http://myfj.cnjournals.com myfj_sadri@comac.cc (021)20866796

DOI: 10.19416/j.cnki.1674-9804.2020.03.008

安全性分析在通用飞机航电系统架构设计中的应用

王焱滨* 曾 强

(中电科航空电子有限公司,成都 611731)

摘 要: 本文通过研究通用飞机航电系统的基本功能需求和系统特点,总结了通用飞机航电系统的基本组成。通过对相关适航规章的分析,研究了大气、航姿、通信、导航、监视等典型功能失效状态的分类要求;针对典型的II类涡轮螺旋桨式通用飞机,以满足功能失效概率要求为目标,采用故障树分析手段,研究了航电系统主要功能的备份需求,由此得出系统的基本逻辑架构。

关键词: 通用飞机;航空电子系统;安全性分析;故障树;备份需求;系统架构

中图分类号: V243 **文献标识码:** A **OSID:**

0 引言

据统计,目前全球通用飞机大约占民用飞机数量的90%,而90%的通用飞机注册在美国和欧洲地区,尤其是美国,通用航空产业非常成熟。虽然我国的通用航空产业当前还处于起步阶段,但是在市场需求的推动下,随着低空的逐步开放,通用航空产业面临巨大的发展机遇。

航电系统是通用飞机的重要组成部分,安全可靠、经济舒适的航电系统是飞机市场竞争力的重要保证。目前国外有多家供应商,可以提供通用飞机航电系统产品,比较典型的如 Garmin 公司的 G1000、Avidyne 公司的 Entegra、Honeywell 公司的 Primus Apex 以及 L-3 公司的 SmartDeck 等。不同种类通用飞机的航电系统架构差异很大[1-4],如 Honeywell 的 Primus Apex 系统,采用集成模块化航电(Integrated Modular Avionics,简称 IMA)架构,模块化航电单元(Modular Avionics Units,简称 MAU)是系统的处理核心;GARMIN 的 G1000 系统[5]采用显示和处理功能合二为一的综合显示器,综合显示器是系统处理核心,通过综合无线电设备外接大气、航姿、航管等外围传感器;AVIDYNE 的 Entegra 系统是以两个综合飞行显示器(包含液晶显示模块与机箱,机箱中包括核心处理、大气航姿、通信导航、接口等模块)为核心,通过接口模块扩展其他功能。因此,首先需要根据飞机的种类和特点以及用户的不同需求,确定其航电系统架构。不管是 25 部飞机还是 23 部飞机,其航电系统的开发时均是多阶段反复迭代的 V 形过程[6],在这个过程中,系统的设计就是各层需求的分解和定义过程,而安全性分析是系统需求分解和架构设计中需要依据的重要手段。近年来国内一些单位虽然开展了通用飞机航电的研究,但主要是针对国外典型产品;在系统架构设计上,目前尚无文献针对通用飞机航电系统的特点,从安全性分析的角度对其主要功能的冗余备份需求进行系统的论证。

本文按照适航研制要求,以对通用飞机航电系统的基本功能需求、系统特点和基本组成的研究为切入点,通过对 CCAR-23 部适航规章[7]及其 AC23.1309-1E 咨询通告[8]的分析,研究其功能失效状态的分类要求;针对典型的 II 类涡轮螺旋桨式飞机,通过故障树分析对系统各主要功能

* 通信作者. E-mail: wangyb@cetca.net.cn

引用格式: 王焱滨,曾强. 安全性分析在通用飞机航电系统架构设计中的应用[J]. 民用飞机设计与研究,2020(3):42-48.
WANG Y B, ZENG Q. Application of safety analysis in the design of general aircraft avionics system architecture[J]. Civil Aircraft Design and Research,2020(3):42-48(in Chinese).

