ICS 03.220.40
CCS L 60

团 体 标 准

T/CIN 014—2023

自动化集装箱码头数据中心技术要求

Technical requirements for data centers of automated container terminal

2023－06－02 发布

2023－09－02 实施

中国航海学会 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。

本文件由中国航海学会提出并归口。

本文件起草单位：青岛港国际股份有限公司、青岛新前湾集装箱码头有限责任公司、交通运输部科学研究院、山东港口科技集团青岛有限公司、交通运输部规划研究院、华为技术有限公司。

本文件主要起草人：张蕾、李波、徐斌、汪炜、李永翠、王伟、徐永宁、张子青、凌方、李益民、徐坤三、张华、孙秀良、刘长辉、汤雪、李亚敏、齐越、姚海元、黄敏、赵娜、王涛、杜明

自动化集装箱码头数据中心技术要求

1 范围

本文件规定了自动化集装箱码头数据中心的构成和总体要求，以及网络系统、计算与存储资源、备份与容灾、安全系统、运维管理系统和机房基础设施等技术要求。

本文件适用于自动化集装箱码头数据中心的建设、运维和升级改造。

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 18233.1 信息技术 用户建筑群通用布缆 第1部分：通用要求
GB/T 18233.5 信息技术 用户建筑群通用布缆 第5部分：数据中心
GB/T 20984 信息安全技术 信息安全风险评估方法
GB/T 20988 信息安全技术 信息系统灾难恢复规范
GB/T 22239 信息安全技术 信息系统安全等级保护基本要求
GB/T 28448 信息安全技术 网络安全等级保护测评要求
GB/T 28449 信息安全技术 网络安全等级保护测评过程指南
GB/T 30285 信息安全技术 灾难恢复中心建设与运维管理规范
GB/T 31240 信息技术 用户建筑群布缆的路径和空间
GB/T 32399 信息技术 云计算 参考架构
GB/T 34982 云计算数据中心基本要求
GB/T 37933 信息安全技术 工业控制系统专用防火墙技术要求
GB/T 39204 信息安全技术 关键信息基础设施安全保护要求
GB/T 39680 信息安全技术 服务器安全技术要求和测评准则
GB 40879 数据中心能效限定值及能效等级
GB/T 41267 网络关键设备安全技术要求 交换机设备
GB/T 41269 网络关键设备安全技术要求 路由器设备
GB 42250 信息安全技术 网络安全专用产品安全技术要求
GB 50057 建筑物防雷设计规范
GB 50174 数据中心设计规范
GB 50311 综合布线系统工程设计规范
GB 50343 建筑物电子信息系统防雷技术规范

3 术语和定义、缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

超融合架构 hyper converged infrastructure

在同一套单元设备将虚拟化的计算、网络、存储资源和技术进行整合，提供数据删除、在线数据压缩、备份、快照等功能，且可通过网络实现多节点设备聚合，具备高兼容性和可扩展性的架构。

3.1.2

虚拟化 virtualization

将计算机实体资源（如服务器、网络、内存及存储等）予以抽象、转换、模拟为逻辑资源的过程。

3.2 缩略语

下列缩略语适用于本文件。

BFD：双向转发检测（Bidirectional Forwarding Detection）
CPU：中央处理器（Central Processing Unit）
DNS：域名系统（Domain Name System）
ID：身份标识号（Identity document）
IP：因特网协议（Internet Protocol）
LUN：逻辑单元号（Logical Unit Number）
LV：逻辑卷（Logical Volume）
NFS：网络文件系统（Network File System）
PLC：可编程逻辑控制器（Programmable Logic Controller）
RAID：独立冗余磁盘阵列（Redundant Arrays of Independent Disks）
SMB：信息服务块（Server Message Block）
SSD：固态硬盘（Solid State Disk或Solid State Drive）
SSL：安全套接层（Secure Sockets Layer）
UPS：不间断电源（Uninterruptible Power Supply）
USB：通用串行总线（Universal Serial Bus）
WEB：全球广域网（World Wide Web）
4G：第四代移动通信技术（The 4 Generation Mobile Communication Technology）
5G：第五代移动通信技术（The 5 Generation Mobile Communication Technology）

