http：//myfj.cnjournals.com myfj_sadri@163.com （021）20866796

DOI：10.19416/j.cnki.1674-9804.2024.02.014

基于故障树分析的民用飞机结冰探测系统架构设计

沙昭君* 王延胜 胡伟学

（上海飞机设计研究院，上海 201210）

摘 要：飞机结冰会造成全机气动性能下降、飞行品质降级等一系列问题，对飞行安全造成极大的威胁。现代民用飞机普遍装备结冰探测系统以应对飞行中的结冰问题。结冰探测系统通过向飞行机组发送结冰告警，来帮助飞行机组判断开启防冰系统的时机。首先对民用飞机结冰探测系统的故障树分析特点进行介绍，然后根据结冰探测系统的功能需求，针对结冰探测系统进行初步的架构设计，之后采用故障树分析的方式分析结冰探测系统主要失效模式的失效概率，过程中发现初步架构的失效模式的失效概率远不能满足系统安全性需求，最后通过对系统架构进行冗余设计，确保系统架构设计满足系统安全性需求。

关键词：结冰探测系统；故障树分析；架构设计

中图分类号：V244.1+5 **文献标识码**：A **OSID**：

0 引言

现代民机的安全性评估可以分为四个阶段：功能危险性分析（functional hazard analysis，简称FHA）、初步系统安全性分析（preliminary system safety assessment，简称PSSA）、系统安全性分析（system security analysis，简称SSA）和共因分析（common cause analysis，简称CCA）[1-2]。故障树分析在民机的安全性评估过程中起重要作用，能够定量分析失效事件是否满足安全性要求。作为一种演绎性的失效分析方法，故障树分析方法集中在一个具体的不希望事件上，并且能提供一种确定引起该事件原因的方法。换句话说，故障树分析是一种自上而下的系统评价程序，针对某一特定的不希望事件，形成定性模型，然后进行评价。故障树分析从一个不希望的顶事件开始，系统性地确定系统功能块的所有单个故障及失效组合。随着分析逐步向下开展，不断细化设计层级直到揭示出底事件或直到满足该顶事件要求为止[3]。

开展故障树分析的主要作用包括：

1）能够提前判断架构设计是否满足安全性要求，指导系统架构设计；

2）便于评估设计更改对于安全性的影响；

3）能够定量表示顶事件的发生概率；

4）能够预计下层事件分配概率；

5）能够评估暴露时间间隔、潜伏时间以及处于风险中的时间间隔对系统的全面影响；

6）能够评估共因故障的源头。

民用飞机结冰探测系统通常由两支结冰探测器组成，对称安装在机头两侧，飞机进入结冰环境后，结冰探测器探测到结冰条件，发出结冰告警信号，提醒机组作动防冰系统或飞离结冰空域[4-6]。结冰探测器的种类有很多，包括放射线技术传感器、热交换技术传感器、谐振技术传感器和磁滞伸缩技术传感器等[7-10]。

目前国内外对于结冰探测系统的研究工作主要集中在对结冰探测器的设计研究，对结冰探测系统安全性的研究较少，且较少考虑结冰探测系统在

* 通信作者. E-mail：shazhaojun@comac.cc

引用格式：沙昭君，王延胜，胡伟学. 基于故障树分析的民用飞机结冰探测系统架构设计[J]. 民用飞机设计与研究，2024(2)：87-94. SHA Z J，WANG Y S，HU W X. Design of civil aircraft ice detection system architecture based on fault tree analysis [J]. Civil Aircraft Design and Research，2024(2)：87-94(in Chinese).

