GJB

中华人民共和国国家军用标准

FL 0137

GJB 5234—2004
代替 GJB/Z 117—99

军用软件验证和确认

Military software verification and validation

2004—09—20 发布　　2005—01—01 实施

中国人民解放军总装备部　批 准

目　次

前　言

本标准代替 GJB/Z 117－1999《军用软件验证和确认计划指南》。

本标准与 GJB/Z 117－1999 相比主要有下列变化：

a) GJB/Z 117－1999 参照 IEEE Std 1012－1986《软件验证和确认计划》制定，本标准主要参照 IEEE 1012－1998《软件验证和确认》，并加入了 IEEE 1059－1993《软件验证和确认计划指南》的部分内容；

b) GJB/Z 117－1999 规定了软件验证和确认计划(SVVP)的内容和格式，本标准不仅详细规定了软件验证和确认计划(SVVP)的内容和格式，还规定了在整个软件生存周期过程中进行验证和确认所需执行的任务及其输入和输出。

本标准的附录 A、B、C、D、E、F、G 是资料性附录。

本标准由中国人民解放军总装备部电子信息基础部提出。

本标准起草单位：信息产业部电子第四研究所、总参谋部第六十一所、总装备部测量通信总体研究所、中国航天科工集团第 706 所。

本标准起草人：韩红强、冯　惠、王　纬、高　林、许聚常、韩　柯。

引　言

军用软件验证与确认标准是一个涉及软件生存周期过程中获取、供应、开发、运行和维护的过程标准。

本标准的目的在于：

a) 为支持软件生存周期过程的验证和确认过程、活动和任务建立一个公共框架；

b) 定义验证和确认的任务、要求的输入和要求的输出；

c) 使用一个四级方案标识与软件完整性级别相对应的最低限度验证和确认任务；

d) 定义软件验证和确认计划(SVVP)的内容。

军用软件验证和确认

1 范围

本标准规定了军用软件验证和确认过程以及军用软件验证和确认计划(以下简称 SVVP)的编制要求。验证和确认过程确定一个已知活动的开发产品是否符合活动要求，软件是否满足它的预期用途和用户需要。验证和确认过程可包括软件产品和过程的分析、评价、评审、审查、评估和测试。

本标准适用于那些处于开发、维护和重用中的军用软件。本标准的使用者可根据具体的软件项目剪裁实施本标准。

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。凡注明日期或版次的引用文件，其后的任何修改单(不包括勘误的内容)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。凡不注明日期或版次的引用文件，其最新版本适用于本标准。

GJB 438A－1997 武器系统软件开发文档

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1 验收测试 acceptance testing

a) 确定一系统是否符合其验收准则且能使客户确定是否接收此系统的正式测试。

b) 使用户、客户或其他授权实体确定是否接受系统或部件的正式测试。

3.1.2 部件测试 component testing

为验证一个软件元素(例如单元、模块)或软件元素集的设计的准确实现和对程序要求的符合性而进行的测试。

3.1.3 关键性分析 criticality analysis

针对系统失效、系统老化或未能满足软件要求或系统目标所造成影响的严重性而进行的软件特性(例如，安全性、安全保密性、复杂性和性能)的结构化评估。

3.1.4 危险 hazard

在人身伤害和健康、财产、环境的损害等方面的潜在伤害来源或具有潜在伤害的情形。

3.1.5 危险分析 hazard analysis

对由系统开发或运行导致的软件的不良后果进行的系统定性或定量的评价。这些后果可能包括损害、疾病、死亡、任务失败、经济损失、财产损失、环境破坏或负面社会影响。本评价可包括分类、消除、减少或缓解危险的审查或分析方法。

3.1.6 危险标识 hazard identification

认识到危险存在并定义其特性的过程。

3.1.7 独立验证和确认 independent verification and validation

由在技术、管理和财务上与开发组织具有规定程度独立性的组织执行的验证和确认过程。

3.1.8 集成测试 integration testing

有关软件程序的一种有序的、递增的测试过程，在该过程中，对软件元素、硬件元素或软硬件元素进行组合并测试，直到整个系统集成起来以表明其是否符合程序设计及系统的能力和需求。

3.1.9 **完整性级别 integrity level**

项的某个特性的取值范围的一种表示，该特性取值范围对将系统风险保持在可接受的限度内是必需的。对于执行缓解功能的项，此特性是指项必须执行缓解功能的可靠性。对于因其失效能导致威胁的项，此特性是指对该失效的频率的限制。

3.1.10 **接口设计文档 interface design document (IDD)**

描述系统与众多部件之间接口的体系结构和设计的文档集。这些描述包括控制算法、协议、数据内容与格式、性能。

3.1.11 **接口需求规格说明 interface requirement specification (IRS)**

规定系统间或部件间接口的需求的文档集。这些需求包括对格式和计时的约束条件。

3.1.12 **最低限度任务 minimum tasks**

针对所指定的软件完整性级别而要求的那些验证和确认任务。

3.1.13 **可选任务 optional tasks**

针对特定应用需求可附加到最低限度验证和确认任务的那些验证和确认任务。

3.1.14 **要求的输入 required inputs**

执行任一生存周期活动中要求的最低限度验证和确认任务时必需的一些项。

3.1.15 **要求的输出 required outputs**

执行任一生存周期活动中要求的最低限度验证和确认任务而产生的一些项。

3.1.16 **风险 risk**

特定危险事件的频率或概率与后果的综合。

3.1.17 **风险分析 risk analysis**

系统地使用可用信息来标识危险并估计对于个人或人群、财产或环境的风险。

3.1.18 **软件设计描述 software design description**

为便于分析、策划、实现和决策而产生的软件的一种表示。软件设计描述可用作交流软件设计信息的媒体，也可以认为是系统的蓝图或模型。

3.1.19 **软件验证和确认计划 software verification and validation plan**

描述进行软件验证和确认的计划。

3.1.20 **软件验证和确认报告 software verification and validation report**

验证和确认结果和软件质量评估的文档集。

3.1.21 **系统测试 system testing**

为验证和确认系统是否达到其原始目标而对集成的硬件和软件系统进行测试的活动。

3.1.22 **确认 validation**

通过检查和提供客观证据，证实特定预期用途的需求是否得到满足。

注 1：在设计和开发中，确认关系到检查产品是否符合用户要求的过程。

注 2：一般是在规定的操作条件下对最终产品进行确认。在早期阶段，这样做可能也是必要的。

注 3：“已确认的”一词用来表示相应的状态。

注 4：如果有几种不同的预期用途，可进行多种确认。

注 5：特定预期用途的需求通常是指需求规格说明或合同中规定的需求。

3.1.23 **验证 verification**

通过检查和提供客观证据，证实规定的需求已经得到满足。

注 1：在设计和开发中，验证是指对某项指定活动的结果进行检查的过程，以确定该活动是否符合该活动声明的需求。

注 2：“已验证的”一词用来表示相应的状态。

3.2 **缩略语**

本标准采用下列缩略语：

COTS (Commercial-Off-The-Shelf)　商业现货

IDD (Interface Design Document)　接口设计文档

IRS (Interface Requirements Specification)　接口需求规格说明

IV&V (Independent Verification and Validation)　独立验证和确认

SDD (Software Design Description)　软件设计描述

SRS (Software Requirements Specification)　软件需求规格说明

SVVP (Software Verification and Validation Plan)　软件验证和确认计划

SVVR (Software Verification and Validation Report)　软件验证和确认报告

V&V (Verification and Validation)　验证和确认

4　软件完整性级别

基于其预期用途及关键或非关键的系统应用，软件展示了不同的关键性。一些软件系统对关键的、维持生存的系统起作用，而其他的软件系统是非关键的、独立的研究工具。软件关键性描述了一个系统的预期用途和应用。本标准使用软件完整性级别的方法来量化软件关键性。软件完整性级别表示了将风险维持在可接受限度内所必需的软件关键性的值域。这些软件特性可能包括安全性、安全保密性、软件复杂性、性能、可靠性或其他特性。关键的、高完整性的软件通常要求更大范围、更严格的 V&V 任务的应用。

为了策划 V&V 过程，软件完整性级别一般在开发过程的早期指定，最好在系统需求分析和体系结构设计活动的过程中指定。软件完整性级别可指派到软件需求、功能、功能组，或软件部件或子系统。指定的软件完整性级别可随软件的演化而变化。开发组织选择的设计、编码、规程和技术实现的特征能提升或降低软件关键性，进而提升或降低为软件指定的相应的软件完整性级别。需方可接受的降低风险的方法也可被用于降低软件关键性，因而允许选择一个更低的完整性级别。通过实施贯穿于软件开发过程中的 V&V 关键性分析任务而对软件完整性级别的指定进行不断更新和评审。

本标准的使用者可以选择任何定义了指定软件完整性级别需求的软件完整性方案(例如从现存的标准得到)。为一个项目建立的软件完整性级别源于需方、供方、开发方和独立保证机构(例如管理实体或负责的代理机构)间的协议。如果尚未定义软件完整性方案，V&V 工作计划应规定一个软件完整性方案。

为识别适用于所选择的不同软件完整性级别方案的最低限度 V&V 任务，本标准的使用者应将本标准的软件完整性方案和相关最低限度 V&V 任务映射到他们选择的软件完整性级别方案。该软件完整性级别方案和相关最低限度 V&V 任务的映射应记录在 SVVP 中。表 15 规定了每个软件完整性级别应执行的最低限度 V&V 任务。

表 1 定义了本标准用作示例的四个软件完整性级别。表 2 描述了四个软件完整性级别中每个级别的软件错误的后果。这些软件完整性级别之间会有交叠，因而允许对由应用决定的可接受风险进行单独解释。如果系统中没有出现与软件错误有关的后果，则可指定软件完整性第 0 级。对于软件完整性第 0 级，不执行任何 V&V 任务。

表 1　软件完整性级别指定

软件完整性级别	描述	关键性
4(A)	引起系统灾难性后果的功能或系统特性方面的错误，促使该错误出现的运行状态以相当、大概或偶尔的可能性出现；或者引起严重性后果的错误，而促使该错误出现的运行状态以相当或大概的可能性出现。	高

表 1(续)

软件完整性级别	描述	关键性
3(B)	引起灾难性后果的功能或系统特性方面的错误，促使该错误出现的运行状态以偶尔或极小的可能性出现；或者引起严重性后果的错误，而促使该错误出现的运行状态以大概或偶尔的可能性出现；或者引起微小后果的错误，而促使该错误出现的运行状态以相当或大概的可能性出现。	较高
2(C)	引起严重性后果的功能或系统特性方面的错误，促使该错误出现的运行状态以偶尔或极小的可能性出现；或者引起微小后果的错误，而促使该错误出现的运行状态以大概或偶尔的可能性出现；或者引起可忽略的后果的错误，而促使该错误出现的运行状态以相当或大概的可能性出现。	中
1(D)	引起严重性后果的功能或系统特性方面的错误，促使该错误出现的运行状态以极小的可能性出现；或者引起微小后果的错误，而促使该错误出现的运行状态以偶尔或极小的可能性出现；或者引起可忽略的后果的错误，而促使该错误出现的运行状态以大概、偶尔或极小的可能性出现。	低
注：由于在其他一些军用标准中以 A、B、C、D 四级对软件完整性级别进行分级，本标准为做到与其他标准的衔接一致，故在表中同时列出 4、3、2、1 和对应的 A、B、C、D 两种分级方法。		

表 2　后果的定义

后果	定义
灾难性的	丧失生命，任务完全失败，系统安全性和安全保密性的丧失，或广泛的财务或社会损失。
严重性的	主要的和长久的伤害，任务部分损失，重大系统损害，或重大财务或社会损失。
微小的	严重的伤害或病症，次要任务降级，或一些财务或社会损失。
可忽略的	轻微的伤害或病症，对系统性能的轻微影响，或操作人员的不便。

表 3 阐明了表 1 和表 2 所示的基于风险的方案。根据错误的后果和促使该错误出现的运行状态出现的可能性的组合，对表中的每个单元指定了软件完整性级别。一些单元反映了不止一个软件完整性级别，这表明可根据系统应用和缓解风险的建议来选择软件完整性级别的最终指定。对于一些工业应用，出现可能性的分类的定义可表示为由分析导出或从系统需求导出的概率图。

表 3　软件完整性级别指定的图例

错误后果	导致该错误的运行状态出现的可能性			
	相当的	大概的	偶而的	极小的
灾难性	4	4	4 或 3	3
严重性	4	4 或 3	3	2 或 1
微小的	3	3 或 2	2 或 1	1
可忽略的	2	2 或 1	1	1

对于没有软件完整性准则应用的软件部分(即，那些处于第 1 级之下的软件部分)，本标准不适用。为软件部件指定软件完整性级别的根据应记录在 V&V 任务报告和 V&V 最终报告中。

指定给可重用软件的完整性级别应遵循该项目采用的完整性级别方案(参见附录 D)，应对可重用软件在应用环境下的使用情况进行评价。

通过选择软件完整性级别及其相应最低限度 V&V 任务和补充的可选 V&V 任务，对 V&V 过程进行剪裁以适应特定系统需求和应用。补充的可选 V&V 任务允许 V&V 工作指出特定于应用的软件特性。附录 G 对可选 V&V 任务进行了描述。

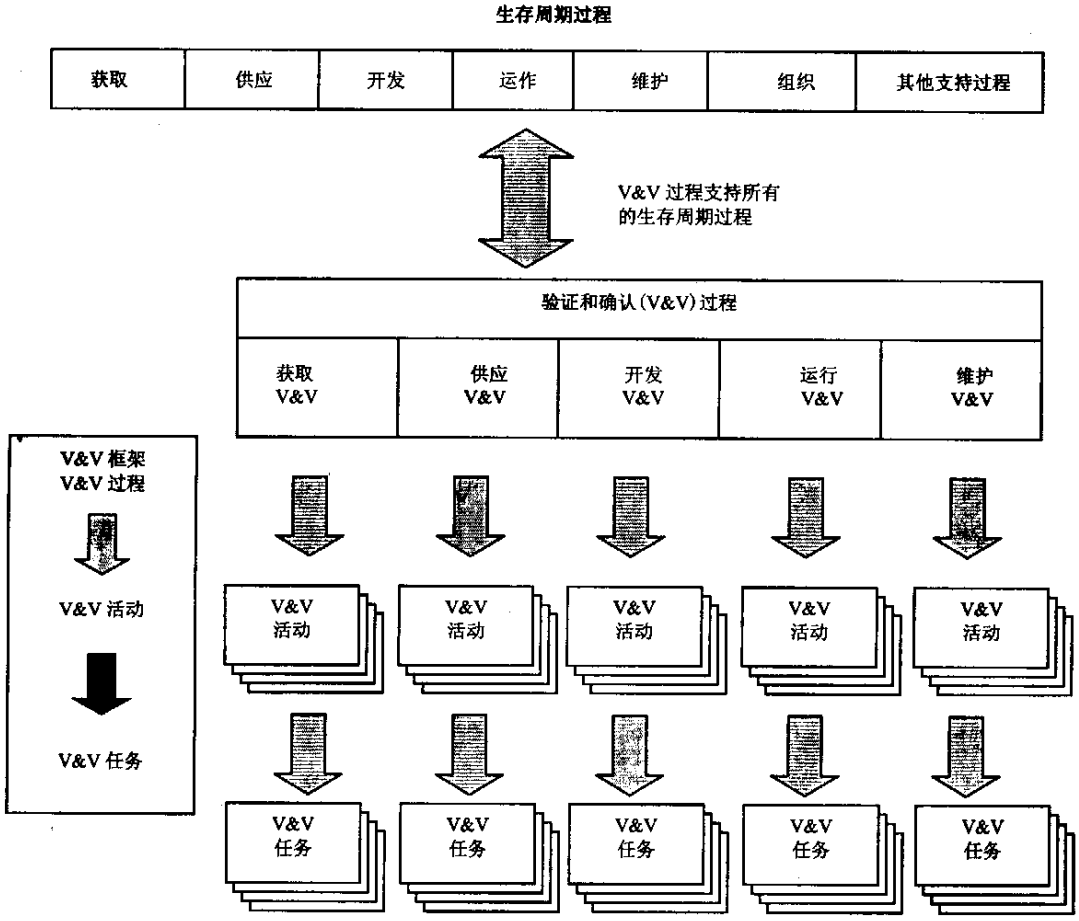
5 V&V 过程

5.1 综述

V&V 过程支持所有的软件生存周期过程。本标准主要涉及包括获取、供应、开发、运作和维护过程在内的软件生存周期基本过程。在软件生存周期内，V&V 过程、活动和任务的层次关系见图 1。本章描述了获取过程、供应过程、开发过程、运作过程和维护过程的 V&V 活动和任务，还描述了管理这些 V&V 活动和任务的管理过程。支持以上过程的 V&V 输入、V&V 活动、V&V 任务和 V&V 输出示例见图 2。最低限度 V&V 活动和任务在下列条文中提及并在表 4 至表 14 中定义。附录 B 显示了从所有 GB/T 8566－2001 V&V 要求(即，过程、活动和任务)到本标准的 V&V 活动和任务的映射。

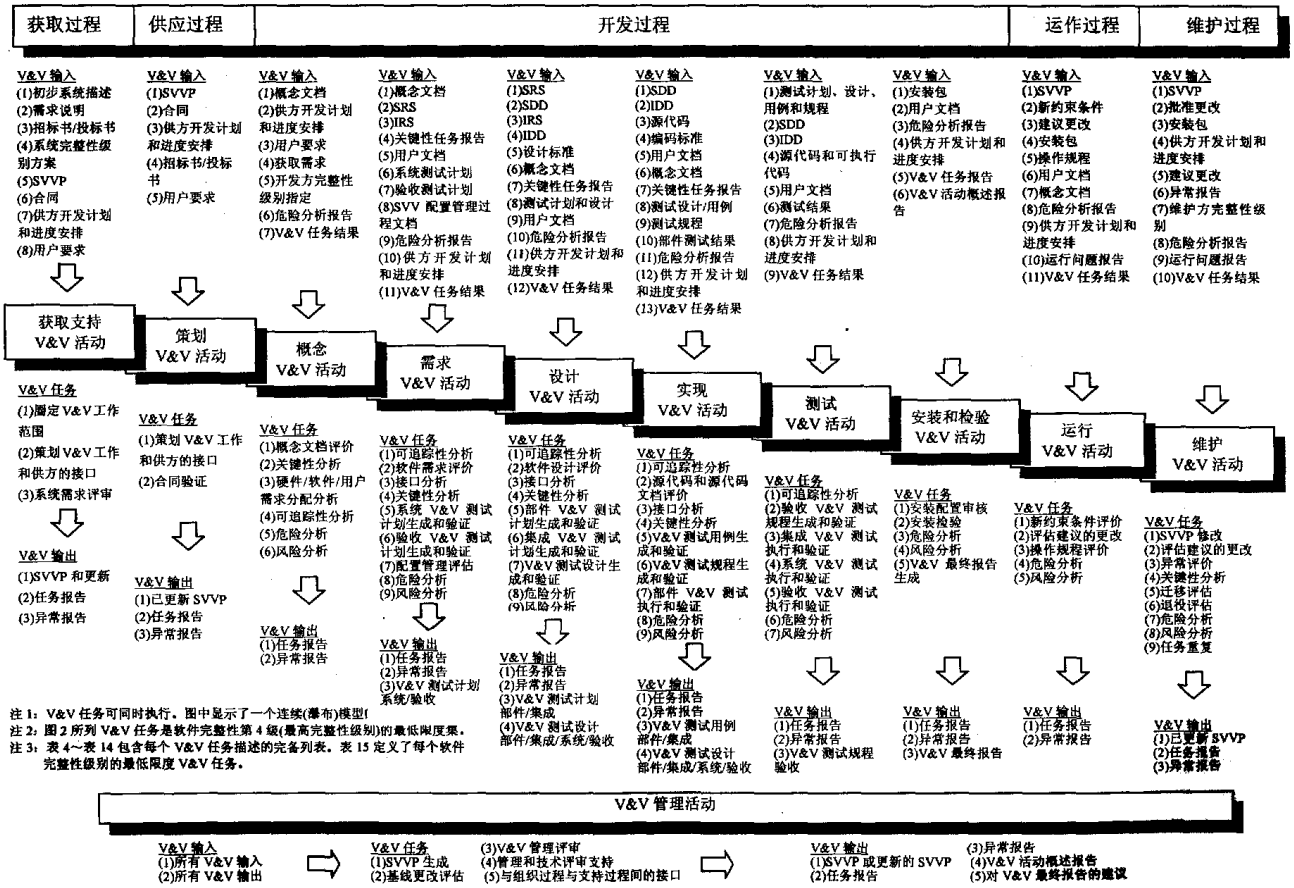
V&V 工作应遵循表 4 至表 14 中描述的任务、输入和输出。V&V 工作应执行表 15 中指定软件完整性级别规定的最低限度 V&V 任务。如果本标准的用户已经选择了一个不同的软件完整性级别方案，那么将该完整性级别方案映射到表 15，即可得到用户的每个软件完整性级别的最低限度 V&V 任务的定义。

