中国民用航空总局

咨 询 通 告

编　　号：AC—21—02

生效日期：2000 年 1 月 10 日

机载系统和设备合格审定中的软件审查方法

航 空 器 适 航 司

中 国 民 用 航 空 总 局 航 空 器 适 航 司

咨 询 通 告

编　　号：AC-21-02
生效日期：2000 年 1 月 10 日
编制部门：CDC
批 准 人：

机载系统和设备合格审定中的软件审查方法

目　　录

机载系统和设备合格审定中的软件审查方法

1. 目的

本通告简要说明了在机载系统和设备的合格审定中如何使用RTCA/DO-178B 或 EUROCAE/ED-12B “机载系统和设备合格审定中对软件的考虑”来进行机载软件的适航审查。

本通告旨在为适航审查人员和申请人及其相关供应商更好地理解和掌握RTCA/DO-178B 或 EUROCAE/ED-12B(以下简称 DO-178B/ED12B) 的要求，进而更好地进行机载软件的符合性证明和审查活动提供指导。

作为一种指导性资料，本通告所提供的方法不是唯一的，也不是强制性的。

2. 依据和背景

本通告是在国内机载软件审查实践的基础上，依据 DO-178B/ED-12B 并参考波音公司培训教材 “审定工程师在机载设备和系统审定中的作用”制定的。随着软件审查工作经验的积累，今后还将不断对其进行修订和完善。

3. 相关文件

CCAR-21 部、23 部、25 部、27 部、29 部和 183 部等;

RTCA/DO-178B 和 EUROCAE/ED-12B;

AC 25.1309-1A/AMJ 25-1309、AC 23.1309-1C 等。

4. DO-178B/ED-12B 与软件审查

DO-178B/ED-12B 为在当前的机载系统及设备的合格审定中如何保证这些系统和设备的软件满足适航要求提供了一种可接受的方法。它适用于型号合格证/型号认可证(TC/VTC)、补充型号合格证/补充型号认可证(STC/VSTC)或 TSOA/PMA/VDA 的申请人和这些申请人的相关供应商。图 4-1 表明了 DO-178B/ED-12B 在适航审定过程中的应用面。

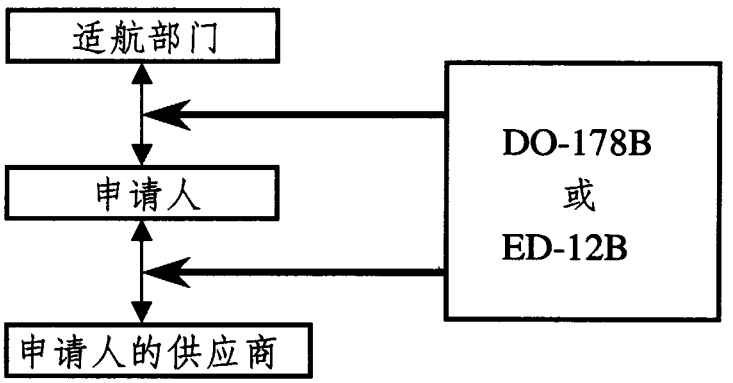

图 4-1 DO-178BED-12B 的应用面

DO-178B/ED-12B 是在 RTCA/DO-178A(或 EUROCAE/ED-12A)的基础上，根据 1985 年后机载软件审查的新经验于 1992 年 12 月 6 日由 RTCA（美国航空无线电技术委员会）和 EUROCAE（欧洲民用航空设备协会）共同批准和发布的。

DO-178B/ED-12B 就机载软件如何满足适航要求给予了如下的指导:

★ 确定了软件等级与软件生存周期过程的目标要求之间的对

应关系；

★ 确定了各软件生存周期过程的目标；

★ 说明了如何达到这些目标的基本方法和设计上的考虑；

★ 说明了如何来表明对这些目标要求的符合性。

DO-178B/ED-12B 附件 A（按软件等级确定的过程目标及输出）中的表 A-1 至表 A-10 概括地表述了这些指导。有关这些附表的内容详见本文附录。

5. 软件等级和失效情况类别

软件等级是由其失效情况的类别来决定的。而软件失效情况的类别定义则与系统失效情况的类别定义完全相同。同时，软件失效情况的类别与系统失效情况的类别一样，都是通过系统的安全性评估来确定的，即：在确定系统的审定基础时确定的。但是，与硬件不同的是：按某一软件等级来开发软件并不意味着对该软件进行了失效率的分配，因此在系统的安全性评估过程中，软件等级或基于该等级的软件可靠率是不能够像硬件的失效率那样来进行分配的。然而，这并不影响在一个具有多模块（部件）的分区软件内部构成软件模块（部件）之间的并联或串联关系，从而使得其中各软件模块（部件）的失效对某一软件功能产生不同的影响。

失效情况类别和软件等级的定义以及确定软件等级的指南可详见 DO-178B/ED-12B 的 2.2 节。表 5-1 给出了软件等级与失效情况类别的对应关系和简要说明。