民用飞机领域告警方面的需求。本文根据结冰探测系统的功能，初步搭建结冰探测系统架构。结合民用飞机结冰探测系统告警方面的要求，针对民用飞机结冰探测系统特有的“未通告的结冰探测功能丧失”和“通告的结冰探测功能丧失”两种失效模式进行故障树分析，计算故障树顶事件的失效概率，通过和结冰探测系统的安全性指标进行对比，优化结冰探测系统架构，最终形成满足安全性指标的结冰探测系统架构设计，为以后结冰探测系统方案设计提供指导。

1　结冰探测系统初步架构

1.1　结冰探测系统

结冰探测系统主要由布置在机头的结冰探测器组成。结冰探测器探测大气中的结冰条件，并输出探测结果，通过航电系统传输到指示记录系统，为飞行员提供结冰告警显示信息。

结冰探测系统初步架构仅需一支结冰探测器即可满足结冰探测系统的功能要求，如图 1 所示。

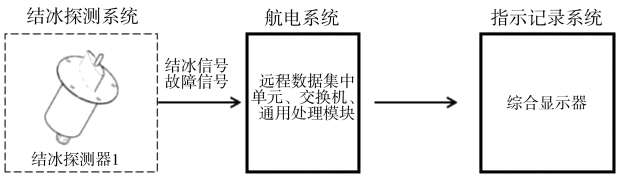

图 1　结冰探测系统初步架构方案

1.2　结冰探测器接口信息

结冰探测器主要接口信息如表 1 所示，包括一个电源输入接口、两个信号输出接口和三个接地接口。

表 1　结冰探测器主要接口信息

序号	接口	接口描述
1	$P_{in}1$	电源输入
2	$P_{out}1$	结冰信号输出
3	$P_{out}2$	故障信号输出
4	$P_{Ground}1$	电源输入接地
5	$P_{Ground}2$	信号接地
6	$P_{Ground}3$	壳体接地

结冰探测器接口交互示意图见图 2。电源系统通过电源输入接口为结冰探测器供电。结冰探测器通过结冰信号输出接口和故障信号输出接口提供结冰信号和结冰探测器故障信号。结冰探测器还通过电源接地接口形成电源供电回路、信号接地接口形成信号传输回路以及壳体接地接口形成防静电回路。

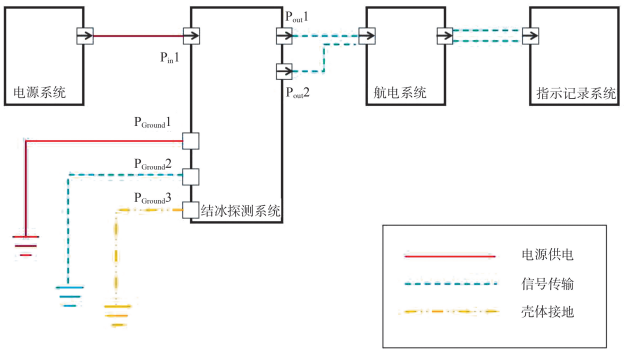

图 2　结冰探测器接口交互示意图

2　结冰探测系统故障树分析

2.1　结冰探测系统安全性指标

通常结冰探测系统需要满足的安全性指标要求如表 2 所示，需要结冰探测器的结冰探测功能和信号传输链路的传输功能两部分叠加。

表 2　结冰探测系统安全性指标要求

序号	失效模式	失效概率
1	未通告的结冰探测功能丧失	10^{-9}
2	通告的结冰探测功能丧失	10^{-5}

2.2　结冰探测系统故障树分析

针对探测器的结冰探测功能，主要包括结冰探测器输出状态正常、显性故障和隐性故障 3 种状态，其底事件和失效概率见表 3。对应的故障树分析见图 3 至图 5，其中底事件失效概率为业界标准量级水平。

