基于系统工程过程论验证和确认

邓林，邓明

（中国电子科技集团公司第二十九研究所，成都 610036）

摘要：为了解析工程过程验证和确认之间的关系，明确两者的作用和方法。对两个概念的形成溯源、异同比较、关系分析、方法应用等角度展开分析和论述。验证和确认是系统工程过程中非常重要的两个技术过程，两个过程中的若干活动的方法比较相似，甚至相同，容易引起混淆。分析结果表明，两者目的不同，方法相似。验证（Verification）和确认（Validation）是系统工程的技术过程中非常重要的两个子过程，是整体过程中的不可缺少的两个环节，区别在于验证过程是确定设计过程和结果是正确的，确认过程则是确定所设计的对象是正确的，是符合利益相关方需求的。

关键词：系统工程；验证；确认

DOI：10.7643/ issn.1672-9242.2017.11.005

中图分类号：TJ01；TB21 **文献标识码：**A

文章编号：1672-9242(2017)11-0027-03

Verification and Validation Based on System Engineering Process Theory

DENG Lin, *DENG Ming*

(The 29th Research Institute of China Electronics Technology Group Corporation, Chengdu 610036, China)

ABSTRACT: To analyze the relationship between verification and validation of engineering processes and clarify the roles and methods of both, this paper analyzed and discussed the two concepts from traceability, similarities and differences, relationship analysis, method application, etc. Verification and validation are two important technical processes in system engineering. Methods of several activities in two processes are similar, even the same, and confusing. The results show that their purposes were different, while their methods were similar. Verification and validation are two very important sub-processes in technical process of system engineering. They are essential for the integral process. Their difference is that: the verification process is to determine the design process and the results are correct, the confirmation process is to determine the design of the object is correct. They are in line with the needs of stakeholders.

KEY WORDS: system engineering; verification; validation

验证和确认是系统工程过程中非常重要的两个技术过程，由于两个过程中若干活动的方法比较相似，甚至相同。因而，我们对这两个不同目的过程的概念和应用上存在不少困惑。如术语如何形成的，术语概念的异同是什么，验证和确认之间的关系是什么，什么时机运用验证或者确认，验证和确认过程有哪些活动。

由于不同标准对这两个术语定义不尽相同，如国际标准化组织 ISO、美国民用航空航天局 NASA、美国国防部 DOD、国际系统工程学会 INCOSE。因此，更有必要理清它们之间的关系已便于合理应用。

1 术语的形成

由于这两个词是由西方语系英语翻译过来的词，因此要搞清其本质，须从词源角度先看看这两个词的本意是什么。

验证（Verification）：牛津英语（Oxford）给出解释为，名词，词起源于古法国 16 世纪早期，来源于拉丁文，从动词 verificare（verify），从“真实”。意为确定某物的真实性、准确性或有效性的过程。词义落脚点在过程（process）。标准（3.8.12，ISO

收稿日期：2017-07-11；**修订日期：**2017-08-26

作者简介：邓林（1972—），男，四川遂宁人，高级工程师，主要研究方向为环境可靠性工程/质量工程技术。

9000:2015(E))给出的解答是,通过提供客观证据(可以用观察、演示、测试、试验和分析等方法获得证据)证实规定的要求已经实现[1]。

确认(Validation):牛津英语(Oxford)给出解释为,名词,词形成于 17 世纪中期,有律例或法律上“有效”的意义,来源于 16 世纪晚期的拉丁文动词的 validus(valid),从“有效”。意为检查或证明某物有效性或准确性的措施;或在法律或官方上做出可以接受决策的措施。词义落脚点在措施(action)。标准(3.8.13,ISO 9000:2015(E))给出的解答是,通过提供客观证据,证实预期的使用和应用要求已经实现[2]。

2　术语概念的异同

从标准上来看,验证是证实规定的要求已被实现,确认是证实预期的使用和应用要求已被实现,虽然同是证实要求已被实现,但验证的对象是规定的要求,而确认的对象则是预期的使用和应用要求。这是两个概念相近,但对象不同,具有差异性的术语,易引起混淆。在特定领域,为易于理解,其术语定义还被细化,如 ANSI/GEIA-STD-0009 给出了特定的验证(Verification)术语定义:通过提供和检查客观证据,证实最终产品(被设计、编码或组装而成的产品)的规定要求已经实现[3]。