4 构成和总体要求

4.1 构成

4.1.1 自动化集装箱码头数据中心（以下简称“数据中心”）应由支持码头生产业务运行的网络系统、计算与存储资源、备份与容灾、安全系统、运维管理系统、机房基础设施等构成，宜采用模块化组合方式配置，如图1所示。

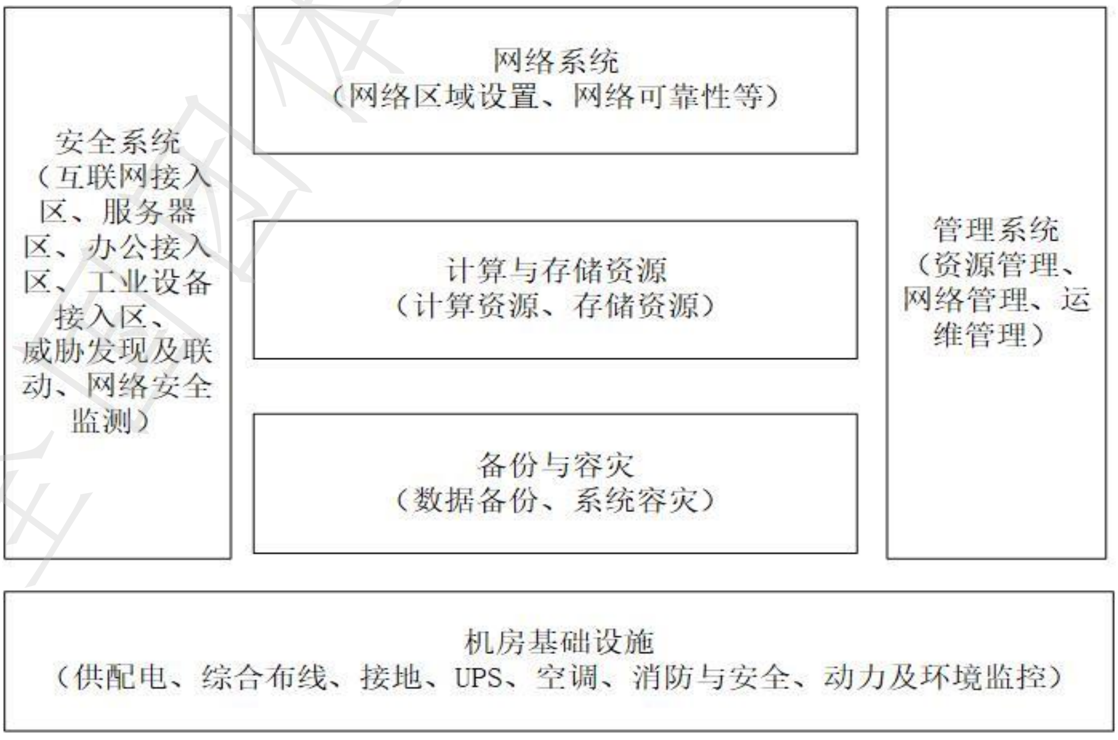

图1 自动化集装箱码头数据中心构成图

4.1.2　网络系统由内部网络和外部互联网组成，内部网络应支持办公管理、生产作业和工业控制，满足码头运营和对外服务的网络环境要求。
4.1.3　计算与存储资源由物理服务器、虚拟服务器、存储等组成，按存在形式分为物理资源和逻辑资源，应满足码头运营系统所需基础资源的要求。
4.1.4　备份与容灾由数据备份和系统容灾组成，应具备数据中心灾难情况迅速恢复数据和系统的能力。
4.1.5　安全系统由互联网接入区、服务器区、办公接入区、工业设备接入区等区域安全组成，宜提供威胁发现及联动、网络安全监测等安全功能，支持对数据中心网络安全和信息安全的必要监测、威胁发现、预警处置，满足数据中心整体运营安全需要。
4.1.6　运维管理系统包括资产管理、监控管理、运维报警管理等，应支持数据中心运行状态的在线管理，宜满足数据中心智能运维管理要求。
4.1.7　机房基础设施包括供配电、综合布线、接地、UPS、温湿度控制、消防与安全、动力及环境监控等，应满足支撑数据中心运行环境要求，宜采用模块化组合方式配置。

