



恒创工程技术研究协会

HETRA

ICS 03.220.50

CCS V09

团体标准

T/HETRA 0112—2026

民航运行安全风险识别技术规范

Technical specification for civil aviation operational safety risk identification

2026-05-14 发布

2026-06-01 实施

恒创工程技术研究协会 发布





目 次

目 次	2
前 言	5
引 言	6
1 范围	7
2 规范性引用文件	7
3 术语和定义	7
3.1 运行安全风险	7
3.2 飞行数据回溯	8
3.3 异常	8
3.4 操作偏差	8
3.5 风险识别模型	8
3.6 可追溯性	8
3.7 失效安全	8
4 总体原则	9
4.1 合法合规	9
4.2 安全优先	9
4.3 证据驱动	9
4.4 人机协同	9
4.5 持续改进	9
5 组织与职责	9
5.1 责任体系	9
5.2 专业复核	10
5.3 变更授权	10
6 数据范围与治理	10
6.1 数据范围	10
6.2 数据分级分类	10
6.3 数据字典	10
6.4 质量状态	11



7	处理流程	11
7.1	流程组成	11
7.2	阶段划分	11
7.3	规则与模型并行	11
7.4	异常降级	12
8	飞行数据回溯	12
8.1	航段重构	12
8.2	基线比对	12
8.3	事件关联	12
8.4	趋势分析	12
9	异常识别	12
9.1	识别类型	12
9.2	阈值管理	13
9.3	模型要求	13
9.4	误报与漏报	13
10	气象风险评估	13
10.1	数据融合	13
10.2	风险对象	13
10.3	时空匹配	13
10.4	最低标准边界	13
11	机组疲劳风险预测	14
11.1	管理边界	14
11.2	输入因素	14
11.3	模型验证	14
11.4	处置原则	14
12	操作偏差分析	14
12.1	基准建立	14
12.2	偏差分类	14
12.3	情境解释	15
12.4	公正文化	15
13	风险融合与分级	15



13.1	风险融合	15
13.2	可能性与严重度	15
13.3	不确定性	15
13.4	否决条件	16
14	预警输出与闭环处置	16
14.1	预警内容	16
14.2	分级通知	16
14.3	人工复核	16
14.4	闭环状态	16
15	效果验证	16
15.1	验证计划	16
15.2	指标	17
15.3	独立复核	17
15.4	运行监测	17
16	信息安全与个人信息保护	17
16.1	最小必要	17
16.2	访问控制	17
16.3	安全保护	17
16.4	留存与销毁	17
17	接口与可追溯性	18
17.1	接口要求	18
17.2	审计日志	18
17.3	版本管理	18
18	技术验收与持续改进	18
18.1	验收资料	18
18.2	验收判定	18
18.3	定期评审	18
附 录 A		19
附 录 B		20
附 录 C		21
参 考 文 献		22



恒创工程技术研究协会

HETRA

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由恒创工程技术研究协会提出。

本文件由恒创工程技术研究协会归口。

本文件起草单位：广州虹瑛科技有限公司。

本文件主要起草人：赵冰。



引 言

民航运行安全风险识别需要综合飞行数据、运行环境、人员状态和组织管理信息，并将识别结果纳入航空运营人的安全管理体系。本文件面向风险识别系统的研发、部署、运行和验证，建立从数据接入、质量控制、特征构建、异常识别、风险融合、预警输出到效果验证的可追溯技术闭环。

本文件不替代适用的民用航空规章、运行规范、飞行手册、标准操作程序或经批准的安全管理制度，也不直接设定机型超限值、气象运行最低标准和机组值勤限制。相关阈值应以现行规章、批准文件、制造商资料和航空运营人经批准的控制标准为依据。



民航运行安全风险识别技术规范

1 范围

本文件规定了民航运行安全风险识别的数据要求、处理流程、飞行数据回溯、异常识别、气象风险评估、机组疲劳风险预测、操作偏差分析、风险融合、预警输出、效果验证以及信息安全要求。

本文件适用于公共航空运输和通用航空运行安全风险识别系统的设计、开发、部署、运行、维护与技术验收。机场、空中交通服务和航空运行保障单位可参照使用。

本文件输出的识别结果用于安全风险管理和辅助决策，不应替代飞行机组、签派、空中交通管制人员或运行控制人员依法依规作出的运行决策。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。凡是注日期的引用文件，仅该日期对应的版本适用于本文件；凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 24353—2022 风险管理 指南