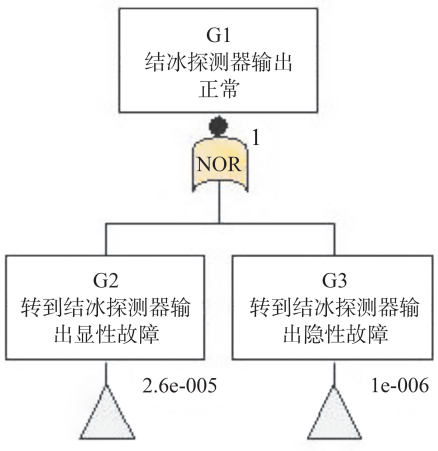

图 3　结冰探测器输出正常(G1)故障树

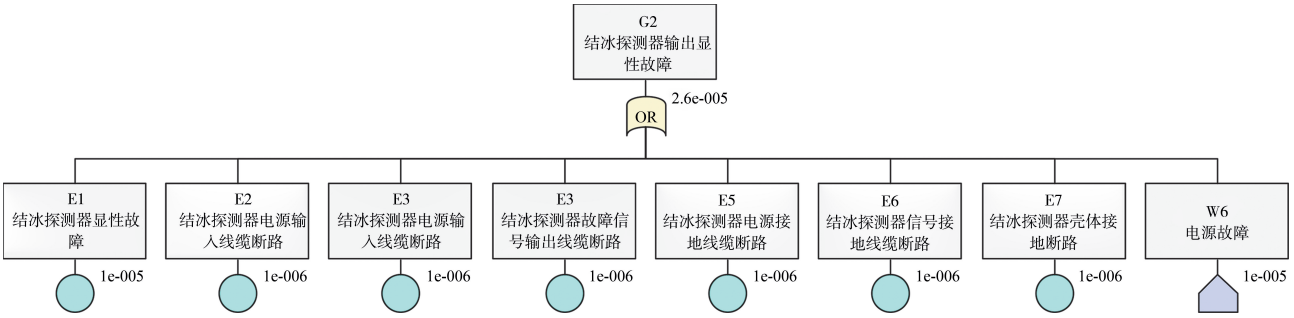

图 4　结冰探测器输出显性故障(G2)故障树

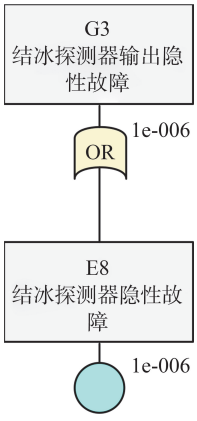

图 5　结冰探测器输出隐性故障(G3)故障树

表 3　结冰探测器输出状态表

项目	编号	中间事件	编号	底事件	失效概率
结冰探测器输出状态	G1	正常	/	/	≈1
	G2	显性故障	E1	结冰探测器显性故障	10^{-5}
			E2	电源输入线缆断路	10^{-6}
			E3	结冰信号输出线缆断路	10^{-6}
			E4	故障信号输出线缆断路	10^{-6}
			E5	电源接地线缆断路	10^{-6}
			E6	信号接地线缆断路	10^{-6}
			E7	壳体接地线缆断路	10^{-6}
	G3	隐性故障	W6	电源系统故障	10^{-5}
			E8	结冰探测器隐性故障	10^{-6}

针对信号传输链路的传输功能，主要包括输出链路状态正常、航电信号错误、航电信号丢失、航电到指示记录线缆断路、指示记录信号错误、指示记录信号丢失 6 种状态，底事件和失效概率见表4。

表 4　输出链路状态表

项目	编号	底事件	失效概率
输出链路状态	/	正　常	≈1
	W1	航电信号错误	10^{-5}
	W2	航电信号丢失	10^{-8}
	W3	航电到指示记录线缆断路	10^{-6}
	W4	指示记录信号错误	10^{-5}
	W5	指示记录信号丢失	10^{-6}

结合结冰气象情况，将结冰探测器的结冰探测功能状态和信号传输链路的传输功能状态两部分叠加，判断对最终指示记录系统显示结果的影响见表 5。

表 5　功能状态叠加

输出链路状态	结冰探测器输出状态	结冰气象	结冰探测器信号输出		指示记录显示状态		导致的失效模式
			结冰	故障	结冰	故障	
正常	正常	否	否	否	否	否	无影响
		是	是	否	是	否	无影响
	显性故障	否	否	是	否	是	2
		是	否	是	否	是	2
	隐性故障	否	否	否	否	否	无影响
		是	否	否	否	否	1
航电信号丢失	正常	否	否	否	否	否	无影响
		是	是	否	否	否	1
	显性故障	否	否	是	否	否	无影响
		是	否	是	否	否	1
	隐性故障	否	否	否	否	否	无影响
		是	否	否	否	否	1

表5(续)

