

中文引用格式:董磊,刘嘉琛,孙紫荆,等. 面向 SPO 模式多阶段任务的 IMA 系统级联影响分析[J]. 中国安全科学学报, 2026, 36(2): 84-92.

英文引用格式:DONG Lei, LIU Jiachen, SUN Zijing, et al. Cascading effect analysis of IMA system for multi-phased mission in SPO mode[J]. China Safety Science Journal, 2026, 36(2): 84-92.

面向 SPO 模式多阶段任务的 IMA 系统 级联影响分析*

董磊^{1,2}副研究员, 刘嘉琛^{**3}讲师, 孙紫荆⁴工程师,
陈曦^{1,2}助理研究员, 王鹏^{1,2}研究员

(1 中国民航大学 民航航空器适航审定技术重点实验室, 天津 300300; 2 中国民航大学 科技创新研究院, 天津 300300; 3 空军工程大学 装备管理与无人机工程学院, 陕西 西安 710051;
4 航空工业西安航空计算技术研究所, 陕西 西安 710065)

中图分类号: X949

文献标志码: A

DOI: 10.16265/j.cnki.issn1003-3033.2026.02.0148

基金项目: 中央高校基本科研业务费(3122024037); 民用航空器适航审定技术重点实验室开放基金资助(SH2023101701)。

【摘要】 为解决单一飞行员驾驶(SPO)模式下综合模块化航电(IMA)系统安全性分析状态空间爆炸、致因关系不明确等问题, 首先, 定义 SPO 模式多阶段任务剖面, 确定不同任务阶段的 IMA 系统驻留应用及失效判据; 然后, 引入级联影响分析(CEA)概念, 构建级联故障传播定量计算模型, 设计级联失效概率和级联风险系数评估故障在 IMA 系统中的传播速度、传播范围及影响程度; 最后, 针对 SPO 模式案例对比不同任务阶段和不同初始故障条件下 IMA 系统的故障传播影响趋势。结果表明: 所提模型能够表征 IMA 系统故障的直接影响和间接影响, 若以主飞行控制和综合导航为初始故障事件则更容易造成级联失效, 需要针对性地对关键驻留应用采取备份、监控或重构措施。

【关键词】 单一飞行员驾驶(SPO); 多阶段任务; 综合模块化航电(IMA); 级联影响分析(CEA); 驻留应用

Cascading effect analysis of IMA system for multi-phased mission in SPO mode

DONG Lei^{1,2}, LIU Jiachen³, SUN Zijing⁴, CHEN Xi^{1,2}, WANG Peng^{1,2}

(1 Key Laboratory of Civil Aircraft Airworthiness Technology, Civil Aviation University of China, Tianjin 300300, China; 2 Science and Technology Innovation Research Institute, Civil Aviation University of China, Tianjin 300300, China; 3 Equipment Management and UAV Engineering College, Air Force Engineering University, Xi'an Shaanxi 710051, China; 4 Xi'an Aeronautics Computing Technique Research Institute, Aviation Industry Corporation of China, Xi'an Shaanxi 710065, China)

Abstract: To address the problems of state-space explosion and unclear causal relationships in the safety analysis of IMA system under the future SPO mode, multi-phase mission profiles for the SPO mode were

* 文章编号: 1003-3033(2026)02-0084-09; 收稿日期: 2025-08-15; 修稿日期: 2025-12-21

** 通信作者: 刘嘉琛(1996—), 男, 陕西西安人, 博士, 讲师, 主要从事系统安全性设计与评估、航空人工智能可信性方面的研究。E-mail: jc0419@foxmail.com。

first defined, and the resident applications and fault criteria for different mission phases were identified. The concept of CEA was introduced, and a quantitative computational model for cascading fault propagation was developed. Methods for evaluating the probability of cascading faults and the cascade risk coefficient were designed to assess the propagation speed, scope, and impact severity of faults within the IMA system. Finally, a comparative analysis was conducted under an SPO scenario to examine how cascading faults affect the IMA system across different mission phases and initial fault conditions. The results show that the proposed model can characterize both the direct and indirect impacts of faults in the IMA system. When primary flight control and integrated navigation are initial fault events, cascading faults are more likely to occur, indicating that targeted backup, monitoring, or reconfiguration measures for key resident applications are required.

Keywords: single-pilot operations (SPO); multi-phased mission; integrated modular avionics (IMA); cascading effect analysis (CEA); resident applications

0 引言

在民用飞机智能化、低成本化的发展趋势下,国内外民航界正在积极探索和研发单一飞行员驾驶 (Single-Pilot Operations, SPO) 技术^[1]。SPO 将是未来民机发展的主要方向之一,其通过先进智能航电系统和地面操作员提供远程飞行支持服务,协助飞行机组实现对飞机运行的控制^[2-3]。

SPO 模式人机交互的特点在于自动化系统高度智能化,并且更加强调人机一体化,机器不再作为飞行员使用的工具,而是作为“副驾驶”与飞行员一起控制和管理飞机^[4]。目前,已有诸多研究开始尝试将智能化技术以功能应用的形式驻留在综合模块化航电 (Integrated Modular Avionics, IMA) 系统中,形成多种面向 SPO 模式的航电综合架构。如 LIM Yixiang 等^[5]提出包含飞行员负荷评估功能和任务管理功能的智能模块,并将其与飞行管理、通信及监视等功能进行综合,在考虑 IMA 技术标准的基础上构建面向 SPO 模式的航电功能分配方案;YIN 等^[6]以是否支持地面站和是否自动驾驶对 SPO 模式进行分类,分析不同 SPO 模式下 IMA 系统的航电功能需求变化情况,主要涉及通信、监视、导航、显示、平台计算和智能化功能;CHEN Yong 等^[7]从任务层、功能层、资源层和执行层对 SPO 模式下的航电系统进行建模,提出一种 DFCluster 算法来挖掘不同 SPO 模式任务的功能-资源矩阵及其对应潜在危险元素或传播机制;ZOLGHADRI 等^[8]引入学习支持组件来增强 SPO 模式下的飞行管理能力,强调驻留在 IMA 系统中的智能化模型需要注意计算负载优化、多传感器数据融合和网络安保等问题,以避免 SPO 模式的认知混淆与信息冲突。可以看出,IMA 系统