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

AC-396-09R1 飞行品质监控信息管理办法

AC-121-FS-014R1 CCAR-121 部合格证持有人的疲劳管理要求

3 术语和定义

3.1 运行安全风险

operational safety risk

民航运行活动中危险源导致不利后果的可能性与后果严重度的组合。



3.2 飞行数据回溯

flight data retrospective analysis

基于已完成航段的飞行参数、事件记录和运行环境信息，对运行过程进行重构、比对和趋势分析的活动。

3.3 异常

anomaly

相对于适用规则、批准阈值、历史基线或同类运行分布显著偏离且需要进一步核验的状态、事件或组合模式。

3.4 操作偏差

operational deviation

实际操作或运行轨迹相对于适用程序、计划、指令或经批准基线的偏离。

3.5 风险识别模型

risk identification model

利用规则、统计方法、机器学习方法或其组合，对风险信号进行提取、关联和分类的计算组件。

3.6 可追溯性

traceability

能够从识别结论追溯至数据来源、版本、处理步骤、规则或模型、参数配置和人工处置记录的能力。

3.7 失效安全

fail-safe

当数据、模型、接口或基础设施异常时，使系统进入可控状态并避免输出无依据确定性结论的能力。



4 总体原则

4.1 合法合规

组织应识别并持续跟踪适用的民用航空规章、运行规范、强制性标准、数据安全和个人信息保护要求。系统规则与适用文件不一致时，应以具有更高约束力或经批准的文件为准。

4.2 安全优先

风险识别应服务于危险源识别、风险评估、风险控制和 safety 保证，不应以减少告警数量、提高模型命中率或降低运行成本为由削弱安全控制。

4.3 证据驱动

每项风险结论应关联原始数据、数据质量状态、识别规则或模型版本、阈值来源、置信信息和处置记录。不能形成充分证据链时，应标记为待核验，不应输出为确定性结论。

4.4 人机协同

系统应明确自动识别、人工复核和运行决策的责任边界。涉及高风险或重大运行影响的识别结果，应由具备相应资质或授权的人员复核。

4.5 持续改进

组织应根据运行变化、事件调查、反馈记录、模型漂移和验证结果持续调整数据字典、规则、模型和控制措施。

5 组织与职责

5.1 责任体系

组织应指定风险识别工作的归口部门，并明确安全管理、飞行运行、运行控制、签派、机务、信息技术、数据治理和人员疲劳管理等相关岗位的职责、权限和协同机制。



5.2 专业复核

组织应建立规则和模型的专业复核机制。复核人员应理解适用规章、运行场景、数据限制和模型适用边界，并履行利益冲突回避和保密义务。

5.3 变更授权

规则、模型、风险分级、关键数据源和预警策略的新增、修改、停用和回退应经过评估、测试、批准和留痕。未经授权的配置不应进入生产环境。

6 数据范围与治理

6.1 数据范围

组织应依据识别目标确定数据范围，宜包括飞行记录参数、航班计划与实际运行、航空器和机组排班、机场与航路、气象、放行与签派、空中交通服务、维修状态、安全报告、训练和运行限制等数据。

- a) 飞行数据应关联航班、航段、航空器、机型、时间基准和数据采集设备信息；
- b) 气象数据应关联来源、观测或预报时刻、有效时段、空间位置和产品版本；
- c) 疲劳相关数据应限定为实现风险管理目标所必需的数据，并实施最小化处理；
- d) 人工录入数据应记录录入者、录入时间、来源和复核状态。

6.2 数据分级分类

组织应根据敏感程度、业务影响和法规要求对数据分级分类，并为不同级别数据配置访问、传输、存储、使用、共享、留存和销毁控制。

6.3 数据字典

每一数据项应具有唯一标识，并记录名称、含义、单位、类型、取值域、时间基准、来源系统、更新频率、质量规则、责任人和版本。机型相关参数应区分机型、构型、软件版本和采集映射差异。



6.4 质量状态

数据进入分析前应完成格式、完整性、合理性、一致性、时序性、唯一性和来源校验。必填元数据缺失、时间基准不明、关键参数无法解码或来源不可追溯的数据不应进入确定性风险判定。

表 1 数据质量控制要求

质量维度	控制要求	验证证据
完整性	检查必填字段、航段连续性和关键参数覆盖情况	缺失率报告、拒收或降级记录
准确性	与权威源、机载记录或人工核验样本比对	比对记录、差异分析
一致性	检查跨系统编码、单位、时间和主数据一致性	映射表、对账结果
时效性	记录采集、传输、处理和入库时间	链路时延统计
可追溯性	保留来源、校验、转换和版本信息	数据血缘记录