的备份策略进行研究，由此探讨了通用飞机航电系统的基本逻辑架构。

1　通用飞机航电系统功能需求及实现特点

1.1 功能需求

通用飞机航电系统主要包括驾驶舱显示控制以及外围传感器等部分，其主要系统功能需求如表 1 所示。

表 1　系统功能需求

需求种类	功能要求
显示大气数据信息功能	空速、高度、爬升速度等大气数据信息
显示姿态信息功能	俯仰、滚转等姿态信息
显示导航信息功能	航向、航道、航道偏离、飞行计划、导航台、机场、空域、航路点、航图等导航信息
显示飞机参数信息功能	发动机和燃油等参数信息
导航功能	卫星导航及地基导航，一般采用的导航手段为 GPS、甚高频全向信标（VHF Omni-directional Range，简称 VOR）、仪表着陆系统（Instrument Landing System，简称 ILS）、无线电信标等
通信功能	机内通话、与地面及其他飞机之间的 VHF 话音通信以及广播等功能
监视功能	提供监视本机的手段，一般采用 S 模式航管应答
备份仪表功能	地平仪、气压高度表、空速表、磁罗盘等
告警功能	通过声音、显示、灯光实现飞机系统故障告警
可扩展功能	自动相关监视、北斗短报文、近地告警、防撞告警、合成视景、自动驾驶、测距器等功能

1.2 实现特点与系统组成

与运输类飞机一样，通用飞机航电系统同样遵循飞机系统研发的一般规律。但由于通用飞机及其航电系统的技术门槛相对较低，从业单位众多，竞争激烈，只有控制成本才能保证具有市场竞争力。为了最大限度地降低成本，通用飞机航电的实现一般有以下特点：

（1）综合化设计。从减小体积重量、降低成本和实用的角度，充分考虑航电系统的综合化。目前，主流的通用飞机航电系统均是综合化的系统；

（2）采用常规系统总线。与大型飞机相比，通用飞机航电系统相对简单，其数据传输要求不高，按照经济实用的原则，系统往往采用一些常规数字总线，如 429/422/232/以太网等；

（3）可扩展性设计。采用可扩展的体系架构，在保持基本架构不变的基础上，功能可以根据需要灵活配置。通过加载软件或增减设备模块，适应不同的飞机需求；

（4）通用化设计。对于基本航电所需要的综合显示器、大气、航姿、通信、导航、航管应答等常规功能模块，采用通用化设计思路，可适用于多种飞机，降低研发成本。

按照以上特点要求，参照国外典型通用飞机航电架构，我们可以得出通用飞机航电的基本组成，主要包括综合显示、综合接口处理、飞机传感器、独立仪表等几个部分。综合显示器一般由两部显示器，主飞行显示器（Primary Flight Display，简称 PFD）和多功能显示器（Multi-function Display，简称 MFD）组成，实现综合显示、系统操作和核心处理三大功能，飞行员通过综合显示器执行相关操作控制、感知和监控飞机的飞行；综合接口处理主要用于完成飞机传感器与综合显示之间的数据接口和处理；飞机传感器包括大气数据、航向姿态、通信、导航和监视等；独立仪表主要作用是备份显示重要飞行信息。系统主要组成如图 1 所示，每一个组成部分是否需要冗余备份，需要通过安全性分析等系统设计过程来确定。

