空管自动化系统软件故障风险评估及管理措施

刘晶

民航局空管局技术中心，北京，100015；

摘要：本文以空管自动化系统软件故障 2018 年建立软件管理平台以来的数据为基础，总结主流厂家自动化系统历年来的软件故障情况和特点；通过风险矩阵分析法建立软件故障分析模型，对自动化系统软件故障的运行风险进行了分析，有针对性的对不同风险指数的软件故障提出风险管控措施，为后续的系统运行风险分级管控和维护工作提出参考，以降低空管自动化系统软件故障对空管系统运行造成的影响。

关键词：空管自动化系统；风险矩阵分析法；软件故障；

DOI:10.69979/3041-0673.25.02.034

前言

民航空管自动化系统作为民航空管管制员对空实施指挥的核心系统，随着民航运输量的快速增长，系统的软件运行的稳定性和可靠性直接影响着民航运行的安全和效率。为了有效管控系统运行风险，民航系统下发了风险分级管控隐患排查治理双重预防机制，空管自动化系统均制定了风险评估，但主要以单个现场历史经验为主的定性分析。

本文以空管自动化系统软件故障 2018 年建立软件管理平台以来的数据为基础，首先总结多个厂家自动化系统历年来的软件故障情况，分析了软件故障集中的功能和模块，进而提炼出系统软件故障的特点；其次选用常用的半定量法——风险矩阵分析法建立软件故障分析模型，对自动化系统软件故障的运行风险进行了分析，有针对性的对不同风险指数的软件故障提出风险管控措施，为后续的系统运行风险分级管控和维护工作提出参考，以降低空管自动化系统软件故障对空管系统运行造成的影响。

1 系统运行情况和故障分析

民航空管行业内使用的自动化系统来自六个不同国内外厂家，在 44 个空管分局（站）共计使用 80 余套自动化系统软件，自空管自动化系统软件管理平台 2018 年上线以来，记录了自动化系统故障情况如图 1 所示。

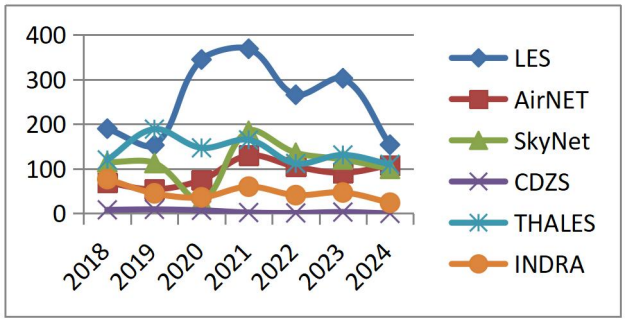

图 1 各厂家自动化系统软件故障数

由图 1 可以看出，空管自动化系统各厂家故障呈现出“下降-上升-下降”的趋势，这符合自 2014 年国产厂家空管自动化系统开始由应急系统升为备份系统且故障纳入统一管理后，国产厂家到 2019 年故障数量逐步下降；在 2020 年空管局开始推进主备自动化系统常态化使用，备份自动化系统每月使用时长逐步增长，随着而来前期未发现的软件故障开始增加，到 2024 年自动化系统故障逐步下降，软件成熟度更高，系统进入稳定运行阶段。同时，由于全国各现场自动化系统软件逐年有新的系统上线，上线初期会出现由于系统适应性的故障数量增加，使得故障数在一些年度出现小幅上涨。国外两厂家的曲线基本保持水平变化不大，这是由于国外厂家投产时间较长且系统使用范围广，系统运行基本平稳。

空管自动化系统由多个功能模块构成，不同厂家的系统功能模块略有区别但系统主要功能模块大体相同，主要分为监视数据处理、飞行数据处理、告警处理、管制席位人机界面、技术监控、系统参数管理、数据通信等。

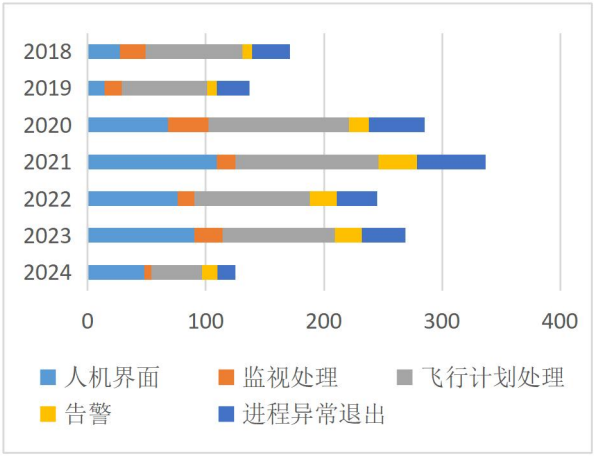

图 2 系统主要故障模块故障数

表 1 系统主要故障模块故障数比例

年份	人机界面	监视处理	飞行计划处理	告警	进程异常退出
2024	31.10%	4.10%	28.20%	8.31%	9.34%
2023	14.21%	11.58%	43.16%	4.21%	16.84%
2022	29.70%	7.92%	31.35%	7.59%	12.21%
2021	28.57%	5.26%	36.84%	8.65%	12.78%
2020	29.54%	4.34%	32.79%	8.94%	15.72%
2019	19.71%	9.86%	34.49%	4.93%	13.62%
2018	9.15%	9.80%	47.06%	5.23%	18.30%