中航电功能与硬件资源不再一一对应,而是依据 SPO 模式的需求动态配置各不同航电功能所需资源,在提高资源利用率、增强航电系统灵活性和适应性等方面具有显著优势,但也对航电系统的综合设计技术与安全性设计与评估技术提出越来越高的要求^[9]。

当前民机的安全性工作是以中国民航规章 (China Civil Aviation Regulation, CCAR) 25.1309 条款^[10]为核心,以航空航天推荐准则 (Aerospace Recommended Practice, ARP) 4761A^[11]和 ARP 4754B^[12]等适航指导材料为基础开展的,安全性评估过程主要包括功能危害评估 (Functional Hazard Assessment, FHA)、初步系统安全性评估 (Preliminary System Safety Assessment, PSSA) 和系统安全性评估 (System Safety Assessment, SSA) 等,安全性分析方法主要包括故障树分析、关联图分析和马尔可夫分析等。然而,IMA 系统功能高度集成、资源高度共享、数据高度融合,这种高度综合化增加了系统的复杂性和故障耦合风险^[13]。虽然传统安全性分析方法已经发展的比较成熟,但随着航电系统综合范围的扩大和综合程度的加深,暴露出重复建模、致因关系不明确、状态空间爆炸等局限,难以准确描述 IMA 系统中复杂失效传播机制^[9,14]。近年来,部分学者开始考虑采用 4761A 附录中新补充的级联影响分析 (Cascading Effects Analysis, CEA) 解决上述问题。如杨海云等^[15]借鉴分层危害识别与传播分析 (Hierarchically Performed Hazard Origin and Propagation Studies, HIP-HOPS) 方法构建了 IMA 级联失效的层次化传播模型,通过扩展的失效模式与影响分析 (Failure Mode and Effects Analysis, FMEA) 检查输入/输出接口故障,迭代识别级联影

响范围并生成 CEA 树;WU Yuqian 等^[16]使用状态机建立了面向运行过程的航电系统分层功能框架,并通过动态搜索算法自动生成失效传播路径和最小割集;FENG Zhen 等^[17]提出一种自下而上的结构化方法来分析由 IMA 共享数据和资源失效引起的级联影响,包括初始失效模式的识别、直接和间接影响的捕获、综合评估与验证等。

鉴于此,笔者拟深入剖析 SPO 模式的多阶段任务特性,针对传统安全性分析方法的局限,设计基于级联影响的失效传播定量计算模型,将 IMA 系统驻留应用(节点)在给定时刻的失效概率作为离散动态系统的状态变量,并在此基础上分析不同任务阶段和不同初始故障条件下 IMA 系统的级联失效传播速度和传播范围,评估航电功能在 SPO 模式不同任务阶段的级联风险,以期避免 SPO 模式航电系统的过设计或欠设计。

1 SPO 模式多阶段任务特性研究

现代复杂系统的一个典型特点是具有多功能、多阶段和多任务等特性,这种具有多个连续且不重叠的任务阶段的复杂系统称为多阶段任务系统,多阶段任务系统在不同阶段中的配置形式、失效标准

等可能都不相同。

1.1 SPO 模式多阶段任务剖面分析

对于 SPO 模式而言,可根据机组控制能力和飞行驾驶条件将其分为 3 种类型的任务阶段,机组控制能力描述了 SPO 飞行员在飞行过程中身体条件是否可以达到操控飞机的能力,由健康和失能区分;飞行驾驶条件指的是除飞行员状态之外影响飞行的各种因素,如飞机系统状态、天气条件和机场可用性等,由标称驾驶和非标称驾驶区分^[18-19]。

任务阶段 1 的飞行员健康,飞行驾驶条件较好,此阶段不需地面操作员介入,仅依赖智能航电系统部分功能便能满足大部分飞行支持需求。任务阶段 2 出现非标称驾驶条件,飞行员负荷增加,此时需地面操作员协助,航电系统需大幅提升基于轨迹的运行与间隔管理等智能化能力,并预留地面站紧急控制接口,强化通信与其他子系统间的耦合与数据共享。任务阶段 3 的飞行员失能,航电系统需要具备自主计划生成和航迹规划能力,强化智能监视与冲突自动处理,并支持全自主飞行作为地面站通信失效时的备份控制手段。不难发现,SPO 模式各任务阶段的参与角色职责与航电功能需求均不相同,具体任务剖面分析见表 1。

表 1 SPO 模式任务剖面分析

Table 1 Mission profile analysis of SPO mode

任务阶段	参与角色职责			航电功能需求				
	单一飞行员	智能航电系统	地面操作员	管理	监视	显示	飞行	通信
阶段 1	A3	B1	×	↗	↗	—	—	—
阶段 2	A2	B2	C1	↑	↗	—	—	↑
阶段 3	×	B3	A2	↑	↑	×	↑	↑

注:A 表示主要职责,B 表示次要职责,C 表示第三职责;1 表示低能力,2 表示有限能力,3 表示完全能力;↗表示小幅增强,↑表示大幅增强,↓:大幅下降,—表示保持不变,×表示不需要。