4.2　总体要求

4.2.1　应易于升级和扩充，适应码头业务规模扩大和生产发展需要，支持与需连接网络的互连互通。
4.2.2　宜符合 GB 50174 中 B 级或 A 级相关要求，满足数据中心安全、稳定、连续运行的要求。
4.2.3　应具备 7×24h 不间断运行能力，支持关键业务不间断运行。
4.2.4　应建立应急机制，制定备份和恢复措施，满足意外情况及时恢复数据中心正常运行的相关要求。
4.2.5　应建立日常管理制度和网络信息安全制度，满足数据中心安全运行的相关要求。
4.2.6　宜采用双活数据中心架构，满足紧急情况单数据中心承载全部系统的运行要求。
4.2.7　宜采用二层虚拟网络互联，构建跨多数据中心网络，并与物理网络解耦。
4.2.8　数据中心关键设备宜采用国产化技术产品进行部署。
4.2.9　网络关键设备的安全应符合 GB/T 41267、GB/T 41269 的相关要求。
4.2.10　网络安全专用产品安全应符合 GB 42250 的相关要求。
4.2.11　关键信息基础设施安全保护应符合 GB/T 39204 的相关要求。
4.2.12　能效应符合 GB 40879 的相关要求，不断实现能效等级的提高。
4.2.13　采用云计算的数据中心应符合 GB/T 32399、GB/T 34982 的相关要求。

5　网络系统

5.1　网络区域设置

5.1.1　网络区域划分

自动化集装箱码头网络系统应分区进行设计和部署，满足弹性化（业务快速扩张和灵活部署）、虚拟化、资源整合与共享以及高效运维与能耗管理的需要，支持系统的应变能力、容错能力和纠错能力。网络系统分为核心区、互联网接入区、业务接入区、运维管理区和监管单位接入管理区等区域，网络系统如图2所示。

