DOI:10. 20079/j. issn. 1001-893x. 240424003

一种基于 Bow-tie 模型的 ADS-B IN 应用安全评估方法*

肖 阳[1],王 洪[1,2],赵子安[2]

(1. 电子科技大学长三角研究院(湖州),浙江 湖州 313000;2. 电子科技大学 信息与通信工程学院,成都 611731)

摘 要:广播式自动相关空空监视(Automatic Dependent Surveillance-Broadcast IN,ADS-B IN)应用能够在飞行活动中为飞行员提供诸多便利,而安全性是实现 ADS-B IN 应用优势的前提。针对 ADS-B IN 应用在实际飞行活动中可能存在的安全性问题,引入了一种基于 Bow-tie 模型的安全评估方法。该方法通过对预设危险进行分析,得出危险发生的最大可接受概率,进而推导出为实现这一概率所需的 ADS-B 设备失效率或通信数据链路完整性等安全要求。在对该方法进行阐述的基础上,给出了一个具体实施案例,对该方法做进一步说明。

关键词:广播式自动相关监视;Bow-tie 模型;事件树分析;故障树分析

开放科学(资源服务)标识码(OSID):

中图分类号:V243 **文献标志码**:A **文章编号**:1001-893X(2025)11-1886-08

Operational Safety Assessment of ADS-B IN Applications Based on the Bow-tie Model

XIAO Yang[1], WANG Hong[1,2], ZHAO Zi'an[2]

(1. Yangtze Delta Region Institute(Huzhou), University of Electronic Science and Technology of China, Huzhou 313000, China; 2. School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)

Abstract: Automatic Dependent Surveillance-Broadcast IN(ADS-B IN) applications can provide numerous conveniences for pilots during flight operations, with safety being the prerequisite for realizing the advantages of ADS-B IN applications. A Bow-tie model-based safety assessment method is introduced to address potential safety issues associated with ADS-B IN applications in actual flight activities. By analyzing pre-defined hazards, the maximum acceptable probability of hazard occurrence is determined, which in turn leads to the derivation of safety requirements such as the failure rate of ADS-B equipment or the integrity of communication data links necessary to achieve this probability. Based on the explanation of this method, a specific implementation case is presented to further illustrate its application.

Key words: ADS-B; Bow-tie model; event tree analysis; fault tree analysis

0 引 言

广播式自动相关监视(Automatic Dependent Surveillance-Broadcaset, ADS-B)是一种依靠机载导航系统获取飞机位置的监视系统,由地面系统和机载设备组成。它通过通信数据链路,将本机的位置和其他飞行状态信息以一定周期自动发送给地面或其他在一定范围内配备了 ADS-B 的飞机。美国航空无线电委员会(Radio Technical Commission for

* 收稿日期:2024-04-24;修回日期:2024-09-27
通信作者:王洪 Email:icdo_y@163.com

Aeronautics,RTCA)为 ADS-B 系统开发了一系列的机载监视应用,这些应用利用 ADS-B 系统所提供的数据,协助飞行员进行机场场面滑行、跟随进近、高度层变更等操作,增强飞行员的交通情景感知,提升空管的空中交通管制效率,实现提高运行效率、增大空中交通流量、保障飞行安全等诸多益处。在 FAA 的颁发的技术标准规定[1](Technical Standard Order,TSO)中上将这些应用统称为 ADS-B IN 应用[1]。根据相关标准,目前主流的 ADS-B IN 应用共有 8 种[2]:增强视景获取(Enhanced Visual Acquisition, EVAcq);空中情景意识(Airborne Situation Awareness,AIRB);场面情景意识(Surface Situation Awareness,SURF);进近目视间隔(Visual Separation on Approach,VSA);高度变更程序(In-Trail Procedure, ITP);带告警的交通情景意识(Traffic Situation Awareness with Alerts,TSAA),也称为 ADS-B 交通咨询系统(ADS-B Traffic Advisory System,ATAS);CDTI 辅助目视间隔(CDTI Assisted Visual Separation,CAVS);驾驶舱间隔管理(Flight-deck Interval Management,FIM),它们在不同的飞行阶段发挥作用。

