

T/ISC

团 体 标 准

T/ISC XXXX—2026

智算中心 OCS 运维安全管理规范

Specification for Operation and Maintenance Security Management of OCS in
Intelligent Computing Centers

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。

2026 - XX - XX 发布

2026 - XX - XX 实施

中国互联网协会 发布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语、定义与缩略语 1

4 缩略语 1

5 基本要求 2

6 系统运行 2

7 系统维护 3

8 安全要求 3

9 故障响应要求 6

附录 A（规范性） OCS 日常维护与变更操作记录表 7

附录 B（规范性） OCS 无损维护操作流程示例 8

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。

本文件由中国互联网协会归口。

本文件起草单位：。

本文件主要起草人：。

智算中心 OCS 运维安全管理规范

1 范围

本文件规定了智算中心OCS的基本要求、系统运行、系统维护、安全要求和故障响应要求。
本文件适用于智算中心OCS运维与安全管理。

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 50174—2017 数据中心设计规范

3 术语、定义与缩略语

下列术语和定义适用于本文件。

3.1

故障域 failure domain

在发生故障或执行运维操作时，受影响的网络资源范围

3.2

光路重构 optical circuit reconfiguration

在不改变物理布线的前提下，通过OCS控制平台对光交换矩阵进行重新编程，实现光连接关系的动态调整过程。

3.3

无损维护 lossless maintenance

在不影响在线业务流量的前提下，对OCS网络进行维护、链路调整或拓扑重构的运维方式。

3.4

数据平面 data plane

OCS网络中，由光交换设备、光纤链路及相关传输资源构成，按照已建立的光路连接关系实现算力业务数据传输与交换的网络功能平面。

3.5

控制平面 control plane

OCS网络中，由控制器、控制协议及相关控制功能模块构成，对光交换网络资源、拓扑连接关系和光路建立、调整及释放过程实施控制的逻辑功能平面。

3.6

光路硬锁定 optical circuit hard lock

OCS网络中，当控制平面完全失效时，光交换设备依据本地保存的最后一次有效光交换矩阵配置，维持现有光交叉连接状态并禁止连接关系变更的一种光路保护机制。

3.7

运维管理平面 operation and management plane

OCS系统中，由管理软件、管理接口及相关功能模块构成，对系统设备、网络资源、运行状态和运维活动实施统一管理的逻辑功能平面。

4 缩略语

下列缩略语适用于本文件。

CPU：中央处理器（Central Processing Unit）

OCS: 光电路交换机 (Optical Circuit Switch)

5 基本要求

5.1 制度要求

5.1.1 应制定 OCS 网络维护计划, 明确维护周期、维护时间窗口、维护人员安排及维护内容, 并对维护活动可能产生的业务影响进行评估和记录。

5.1.2 应建立覆盖 OCS 网络全生命周期的档案管理制度, 对 OCS 的物理连接关系、逻辑拓扑模型以及历史运行数据进行数字化归档, 确保相关信息可查询、可追溯。

5.1.3 档案管理内容宜包括但不限于光纤连接映射关系、光路配置记录、拓扑变更历史及历史流量矩阵等信息, 数据保留周期应不少于 6 个月, 用于支持网络可达性验证、故障定位和拥塞问题溯源。

