文章编号:1671-4598(2020)01-0044-04 DOI:10.16526/j.cnki.11—4762/tp.2020.01.011 中图分类号:TP391 文献标识码:A

基于故障树分析方法的民机飞机驾驶舱门控制逻辑改进设计

陆 峥,刘 剑
(上海飞机客户服务有限公司,上海 200241)

摘要:驾驶舱门是保护飞行机组人员安全,保障飞行安全的重要阻隔屏障;自德国蓄意坠机事件发生后,如何兼顾保障安全和防止飞行员蓄意控制飞机,成为民用飞机驾驶舱门设计关注的焦点;针对蓄意坠机中飞机驾驶舱遭遇非法控制的顶事件,构建了故障树模型;开展了故障树的定量和定性分析,查找出飞机遭遇非法控制的薄弱环节,并提出了针对性的建议措施;针对飞行员离开驾驶舱后存在无法进入被锁驾驶舱的重大驾驶舱门控制逻辑缺陷,重新分配了驾驶舱门控制权限,提出了改进的驾驶舱门控制流程和逻辑;改进后的故障树可靠性分析结果表明,飞行员失常事件的关键重要度由0.99大幅降至$4.02*10^{-4}$,对飞机遭遇非法控制顶事件的影响非常小;顶事件发生率下降为$5.02*10^{-11}$,飞行安全性得到了有效提升。

关键词:飞机;驾驶舱;故障树;控制逻辑;蓄意坠机

Improved Design of Control Logic for Civil Aircraft Cockpit Door Based on Fault Tree Analysis

Lu Zheng, Liu Jian
(Shanghai Aircraft Customer Service Co. Ltd., Shanghai 200241, China)

Abstract: Cockpit door is an important barrier to protect flight crew and flight safety. Since the tragedy of German deliberate crash happened in 2015, how to balance between ensuring flight safety and preventing pilots from deliberately controlling aircraft has become the focus of civil aircraft cockpit door design. To deal with the top event of illegal control of an aircraft's cockpit in a deliberate crash case, the fault tree model is constructed. The quantitative and qualitative analysis of the fault tree is carried out to find out the weakness to prevent an aircraft from encountering illegal control. And the corresponding suggestions and measures are put forward. To solve the serious logic defect of cockpit door control that pilots can not pass the locked door again after leaving the cockpit, the control priority of cockpit door is reallocated. The improved control flow and logic of cockpit door are proposed. After performing the reliability analysis of the new fault tree, the results show that the critical importance of pilots' abnormal event decreases significantly from 0.99 to $4.02*10^{-4}$, which had little impact on the illegal control of the aircraft. The incidence of the top accident also decreases to $5.02*10^{-11}$, and flight safety has been effectively improved.

Keywords: aircraft; cockpit; fault tree; control logic; deliberate crash

0 引言

驾驶舱门是安装在飞机客舱和驾驶舱之间的可锁舱门。震惊世界的“9.11”恐怖袭击事件发生后,为保障驾驶安全及飞行机组的人身安全,国际民航组织和各国适航当局都修改了适航条例,明确要求所有民航运输类客机必须安装具备防暴力入侵以及防爆的驾驶舱门。

按照CCAR-25部中关于驾驶舱的保护适航条款相关要求[1],驾驶舱门必须可锁,能够阻止未被授权的人员进入驾驶舱;以及能抵御轻型武器的活力或爆炸装置的穿透,以保证机组人员的安全。目前,飞机上通常在驾驶舱内侧安装有驾驶舱门控制系统,可以有效阻止未经授权的非机组人员进入驾驶舱抢夺飞机控制权,为飞行员提供安全保护。因此飞行机组人员具有驾驶舱门的最高控制权限。

