军用软件产品的质量保证

船舶系统工程部　彭卫华

[按]今年8月，七院科技发展部在海南省三亚市组织召开了一次可靠性专题研讨会。与会专家提交的论文从不同角度上阐述了我院开展可靠性工作情况，并从理论上对可靠性作了研讨。应大会组织者要求，本刊作为专辑发表，期望对指导各单位开展可靠性研究起点作用，同时借此推动舰船及其装备的可靠性水平。

摘　要：从工程和管理的角度，提出了保证和提高军用软件产品质量和可靠性水平的要求、途径和方法。

关键词：软件；质量；质量保证

1.引　言

随着计算机技术迅猛发展及其在军事工程的广泛应用，软件的质量越来越受到人们的关注。如何保证和提高软件产品的质量，成为军工产品研制和质量管理的一项新课题。

目前我国绝大多数软件的设计与开发还停留在那种手工作坊式的生产阶段。这种初级的生产组织方式显然已无法满足使用要求日益苛刻、规模日益庞大的军用软件产品的质量要求，只有逐步实现软件产品的设计开发从个体方式向工业化转变、按科学规律开发软件、开展软件的可靠性设计并对其实施严格的质量管理才是保证和提高软件尤其是军用软件产品的质量和可靠性水平的根本途径和方法。

2.转变观念，促进软件产品工业化

对于大多数软件人员来讲，软件开发即意味着按自己的思维习惯和思维定式运用某种语言进行程序编制；编程结束后只是使用有限的输入进行调试，通过后即完成了软件的测试。在这种"自编、自导、自演"的指导思想下开发的软件产品只能算是一种工艺品，由此带来的后果是明显的：软件的可读性极差；软件难以维护和扩展；质量隐患无法从根本上得以剔除；软件产品的质量和可靠性难以保证，这就是软件的质量和可靠性水平不高的结症所在。因此，软件人员应该彻底与这种传统的软件设计思想决裂，借鉴硬件的设计经验，实现软件的工业化生产。

软件的工业化生产与硬件是类似的。软件设计人员设计图纸——详细设计报告；软件工人（一般高中毕业生经短期培训即可）按详细设计报告编制程序；软件检测人员对设计报告、程序分别进行检查和测试，发现错误或故障首先修改设计报告，然后修改程序，修改后进行进一步的检测，直到满足交付要求。

对于军用软件用户即军方来讲也需要更新观念。在相当长的一段时期里，用户存在一种思想倾向，认为软件开发就是一个或几个人凑起来在计算机上编程，几乎没有任何生产成本。其实不然，美国国防部1991－1992年度国防经费支出中，软件费用占10%，达300亿美元；美国最新一期《商业周刊》评

出1994年度市场价值增幅最大的25种产业，计算机软件及服务业名列榜首，达412.31亿美元(计算机及其外围设备排名第四)。虽然我国经济实力不能同美国相比，但以上数据仍然能说明一定的问题。软件是一种知识密集、技术密集、经济价值极高的技术产品，它凝聚了软件设计人员的知识、智慧和经验；复杂软件产品更需要长时间的充分测试。因此，要获得高质量高可靠的软件产品需要较高的投入，而且这种投入比例同硬件研制投入相比，比例将越来越大已经成为一种必然的趋势。

实现软件产品工业化不是一蹴而就的，需要创造许多先决条件。其中，观念的改变与更新是促进软件产品工业化的首要条件。

3.按瀑布模型开发软件

同硬件的研制类似，软件产品同样需要按一定的科学规律顺序地按阶段地开发与研究，这也是软件工业化生产的基本要求。瀑布模型(Waterfall Model)是美国国防部标准规定的软件开发模式，对我国军用软件的开发亦有较好的借鉴作用。

瀑布模型要求软件开发要遵循自上而下、分阶段顺序开发的科学规律，其主要内容为：系统需求分析；软件需求分析；概要设计；详细设计；编程及单元测试；模块组装及测试；软件配置项目测试；系统综合和试验。

系统需求分析，即从硬软件结合的大系统出发，了解用户的要求及现实环境，分析系统要完成的功能，对系统功能进行分解，确定约束条件，规定硬软件的任务需求。

软件需求分析，即确定软件的运行环境，功能和性能要求，接口设计要求，编写用户手册概要，确认测试准则。

概要设计，即根据软件需求说明，建立系统的总体结构同模块间的关系，定义各功能模块的接口，设计数据库及数据结构，规定设计限制，制订组装测试计划。

详细设计，即将概要设计中产生的功能模块进行过程描述，设计功能模块的内部细节，包括算法、数据结构和流程框图，为编写源程序提供必要的规范。

编程及单元测试：即将详细设计说明转化为所要求的程序设计语言或数据库语言编制的源程序，并对源程序进行程序单元测试，验证程序模块接口与详细设计规范的一致性。

模块组装及测试，即根据概要设计中各功能模块的说明及制订的组装测试计划，将经过单元测试的模块逐步进行组装和测试，提供可运行的软件系统源程序及组装测试分析报告，进行软件可靠性预计。

软件配置项目测试，即复杂软件系统在更多模块上的组装及测试。系统综合和试验，即根据软件需求规范中定义的全部功能和性能要求及测试计划测试整个系统，验证系统是否满足要求。