5.2 人员要求

5.2.1 运维人员应具备光通信、数通网络及智算中心基础设施运维的专业知识, 并经过 OCS 设备厂商或行业组织的专业技术培训, 具备相应的运维能力。

5.2.2 关键运维操作宜实行分级授权或双人操作机制, 并对操作过程进行记录, 以降低误操作风险。

5.2.3 运维团队应每半年至少开展一次应急演练, 覆盖光链路中断、控制器故障和管理通信中断等场景, 并记录告警送达、人员确认、处置启动和业务恢复时间。

5.3 设备运行要求

5.3.1 OCS 设备运行环境温度应保持在 0℃至 35℃范围内, 并满足设备技术规范对湿度和供电及散热的要求。

5.3.2 应对接入 OCS 的数千芯光纤实施标签化、自动化管理。宜采用高密度配线架等方式, 减少人工插拔带来的物理损伤风险。

5.3.3 机房应提供 2N 或者 N+1 的冗余供电条件及精确的温控系统, 确保设备在最优温区工作。

5.3.4 OCS 运维系统应支持对关键光链路性能指标 (包括但不限于位错误率、光功率水平等) 进行实时监测和自动化校验, 确保新建立或重构的逻辑链路在承载业务流量前满足既定的服务等级要求。

6 系统运行

6.1 一般要求

6.1.1 OCS 系统应按照既定的运行策略和运维流程运行, 运维管理平面应与智算中心统一的监控与管理平台对接, 实现 OCS 系统运行状态监测、配置管理及运维操作管理。

6.1.2 OCS 系统运行过程中, 应保持系统配置状态的一致性和可控性, 未经批准不应擅自调整系统参数或网络拓扑。

6.1.3 系统运行状态、关键操作和异常事件应进行记录, 并支持查询与追溯, 以满足运行分析和安全审计的要求。

6.1.4 OCS 系统在运行过程中发生异常时, 应按照预定流程进行处置, 并在必要时触发故障规避或恢复机制, 降低对业务运行的影响。

6.1.5 自动故障检测及保护恢复指标应根据故障类型和业务服务等级分别规定, 并通过测试验证。对于光路径中断故障, 在满业务负载条件下, 自动保护倒换或光路重构恢复时间 (从故障发生至备用光路建立并承载业务流量恢复的端到端时间) 应不大于 30 ms。

6.2 运行环境

6.2.1 OCS 系统运行的机房环境应符合 GB 50174—2017 对数据中心主机房的相关规定, 满足 A 级或 B 级数据中心在温度、湿度、供电、散热及防尘等方面的强制要求。

6.2.2 系统运行环境应具备稳定的电力供应条件, 关键设备宜配置不间断电源或冗余供电系统, 以防止因供电异常导致系统中断。

6.2.3 光纤布线环境应规范、有序, 光纤配线架和光缆资源应统一管理, 避免因环境混乱或标识不清

引发运行风险。

6.2.4 运行环境发生变化或调整时，应评估其对 OCS 系统运行的影响，并采取相应的防护或调整措施。

7 系统维护

7.1 一般要求

7.1.1 无损维护原则：维护前应确认备用路径可用、承载能力满足要求，并完成受影响业务迁移及目标路径排空验证。满足无损维护条件时，应按经验证的流程执行维护；不满足条件时，应经业务影响评估和批准后，在约定维护窗口内实施。各阶段应规定完成条件、超时时间、失败处理及回退措施。

7.1.2 失效安全保障：OCS 系统应具备失效静态保护能力。当控制平面失联或发生故障时，OCS 设备应维持最后一次有效配置对应的光交叉连接状态；当控制平面完全失效时，应支持光路硬锁定机制，防止因控制异常导致已建立的光路连接关系发生非预期变更。

7.1.3 风险控制与分域操作：所有的维护操作应严格限制在单一故障域内（如不超过全网容量的 25%），且在进入下一阶段前必须确认当前操作已成功完成，防止故障连锁反应。

7.2 维护方式

7.2.1 远程巡检与诊断：应依托集中控制与运维平台开展远程巡检，支持实时拓扑感知、链路状态监测和性能分析；宜结合分析工具，对历史流量和路径状态进行回溯，辅助故障定位与根因分析。

7.2.2 现场巡检与作业：当需要进行物理层检查或操作时，应由运维人员进入机房实施现场巡检，重点检查光纤链路受压或弯折情况、设备指示灯状态、风道与散热环境洁净度等远程手段难以感知的内容。

7.3 巡检

7.3.1 巡检计划制定：应根据智算中心的算力任务周期制定年度、季度、月度及周巡检计划。巡检计划应根据智算集群的扩容阶段进行动态调整。

7.3.2 巡检内容宜包括设备运行状态、光链路状态、关键性能指标、告警信息及环境条件等。

7.3.3 巡检宜根据系统规模和运行重要性分为日常巡检、定期巡检和专项巡检，并对巡检结果进行记录和分析。

7.4 维护人员

7.4.1 从事 OCS 系统维护的人员应具备相应的专业能力，熟悉光网络和数据中心运维相关技术。

7.4.2 应明确维护人员的职责分工和权限范围，关键维护操作应由具备相应资质或授权的人员实施。

7.4.3 应定期对维护人员开展技术培训和安全教育，提升其对系统运行状态、故障处理和安全风险的认知能力。

7.4.4 维护人员的操作行为应纳入审计和记录范围，确保维护过程可追溯。

8 安全要求

8.1 网络安全

8.1.1 应实现 OCS 控制平面与业务数据平面的物理或逻辑强隔离。控制信道应走专用带外管理网络，严禁控制流与业务流在同一物理光路中混合传输。

8.1.2 OCS 系统应纳入智算中心统一的网络安全防护体系，合理划分网络边界和安全域，防止未经授权的访问和操作。

8.1.3 应对拓扑重构指令的频次、时段及影响范围进行持续监测。针对短时间内出现的大规模或异常频率的拓扑变更请求，应触发自动拦截机制，并执行二次人工校验或审批流程。