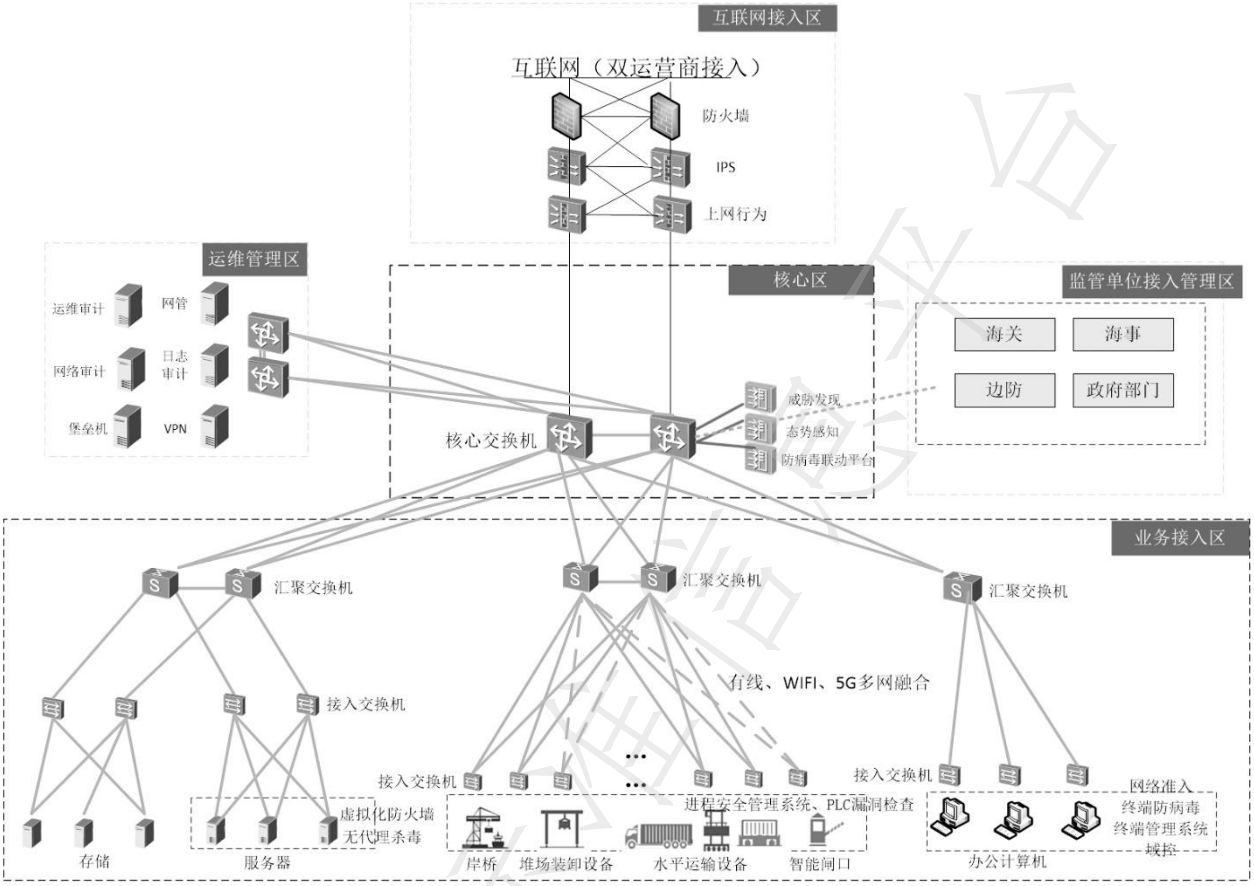

图2　自动化集装箱码头网络系统图

5.1.2　核心区

5.1.2.1　应提供连接内部各业务区域、灾备中心和外部用户接入的网络，具有高可靠性、不间断持续转发的能力。
5.1.2.2　应采用万兆及万兆以上速率的核心交换机，且具备高密端口接入功能，支持无阻塞大容量交换。
5.1.2.3　应采用具备虚拟化、逻辑隔离、负载均衡等功能的核心交换机，满足核心区数据交换、路由转发、网络隔离、链路互备等需求。
5.1.2.4　宜采用双机互备模式，保障核心区的安全稳定运行。

5.1.3　互联网接入区

5.1.3.1　应配置交换路由，对内网和互联网的路由信息进行转换和维护。
5.1.3.2　宜采用多因子认证和最小权限配置，满足接入用户的合法性和唯一性。
5.1.3.3　应配置不同运营商、不同路由的两条或两条以上链路，支持流量负载均衡功能，且链路带宽满足业务需求。
5.1.3.4　宜支持不改变当前网络配置的灵活扩容。

5.1.4　业务接入区

5.1.4.1　应按功能划分服务器区、办公区、工业设备区等业务区域，对不同区域进行隔离，满足安全性和扩展性要求。
5.1.4.2　宜采用物理路径不同的双链路方式，实现汇聚交换机至核心交换机、汇聚交换机至接入交换机互联，支持用户通过接入交换机及汇聚交换机访问服务器、网络、应用系统等资源。
5.1.4.3　服务器区应采用独立网段设计，用于服务器和应用系统的部署。
5.1.4.4　办公区应按组织、业务划分用户组，支持终端部署，满足不同用户组终端的访问互联需求。

