SAACC
民航上海审定中心

2018

从规章到代码 – 适航浅谈

中国民用航空上海航空器适航审定中心

2018.12.3

00 自我介绍

李煜

2005年~2009年 东南大学 电气工程学院 本科

2009年~2012年 上海交通大学 航空航天学院 硕士

2012年~2018年 昂际航电 工程师

显示系统软件开发工程师

IMA系统软件验证工程师

IMA软件工具开放工程师

IMA系统安全性分析工程师

2018年 民航上海航空器适航审定中心 电子电气专业 审查员

SAACC
民航上海审定中心

PART 1
从规章到代码

00 关于题目和分享会目标

你很难从本次分享会学习到：

1） 适航法规和适航体系

2） DO-178B的具体内容

希望你从这次分享会学习或体会到：

从规章到代码

从哪里来，到哪里去

以25部1309条款和
DO178B 标准为例

00 目录和大纲

1） 航空规章
2） 咨询公告-审定程序
3） 系统开发的方法 – ARP4754A
4） 系统安全性分析的方法 - ARP4761
5） 引入错误的根本原因
6） 研制保证等级
7） 软件研制的方法 – DO-178B

00 航空规章

问题讨论：

如果交大的某一个同学，自己在宿舍或者实验室造了一架飞机出来，准备自己开出去飞了玩，请问他需要申请适航证吗？

如果这位同学准备驾驶这架自己造的飞机带着女朋友或者男朋友出去飞？需要申请适航证吗？

如果这位同学准备驾驶这架自己造的飞机带着全班同学出去旅行？需要申请适航证吗？

00 航空规章 – 责任

航空规章适航规章

- 政府代表公众利益
- 最低的安全和性能标准
- 行业良性发展的规范

适航规章 – 审定基础

- CCAR-25，CCAR-91，CCAR-121， CCAR-145

00 25部 1309条

(a) 凡航空器适航标准对其功能有要求的设备、系统及安装，其设计必须保证在各种可预期的运行条件下能完成预定功能。

(b) 飞机系统与有关部件的设计，在单独考虑以及与其它系统一同考虑的情况下，必须符合下列规定：

(1) 发生任何妨碍飞机继续安全飞行与着陆的失效状态的概率为极不可能；

(2) 发生任何降低飞机能力或机组处理不利运行条件能力的其它失效状态的概率为不可能。

(c) 必须提供警告信息，向机组指出系统的不安全工作情况并能使机组采取适当的纠正动作。系统、控制器件和有关的监控与警告装置的设计必须尽量减少可能增加危险的机组失误。