输出链路状态	结冰探测器输出状态	结冰气象	结冰探测器信号输出		指示记录显示状态		导致的失效模式
			结冰	故障	结冰	故障	
航电信号错误	正常	否	否	否	是	否	误告警
					否	是	2
		是	是	否	否	否	1
					是	是	2
	显性故障	否	否	是	否	否	无影响
					是	是	2
		是	否	是	否	否	1
					是	是	2
	隐性故障	否	否	否	是	否	误告警
					否	是	2
		是	否	否	是	否	无影响
					否	是	2
航电到指示记录线缆断路	正常	否	否	否	否	是	2
		是	是	否	否	是	2
	显性故障	否	否	是	否	是	2
		是	否	是	否	是	2
	隐性故障	否	否	否	否	是	2
		是	否	否	否	是	2
指示记录信号丢失	正常	否	否	否	否	否	无影响
		是	是	否	否	否	1
	显性故障	否	否	是	否	否	无影响
		是	否	是	否	否	1
	隐性故障	否	否	否	否	否	无影响
		是	否	否	否	否	1
指示记录信号错误	正常	否	否	否	是	否	误告警
					否	是	2
		是	是	否	否	否	1
					是	是	2
	显性故障	否	否	是	否	否	无影响
					是	是	2
		是	否	是	否	否	1
					是	是	2

表5(续)

输出链路状态	结冰探测器输出状态	结冰气象	结冰探测器信号输出		指示记录显示状态		导致的失效模式
			结冰	故障	结冰	故障	
指示记录信号错误	隐性故障	否	否	否	是	否	误告警
					否	是	2
		是	否	否	是	否	无影响
					否	是	2

梳理表 5 得到导致结冰探测系统失效模式的事件组合见表 6。

其中中间事件 G4-G9 的故障树见图 6 至图 11。

表 6　导致失效模式的事件组合

失效模式	编号	结冰探测器输出状态	编号	中间事件	输出链路状态
未通告的结冰探测功能丧失	G1	正常	G4	组合结冰探测器输出正常引起未通告丧失的链路	航电信号错误
					航电信号丢失
					指示记录信号错误
					指示记录信号丢失
	G2	显性故障	G5	组合结冰探测器输出显性故障引起未通告丧失的链路	航电信号错误
					航电信号丢失
					指示记录信号错误
					指示记录信号丢失
	G3	隐性故障	G6	组合结冰探测器输出隐性故障引起未通告丧失的链路	正常
					航电信号丢失
					指示记录信号丢失
通告的结冰探测功能丧失	G1	正常	G7	组合结冰探测器输出正常引起通告丧失的链路	航电信号错误
					航电到指示记录线缆断路
					指示记录信号错误
	G2	显性故障	G8	组合结冰探测器输出显性故障引起通告丧失的链路	正常
					航电信号错误
					航电到指示记录线缆断路
					指示记录信号错误

表6(续)

失效模式	编号	结冰探测器输出状态	编号	中间事件	输出链路状态
通告的结冰探测功能丧失	G3	隐性故障	G9	组合结冰探测器输出隐性故障引起通告丧失的链路	航电信号错误 航电到指示记录线缆断路 指示记录信号错误

