文章编号:1674-8190(2024)02-108-09

基于STPA的飞机交流系统供电转换安全性分析方法研究

田毅[1,3],陈杰辉[2],袁海宵[4],马世耀[2]
(1.中国民航大学 安全科学与工程学院,天津 300300)
(2.中国民航大学 中欧航空工程师学院,天津 300300)
(3.天津市航空装备安全性与适航技术创新中心,天津 300300)
(4.上海飞机设计研究院 电气集成部,上海 201210)

摘 要: 飞机交流发电系统是整机的主要电力来源,应对其进行完善的安全性分析。传统安全性分析方法对系统组件间非线性交互引起的安全问题关注较少,当研制型号支持数据不足时,存在分析遗漏风险。根据典型交流发电系统供电转换过程基本特点,基于STPA方法构建安全控制结构图,识别不安全控制行为(UCA),引入相似系统的失效模式及影响分析(FMEA)结果,分析UCA致因因素和致因场景,使用时间自动机理论的形式化工具进行系统建模与验证;通过专家评判及事故对比来验证该方法的正确性。结果表明:在传统分析方法的基础上引入STPA方法,能够有效识别出不安全控制行为和事故发生的原因,该方法可以作为传统方法的有效补充。

关键词: 飞机交流发电系统;STPA;UCA;时间自动机理论
中图分类号: V242.2 **文献标识码:** A
DOI: 10.16615/j.cnki.1674-8190.2024.02.12

Research on the safety analysis method of power supply conversion of aircraft AC system based on STPA

TIAN Yi[1,3], CHEN Jiehui[2], YUAN Haixiao[4], MA Shiyao[2]
(1. College of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China)
(2. Sino-European Institute of Aviation Engineering, Civil Aviation University of China, Tianjin 300300, China)
(3. Tianjin Aviation Equipment Safety and Airworthiness Technology Innovation Center, Tianjin 300300, China)
(4. Electrical Integration Department, Shanghai Aircraft Design and Research Institute, Shanghai 201210, China)

Abstract: The aircraft AC power generation system is the main source of power for the whole aircraft, so a complete safety analysis is required. Traditionally safety analysis pays less attention to the security problems caused by nonlinear interaction between system components. Especially when the support data of the developed model is insufficient, there is a risk of analysis omission. According to the basic characteristics of the power supply conversion process of AC power generation system, this paper constructs a safety control structure chart and identify unsafe control action (UCA) based on the STPA method, and introduces the failure model and effect analysis (FMEA) of similar system to analyse the UCA cause factor and cause scenario. Using formal tool of timed automata theory, the system modeling and verification are carried out. The correctness of this methods is confirmed by expert evaluation and accident comparison. The result shows that the introduction of STPA based on traditional safety analysis methods can effectively identify unsafety control action and the causes of accident, which can be an effective supplement to the traditional method.

Key words: AC power system of aircraft; STPA; UCA; the theory of timed automata

收稿日期: 2023-02-14; **修回日期:** 2023-05-11
基金项目: 天津市航空装备安全性与适航技术创新中心开放基金(JCZX-2022-KF-07)
通信作者: 陈杰辉(1997—),男,硕士研究生。E-mail: cauccjh@163.com
引用格式: 田毅,陈杰辉,袁海宵,等. 基于STPA的飞机交流系统供电转换安全性分析方法研究[J]. 航空工程进展,2024,15(2):108-116.
TIAN Yi, CHEN Jiehui, YUAN Haixiao, et al. Research on the safety analysis method of power supply conversion of aircraft AC system based on STPA[J]. Advances in Aeronautical Science and Engineering, 2024, 15(2): 108-116. (in Chinese)

0　引　言

航空器的运行安全一直是人们重点关注的问题。随着航空技术的发展,航空器系统和部件的可靠性在不断地完善,但航空事故和危险事件仍时有发生,重大航空事故给人们造成严重的生命和财产损失。大型客机交流发电系统作为飞机关键系统之一,向飞机用电设备提供三相交流电,决定发电机的电能输出和供电方式的转换等[1]。交流发电系统的正常运行直接影响到整机的安全。

国内外研究者们基于ARP4761中传统安全性分析方法对飞机发电系统开展安全性分析,传统安全性分析方法包括故障树分析和失效模式及影响分析(Failure Mode and Effect Analysis,简称FMEA)等。孙永全等[2]通过分析飞机交流发电系统各组成部分的可靠性逻辑关系,构造系统的动态故障树,对系统进行安全性分析;曹涛等[3]基于故障树确定飞机电源系统在设计过程中引起系统故障的各种因素及逻辑关系,确定故障发生的各种可能原因,找出系统设计的薄弱环节,采取措施以提高系统安全性;Telford等[4]利用故障树分析、马尔科夫分析和贝叶斯分析相结合的方法,减少电动飞机电源系统可靠性分析的计算量;Nystrom等[5]采用故障树分析方法对飞机电源系统进行安全性分析,发现系统设计两个冗余比较合理。传统安全性分析方法重点关注组件失效问题,假设事故是由线性故障链引发的[6],忽视了组件之间非线性交互所引发的安全性问题。随着多电飞机概念的提出,飞机发电系统内部控制关系愈加复杂,传统安全性分析方法难以进行全面分析,亟需探索更为有效的安全性分析方法。