表 5-1 软件等级与失效情况之间的关系

失效情况	软件等级	简 要 说 明
灾难性的	A 级	软件异常会导致的后果是：航空器无法安全飞行和着陆。
危险的	B 级	软件异常会导致的后果是：严重地降低了航空器或机组在克服不利运行情况时的能力。
重要的	C 级	软件异常会导致的后果是：显著地降低了航空器或机组在克服不利运行情况时的能力。
次要的	D 级	软件异常会导致的后果是：轻微地降低了航空器或机组在克服不利运行情况时的能力。
无影响的	E 级	软件异常会导致的后果是：不会影响航空器或机组的任何能力。

6. 软件审查概述

在确定审定基础的阶段，通过对系统需求的分配和对系统安全性的评估等过程，系统分配给软件的功能以及软件的等级就确定了。由此，便进入到了对软件的具体开发和审查阶段。以下各条简要说明了在软件开发和审查的整个阶段中，软件的各个生存周期过程及其相互关系，以及软件审查的基本流程和方法等。

6.1 软件审查与软件生存周期过程

软件审查是实现型号/系统审定目标不可缺少的环节之一。如图 6-1 所示，软件审查出自于型号/系统审查过程，最后又回到并结束于型号/系统审查的过程之中。软件生存周期过程包括：软件计划过程、软件开发过程和贯穿于这两个过程之中的软件合成过程。同时，软件开发过程被进一步细划为软件需求过程、软件设计过程、软件编码过程和软件综合过程——它们构成了软件产品开发的主线。而软件合成过程则被细划为软件验证过程、软件配置管理过程、软件质量保证过程和软件审定联络过程。其中，软件验证过程构成了软件审查的主线。