对 ADS-B 系统进行安全分析,是保障系统及功能安全运行的必要手段[3]。Ali 等人[4]利用概率安全评估方法,对导致 ADS-B 系统进入失效模式的原因及所导致的危险进行了分析。Olaganathan 等人[5]研究了 ADS-B 系统中可能产生的危险,给出了每种危险的影响和风险程度。这两项研究分析了 ADS-B 系统的失效模式,忽略了 ADS-B IN 应用功能的安全分析。Sesso 等人[6]将 GNSS 数据的完整性作为参考指标,通过与参考雷达系统对比的方式,分析了 ADS-B 系统在无雷达区域运行监视功能的安全性。Zeitlin 等人[7]基于 ADS-B 系统的空中冲突解决应用与 TCAS 对比的方式对 ADS-B 进行了定性的安全分析。Yiu 等人[8]对 ADS-B 在动态空域中告警能力的安全性进行了分析。上述这些研究都是针对 ADS-B 系统的某一种具体功能应用所开展的安全分析,无法适用于其他的 ADS-B IN 应用。

本文针对 ADS-B IN 应用,在考虑相关 RTCA 标准[9-11]中所规定的 ADS-B IN 应用运行操作流程的基础上,引入了一种通用的安全评估方法。本方法关注于 ADS-B 系统的具体功能应用,利用 Bow-tie 模型对其在运行过程中可能造成的危险进行分析,得到相应的安全要求,使得危险的发生概率在可接受的范围之内。

1　基于 Bow-tie 模型的 ADS-B IN 应用安全评估方法介绍

1.1　Bow-tie 模型

Bow-tie 模型从左到右依次为危险发生的原因、危险源以及危险发生后所导致的后果,很好地结合了故障树分析和事件树分析各自的优势,其模型如图 1 所示。从危险源出发,利用事件树分析,沿时间线向后推出危险发生所造成的结果,帮助完善危险发生后的处理办法。利用故障树分析沿时间线往前推出导致危险发生的系统内因,可以优化系统设计、提供维修策略等,从而预防危险的发生。Bow-tie 模型通过对危险发生的前因后果进行全方面的分析,帮助人们更细致地分析 ADS-B IN 应用的危险情景,达到预防安全性事故发生的目的。

图 1　Bow-tie 模型

1.2　基于 Bow-tie 模型的 ADS-B IN 应用安全评估方法

ADS-B IN 应用安全评估的主要目的是得出待评估应用的安全要求,将应用在运行中所可能发生的运行危险概率限制在可接受的范围之内。本安全分析方法首先通过对应用在运行中的危险情况进行分析,确定危险的最大可接受发生概率,即安全目标(Safety Objective,SO);随后利用故障树分析法分析 ADS-B 系统中可能导致危险发生的内因,以此确定对相关系统元素的安全要求及安全假设,以确保安全目标的实现。

Bow-tie 模型结合了事件树分析和故障树分析,对事故发生的前因后果进行深入分析。图 2 展示了本评估方法的模型。评估过程由运行危险评估(Operational Hazard Assessment,OHA)和安全目标及要求分配(Allocation Safety Objectives and Requirements,ASOR)两部分组成。模型图的左侧代

表运行危险发生的原因,右侧代表危险所造成的后果,通过一系列事件链将危险产生原因、危险和危险导致的后果关联起来,并以图表的形式描述导致事故发生的路径。

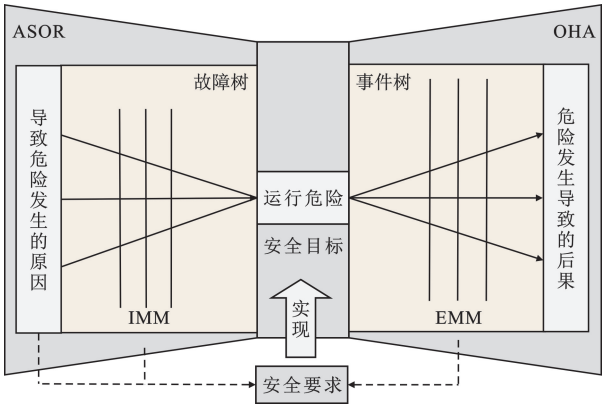

图 2 ADS-B IN 应用安全评估的 Bow-tie 模型

模型中右侧为 OHA 流程。在 OHA 流程中利用事件树分析,确定运行危险的 SO。事件树以假设运行危险的发生作为分析的起点。外部缓解手段(External Mitigation Means,EMM)以及环境条件作为中间事件,引导运行危险发生后的不同走向。在事件树的末端为各种可能发生的结果,每种后果都需要进行相应的严重程度及发生概率分析。最后利用事件树分析的结果,计算得到运行危险的安全目标。