2015年3月4日,德国之翼客机坠毁事件发生。官方发布的事件调查报告确认,该坠毁事件是由当班客机副驾驶蓄意改变自动驾驶模式下的飞机巡航高度设定,导致飞机加速下降直至坠毁。在发现飞机异常下降期间,客舱机组人员试图通过使用舱门密码键盘、驾驶舱内话设备及拍打舱门等措施请求进入驾驶舱。但该肇事飞行员始终未打开驾驶舱门,最终造成飞机坠毁,机上144名乘客和6名机组人员全部遇难。

蓄意坠机事件发生,暴露了飞行员权限过大;当发生蓄意恶性事件时,无法进入驾驶舱进行纠正。因此次,有必要进行防止蓄意坠机的驾驶舱门禁系统研究。

收稿日期:2019-06-12; **修回日期**:2019-07-19。

作者简介:陆 峥(1964-),男,上海市人,高级工程师,主要从事飞机经济性与安全性、飞机舱门设计、适航与维修性等技术方向的研究。

通讯作者:刘 剑(1980-),男,江苏靖江人,高级工程师,主要从事飞机经济性与安全性,民机客舱舒适性,客舱人机工程分析方向的研究。

1　现有飞机驾驶舱门控制原理

1.1　驾驶舱门禁控制系统

驾驶舱门禁控制系统如图 1 所示[2-4]，主要由舱门控制器、电磁锁、传感器、密码输入板、警告指示灯和蜂鸣器以及控制面板等组成。

舱门控制器是驾驶舱门控制系统的核心，管理来自密码输入板（客舱内）、控制面板（驾驶舱内）的控制信号或请求信号，按照预先设定的舱门控制逻辑顺序，对驾驶舱门的打开和关闭进行管理控制。

密码输入板安装在靠近客舱一侧的驾驶舱门上，客舱乘务人员输入密码后可发出请求进入驾驶舱；同时密码板上还设置有指示灯，用于提示当前驾驶舱门的状态。电磁锁是舱门的锁定机构。若驾驶舱门闭合，当有外部电源供电时，电磁锁处于锁闭状态，驾驶舱门将锁定。驾驶舱外的人员将无法打开驾驶舱门；当电源断开时，电磁锁处于开锁状态，此时驾驶舱外的人员可以打开驾驶舱门。

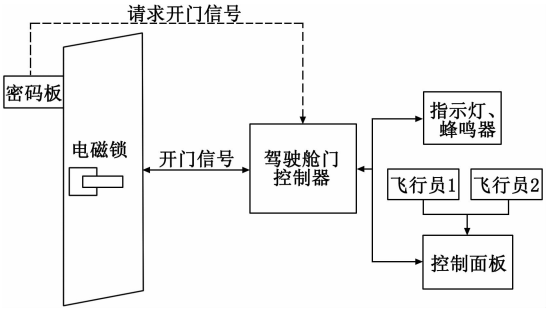

图 1　驾驶舱门控制系统原理

舱门控制器输出的告警和指示信息由指示灯和蜂鸣器输出，提示机组人员有人请求进入驾驶舱或者舱门控制系统出现的异常。

控制面板安装在驾驶舱内的中央操纵台上，主副飞行员都可以操纵驾驶舱门上锁或解锁。

1.2　驾驶舱门控制逻辑

驾驶舱门的实际控制逻辑如图 2 所示。

正常进入驾驶舱流程：如前所述，驾驶舱门控制系统通电后，电磁锁会闭锁，舱门会被锁定。客舱内人员需要在密码板上按“＃”键请求进入驾驶舱。飞行员在确认请求者身份后，将控制面板上的三位开关置于“Unlock”解锁位置，此时驾驶舱门电磁锁解锁，门外人员可以开门进入驾驶舱。如果飞行员发现可疑情况，可以将三位开关置于“Deny”拒绝位置，此时电磁锁仍然处于闭锁状态，驾驶舱门持续关闭。

