提供其他帮助。

5.14 软件移交准备

5.14.1 可执行软件的准备

开发方应准备需要向保障机构现场移交的可执行软件,包括在目标计算机上安装和运行该软件所必需的所有批处理文件、命令文件、数据文件或其他软件文件。其结果应包括 GJB 438B-2009 中软件产品规格说明(SPS)内有关可执行软件方面全部适用项。

5.14.2 源文件准备

开发方应准备需要向保障机构现场移交的源文件,包括重新生成该可执行软件所必需的所有批处理文件、命令文件、数据文件或其他文件。其结果应包括 GJB 438B-2009 中软件产品规格说明(SPS)内有关源文件方面全部适用项。

5.14.3 为保障机构现场准备版本说明

开发方应标识和记录为保障机构现场准备的软件的准确版本。这种信息应包括 GJB 438B-2009 中软件版本说明(SVD)中规定的全部适用项。

5.14.4 已建成的 CSCI 设计和有关信息的准备

开发方应确保每个 CSCI 的设计说明与“已建成”的软件相一致,并定义和记录下列事项:

- a) 验证该软件拷贝所使用的方法;
- b) 测量到的该 CSCI 的硬件资源利用率;

- c) 支持该软件所需的其他信息;
- d) CSCI 的源文件与软件单元之间的可追踪性;
- e) 计算机硬件资源的利用率测量与涉及它们的 CSCI 需求之间的可追踪性。

其结果应包括 GJB 438B-2009 中软件产品规格说明 (SPS) 内有关合格性、软件保障和可追踪性等方面的全部适用项。

注: 在硬件开发中, 最终产品是一个经过批准的设计, 根据该设计, 就可以制造出硬件项, 这种设计是用产品规格说明来表示的。但在软件开发中, 最终产品是软件, 而不是它的设计, “制造”是该软件的电子复制, 而不是根据设计重建。“已建成”的设计并不是作为产品包含在软件产品规格说明中, 而是作为可以帮助保障机构理解该软件的信息, 以便修改、增强和从其他方面支持该软件。

5.14.5 系统/子系统设计说明的检查

开发方应参与系统/子系统设计说明的检查, 以使它和“已建成”的系统相一致。其结果应包括 GJB 438B-2009 中系统/子系统设计说明 (SSDD) 规定的全部适用项。

5.14.6 保障手册的准备

5.14.6.1 计算机编程手册

开发方应标识和记录在开发或运行该软件的计算机上编程所需的信息。这些信息应包括 GJB 438B-2009 中计算机编程手册 (CPM) 规定的全部适用项。

5.14.6.2 固件保障手册

开发方应标识和记录在安装该软件的固件上进行编程和重编程所需的信息。这些信息应包括 GJB 438B-2009 中固件保障手册 (FSM) 规定的全部适用项。

注: 并非所有的系统都需要 5.14.6 所列的各种手册。需方应确定哪些手册是适用的, 哪些是需要编制的。所有这些手册都允许用包含所需信息的商用手册或其他手册来替代。5.14.6 中所列的各种手册是系统/子系统设计说明 (SSDD) 和软件产品规格说明 (SPS) 的补充, 是作为软件保障信息的主要来源。在 5.13.3 中提到的用户手册对保障人员也是有用的。

5.14.7 移交到指定的保障机构现场

开发方应:

- a) 在合同指定的保障环境中安装并检测可交付的软件。
- b) 向需方演示交付软件能够使用合同指定或需方批准的硬件和如下软件来重新生成 (即编译/连接/装载成一个可执行的产品) 和维护:
 - 1) 现货软件产品;
 - 2) 需方已有的软件产品;
 - 3) 按合同交付的软件产品。
- c) 按合同规定为保障机构提供培训。
- d) 按合同规定为保障机构提供其他帮助。

5.15 软件验收支持

5.15.1 支持需方进行软件验收测试和评审

开发方应按合同规定向需方提出软件验收申请, 并为需方进行软件验收测试、评审和审核提供支持。开发方应将软件验收测试、评审和审核的结果记录在软件开发文件 (SDF) 中。

注: 关于软件验收的进一步要求, 参见 GJB 1268A-2004。

5.15.2 交付软件产品

验收通过后, 开发方应在对软件产品进行必要的修改后, 按合同规定完成并向需方交付软件产品。

5.15.3 提供培训和支持

开发方应按合同规定为需方和软件用户提供必要的培训。

5.15.4 软件产品定型支持

开发方应按合同规定为软件产品定型提供有关文档,包括软件研制总结报告(SDSR)、软件产品规格说明(SPS)、软件质量保证报告(SQAR)和软件配置管理报告(SCMR)等。

5.16 软件配置管理

5.16.1 配置标识

在参与 5.5.2 中系统体系结构设计时,开发方应参与选择 CSCI,标识置于配置控制下的实体,并为置于配置控制下的每一个 CSCI 及其每一个附属实体分配一个项目唯一的标识符。这些实体应包括合同中要求开发的或用到的软件产品以及软件开发环境的元素。标识方案应考虑所有实体实际受控的级别,例如,计算机文件、电子媒体、文档、软件单元、配置项。标识方案应包括每个实体的版本、修订和发布状态。

5.16.2 配置控制

开发方应建立并执行:

- a) 指定每个已被标识实体必须经受的控制级别(例如,作者控制、项目级控制、需方控制)的规程;
 - b) 指定在每个级别上有权进行更改和批准更改的个人或组(例如,程序员/分析员、软件负责人、项目经理、需方)的规程;
 - c) 申请批准更改、处理更改申请、跟踪更改、分发更改和保持过期版本等工作所应遵循的步骤。
- 对已由需方控制的实体有影响的更改,应按合同规定的形式和手续(若有的话)向需方提出建议。

注:本标准中的许多要求涉及到“项目级或更高级配置控制”。若一个项目未选定“项目级”作为一个控制级别,那么软件开发计划宜说明如何将这要求映射到所选定的级别上。

5.16.3 配置状态记实

开发方应建立并在整个合同期间保持已经置于项目级或更高级别配置控制下的所有实体的配置状态的记录。这些记录可包括每个实体的当前版本/修正版/发布版、对该实体自纳入项目级或更高级别配置控制下后进行更改的记录、以及影响该实体的问题/更改报告的状态。

5.16.4 配置审核

开发方应为需方按合同规定进行配置审核提供支持。

注:配置审核可以称为功能配置审核和物理配置审核。

5.16.5 软件发行管理和交付

开发方应建立并执行可交付软件产品的包装、存储、处理和交付的规程。开发方在合同期内应保持可交付软件产品的主拷贝。

注:关于软件配置管理的进一步要求,见 GJB 5235-2004。

5.17 软件产品评价

5.17.1 过程中的和最终的软件产品评价

开发方应对执行本标准要求的软件产品进行过程中的评价。此外,对每一个交付的软件产品,在交付之前,开发方应进行最终的评价。附录 E 给出了需要评价的软件产品、应用的准则以及准则的定义。

5.17.2 软件产品评价记录

开发方应准备并保持每个软件产品的评价记录。这些记录在合同期内均应保持。置于项目级或更高级配置控制下的软件产品的问题应按 5.19 的要求进行处理。

5.17.3 软件产品评价的独立性

负责软件产品评价的人员应不是开发该软件产品的人员,但这并不排除开发该软件产品的人员参加评价工作(例如,参加该产品的走查)。

5.18 软件质量保证

5.18.1 软件质量保证评价

开发方应对软件开发活动和得到的软件产品,按计划定期地或事件驱动地进行评审和审核:

- a) 保证合同中或软件开发计划中要求的每项活动都按照合同和软件开发计划进行;
- b) 保证合同中或软件开发计划中要求的每项软件产品都存在,并已进行了本标准 and 合同条款所要求的软件产品的评价、测试和纠正措施。

5.18.2 软件质量保证记录

开发方应为每个软件质量保证活动准备并保持记录。这些记录在合同期内均应保持。置于项目级或更高级配置控制下的软件产品中的问题和在合同要求的和软件开发计划所说明的活动中的问题都应按 5.19 的要求进行处理。

5.18.3 软件质量保证的客观性

负责进行软件质量保证评价的人员应不是开发该软件产品、执行该项活动或者负责该软件产品或活动的人员。但这并不排除后者参加评价工作。负责软件质量保证的人员应具有资源、职责、权限和组织上的独立性,以便能够进行客观的软件质量保证评价并启动和验证纠正措施。

5.19 纠正措施

5.19.1 问题/更改报告

开发方应编写问题/更改报告,说明在置于项目级或更高级配置控制下的软件产品中发现的每一个问题,以及在合同要求或在软件开发计划所说明的活动中的每一个问题。问题/更改报告应描述问题,所需的纠正措施和至今已采取的纠正措施。这些报告应作为纠正措施系统的输入信息。

5.19.2 纠正措施系统

开发方应实现一个纠正措施系统,以处理置于项目级或更高级配置控制下的软件产品中所发现的每一个问题,以及在合同或在软件开发计划所描述的活动中的每一个问题。该系统应满足下列要求:

- a) 该系统的输入信息应由问题/更改报告组成;
- b) 该系统应是闭环的。确保所发现的问题能及时报告并进入该系统,纠正工作得以启动并且问题得到解决,状态得以跟踪,并且问题的记录在合同期内得以保持;
- c) 每一个问题应按附录 D 中给出的或其他经批准的类别和严重性等级的规定进行分类;
- d) 对报告中提出的问题应加以分析并预测其趋势;
- e) 对纠正措施应进行评价,以确定问题是否已得到解决,不利趋势是否得到扭转,更改是否已正确地实现且未引起另外的问题。

5.20 联合评审

5.20.1 联合技术评审

开发方应计划并参与联合技术评审,地点和时间由开发方提出并经需方批准。评审应由具有被评审软件产品的技术知识的人员参加。这种评审应集中在过程中的和最终的软件产品上,而不是在专为该评审准备的资料上。联合技术评审应实现下列目标:

- a) 应用附录 E 中提供的软件产品评价准则对演进中的软件产品进行评审;对提出的技术方案进行评审并演示;对技术工作提供深入的了解并获得反馈;暴露并解决技术问题;
- b) 评审项目状态,暴露关于技术、成本和计划进度等问题的近期和长期风险;
- c) 在参加评审人员的权限内,对已标识风险的缓解策略达成一致;
- d) 明确将在联合管理评审中提出的风险和问题;
- e) 确保在需方与开发方的技术人员之间及时沟通。

5.20.2 联合管理评审

开发方应计划并参与联合管理评审,地点和时间由开发方提出并经需方批准。联合管理评审前,需方应已事先评审了所考虑的工作产品,并且为解决存在的问题已进行了一次或多次联合技术评审。联合管理评审应由对成本和进度有决策权的人员参加,并应实现下列目标:

- a) 使管理者全面了解项目的状态、遵循的法规、达成的技术协议,以及演进中的软件产品的总体状态;

- b) 解决在联合技术评审中未能解决的问题;
- c) 对在联合技术评审中不能解决的近期和长期风险的缓解策略达成一致;
- d) 明确并解决在联合技术评审时未提出的管理级的问题和风险;
- e) 获得按时完成项目所需的承诺和需方批准。

5.21 测量和分析

开发方应在整个软件开发过程中对有关过程和产品进行必要的测量和分析,应利用测度支持管理和提高产品质量,并向需方通报有关状态。附录 F 给出了可供选用的测度例子。开发方应:

- a) 制定测量与分析计划,其中应反映 b)、c)、d)和 e)的内容,该计划也可以纳入软件开发计划中;
- b) 根据具体项目的需要标识和定义一组测度;
- c) 明确要采集的数据;
- d) 说明这些数据的解释和应用的方法;
- e) 建立测量数据的管理和报告机制;
- f) 按计划要求收集、解释、应用和报告测量与分析的结果。

注:关于测量和分析的进一步要求,参见 GJB 5000A-2008 中 6.2 测量和分析过程域。

5.22 风险管理

开发方应在整个软件开发过程中进行风险管理。开发方应:

- a) 制定风险管理计划,风险管理计划也可以纳入软件开发计划中;
- b) 标识、分析和排序软件开发项目中潜在的技术、成本和进度风险;
- c) 制定管理风险的策略;
- d) 实施风险管理策略,跟踪和控制风险。

注:关于风险管理的进一步要求,参见 GJB 5000A-2008 中 6.3 项目监控过程域中 SP1.3 监督项目风险、6.4 项目策划过程域中 SP2.2 标识项目风险以及 7.8 风险管理过程域。

5.23 保密性有关活动

开发方应满足合同中规定的保密性方面的要求。这些要求可能会影响软件开发工作,影响所得到的软件产品,或同时影响两者。

5.24 分承制方管理

如果有分承制方,那么开发方应将所有必要的主合同要求纳入子合同,以确保按照主合同要求开发软件产品。

注:关于分承制方管理的进一步要求,参见 GJB 5000A-2008 中 6.7 供方协议管理过程域。

5.25 与软件独立验证和确认(IV&V)机构的联系

开发方应按合同规定和软件独立验证和确认(IV&V)机构建立联系。

5.26 与相关开发方的协调

开发方应按合同规定与相关开发方、工作组等进行协调。相关开发方指的是在同一个或有关的系统中承担与本软件相关的其他开发工作的组织,不包括本软件分承制方。

5.27 项目过程的改进

开发方应:

- a) 定期评估项目所使用的过程,以确定其适用性和有效性;
- b) 基于这些评估,标识对这些过程必要和有益的改进;
- c) 以建议修订软件开发计划的形式标明这些改进,如果获得批准,则对该项目实现这些改进。

注:关于过程改进的进一步信息,参见 GJB 5000A-2008 中 7.4 组织过程焦点过程域。

附录 A
(资料性附录)
活动与多个构建版的映射

表 A.1 提供了活动如何应用到多个构建版的例子。关于策划构建版、确定每个构建版有哪些活动以及如何安排这些活动的指南参见附录 G。

表 A.1 活动与多个构建版的一种可能的映射

活动	构建版			
	构建版 1	构建版 2	构建版 3	构建版 4
5.2 项目策划和监控	√	√	√	√
5.3 软件开发环境建立	√	√	√	√
5.4 系统需求分析	√	√		
5.5 系统设计	√	√	√	
5.6 软件需求分析	√	√	√	√
5.7 软件设计	√	√	√	√
5.8 软件实现和单元测试	√	√	√	√
5.9 单元集成和测试	√	√	√	√
5.10 CSCI 合格性测试		√	√	√
5.11 CSCI/HWCI 集成和测试		√	√	√
5.12 系统合格性测试			√	√
5.13 软件使用准备	√	√	√	√
5.14 软件移交准备				√
5.15 软件验收支持	√	√	√	√
5.16 软件配置管理	√	√	√	√
5.17 软件产品评价	√	√	√	√
5.18 软件质量保证	√	√	√	√
5.19 纠正措施	√	√	√	√
5.20 联合评审	√	√	√	√
5.21 测量和分析	√	√	√	√
5.22 风险管理	√	√	√	√
5.23 保密性有关活动	√	√	√	√
5.24 分承制方管理	√	√	√	√
5.25 与软件独立验证和确认 (IV&V) 机构的联系	√	√	√	√
5.26 与相关开发方的协调	√	√	√	√
5.27 项目过程的改进	√	√	√	√
注：“√”表示采用这个活动。				

附录 B

(规范性附录)

采用可重用软件产品对本标准的解释

B.1 可重用软件产品的评价准则

开发方应在软件开发计划中规定为满足合同要求而采用的可重用软件产品的评价准则。一般准则是软件产品满足规定要求的能力和在系统寿命期内费效比较优。具体准则的例子如下：

- a) 提供所需功能并满足所需约束的能力。
- b) 提供所需安全性和保密性的能力。
- c) 由已建立的跟踪记录所证实的可靠性/成熟度。
- d) 可测试性。
- e) 与其他系统及系统外部元素的互操作性。
- f) 现场部署问题，包括：
 - 1) 对复制/分发软件或文档的限制；
 - 2) 适用于每份拷贝的许可或其他费用。
- g) 可维护性，包括：
 - 1) 该软件产品将需要修改的可能性；
 - 2) 实现这一修改的可行性；
 - 3) 文档和源文件的可用性与质量；
 - 4) 供方继续支持当前版本的可能性；
 - 5) 在当前版本得不到支持时，对系统的影响；
 - 6) 需方对软件产品的资料权限；
 - 7) 可得到的保证期。
- h) 使用该软件产品的短期及长期费用影响。
- i) 使用该软件产品的技术、成本及进度风险，以及所作的权衡。

B.2 针对可重用软件产品对本标准活动的解释

下列规则适用于解释本标准：

- a) 任何要求开发软件产品的需求都可以用能实现这些需求并满足软件开发计划中所确立准则的可重用软件产品来满足。可重用软件产品可按其原样使用，或修改后使用，可以用来满足部分或全部需求。例如，某个需求可通过使用现有的计划、规格说明或设计得到满足。
- b) 当要采用的可重用软件产品是软件本身时，本标准中的某些要求需作特定的解释。表 B.1 提供了这种解释。关键在于该软件是否要修改；不修改的软件是组成一个完整的 CSCI 还是仅仅是其中的一个或多个软件单元；不修改的软件是否有良好的执行记录（作这种判断不存在严格准则）。

表 B.1 采用可重用软件产品对本标准的解释

本标准要求的活动	可重用软件产品					对在项目执行期间要作修改的软件单元
	对不作修改便可使用的 CSCI		对不作修改便可使用的软件单元			
	有良好的执行记录	执行记录没有或不全	有良好的执行记录	执行记录没有或不全		
5.2 项目策划和监控	项目计划包含本表中的活动。					

表 B.1 (续)

