ICS
CCS 点击此处添加 CCS 号

MH

中 华 人 民 共 和 国 民 用 航 空 行 业 标 准

MH/T XXXX—XXXX

民用航空生产运行工业控制系统网络安全防护技术要求

Technical requirements for cybersecurity protection of civil aviation productive operation industrial control systems

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国民用航空局　　发 布

目　　次

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。

本文件由中国民用航空局人事科教司提出。

本文件由中国民航科学技术研究院归口。

本文件起草单位：中国航空油料集团有限公司、中国民用航空局第二研究所、中国民航信息网络股份有限公司、北京博维航空设施管理有限公司、中国民航大学、上海虹桥国际机场有限责任公司、广州白云国际机场股份有限公司、四川省机场集团有限公司成都天府国际机场分公司、云南机场集团有限责任公司、新疆机场（集团）有限责任公司、民航成都物流技术有限公司、之江实验室、杭州安恒信息技术股份有限公司、中孚安全技术有限公司、中电长城网际系统应用有限公司、傲拓科技股份有限公司、杭州中电安科现代科技有限公司、亚信科技（成都）有限公司、麒麟软件有限公司、北京六方云科技有限公司、深信服科技股份有限公司。

本文件主要起草人：周文、吴宏刚、李绪国、张俊、李磊、陈昭、任伟、吴啟彪、顾兆军、周景贤、贺胜中、杨洪宇、杨建伟、李昉、梁钰涓、杨洪欣、杨汶佼、张海敏、罗圣美、任江、姚文广、张俊峰、李晗、张大朋、李江力、李长京、刘翱、张雯、林嵩松、安成飞、周启鹏、赵强、张博、郭占先、楚鹏、张衍顺、赵学全。

民用航空生产运行工业控制系统网络安全防护技术要求

1 范围

本文件规定了民用航空生产运行工业控制系统现场设备、控制设备、工业主机、网络设备、防护设备等设备级安全技术要求，以及分区分域与隔离防护、数据与通信安全、安全监控与应急处置、系统运维安全、软件供应链安全等系统级安全技术要求。

本文件适用于民用航空生产运行工业控制系统网络安全规划设计、建设和运营维护过程，也可作为行业管理部门开展监督检查工作的依据。

注：本文件中提及的技术要求除特别说明外，适用于网络安全等级保护第一级、第二级和第三级系统。

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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2022 信息安全技术 术语

GB/T 37933—2019 信息安全技术 工业控制系统专用防火墙技术要求

3 术语和定义

GB/T 22239—2019、GB/T 25069—2022、GB/T 37933—2019界定的以及下列术语和定义适用于本文件。

3.1

飞行区 airfield area

机场内由建筑物和室外隔离设施所围合的区域，包含跑道、滑行道、机坪等设施和场地。

[来源：MH/T 5002—2020，2.1.7]

3.2

航站区 passenger terminal area

机场内航站楼及其配套的站坪、交通、服务等设施所在的区域。

[来源：MH/T 5002—2020,2.1.8]

3.3

工作区 comprehensive supporting area

机场内飞行区、航站区、货运区、机务维修区以外的区域，包含机场管理机构、驻场单位的生产保障等设施和场地。

[来源：MH/T 5002—2020,2.1.11]

3.4

现场设备 field equipment

民航运行过程中用于感知与操作运行过程,并具有计算和信息处理能力的传感设备与执行设备单元。

3.5

控制设备 control equipment

民航运行过程中用于控制执行器以及采集传感器数据的装置。

注：包括可编程逻辑控制器（PLC）、直接数字控制器（DDC）以及远程终端单元（RTU）等进行运行过程控制的单元设备。

3.6

工业主机 industrial host

民航运行过程中控制各业务环节涉及组态、工作流程和工艺管理、状态监控、运行数据采集以及重要信息存储等工作的设备。

注：包括工程师站、操作员站、服务器等。

3.7

双机热备　dual-machine hot standby

通过网络连接主机和从机，正常情况下主机处于工作状态，从机处于监视状态，一旦主机异常，从机自动代替主机。

3.8

行李处理系统　baggage handling system

使用条码识别技术和智能控制技术对旅客托运的行李进行集中传送、分拣与处理的自动化系统。

[来源：MH/T 5103—2004，3.9]