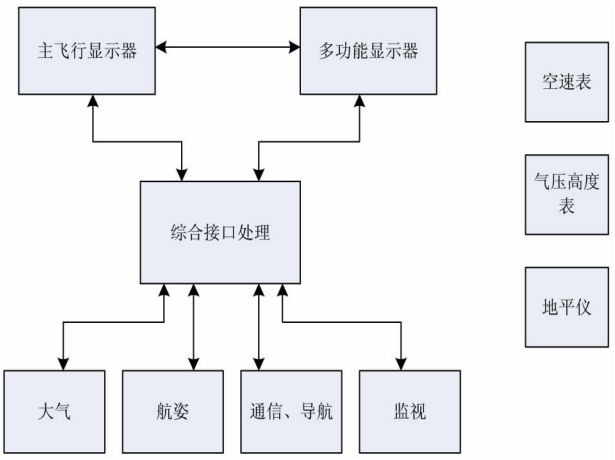

图 1　系统主要组成

2　基于安全性分析的架构研究

2.1 安全性分析简介

在民用飞机系统开发活动中，按照 SAE ARP 4754A《民用飞机和系统开发指南》要求，安全性分析过程融合到开发过程的各个阶段。安全性分析按

照 SAE ARP4761《民用机载系统和设备的安全性评估指导和方法》所推荐的方法进行，主要包括功能危害性评估（Function Hazard Assessment，简称 FHA）、初步系统安全性评估（Preliminary System Safety Assessment，简称 PSSA）、系统安全性评估（System Safety Assessment，简称 SSA）、共因分析（Common Cause Analysis，简称 CCA）等方法[9]。FHA 是功能危害性评估，用于检查和评估飞机系统功能，并按照危害等级定义各功能失效状态；PSSA 是初步安全性评估，通过故障树等手段分析影响系统功能失效状态的各种失效条件的组合，将设计保证等级分配到系统各组成部分，确定所设计系统架构能够满足系统安全性目标；SSA 是安全性评估，对系统研制结果的综合分析，以评估是否满足系统相关安全性要求；CCA 是共因分析，用于分析系统的冗余、使用共同的组件、共同的作用机制等导致的失效。安全性分析过程在系统开发各个阶段迭代进行，不断改进完善，与系统的设计相互作用。

2.2 通用飞机航电系统安全性需求

民航规章第 23 部的咨询通告对于不同种类通用飞机的不同危害性级别失效状态，给出了对应的概率要求及软件/复杂硬件研制保证等级要求，如表 2 所示。

表 2　不同飞机、失效类别对应的概率和软/硬件研制等级

飞机种类	较小的	较大的	危险的	灾难的
一类（6 000 lb 以下单发活塞飞机）	$<10^{-3}$D	$<10^{-4}$C	$<10^{-5}$C	$<10^{-6}$C
二类（6 000 lb 以下其他飞机）	$<10^{-3}$D	$<10^{-5}$C	$<10^{-6}$C	$<10^{-7}$C
三类（6 000 lb 以上各类飞机）	$<10^{-3}$D	$<10^{-5}$C	$<10^{-7}$C	$<10^{-8}$B
四类（9 座 ~ 19 座通勤类飞机）	$<10^{-3}$D	$<10^{-5}$C	$<10^{-7}$B	$<10^{-9}$A

按照 AC23.1309-1E 的飞机功能危害性等级建议，选择影响系统架构的一些重要功能失效状态，并参照 AC23.1309-1E 中的失效状态类别作为这些功能失效状态的简要 FHA 分析结果，如表 3 所示。针对市场占有率较高的典型的涡轮螺旋桨式通用飞机（表 2 中 II 类）确定其定量概率要求。通飞航电重要功能包括气压高度、姿态、主导航、空速、话音通信等，它们的功能丧失或误导的概率要求将直接影响航姿传感器、大气数据计算机、GPS、ILS 等主要飞机传感器设备的配置，同时通过对这些功能失效状态的分析，也对飞机综合显示器、综合接口处理等公共资源的配置提供指导。

表 3　功能失效的危害性分类

航电功能	全部功能丧失	主显示器显示功能丧失	显示误导信息
姿态信息显示功能	CAT	MAJ	CAT
空速信息显示功能	MAJ	MIN	MAJ
气压高度信息显示功能	HAZ	MIN	CAT
主导航信息显示功能	MAJ	MAJ	MAJ
话音通信功能	MIN	MIN	MIN
航管应答功能	MIN	R	MIN