本标准要求的活动	可重用软件产品				
	对不作修改便可使用的 CSCI		对不作修改便可使用的软件单元		对在项目执行期间要作修改的软件单元
	有良好的执行记录	执行记录没有或不全	有良好的执行记录	执行记录没有或不全	
5.3 软件开发环境建立	合适时, 为执行本表中的活动, 建立和应用软件测试环境、软件开发资料库和软件开发文件。				应用本条的全部要求。
5.4 系统需求分析	在定义运行方案和系统需求时, 考虑软件的能力。				
	使用测试/执行记录去核实满足需要的能力。	测试以核实满足需要的能力。	使用测试/执行记录去核实满足需要的能力。	测试以核实满足需要的能力。	使用测试或记录来确定满足需要的潜力。
5.5.1 系统级设计决策	在设计系统行为和作其他系统级设计决策时, 考虑软件的能力与特性。				
5.5.2 系统体系结构设计	在系统的体系结构中纳入该 CSCI 并对其分配系统需求。		在指定的 CSCI 中考虑该单元的能力与特性, 并对其分配系统需求。		
5.6 软件需求分析	规定该 CSCI 必须满足的项目特定需求; 通过记录或回归测试验证该 CSCI 能满足这些需求。		在规定 CSCI 的需求时, 考虑作为其一部分的该单元的能力与特性。		
5.7.1 CSCI 级设计决策	不要求: CSCI 级设计决策已经进行。(记录“已建成”设计是 5.14 中的活动)		在设计 CSCI 行为和作其他 CSCI 级设计决策时, 考虑该单元的性能与特性。		
5.7.2 CSCI 体系结构设计	不要求: CSCI 的体系结构已定义。(记录“已建成”设计是 5.14 中的活动)		在 CSCI 的体系结构中纳入该单元, 并对它分配 CSCI 需求。		
5.7.3 CSCI 详细设计	不要求: CSCI 的详细设计已定义。(记录“已建成”设计是 5.14 中的活动)		不要求: 该单元已设计。(记录“已建成”设计是 5.14 中的活动)		根据需要修改该单元的设计。
5.8.1 软件实现	不要求: 该 CSCI 的各单元软件均已实现。		不要求: 该单元软件已实现。		修改该单元的软件。
5.8.2~5.8.5 单元测试	不要求: 该 CSCI 的单元已测试。	如有疑问并且单元可访问, 就有选择地执行。	不要求: 该单元已测试。	执行此项测试。	
5.9 单元集成和测试	不要求: 该 CSCI 的单元已集成。	如有疑问并且单元可访问, 就有选择地执行。	执行, 但已经作过测试/验证的集成除外。	执行此项测试。	
5.10 CSCI 合格性测试	不要求: CSCI 已经作过测试/验证。	执行此项测试。	将该单元纳入 CSCI 合格性测试。		
5.11 CSCI/HWCI 集成和测试	执行, 但已作过测试和验证的集成除外。	将该 CSCI 纳入 CSCI/HWCI 的集成和测试。	将该单元纳入 CSCI/HWCI 的集成和测试。		
5.12 系统合格性测试	将该 CSCI 纳入系统合格性测试。		将该单元纳入系统合格性测试。		
5.13 软件使用准备	将该 CSCI 或单元的软件纳入可执行软件; 纳入版本说明; 处理许可问题; 适当时, 通过现有、新编或修改了的用户/操作员手册涵盖该 CSCI 或单元的使用; 作为全系统的一个部分安装该 CSCI 或单元; 适当时, 把它的使用包括在提供的培训中。				
5.14 软件移交准备	将该 CSCI 或单元的软件纳入可执行软件; 如果可得到, 为它们准备源文件; 纳入版本说明; 处理许可问题; 为已知设计的软件准备或提供“已建成”的设计说明; 在保障机构现场安装该 CSCI 或单元; 如果源程序可得到则演示重新生成的能力; 纳入提供的培训中。				

表 B. 1 (续)

本标准要求的活动	可重用软件产品				
	对不作修改便可使用的 CSCI		对不作修改便可使用的软件单元		对在项目执行期间要作修改的软件单元
	有良好的执行记录	执行记录没有或不全	有良好的执行记录	执行记录没有或不全	
5.15 软件验收支持	将该 CSCI 纳入软件验收。注意不重复已做过的测试、评审和审核。		将该单元纳入软件验收。注意不重复已做过的测试、评审和审核。		
5.16 软件配置管理	应用于组成该软件的所有已准备的、修改的、或使用的软件产品。				
5.17 软件产品评价	应用于组成该软件的所有已准备的或修改的软件产品；对于使用而未修改的软件产品也适用，除非有可信的执行记录或有以往的评价证据表明这种评价是重复的。				
5.18 软件质量保证	应用于所有执行的活动和在组成该软件的所有已准备的、修改的、或使用的软件产品。				
5.19 纠正措施	应用于所有执行的活动和在组成该软件的所有已准备的或修改的软件产品。				
5.20 联合评审	包括组成该软件的所有已准备的或修改的软件产品。				
5.21 测量和分析	应用本条的全部要求。				
5.22 风险管理	应用本条的全部要求。				
5.23 保密性有关活动	应用本条的全部要求。				
5.24 分承制方管理	不要求。			应用本条的全部要求。	
5.25 与独立验证和确认 IV&V 机构的联系	应用本条的全部要求。				
5.26 与相关开发方的协调	应用本条的全部要求。				
5.27 项目过程的改进	不要求。		应用本条的全部要求。		
注：对于给定的可重用软件类型，如果需要本标准要求的某项活动时，该表针对该活动给出了相应解释。					

附录 C
(资料性附录)

一个系统或 CSCI 按多个构建版开发时各项活动的实施建议

C.1 项目策划和监控的实施建议

如果一个系统或 CSCI 按多个构建版开发,那么每一个构建版的策划宜解释为:

- a) 合同的总体策划;
- b) 当前构建版的详细策划;
- c) 涉及合同中后续构建版的策划,其详细程度与可用的信息相一致。

C.2 软件开发环境建立的实施建议

如果一个系统或 CSCI 按多个构建版开发,那么在每一个构建版建立软件开发环境宜理解为建立完成该构建版的任务所需要的环境。

C.3 系统需求分析的实施建议

如果系统按多个构建版开发,那么系统需求可能到最后一个构建版的需求确定后才完全定义。开发方的策划宜标识在每个构建版中要定义的系统需求子集和在每个构建版中要实现的子集。对一个特定构建版的系统需求分析宜理解为对那些已标识为该构建版的系统需求的定义。

C.4 系统设计的实施建议

如果系统按多个构建版开发,那么系统设计可能到最后一个构建版的设计确定后才完全定义。开发方的策划宜标识每个构建版中要定义的系统设计部分。特定构建版的系统设计宜理解为对已标识为该构建版的系统设计部分的定义。

C.5 软件需求分析的实施建议

如果 CSCI 按多个构建版开发,那么它的需求可能到最后一个构建版才完全定义。开发方的策划宜标识每个构建版中要定义的 CSCI 需求的子集和每个构建版中要实现的子集。对一个给定构建版的软件需求分析宜理解为对已标识为该构建版的 CSCI 需求的定义。

C.6 软件设计的实施建议

如果 CSCI 按多个构建版开发,那么它的设计可能要到最后一个构建版才完全定义。每个构建版中的软件设计宜满足分配到该构建版的 CSCI 需求。

C.7 软件实现和单元测试的实施建议

如果 CSCI 按多个构建版开发,那么该 CSCI 的软件实现和单元测试要持续到最后一个构建版才能完成。在每个构建版中软件实现和单元测试宜理解为对那些为满足要在该构建版中实现的 CSCI 需求所需的软件单元(或单元的某些部分)的实现和测试。

C.8 单元集成与测试的实施建议

如果一个 CSCI 按多个构建版开发,那么这个 CSCI 的单元集成和测试工作将持续到最后一个构建版才能完成。每一个构建版中的单元集成和测试工作宜理解为将在这个构建版中开发的软件与在这个构建版和以前的构建版中开发的其他软件集成起来并测试。

C.9 CSCI 合格性测试的实施建议

如果 CSCI 按多个构建版开发,那么该 CSCI 合格性测试要持续到该 CSCI 的最后一个构建版,或可能持续到后面包含与该 CSCI 有接口关系的其他配置项的构建版才能完成。对每个构建版的 CSCI 合格性测试宜理解为每个 CSCI 当前构建版测试的策划与执行,以确保在该构建版中要实现的 CSCI 各项需求已经得到满足。

C.10 CSCI/HWCI 集成和测试的实施建议

如果系统或 CSCI 按多个构建版开发,那么 CSCI/HWCI 集成和测试工作要持续到最后一个构建版才能完成。每一构建版进行的 CSCI/HWCI 集成和测试宜理解为将每个 CSCI 的当前构建版与其他 CSCI 的当前构建版及 HWCI 集成起来并测试,以确保在该构建版要实现的系统需求已经得到满足。