模型中左侧为 ASOR 流程。在 ASOR 流程中利用故障树对运行危险进行分解,确定导致危险发生的基本原因。随后依照故障树图将运行危险的发生概率分解到各个基本原因,这些基本原因可能来自于人为、环境以及机载设备等。内部缓解手段(Internal Mitigation Means,IMM)可以预防运行危险的发生。经过对基本原因的分析,确定相应的安全要求,从而实现运行危险的安全目标。

2 OHA 流程

OHA 流程的主要目的为计算出运行危险的安全目标,即运行危险的最大可接受发生概率。实施步骤可大致分为 4 步:确定运行危险、确定后果并分配严重程度等级、分配总体安全目标(Safety Target,ST)并计算 Pe,最后计算运行危险的安全目标,如图 3 所示。

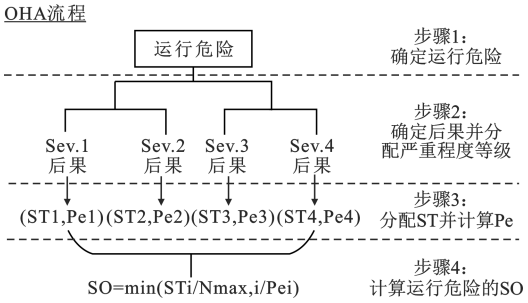

图 3 OHA 流程

2.1 确定运行危险

运行危险指飞行员在使用 ADS-B IN 应用执行飞行任务的过程中,可能导致安全性事故发生的异常情况。在确定运行危险时,首先需要确定 ADS-B IN 应用的运行环境、操作流程和相应的空中管制程序,作为 ADS-B IN 应用的标准操作条件及流程。随后对其标准操作条件及流程进行分析,考虑当某些标准操作条件未满足或标准操作未执行时,对安全性是否产生不利影响,以此确定应用的运行危险。

2.2 确定后果并分配严重程度等级

事件树分析按照事件发生的先后顺序确定运行危险所造成的后果。在事件树分析中,危险的缓解手段取决于应用的操作流程、程序及所处的环境条件。

事件树通常以二叉树的形式来呈现缓解手段的“成功”和“失败”,每一次分支都对应着一种缓解手段,在分支的末端描述了运行危险发生所造成的后果,见图 4。

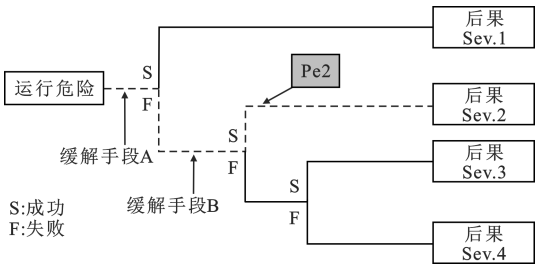

图 4 事件树图

事件树中的缓解手段包括环境条件和 EMM。环境条件指航空器所处的空域密度、气象条件和空域类型等信息,其并不总是能够起到缓解危险的作用,例如在空域密度较高的环境中,该环境条件可能造成飞行员和管制员工作量的增加。EMM 主要指的是飞行员使用 ADS-B IN 应用的操作规定,包括常规的操作流程和异常情况的处理,例如当飞行员发

现应用发生错误时,可以选择忽略其所提供的信息。

随后根据危险分类矩阵(Hazard Classification Matrix,HCM)[12],如表 1 所示,为每一个后果分配相应的严重程度等级(Severity,Sev)。

表 1　危险分类矩阵

影响	灾难性的(Sev. 1)	危险的(Sev. 2)	严重的(Sev. 3)	轻微的(Sev. 4)
对 ATC 的影响	间隔完全丢失	间隔极大地减少或在相当长的一段时间内失去空中管制	间隔显著减少空管管制能力显著降低	间隔略有减少或空管的工作量显著增加
对飞机运营的影响	机身受损或发生碰撞	安全裕度大幅降低	安全裕度显著降低	安全裕度略有下降

严重程度等级从 1~5 严重性依次降低,其中严重程度等级 5 可视为不存在安全影响,用 Sev. 1~Sev. 5 对严重程度等级进行表示。运行危险的后果按照受影响的对象可以大致分为 4 种类型,分别为对飞机操作造成影响、对飞机乘员造成影响、对飞行员造成影响和对空中管制造成影响。每个后果所造成的影响往往杂糅了对多种目标的影响,在分析过程中,通常将最高的严重程度等级分配给后果。

