ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

T/CAICI

中 国 通 信 企 业 协 会 团 体 标 准

T/CAICI XXXX—XXXX

智能计算系统集成技术规范

Technical Specification for System Integration of Intelligent Computing

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国通信企业协会　　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。

本文件由中国通信企业协会标准化管理委员会提出并归口。

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。

本文件起草单位：中国移动通信集团设计院有限公司、中盈优创资讯科技有限公司、神州数码系统集成服务有限公司、亚信科技(中国)有限公司、北京华胜天成科技股份有限公司、吉林吉大通信设计院股份有限公司

本文件主要起草人：周维、杨同鹏、杨洋、肖伟、张培才、乔宏生、钱云鼎、田科伟、黄健、王士迪、吕诗元、张攀、周洋、许碧洲、田盛泰、张敬琛

本文件为中国通信企业协会首次发布。

引　　言

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。

智能计算系统集成技术规范

1 范围

本标准规定了智能计算系统集成（下文简称“智算系统集成”或“智算集成”）工作的主要细则、流程、步骤与相关操作规范，供系统集成专业人员从事智能计算系统集成工作使用，适用于智能计算系统集成作业。

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。

表2.1 规范性引用文件表

序号	标准编号	标准名称	发布单位
1	GB 50689-2011	通信局(站)防雷与接地工程设计规范	中华人民共和国住房和城乡建设部
2	YD 5054-2019	通信建筑抗震设防分类标准	中华人民共和国工业和信息化部
3	YD 5003-2014	通信建筑工程设计规范	中华人民共和国工业和信息化部
4	YD5059-2005	电信设备安装抗震设计规范	中华人民共和国工业和信息化部

3 术语和定义

下列术语和定义适用于本文件。

表3.1 术语、定义和缩略语说明

词语	解释
HLD	High Level Design，高阶设计文件
LLD	Low Level Design，低阶设计文件
AI	Artificial Intelligence，人工智能
GPU	Graphics Processing Unit，图形处理单元
NPU	Neural Processing Unit，神经处理单元
CPU	Central Processing Unit，中央处理器
NVMe SSD	Non-Volatile Memory Express Solid State Drive，非易失性内存标准固态硬盘
FPGA	Field-Programmable Gate Array，现场可编程门阵列
ASIC	Application-Specific Integrated Circuit，专用集成电路
KVM	Kernel-based Virtual Machine，基于内核的虚拟机
HDD	Hard Disk Drive，机械硬盘
RDMA	Remote Direct Memory Access，远程直接内存访问

词语	解释
IOPS	Input/Output Operations Per Second，每秒输入/输出操作数
IB	InfiniBand，一种参数面组组网技术
RoCE	RDMA over Converged Ethernet，一种参数面组网技术
VLAN	Virtual Local Area Network，虚拟局域网
VxLAN	Virtual Extensible LAN，虚拟可扩展局域网
IPS	Intrusion Prevention System，入侵防御系统
IDS	Intrusion Detection System，入侵检测系统
DDoS	Distributed Denial of Service，分布式拒绝服务
HostOS	Host Operating System，主机操作系统
GuestOS	Guest Operating System，客户操作系统
TCP/IP	Transmission Control Protocol/Internet Protocol，传输控制协议/互联网协议
BIOS	Basic Input Output System，基本输入输出系统
RAID	Redundant Arrays of Independent Disks，磁盘阵列
IO	Input/Output，输入/输出
NTP	Network Time Protocol，网络时间协议
DNS	Domain Name System，域名系统
AZ	Availability Zone，可用区
HA	High Availability，高可用性
POD	Point of Delivery，一般理解为云资源池的最小交付单元
DWPD	Drive Writes Per Day，每天全盘写入次数
API	Application Programming Interface，应用程序编程接口
SDK	Software Development Kit，软件开发工具包
POSIX	Portable Operating System Interface，可移植操作系统接口
EC	Erasure Coding，纠删码
RBAC	Role-Based Access Control，基于角色的访问控制
LDAP	Lightweight Directory Access Protocol，轻量级目录访问协议
AD	Active Directory，活动目录
ITSM	IT Service Management，信息技术服务管理
REST API	Representational State Transfer Application Programming Interface，表述性状态转移应用程序编程接口
PFC	Priority-based Flow Control，基于优先级的流量控制
MC-LAG	Multi-Chassis Link Aggregation Group，多机箱链路聚合组
ISSU	In-Service Software Upgrade，在线软件升级
IPMI	Intelligent Platform Management Interface，智能平台管理接口
OSPF	Open Shortest Path First，开放最短路径优先
BGP	Border Gateway Protocol，边界网关协议
ECMP	Equal-cost multi-path routing，等价多路径路由
ECN	Explicit Congestion Notification，显式拥塞通知
VRF	Virtual Routing and Forwarding，虚拟路由和转发
DPI	Deep Packet Inspection，深度包检测
SDN	Software-Defined Networking，软件定义网络
QoS	Quality of Service，服务质量