系统综合与试验，即根据软件需求规范中定义的全部功能和性能要求及测试计划测试整个系统，验证系统是否满足要求。

国内外的软件开发实践已经充分证明：按科学规律分阶段顺序开发软件往往事半功倍；相反，超越科学规律则会带来混乱，往往事倍功半。

4.提高软件产品质量和可靠性的几种设计方法

军用软件产品的质量和可靠性直接影响到武器装备的战斗力。因此，软件开发和设计人员应千方百计致力于提高软件产品的质量和可靠性。在诸多的软件设计方法中，模块化设计、结构化设计、标准化设计、冗余设计和容错设计均可有效地提高软件的质量和可靠性。

模块化设计：将软件系统作为一组模块集合来开发，这样可以使程序容易被人理解：容易编程、调试、查错、测试和修改。模块应尽可能设计成单入口和单出口，内聚度应尽可能高。模块规模要适当，可执行源代码语句一般控制在100行以下，最多不应超过200行，系统平均不超过60行。模块之间尽可能只有调用参数关系，且参数应尽可能少、耦合性尽可能弱。

结构化设计：GJB437－88《军用软件开发规范》规定了模块的5种控制结构：顺序(SEQUENCE)结构、条件转移(IF THEN ELSE)结构、当循环(DO WHILE)结构、直到循环(DO UNTIL)结构和分情况(CASE)结构。这5种基本结构都只有一个入口和一个出口，使用这种单入口的基本结构单位容易嵌套，以实现复杂处理。5种基本结构之外的控制方式尽可能不用，尤其不要使用转移(GO TO)语句。

不得已使用时，必须在同一程序单元内转移，且应向转移语句所在点的前方转移。

标准化设计：为了减少重复劳动，缩短开发周期，节省费用，提高可靠性，软件的开发也应象硬件那样尽量使用软件标准件，提高软件的标准化系数。从可靠性的角度看，软件标准件是严格按软件工程要求生产的，有完备的文档资料，经过了严格的测试及广泛的应用、改进，具备很高的可靠性；从成本和进度的角度看，软件标准件无需重新设计和测试，既降低了成本又加快了进度。

冗余设计：冗余技术是常用的一种可靠性设计方法，为了提高可靠性、软件的开发也需要开展冗余设计。但是，软件的冗余与硬件不同：相同的硬件可以组成冗余系统，而相同的软件则不能形成冗余。因为相同的软件具有相同的缺陷和错误，在相同的使用条件下只会一错都错，起不到冗余作用。所以，软件冗余必须用具有相同功能的“相异”软件组成冗余系统，冗余设计需要采用多版本程序设计，并要保证程序之间的独立性。

容错设计：这是一种软硬件结合的设计方法。其设计思想就是要求软件设计时要充分考虑到硬件出现常见的、不可避免的或不能完全纠正的故障时，软件应能够采取必要的措施以保证系统仍然能够连续地正确运行或提供保护。如电源失效是一种常见的计算机故障，软件应设计成能够实现配合硬件在电源失效时提供安全的系统关闭，消除不安全隐患的功能。

5.对软件产品实施严格的质量管理

军用软件作为一种特殊的军工产品，也需要象硬件那样在其寿命期内实施严格的质量管理。

组织落实上，军用软件设计师系统与软件的质量保证职能机构形成矩阵结构，分别行使先例各自的职责。设计师系统按瀑布模型开发软件，对软件的质量和可靠性负技术责任；质量保证机构独立于设计师系统行使监督、检查、协调与控制职能。设计师系统应与软件的质量保证机构紧密配合，实行矩阵管理。

军用软件产品的质量管理应重点抓好设计评审、技术状态的管理、文档的控制及质量信息的管理工作。

按瀑布模型开发的军用软件产品应分阶段进行设计评审，以监控软件的设计。软件开发过程中所要进行的设计评审主要有系统要求评审、系统设计评审、概要设计评审、详细设计评审、软件验证和确认测试计划评审等5种类型。各类设计评审的具体要求与硬件类似。需要指出的是：很多成功的设计已经证明，设计评审是一种对于提高设计质量非常有效的技术方法，设计师系统和质量保证机构不应使设计评审走过场。

技术状态的管理对软件来讲亦称配置管理，其主要工作是：标识和确定系统的配置项，在系统寿命周期内控制这些配置项的投放和变更，记录并报告技术和变更要求，验证配置项的完备性和正确性。技术状态的管理对军工产品来讲尤为重要。

文档的控制是保证软件质量的重要环节。完备的文档是高质量软件的一个重要组成部分，也是软件工业化的一个重要标志。军用软件的开发与设计应提供13种文档：可行性研究报告、项目开发计划、软件需求说明、数据要求说明、概要设计说明、详细设计说明、数据库设计说明、用户手册、操作手册、程序维护手册、测试计划、测试分析报告、安装实施过程。软件设计人员应按规范编制所有文档，并以此作为设计评审的支撑性文件。

软件的质量信息管理应作为军工产品承制单位建立的“故障报告、分析和纠正措施系统(FRACAS)”的一部分，设计师系统按FRACAS的要求开展具体工作，质量保证机构对其实施监督、检查，并提供指导和支援。

6.结束语

1992年1月，美国宇航局失效分析实验室发表文章指出：当前NASA系统的软件故障率是硬件的十倍，这也许能给我们一些启示。不难预见，我国军用软件产品的开发和管理如果不能尽快实现工业化的转变，那么武器装备将会因为软件产品的质量水平不高而背上沉重的包袱。因此，尽可能早地实现军用软件产品的开发和管理步入规范化的轨道，从管理和工程两个方面共同来保证软件产品的质量已是当务之急。

参考文献(略)