这些过程之间的基本关系如图 6-2 所示。

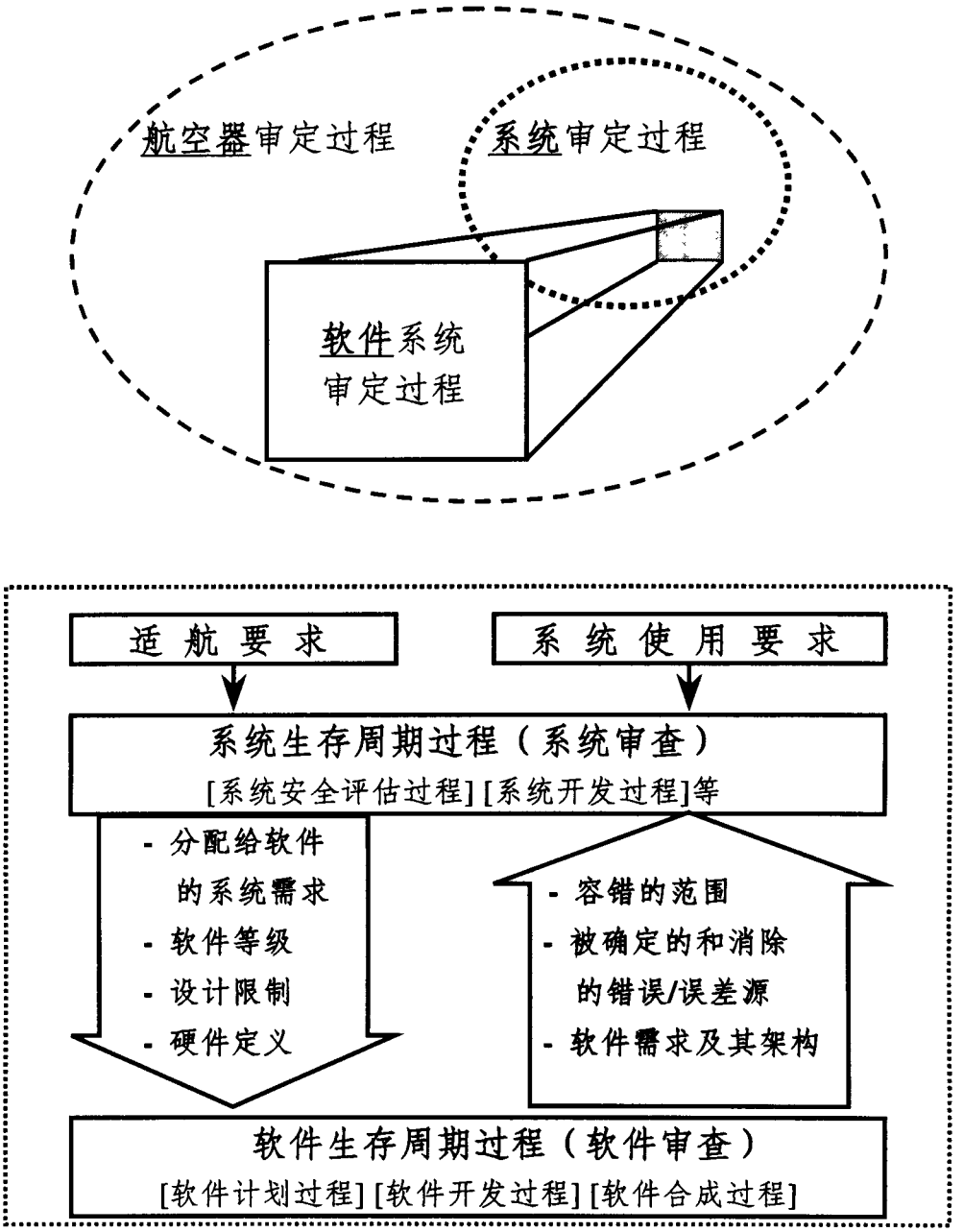

图 6-1 软件审查与型号/系统合格审定之间的关系示意

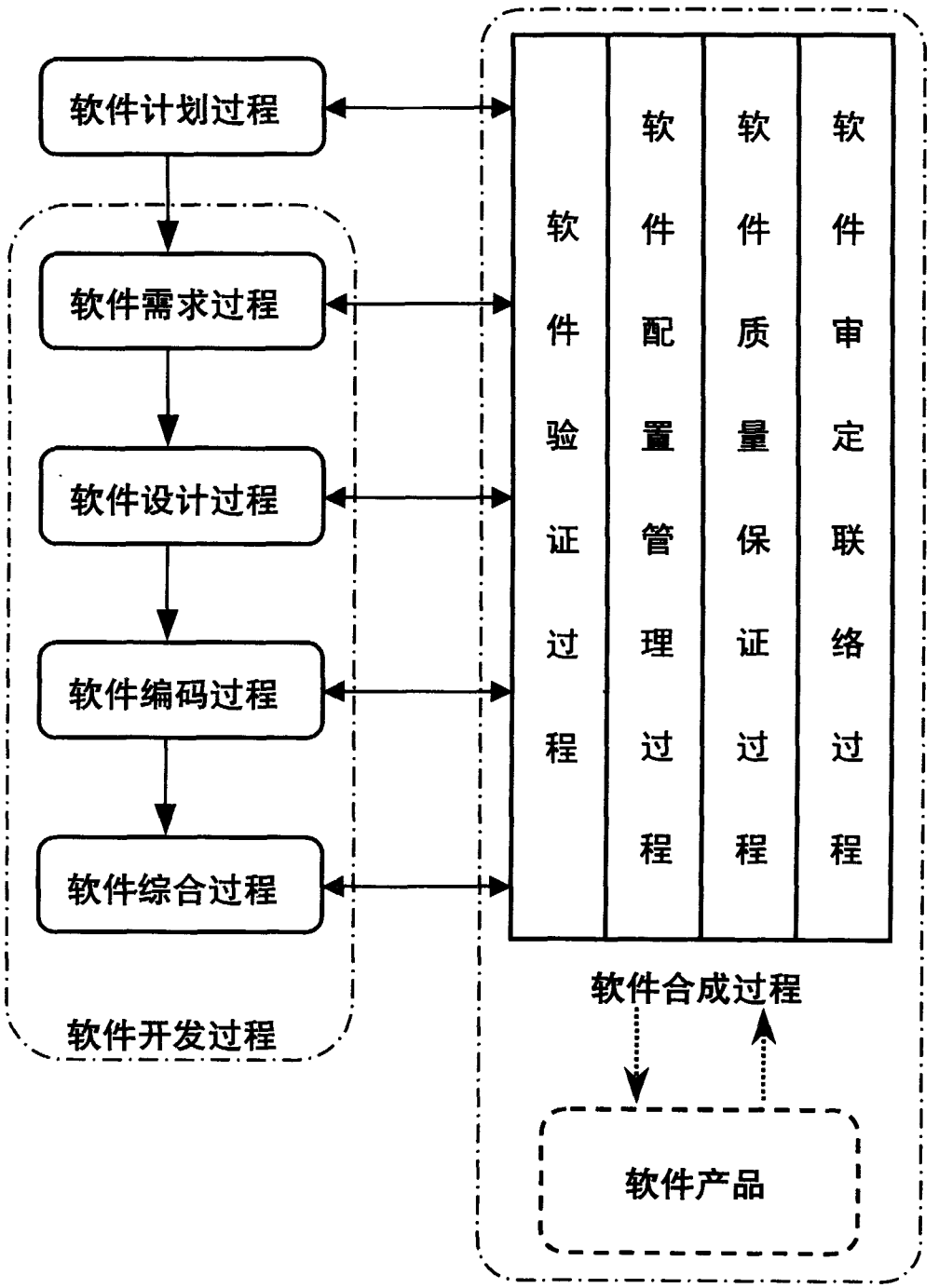

图 6-2 软件各生存周期过程之间基本关系的示意

6.2 软件审查的基本流程和方法

软件生存周期过程的特殊性决定了在确保软件产品的安全性(可靠性)、可追踪性、可验证性和可维护性的过程中软件审查方法的特点。如图 6-3 所示，软件审查的基本流程和方法是依据在型号/系统的审定基础中所确定的软件等级，按 DO-178B/ED-12B 附件 A(按软件等级确定的过程目标及输出）表 A-1 至表 A-10 中所确定的该软件等级在每一软件生存周期过程中的目标要求和符合性方法，逐项审查申请人对这些目标要求的符合性输出，而这些输出就是 DO-178B/ED-12B 第 11 章中所述的 20 种“软件生存周期文档”(必要时，还包括第 12.2 节中有关软件开发工具和验证工具的鉴定文档等)。其中，软件审定计划、软件配置索引和软件实施概要是适航部门在审查并批准申请人的符合性方法和符合性证据时最基本的三份文档。必须注意的是，DO-178B/ED-12B 所给出的目标要求和符合性方法都是原则性的，申请人应针对其欲开发软件的实际情况并运用软件工程的专业知识将这些目标要求和符合性方法具体化。同时，为了便于表明对审定基础中有关软件要求的符合性，申请人还应参照上述表 A-1～A-10 的内容编制具体的“软件符合性检查单”并提交给审查人员。审查人员首先应注意审查软件审定计划，批准申请人所采用的符合性方法，然后审查软件开发过程和合成过程的符合性情况，其重点是评审和分析软件的可追踪性和可验证性，检查各项验证测试（必要时也包括试飞）的规程（程序）和结果以及对软件验证结果的覆盖分析等内容，以确保申请人:

①落实了对该软件的安全性考虑;

②加载了该软件的系统/设备符合安全性要求;

③能够持续地生产出经批准的软件产品。

注: 若申请人习惯于按照“需求评审阶段(RR)”、“初步设计评审阶段(PDR)”、“关键设计评审阶段(CDR)”、“试验准备评审阶段

(TRR)”和“首件检验阶段(FAI)”的“阶段”方式来表明对 DO-178B/ED-12B 的符合性，则其必须在软件审定计划中定义这些阶段与各软件生存时期过程的对应关系，并落实软件对所有相关目标的符合性。

6.3 对替代方法的说明

这里的替代方法是指能够被用来满足 DO-178B/ED-12B 的某个或某些目标要求的其它方法。替代方法不能脱离软件开发过程这个主线。需要说明的是，DO-178B/ED-12B 并不限制采用该标准以外的其它符合性方法来满足其目标要求。但在采用替代方法时，申请人应：

1. 表明该替代方法将满足 DO-178B/ED-12B 的某个或某些目标要求；
2. 在软件审定计划中表明该方法对软件开发过程和生存周期文档的影响以及采用该方法的合理性（即，表明采用该方法仍可满足系统的安全目标要求）；
3. 取得适航部门的认可；
4. 通过软件计划、规程和预期的结果以及该替代方法的使用证据来表明采用该方法的合理性。

目前，常见的替代方法有：可用于软件开发过程的形式法、可替代某一软件验证活动的穷举输入测试法、对多版本非相似软件的验证方法、可用于软件验证过程的软件可靠性模型以及产品的使用经验等。DO-178B/ED-12B 的 12.3 节给出了在采用这些替代方法时的指南。

对于从前按 DO-178A/ED-12A 所批准的早期软件而言，DO-178A/ ED-12A 也可被看作是一种替代的方法。但需要注意的是：由于 DO-178A/ED-12A 在有关用户可更改软件（如，数据库）、用户可选择的选装软件、软件开发和验证工具、从前开发的模块化软件以

及现场可加载软件等方面没能提供足够的符合性方法，故要使用这类的早期软件时，就必须按 DO-178B/ED-12B 中的相应要求来补充表明对有关适航要求的符合性。

6.4 对采用从前开发之软件的要求（含软件更改的情况）

在这里，从前开发的软件是指从前按 DO-178B/ED-12B 的生存周期过程或与之相等效的那些过程所开发的软件。

在采用这类软件时，将会涉及到下列的情况或其中的一部分：

- 因型号/系统的需要和使用的经验等，对从前开发的软件进行更改；
- 将已批准的某型航空器的软件用在其它的新型号上；
- 用在新的目标处理器（机）或新的硬件上，或与其它的新软件进行综合，以及更改软件的开发环境等；
- 因航空器改装等的需要，提高原有软件的开发基线（如，提高该软件的软件等级等）；
- 软件的配置管理过程和质量保证过程应计及对从前开发之软件的新应用。

DO-178B/ED-12B 的 12.1 节给出了有关上述情况的指南。

6.5 软件开发工具和验证工具的鉴定

软件工具可分为两类，一类为开发工具，另一类为验证工具。

当 DO-178B/ED-12B 中的方法和过程通过采用软件工具得以省略、简化或自动进行且不再按该标准的第 6 章进行验证时，就需要对这些软件工具进行鉴定。

对软件工具的鉴定是通过软件工具的鉴定过程来完成的。该过程的目标就是要确保软件工具所提供的置信度至少能够达到等效于DO-178B/ED-12B 中那些被该工具省略、简化或自动进行了的过程。

DO-178B/ED-12B 的 12.2 节提供了有关软件工具鉴定目标、准则、文档及其批准的指南。

7. 软件委任工程代表(DER)的工作和基本职责

在软件审查过程中，软件委任工程代表（简称，软件 DER）的工作就是通过评估软件的各生存周期过程及其符合性文档来确定软件是否符合审定基础的要求。具体内容包括:

- 评估软件计划、软件产品的具体标准和规程的符合性;
- 评估这些计划和规程在开发过程、验证过程、配置管理过程和质量保证过程中的实施情况;
- 协助 DMIR 确保质保系统对软件过程的监督和评审;
- 监督申请人解决在软件过程中和软件产品中所暴露出的符合性问题;
- 向适航部门提供软件的符合性证据等;

软件 DER 的基本职责包括:

- 监督软件过程及其输出对 DO-178B/ED-12B 的符合性;
- 参与评估与安全性相关的软件问题;
- 参与准备“软件实施概要”文档;
- 参与协调同适航部门的联络工作;
- 将适航部门所关心的软件问题通知申请人的供应商;
- 准备有关软件审查的支持性材料（如 DER 的工作记录、评审记录和试验观察记录等）并提交给适航部门;

- 参与准备关于系统的审定计划;
- 及时报告适航部门在软件过程中和软件产品中所发现的设计问题以及对这些问题的评估意见和纠正措施的建议等。

8. 软件质量保证

鉴于软件产品的特性， DO-178B/ED-12B 尤其强调了对软件设计及设计更改阶段的质量保证要求。

在软件质量保证的过程中，申请人的质保系统应按照经批准的软件质量保证计划，通过监督和评审软件的各生存周期过程及其输出来确保：在各过程中的缺陷或问题均能够被查出并得以评估、跟踪和解决，以及各软件过程的目标得以满足。由此，确保软件产品符合审定基础的要求。软件质量保证的工作目标包括：

- 从组织机构上和过程管理的程序上确保软件的开发过程和合成过程（包括对软件的更改）符合经批准的软件计划、具体标准和规程等;
- 在进/出每一个软件生存周期过程时确保满足相应的过程转换准则;
- 确保软件产品的符合性评审得以进行;
- 确保可持续地生产出经批准的软件产品。

软件质量保证活动与其它的质量保证活动一样，应具有相应的独立性和权威性，并应在其它软件生存周期过程的活动中发挥主动性。软件质量保证过程的具体工作详见DO-178B/ED-12B 的 8.2 和 8.3 节。

