机场自动旅客运输系统的安全风险识别及危害控制

付世亮[1,2] 朱冬进[2] 王良良[2]

（1. 南京航天航空大学民航学院，211106，南京；2. 中车浦镇阿尔斯通运输系统有限公司，241060，芜湖//第一作者，高级工程师）

摘 要 引入安全风险接受和危害控制的沙漏模型原则，采用PHA（初步危害分析）法对机场APM（自动旅客运输）系统的风险识别和危害控制进行研究。对机场APM的系统集成层进行初步危害辨识，列出机场APM系统集成层的风险清单。对初步危害进行后果和损失分析，并根据历史经验给出初步的危害原因。针对可能造成危害的原因，为相关责任方提供了相应的保障措施，并形成了初步的系统安全需求，可作为后续子系统或核心机电设备的设计输入。

关键词 城市轨道交通；自动旅客运输系统；安全风险识别；初步危害分析；危害控制措施

中图分类号 U239.592

DOI：10.16037/j.1007－869x.2023.03.025

Safety Risk Identification and Hazard Control of Airport Automated People Mover System

FU Shiliang, ZHU Dongjin, WANG Liangliang

Abstract With the introduction of hourglass model principle for safety risk acceptance and hazard control, the safety risk identification and hazard control of airport APM (automated people mover) system is studied with PHA (preliminary hazard analysis) method. By preliminarily identifying the hazard of airport APM system integration level, the risk list of airport APM system integration level is pulled out. Consequence and loss of the preliminary hazard are analyzed and the causes of preliminary hazard according to historical experience are given. According to the possible hazard causes, relevant guarantee measures are provided for the associated responsible parties, and the preliminary requirements for system safety are formed, which can be used as the design input for subsequent subsystems or core electromechanical equipment.

Key words urban rail transit; APM system; safety risk identification; preliminary hazard analysis; hazard control measures

First-author's address College of Civil Aviation, Nanjing University of Aeronautics and Astronautics, 211106, Nanjing, China

机场APM（自动旅客运输）系统主要用以解决机场交通内部枢纽中心、航站楼及卫星厅之间的旅客运输需求，需满足机场昼夜不间断运营的要求，还需具备高可靠性和高安全性。本文引入风险识别和危害控制的沙漏模型，采用PHA（初步危害分析）法对机场APM系统的安全风险识别和危害控制进行研究。

1 机场APM系统安全风险识别和危害控制概述

在CENELEC（欧洲电工标准化委员会）制定的EN 50126-1：2017[1]、EN 50126-2：2017[2]等铁路安全防护标准中，都定义了适用于轨道交通行业的安全系统方法。本文在构建机场APM系统的风险接受和危险控制框架时引入沙漏模型，通过沙漏模型规范轨道交通线路责任单位和设备供应商之间的工作范围、安全职责和接口信息。

机场APM系统具有其特殊性：系统具有多个核心机电设备，且系统集成大多为交钥匙工程。从架构上看，机场APM系统可分为两个层次：一是系统集成层，指机场APM总承包商/系统集成方，或机场APM系统的责任单位；二是子系统/核心设备层，即车辆、信号、供电轨及站台门等核心设备。

机场APM系统风险识别和危害控制的重点为：①机场APM系统集成层的风险分析，以获取系统整体的安全目标和系统规范要求；②子系统/核心设备层的危害分析，以及安全设计过程中的危害控制，以确保系统整体安全目标的落实和系统规范的实现；③根据子系统危害分析结果更新修正系统集成层的危险清单，使其安全目标和系统规范要求合理、合规、可执行。

对于总承包商/系统集成方而言，需要规范机场APM系统的风险接受原则，通过风险分析获取整个机场APM系统对于设备操作和维护、技术安

全等方面的需求;子系统/核心机电设备则通过采取危害控制技术与措施(包括原因分析、对已定义的危险源进行提炼和优化、危害控制技术等),确保满足风险分析所得出的系统安全要求。

对于机场 APM 系统集成层的风险定义和评价,由于缺乏可借鉴的数据和资料,且能获得的系统设计信息非常有限,目前仍难以根据各子系统/核心机电设备的功能、组成及产品设计等信息进行由下至上的风险因果分析。因此,本文采用 PHA(初步危害分析)法对机场 APM 系统进行风险分析是符合实际的。