5.1.4.5 工业设备区应提供作业设备、工业控制系统、传感器等的接入网络，满足信息互联互通的要求。

5.1.4.6 工业设备区网络宜采用有线网、无线网的多网融合架构，无线网宜选用 5G、4G 等专网方式，且避免通信间相互干扰，满足安全、高效、可靠的要求。

5.1.5 运维管理区

5.1.5.1 应部署网络运维管理等系统，满足数据中心网络设备状态监控管理和维护管理的要求。

5.1.5.2 宜独立成网，并与其他区域有限访问。

5.1.6 监管单位接入管理区

5.1.6.1 监管单位接入管理区应根据业务需要选取如下方式：

a) 港口共享；

b) 码头独立配备。

5.1.6.2 宜独立成网，并与其他区域有限访问。

5.2 网络可靠性

5.2.1 应具备有效的安全控制，提供按业务权限进行分区隔离功能，核心业务宜采取物理隔离。

5.2.2 应具有良好的可扩展性，宜选取集成度高、通用性强的产品。

5.2.3 应合理规划、分配网络 IP 地址，支持网络资源的便捷管理。

5.2.4 应采用冗余部署的网络拓扑结构，避免单点风险。

5.2.5 应冗余配置关键设备及其电源、主控板等关键部件。

5.2.6 应提供冗余备份或负载均衡的关键链路。三层网络宜具备等价路径辅助部署 BFD 快速检测故障的功能，实现设备故障的快速切换。

5.2.7 宜支持基于 SSL 协议建立网络连接，提供数据安全传输。

5.2.8 宜采用网络切片等技术，实现不同业务数据在不同切片中承载，保障网络传输质量。

6 计算与存储资源

6.1 计算资源

6.1.1 计算资源主要包括物理服务器（以下简称“物理机”）和虚拟服务器（以下简称“虚拟机”），虚拟机由物理机采用虚拟化（云化）平台划分和管理的逻辑服务器资源。

6.1.2 应具备 7×24h 连续工作的能力，可用性大于 99.99%。

6.1.3 应配备时间服务器，保证数据中心所有计算资源时间统一。

6.1.4 应配备相应的日常管理平台，对计算资源的 CPU、内存、用户、存储、网络、日志收集、性能分析、故障诊断、权限等进行在线管理。

6.1.5 应具备安全性，防止恶意软件或病毒攻击，并对数据进行定期备份，宜对数据进行加密。

6.1.6 应具有可扩展性，支持计算资源扩展，满足不断变化的需求。

6.1.7 应具有足够的处理能力和存储能力，满足应用程序的要求。

6.1.8 应支持各类操作系统和软件，且方便与其他应用程序和服务集成。

6.1.9 物理机满足下列要求：

a) 物理机内部组件除主板外应冗余配置，具有硬件管理功能和一定的容错能力；

b) 宜采用RAID1或RAID5的硬盘数据存储方式；

c) 应按“生产运行”、“开发测试”等不同用途分别构建独立集群。

6.1.10 虚拟机满足下列要求：

a) 应能够独立运行，且在运行期间不应受到其他系统或应用程序的干扰；

b) 应由虚拟化（云化）平台进行配置和管理；

c) 应与底层硬件隔离，防止其他应用程序或系统访问硬件资源；

d) 应具有可扩展性，支持硬件扩展，满足不断变化的需求。

6.1.11 虚拟化（云化）平台满足下列要求：

a) 虚拟化平台由服务器、存储、网络等虚拟化软件及管理控制平台组成；
b) 采用虚拟化平台管理的物理机宜组建集群，至少具备4个计算节点和冗余万兆网络接入能力；
c) 虚拟化平台应具备集群化容灾能力；
d) 虚拟化平台应实现计算资源的管理网、业务网和数据网分离；
e) 虚拟化平台应具备高可用性，实现单点故障不影响虚拟机运行，满足业务连续性要求；
f) 应具备虚拟机在线迁移功能，实现虚拟机的动态迁移和服务不中断；
g) 应具备统一资源管理功能；
h) 应具备按需资源调配、模板部署等功能；应支持自定义角色和权限，实现资源的分级管理。

6.2 存储资源

6.2.1 存储资源包括存储设备（如整套磁盘阵列）、存储网关、块存储、文件存储等，存储设备和存储网关、块设备为物理资源，文件存储等为逻辑资源。
6.2.2 存储设备应采用全冗余、模块化结构，控制器数量应不少于 2 个，双控制器应能同时访问同一个数据单元；支持多种 RAID 保护方式，宜提供多通道路径访问，实现对应用透明自动故障通道的切换和负载均衡。
6.2.3 存储网关应具有同构或异构存储间的虚拟化和数据镜像功能，提供不停机维护和在线调整（包括软、硬件升级、扩容、设备更换等操作），后端数据应能被不同数据中心的物理机或虚拟机同时存取。
6.2.4 块存储应为采用 RAID 或 LV 技术对物理设备和磁盘进行逻辑处理的存储资源，实现数据存储的底层保护。
6.2.5 文件存储宜采用分布式架构，应能提供多个计算节点同时挂载和使用，宜采用后端多副本存储方式，并具备协议兼容性，支持 NFS 和 SMB 协议等。
6.2.6 存储资源应支持结构化或非结构化数据存取。
6.2.7 虚拟化、超融合或云化架构使用的存储宜采用分布式架构，利用 SSD 高速硬盘实现高性能的读/写缓存，且具备固态磁盘缓存的横向扩展能力；应采用多副本存储方式（至少 2 副本，推荐 3 副本存储），每台物理机最少配置 2 个磁盘组，缓存层 SSD 的持久度等级、性能等级应为 C 级或更高。

