ICS 35.080
L 77

中华人民共和国国家标准

GB/T 32423—2015

系统与软件工程　验证与确认

System and software engineering—Verification and validation

2015-12-31 发布　　2016-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准起草单位:中国航天科技集团公司软件评测中心、中国电子技术标准化研究院、国家应用软件产品质量监督检验中心、国网河南省电力公司电力科学研究院、国家网络软件产品质量监督检验中心(济南)、上海计算机软件技术开发中心。

本标准主要起草人:杨桂枝、王玲、张刚、王瑞、梁勇、樊星、相福民、王威、任佩、张威、牛霜霞、魏广路、吕宏宇、蔡立志、刘振宇、赵颖颖。

引　言

0.1　背景与概述

本标准是一项过程标准，可以看作是 ISO/IEC 15288:2008 和 ISO/IEC 12207:2008 中有关 V&V 的进一步细化过程。验证与确认(V&V)过程确定某一给定活动的研发产品是否符合活动要求，以及产品是否满足其预期用途和用户需求。确定活动可能包括产品和过程的分析、评价、评审、审查、评估和测试。

V&V 过程包括验证过程和确认过程。验证过程提供客观证据证明产品是否实现如下要求：

a)　在每个生存周期过程中，所有活动都遵循需求要求(如，正确性、完备性、一致性和准确性)；

b)　在生存周期过程中，满足标准、惯例和公约；

c)　成功完成每个生存周期活动，并满足启动下一步生存周期活动的所有标准(即正确生产产品)。

确认过程提供客观证据证明产品是否实现如下要求：

a)　在每个生存周期活动结束时，满足分配给产品的系统需求；

b)　解决恰当的问题(如，正确建立自然规律模型和执行商业规则，并使用适当的系统假设)；

c)　满足操作环境中的预期用途和用户需求(即生产正确的产品)。

验证过程和确认过程是相互关联和相互补充的过程，他们互相利用对方的过程结果，为每一个生存周期活动建立更加完善的完成准则和分析、评价、评审、检查、评估和测试 V&V 任务。表 4、表 9、表 14 和表 19 中描述的 V&V 任务准则唯一定义了 V&V 过程的符合性要求。

要获取充分的证据，需要在执行 V&V 任务所花时间、有限的系统条件和假设之间进行权衡。每个项目宜对充分的证据(即选择一个完整性级别，以建立一个基本参数)、时间进度、V&V 分析和测试任务范围(即系统条件和假设范围)的准则进行定义。

本标准不指定任一组织执行 V&V 任务的职责。分析、评价和测试活动可由多个组织执行，而对每一组织的多用途目标，方法和目的会有所不同。

ISO/IEC 15288:2008 和 ISO/IEC 12207:2008 要求开发方作为实现的一个完整部分，执行各种测试和评价任务。本标准中所描述的技术可能有助于执行开发方测试和评价。因此，本标准所指开发方实施的验证与确认活动，可以理解为用于实现的测试和评价任务的参考。

0.2　目的

本标准的目的在于：

a)　为支持所有的系统、软件和硬件的生存周期过程而建立一个 V&V 过程、活动和任务的公共框架；

b)　定义每个生存周期过程的 V&V 任务、要求的输入和要求的输出；

c)　识别对应于四级完整性方案的最低限度 V&V 任务；

d)　规定 V&V 计划(SVVP)的内容。

0.3　应用领域

本标准适用于所有应用系统。当实施某一系统、软件或硬件元素的 V&V 时，元素作为系统的一部分，检查其与系统的交互很重要。本标准识别系统需考虑的重要因素，V&V 过程和任务在确定正确性和其他 V&V 属性(如，完备性、准确性、一致性和可测试性)时处理这些因素。

