ICS 03.220.50
CCS V 07

T/CCAATB

中 国 民 用 机 场 协 会 团 体 标 准

T/CCAATB 0068—2024

民用运输机场弱电信息系统运行维护要求

Operation and maintenance requirements for weak current information systems in civil transport airports

2024 - 9 - 19 发布　　2024 - 10 - 18 实施

中国民用机场协会　　发 布

目　次

前　言

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

《民用运输机场弱电信息系统运行维护要求》共分8章，分别是范围、规范性引用文件、术语和定义、缩略语、概述、运行维护管理要求、运行维护技术要求、运行维护其他相关要求，着重规定民用运输机场弱电信息系统运行维护管理要求、技术要求和其他相关要求内容等。

本文件由广东机场白云信息科技股份有限公司提出。

本文件由中国民用机场协会归口。

《民用运输机场弱电信息系统运行维护要求》由主编单位负责日常管理。执行过程中如有意见和建议，请函告广东机场白云信息科技股份有限公司（地址：广东省广州市白云区新白云国际机场西南商务区A栋；邮编：510440；电话：020-36066009；电子邮箱：10680142@gdairport.com），以便修订时参考。

本文件主要起草单位：广东机场白云信息科技股份有限公司、中国民航大学、广州白云国际机场股份有限公司、北京首都国际机场股份有限公司、深圳市机场（集团）有限公司。

本文件主要起草人：关华、杨洪宇、王静、邹勇彬、张民、牟松、刘春波、张利、岳亚飞、邓壮志、李永华、笪令、王婷、韩孟龙、吴嘉毅、黄诚智、顾兆军、王钊、林勤康、颜昭昊、霍纬纲、温华山、李颖、张喆、张宇、李建伏、严巍。

本文件参与起草单位：首都机场集团有限公司北京大兴国际机场、云南机场集团有限责任公司、湖北国际物流机场有限公司、广东省机场管理集团韶关丹霞机场有限公司。

本文件参与编写人员：李标、李昉、朱方海、刘鸣秋、王新刚、王洁、董雷、陈慕来。

本文件主要审查人（按姓氏拼音为序排列）：曹伟、陈永刚、杜伟军、邓正保、胡志兵、衡闻琦、李冰、蒋冰、秦倩、吴海燕、王欣、王伟、赵东平。

本文件为首次发布。

民用运输机场弱电信息系统运行维护要求

1 范围

本文件描述了民用运输机场弱电信息系统运行维护体系，规定了弱电信息系统运行维护的管理要求、技术要求和其他相关要求。

本文件适用于超大型、大型和中型民用运输机场（含军民合用运输机场民用部分）安全保卫、旅客服务、航班保障、货运服务等各类弱电信息系统的运行维护活动，也可供小型民用运输机场（含军民合用运输机场民用部分）弱电信息系统运行维护活动参考。

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。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 28827.1 信息技术服务 运行维护第1部分：通用要求

MH/T 5002—2020 运输机场总体规划规范

3 术语和定义

GB/T 28827.1界定的以及下列术语和定义适用于本文件。

3.1

运行维护管理机构 management department of operation and maintenance

弱电信息系统运行维护的责任单位或部门。

3.2

运行维护服务机构 service department of operation and maintenance

弱电信息系统运行维护服务的实施单位、团队或外包服务商。

3.3

运行维护服务 operation and maintenance service

采用信息技术手段及方法，依据需方提出的服务要求，对其弱电信息系统的机房基础设施、物理资源、虚拟资源、平台资源、应用、数据和前端设备，以及满足用户使用弱电信息系统过程中的需求等提供的综合服务。

[GB/T 28827.1-2022，定义3.1，有修改]

3.4

更新 device renovation

系统设计寿命到期或不满足正常运行需求，对系统进行的整体或局部的优化、升级或替换作业。

4 缩略语

下列缩略语适用于本文件。

AP　访问接入点（Access Point）
BGP　边界网关协议（Border Gateway Protocol）
CPU　中央处理器（Central Processing Unit）
DDoS　分布式拒绝服务（Distributed Denial of Service）
HBA　主机总线适配器（Host Bus Adapter）
IOPS　每秒输入输出操作数（Input/Output Operations Per Second）
IP　互联网协议（Internet Protocol）
IDS　入侵检测系统（Intrusion Detection System）
IPS　入侵防御系统（Intrusion Prevention System）
NTP　网络时间协议（Network Time Protocol）
OSD　屏幕菜单式调节方式（On-Screen Display）
OSPF　开放最短路径优先路由协议（Open Shortest Path First）
RAID　独立磁盘冗余阵列（Redundant Arrays of Independent Disks）
SQL　结构化查询语言（Structured Query Language）
STP　生成树协议（Spanning Tree Protocol）
VRRP　虚拟路由冗余协议（Virtual Router Redundancy Protocol）
WAF　WEB应用防火墙（Web Application Firewall）

5　概述

5.1 运行维护目标

机场弱电信息系统运行维护工作的目标是通过实施管理措施和技术手段，对弱电信息系统运行环境、业务应用等提供综合服务，保障弱电信息系统的可靠、稳定和安全运行，确保机场业务用户能够获得高质量、连续性的服务。

5.2 运行维护相关方

机场弱电信息系统运行维护相关方包括：

a） 运行维护管理机构；
b） 运行维护服务机构；
c） 弱电信息系统使用部门。

5.3 运行维护模式

机场弱电信息系统运行维护模式分为自行运维、外包运维和混合运维三种方式：

a） 自行运维是指各单位运行维护管理机构或其下属单位作为运行维护服务机构承担机场弱电信息系统的运行维护工作；
b） 外包运维是指由运行维护管理机构以外的专业信息技术服务单位作为运行维护服务机构承担机场弱电信息系统的运行维护服务工作；
c） 混合运维是指机场弱电信息系统部分资源采用自行运维，部分资源采用外包运维。

5.4 运行维护体系

机场弱电信息系统运行维护体系由运行维护管理要求和运行维护技术要求两部分构成，见图1，其中：

a） 运行维护管理要求包括运行维护服务提供过程中运行维护服务机构要遵循的策划、实施、检查和改进的管理原则，以及运行维护服务机构应具备的能力要素等相关要求；

b） 运行维护技术要求包括机场弱电信息系统运行维护对象以及运行维护过程中开展的运行维护活动。

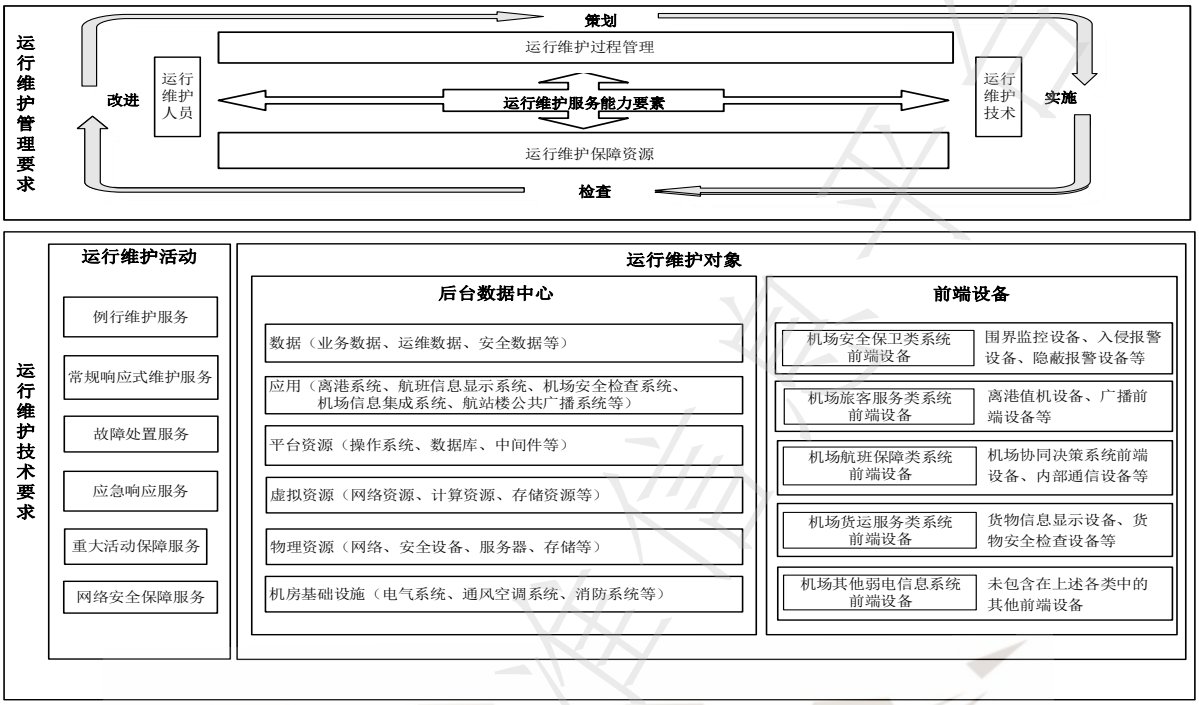

图1 民用运输机场弱电信息系统运行维护体系

6 运行维护管理要求

6.1 总则

运行维护服务过程中应结合机场业务对机场弱电信息系统的网络化、数字化和智能化要求，识别运行维护需求或期望，按照策划、实施、检查、改进的方式对运行维护服务能力进行管理，提供人员、技术、过程、资源等关键能力要素支持，保证运行维护服务交付质量满足服务级别协议要求，对运行维护服务结果、服务交付过程以及相关管理体系进行监督、测量、分析和评审，并实施改进，同时做好工作记录，以实现运行维护服务能力的持续提升。