词语	解释
SR-IOV	Single Root I/O Virtualization，单根 I/O 虚拟化
DPDK	Data Plane Development Kit，数据平面开发套件
iSER	iSCSI Extensions for RDMA，iSCSI 扩展用于远程直接内存访问
SRP	SCSI RDMA Protocol，SCSI 远程直接内存访问协议
ACL	Access Control List，访问控制列表
CUDA	Compute Unified Device Architecture，统一计算设备架构
CANN	Compute Architecture for Neural Networks，神经网络计算架构
PDU	Power Distribution Unit，电源分配单元
OS	Operating System，操作系统
MTU	Maximum Transmission Unit，最大传输单元
LACP	Link Aggregation Control Protocol，链路聚合控制协议
HCA	Host Channel Adapter，主机通道适配器
CVE	Common Vulnerabilities and Exposures，通用漏洞和暴露
SSL	Secure Sockets Layer，安全套接层

4 智算系统集成工作范围要求

智能计算系统集成工作主要针对工程设计的延伸细化与落地实施，包括集成方案设计、辅材/辅料供应、工程实施监控与督导、设备配置与调测、测试与验收等步骤。

图 4.1 智算系统集成工作范围及流程示意图

4.1 集成方案设计

1. 编制智算中心集成实施方案，包括项目进度管理、采购管理、质量管理、成本管理、风险管理等内容。集成实施方案对项目实施进行进行总体控制，保障项目成果按照预定目标交付。

2. 编制智算中心集成高阶设计方案 HLD 及低阶设计方案 LLD，包括计算资源规划、存储资源规划、网络资源规划、安全规划等内容。集成详细设计方案是项目交付的核心技术数据，用于指导综合布

线、设备配置、资源发放、对接联调、安全防护等环节的工作。

4.2 线缆辅材提供

1. 根据工程实际需求，依据工程规范要求，提供工程涉及的硬件设备连接所需的通信线缆及接头，主要包括：尾纤、网线等。常见的尾纤类型包括：多模/单模双芯 LC-LC 光纤、单模/多模双芯 LC-FC 光纤、多模 MPO-MPO 光纤等；常见的网线类型包括：六类屏蔽双绞线、六类非屏蔽双绞线等。设备连接范围包括：普通计算服务器至组网设备互联、智算服务器至组网设备互联、存储服务器至组网设备互联、组网设备间级联、组网设备与安全设备互联、成对组网/安全设备间互联等；

2. 提供工程辅料，包括光衰、光纤套管、绕纤筒、下纤槽、水晶头、工业连接器、标签、热缩管、扎带、铜鼻子、缠绕管、接线柱、理线架、保温棉等工程所需的辅料；

3. 根据工程实际需求，提供、制作工程项目所有标签，并根据项目技术规范要求生成设备二维码等编号信息，一并制作到标签中。

4.3 工程实施监控与督导

1. 设备到货监控：根据总体工期安排，严格把控各软、硬件厂商设备到货进度，对到货延迟风险提前提出预警，并协调相关资源推进到货时间；

2. 施工进度监控：根据总体工期安排，严格把控施工单位、软硬件厂家施工步骤及时间，识别项目延期风险，合理调度资源，保障施工进度满足总体要求。

3. 施工质量监控：监控施工过程中的质量控制措施，确保所有设备的安装符合行业标准和项目要求；

4. 安全生成监控：确保施工现场遵守安全规程，预防事故的发生；

5. 设备安装督导：督导工程中购买的所有硬件设备安装、上架、上电，为现场施工人员提供技术指导和支持，确保按照设计图纸和技术规范进行安装作业；

6. 设备配置督导：督导软、硬件设备厂家初始化配置及作业，确保按照设计图纸和技术规范进行设备配置。

4.4 设备配置调测

1. 确保本工程中所有硬件设备的可用性，确保所有硬件设备的互联及功能要求达到软件部署的条件和系统建设的总体目标。负责解决计算子系统、网络子系统、存储子系统、安全子系统等各硬件设备安装、配置及调测出现的问题，并作为产生任何问题时的第一响应单位，协调、督导相关单位完成问题处理；