1.2 SPO 模式航电系统驻留应用分析

随着技术的发展,飞机航电由联邦式向综合模块化体系结构演进。对于联合式航电系统,各航电功能采用独立的设计,航电系统功能与资源一一绑定;而对于 IMA 系统,各航电功能采用驻留应用的方式共享航电平台,给多功能间共享、重用资源提供技术基础。此时航电功能与硬件资源不再一一对应,而是依据 SPO 模式各任务阶段动态配置各不同航电功能所需资源^[20],具体配置方案见表 2。

在任务阶段 1 中,航电系统需求主要集中于对飞行员的支持;当进入到任务阶段 2 后,SPO 模式对于人机交互相关的航电功能需求更高;对于任务阶段 3,航电功能需要实现全自主驾驶。因此,IMA 系

表 2 SPO 模式各任务阶段的驻留应用

Table 2 Resident applications for each mission phase in SPO mode

功能	驻留应用	阶段 1	阶段 2	阶段 3
管理	综合导航	√	√	√
	性能计算	√	√	×
	飞行计划	√	√	√
	轨迹导引	√	√	√
监视	空中交通防撞	√	√	√
	地形感知与告警	√	√	√
	气象探测	√	√	√
	机载防撞	√	√	√
显示	综合显示 1	√	√	×
	综合显示 2	√	√	×

续表 2

功能	驻留应用	阶段 1	阶段 2	阶段 3
飞行	自动飞行控制	√	√	√
	主飞行控制	√	√	√
	自动推力控制	√	√	√
通信	指挥通信	×	√	√
	控制通信	×	×	√
	空管通信	√	√	×
智能	负荷评估	√	√	√
	任务分配	√	√	√
	自然语言处理	√	√	×
	智能防撞	×	√	√
	自动化配置	√	√	√
	视觉着陆	×	×	√
	性能优化	×	×	√

注:√表示有应用驻留;×表示无应用驻留。

表 3 航电驻留应用的失效影响判据

Table 3 Failure impact criteria for avionics resident applications

定性要求	无概率要求	可能的	微小的	极微小	极不可能
定量要求/(1 次·飞行小时 ⁻¹)	无概率要求	≤10 ⁻³	≤10 ⁻⁵	≤10 ⁻⁷	≤10 ⁻⁹
失效状态分类	无安全性影响	轻微的	重大的	危险的	灾难性的
影响等级分类	V	IV	III	II	I
驻留应用分类	不适用	非必要功能	低必要功能	高必要功能	关键功能

2 IMA 系统 CEA 模型

2.1 IMA 系统级联影响来源

SAE ARP 4761A 的附录中新增 CEA 方法,这是一种自下而上的安全性分析方法,主要针对机载公共资源,迭代评估其失效模式或失效组合对飞机/系统的整体影响。公共资源是飞机上多个系统共用的资源。包括能源类(电源、液压源、气源、动力装置等)和数据类(IMA、大气数据、惯导数据、导航数据、轮载信号、襟翼位置信号等)。CEA 的简化过程如图 1 所示,可用于支持 FHA、PSSA 等多种安全性分析工作^[11]。

IMA 系统的分区软件由驻留应用程序软件和基本分区操作系统软件组成。如图 2 所示,每一个驻留应用通过调用 IMA 处理模块的应用/执行接口来完成一项基本功能,基本分区操作系统为驻留应用的运行提供支持。每个 IMA 处理模块内部可以嵌入不同数量的驻留应用,各个分区的驻留应用通过传感器获取相应数据,通过航空数据网络传递数据,共同完成所有的航空电子系统任务。

然而,IMA 系统综合化带来收益的同时也增加了系统复杂性,如功能交联、软件与硬件交互等。这

统需要调整不同类别航电功能的驻留方案,以此实现“任务-功能-资源”的动态配置,有助于提高 SPO 模式下各阶段任务的航电系统支撑能力。

1.3 航电驻留应用失效影响判据

虽然 IMA 系统在共享的高性能平台上通过时空分区机制实现了多个航电功能集成,通过时空分区的机制保证不同驻留应用综合执行,但是不同航电驻留应用失效对安全性的影响程度不同^[21]。参考民机适航当局与工业界普遍接收的失效概率术语^[11],结合国内 IMA 系统安全性设计与评估工程经验,给出航电驻留应用的失效影响判据,见表 3。