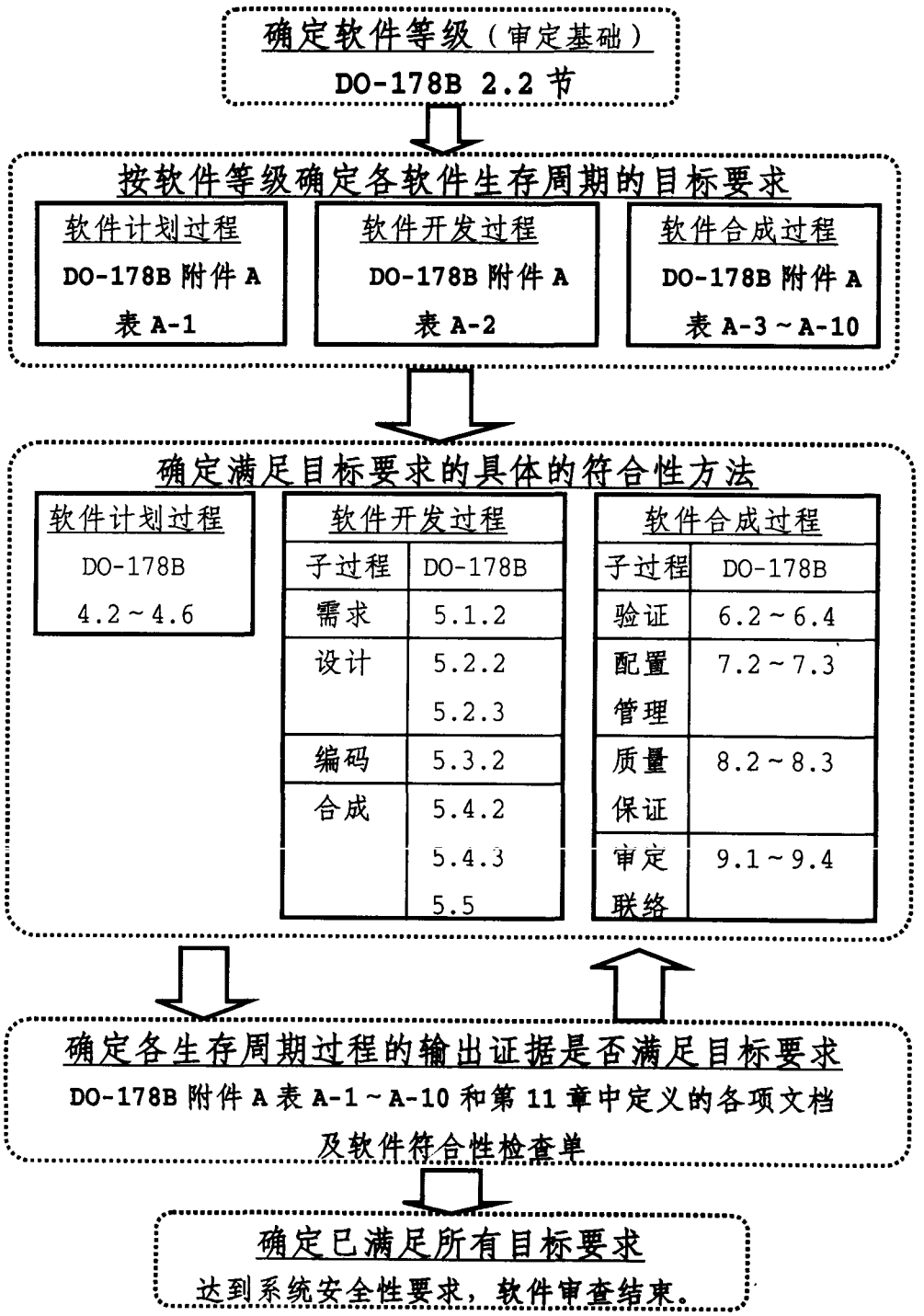

图 6-3 软件审查的基本流程和方法

9. 附录—DO-178B/ED-12B 附件 A 表 A1 ~ A10

表 A-1 软件计划过程

序号	目标要求		对各软件等级的适用性				输出的文档	对各软件等级输出文档的控制类别				
	说明	条目	A	B	C	D	说明	条目	A	B	C	D
1	开发过程和合成过程的活动得以定义	4.1a 4.3	○	○	○	○	软件审定计划 软件开发计划 软件验证计划	11.1 11.2 11.3	① ① ①	① ① ①	① ② ②	① ② ②
2	过程间的转换准则、相互关系和顺序得以定义	4.1b 4.3	○	○	○		软件配置管理(SCM)计划	11.4	①	①	②	②
3	软件生存周期环境得以定义	4.1c	○	○	○		软件质量保证(SQA)计划	11.5	①	①	②	②
4	其它必须考虑的因素得以表明	4.1d	○	○	○	○						
5	软件的开发标准得以定义	4.1e	○	○	○		软件需求标准 软件设计标准 软件编码标准	11.6 11.7 11.8	① ① ①	① ① ①	② ② ②	
6	各软件计划符合DO-178B标准	4.1f 4.6	○	○	○		SQA记录 软件验证结果	11.19 11.14	② ②	② ②	② ②	
7	各软件计划是相互协调的	4.1g 4.6	○	○	○		SQA记录 软件验证结果	11.19 11.14	② ②	② ②	② ②	

说明：“条目”—指DO-178B中的章节号；
“●”—指目标应在独立性的条件下予以满足；
“○”—指目标应予以满足；
“空格”—指可由申请人决定是否要满足目标的要求；
“①”—指文档应满足1类控制要求；
“②”—指文档应满足2类控制要求。

（注：独立性是指为确保实施目标评定的某种责任分工。对于软件验证过程而言，当被验证项是由不负责该项目开发的人员来进行验证时就满足了独立性的条件，并且，可使用验证工具来达到等效于人工验证的独立性。对于软件质量保证过程而言，还包括了确保纠正措施的权力。）

表 A-2 软件开发过程

序号	目标要求		对各软件等级的适用性				输出的文档	对各软件等级输出文档的控制类别				
	说明	条目	A	B	C	D	说明	条目	A	B	C	D
1	高级需求得以开发	5.1.1a	○	○	○	○	软件需求文档	11.9	①	①	①	①
2	派生的高级需求得以定义	5.1.1b	○	○	○	○	软件需求文档	11.9	①	①	①	①
3	软件的架构得以开发	5.2.1a	○	○	○	○	软件设计文档	11.10	①	①	②	②
4	低级需求得以开发	5.2.1a	○	○	○	○	软件设计文档	11.10	①	①	②	②
5	派生的低级需求得以定义	5.2.1b	○	○	○	○	软件设计文档	11.10	①	①	②	②
6	源代码得以开发	5.3.1a	○	○	○	○	源代码	11.11	①	①	①	①
7	生成可执行目标代码并在目标计算机上得以综合	5.4.1a	○	○	○	○	可执行目标代码	11.12	①	①	①	①

说明：“条目”—指 DO-178B 中的章节号；
“●”—指目标应在独立性的条件下予以满足；
“○”—指目标应予以满足；
“空格”—指可由申请人决定是否要满足目标的要求；
“①”—指文档应满足 1 类控制要求；
“②”—指文档应满足 2 类控制要求。

（注：独立性是指为确保实施目标评定的某种责任分工。对于软件验证过程而言，当被验证项是由不负责该项目开发的人员来进行验证时就满足了独立性的条件，并且，可使用验证工具来达到等效于人工验证的独立性。对于软件质量保证过程而言，还包括了确保纠正措施的权力。）

表 A-3 对软件需求过程输出的验证

序号	目标要求		对各软件等级的适用性				输出的文档	对各软件等级输出文档的控制类别				
	说明	条目	A	B	C	D	说明	条目	A	B	C	D
1	高级需求符合系统需求	6.3.1a	●	●	○	○	软件验证结果	11.14	②	②	②	②
2	高级需求是准确的和协调一致的	6.3.1b	●	●	○	○	软件验证结果	11.14	②	②	②	②
3	高级需求与目标计算机是兼容的	6.3.1c	○	○			软件验证结果	11.14	②	②		
4	高级需求是可验证的	6.3.1d	○	○	○		软件验证结果	11.14	②	②	②	
5	高级需求符合标准要求	6.3.1e	○	○	○		软件验证结果	11.14	②	②	②	
6	高级需求可追踪到系统需求	6.3.1f	○	○	○	○	软件验证结果	11.14	②	②	②	②
7	算法是准确的	6.3.1g	●	●	○		软件验证结果	11.14	②	②	②	

说明：“条目”—指 DO-178B 中的章节号；
“●”—指目标应在独立性的条件下予以满足；
“○”—指目标应予以满足；
“空格”—指可由申请人决定是否要满足目标的要求；
“①”—指文档应满足 1 类控制要求；
“②”—指文档应满足 2 类控制要求。