C.11 系统合格性测试的实施建议

如果系统按多个构建版开发,整个系统的合格性测试要到最后一个构建版才进行。每个构建版中的合格性测试宜理解为策划和执行系统当前构建版的测试,以确保要在该构建版实现的系统需求已经得到满足。

C.12 软件使用准备的实施建议

如果软件按多个构建版开发,那么开发方的策划宜标明每个构建版中要在用户现场安装什么软件(若有的话),安装到什么范围(如全部安装或只给选定的评价人员安装)。对每个构建版的软件使用准备工作宜理解为包括为执行该构建版的安装计划所必需的那些活动。

C.13 软件移交准备的实施建议

如果软件按多个构建版开发,那么开发方的策划宜明确在每个构建版中要向保障机构提供什么软件(若有)。对每个构建版中软件移交的准备工作宜理解为为执行该构建版的移交计划所必需的那些活动。

C.14 软件验收支持的实施建议

如果系统或 CSCI 按多个构建版开发,那么整个系统或 CSCI 的验收要到最后一个构建版完成时才进行。每个构建版中的软件验收宜理解为策划和执行当前构建版的验收,以确保要在该构建版实现的系统需求已经得到满足。

C.15 软件配置管理的实施建议

如果系统或 CSCI 按多个构建版开发,那么每个构建版的软件产品可能是前面一些构建版软件产品的精细化或是对它们的增加部分。对每一个构建版的软件配置管理宜理解为是在该软件产品上下文中发生的,并且控制是在该构建版开始时就位的。

C.16 软件产品评价的实施建议

如果系统或 CSCI 按多个构建版开发,那么每个构建版的软件产品宜以该构建版建立的目标为依据进行评价。满足这些目标的软件产品就可认为是满意的,即使它遗漏了后面构建版开发工作所需要的信息也无妨。

C.17 软件质量保证的实施建议

如果系统或 CSCI 按多个构建版开发,那么每个构建版的活动和软件产品的评价宜以该构建版建立的目标为依据。满足这些目标的活动或软件产品就可认为是满意的,即使遗漏了一些为后面构建版所需的信息也无妨。软件质量保证策划包括在软件开发策划(见 5.2.1)中。

C.18 联合评审的实施建议

如果系统或 CSCI 按多个构建版开发,那么联合评审的类型和采用的准则就依赖于每个构建版的目标。能满足这些目标的软件产品就可认为是满意的,即使它们遗漏了为后面构建版开发所需要的信息也无妨。

附录 D
(规范性附录)
问题报告的类别及严重性等级

D.1 范围

本附录包含对提交给纠正措施系统的每个问题的类别及严重性等级划分方面的要求,但这些要求可由需方进行剪裁;如果得到需方的认可,开发方可以使用替代的问题分类方法及严重性等级划分方法。

D.2 问题类别

开发方应:

- a) 对软件产品中的每个问题指派表 D.1 中的一个或多个类别;
- b) 对活动中的每个问题指派表 A.1 中的一个或多个活动类别(见附录 A)。

表 D.1 软件产品问题的类别

问题类别	适用于下列范围的问题
计划	为项目制定的计划
方案	运行方案
需求	系统需求或软件需求
设计	系统设计或软件设计
编码	软件编码
数据库/数据文件	数据库或数据文件
测试信息	测试计划、测试说明或测试报告
手册	用户、操作员手册或保障手册
其他	其他软件产品

D.3 严重性等级

开发方应对软件产品或活动中的每个问题指派表 D.2 中的一个严重性等级。

表 D.2 问题的严重性等级

严重性等级	所适用的问题性质
1	a) 有碍于运行或任务的基本能力的实现。 b) 危害安全性、保密性或其他指定为“关键的”要求。
2	a) 对运行或任务的基本能力产生不利影响且没有已知的变通解决方案。 b) 对项目的技术、费用或进度风险或对系统寿命期的支持产生不利影响,且没有已知的变通解决方案。
3	a) 对运行或任务的基本能力产生不利影响,但变通解决方案已知。 b) 对项目的技术、费用或进度风险或对系统寿命期的支持产生不利影响,但变通解决方案已知。
4	a) 给用户/操作员带来不便或烦恼;但不影响所要求的运行或任务的基本能力。 b) 给开发或支持人员带来不便或烦恼;但不妨碍所要求工作的完成。 c) 任何其他影响。

附录 E
(规范性附录)
软件产品评价

E.1 范围

本附录指出要进行评价的软件产品以及评价所使用的准则，并给出这些评价准则的定义。本附录的要求可由需方进行剪裁；如果得到需方的认可，开发方可以使用替代的准则或定义。

E.2 软件产品及其评价准则

表 E.1 给出应进行评价的软件产品，并给出了其评价的准则。对每个软件产品及准则均加了标号，以便于标识和剪裁。软件产品用阿拉伯数字标识；评价准则用准则和阿拉伯数字标识。E.3 给出了那些含意不能自明的准则的定义，准则 15 含意自明，无需重复定义。

为了进行评价，软件产品可以硬拷贝或非硬拷贝的形式提交。对于系统级产品评价应解释为参与^a这些评价。有些评价准则是主观的，因此，不要求证明这些准则已得到满足，只要求使用这些准则进行评价并指出可能存在的问题，以便讨论和解决。

^a 本标准要求软件开发方参与软件所在系统层面的活动。若所在系统是硬件-软件系统(例如一个雷达系统)，则“参与”指参加；若所在系统是软件系统(例如一个地理信息系统)，则“参与”是指负责。

E.3 准则定义**E.3.1 准则 1: 准确陈述(某项)**

该准则适用于用户/操作员/程序员的操作，以及“已建成”的设计与版本的描述，表示这些操作或描述正确地陈述了该软件或其他所描述的项。

E.3.2 准则 2: 充分的测试用例、规程、数据和结果

如果测试用例覆盖了所有适用的需求或设计决定，并且详细说明了所使用的输入、预期的结果以及用来评价这些结果的准则，那么这些测试用例就是充分的。如果测试规程详细说明了执行每个测试用例要遵循的步骤，那么这些测试规程就是充分的。如果测试数据使能执行所计划的测试用例和测试规程，那么这些测试数据就是充分的。如果测试或预演能说明所有测试用例的结果，并指出所有的准则均已得到满足(可能经过修改和回归测试之后)，那么这些测试或预演结果就是充分的。

E.3.3 准则 3: 与指定的产品一致

该准则表示：

- a) 一个软件产品的陈述或表示与另一个指定软件产品的陈述或表示不相矛盾；
- b) 给定的术语、首字母缩写词或缩写词在所有的软件产品中具有相同的含义；
- c) 在所有的软件产品中，用相同的名字或描述引用一个给定条款或概念。

E.3.4 准则 4: 包含(某特定文档中)所有适用的信息

该准则用文档来指定要求软件产品具有的内容，而不管某个可交付文档是否已订购。对每个文档的章条标题的适用范围可做调整。文档中所规定的格式(即所要求的章条划分和编号)与本评价无关。

E.3.5 准则 5: 覆盖(给定的一组条款)

一个软件产品“覆盖”了给定的一组条款是指该组中的每一个条款均已在该软件产品中得到安排。例如，一个计划覆盖了工作说明(SOW)，是指工作说明(SOW)中的每一条规定均在该计划中得到了安排；一个设计覆盖了一组需求，是指在这个设计中每一项需求均得到了处理；一个测试计划覆盖了一组需求，是指每一项需求都是一个或多个测试的主题。“覆盖”对应于需求、设计、以及测试计划/说明等文档的向下可追踪性(例如，从需求到设计)。

E.3.6 准则 6: 可行

该准则表示, 根据评价者的学识和经验, 给定的方案、一组需求、设计、测试等没有违反已知的原则或经验教训, 否则将不可能实现。

E.3.7 准则 7: 遵循软件开发计划

该准则表示, 有证据表明该软件产品一直按照软件开发计划所要求的方式进行开发。例如, 遵循了计划所要求的设计与编码标准。对软件开发计划本身, 该准则适用于对最初的计划进行的修订。

E.3.8 准则 8: 内部一致

该准则表示:

- a) 在一个软件产品中不存在彼此矛盾的两种陈述或表示;
- b) 贯穿该软件产品, 给定的术语、首字母缩写词或缩写词具有相同的含义;
- c) 贯穿该软件产品, 用相同的名字或描述引用一个给定条款或概念。

E.3.9 准则 9: 满足合同资料要求清单要求(如适用)

如果被评价的软件产品是合同资料要求清单所规定的, 且已安排在评价期间交付, 则本准则适用。本准则关注的是合同资料要求清单中规定的格式、标记及其他条款, 而不是其他准则所涉及的内容。

E.3.10 准则 10: 满足工作说明或软件研制任务书要求(如适用)

