民用客机机载软件SOI评审初探

SOI Review for Civil Aircraft Airborne Software

陈一可／中国商飞上海飞机设计研究院

摘　要：依据民航对机载软件SOI的相关定义和指导性文件的解读，结合某型号民机审定经验，阐述了机载软件SOI评审的定义和执行方法等内容。

关键词：机载软件；阶段介入性评审；DO−178B目标
Keywords：airborne software；SOI；DO−178B objectives

1 SOI的定义

SOI（Stage of Involvement）称为阶段介入性评审，是美国联邦航空局（FAA）为了监控软件的生命周期过程，并确定其与DO−178B的符合性而定义的对机载软件的过程监控的评审方式。它是FAA颁布的关于机载软件批准方面的指南，面向的群体是FAA审查人员及具有软件授权的工程委任代表（DER），文件内容主要包括对上述人员在软件审查过程中需要进行的一系列活动的指导，以及一些特殊的审查考虑。

FAA Order 8110.49第2章“软件评审过程（Software Review Process）”中对SOI评审进行了明确定义，共分为4个阶段。

SOI#1——软件计划阶段评审（Software Planning Review）；

SOI#2 ——软件开发阶段评审（Software Development Review）；

SOI#3——软件验证阶段评审（Software Verification Review）；

SOI#4——软件最终审定评审（Final Certification Software Review）。

2 SOI的具体过程

2.1 软件计划阶段评审

软件计划阶段评审（SOI#1）是局方对软件介入的首次审核，主要针对软件的各类计划进行评审。当然作为计划的一部分，一些开发标准也是包括在这个评审中的。因此SOI#1主要评审的数据是DO−178B中定义的软件计划文件，包括以下几方面。

1）软件合格审定计划（PSAC）；

2）软件开发计划（SDP）；

3）软件验证计划（SVP）；

4）软件构型管理计划（SCMP）；

5）软件质量保证计划（SQAP）；

6）工具鉴定计划（TQP）（视情况需要）；

7）开发标准，包括软件需求标准，软件设计标准，软件编码标准。

而上述评审数据的重点是PSAC，由于PSAC是局方至少需要批准的三份数据之一（其余两份是SCI和SAS，后文将有介绍），同时PSAC可以说是对整个软件计划的汇总，是其他计划和标准文件的总纲。因此PSAC得到局方批准是SOI#1完成的重要指标之一。

SOI#1的最终目的是要满足DO−178B 附录A Table A−1“计划相关”的所有目标、Table A−8“构

案，液压能源系统所有元件以及管路都不从客舱和驾驶舱经过，保证了防火安全性，符合条款要求。

3 结论

综上所述，液压能源系统的防火适航条款均有相应的措施表明其符合性，符合性验证工作还需通过详细的计算分析、试验验证、符合性检查等方法来实现。由于适航条款仅是型号设计过程中保证安全性的最低要求。本文从适航条款方面来说明该型号民机的液压系统防火设计满足基本要求，所以该型号飞机的更高安全性要求必须通过更详细更严谨的适航验证工作来体现。 AST

参考文献

[1] CCAR−25R4中国民用航空规章第25部运输类飞机适航标准[S]. CAAC.

作者简介

张瑞华，助理工程师，主要从事液压系统设计适航工作。

型管理相关”（目标 1–4）、Table A–9“质量保证相关”（目标 1）和 Table A–10“合格审定相关”（目标 1–2），同时软件的级别已经通过系统安全性分析过程确定（在系统初步安全性分析文件PSSA中落实）。

2.2 软件开发阶段评审

SOI#2主要是评估及检查软件的开发过程是否按照SOI#1已经确定的软件计划执行、开发出了软件实体数据，主要包括软件高级别需求（SRD）、软件设计（SDD）即软件低级别需求和架构、源代码，以及上述数据相关的评审和分析记录。

SOI#2的目的是评估与DO–178B Table A–2（目标1–6）、Table A–3和Table A–4所有目标、Table A–5（目标1–6）、Table A–8（目标1–4，6）、Table A–9（目标1–2）和Table A–10（目标1–2）的符合性。从评估的目标看出，FAA规定的SOI#2没有包括对可执行代码的产生和相关验证提出要求。这部分将在SOI#3进行评估。