以国产主要厂家 2018 年到 2024 年故障发生模块为代表进行分析，可以得到图 2 中系统出现故障较多的模块分别为人机界面、监视数据处理、飞行计划处理、告警及进程异常退出五类。从图 2 和表 1 中的故障数和在相应年份的占比中可以看出：

一是飞行数据处理故障是占比最多的软件故障模块，且基本保持着相同的数量和比例，在 2024 年度出现了小幅下降，主要是由于飞行数据处理模块与外部系统接口较多，软件实现的功能也较多，即与系统内其他模块通信和调用也较多，故障主要集中在报文处理、AIDC 移交等方面。

二是人机界面模块的软件故障数量为次多的模块，在从 2020 年备用自动化系统使用频繁后，人机界面故障数量有所上升；在 2024 年由于该系统在多个地区先后上线运行，出现人机界面故障的数量再次上升的情况。

三是进程的异常退出故障数占比逐年下降的趋势，系统软件的异常退出主要表现内存溢出导致的系统人机界面或主要功能进程的异常退出，发生数量相对较低，但对系统功能的正常使用造成很大的影响。

四是监视数据处理和告警处理两个模块功能较为稳定，监视数据处理的输入数据源、输出数据及交互模块相对单一，系统表现相对稳定。

2 风险评估模型

风险矩阵法通过构造风险矩阵图，分析一个项目、一种方法或一个系统的潜

在风险，是一种有效的风险管理工具。[1]该方法因其概念清晰、使用方便、评估结果简洁易懂，有利于风险管理工作的开展，且在我国的隧道、桥梁、地铁等行业的建议指南中都作为基本的风险评估方法。[2]

使用风险矩阵法能够更好的将风险因素进行量化分析，直观的分析风险的要素的影响程度，进而能够针对不同等级的风险制定相应的管控措施。依照风险发生的可能性 L 和风险发生后果的严重性 S，对风险发生后的风险度进行评价，可以针对不同等级的风险提出有针对性的管控措施，进而达到对风险的管理控制目的。

以空管自动化系统软件发生故障为分析对象，根据空管自动化系统行业对故障的严重性分类标准，可以得到自动化系统软件故障风险严重性等级 S，分为 4 个等级，如表 2 所示：

表 2 空管自动化系统软件故障风险严重性等级（S）

等级	说明	损害程度
S1	灾难性	导致系统无法提供运行服务
S2	重大的	导致系统单一功能失效
S3	较小的	导致系统局部功能或性能异常，但能保证基本管制服务
S4	轻微的	基本未对管制运行造成影响

根据过往的空管自动化系统软件故障管理经验和软件行业质量要求，可以得到空管自动化系统软件故障发生的可能性等级 L，如表 3 所示：

表 3 空管自动化系统软件故障风险发生可能性（L）

等级	说明	发生频率
L1	经常性故障	故障发生的可能性很高，容易复现的故障
L2	频繁故障	故障时有发生
L3	偶发故障	故障发生概率较低，很难复现的故障
L4	极小可能故障	故障发生概率很低

风险评价指数（R）可以通过将风险发生可能性（L）和风险的严重性（S）确定最终的风险等级，其计算公示为：

$$R = F(L,\ S) \qquad (1)$$

风险评价指数 R 可以采用矩阵的形式进行表述，参数 $L(L_1 \ldots . L_m)$ 和参数 $S(S_1 \ldots . S_n)$ 构建的 $m * n$ 阶矩阵，从而计算风险评价指数在交叉点位置的值。[3]根据评价方法，将空管自动化系统软件故障的风险发生可能性和风险的严重性构建一个二维矩阵，确定风险等级评价的矩阵，如图 3 所示：