2. 完成本工程中所有软件系统的安装、部署、调试、系统测试等工作，确保软件环境满足云、容器等资源调度的要求，确保软件环境满足业务系统，例如模型训练、模型推理等，开展实际业务部署的

需求。

4.5 测试与验收

1. 编制测试验收方案：编制测试验收计划，制定测试用例，定义测试验收标准，用于指导整体测试验收工作；

2. 开展测试验收工作：完成测试验收环境的准备，包括测试工具的部署、对接等。根据测试验收方案，展开所有测试用例，完成包括自动化测试及手动测试在内的所有测试工作。智算系统集成方案设计要求。

5 智算系统集成方案设计要求

5.1 总体技术要求

智算系统需要具备强大的并行计算、分布式存储、高速互联和安全管理能力，以支持大规模 AI 训练和推理任务的开展。一般，计算架构上需要使用 GPU、NPU 等专用硬件，数据存储采用分布式存储优化非结构化数据处理，网络需满足高速互联和低延迟以支持大规模分布式计算，安全方面需要从硬件到软件、从数据到模型的全方位防护。

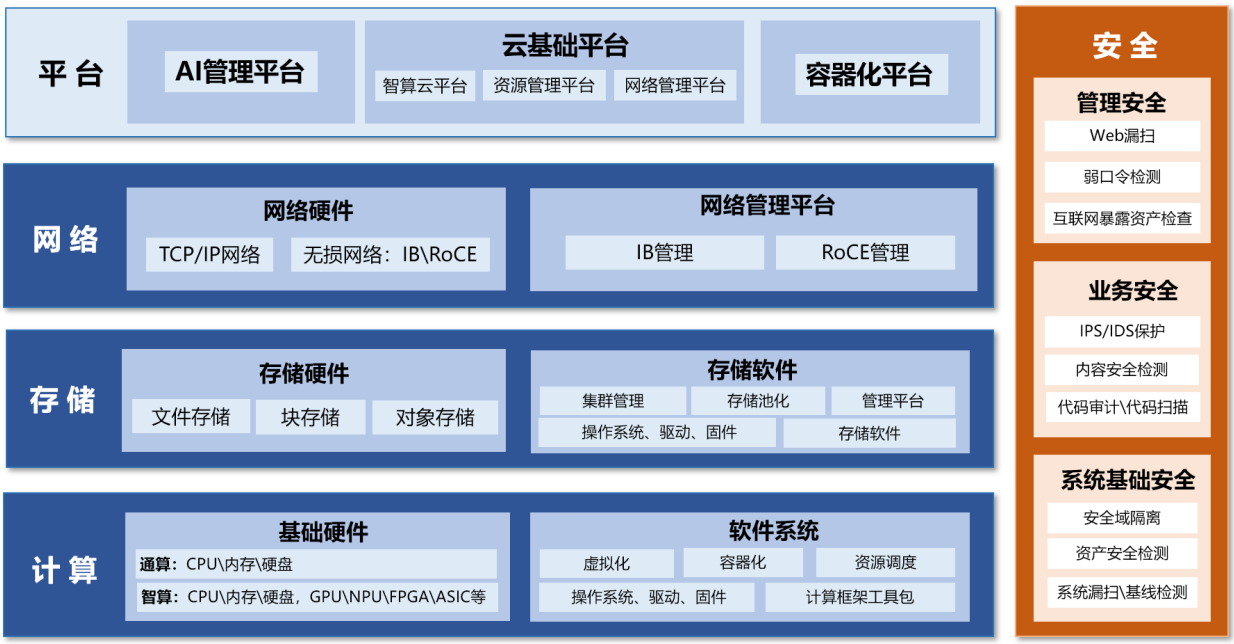

图 5.1 智算系统集成架构图

1. 计算子系统

计算子系统是智算的核心，直接影响系统性能与效率。它需整合多元算力资源，并实现智能调度，应满足大规模训练和推理的需求，结合云计算、边缘计算。同时应支持算力资源池化技术，以支持灵活