图 1 为机场 APM 系统风险接受和危害控制的框架结构。该框架结构对总承包方/系统集成方的职责,以及子系统/核心机电设备的职责进行定义,这说明机场 APM 系统的安全工作需要从系统集成层开始自上而下进行规划,并由具体各子系统进行实施,从而确保安全工作的统筹管理得以顺利地完成。

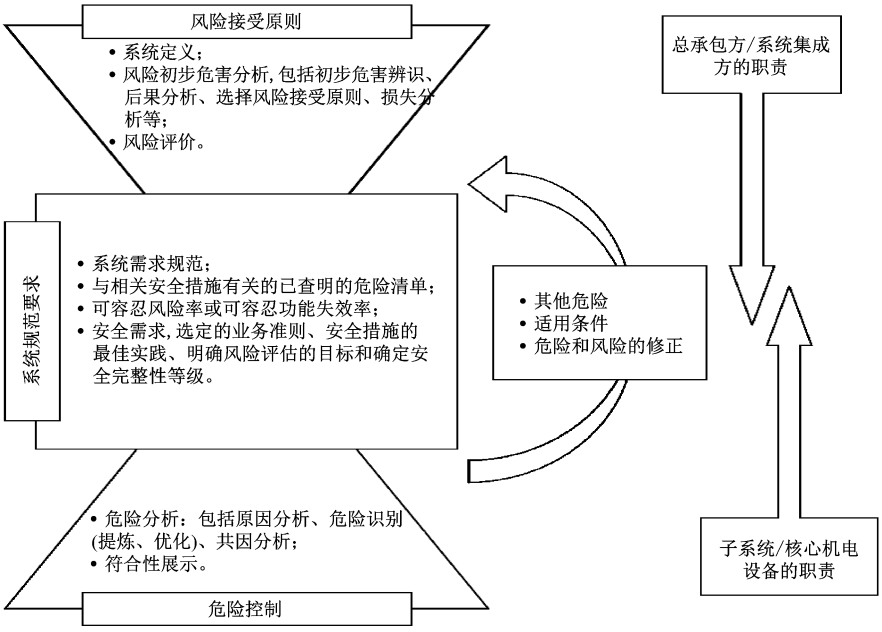

图 1　机场 APM 系统风险接受和危害控制框架结构示意图

Fig. 1　Structure diagram of risk acceptance and hazard control framework of airport APM system

2　PHA 法概述

PHA 法是一个识别危险源、危险原因、危险后果和风险水平,以及指导制定减少危险/风险措施的安全分析工具。PHA 法的重点在于对系统的所有危险状态有一个初步、总体的认识,而不是控制所有的风险。

基于 PHA 法,机场 APM 系统的初步危害分析用于识别系统集成层的所有危险源和定义子系统/核心设备层的安全需求。其目的主要包括 3 个方面:①识别和定义必须控制的主要危险;②确定机场 APM 系统集成层引发主要危险的原因及可能造成的后果;③对危险的风险等级进行初步评估,以确定哪些危险在子系统/核心设备层的危险分析中需要进行进一步的定性和定量分析。

PHA 法得到的结果将转化为最初的安全需求,因此计算发生每个危害的可接受概率或可容忍概率,并将此作为机场 APM 系统集成层的安全目标。识别和分析得到的危害将持续在各子系统/核心机电设备层进一步进行分析和评估,使各危害最终得以有效控制,使整个机场 APM 系统的风险控制在较低的、可接受的范围内。

3　机场 APM 系统的初步危害分析

机场 APM 系统初步危害分析的流程包含 4 个步骤:①初步危害辨识;②后果和损失分析;③初步原因分析和制定相应的保障措施;④风险等级的判定和危害管理。

3.1　初步危害辨识

初步危害辨识是整个系统风险评估的基础,也是执行整个机场 APM 系统安全保障活动的关键步骤。应全面、系统地识别机场 APM 系统的危害,确

保人员、流程和系统运营模式(包括正常、降级和紧急模式)的全覆盖。在评估过程中,应考虑可能发生的所有潜在危害/事故(包括工作人员错误操作的可能性),无论其发生概率的高低。