6.2 人员管理

为了保证人员能力满足运行维护服务要求，应进行人员管理，具体要求为：

a） 应具备专职的运行维护团队或部门，并具备合理的岗位和人员管理机制；

b） 应从人员管理、岗位结构、技能要求、知识要求、经验要求等方面开展人员管理活动；

c） 应对参与运行维护服务的不同角色有明确分工和职责定义；

d） 应根据运行维护对象对应的作业区域和作业性质，确定运行维护人员应具备的资质能力，包括但不限于如操作系统、数据库、网络、网络安全等信息系统维护相关的资质，以及高空作业证、电工作业证、动火上岗证明、控制区相关证件等；

e） 应在运行维护人员上岗前对其进行网络安全背景审查，与其签订网络安全与保密协议，明确安全职责、离岗后的脱密期限等；

f） 应定期对运行维护人员开展包括网络安全、空防安全、作业安全、保密教育等相关培训工作，并定期开展考核，其中，网络安全培训的时长和内容应符合国家和民航行业有关要求；

g） 运行维护人员离岗时，应及时终止其所有访问权限，收回与身份鉴别相关的软硬件设备，并令其承诺调离后的保密义务；

h） 应以发展策略为导向建立机场弱电信息系统运行维护服务能力绩效考核管理机制，以机场弱电信息系统运行维护服务管理目标和年度运行维护服务计划为依据制定关键业绩指标，并将其分解至相关的部门和岗位，应将运行维护服务考核指标和考核制度纳入绩效考核体系，确保考核的整体有效性。

6.3 技术管理

运行维护服务过程中应实施技术管理，具体要求为：

a） 应根据运行维护服务能力策划要求，实施技术管理活动，确保组织具备预防风险、发现问题、解决问题和优化创新的技术能力，为控制运行维护服务的成本和质量，可借助外包服务商的专业技术优势，合理利用资源，降低自身技术保障能力不足的风险；

b） 应根据运行维护服务需求及整体策划方案，开展技术研发活动，保证技术可靠、可用；

c） 应确定技术研发成果在资源、人员和过程中的应用方案，确保技术成果在运行维护服务中得到应用。

6.4 过程管理

运行维护服务过程中应实施过程管理，具体要求为：

a） 应规范运行维护服务活动所遵循的规则和各环节参与人员的职责；

b） 应根据运行维护服务目标或年度计划，制定运行维护服务过程规范，有效提高运行维护效率和服务质量；

c） 应包括服务级别管理、服务报告管理、服务请求管理、事件管理、问题管理、变更管理、配置管理、发布管理、服务可用性和连续性管理、信息安全管理等，可依据服务需求进行过程组合和增加；

d） 应根据服务级别协议制定各项过程要求和关键指标，确保组织具备场景下所需的服务能力并支撑服务价值实现；

e） 应对运行维护过程建立考核管理机制，增加考核评价，以机场弱电信息系统运行维护服务管理目标和年度运行维护服务计划为依据制定关键业绩指标，并将其分解至相关的部门和岗位，应将运行维护服务考核指标和考核制度纳入绩效考核体系，确保考核的整体有效性。

6.5 资源管理

运行维护服务过程中应根据运行维护服务能力策划方案，按需建立和管理运行维护资源，包括运行维护工具、服务台、服务数据、备件库、软件库、服务知识库以及前端设备运行维护过程所需专用工具、施工作业车辆以及专用防护服饰、危险警示牌以及其他的安全措施工具等以支撑不同服务场景的服务需求的实现，并与人员、过程和技术结合，保证资源能力满足价值实现过程中服务提供的需求。

7 运行维护技术要求

7.1 运行维护对象

7.1.1 概述

7.1.1.1 运行维护服务过程中应根据机场业务对机场弱电信息系统的运行维护服务需求和特点，识别运行维护对象。

7.1.1.2 机场弱电信息系统运行维护对象分为前端设备和后台数据中心两大类，其中：

a） 前端设备运行维护对象包括机场安全保卫类系统前端设备、机场旅客服务类系统前端设备、机场航班保障类系统前端设备、机场货运服务类系统前端设备以及机场其他弱电信息系统前端设备；

b） 后台数据中心运行维护对象包括机房基础设施、物理资源、虚拟资源、平台资源、应用和数据。

7.1.2 前端设备

前端设备运行维护对象包括：

a） 机场安全保卫类系统前端设备：主要指用于预防、阻止或延缓针对机场、航空器及导航设备等的非法干扰行为，保护机场区域内人员及财产安全的安全防范系统的前端设备及相关设备，包括但不限于围界报警、音频和视频监控、安全检查、门禁、机场控制区通行证件管理等系统的前端设备；

b） 机场旅客服务类系统前端设备：主要指对机场旅客出行相关业务进行服务的一类前端设备，包括但不限于离港、航班信息显示、航站楼公共广播、行李处理、旅客自助服务类等系统的前端设备；

c） 机场航班保障类系统前端设备：主要指对机场航班运行相关业务进行保障服务的一类前端设备，包括但不限于机场协同决策、内部通信等系统的前端设备；

d） 机场货运服务类系统前端设备：主要指对机场货运相关业务进行服务的一类前端设备，包括但不限于货物信息平台、货物安全检查等系统的前端设备；

e） 机场其他弱电信息系统前端设备：主要指未包含在上述各类中的为机场运行相关业务进行服务的机场弱电信息系统前端设备。

7.1.3 后台数据中心

按照运行维护的资源分层视角，后台数据中心运行维护对象包括：

a） 机房基础设施：

1）电气系统：包括供配电系统、通风空调系统、电源系统、照明系统、电缆及母线槽、防雷与接地等；

2）智能化系统：包括环境和设备监控系统、安全防范系统、综合布缆系统等。

b） 物理资源：

1）网络与通信资源：包括通信线路、路由器、交换机、负载均衡、语音以及通信传输设备等；

2）安全设备：包括防火墙、IDS、IPS、WAF、密码设备、安全审计设备、日志设备等；

3）服务器：包括 PC 服务器、小型机和大型机等；

4）存储设备：包括磁盘阵列、磁带库、光盘库等。

c） 虚拟资源：

1）虚拟网络资源：包括虚拟网络设备、虚拟链路、虚拟机网络等；

2）虚拟计算资源：包括虚拟机、虚拟机宿主机等；

3）虚拟存储资源：包括虚拟存储卷、存储控制器、存储链路等。

d） 平台资源：

包括支撑应用系统运行的环境，如操作系统、数据库、中间件等。

e） 应用：

1）实现业务功能的各种应用软件，如离港系统、航班信息显示系统、机场安全检查系统、机场信息集成系统、行李处理系统、航站楼公共广播系统、机场围界报警系统、视频监控系统、门禁系统、机场安检信息管理系统、时钟系统等弱电信息系统对应的应用软件；

2）后台数据中心应用于自身管理的工具软件，如监控软件、流程管理软件、安全分析软件等。

f） 数据：

1）业务数据：系统采集、分析并存储的各种信息载体等；
2）运行维护数据：数据中心运行维护过程中，产生的各类运行维护信息、运行状态日志、故障处理文档等信息；
3）网络安全数据：在业务运行和运行维护过程中与网络安全相关的数据。

7.2 运行维护活动

7.2.1 概述

7.2.1.1 运行维护服务过程中应根据不同机场弱电信息系统的运行维护服务级别要求、服务特点和服务需求，构建并开展各类运行维护活动。
7.2.1.2 机场弱电信息系统运行维护活动应包括例行维护服务、常规响应式维护服务、故障处置服务、应急响应服务、重大活动保障服务、网络安全保障服务等活动。
7.2.1.3 应在满足业务连续性的前提下进行，特别应考虑机场地理位置所带来的天气环境等自然因素对运行维护活动的影响。
7.2.1.4 运行维护活动过程中应满足空防安全要求，对前端设备运行维护人员，需定期组织运行维护证件使用培训，制定证件使用管理办法，定期对证件使用进行考核。
7.2.1.5 运行维护活动过程中应满足作业安全要求，对于需要开展的高空作业、动火作业、户外作业等，需制定手指口述规范，并进行宣贯，加强现场监管、信息传递，规范工作流程，完善制度标准；运行维护服务人员必须根据施工安全规定进行规范施工，必须佩带室外专用工具、专用防护服饰、危险警示牌以及其他的安全措施工具。
7.2.1.6 运行维护服务过程中应根据不同的运行维护对象，围绕其运行维护活动制定相应的运行维护工作内容。具体运行维护工作内容见附录A。
7.2.1.7 运行维护活动过程中宜逐步沉淀形成机场弱电信息系统运维知识库，并在运行维护服务过程中引入知识库作为操作参考和决策指导，提升维护操作的规范性、准确度和有效性。