3.9

楼宇自动化系统　building automation system

对航站楼内所控机电设备的状态进行集中监视，分散控制、测量的管理系统的总称。

[来源：MH/T 5009—2016，2.2.1]

3.10

油库供油自动化系统　automation system of oil supply in oil depot

实现油品收发、储存、灌油等过程自动控制，以及对相关设备的运行状态进行监测和报警的系统。

3.11

长输管道自动化系统　automation system of long oil pipeline

实现对炼厂、码头、中转库至机场油库之间输送民用航空燃料的管道进行自动控制，对各设备的运行情况和工艺参数进行监控，并能对关键设备进行远程控制的系统。

4　缩略语

下列缩略语适用于本文件。

APT：高级持续性威胁（Advanced Persistent Threat）
CPU：中央处理器（Central Processing Unit）
DMZ：非军事区（Demilitarized Zone）
DoS：拒绝服务（Denial of Service）
IP：互联网协议（Internet Protocol）
OLE：对象连接与嵌入（Object Linking and Embedding）
OPC：用于过程控制的对象连接与嵌入（OLE for Process Control）
RPO：恢复点目标（Recovery Point Objective）
RTO：恢复时间目标（Recovery Time Objective）
SSH：安全外壳（Secure Shell）
SFTP：安全文件传输协议（SSH File Transfer Protocol）

5　安全防护范围

民用航空生产运行工业控制系统一般包括飞行区的助航灯光系统、航站区的行李处理系统、楼宇自动化系统，以及工作区的油库供油（长输管道）自动化系统。典型示例见附录A。

按照GB/T 22239—2019附录G，本文件中民用航空生产运行工业控制系统安全防护范围涉及过程监控层、现场控制层和现场设备层，包括以下内容：

a）　设备级安全：现场设备、控制设备、工业主机、网络设备、防护设备等软硬件资产安全；
b）　系统级安全：分区分域与隔离防护、数据与通信安全、安全监控与应急处置、系统运维安全、软件供应链安全等内容。

6　设备级安全技术要求

6.1　现场设备安全

6.1.1　现场设备应具有受控接口，仅允许经授权的通信或控制信号接入。

6.1.2 网络安全等级保护第三级系统的现场设备宜采用嵌入式安全模块，具备身份鉴别等功能。

6.2 控制设备安全

6.2.1 本体安全

6.2.1.1 网络安全等级保护第三级系统的本体安全应满足以下要求：

a) 设置控制设备 CPU 访问级别，合理分配对实时数据的读写权限；
b) 配置控制设备的程序密码保护和机密组态数据保护机制；
c) 使用设备原厂商的专用系统对控制设备进行固件升级或更新；
d) 通过其他方式修补存在安全漏洞且难以实现补丁更新的控制设备漏洞。

6.2.1.2 网络安全等级保护第三级系统的本体安全宜采用嵌入式安全模块,具备身份鉴别、访问控制、加密传输等功能。

6.2.2 数据与通信安全

6.2.2.1 第三方系统不应通过直接连接控制设备的方式采集数据；如确需连接，应采用安全可靠的接入认证和访问控制措施。

6.2.2.2 控制设备与上位控制或管理设备之间宜采用经国家密码主管部门核准的商用密码技术保护传输数据的完整性、保密性,控制设备加解密运算性能不低于 100 Mbps，上位控制或管理设备加解密运算性能不低于 200 Mbps，整体加解密对于通信延时影响不应大于 10%。