系统理论分析过程(System Theory Process Analysis,简称STPA)是美国麻省理工学院提出的一种基于系统理论事故过程模型(Systems Theoretic Accident Model and Process,简称STAMP)的新型安全性分析方法[7]。STPA基于系统理论和控制理论,把复杂系统的安全性分析当成控制问题来解决。不同于传统安全性分析方法的线性分析,STPA充分考虑组件之间的非线性交互,能有效分析交互组件导致危险发生的过程[8]。

目前,针对飞机交流发电系统进行STPA分析的相关研究未见报道,故本文基于STPA方法构建系统安全控制结构,识别不安全控制行为(Unsafe Control Action,简称UCA);采用形式化建模工具UPPAAL建立系统形式化模型并进行UCA验证,借助相似型号的FMEA结论识别UCA的危险致因因素和致因场景;通过专家评判以及事故对比分析结果,验证本文所提基于STPA的飞机交流系统供电转换安全性分析方法的正确性和有效性。

1　飞机交流系统供电转换原理

大型客机有单独供电和并联供电两种供电方式。对于双发动机或双发电机飞机,一般都采用单独供电方式,以波音737NG为例,如图1所示。交流发电系统为飞机提供115 V/400 Hz的交流电[9],系统由左/右主交流发电子系统和辅助交流发电子系统构成。主交流发电子系统包括整体传动发电机(Integrated Drive Generator,简称IDG)、发电机控制器(Generator Control Unit,简称GCU)、汇流条功率控制器(Bus Power Control Unit,简称BPCU)、发电机电路断路器(Generator Circuit Breaker,简称GCB)、汇流条连接断路器(Bus Tie Breaker,简称BTB)和交流转换汇流条(Transfer BUS);辅助交流发电子系统包括APU发电机(Auxiliary Power Unit Generator)、APU发电机控制器(APU Generator Control Unit,简称AGCU)和辅助电源断路器(Auxiliary Power Breaker,简称APB)。

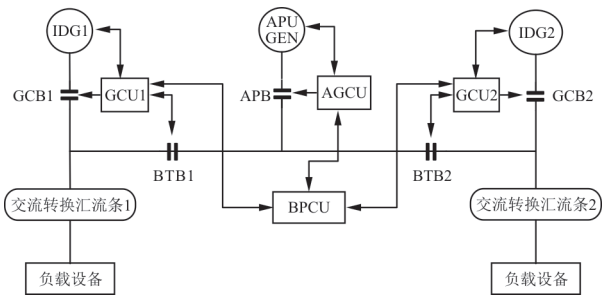


图1　单独供电模式简化控制原理图

Fig. 1　Schematic of independence power supply mode

正常供电时,由各台发电机分别向各自的交流汇流条供电,两个供电通道相互独立。当其中一台发电机如IDG2发生故障时,GCU2控制GCB2

断开，BPCU收到GCB2断开信号时，发出控制指令使GCU1和GCU2分别接通BTB1和BTB2，两个交流汇流条相连，实现2号交流汇流条从IDG2供电到1号交流汇流条供电的交流供电转换。

根据用电设备的重要性，飞机上的汇流条一般分为主汇流条（正常汇流条）、转换汇流条（重要汇流条）和应急汇流条（备用汇流条）三个级别[10]。不会对飞行安全造成影响的设备由主汇流条供电，对飞行安全有重要影响的设备由转换汇流条供电，直接关系到飞行安全的设备由应急汇流条供电。

GCU通过监视和检查各自IDG提供的电流，频率、电压等实现对系统和IDG的保护；GCU还监控GCB和BTB的状态，并发送控制信号。断路器是主要的电源切换执行单元，在断路器内部有主触点和辅助触点，主触点负责传导电流，辅助触点提供断路器状态指示，并向控制组件（GCU、BPCU）和面板P5-4的指示灯指示断路器的状态。BPCU负责飞机电网的电能分配、控制与保护。BPCU还能监控来自外部电源的电力质量和功耗。

2 STPA形式化拓展

STPA通过构建系统的安全控制结构来描述系统的组成和组件间的控制—反馈路径，进而分析潜在的危险，利用致因分析框架图识别致因场景，如图2所示。该方法的实施一般分为四个步骤：定义分析目的，建立控制结构，识别不安全控制行为（UCA），识别致因场景。