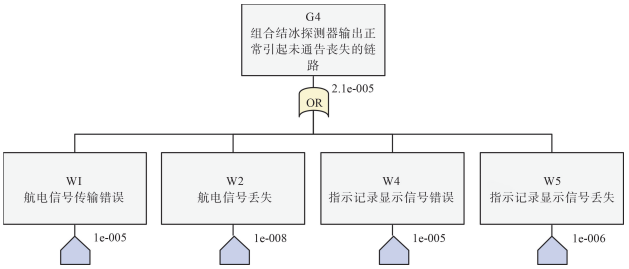

图 6　组合结冰探测器输出正常引起未通告丧失的链路(G4)故障树

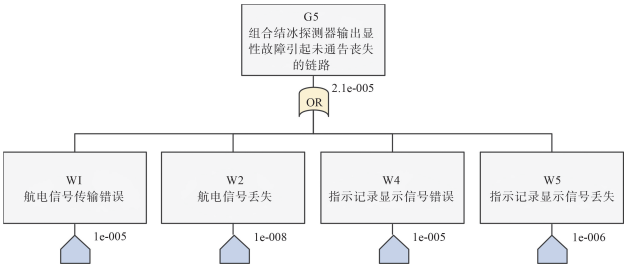

图 7　组合结冰探测器输出显性故障引起未通告丧失的链路(G5)故障树

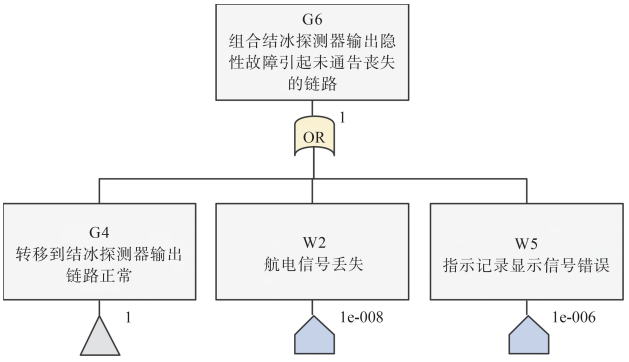

图 8　组合结冰探测器输出隐性故障引起未通告丧失的链路(G6)故障树

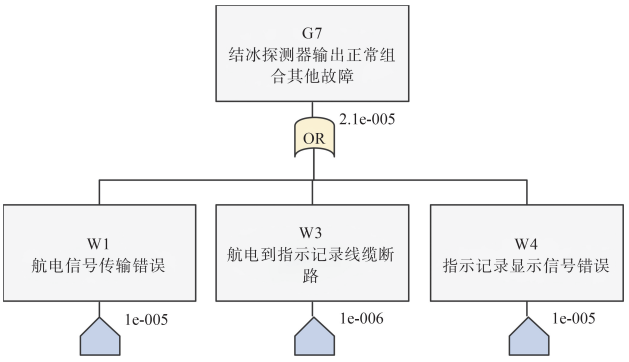

图 9　组合结冰探测器输出正常引起通告丧失的链路(G7)故障树

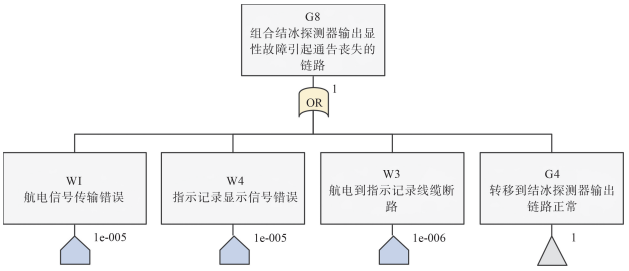

图 10　组合结冰探测器输出显性故障引起通告丧失的链路(G8)故障树

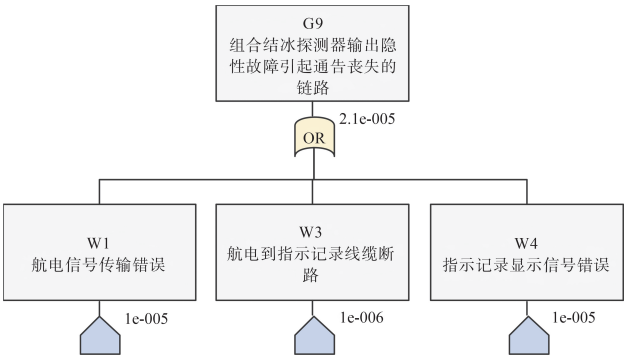

图 11　组合结冰探测器输出隐性故障引起通告丧失的链路(G9)故障树

最终形成两种失效状态的故障树见图 12 和图 13。失效状态 1“未通告的结冰探测功能丧失”，其失效概率为 2.2×10^{-5}，远大于 10^{-9} 的要求；失效状态 2“通告的结冰探测功能丧失”，其失效概率为 4.7×10^{-5}，略大于 10^{-5} 的要求。因此，需要对结冰探测系统架构进行冗余设计。