6.2.3 边界安全防护

网络安全等级保护第三级系统的边界安全防护应满足以下要求：

a) 控制设备前部署工控防火墙等访问控制设备，能解析工业控制协议数据包并阻止非法数据包、异常指令与控制器通信，支持协议读写方向控制、数据值域限制等指令级配置操作，所造成的系统延时不大于 150 us；
b) 按照 GB/T 37933—2019 中 6.1.3 的要求，控制设备前部署的访问控制设备性能指标应符合表 1 要求。

表1 访问控制设备性能指标

设备类型		性能指标		
		吞吐量	吞吐量达90%时平均时延（us）	最大连接速率（个每秒）
百兆级设备	64字节短包	≥线速的10%	≤500	≥1 500
	256字节中长包	≥线速的30%	≤500	≥1 500
	512字节长包	≥线速的50%	≤500	≥1 500
千兆级设备	64字节短包	≥线速的20%	≤200	≥5 000
	256字节中长包	≥线速的40%	≤200	≥5 000
	512字节长包	≥线速的70%	≤200	≥5 000

6.3 工业主机安全

6.3.1 本体安全

6.3.1.1 本体安全应满足以下要求：

a) 安装主机防护类软件，仅允许主机执行已知安全程序，实时监控主机进程、服务、网络端口和外接设备状况，及时阻止执行非授权应用或篡改信任应用的行为，阻止启动非法进程或开放非法端口；
b) 统一管理主机外部设备和外设接口，针对不同身份配置相应的可读、可写等权限，通过设备自带的安全管理软件或外设安全防护手段进行访问控制，消除 U 盘、移动硬盘等移动介质使用时可能出现的安全威胁；

c) 定期扫描操作系统和应用软件的漏洞，首先通过线下形式测试验证漏洞补丁更新程序，并在不影响系统可用性和稳定性的前提下更新；如难以修补漏洞，采取其他等效安全加固措施，防止漏洞被利用。

6.3.1.2 网络安全等级保护第三级系统应具备身份加密认证、数据加密传输等功能。

6.3.1.3 工程师站、操作员站、OPC 服务器、实时数据库服务器等工业主机设备宜部署经验证的防恶意代码软件，通过离线模拟验证恶意代码库更新程序，并在不影响系统可用性、实时性和稳定性的情况下更新程序。

6.3.2 数据与通信安全

6.3.2.1 数据与通信安全应满足以下基本要求：

a) 工业主机与其他系统交换数据时，设置访问控制策略并控制两系统之间的数据交换行为，只允许交换符合安全策略的指定格式数据；
b) 工业主机之间点对点通信时，对建立的会话采用相应身份认证机制，会话目的达到后及时关闭会话，并提供会话超时重新认证功能；
c) 及时备份设备运行数据、生产数据等重要数据，至少每天进行一次差分备份、每月进行一次全备份，数据发生较大调整后立即全备份；
d) 在实时数据库同步结束后完全清除数据，释放或重新分配存储空间，防止恶意恢复数据。

6.3.2.2 网络安全等级保护第三级系统的数据与通信安全应满足以下要求：

a) 采用冷备机制备份鉴别数据、重要业务数据、重要审计数据和重要配置数据，至少每天对重要业务数据和重要审计数据进行一次差分备份、每月进行一次全备份，在鉴别数据、重要配置数据调整后立即全备份；
b) 对工程师站、操作员站、OPC 服务器、实时数据库服务器等主机设备内的系统组态信息、控制程序、实时数据库用户及密码表项、OPC 服务器数据文件等重要信息资源设置敏感标记；
c) 通过具备工业协议深度解析能力的防护设备，实现对工程师站、操作员站、OPC 服务器、实时数据库服务器等重要资产数据点位级访问控制；
d) 通过广域网交换控制指令或相关数据时，采用经国家密码主管部门核准的商用密码技术实现身份认证、访问控制和数据加密传输。

6.3.3 边界安全防护

6.3.3.1 边界安全防护应满足以下要求：

a) 在对外提供 Web 服务的工业主机前部署 Web 应用防火墙等防护措施，阻止攻击者通过 web 界面渗透至工业控制系统；
b) 移动互联、无线接入设备接入工业主机前，采取身份认证和访问控制措施，阻止非授权访问，访问控制策略应包含 IP 地址和端口号、网络地址、MAC 地址以及应用协议。