7 备份与容灾

7.1 应提供计算资源、存储资源、网络资源、通信资源的可靠备份能力，容灾备份应符合 GB/T 20988 的有关规定，灾难恢复能力等级不应低于 GB/T 20988 确定的第 5 级要求，实现关键数据零丢失。容灾备份中心建设和维护应符合 GB/T 30285 的相关要求。
7.2 应具备数据备份和业务系统整体备份两种方式，实现数据和业务系统快速恢复，以及按任意时间点的数据恢复，并配合应用需求实现快速回滚。
7.3 应具有灵活的备份策略，支持全量、增量、差量、累计增量等多种备份方式。
7.4 应具备集中备份管理能力，并定期进行备份数据校验和备份数据恢复测试。
7.5 应采用本地离线备份和异地离线存储相结合的数据备份方式，本地和异地备份设备均应使用独立设备，且不应与其他业务系统混用。数据应至少有 2 份副本并分别存储在不同的存储设备上。
7.6 应采用统一备份管理系统，功能包括设备状态和性能信息、备份运行情况、配置信息、作业运行参数、备份数据状态和备份恢复情况等管理，宜提供图形化、WEB 等展示方式。
7.7 应具有高可靠性容灾机制，支持服务器集群高可用。
7.8 应具备自动负载均衡和性能调节能力，实现系统易扩展和高容错。

8 安全系统

8.1 互联网接入区安全

8.1.1 应部署防火墙进行内网与互联网隔离，并关闭互联网对内网的直接访问权限和非正常业务服务端口，配置访问控制策略，宜采用白名单制，实现内网安全。
8.1.2 应配置入侵防御设备，支持对攻击行为、恶意行为的检测和防御。
8.1.3 应配置上网行为管理，支持对网络访问权限和行为的控制和监管。

8.1.4 应配置 DNS 防劫持功能，防止正常域名被劫持。
8.1.5 应配置抗拒绝服务攻击设备，识别和防御各种分布式拒绝攻击行为，避免因网络带宽占用和服务器资源耗尽等导致无法正常提供服务。

8.2 服务器区安全

8.2.1 应符合 GB/T 39680 的相关规定。
8.2.2 应部署防火墙，进行服务器区与其他网络区域的隔离，并以最小授权原则配置用户访问服务器的权限。
8.2.3 应部署软件定义网络系统和服务器虚拟化防火墙，实现虚拟机之间的微分段和隔离防护，支持互联网应用服务器和生产业务服务器之间流量的高效检测和隔离，满足虚拟化环境网络安全要求。
8.2.4 应部署服务器和虚拟化防病毒系统，实现服务器和虚拟机的病毒自动检测和处置。
8.2.5 宜部署 WEB 应用防火墙、网页防篡改系统，防范 WEB 应用服务器的访问攻击和网站页面的非法篡改。
8.2.6 宜采用 Linux 或其他国产服务器操作系统。
8.2.7 宜采用域控系统对 Windows 服务器操作系统进行管理。

8.3 办公接入区安全

8.3.1 应部署网络准入管理系统，实现身份鉴别、安全性检查、用户授权和安全域划分。
8.3.2 应部署桌面终端管理、终端防护、防病毒等系统，并关闭计算机终端 USB 端口，开启计算机终端防火墙。

8.4 工业设备接入区安全

8.4.1 应部署防火墙，并符合 GB/T 37933 的相关要求，实现工业设备接入区与其他网络的隔离。
8.4.2 码头自动化装卸设备和自动化水平运载工具的嵌入式装置和工控系统不宜连接外设。必要连接外设时，应经专家研判并确认安全，方可进行外设连接配置。
8.4.3 宜在码头自动化装卸设备和自动化水平运载工具的嵌入式装置和工控系统上部署进程安全管理系统和 PLC 漏洞检查工具，支持进程自动检测和处置，以及漏洞的定期扫描。
8.4.4 宜在工业主机登录、应用服务资源访问、工业云平台访问等过程中使用身份认证管理，并对关键设备、系统和平台的访问采用多因素认证。
8.4.5 应拆除或封闭工业主机上非必要 USB、光驱、无线等接口，确需使用时，应通过主机外设安全手段进行访问控制。
8.4.6 工业控制、工业通信设备和软件系统的登录账户及密码应设置登录口令复杂度校验，不应使用默认口令或弱口令，并定期进行口令更换。

8.5 威胁发现及联动控制

8.5.1 宜部署威胁发现系统，实时、有效地掌握网络安全状态，追溯病毒及威胁源头，对网络安全环境进行智能分析，提高网络、数据的安全系数。
8.5.2 宜部署联动控制系统进行统一管理，包括但不限于防火墙、服务器防病毒、威胁发现、深度防御、网络设备等安全相关系统。控制系统应能基于威胁发现与安全相关系统实现联动控制。