并非所有的软件项目都包括上面列出的每个生存周期过程。为遵循本标准，V&V 过程应涉及软件项目使用的有关的生存周期过程。



注 1："其他支持过程"包括"文档编制"、"配置管理"、"质量保证"、"联合评审"、"审核"、和"问题解决"。
注 2：V&V 活动管理与所有 V&V 活动并发。
注 3：所有 V&V 任务的任务描述、输入和输出包含在表 4 至表 14 中。

图 1 V&V 过程、活动和任务层次



注 1：V&V 任务可同时执行。图中显示了一个连续(瀑布)模型(

注 2：图 2 所列 V&V 任务是软件完整性第 4 级(最高完整性级别)的最低限度集。

注 3：表 4～表 14 包含每个 V&V 任务描述的完备列表。表 15 定义了每个软件完整性级别的最低限度 V&V 任务。

图 2　软件 V&V 概述示例

一些 V&V 活动和任务包括分析、评估和测试，它们可由多方组织(例如，软件开发、项目管理、质量保证、V&V)执行。例如，风险分析和危险分析可由项目管理、软件开发和 V&V 工作执行。V&V 工作执行这些任务得到基本证据，这些证据显示了软件产品是否满足其需求。这些 V&V 分析是对其他分析的补充，并不排除或代替由其他组织执行的分析。这些分析工作与其他组织协调的程度应编入 SVVP 的组织职责部分，而附录 F 提供了一个组织关系图示例。

本标准的用户应在 SVVP 中说明 V&V 过程，定义必要的信息和工具来管理和执行这些过程、活动、任务，并使 V&V 过程与该项目的其他有关方面相协调。V&V 活动和任务的结果应记录在任务报告、活动摘要报告、异常报告、V&V 测试记录和 V&V 最终报告中。

5.2 过程：管理

5.2.1 概述

管理过程包含通用活动和任务，这些活动和任务可由管理其相应过程的任何一方使用。这些管理任务要：

a) 准备过程执行的计划；
b) 启动计划的实施；
c) 监督计划的执行；
d) 分析计划执行过程中发现的问题；
e) 报告过程进展；
f) 确保产品满足需求；
g) 评估评价结果；
h) 确定任务是否完成；
i) 检查结果完备性。

5.2.2 活动：V&V 管理

一般情况下，在所有的软件生存周期过程和活动中都执行 V&V 管理活动。该活动将持续地评审 V&V 工作，基于更新的项目进度和开发状态对 SVVP 进行必要的修订，并与开发方以及诸如质量保证、配置管理、评审和审核等其他支持过程协调 V&V 结果。V&V 管理评估对系统和软件提出的每个更改，标识受更改影响的软件需求，并规划涉及更改的 V&V 任务。对提出的每个更改，V&V 管理评估是否在软件中引入任何新的危险或风险，并标识更改对指定软件完整性级别的影响。如果软件完整性级别或危险或风险发生变化，则通过添加新的 V&V 任务或增加已存在 V&V 任务的范围和强度来修改 V&V 任务计划。V&V 活动管理监督并评价所有的 V&V 输出。通过使用 V&V 度量和其他定性的与定量的测量，V&V 管理活动提出了程序趋势数据和可能的风险问题，并提供给开发方和需方以便他们及时了解情况并提出解决方案。在关键的程序里程碑(例如，需求评审、设计评审、测试准备就绪)处，V&V 管理整合 V&V 结果以确定是否进入下一系列软件开发活动的证据。一旦需要，V&V 管理将确定是否需要因开发方对软件程序的更改而重新执行 V&V 任务。

在选定适当的软件完整性级别后，V&V 工作应从下列任务中执行对 V&V 管理的最低限度 V&V 任务(见表 4)：

a) 任务：软件验证和确认计划(SVVP)生成；
b) 任务：基线更改评估；
c) 任务：V&V 管理评审；
d) 任务：管理和技术评审支持；
e) 任务：与组织过程及支持过程的接口。

5.3 过程：获取

5.3.1 概述

表 4　V&V 管理活动的任务、输入和输出

V&V 任务	要求的输入	要求的输出
V&V 管理活动(与所有过程并行)		
a) **软件验证和确认计划(SVVP)生成。**为所有生存周期过程生成 SVVP。SVVP 需要在整个生存周期中更新。其他活动的输出是 SVVP 的输入。在需求 V&V 活动之前建立 SVVP 基线。标识 SVVP 中的项目里程碑。安排 V&V 任务以支持项目管理评审和技术评审。参见第 7 章的 SVVP 概述和内容示例。	SVVP(可能有的) 合同 概念文档(例如，需求陈述、高级策划报告、项目启动备忘录、可行性研究、系统需求、管理规则、规程、策略、客户验收准则和需求、获取文档、商业规则、系统结构草案) 供方开发计划和进度安排	SVVP 或更新的 SVVP
b) **基线更改评估。**评价建议的软件更改(例如，异常修改和需求更改)对先前完成的 V&V 任务的影响。策划重新执行受影响的任务或启动新任务，以处理软件基线更改或迭代的开发过程。验证和确认该更改与系统需求一致，并且不直接或间接地对需求造成负面影响。负面影响是一种造成新的系统危险和风险，或影响以前已解决的危险和风险的变化。	SVVP 建议的更改 危险分析报告 由 V&V 任务标识的风险	已更新的 SVVP 任务报告——基线更改评估 异常报告
c) **V&V 管理评审。**评审和总结 V&V 工作，以确定 V&V 任务变化或调整 V&V 工作。推荐是否进入下一系列 V&V 和生存周期开发活动，并为 SVVP 中标识的组织提供任务报告、异常报告和 V&V 活动摘要报告。验证所有 V&V 任务是否遵循 SVVP 中定义的任务需求。验证 V&V 任务结果所具有的支持证据。评估所有 V&V 结果，并提供程序验收与合格性的建议作为 V&V 最终报告的输入。V&V 管理评审可使用诸如 IEEE Std 1028-1988 所提供的任何评审方法。	SVVP 和更新 供方开发计划和进度安排 V&V 任务结果[例如，技术成就、V&V 报告、资源利用、V&V 度量(参见附录 E)、计划和已标识风险]	已更新的 SVVP 任务报告——建议书、V&V 活动摘要报告、V&V 最终报告建议
d) **管理和技术评审支持。**通过评估评审材料、参加评审和提供任务报告与异常报告，来支持项目管理评审和技术评审(例如，初步设计评审和关键设计评审)。依照所有软件产品和文档的批准进度对及时交付进行验证。管理和技术评审支持可使用诸如 IEEE Std 1028-1988 所提供的任何评审方法。	V&V 任务结果 评审材料(例如，SRS、IRS、SDD、IDD、测试文档)	任务报告——评审结果 异常报告
e) **与组织及支持过程的接口。**协调 V&V 工作与组织(例如，管理、改进)和支持过程(例如，质量保证、联合评审、和问题解决方案)。标识要与这些过程交换的 V&V 数据。在 SVVP 中编写数据交换需求。	SVVP SVVP 中标识的源于组织和支持过程的数据	更新的 SVVP

获取过程从定义获取系统、软件产品或软件服务的需求(例如，需求陈述)开始，随后制定和发布招标书，选择供方和管理获取过程，直到验收系统、软件产品、或软件服务。V&V 工作使用获取过程来圈定 V&V 工作的范围，策划供方和需方间的接口，评审包含在标书中的系统需求草案。

5.3.2　活动：获取支持 V&V

获取支持 V&V 活动涉及项目启动、招标、合同准备、供方监督、及验收和完成。

在选定适当的软件完整性级别后，V&V 工作应从下列任务中执行针对获取支持 V&V 的最低限度 V&V 任务(见表 5)：

a)　任务：圈定 V&V 工作范围；

b)　任务：设计 V&V 工作和供方间的接口；

c)　任务：系统需求评审。

表 5　获取支持 V&V 活动的任务、输入和输出

V&V 任务	要求的输入	要求的输出
获取支持 V&V 活动(获取过程)		
a) **圈定 V&V 工作范围。**确定项目 V&V 软件关键性(例如，安全性、安全保密性、任务关键性、技术复杂性)。为系统和软件指定一个软件完整性级别。确定独立性程度(参见附录 C)，若 V&V 工作需要的话。提供 V&V 预算评价，包括要求的测试设备和工具。为圈定 V&V 工作范围，应执行下列步骤： 1) 采用为项目指定的系统完整性方案。如果不存在系统完整性级别方案，就选择一个。 2) 使用表 15 和选定的软件完整性级别方案，确定软件完整性级别的最低限度 V&V 任务。 3) 必要时，增加可选 V&V 任务。 4) 根据表 4 至表 14 规定的 V&V 任务、输入和输出的描述确定 V&V 的范围。	初步系统描述 需要说明 招标书(RFP)或投标书 系统完整性级别方案	更新的 SVVP
b) **策划 V&V 工作与供方的接口。**为每个 V&V 任务设计 V&V 进度。标识由 V&V 过程评价的开发过程和产品的初步清单。描述 V&V 对专用和机密信息的访问权。建议与需方协调该计划。将项目软件完整性级别方案纳入策划过程。	SVVP 招标书或投标书 合同 供方开发计划和进度安排	更新的 SVVP
c) **系统需求评审。**评审招标书或投标书中的系统需求(例如，系统需求规格说明、可行性研究报告、商业规则描述)，以 1) 验证需求与用户要求的一致性； 2) 确认需求是否能用规定的技术、方法和为项目定义的算法满足(可行性)； 3) 验证需求中是否提供了能由测试证实的目标信息(可测试性)。评审其他需求诸如可交付物定义、适合的依从性标准和规章清单、用户要求等的完备性、正确性和准确性。	初步系统描述 需求说明 用户要求 招标书或投标书	任务报告 系统需求评审 异常报告

5.4　过程：供应

5.4.1　概述

供应过程可由编制投标书以答复需方的招标书来启动，也可由与需方签订合同而提供系统、软件产品、或软件服务来启动。随后确定管理和保证项目所需规程和资源，包括编制项目计划，执行计划，直到将系统、软件产品或软件服务交付给需方。V&V 工作使用供应过程的产品验证招标需求与合同需求是否一致、是否满足用户要求。V&V 策划活动使用包括程序进度的合同需求来修改并更新供方与需方间的接口计划。

5.4.2　活动：策划 V&V

策划 V&V 活动涉及启动、投标准备、签约、策划、执行与控制、评审与评价、交付与实施等活动。

在选定适当的软件完整性级别后，V&V 工作应从下列任务中执行针对策划 V&V 的最低限度 V&V 任务(见表 6)：

a)　任务：策划 V&V 工作和供方间的接口；

b)　任务：合同验证。

表 6　策划 V&V 活动的任务、输入和输出

V&V 任务	要求的输入	要求的输出
策划 V&V 活动(供应过程)		
a) **策划 V&V 工作和供方的接口。**评审供方开发计划和进度安排，协调 V&V 工作与开发活动。建立与开发工作交换 V&V 数据和结果的规程。建议与需方协调该计划。将项目软件完整性级别方案纳入策划过程。	SVVP 合同 供方开发计划和进度安排	更新的 SVVP

表 6(续)

V&V 任务	要求的输入	要求的输出
策划 V&V 活动(供应过程)		
b) **合同验证。**验证 1) 系统需求(由招标书或投标书、合同)是否满足用户要求并与用户要求一致； 2) 是否编写了用于需求更改管理和标识处理问题的管理层次的规程； 3) 是否编写了各方的接口和协作规程，包括所有权、担保、版权和机密性； 4) 是否依据需求编写了验收准则和规程。	SVVP 招标书或投标书 合同 用户要求 供方开发计划和进度安排	更新的 SVVP 任务报告——合同验证 异常报告

5.5 过程：开发

5.5.1 概述

开发过程包含开发方的活动和任务。该过程包含与软件产品有关的需求分析、设计、编码、集成、测试、安装和验收等活动。V&V 活动验证和确认这些活动和产品。V&V 活动被划分为概念 V&V、需求 V&V、设计 V&V、实现 V&V、测试 V&V、安装和检验 V&V。

5.5.2 活动：概念 V&V

概念 V&V 活动分析和评价解决用户问题的特定实现解决方案。在概念 V&V 活动期间，系统体系结构已选定，对硬件、软件和用户接口部件分配系统需求。概念 V&V 活动涉及系统体系结构设计和系统需求分析。V&V 的目标是验证系统需求的分配，确认选定的解决方案，确保没有采纳错误的解决方案。

在选定适当的软件完整性级别后，V&V 工作应从下列任务中执行针对概念 V&V 的最低限度 V&V 任务(见表 7)：

a) 任务：概念文档评价；
b) 任务：关键性分析；
c) 任务：硬件/软件/用户需求分配分析；
d) 任务：可追踪性分析；
e) 任务：危险分析；
f) 任务：风险分析。

表 7 概念 V&V 活动的任务、输入和输出

V&V 任务	要求的输入	要求的输出
概念 V&V 活动(开发过程)		
a) **概念文档评价。**验证概念文档是否满足用户要求并与获取要求一致。确认接口系统的约束条件和建议步骤的约束条件或限制条件。 分析系统需求并对下列方面满足用户要求进行确认： 1) 系统功能； 2) 端对端系统性能； 3) 功能需求的可行性与可测试性； 4) 系统体系设计； 5) 运行和维护需求； 6) 来自适用的现存系统的迁移需求。	概念文档 供方开发计划和进度安排 用户要求 获取需求	任务报告——概念、文档、评价 异常报告

表 7(续)

V&V 任务	要求的输入	要求的输出
概念 V&V 活动(开发过程)		
b) **关键性分析**。确定是否为需求、详细功能、软件模块、子系统或其他软件划分建立了软件完整性级别。验证所指定的软件完整性级别的正确性。如果未指定软件完整性级别，那么为系统需求指定软件完整性级别。记录指定给各个软件部件(例如，需求、详细功能、软件模块、子系统或其他软件划分)的软件完整性级别。 出于 V&V 策划目的，指定给单个要素的最关键的软件完整性级别应该是指定给整个软件的完整性级别。验证任一软件部件能否影响指定了更高软件完整性级别的单个软件部件，如果这种情况存在，那么为该软件部件指定同一高度的软件完整性级别。	概念文档(系统需求) 开发方完整性级别指定	任务报告——软件完整性级别 任务报告——关键性分析 异常报告
c) **硬件/软件/用户需求分配分析**。对照用户要求，验证为硬件、软件和用户接口分配的概念需求的正确性、准确性和完备性。 1) 正确性 验证分配给硬件、软件和用户接口的性能需求(例如，计时、响应时间和生产量)是否满足用户要求。 2) 准确性 验证内部和外部接口对数据格式、接口协议、每个接口的数据交换频率和其他关键性能需求的规定，以证明其对用户需求的依从性。 3) 完备性 ① 验证诸如功能多样性、故障检验、故障隔离、诊断与出错恢复特定需求应用是否满足用户要求。 ② 验证用户对系统的维护需求是否得以完全规定。 ③ 验证来自现存系统的迁移和系统的替换是否满足用户要求。	用户要求 概念文档	任务报告——硬件/软件/用户需求分配分析 异常报告
d) **可追踪性分析**。标识将由软件完全或部分实现的所有系统需求。验证这些系统需求可追踪到获取要求。从系统需求开始进行软件需求可追踪性分析。	概念文档	任务报告——可追踪性分析 异常报告
e) **危险分析**。分析对于和来自于概念系统的潜在危险。此分析应 1) 标识潜在系统危险； 2) 评估每个危险的严重性； 3) 评估每个危险的概率； 4) 标识每个危险的缓解策略。	概念文档	任务报告——危险分析 异常报告
f) **风险分析**。标识技术和管理风险。为消除、降低或缓解风险提供建议。	概念文档 供方开发计划和进度安排 危险分析报告 V&V 任务结果	任务报告——风险分析 异常报告

5.5.3 活动：需求 V&V

需求 V&V 活动确定了功能性和性能需求、软件外部接口、合格性需求、安全性和安全保密性需求、人因工程、数据定义、软件用户文档、安装和验收需求、用户操作和执行需求、用户维护需求。需求 V&V 活动涉及软件需求分析。V&V 的目标是，确保需求的正确性、完备性、准确性、可测试性和一致性。

在选定适当的软件完整性级别后，V&V 工作应从下列任务中执行针对需求 V&V 的最低限度 V&V 任务(见表 8)：

a) 任务：可追踪性分析；

b) 任务：软件需求评价；

c) 任务：接口分析；

d) 任务：关键性分析；
e) 任务：系统 V&V 测试计划生成和验证；
f) 任务：验收 V&V 测试计划生成和验证；
g) 任务：配置管理评估；
h) 任务：危险分析；
i) 任务：风险分析。

表 8 需求 V&V 活动的任务、输入和输出

V&V 任务	要求的输入	要求的输出
需求 V&V 活动(开发过程)		
a) **可追踪性分析**。追踪软件需求(SRS 和 IRS)到系统需求(概念文档)，系统需求到软件需求。分析标识出的正确性、一致性、完备性和准确性的关系。任务准则如下： 1) 正确性： 确认每个软件需求与其系统需求之间的关系是否正确。 2) 一致性： 验证软件与系统需求之间的关系是否按一致的详细程度来规定。 3) 完备性： ① 验证每个软件需求能否足够详细地追踪到一个系统需求，以表明对系统需求的依从性。 ② 验证与软件有关的所有系统需求可追踪到软件需求。 4) 准确性： 确认系统性能和运行特性由可追踪的软件需求准确规定。	概念文档(系统需求) SRS IRS	任务报告——可追踪性分析 异常报告
b) **软件需求评价**。评价 SRS 和 IRS 需求(例如，功能性、能力、接口、合格性、安全性、安全保密性、人为因素、数据定义、用户文档、安装和验收、用户运行、用户维护)的正确性、一致性、完备性、准确性、可读性和可测试性。任务准则如下： 1) 正确性： ① 验证和确认软件需求满足在系统假设和约束条件下配置给软件的系统需求。 ② 验证软件需求是否遵循标准、引用文件、规章、政策、法律和商业规则。 ③ 使用逻辑和数据流以及领域专业知识、原型结果、工程原理或其他基础知识确认状态顺序和状态变化。 ④ 确认数据和控制流满足功能性和性能需求。 ⑤ 确认数据用法和格式。 2) 一致性： ① 验证所有的术语和概念是否编写一致。 ② 验证功能交互和假设是连续一致的，并满足系统需求和获取需求。 ③ 验证软件需求具有内部一致性，系统需求具有外部一致性。 3) 完备性： ① 验证在系统假设和约束条件下，下列要素是否处于 SRS 或 IRS 之中： —功能性(例如，算法、状态/模式定义、输入/输出确认、异常处理、报告和日志)； —过程定义和进度安排； —硬件、软件和用户接口描述； —性能准则(例如，时间、规模、速度、能力、准确性、精度、安全性和安全保密性)； —关键配置数据； —系统、设备和软件控制(例如，初始化、事务和状态监控、(自检)。	概念文档 SRS IRS	任务报告——软件需求评价 异常报告