3　结冰探测系统架构设计

3.1　结冰探测系统冗余架构方案

考虑一支结冰探测器无法满足结冰探测系统安

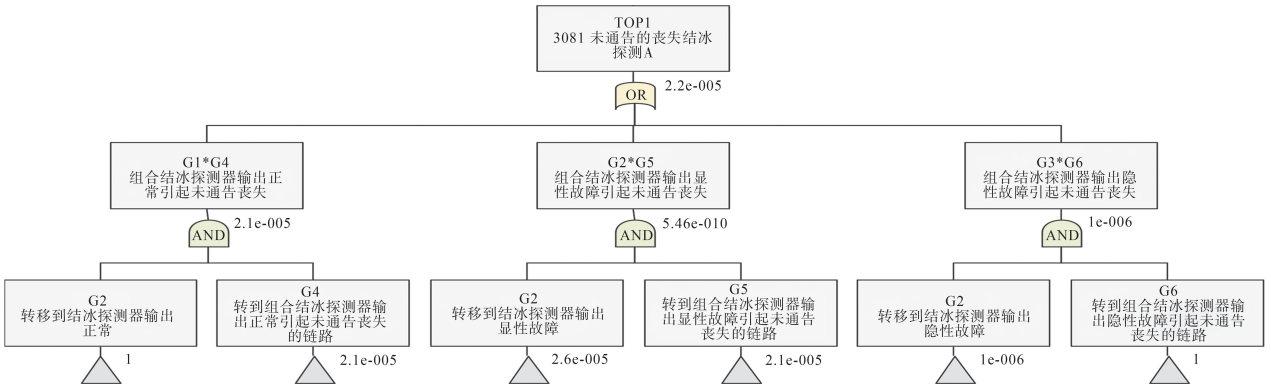

图 12　未通告的结冰探测功能丧失

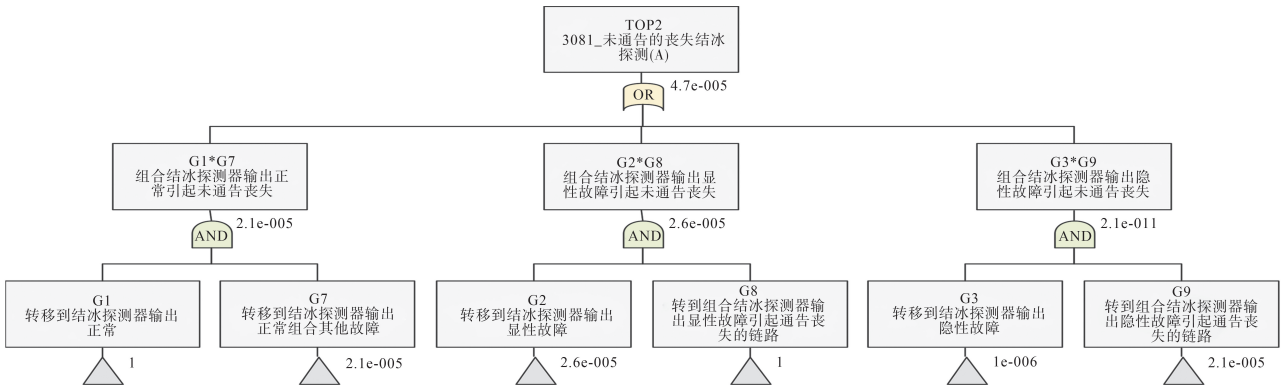

图 13　通告的结冰探测功能丧失

全性指标要求,采用两支结冰探测器进行系统冗余设计,并假设两支结冰探测器对应的航电系统(相互独立的航电链路)和指示记录系统(相互独立的综合显示器)相互独立。形成冗余的结冰探测系统架构见图 14。