的资源管理与弹性分配。

(1) 计算子系统硬件资源

计算子系统硬件资源一般采用高性能多核 CPU，配置高速大容量内存以支撑大数据处理，结合本地 NVMe SSD 与分布式存储提升读写效率，整合高性能 GPU/NPU/FPGA/ASIC 等多元算力资源，为上层训练/推理业务提供基础的算力资源。

(2) 计算子系统软件资源

计算子系统软件资源一般基于主流 Linux 操作系统，运行虚拟化与容器化工具平台，部署 KVM、Docker、Kubernetes 等实现资源隔离和调度，结合 AI 平台实现一站式 AI 调度与运维管理服务，为上层训练/推理业务提供基础的软件环境。

(3) 计算资源建设方案

注重资源池化，实现统一管理 CPU、GPU、FPGA、ASIC 等异构资源，支持横向与纵向扩展；基于算力平台部署，如 Kubernetes、Openstack 等调度系统与 AI 平台，实现集中管理和快速开发部署。

2. 存储子系统

智算的存储系统需同时满足超高吞吐、低延迟、海量扩展性以及与计算架构深度协同的需求。应用需求包括大文件连续读写、小文件高频随机访问、GPU Direct 支持、热/温/冷数据分层存储、自动数据迁移等业务场景，对存储子系统设计提出较大挑战。

一般情况下，智算中心存储系统应采用分布式架构，通过多节点分散存储数据，确保高扩展性和容错性，并支持文件存储（如模型配置、脚本）和对象存储（如训练数据集、推理结果），实现数据全流程无缝对接。

(1) 分级存储体系

- 热数据层：全闪存（NVMe/SSD），低延迟，用于高频访问数据（训练集、Checkpoint）；
- 温数据层：混闪（HDD+SSD），平衡性能与成本，存储中间结果和历史日志；
- 冷数据层：大容量冷存（磁带/云归档），存放低频访问数据（备份、归档）。

(2) 高性能存储网络

采用 RDMA（RoCE/InfiniBand），提供高带宽、低时延（微秒级），减少 GPU 等待时间。多轨冗余设计，避免单点故障，并优化流量调度（如训练数据优先传输）。

(3) 核心性能与容量要求

高吞吐与高 IOPS，满足大规模数据并行加载。线性扩展至 PB~EB 级，支持按需弹性扩容。

(4) 集群规划

高性能集群（全闪存）、大容量集群（混闪）、归档集群（冷存），按业务需求划分存储池，确保负载均衡与高可用。该架构通过“分布式存储+智能分层+无损网络”，全面支撑 AI 训练、推理及数据全生命周期管理，兼顾性能、成本与可靠性。

3. 网络子系统

智算网络需要满足无丢包、低延迟、大带宽通信的需求，负责智算集群通信及数据存储的网络平面一般采用 InfiniBand、RoCEv2 等高速网络协议/技术。

(1) 网络架构应采用分层分域设计

根据不同的功能划分多个层级，如接入层、核心层、出口层等；根据业务类型划分多个区域，如管理平面、业务平面、存储平面、参数平面、数据平面等。

(2) 网络拓扑

通常采用 Clos、Fat-Tree、Torus、Dragonfly 等。

(3) 计算网络

计算节点之间互联，根据业务类型可选用以太网络，或支持 RDMA 技术的 InfiniBand 或 RoCE 等。

(4) 存储网络

连接计算节点和存储系统，根据业务类型可选用以太网络，或支持 RDMA 技术的 InfiniBand 或 RoCE 等。

(5) 管理网络

用于系统管理、监控和部署，通常采用以太网络。通常分为带外和带内两种类型。

带外网络用于服务器、网络设备和其它专用设备的硬件管理，通过物理或逻辑隔离实现设备硬件层的远程管理。

带内网络用于服务器、网络设备和其它专用设备系统或应用层面的管理。

4. 安全子系统

智算对安全子系统要求涵盖系统、业务和管理三方面：系统层通过漏洞管理、基线加固和网络隔离构建防御；业务层确保内容合规、代码安全和入侵防护；管理层强化认证和暴露面管控，形成检测-防护-监控闭环，实现全维度安全保障。