表 8(续)

V&V 任务	要求的输入	要求的输出
需求 V&V 活动(开发过程)		
② 验证 SRS 和 IRS 是否满足规定的配置管理规程。 4) 准确性： ① 确认逻辑、计算和接口精度(例如，截断法和舍入法)满足系统环境下的需求。 ② 确认建立的物理现象模型遵从系统准确性需求和自然规律。 5) 可读性： ① 验证文档对预期读者是明了的、可理解的和无歧义的。 ② 验证文档定义了所有首字母缩写词、助记法、缩略语、术语和符号。 6) 可测试性： 验证是否具有用于确认 SRS 和 IRS 需求的目标验收准则。	概念文档 SRS IRS	任务报告——软件需求评价 异常报告
c) **接口分析**。验证和确认软件与硬件、用户、操作人员、及其他系统的接口的需求是正确、一致、精确和可测的。任务准则如下： 1) 正确性： 确认外部和内部的系统与软件接口需求。 2) 一致性： 验证 SRS 与 IRS 对接口的描述是一致的。 3) 完备性： 验证每个接口都得到描述并包括了数据格式和性能准则(例如，时间、带宽、准确性、安全性和安全保密性)。 4) 准确性： 验证每个接口是否以要求的准确性提供信息。 5) 可测试性： 验证是否具有用于确认接口需求的目标验收准则。	概念文档 SRS IRS	任务报告——接口分析 异常报告
d) **关键性分析**。使用 SRS 和 IRS 评审和更新源于先前关键性任务报告的现存关键性分析结果。实现方法和连接技术可导致先前指定给软件要素(即，需求、模块、功能、子系统、其他软件划分)的软件完整性级别提升或下降。验证没有因评审已修改软件完整性级别而引起不一致的或不期望的软件完整性结果。	任务报告——关键性 SRS IRS	任务报告——关键性分析 异常报告
e) **系统 V&V 测试计划生成和验证**。(对于软件完整性第 3 和第 4 级)策划系统 V&V 测试以确认软件需求。策划系统需求对测试设计、用例、规程、和结果的追踪。策划测试设计、用例、规程和结果的文档编制。系统 V&V 测试计划应涉及下列内容： 1) 作为系统环境下完整的软件最终项，对所有系统需求(例如，功能性、性能、安全、运行和维护)的依从性； 2) 用户文档的(例如，培训材料、程序变化)充分性； 3) 在边界(例如，数据、接口)和强度条件下的性能。验证系统 V&V 测试计划是否遵循项目定义的测试文档目的、格式和内容(见 GJB 438A－1997)。 确认系统测试计划满足下列准则： 1) 系统需求的测试覆盖率； 2) 所用测试方法和标准的适合性； 3) 对预期结果的依从性； 4) 系统合格性测试的可行性； 5) 运行和维护需求的可行性与可测性。 (对于软件完整性第 1 和第 2 级)验证开发方系统测试计划遵循定义了测试文档目的、格式和内容(见 GJB 438A－1997)的项目。 确认系统测试计划满足下列准则： 1) 系统需求的测试覆盖率； 2) 所用测试方法和标准的适合性； 3) 对预期结果的依从性； 4) 系统合格性测试的可行性；	概念文档(系统需求) SRS IRS 用户文档系统测试计划	异常报告 系统 V&V 测试计划

表 8(续)

V&V 任务	要求的输入	要求的输出
需求 V&V 活动(开发过程)		
5) 运行和维护能力。	概念文档(系统需求) SRS IRS 用户文档系统测试计划	异常报告 系统 V&V 测试计划
f) **验收 V&V 测试计划生成和验证。**(对于软件完整性第 3 和第 4 级)策划验收 V&V 测试以确认软件在运行环境下正确地实现了系统和软件需求。任务准则为: 1) 在运行环境下对验收需求的依从性; 2) 用户文档的充分性。 策划验收测试需求对测试设计、用例、规程和执行结果的追踪。策划测试任务和结果文档。验证验收 V&V 测试计划是否遵循项目定义的测试文档目的、格式和内容(见 GJB 438A－1997)。确认验收测试计划满足下列准则: 1) 系统需求的测试覆盖率; 2) 对预期结果的依从性; 3) 运行和维护的可行性(例如,依据用户要求运行和维护的能力)。 (对于软件完整性第 2 级)验证开发方验收测试计划是否遵循项目定义的测试文档目的、格式和内容(见 GJB 438A－1997)。确认开发方验收测试计划满足了下列准则: 1) 系统需求的测试覆盖率; 2) 对预期结果的依从性; 3) 运行和维护(例如,依据用户要求运行和维护的能力)的可行性。 (软件完整性第 1 级没有验收测试需求。)	概念文档 SRS IRS 用户文档 验收测试计划	验收 V&V 测试计划 异常报告
g) **配置管理评估。**验证配置管理过程是完整和充分的。任务准则如下: 1) 完备性: 验证拥有用于描述软件产品功能性、跟踪程序版本和管理变化的过程。 2) 充分性: 验证配置管理过程对于开发复杂性、软件和系统规模、软件完整性级别、项目计划和用户要求是充分的。	软件配置管理过程文档	任务报告——配置管理评估 异常报告
h) **危险分析。**确定软件引入的系统危险。危险分析应 1) 标识导致每个系统危险的软件需求; 2) 确认软件对每个危险的处理、控制或缓解。	SRS IRS 危险分析报告	任务报告——危险分析 异常报告
i) **风险分析。**使用先前的任务报告评审和更新风险分析。为消除、降低或缓解风险提供建议。	概念文档 SRS IRS 供方开发计划和进度安排 危险分析报告 V&V 任务结果	任务报告——风险分析 异常报告

5.5.4 活动:设计 V&V

在设计 V&V 活动中,软件需求被转化为每个软件部件的体系结构和详细设计。设计包括数据库和接口(软件外部、软件部件间、软件单元间)。设计 V&V 活动涉及软件体系结构设计和软件详细设计。V&V 的目标是表明设计是软件需求的正确、准确和完备的转化,而且没有引入非预期的特征。

在选定适当的软件完整性级别后,V&V 工作应从下列任务中执行针对设计 V&V 的最低限度 V&V 任务(见表 9):

a) 任务：可追踪性分析；
b) 任务：软件设计评价；
c) 任务：接口分析；
d) 任务：关键性分析；
e) 任务：部件V&V测试计划生成和验证；
f) 任务：集成V&V测试计划生成和验证；
g) 任务：V&V测试设计生成和验证；
h) 任务：危险分析；
i) 任务：风险分析。

表 9 设计 V&V 活动的任务、输入和输出

V&V 任务	要求的输入	要求的输出
设计 V&V 活动(开发过程)		
a) **可追踪性分析**。追踪设计要素(SDD 和 IDD)到需求(SRS 和 IRS)，及需求到设计要素。分析正确性、一致性和完备性的关系。任务准则如下： 1) 正确性： 确认每个设计要素和软件需求间的关系。 2) 一致性： 验证设计要素和软件需求间的关系是否按一致的详细程度来规定。 3) 完备性： ① 验证所有的设计要素都可追踪到软件需求。 ② 验证所有的软件需求都可追踪到设计要素。	SRS SDD IRS IDD	任务报告——可追踪性分析 异常报告
b) **软件设计评价**。评价设计要素(SDD 和 IDD)的正确性、一致性、完备性、准确性、可读性和可测性。任务准则如下： 1) 正确性： ① 验证和确认源代码部件满足软件设计。 ② 验证源代码部件遵循标准、引用文件、规章、政策、法律、和商业规则。 ③ 使用逻辑和数据流以及领域专业知识、原型结果、工程原理或其他基础知识确认源代码部件的状态顺序和状态变化。 ④ 确认数据和控制流满足功能性和性能需求。 ⑤ 确认数据用法和格式。 ⑥ 评估编码方法和标准的适合性。 2) 一致性： ① 验证所有的术语和代码概念是否编写一致。 ② 验证源代码部件之间具有内部一致性。 3) 完备性： ① 验证在系统假设和约束条件，下列要素是否处于 SDD 中： －功能性(例如，算法、状态/模式定义、输入/输出确认、异常处理、报告和日志)； －过程定义和进度安排； －硬件、软件和用户接口描述； －性能准则(例如，时间、规模、速度、能力、准确性、精度、安全性和安全保密性)； －关键配置数据； －系统、设备和软件控制(例如，初始化、事务和状态监控、自检)。 ② 验证 SDD 和 IDD 满足了特定配置管理规程。 4) 准确性： ① 确认逻辑、计算和接口精度(例如，截断法和舍入法)满足系统环境下的需求。	SRS IRS SDD IDD 设计标准(例如，标准、惯例和约定)	任务报告——软件设计评价 异常报告

表 9(续)

V&V 任务	要求的输入	要求的输出
设计 V&V 活动(开发过程)		
② 确认所建物理现象模型是否遵从系统准确性需求和自然规律。 5) 可读性： ① 验证文档对预期读者是明了的、可理解的和无歧义的。 ② 验证文档定义了所有首字母缩写词、助记法、缩略语、术语、符号和设计语言。 6) 可测试性： ① 验证是否具有用于确认每个软件设计要素和系统设计的目标验收准则。 ② 验证每个软件设计要素对于目标验收准则是否可测。		
c) **接口分析。**验证和确认软件设计与硬件、用户、操作人员、软件和其他系统的接口的正确性、一致性、完备性、准确性和可测试性。任务准则如下： 1) 正确性： 确认系统需求环境下的外部和内部软件接口设计。 2) 一致性： 验证 SDD 和 IDD 之间的接口设计是否一致。 3) 完备性： 验证每个接口是否都得到描述并包括了数据格式和性能准则(例如，时间、带宽、准确性、安全性和安全保密性)。 4) 准确性： 验证每个接口以要求的准确性提供信息。 5) 可测试性： 验证具有用于确认接口需求的目标验收准则。	概念文档(系统需求) SRS IRS SDD IDD	任务报告——接口分析 异常报告
d) **关键性分析。**使用 SDD 和 IDD 来评审和更新源于先前关键性任务报告的现有关键性分析结果。实现方法和连接技术可导致先前指定给软件要素(即，需求、模块、功能、子系统、其他软件划分)的软件完整性级别的提升或下降。验证没有因评审已修改软件完整性级别而引入不一致的或不期望的软件完整性结果。	任务报告——关键性 SDD IDD	任务报告——关键性分析 异常报告
e) **部件 V&V 测试计划生成和验证。**(对于软件完整性第 3 和第 4 级)策划部件 V&V 测试以确认软件部件(例如，单元、源代码模块)正确实现了部件需求。任务准则为 1) 对设计需求的依从性； 2) 时间、规模和准确性的评估； 3) 边界的和接口的、及处于强度和错误条件下的性能； 4) 需求测试覆盖率和软件可靠性与可维护性的测量。 策划设计需求的追踪以测试设计、用例、规程和结果。策划测试任务和结果的文档。验证部件 V&V 测试计划是否遵循项目定义的测试文档目的、格式和内容(见 GJB 438A－1997)。确认部件 V&V 测试计划满足下列准则： 1) 对软件需求和设计的可追踪； 2) 对软件需求和设计的外部一致性； 3) 单元需求间的内部一致性； 4) 每个单元的需求的测试覆盖率； 5) 软件集成和测试的可行性； 6) 运行和维护(例如，依据用户要求运行和维护的能力)的可行性。 (对于软件完整性第 2 级)验证开发方部件测试计划是否遵循项目定义的测试文档目的、格式和内容(见 GJB 438A－1997)。确认开发方部件测试计划满足了下列准则： 1) 对软件需求和设计的可追踪； 2) 对软件需求和设计的外部一致性； 3) 单元需求间的内部一致性；	SRS SDD IRS IDD 部件测试计划	部件 V&V 测试计划 异常报告

表 9(续)

V&V 任务	要求的输入	要求的输出
设计 V&V 活动(开发过程)		
4) 单元的测试覆盖率； 5) 软件集成和测试的可行性； 6) 运行和维护(例如，依据用户要求运行和维护的能力)的可行性。 (软件完整性第 1 级没有部件测试需求。)	SRS SDD IRS IDD 部件测试计划	部件 V&V 测试计划 异常报告
f) **集成V&V测试计划生成和验证。**(对于软件完整性第3和第4级)策划集成测试以确认软件正确地实现了软件需求和设计，而每个软件部件(例如，单元或模块)相互渐增地集成。任务准则为 1) 对每个集成阶段的逐渐增大的功能需求的依从性； 2) 时间、规模和准确性的评估； 3) 边界的和强度条件下的性能； 4) 需求测试覆盖率和软件可靠性的测量。 设计需求追踪以测试设计、用例、规程和结果。设计测试任务和结果的文档。验证集成 V&V 测试计划遵循定义了测试文档目的、格式和内容(见 GJB 438A－1997)的项目。确认集成 V&V 测试计划满足下列准则： 1) 对系统需求的可追踪； 2) 系统需求的外部一致性； 3) 内部一致性； 4) 软件需求的测试覆盖率； 5) 所用测试标准和方法的适合性； 6) 对于预期结果的符合性； 7) 软件合格性测试的可行性； 8) 运行和维护(例如，依据用户要求运行和维护的能力)的可行性。 (对于软件完整性第 1 和第 2 级)验证开发方集成测试计划遵循定义了测试文档目的、格式和内容(见 GJB 438A－1997)的项目。确认开发方集成测试计划满足下列准则： 1) 对系统需求的可追踪； 2) 系统需求的外部一致性； 3) 内部一致性； 4) 软件需求的测试覆盖率； 5) 测试标准和方法的适合性； 6) 对于预期结果的符合性； 7) 软件合格性测试的可行性； 8) 运行和维护(例如，依据用户要求运行和维护的能力)的可行性。	SRS IRS SDD IDD 集成测试计划	集成 V&V 测试计划 异常报告
g) **V&V 测试设计生成和验证。**(对于软件完整性第 3 和第 4 级)设计如下测试： 1) 部件测试； 2) 集成测试； 3) 系统测试； 4) 验收测试。 继续 V&V 测试计划要求的追踪。验证 V&V 测试设计遵循定义了测试文档目的、格式和内容(见 GJB 438A－1997)的项目。确认 V&V 测试设计满足 V&V 任务中 5.5.4 的任务 e)、5.5.4 的任务 f)、5.5.3 的任务 e)、5.5.3 的任务 f)的有关部件、集成、系统和验收测试的各自的准则。 (对于软件完整性第 1 和第 2 级)验证开发方测试设计遵循定义了测试文档目的、格式和内容(见 GJB 438A－1997)的项目。确认开发方测试设计满足 V&V 任务中 5.5.4 的任务 e)、5.5.4 的任务 f)、5.5.3 的任务 e)、5.5.3 的任务 f)的有关部件(仅第 2 级)、集成(第 1 和第 2 级)、系统(第 1 和第 2 级)和验收(仅第 2 级)测试的各自的准则。	SDD IDD 用户文档 测试计划 测试设计	部件 V&V 测试设计 集成 V&V 测试设计 系统 V&V 测试设计 验收 V&V 测试设计 异常报告

表 9(续)

V&V 任务	要求的输入	要求的输出
设计 V&V 活动(开发过程)		
h) **危险分析**。验证逻辑设计和相关的数据要素正确地实现了关键性需求并且未引入新危险。更新危险分析。	SDD IDD 危险分析报告	任务报告——危险分析 异常报告
i) **风险分析**。使用先前的任务报告评审和更新风险分析。为消除、降低或缓解风险提供建议。	SDD IDD 供方开发计划和进度安排 危险分析报告 V&V 任务结果	任务报告——风险分析 异常报告

5.5.5 活动：实现 V&V

实现 V&V 活动将设计转化为代码、数据库结构和相关的可执行机器表示。实现 V&V 活动涉及软件编码和测试。V&V 的目标是验证和确认这些转化是正确、准确和完备的。

在选定适当的软件完整性级别后，V&V 工作应从下列任务中执行针对实现 V&V 的最低限度 V&V 任务(见表 10)：

a) 任务：可追踪性分析；
b) 任务：源代码和源代码文档评价；
c) 任务：接口分析；
d) 任务：关键性分析；
e) 任务：V&V 测试用例生成和验证；
f) 任务：V&V 测试规程生成和验证；
g) 任务：部件 V&V 测试执行和验证；
h) 任务：危险分析；
i) 任务：风险分析。

表 10 实现 V&V 活动的任务、输入和输出

V&V 任务	要求的输入	要求的输出
实现 V&V 活动(开发过程)		
a) **可追踪性分析**。追踪源代码部件到相应设计规格说明、设计规格说明到源代码部件。分析标识的正确性、一致性和完备性的关系。任务准则如下： 1) 正确性： 确认源代码部件和设计要素间的关系。 2) 一致性： 验证源代码部件和设计要素间的关系规定为一个一致的详细的级别。 3) 完备性： ① 验证所有源代码部件可从设计要素追踪到。 ② 验证所有设计要素可从源代码部件追踪到。	SDD IDD 源代码	任务报告——可追踪性分析 异常报告
b) **源代码和源代码文档评价**。评价源代码部件(源代码文档)的正确性、一致性、完备性、准确性、可读性和可测试性。任务准则如下： 1) 正确性： ① 验证和确认源代码部件满足软件设计。 ② 验证源代码部件遵循标准、引用文件、规章、政策、法律和商业规则。	源代码 SDD IDD 编码标准(例如，标准、惯例、项目限制条件、和约定) 用户文档	任务报告——源代码和源代码文档评价 异常报告

表 10(续)