查阅文献后发现,在管理体系过程和系统工程过程中,验证和确认还是两个非常重要的过程,如 ISO/IEC/IEEE 15288:2015(E) 系统和软件工程-系统的生命周期过程,其中将验证过程和确认过程作为其四大过程之一,技术过程 14 个子过程中的两个重要技术过程。分别是 6.4.9 验证和 6.4.11 确认,并进行了标准化的描述[4],很值得学习。国际系统工程学会 2015 年发布的第 4 版系统工程师手册(INCOSE-TP-2003-002-04)同样将验证(4.9)和确认(4.11)放入技术过程中进行了详细的说明[5]。

对于这些概念,应注意广泛查阅相关资料中的异同点,以助于学习、理解、掌握这些概念。综合各方论述,建议参考国际标准化组织 ISO/IEC/IEEE 15288:2015(E),对验证过程和确认过程的目的说明,有助于我们理解这两个术语概念。

标准对于验证过程的目的描述如下:验证过程的目的是提供客观证据,证明系统或系统要素符合其规定的要求和规格。验证过程使用适当的方法、技术、标准或规则,来识别已实现系统或生命周期过程中与描述信息项(如系统要求或体系结构描述)不一致的各种异常(包括错误、缺陷和故障)。这一过程为识别异常的判别准确度提供了必要的信息。验证过程是确定“产品设计正确”,确认过程则是确定“设计的产品正确,是所需的”[4]。

标准对于确认过程的目的描述如下:确认过程的目的是提供客观证据,证明系统在预期的工作环境中,以及预期的使用条件下,实现其业务或任务目标以及相关方(也称为利益相关方,指有权、利益、投资,可影响系统涉及开发决策或活动的个人或组织)的相关要求,以及达成其预期的使用用途。进行系统或系统要素确认的目标,是在特定的工作条件下,取得系统或系统要素实现其预期任务或使用能力的置信度。确认结果是由相关方批准认可的。这一过程为针对引入异常的过程点,利用适宜的技术过程解决各种识别出的异常,提供了必要的信息。确认也适用于系统定义和实现过程中产出的工程工件(可视其为系统元素)[4]。

通过以上解析,大致可以得出这两者概念的异同。相同的是两者都是证实要求已被实现,不同的是验证用于证实事做对了,确认则用于证实相关方的钱花没有白花,东西做正确了,所得即所需。

3　验证和确认之间的关系

要了解这两个过程之间的关系,首先需要去了解系统工程技术过程中,这两个过程是什么,做什么。

对于一个成功的验证过程,标准认为有以下几个衡量标准:影响需求、架构和设计的验证限制条件已被识别;所有验证所需的支持系统或配套设施是有效的;系统和系统元素已得到验证;纠正措施所需的,由数据归纳出的信息,已得到报告或记录;已实现系统符合需求、架构和设计的客观证据已提供;验证结论和各类异常(错误、缺陷和故障)已被识别;各类已验证系统元素的可追溯性已被建立。

标准认为,一个成功的确认过程应有如下衡量标准:相关方的需求确认标准已定义;相关方要求的可用服务/功能已确定;影响需求、架构、设计确认的限制已识别;系统或系统元素已得到确认;所有确认所需的支持系统或配套设施是有效的;确认结论和各类异常(错误、缺陷和故障)已被识别;已实现的系统或系统元素符合相关方要求的客观证据已提供;各类已确认系统元素的可追溯性已被建立。

综合上述描述可以看出,对同一系统或系统元素对象而言,验证应在确认之前。验证是证实对象的形成过程是对的,结果是符合设计规格和要求的。确认则是证实已形成的结果在预期的使用条件和预期使用环境中,能够实现相关方对其的预期应用和任务能力要求,且经过相关方的认可批准。可以说,二者过程之间,活动和方法相近,目的不同。

运用时机方面,对同一系统或系统元素对象,验证在其实现过程中,需要对过程和过程的输出实施验证,以证实做对了。确认则是在其实现之后,运用特定方法对其实施结果进行确认,以证实做正确了且符