7 处理流程

7.1 流程组成

风险识别流程应至少包括数据接入、质量校验、标准化、航段与阶段划分、特征构建、单项识别、跨域关联、风险评估、预警输出、人工复核、闭环处置和效果验证。

7.2 阶段划分

飞行阶段划分规则应按机型和运行场景进行验证。系统应记录阶段边界的判断依据，并在边界不确定时保留不确定性标记。

7.3 规则与模型并行

法规、运行手册或批准标准已经明确的判定条件，应优先采用可解释规则。统计或机器学习模型可用于发现复合模式和弱信号，但不应覆盖或降低强制性控制要求。



7.4 异常降级

数据源中断、时间不同步、模型不可用、接口失败或计算资源不足时，系统应告警并执行经批准的降级或回退策略，不应静默补值、隐瞒失败或继续输出无依据的高置信结论。

8 飞行数据回溯

8.1 航段重构

系统应基于统一时间轴重构航段，关联计划、实际运行、航空器构型、机场跑道、航路、气象和运行限制。重构结果应能够回放关键参数、事件和阶段变化。

8.2 基线比对

系统应支持与批准阈值、机型或构型基线、机场或航路基线、同类航段分布和历史趋势进行比对。所用基线应记录适用范围、样本期间、样本量、版本和批准状态。

8.3 事件关联

单一参数超限应结合飞行阶段、持续时间、变化率、相关参数、运行环境和机组处置进行关联分析。系统应避免仅凭瞬时噪声或孤立数据点形成确定性结论。

8.4 趋势分析

系统应支持按机型、航空器、机场、跑道、航路、机组群体、时间段和运行条件进行趋势分析，并能够区分样本构成变化与风险水平变化。

9 异常识别

9.1 识别类型

异常识别应覆盖规则超限、时序异常、关联异常、群体偏离、罕见组合和趋势突变。每种方法应明确输入、输出、适用场景、限制和核验方法。



9.2 阈值管理

阈值应来源于适用规章、批准文件、制造商资料、运行手册、经验证的历史基线或经批准的风险分析。阈值配置应包含来源、版本、适用对象、生效时间、停用时间和批准记录。

9.3 模型要求

采用机器学习模型时，应形成模型说明文件，至少包括训练和验证数据范围、特征、标签、算法版本、性能指标、适用边界、已知偏差、可解释方法、漂移监测和回退条件。

9.4 误报与漏报

组织应分别统计误报、漏报和无法判定情况，并按风险后果确定优化优先级。不得以降低误报为由无评估地提高阈值，也不得以提高召回率为由输出无法有效处置的大量低质量告警。

10 气象风险评估

10.1 数据融合

气象风险评估应关联机场实况、预报、重要气象情报、航路气象、雷达或卫星产品以及机载观测等可用数据，并记录各数据的时空分辨率、有效时段和更新状态。

10.2 风险对象

评估对象宜包括对流天气、雷雨、风切变、颠簸、结冰、低能见度、低云、侧风、顺风、高温、高原和跑道表面状况等影响运行安全的气象与环境因素。

10.3 时空匹配

系统应按照航班计划和实际轨迹进行时空匹配，区分观测、临近预报和趋势预报。超出产品有效范围或空间覆盖的数据不应直接用于确定性判定。

10.4 最低标准边界

涉及起飞、进近、着陆、备降和航路运行最低标准的判断，应引用适用的运行规范、机场和航图资料以及经批准的航空运营人标准。系统不应自行降低或替代这些标准。



11 机组疲劳风险预测

11.1 管理边界

疲劳风险预测应纳入航空运营人的疲劳管理或疲劳风险管理体系，并与排班、值勤、休息、疲劳报告和安全保证过程衔接。预测结果不应作为对个人进行惩罚性评价的唯一依据。

11.2 输入因素

输入因素宜包括飞行时间、飞行值勤期、值勤期、休息期、备份、夜间和跨时区运行、连续值勤、任务复杂度、延误、报告信息以及经合法授权使用的其他因素。

11.3 模型验证

生物数学模型或统计模型应说明科学依据、校准数据、适用人群和限制。组织应结合疲劳报告、调查、调查问卷、审计和安全绩效指标开展验证，不应把单一模型分值等同于个体实际警觉状态。