V&V 任务	要求的输入	要求的输出
实现 V&V 活动(开发过程)		
③ 使用逻辑和数据流以及领域专业知识、原型结果、工程原理或其他基础知识确认源代码部件状态顺序和状态变化。 ④ 确认数据和控制流满足功能性和性能需求。 ⑤ 确认数据用法和格式。 ⑥ 评估编码方法和标准的适合性。 2) 一致性： ① 验证所有术语和代码概念是否编写一致。 ② 验证源代码部件之间具有内部一致性。 ③ 确认软件设计和需求的外部一致性。 3) 完备性： ① 验证在系统假设和约束条件下，下列要素是否处于源代码之中： －功能性(例如，算法、状态/模式定义、输入/输出确认、异常处理、报告和日志)； －过程定义和进度安排； －硬件、软件和用户接口描述； －性能准则(例如，时间、规模、速度、能力、准确性、精度、安全性和安全保密性)； －关键配置数据； －系统、设备和软件控制(例如，初始化、事务和状态监控、自检)。 ② 验证源代码文档是否满足规定的配置管理规程。 4) 准确性： ① 确认系统环境下的逻辑、计算和接口精度(例如，截断法和舍入法)。 ② 确认建立的物理现象模型遵从系统准确性需求和自然规律。 5) 可读性： ① 验证文档对预期读者是明了的、可理解的和无歧义的。 ② 验证文档定义了所有首字母缩写词、助记法、缩略语、术语和符号。 6) 可测试性： ① 验证拥有用于确认每个源代码部件的目标验收准则。 ② 验证每个源代码部件依目标验收准则是可测试的。	源代码 SDD IDD 编码标准(例如，标准、惯例、项目限制条件、和约定) 用户文档	任务报告——源代码和源代码文档评价 异常报告
c) **接口分析**。验证和确认软件源代码与硬件、用户、操作人员、软件和其他系统的接口的正确性、一致性、完备性、准确性和可测试性。任务准则如下： 1) 正确性： 确认在系统需求环境下的外部和内部软件接口代码。 2) 一致性： 验证源代码部件间和外部接口(即，硬件、用户、操作人员和其他软件)的接口代码是一致的。 3) 完备性： 验证每个接口都进行了描述并包括数据格式和性能准则(例如，时间、带宽、准确性、安全性和安全保密性)。 4) 准确性：	概念文档(系统需求) SDD IDD 源代码 用户文档	任务报告——接口分析 异常报告

表 10(续)

V&V 任务	要求的输入	要求的输出
实现 V&V 活动(开发过程)		
验证每个接口是否都以要求的准确性提供信息。 5) 可测试性： 验证是否具有用于确认接口代码的目标验收准则。	概念文档(系统需求) SDD IDD 源代码 用户文档	任务报告——接口分析 异常报告
d) **关键性分析。**使用源代码评审和更新源于先前关键性任务报告的现存关键性分析结果。实现方法和连接技术可导致先前指定给软件要素(即，需求、模块、功能、子系统、其他软件划分)的软件完整性级别提升或下降。验证没有因评审已修改软件完整性级别而引入不一致的或不期望的软件完整性结果。	任务报告——关键性源代码	任务报告——关键性分析 异常报告
e) **V&V 测试用例生成和验证。**(对于软件完整性第 3 和第 4 级)开发如下 V&V 测试用例： 1) 部件测试； 2) 集成测试； 3) 系统测试； 4) 验收测试。 继续 V&V 测试计划要求的追踪。验证 V&V 测试用例是否遵循项目定义的测试文档目的、格式和内容(见 GJB 438A－1997)。确认 V&V 测试用例满足 V&V 任务中 5.5.4 的任务 e)、5.5.4 的任务 f)、5.5.3 的任务 e)、5.5.3 的任务 f)的有关部件、集成、系统和验收测试的各自的准则。 (对于软件完整性第 1 和第 2 级)验证开发方测试用例是否遵循项目定义的测试文档目的、格式和内容(见 GJB 438A－1997)。确认开发方测试用例满足 V&V 任务中 5.5.4 的任务 e)、5.5.4 的任务 f)、5.5.3 的任务 e)、5.5.3 的任务 f)的有关部件(仅第 2 级)、集成(第 1 和第 2 级)、系统(第 1 和第 2 级)和验收(仅第 2 级)测试的各自的准则。	SRS IRS SDD IDD 用户文档 测试设计 测试用例	部件 V&V 测试用例 集成 V&V 测试用例 系统 V&V 测试用例 验收 V&V 测试用例 异常报告
f) **V&V 测试规程生成和验证。**(对于软件完整性第 3 和第 4 级)开发如下 V&V 测试规程： 1) 部件测试； 2) 集成测试； 3) 系统测试。 继续 V&V 测试计划要求的追踪。验证 V&V 测试规程是否遵循项目定义的测试文档目的、格式和内容(见 GJB 438A－1997)。确认 V&V 测试规程满足 V&V 任务中 5.5.4 的任务 e)、5.5.4 的任务 f)、5.5.3 的任务 e)、5.5.3 的任务 f)的有关部件、集成和系统测试的各自的准则。 (对于软件完整性第 1 和第 2 级)验证开发方测试规程是否遵循项目定义的测试文档目的、格式和内容(见 GJB 438A－1997)。确认开发方测试规程满足 V&V 任务中 5.5.4 的任务 e)、5.5.4 的任务 f)、5.5.3 的任务 e)、5.5.3 的任务 f)的有关部件(仅第 2 级)、集成(第 1 和第 2 级)、系统(第 1 和第 2 级)和验收(仅第 2 级)测试的各自的准则。	SRS IRS SDD IDD 用户文档 测试用例 测试规程	部件 V&V 测试规程 集成 V&V 测试规程 系统 V&V 测试规程 异常报告

表 10(续)

V&V 任务	要求的输入	要求的输出
实现 V&V 活动(开发过程)		
g) **部件 V&V 测试执行和验证。**(对于软件完整性第 3 和第 4 级)执行 V&V 部件测试。分析测试结果以确认软件正确实现了设计。确认测试结果可追踪到在测试计划文档中由测试可追踪性建立的测试准则。按部件 V&V 测试计划的要求记录结果。使用 V&V 部件测试结果来确认软件满足了 V&V 测试验收准则。记录真实的和预期的测试结果间的差异。 (对于软件完整性第 2 级)使用开发方部件测试结果来确认软件满足了测试验收准则。 (软件完整性第 1 级没有部件测试需求。)	源代码 可执行代码 SDD IDD 部件测试计划 部件测试规程 部件测试结果	任务报告——测试结果 异常报告
h) **危险分析。**验证实现和相关的数据要素是否正确地实现了关键需求并且不引入新的危险。更新危险分析。	源代码 SDD IDD 危险分析报告	任务报告——危险分析 异常报告
i) **风险分析。**使用先前的任务报告评审和更新风险分析。为消除、降低或缓解风险提供建议。	源代码 供方开发计划和进度安排 危险分析报告 V&V 任务结果	任务报告——风险分析 异常报告

5.5.6 活动：测试 V&V

测试 V&V 活动覆盖软件测试、软件集成、软件合格性测试、系统集成和系统合格性测试。测试 V&V 活动及它与软件生存周期的关系如图 3 中所示。V&V 的目标是确保通过执行集成测试、系统测试和验收测试使软件需求和分配给软件的系统需求得到满足。

对于软件完整性级别 3 和 4 而言，V&V 工作应生成自己的 V&V 软件和系统测试产品(例如，计划、设计、用例、规程)，执行并记录自己的测试，并对照软件需求验证开发过程的测试计划、设计、用例、规程和结果。对于软件完整性级别 1 和 2 而言，V&V 工作应验证开发过程的测试活动和产品(例如，测试计划、设计、用例、规程、及执行结果)。

在选定适当的软件完整性级别后，V&V 工作应从下列任务中执行针对测试 V&V 的最低限度 V&V 任务(见表 11)：

a) 任务：可追踪性分析；
b) 任务：验收 V&V 测试规程生成和验证；
c) 任务：集成 V&V 测试执行和验证
d) 任务：系统 V&V 测试执行和验证；
e) 任务：验收 V&V 测试执行和验证；
f) 任务：危险分析；
g) 任务：风险分析。

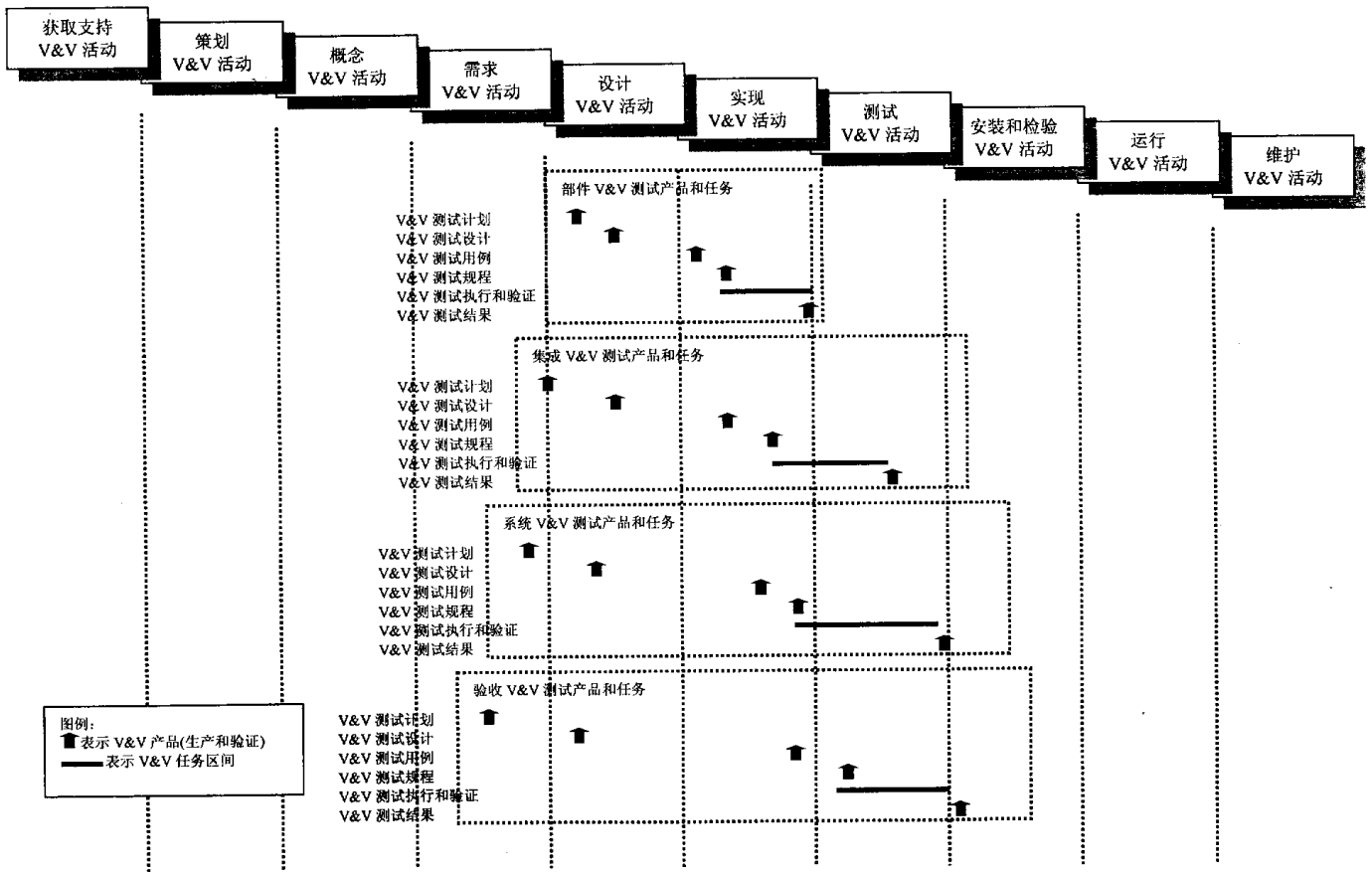


图 3　V&V 测试产品和测试执行任务的时段图示例

表 11　测试 V&V 活动的任务、输入和输出

V&V 任务	要求的输入	要求的输出
测试 V&V 活动(开发过程)		
a) **可追踪性分析**。分析在 V&V 测试计划、设计、用例和规程中的正确性和完备性的关系。对于正确性，验证在 V&V 测试计划、设计、用例和规程间是否具有有效的关系。对于完备性，验证所有 V&V 测试规程可追踪到 V&V 测试计划。	V&V 测试计划 V&V 测试设计 V&V 测试规程	任务报告——可追踪性分析 异常报告
b) **验收 V&V 测试规程生成和验证**。(对于软件完整性第 3 和第 4 级)制定验收 V&V 测试规程。继续验收 V&V 测试计划要求的追踪。验证 V&V 测试规程是否遵循项目定义的测试文档目的、格式和内容(见 GJB 438A－1997)。确认验收 V&V 测试规程满足 V&V 任务中 5.5.3 的任务 f)的准则。 (对于软件完整性第 2 级)验证开发方验收测试规程是否遵循项目定义的测试文档目的、格式和内容(见 GJB 438A－1997)。确认开发方测试规程满足 V&V 任务中 5.5.3 的任务 f)的准则。 (软件完整性第 1 级没有验收测试需求。)	SDD IDD 源代码 用户文档 验收测试计划 验收测试规程	验收 V&V 测试规程 异常报告
c) **集成 V&V 测试执行和验证**。(对于软件完整性第 3 和第 4 级)执行 V&V 集成测试。分析测试结果以验证软件部件是否正确地集成。确认测试结果可追踪到在测试计划文档中由测试可追踪性建立的测试准则。按集成 V&V 测试计划的要求记录结果。使用 V&V 集成测试结果来确认软件是否满足 V&V 测试验收准则。记录实际的和预期的测试结果的差异。 (对于软件完整性第 1 和第 2 级)使用开发方集成测试结果来验证软件是否满足了测试验收准则。	源代码 可执行代码 集成测试计划 集成测试规程 集成测试结果	任务报告——测试结果 异常报告
d) **系统 V&V 测试执行和验证**。(对于软件完整性第 3 和第 4 级)执行 V&V 系统测试。分析测试结果以确认软件是否满足了系统需求。确认测试结果可追踪到在测试计划文档中由测试可追踪性建立的测试准则。按系统 V&V 测试计划的要求记录结果。使用 V&V 系统测试结果来确认软件是否满足了 V&V 测试验收准则。记录实际的和预期的测试结果间的差异。 (对于软件完整性第 1 和第 2 级)使用开发方系统测试结果来验证软件是否满足测试验收准则。	源代码 可执行代码 系统测试计划 系统测试规程 系统测试结果	任务报告——测试结果 异常报告
e) **验收 V&V 测试执行和验证**。(对于软件完整性第 3 和第 4 级)执行验收 V&V 测试。分析测试结果以确认软件是否满足了系统需求。确认测试结果可追踪到在测试计划文档中由测试可追踪性建立的测试准则。按验收 V&V 测试计划的要求记录结果。使用验收 V&V 测试结果来确认软件是否满足了 V&V 测试验收准则。记录实际的和预期的测试结果间的差异。 (对于软件完整性第 2 级)使用开发方验收测试结果来验证软件是否满足了测试验收准则。 (软件完整性第 1 级没有验收测试需求。)	源代码 可执行代码 用户文档 验收测试计划 验收测试规程 验收测试结果	任务报告——测试结果 异常报告
f) **危险分析**。验证测试仪器没有引入新危险。更新危险分析。	源代码 可执行代码 测试结果 危险分析报告	任务报告——危险分析 异常报告
g) **风险分析**。使用先前的任务报告评审和更新风险分析。为消除、降低或缓解风险提供建议。	供方开发计划和进度安排 危险分析报告 V&V 任务结果	任务报告——风险分析 异常报告

5.5.7　活动：安装和检验 V&V

安装和检验 V&V 活动是指在目标环境下对软件产品的安装、以及需方对软件产品的验收评审和测试。安装和检验 V&V 活动涉及软件安装和软件验收支持。V&V 的目标是验证和确认在目标环境下软件安装的正确性。

在选定适当的软件完整性级别后，V&V 工作应从下列任务中执行针对安装和检验 V&V 的最低限

度 V&V 任务(见表 12)：

a) 任务：安装配置审核；
b) 任务：安装检验；
c) 任务：危险分析；
d) 任务：风险分析；
e) 任务：V&V 最终报告生成。

表 12 安装和检验 V&V 活动的任务、输入和输出

V&V 任务	要求的输入	要求的输出
安装和检验 V&V 活动(开发过程)		
a) **安装配置审核**。验证正确地安装和运行软件需要的所有软件产品是否都在安装包内。确认所提供的与场所有关的参数和条件是否正确。	安装包(例如，源代码、可执行代码、用户文档、SDD、IDD、SRS、IRS、概念文档、安装规程、特定场地参数、安装测试、配置管理数据)	任务报告——安装配置审核 异常报告
b) **安装检验**。进行分析或测试以验证已安装的软件与经受 V&V 的软件是否一致。验证软件代码和数据库按规定进行初始化、执行和终止。在软件从一个版本到下一个版本的转换中，V&V 工作应确认软件能在不影响剩余系统部件的性能的情况下从系统删除。V&V 工作应验证在包括用户通知的转换过程中连续地运行和服务的需求。	用户文档 安装包	任务报告——安装检验 异常报告
c) **危险分析**。验证安装规程和安装环境是否未引入新危险。更新危险分析。	安装包 危险分析报告	任务报告——危险分析 异常报告
d) **风险分析**。使用先前的任务报告评审和更新风险分析。为消除、降低或缓解风险提供建议。	安装包 供方开发计划和进度安排 V&V 任务结果	任务报告——风险分析 异常报告
e) **V&V 最终报告生成**。在 V&V 最终报告中总结 V&V 活动、任务和结果，包括异常的状态和处理。提供对于软件质量的全面评估和建议。	V&V 活动总结报告	V&V 最终报告

5.6 过程：运作

5.6.1 概述

运作过程包括软件产品的运行和对用户的运行支持。运行 V&V 活动评价在预期运行环境中任何更改的影响，评估任何建议的更改对系统的影响，评价符合预期用途的操作规程，并分析影响用户和系统的风险。

5.6.2 活动：运行 V&V

运行 V&V 活动是最终用户在运行环境下对软件的使用的评价。运行 V&V 活动涉及运行测试、系统运行和对用户的支持。V&V 的目标是评价系统的新的约束条件，评估建议的更改和它们对软件的影响，并评价操作规程的正确性和可用性。

在选定适当的软件完整性级别后，V&V 工作应从下列任务中执行针对运行 V&V 的最低限度 V&V 任务(见表 13)：

a) 任务：对新约束条件的评价；
b) 任务：评估建议的更改；
c) 任务：运行规程评价；
d) 任务：危险分析；
e) 任务：风险分析。

5.7 过程：维护

5.7.1 概述

由于问题的出现、需要改进或适应新的需求而导致对软件产品的代码和相关文档进行修改时，维护过程即被激活。维护V&V活动涉及在运作过程期间软件的修改(例如，增强、添加、删除)、迁移或退役。

表 13 运行 V&V 活动的任务、输入和输出

V&V 任务	要求的输入	要求的输出
运行 V&V 活动(运作过程)		
a) **新约束条件评价。**评价关于系统或软件需求的新约束条件(例如，运行需求、平台特性、运行环境)以验证 SVVP 的适应性。软件更改视为维护活动(见 5.7.2)。	SVVP 新约束条件	任务报告——新约束条件评价
b) **评估建议的更改。**评估建议的更改(例如，修改、增强或附加)以确定这些变化对系统的影响。确定 V&V 任务重复的程度。	建议的更改 安装包	任务报告——评估建议的更改
c) **操作规程评价。**验证操作规程是否与用户文档一致并且遵循系统需求。	操作规程 用户文档 概念文档	任务报告——操作规程评价 异常报告
d) **危险分析。**验证操作规程和运行环境是否未引入新的危险。更新危险分析。	操作规程 危险分析报告	任务报告——危险分析 异常报告
e) **风险分析。**使用先前的任务报告评审和更新风险分析。为消除、降低或缓解风险提供建议。	安装包 建议的更改 危险分析报告 供方开发计划和进度安排 运行问题报告 V&V 任务结果	任务报告——风险分析 异常报告