合相关方的需求，如图 1 所示。

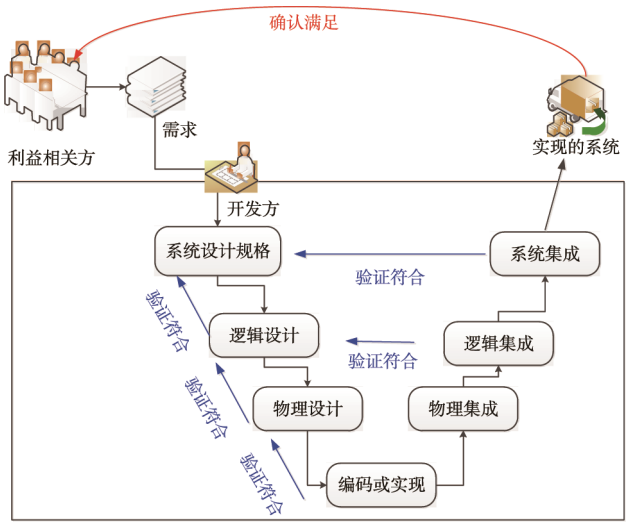

图 1　验证与确认的时机

4　验证和确认过程有哪些活动

从多份参考资料中可以看出，验证过程和确认过程非常相似，就像同一工具使用在不同对象上一样，目的虽不同，方法却一致。

标准对验证过程活动描述为：验证策略通常会基于成本、进度、风险三个维度，权衡出最小化代价的方案，用以证实系统或系统元素已符合设计要求。验证过程分为 3 个子过程[4]。

1）验证准备，包含 7 个活动。分别是识别验证范围和相应的验证措施；识别可能限制验证措施可行性的各类约束条件；为每一个验证措施，选择适宜的验证方法、技术，以及相应的标准；定义验证策略；在验证策略中，识别系统约束，并纳入到系统需求、架构、设计规格要求中；识别并策划所有验证所需的支持系统或配套设施；获得或获取这些支持系统或配套设施的使用或访问权限，用于实施验证活动。

2）验证实施，包含两个活动。分别是定义验证活动程序，每个程序支持一个或一组验证措施；执行验证程序。

3）验证结果管理，包含 5 个活动。分别是记录验证结果以及所遇到的任何异常；记录操作过程中的失效事件和问题，并跟踪其解决过程形成的各类决议；获取有关系统或系统元素满足特定要求的利益相关方协议；维护已验证系统元素之间的可追踪性；对各类已选定为基线的，提供验证的关键信息项。

与验证过程相似，确认过程也分为 3 个子过程[4]。

1）确认准备，包含 7 个活动。分别是识别确认范围和相应的确认措施；识别可能限制确认措施可行性的各类约束条件；为每一个确认措施选择适宜的确认方法、技术，以及相应的标准；定义确认策略；在确认策略中，识别系统约束，并纳入到利益相关者要求中；识别并策划所有确认所需的支持系统或配套设施；获得或获取这些支持系统或配套设施的使用或访问权限，用于实施确认活动。

2）确认实施，包含 3 个活动。分别是定义确认活动程序，每个程序支持一个或一组验证措施；在指定的环境中，执行确认程序；评审确认过程给出的结论，用以确定利益相关方所提出的系统各种功能使用要求是已实现且可用的。

3）确认结果管理，包含 5 个活动。分别是记录确认结果以及所遇到的任何异常；记录操作过程中的失效事件和问题，并跟踪其解决过程形成的各类决议；获取有关系统或系统元素满足特定要求的利益相关方协议；维护已确认系统元素之间的可追踪性；对各类已选定为基线的，提供确认的关键信息项。

以上验证和确认过程中的子过程和各子过程中的活动非常相似，但目的不同。特别是两个过程的实施过程，验证强调的是可执行性，确认则是强调评审验证结论，用以证实已实现系统满足利益相关方最初提出的使用和应用需求。

5　结论

验证和确认是系统工程的技术过程中非常重要的两个子过程[6]，是整体过程中不可缺少的两个环节，验证过程用以确保技术实现过程的正确性，避免或消除出现局部与整体之间的偏差。通过验证过程，可以有效地降低系统实现过程中的过程或技术来带的偏差和异常风险。确认过程则是确保已实现系统或系统元素是正确的，是符合利益相关方最初提出的系统或系统元素的开发需求，即得到的结果对于利益相关方来讲，是正确的。也可以反过来理解，设计过程和结果虽正确，但不一定是利益相关方想要的。

归纳为一句话：验证过程是确定设计过程和结果是正确的，确认过程则是确定设计的对象是正确的，是满足利益相关方需求的。

参考文献：

[1] ISO 9000, Quality Management Systems—Fundamentals and Vocabulary[S].
[2] ISO 9000—2015, Quality Management Systems—Fundamentals and Vocabulary[S].
[3] ANSI/GEIA-STD-0009, Reliability Program Standard for Systems Design, Development, and Manufacturing[S].
[4] ISO/IEC/IEEE 15288, Systems and software engineering—System life cycle processes[S].
[5] INCOSE-TP-2003-002-04, Systems Engineering Handbook, a Guide for System Life Cycle Processes and Activities[S].
[6] NASA/SP-2016-6105 Rev2, NASA Systems Engineering Handbook[S].