紧急进入驾驶舱流程：当客舱人员发现驾驶舱内发生意外需要进入驾驶舱时，可使用应急进门程序。客舱人员通过密码板输入紧急密码＋“＃”键，密码检验正确后，系统将发出 30 s 提示音信息。如果飞行机组人员发生意外，30 s 内没有进行任何控制面板操作，驾驶舱门电磁锁将在 30 s 时间到后解锁，舱门可以打开。若机组人员没有失能想拒绝客舱人员进入，则可操作控制面板上的三位开关置于“Deny”拒绝位，此时驾驶舱门仍然保持上锁状态，客舱人员被拒绝进入。

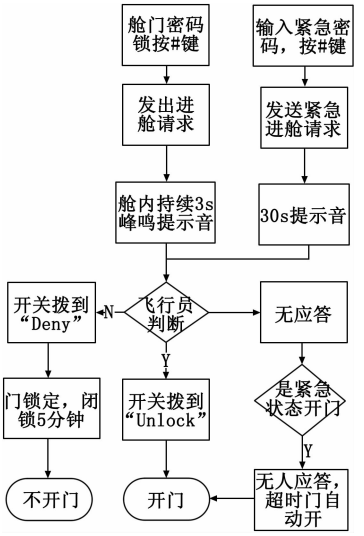

图 2　驾驶舱门控制逻辑

2　蓄意坠机事件及其故障树分析

2.1　蓄意坠机事件分析

目前民用运输飞机普遍采用双人制机组，工作负荷、运行成本、安全性都达到了较好的平衡。911 事件发生之后，为避免民航航班被恐怖分子当做“导弹”攻击平民，飞机上的驾驶舱舱门设计对安全性的考虑放在了首位。设计中预设的事故场景是传统的劫机事件，即：飞行员在驾驶舱，劫机分子在客舱，劫机分子试图通过暴力手段进入驾驶舱接管飞机。现代客机的舱门较好的满足了该场景下的飞行安全。只要锁死舱门，小口径武器、消防斧及一般破拆手段都无法破坏锁死机构。匹配严格的机场安检，基本可杜绝劫机后实施恐怖袭击的可能。

但这种预设场景为飞行员蓄意坠机事件留下了可利用的空档。肇事飞行员在同组另一名飞行员离开驾驶舱的时候，通过锁死驾驶舱门能自由进行危险操作。即使地面人员或其他机组成员能够发现肇事飞行员作出了危险操作，仍然无法干预飞机飞行过程。此时肇事飞行员拥有对飞机的绝对控制权。

2.2　蓄意坠机事件故障树建立

故障树分析（FTA）是定性的可靠性分析的重要方法工具[8-9]。故障树分析是演绎推理，采用从上到下的方式，分析复杂系统初始失效及事件的影响。故障树建模过程的本质是研究系统失效（顶事件）与部件失效（底事件）之间的因果关系。