(1) 系统基础安全

系统基础安全防护围绕漏洞管理、基线加固和网络隔离展开，构建纵深防御体系。

漏洞与暴露面管理，使用漏扫工具检测系统漏洞（如权限缺陷、访问控制问题），重点扫描虚拟化/容器平台风险（如目录遍历）。定期探测互联网暴露资产（IP、端口），及时收敛攻击面。

安全基线与主机防护，通过基线检查关闭非必要服务和端口，定期修补主机漏洞。部署实时防护（如入侵检测、防病毒）提升动态防御能力。

安全域隔离，划分安全域（如 DMZ、内网）并设置差异化的访问策略。基于业务需求配置防火墙规则，限制横向访问。

(2) 业务安全

业务安全防护聚焦内容合规、代码安全和入侵防御三大核心。

内容与数据安全，检测敏感数据防止泄露，动态监控关键页面合规性，审计代码中的硬编码密码、不安全引用及开源组件漏洞（关联 CVE 编号）。

代码安全管控，在部署前扫描源代码和开源组件，识别漏洞并修复，检测非登录状态下的接口暴露风险及后台程序安全性。

入侵防御与审计，通过 IPS/IDS 划分可信区域，配置策略模板阻断攻击，记录系统日志，确保安全事件可追溯。

(3) 管理安全

管理安全重点围绕身份认证与资产暴露面管控展开。

账户安全强化，通过弱口令检测工具强制密码复杂度与有效期，禁用常见弱密码，采用非暴力方式检查网络资产密码安全，杜绝明文存储/传输。

互联网资产风险管控，动态探测公网暴露资产（IP/域名），自动化发现潜在风险点。限制安全检测平台的公网直连，严格划分安全域。支持多网段并行扫描与 SSL 加密通信，保障检测过程安全性。

5.2 计算方案技术要求

计算方案需支持异构计算，高效整合 CPU、GPU、NPU 等多元算力资源，并实现智能调度。同时，计算方案应满足大规模深度学习训练与推理优化的需求，通过算力资源池化技术，将分散的物理计算资源虚拟化为统一的逻辑资源池，以支持灵活的资源管理与弹性分配。

5.2.1 硬件方案

1. CPU：计算/训练/推理节点服务器应采用高性能多核处理器，支持 x86_64、ARM64 或 RISC-V 架构，满足大规模计算任务需求。

2. GPU：训练/推理节点服务器应支持高性能 GPU 加速计算，采用如英伟达 H100、华为昇腾 910 等硬件系统，满足智算中心训练或推理的算力需求。

3. 内存：训练/推理节点服务器应支持大容量高速内存，满足大规模数据处理需求。

4. 存储：计算/训练/推理节点服务器应支持本地高速存储，如 NVMe SSD 等；支持远端高性能存储，如分布式块存储、分布式文件存储等，确保数据读写高效性。

5. 网络：常规 TCP/IP 协议栈为所有节点必须支持的技术能力，按需匹配接口速率；训练/推理节点服务器应支持高速无损网络，如 InfiniBand、RoCEv2 等，确保计算节点间通信无丢包、低延迟、高带宽。

5.2.2 软件方案

1. 服务器基础设置

(1) BIOS 规划：规划主机启动方式、CPU 休眠模式、能效方案、CPU 自动调频、超线程、超

频等信息；

(2) RAID 规划：规划主机 RAID 的级别、成员盘数、条带大小、读策略、写策略、IO 策略、物理盘缓存状态、访问策略、初始化类型等信息；

2. 服务器操作系统

(1) 基础信息：规划主机操作系统版本、内核版本、CPU 架构、主机命名规则、安装模式等信息；

(2) 系统参数：规划主机操作系统分区方案、Swap 空间、时区、NTP、DNS、字符编码、kdump 状态、图形界面、远程登录等信息；

3. 虚拟化及资源调度平台规划：利用虚拟化及容器技术，如 KVM、XEN、Dockers 等，将物理资源抽象成逻辑资源，并利用调度平台，如 OpenStack、ZStack、Kubernetes 等，通过统一接口自动化管理对应的逻辑资源，以便于业务系统的调度与应用。规划过程中主要涉及智算云平台 Region、AZ、HA 等规划，智算容器集群 POD 等规划，分权分域规划，系统南北向接口对接规划等内容；