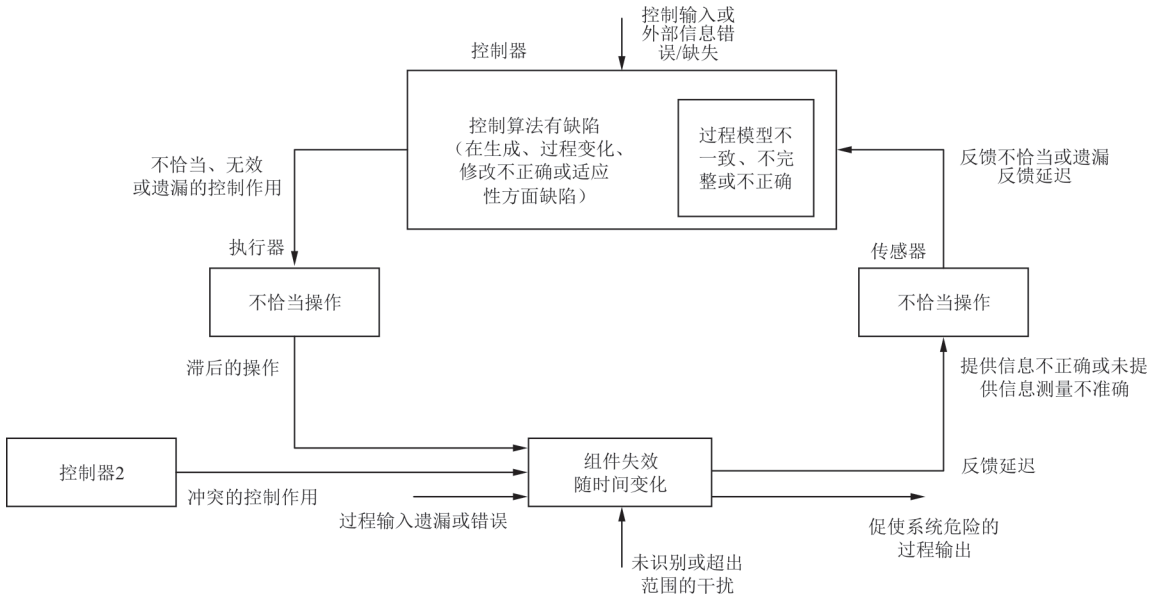


图2 STPA致因分析框架图

Fig. 2 STPA causal analysis framework diagram

为了准确识别更详细的UCA致因因素和致因场景，关注系统低层级组件的失效情况，考虑基于系统FMEA的数据进行STPA分析。FMEA首先识别子系统和系统中组件的失效模式，然后确定失效模式的失效原因。这个过程与STPA识别UCA进而确定UCA的致因因素和致因场景相似[11]。STPA中控制行为的定义与FMEA中部件功能的定义类似，因此将FMEA部件的失效模式转化为UCA；从FMEA的失效原因提取UCA致因因素和致因场景。

由于建立的STPA控制结构图用于直观描述系统组件间的控制与反馈关系，不能进一步进行形式化验证，因此将基于时间自动机理论的模型检测工具UPPAAL引入到STPA的分析中。将系统控制结构图转换成UPPAAL模型，以验证识别的不安全控制行为（UCA），分析过程如图3所示。首先定义系统级事故与危险，根据控制原理图构建安全控制结构图，辨识控制转换过程中存在的不安全控制行为UCA，然后根据安全控制结构图与系统架构信息建立形式化模型，建模完成后进行模型正确性验证以及UCA可达性验证，最后对UCA进行致因场景分析。

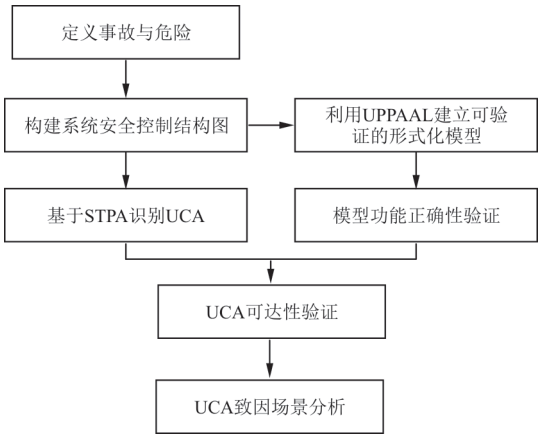


图3　STPA与形式化方法结合的安全性分析流程图

Fig. 3　Flow chart of safety analysis combining STPA and formal method

3　交流系统供电转换安全性分析实施

3.1　定义事故与危险

飞机在飞行过程中,交流发电系统故障可能导致三种不同的事故:人员伤亡(A1),飞机受损(A2),飞行任务失败(A3)。根据交流发电系统级事故相关的定义以及系统的应用场景,从飞机性能与安全裕度(H1),机组人员的工作负荷(H2)以及乘客状态(H3)进行系统级危险分析[12],包括飞机性能与安全裕度的略微降低(H1-1),飞机性能与安全裕度的显著降低(H1-2),飞机性能和安全裕度的极大降低(H1-3),丧失飞机性能(H1-4);机组人员工作负荷轻微增加(H2-1),机组人员工作负荷显著增加(H2-2),机组人员出现身体不适的情况(H2-3),机组人员丧失对飞机的控制能力(H2-4);给乘客带来不便(H3-1),乘客身体感到不适且可能会受伤(H3-2),乘客受到严重或者致命伤害(H3-3)。