选择飞机遭遇非法控制作为顶事件进行故障树分析，建立故障树模型如图 3 所示。故障树共有 7 个中间事件和 8 个底事件。

由于劫机事件发生牵涉多方面的因素。为便于进行故

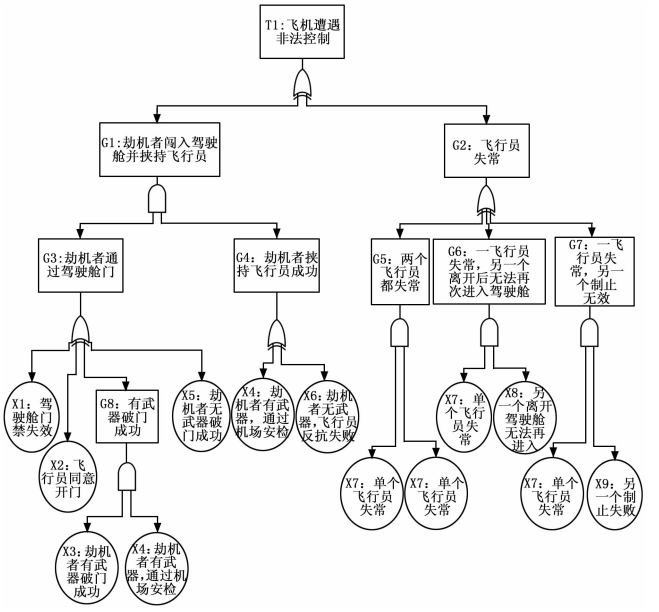

图 3 飞机遭遇非法控制顶事件故障树

障树分析，采用模型简化的方法，抓住核心关键因素，舍弃其他不重要因素。因此，在进行故障树建模时，只考虑飞机遭遇非法控制的核心关键因素：飞行员个人行为、劫机者行为与驾驶舱门。其他因素，如飞机电子系统蓄意远程劫持控制、机场安检失效的具体因素等暂不考虑。

故障树中底事件如表 1 所示。为方便后续定量计算分析，参考相关工程系统失效率和社会人口活动大数据，对底事件的发生率数据进行了部分假定。

表 1 故障树底事件及其发生率

编号	底事件名称	发生率
q_1	驾驶舱门禁失效	$0.05*10^{-6}$/h
q_2	飞行员同意开门	$0.001*10^{-6}$/h
q_3	劫机者有武器,破门成功	0.5/h
q_4	劫机者携带武器,通过机场安检	$0.0001*10^{-6}$/h
q_5	劫机者无武器,破门成功	$0.05*10^{-6}$/h
q_6	劫机者无武器,飞行员反抗失败	$2*10^{-6}$/h
q_7	单个飞行员失常	$0.01*10^{-6}$/h
q_8	另一人离开驾驶舱无法进入驾驶舱	0.5/h
q_9	另一人制止失败	$2*10^{-6}$/h

2.3 故障树分析

1）故障树定性分析

对于故障树而言，最小割集的阶数越小，一阶最小割集数量越多，则故障树顶事件发生的可能性越大。

通过布尔运算对图 3 故障树进行分析，得到最小割集 9 个，分别为 $\{q_1, q_4\}$，$\{q_1, q_6\}$，$\{q_2, q_4\}$，$\{q_2, q_6\}$，$\{q_3, q_4\}$，$\{q_5, q_6\}$，$\{q_7, q_7\}$，$\{q_7, q_8\}$，$\{q_7, q_9\}$。全部为二阶最小割集。

可以看出不存在由于单个因素作用直接导致恶性事件发生的可能性。

2）故障树定量分析

进一步对故障树进行定量分析，求出故障树顶事件的发生概率以及故障树中各底事件的重要度，并根据重要度的大小排序确定故障诊断和维护顺序。

计算方法如下：

若故障树有 n 个最小割集，分别为 E_1，E_2，…，E_n，则故障树顶事件 T 的发生概率为

$$P(T) = P(E_1 \cup E_2 \cup \cdots \cup E_n) = P(E_1 + E_1'E_2 + E_1'E_2'E_3 + \cdots + E_1'E_2'\cdots E_n) \quad (1)$$

式中，E_n'（n=1，2，3）为事件 E_n 的逆事件。

对式（1）进行运算，代入各最小割集的发生率，即可求出故障树顶事件的发生率为 $5.05*10^{-9}$。

对故障树的重要度进行分析，研究底事件发生对顶事件发生的贡献大小，得到不同底事件的重要度排序。故障树重要度包括概率重要度 I_p 和关键重要度 I_c，如式（2）和式（3）所示。

$$I_p = \frac{\partial Q}{\partial q_i} \quad (2)$$

$$I_c = \frac{q_i}{Q}\frac{\partial Q}{\partial q_i} \quad (3)$$

式中，Q 为顶事件的不可靠度；q_i 为第 i 个底事件的发生率。

故障树重要度分析计算结果如表 2 所示。从表中可以看出底事件 q_4，q_7 概率重要度相对较高，其他底事件概率重要度很小。这说明劫机者携带武器通过机场安检、单个飞行员失常的概率一旦发生变化，必然会对顶事件发生率引起重大变化。