2.3　分配 ST 并计算“Pe”

ST 表示空中交通管理(Air Traffic Management,ATM)系统中具有某一特定严重程度等级的所有后果的最大可接受发生概率之和,例如,ST1 对应 ATM 系统中所有严重程度等级为 1 的后果的最大可接受发生概率。根据文献[13],风险分类方案(Risk Classification Scheme,RCS)为每个 ST 分配了相应的量化概率,见表 2。

表 2　风险分类方案

ST	AF=1 的量化概率(每飞行小时)	AF=10 的量化概率(每飞行小时)
ST1	10^{-8}	10^{-9}
ST2	10^{-5}	10^{-6}
ST3	10^{-4}	10^{-5}
ST4	10^{-1}	10^{-2}

根据国际民航组织对风险的定义,风险指的是运行危险所造成的后果的发生概率和与此运行危险所造成后果的严重程度等级之积,即

$$R=\mathrm{Sev}\times P \tag{1}$$

式中:R 表示风险;Sev 表示后果的严重程度等级;P 表示后果的发生概率。RCS 通过分配 ST 值方式限定了后果的发生概率 P,将相应严重程度等级的后果所造成的安全风险控制在了可接受的范围之内。设置 AF(Ambition Factor)因子可以增加 ST 的严苛性,实现更严格的安全风险管理。

“Pe”为条件概率,它表示在危险发生导致某一特定后果发生的概率。基于历史数据和仿真结果,对缓解手段的成功概率进行量化,结合事件树分析结果,计算概率“Pe”。图 4 中 Pe2 的计算取决于缓解手段 A 与缓解手段 B 之间的逻辑关系:当缓解手段 A 失败和缓解手段 B 成功同时发生导致严重程度等级为 2 的后果发生时,则 Pe2 的值为事件和运算的概率值,否则为事件与运算的概率值。一般地,各个缓解手段之间相互独立。

2.4　计算运行危险的安全目标

RCS 为每一种严重程度等级中的所有后果给出了总体最大可接受发生概率 ST,因此在进一步计算运行危险的 SO 之前,还需要确定各个严重程度等级所对应的危险数量。根据文献[14],ATM 危险总量和各个严重程度等级的 ATM 危险数量分布如表 3 所示。表中,$N_{\max,i}$ 表示某一特定严重程度的 ATM 危险量,其中 i 表示严重程度等级。从表中可以看出,ATM 危险共有 125 种,其中严重程度等级为 4 的有 73 种。

表 3　危险数量分布

严重程度等级	$N_{\max,i}$
Sev. 1	2
Sev. 2	25
Sev. 3	25
Sev. 4	73
总计	125

运行危险的最大可接受发生概率 SO 计算公式如下:

$$\mathrm{SO}=\min\left(\frac{\mathrm{ST}_i}{\frac{N_{\max,i}}{\mathrm{Pe}_i}}\right),i=1,2,3,4 \tag{2}$$

式中:i 表示严重程度等级;$N_{\max,i}$ 表示 ATM 系统中严重程度等级为 i 的危险最大总数;Pe_i 表示严重程度等级 i 的危险后果发生的条件概率;ST_i 表示严重程度等级 i 的所有危险后果的总体最大可接受发生概率。此过程中确定了危险的 SO。

3　ASOR 流程

ASOR 流程的目的是确定 ADS-B IN 应用的安

全要求,保障运行危险的安全目标在可接受的范围之内。

ASOR 流程可大致分为 3 步,分别为构建故障树、分配 SO 和确定安全要求。ASOR 流程的步骤如图 5 所示,其中 BC 代表基本原因(Basic Cause)。

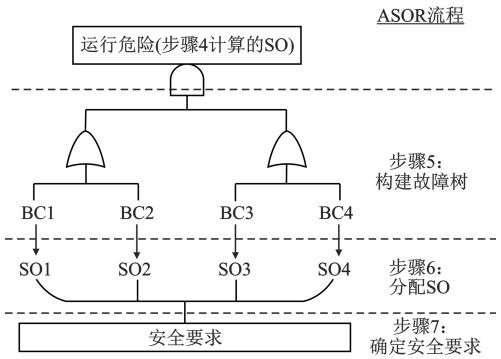

图 5 ASOR 流程

3.1 构建故障树

构建故障树的目的是确定导致危险发生的基本原因。在构建故障树之前,需要建立 ADS-B IN 应用的功能架构。功能架构中包含了实现应用功能所需的功能模块,整个架构可以分为 3 个子系统,分别为地面子系统、接收子系统和发送子系统。