7.2.2 例行维护服务

例行维护服务主要包括日常监控巡检服务、健康检查、系统更新等内容，具体服务要求如下：
a） 应根据不同系统的运行维护服务级别要求，以及前端设备和后台数据中心的特点和维护需求，明确例行维护服务对象、内容和要求，制定例行维护计划和例行维护手册；
b） 日常监控巡检服务中，对于与航班流、旅客流、行李流、货物流等业务执行强相关的重要弱电信息系统，如机场信息集成系统、离港系统、机场安全检查系统、机场安检信息管理系统、行李处理系统等，以及涉及机场安防的弱电信息系统，如机场围界报警系统、视频监控系统、门禁系统等，应加强监控密度，实施重点保障，对异常指标应做出告警提示，并做好监控记录；其他弱电信息系统可定期监控，后台数据中心可采用实时自动监控和定期人工监控的方式进行，前端设备则需定期进行人工巡检，做好监控巡检记录；
c） 周期性维护服务中，其运行维护对象应包括机场弱电信息系统所涉及的前端设备和后台数据中心，以及换季时可下线设备和备份介质等，不同维护对象可按照月度维护、季度维护、半年度维护或年度维护等维护频次开展周期性维护服务；
d） 周期性维护服务计划的制定应考虑下一年度重大活动保障的开展，如重大政治活动、重要社会活动、重要节假日等，应在重大活动保障之前完成该周期内的所有维护工作；应考虑错峰维护，尽量选择航后或航班较少时段开展，重点设备应与相关运行部门确认后再实施维护作业；应考虑南北方不同气候条件下的换季维护，需要协调的资源要素等；应确保每年对全机场全设备至少覆盖一次；
e） 周期性维护服务手册的制定应考虑安全要求以及当地气候特点等，并有针对性地列明维护操作步骤；

f） 应在运行维护管理机构的组织下，定期对运行维护对象的运行状况进行分析和评估，并根据实际情况，通过参数配置或参数调整等方式针对性地开展优化改善工作，主要包括为保持运行维护对象在新环境中可持续运行而实施的适应性优化改进、为增强系统安全性、可用性和可靠性而进行的增强性改进、为检测和纠正运行维护对象运行过程中潜在的问题或缺陷而进行的预防性改进等，并做好相关记录；

g） 应针对例行维护服务中发现的问题制定相应的处理流程，并在维护服务过程中做好维护工作记录，对于例行维护服务中发现的问题应根据事先制定的工作流程进行通知、通告及处置。

7.2.3 常规响应式维护服务

运行维护服务过程中应开展常规响应式维护服务，具体要求如下：

a） 应根据机场弱电信息系统业务运行需要和用户请求进行前端设备和后台数据中心的配置变更、系统升级改造配合、信息更新、系统资源运行状态数据统计分析、运行评估等响应式维护服务；

b） 应根据不同的常规响应式维护服务请求，制定申请审批、通知、通告等工作流程，并在常规响应式维护工作开展前按照该工作流程执行；

c） 常规响应式维护工作实施前应制定具体实施方案，以保证系统的安全稳定可靠运行及可恢复性；

d） 常规响应式维护工作实施前应考虑南北方机场因地理位置差异而存在的雷雨、大风、大雪、大雾、沙尘暴、结冰等各类不同极端天气情况，做好人员和资源调度管理；

e） 常规响应式维护工作实施后应做好响应维护工作记录。

7.2.4 故障处置服务

运行维护服务过程中应开展故障处置服务，具体要求如下：

a） 应提供故障处置服务，在故障发生时应根据服务级别要求，在规定的时间内消除故障影响，并最终清除故障；

b） 应制定故障受理流程，在获取故障所属系统、发生的位置和影响范围等信息后，可首先预判故障属于前端设备故障还是后台数据中心故障，是否需要进入航站楼隔离区，是否在塔台和邻近航站楼的围界区域，是否需要高空作业、动火作业等危险作业，以此调度相关资质人员进行快速精准的故障处置；

c） 应根据业务特点，按照故障的严重性和受影响系统的重要性，对故障进行级别划分，可分为特别重大、重大、较大和一般四个等级。对于重大及以上故障应提前制定应急预案，其他级别故障应预设故障处理流程，并于故障发生时，按预先制定的应急预案或处理流程进行处置，同时还应建立故障升级机制，以及信息系统用户部门与运行维护服务机构之间的联动机制，必要时应启动现场业务应急处理，如对于航站楼区域故障，若故障不能立即修复，应在故障现场做出设备维修提示，并派专人现场处理；

d） 故障处置宜遵循“先抢通、后修复，先核心、后边缘”的原则，优先考虑空防安全，其次确保重要业务的恢复，特殊情况酌情处理；

e） 故障处置完成后应及时记录故障处理方法、做好故障总结，并定期进行统计分析，对发生频次较多的故障现象应进行重点分析，采取相应措施，降低故障发生率；

f） 应建立信息报送机制，根据故障级别向机场运行维护相关方及时报送故障情况和处置过程信息。

7.2.5 应急响应服务

运行维护服务过程中应开展应急响应服务，具体要求如下：

a） 应提供应急响应服务，建立与业务联动的应急响应机制，确保按预先制定的应急处置流程处置突发事件；

b） 应制定应急响应流程，依据机场弱电信息系统应急预案相关规定，应急响应流程宜包括应急预案启动、事态控制、应急恢复、应急结束等环节；
c） 应提前编制整体应急预案，并经由运行维护服务机构、运行维护管理机构、信息系统用户部门共同评审通过后正式发布；
d） 应针对弱电信息系统不同的服务级别明确相应的应急响应级别，针对重要系统制定专项应急预案，建立多手段、多层次的保障机制，应急预案宜包括编制目的、适用范围、系统说明、故障等级定义、应急预案启动条件、应急处置流程、应急组织等；
e） 应定期进行应急预案的培训、桌面演练与实战演练；
f） 应急响应结束后应及时进行总结，同步优化、调整和完善应急预案。

7.2.6 重大活动保障服务

运行维护服务过程中应开展重大活动保障服务，具体要求如下：
a） 应制定重大活动保障方案，明确重大活动保障范围及保障内容，在重大政治活动、重要社会活动、重要节假日等关键时期开展重点保障活动，对核心系统提供重点保障服务，从驻场人员、备品备件、备用措施、前端设备加固等方面予以重点保障，提升系统运行的可靠性；
b） 应制定重大活动保障工作流程，开展资产摸底工作和网络安全自查工作，对应急预案进行再梳理再完善，以应对重大活动保障期间的突发事件；
c） 重大活动保障服务期间，对与航班流、旅客流、行李流、货物流等业务执行强相关的重要弱电信息系统，以及涉及空防安全的弱电信息系统，应加强巡检，增派驻场人员，加强安全检查，并停止不必要的系统更新、施工作业等活动；
d） 重大活动保障服务期间，应强化实时监测，重点加强核心系统、互联网出入口、门户网站、公共区域显示大屏和电脑终端等保障对象的网络安全管理和防护工作，加强运行维护保障团队的常态化值守，落实每日零报告制度；
e） 重大活动保障服务结束后，应及时开展工作总结，做好工作记录，对重大活动保障期间发现的问题应根据事先制定的工作流程进行通知、通告及处置，对发生的关键问题应进行重点分析，总结经验，并反馈于运行维护服务相关部门。

7.2.7 网络安全保障服务

运行维护服务过程中应开展网络安全保障服务，具体要求如下：
a） 应满足法律法规、行业监管、标准规范的要求；
b） 应确保网络和信息系统及相关数据的保密性、可用性和完整性等；
c） 应包括但不限于安全管理制度、安全管理岗位、安全状态监控、安全事件处置、安全威胁监测、安全检查和优化等；
d） 应定期进行系统脆弱性评估，分析系统存在的安全隐患，并提出改进建议；
e） 应实时监测系统安全威胁，对于发现的安全威胁可根据预设工作流程进行通知、通告及处置；
f） 应及时对网络安全事件进行处置，处置的原则是先阻断后处理。
g） 应及时开展网络安全工作总结，做好工作记录，对发生的关键问题应进行重点分析，总结经验，并反馈于运行维护服务相关部门。

8 运行维护其他相关要求

8.1 设备更新要求

运行维护服务过程中应定期组织开展对机场弱电信息系统设备的评估与论证，对满足更新和改造要求的设备进行更新和改造，以保障业务运行安全和提高运行效率。设备更新要求见附录B。

8.2 维护服务成本度量要求

运行维护服务过程中应考虑维护服务成本度量，具体要求如下：

a） 应根据机场弱电信息系统业务规模与运行维护服务场景和需求，对其运行维护服务成本进行合理度量，做好运行维护服务成本管理。

b） 机场弱电信息系统运行维护服务成本计算应从基础环境运维、硬件运维、软件运维、安全运维、运维管理以及其他运维服务（如数据迁移、应用迁移、云迁移、机房或设备搬迁）等多方面分别进行成本度量，并应考虑不同运行维护对象的服务级别、生命周期及其运行年限、部署方式、所在位置和距离等因素所带来的运维工作量的不同而导致的运维成本的变化。

c） 机场弱电信息系统运行维护模式若采用外包运维或混合运维的方式开展，则运行维护成本度量方式也可以由运行维护相关方通过协商确定，采用如基于运行维护资产建设总额比例计算等方式确定。

8.3 外包运维服务要求

对于外包运维或混合运维中的外包运维部分应开展外包运维服务管理，具体要求如下：

a） 应对外包运维服务需求进行分析，明确外包运维服务范围、目的、要求，以及驻场运维或远程运维等外包运维服务形式；

b） 应对外包服务商服务过程进行管理，明确外包服务商的服务范围、服务内容、服务级别、服务时间窗口等，建立服务报告制度和沟通机制；

c） 应建立对外包服务人员的安全管理机制，对外包服务人员进行安全背景调查、征信调查等，同时签订保密协议，确保相关信息不被泄露；

d） 对于依MH/T 5002-2020中4.1.3划分的不同规模的机场，超大型机场和大型机场应优先选择具有信息技术服务运行维护服务能力成熟度二级及以上等级证书的运行维护外包服务商；中型机场宜优先选择具有信息技术服务运行维护服务能力成熟度三级及以上等级证书的运行维护外包服务商；小型机场宜优先选择具有信息技术服务运行维护标准符合性证书的运行维护外包服务商；

e） 应优先选择具有质量管理体系认证证书、信息安全管理体系认证证书、信息技术服务管理体系认证证书，并具备安全生产、安全施工维修等资格证明，同时具有信息化运维平台的运行维护外包服务商。