因机场 APM 系统包括车辆、轨旁及核心机电等子系统,其部分危害的发生不仅在正常运营条件下,还可能在系统运营故障或异常(降级模式或紧急模式)情况下发生。因此需要结合机场 APM 项目具体的运营条件、设备工作模式等因素进行场景细分。针对机场 APM 系统的组成和功能特点,本文从可预见的事故识别、系统的物理条件、人员的不适当行为及系统的特殊危害 4 个方面进行危险源的识别。

1) 可预见的事故识别。根据机场 APM 系统的列车运行路线,确定是否存在需要额外控制的任何潜在高风险,这些风险主要包括:①两列及多列车间发生的事故,如脱轨、碰撞等;②列车车厢内发生的事故,如乘客在上下车时发生意外(如被困在站台门中间、穿高跟鞋的女士被绊倒等)故障,以及乘客在车内发生滑到、触电等事故;③在车站(包括站台、楼梯等区域)发生事故。

2) APM 系统的物理条件。结合轨道交通行业事故统计及经验,总结筛选出 APM 系统因物理条件引起的危害,主要包括热效应、电磁场及放射性等。

3) 人员的不适当行为。主要包括:①系统功能降级或非正常时人员的手动误操作;②人员错误行为,包括故意破坏的活动;③其他人的不安全行为,包括不遵守规则制度等。

4) 机场 APM 系统的特殊危害。机场 APM 系统主要用于承担机场航站楼内部的旅客输送任务,由于机场特定的运行环境,机场 APM 系统在应用上与传统的地铁和轻轨有一定的差异。此外,机场 APM 系统面对的多为商务客流,这使得机场 APM 系统在服务品质和服务标准上的要求更高。这些差异导致机场 APM 系统存在特殊的危害,主要包括:①空间舒适感要求高,需考虑乘客大多携带行李这一特点;②为了与机场航班服务时间同步,机场 APM 系统需昼夜不间断运行;③机场 APM 系统必须具有高可用性,不能因机场 APM 系统维修或故障导致航班延误;④考虑机场管制区域安全,列车内不再设置贯通道,而是针对不同的客流类型在车站站台设置物理隔断。

通过对机场 APM 系统进行初步危害辨识,将有可能产生的危害进行分类并编号,得到机场 APM 系统集成层的风险清单,如表 1 所示。

3.2 危害的后果和损失分析

基于机场 APM 系统的运行环境对危害的后果和损失分析,主要是对机场 APM 系统的实际运行环境和管理机制(主要包括机场 APM 的外部接口、运营维护人员的操作规则、应急/故障处置流程等)进行分析。在初步危害辨识的基础上,分析引发此危害的子系统及可能影响的子系统,进而推测危害对整个机场 APM 系统可能产生的影响,评估危害造成后果和损失的严重性等级。

机场 APM 系统危害的后果和损失分析不应仅针对可能导致事故的危害最后情况,还应全面仔细识别事故的诱因。后果和损失分析需要考虑 3 个维度:①人员伤害,即导致人员受伤或死亡的情况;②环境的损害,主要包括财产损失、环境污染和其他影响等情况;③商业及机场形象损失,主要包括财产损失、乘客投诉等情况。

3.3 初步原因分析和制定相应的保障措施

在机场 APM 系统的初步危害分析中,将根据历史经验给出初步的危害原因。针对危害可能形成的原因,为相关责任方提供相应的保障措施,并形成初步的系统安全需求,使之成为后续子系统或核心机电设备的设计输入。

初步原因分析根据技术故障、人为错误、运营维护管理失效及外部因素等 4 个方面开展。其相关责任方具体包括:①机场 APM 系统集成方;②车辆、信号、供电、站台门、运营管理及调度等子系统/核心机电设备的责任方;③设备维保团队、运营管理团队;④土建、消防等其他责任方。