构建故障树以运行危险为顶事件,根据应用的监视功能架构和操作流程,分析引起运行危险发生的原因,对危险自顶向下进行分解。故障树的示意图见图 6,失效模式描述 ADS-B IN 应用中的功能模块无法正常功能的情况,对它们进行彻底分解,可以得到导致危险发生的基本原因。基本原因作为故障树的底事件,可以将其分为 4 种类型,分别为技术、程序、人为和环境原因。

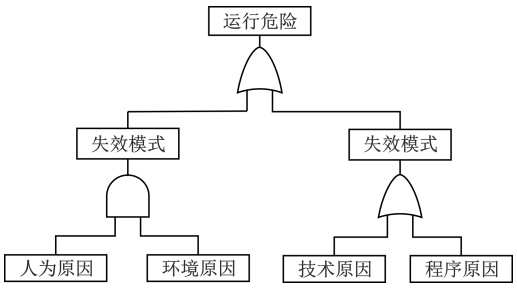

图 6 故障树示意

故障树的各个节点之间通过与非门连接,详细地展示了基本原因之间的相互影响和导致运行危险发生的途径。当某一基本原因在底事件中多次出现时,可以利用布尔代数对故障树进行简化分析。一般地,我们认为各个基本原因之间相互独立,因此与门中的上层事件的概率可以表示成下层事件概率的乘积,或门中上层事件的概率则可以表示成下层事件和运算的概率。

3.2 分配 SO

此步骤的目的为每个基本原因设置合适的概率要求。在对基本原因进行概率分配时,首先利用已有的文献研究和历史数据对概率进行分配和验证,例如 GNSS 系统的失效率和人员操作失误率等。在对人员操作失误率通常采用定性的方式描述其发生频率,如表 4 所示,其每个频率对应了一个量化的发生概率[14]。然后基于首次分配所得结果和故障树的逻辑结构,利用与非门的事件概率计算原则,为剩余的基本原因分配概率,这些基本原因通常是与 ADS-B IN 应用相关的技术性原因。

表 4 定性频率的量化概率

定性的频率	定量的概率
非常频繁的	$10^{-2}\sim10^{-1}$
频繁的	$10^{-3}\sim10^{-2}$
稀少的	$10^{-4}\sim10^{-3}$
非常稀少的	$10^{-5}\sim10^{-4}$

值得注意的是,安全目标可能存在多种不同的分配方式,为了找到最优的解决方案,需要综合考虑应用的功能架构、要求和程序等。最优分配方案的确定必须在充分考虑所有的利益相关方并确定合适的缓解手段的前提条件下进行。当某一基本原因在多个危险的故障树中出现时,其最终概率值的分配应当取概率值最小值。

3.3 确定安全要求

基于前述步骤所得结论,对基本原因展开研究。每一个基本原因都将确定一个安全要求或安全假设,这取决于基本原因的性质。一般地,与人员、环境和管制程序相关的基本原因将产生安全假设,假设的合理性将通过实验进行验证。与通信数据链路和 ADS-B IN 应用设备相关的基本原因为安全要求的主要来源。此过程在相关专家的研讨下进行确定并验证。

4 案例研究

空中情景意识(Enhanced Traffic Situational Awareness During Flight Operations,AIRB)应用是一种 ADS-B IN 应用,它能够在任意飞行阶段、气象条

件以及空域类型中增强飞行员的交通情景意识。飞行员通过交通显示屏获取 AIRB 应用所提供的信息,结合空管或窗外信息,实现对周边交通更精确清晰的意识。AIRB 应用不仅能够增强飞行安全和空中交通管制的效率,还能帮助飞行员更好地识别和规避危险事故的发生。下面将 AIRB 应用安全评估过程作为本文中评估方法的应用实例,给出 AIRB 应用安全评估过程的结果。

4.1　OHA 结果

首先,对 AIRB 应用的操作流程和空中管制程序进行分析,确定了 AIRB 应用的一个运行危险。

OH:飞行员被交通显示器信息误导,认为存在威胁情况,而实际上没有。

AIRB 飞机(指装备了 AIRB 应用的飞机)在运行危险发生时所处的情景决定了其环境条件以及后续可能采取的危险缓解措施,两者统称为屏障。因此在应用设计阶段对危险进行事件树分析之前,还需要预设 AIRB 飞机运行危险发生时所处情景。环境条件通常包括 AIRB 飞机是否能够接收到空中交通服务、其所处的气象条件、所处空域类型及空域密度等。AIRB 飞机的所处的环境条件在一定程度上决定了该危险发生所造成后果的严重程度等级。