(d) 必须通过分析，必要时通过适当的地面、飞行或模拟器试验，来表明符合本条（b）的规定。这种分析必须考虑下列情况：

(1) 可能的失效模式，包括外界原因造成的故障和损坏；

(2) 多重失效和失效未被检测出的概率；

(3) 在各个飞行阶段和各种运行条件下，对飞机和乘员造成的后果；

(4) 对机组的警告信号，所需的纠正动作，以及对故障的检测能力。

00 咨询公告和审定程序

咨询公告（AC）：

告知申请人认可某一种方法（但不是唯一的方法）作为满足条款的证据。

审定程序（AP or Order）：

告知审查人如何审批申请人提供的证据，以确定其是否符合条款的要求。

举例：

AC_25.1309-1A 认可SAE ARP4754A 是满足25.1309条款的一种方法。

AC_20-115C 认可RTCA DO 178C 是满足25.1309条款关于软件的一种方法。

AC_20-153B 认可 RTCA-DO 200B 是满足25.1309条款关于航空数据库条一种方法。

FAA_Order_8110_105A 是指导审查人员审查DO-254硬件符合性证据的指导

00 SAE ARP4754A

CCAR 25.1309 | AC_25.1309-1A | SAE ARP4754A

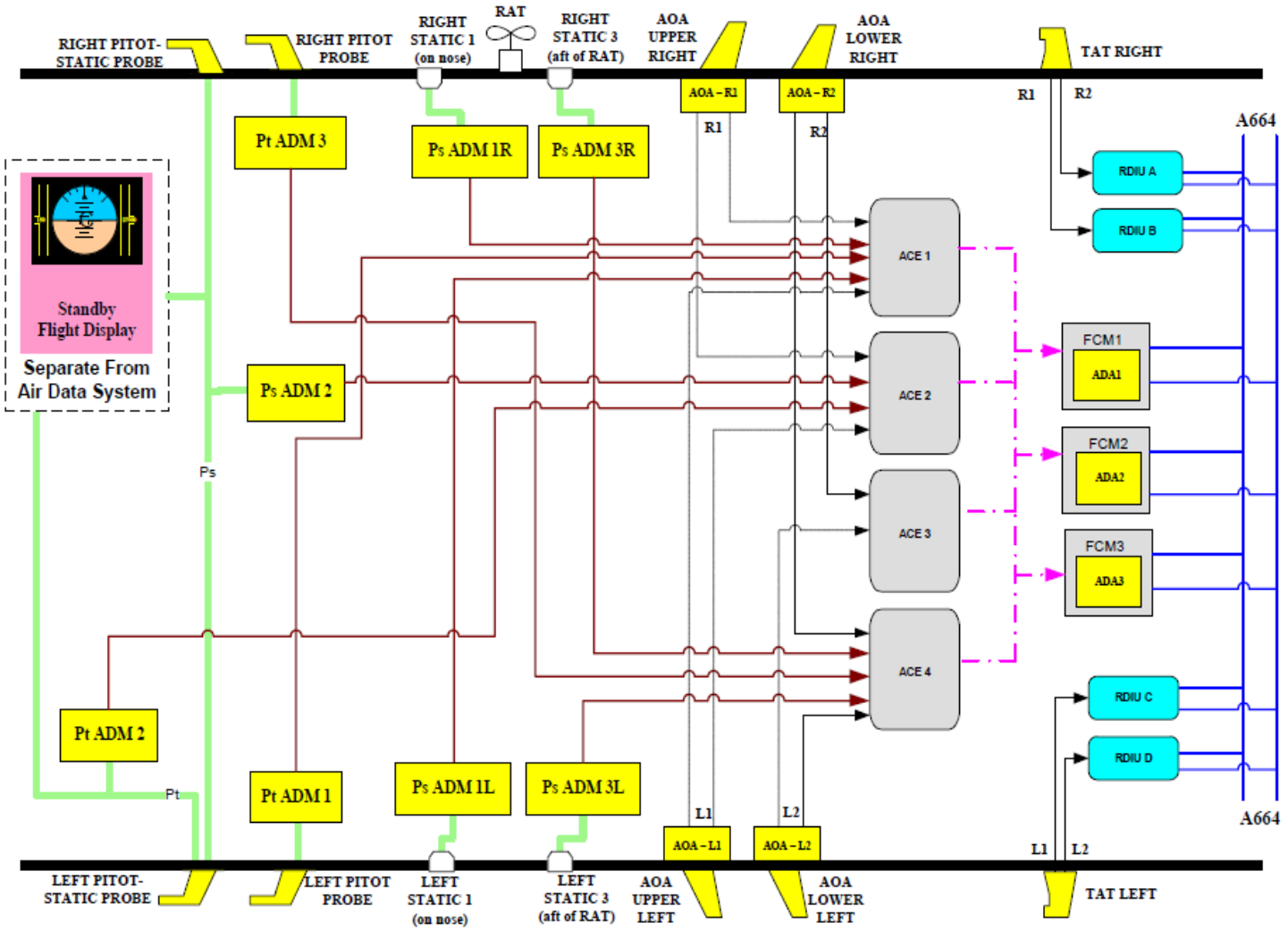
ARP4754A - 以系统安全性为目标，指导民用飞机和航空系统开发的指南。

核心的概念：

1） 系统功能 – 系统的需求
2） 系统功能的安全性目标 – 系统功能的失效状态
3） 系统架构 - 系统设计
4） 各个设备或者组件 – 硬件或者软件

00

SAE ARP4754A
大气系统 ADS



系统功能

F01: 提供空速

功能失效的危害分析

FC01-01：完全丧失空速

FC01-02：提供错误的空速

系统架构

空速管数量，表决逻辑

安全性目标

部件（软件或者硬件）

失效概率，研制保证等级

SAACC
Shanghai Aircraft Airworthiness Certification Center of CAAC

00 SAE ARP4761

安全性目标

部件（软件或者硬件）
失效概率，研制保证等级

失效概率 vs 研制保证等级

导致失效的两种原因：

1）硬件的随机失效 （equipment random hardware failure ）
2）在开发过程中人为引入错误导致的失效

减缓这两种诱因的方法：

1）设计 - 架构和分析
2）开发严格程度 （development rigor）

00 DO-178B/C

核心：

DO 178B/C 的核心主题是在预先已经确定了安全性需求的前提下，如何开展研制方面的保证已经相应的测试。

DO 178B/C 是基于过程保证，面向目标的研制保证方法。

按照相应研制保证等级DAL-A来开发的软件，可认为由于开发过程引入错误的概率低于 1E-9/PFH

CCAR 25.1309

AC_25.1309-1A

AC_20-115B/C

AC_20-152

SAE ARP4754A

SAE ARP4761

DO-178B/C

DO-254

SAACC
民航上海审定中心

PART 2
从规章到代码 – DO 178B

00 任务讨论

任务讨论：

系统工程师分配给软件工程师一个任务，这个任务是这样子的：