作为机场 APM 系统集成层的危害分析,其保障措施分为现有的保障措施和可能的保障措施两方面。制定措施时可借鉴其他类似的轨道交通产品和系统的经验,包括所参考系统中已确认执行的保障措施和可能的保障措施两个部分,并形成机场 APM 系统的安全要求。将安全要求转交给各子系统和相关方,其中一部分措施将作为子系统层次的安全要求,使之成为后续设计的输入条件。

3.4 风险等级的判定和危害管理

机场 APM 系统中确定的所有危害都需要通过危害日志进行记录、管理和转移。危害日志是以数据库形式存在的一种工具,用于记录已识别出的危

表 1　机场 APM 系统集成层的风险清单

Tab. 1　Risk list of airport APM system integration level

风险类型	编号	危害描述
列车脱轨（DR）	DR-01	轨道上有异物
	DR-02	车辆结构故障
	DR-03	轨道结构或道岔故障
	DR-04	极端环境条件（如大风、地震等）
	DR-05	列车超速行驶
列车碰撞（CC）	CC-01	FAO（全自动运行）模式下列车间发生碰撞
	CC-02	手动驾驶模式下列车间发生碰撞
	CC-03	FAO 下列车与维护人员发生碰撞
	CC-04	手动驾驶列车运行期间列车（或维修救援车辆）与维护人员发生碰撞
	CC-05	列车与乘客（或非维护人员）发生碰撞
	CC-06	列车与轨道道岔发生碰撞
	CC-07	列车与侵入限界的结构发生碰撞
列车产生过大的冲击力或减速度（EJ）	EJ-01	过大的正冲击或加速度
	EJ-02	过大的反冲击或减速度
列车车门或站台门的危害（DH）	DH-01	列车进站、停靠或出站时因列车车门和站台门造成的危害（如站台门障碍物检测失效、门防夹检测失效及列车的非预期开门等）
因火灾/烟雾造成人员伤害或设施显著损坏（FS）	FS-01	车站设备房发生火灾/烟雾
	FS-02	车辆段（含停车场）发生火灾/烟雾
	FS-03	变电站发生火灾/烟雾
	FS-04	列车上发生火灾/烟雾
	FS-05	车站站台区域发生火灾/烟雾
	FS-06	隧道/轨旁区域发生火灾/烟雾
触电（EL）	EL-01	维护人员触电
	EL-02	非维护人员触电
	EL-03	设备短路
人身伤害（PI）	PI-01	物体带尖锐或突出的边缘引发人员受伤
	PI-02	车站站台区域或车辆内部表面潮湿，造成乘客滑倒、绊倒或跌倒
	PI-03	乘客碰到破碎玻璃
	PI-04	维护人员在工作期间接触到危险材料（热物体/表面/液体/化学品等）
	PI-05	因车站布局/应急程序/通信设备等设施或管理机制导致疏散救援时间增加
	PI-06	紧急通道/疏散通道失效
	PI-07	人员在紧急通道/疏散通道上滑倒、绊倒或跌倒
	PI-08	对残疾人造成的人身伤害（如无法安全地进入或离开列车等）
	PI-09	因通风不足造成人员窒息
	PI-10	因设备故障导致人员被困在列车内
	PI-11	工作人员在运营和维护期间受到伤害
接触有害物质（HM）	HM-01	列车释放有害物质
	HM-02	火灾释放有毒物质
	HM-03	不法分子故意将危险物质置于列车内
	HM-04	未经培训的人员碰触了含有害物质的设备
安全漏洞（SB）	SB-01	APM 系统的安防系统失效
过量的电磁干扰（EM）	EM-01	车辆内部系统受到电磁干扰
	EM-02	轨旁设施受到电磁干扰
	EM-03	外部环境和个人设备（如医疗、电子产品等）受到电磁干扰
爆炸（EX）	EX-01	车站设备房、变电站或轨道区域内发生爆炸
	EX-02	车辆段（含停车场）发生爆炸
	EX-03	列车上发生爆炸
	EX-04	车站站台区域内发生爆炸

害，以及已采取的或将要采取的保障措施。

初步危害分析中识别得到每个危害均包括 4 种状态：开放、消除、导出和关闭。保障措施落实后，已识别危害的发生概率应降低至可容许的水平。如果危害的最终剩余风险仍处于“无法容忍高”或“可接受中等”水平，则需对该危害所涉及的子系统