注：CAT 为灾难级，HAZ 为危险级，MAJ 为较大的，MIN 为较小的，R 为不考虑

2.3 安全性分析过程

PSSA 分析将以 FHA 分析的结果作为输入，对涉及到的功能失效进行分析，采用理论方法定量探究失效的因果关系，并指导系统架构设计使其满足安全性需求。分析的方法一般有故障树分析法（Fault Tree Analysis，简称 FTA）和马尔科夫分析法（Markov Analysis，简称 MA）等。这里采用故障树分析法分别对姿态、空速、气压高度、主导航信息等几个功能的失效状态进行分析。通过对系统功能线程涉及到的设备故障概率的分配与评估，从满足安全性需求的角度论证系统各功能设备是否需要冗余备份。为了简化分析过程，以下 FTA 不考虑系统具体的联接方式，仅从系统逻辑组成的角度进行分析。

2.3.1 姿态信息失效状态的分析

姿态信息显示功能包括综合显示器显示和备份仪表显示。向机组提供姿态信息功能丧失的故障树图如图 2 所示。从图中可以看出，虽然有独立的地平仪表，但是 AC23.1309-1E 规定姿态信息主显示手段丧失的类别是 MAJ，因此在故障树中对显示器丧失姿态信息分配的概率是 1E-5，由此分解下去，基于现有设备可靠性水平，显然一个航姿或一个综合接口是无法满足要求的。所以由姿态信息丧失的安全性分析可以得出系统至少需要两个航姿和两个综合接口。

在研究提供误导的姿态信息时，存在两种情况，一种是由于显示器显示错误信息引起的误导，另一种是在显示器显示信息丧失的情况下备份仪表导致的误导。对于第一种情况，显然一个航姿或一个综

合接口无法满足显示器显示误导信息的概率要求，采用两个航姿和两个综合接口，系统可以通过对主备数据的比对，自动判断姿态数据是否有误，只有在主备数据均有误的情况下才可能导致误导发生，从而在必要时给出告警信息，极大地避免了显示误导信息的可能。故障树如图 3 所示。