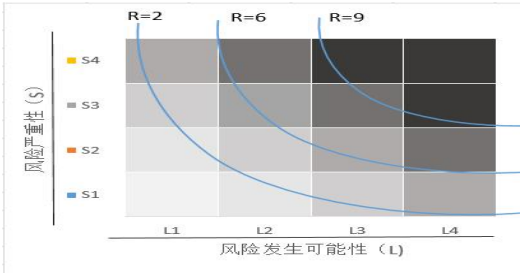

图 3 空管自动化系统故障的风险矩阵

由图3可以看出，图中的浅白色为可以忽略的风险，浅灰色为可以接受的风险，深灰色为可控的风险，黑色即为不可接受的风险，需要严格控制。通过分析自动化系统故障所在的风险矩阵象限，可以看出空管自动化系统故障风险大多集中在深灰色区域，即为发生频率较高同时故障风险的严重性为S3或S4，在整个故障占比中达到了53.03%，即造成的损害程度较低，为可控的风险；空管自动化系统故障处在黑色象限的故障较少，是需要严格控制的风险。

3 风险控制措施

针对上述空管自动化系统故障风险评估模型的结果，可以看出，空管自动化系统故障风险评价落在白色矩阵中占比大约为3.8%，占比不高，在自动化系统日常运行过程中加强对该类故障的维护，通过系统离线数据配置修改等方式减少故障发生率。

浅灰色矩阵的软件故障中，故障主要为系统席位上非关键功能故障及报文处理处理中的飞行计划报文解析、计划变更匹配错误等，该类故障发生频率不高，对系统正常运行造成的风险后果在可接受范围内，可以等待系统故障详细调查后针对故障原因进行软件补丁或版本的修复，日常工作中应注意该类故障的记录和汇总，在运行一段时间后进行讨论和故障调查分析，识别其中故障较为集中的模块或功能集合，督促自动化系统生产厂家在后续版本中修复该类问题，避免造成故障风险等级升级。

深灰色矩阵中的软件故障占比约为10%，故障主要集中在系统席位进程的偶发退出、报文或监视数据处理服务器（均为主备双服务器配置）单服务器进程退出、席位管制主要功能出现偶发失效和航迹出现偏离等，对系统运行服务造成一定影响但未发生严重后果，此类软件故障为可控风险，针对此类风险应及时调查故障原因，尽快以软件补丁方式修复相关故障；同时制定该类风险的自动化系统故障台账，对发生频率高、未能定位原因的故障制定缓解措施。

黑色矩阵中的软件故障为不可接受需要严格控制风险后果的系统缺陷，发生概率较低，在7年故障总和中占比约为1.3%，故障主要为系统内存溢出造成的全系统席位退出、系统报文处理服务器双机因系统数据库异常退出、系统监视数据全部消失等异常情况，该类故障会造成系统运行服务的瘫痪，对管制服务造成严重影响，风险不可接受需要在故障发生前予以重点关注和管控，该类故障应制定风险清单，制定详细的管控措施和预防机制。针对该类故障，厂家应在开发过程中注意正确释放已分配内存，优化算法，减少算法中递归深度，在单元测试过程中使用具内存分析能力的开发工具和运行环境来检查内存使用情况，减少内存溢出风险；对于程序中数组越界导致的主要模块程序崩溃的软件故障，厂家在软件代码编写中应减少错误数组索引的实物，在后续的软件测试中厂家应采取边界检查、动态调试等方法在工厂测试中识别数组越界错误，同时在软件上线前，开展第三方测试和现场测试，保证测试时间和覆盖，减少类似风险。系统航迹偏离的故障由于自动化系统监视源主要有一、二次雷达、ADS-B、MLAT等等，多监视源的融合同时又会受到监视源本身信号质量的影响，造成融合后的监视数据航迹不准确，对于自动化系统监视数据融合处理模块的软件算法要求也不断提高，监视源算法也成为新的风险点，应加强对该模块的故障管控。

4 结论

本文首先分析了多个厂家空管自动化系统2018年以来的软件故障数据，并以典型厂家对以往故障数据中容易发生故障的软件功能模块进行了分析，根据分析结论使用风险矩阵方法识别出空管自动化系统软件故障的风险矩阵，针对不同风险指数的软件故障提出了不同的风险管控措施，使得自动化系统软件故障风险管理更加精细化，对于后续系统运行稳定性提出维护建议，给自动化系统软件的分析和维护提供参考。

参考文献

[1]Richard D.P.Perspective on assessment in tunneling[M].ASCE Geo-Institute Conference,Univer-sity of Illinois,1999.

[2]阮欣，尹志逸，陈艾荣. 风险矩阵评估方法研究与工程应用综述，同济大学学报（自然科学版），2013，41（3）：381-385.

[3]邹德均，周诗建，宫良伟. 风险矩阵评估法在矿井安全生产中的应用，煤矿安全，2017,48（2）：234-236.

作者简介：刘晶(1987-),女，汉,陕西,硕士,高级工程师，空中交通管理研究，民航局空管局技术中心