该准则表示软件产品满足工作说明(SOW)或软件研制任务书(SDTD)中对它提出的所有要求。例如, SOW 或 SDTD 可能对运行方案或设计提出约束条件。

E.3.11 准则 11: 提出的方法合理

该准则表示, 根据评价者的知识及经验认为, 所给定的计划描述了执行这些必要活动的合理方法。

E.3.12 准则 12: 显示出(受测试项目)满足要求的证据

该准则表示, 已记录的测试结果表明, 受测试项或是一次通过了全部测试, 或是经过修改和回归测试最终通过各种测试。

E.3.13 准则 13: 可测试

对于一个需求或一组需求, 如果能够设计一个客观可行的测试用以确定每个需求是否得到满足, 就称其为可测试的。

E.3.14 准则 14: 可理解

该准则表示“能为预期的读者所理解”。例如, 为程序员之间交流所提供的软件产品就无需为非程序员所理解。产品正确地指明了它的读者且对于这些读者是可理解, 则认为符合本准则。

表 E.1 软件产品和相关的评价准则

软件产品	评价准则						附加准则
	准则 4: 包含如下文档中所有适用的信息	准则 10: 满足 SOW 或 SDTD 要求	准则 9: 满足合同资料要求清单要求	准则 14: 可理解	准则 8: 内部一致	准则 7: 遵循软件开发计划	
1. 软件开发计划(5.2.1)	√ SDP	√	√	√	√	√{修订}	准则 5: 覆盖 SOW 或 SDTD 及合同资料要求清单中所有活动/可交付项; 准则 3: 与其他项目计划一致; 准则 11: 提出合理的开发方法。
2. 软件配置管理计划(5.2.1)	√ SCMP	√	√	√	√		准则 3: 与项目计划一致; 准则 11: 提出合理的管理方法。
3. 软件质量保证计划(5.2.1)	√ SQAP	√	√	√	√		准则 3: 与项目计划一致; 准则 11: 提出合理的管理方法; 准则 12: 显示出满足要求的证据。

表 E.1(续)

软件产品	评价准则						附加准则
	准则 4: 包含如下文档中所有适用的信息	准则 10: 满足 SOW 或 SDTD 要求	准则 9: 满足合同资料要求清单要求	准则 14: 可理解	准则 8: 内部一致	准则 7: 遵循软件开发计划	
4. 软件测试计划(5.2.2, 5.2.3)	√ STP	√	√	√	√	√	准则 5: 覆盖 SOW 或 SDTD 中所有与软件有关的合格性活动; 准则 5: 覆盖受测试项的所有要求; 准则 3: 与其他项目计划一致; 准则 11: 提出合理的测试方法。
5. 软件安装计划(5.2.4)	√ SIP	√	√	√	√	√	准则 5: 覆盖 SOW 或 SDTD 中所有用户现场安装活动; 准则 3: 与其他项目计划一致; 准则 11: 提出合理的安装方法。
6. 软件移交计划(5.2.5)	√ STrP	√	√	√	√	√	准则 5: 覆盖 SOW 或 SDTD 中所有与移交有关的活动; 准则 3: 与其他项目计划一致; 准则 11: 提出合理的移交方法。
7. 运行方案(5.4.2)	√ OCD	√	√	√	√	√	准则 6: 可行。
8. 系统需求(5.4.3)	√ SSS, IRS	√	√	√	√	√	准则 5: 覆盖运行方案; 准则 6: 可行; 准则 13: 可测试。
9. 系统级设计决策(5.5.1)	√ SSDD, IDD, DBDD	√	√	√	√	√	准则 3: 与系统需求一致; 准则 6: 可行。
10. 系统体系结构设计(5.5.2)	√ SSDD, SDTD, IDD	√	√	√	√	√	准则 5: 覆盖系统需求; 准则 3: 与系统级设计决策一致; 准则 6: 可行。
11. CSCI 需求(5.6)	√ SRS, IRS	√	√	√	√	√	准则 5: 覆盖分配到该 CSCI 的系统需求; 准则 6: 可行; 准则 13: 可测试。
12. CSCI 级设计决策(5.7.1)	√ SDD, IDD, DBDD	√	√	√	√	√	准则 3: 与 CSCI 需求一致; 准则 6: 可行。
13. CSCI 体系结构设计(5.7.2)	√ SDD, IDD	√	√	√	√	√	准则 5: 覆盖 CSCI 需求; 准则 3: 与 CSCI 级设计决策一致; 准则 6: 可行。
14. CSCI 详细设计(5.7.3)	√ SDD, IDD, DBDD	√	√	√	√	√	准则 5: 覆盖分配到每个单元的 CSCI 需求; 准则 3: 与 CSCI 级设计决策一致。
15. 已实现的软件(5.8.1)	—	√	√	√	√	√	准则 5: 覆盖 CSCI 详细设计。
16. CSCI 合格性测试说明(5.10.3)	√ STD	√	√	√	√	√	准则 5: 覆盖所有 CSCI 需求。

表 E. 1(续)

软件产品	评价准则						附加准则
	准则 4: 包含如下文档中所有适用的信息	准则 10: 满足 SOW 或 SDTD 要求	准则 9: 满足合同资料要求清单要求	准则 14: 可理解	准则 8: 内部一致	准则 7: 遵循软件开发计划	
17. CSCI 合格性测试结果 (5.10.7)	√ STR	√	√	√	√	√	准则 5: 覆盖所有计划的 CSCI 合格性测试用例; 准则 12: 显示证据证明 CSCI 满足其需求。
18. 系统合格性测试说明 (5.12.3)	√ STD	√	√	√	√	√	准则 5: 覆盖所有系统需求。
19. 系统合格性测试结果 (5.12.7)	√ STR	√	√	√	√	√	准则 5: 覆盖所有计划的系统合格性测试用例; 准则 12: 显示证据证明系统满足其需求。
20. 可执行软件 (5.13.1, 5.14.1)	—	√	√	√	√	√	准则 10: 满足交付要求; 准则 15: 执行所需的所有软件均已提供; 准则 3: 版本与通过测试的版本完全一致; 准则 1: 可交付的媒体已准确地作了标记。
21. 软件版本说明 (5.13.2, 5.14.3)	√ SVD	√	√	√	√	√	准则 1: 准确地标识所交付的每一个软件成分(文件、单元、CSCI 等)的版本; 准则 1: 准确地标识所纳入的修改。
22. 软件用户手册 (5.13.3.1)	√ SUM	√	√	√	√	√	准则 1: 对本手册预期的读者准确地描述软件的安装和使用。
23. 软件输入/输出手册 (5.13.3.2)	√ SIOM	√	√	√	√	√	准则 1: 对本手册预期的读者准确地描述软件的输入/输出。
24. 软件中心操作员手册 (5.13.3.3)	√ SCOM	√	√	√	√	√	准则 1: 对本手册预期的读者准确地描述软件的安装与运作。
25. 计算机操作手册 (5.13.3.4)	√ COM	√	√	√	√	√	准则 1: 准确地描述计算机的运行特性。
26. 源文件 (5.14.2)	√ SPS	√	√	√	√	√	准则 10: 满足交付要求; 准则 15: 存在所有要求的软件; 准则 3: 版本与通过测试的版本完全一致; 准则 1: 可交付的媒体已准确地做了标记。
27. “已建成”的 CSCI 设计及有关信息 (5.14.4)	√ SPS	√	√	√	√	√	准则 1: 准确地描述 CSCI 的“已建成”设计; 准则 1: 准确地描述编制/构建规程; 准则 1: 准确地描述修改规程; 准则 5: 源文件覆盖 CSCI 设计中的所有单元; 准则 10: 测量到的资源利用满足 CSCI 需求。

表 E. 1 (续)

软件产品	评价准则						附加准则
	准则 4: 包含如下文档中所有适用的信息	准则 10: 满足 SOW 或 SDTD 要求	准则 9: 满足合同资料要求清单要求	准则 14: 可理解	准则 8: 内部一致	准则 7: 遵循软件开发计划	
28. “已建成”的系统设计(5.14.5)	√ SSDD	√	√	√	√	√	准则 1: 准确地描述“已建成”的系统设计。
29. 计算机编程手册(5.14.6.1)	√ CPM	√	√	√	√	√	准则 1: 准确地描述计算机的编程特征。
30. 固件保障手册(5.14.6.2)	√ FSM	√	√	√	√	√	准则 1: 准确地描述固件的编程特征。
31. 软件研制总结报告(5.15.4)	√ SDSR	√	√	√	√	√	准则 1: 准确地反映了软件研制过程。
32. 软件配置管理报告(5.15.4)	√ SCMR	√	√	√	√	√	准则 1: 准确地反映了软件配置管理过程。
33. 软件质量保证报告(5.15.4)	√ SQAR	√	√	√	√	√	准则 1: 准确地反映了软件质量保证过程。
34. 软件开发文件的抽样(5.8.2, 5.8.5, 5.9.1, 5.9.4, 5.10.4, 5.11.1, 5.11.4, 5.12.4)	—	√	—	√	√	√	准则 15: 是正在进行中的最新内容; 准则 2: 有充分的单元测试用例/规程/数据/结果; 准则 2: 有充分的单元集成测试用例/规程/数据/结果; 准则 2: 有充分的 CSCI 合格性预演结果; 准则 2: 有充分的 CSCI/HWCI 集成测试用例/规程/数据/结果; 准则 2: 有充分的系统合格性预演结果。
注: 表中“√”表示适用, “—”表示不适用。							