4. AI 平台规划：基于云计算技术，提供人工智能相关服务和解决方案的平台。规划过程中主要涉及资源配置规划、逻辑网络规划、系统对接规划等内容。

5.3 存储方案技术要求

5.3.1 硬件方案

1. 架构规划

应使用分布式存储架构，支持文件、对象、块等协议。元数据服务需具备高吞吐量和低延迟，支持海量小文件（百万至十亿级）高效访问。支持通过单一命名空间统一提供文件、对象、块服务，简化数据管理和访问。

2. 集群规划

(1) 高性能集群：采用全闪存节点 NVMe SSD，重点保障存储性能；

(2) 大容量集群：采用混闪节点 SSD + HDD，兼顾存储性能与容量；

(3) 归档集群：独立冷存设备磁带库（LTO-9+）或高密蓝光存储，重点保障存储容量。

3. 存储网络

(1) 网络架构需为无阻塞 CLOS 或 Fat-Tree 结构；

(2) 推荐使用 RDMA 网络：≥100Gbps 单网卡速率，智能无损网络（RoCEv2/InfiniBand）组网。使用专用 RDMA 网卡（支持 GPU Direct Storage），多轨冗余交换机；

(3) 可以使用 TCP/IP 网络：≥25Gbps 单网卡速率，通过端口绑定等技术提高带宽和冗余。

4. 扩展性设计

应支持在线增删节点，容量弹性扩展至 EB 级，满足容量需求和性能的线性增长。

5.3.2 软件方案

1. 存储协议与互通
   (1) 支持文件存储与对象存储协议；
   (2) 支持通过控制台、API、SDK、命令行等方式进行存储资源操作，可以根据需求进行切换；
   (3) 支持标准的文件系统接口；
   (4) 支持高性能并行文件系统协议。
2. 智能分层体系
   (1) 存储池分级
   - 热数据层（全闪存池）：存储训练集/Checkpoint；
   - 温数据层（混闪池）：存储日志/中间结果；
   - 冷数据层（归档池）：存储备份/归档。

   (2) 自动迁移：自动迁移策略应支持基于多种条件组合（如访问频率、文件大小、文件类型、用户/项目标签、创建时间）进行细粒度设定。
3. 数据保护功能
   (1) 支持灵活配置不同业务或目录的数据保护策略，如副本数、EC 策略、快照策略等；
   (2) 支持数据生命周期管理，如自动迁移规则编排等；
   (3) 支持效率优化，如实时压缩、全局去重等。
4. 安全及合规
   (1) 权限控制：RBAC 角色策略（管理员/用户/审计员），支持与 LDAP/AD 等外部认证系统集成，实现统一身份管理；
   (2) 审计合规：支持全量操作日志记录，保留时限不小于 1 年。
5. 管理平台
   (1) 应采用集中控制台功能；
   (2) 具备实时监控（带宽/IOPS/延迟热力图等）能力；
   (3) 支持自动故障切换与告警，支持与主流 ITSM 平台集成。

5.4 网络方案技术要求

5.4.1 网络架构要求

1. 总体网络架构要求
   (1) 智算系统网络架构宜采用分层结构，网络架构可分为出口层、核心层、智算集群网络等三层架构，对于小规模智算系统，可核心层和智算集群网络可合并为一层；
   (2) 出口层负责智算系统内部和外部网络互联互通，对外完成与外部设备高速互联，对内负责

与核心层交换设备互联，并对内网和外网的路由信息进行转换和维护。出口层根据安全需求可部署防火墙、流量清洗等设备；

(3) 核心层实现多个 POD 之间的互联互通，并将访问外部网络的流量进行汇聚，送往出口层；

(4) 智算集群网络实现智算集群的建立，提供训练智算资源或是推理智算资源；

(5) 智算系统宜根据网络用途分为不同的网络平面，可分为参数面网络、存储面网络、业务面网络、带外管理面网络等，不同的网络平面根据集群规模情况可进行物理隔离或是逻辑隔离；