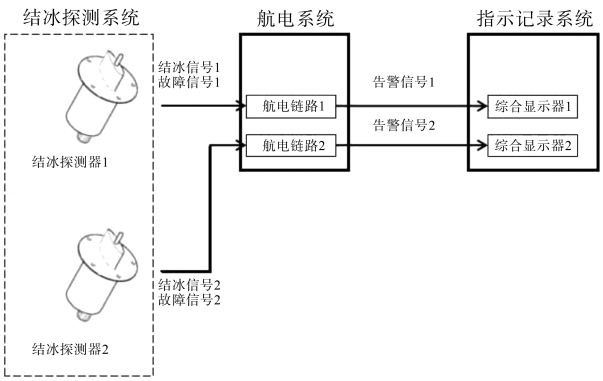

图 14　结冰探测系统冗余架构方案

结冰探测系统冗余架构方案的失效状态 1“未通告的结冰探测功能丧失”和失效状态 2“通告的结冰探测功能丧失”的故障树分析见图 15 和图 16。失效状态 1“未通告的结冰探测功能丧失”的失效概率为 2.55×10^{-9},略大于 10^{-9},仍不满足安全性要求。失效状态 2“通告的结冰探测功能丧失”的失效概率为 2.21×10^{-9},远小于 10^{-5},满足安全性要求。但由于该故障树尚未考虑航电系统和指示记录系统的共模影响,所以仍需要进一步改进。

经过上述分析可知,“通告的结冰探测功能丧失”的失效概率远大于设计要求,仅“未通告的结冰探测功能丧失”的失效概率略高于设计要求,主要是由于传输链路中信号丢失导致的,包括航电信号丢失和指示记录信号丢失。因此,可以通过增加硬线或总线信号传输链路等方式,降低“航电信号丢失”的失效概率,进而降低“未通告的结冰探测功能丧失”的失效概率。一般飞行手册中会增加相关操作程序,飞行机组可根据结冰探测器“ICE DETECTED”告警或“总温≤10 ℃+可见湿气”来判断结冰气象条件。此时,“未通告的结冰探测系统功能丧失”的失效影响是较大的,无需满足 10^{-9} 的失效概率要求,只需满足 10^{-5} 的失效概率要求。所以采用两支结冰探测器的冗余结冰探测系统架构能够满足对于结冰探测系统的失效概率要求。