附 录 F
(资料性附录)
可供选用的测度

如下给出了一组可供软件开发项目选择使用的测度：

- a) 需求易变性：在某段时间内需求及其变更的总数；
- b) 软件规模：在某段时间内计划的和实际的单元数量，代码行数或其他规模测量；
- c) 软件人员的配备：在某段时间内计划的和实际的配备水平；
- d) 软件的复杂性：每一个软件单元的复杂性；
- e) 软件进展：在某段时间内计划的和实际的已设计、实现、单元测试和集成的软件单元数量；
- f) 问题/变更报告状态：问题总数、已解决数、当前报告阶段尚未解决的数目、待解决时间、严重性等级；
- g) 构建版发布内容：每个构建版计划发布的和实际发布的软件单元的数量；
- h) 计算机硬件资源的利用：在某段时间内计划的和实际的计算机资源(例如处理器能力、内存容量、输入/输出设备能力、辅助存储设备的能力和通信/网络设备能力)的利用；
- i) 里程碑执行情况：计划的和实际的关键项目里程碑的日期；
- j) 报废/返工：在软件产品已置于项目级或更高级配置控制之下后，对它们进行替换或修正所花费的资源量；
- k) 重用效果：将重用软件产品的有关的指标与新的软件产品的相应的指标作比较。

附录 G
(资料性附录)
关于项目策略、剪裁和构建版策划的指南

G.1 范围

本附录给出三种项目策略，并指出在这些策略下如何应用本标准，以及在一个再工程项目中如何应用本标准。

G.2 可选择的项目策略

如下概述了三种项目策略，策略的关键特征见表 G.1。

- a) 一次完成设计。“一次完成设计”策略基本上是“一次设计，一次通过”的策略。简而言之，就是：确定用户需要、定义需求、设计系统、实现系统、测试、纠错和交付。
- b) 增量式。“增量式”策略确定用户需要和定义系统需求后，按构建版顺序依次完成其余的开发任务。第一个构建版纳入部分计划的能力，下一个构建版再增加一些能力等等，直到系统全部完成。
- c) 演进式。“演进式”策略也是按构建版开发系统，但与“增量式”不同之处是承认用户的需要不完全清楚，不可能预先定义全部需求。采用此策略时，用户需要和系统需求预先仅被部分地定义，然后在每个随后的构建版中逐步完善。

表 G.1 三种项目策略的关键特征

项目策略	首先定义所有需求？	存在多次开发循环？	现场安装中间软件？
一次完成设计	是	否	否
增量式	是	是	可能
演进式	否	是	是

G.3 选择一种合适的项目策略

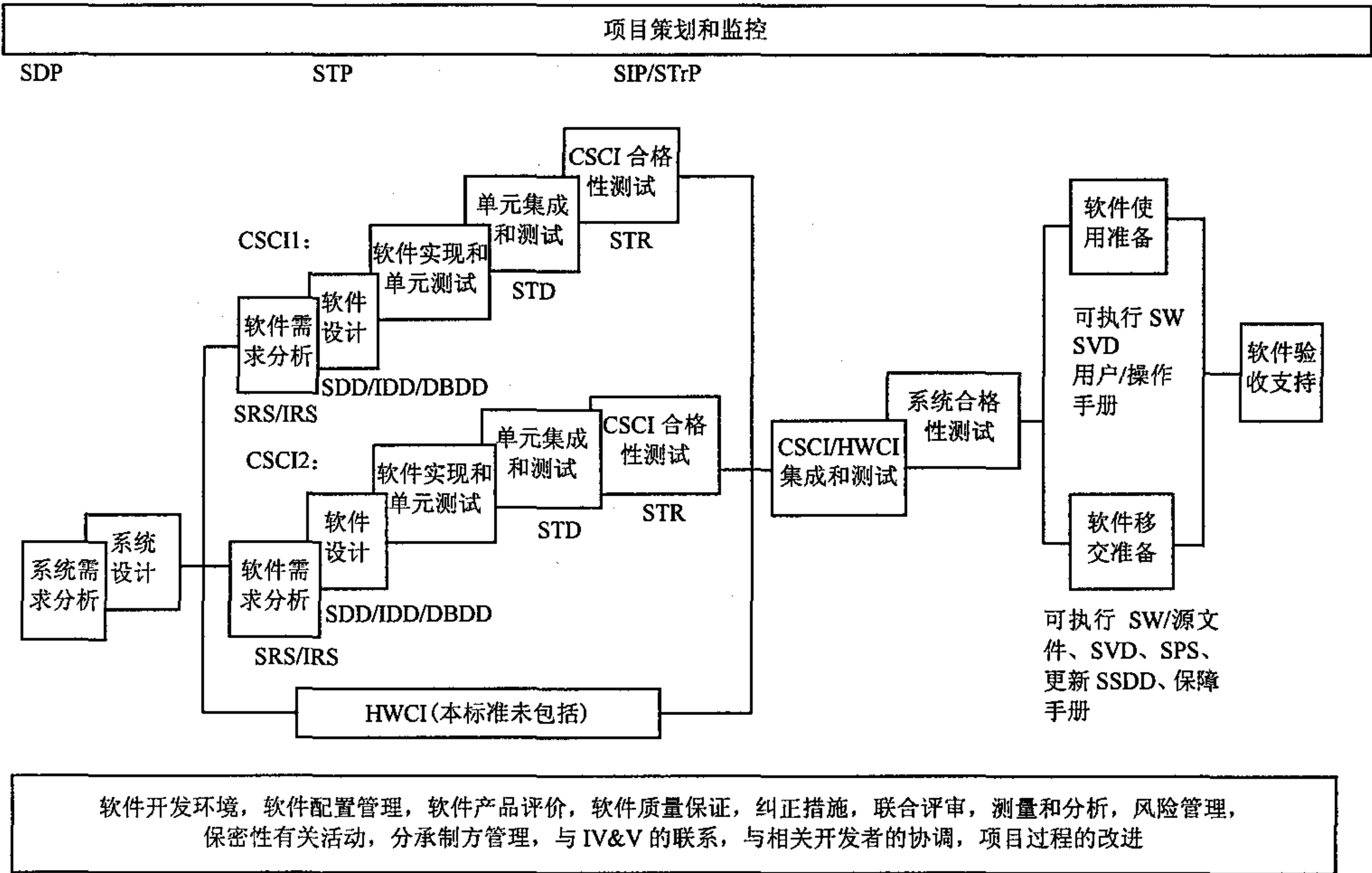
项目策略由需方选择，但未来的或已选定的开发方也可给出建议。图 G.1 说明选择一种合适策略所使用的风险分析方法，这种方法就是：列出每种策略的风险项(负面的)和机会项(正面的)；为每个项确定风险和机会的等级(高、中、低)；根据风险和机会的权衡做出使用哪种策略的决定。图 G.1 中的内容仅仅是个例子，实际分析可以使用其他方法，记录在最后一行中的“决定”表明选择了这种策略。

G.4 本标准与项目策略的关系

项目策略通常适用于整个系统。对系统中的软件可以采用相同的策略去获取，也可以采用不同的策略去获取，例如，要求所有软件均在系统的第一个构建版完成。图 G.2、图 G.3 和图 G.4 表明在图 G.1 中给出的每一种项目策略如何应用本标准。图 G.5 表明本标准如何应用于再工程的项目中。图 G.2~图 G.5 进行了必要的简化。例如，它们表示本标准的活动是依次进行的，而实际上这些活动是延续的、重叠的、迭代的；它们把每个软件产品看作一个单一实体，没有描述其早期草案和改进；它们用相应文档名表示每个软件产品，而该实际软件产品是该文档所要求的信息，不一定采用硬拷贝文档的形式。