(6) 如果需要进行双机集群推理，需要为每台推理服务器的智算网卡配置参数面网络，用于服务器间数据同步，单机推理时可无需连线；

(7) 参数面网络协议应根据设计要求选择 IB 协议或是 RoCE v2。

2. RoCE v2 参数面网络架构技术要求

(1) 参数面网络应部署为专用网络，在网络层设备上不需要和其它网络相连；

(2) 大中规模参数面网络场景采用两层或多层无阻塞网络 Fat-Tree（胖树），小规模场景可以采用一层网络组网；

(3) 参数面网络应采用无阻塞 1:1 无收敛网络架构，即 Leaf 交换机上行不收敛，即 Leaf 交换机上行总带宽不低于下行总带宽；

(4) 对同一台 Leaf 交换机应保证与每台 Spine 交换机的连接数相同；

(5) Spine 的总端口数大于等于 Leaf 的总上行端口数；

(6) 每台 Leaf 与每台 Spine 的链路数宜为偶数，实现更好的负载均衡效果；

(7) 每台 Leaf 交换机宜独立部署；

(8) Leaf 和 Spine 之间采用 Fullmesh 全连接，提供网络负载均衡。

3. IB 参数面网络架构技术要求

(1) 参数面网络应部署为专用网络，在网络层设备上不需要和其它网络相连；

(2) 大中规模参数面网络场景采用两层或多层无阻塞网络 Fat-Tree（胖树），小规模场景可以采用一层网络组网；

(3) 参数面网络应采用无阻塞 1:1 无收敛网络架构，即 Leaf 交换机上行不收敛，即 Leaf 交换机上行总带宽不低于下行总带宽；

(4) 对同一台 Leaf 交换机应保证与每台 Spine 交换机的连接数相同；

(5) Spine 的总端口数大于等于 Leaf 的总上行端口数；

(6) 每台 Leaf 与每台 Spine 的链路数宜为偶数，实现更好的负载均衡效果；

(7) 每台 Leaf 交换机宜独立部署；

(8) Leaf 和 Spine 之间采用 Fullmesh 全连接，提供网络负载均衡；

(9) IB 网络应多轨道组网方式，即服器上同一 GPU 编号对应的网卡上联到同一台 ToR 交换机；

(10) IB 网络子网管理器 SM（Subnet Manager）宜设置在 IB 网络管理服务器上，如果没有单独的 IB 网络管理服务器，子网管理器可设置在服务器或是网络设备上；

(11) IB 网络子网管理器节 SM（Subnet Manager）点宜部署多个（主备模式），避免单点故障。

4. 业务网络平面架构技术要求

(1) 接入层业务网络宜采用双机冗余结构，双机多链路互联，应支持跨机箱链路捆绑，可使用 MC-LAG 技术或是堆叠技术，如果采用堆叠技术，应支持 ISSU 并能在现网应用；

(2) 根据智算集群规模可业务网络汇聚层或是核心交换机。

5. 存储网络平面架构技术要求

(1) 存储网络平面采用传统 TCP/IP 协议：存储网络接入层宜采用双机冗余结构，双机多链路互联，应支持跨机箱链路捆绑，可使用 MC-LAG 技术或是堆叠技术，如果采用堆叠技术，应支持 ISSU 并能在现网应用；大中型网络规模应设置存储汇聚交换机，存储汇聚交换机宜成对部署；小规模架构下，可以不配置汇聚层；

(2) 存储网络平面采用 RoCE 协议：存储网络接入层宜采用双机冗余结构，双机间通过多条 RDMA 链路互联，应采用支持基于 RDMA 的跨机箱链路聚合技术，可使用 MC-LAG 技术或是堆叠技术，如果采用堆叠技术，应支持 ISSU 并能在现网应用，应全面支持并正确配置保障 RoCE 无损特性的关键机制。大中型网络应设置专用的 RoCE 存储汇聚交换机，并成对部署，形成冗余核心；小规模架构下，可不配置独立汇聚层，应确保接入层具备足够的无阻塞带宽和强大的流量控制能力；