复杂系统的动态变化和系统中响应变化的激励和条件的不同逻辑路径的多样性，要求 V&V 活动检查系统对每一种可能的条件变化的正确性。模拟复杂的，真实世界条件的能力是有限的，因此，对于期望的解决方案，V&V 活动检查建模的限制是否是现实的、合理的。系统条件的无限组合赋予 V&V 活动运用有限的分析、测试、模拟和演示技术建立一套合理的证据体系证明系统的正确性的挑战。

系统提供了一种通过集成一个或多个过程、硬件、软件、设施和人员来满足规定的需要或目标的能力。这些关系要求 V&V 过程要考虑所有系统元素（软件和硬件）的交互。V&V 过程处理以下与系统的交互：

a) 环境：确定系统正确地说明了所有条件，自然现象、自然规律、商业规则、物理性质和系统运行环境的全部范围；

b) 操作员/用户：确定系统向操作员或用户传达系统正确的状态/条件，正确处理所有的操作员/用户的输入，以产生所需结果。对于错误的操作员/用户输入，确保保护系统免于进入危险状态或失控状态。确认操作员/用户策略和规程（如，保密安全性、接口协定、数据表现、系统假设）得到一贯应用并在每个部件接口中使用；

c) 其他软件、硬件和系统：确定软件或硬件部件依据需求与系统中的其他部件正确接口，并确定错误不会在系统部件之间传播。

V&V 过程的范围包括运行环境，操作人员和用户，硬件，软件，数据处理（如，向用户提供服务的过程），规程（如，操作人员指南）和设施。本标准的用户宜考虑将 V&V 作为行业标准定义的软件生存周期过程的一部分，如，ISO/IEC 12207：2008、IEEE Std 1074-2006 或 ISO/IEC 15288：2008。

为解决整个系统的问题，系统、软件和硬件 V&V 宜进行 V&V 任务相关的集成性分析，提供输入和对其他 V&V 任务的分析。已完成的生存周期过程结果，为其他生存周期过程的 V&V 任务提供了宝贵的和必要的输入。某一 V&V 任务的结果和发现可能会导致要用新的数据对以前完成的 V&V 任务再次进行分析。采用严格的系统工程技术的 V&V 任务（包括对技术的和软/硬件的具体过程的反馈）之间的这种关系，是集成系统和软硬件 V&V 的一个重要途径。V&V 结果为其他过程提供了可用于过程改进的早期异常监测和潜在过程趋势。本标准中描述的 V&V 过程和任务可以与系统工程和过程改进模型结合使用，如能力成熟度模型集成 CMU/SEI-2010-TR-033。

本标准兼容所有生存周期模型（如系统、软件和硬件），但并非所有生存周期模型都采用本标准中所列的全部过程。

0.4 V&V 目标

V&V 过程对整个生存周期的产品和过程进行客观评估。该评估论证需求是否正确、完整、准确、一致和可测试。V&V 过程确定某一指定活动的产品是否符合该活动要求，是否满足其预期用途和用户需要。这种确定过程可包括产品和过程的评估、分析、评价、评审、审查和测试。V&V 任务应与所有生存周期阶段并行，而不是在生存周期阶段结束后。

V&V 结果为程序带来下列益处：

a) 促进异常的早期监测和纠正；

b) 加强管理，发现过程和产品的风险；

c) 支持生存周期过程以确保符合项目执行、进度和预算要求；

d) 提供性能的早期评估；

e) 提供符合性的客观证据以支持正式认证过程；

f) 改进获取、供应、开发和维护过程的产品；

g) 支持过程改进活动。

0.5 标准的组织结构

引言　提供本标准的使用指南。

第 1 章　范围。

第 2 章　符合性。

第 3 章　术语、定义和缩略语。

第 4 章　描述 V&V 过程和 ISO/IEC 15288:2008 和 ISO/IEC 12207:2008 中的生存周期过程之间的关系,以及 V&V 标准如何在多系统的某一系统概念内,从系统到软件或硬件部件递归地应用 V&V 标准。