进一步考察底事件的关键重要度，数值越大说明底事件发生引发故障树顶事件发生的可能性越大。从表中可以看出 q_7，q_8，q_3，q_4 底事件最为紧要。

表 2 故障树底事件重要度

底事件	概率重要度	关键重要度
q_1	$2*10^{-6}$	$1.98*10^{-5}$
q_2	$2*10^{-6}$	$3.96*10^{-7}$
q_3	$1*10^{-10}$	0.01
q_4	0.5	0.01
q_5	$2*10^{-6}$	$1.98*10^{-5}$
q_6	$1.01*10^{-7}$	$4*10^{-5}$
q_7	0.5	0.99
q_8	$1*10^{-8}$	0.99
q_9	$1*10^{-8}$	$3.96*10^{-6}$

为提升飞行安全，保障公众利益，应对上述底事件的发生，航空界可采取针对性的应对措施：1）加强安检，避免杀伤性武器带入飞机。如果武器带入飞机，劫机者能够轻而易举破门和挟持飞行员，进而控制飞机作出重大伤害性事件；

2）加强飞行员失常监测和引导。由于飞行员思想状态具有一定的隐蔽性和欺骗性。因此航空公司要重在平时的思想状态监测、引导和防范，要在航前重点监测；

3）针对飞行员离开驾驶舱后无法进入驾驶舱的缺陷，必须从驾驶舱门控制逻辑上加以改进，使得飞行员离开后仍然能够打开驾驶舱门。

3　驾驶舱门控制系统控制逻辑改进

由上文事件故障树分析可见，此类驾驶舱门禁系统虽然满足了反恐防暴的要求，但在蓄意坠机事件中反而成为了悲剧发生的必要条件。其原因并非技术问题，而是飞机设计时预设的场景给予了驾驶舱内飞行员过高的权限。

因此，针对蓄意坠机事件，必须重新设计驾驶舱门控制逻辑，赋予离开驾驶舱的飞行员能够打开驾驶舱门的权限，避免类似事件再度发生。

为了“让合适的人在恰当的时刻拥有进出驾驶舱的最高权限”，本文研究确定了门禁最高权限优化分配方案如下表 3。

表 3　多种预设场景的门禁最高权限分配

序号	预设场景	最高权限分配
1	双飞行员在座，无失能，遭遇劫机	驾驶舱机组
2	单飞行员在座，无失能，无劫机	离座飞行员
3	单飞行员在座，无失能，遭遇劫机	驾驶舱机组
4	双飞行员在座，单人失能，无劫机	客舱机组
5	双飞行员在座，双人失能，无劫机	客舱机组

由表 3 中的最高权限分配方案可见，遭遇劫机时，驾驶舱内的飞行机组有门禁最高权限，消除了恐怖分子突袭驾驶舱的可能。单飞行员在座时，离座的飞行员有门禁最高权限，能够及时返回驾驶舱中，防止在座飞行员实现蓄意坠机的意图。单飞行员在座且遭遇劫机时，驾驶舱内的飞行机组重新获得门禁最高权限，防止恐怖分子趁隙进入驾驶舱。出现驾驶舱飞行机组失能情况时，客舱机组有进入驾驶舱的最高权限。该方案能够有效应对多种预设场景，预防劫机和蓄意坠机事件，保证飞行安全。

根据上述权限更改思路，重新设计驾驶舱开门逻辑流程如图 4 所示。

正常飞行时，机组将两侧旋钮都放在 AUTO 位。左右两座飞行员在接到异常的客舱进入请求后，同时将门禁控制旋钮调至 DENY 位置。此时驾驶舱舱门锁死，两名飞行员共同拥有最高权限。任一侧旋钮未调至 DENY 位置或从 DENY 位置离开或两座飞行员操作间隔超过某一限度，则门锁仍然可由客舱输入紧急进入密码予以打开。