软件的修改应作为开发过程看待，并按 5.2(管理过程)和 5.5(开发过程)中的描述加以验证和确认。在维护过程中应对软件完整性级别的指定进行评估。软件完整性级别的指定应进行适当修改以反映维护过程的需求。这些修改可能源于为纠正软件错误(例如，纠正性的)、为适应一个已改变的运行环境(例如，适应性的)、为响应附加的用户请求或增强(例如，完善性的)而规定的需求。

5.7.2 活动：维护 V&V

维护 V&V 活动覆盖软件的修改(例如，纠正性的、适应性的、完善性的)、迁移或退役。软件的迁移是指软件移到一个新的运行环境。对于软件的迁移，V&V 工作应验证所迁移的软件满足了 5.5 到 5.6 的需求。软件的退役是运行和维护组织对现行支持的撤销，部分或全部地由一个新系统代替，或安装一个已更新的系统。

如果软件依据本标准验证，在维护过程中应继续遵循本标准。如果软件不依据本标准验证，且无适当的文档可用或适当的文档不充分，V&V 工作将确定是否应生成缺失的或不完整的文档。在决定是否生成缺失的文档时，应考虑指定的软件完整性级别的最低限度 V&V 需求。

维护 V&V 活动涉及问题和修改分析、修改的实施、维护评审/验收、迁移和软件退役。V&V 的目标是评估所建议的更改和它们对软件的影响，评价运行期间发现的异常，评估迁移需求，评估退役需求并重新执行 V&V 任务。

在选定适当的软件完整性级别后，V&V 工作应从下列任务中执行针对维护 V&V 的最低限度 V&V 任务(见表 14)：

a) 任务：SVVP 修改；
b) 任务：评估建议的更改；
c) 任务：异常评价；
d) 任务：关键性分析；
e) 任务：迁移评估；

f) 任务：退役评估；
g) 任务：危险分析；
h) 任务：风险分析；
i) 任务：任务重复。

表 14 维护 V&V 活动的任务、输入和输出

V&V 任务	要求的输入	要求的输出
维护 V&V 活动(运作过程)		
a) **SVVP 修订。**修订 SVVP 以遵循批准的更改。当没有本标准要求的开发文档集可用时，生成一个新的 SVVP 并考虑附录 D(可重用软件的 V&V)中的方法来导出要求的开发文档集。	SVVP 批准的更改 安装包 供方开发计划和进度安排	已更新 SVVP
b) **评估建议的更改。**评估建议的更改(例如，修改、增强或附加)以确定这些变化对系统的影响。确定 V&V 任务重复的程度。	建议的更改 安装包 供方开发计划和进度安排	任务报告——评估建议的更改
c) **异常评价。**评价软件运行异常的影响。	异常报告	任务报告——异常评价
d) **关键性分析。**为建议的修改确定软件完整性级别。确认维护方提供的完整性级别。出于 V&V 策划目的，指定给软件的最高完整性级别应是软件系统的完整性级别。	建议的更改 安装包 维护方完整性级别	任务报告——关键性分析 异常报告
e) **迁移评估。**评估软件需求和实现是否指出： 1) 特定迁移需求； 2) 迁移工具； 3) 软件产品和数据转换； 4) 软件归档； 5) 先前的环境支持； 6) 用户通知。	安装包 批准的更改	任务报告——迁移评估 异常报告
f) **退役评估。**对于软件退役，评估安装包是否指出： 1) 软件支持； 2) 对现存系统和数据库的影响； 3) 软件归档； 4) 转换为一个新的软件产品； 5) 用户通知。	安装包 批准的更改	任务报告——退役评估
g) **危险分析。**验证软件修改正确实现了关键性需求并且没有引入新危险。更新危险分析。	建议的更改 安装包 危险分析报告	任务报告——危险分析 异常报告
h) **风险分析。**使用先前的任务报告评审和更新风险分析。为消除、降低或缓解风险提供建议。	安装包 建议的更改 危险分析报告 供方开发计划和进度安排 运行问题报告 V&V 任务结果	任务报告——风险分析 异常报告
i) **任务重复。**按需执行 V&V 任务以确保 1) 计划的更改被正确实现； 2) 文档完整且通用； 3) 更改没有导致不可接受的或不可预期的系统行为。	批准的更改 安装包	任务报告 异常报告

表 15　指定给每个软件完整性级别的最低限度 V&V 任务

生存周期过程	获取				供应				开发																				运行				维护			
V&V 活动	获取支持 V&V 活动				计划 V&V 活动				概念 V&V 活动				需求 V&V 活动				设计 V&V 活动				实现 V&V 活动				测试 V&V 活动				安装检验 V&V 活动				运行 V&V 活动				维护 V&V 活动			
软件完整性级别	级别				级别				级别				级别				级别				级别				级别				级别				级别			
	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1
验收 V&V 测试执行和验证																									X	X	X									
验收 V&V 测试计划生成和验证													X	X	X																					
验收 V&V 测试规程生成和验证																									X	X	X									
异常评价																																	X	X	X	
部件 V&V 测试执行和验证																					X	X	X													
部件 V&V 测试计划生成和验证																	X	X	X																	
概念文档评价									X	X	X																									
配置管理评估													X	X																						
合同验证					X																															
关键性分析									X	X	X		X	X	X		X	X	X		X	X	X										X	X	X	
新约束条件评价																																	X	X	X	
硬件/软件/用户需求分配分析									X																											
危险分析									X	X			X	X			X	X			X	X			X	X			X	X			X	X		
安装检验																													X	X						
安装配置审核																													X	X						
接口分析													X	X	X		X	X	X		X	X	X													
集成 V&V 测试执行和验证																									X	X	X	X								

表 15(续)

生存周期过程		获取				供应				开发																				运行				维护			
V&V 活动		获取支持 V&V 活动				计划 V&V 活动				概念 V&V 活动				需求 V&V 活动				设计 V&V 活动				实现 V&V 活动				测试 V&V 活动				安装检验 V&V 活动				运行 V&V 活动				维护 V&V 活动			
软件完整性级别		级别				级别				级别				级别				级别				级别				级别				级别				级别			
		4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1
V&V 管理	a) 基线更改评估									X				X	X	X		X	X	X		X	X	X		X	X	X		X	X			X	X		
	b) 组织支持过程接口	X	X			X	X			X	X			X	X			X	X			X	X			X	X			X	X			X	X		
	c) 管理和技术评审支持									X	X			X	X			X	X			X	X			X	X			X	X			X	X		
	d) V&V 管理评审	X	X	X		X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	e) 软件 V&V 计划生成									X	X	X	X																					X	X	X	X
迁移评估																																		X	X		
操作规程评价										X	X	X	X																			X	X					
设计 V&V 工作和供方之间的接口		X	X	X		X	X	X																													
评估建议的更改																																X	X	X		X	X	X	
风险分析										X	X			X	X			X	X			X	X			X	X			X	X			X	X		
退役评估																																		X	X		
圈定 V&V 工作范围		X	X	X																																	
软件设计评价																		X	X	X	X																	
软件需求评价														X	X	X	X																					
SVVP 修改																																		X	X	X	X

表 15(续)

生存周期过程		获取				供应				开发																运行				维护			
V&V 活动		获取支持 V&V 活动				计划 V&V 活动				概念 V&V 活动				需求 V&V 活动				设计 V&V 活动				实现 V&V 活动				测试 V&V 活动				安装检验 V&V 活动				运行 V&V 活动				维护 V&V 活动			
软件完整性级别		级别				级别				级别				级别				级别				级别				级别				级别				级别			
		4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1
源代码和源代码文档评价																						X	X	X	X																
系统需求评审		X	X	X	X																																				
系统 V&V 测试执行和验证																										X	X	X	X												
系统 V&V 测试计划生成和验证														X	X	X	X																								
任务重复																																						X	X	X	X
可追踪性分析										X	X	X		X	X	X		X	X	X		X	X	X		X	X	X													
V&V 最终报告生成																														X	X	X									
V&V 测试设计生成和验证	a) 部件																	X	X	X																					
	b) 集成																	X	X	X	X																				
	c) 系统																	X	X	X	X																				
	d) 验收																	X	X	X																					
V&V 测试用例生成和验证	a) 部件																					X	X	X																	
	b) 集成																					X	X	X	X																
	c) 系统																					X	X	X	X																
	d) 验收																					X	X	X																	
V&V 测试规程生成和验证	a) 部件																					X	X	X																	
	b) 集成																					X	X	X	X																
	c) 系统																					X	X	X	X																

注：表中的“X”表示在该列所对应的软件完整性级别下必须执行该行所对应的 V&V 任务。

6 软件 V&V 报告、管理和文档要求

6.1 V&V 报告要求

V&V 报告产生于整个软件生存周期中。SVVP 应规定所有 V&V 报告的内容、格式和时间选择。软件验证和确认报告(SVVR)包括所有 V&V 报告。V&V 报告应包括要求的 V&V 报告(即，V&V 任务报告、V&V 活动摘要报告、V&V 异常报告和 V&V 最终报告)。V&V 报告也可包括可选报告。报告要求在附录 A 的第 6 章中进行描述。

6.2 V&V 管理要求

SVVP 描述了支持 V&V 工作的 V&V 管理要求。这些 V&V 管理要求应包括下列内容：

a) 异常解决方案和报告；

b) 任务重复策略；

c) 偏离策略；

d) 控制规程；

e) 标准、实践和约定。

V&V 管理要求在附录 A 的第 7 章中进行描述。

6.3 V&V 文档要求

6.3.1 V&V 测试文档

V&V 测试文档应包括部件、集成、系统和验收测试的测试计划、设计、用例、规程和结果。V&V 测试文档应遵循项目定义的测试文档目的、格式和内容(见 GJB 438A－1997)。有关部件、集成、系统、和验收测试的 V&V 任务描述如表 4 至表 14 所示。

6.3.2 SVVP 文档

V&V 工作应生成符合如附录 A 所描述的 SVVP。SVVP 应在整个软件生存周期中得到维护。

SVVP 应包括在 6.1、6.2 和 6.3.1 中定义的 V&V 文档要求。

SVVP 应包含附录 A 的第 1 到第 8 章所描述的内容。针对附录 A 的编写要求，如果 SVVP 的某一章或某一章内必要的段落没有相应的信息，那么在该章或该条的开头除了写明“本章/条不适用于本计划”外，还宜写明不适用的理由。当需要时，附加的章条可加在 SVVP 的第 8 章后。如果该计划引用了其他文档的某些材料，则应在该计划的正文中标出。附录 A 中所列的 SVVP 章条号用以增强本标准的可操作性，并非遵循本标准的强制性要求。

SVVP 章条号和章条名如下列框内所示：

软件 V&V 计划

1 目的
2 引用文件
3 术语和定义
4 V&V 综述
4.1 组织
4.2 主进度
4.3 软件完整性级别方案
4.4 资源摘要
4.5 职责
4.6 工具、技术和方法
5 V&V 过程
5.1 过程：管理
5.1.1 活动：V&V 管理
5.2 过程：获取
5.2.1 活动：获取支持 V&V
5.3 过程：供应
5.3.1 活动：策划 V&V
5.4 过程：开发
5.4.1 活动：概念 V&V
5.4.2 活动：需求 V&V
5.4.3 活动：设计 V&V
5.4.4 活动：实现 V&V
5.4.5 活动：测试 V&V
5.4.6 活动：安装和检验 V&V
5.5 过程：运行
5.5.1 活动：运行 V&V
5.6 过程：维护
5.6.1 活动：维护 V&V
6 V&V 报告要求
7 V&V 管理要求
7.1 异常解决方案和报告
7.2 任务重复策略
7.3 偏离策略
7.4 控制规程
7.5 标准、实践和约定
8 V&V 文档要求

附 录 A
（资料性附录）
SVVP 内容编写要求与说明

SVVP 的编写要求和格式如下。

1 目的

SVVP 应描述软件 V&V 工作的目的、目标和范围。应标识正在编写其计划的软件项目，以及由软件 V&V 工作包含的特定软件过程和产品。

SVVP 目的陈述提供了对于软件 V&V 工作的最高层次描述。在目的陈述中一般论述下列议题：

a) 标识 SVVP 将应用于哪个项目，并描述为什么制定计划；

b) 陈述 SVVP 要满足的目标。例如，一项具体的 V&V 工作可能是用来确认所有的安全需求得到满足。另一份计划可能与确认性能需求有关；

c) 清晰地描述 V&V 工作和职责；

d) 定义 SVVP 对软件的应用范围。明确地列举 SVVP 将应用到的软件的每一部分及 SVVP 未涉及到的每一部分。例如，也许一个计算机系统的三个子系统只有两个列入 SVVP（来自以前系统的第三个部件可能是没有变化的）；或者 SVVP 仅为设计验证而应用。

2 引用文件

SVVP 应标识所遵循的标准、文件、SVVP 引用文件、任何补充或实施 SVVP 的支持文件。

3 术语和定义

SVVP 应定义或引用所有在 SVVP 中使用的术语、符号和缩略语，并尽可能使用 GB/T 11457 中的术语和定义。

4 验证和确认综述

SVVP 应描述执行软件 V&V 所必需的组织、进度、软件完整性级别方案、资源、职责、工具、技术和方法。

4.1 组织

SVVP 应描述 V&V 工作的组织，包括所需的独立性（参见本标准附录 C）程度。SVVP 应描述 V&V 过程与其他过程诸如开发、项目管理、质量保证和管理配置的关系。SVVP 应描述 V&V 工作内部的沟通渠道、解决 V&V 任务引起的问题的权限、批准 V&V 产品的权限。附录 F 提供了一个组织关系图示例。

V&V 工作的具体的组织结构将取决于开发过程中系统的特性、开发组织和获取组织以及合同的安排。

当策划 V&V 工作组织时，应考虑下列情况：

a) 在可能共负责任的地方，对每项任务（例如：接受输入、执行任务、分析结果、报告结果以及基于结果做出决定）分配具体职责；

b) 遇到职责重叠时进行准确的分配；

c) 用图表展示 V&V 工作的控制和数据流，以阐明职责。

4.2 主进度

SVVP 应描述项目生存周期和里程碑，包括完成日期。它应概括 V&V 任务和任务结果的进度作为对开发、结构和支持过程（例如，质量保证和配置管理）的反馈。应依照任务重复策略安排 V&V 任务重新执行。

如果 SVVP 中使用的生存周期不同于本标准的生存周期模型，本条应描述如何满足本标准的所有要求（例如，通过对本标准的过程、活动、任务、输入和输出的交叉引用）。策划 V&V 任务

时，应认识到 V&V 过程是重复迭代的。任务可以用文字、表格或图形的形式来描述。

主进度概述了各种 V&V 任务和它们在整个项目环境内的关系。目的是要清楚地说明 V&V 活动和项目任务间的材料的顺序流。这有助于确保，在更大的项目环境中 V&V 任务得到合适的放置，且它们的可交付产品被识别。应认识到主进度的制定将是一个重复的过程。

制定主进度时，V&V 策划者应致力于 V&V 任务和它们在项目进度中的位置，并强调关键的 V&V 任务、可交付的产品和完成日期。如果要执行一项独立的 V&V 工作，需要强调交付材料的接口、评审、完成会议等。进度表示(例如：甘特进度表、计划评审表、临界途径法)和有些情况下的进度流分析有许多形式。使用的方法应与其他项目要素一致。

4.3 软件完整性级别方案

SVVP 应描述达成一致的为系统建立的软件完整性级别方案，和选定方案到本标准所使用模型的映射。SVVP 应记录软件完整性级别到单个部件的指定(例如，需求、详细功能、软件模型、子系统、或其他软件划分)，其中有在程序中指定的不同的软件完整性级别。对于每个 SVVP 更新，应对软件完整性级别指定重新评估，以反映因体系选择、详细设计选择、代码构成用法或其他开发活动而导致的可能在完整性级别中出现的变化。

4.4 资源摘要

SVVP 应概述 V&V 资源。资源类型包括人员配备、设施、设备、实验室、实验室配置、工具(软件和硬件)、预算和资金需求、文档集、特殊的规程和条件(如安全、访问权和/或控制)。具体说明如下：

a) 使用图表和表格作为表示资源用途的有效方法。资源使用图与日历时间或生存周期阶段相比较，给出了包含在不同任务或阶段中的相关工作量的快速理解。资源使用表，也通过日历时间或生存周期阶段，帮助资源使用与预算或与其他项目工作的需求相比较。

b) 包括在设备和实验室概述中的需要的设备类型、需要的期限、特殊配置和其他外围设备，将必须执行全部的 V&V 操作。

c) 在摘要的工具部分中列出了将在整个 V&V 工作中使用的各种工具。工具可以再细分为软件和硬件。

d) 在预算和资金需求方面，考虑所有的资源并估计到追加工具和人员以应对意外。

4.5 职责

SVVP 应标识负责执行每个 V&V 任务的组织要素。对于将任务分配给多个要素时，应标出每个要素的特定职责。该条也可以是每个生存周期阶段中定义的角色和职责的概述。

V&V任务有两层职责——在项目中分配到不同的组织部门的总职责和对于要执行的任务的特定职责。总职责的概述可以在SVVP的该条中描述，或在别的项目层计划(例如：项目管理计划)中描述。如果在别的文档中描述，该条应包括概述和对其他文档的引用。特定职责可以在该条中描述，或该条可以概述SVVP的生存周期阶段部分中定义的职责。

4.6 工具、技术和方法

SVVP 应描述在 V&V 过程中使用的文档、硬件和软件 V&V 工具、技术、方法、运行与测试环境。每个工具、工艺和方法的获取、培训、支持和合格性信息应包含在内。

在 V&V 工作中描述 V&V 方法、工具和技术以及它们的作用。可以以文字或图形的形式来描述。应包括对技术或工具描述的引用。可以制定一分单独的工具计划，用于软件工具的获取、开发或修改。因此，SVVP 的该条应涉及到工具计划。如果要获取或开发工具，那么在 V&V 进度中应包括获取和开发工具的进度。确定是否对工具的获取和开发考虑了足够的时间和适当的任务。

将代码插入软件的工具应进行与最高软件完整性级别一样严格的验证和确认。不插入代码的工具应进行验证和确认以确保它们满足运行要求。如果能证明工具功能的划分，仅应对那些在 V&V 过程中使用的功能进行验证以证明它们正确执行了其预期用途。

SVVP 应记录 V&V 使用的度量方法(参见附录 E)，并描述这些度量方法如何支持 V&V 目标。

当策划使用工具、技术和方法时，应考虑下列内容：

a) 描述或引用 V&V 手段所选择的方法；

b) 人员经验和必须的培训；

c) 用于方法的专门工具和专门技术；

d) 每种工具和技术怎样加强方法；

e) 与工具或技术有关的风险；

f) 每种工具的状态

1) 是否新获取的；

2) 是否必须更改或完全可以使用；

3) 所要求的量化是否有效；

4) 它的文档是否可接受；

5) 工具是否有专利权；

g) 获取或开发进度；

h) 必要的支持(硬件，其他软件)；

i) 高风险工具的选择方法。

5 V&V 过程

SVVP 应标识本标准第 5 章描述的每个 V&V 过程要执行的 V&V 活动和任务，并应记录那些 V&V 活动和任务。SVVP 应包含所有软件生存周期过程的 V&V 活动和任务的综述。

5.1 “软件生存周期”[1)]