6.3.3.2 网络安全等级保护第三级系统的边界安全防护应满足以下要求：

a) 部署在工业主机前的访问控制设备具备双机热备能力，当主设备自身断电或出现其他软硬件故障时，备用设备立即发现并接管主设备的工作；
b) 不使用双网卡设备与其他系统通信；如已使用且难以更改网络结构，与其他系统采取安全可靠的单向技术隔离措施。

6.4 网络设备安全

网络设备安全应满足以下要求：

a) 保证设备性能满足业务高峰时的需求，CPU 和内存使用率峰值不应大于 70%；
b) 在核心网络接口处限制网络最大流量和网络连接数；
c) 对重要网段采取技术措施以防止地址欺骗；
d) 支持核心交换机等关键网络设备整机主备切换功能，或支持关键部件冗余功能，在设备或关键部件运行状态异常时能自动切换到冗余设备或冗余部件。

6.5 防护设备安全

6.5.1 本体安全

6.5.1.1 本体安全应满足以下要求：

a) 能避免对自身未经授权的修改和破坏；
b) 不存在已公布的高危漏洞，预装软件、补丁包/升级包不应存在恶意程序，不存在未声明的功能远程调试接口、带内管理等访问接口；
c) 控制设备与工业主机之间的串接类设备具备旁路功能，设备出现故障时自动启动旁路功能并报警；
d) 具备在线或离线升级功能，升级过程中进行双向身份鉴别并具有升级包校验机制，以防止得到错误或伪造的升级包。

6.5.1.2 本体安全宜支持导入策略的校验和导出策略的加密机制。

6.5.2 身份识别与认证

身份识别与认证应满足以下要求：

a) 对用户身份进行唯一性标识，区分管理员、操作员和审计员角色，对不同角色赋予不同权限，并在使用过程中验证用户身份；
b) 具备双因子身份鉴别功能，防止攻击者通过未授权的方式进入系统，从而破坏审计数据、配置数据等信息；
c) 管理用户身份认证过程，当用户身份认证错误次数达到阈值时，采取措施阻止上述尝试认证行为；
d) 具备初次登录强制更改口令功能，并具备包含字母大小写、数字、特殊字符等不低于 8 位的口令设置功能。

6.5.3 数据保护

数据保护应满足以下要求：

a) 保护安全功能数据免受未授权的查看、修改和删除；
b) 具备会话交互超时中断功能，可自定义超时时间；
c) 能加密安全功能数据，以保证数据在网络传输过程中不被泄露和篡改。

7 系统级安全技术要求

7.1 分区分域与隔离防护

7.1.1 安全区域划分

安全区域划分应满足以下要求：

a) 与其他系统划分明确的网络边界；
b) 基于自身业务特点将系统内部划分不同安全域，支持在同一安全域内部署统一的防护策略，并能合规控制内部数据的访问和传输行为；
c) 根据业务需要，采用划分虚拟局域网（VLAN）等技术，将系统各网段的服务器、工作站等主机设备安全隔离；
d) 系统测试环境不连接生产环境。

7.1.2 边界隔离防护

7.1.2.1 边界隔离防护应满足以下要求：

a) 在与其他系统边界部署访问控制设备，启用访问控制功能，设定访问控制策略，对来自外部的访问经源地址、目的地址、源端口、目的端口和协议等检查后允许或拒绝数据包出入；
b) 在系统内部不同区域边界部署工控防火墙等隔离防护设备，解析常用工业控制协议数据包并过滤恶意代码，阻止进出区域边界的非法数据包和异常指令，支持协议读写方向控制、数据值域限制等指令级配置操作；
c) 采取无线安全检测防护措施识别和阻断未经授权的无线设备接入系统，有效检测和阻断无线扫描、无线破解、无线拒绝服务等攻击行为。