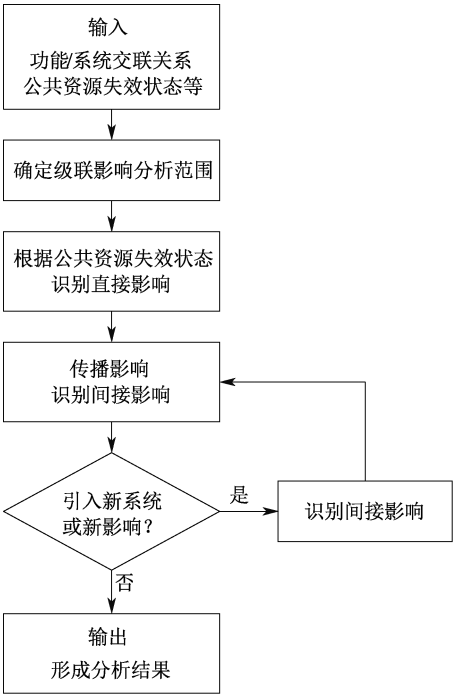


图 1 机载公共资源的 CEA 流程

Fig. 1 CEA process for airborne public resources

使得系统故障在综合过程中的蔓延、混沌和不确定性对系统可用性产生较大影响,并能引发故障传播问题。具体来说,不同驻留应用在物理实现过程中

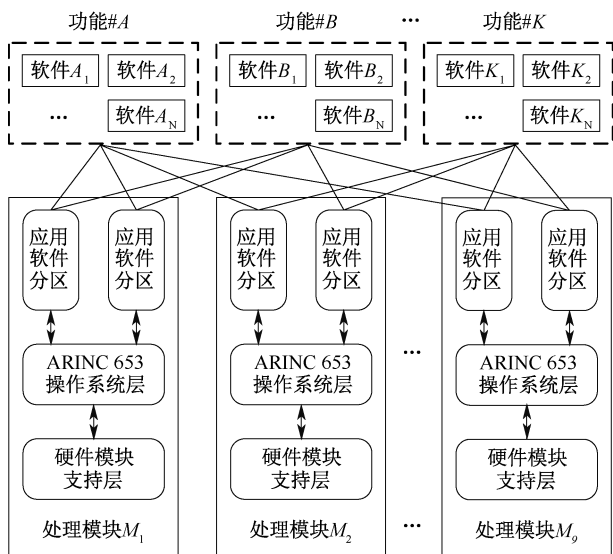


图2 IMA系统架构

Fig. 2 Architecture of IMA system

存在数据共享,直接影响由 IMA 系统中的自身故障表征,而间接影响会通过驻留应用之间的关联网络传播至其他应用。如一个驻留应用发生了堆栈溢出,就会导致 IMA 系统内其他分区出现相互感染的情况,甚至会扩到整个功能层。因此,有必要研究 IMA 系统的级联失效影响分析方法。

2.2 基于级联影响的 IMA 系统故障传播模型

在多阶段任务系统的基础上加入离散时间变量,可将其扩展为离散动态系统,此时系统的状态以离散的时间步长演变,确定一组随时间变化的系统状态序列^[22]。使用一个 0~1 之间的标量 $x(t)$ 作为系统的状态变量,该标量表示系统节点(驻留应用) x 在某一时刻处于失效状态的概率。其中, $t \in T$, T 表示一个离散时间集。为方便起见,在模型中设置 $T = 0, 1, \dots, t$, 也可根据模型的要求使用不同的时间尺度。当系统中有 n 个节点 $x_1, x_2, \dots, x_n$, 系统的状态变量在 t 时刻被记录为 $X(t)$, 其中, $X(t) = (x_1(t), x_2(t), \dots, x_n(t))^T, t \in T$ 。根据上述定义, IMA 系统的离散动态模型如下:

$$\begin{cases} X(t+1) = f(X(t), t) \\ t = 0, 1, \dots \end{cases} \quad (1)$$

式中: $X(0)$ 为初始状态; f 为一个非线性映射。系统中节点 $x_i \in \{x_1, x_2, \dots, x_n\}$ 的事件可划分为以下几种类型:故障事件 $F_{x_i}(t)$ 、直接故障事件 $D_{x_i}(t)$ 、级联失效事件 $C_{x_i}(t)$ 和因 x_j 节点故障而导致的级联失效子事件 $C_{x_i}^{x_j}(t)$ 发生的概率可表示为:

$$\Pr(F_{x_i}(t)) = \Pr(D_{x_i}(t) \cup C_{x_i}(t)),$$

$$t = 0, 1, \dots \quad (2)$$

然而,在 IMA 系统的 CEA 中,故障由初始条件设置,在接下来的离散时间内只分析间接影响的传播效果,则有:

$$\Pr(D_{x_i}(t)) = 0, t = 1, 2, \dots \quad (3)$$

$$x_i \in \{x_1, x_2, \dots, x_n\} \quad (4)$$

进一步地,若存在单个节点 x_j 与 x_i 关联,由级联而导致节点失效的概率为 $\Pr(C_{x_i}(t+1))$, 可得:

$$\Pr(C_{x_i}(t+1)) = \Pr(C_{x_i}^{x_j} | F_{x_j}) \Pr(F_{x_j}(t)) \quad (5)$$

此时 $C_{x_i} = C_{x_i}^{x_j}$ 且 $\Pr(C_{x_i} | F_{x_j}) = \Pr(C_{x_i}^{x_j} | F_{x_j})$, 若存在多个节点与 x_i 相关联,如节点 x_j 和节点 x_k 共同影响节点 x_i , 则有 $C_{x_i} = C_{x_i}^{x_j} \cup C_{x_i}^{x_k}$, 即:

$$\begin{aligned} \Pr(C_{x_i}) &= \Pr(C_{x_i}^{x_j}) + \Pr(C_{x_i}^{x_k}) - \Pr(C_{x_i}^{x_j}) \Pr(C_{x_i}^{x_k}) = \\ &= 1 - (1 - \Pr(C_{x_i}^{x_j})) (1 - \Pr(C_{x_i}^{x_k})) \end{aligned} \quad (6)$$

考虑到 $\Pr(C_{x_i}^{x_j}) = \Pr(C_{x_i}^{x_j} | F_{x_j}) \Pr(F_{x_j})$, $\Pr(C_{x_i}^{x_k}) = \Pr(C_{x_i}^{x_k} | F_{x_k}) \Pr(F_{x_k})$ 和离散时间 t 的状态转移,此时节点 x_i 的失效概率为:

$$\begin{aligned} \Pr(C_{x_i}(t+1)) &= 1 - (1 - \Pr(C_{x_i}^{x_j} | F_{x_j}) \Pr(F_{x_j}(t))) \\ &\quad (1 - \Pr(C_{x_i}^{x_k} | F_{x_k}) \Pr(F_{x_k}(t))) \end{aligned} \quad (7)$$