附 录 A

（资料性附录）

机场弱电信息系统运行维护工作内容

A.1 概述

运输机场弱电信息系统运行维护机构应根据前端设备和后台数据中心两大类运行维护对象的应用模式和服务模式，以及运行维护活动类别，制定其运行维护工作内容。

A.2 前端设备运行维护工作内容

按照机场弱电信息系统前端设备业务需求和分散式运维的特点，前端设备运行维护工作又包括机场安全保卫类系统前端设备、机场旅客服务类系统前端设备、机场航班保障类系统前端设备、机场货运服务类系统前端设备以及机场其他弱电信息系统前端设备的运行维护工作。

A.2.1 机场安全保卫类系统前端设备

机场安全保卫类系统前端设备维护服务应包括下列内容：

a） 定期对机场安全保卫类系统前端设备进行例行维护服务，应确保：

1）设备外观完整。

2）设备运行正常，功能完整。

3）7×24 小时运行。

4）联动时效符合建设交付状态。

5）前端设备数据回传至后台系统时其时效应满足建设交付状态。

6）在外场使用的前端设备应确保安装牢固，避免产生机场外来物。

7）每 12 个月针对视频监控系统、门禁系统、机场围界报警系统等开展定期检测工作。

此外，对于视频监控设备应确保摄像机角度正常，支架未倾斜倒塌，监控摄像头掉线时及时处理，视频监控实况及录像正常，清晰度符合建设交付时的状态；对于门禁设备应确保读卡器工作正常、无报警提示，门禁刷卡器可正常刷卡开门，关门后门可正常闭合，生物识别设备及门禁读卡器可正常输入及传输时效满足建设交付时的状态。

b） 根据需要对机场安全保卫类系统前端设备进行常规响应式维护服务，其内容至少包括：

1）设备的入网、离网和变更。

2）设备软件安装、配置和问题解答。

3）外联设备的安装和配置等。

c） 根据服务级别要求开展故障处置服务工作，按时修复机场安全保卫类系统前端设备故障。

d） 根据服务级别要求按时对机场安全保卫类系统前端设备进行应急响应服务。

e） 定期对机场安全保卫类系统前端设备进行网络安全保障服务，其内容至少包括：

1）安全管理软件、防病毒软件的有效性。

2）使用人信息、设备管理标识等信息的一致性。

3）空防安全、作业安全相关管理制度的符合性。

A.2.2 机场旅客服务类系统前端设备

对机场旅客服务类系统前端设备的维护服务应包括下列内容：

a） 定期对机场旅客服务类系统前端设备进行例行维护服务，应确保：

1）设备外观整洁，无明显损坏。

2）设备运行正常，功能完整。

3）设备传输信息准确。

4）设备维护时应采取围蔽措施。

此外，对于航班信息显示系统前端设备应确保信息更新及时，显示清晰，航时一直在线；对于航站楼公共广播系统前端设备应确保广播音量适中，声音清晰柔和；对于离港前端设备和旅客自助服务类设备应确保各类耗材充足；对于旅客 Wi-Fi 应重点考虑人员密集处的覆盖面、容量和通信质量三者之间的关系以调整无线 AP 的分布；对于人脸识别设备应考虑光线等环境因素对设备使用的影响。

b） 根据需要对机场旅客服务类系统前端设备进行常规响应式维护服务，其内容至少包括：

1）设备的入网、离网和变更。

2）设备软件安装、配置和问题解答。

3）外联设备的安装和配置等。

c） 根据服务级别要求开展故障处置服务工作，按时修复机场旅客服务类系统前端设备故障。

d） 根据服务级别要求按时对机场旅客服务类系统前端设备进行应急响应服务。

e） 定期对机场旅客服务类系统设备前端设备进行网络安全保障服务，其内容至少包括：

1）安全管理软件、防病毒软件的有效性。

2）使用人信息、设备管理标识等信息的一致性。

3）空防安全、作业安全相关管理制度的符合性。

A.2.3 机场航班保障类系统前端设备

机场航班保障类系统前端设备维护服务应包括下列内容：

a） 定期对机场航班保障类系统前端设备进行例行维护服务，应确保：

1）设备外观正常。

2）设备运行正常，功能完整。

3）设备航时或工作期间处于在线状态。

此外，对于在外场使用的前端设备应确保安装牢固，避免产生机场外来物；对于内通系统应确保不存在号码冲突，录音功能正常。

b） 根据需要对机场航班保障类系统前端设备进行常规响应式维护服务，其内容至少包括：

1）设备的入网、离网和变更。

2）设备软件安装、配置和问题解答。

3）外联设备的安装和配置等。

c） 根据服务级别要求开展故障处置服务工作，按时修复机场航班保障类系统前端设备故障。

d） 根据服务级别要求按时对机场航班保障类系统前端设备进行应急响应服务。

e） 定期对机场航班保障类系统前端设备进行网络安全保障服务，其内容至少包括：

1）安全管理软件、防病毒软件的有效性。

2）使用人信息、设备管理标识等信息的一致性。

3）空防安全、作业安全相关管理制度的符合性检查。

A.2.4 机场货运服务类系统前端设备

机场货运服务类系统前端设备维护服务应包括下列内容：

a） 定期对机场货运服务类系统前端设备进行例行维护服务，应确保：

1）设备运行正常。

2）设备功能完整。

b） 根据需要对机场货运服务类系统前端设备进行常规响应式维护服务，其内容至少包括：

1）设备的入网、离网和变更。

2）设备软件安装、配置和问题解答。

3）外联设备的安装和配置等。

c） 根据服务级别要求开展故障处置服务工作，按时修复机场货运服务类系统前端设备故障。

d） 根据服务级别要求按时对机场货运服务类系统前端设备进行应急响应服务。

e） 定期对机场货运服务类系统前端设备进行网络安全保障服务，其内容至少包括：

1）安全管理软件、防病毒软件的有效性。

2）使用人信息、设备管理标识等信息的一致性。

3）空防安全、作业安全相关管理制度的符合性检查。

A.3 后台数据中心运行维护工作内容

按照后台数据中心运行维护的资源分层视角，其运行维护工作又包括机房基础设施、物理资源、虚拟资源、平台资源、应用以及数据等六个层次的工作内容。

A.3.1 机房基础设施

机房基础设施维护服务应包括下列内容：

a） 定期对机房基础设施进行例行维护，包括供配电系统、通风空调系统、电源系统、照明系统、电缆及母线槽、防雷与接地等电气系统设施，环境和设备监控系统、安全防范系统、综合布缆系统等智能化系统，对以上机房基础设施的动态指标、静态指标、运行状况和发展趋势等进行记录、分析和告警，确保其有效性。

b） 实时监测机房超温、超湿、漏水、火情、非法入侵等异常情况。

c） 定期进行综合布线检查。

d） 根据服务级别要求按时修复故障设施。

e） 制定应急预案，应急预案可纳入整体应急预案中，并应定期进行预案演练。

f） 做好机房出入管理，人员进出应审批并登记，门禁记录宜每月检查并留存。

g） 定期进行总结评估，对机房基础设施运行状况及运行维护工作情况进行分析，提出改进意见。

h） 做好机房基础设施技术资料的收集、整理，定期提交机房基础设施清单，定期绘制、更新机房机柜布置图；做好运行维护工作过程文档的收集、存档。

i） 每年对机房防雷接地装置开展检测。

A.3.2 物理资源

物理资源主要包括计算机网络、网络安全设施、服务器以及存储等。

A.3.2.1 计算机网络

计算机网络维护服务应包括下列内容：

a） 实时或定期监控计算机网络运行状况，其内容至少包括：

1）网络设备的健康状况、整体运行状态、各项硬件资源开销状况。

2）链路健康状况，如端到端时延变化、链路端口工作稳定性、链路负载情况、部署路由策略情况等。

3）端到端选路变化、路由条目变化。

4）网络设备 CPU、内存占用率情况。
5）端口流量速率，丢包错包以及广播风暴等情况。
6）管理权限用户的行为审计。
7）设备软件配置变动审计。
8）设备日志审计。
9）安全事件审计。

b） 对网络资源进行预防性检查时，应确定性能检查内容和脆弱性检查内容。
性能检查的内容应至少包括：
1）设备机身、板卡或模块的工作情况。
2）CPU 使用峰值情况。
3）内存使用峰值情况。
4）FLASH（非易失内存）存储空间。
5）板卡、风扇、温度等运行情况。
6）主要端口的利用率。
7）链路的健康状态，包括 IP 包传输时延、IP 包丢失率、IP 包误差率、无效 IP 包（包括攻击性 IP 包、欺骗性 IP 包、垃圾 IP 包等）。
8）主要端口的状态，例如 STP、VRRP 等协议。
9）路由协议状态，例如 OSPF / BGP 等协议。
10）检查其他的关键指标项，例如各类关键表项、会话连接数等。
脆弱性检查的内容应至少包括：
1）系统版本是否需要升级或修复。
2）设备链路的冗余度要求。
3）安全事件周期性整理分析。
4）设备生命周期评估。
5）备件可用性周期性检查。
6）业务带宽是否满足业务高峰需求。
7）网络边界防护控制评估。

c） 定期对计算机网络设备进行常规作业，根据系统运行要求，确定操作内容和周期，其内容应至少包括：
1）网络设备健康检查，主要设备应定期进行包括性能分析、安全审计的全面健康检查。
2）设备登录口令定期修改。
3）网络设备固件升级。
4）网络设备配置文件定期备份，设备配置变化及时备份。
5）设备操作系统软件备份及存档。
6）系统微码升级。
7）设备软件配置备份及存档。
8）监控系统日志备份及存档。
9）监控系统日志数据分析与报告生成。
10）网络配置变更文件的审核。
11）网络配置变更的操作。
12）网络配置变更的记录。
13）安全设备特征库升级。
14）安全审计类分析报告。