7.1.2.2 网络安全等级保护第三级系统与不存在数据通信的其他系统边界应采取物理隔离措施；如与其他系统存在数据通信，应在系统边界采取单向技术隔离措施，确保策略配置安全有效。

7.2 数据与通信安全

网络安全等级保护第三级系统的数据与通信安全应满足以下要求：

a) 在向其他系统传输数据时，采用经国家密码主管部门核准的商用密码技术校验通信数据的完整性和机密性；
b) 支持自动密钥协商机制；
c) 支持证书、用户名口令、机器码、动态令牌等多种认证因子组合捆绑认证，支持网关设备和客户端双向身份认证。

7.3 安全监控与应急处置

7.3.1 监测审计

7.3.1.1 监测审计应满足以下要求：

a) 在关键网络节点部署监测审计设备，支持威胁告警规则自定义模式，及时识别木马病毒或主机受控等网络异常和入侵行为。
b) 监测审计设备应具备如下能力：
   1) 感知和识别各类工业控制系统信息资产；
   2) 审计、跟踪和报警工程师站、操作员站、控制设备以及实时数据库服务器等设备的安全事件，并分析潜在侵害；
   3) 以便于理解的方式提供审计记录和查询方法，分析审计记录并生成报表；
   4) 控制对审计记录的访问权限，并监测文件的状态变化、修改行为等；
   5) 对工业协议提供操作功能码、数据类型、值域、读写方向等要素的审计记录；
   6) 支持对工业控制协议应用数据进行分析和还原，支持系统常用的工业控制协议；
   7) 监视系统边界和关键网络节点的常见攻击行为，如端口扫描攻击、木马后门攻击、DoS 攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫等；
   8) 实时记录攻击源 IP、攻击类型、攻击目标 IP、攻击时间等攻击行为信息，并及时报警。

7.3.1.2 网络安全等级保护第三级系统的监测审计设备应具备检测和分析新型网络攻击行为能力，并及时更新产品特征库。

7.3.2 集中管控

7.3.2.1 网络安全等级保护第三级系统的集中管控应满足以下要求：

a) 划分单独的安全管理区，部署具备数据采集与监测审计功能的设备，集中监测网络链路、安全设备、网络设备和服务器等运行状况，支持通过标准网络管理协议集中监控工业交换机、工程师站、服务器等设备资产；
b) 部署具备集中管控功能的设备，集中管理系统中的安全设备。

7.3.2.2 网络安全等级保护第三级系统宜部署具备以下网络安全态势感知和管理功能的平台。

a) 能分析研判链路、安全设备、网络设备和服务器等日志中的威胁信息；
b) 能采集和分析网络流量、异常行为、威胁告警日志、资产漏洞等不同种类数据；
c) 能分析、评估和展示资产、威胁和攻击等多种态势；
d) 能基于已知的安全威胁事件，以攻击链方式展示威胁路径过程和攻击手法；
e) 能自定义安全威胁事件功能，对安全风险形成工单并下发预警通知。

7.3.3 事件应急处置

7.3.3.1 物理抑制

物理抑制应满足以下要求：

a) 立即切断系统与外部网络之间连接，如关闭网络设备或切断线路；
b) 在不影响系统正常运行的情况下，立即关闭上位控制设备。

7.3.3.2 网络抑制

网络抑制应及时收集事件的报警、过滤信息，调整边界隔离防护设备的访问控制和过滤规则，封禁攻击威胁IP，阻断异常指令、非法数据包在系统内传播。

7.3.3.3 应用抑制

应用抑制应满足以下要求：

a) 禁用或删除被攻破的应用账号和攻击者生成的应用账号；
b) 关闭应用服务，避免系统继续遭受攻击。

7.3.3.4 主机抑制

网络安全等级保护第三级系统的主机抑制应满足以下要求：

a) 应禁用或删除主机中被攻破的账号和攻击者生成的账号；
b) 应修复设备原有的访问控制、日志、审计等安全机制。

7.3.3.5 威胁清除

威胁清除应满足以下要求：

a) 经有效评估后，有针对性地扫描和查杀工业主机感染的木马、病毒，及时消除恶意文件；
b) 修复被感染的工业主机存在的已被利用或可能会被利用的高危漏洞；
c) 修改所有账户的口令。