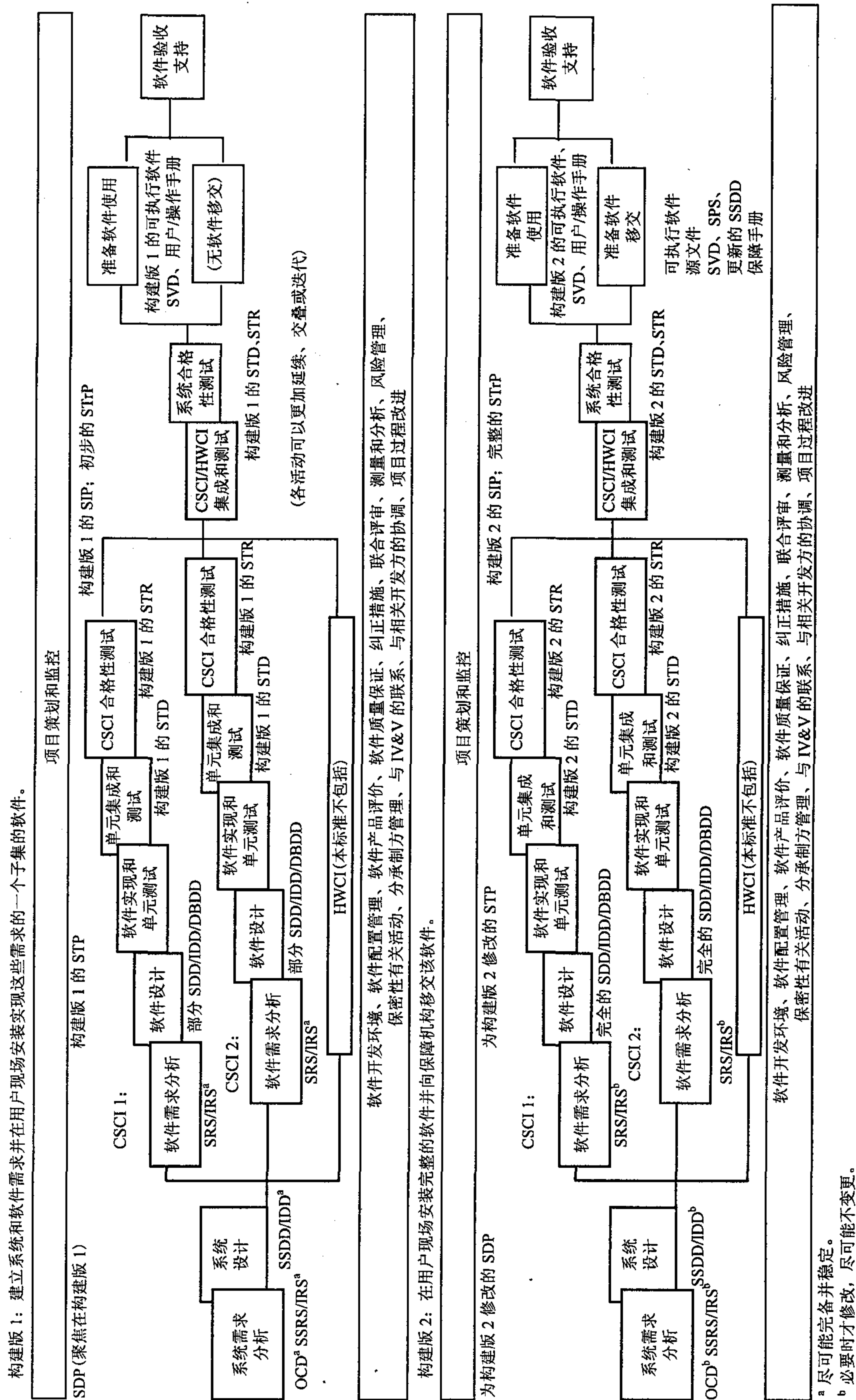
一次完成设计		增量式		演进式	
风险项 (反对这个策略的理由)	风险 级别	风险项 (反对这个策略的理由)	风险 级别	风险项 (反对这个策略的理由)	风险 级别
a) 没有很好地理解需求; b) 系统太大以至不能一次完成; c) 预期任务技术的快速变更-可能会导致需求的改变; d) 现在可用的人力或预算有限。	高中高 中	a) 没有很好地理解需求; b) 在第一次交付时用户就要求所有的能力; c) 预期任务技术的快速变更-可能会导致需求的改变。	高中高	在第一次交付时用户就要求所有的能力	中
机会项 (使用这个策略的理由)	机会 级别	机会项 (使用这个策略的理由)	机会 级别	机会项 (使用这个策略的理由)	机会 级别
a) 在第一次交付时用户就要求所有的能力; b) 用户要求立即取消旧的系统。	中 低	a) 需要早期能力; b) 系统自然地分解为增量; c) 财力/人力将逐步增加。	高中高	a) 需要早期能力; b) 系统自然地分解为增量; c) 财力/人力将逐步增加; d) 为理解全部需求, 需要得到用户的反馈和对技术变更进行监视。	高中高高
				决定: 使用该策略	