运行危险发生后,飞行员和管制员将采取一系列的缓解措施来降低其所可能造成的影响,这些缓解措施即为 EMM。EMM 通常包括飞行员使用 AIRB 应用执行飞行任务时的常规性操作以及在发现异常情况后处理流程,例如飞行员需要时刻对窗外信息、无线电信息和交通显示屏信息进行一致性检查等。为进行说明,此处对 AIRB 飞机的所处环境类型 I 作如下设定:

运行环境 I:AIRB 飞机和感兴趣的交通都在 A、B、C 或 D 类空域中以仪表飞行规则飞行,所处空域提供雷达服务,气象条件为仪表气象条件,且该区域交通密度较高。

根据 AIRB 应用的操作流程,将环境类型 I 中的 OH 从发生到所有的缓解措施均失效分为 3 个阶段,分别为 P_0、P_1、P_2。在 P_0 阶段,AIRB 飞机的飞行员根据交通显示屏和空管的无线电信息对交通情景状况进行评估;P_1 阶段中飞行员准备采取避撞的机动措施导致与其他飞机的安全裕度降低;P_2 阶段中,飞行员已经采取了避撞机动操作并导致了与其他飞机间的安全裕度降低。表 5 中 B1~B8 为 OH_I 危险发生后的屏障,各屏障的成功概率为根据航空安全数据库所给出的保守估计值。

表 5　各屏障成功概率及屏障描述

屏障	屏障描述	成功概率/%
B1	空管接收到 AIRB 飞机的无线电信息并意识到飞行员的交通情景意识是错误的,随后联系飞行员解决这一情况	99.000
B2	AIRB 飞机公布他们的操作意图。空管意识到这一操作可能导致其安全裕度降低并联系飞行员解决这一情况	99.900
B3	AIRB 飞机的机动操作没有导致与感兴趣飞机或者周边飞机的安全裕度降低	99.999
B4	空管注意到 AIRB 飞机导致安全裕度降低的操作,并根据管制程序在安全裕度显著降低之前向飞行员发布纠正措施	99.990
B5	在安全裕度显著降低之后,AIRB 飞行员通过目视侦查碰撞风险,并进行机动操作规避其他飞机	20.000
B6	在安全裕度显著降低之后,其他飞机的飞行员通过目视侦查碰撞风险,并进行机动操作规避 AIRB 飞机	20.000
B7	空管发现存在碰撞风险并发布纠正措施。相关飞机根据空管提供的碰撞规避服务避免碰撞发生	99.900
B8	适当的时机和空间位置避免飞机发生碰撞	90.000

在事件树中依据屏障分析出危险发生之后所可能导致的后果,并根据各个屏障的成功概率和逻辑关系,计算出每种后果的发生概率。后果的严重程度等级也在此时分析给出。图 7 展示了 OH_I 事件树分析的结果,在事件树末端给出了评估结果。

	P_0	P_1			P_2				评估结果	
OH	B1	B2	B3	B4	B5	B6	B7	B8	Sev	Pe
	S								5	9.90×10^{-1}
OH_1		S							4	9.90×10^{-3}
	F		S						5	1.00×10^{-5}
		F		S					4	1.00×10^{-10}
			F		S				3	2.00×10^{-15}
				F		S			3	1.60×10^{-15}
					F		S		3	6.39×10^{-15}
						F		S	2	5.76×10^{-18}
							F			
								F	1	6.40×10^{-19}

图 7　OH_I 的事件树分析结果

最后由 SO 的计算公式,得到 OH_I 的 SO 为 1.40×10^{-3}。计算结果如表 6 所示。

表 6 OH_I 的 SO 计算结果

Sev	Pe	ST(AF = 10)	SO
1	6.40×10^{-19}	1.0×10^{-9}	7.81×10^{8}
2	5.76×10^{-18}	1.0×10^{-6}	6.94×10^{9}
3	9.99×10^{-15}	1.0×10^{-5}	4.00×10^{7}
4	9.99×10^{-3}	1.0×10^{-2}	1.40×10^{-3}