在巡航阶段，任一飞行员均可离开驾驶舱。离开前需先将一侧门禁控制旋钮调至“LEAVE”位置。另一侧门禁控制旋钮仍然在“AUTO”位置。驾驶内的舱门密码器（或指纹采集器）激活。飞行员出舱时须在舱门密码器上点击设置个人密码（或在指纹采集器上使用某个手指采集指纹）才能开门。该飞行员离开后，舱门关闭自动上锁。此时最高进出权限转是该飞行员的个人密码（或某手指指纹）。实现上述驾驶舱门禁控制逻辑电路图如图 5 所示。

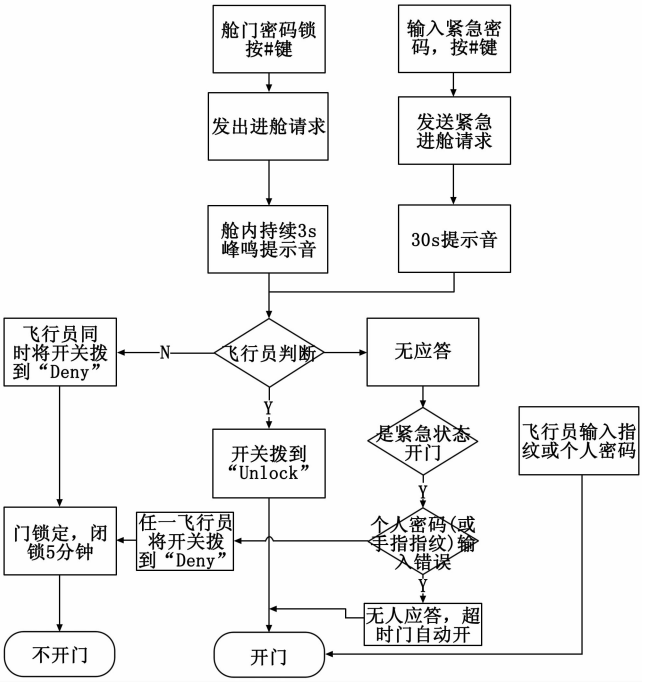

图 4　改进后驾驶舱门控制逻辑流程图

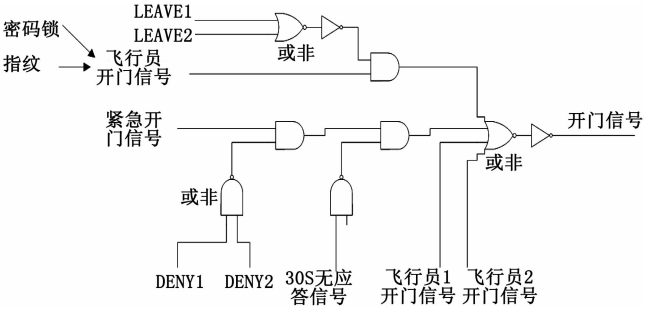

图 5　改进后驾驶舱门禁控制逻辑电路图

4　改进后可靠性分析

根据上述改进思路——重新赋予离开驾驶舱的飞行员开门权限，故障树中的中间事件 G6 和底事件 X8 得以消除。故障树的最小割集也缩减为 8 个。故障树顶事件的发生率大幅度下降，为 $5.02 * 10^{-11}$。改进后的底事件重要度如表 4 所示。

表 4　改进后底事件重要度

底事件	概率重要度	关键重要度
q_1	$2 * 10^{-6}$	0.002
q_2	$2 * 10^{-6}$	$3.98 * 10^{-5}$
q_3	$1 * 10^{-10}$	0.996
q_4	0.5	0.996
q_5	$2 * 10^{-6}$	0.002
q_6	$1.01 * 10^{-7}$	0.004
q_7	$2.02 * 10^{-6}$	$4.02 * 10^{-4}$
q_8	0	0
q_9	$1 * 10^{-8}$	$3.98 * 10^{-4}$

（下转第 53 页）