图 G.1 为确定适当的项目策略而进行风险分析的例子



注: 所有活动都可能比本图所示要更为延续、交叠和迭代。

图 G.2 本标准应用于一次完成设计策略的一种可能方式



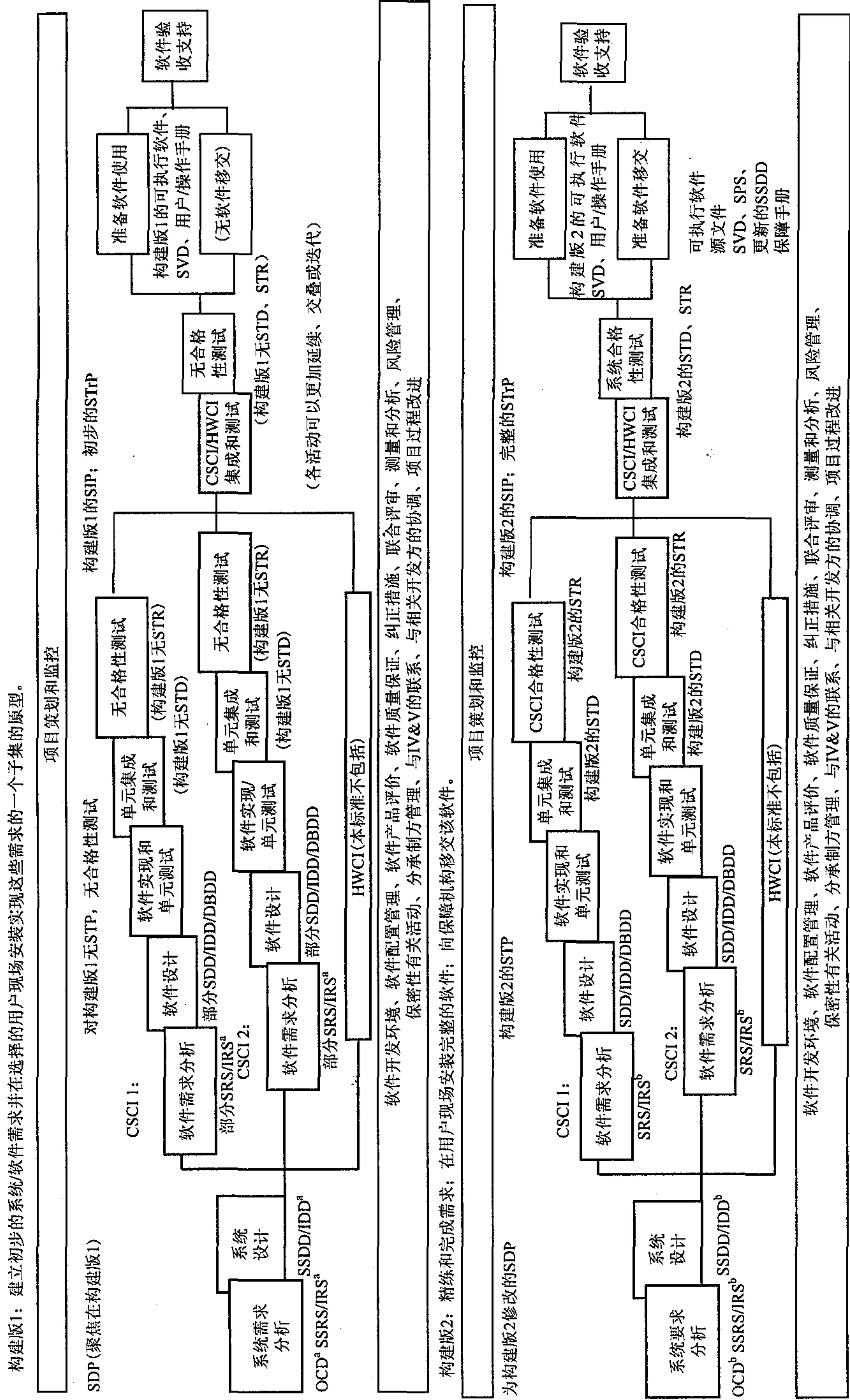


图 G.4 本标准应用于演进式开发策略的一种可能方式

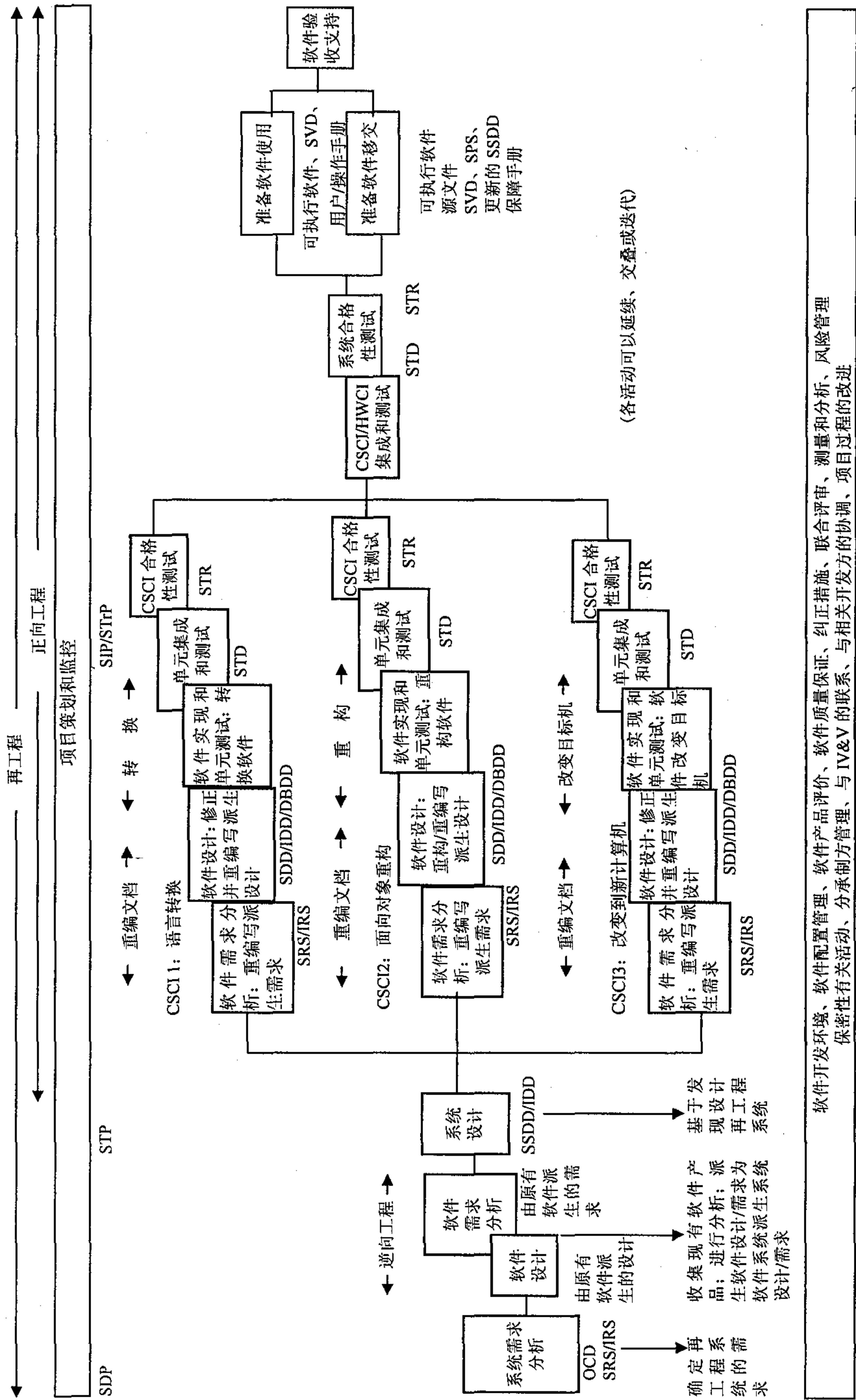


图 G.5 本标准应用于再工程项目的一种可能方式

G.5 软件构建版的策划和本标准的剪裁

G.5.1 概述

对一个项目策划软件构建版和为每一个构建版剪裁本标准有几种方法。例如，需方可以为整个合同选择一种总的项目策略并剪裁本标准，而由开发方安排软件构建版并为每个构建版提出剪裁建议。另一种方法是，需方可以在合同中安排软件构建版并规定每个构建版的剪裁。方法的选择依赖于项目。G.5.2~G.5.5 提供策划软件构建版和剪裁本标准的指南，并未试图划分哪些是需方的活动，哪些是开发方的活动。

G.5.2 标识构建版及其目标

软件构建版策划的第一步是安排一个或多个构建版的序列，并标识每个构建版的目标。表 G.2 为这种策划的一个例子。在表 G.2 中，系统/子系统规格说明 (SSS) 已存在，其需求的实现分四个构建版完成。其中的两个构建版是交付给选定用户的原型，另外两个才是实际现场安装的。构建版 4 的进一步目标是将软件移交到指定的保障机构。

G.5.3 标识每个构建版中要执行的本标准活动

软件构建版策划的下一步是标识在每个构建版中本标准哪些活动适用，并且确定它们的适用范围。表 G.2 指出了每个活动要在哪些构建版中执行，并包括有关每个构建版中每个活动的性质的说明。例如，表 G.2 表明每个构建版将包括软件开发策划 (5.2.1)，但是在每个构建版中该策划的性质会变更。有些活动在给定的构建版中根本不适用，有些则在所有的构建版中都同样适用，而有些则在不同的构建版中有不同的应用。由于项目的某些方面 (如 CSCI 的类型和数目等) 在填写工作表时，可能尚未确定，因此，工作表本身的填写就可能是递增式的。下述指南适用：

- a) 不同的决定适用于项目中不同类型的软件。这些差异将在同一个工作表的条款中给出，或者对项目中不同类型的软件使用不同的工作表。
- b) 如果初期构建版是用来做实验，开发“抛弃式”软件以达到明确系统方案或系统需求，那么在这个过程中可以适当地放弃某些形式化的东西，例如编码标准，这些编码标准以后将在实际的软件上强制执行。如果初期开发的软件以后会使用，那么这些形式化的东西从一开始就是合适的。这些决定依赖于项目。

G.5.4 记录剪裁决定

项目开始之前由需方做出的剪裁决定，并应在 SOW 或 SDTD 中详细说明。开发方提出的剪裁建议可以通过对招标书草案的反馈、在招标书的书面响应中提出建议、软件开发计划、项目期间的联合评审、或者通过其他方式进行交流。剪裁决定的细化可随项目的进展而逐步完善。涉及合同变更的剪裁决定宜得到相应的处理。

G.5.5 每个构建版中所选活动的安排

构建版策划的另一个重要步骤是安排每个构建版中的活动。由于作了剪裁，需方可以设置大体的里程碑，由开发方提供详细说明或者提供具体的安排。下述指南适用：

- a) 允许各 CSCI 有不同的时间安排可更好地进行开发。常见的错误是要求所有 CSCI 的开发必须“步法一致”，在同一时刻到达关键的里程碑。
- b) 各软件单元进度安排中的灵活性可能是必要的。与上述类似的错误是要求各软件单元的开发必须“步法一致”，所有设计都要在某个日期之前完成，在某个日期之前实现等等。
- c) 本标准中的活动不必按顺序完成。可以同时进行几项，而且一项活动可以在一个构建版或多个构建版中连续地或断续地完成。每个构建版中的活动宜以最适合该项目工作的方式进行安排。

表 G.2 一个项目的构建版策划的例子

构建版开发期间要完成的 活动		构建版			
		1	2	3	4
章条	活动	向选定的用户交付一个运行原型，该原型满足下列系统级需求：SSS-1、SSS-5、SSS-1250	向选定的用户交付一个运行原型，该原型满足构建版1以及SSS-2、SSS-3、SSS-15、SSS-1249的需求	向所有的用户交付已测试过的系统，该系统满足构建版1和2以及SSS-4、SSS-7、SSS-10、SSS-1248的需求	向所有的用户交付已测试过的系统，该系统满足所有系统级需求；移交给指定的保障机构
5.2	项目策划和监控				
5.2.1	软件开发策划	是：详细策划构建版1；概要地策划构建版2-4	是：详细计策划构建版2；概要地策划构建版3-4	是：详细策划构建版3；概要地策划构建版4	是：详细策划构建版4
5.2.2	CSCI 测试策划	否：在这个构建版中不进行 CSCI 合格性测试	否：在这个构建版中不进行 CSCI 合格性测试	是：在这个构建版中策划 CSCI 合格性测试	是：在这个构建版中修改 CSCI 合格性测试
5.2.3	系统测试策划	否：在这个构建版中不进行系统合格性测试	否：在这个构建版中不进行系统合格性测试	是：在这个构建版中策划系统合格性测试	是：在这个构建版中修改系统合格性测试
5.2.4	软件安装策划	否：由用户自己安装	否：由用户自己安装	是：策划在用户现场的安装工作	是：按需要修改构建版4的安装
5.2.5	软件移交策划	是：仅仅非常初步的策划	是：修改最初的计划	是：修改最初的计划	是：完成移交策划
5.2.6	计划的跟踪；执行管理评审	是：对于在执行的计划	是：对于在执行的计划	是：对于在执行的计划	是：对于在执行的计划
5.3	软件开发环境建立				
5.3.1	软件工程环境	是：按构建版1的需要	是：按构建版2的需要修改	是：按构建版3的需要修改	是：按构建版4的需要修改

参考文献

- GJB 1268A-2004 军用软件验收要求
GJB 5000A-2008 军用软件研制能力成熟度模型
GJB 5235-2004 军用软件配置管理
GJB/Z 141-2004 军用软件测试指南
-