7.3.3.6 系统恢复

7.3.3.6.1 系统恢复应满足以下要求：

a) 借助备份数据尽快将所有被攻破的系统恢复到正常工作状态；
b) 系统数据恢复能力符合 RTO 小于 12 h、RPO 小于 1 d。

7.3.3.6.2 网络安全等级保护第三级系统数据恢复能力还应满足 RTO 小于 10 min、RPO 小于 30 min。

7.4 系统运维安全

7.4.1 运维操作

运维操作应满足以下要求。

a) 设置运维人员专用账号，建立运维行为安全基线。
b) 建立系统测试、变更管理等运维操作审批流程，通过审批后执行运维操作，审批内容至少包括：实施方案、风险评估、应急措施等。
c) 运维工具接入前查杀病毒和恶意代码，操作过程中保留不可更改的日志记录，操作结束后删除工具中的敏感数据。
d) 如具备测试系统，优先在测试系统中验证运维操作行为的安全性。
e) 对数据库执行增删改查等操作前测试结构化查询语句并备案，运维人员仅执行已备案语句。
f) 实时监控运维过程，及时对高危指令告警，设置拒绝执行高危指令规则，切断异常会话。

7.4.2 运维行为审计

运维行为审计应满足以下要求：

a) 采用技术手段对运维人员进行身份鉴别、访问控制和行为审计；
b) 对系统实行基于唯一身份标识的全局实名制管理，统一账号；
c) 运维行为审计记录包括运维日期和时间、用户、事件类型、事件是否成功及其他与审计有关的信息；
d) 对系统数据调用行为进行审计，审计和控制数据库操作行为；
e) 实时监控 SSH、SFTP 和数据库的高危操作指令，必要时告警、阻断会话或二次审批；
f) 监控远程访问用户执行数据调入和调出请求的行为，并单独进行行为审计和数据分析；
g) 保护审计记录，避免受到未经授权的删除、修改或覆盖等；
h) 不明文记录用户口令等敏感数据；

i） 审计日志留存不少于6个月。

7.5 软件供应链安全

7.5.1 系统开发软件资产库

系统开发软件资产库应满足以下要求：

a） 建立软件资产库，存储开发环境、源代码、组件库、配置文件、开发文档、软件物料清单（SBOM）、授权码等数据；
b） 使用软件资产库中安全的开源组件和第三方组件进行软件开发；
c） 使用软件资产库中安全的开发工具进行代码编辑、集成、编译等；
d） 对软件资产库设置身份认证和访问控制机制，防止软件资产数据被删除、被破坏、被篡改、被泄露、被植入恶意代码等。

7.5.2 开发代码安全性检测

7.5.2.1 开发代码安全性检测应满足以下要求：

a） 在系统开发阶段静态检测整体软件代码，优化代码结构，保留软件代码开发阶段的安全检测报告与修复方案；
b） 在系统发布阶段整体封装软件代码，并在运行阶段检测软件完整性；
c） 在系统部署与测试阶段对监控软件、组态软件、外部数据接口进行动态代码检测，检查输入输出的预期结果一致性和有效性，检查代码健壮性，防止出现内存泄漏、异常值返回等情况。

7.5.2.2 网络安全等级保护第三级系统应在系统部署与测试阶段，委托具有资质的第三方测评机构进行安全性测评并出具测评报告。

7.5.2.3 网络安全等级保护第三级系统宜在系统部署与测试阶段，委托具有资质的第三方测评机构分析源代码自主率并出具测评报告。

7.5.3 开发软件开源组件及其安全性检测

7.5.3.1 开发软件开源组件及其安全性检测应满足以下要求：

a） 在系统发布阶段分析软件成分，梳理软件中所有组件信息和组件间依赖关系，形成符合软件物料清单标准要求的软件成分信息数据；
b） 在系统部署与测试阶段对软件的开源组件和第三方组件进行检测，检查组件的安全性和开源许可证合规性，防止出现开源组件有高危漏洞或者开源许可证有冲突等情况。