3.2　构建安全控制结构

安全控制结构是一个控制—反馈回路,系统不同组件之间通过相关的控制命令和信息反馈进行交互。飞行员通过驾驶舱面板开关对交流发电系统进行控制并获取系统反馈的状态信息;控制器GCUs、BPCU和AGCU对系统进行控制与保护,包括发电机电源质量的监控和控制、断路器通断控制和位置信息监控。交流发电系统安全控制结构如图4所示。

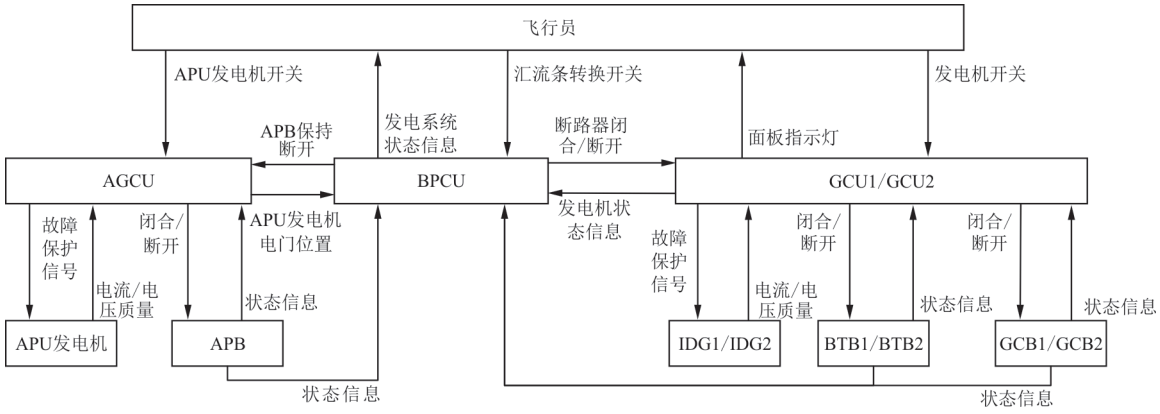


图4　交流发电系统供电转换控制结构图

Fig. 4　AC power system circuit breaker control structure diagram

3.3　识别不安全控制行为

STPA分析中,危险的产生被认为是由于UCA的实施造成的。UCA是特定情景及最坏环境下可能导致危险的控制行为,一般可分为四种:没有提供相应控制行为导致危险,提供相应控制行为后导致危险,提供相应控制行为但提供节点过早、过晚或顺序错误导致危险,提供的控制行为持续时间太长或停止过早导致危险[13]。结合交流发电系统FMEA中相关的故障模式和故障原因,获得更具体的UCA和致因场景。根据供电转换控制结构图(图4)中相关控制器和断路器之间的交互情况,基于已有某相似型号飞机交流发电系统的FMEA数据,详细识别供电转换过程中可能出现的UCA,如表1所示。

表1 不安全控制行为
Table 1 Unsafe control action

控制行为	未提供控制行为	提供错误的控制行为	控制行为提供节点错误	控制行为时长错误
BTB闭合/断开控制行为	UCA-1：GCU控制器在单发电机失效情况下，未提供BTB闭合命令(H-1，H-2) UCA-2：GCU控制器在单发电机供电情况下，未提供BTB闭合命令(H-1，H-2)	UCA-3：GCU控制器在失效发电机重启后，提供BTB闭合命令(H-1，H-2，H-3)	N/A	N/A
GCB闭合/断开控制行为	UCA-4：GCU控制器在单发电机失效情况下，未提供GCB断开命令(H-1，H-2)	UCA-5：GCU控制器在单发电机失效情况下，提供GCB闭合命令(H-1，H-2)	N/A	N/A
APB闭合/断开控制行为	UCA-6：AGCU控制器在单发电机失效情况下，未提供APB闭合命令(H-1，H-2)	UCA-7：AGCU控制器在单发电机失效情况下，提供APB断开命令(H-1，H-2)	N/A	N/A

3.4 基于时间自动机理论的形式化验证

根据系统的特性，选用基于时间自动机理论的形式化建模工具UPPAAL实现交流系统供电转换控制交互关系的建模，建模完成后，采用巴科斯范式(Backus-Naur Form，简称BNF)语法验证时间自动机网络[14-15]，验证模型系统的逻辑正确性以及不安全控制行为UCA的验证。