软件应在用户按下回车键的时候，在屏幕上显示“Hello World！ “

动手直接写了呗，5分钟搞定。

写软件就是小菜一碟，写报告才是头大啊

完全写不来，发到BBS上 求大神帮忙?

找一个上一届师兄写好的，照抄一下。

跟同桌商量一下，等我写好了，请他帮我看看。

发邮件跟老师确认一下，真有那么简单?

00 计划 planning

软件合格审定计划PSAC

对接系统开发的分配给软件的安全性目标，适航合格审定的基础

软件开发计划 SDP

对所有软件开发活动的计划，定义目标和需求，开发方法，如何设计，最后的成果

软件验证计划 SVP

对所有软件验证活动的计划，独立性要求，验证方法，编译环境，多版本非相似

软件构型管理计划 SCMP

对所有软件构型管理活动的计划，版本管理，变更控制，评审，供应商管理

软件过程保证计划 SQAP

对所有软件过程保证活动的计划，过程执行的审计，记录

00 标准 standard

软件需求标准

需求层级定义，符号的定义，格式的定义，衍生需求的反馈等

软件设计标准

设计表述的方法，命名规则，中断使用，全局变量的限制，异常的处理

设计的工具，循环数量，指针使用

软件编码标准

编码语言的限制，最大代码行数，缩进空格数，源代码的文档化表示

变量的命名规则，子函数的限制，数据耦合程度的限制。

00 开发 Development

软件需求文档

软件高层需求

软件设计文档

软件架构描述和软件低层需求文档

软件源代码

源代码，编译文件，链接文件等。

软件可执行代码

可在目标机器上执行的代码

00 验证 Verification
确认 Validation

确认(Validation)的方法有哪些?

评审，分析，仿真

验证(Verification)的方法有哪些?

评审，分析，测试

软件验证的用例和规程

a) 评审和分析的规程

b) 测试用例

c) 测试规程

软件验证的结果

a) 评审记录，

b) 分析记录

c) 测试记录

00 验证 Verification
确认 Validation

需要进行确认的生命周期数据

a) 所有计划文档
   - 评审
b) 所有需求文档和设计文档 -
   - 评审或者仿真（工具）
c) 所有的软件源代码
   - 评审 (工具)

需要进行验证的生命周期数据

a) 可执行代码满足需求
   - 测试
b) 可执行代码需求覆盖
   - 分析（基于追溯性）
c) 可执行代码的结构覆盖
   - 分析 （工具）
d) 高层需求，设计表述，低层需求，代码之间的追溯性
   - 分析 （工具）

00 MCDC

结构覆盖分析 Structure Coverage Analysis

对于A级软件，其结构覆盖率是要求 修正判定条件覆盖 (MCDC) 达到100%的。

00 构型管理 configuration management

软件构型索引

软件高层需求

问题汇报机制

软件架构描述和软件低层需求文档

构型管理记录

软件架构描述和软件低层需求文档

00 质量保证 quality assurance

问题讨论：

00 审定联络 Certification Liaison

符合性方法和计划

PSAC 的沟通和批准

符合性证据

局方进行数据的评审和现场的审计

向局方递交符合性的数据

1) PSAC
2) SCI
3) SAS


SAACC
民航上海审定中心
THANK YOU
谢谢