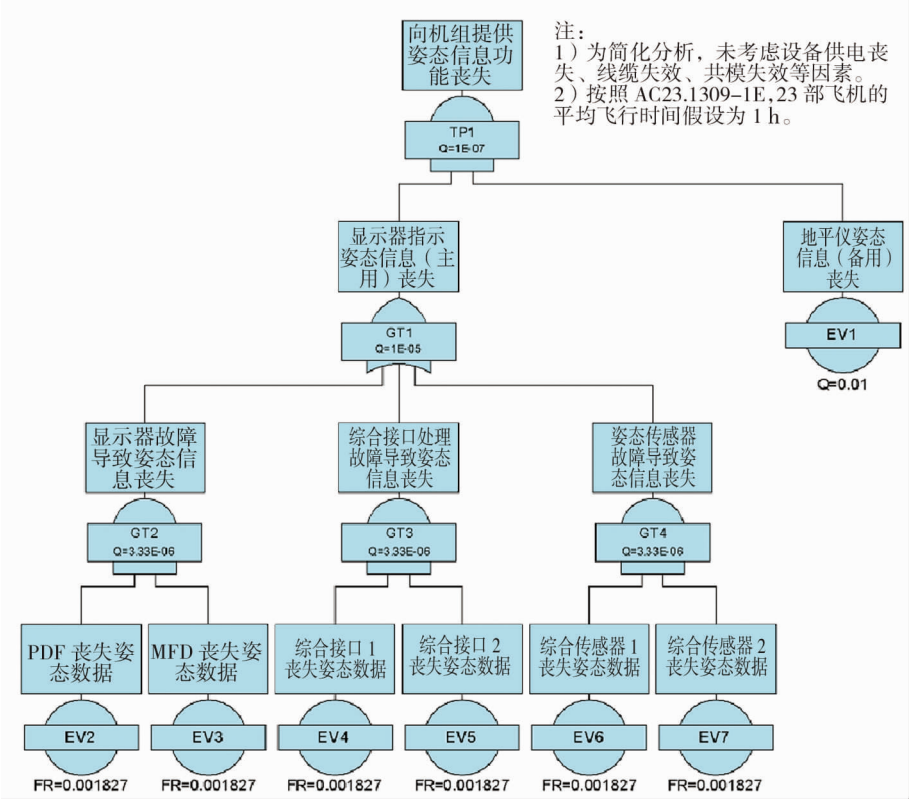

图 2　姿态信息丧失故障树分析

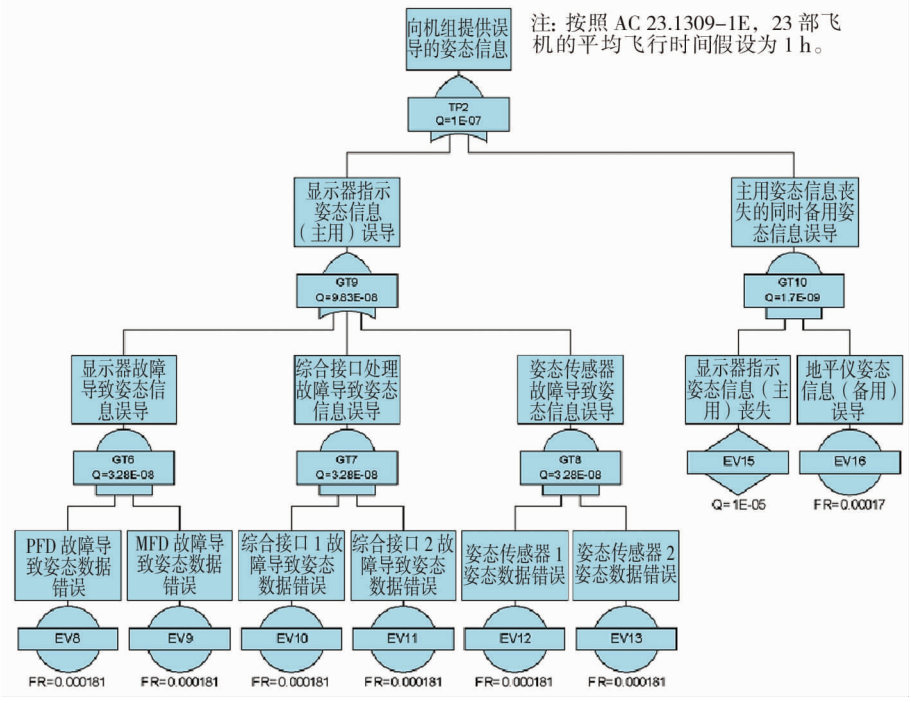

图 3　姿态信息误导故障树分析

2.3.2 空速和气压高度信息失效状态的分析

空速和气压高度的失效状态采用与姿态失效状态相同的分析方法。从功能丧失的角度分析，由于有空速表和气压高度表，而且显示器功能丧失的类别仅是 MIN，所以采用一套大气数据机即可满足系统安全性要求。从提供误导信息的角度分析，因气压高度信息误导的危害程度更高，为 CAT 类，所以此处对气压高度信息误导进行故障树分析，分析表明至少应包含两套大气数据机，才能满足安全性要求。气压高度误导的故障树分析如图 4 所示。