相似的,如果有 m 个节点 $\{x_1, x_2, \dots, x_m\}$ 与节点 x_i 相关联,此时节点 x_i 的失效概率为:

$$\Pr(C_{x_i}(t+1)) =$$

$$1 - \prod_{j=1}^m (1 - \Pr(C_{x_i}^{x_j} | F_{x_j}) \Pr(F_{x_j}(t))) \quad (8)$$

对于任何与 x_i 相连的节点 x_j , 失效的条件概率 $\Pr(C_{x_i}^{x_j} | F_{x_j})$ 表示节点 x_i 的级联失效事件 $C_{x_i}^{x_j}$ 是由节点 x_j 的故障时间 F_{x_j} 触发的, 并且已知失效的条件概率 $\Pr(C_{x_i}^{x_j} | F_{x_j})$ 的值在 0~1 之间。 $\Pr(C_{x_i}^{x_j} | F_{x_j})$ 值越接近 1, 说明节点间的关联性越强。这意味着上游节点的故障更容易传递到关联节点 x_i , 从而导致关联节点 x_i 的失效。当 $\Pr(C_{x_i}^{x_j} | F_{x_j}) = 0$ 时, 意味着 2 节点无交联。

结合 IMA 系统中资源重用、信息传递和数据共享产生的耦合关联, 单个 CPM 的失效可通过故障传播对整个系统产生影响^[23]。因此, 为便于研究的开展, 可将 IMA 系统中节点 x_j 故障导致节点 x_i 发生失效的概率设定为一个已知的固定值, 参照文献[24]将其设定为 $p_{ij} = \Pr(C_{x_i}^{x_j} | F_{x_j}) = 2 \times 10^{-5}$ /飞行小时。如果一个 IMA 系统有 n 个驻留应用, 则存在 n^2 个交联关系, 即存在 n^2 个条件概率, 由此可得 $n \times n$ 的级

联耦合矩阵如下所示:

$$P = (p_{ij})_{n \times n} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & \vdots & & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{bmatrix} \quad (9)$$

此时,IMA 系统的离散动态模型可被扩展为下式:

$$f(X(t)) = f \begin{pmatrix} x_1(t) \\ x_2(t) \\ \vdots \\ x_n(t) \end{pmatrix} = \begin{pmatrix} x_1(t+1) \\ x_2(t+1) \\ \vdots \\ x_n(t+1) \end{pmatrix} = \begin{pmatrix} 1 - \prod_{j=1}^n (1 - p_{1j}x_j(t)) \\ 1 - \prod_{j=1}^n (1 - p_{2j}x_j(t)) \\ \vdots \\ 1 - \prod_{j=1}^n (1 - p_{nj}x_j(t)) \end{pmatrix} \quad (10)$$

$X(t+1), t=0,1,\dots$
式中 $X(0)$ 为系统状态变量的初始值。在模拟 IMA 系统的级联失效影响时,以根据全局分析的需要设置不同初始值,且在 $t+1$ 时刻只考虑间接影响的传播,不考虑直接故障事件的发生,由此建立基于级联影响的 IMA 系统故障传播模型。

2.3 IMA 系统级联失效评价指标

采用级联失效概率和级联风险系数来表征驻留应用级联失效对 IMA 系统的传播速度、传播范围和影响程度^[25]。若 IMA 系统中共有 n 个驻留应用,则系统层的级联失效概率为:

$$P_s(t) = \frac{\sum_{i=1}^n Pr(F_{x_i}(t))}{n} \quad (11)$$

若某航电功能包括 k 个驻留应用,则功能层的级联失效概率为:

$$P_f(t) = \frac{\sum_{i=1}^k Pr(F_{x_i}(t))}{k} \quad (12)$$

IMA 系统的级联风险为:

$$r(t) = \sum_{i=1}^n (Pr(F_{x_i}(t)) \times \alpha_i) \quad (13)$$

式中: $Pr(F_{x_i}(t))$ 为节点 x_i 在时刻 t 的级联失效概率,可由 2.2 节建立的计算模型求得; α_i 为驻留应用分类对应的级联失效影响系数,可由 1.3 节的驻留应用失效影响判据得出。接下来,进一步给出 IMA 系统的平均级联风险计算方法,如下式:

$$R = \frac{1}{T} \int_{t=1}^T r(t) dt \quad (14)$$

3 SPO 模式下 IMA 系统的级联影响仿真

SPO 模式下的航电系统具有平台资源共享、功能耦合交联、失效机制复杂的特点。出于篇幅限制,以 SPO 模式任务阶段 1 和阶段 3 为例开展 IMA 系统级联影响的仿真对比试验。在 1.1 节和 1.2 节对 SPO 模式多阶段任务特性研究的基础上,给出 IMA 系统在 2 个 SPO 模式任务阶段的驻留应用交联关系,如图 3 所示。