4.2 ASOR 结果

图 8 展示了 AIRB 应用的功能架构,分为发送域和接收域,子系统的接口之间用直线表示。功能架构展示了实现 AIRB 应用的必要功能。

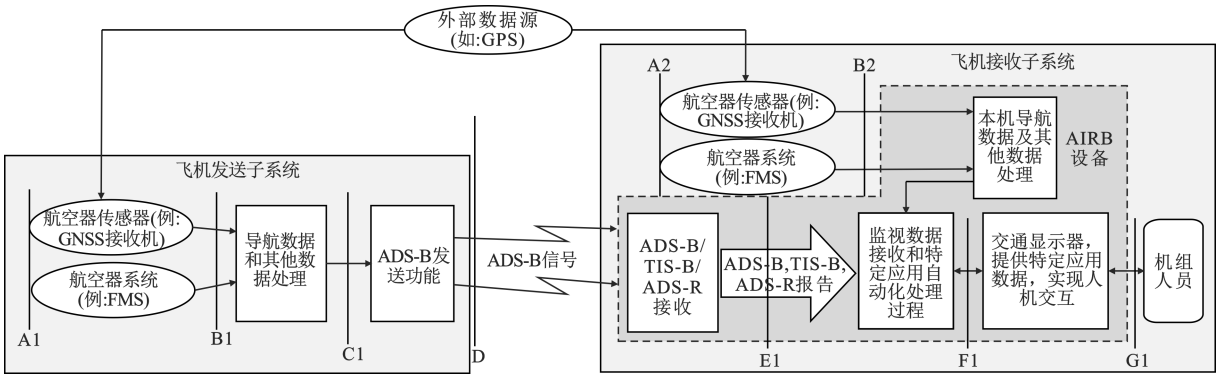

图 8 AIRB 应用的功能架构

此运行危险发生可能原因如下:

1)交通显示器上显示“不存在有威胁的飞机”,但是飞行员对此信息的理解出现错误,并且认为存在有威胁的飞机。这是一种人为的基本原因(Human Factor,HF),其发生概率为 1.0×10^{-3} 每飞行小时。

2)交通显示器错误的显示“存在有威胁的飞机”,飞行员被这一信息误导。这种情况发生的原因是因为系统中的显示数据发生了损坏,并且这些损坏的数据以一种合乎逻辑、一致且连续的方式在交通显示器上显示出了一个虚构的威胁飞机。

交通显示器的显示信息发生损坏,是由于 ADS-B 系统数据完整性失效或者是位置测量数据不准确。在飞机接收子系统中,数据完整性失效可能发生在 D/A2→G1,其导致 AIRB 数据损坏的概率为 1.0×10^{-3}(R-01),水平位置测量数据不准确且大于误差范围发生在 A2→B2,其发生概率为 1.0×10^{-3}(R-02)。在飞机发送子系统,数据完整性失效可能发生在 A1→D,其导致 AIRB 数据损坏的概率为 1.0×10^{-3}(T-01),水平位置测量数据不准确且大于误差范围发生在 A1→B1,其发生概率为 1.0×10^{-3}(T-02)。

当交通显示器的显示信息损坏时,要使得机组人员认为存在威胁情况,还需要交通显示器以一种符合逻辑、一致且连续方式的将感兴趣交通显示成有威胁的飞机,假设这一情况发生概率为 10%(ENV)。

OH_I 的故障树分解情况如图 9 所示。图 9 中给出了每种基本原因的发生概率。根据基本原因的性质,分析出安全要求为 R-01、R-02、T-01、T-02。通过基本原因发生概率计算顶事件危险的发生概率为 1.40×10^{-3},实现了 OHA 阶段中危险的安全目标。