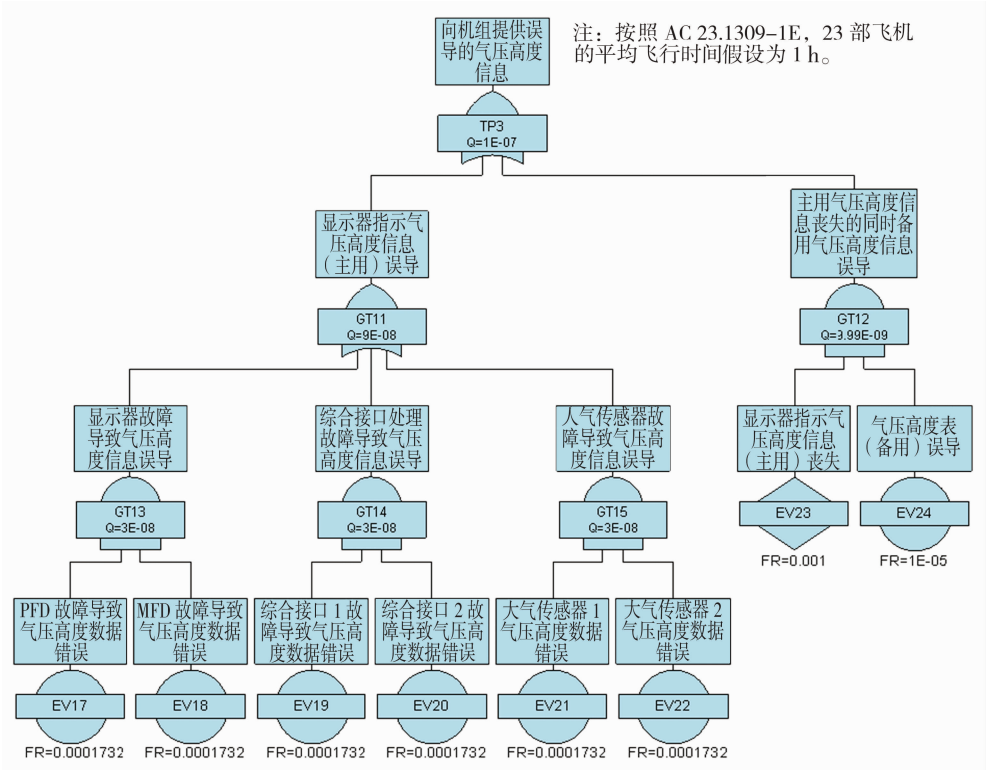

图 4　气压高度信息误导故障树分析

2.3.3 主导航信息失效状态的分析

通用飞机航电系统主用导航手段主要是 GPS、ILS 等，GPS 是飞机巡航阶段主用导航手段，ILS 用于着陆阶段。对于主导航信息的失效状态，虽然其失效类别是 MAJ，对应概率要求是 1E-5/FH，但是由于没有独立备份仪表，从故障树分析来看，系统需要至少两套主用导航源，才能满足功能丧失状态对应的概率要求。主导航信息丧失的故障树分析如图 5 所示。

2.3.4 通信和监视失效状态的分析

系统架构研究中，话音通信是一个重要功能。从安全性分析角度看，话音通信的安全性级别要求不高，功能丧失的失效类别仅是 MIN，但是从使用的角度，CCAR-91 部第 91.411 条款中[10]，明确要求航空器至少需要安装两套独立的无线电通信接收机和发射机。航管应答功能丧失和误导失效状态类别均是 MIN，因此仅对丧失的失效状态进行分析，分析表明，系统配备一套应答机即可满足安全性要求。航管应答功能丧失的故障树分析如图 6 所示。

3　系统基本逻辑架构

通过以上分析，我们可以得出典型的 II 类涡轮螺旋桨式通用飞机航电系统各功能设备的基本配置要求，除配置两台综合显示器外，系统至少需要两套综合接口，两套航姿、大气数据、GPS 和 ILS、通信电台以及一套航管应答机。分析结果与当前主流通用飞机航电系统产品一致。系统基本逻辑架构如图 7 所示。

当然，在系统实际设计中，还需要考虑具体的连接方式，通用飞机航电往往根据具体的数据传输需求采用低成本高可靠的常规总线，如 429/422/232/以太网等。另外，设备可以设计成多种形态，比如：GARMIN 的 G1000 系统将一套接口处理、通信、导航等功能集成在一个 GIA63 设备中；AVIDYNE 的