基于 ALARP(最低合理可行)原则进行评估,以证明风险已降至尽可能低的合理水平。

4　机场 APM 系统的风险识别和危害分析

4.1　危害分析过程的案例说明

在采用 PHA 法对机场 APM 系统进行初步危害分析的过程中,基于机场 APM 系统集成层风险的进一步分析,根据系统集成层的 57 种危害识别出 105 种产生这些危害的可能原因。表 2 以危害编号 CC-01(FAO 模式下列车间发生碰撞)这一运营场景为例,说明机场 APM 系统的风险识别和危害分析过程。

表 2　FAO 模式下列车间碰撞的危害分析过程

Tab. 2　Hazard analysis process of collision between trains under FAO mode

危害描述	危害的影响	危害造成可能原因	相应的子系统/责任方	相关的安全要求	保障措施
FAO 模式下列车间发生碰撞	前后两列车相撞,导致设备损坏或乘客伤亡	列车行进方向错误	信号子系统	① 列车须按照预定的交通指示方向运行;②列车不允许向后移动	① 列车自动防护应根据列车自动控制提供的进路锁定列车运行方向,防止列车向错误方向行驶;②列车自动防护应提供倒溜防护和施加紧急制动功能
			车辆子系统	不能发生因设备故障导致列车行进方向错误的情况	应提供可靠的车辆牵引设计;应提供车辆前进方案所需要的使能信号
			运营管理团队	在设置或取消恢复进路时,运营人员须确认被设置或取消的恢复进路与预期要操作的进路一致	定义操作规范,并对人员进行培训

4.2　机场 APM 系统的风险识别结果

本文对机场 APM 系统的每条危害进行了详细的原因分析和后果分析,系统集成层的每一种危害都可能涉及到一个或多个相关责任方。在所识别出的系统集成层的危害中,车辆子系统涉及 49 项,信号子系统涉及 34 项,供电子系统涉及 10 项,站台门子系统涉及 17 项,运营管理及调度子系统涉及 17 项,车辆段设备涉及 7 项,运营管理团队涉及 20 项,设备维保团队涉及 14 项,土建(含消防、站台、供电)等其他责任方共涉及 21 项。

通过基于 ALARP 原则的评估分析,最终可得到:风险可容忍级别为“无法容忍”的初始风险为 32 条,占比为 30.4%;风险可容忍级别为“可容忍”的初始风险为 71 条,占比为 67.7%;风险可容忍级别为“可接受”的初始风险为 2 条,占比为 1.9%。

需要注意的是,在对机场 APM 系统集成层进行初步危害分析时,由于所有可能的保障措施的可行性并没有得到最终确认,也没有在产品设计中得以实施,因此这里 PHA 分析并未考虑残余风险评估,仅通过风险分析将所有危害转移到各子系统,并将安全要求传递给各子系统。因此,需要在各子系统或核心机电设备的产品设计中对相关的安全要求和保障措施进行确认。

5　结语

基于机场 APM 为多核心机电设备、系统集成应用采用交钥匙方式等的特殊性,本文从 APM 项目系统集成层和子系统/核心机电设备层两个层次分别定义了安全相关活动的工作范围、安全职责和接口信息。将 APM 系统集成层的初步危害分析结果作为识别得到的危险源,提供了机场 APM 系统集成层的危害风险清单,并将相关的安全要求和保障措施作为各子系统/核心机电设备层进一步分析和证明其合规性输入的依据。

采用 PHA 法对机场 APM 系统的系统集成层进行安全分析,可以系统地发现各种潜在风险,并形成系统安全要求。这些安全要求将转移给各子系统和相关责任方,并成为后续设计的输入。本研究可为设计阶段机场 APM 系统安全性的提高提供参考。

参考文献

[1]　CENELEC. Railway applications — the specification and demonstration of reliability, availability, maintainability and safety (RAMS) – part 1: generic RAMS process: EN 50126-1: 2017 [S]. Brussels: CENELEC, 2017.

(下转第 142 页)