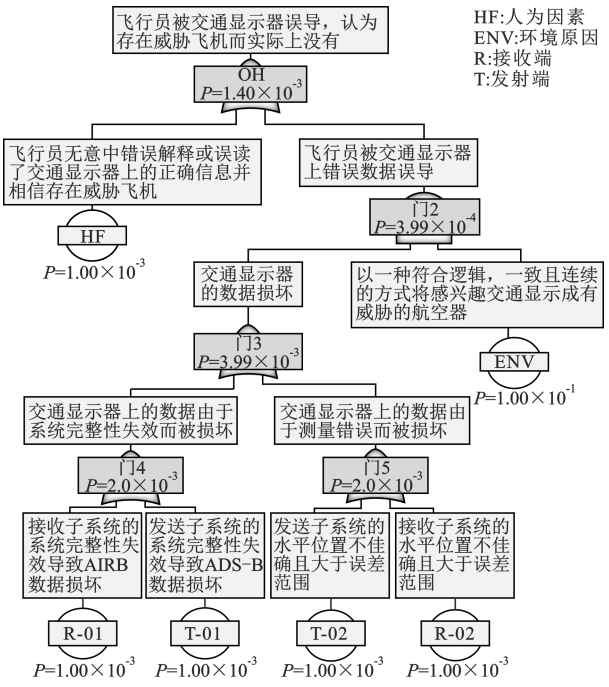

图 9 OH_I 的故障树分解

5　结束语

本文引入了一种基于 Bow-tie 模型的 ADS-B IN 应用的安全评估方法。区别于系统级的安全分析方法,该方法对 ADS-B 系统应用的功能进行安全分析,并得出相应的量化安全要求,实现对危险发生概率的控制。本文利用该方法对 AIRB 应用的设计进行了安全评估,得出了 AIRB 应用的运行危险的安全目标及安全要求,以此对该方法的应用做出了进一步的说明。该方法对 ADS-B IN 应用开发、维修保障及人员操作训练均具有重要的实践意义。

值得注意的是,本文中所使用的数据由国外的民航安全组织相关文献中给出,其在国内的适用性仍需要进行进一步的研究。

参考文献:

[1] FAA. Avionics supporting automatic dependent surveillance-broadcast (ADS-B) aircraft surveillance applications(ASA): TSO-C195c[S]. Washington DC: FAA,2023:3-10.

[2] 王洪. 飞机监视应用系统、航迹融合与 ADS-B In 应用[J]. 电讯技术,2019,59(12):1488-1494.

[3] APAC. ADS-B implementation and operations guidance document:edition 11.0[S]. Melbourne:APAC,2018:29-43.

[4] ALI B S, OCHIENG W Y, MAJUMDAR A. ADS-B: probabilistic safety assessment [J]. Journal of Navigation,2017,70(4):887-906.

[5] OLAGANATHAN R. Safety analysis of automatic dependent surrveillance-broadcast(ADS-B) system[J]. International Journal of Aerospace and Mechanical Engineering,2022,5(2):50-64.

[6] SESSO D B,VISMARI L F,SILVA NETO A V,et al. Using data integrity as an improvement characteristic to assess the safety of ADS-B-based systems [C]//2015 IEEE International Conference on Dependable Systems and Networks Workshops. Rio de Janeiro:IEEE,2015:88-95.

[7] ZEITLIN A D. Safety assessments of ADS-B and ASAS [C]//USA/Europe Air Traffic Management R&D Seminar. Savannah:FAA,2021:89-102.

[8] YIU C Y, TAM T K, NG K K H. An ADS-B aided dynamic traffic alert for robust safety assessment in controlled airspace [C]//2021 IEEE International Conference on Industrial Engineering and Engineering Management. Singapore:IEEE,2021:319-323.

[9] Safety, performance and interoperability requirements document for enhanced traffic situational awareness during flight operations(ATSA-AIRB):RTCA DO-319 [S]. Washington DC:RTCA,2010.

[10] Safety, performance and interoperability requirements document for the in-trail procedure in oceanic airspace (ATSA-ITP) Application: RTCA DO-312 [S]. Washington DC:RTCA,2008.

[11] Safety, performance and interoperability requirements document for enhanced visual separation on approach (ATSA-VSA):RTCA DO-314[S]. Washington DC: RTCA,2008.

[12] Guidelines for approval of the prevision and use of air traffic services supported by data communications:RTCA DO-264[S]. Washington DC:RTCA,2000.

[13] EUROCONTROL. Eurocontrol safety regulatory requirement (ESARR4)[S]. Brussels:EUROCONTROL,2001:10-34.

[14] EUROCAE. Process for specifying risk classification scheme and deriving safety objectives in ATM: EUROCAE ED 125[S]. Paris:EUROCAE,2010.

作者简介:

肖　阳　男,1999 年生于四川蓬安,2022 年获学士学位,现为硕士研究生,主要研究方向为 ADS-B 系统。

王　洪　男,1974 年生于四川仁寿,2007 年获博士学位,现为副教授,主要研究方向为飞机环境监视技术、雷达系统与信号处理。

赵子安　男,2001 年生于河北石家庄,2023 年获学士学位,现为硕士研究生,主要研究方向为雷达系统。