SOI#2的评审主要以线性评审（Thread Review）的方式进行，即对软件需求、设计、代码和验证结果按照追溯性关系进行抽样检查。抽样必须覆盖所有的功能模块，同时兼顾高危害级别失效事件相关的需求。

2.3 软件验证阶段评审

SOI#3是重点评估生成的软件产品（主要是可执行代码）是否满足软件产品需求（主要是软件各层级需求）。而对这一目标的验证方法主要是对可执行代码的测试，以及对测试结果的分析。所以SOI#3所需要评估的数据主要包括软件需求数据（SRD）、软件设计数据（SDD）、测试用例及程序（Test Cases and Procedures）、验证结果（VR），特别注意对需求覆盖性和结构覆盖性的分析。

SOI#3需要评估的DO–178B目标包括Table A–5 目标7，Table A–6、A–7和A–8所有目标，Table A–9 目标1–2和Table A–10所有目标。

SOI#3评审同样可以采用线性评审的方式进行，抽样准则与SOI#2一致。

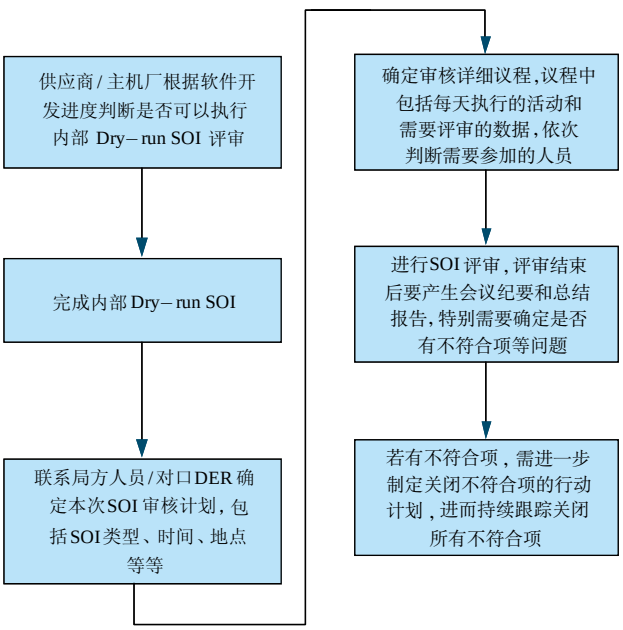

图1 建议性SOI执行流程

2.4 软件最终审定评审

SOI#4作为最后一阶段性评审，可以理解为对所有已完成工作的确认和复查，确定所有DO–178B规定的、计划文件中定义的活动都已经完成，并且有相应的证据结果纳入了正式的构型控制下。检查重点是SOI#3完成后进行的软件验证结果，确保其实现所有需求和设计完成所有计划中定义的活动、满足所有的DO–178B目标。

着重评审的数据是软件构型索引（SCI）和软件完成综述（SAS），保证完成活动软件的符合性评审，也就是DO–178B附录A 从Table A–1到A–10的所有目标的符合性评审。因此，SCI和SAS的批准可作为SOI#4完成的标志性事件。

3 总结

尽管正式的SOI评审是适航当局的行为，但一般在局方执行SOI评审前，主机厂或供应商可按照SOI审查思路进行内部预备SOI评审（Dry–run SOI），以提前发现问题、解决问题，更好地完成符合性验证，具体流程可参考图1。

值得注意的是，SOI仅仅只是软件开发过程中符合性评审的形式之一，主机厂还应有其他形式的活动介入供应商的软件研发过程中以监控其过程，如远程评审、Peer Review等方式，主旨都是围绕软件的符合性数据和DO–178B目标。如果主机厂能够派出具备DER资质的人员或非常熟悉系统或软件的工程师与软件开发商一同工作，在软件开发过程中实时介入，更是行之有效的监控方法。 AST

参考文献

[1] FAA Order 8110.49—Software approval guidelines[Z].FAA, 2003–6.

作者简介

陈一可，助理工程师，主要负责机载软件管理工作。