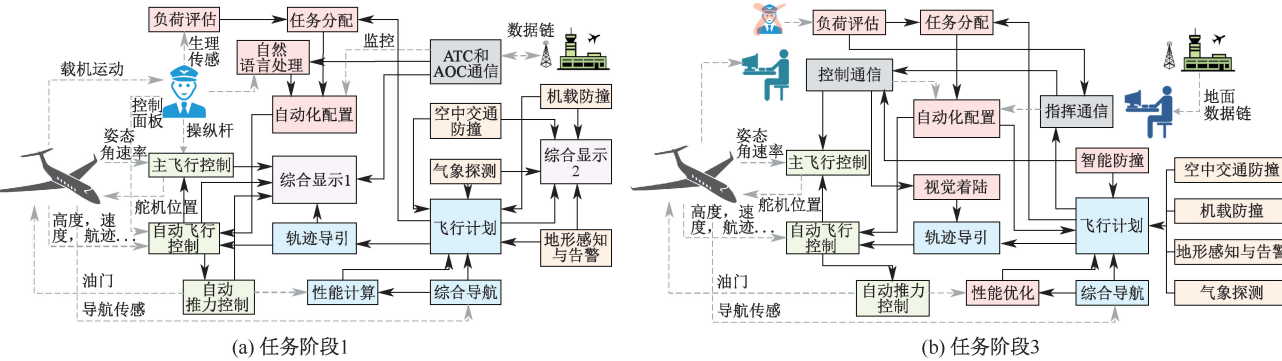


图 3 SPO 模式不同任务阶段的驻留应用交联关系

Fig. 3 Interconnections of resident applications in different mission phases of SPO mode

3.1 IMA 系统故障传播分析

为进一步识别 IMA 系统在不同 SPO 模式任务阶段下级联影响的故障传播速度与传播范围,假设在初始故障事件下只有一个驻留应用发生故障,其

他驻留应用保持正常状态。以轨迹导引和自动飞行控制的初始故障事件为例,面向 SPO 模式任务阶段 1 开展仿真,对比离散时间内的级联失效概率变化情况如图 4 所示。

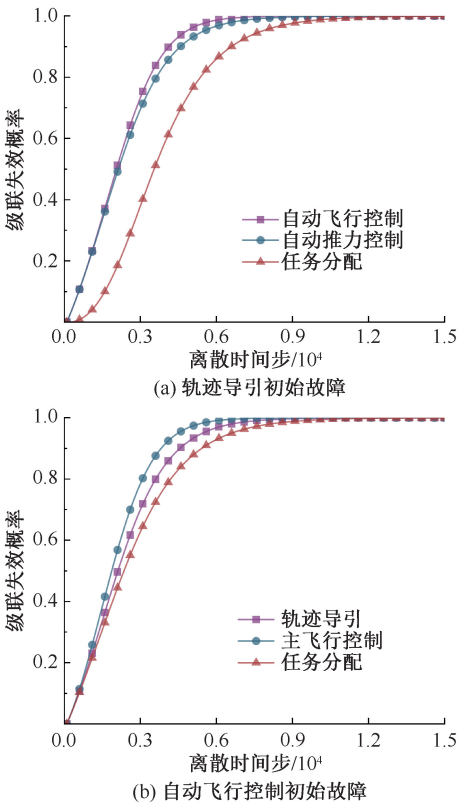


图4 SPO 模式任务阶段一不同初始故障的级联失效概率

Fig. 4 Cascading failure probabilities of different initial faults in SPO mode mission phase one

从图4可以看出,在SPO模式任务阶段1中,不同初始故障在IMA系统中的传播速度与传播范围各不相同。例如:若以轨迹导引为初始故障事件,与其耦合关联较强的自动飞行控制应用失效概率增长较快,与其关联度较弱的任务分配应用则失效概率增长较慢。同理,还可分析SPO模式任务阶段3中的故障传播情况,如图5所示。与SPO模式任务阶段1相比,任务阶段3中传统驻留应用的故障传播速度更慢。

3.2 IMA 系统级联风险分析

为进一步分析IMA系统级联失效对安全性的影响,结合1.3节给出的失效影响判据,评估航电驻留应用的分类等级,见表4。

基于SPO模式航电驻留应用的分类等级,能够根据式(13)和式(14)计算不同SPO模式任务阶段、不同初始故障事件下的级联风险系数。按照航电功能进行分类整理得到功能层级联风险,如图6和图7所示。若按照航电驻留应用分类整理,经过归一化处理后的平均级联风险排名,见表5。

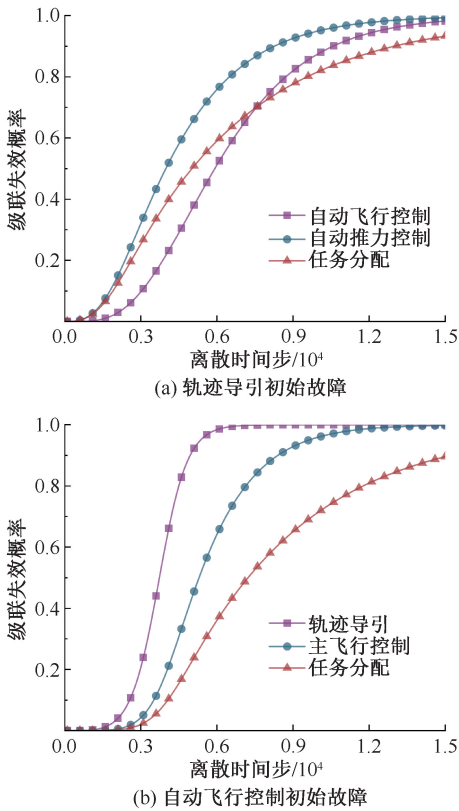


图5 SPO 模式任务阶段3不同初始故障的级联失效概率

Fig. 5 Cascading failure probabilities of different initial faults in SPO mode mission phase 3

表4 航电驻留应用的分类等级

Table 4 Classification levels for avionics resident applications

驻留应用	分类等级	驻留应用	分类等级
综合导航	高必要	性能计算	低必要
飞行计划	高必要	轨迹导引	低必要
空中交通防撞	高必要	地形感知与告警	低必要
气象探测	低必要	机载防撞	高必要
综合显示1	高必要	综合显示2	低必要
自动飞行控制	高必要	主飞行控制	关键
自动推力控制	低必要	指挥通信	高必要
控制通信	关键	AOC和ATC通信	低必要
负荷评估	高必要	任务分配	低必要
自然语言处理	低必要	智能防撞	高必要
自动化配置	低必要	视觉着陆	高必要
性能优化	高必要		