SVVP 应包括 SVVP 概述(文本框)中所示的 5.1 到 5.6 的 V&V 活动和任务。

对每个 V&V 活动，SVVP 都应给出以下 8 个方面的内容：

a) V&V 任务

SVVP 应标识要执行的 V&V 任务。表 4 至表 14 描述了最低限度 V&V 任务、任务准则、及要求的输入和输出。表 15 规定了每个软件完整性级别应执行的最低限度 V&V 任务。软件完整性第 4 级的最低限度任务在图 2 中合并为图解形式。

也可执行可选 V&V 任务以增加 V&V 工作来满足项目要求。可选 V&V 任务列在附录 A 的表 1 中，并在附录 G 中进行描述。附录 A 的表 1 中的列表是说明性的且并不详尽。本标准允许在适当的时候使用可选的 V&V 任务。

一些 V&V 任务适用于多于一个的软件完整性级别。执行和记录任务的严格程度和密度应与软件完整性级别相称。当软件完整性级别减少时，与 V&V 任务相关的所要求的范围、密度和严格程度也同样减少。例如，为第 4 级完整性软件而执行的危险分析可正式记录，并考虑中间级别的失效；软件完整性第 3 级软件的危险分析可仅考虑重大软件失效，并作为设计评审过程的一部分而正式记录。

测试需要超越多个开发活动的超前策划。生存周期的特定过程中的测试文档和它的事件如图 2 和图 3 所示。

b) 方法和规程

SVVP 应为每个任务描述方法和规程，包括在线访问、开发过程状态的观察/评价。SVVP 应定义用于评价任务结果的准则。

1) “软件生存周期”V&V 部分是 5.2 过程：管理；5.3 过程：获取；5.4 过程：供应；5.5 过程：开发；5.6 过程：运行；和 5.7 过程：维护。

表 1　在生存周期中可选 V&V 任务和建议的应用

生存周期过程		获取	供应	管理	概念	需求	设计	实现	测试	安装和检验	运行	维护
算法分析						X	X	X				X
审核执行						X	X	X	X	X		X
审核支持				X		X	X	X	X	X		X
控制流分析						X	X	X				X
费用分析		X	X	X	X	X	X	X	X	X		X
数据库分析						X	X	X	X			X
数据流分析						X	X	X				X
灾难复原计划评估				X	X	X	X	X			X	X
分布式体系评估					X	X	X					X
可行性研究评价		X	X	X	X	X	X					X
独立风险评估		X	X	X	X	X	X	X	X	X	X	X
审查	概念					X	X	X	X	X		X
	设计						X					X
	需求					X						X
	源代码							X				X
	测试用例						X	X	X	X		X
	测试设计						X	X		X		X
	测试计划					X	X	X		X		X
运行评价											X	
性能监控					X	X	X	X	X	X	X	X
安装后确认										X	X	X
项目管理监督支持		X	X	X	X	X	X	X	X	X	X	X
合格性测试									X	X		X
回归分析和测试						X	X	X	X	X		X
重用性评估		X	X	X	X	X	X					X
安全保密性评估		X		X	X	X	X	X	X	X		X
模拟分析					X	X	X	X	X	X	X	X
规模和时间分析						X	X	X	X			X
系统软件评估								X	X	X	X	X
测试认证									X	X	X	X
测试评价						X	X	X	X	X	X	X
测试见证									X	X	X	X
培训文档评价						X	X	X	X	X	X	X
用户文档评价				X	X	X	X	X	X	X	X	X
用户培训				X					X	X	X	X
V&V 工具计划生成		X	X	X								X

表 1(续)

生存周期过程		获取	供应	管理	概念	需求	设计	实现	测试	安装和检验	运行	维护
走查	设计						X					X
	需求					X						X
	源代码							X				X
	测试								X	X		X

注：表中的“X”表示在该列所对应的生存周期过程的活动中可以选择执行该行所对应的 V&V 任务。

c) 输入

SVVP 应标识每个 V&V 任务要求的输入。SVVP 应规定每个输入的出处和格式。最低限度 V&V 任务要求的输入在表 4 至表 14 中标识。其他输入也可使用。对于任一 V&V 活动和任务，所有要求的来自于先前活动和任务的输入可简要使用，只有基本输入列在表 4 至表 14 中。

d) 输出

SVVP 应标识每个 V&V 任务要求的输出。SVVP 应规定每个输出的目的、格式和接收方。每个 V&V 任务要求的输出在表 4 至表 14 中标识。其他输出也可产生。

V&V 管理和 V&V 任务的输出应成为随后适当时的过程和活动的输入。

e) 进度

SVVP 应描述 V&V 任务的进度。SVVP 应为启动和完成每个任务、每个输入的接收和准则、每个输出的交付建立特定的里程碑。

f) 资源

SVVP 应标识 V&V 任务性能的资源。SVVP 应规定资源分类(例如，人员配备、装备、设施、行程和培训)。

g) 风险与假设

SVVP 应标识与 V&V 任务相关的风险(例如，进度、资源或技术步骤)和假设。SVVP 应提供消除、减少和缓解风险的建议。

h) 目标与职责

SVVP 应标识组织结构要素或执行 V&V 任务的单个职责。

6 V&V 报告要求

本章应描述如何记录执行计划的结果。V&V 报告应贯穿整个软件生存周期。本章应规定所有 V&V 报告的内容、格式和时机。这些 V&V 报告将构成最终的软件验证和确认报告(SVVP)。

V&V 报告通常应包括任务报告、V&V 活动摘要报告、异常报告和 V&V 最终报告。任务报告、V&V 活动摘要报告和异常报告的提供是作为对涉及每个软件产品和过程的技术质量的软件开发过程的反馈。

V&V 报告也可包括可选报告诸如特殊研究报告。

要求的 V&V 报告应包括下列内容：

a) 任务报告

V&V 任务报告应记录 V&V 任务结果和状态，并以合适的格式做技术披露。任务报告实例包括下列内容：

1) 异常评价；
2) 基线更改评估；
3) 概念文档评价；
4) 配置管理评估；

5) 合同验证；
6) 关键性分析；
7) 新约束条件评价；
8) 硬件/软件/用户需求分配分析；
9) 危险分析；
10) 安装检验；
11) 安装配置审核；
12) 接口分析；
13) 迁移评估；
14) 操作规程评价；
15) 评估建议的更改；
16) 建议；
17) 评审结果；
18) 风险分析；
19) 软件设计评价；
20) 软件完整性级别；
21) 软件需求评价；
22) 源代码和源代码文档评价；
23) 系统需求评审；
24) 测试结果；
25) 可追踪性分析。

b) V&V 活动摘要报告

活动摘要报告应概括 V&V 任务的结果，该 V&V 任务是为下列每个 V&V 活动而执行：获取支持、策划、概念、需求、设计、实现、测试、及安装与检验。根据在特定的阶段内执行的 V&V 活动的广度和深度，阶段摘要报告可以是一份详尽的正式的文档，或是一份简短的非正式通知。对于运行活动和维护活动，V&V 活动摘要报告可以是对以前的 V&V 活动摘要报告的更新，或者是单独的文档。每个 V&V 活动摘要报告应包含下列内容：

1) 已执行 V&V 任务描述；
2) 任务结果摘要；
3) 异常和解决方案摘要；
4) 软件质量评估；
5) 技术和管理风险的标识与评估；
6) 建议。

c) 异常报告

异常报告应记录每个由V&V工作检测到的异常。应评价每个异常对软件系统的影响，并评估其是否为关键异常(例如，IEEE Std 1044－1993)。应修改V&V活动和任务的适用范围与应用领域，以指出引起这些异常和风险的原因。每个异常报告应包含下列内容：

1) 描述和在文档或代码中的位置；
2) 影响；
3) 异常原因和错误脚本描述；
4) 异常关键性层次；
5) 建议。

d) V&V 最终报告

V&V 最终报告汇总并合并软件异常、V&V 任务以及所有 V&V 阶段报告的结果。V&V 最终报告根据 V&V 工作结果准备，并且 V&V 最终报告提供全面的软件质量的评估和对产品和/或开发过程的任何建议。该报告应在安装和检验活动的末尾或获得 V&V 工作结论时发布。V&V 最终报告应包括下列内容：

1) 所有生存周期 V&V 活动摘要；
2) 任务结果摘要；
3) 异常和解决方案摘要；
4) 整体软件质量评估；
5) 课程学习/最佳实践；
6) 建议。

有些情况下可能还需要一些其他的可选报告。这些可选的报告是一些专门的 V&V 研究的结果或是一些其他的未预见的活动的结果。和所有的 V&V 报告一样，要求及时地、正确地发布可选的报告。它们应标识 V&V 活动的目的、描述使用的方法并以适当的级别报告它们的结果。可选报告可包括下列内容：

a) 特殊研究报告

这些报告应描述在软件生存周期过程中实施的任何特殊 V&V 研究。报告的标题可依主题而改变。该报告应记录技术和管理任务的结果，并包括下列内容：

1) 目的和目标；
2) 步骤；
3) 结果摘要。

b) 其他报告

这些报告应描述在 SVVP 中未定义的任务的结果。报告标题可依主题而改变。这些其他的任务报告可包括，例如，质量保证结果、终端用户测试结果、安全评估报告、或配置和数据管理状态结果。

7 V&V 管理要求

本章应描述异常解决方案和报告，任务重复策略，偏离策略，控制规程，标准、惯例与约定。对于具体的 V&V 工作，可以经常从已确定的规程、策略、标准、约定和惯例中采用或裁剪必要的规程。

SVVP 的本部分应标识任何现存的将作为本 V&V 计划的一部分而实现的管理规程和任何将作为 V&V 工作的一部分而编制并实现的规程。现存的规程也应在 SVVP 的第 2 章中作为引用而标识。

本章应为每个将被使用的规程标识生存周期过程和 V&V 任务。应表明每个规程的实现的程度。本章也应指明负责每个规程的实施、评价和维护的人员或组织的要素，并规定将如何监控和保证依从性。

为了表示不同的负责组织的关系，可以提供图表。为确保有效，管理规程应与 SVVP 的其他地方定义的结构和职责保持一致。

一项V&V工作由管理者和技术任务两部分组成，并且对于在项目中生成的信息至少宜标识三类读者——执行V&V任务的人员、执行开发任务的人员和管理者。为了保证满足每类读者的不同的信息需求，管理规程可以包括一个或多个分发表。如果预先确定了开发文档集、正式的V&V文档集、备忘录、会议记录、状态报告等的适当的分发，则可能会促进信息流，避免许多误解。

7.1 异常解决方案和报告

SVVP 应描述报告和解决异常的方法，包括报告异常的准则、异常报告分布列表、解决异常

的权限与时间线。该部分应定义异常关键性级别，在 V&V 工作正式进入下一个生存周期阶段前，应圆满地解决每个关键异常。软件异常的分类可参见 IEEE Std 1044－1993。

基于以前已验证的软件产品或引用文档，标准定义了所有在文档集中或软件运行中观察到的偏离期望的异常。

SVVP 将为异常报告和解决方案描述清晰和明确的规程，所以每个参与者都能确定它们在过程中的作用。在开发过程中尽可能早地报告并解决异常具有显而易见的好处。应提供记录异常及其解决方案的具体方法，包括异常报告形式的使用。

除了追踪异常报告和解决方案以外，异常报告过程可以是软件验证和确认工作中数据采集的基本方法。异常的数量和关键性级别可以确定工作能否正式地进入下一个生存周期阶段。象根本原因分析这样的过程监控活动的数据也依赖于来自异常报告过程中的数据。

7.1.1 报告的方法和准则

SVVP 宜包括报告异常的准则。应清楚地定义在何种情况下正式报告异常。应避免被不必要的通知中断开发过程。异常报告过程从非正式的变化到正式的、从人工的变化到全自动的报告和追踪。项目规模和关键性问题决定系统的复杂性。

V&V 策划应涉及异常报告过程中非正式意见的作用。问题可以包括是否一直承认非正式意见。如果承认非正式意见，则应论述：

a) 非正式意见将采用的形式(例如：备忘录、打电话)；

b) 何时使用非正式意见(例如：用于早期的通知单、和异常报告一起去遵循)；

c) 不要求非正式意见的问题分类(例如：次要的或当前范围之外)是充分的并且是正式通知。

但是，非正式意见经常是有用的，应注意确保所有重要问题得到正式记录并引起适当人员的注意。应记录并报告所有的异常。

V&V 策划应详细说明：

a) 谁负责记录异常并分析其影响、关键性等；

b) 谁有责任和权利批准异常报告的发布。

有些情况下，V&V 活动与软件质量保证活动一道执行，例如：V&V 人员提供审核支持，出席评审会议、监控测试。在这些情况下，SVVP 应详细说明 V&V 异常报告是否要由其他组复制问题报告。例如：如果 V&V 人员监控测试并发现测试组织的测试事件报告是满足要求的，则有可能不需要区分供测试的 V&V 异常报告。然而，由测试者报告的不满足要求的任何事例，在这种情况下都将是 V&V 异常报告的对象。

7.1.2 异常报告分发

SVVP 宜包括一个异常报告分发表。应清楚地定义异常报告的分发计划，包括谁得到每份报告、在什么情况下得到以及得到的原因的详细说明。

应在需要信息、追踪及行动的地方分发报告。如果报告按照优先权原则分发，则应定义优先级别并确定分发准则。

分发表将依赖于 V&V 工作的组织和独立性程度。例如：如果执行 V&V 任务的人员是独立于开发组的，则异常报告既应分发给开发组，也应分发给用户(或开发组的高层管理者)。

7.1.3 异常解决方案的方法和准则

异常的解决方案可以导致文档集、软件或硬件的更改。异常的解决方法可能是复杂的、主观的和耗费资源的任务。

在 V&V 工作可以进入下一个生存周期阶段以前，应圆满地解决每项关键异常。

计划应详细说明用于确定异常的关键性、异常的影响和解决异常报告的发出者和负责解决异常的人员间的差异的规程。

关于异常报告的职责和权利应在 SVVP 中规定。这些职责和权利应包括：

a) 对异常报告做出响应的职责；

b) 评价响应和解决异常的权利；

c) 追踪异常报告状态(未决的与已解决的)职责。

为使其有效，在这方面的职责和权利的规格说明书应与在 SVVP 的其他地方规定的组织和职责一致。

7.1.4 时机

V&V 策划应论述报告异常及其解决方案的时机因素。异常报告应迅速地发送。在某些情况下，可以提供每日报告或更频繁的报告。应权衡 V&V 结果的及早通知，防备开发过程可能的中断。

需要有效的规程以保证异常报告是有效的、必要的和及时的。SVVP 可以要求按照一些预定的分类方案把异常分组并使异常适合于分发，以便更容易地了解异常间的关系。如果是这样的话，应规定最大的可允许的控制时间。对于不同的分类，最大的可允许的控制时间可能也不同。

SVVP 应包括解决异常的时限。

7.2 任务重复策略

当 V&V 任务输入被更改或任务规程被更改时，SVVP 应描述用于确定 V&V 任务重复程度的准则。这些准则可包括更改评估、软件完整性级别，和对预算、进度与质量的影响。

输入到 V&V 工作的软件产品是经常被更改的，例如：异常纠正的结果、性能增强、需求更改等。当产生更改时，通过重复以前的任务或启动新的任务来迭代 V&V 任务。为了确保正确地实现已计划的更改、所有的文档集都是完成的和最新的并且软件性能中没有出现不可接受的更改，V&V 任务迭代是必须的。

管理规程应包括评价更改时用于适当地分配 V&V 资源的准则。如果没有这样的规程，资源可能在一个或多个域中过分扩展，有损于作为整体的项目。

当 V&V 任务的输入更改时，用于确定将被重复的 V&V 任务的程度的准则可以包括更改、关键性、成本、进度或质量影响的评估。历史数据会有助于该策划。

在选择准则时要考虑的问题可以包括：

a) 在响应更改时，开发文档集的什么部分将被重新评价？例如：软件需求规格说明书的修订本要求评审整个文档吗？还是仅仅评审由开发人员标识的、为响应异常报告而修订的那些部分？

b) 当更改软件时，何种程度的回归测试将是必需的？(部件？集成？系统？验收？)

c) 必须要重复 V&V 任务直到解决了所有的异常吗？(对于非关键异常，这可能是不必要的或不实际的)

d) 该 V&V 工作将持续到运行和维护吗？如果不是，在何处考虑维护更改，在何处考虑更改超出了当前 V&V 范围？

7.3 偏离策略

SVVP 应描述偏离计划时用的规程和准则。偏离所需的信息应包括任务标识、基本原理、和对软件质量的影响。SVVP 应标识批准偏离的权限职责。

项目更改或外部因素使得有可能偏离 SVVP。在允许偏离存在之前，任何这样的偏离都应记录并得到批准。

宜编制标准表格，包括任务标识、偏离率、以及对软件质量的影响。也可以包括追踪信息。应标识编制和批准偏离请求的人员。对于较小、不太正式的项目，以备忘录形式记录要求的信息即可。

编制和批准偏离 SVVP 请求的权力应与编写和批准自身的 SVVP 的那些权力是相当的。当定义必要的权力层次时，应考虑软件关键性。

在 SVVR 中报告执行 SVVP 中的偏离。已批准的偏离可以在 V&V 最终报告中通过包括表格

或备忘录的副本，或通过列出对引用独自可用的表格或备忘录来记录。适用于给定的任务或阶段的偏离也应在相应的 V&V 任务报告或阶段摘要报告中记录。

依据 SVVP 的可追溯的修订版清除过去的偏离是不适当的。然而，有些偏离影响了今后计划的 V&V 任务。如果预计偏离将再次出现，或偏离对剩余活动有重要的影响，可以考虑修订 SVVP。

7.4 控制规程

SVVP 应标识应用于 V&V 工作的控制规程。这些规程应描述如何配置、保护和存贮软件产品和 V&V 结果。

这些规程可描述质量保证、配置管理、数据管理、或其他活动，如果它们不由其他工作涉及。SVVP 应描述 V&V 工作应如何遵从现存的安全条目，如何保护 V&V 结果的有效性免遭未经授权的改造。

明确定义的规程对软件产品(V&V 评价的输入)的有效控制和软件 V&V 工作的结果(V&V 输出)是必要的。这些规程，特别是那些用于软件质量保证和配置及数据管理的规程，与用于软件开发的那些规程是相似的。在许多情况下，可以在这里使用相同的规程。如果是这样，那些规程可以通过引用来合并。应连同所有必要的修改一起标识那些规程将被实施的程度。已计划的或制定中的新的规程也应标识。

规程的集合应描述软件产品和软件 V&V 结果应怎样来配置、保护和贮存。它们至少应描述 SVVP 材料如何遵循现有的安全措施，以及如何保护 V&V 结果的有效性免遭偶然或故意的损害。

本标准把配置管理列为一项可选的 V&V 任务。理论上，已经实现了用于开发的有效的软件配置管理规程。如果未实现，建议软件配置管理规程作为 V&V 的一部分而实现。如果要保护 V&V 结果的有效性，那么 V&V 产品的配置管理也是重要的。

为了确保结果有效，控制规程应包括标识软件项(包括文档集)、控制和实现更改、记录和报告更改实现状态的方法。如果 V&V 结果要与被评价的产品正确地结合，并且 V&V 任务是已执行的，则这些配置管理的过程是必须的。评审和审核有助于确保这些过程的有效性。代码和媒体控制也是必需的，可以作为配置管理的一部分。最后，应论述记录的收集、维护和保管。