3.4.1 建模方法

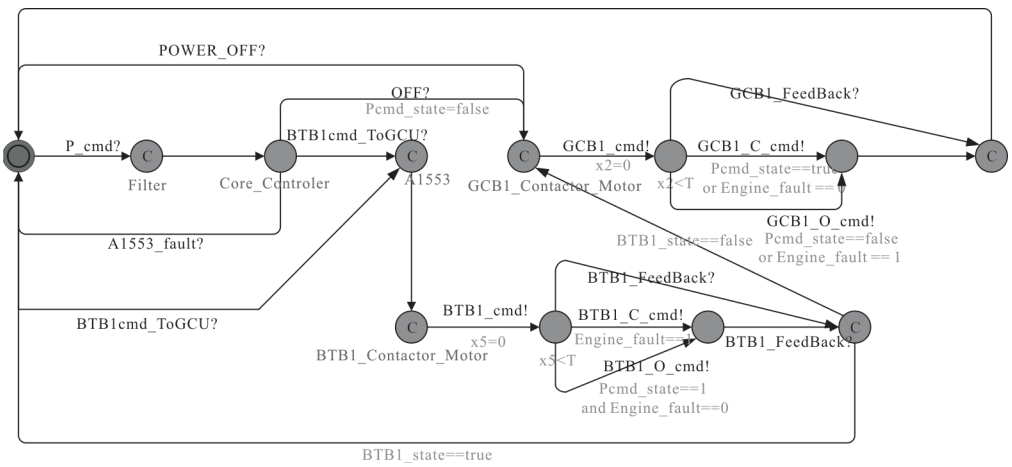
时间自动机是一个(S,S_0,C,A,E,I)的六元组，其中S是位置的状态位置集合；$S_0\in S$是初始的状态位置；C是时钟变量集合；A是事件集合；E是一个状态转移集合，I是一个映射，为状态位置集合S中每个s映射一个时钟约束。时间自动机网络是一组时间自动机的积，不同的时间自动机之间通过握手进行同步通信，可用于模拟系统内组件之间的控制与反馈的关系，用$a!$代表发出同步的信息，用$a?$代表接收到同步信息，a为同步的名称。当一个时间自动机发送完$a!$，则接收到$a?$的另一个时间自动机同步转移到下一个状态位置。

UPPAAL能实现系统内组件的不同状态转移，能对不同组件间的控制—反馈关系进行描述，并分析时间自动机网络可达性，从而验证系统安全相关性质。对系统进行建模时可以在状态转移基础上考虑时钟，可以对交流发电系统涉及的时序关系进行定义。

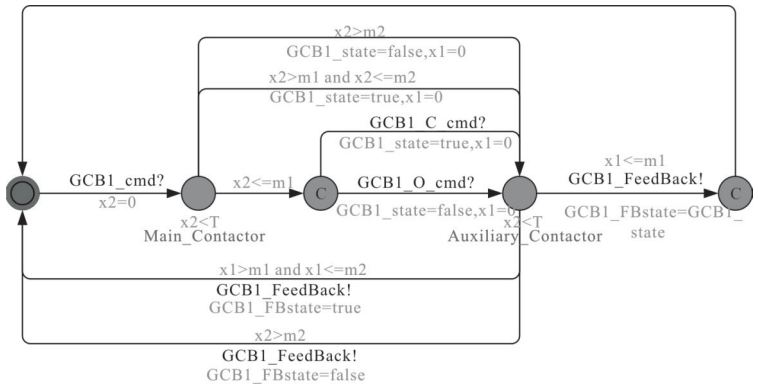
3.4.2 系统建模

根据交流发电系统相关组件内部结构、功能、组件失效信息以及发电系统供电转换控制结构图进行UPPAAL模型的建立。在断路器BTB和GCB的控制关系中，左右两侧组件和控制关系都相同，并且当出现单发失效供电时，BTB1和BTB2其中任意一个断开，都会导致故障侧转换汇流条出现断电情况，这种情况下，两个BTB是一种或关系，故只需完成一侧控制关系的UPPAAL建模。

模型中通过时钟变量的定义来区分组件内相关结构的工作状态，m1代表结构工作最大时间限制，当时钟变量小于或者等于m1时，结构处于正常工作状态；当时钟变量大于m1时，结构处于故障状态，如断路器触点包括故障断开和故障闭合两种故障状态。系统相关组件的部分UPPAAL模型图如图5所示。



(a) GCU时间自动机



(b) GCB时间自动机

图5　相关组件UPPAAL模型图(部分)

Fig. 5　UPPAAL model diagram of the related components (portion)

3.4.3　模型正确性验证

建模完成后,需要进行模型正确性相关验证。除了人工检查,还需要通过UPPAAL验证器进行验证,验证模型是否符合预期的定义功能和性质。验证原理是利用时序逻辑公式在时间自动机网络模型中进行穷举搜索,具体逻辑公式是通过将需要验证的属性转化为BNF语句。BNF语法基本定义包括:E< >p表示存在一条转移路径,p在该路径下某一状态为真;E[ ]p表示存在一条转移路径,p在该路径下所有状态下均为真;A< >p表示对于所有路径,p在任一路径的某一状态为真;A[ ]p表示对于所有路径,p在任一路径的所有状态下均为真。P imply Q表示只要P发生则Q发生。