15）周期性关键设备主备切换 / 应急演练。

d） 根据需要对计算机网络进行常规响应式维护服务，根据系统运行要求，确定事件驱动响应和服务请求响应的具体服务内容，其中，事件驱动响应为针对物理资源的故障引起的业务中断或运行效率无法满足正常运行要求而进行的响应服务，服务请求响应为根据应用系统运行需要或需方的请求而进行的响应服务。

事件驱动响应应包括但不限于：

1）故障定位。

2）停止、启动进程。

3）中断、连通网络连接。

4）关闭、启动端口。

5）网络备件更换。

6）更改、恢复配置。

服务请求响应应包括但不限于：

1）增加、降低网络接入的数量或速度。

2）更改网络设备配置。

3）启动、关闭端口或服务。

4）更换、更新或升级设备硬件或软件。

5）网络规划调整。

6）网络资源分配。

e） 应对网络资源进行优化改善，根据系统运行要求，确定适应性改进、增强性改进和预防性改进的具体服务内容。其中，适应性改进为根据系统及其软硬件环境的运行要求，对网络资源进行必要的调整；增强性改进为根据系统及其软硬件环境的运行状况，对网络资源进行调整、扩容或升级；预防性改进为根据系统及其软硬件环境的运行趋势，对网络资源的脆弱点实施改进作业。

适应性改进应包括但不限于：

1）路由策略调整。

2）设备或链路负载调整。

3）网络安全加固。

4）网络敏感数据加密。

5）监控对象覆盖范围调整。

6）局部交换优化。

7）局部冗余优化。

增强性改进应包括但不限于：

1）硬件容量变化，如网络设备硬件、软件升级、带宽升级等。

2）整体网络架构变动。

3）安全设备特征库升级。

4）网络架构容量变化，如网络子系统的增减等。

5）系统功能变化，如新增功能区、新增安全系统、新增审计系统等。

6）路由协议应用及部署调整。

7）整体安全策略收紧。

8）交换优化。

9）冗余优化。

预防性改进应包括但不限于：

1）配置参数优化，例如关闭不必要的服务、打开缺省的增强功能、加快三层网络路由收敛速度、加快二层网络生成树收敛速度等。

2）网络安全优化，例如：添加防火墙、IPS、WAF、抗 DDoS 等安全设备。

3）提高软件配置命令可读性。

f） 应对网络进行应急响应服务，制定应急预案，并可纳入整体应急预案中，应定期进行预案演练。

g） 定期进行总结评估，对计算机网络运行状况及运行维护工作情况进行分析，提出改进意见。

h） 做好计算机网络技术资料的收集、整理，宜定期提交计算机网络设备及线路清单，定期绘制、更新详细网络拓扑图，定期提交网络资源分配情况表，做好运行维护工作过程文档的收集、存档。

A.3.2.2 网络安全设施

网络安全设施维护服务应包括下列内容：

a） 实时或定期监控安全设施运行状况，至少包括下列内容：

1）安全设施运行状态。

2）安全设施系统日志分析。

3）安全设施健康检查，主要设备应定期进行全面健康检查。

4）安全设施登录口令定期修改。

5）安全设施配置文件备份。

6）安全设施固件及系统软件升级。

7）安全策略审核。

b） 根据需要对网络安全设施进行常规响应式维护服务，其内容至少包括下列内容：

1）安全策略调整等配置变更。

2）配合完成信息系统安全等级保护测评相关工作。

3）安全预警信息发布。

c） 根据服务级别要求按时修复安全设施故障，按时处置恶意代码爆发、黑客入侵等安全事件。

d） 制定应急恢复预案，并纳入整体应急预案中，宜定期进行演练。

e） 定期进行总结评估，对安全设施运行状况、信息系统安全状况及运行维护工作情况进行分 析，提出改进意见。

f） 定期使用网络安全设施进行信息系统安全威胁监控分析。

g） 定期使用网络安全设施进行信息系统安全脆弱性扫描和分析，发现安全漏洞、提出加固建议。

h） 做好网络安全设施技术资料的收集、整理，宜定期绘制安全设施拓扑图，定期整理安全策略，定期提交信息系统安全风险评估报告，做好运行维护工作过程文档的收集、存档。

A.3.2.3 服务器

服务器维护服务应包括下列内容：

a） 实时或定期监控服务器运行状况，其内容至少包括：

1）服务器整体运行情况。

2）服务器电源工作情况。

3）服务器 CPU 工作情况。

4）服务器内存工作情况。

5）服务器硬盘工作情况。

6）服务器接口工作情况。

b） 对服务器进行预防性检查时，应确定性能检查内容和脆弱性检查内容。

性能检查的内容应至少包括：

1）服务器的资源分配情况和策略。

2）CPU 使用峰值情况。

3）内存使用峰值情况。

4）文件系统空间使用情况。

5）I/O 读写情况。

6）网络流量情况等。

7）与存储的链路运行状态。

8）硬件日志情况。

脆弱性检查的内容应至少包括：

1）服务器资源使用是否超过预定阀值。

2）服务器关键部件是否满足运行冗余度要求。

3）服务器关键部件的微码版本是否需要升级。

4）服务器硬盘是否 RAID 保护。

5）系统微码、操作系统版本一致性检查。

6）硬件型号、系统版本兼容性检查。

7）接口链路状态是否有异常情况。

c） 定期对服务器进行常规作业，根据系统运行要求，确定操作内容和周期，其内容应至少包括：

1）系统微码升级。

2）配置文件备份。

3）过期日志和文件系统空间清理。

4）服务器硬盘 RAID 配置检查（如有 RAID 控制器）。

5）更换控制器电池（如有 RAID 控制器）。

6）服务器健康检查，主要设备应定期进行包括性能分析、安全审计的全面健康检查。

7）服务器登录口令定期修改。

8）服务器固件及系统软件升级。

9）备份策略审核。

10）系统重启。

d） 根据需要对服务器进行常规响应式维护服务，根据系统运行要求，确定事件驱动响应和服务请求响应的具体服务内容，其中，事件驱动响应为针对服务器的故障引起的业务中断或运行效率无法满足正常运行要求而进行的响应服务；服务请求响应为根据应用系统运行需要或需方的请求而进行的响应服务。

事件驱动响应应包括但不限于：

1）服务器重启。

2）更换故障部件，包括主板、电源、CPU、内存、硬盘等。

3）服务器关键部件微码升级。

4）服务器配置变更。

5）服务器备份策略调整。

6）服务器硬盘 RAID 配置修复。

服务请求响应应包括但不限于：

1）服务器设备搬迁。

2）服务器设备停机演练。

3）服务器设备清洁维护等。

4）服务器硬件扩容。

5）集群环境搭建和切换演练。

e） 应对服务器资源进行优化改善，根据系统运行要求，确定适应性改进、增强性改进和预防性改进的具体服务内容。其中，适应性改进为根据系统及其软硬件环境的运行要求，对服务器资源进行必要的调整；增强性改进为根据系统及其软硬件环境的运行状况，对服务器资源进行调整、扩容或升级；预防性改进为根据系统及其软硬件环境的运行趋势，对服务器资源的脆弱点实施改进作业。

适应性改进应包括但不限于：

1）服务器硬盘 RAID 配置调整。

2）服务器网络、光纤链路冗余调整。

3）服务器电源供电接入冗余调整。

增强性改进应包括但不限于：

1）为本服务器从存储系统上分配更大空间。

2）服务器 CPU 个数增加。

3）服务器内存容量增加。

4）服务器磁盘空间扩容。

5）服务器网卡和 HBA 接口卡增加等。

预防性改进应包括但不限于：

1）检查服务器硬盘 RAID 配置，及时修复或更换故障硬盘。

2）增加服务器网卡、光纤卡以及链路冗余情况。

3）增加服务器电源供电模块冗余。

f） 制定应急预案，应急预案可纳入整体应急预案中，应定期进行预案演练。

g） 定期进行总结评估，对服务器运行状况及运行维护工作情况进行分析，提出改进意见。

h） 做好服务器技术资料的收集、整理，宜定期提交服务器设备清单，定期绘制服务器连接图，做好运行维护工作过程文档的收集、存档。

A.3.2.4 存储

存储维护服务应包括下列内容：

a） 定期对各类存储系统进行巡检，查看并记录设备运行状况及告警信息。

b） 实时或定期监控存储系统运行状况，其内容至少包括：

1）存储系统 CPU、内存占用率情况。

2）存储设备控制器工作情况。

3）存储设备电源工作情况。

4）存储设备数据存储介质工作情况。

5）存储设备接口工作情况。

6）存储设备数据存储介质空间使用情况。

7）存储设备读写速率情况。

8）存储设备读写命中率情况。

9）存储系统日志检查分析。

c） 对存储进行预防性检查时，应确定性能检查内容和脆弱性检查内容。

性能检查的内容应至少包括：

1）I/O 读写速率情况。

2）读、写缓存分配比例情况。

3）数据读、写命中率情况。
4）存储硬盘空间使用情况。
5）存储系统日志情况。
6）磁带读取和写入速率情况。
7）磁带池使用情况。

脆弱性检查的内容应至少包括：

1）存储关键硬件部件是否满足运行冗余度要求。
2）当前微码版本是否需要升级。
3）存储配置备份机制是否完善。
4）存储管理软件是否需要升级或打补丁。
5）存储空间使用比例是否达到预定告警阀值。
6）存储设备的离线记录检查。
7）存储介质的坏块记录检查。
8）系统微码版本一致性检查。

d） 定期对存储进行常规作业，根据系统运行要求，确定操作内容和周期，其内容应至少包括：

1）系统微码升级。
2）更换控制器电池。
3）介质读、写正常性测试。
4）配置文件备份。
5）过期运行日志清理。
6）存储系统健康检查，主要设备应定期进行包括容量分析、性能分析的全面健康检查。
7）存储系统登录口令定期修改。
8）存储系统固件及系统软件升级。
9）链路端口访问测试。

e） 根据需要对存储进行常规响应式维护服务，根据系统运行要求，确定事件驱动响应和服务请求响应的具体服务内容，其中，事件驱动响应为针对存储的故障引起的业务中断或运行效率无法满足正常运行要求而进行的响应服务。服务请求响应为根据应用系统运行需要或需方的请求而进行的响应服务。