控制的第一步是标识要控制的项。不同的 V&V 输入和输出应与每项(例如：名称、版本/修订本、日期)的唯一标识条款一起列出。

要控制的项包括：

a) 计算机文件和文档；

b) 应用软件、操作系统软件、库、测试驱动程序、测试数据等；

c) 在获得 V&V 结果时作为资源使用的任何自动化工具，必要时可使得那些结果再现。

V&V 输入和输出的标识包括形式(例如：纸、软盘)和格式(例如：GB/T 1988 纯文本)。应考虑状态(例如：草案或正式文本)。应定义 V&V 输入文档的发布和 V&V 结果的发布准则。

规程应规定控制和实现对计算机文件和文档集的更改的方法。需要有效的更改控制以避免在移动目标上尝试 V&V。

需要考虑的事项包括：

a) 更改评审权和职责；

b) 更改建议的编制、优先安排和批准；

c) 实现已批准的更改建议的方法；、

d) 软件库控制规程，例如：访问控制、读/写保护、更改历史、档案。

为了记录和报告更改实现状态，需要状态说明规程。应了解每一项的当前状态信息，并定期发布报告。可以收集的信息的例子是：

a) 每个计算机文件或文档的最新版本/修订本；

b) 与每项有关的更改建议的状态(例如：未决的对已讨论的对已批准的)；

c) 每项的异常报告的状态(例如：未决定的对已解决的)；

d) 每项已完成的 V&V 任务；

e) 每项的评审/审核历史；

f) 适用于最新 SVVP 版本/修订本的批准偏离。

为了监控控制规程的有效性，应考虑评审和审核。应定义在这些评审和审核中的组织的作用。应规定在生存周期中将出现评审和审核的节点，以及将包含在每个节点中的项。应说明标识和解决问题的方法。

代码控制可以被解释为保护或确保已完成的代码的有效性的必要的方法和手段。代码控制可以作为配置管理过程的一部分执行。以上描述的过程可以用于覆盖许多代码控制要素，例如控制代码的规格说明书、代码标识、软件库的使用以及代码更改控制。为了遵循现有的安全规定，也需要规程去描述控制下的软件的物理位置、获取副本的要求、位置、维护和备份副本的使用。

媒体控制与贮存计算机文件的物理媒体的保护有关，包括存储和恢复(包括远距离存储)、访问限制以及避免物理降级的环境控制。在代码控制中，应涉及现有的安全规定。

对于记录收集、维护和保留的规定应包括要保存的记录的标识、它们将被维护的方式的规格说明书(例如：硬拷贝、微缩胶片)，以及对于所涉及的记录的每种类型的保留时间长短的规格说明书。在这方面的组织职责包括发起、收集、维护、分类和保护记录。也应考虑访问、更改、清除或销毁记录的权力。

7.5 标准、惯例和约定

SVVP 应标识管理 V&V 任务执行的标准、惯例和约定，包括内部结构标准、惯例和策略。本条应标识管理 V&V 任务的实际执行的标准、惯例和约定。

下面是一般的可应用的标准、惯例和约定的例子：

a) 评价软件将要依据的软件需求、设计、实现、测试和文档集的标准；

b) V&V 任务的详细的规程；

c) 软件评价中使用的详细清单；

d) 评审和审核标准；

e) V&V 程序的质量保证需求；

f) 合同要求的所有标准、惯例和约定。

根据项目环境，可以要求如下特定的标准、惯例和约定：

a) 国家标准；

b) 国家军用标准；

c) 行业标准；

d) 企业标准；

e) 政策法规。

8 V&V 文档要求

SVVP 应定义测试文档的目的、格式和内容。这些测试文档的格式描述可在 GJB 438A－1997 中找到。如果 V&V 工作使用不同于本标准中的测试文档或测试类型(例如，部件、集成、系统、验收)，软件 V&V 工作应展示一个由建议测试文档和执行到本标准定义的测试项目的映射。应在测试计划、测试设计、测试用例、测试规程文档中实施表 4 至表 14 定义的测试计划任务。

SVVP 应描述下列 V&V 测试文档的目的、格式和内容：

a) 测试计划；

b) 测试设计说明；

c) 测试用例说明；

d) 测试规程说明；

e） 测试报告。

所有 V&V 结果和发现都应记录在 V&V 最终报告中。

附 录 B
（资料性附录）
从 GB/T 8566－2001 中 V&V 要求到本标准 V&V 活动和任务的映射

表 B.1 显示了从所有 GB/T 8566－2001 中 V&V 要求（即，过程、活动和任务）到本标准的 V&V 活动和任务的映射。

表 B.1 的第 1 列列出了 GB/T 8566－2001 的 V&V 过程和活动的章条号和标题。表 B.1 的第 2 列列出了本标准的章、条、表和附录，它们指出了第 1 列的主题。在没有指定条标题的地方，创建章标题以反映章内容。这些导出的条标题被标以 "[a]"。

表 B.1 映射

GB/T 8566－2001 V&V 要求	本标准 V&V 活动和任务	
	位置	描述
5.1.4.1 供方监督 V&V	5.3.2 表 5，任务 a)、b)和 c)	活动：获取支持 V&V 获取支持 V&V 任务
5.2.4.5 h) 和 5.2.5.5 V&V 连接[a]	5.3.2 表 5，任务 b) 5.4.2 表 6，任务 a) 附录 C	活动：获取支持 V&V 策划 V&V 工作和供方间的接口 活动：策划 V&V 策划 V&V 工作和供方间的接口 IV&V 定义
5.2.6.3 验证和确认[a]	所有的条、表、图和附录	软件 V&V
5.3.2 系统需求分析	5.3.2 表 5，任务 c) 5.5.2 表 7，任务 a)和 d)	活动：获取支持 V&V 系统需求评审 活动：概念 V&V 概念 V&V 任务（概念文档评价、可追踪性分析）
5.5.5 和 5.5.6 迁移和软件退役	5.7.2 表 14，任务 b)	活动：维护 V&V 评估建议的更改
6.4.1 验证过程实现[a]	第 4 章 第 6 和 7 章及附录 A 6.2 和附录 A 第 7 章	V&V 软件完整性级别 软件 V&V 报告、管理和文档要求；SVVP 概述 V&V 管理要求
6.4.1.1 待验证软件的关键性[a]	第 4 章 表 1 表 2 附录 D	V&V 软件完整性级别 软件完整性级别指定 后果定义 可重用软件的 V&V
6.4.1.2 验证过程[a]	第 6 和 7 章及附录 A	软件 V&V 报告、管理和文档要求，SVVP 概述
6.4.1.3 和 6.4.1.4 验证范围和严密性[a]	表 15 附录 C	为每个软件完整性级别指定的最低限度 V&V 任务 IV&V 定义
6.4.1.5 验证计划[a]	第 6 和 7 章及附录 A	软件 V&V 报告、管理和文档需求，SVVP 概述
6.4.1.6 问题和不合格报告[a]	6.2 和附录 A 第 7 章	V&V 管理需求
6.4.2 验证	第 5 章	V&V 过程
6.4.2.1 合同验证	5.4.2 表 6，任务 b)	活动：策划 V&V 合同验证

表 B.1(续)

GB/T 8566—2001 V&V 要求	本标准 V&V 活动和任务	
	位置	描述
6.4.2.2 过程验证	5.3 5.4 5.5	过程：获取 过程：供应 过程：开发
6.4.2.3 需求验证	5.3.2 表 5，任务 c) 5.5.2 表 7，任务 a) 5.5.3 表 8，任务 a)～i)	活动：获取支持 V&V 系统需求评审 活动：概念 V&V 概念文档评价 活动：需求 V&V 需求 V&V 任务
6.4.2.4 设计验证	5.5.4 表 9，任务 a)～i)	活动：设计 V&V 设计 V&V 任务
6.4.2.5 代码验证	5.5.5 表 10，任务 a)～i)	活动：实现 V&V 实现 V&V 任务
6.4.2.6 集成验证	5.5.6 表 11，任务 c)	活动：测试 V&V 测试 V&V 任务
6.4.2.7 文档验证	5.3.2 表 5，任务 c) 5.4.2 表 6，任务 b) 5.5.2 表 7，任务 a) 5.5.3 表 8，任务 b)和 c) 5.5.4 表 9，任务 b)和 c) 5.5.5 表 10，任务 b)和 c) 5.5.7 表 12，任务 a) 5.6.2 表 13，任务 c)	活动：获取支持 V&V 系统需求评审 活动：策划 V&V 合同验证 活动：概念 V&V 概念文档评价 活动：需求 V&V 软件需求评价和接口分析 活动：设计 V&V 软件设计评价和接口分析 活动：实现 V&V 源代码和源代码文档评价和接口分析 活动：安装和检验 V&V 安装配置审核 活动：运行 V&V 操作规程评价
6.5.1 确认过程实现[a]	第 4 章 第 6 和 7 章及附录 A 6.2 和附录 A 第 7 章 附录 C、D 和 E	V&V 软件完整性级别 软件 V&V 报告、管理和文档需求，SVVP 概述 V&V 管理要求 IV&V 的定义，可重用软件 V&V，V&V 度量
6.5.1.1 待确认软件的关键性[a]	第 4 章 表 1 表 2 附录 D	V&V 软件完整性级别 软件完整性级别指定 后果定义 可重用软件的 V&V
6.5.1.2 确认过程[a]	第 6 和 7 章及附录 A	软件 V&V 报告、管理和文档需求，SVVP 概述
6.5.1.3 确认范围和严密性[a]	表 15 附录 C	为每个软件完整性级别指定的最低限度 V&V 任务 IV&V 的定义

表 B. 1(续)

GB/T 8566－2001 V&V 要求	本标准 V&V 活动和任务	
	位置	描述
6.5.1.4 确认计划[a]	第 6 和 7 章及附录 A	软件 V&V 报告、管理和文档需求，SVVP 概述
6.5.1.5 问题和不合格报告[a]	6.2 和附录 A 第 7 章	V&V 管理要求
6.5.2 确认	第 5 章	V&V 过程
6.5.2.1 确认测试准备[a]	5.5.3 表 8，任务 e)和 f) 5.5.4	活动：需求 V&V 系统 V&V 测试计划生成和验证，验收 V&V 测试计划生成和验证 活动：设计 V&V
6.5.2.1 确认测试准备[a]	表 9，任务 e)、f)和 g) 5.5.5 表 10，任务 e)和 f) 5.5.6 表 11，任务 b)	部件 V&V 测试计划生成和验证，集成 V&V 测试计划生成和验证，和 V&V 测试设计生成和验证 活动：实现 V&V V&V 测试用例生成和验证，和 V&V 测试规程生成和验证 活动：测试 V&V 验收 V&V 测试规程生成和验证
6.5.2.2 确认测试可追踪性[a]	5.5.5 表 10，任务 g) 5.5.6 表 11，任务 c)、d)和 e)	活动：实现 V&V 部件 V&V 测试执行和验证 活动：测试 V&V 测试 V&V 任务
6.5.2.3 进行确认测试[a]	5.5.5 表 10，任务 g) 5.5.6 表 11，任务 c)、d)和 e)	活动：实现 V&V 部件 V&V 测试执行和验证 活动：测试 V&V 测试 V&V 任务
6.5.2.4 确认软件预期用途[a]	5.5.2 表 7，任务 a) 5.5.3 表 8，任务 b)和 c) 5.5.4 表 9，任务 b)和 c) 5.5.5 表 10，任务 b)和 c) 5.5.6 表 11，任务 d)和 e)	活动：概念 V&V 概念文档评价 活动：需求 V&V 软件需求评价和接口分析 活动：设计 V&V 软件设计评价和接口分析 活动：实现 V&V 源代码和源代码文档评价，和接口分析 活动：测试 V&V 系统 V&V 测试执行和验证，和验收 V&V 测试执行和验证
6.5.2.5 软件安装测试[a]	5.5.7 表 12，任务 a)～d)	活动：安装和检验 V&V 安装和检验 V&V 任务

本标准定义了 11 个 V&V 活动，如表 B.2 第 1 列所示，它们是 V&V 过程的一部分。11 个 V&V 活

动中的每个活动都支持在表 B.2 第 2 和第 3 列所示的 GB/T 8566－2001 软件生存周期过程和活动。

表 B.2　从本标准 V&V 活动到 GB/T 8566－2001 软件生存周期过程和活动的映射

V&V 活动	GB/T 8566－2001 软件生存周期	
	过程	活动
获取支持 V&V	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
策划 V&V	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 V&V	开发	—过程实现 —系统需求分析
概念 V&V	开发	—系统体系结构设计
需求 V&V	开发	—软件需求分析
设计 V&V	开发	—软件体系结构设计 —软件详细设计
实现 V&V	开发	—软件编码和测试
测试 V&V	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 V&V	开发	—软件安装 —软件验收支持
运行 V&V	运行	—过程实现 —运行测试 —系统运行 —用户支持
维护 V&V	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
V&V 管理	所有过程	—所有活动

附 录 C
（资料性附录）
独立验证和确认(IV&V)的定义

C.1 独立性参量

IV&V 由 3 个参量定义：技术独立性、管理独立性和财务独立性。

C.1.1 技术独立性

技术独立性要求 V&V 工作使用不牵涉软件开发的人员。IV&V 工作必须明确地表达自己对该问题以及所建议的系统如何解决该问题的理解。技术独立性(“不同观点”)是发觉那些容易被离解决方案太近的人忽略的微小错误的重要方法。

对于软件工具而言，技术独立性意味着 IV&V 工作使用或开发自有的一系列与开发方的工具分开的测试和分析工具。允许在计算机支持环境(例如，编译器、汇编程序、应用程序)或系统仿真方面实行工具共享，因为各自使用独立的版本花费昂贵。对于共享工具，IV&V 对工具进行合格性测试以确保公用工具不包含错误，该错误可能掩盖处于分析和测试中的软件的错误。

C.1.2 管理独立性

这要求将 IV&V 工作的职责授予与开发和程序管理组织分开的组织。管理独立性还意味着 IV&V 工作独立地选择部分软件和系统进行分析和测试，选择 IV&V 技术，确定 IV&V 活动的进度，并选择要对其采取措施的特定技术议题和问题。IV&V 及时地并且同时向开发组织和程序管理组织提供调查结果。必须允许 IV&V 工作不受开发组织任何直接或间接的限制(例如，不要求先得到开发组织的批准)或负面压力地将 IV&V 结果、异常和调查结果提交给程序管理组织。

C.1.3 财务独立性

这要求将 IV&V 预算控制授予独立于开发组织的一个组织。这种独立性可防止 IV&V 工作因为资金已转移或已被施加负面财务压力或影响，而不能完成其分析、测试或及时交付结果的情形。

C.2 独立性形式

在 V&V 组织内所授予的这 3 个独立性参量(技术的、管理的和财务的)的程度决定了所能达到的独立性程度。

可对 V&V 组织采用多种独立性形式。最流行的四种是 1)传统式；2)改进式；3)内部式；4)嵌入式。表 C.1 阐明了这 4 种形式所达到的独立程度。

表 C.1 IV&V 的形式

IV&V 的形式	技术的	管理的	财务的
传统式	I	I	I
改进式	I	“I”	I
内部式	“I”	“I”	“I”
嵌入式	i	i	i
注：I=严格独立性；“I”=有条件的独立性；i=最小维护。			

C.2.1 传统式 IV&V

传统式 IV&V 包含所有三个独立性参量。IV&V 职责授予与开发组织分开的一个组织。IV&V 与开发组织保持密切工作关系，以确保 IV&V 调查结果和建议尽快综合到开发过程中。通常，传统式 IV&V 由一个组织执行(例如，供方)，而开发工作由一个分开的组织执行(即，另一卖方)。通过施加于系统开发的规章和标准，软件完整性第 4 级(即，丧失生命、任务损失、重大社会或财务损失)通常要求进行传

统式 IV&V。

C.2.2 改进式 IV&V

改进式 IV&V 用于许多大型程序，在这些大型程序中选择系统集成主管来管理整个系统开发包括 IV&V。集成主管选择组织来帮助系统开发并执行 IV&V。在改进式 IV&V 形式中，需方通过将此职责转给集成主管来减少自己的获取时间。由于集成主管执行全部或一些开发工作，管理独立性便因将 IV&V 工作报告交给集成主管而被迫折衷。由于 IV&V 工作明确表述了对系统解决方案的无偏见观点并使用了独立工作人员执行 IV&V，技术独立性得以保持。由于为 IV&V 工作留出了单独预算，财务独立性得以保持。改进式 IV&V 工作适合于具有软件完整性第 3 级(即，重要的任务和目的)的系统。

C.2.3 内部 IV&V

开发方用它本组织之内的人员实施的 IV&V 就是内部 IV&V，尽管这些人员不一定直接牵涉开发工作。技术的、管理的和财务独立性要进行折衷。技术独立性要进行折衷，是因为使用掩盖了开发方错误的同一假设或开发环境，IV&V 分析和测试易于忽略错误。管理独立性要进行折衷，是因为内部 IV&V 工作使用与开发组一样的公共工具和共同分析规程。来自开发组的同行的压力可能对 IV&V 工作如何积极地分析和测试软件产生负面影响。财务独立性要进行折衷，是因为开发组控制 IV&V 预算。由于开发压力和需求改投 IV&V 资金以解决开发问题，IV&V 资金、资源和进度可能减少。内部 IV&V 工作的益处是可以使用了解该系统及其软件的人员。当独立性程度没有明确表述，并且先前人员的知识带来的益处胜过客观性带来的益处时，就使用这种 IV&V 形式。

C.2.4 嵌入式 IV&V

这种形式在使用开发组织的人员(他们最好不直接涉及开发工作)方面与内部 IV&V 相似。嵌入式 V&V 致力于确保对开发规程和过程的依从性。嵌入式 V&V 组织与开发组织并肩工作，并与开发人员参加相同的审查、走查和评审工作(即，技术独立性的折衷)。不特地要求嵌入式 V&V 独立评估原始解决方案或进行独立测试(即，管理独立性的折衷)。财务独立性要进行折衷，因为 IV&V 人力资源分配由开发组控制。嵌入式 V&V 使 V&V 结果能快速地反馈给开发过程，但折衷了 V&V 组织的技术、管理和财务独立性。

附 录 D
（资料性附录）
可重用软件的 V&V

本附录提供了实施可重用软件 V&V 的指南。可重用软件（部分的或整体的）包括来自软件库的软件、为其他应用开发的定制软件、传统软件或商业现货（COTS）软件。

表 4 至表 14 的 V&V 任务被应用于可重用软件，就如同它们应用于新开发的软件。然而，这些任务的输入对于可重用软件可能得不到，从而降低软件产品和过程的可见性。例如，源代码可能不能用于评价，文档可能不完备，或者开发过程可能未知。可重用软件 V&V 的输入应从任何可用来源获得。这种输入的一些来源的实例如下：

a） 审核结果；
b） 黑盒测试结果；
c） 设计过程文档；
d） 工程评判；
e） 运行历史；
f） 原始开发方会谈；
g） 先前的危险分析结果；
h） 先前的 V&V 结果；
i） 产品文档；
j） 原型制作结果；
k） 逆向工程结果；
l） 软件开发方笔记；
m） 软件完整性级别；
n） 所依从的标准；
o） 静态代码分析结果；
p） 测试历史；
q） 试验集成结果；
r） 用户会谈。

如果不能在合适的级别执行可重用软件 V&V，那么只要与此用途相关的风险已识别出来并已在风险缓解策略中有所说明，可重用软件仍可以使用。如果显示等价的可选择的 V&V 任务能满足表 4 至表 14 的相同准则，那么允许将表 4 至表 14 的 V&V 任务进行替换。