11.4 处置原则

当预测结果表明疲劳可能影响安全运行时，应按经批准的疲劳管理制度开展评估和风险缓解。系统应保留预测依据、人工判断和措施执行记录。

12 操作偏差分析

12.1 基准建立

操作偏差分析应以适用规章、批准的运行手册、标准操作程序、空中交通管制指令、航班计划和安全通告为基准，并明确各基准的优先级和适用范围。

12.2 偏差分类

偏差宜按程序偏差、轨迹偏差、速度或高度偏差、能量管理偏差、构型偏差、通信与协同偏差和处置时序偏差分类。



12.3 情境解释

系统应结合天气、空域、机场、航空器状态、交通流、管制指令和非正常情况解释偏差。依法依规采取的安全处置不应仅因偏离原计划而被判定为不安全操作。

12.4 公正文化

偏差分析结果的使用应符合安全信息保护和公正文化原则，区分无意差错、系统诱因、可接受的适应性行为、鲁莽行为和故意违规，并由授权人员作出最终判断。

13 风险融合与分级

13.1 风险融合

系统应将飞行数据、气象、疲劳、操作偏差、航空器状态和组织因素按事件链或危险源关联，不对重复信号简单累加。融合逻辑应可解释并可回放。

13.2 可能性与严重度

组织可采用 5 级可能性和 5 级严重度矩阵进行初筛。等级定义、样本口径和风险可接受准则应由组织结合适用法规和运行特点批准。

表 2 风险等级建议映射

风险值 $R=L \times S$	建议等级	处置要求
1~4	低	记录并纳入趋势监测
5~9	中	由责任部门评估并跟踪措施
10~16	高	及时复核，制定并验证缓解措施
17~25	重大	立即升级至授权决策层并按应急或重大风险程序处置

注：本表用于风险管理分级，不替代民航规章、运行规范或航空运营人经批准的专项判定标准。

13.3 不确定性

风险结论应同时给出数据质量、模型置信、适用边界和关键假设。当不确定性可能改变风险等级时，应采用较保守的处置或转人工复核。



13.4 否决条件

存在法规或批准文件明确禁止的情形、关键数据无法核验、模型超出适用边界或系统处于失效状态时，不应仅依据综合评分作出安全可接受结论。

14 预警输出与闭环处置

14.1 预警内容

预警应至少包括唯一编号、风险对象、发生或预测时段、风险等级、触发依据、关键证据、数据质量、置信信息、适用限制、建议复核角色和状态。

14.2 分级通知

预警通知范围和时效应与风险等级、运行阶段和责任权限相匹配。系统应防止无关人员获取敏感信息，并保留发送、接收、确认和升级记录。

14.3 人工复核

复核人员应能够查看证据链、关联数据和规则或模型说明，并记录确认、驳回、调整等级、合并、分派和关闭理由。

14.4 闭环状态

风险事项应按新建、待复核、已确认、处理中、待验证、已关闭或经批准的等效状态管理。关闭前应核验措施实施情况和残余风险。

15 效果验证

15.1 验证计划

上线或重大变更前应制定验证计划，明确目标、场景、样本、基准、指标、接受准则、责任人和异常处置。验证数据应覆盖正常、异常、边界、缺失、噪声、延迟和跨系统不一致场景。



15.2 指标

验证指标宜包括精确率、召回率、误报率、漏报率、提前量、处理时延、可用性、人工复核一致性、处置完成率和风险重复发生率。指标应报告样本量、统计期间和不确定性，不应仅报告总体平均值。