（注：独立性是指为确保实施目标评定的某种责任分工。对于软件验证过程而言，当被验证项是由不负责该项目开发的人员来进行验证时就满足了独立性的条件，并且，可使用验证工具来达到等效于人工验证的独立性。对于软件质量保证过程而言，还包括了确保纠正措施的权力。）

表 A-4 对软件设计过程输出的验证

序号	目标要求		对各软件等级的适用性				输出的文档	对各软件等级输出文档的控制类别				
	说明	条目	A	B	C	D	说明	条目	A	B	C	D
1	低级需求符合高级需求	6.3.2a	●	●	○		软件验证结果	11.14	②	②	②	
2	低级需求是准确的和协调一致的	6.3.2b	●	●	○		软件验证结果	11.14	②	②	②	
3	低级需求与目标计算机兼容	6.3.2c	○	○			软件验证结果	11.14	②	②		
4	低级需求是可验证的	6.3.2d	○	○			软件验证结果	11.14	②	②		
5	低级需求符合标准要求	6.3.2e	○	○	○		软件验证结果	11.14	②	②	②	
6	低级需求可追踪到高级需求	6.3.2f	○	○	○		软件验证结果	11.14	②	②	②	
7	算法是准确的	6.3.2g	●	●	○		软件验证结果	11.14	②	②	②	
8	软件架构与高级需求兼容	6.3.3a	●	○	○		软件验证结果	11.14	②	②	②	
9	软件架构是协调一致的	6.3.3b	●	○	○		软件验证结果	11.14	②	②	②	
10	软件架构与目标计算机兼容	6.3.3c	○	○			软件验证结果	11.14	②	②		
11	软件架构是可验证的	6.3.3d	○	○			软件验证结果	11.14	②	②		
12	软件架构符合标准要求	6.3.3e	○	○	○		软件验证结果	11.14	②	②	②	
13	软件分区的完整性得以确认	6.3.3f	●	○	○	○	软件验证结果	11.14	②	②	②	②

说明：“条目”—指 DO-178B 中的章节号；
“●”—指目标应在独立性的条件下予以满足；
“○”—指目标应予以满足；
“空格”—指可由申请人决定是否要满足目标的要求；
“①”—指文档应满足 1 类控制要求；
“②”—指文档应满足 2 类控制要求。

表 A-5 对软件编码及综合过程输出的验证

序号	目标要求		对各软件等级的适用性				输出的文档	对各软件等级输出文档的控制类别				
	说明	条目	A	B	C	D	说明	条目	A	B	C	D
1	源代码符合低级需求	6.3.4a	●	●	○		软件验证结果	11.14	②	②	②	
2	源代码符合软件架构	6.3.4b	●	○	○		软件验证结果	11.14	②	②	②	
3	源代码是可验证的	6.3.4c	○	○			软件验证结果	11.14	②	②		
4	源代码符合标准要求	6.3.4d	○	○	○		软件验证结果	11.14	②	②	②	
5	源代码可追踪到低级需求	6.3.4e	○	○	○		软件验证结果	11.14	②	②	②	
6	源代码是准确的和协调一致的	6.3.4f	●	○	○		软件验证结果	11.14	②	②	②	
7	软件综合过程的输出是完整的和正确的	6.3.5	○	○	○		软件验证结果	11.14	②	②	②	

说明：“条目”—指 DO-178B 中的章节号；
“●”—指目标应在独立性的条件下予以满足；
“○”—指目标应予以满足；
“空格”—指可由申请人决定是否要满足目标的要求；
“①”—指文档应满足 1 类控制要求；
“②”—指文档应满足 2 类控制要求。

表 A-6 对软件综合过程输出的测试

序号	目标要求		对各软件等级的适用性				输出的文档	对各软件等级输出文档的控制类别				
	说明	条目	A	B	C	D	说明	条目	A	B	C	D
1	可执行目标代码符合高级需求	6.4.2.1 6.4.3	○	○	○	○	软件验证用例及规程 软件验证结果	11.13 11.14	① ②	① ②	② ②	② ②
2	可执行目标代码对于高级需求是健壮的	6.4.2.2 6.4.3	○	○	○	○	软件验证用例及规程 软件验证结果	11.13 11.14	① ②	① ②	② ②	② ②
3	可执行目标代码符合低级需求	6.4.2.1 6.4.3	●	●	○		软件验证用例及规程 软件验证结果	11.13 11.14	① ②	① ②	② ②	
4	可执行目标代码对于低级需求是健壮的	6.4.2.2 6.4.3	●	○	○		软件验证用例及规程 软件验证结果	11.13 11.14	① ②	① ②	② ②	
5	可执行目标代码与目标计算机是兼容的	6.4.3a	○	○	○	○	软件验证用例及规程 软件验证结果	11.13 11.14	① ②	① ②	② ②	② ②

说明：“条目”—指 DO-178B 中的章节号；
“●”—指目标应在独立性的条件下予以满足；
“○”—指目标应予以满足；
“空格”—指可由申请人决定是否要满足目标的要求；
“①”—指文档应满足 1 类控制要求；
“②”—指文档应满足 2 类控制要求。