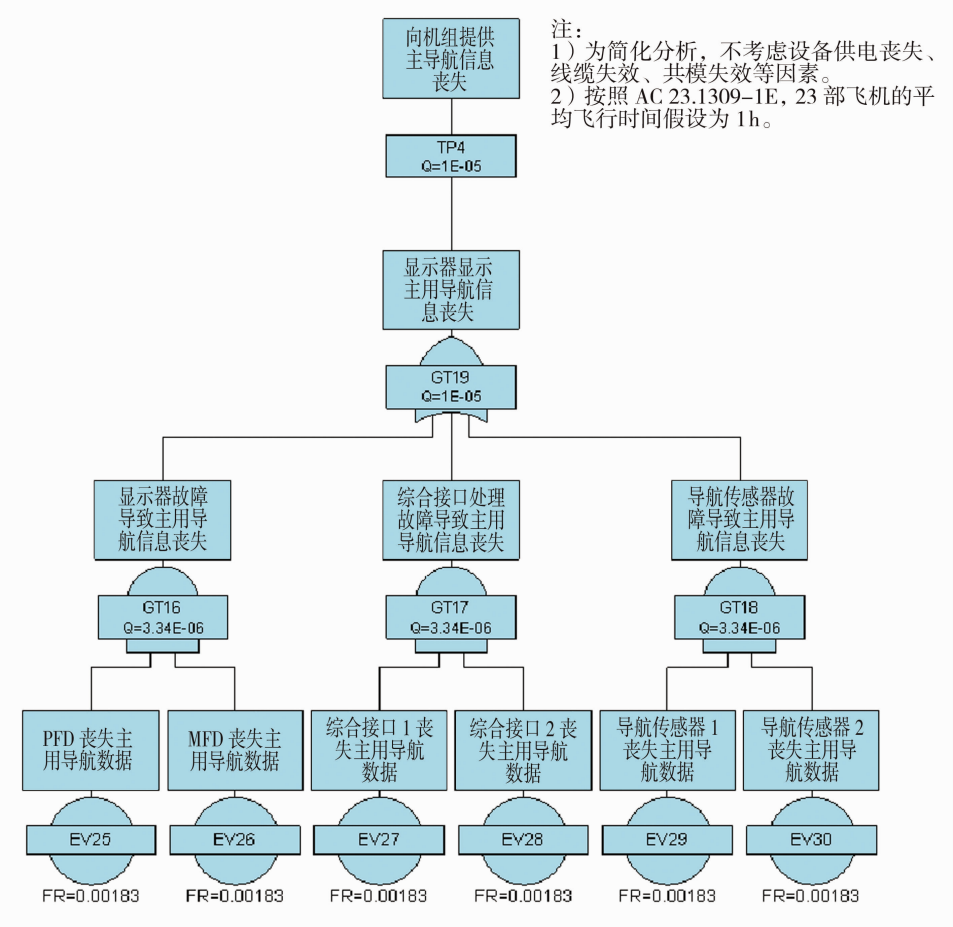

图 5　主导航信息丢失故障树分析

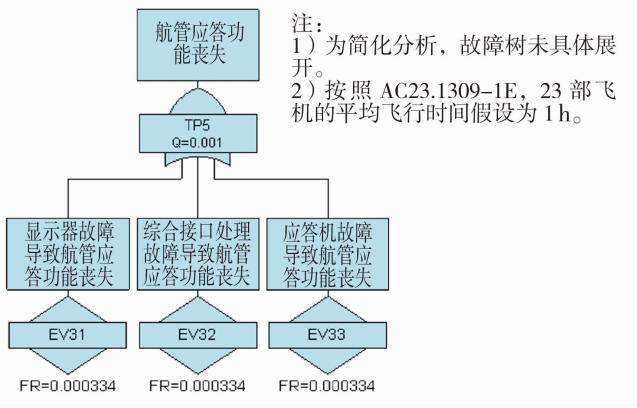

图 6　航管应答功能丢失故障树分析

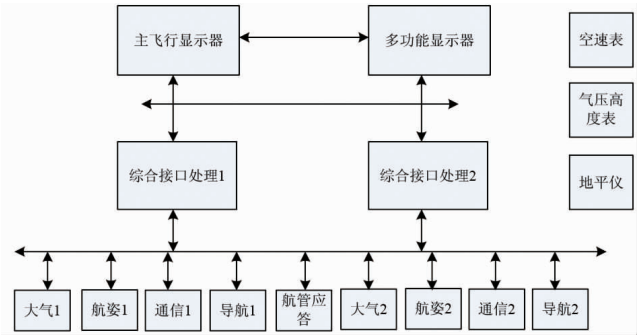

图 7　系统基本逻辑架构

Entegra 系统将一套显示器、接口处理、大气航姿以及通信导航等功能集成在一个 IFD 设备中，综合化程度更高。关于这两个方面，需要针对系统装机实际情况和实际需求进行设计考虑，本文不对此进行深入探讨。

4　结论

随着技术的发展，通用飞机航电系统综合化、智能化程度必然越来越高，为实现系统的安全性和经济性的平衡，必须对航电系统的架构设计进

行充分的论证。本文针对典型的 II 类涡轮螺旋桨式通用飞机,通过系统故障树分析方法,研究了航电系统各主要功能配置的一般规律,可以为通用飞机航电系统设计和适航研制提供良好的思路和借鉴。

参考文献:

[1] 徐新丽, 万会兵. 先进通用飞机航电系统概述[J]. 航空电子技术, 2015, 46(2): 32-35.

[2] 李鹏, 张磊, 窦爱萍. 通用飞机航空电子系统技术发展研究[J]. 电子技术, 2013 (10): 5-7 +10.

[3] 赵明. 通用飞机综合航电技术发展综述[J]. 电讯技术, 2014, 54(3): 374-378.

[4] 宋成艳, 杨永华, 杨明. 基于 APEX 的飞机综合信息显示系统[C]// 2013 年首届中国航空科学技术大会论文集. 北京: 中国航空学会, 2013: 315-319.

[5] GARMIN. G1000 Pilot's Guide for the Socata TBM 850 [EB/OL]. (2011-10) [2019-09-17]. https://www.manualslib.com/.

[6] SAE International. Guidelines for Development of Civil Aircraft and Systems: SAE ARP4754A [S/OL]. (2010-12-21) [2019-09-20]. https://www.sae.org/.

[7] 中国民用航空总局. 正常类、实用类、特技类和通勤类飞机适航规定:CCAR-23-R3[S]. 北京: 中国民用航空总局, 2004.

[8] Federal Aviation Administration. System Safety Analysis and Assessment for Part 23 Airplanes: AC23.1309-1E [S/OL]. (2011-11-17) [2019-09-20]. https://www.faa.gov/.