事件驱动响应应包括但不限于：

1）存储重启。
2）配置文件恢复。
3）更换故障部件，包括电源、硬盘等。
4）微码升级。
5）存储管理软件补丁安装。
6）数据修复。

服务请求响应应包括但不限于：

1）存储空间划分、调整等配置变更。
2）存储系统数据迁移、同步、复制等。
3）存储设备搬迁。
4）存储设备停机演练。
5）存储设备清洁维护。
6）存储硬盘空间扩容。
7）新增主机分配存储空间。
8）主机端多路径软件的安装配置。

f） 应对存储资源进行优化改善，根据系统运行要求，确定适应性改进、增强性改进和预防性改进的具体服务内容。其中，适应性改进为根据系统及其软硬件环境的运行要求，对存储资源进行必要的调整；增强性改进为根据系统及其软硬件环境的运行状况，对存储资源进行调整、扩容或升级；预防性改进为根据系统及其软硬件环境的运行趋势，对存储资源的脆弱点实施改进作业。

适应性改进应包括但不限于：

1）存储设备读写高速缓存（Cache）比例调整。

2）存储设备 RAID 保护级别调整。

3）存储设备新增硬盘，包括新增磁盘扩展柜。

4）存储设备逻辑盘的容量调整。

5）存储设备分配主机的调整。

6）磁带池的配置调整。

7）光纤交换机存储网络区域（ZONE）规划调整。

增强性改进应包括但不限于：

1）存储设备控制器、硬盘等部件的微码升级。

2）存储设备新增硬盘扩容，包括新增磁盘扩展柜。

3）存储设备高速缓存（Cache）容量增加。

4）磁带池的容量调整，包括新增磁带。

5）磁带驱动器的新增。

6）存储设备光纤模块的升级。

7）光纤交换机的光纤模块升级。

8）光纤交换机的端口激活扩容，包括新增光模块。

9）存储设备管理软件的版本升级。

预防性改进应包括但不限于：

1）收集磁盘空间的使用情况，及时清理垃圾数据或增加存储设备容量。

2）查看存储控制器电池的使用情况，及时更换新的电池。

3）检查存储设备的电源是否老化，及时更换新的电源。

4）查看磁带驱动器的使用情况，及时清洗磁头。

5）查看存储设备的读写性能，适时调整存储控制器的高速缓存（Cache）容量。

g） 制定应急预案，应急预案可纳入整体应急预案中，定期进行预案演练。

h） 定期进行总结评估，对存储系统运行状况及运行维护工作情况进行分析，提出改进意见。

i） 做好存储系统技术资料的收集、整理，宜定期提交存储资源分配使用清单，定期绘制存储系统连接图，做好运行维护工作过程文档的收集、存档。

A.3.3 虚拟资源

虚拟资源主要包括虚拟网络资源、虚拟计算资源及虚拟存储资源等。在后台数据中心运行维护过程中，对虚拟资源进行监控时，应根据具体对象确定监控内容和指标。根据数据中心的虚拟资源配置情况，各类虚拟资源的监控内容应至少包括下表中的所述项。

A.3.3.1 虚拟网络资源

虚拟网络资源维护服务应包括下列内容：

a） 实时或定期监控虚拟网络资源运行状况，其内容至少包括：

1）虚拟网络资源分配状况。

2）虚拟网络资源的健康状态。
3）虚拟网络资源的链路状况，如端到端时延变化、链路端口工作稳定性、链路负载等。
4）虚拟网络资源配置变动。
5）虚拟网络资源操作日志。
6）虚拟网络资源安全事件。
7）虚拟网络控制器性能的监控。

b） 根据服务级别要求按时修复发生的虚拟网络资源故障。
c） 制定应急预案，应急预案可纳入整体应急预案中，应定期进行预案演练。
d） 定期进行总结评估，对虚拟网络资源运行状况及运行维护工作情况进行分析，提出改进意见。
e） 做好虚拟网络资源技术资料的收集、整理，宜定期提交虚拟网络资源分配使用清单，做好运行维护工作过程文档的收集、存档。

A.3.3.2 虚拟计算资源

虚拟计算资源维护服务应包括下列内容：

a） 实时或定期监控虚拟计算资源运行状况，其内容至少包括：
1）虚拟计算资源分配状况。
2）虚拟计算资源群集容量状况、性能状况。
3）虚拟机宿主机及虚拟机 CPU 负荷。
4）虚拟机宿主机及虚拟机磁盘 I/O 负荷。
5）虚拟机宿主机及虚拟机内存负荷。
6）虚拟机宿主机及虚拟机网络 I/O 负荷。
7）虚拟机宿主机及虚拟机网络链路状态。
8）虚拟机宿主机及虚拟机管理代理进程。
9）虚拟机宿主机及虚拟机计算资源分配。
10）虚拟机宿主机及虚拟机系统日志异常。
11）引发性能问题的虚拟机快照管理（如捕获、克隆）。

b） 根据服务级别要求按时修复发生的虚拟计算资源故障。
c） 制定应急预案，应急预案可纳入整体应急预案中，应定期进行预案演练。
d） 定期进行总结评估，对虚拟计算资源运行状况及运行维护工作情况进行分析，提出改进意见。
e） 做好虚拟计算资源技术资料的收集、整理，宜定期提交虚拟计算资源分配使用清单，做好运行维护工作过程文档的收集、存档。

A.3.3.3 虚拟存储资源

虚拟存储资源维护服务应包括下列内容：

a） 实时或定期监控虚拟存储资源运行状况，其内容至少包括：
1）虚拟机宿主机使用存储的相关属性状态监控（如多路径状态监控）。
2）自动化事件监控（发生自动迁移、虚拟机重启等自动化事件）。
3）虚拟存储资源分配策略与空间使用状况。
4）瘦供给模式下容量监控。
5）服务控制器 CPU 负载情况。
6）服务控制器内存消耗情况。
7）服务控制器整体数据吞吐带宽、IOPS、响应时间和请求队列时间。
8）服务控制器后端数据吞吐带宽、IOPS、响应时间和请求队列时间。
9）服务控制器高速缓存（Cache）利用情况。

10）虚拟存储卷访问吞吐率、IOPS、响应时间和请求队列时间。
11）仲裁控制点（磁盘、光纤链路、服务器等）健康性。
12）服务控制器前后端 I/O 链路。
13）服务控制器后端分布式物理存储健康性。
14）服务控制器各服务网络端口监听情况。
15）服务控制器服务进程的运行状态。
16）服务控制器日志。

b） 根据服务级别要求按时修复发生的虚拟存储资源故障。
c） 制定应急预案，应急预案可纳入整体应急预案中，应定期进行预案演练。
d） 定期进行总结评估，对虚拟存储资源运行状况及运行维护工作情况进行分析，提出改进意见。
e） 做好虚拟存储资源技术资料的收集、整理，宜定期提交虚拟存储资源分配使用清单，做好运行维护工作过程文档的收集、存档。

A.3.4 平台资源

A.3.4.1 操作系统

操作系统维护服务应包括下列内容：

a） 实时或定期监控操作系统运行状况，其内容至少包括:
1）操作系统 CPU 使用情况。
2）操作系统内存使用情况。
3）操作系统磁盘使用情况。
4）操作系统网络接口状态、流量、逻辑端口连接数。
5）操作系统光纤接口状态和流量。
6）操作系统重要文件系统空间使用情况。
7）操作系统日志情况。

b） 对平台资源进行预防性检查时，应根据具体的运行维护对象，确定操作系统性能检查内容和脆弱性检查内容。
性能检查内容包括下列内容：
1）操作系统 CPU 使用峰值情况。
2）操作系统内存使用峰值情况。
3）操作系统硬盘使用情况。
4）操作系统重要文件系统空间使用情况。
5）磁盘 I/O 读写情况。
6）网络 I/O 读写情况等。
脆弱性检查内容包括下列内容：
1）操作系统是否安装相关风险补丁。
2）是否需要升级系统微码。
3）是否关闭不必要的服务进程或监听端口。
4）关键机密系统数据安全防护设置是否满足要求。
5）系统使用资源是否超过预定阀值。
6）操作系统版本一致性检查。