第 5 章　描述使用完整性级别来确定 V&V 过程的范围和严格程度。

第 6 章　解释在本标准中如何描述 V&V 任务。

第 7 章　描述公共的 V&V 任务。即,本标准应用到系统、软件或硬件时公共的 V&V 任务。

a)　表 4 包含 V&V 任务和活动以及公共的 V&V 任务和活动的准则;

b)　表 5 包含对每一个完整性级别,公共的 V&V 任务的最低限度任务;

c)　表 6 包含可选的公共 V&V 任务;

d)　表 7 概要描述公共 V&V 活动和任务;

e)　表 8 概要描述 V&V 测试产品和任务。

第 8 章　描述系统 V&V 任务。

a)　表 9 包含 V&V 的任务和活动以及系统 V&V 任务和活动的准则;

b)　表 10 包含对每一个完整性级别,系统 V&V 任务的最低限度任务;

c)　表 11 包含可选的系统 V&V 任务;

d)　表 12 概要描述系统 V&V 活动和任务;

e)　表 13 概要描述系统 V&V 测试产品和任务。

第 9 章　描述软件 V&V 任务。

a)　表 14 包含 V&V 任务和活动以及软件 V&V 任务和活动的准则;

b)　表 15 包含对每一个完整性级别,软件 V&V 任务的最低限度任务;

c)　表 16 包含可选的软件 V&V 任务;

d)　表 17 概要描述软件 V&V 活动和任务;

e)　表 18 概要描述软件 V&V 测试的产品和任务。

第 10 章　描述硬件 V&V 任务。

a)　表 19 包含 V&V 任务和活动以及硬件 V&V 任务和活动准则;

b)　表 20 包含对每一个完整性级别,硬件 V&V 任务的最低限度任务;

c)　表 21 包含可选的硬件 V&V 任务;

d)　表 22 概要描述硬件 V&V 活动和任务;

e)　表 23 概要描述硬件 V&V 测试的产品和任务。

第 11 章　描述 V&V 报告、行政管理和记录的要求。

第 12 章　描述 V&V 计划的内容。

本标准的组织结构使 V&V 过程(系统、软件或硬件)能够单独引用或以任意组合引用。V&V 过程可以如下任何一种组合来完成:系统 V&V(第 8 章),软件 V&V(第 9 章),硬件 V&V(第 10 章),系统/软件 V&V(第 8 章和第 9 章),系统/硬件 V&V(第 8 章和第 10 章),软件/硬件 V&V(第 9 章和第 10 章),以及系统/硬件/软件 V&V(第 8 章至第 10 章)。一些 V&V 任务对系统、软件和硬件 V&V 是公共的;为了在每一部分不重复这些 V&V 任务,第 7 章一次性列出了公共 V&V 任务。执行任意 V&V 任务都可以调用公共 V&V 任务。表 1 说明了这些组合。

表 1　V&V 活动组合

V&V 范围	公共	系统	软件	硬件
仅限系统	×[1)]	×		
仅限软件	×		×	
仅限硬件	×			×
系统和软件	×	×	×	
系统和硬件	×	×		×
软件和硬件	×		×	×
系统、软件和硬件	×	×	×	×

第 4 章至第 6 章包含 V&V 范围内的适用于所有组合的指南。第 11 章包含 V&V 范围内的所有组合的报告要求。第 12 章包含一个 V&V 计划示例。

表 4、表 9、表 14 和表 19 提供每一个生存周期过程的 V&V 任务描述，输入和输出。表 5、表 10、表 15 和表 20 列出不同完整性级别所要求的最低限度 V&V 任务。表 6、表 11、表 16 和表 21 列出可选的 V&V 任务，及其在系统生存周期中的建议应用。这些可选的 V&V 任务可以添加到最低限度 V&V 任务中，对 V&V 过程进行剪裁以满足项目需要。