[9] SAE International. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment: ARP 4761 [S/OL]. (1996-12-01) [2019-09-20]. https://www.sae.org/.

[10] 中国民用航空总局. 一般运行和飞行规则:CCAR-91-R2[S]. 北京: 中国民用航空总局, 2007.

作者简介

王焱滨　男,博士,高级工程师。主要研究方向:运输类飞机、通用飞机航空电子系统集成。E-mail: wangyb@cetca.net.cn

曾　强　男,硕士,工程师。主要研究方向:航空电子系统安全性、可靠性设计与分析。E-mail: zengq@cetca.net.cn

Application of safety analysis in the design of general aircraft avionics system architecture

WANG Yanbin *　ZENG Qiang

(CETC Avionics Co., Ltd, Chengdu 611731, China)

Abstract: The basic composition of general aircraft avionics were summarized by studying the basic functional requirements and system characteristics in this paper. Classification requirements of failure conditions for typical functions such as atmosphere, attitude, communication, navigation and monitoring were studied by analyzing the relative airworthiness regulations. For typical class Ⅱ turbine general airplane, the redundancy requirement of major functions of the avionics system were studied by fault tree analysis in order to meet the requirements of the typical functional failure probability and basic logic architecture of system was obtained.

Keywords: general aircraft; avionics system; safety analysis; fault tree; redundancy requirement; system architecture

* Corresponding author. E-mail: wangyb@cetca.net.cn