8.2 流量监控

8.2.1 应建立覆盖 OCS 网络流量监控机制，对关键链路和重要业务的流量特征进行监测和分析。

8.2.2 在检测到流量异常或安全风险时，应按照既定流程进行处置，并保留相关记录以备审计。

8.3 数据安全

8.3.1 应对 OCS 系统运行过程中产生的配置数据、运行日志和监控数据进行统一管理，防止数据泄露、篡改或丢失。

8.3.2 应对 OCS 运维系统的访问采用多因素认证。

8.3.3 涉及系统配置和运行状态的关键数据，应采取必要的完整性保护措施，确保数据在存储和传输过程中未被未经授权地修改。

8.4 备份与恢复

8.4.1 极端故障下（如主备控制器双重宕机），系统应在 3 分钟内调用本地最后一次有效缓存完成光路硬锁定。

8.4.2 系统应每日自动备份 OCS 的全局拓扑配置文件及交叉矩阵映射表。备份数据宜存储于安全存储介质中。

8.4.3 备份数据应采取异地或隔离网段安全存储，历史备份数据的保留周期应不少于 6 个月。

8.4.4 运维团队每半年应至少开展一次全面的数据与控制面恢复演练，并输出演练评估报告。

8.5 设备安全

8.5.1 OCS 设备应纳入智算中心统一的资产管理体系，建立设备资产台账，记录设备型号、序列号、部署位置、管理地址、软件版本、控制器归属、端口使用状态、光纤连接关系及责任人等信息，并保持台账与实际部署状态一致。

8.5.2 OCS 设备的安装、迁移、更换、下线和报废应履行审批流程，并对涉及的光路连接关系、控制策略、配置文件和业务影响范围进行评估和记录。

8.5.3 OCS 设备所在机柜、配线区域和管理终端应采取物理访问控制措施。非授权人员不应接触 OCS 设备、光纤配线架、控制器、管理接口及本地维护端口。

8.5.4 OCS 设备本地维护接口应默认关闭或处于受控状态。确需启用本地串口、管理网口、USB 接口或调试接口时，应履行授权审批流程，限定启用时间、操作人员和操作范围，并在维护结束后及时关闭或恢复安全配置。

8.5.5 OCS 设备应禁用不必要的服务、端口和协议。远程管理宜采用加密协议和身份认证机制，不应使用明文协议进行设备管理、配置下发和日志传输。

8.5.6 OCS 设备应使用唯一的管理账号和安全凭证，不应使用默认账号、默认口令或共享账号。设备账号、口令、密钥和证书应按照智算中心统一的身份认证和凭证管理制度进行管理。

8.5.7 OCS 设备的系统软件、固件、控制程序和补丁应通过可信来源获取，并在升级前进行完整性校验、兼容性验证和回退方案确认。未经验证的软件、固件或补丁不应在生产环境中直接部署。

8.5.8 OCS 设备升级、参数调整、控制策略变更和光路重构等操作应纳入变更管理流程。关键操作应执行审批、复核、备份、实施、验证和记录闭环，确保操作过程可追溯。

8.5.9 OCS 设备应具备配置保护能力。设备运行配置、交叉矩阵映射关系、拓扑策略、控制参数和校准参数应定期备份，并防止未经授权的读取、导出、修改或删除。

8.5.10 OCS 设备应具备异常状态保护能力。当控制平面异常、管理链路中断、配置下发失败或控制器不可用时，设备宜保持最后一次有效光路连接状态，避免因控制异常导致数据平面中断或大范围拓扑震荡。

8.5.11 对于 MEMS 类 OCS 设备，应重点防范机械振动、灰尘污染、镜面污染、驱动异常和机械动作寿命衰减等风险。宜对微镜阵列动作次数、驱动电压、切换成功率、插入损耗变化和设备振动状态进行监测，并在达到寿命预警阈值或性能劣化阈值时触发维护流程。