验证通过说明建立的自动机网络模型能够覆盖系统逻辑和功能状态,保证模型的完整性。验证的性质及结果如表2所示,可以看出:模型在表2中所要验证的系统性质均能满足。

表2　系统逻辑正确性和活性验证

Table 2　System logic correctness verification

验证性质	BNF表达式	结果
系统无锁死	A[ ] not deadlock	满足
发电机开关置于ON位,GCU给相应BTB发出断开命令	E<>(Pcmd_state==1) imply (GCU_Controler.BTB_Contactor_Motor and BTBcmd_o==0 and BTB.Auxiliary_Contactor)	满足
BTB接收到断开命令,动作断开	E<>((BTBcmd_o == 0 and BTB.Auxiliary_Contactor) imply (BTB_state==0))	满足
GCU监控BTB状态指示断开,IDG电源质量满足并保持20 s,GCU发出GCB闭合命令	E<>((BTB_FBstate == 0 and GCU_Controler.GCB_Contactor_Motor and IDG_Gen.Power_Quality_OK and Time_Powerok>=20) imply (GCBcmd_o==1))	满足
GCB接收到闭合命令,动作闭合	E<>((GCBcmd_o == 1 and GCB.Auxiliary_Contactor) imply (GCB_state==1))	满足
IDG发电机故障失效,GCU检测到IDG失效情况,发出失效IDG侧的GCB断开命令	E<>(IDG_Gen.Generator_failure and Gen_F_FB==1 and GCU_Controler.GCB_Contactor_Motor imply GCBcmd_o == 0)	满足
失效IDG侧的GCB接收到断开命令,动作断开	E<>((GCBcmd_o == 0 and GCB.Auxiliary_Contactor) imply (GCB_state==0))	满足
APU发电机开关置ON位,APU发电机电源质量满足要求,AGCU给APB发出闭合命令	E<>(P5_Modules.APUOn and APU_Gen.Power_Normal and AGCU_Controler.APB_Contactor_Motor) imply (APBcmd_o == 1)	满足
APB接收到闭合命令,动作闭合	E<>(APBcmd_o == 1 and APB.Auxiliary_Contactor) imply (APB_state == 1)	满足
APB闭合后,BPCU给GCU发出失效IDG侧的BTB闭合命令	E<>(APB_state == 1 and BPCU_Controler.Communication_Module and GCU_Controler.BTB_Contactor_Motor) imply (BTBcmd_o == 1)	满足
失效IDG侧的BTB接收到闭合命令,动作闭合	E<>((BTBcmd_o == 1 and BTB.Auxiliary_Contactor) imply (BTB_state == 1))	满足

3.4.4 不安全控制行为验证

根据3.4.1节建立的UPPAAL模型可进行状态可达性分析，利用BNF语句加以验证，可以验证STPA所识别的UCA。验证结果如表3所示。验证满足说明至少存在一条转移路径使得UCA发生，验证不满足说明不存在转移路径使得UCA发生。

表3 UCA可达性验证

Table 3 UCA reachability verification

UCA	BNF验证语句	结果
UCA-1	E<>(IDG_Gen. Generator_failure and Gen_F_FB == 1 and BTBcmd_o==0 and BTB_state == 0 and BTB. Auxiliary_Contactor)	满足
UCA-2	E<>(IDG_Gen. Generator_failure and APU_Gen. Power_abNormal and Gen_F_FB == 1 and BTBcmd_o== 0 and BTB_state == 0)	满足
UCA-3	E<>(IDG_Gen. Power_Quality_OK and Gen_F_FB == 0 and Time_Powerok >= 20 and BTBcmd_o==1)	不满足
UCA-4	E<>(IDG_Gen. Generator_failure and GCU_Controler. Idle and GCBcmd_o == 0 and GCB_state == 1)	满足
UCA-5	E<>(IDG_Gen. Generator_failure and Gen_F_FB == 1 and GCBcmd_o == 1)	不满足
UCA-6	E<>(IDG_Gen. Generator_failure and Gen_F_FB == 1 and APBcmd_o == 1 and APB. Auxiliary_Contactor and APB_state ==0)	满足
UCA-7	E<>(IDG_Gen. Generator_failure and Gen_F_FB == 1 and APBcmd_o == 0 and APB. Auxiliary_Contactor and APB_state == 0)	满足

3.5 致因场景分析

通过专家评判，判别识别出的UCA对系统确有安全性影响，并且UCA-1的发生会使某一交流转换汇流条出现断电情况，导致的安全风险大。本文以“UCA-1：GCU控制器在单发电机失效情况下，未提供BTB闭合命令”为例开展进一步分析。通过交流发电系统供电转换控制结构和STPA致因分析框架，可以得到交流供电转换的致因分析框架，包括产生危险的4类原因，14条通用因素，如图6所示。