7.5.3.2 开发软件开源组件及其安全性检测宜委托具有资质的第三方测评机构，测试开源组件安全性并出具测评报告。

7.5.4 开发软件上线前安全性检测

7.5.4.1 开发软件上线前安全性检测应满足以下要求：

a） 对监控软件、组态软件、信息存储等应用软件进行权限验证，明确操作授权级别，梳理系统的角色和操作访问控制关系，防止出现权限绕过和超级管理员权限账号等风险；
b） 检测监控软件、组态软件、数据库软件和操作系统漏洞，修复相关漏洞后方可上线；
c） 检测外部数据接口，防止出现接口协议漏洞、未授权数据调用、未授权访问等异常行为；
d） 检查与其他系统之间通信链路的脆弱性，防止出现信息泄露。

7.5.4.2 网络安全等级保护第三级系统开发软件上线前安全性检测应满足以下要求：

a） 对软件进行国密算法数字签名处理，在部署阶段校验文件来源和完整性；
b） 委托具有资质的第三方测评机构开展安全测试，并出具测评报告。

附 录 A
（资料性）
民用航空生产运行工业控制系统典型示例

A.1 概述

民用航空生产运行工业控制系统一般包括飞行区的助航灯光系统，航站区的行李处理系统和楼宇自动化系统，以及工作区的油库供油（长输管道）自动化系统。这些系统在维护机场运行秩序、保障飞行安全方面发挥重要作用，对信息传输的低时延性、高可靠性提出很高要求，一旦系统遭受恶意入侵或网络攻击，会导致控制设备发生非正常停机、信息误判断或发送错误控制指令等异常行为，会直接对机场的运行秩序造成影响。

A.2 助航灯光系统

助航灯光系统是指利用计算机技术、网络技术和检测技术对机场跑道、滑行道的目视助航灯光进行检测和控制，记录灯光和供电回路，实现员工管理并为日后复查、维修提供数据依据，是一个高可靠性分布式系统。系统分为塔台、维修中心和灯光站三个部分，通过计算机网络实现上述部分之间的信息传递和交换。

单灯监控设备是助航灯光监控系统的组成部分，用于提供机场灯光设备的监视、故障定位和选择性开关等功能，一般包括单灯控制计算机、单灯监控主机、单灯监控装置以及必要的探测传感器。

助航灯光系统具有以下业务特点。

——可靠性：系统对机场飞行区安全与飞行器安全非常重要，助航灯光系统重点保障飞行器在夜间和复杂气象条件下的正常起落飞行，对整体系统软硬件可靠性提出很高要求。

——实时性：系统需要在规定时间内迅速执行灯光控制指令，并且及时反馈灯光状态至塔台内的监控平台。

——安全性：系统的控制权限划分非常清晰，控制一般由权限最高的中心控制计算机对灯光回路实施控制。控制权限可以通过授权方式下放到主/次灯光站，因此需要确保系统的权限管理以及运维操作的安全性。

A.3 行李处理系统

行李处理系统是使用条码识别技术和智能控制技术对旅客托运的行李进行集中传送、分拣与处理的自动化系统。系统通过与机场航班集成系统、离港系统、安全检查系统等外部系统进行数据交互，实时获取航班及行李源信息，并在综合分析设备运行状态的基础上，动态分配可用设备资源，实现对旅客托运行李的跟踪识别、路由控制、设备状态监控、航班信息处理、行李源信息处理等功能。

行李处理系统具有以下业务特点。

——可靠性：系统的可靠运行对机场运营非常重要，对系统的硬件可靠性、控制软件合理性、分拣容错率方面提出了很高的要求，在不间断承担行李识别、运输、转存的过程中，要求系统对临时任务的灵活处理并且不影响整体控制流程。