c） 定期对平台资源进行常规作业，根据系统运行要求确定操作内容和周期。根据操作系统资源配置情况，其常规作业的内容应至少包括:
1）操作系统版本升级和补丁安装。

2）操作系统磁盘读、写正常性测试。

3）操作系统输入、输出设备读写测试（光驱、内置磁带机）。

4）操作系统配置文件备份。

5）操作系统备份。

6）操作系统登录口令定期修改。

7）操作系统过期运行日志清理。

8）网络通信正常性测试。

9）操作系统临时文件清理。

10）操作系统端口访问测试。

11）周期性关键设备主备切换（主备机阶段轮换承载业务运行）/应急演练。

d） 对操作系统资源进行响应支持时，应根据系统运行要求，确定事件驱动响应和服务请求响应的具体服务内容。

事件驱动响应应包括：

1）操作系统崩溃。

2）操作系统 CPU、内存等资源耗尽。

3）操作系统服务进程无效。

4）操作系统文件系统空间不够。

5）操作系统接口无法通讯。

6）操作系统无法识别外置存储空间。

服务请求响应应包括：

1）操作系统版本升级。

2）操作系统死机修复。

3）操作系统文件系统损坏修复。

4）操作系统文件系统空间扩容。

5）操作系统 IP 地址修改。

6）操作系统参数调整。

7）操作系统日志清理。

e） 对操作系统资源进行优化改善时，应根据系统运行要求，确定适应性改进、增强性改进和预防性改进的具体服务内容。

操作系统适应性改进应包括：

1）操作系统交换区容量调整。

2）操作系统内核参数调整。

3）操作系统文件系统使用空间调整划分。

操作系统增强性改进应包括：

1）操作系统版本升级。

2）操作系统内存扩容。

3）操作系统磁盘空间扩容。

4）操作系统的网卡、光纤卡数量增加。

5）操作系统参数调优。

操作系统预防性改进应包括：

1）操作系统的垃圾数据删除，数据空间释放。

2）操作系统文件系统扩容。

3）操作系统的网卡、光纤卡冗余增加。

4）操作系统用户权限合理分配。

5）操作系统进程服务端口调整。

f） 定期进行总结评估，对操作系统资源运行状况及运行维护工作情况进行分析，提出改进意见。

g） 做好操作系统资源技术资料的收集、整理，做好运行维护工作过程文档的收集、存档。

A.3.4.2 数据库

数据库维护服务应包括下列内容：

a） 实时或定期监控数据库运行状况，其内容至少包括:

1）数据库运行状态。

2）数据库主要进程运行情况。

3）数据库连接是否正常。

4）数据库表空间使用情况。

5）数据库日志是否有异常。

6）数据库会话数。

7）数据库日常备份是否正常等。

b） 定期对平台资源进行预防性检查，根据系统运行要求，确定数据库性能检查内容和脆弱性检查内容。

性能检查内容包括下列内容：

1）数据库的顶级（TOP）SQL 情况（如果数据库支持）。

2）数据库 CPU 使用情况。

3）数据库内存使用情况。

4）数据库表空间使用情况。

5）数据库锁情况。

6）数据库会话数和操作系统进程数情况。

7）数据库缓冲区（BUFFER）等命中率情况。

8）数据库等待事件情况（如果数据库支持）。

脆弱性检查内容包括下列内容：

1）数据库是否安装相关风险补丁。

2）表空间的使用是否达到了预定阀值。

3）数据库关键文件是否做了镜像。

4）数据库备份策略是否合理。

5）数据库是否存在异常用户（如果数据库支持）。

6）数据库版本一致性检查。

7）操作系统配置是否符合数据库运行的要求。

c） 定期对平台资源进行常规作业，根据系统运行要求确定操作内容和周期。根据数据库资源配置情况，其常规作业的内容应至少包括:

1）监听连接正常性测试。

2）数据库正常登录测试。

3）SQL 执行正常性测试。

4）表空间正常访问测试。

5）表读写正常性测试。

6）客户端连接测试。

7）数据库备份。

8）数据库登录口令定期修改。

9）过期归档日志清除。

d） 对数据库资源进行响应支持时，应根据系统运行要求，确定事件驱动响应和服务请求响应的具体服务内容。

事件驱动响应应包括：

1）数据库宕机、锁死。

2）数据文件坏块修复。

3）数据库重启。

4）数据库监听端口冲突。

5）数据库备份恢复。

6）数据库解锁。

服务请求响应应包括：

1）数据库版本升级。

2）数据库灾难恢复。

3）数据清理和维护。

e） 对数据库资源进行优化改善时，应根据系统运行要求，确定适应性改进、增强性改进和预防性改进的具体服务内容。

数据库适应性改进应包括：

1）数据库索引调整。

2）数据库执行 SQL 计划调整。

3）数据表参数调整。

4）数据库对象的调整。

5）主机操作系统内核参数调整。

6）数据库参数调整。

7）临时表空间、用户表空间调整。

8）数据库物理部署的调整（迁移至新服务器或者数据库存储阵列调整）。

9）调整数据库备份策略。

数据库增强性改进应包括：

1）数据库版本升级、打补丁。

2）因主机 CPU 个数、内存容量增加而调整数据库相应的参数。

3）因主机存储的增加而调整数据库表空间容量。

4）数据库安全备份架构构建以提高可用性。

5）数据库调优等。

数据库预防性改进应包括：

1）增加数据库表空间、数据文件空间使用范围。

2）对数据库存在的无效对象处理。

3）数据库用户的权限合理分配或收回。

f） 根据服务级别要求按时修复发生的数据库系统故障。

g） 定期进行总结评估，对数据库系统运行状况及运行维护工作情况进行分析，提出改进意见。

h） 做好数据库系统技术资料的收集、整理，宜定期提交数据库资源分配使用清单，做好运行维护工作过程文档的收集、存档。

A.3.4.3 中间件及其他基础软件

中间件及其他基础软件维护服务应包括下列内容：

a） 实时或定期监控中间件及其他基础软件运行状况，其内容至少包括：

1）中间件及其他基础软件运行状态。
2）分析中间件及其他基础软件日志。
3）主要进程运行状态。
4）应用服务运行情况。
5）中间件通信网络连接情况。
6）中间件日志是否有报错信息。

b） 定期对平台资源进行预防性检查，根据系统运行要求，确定中间件性能检查内容和脆弱性检查内容。

性能检查内容包括下列内容：
1）中间件服务器业务 CPU 使用峰值情况。
2）中间件服务器业务内存使用峰值情况。
3）中间件服务器业务会话连接数情况。

脆弱性检查内容包括下列内容：
1）中间件是否满足运行冗余度要求。
2）中间件是否安装相关风险补丁。
3）中间件的数据库连接口令配置文件是否存在明文。
4）相关重要运行程序是否有保留备份。
5）操作系统配置是否符合中间件运行的要求。
6）系统使用资源是否超过预定阀值等。
7）中间件版本一致性检查。

c） 定期对平台资源进行常规作业，根据系统运行要求确定操作内容和周期。根据中间件配置情况，其常规作业的内容应至少包括:
1）备份配置文件。
2）中间件登录口令定期修改。
3）备份重要运行日志。
4）清除过期日志。
5）交易连接正常性测试。

d） 对中间件进行响应支持时，应根据系统运行要求，确定事件驱动响应和服务请求响应的具体服务内容。

事件驱动响应应包括：
1）服务进程假死。
2）应用服务掉线或重启。
3）配合业务应用进行配置变更。
4）配置文件恢复。
5）守护服务调整。

服务请求响应应包括：
1）中间件新增应用服务。
2）中间件参数调整。
3）中间件软件版本升级。
4）配合业务应用进行中间件性能监控和优化等。

e） 对中间件进行优化改善时，应根据系统运行要求，确定适应性改进、增强性改进和预防性改进的具体服务内容。

适应性改进应包括：

1）中间件参数配置优化。
2）数据库连接参数调整。
3）连接池参数调整。
4）相关操作系统参数调整。
增强性改进应包括：
5）中间件版本升级、打补丁。
6）由于主机 CPU 个数、内存容量增加调整中间件相应的参数。
预防性改进应包括：
1）删除临时文件，释放数据空间。
2）监控主要参数以及时调优。
3）应用备份策略调整。
4）定期备份。

f） 根据服务级别要求按时修复发生的中间件故障。

g） 制定应急预案，应急预案可纳入整体应急预案中，应定期进行预案演练。

h） 定期进行总结评估，对中间件运行状况及运行维护工作情况进行分析，提出改进意见。

i） 做好中间件技术资料的收集、整理，做好运行维护工作过程文档的收集、存档。

A.3.5 应用

在后台数据中心运行维护过程中，对应用及相关资源进行监控时，应根据具体的运行维护对象，确定监控内容和指标。

要保障数据中心应用的正常运行，需要平台资源的配置满足应用要求，同时需对应用系统本身的资源和业务进行监控。

业务应用维护服务应包括下列内容：

a） 实时或定期监控业务应用运行状况，其内容至少包括：
1）应用的请求和反馈响应时间。
2）资源消耗情况。
3）进程、线程状态。
4）服务或端口响应情况。
5）会话内容情况。
6）日志和告警信息。
7）数据库连接情况。
8）存储连接情况。
9）作业执行情况。
10）消息队列、共享内存。

b） 应定期对应用进行预防性检查，其内容应至少包括：
1）应用的请求和反馈响应情况。
2）关键进程及资源消耗检查、分析。
3）主机操作系统的漏洞扫描、补丁检查。数据库中间件等系统软件的补丁检查。
4）系统病毒定期查杀。
5）应用软件的口令安全情况。
6）应用软件的日志审计、分析。
7）批处理作业的日志审计、分析。
8）应用系统支撑环境的备份和恢复检查。