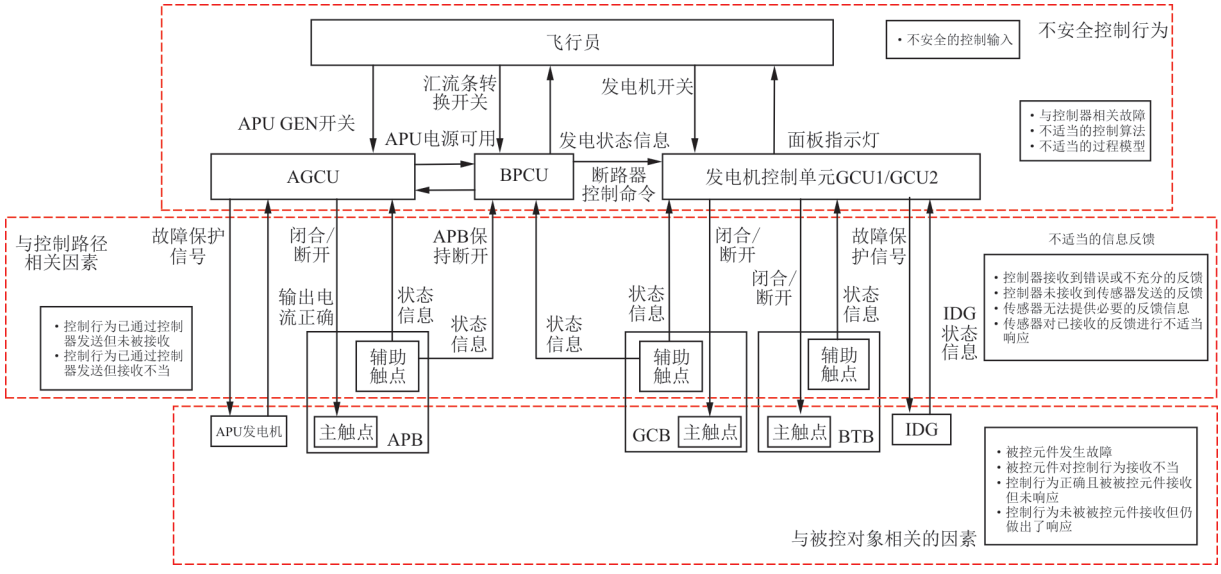


图6 交流发电系统致因分析框架

Fig. 6 Framework for causal analysis of AC power system

根据致因分析能够识别出UCA-1的致因场景如下:

1) 与反馈信息不适当相关的致因场景1

单发电机失效,GCU控制器未提供BTB闭合命令是因为GCU错误地认为发电机失效侧的GCB处于闭合状态(GCB和BTB状态互锁),GCU过程模型发生错误。GCB处于断开状态,由于GCB辅助触点故障(或GCU对GCB辅助触点信号检测失效),导致反馈给GCU错误的状态信息,GCU未驱动BTB闭合。

2) 与控制路径相关的致因场景2

控制器GCU在单发电机失效情况下提供BTB闭合命令,由于BTB驱动线路失效,BTB无法接收到控制器的控制指令,因此BTB没有受控闭合。

3) 与被控对象相关的致因场景3

控制器GCU在单发电机失效情况下提供BTB闭合命令,由于BTB主触点故障断开,BTB不能受控闭合。

在上述三类情景之下,都能够导致UCA-1的发生。2011年4月25日,瑞安航空一架波音737-800型飞机在起飞过程中出现一个交流转换汇流条断电,造成自动安定面配平停止工作,应答机上高度报告消失等关联故障,导致飞机迫降。事故调查报告[16]指出,事故是因为IDG2发生相间短路,GCB2断开将故障的IDG2与2号转换汇流条隔离;由于GCB2辅助触点故障,给GCU2和BPCU提供GCB2处于闭合的错误信号,控制器错误认为IDG2还连接着2号转换汇流条,导致控制器控制逻辑发生错误。由于单独供电模式,控制器锁定BTB处于断开位置,导致APU发电机和1号转换汇流条中的电源无法接入到2号转换汇流条,最终出现2号转换汇流条失去电源的情况。分析得到的致因场景1能够覆盖事故调查结论。

4　结　论

1) 通过飞机交流发电系统的应用,验证了基于系统的FMEA数据,并将STPA与形式化分析相结合的方法能够有效识别交流发电系统潜在发生的UCA和致因场景。该方法可作为飞机电源系统安全性分析的有效补充手段,也可用于事故调查分析。

2) 瑞安航空事故报告指出,系统设计阶段采用的传统故障树分析没有涉及到该事故致因场景,而本文通过STPA方法识别出事故致因场景的发生,能够有效解决传统安全性分析方法忽视组件之间非线性交互的问题。

参 考 文 献

[1] 周洁敏. 飞机电气系统[M]. 北京: 科学出版社, 2010.
ZHOU Jiemin. Aircraft electrical system[M]. Beijing: Science Press, 2010. (in Chinese)