从图6和图7可以看出,在SPO模式任务阶段1中,级联风险趋于稳定的速度比任务阶段3更快,但随着SPO模式引入智能化驻留应用,IMA系统中各航电功能的级联风险整体呈上升趋势。由表5可知:不论何种SPO模式任务阶段,以主飞行控制和

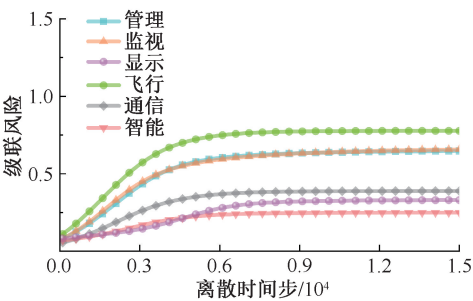


图 6 SPO 模式任务阶段 1 的航电功能级联风险

Fig. 6 Cascading risk of avionics functions in SPO mode mission phase 1

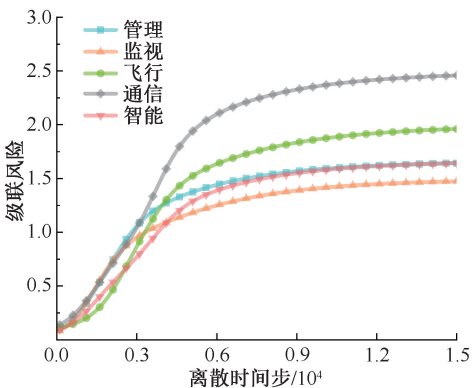


图 7 SPO 模式任务阶段 3 的航电功能级联风险

Fig. 7 Cascading risk of avionics functions in SPO mode mission phase 3

综合导航为初始故障事件的 IMA 系统平均级联风险始终较高,需要在 SPO 模式航电系统早期的架构

表 5 SPO 模式下 IMA 系统的平均级联风险

Table 5 Average cascading risk of IMA system in SPO mode

离散时间步	SPO 模式任务阶段	平均级联风险排名				
0.5×10 ⁴	任务阶段 1	主飞行控制 0.104 2	综合导航 0.074 7	机载防撞 0.070 9	空中交通防撞 0.070 9	自动飞行控制 0.069 5
	任务阶段 3	主飞行控制 0.180 4	综合导航 0.152 9	性能优化 0.152 9	智能防撞 0.149 3	指挥通信 0.149 1
1.0×10 ⁴	任务阶段 1	主飞行控制 0.275 8	综合导航 0.199 4	机载防撞 0.193 4	空中交通防撞 0.193 4	飞行计划 0.190 9
	任务阶段 3	主飞行控制 0.559 5	控制通信 0.516 1	综合导航 0.416 3	性能优化 0.416 3	指挥通信 0.409 0
1.5×10 ⁴	任务阶段 1	主飞行控制 0.450 6	综合导航 0.330 1	机载防撞 0.323 4	空中交通防撞 0.323 4	飞行计划 0.328 8
	任务阶段 3	主飞行控制 1.000 0	控制通信 0.960 9	综合导航 0.713 3	性能优化 0.713 3	飞行计划 0.707 3

设计阶段针对性地采取备份、监控或重构措施。对于 SPO 模式任务阶段 3,与通信功能相关的驻留应用平均级联风险显著上升,需要选择低时延、高可靠、大带宽特性的指挥通信与控制通信技术方

案,以此支持地面操作员的决策和对飞机的远程控制。

属性,而是随任务阶段动态演变的。

2) IMA 系统的高度综合化与智能化是 SPO 模式级联风险放大的内因。为实现自主飞行而引入的新增智能应用及更紧密的数据交联,虽然提升了系统能力,但同时也形成了更复杂的故障传播路径。

3) 研究不足在于对仿真场景的简化,仅限于选定的 SPO 模式任务阶段和单一故障假设,未能全面捕捉真实多变量交互的复杂动态环境,可能会低估 IMA 系统级联影响的涌现性。

4 结 论

1) 仿真结果表明:从常规飞行(阶段 1)到自主飞行(阶段 3),IMA 系统整体风险水平呈上升趋势,这说明 SPO 模式下航电系统的级联风险并非静态

参 考 文 献

[1] 时统宇,马煜森,曹宇杰,等. 基于改进功能共振分析法的 SPO 风险演化[J]. 中国安全科学学报, 2024, 34(6): 29-38.

SHI Tongyu, MA Yusen, CAO Yujie, et al. SPO risk evolution based on improved functional resonance analysis method[J]. China Safety Science Journal, 2024, 34(6): 29-38.

[2] NEIS S M, KLINGAUF U, SCHIEFELE J. Classification and review of conceptual frameworks for commercial single pilot operations[C]. Proceedings of the IEEE/AIAA 37th Digital Avionics Systems Conference, 2018: 1-8.