c） 应定期对应用进行常规作业，根据具体的运行维护对象，确定操作内容和周期。根据应用配置情况，各类应用常规作业的内容应至少包括：

1）健康检查，关键系统应定期进行全面健康检查，包括安全审计。

2）业务应用数据的校核、清理。

3）业务应用性能分析、优化。

4）业务应用管理员登录口令定期修改。

5）补丁升级。

6）版本升级。

7）日志清理。

8）启动或停止服务或进程。

9）增加或删除用户账号，并做好清晰记录。

10）更新系统或用户口令。

11）建立或终止会话连接。

12）作业提交。

13）软件备份。

14）应用参数配置修订。

d） 应对应用进行响应支持，根据不同的运行维护对象和系统运行要求，确定事件驱动响应和服务请求响应的具体服务内容。

事件驱动响应为针对应用故障而进行的响应服务，包括但不限于：

1）应用级启停。

2）系统级启停。

服务请求响应为根据应用系统运行需要或需方的请求，进行及时响应和处理，包括但不限于：

按服务请求指示进行用户增加。

1）业务应用权限变更、业务流程调整等配置变更。

2）业务应用数据的添加、修改、删除及导入、导出。

3）业务应用系统补丁升级。

4）口令修改。

5）参数调整。

e） 应定期进行优化改善，根据系统运行要求，确定具体服务内容，包括但不限于：

1）应用消息队列、共享内存优化。

2）应用服务能力优化，例如：应用进程数、应用线程数的优化。

3）应用日志级别及日志空间的调整。

4）应用版本及配置的升级、打补丁。

5）日志代码优化升级、日志监控分析代码优化升级。

f） 根据用户需求进行软件功能性完善等开发工作。

g） 制定应急预案，应急预案可纳入整体应急预案中，应定期进行预案演练。

h） 定期进行总结评估，对业务应用运行状况及运行维护工作情况进行分析，提出改进意见。

i） 做好业务应用技术资料的收集、整理，做好运行维护工作过程文档的收集、存档。

从具体机场弱电信息系统业务支持角度考虑，其运行维护工作内容还应确保：

a） 机场信息集成系统

1）可以正常流转航班动态信息。

2）可以正常进行登机口分配、机位分配、值机柜台分配、行李转盘分配等操作。

b） 离港系统

1）可以正常处理航班动态信息。
2）可以正常处理旅客值机、登机、控制和配载信息。
3）可以正常处理行李信息。
4）可以正常接收周边系统发来的消息。

c） 航班信息显示系统
1）航显屏可以正常显示航班信息。
2）航班信息可以正常上下屏。
3）可以进行值机柜台图片发布操作。

d） 航站楼公共广播系统
1）自动广播可以正常触发播放各类广播语音。
2）广播语音播放内容一致。
3）可以正常播放人工广播。

e） 机场安全检查系统
1）可以在验证台客户端界面通过扫描旅客登机牌或读取证件正常查验旅客信息。
2）可以在随身行李开包台客户端界面通过标记异常物品登记或放行旅客行李。
3）可以在交运客户端界面通过输入航班号和旅客信息，发布拦截，实时传输至验证台工作站。
4）可以对旅客信息、行李图片、视频等进行反查。
5）数据保存时限不少于 90 天。

f） 机场围界报警系统
1）可以正常接收前端设备触发的振动光缆报警，可以触发视频联动。
2）可以正常接收前端设备触发的跨线入侵报警，可以触发视频联动。
3）报警信号在控制中心的显示时延满足机场安防要求。
4）客户端可以正常调取实时视频及录像。
5）视频图像数据和相关信息保存时限不少于 90 天。

g） 视频监控系统
1）实时视频可以正常播放。
2）录像可以正常检索、下载及播放。
3）球机正常可控。
4）摄像机图像有设置时间、编号、位置信息的 OSD 显示信息。
5）音频和视频图像信息资料的保存时限不少于 90 天。

h） 门禁系统
1）可以正常接收前端设备的刷卡及报警事件。
2）门禁事件与视频的联动正常。
3）可以判断通行证件真伪性、合法性和授权通行。
4）可以按照系统划分的权限进行控制。
5）门禁事件在控制中心显示时延满足机场安防要求。
6）控制器与服务器断联后仍能记录刷卡数据，并能在连接恢复后自动上传数据。

i） 时钟系统
1）母钟可以正常接收来自时标接收单元的信号。
2）母钟与子钟可以正常进行时间同步。
3）可以提供 NTP、串行通信等接口中的一种或多种为需授时的设备或系统授时。

j） 行李处理系统
1）可以正常接收航班动态信息。
2）可以正常处理行李各类报文信息。

3）可以正常接收周边系统发来的消息。

A.3.6 数据

数据资源维护服务主要针对通用基础数据及元数据，业务应用数据的维护服务纳入业务应用系统维护工作中，数据资源维护服务应包括下列内容：

a） 实时或定期对数据资源进行监控，应根据具体的运行维护对象，确定监控内容和指标。其监控内容应至少包括：
   1）数据变化速率。
   2）数据存储。
   3）数据对象使用频度。
   4）数据有效性。
   5）数据安全。
   6）数据产生、存储、备份、分发、应用过程。

b） 应定期对数据进行预防性检查，其内容应至少包括：
   1）数据完整性、一致性。
   2）数据的冗余。
   3）数据存储空间。
   4）数据安全。

c） 应定期对数据进行常规作业，根据具体的运行维护对象，确定操作内容和周期，各类数据常规作业的内容应至少包括：
   1）对数据产生、存储、备份、分发、销毁等过程进行的操作。
   2）对数据资源的处理：包括校核、编辑、整理等。
   3）对数据安全等内容按事先规定的程序进行的例行性作业。
   4）数据提取。
   5）数据验证。
   6）数据清洗。
   7）数据配置管理。
   8）数据资源的发布。
   9）数据资源的入库、存档。
   10）定期进行数据清理工作。

d） 应根据不同的业务数据特性和应用范围，对数据进行梳理、优化，并提出改善建议，对数据的优化改善往往会涉及对应用的变更。数据的优化改善服务包括但不限于：
   1）数据存储方案。
   2）数据重构方案。

e） 制定数据应急预案，应急预案可纳入整体应急预案中，应定期进行预案演练。

f） 定期进行总结评估，对数据运行状况及其维护工作情况进行分析，提出改进意见。

g） 做好数据资料的收集、整理。

h） 做好运行维护工作过程文档的收集、存档。

附 录 B

（资料性附录）

机场弱电信息系统设备更新要求

B.1 概述

机场弱电信息系统设备更新的总目标应为保障系统运行安全、提高业务运行效率和服务质量，具体目标应为保证各系统设备的安全功能和使用功能不因时间推移而下降，各项技术指标、技术参数始终保持在容许的范围内。

设备的更新应按最新的国家和行业相关标准执行，不得降低现有设备的质量和技术水平。更新后的设备，应处于良好状态，并应符合下列规定：

a） 各项性能指标及技术参数应满足更新设计的要求并不应低于更新前的水平。

b） 设备应稳定可靠地运行，可靠性指标如平均无故障时间、完好率、服务可靠度等不应低于更新前的指标。

c） 各种设备的安全保护装置可靠性不应低于设计水平和更新前的水平。

d） 各种机场安全保卫类系统前端设备，如探测感应设备、报警处理器、围界声音警示设备等，以及机房安全防护设备，如火灾自动报警、水消防、气体灭火等，在更新后应进行测试和演习，并需通过相关部门验收。

e） 设备的运行和操作应尽可能地采用正常运行方式和安全操作方式，充分发挥设备的系统功能，最大限度地满足运行要求。

f） 设备的能耗水平、环保性能,应符合现行国家、行业和各地地方标准的规定。

g） 设备应符合国家、行业和各地地方对于网络信息安全的相关要求。

运行维护管理机构应对设计寿命即将到期的设备，在其寿命周期结束前一年对该设备运行质量进行预评估，并及时安排设备更新，以确保安全功能和使用功能的实现。

设备若需在规定的使用年限前报废，应进行技术鉴定，确认不能继续使用，经运行维护管理机构批准后执行。

B.2 更新条件

设备更新可分为整体更新、子系统更新和局部设备更新。

设备在正常使用和维护条件下，其使用年限和报废条件应依据国家标准、行业标准等进行确定，标准规范中没有规定使用年限和报废条件的，应以采购时供应商提供的使用年限和报废条件或采购合同的约定为准。

对于整体更新的设备，其整体使用年限按照新购买设备的使用年限确定；对于子系统或局部设备更新的设备，应考虑其子系统或局部设备是否可以单独再利用，如可以，则该子系统或局部设备的使用寿命可以单独按照其自身使用年限进行计算，如不可以，则其使用寿命跟随其设备整体的剩余寿命进行计算。

设备在常态下符合下列基本条件之一时应进行更新：

a） 经过检修维护仍然无法恢复原设计的 使用功能或者对业务运行造成严重影响时；

b） 在达到物理寿命时；

c） 到达约定的最低使用年限，经分析评估与论证不宜继续使用时。

设备未达到使用年限但符合下列情况之一时，应由运行维护服务机构对设备进行评估与论证，并应向运行维护管理机构提出提前更新的申请：

a） 由于故障率高而严重影响正常运营时；

b） 在安全方面存在重大风险，经过维修后仍不能消除时；

c） 原设计的功能和性能不能满足当前的运行要求；

d） 同类型设备在短时间内出现批量损坏或性能降低，不能满足原设计的功能和性能要求时；

e） 由于关联设备更新或其承载的运行软件升级更新导致设备使用功能无法满足要求时；

f） 备品备件严重短缺致使维修质量难以得到保证时；

g） 由于维修成本高于设备的剩余价值时；

h） 原设计的功能和性能不能满足国家、行业、地方、企业等相关标准和规定等要求时；

i） 属于国家、行业、地方、企业标准规定淘汰的设备。

设备未达到使用年限，但经由运行维护管理机构进行评估与论证之后，可以通过对其更新显著提高系统性能、运行效率或寿命时，可考虑更新。

参 考 文 献

[1] GB/T 28827.4-2019 信息技术服务 运行维护 第4部分：数据中心服务要求
[2] T/CESA 1299-2023《信息技术服务 运行维护服务能力成熟度模型》
[3] SL 715-2015 水利信息系统运行维护规范