表 7、表 12、表 17 和表 22 举例综述对完整性级别为 4 级的 V&V 输入、输出和最低限度 V&V 任务。表 8、表 13、表 18 和表 23 提供了策划 V&V 测试计划、执行和验证活动的指导原则。表 4、表 9、表 14 和表 19，表 5、表 10、表 15 和表 20 利用一个阶段式生存周期模型的示例，说明 ISO/ IEC12207：2008 生存周期过程与本标准中描述的 V&V 活动和任务的映射。

附录 A 描述了 ISO/ IEC12207：2008 和 ISO/IEC 15288：2008 与本标准的 V&V 活动和任务的映射。附录 B 提供了一个基于风险的、四级完整性方案的示例。附录 C 提供了独立验证和确认(IV&V)的定义。附录 D 提供实施重用软件 V&V 的指导原则。附录 E 描述 V&V 度量。附录 F 举例说明与其他项目职责的 V&V 组织结构关系。附录 G 描述了可选 V&V 任务。附录 H 描述执行 V&V 时宜考虑的环境因素。附录 I 讨论系统、软件和硬件之间交互的潜在问题。附录 J 描述危险分析，保密安全性分析，风险分析和它们在 V&V 中的作用。附录 K 提供指定和改变支持系统功能的完整性级别的示例。附录 L 就相关联的 V&V 任务，对比 ISO/IEC 12207：2008 和 ISO/IEC 15288：2008 的过程输出。

0.6　读者

本标准读者包括系统、软件和硬件供方、开发方、维护方、V&V 人员、操作人员、用户以及供方和需方组织中的管理者。

1)　×表示选择对应的活动。

系统与软件工程　验证与确认

1　范围

本标准规定了包括获取、供应、开发、运行、维护和退役的整个生存周期的系统、软件、硬件开发的验证和确认过程。

本标准适用于系统、软件和硬件的获取、开发、维护或重用。

2　符合性

词语“应”(shall) 表示符合本标准的必达要求。词语“宜”(should)和“可”(may)指不要求声明遵循本标准的可选任务。

并非所有 V&V 活动都是从生存周期的获取阶段启动，持续到维护阶段。如果一个项目仅应用选定的生存周期过程，那么如果对项目所选的所有有关联的生存周期过程执行最低限度 V&V 任务，即可以实现对本标准的符合性。任何遵循本标准的声明应标识适用的生存周期过程。在所有情况下，最低限度 V&V 任务是由指定给系统、软件或硬件的完整性级别定义的。对于该项目未应用的生存周期过程，其 V&V 需求和任务是由项目决定的按所需调用的可选 V&V 任务。具体的开发方法和技术(诸如由详细设计而自动生成代码)可以删除开发步骤或把几个开发步骤合并成一个。因而，允许对最低限度 V&V 任务进行相应的改变，并应记录在遵循本标准的任何声明中。

当现存系统、软件或硬件采用本标准且要求的 V&V 输入不可用时，那么 V&V 任务可使用其他可用的项目输入来源或改造要求的输入以满足对本标准的符合性。

系统，软件或硬件，通过证明能满足如下章条中的所有“应”的要求，实现对本标准的符合性。

系统 V&V 的符合性：第 7 章和第 8 章。

软件 V&V 的符合性：第 7 章和第 9 章。

硬件 V&V 的符合性：第 7 章和第 10 章。

放弃符合性须经需方组织批准，并写入验证与确认计划(VVP)中。所需的偏离和放弃信息应包括任务识别，理论依据和质量影响。

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文件。

3.1.1

资产　asset

设计用于不同周境的一个产品(如，设计、规格说明、源码、文档、测试套件、手册规程)。

3.1.2

部件　component

构成系统的部分。部件可以是硬件或软件，且可进一步划分为其他部件。

注：术语“模块(module)”“部件(component)”和“单元(unit)”经常替换使用，或根据上下文以不同的方式被定义为另一个的子元素。这些术语之间的关系尚未标准化。