15.3 独立复核

关键风险识别功能应由未直接承担模型开发的人员复核。采用抽样验证时，应说明抽样框、抽样方法、样本量和代表性限制。

15.4 运行监测

生产运行期间应监测数据漂移、概念漂移、性能衰减、告警积压、接口失败和未闭环风险。达到经批准的触发条件时，应重新校准、限制使用、回退或停用。

16 信息安全与个人信息保护

16.1 最小必要

系统应仅处理实现风险识别目标所必需的数据。能够通过去标识化或群体分析实现目的时，不应使用直接身份信息。

16.2 访问控制

应基于岗位职责实施最小权限、身份鉴别、授权审批和定期复核。对批量导出、规则修改、模型发布和高风险事项关闭等高影响操作应实施增强控制。

16.3 安全保护

敏感数据在传输和存储过程中应采用与风险相适应的安全措施，并建立备份恢复、漏洞管理、安全审计和事件响应机制。

16.4 留存与销毁

组织应依据法规、调查、审计和安全管理需要制定留存期限。超过期限且无继续留存依据的数据应安全删除或匿名化，并保留销毁记录。



17 接口与可追溯性

17.1 接口要求

接口应定义数据结构、编码、单位、时间格式、版本、质量标志、重试机制、幂等要求、错误码和安全控制。接口变更应向前兼容或提供经验证的迁移方案。

17.2 审计日志

系统应记录数据接入、转换、规则命中、模型推理、人工复核、配置变更、导出和关闭等关键操作。日志应防篡改并支持按事项重建处理链。

17.3 版本管理

数据字典、规则、模型、阈值、特征、代码、接口和运行环境应分别版本化，并能够确定任一识别结果所使用的完整版本组合。

18 技术验收与持续改进

18.1 验收资料

技术验收资料应包括需求与适用边界、数据清单和字典、架构与接口、规则和模型说明、验证报告、安全评估、用户和运维手册、变更与回退方案、培训记录以及问题闭环记录。

18.2 验收判定

全部强制性要求应具有可核验的符合性证据。关键风险功能存在未关闭的严重缺陷、证据链断裂、未经授权阈值、不可接受的信息安全风险或无法执行回退时，不应通过验收。

18.3 定期评审

组织应定期评审风险清单、数据质量、模型性能、人工复核结果、处置效果和法规变化。发生重大事件、运行范围变化、机型或系统重大变更时，应开展专项评审。



附录 A

(资料性)

风险识别数据字典要素

风险识别数据字典宜至少包含表 A.1 所列要素。

表 A.1 数据字典要素

类别	要素
标识	数据项唯一标识、中文名、英文名、业务定义
结构	数据类型、长度、格式、单位、取值域、空值规则
来源	来源系统、采集设备、责任人、权威程度
时空	时间基准、采样频率、更新频率、位置参考
质量	完整性、准确性、一致性、时效性和校验规则
安全	分级分类、访问权限、脱敏、留存期限
版本	版本号、生效时间、变更原因、批准记录



附录 B

(资料性)

风险事项记录要素

风险事项记录宜覆盖识别、复核、处置和验证全过程。

表 B.1 风险事项记录要素

阶段	记录要素
识别	事项编号、对象、时间、风险源、触发规则或模型、证据、数据质量
评估	可能性、严重度、风险等级、不确定性、适用边界
复核	复核人、复核时间、意见、等级调整及理由
处置	责任部门、措施、期限、执行证据、升级记录
验证	验证方法、结果、残余风险、关闭批准



附录 C

(资料性)

要求与验证方法示例

表 C.1 给出部分要求与验证方法的对应关系，实施单位宜形成覆盖全部适用条款的要求—验证矩阵。

表 C.1 要求—验证矩阵示例

要求	验证方法	判定准则	证据
6.4 数据质量	构造缺失、错序、重复和错误单位数据	系统正确拒收、降级或标记	测试记录、质量报告
9.2 阈值管理	抽查生产阈值	均可追溯至批准来源和版本	阈值台账、批准记录
14.3 人工复核	执行典型事项复核	证据可见、操作留痕、权限正确	复核日志
15.4 运行监测	模拟漂移和接口失败	触发告警及批准的回退策略	演练记录
17.3 版本管理	回放历史识别事项	可重建完整版本组合	版本清单、回放结果



参考文献

- [1] [1] GB/T 1.1—2020 标准化工作导则 第1部分：标准化文件的结构和起草规则
- [2] [2] 大型飞机公共航空运输承运人运行合格审定规则（CCAR-121 部）
- [3] [3] 民用航空安全管理规定（CCAR-398）
- [4] [4] 民用航空安全信息管理规定（CCAR-396-R3）
- [5] [5] 中国民用航空局. 航空运营人安全管理体系建设要求. AC-121-FS-2008-26R1, 2024
- [6] [6] 中国民用航空局. 飞行品质监控信息管理办法. AC-396-09R1, 2024
- [7] [7] 中国民用航空局. CCAR-121 部合格证持有人的疲劳管理要求. AC-121-FS-014R1, 2024
- [8] [8] ICAO. Safety Management Manual. Doc 9859, 4th edition, 2018
- [9] [9] ICAO. Manual for the Oversight of Fatigue Management Approaches. Doc 9966, 2nd edition, revised 2020
- [10] [10] ICAO. Safety Intelligence Manual. Doc 10159, 1st edition, 2025
- [11] [11] ICAO. Manual of Aeronautical Meteorological Practice. Doc 8896
- [12] [12] ISO 31000:2018 Risk management — Guidelines
- [13] [13] FAA. Advisory Circular 120-82, Flight Operational Quality Assurance
- [14] [14] FAA. Advisory Circular 120-92, Safety Management Systems for Aviation Service Providers
- [15] [15] ICAO, IATA and IFALPA. Fatigue Risk Management Systems Implementation Guide for Operators, 2nd edition, 2015