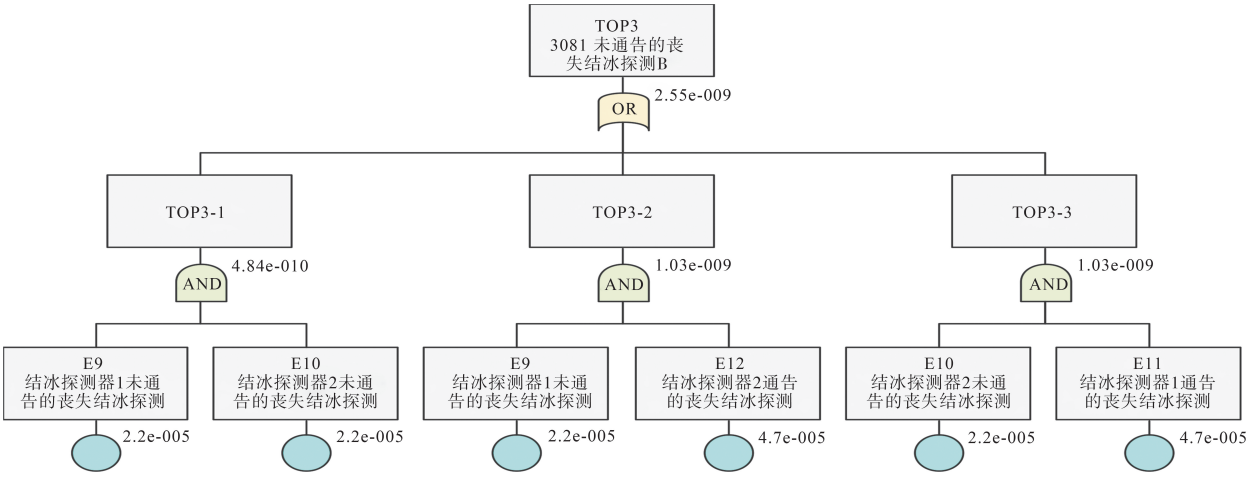

图 15　未通告的结冰探测功能丧失

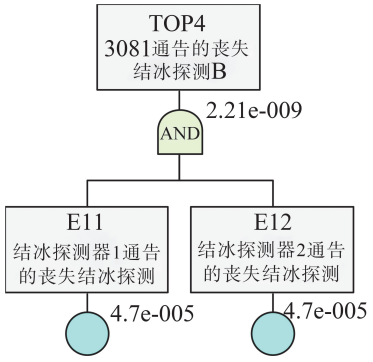

图 16　通告的结冰探测功能丧失

4　结论

本文针对民用飞机结冰探测系统,采用故障树分析的方法,定量计算结冰探测系统失效模式的失效概率。根据失效模式概率和系统安全性需求的差异,对结冰探测系统架构进行冗余设计,最终形成了结冰探测系统架构方案,为结冰探测系统安全性分析及架构设计提供指导。

参考文献:

[1] Society of Automotive Engineers, Inc. Certification considerations for highly-integrated or complex aircraft systems:ARP 4754 [S]. U. S. :Society of Automotive Engineers, Inc, 1996.

[2] 邬龙. 基于环控系统的安全性分析方法研究[D]. 天津:中国民航大学, 2017.

[3] Society of Automotive Engineers, Inc. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment: ARP 4761 [S]. U. S. :Society of Automotive Engineers, Inc, 1996.

[4] 李盼,朱家乐. FAR25 第 129 号修正案对结冰探测系统的影响研究[J]. 飞机设计, 2018,38(1): 76-80.

[5] 史献林,徐佳佳,杨胜华. 主探冰系统自动作动防冰系统的逻辑设计[C]//中国航空学会. 探索 创新 交流——第六届中国航空学会青年科技论坛文集:下册. 北京:航空工业出版社,2014: 1260-1264.

[6] 史献林. 机翼防冰自动作动功能的逻辑设计及验证[J]. 民用飞机设计与研究, 2014(3): 92-95.

[7] 王起达,王同光. 机翼结冰探测技术进展[J]. 航空制造技术, 2009(3): 62-64.

[8] 张杰,周磊,张洪,等. 飞机结冰探测技术[J]. 仪器仪表学报, 2006,27(12): 1578-1586.

[9] 李航航,周敏. 飞机结冰探测技术及防除冰系统工程应用[J]. 航空工程进展, 2010,1(2): 112-115.

[10] 王小辉,车程,瑚洋,等. 基于故障树的飞机结冰探测系统安全性分析[J]. 航空工程进展, 2018,9(2): 268-273.

作者简介

沙昭君　女,硕士,工程师。主要研究方向:民用飞机防冰系统设计。E-mail:shazhaojun@ comac. cc

王延胜　男,硕士,高级工程师。主要研究方向:民用飞机防冰系统设计。E-mail:wangyansheng@ comac. cc

胡伟学　男,硕士,工程师。主要研究方向:民用飞机防冰系统设计。E-mail:huweixue@ comac. cc

Design of civil aircraft ice detection system architecture based on fault tree analysis

SHA Zhaojun * WANG Yansheng HU Weixue

(Shanghai Aircraft Design and Research Institute, Shanghai 201210, China)

Abstract: Aircraft icing will cause a series of problems such as aerodynamic performance degradation and flight quality degradation of the whole aircraft, which will pose a great threat to flight safety. Modern civil aircraft are generally equipped with ice detectors to deal with the problem of icing in flight. The ice detection system sends an ice warning to flight crew to help them determine the time of activating the anti-ice system. This article first introduces the fault tree analysis characteristics of civil aircraft ice detection system. Then based on the functional requirements of ice detection system, a preliminary architecture design is carried out for the ice detection. Then fault tree analysis is used to analyze the failure probability of the main failure mode of the ice detection system. During the process, it is found that the failure probability of the preliminary architecture's failure mode is far from meeting the system requirements. Finally, redundant design is carried out on the system architecture to ensure that it meets the safety requirements of the system.

Keywords: ice detection system; fault tree analysis; architecture design

* Corresponding author. E-mail: shazhaojun@comac.cc