[2] 孙永全, 任和, 陈曦, 等. 基于Monte-Carlo模拟的飞机交流发电系统故障树分析[C]// 全国机械行业可靠性技术学术交流会暨可靠性工程分会全体委员大会. 杭州: 中国机械工程学会, 2013: 137-142.
SUN Yongquan, REN He, CHEN Xi, et al. Fault tree analysis of aircraft AC power generation system based on Monte-Carlo simulation[C]// National Academic Exchange Conference on Reliability Technology in the Machinery Industry and All Committee Members' Meeting of the Reliability Engineering Branch. Hangzhou: Chinese Mechanical Engineering Society, 2013: 137-142. (in Chinese)

[3] 曹涛, 吴善永, 方钧华. 基于故障树的飞机电源系统可靠性分析研究[C]// 第九届长三角科技论坛——航空航天科技创新与长三角经济转型发展分论坛. 南京: 江苏省航空航天学会等, 2012: 329-333.
CAO Tao, WU Shanyong, FANG Junhua. Reliability analysis of aircraft power system based on fault tree analysis[C]// The 9th Yangtze River Delta Science and Technology Forum-Aerospace Science and Technology Innovation and Yangtze River Delta Economic Transformation and Development Sub Forum. Nanjing: Jiangsu Aerospace Society etc, 2012: 329-333. (in Chinese)

[4] TELFORD R D, GALLOWAY S J, BURT G M. Evaluating the reliability & availability of more-electric aircraft power systems[C]// International Universities Power Engineering Conference. [S.l.]: IEEE, 2012: 17-23.

[5] NYSTROM B, AUSTRIN L, ANKARBACK N, et al. Fault tree analysis of an aircraft electric power supply system to electrical actuators[C]// International Conference on Probabilistic Methods Applied to Power Systems. USA: IEEE, 2006: 11-15.

[6] 崔利杰, 田宇, 丛继平, 等. STPA与ARP4761中的安全性分析方法对比研究[J]. 航空工程进展, 2020, 11(4): 508-516.

CUI Lijie, TIAN Yu, CONG Jiping, et al. A comparative study on the safety analysis methods of STPA and ARP4761 [J]. Advances in Aeronautical Science and Engineering, 2020, 11(4): 508-516. (in Chinese)

[7] 肖国松，刘嘉琛，董磊，等. 面向IMA通用系统管理的STPA安全性分析[J]. 中国安全科学学报，2021，31(9)：8-14.
XIAO Guosong, LIU Jiachen, DONG Lei, et al. STPA safety analysis on IMA generic system management[J]. China Safety Science Journal, 2021, 31(9): 8-14. (in Chinese)

[8] 李浩. 基于STAMP理论的机载显示系统安全性分析方法研究[D]. 天津：中国民航大学，2020.
LI Hao. Research on safety analysis method of airborne display system based on the STAMP theory[D]. Tianjin: Civil Aviation University of China, 2020. (in Chinese)

[9] 杨乐. 飞机电源系统的建模方法研究[J]. 科学技术与工程，2013，13(9)：2611-2615.
YANG Le. Research on modeling approach of aircraft electrical power systems[J]. Science Technology and Engineering, 2013, 13(9): 2611-2615. (in Chinese)

[10] 刘建英，任仁良. 飞机电源系统[M]. 北京：中国民航出版社，2013.
LIU Jianying, REN Renliang. Aircraft power system[M]. Beijing: China Civil Aviation Publishing House, 2013. (in Chinese)

[11] CHEN L, JIAO J, ZHAO T. A novel hazard analysis and risk assessment approach for road vehicle functional safety through integrating STPA with FMEA[J]. Applied Sciences, 2020, 10(21): 7400.

[12] 修忠信. 民用飞机系统安全性设计与评估技术概论[M]. 上海：上海交通大学出版社，2013.
XIU Zhongxin. System safety design & assessmet in civil aircraft [M]. Shanghai: Shanghai Jiao Tong University Press, 2013. (in Chinese)

[13] NANCY L. A new accident model for engineering safer systems[J]. Safety Science, 2004, 42: 237-270.

[14] LONGJI D A, EMILIA V. System safety assessment based on STPA and model checking[J]. Safety Science, 2018, 109: 130-143.

[15] 邓雪峰，孙瑞志，聂娟，等. 基于时间自动机的温室环境监控物联网系统建模[J]. 农业机械学报，2016，47(7)：301-308.
DENG Xuefeng, SUN Ruizhi, NIE Juan, et al. Greenhouse environment monitoring IOT system modeling based on timed automata[J]. Transactions of the Chinese Society for Agricultural Machinery, 2016, 47(7): 301-308. (in Chinese)

[16] SIMON H. Incident: Ryanair B738 near Stockholm on Apr 25th 2011, instrument failure, multiple electrical problems [EB/OL]. (2012-11-22)[2023-02-14]. http://avherald.com/h? article=43b86893/0000&opt=4865.

(编辑：马文静)