8.6 安全审计

8.6.1 应部署日志审计系统，记录相关安全事件， 审计记录包括安全事件的主体、客体、时间、类型和结果等内容，并确保日志留存时间不少于 180 天。
8.6.2 应部署运维堡垒机，对运维人员的运维操作行为进行管控和审计。
8.6.3 应部署数据库审计系统，对运维人员的数据库操作行为进行审计和追溯。
8.6.4 应部署网络审计系统，对网络行为进行识别与审计，支持自定义多维度统计分析。

8.7 风险管理

8.7.1 应符合 GB/T 22239 第二级或第二级以上的安全要求，并按 GB/T 28448、GB/T 28449 相关要求进行等级测评，发现不符合情况及时整改。

8.7.2 应按GB/T 20984相关要求进行信息安全状况风险评估，形成风险评估报告，及时发现安全漏洞，制定应对措施。

9 运维管理系统

9.1 资产管理

资产管理应支持对数据中心的基础设施、计算资源、存储资源、网络资源和其他资产的日常管理、统计、核对，范围涵盖设备资产信息、设备用户信息、设备存放信息、设备端口信息等，功能应满足下列要求：

a) 机房资源管理：实现对机房、机架、机位等资源的管理，提供机房、机架、机位信息的增加、修改、释放、查询功能；
b) 计算资源管理：实现对物理机、虚拟机以及计算机群等资源管理，提供资源信息的增加、修改、释放、查询功能；
c) 存储资源管理：实现对存储设备（如整套磁盘阵列）、设备（LUN 设备）、文件系统、对象存储或结构化存储（如数据库）等资源管理，提供资源信息的增加、修改、释放、查询功能；
d) 网络资源管理：实现对 IP 地址、网络带宽、防火墙、负载均衡等资源管理，提供资源信息的增加、修改、释放、查询功能；
e) 其他资产管理：实现数据中心的设备 ID、类型、型号、技术指标、用户信息、设备端口等其他资产信息管理，提供资产信息的增加、修改、释放、查询功能；
f) 数据存储管理：提供数据中心资产管理信息在线保留时间不少于 180 天，历史数据根据不同业务需要进行一定期限的保存。

9.2 监控管理

监控管理包括设备监控、拓扑管理、性能管理、故障管理和统计分析等，应满足下列要求：

a) 设备监控：提供数据中心硬件设备的日常运行监控管理，包括交换机、路由器、防火墙、网络安全设备、服务器、存储等网元；
b) 拓扑管理：提供多种视图模板，按照权限和精细程度不同，对各网元视图进行展示；
c) 性能管理：对网络、服务器等设备性能及实时使用状况进行监控、分析，并形成报告；
d) 故障管理：对不正常的网络和设备运行状况或环境条件进行检测、隔离、校正、告警等；
e) 统计分析：提供全面科学的各网元数据统计分析报表，能全方位展示各网元管理信息；
f) 日志存储：监测、记录运行状态和网络安全事件的日志数据留存时间应不少于 180 天。

9.3 运维报警管理

9.3.1 应部署一体化运维管理平台，进行数据中心软硬件资源的全局管控，具备直观、快速定位故障功能，支持邮件或短信等发送报警，实现自动运维监控和报警。
9.3.2 应部署网络审计系统，对网络行为进行识别、分析和告警。
9.3.3 应部署数据库审计系统，对数据库系统进行多个、多类型事件的交叉关联分析，发现异常进行告警。
9.3.4 应部署综合日志系统，对网络设备、安全设备、服务器和应用系统的日志进行全面集中标准化统一汇集，实现资产运行状况和信息资产的统一监管。

10 机房基础设施

10.1 供配电系统

10.1.1 应采用220 V/380 V电压等级，预留备用容量，满足系统扩展、升级需要，配电电源系统应满足设备供电要求。
10.1.2 机房供配电系统应采用双路电源接入，且双路电源宜取自不同变电站和不同路由。
10.1.3 供配电容量较大时，宜设置专用电力变压器。容量较小时，宜采用专用低压馈电线路供电。
10.1.4 供配电系统应靠近主机房，机房临时用电设备不得使用机房专用供配电系统，以确保机房供配