8.5.12 对于硅基波导类 OCS 设备，应重点防范温度漂移、热串扰、片上调谐器老化、环谐振失锁、校准参数异常和静电损伤等风险。宜对片上温度、调谐电流、锁定状态、波长漂移、光功率变化和校准状态进行监测，并在发生失锁、漂移超限或热稳定性异常时触发告警和处置流程。

8.5.13 OCS 设备涉及光纤插拔、端口调整、板卡更换、控制器切换等现场操作时，应执行防静电、防尘、防误插拔和光接口清洁要求。操作前后应核验端口标签、链路状态、光功率、位错误率和业务影响情况。

8.5.14 OCS 设备应防止未经授权的外设接入。生产环境中不宜使用未备案的移动存储介质、调试电脑、转换线缆和测试工具接入 OCS 设备。确需使用时，应进行安全检查、授权审批和操作记录。

8.5.15 OCS 设备下线、返修、替换或报废前，应对设备中的配置文件、日志文件、账号凭证、拓扑数据、校准数据和缓存数据进行清除或脱敏处理，并保留处置记录。

8.6 监控安全

8.6.1 OCS 系统监控应纳入智算中心统一监控体系，覆盖数据平面、控制平面和运维管理平面，形成对设备状态、光链路状态、拓扑状态、控制状态、安全事件和运维操作的持续监测能力。

8.6.2 OCS 监控系统应对关键运行指标进行实时采集和分析，监控内容应包括但不限于光功率、位错误率、插入损耗、链路连通性、端口状态、拓扑变更、控制器状态、管理接口状态、设备温度、供电状态、风扇状态和告警状态。

8.6.3 OCS 监控系统应具备异常检测能力。对光功率突变、位错误率突增、链路频繁抖动、拓扑重构失败、控制指令异常、设备离线、配置变更异常和管理登录异常等事件，应及时产生告警并记录。

8.6.4 OCS 监控系统应对拓扑重构行为进行重点监控，区分策略授权范围内的自动光路重构与人工维护变更。自动重构应校验请求身份、授权范围、配置版本、端口占用及业务约束，异常判定不应仅以重构频次或是否处于维护窗口为依据；人工维护变更应校验审批状态、维护窗口及故障域授权范围。对未经审批、跨故障域重构、配置不一致、端口冲突或与历史基线明显不一致的重构行为，应触发安全告警，必要时执行阻断、二次确认或人工复核。