- [3] WANG Guoqing, LI Min, WANG Miao, et al. A systematic literature review of human-centered design approach in single pilot operations[J]. Chinese Journal of Aeronautics, 2023, 36(11): 1-23.
- [4] 汪磊, 邵铨睿, 吴昌旭, 等. 基于 QN-MHP 模型的 SPO 人机功能分配研究[J]. 中国安全生产科学技术, 2023, 19(9): 183-189.
WANG Lei, SHAO Kengrui, WU Changxu, et al. Research on human-machine function allocation under SPO based on QN-MHP mode[J]. Journal of Safety Science and Technology, 2023, 19(9): 183-189.
- [5] LIM Yixiang, BASSIEN-CAPSA V, RAMASAMY S, et al. Commercial airline single-pilot operations: system design and pathways to certification[J]. IEEE Aerospace and Electronic Systems Magazine, 2017, 32(7): 4-21.
- [6] YIN J J, ZHU Zhiqiang. Flight autonomy impact to the future avionics architecture[C]. Proceedings of the 37th IEEE/AIAA Digital Avionics Systems Conference, 2018: 1-7.
- [7] CHEN Yong, LUO Yue, WANG Miao, et al. DFCluster: an efficient algorithm to mine maximal differential biclusters for single pilot operations task synthesis safety analysis[J]. Chinese Journal of Aeronautics, 2022, 35(5): 400-418.
- [8] ZOLGHADRI A. Augmented flight management system for future single pilot operations[C]. Proceedings of the 9th International Conference on Control, Decision and Information Technologies, 2023: 29-34.
- [9] 陈勇, 钟科林, 罗悦, 等. 支线客机关键技术与发展方向[J]. 航空学报, 2023, 44(2): 156-180.
CHEN Yong, ZHONG Kelin, LUO Yue, et al. Key technology and future development of regional airliner[J]. Acta Aeronautica et Astronautica Sinica, 2023, 44(2): 156-180.
- [10] CCAR 25.1309—2011, 运输类飞机适航标准[S].
CCAR 25.1309-2011, Airworthiness standards of transport category aircraft[S].
- [11] ARP 4761A-2023, Guidelines for conducting the safety assessment process on civil aircraft, systems, and equipment[S].
- [12] ARP 4754B-2023, Guidelines for development of civil aircraft and systems[S].
- [13] 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.
- [14] 董海勇. 综合模块化航电显示系统的可用性分析方法研究[D]. 西安:西北工业大学, 2020.
DONG Haiyong. Research on availability analysis approach for the display system of integrated modular avionics system[D]. Xi'an: Northwestern Polytechnical University, 2020.
- [15] 杨海云, 孙有朝. 基于类似 HiP-HOPS 的 IMA 系统级联失效模型的分析研究[C]. 第八届民用飞机航电国际论坛, 2019: 147-151.
- [16] WU Yuqian, XIAO Gang, WANG Miao. Cascading failure analysis method of avionics based on operational process state[J]. IEEE Access, 2020, 8: 148 425-148 444.
- [17] FENG Zhen, SHI Zhijian, WANG Yuqing. Research on cascading effect analysis of civil aircraft shared data and resource system failures[C]. Proceedings of the Global Reliability and Prognostics and Health Management, 2021: 1-5.
- [18] 刘嘉琛, 董磊, 陈曦, 等. 基于改进 STPA-DEMATEL 的智能航电系统致因要素分析[J]. 系统工程与电子技术, 2024, 46(6): 2 023-2 033.
LIU Jiachen, DONG Lei, CHEN Xi, et al. Causal factor analysis of AI-based avionics system based on improved STPA-DEMATEL[J]. Systems Engineering and Electronics, 2024, 46(6): 2 023-2 033.
- [19] MATESSA M, STRYBEL T, VU K, et al. Concept of operations for RCO SPO[R]. Ames Research Center, 2017.
- [20] 赵长啸, 何铎, 李浩, 等. 基于效能的先进战斗机航电系统动态重构方法[J]. 航空学报, 2020, 41(6): 355-365.
ZHAO Changxiao, HE Feng, LI Hao, et al. Dynamic reconfiguration method based on effectiveness for advanced fighter avionics system[J]. Acta Aeronautica et Astronautica Sinica, 2020, 41(6): 355-365.
- [21] GUILLAUMET T, FERON E, BAUFRETON P, et al. Task allocation of safety-critical applications on reconfigurable multi-core architectures[C]. Proceedings of the 36th IEEE/AIAA Digital Avionics Systems Conference, 2017: 1-10.
- [22] WU Yipeng, CHEN Zhilong, ZHAO Xudong, et al. Propagation model of cascading failure based on discrete dynamical system[J]. Reliability Engineering & System Safety, 2021, 209: DOI:10.1016/j.res.2020.107424.
- [23] 赵长啸, 李道俊, 孙亦轩, 等. 基于深度强化学习的综合航电系统安全性优化方法[J]. 中国安全科学学报, 2024, 34(7): 123-131.
ZHAO Changxiao, LI Daojun, SUN Yixuan, et al. Integrated avionics system safety optimization method based on deep reinforcement learning[J]. China Safety Science Journal, 2024, 34(7): 123-131.
- [24] 阎芳, 向晨阳, 董磊, 等. DIMA 架构下飞机全电刹车系统故障传播行为分析与评估[J]. 航空学报, 2021, 42(9): 445-461.
YAN Fang, XIANG Chenyang, DONG Lei, et al. Analysis and evaluation of fault propagation behavior of aircraft all-electric brake system under DIMA architecture[J]. Acta Aeronautica et Astronautica Sinica, 2021, 42(9): 445-461.
- [25] WU Yipeng, CHEN Zhilong, ZHAO Xudong, et al. Robust analysis of cascading failures in complex networks[J]. Physica A: Statistical Mechanics and its Applications, 2021, 583: DOI:10.1016/j.physa.2021.126320.

作者简介: 董磊 (1983—),男,天津人,博士,副研究员,主要从事民机安全性评估与适航审定技术等方面的研究。E-mail:l-dong@cauc.edu.cn。