电系统的安全稳定运行。

10.1.5　用电插座分为UPS插座和市电插座，两者应有明显区别标志。

10.1.6　计算机设备供电与空调供电应设互相独立供电回路。

10.1.7　应配备专用柴油发电机等应急供电系统。

10.2　综合布线

10.2.1　综合布线的组成包括配线架、主线缆、水平线缆、汇接点、管理等，设计应符合GB 50311的要求。

10.2.2　综合布线应符合GB/T 18233.1、GB/T 18233.5的相关规定，布缆的线径和空间应符合GB/T 31240的相关规定。

10.3　接地系统

10.3.1　交流工作接地电阻应不大于4Ω；安全保护接地电阻应不大于4Ω；直流工作接地电阻按照计算机系统具体要求确定。

10.3.2　防雷接地应符合GB 50057、GB 50343的相关规定；系统接地和屏蔽接地宜共用一组接地装置，其接地电阻按照两者的最小值确定。

10.3.3　计算机接地系统应采用单点接地，宜采取多个计算机接地系统并经铜排网和接地线接至同一接地干线等电位措施。

10.3.4　防雷接地电阻值应小于10Ω，防静电接地电阻值应小于4Ω，电源保护地电阻值应小于4Ω，电源工作地应小于4Ω。

10.3.5　将机房内所有设备的工作接地、保护接地、防雷接地、防静电接地等接地线均连接到均压等电位网上，满足雷击时所有金属导体处于同一电位水平的要求。

10.3.6　宜采用暗敷设布线。金属屏蔽管敷设布线时，应将屏蔽管接地。光缆入室应将其牵引金属筋接地。

10.4　UPS系统

10.4.1　UPS负载量不宜长期超过其额定容量的80%。

10.4.2　宜尽可能将电池组靠近UPS主机，缩短两者连线长度，增大线截面积，降低连线自感量和线路压降。

10.4.3　应具备UPS运行状态的自动监测和故障预警功能。

10.4.4　应采用2套模块化UPS，接入机房不同电源，组成数据中心核心设备双路供电模式。

10.5　空调系统

10.5.1　应满足机房内计算机设备的温湿度要求。

10.5.2　宜合理组织空调气流，合理分配各个区域冷量，具备定量分配功能。

10.5.3　宜将冷气流和热气流完全隔离、互不影响。

10.5.4　应留有15%～20%余量的空调制冷能力。

10.5.5　应维持一定的正压，主机房与其他房间、走廊间的压差应不小于4.9 Pa，与室外静压差不小于9.8 Pa。

10.5.6　机房空调送风系统应设初效、中效两级空气过滤器，中效空气过滤器计数效率应大于80%，末级过滤装置宜设在正压端或送风口。

10.5.7　机房空调宜采用微模块或冷通道隔离方式，提高空调系统的使用效率。

10.6　消防与安全

10.6.1　应设置自动灭火系统，包括气体灭火系统和火灾自动报警系统，并提供安全逃离措施。

10.6.2　气体消防系统应采用环保型气体灭火系统；灭火系统应具备自动、机械手动和远程操控三种方式启动。

10.6.3　火灾自动报警系统应设有备用电源，当主电源故障时，应自动切换到备用电源。

10.6.4　灭火系统启动前，应发出声光报警信号，延时30s后方可启动气体灭火系统进行灭火。

10.6.5　自动灭火系统应与空调、通风系统联锁，采用电加热器的空调系统应设置无风断电保护。

10.6.6　机房区域安全出口不少于 2 个，且分散布置。出口应设置向疏散方向开启且能自动关闭的防火门，紧急情况下在机房内能向外打开。

10.6.7　配有卤代烷灭火装置的机房，应配置专用空气呼吸器或氧气呼吸器。

10.7　动力及环境监控系统

10.7.1　应具备动力配电、UPS 主机及电池、精密空调、新风、消防、温湿度、漏水及门禁等状态检测功能，在监测达到设定阈值时，应能自动报警，支持短信、电话或邮件报警。

10.7.2　应支持视频图像集中监控管理、机房动力设备和环境状态的集中统一管控。

参 考 文 献

[1] GB/T 2887—2011　计算机场地通用规范
[2] YD/T 2542—2013　电信互联网数据中心（IDC）总体技术要求