8.6.5 OCS 监控系统应支持监控数据的完整性保护和访问控制。监控数据、告警数据、日志数据和拓扑状态数据在采集、传输、存储和展示过程中应防止被未经授权地篡改、删除、伪造或泄露。

8.6.6 OCS 监控系统的访问应实行分级授权。不同角色应按照最小权限原则访问监控视图、告警信息、拓扑信息、配置状态和历史数据。涉及拓扑关系、业务承载关系和安全事件的敏感监控信息应限制访问范围。

8.6.7 OCS 监控系统应记录用户登录、查询、导出、告警确认、阈值修改、监控策略调整、静默告警、关闭告警和删除日志等操作，并保留审计记录。

8.6.8 OCS 监控系统的告警阈值、采集频率、告警策略和自动处置策略应纳入变更管理。未经授权不得擅自修改监控策略、关闭关键告警或调整关键阈值。

8.6.9 OCS 监控系统应具备告警分级和关联分析能力。宜根据业务影响范围、故障域、链路重要性、设备类型和历史基线对告警进行分级，减少误报和漏报，并支持对光链路异常、控制面异常和业务流量异常进行关联分析。

8.6.10 OCS 监控系统应具备监控自身安全防护能力。监控平台、采集代理、接口服务、数据库和消息队列等组件应采取身份认证、访问控制、日志审计和安全加固措施，防止监控系统被攻击后影响 OCS 运行安全。

8.6.11 OCS 监控系统与 OCS 设备、控制器及其他运维平台之间的数据接口应采用安全通信机制。跨系统传输监控数据时，应进行身份鉴别和权限校验，防止非法系统接入或伪造监控数据。

8.6.12 OCS 监控系统应具备时间同步能力。设备、控制器、监控平台和日志系统的时间应保持一致，以确保告警、操作、故障和安全事件能够按时间顺序进行关联分析和追溯。

8.6.13 OCS 监控数据应按照数据重要性和审计要求进行保存。关键运行指标、拓扑变更记录、安全告警、故障告警和操作审计日志的保存周期应不少于 6 个月；涉及重大故障、安全事件或争议追溯的数据应根据事件处置需要延长保存周期。

- 8.6.14 对于 MEMS 类 OCS 设备，监控内容宜包括微镜阵列状态、驱动电压、动作次数、切换成功率、插入损耗变化、串扰变化、设备振动状态和机械寿命预警信息。
- 8.6.15 对于硅基波导类 OCS 设备，监控内容宜包括片上温度、调谐电流、锁定状态、波长漂移、热串扰状态、校准状态、片上监测单元状态和调谐器老化趋势。
- 8.6.16 当监控系统检测到影响业务连续性或安全性的重大异常时，应按照本文件第 8 章故障响应要求触发故障分级、告警推送、应急处置和事后闭环流程。

9 故障响应要求

9.1 故障分级要求

- 9.1.1 应根据 OCS 故障对智算业务、网络连通性及系统稳定性的影响程度，建立分级故障响应机制。
- 9.1.2 故障等级可根据对业务影响程度划分，不同等级故障应对应不同的响应时限和处置流程。

9.2 故障检测与告警

- 9.2.1 运维平台应具备毫秒级故障感知能力，能够对光链路中断、光功率异常、位错误率突变以及控制平面异常等事件进行实时检测。
- 9.2.2 光链路中断类（如光信号丢失、端口失效）：毫秒级检测并告警。
- 9.2.3 性能劣化类（如光功率异常、误码率突变）：结合误码统计周期和性能阈值，秒级或亚秒级检测。
- 9.2.4 控制平面异常类（如控制器心跳超时、管理通信中断）：依据心跳周期和超时阈值，在规定时间内检测。
- 9.2.5 故障警告应根据分级自动推送至相关运维人员。

9.3 故障处置与恢复

- 9.3.1 在发生故障时，应按照预定的故障响应流程开展处置，必要时可采取光路重构、链路切换或资源调整等措施。
- 9.3.2 故障恢复完成后，应对系统运行状态进行确认，确保网络功能和性能恢复至正常水平。

9.4 故障后总结与闭环

- 9.4.1 故障处置完成后，应开展故障原因分析，总结故障发生原因、处置过程和存在的问题。
- 9.4.2 应根据分析结果对运行维护策略、配置管理或故障响应流程进行必要的调整和优化。
- 9.4.3 对于影响范围较大或重复发生的故障，应形成标准化分析报告，并作为运维管理改进、系统优化以及运维人员培训的重要参考依据。

附 录 A
(规范性)

OCS 日常维护与变更操作记录表

OCS日常维护与变更操作记录表见表A. 1。

表 A. 1 OCS 日常维护与变更操作记录表

维 护 单号		操 作 时间		维 护 类 型 (例 行 / 变 更 / 应 急)		涉 及 故障域/端 口	
操 作 人/复核人		授 权 审批单号		当前环 境温度/湿 度		业 务 影响评估	
操 作 步骤简述							
执 行 结果验证							
操 作 人签字				复 核 人 /主管签字			

附 录 B
(规范性)
OCS 无损维护操作流程示例

B.1 适用场景

适用于智算中心在不中断算力训练任务的情况下，对局部光纤链路、接口模块进行更换，或对业务流进行重新调度的场景。

B.2 操作流程步骤

OCS无损维护宜遵循以下5步闭环流程。

- a) 预检与评估：检查控制平面状态及 CPU/内存利用率是否正常；检查目标链路当前流量状态与历史基线；确认备用链路容量满足流量承接需求。
 - b) 流量静默：联动数据中心 SDN 控制器，通过路由调整或流控机制，将即将维护的光链路上的算力业务流量平滑迁移至备用网络路径；确认目标端口流量归零。
 - c) 隔离与重构：锁定目标 OCS 端口的软件状态；执行物理层面的硬件拔插、光纤更换，或者通过控制器下发新的拓扑重构配置指令。
 - d) 验证与校验。
 - 1) 物理层校验：检查新光路的光功率异常告警是否消除，插入损耗是否在技术规范以内（如小于 3 dB）。
 - 2) 逻辑层校验：发送特定探测报文，确认端到端连通性和位错误率达标。
 - e) 流量恢复（Traffic Restore）：解除 SDN 流量隔离策略，使算力业务流量重新切回或分布至新的 OCS 链路上；观测 5—15 分钟业务运行状态，确认无丢包、无降级后关闭维护工单。
-