附 录 E
（资料性附录）
V&V 度量

E.1 综述

V&V 度量应考虑指定给软件和系统的软件完整性级别、应用领域、项目要求和当前行业实际。

本标准考虑两类度量：1）用于评价软件开发过程和产品的度量；2）用于评价 V&V 任务结果和改进 V&V 任务质量与覆盖面的度量。应设立度量值，作为是否令人满意地完成过程、产品或 V&V 任务的指标。

E.2 用于评价软件开发过程和产品的度量

应将度量的使用看作一种评价软件开发过程和产品的 V&V 方法。通过计算一段时间内的评价度量，可以标识问题趋势。没有适用于所有的项目的系列标准度量，所以度量用法可依应用领域和软件开发环境而不同。

IEEE Std 1061－1992 提供了可用的软件质量度量的标准定义。其他与度量相关的标准，诸如 IEEE Std 982.1－1988 和其相应指南 IEEE Std 982.2－1998 也可使用。以下所列是一些有用的度量，但下列度量并不完备：

a) 信息(例如，概念、需求、设计)的完备性；
b) 软件规模；
c) 需求可追踪性；
d) 更改(例如，需求、设计、代码)的数量；
e) 逻辑和数据复杂性；
f) 分析或测试覆盖率(覆盖率类型基于项目和应用需求，可包括需求、代码、功能、模块和测试用例等方面的)；
g) 控制和数据耦合；
h) 真实状态对比计划进展；
i) 在一段时间内发现的缺陷数量；
j) 检测到缺陷时的开发过程的时期；
k) 缺陷类别；
l) 缺陷严重性；
m) 具有同一原因(诸如过程缺陷或工具错误)的系统或重复错误；
n) 修复一个缺陷的时间(对进度的影响)。

E.3 用于评价 V&V 任务和改进 V&V 任务质量与覆盖面的度量

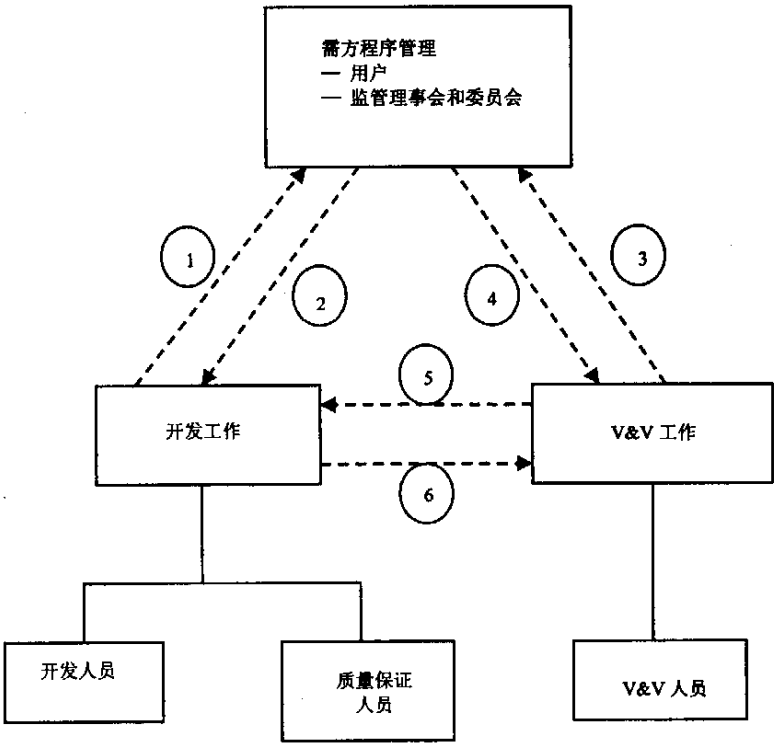
关于 V&V 度量不存在一致意见。要考虑的候选度量分为两类：

a) V&V 质量——测量 V&V 任务的质量和有效性(例如，V&V 标识的缺陷数量与遗漏的缺陷数量的比率)；
b) V&V 覆盖面——测量 V&V 应用的广度和宽度(例如，已验证和确认的软件模块数量与模块总数量的比率)。

V&V 活动管理使用这些度量结果来改变用于 V&V 任务的 V&V 项目资源，从而表明了过程帮助的要求。这些以及类似的 V&V 度量能用于评估 V&V 任务的质量和覆盖面。能用它们对 V&V 过程的持续改进提供反馈。

附 录 F
（资料性附录）
V&V 与项目中其他组织关系的示例

图 F.1 是在软件生存周期过程中实施 V&V 时各组织间的关系。



注：图中的编号行代表如下相应的控制流和数据流：

① 程序文档(例如，概念、需求、设计、用户手册)、源代码、程序状态、程序预算、开发计划和进度的提交。

② 对①中所列开发问题和可交付项的批准、否决和建议。

③ SVVP、V&V 任务结果、异常报告、活动摘要报告和其他特殊报告的提交。

④ 对③中所列 V&V 问题和可交付项的批准、否决和建议。

⑤ 按照需方程序管理的指导提交 V&V 任务结果、异常报告、活动摘要报告和特殊报告。

⑥ 程序文档(例如，概念、需求、设计、用户手册、特殊报告、源代码、程序进度)的提交。

图 F.1 V&V 与其他项目职责的组织关系的图示

附 录 G
（资料性附录）
可选 V&V 任务描述

G.1 算法分析

验证算法、方程、数学公式或表达式的正确实现。根据基本规则和理论重新推导任何重要算法和方程。对比已建立的基准或已证实的过去的历史数据。确认有关系统和软件需求的算法、方程、数学公式或表达式。确保算法和方程适合于问题的解决方案。确认由算法和方程施加的任何约束条件或限制条件的正确性，诸如舍去、截位、表达式化简、最佳拟合估计、非线性解。

G.2 审核执行

对软件过程及其产品是否符合适宜的规章、标准、计划、规程、规格说明和指南提供独立评估。审核可在任何开发阶段应用于任何软件过程或产品。审核可由供方、需方、开发方或其他相关各方诸如管理代理机构启动。审核的发起人选定审核队伍并确定要求的独立程度。审核的发起人和审核队伍的领导决定审核的目的、范围、计划和报告要求。

审核方收集足够的证据来决定软件过程和产品是否满足评价准则。他们标识主要偏离，评估质量、进度、费用方面的风险，并报告他们的调查结果。能审核的过程实例包括配置管理实践、软件工具用法、不同软件工程科目尤其是在开发体系结构、保密问题、培训、项目管理等方面的集成度。

G.3 审核支持

向审核方提供其请求的技术专家的意见。他们可在审核议程等方面代表需方，并在由审核标识的补救活动的 V&V 中提供援助。

G.4 控制流分析

通过图示逻辑控制来评估软件的正确性。检查逻辑流以便标识丢失的、不完整的、或不准确的需求。确认功能中的控制流是否代表了对问题的正确解决。

G.5 费用分析

评价开发过程的费用状态。将预算费用与实际费用相比较。将费用的开支与技术状态和计划进度联系起来。如果显示实际费用落后于预定进度安排并超出估计费用，就要标识程序风险。

G.6 数据库分析

作为设计评审过程一部分的数据库设计评价包括下列内容：

a) 物理限制分析。标识数据库的物理限制，诸如数据结构中的最大记录数量、最大纪录长度、最大数值、最小数值、最大数组长度，并将它们与设计值相比。

b) 索引对存储的分析。对比存储数据的容量来分析多索引用法，以确定所建议的方法是否满足数据检索性能和大小限制的要求。

c) 数据结构分析。在诸如数组、表格和日期格式等记录内，一些数据库管理系统具有特定的数据结构。评审使用这些结构对数据存储和检索要求的潜在影响。

d) 备份和灾难恢复分析。对照数据恢复和系统灾难恢复要求评审所采用的备份方法，并标识不足之处。

G.7 数据流分析

作为设计评审过程的一部分，评价数据流图。这包括下列内容：

a) 符号一致性检查。用于描绘数据流图的不同方法使用很特殊的符号来表示所执行的动作。验证每个符号都得到前后一致地使用。

b) 流平衡。将每个过程块的输出数据与输入数据和过程内的导出数据相比较，以确保当要求时数据是可用的。这个过程不需特别检查时间或序列因素。

c) 导出数据确认。检查过程内导出数据的正确性和格式。由操作人员设计的进入某一过程的数据应经过证实以确保其可用性。

d) 关键字与索引的比较。将用于在过程内从数据存储器中检索数据的数据关键字与数据库索引设计进行比较，以便证实没有使用非法关键字且唯一性特性始终如一。

G.8 灾难恢复计划评估

验证在扩展系统停机的情况下灾难恢复计划足以恢复系统的关键操作。灾难恢复计划应包括下列内容：

a) 灾难恢复团队的身份证明和一份联系清单。

b) 恢复操作规程；

c) 建立可供选择地点的规程包括声音和数据交流、邮件、和支持设备；

e) 计算机设备置换计划；

f) 建立系统备份进度；

g) 存储和检索软件、数据、文档和重要的非现场记录的规程；

h) 移动人员、数据、文档等的后勤工作。

G.9 分布式体系结构评估

评估在建议的体系结构中数据和过程分布的无线通信、费用、备份和恢复特性、停机时间、系统退化以及有关安装软件更新的规定的可行性、时间依从性、适用性。

G.10 可行性研究评价

验证可行性研究是正确的、准确的和完备的。确认所有的逻辑和物理假设(例如，物理模型、商务规则、逻辑过程)、约束条件和用户需求均得到满足。

G.11 独立风险评估

对软件项目的任一方面实施独立风险评估，并报告调查结果。主要从系统的观点来考虑这些风险评估。风险评估的实例包括选定的开发方法论或工具对项目的适合性；与建议的开发进度可选项相关的质量风险。

G.12 审查

审查软件过程以检测在每个选定开发阶段的产品缺陷，从而确保正在研发的软件的质量。依审查功能进行划分，审查过程可包括如下多个步骤：

a) 审查策划；

b) 产品综述；

c) 审查准备；

d) 检查会议；

e) 缺陷返工；

f) 检查解决方案的执行情况。

审查由同级别的开发人员组成的小组执行，包括作者，但不由作者领导。审查小组通常包括三到六

人，有些情况下包括来自测试组、质量保证或 V&V 的人员。为了发现、分类、报告和分析产品的缺陷，参加者担任特定角色。每类审查都经由其预期目的、要求的入口准则、缺陷分类、清单、出口准则、指定人员、及其准备和检查规程而明确定义。审查不讨论工程判断，不建议修正，也不教育项目人员；他们检测异常和问题，而由作者验证这些异常和问题的解决方案。

审查(概念)。验证系统体系结构和需求满足了顾客的要求。验证系统需求是完备且正确的，并且需求的遗漏、缺陷和含糊之处得到检测。

审查(设计)。验证设计能够实现并可追踪到需求，所有接口和程序逻辑是完备且正确的，并且设计的遗漏、缺陷和含糊之处得到检测。

审查(需求)。验证需求满足了顾客需要、能够实现，并且是完整的、可追踪的、可测试的和一致的，所以需求的遗漏、缺陷和含糊之处得到检测。

审查(源代码)。验证源代码实现对设计的可追踪性，所有接口和程序逻辑是完备且正确的，且源代码的遗漏、缺陷和含糊之处可检测到。

审查——测试用例(部件、集成、系统、验收)。验证准确地遵循了(部件、集成、系统、验收)测试计划，一组部件测试用例是完备的，且所有的部件测试用例是正确的。

审查——测试设计(部件、集成、系统、验收)。验证(部件、集成、系统、验收)测试设计与测试计划一致，且测试设计是正确的、完备的和易读的。

审查——测试计划(部件、集成、系统、验收)。验证(部件、集成、系统、验收)测试过程的范围、策略、资源和进度已经完全地且准确地规定，所有要测试的项目和所有需要执行的任务已经定义，确保所有执行测试的必要人员已经标识。

G.13 运行和评价

评估软件部署的准备状态和运行的准备状态。运行评价可包括检查运行测试、审核评审和异常报告的结果。该评价验证软件

a) 对该软件的批量生产来说正确的合适时机；

b) 对特定配置是有效的和正确的。

G.14 性能监控

收集处于运行状态下的软件的性能信息。确定系统和软件性能需求是否得到满足。性能监控是一个连续的过程，并可包括下列项目的评价：

a) 用以确定数据库重组或重编索引的需要的数据库事务处理率；

b) 用于负载均衡时的 CPU 性能监控；

c) 直接访问存储利用率；

d) 确保足够带宽的网络信息流通量；

e) 系统的关键输出(例如，设定频率、预期值域、规定系统报告、事件报告)。

G.15 安装后确认

当可靠性至关重要或软件有可能恶化时，对关键软件执行某种基准测试或定期测试。通过自动或手动地与已确立的基准测试结果进行比较，系统能在软件每次执行之前得到确认。当使用前的基准测试不切实际时，例如对于实时、过程控制和应急使用软件，可在预定间隔内进行定期测试以确保持续的可靠性。

G.16 项目管理监督支持

针对技术和管理方面的议题、风险和问题对项目开发状态进行评估。与需方和开发组织协调监督评估。评价项目计划、进度、开发过程和状态。收集、分析并报告关键项目度量。

G.17 合格性测试

验证所有软件需求依照合格性测试需求而得到测试，合格性测试需求可证实软件运行和维护的可行性。必要时为了验证和确认合格性测试结果的正确性、准确性和完备性而进行任何测试。将合格性测试结果与预期合格性测试结果一起编写成文档。合格性测试的策划可在需求 V&V 活动过程中开始。

G.18 回归分析和测试

当对任何先前检查过的软件产品进行更改时，确定必须重复进行 V&V 分析和测试的范围。评估更改的性质以确定潜在波动或对系统其他方面的副作用和影响。根据更改、纠错和影响评估来重新运行测试用例，以检测由软件修改产生的错误。

G.19 重用性评估

包括商业现货软件的使用、现存软件的修改、专为重用所设计的代码模块的使用。两项重要任务是 1） 标识对最初硬件或软件运行环境的依赖，2） 验证人机接口在新目标环境下正确地起作用。现有软件的重用能经济地改善软件产品的质量。

G.20 安全保密性评估

评价对系统的安全保密性控制，以确保它们保护硬件和软件部件免于未经许可的使用、修改和泄密，并验证授权用户的责任。验证这些控制适合于达到系统保密目标。一次系统保密性评估应包括物理部件（例如，计算机、控制器、网络、调制解调器、无线电频率、红外设备）和逻辑部件（例如，操作系统、实用程序、应用程序、通信协议、数据、管理运行策略和规程）。

G.21 模拟分析

使用模拟来运行软件或部分软件以测量在预定条件和事件下软件的性能。模拟可采取对照特定程序值和输入对软件进行人工走查的形式。模拟也可能是另外一个软件程序，该程序为被检查软件提供输入和模拟环境。模拟分析用于检查关键性能和响应时间需要或软件对异常情况和条件的响应。

G.22 规模和时间分析

收集和分析有关软件功能和资源利用的数据，以确定系统和软件对速度和容量的需求是否得到满足。软件功能和资源利用议题的类型包括，但不局限于下列内容：

a） CPU 负载；

b） 随机存取存储器和辅助存储器（例如，磁盘、磁带）的利用；

c） 网络速度和容量；

d） 输入和输出速度。

规模和时间分析是在软件设计期间开始，并在验收测试期间重复进行。

G.23 系统软件评估

评估系统软件（例如，操作系统、计算机辅助软件工程工具、数据库管理系统、储存库、通信软件、图形用户界面）的可行性、对性能和功能需求的影响、成熟度、承载力、对标准的遵循、开发方对系统软件和硬件的理解和经验，以及软件界面需求。

G.24 测试认证

通过验证是否使用基线化的需求、配置控制过程和可重复的测试来进行，并通过见证该测试来证明测试结果。认证可在软件配置项级或在系统级上完成。

G.25 测试评价

评价测试的需求覆盖率和测试完备性。通过评估软件的运用范围来评估覆盖率。通过确定测试过程中所用输入集合是否为软件所有可能的输入集合的合理的代表性样本，来评估测试完备性。评估测试输入是否包括边界条件输入、极少遇到的输入和非法输入。对某些软件而言，输入一组连续或同步信号到一个或多个处理器来充分地测试软件可能是必要的。

G.26 测试见证

监控在规定测试规程下所执行测试的保真度，并见证测试结果的记录。当测试失败时，测试过程可以下列方式继续：1)对失效实行某种“变通”；2)插入一个临时代码补丁；3)停止测试过程并执行软件修补。在所有情况下，评估测试延续过程的测试过程的不足之处(例如，一些软件未测试或某个补丁永久地留在软件中)、对其他测试的负面影响和配置控制的损失。应对所有受测试失败影响的软件进行回归测试。

G.27 培训文档评价

评价培训材料和规程的完备性、正确性、可读性和有效性。

G.28 用户文档评价

评价用户文档有关用户界面和任何可被用户调用的功能的需求的完备性、正确性和一致性。对用户文档可读性和有效性的评审应包括不熟悉该软件的有代表性的最终用户。在策划验收测试时使用对运行环境具有代表意义的用户文档。

G.29 用户培训

确证用户培训包括有关该系统的管理、运行、应用等方面的特殊规则和行业标准。此培训应基于由系统制造商提供的技术性用户文档和规程。负责系统使用的组织应负责提供合适的用户培训。

G.30 V&V 工具计划生成

准备一份描述支持 V&V 工作所需工具的计划。此计划包括有关每个工具的性能、要求的输入、产生的输出、需要的日期、购买或开发工具的花费等描述。该工具计划还应描述支持 V&V 工作的测试设施和集成测试与系统测试实验室。在定义每个工具要求的性能时，应考虑由选定软件完整性级别规定的 V&V 工作的范围和严格性。

G.31 走查

参与评价过程，在此过程中开发人员引导其他人进行一项产品的结构化检查。确保参与者有资格检查产品，并且不遭受不正当的影响。参见需求走查、设计走查、源代码走查和测试走查的具体描述。

走查(设计)。参与设计走查和设计的更新，以确保完备性、正确性、技术完整性和质量。

走查(需求)。参与需求规格说明走查，以确保在整个生存周期中软件需求是正确的、无歧义的、完备的、可验证的、一致的、可修改的、可追溯的、可测试的和可用的。

走查(源代码)。参与源代码走查，以确保代码是完备的、正确的、可维护的、无逻辑错误的、遵循编码标准和约定、且将有效地运行。

走查(测试)。参与测试文档走查，以确保计划测试是正确的和完备的，且测试结果将得到正确分析。

参 考 文 献

GB/T 8566－2001 信息技术 软件生存周期过程

IEEE Std 982.1－1988 IEEE Standard Dictionary of Measures to Produce Reliable Software

IEEE Std 982.2－1998 IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software

IEEE Std 1012－1998 IEEE Standard for Software Verification and Validation

IEEE Std 1028－1988 IEEE Standard for Software Reviews and Audits

IEEE Std 1044－1993 IEEE Standard Classification for Software Anomalies

IEEE Std 1059－1993 IEEE Guide for Software Verification and Validation Plans

IEEE Std 1061－1992 IEEE Standard for a Software Quality Metrics Methodology

中 华 人 民 共 和 国
国家军用标准
军用软件验证和确认
GJB 5234－2004
*
总装备部军标出版发行部出版
（北京东外京顺路 7 号）
总装备部军标出版发行部印刷车间印刷
总装备部军标出版发行部发行

*
开本 880×1230　1/16　印张 4¼　字数 135 千字
2004 年 12 月第 1 版　2004 年 12 月第 1 次印刷
印数 1－800
*
军标出字第 5819 号　定价 34.00 元