——一致性：系统具有多系统信息共享、联动控制的特性，依据航班信息状态以及机场其他信息系统对于航班的调整，及时更新行李处理流程。

——安全性：系统呈现高度自动化趋势，人工工作量持续减少，需要确保系统的控制流程以及负责实现控制任务的软硬件的安全性，需要将针对工业控制系统的防护手段融入到业务流程中。

A.4 楼宇自动化系统

楼宇自动化系统是对航站楼内所控机电设备的状态进行集中监视，分散控制、测量的管理系统的总称。通过对智能楼宇管理、建筑设备监控管理、智能照明监控管理等系统的集成，实现对航站楼内冷热源设备、空调主机及通风设备、供水设备及排水设备、污水处理设备、室内外照明等机电设备的集中监控管理，包括监视、自动计量和控制设备运行状态，报警管理，季节设置，分析历史数据以及生成运行数据报表等。同时，通过统一接口标准，实现各管理系统间的信息互通，完成联动逻辑。

楼宇自动化系统具有以下业务特点。

——可靠性：系统的可靠运行对机场运营非常重要，对系统的硬件可靠性、控制软件合理性方面提出很高要求，在航站楼内空调、供排水、照明、消防等过程中，要求系统灵活处理临时任务且不影响整体控制流程。

——一致性：系统具有多系统信息共享、联动控制的特性，依据航站楼内设备运行、环境安全状态等变化及时调整楼宇自动化系统运行参数。

——安全性：需要确保系统控制流程以及负责实现控制任务的软硬件的安全性，需要把针对工业控制系统的防护手段融入到业务流程中。

A.5 油库供油（长输管道）自动化系统

油库供油（长输管道）自动化系统从业务属性上可分为：油库供油自动化系统和长输管道自动化系统。

油库供油自动化系统以可编程逻辑控制器（PLC）为主，自动监控管理油库的储油、收油、发油等环节，对收发油流程及日常储存等环节实施信息管理，使油库的生产作业实现微机自动化网络管理，提高生产环节的安全防范措施，并在此基础上形成完整的业务信息反馈与监督控制系统。

长输管道自动化系统以监控和数据采集系统（SCADA）为主，通过主机和以微处理器为基础的远程终端装置远程终端单元（RTU）、PLC等设备，对炼厂、码头、中转库至机场中转库之间的输送民用航空燃料管道进行自动控制，以及对各设备的运行情况和工艺参数进行监控。系统通常在管道中间各阀室设置RTU等终端设备，实时采集进出站的压力和流量，通过专线、4G网络等与总控室之间进行数据传输和双向通信。

系统具有如下业务特点。

——可靠性：系统的可靠稳定运行是确保工业生产安全的基础，在系统的软硬件设计上提出了高可靠性要求，同时系统生产过程自身是连续不间断工作方式，对系统可靠性要求高。

——实时性：系统具有实时闭环控制的特性，各设备按照业务逻辑在固定时间完成特定动作。

——安全性：系统采用计算机通信以及无线接入等技术，应在保障系统功能安全的同时，确保系统网络安全，将网络安全防护措施融入生产控制业务中，保障工业控制系统的可靠稳定运行。

——适应性：系统采集、传输、控制等业务模块采用地理或空间位置上的分散布置方式，系统需要在高温/低温、潮湿/干燥的环境中稳定运行，对环境适应性要求高。

参 考 文 献

[1] GB/T 40813—2021 信息安全技术 工业控制系统安全防护技术要求和测试评价方法
[2] GB/T 41400—2022 信息安全技术 工业控制系统信息安全防护能力成熟度模型
[3] GB 42250—2022 信息安全技术 网络安全专用产品安全技术要求
[4] MH/T 0076—2020 民用航空网络安全等级保护基本要求
[5] MH/T 5002 运输机场总体规划规范
[6] MH/T 5009 民用运输机场航站楼楼宇自控系统工程设计规范
[7] MH/T 5103 民用机场信息集成系统技术规范