表 A-7 对软件验证过程结果的验证

序号	目标 要求		对各软件等级的适用性				输出的 文 档	对各软件等级输出文档的控制类别				
	说 明	条 目	A	B	C	D	说 明	条目	A	B	C	D
1	测试规程是正确的	6.3.6b	●	○	○		软件验证用例及规程	11.13	②	②	②	
2	测试结果是正确的且差异得到了解释	6.3.6c	●	○	○		软件验证结果	11.14	②	②	②	
3	实现了对高级需求的测试覆盖	6.4.4.1	●	○	○	○	软件验证结果	11.14	②	②	②	②
4	实现了对低级需求的测试覆盖	6.4.4.1	●	○	○		软件验证结果	11.14	②	②	②	
5	实现了对软件结构的测试覆盖（经调整的条件/判定）	6.4.4.2	●				软件验证结果	11.14	②			
6	实现了对软件结构的测试覆盖（判定覆盖）	6.4.4.2a 6.4.4.2b	●	●			软件验证结果	11.14	②	②		
7	实现了对软件结构的测试覆盖（语句覆盖）	6.4.4.2a 6.4.4.2b	●	●	○		软件验证结果	11.14	②	②	②	
8	实现了对软件结构的测试覆盖（数据耦合及控制耦合）	6.4.4.2c	●	●	○		软件验证结果	11.14	②	②	②	

说明：“条目”—指 DO-178B 中的章节号；
“●”—指目标应在独立性的条件下予以满足；
“○”—指目标应予以满足；
“空格”—指可由申请人决定是否要满足目标的要求；
“①”—指文档应满足 1 类控制要求；
“②”—指文档应满足 2 类控制要求。

表 A-8 软件配置管理过程

序号	目标要求		对各软件等级的适用性				输出的文档	对各软件等级输出文档的控制类别				
	说明	条目	A	B	C	D	说明	条目	A	B	C	D
1	配置项得以标识	7.2.1	○	○	○	○	软件配置管理(SCM)记录	11.18	②	②	②	②
2	基线和可追踪性得以确立	7.2.2	○	○	○	○	软件配置索引 软件配置管理(SCM)记录	11.16 11.18	① ②	① ②	① ②	① ②
3	问题报告、更改控制、更改评估和配置状态记录得以确定	7.2.3 7.2.4 7.2.5 7.2.6	○	○	○	○	问题报告 软件配置管理(SCM)记录	11.17 11.18	② ②	② ②	② ②	② ②
4	归档、检索和发放得以确定	7.2.7	○	○	○	○	软件配置管理(SCM)记录	11.18	②	②	②	②
5	软件的加载控制得以确定	7.2.8	○	○	○	○	软件配置管理(SCM)记录	11.18	②	②	②	②
6	对软件生存周期环境的控制得以确定	7.2.9	○	○	○	○	软件生存周期环境配置索引 软件配置管理(SCM)记录	11.15 11.18	① ②	① ②	① ②	② ②

说明：“条目”—指 DO-178B 中的章节号；
“●”—指目标应在独立性的条件下予以满足；
“○”—指目标应予以满足；
“空格”—指可由申请人决定是否要满足目标的要求；
“①”—指文档应满足 1 类控制要求；
“②”—指文档应满足 2 类控制要求。

表 A-9 软件质量保证过程

序号	目标要求		对各软件等级的适用性				输出的文档	对各软件等级输出文档的控制类别				
	说明	条目	A	B	C	D	说明	条目	A	B	C	D
1	软件开发过程及软件合成过程符合经批准的各软件计划和标准是得到确保的	8.1a	●	●	●	●	软件质量保证(SQA)记录	11.19	②	②	②	②
2	各软件生存周期过程的转换准则得以满足是得到确保的	8.1b	●	●			软件质量保证(SQA)记录	11.19	②	②		
3	软件的符合性评估得到实施	8.1c 8.3	●	●	●	●	软件质量保证(SQA)记录	11.19	②	②	②	②

说明：“条目”—指 DO-178B 中的章节号；
“●”—指目标应在独立性的条件下予以满足；
“○”—指目标应予以满足；
“空格”—指可由申请人决定是否要满足目标的要求；
“①”—指文档应满足 1 类控制要求；
“②”—指文档应满足 2 类控制要求。

表 A-10 审定联络过程

序号	目标要求		对各软件等级的适用性				输出的文档	对各软件等级输出文档的控制类别				
	说明	条目	A	B	C	D	说明	条目	A	B	C	D
1	申请人与适航部门之间的相互交流和理解得以确立	9.0	○	○	○	○	软件审定计划	11.1	①	①	①	①
2	提出了建议的符合性方法，并且就软件审定计划达成了一致	9.1	○	○	○	○	软件审定计划	11.1	①	①	①	①
3	符合性证据得以提供	9.2	○	○	○	○	软件实施概要 软件配置索引	11.20 11.16	① ①	① ①	① ①	① ①

说明：“条目”—指 DO-178B 中的章节号；
“●”—指目标应在独立性的条件下予以满足；
“○”—指目标应予以满足；
“空格”—指可由申请人决定是否要满足目标的要求；
“①”—指文档应满足 1 类控制要求；
“②”—指文档应满足 2 类控制要求。