(3) 存储网络平面采用传统 IB 协议：IB Fabric 本身设计为无单点故障的网状结构，通过足够的物理路径和子网管理器配置实现高可用。在大中型网络规模中应部署核心交换机，形成非阻塞的 Fabric 骨干，核心层提供边缘交换机间的全连接和高带宽；在小规模架构下，可以不配置独立核心层，采用边缘交换机直连或简单树状结构，应确保拓扑满足带宽和冗余需求。

6. 带外管理网络平面架构技术要求

(1) 带外管理接入交换机千兆交换机单机部署；

(2) 大中型网络规模应设置管理汇聚交换机，管理汇聚交换机宜成对部署；小规模架构下，可以不配置带外管理汇聚，业务管理汇聚可以和带外管理汇聚合并。

5.4.2 路由协议要求

通过现有网络内路由运行状况并参考现有网络架构，从管理和技术两个方面选择路由协议。路由协议的选择应遵循以下原则：

- 管理上层次分明，局部的变动不影响上层路由配置和全局路由配置；
- 技术上应尽量简单、灵活，以提高路由器的处理效率；
- 能够反映出整个网络的层次结构，并与自治域、各子网的 IP 地址分配相结合，做到合理的路由聚合，减少路由表的长度，减轻路由更新给网络带来的负荷。

根据以上原则，不同网络平面以及不同网络层级在路由协议选择与配置过程中，需要重点关注以下内容。

1. RoCE v2 参数面路由协议要求

(3) Leaf 和 Spine 交换机宜配置动态路由协议（如 OSPF、BGP）；

(4) 路由协议的收敛时间应小于 RoCE 的超时重传时间（通常为微秒级），避免因路由切换导致丢包或连接中断。可启用 OSPF 的 Fast Hello 或 BGP 的 Graceful Restart 等特性，缩短收敛时间；

(5) 通过 ECMP（等价多路径）的对称哈希策略实现路径一致性，应配置交换机使用五元组哈希（源/目的 IP、端口、协议），确保同一流的多包走同一路径。禁用基于随机或简单轮询的负载均衡，避免哈希碰撞引发流量不均；

(6) 使用动态路由协议，应与 ECN（显式拥塞通知）、PFC（优先级流量控制）联动，确保路由路径避开拥塞节点。

2. IB 参数面路由协议要求

(1) 路由算法选择支持 minhop（默认）、updn（分层路由）、ftree（胖树优化）等算法，应根据拓扑结构选择；

(2) 在稳定拓扑中应采用静态路由表，禁用动态路由更新，减少 SM 的计算开销。

3. 出口层路由协议要求

(1) 出口路由设备到互联网设备之间宜采用外部动态路由协议；

(2) 出口层设备之间可采用内部动态路由协议或是静态路由协议。

4. 核心层路由协议要求

(1) 核心层设备上联出口层设备宜采用内部动态路由协议；

(2) 核心层设备下联智算集群设备可采用内部动态路由协议或是静态路由协议。

5. 接入层路由协议要求

(1) 成对设置的接入交换机设备上联可采用内部动态路由协议或是静态路由协议，下联宜采用堆叠或 M-lag 方式部署。

5.5 安全方案技术要求

5.5.1 系统基础安全

1. 安全域划分：为满足不同应用系统对网络接入的不同安全隔离要求，根据业务系统的不同安全等级，对资源池内的资源划分安全域分区，将一个资源池划分为不同的子集合。资源池的同一数据中心内的资源划分为互联网接入域、核心交换域、业务数据域和管理维护域等不同区域。

2. 安全补丁：通过集中安全补丁管理策略，来实现补丁的自动分发和安装，及时保障平台各组件的安全。

3. 硬件安全防护系统：通过部署防火墙来实现不同的安全等级，部署抗 DDoS 实现外部流量的攻击拦截，配置 IPS 实现跨域访问的入侵检测。

4. 虚拟化平台安全：针对虚拟化平台，如 Host OS、Hypervisor、中间件、应用软件等，进行安全加固，关闭不需要的端口和进程，减少系统威胁暴露风险。

5. 容器安全：主要包括容器所在主机安全、容器守护进程安全、容器运行安全、容器镜像安全、容器网络安全、容器编排和管理安全等相关技术要求。

5.5.2 业务安全

1. VxLAN/VRF 隔离：安全域分区间通过 VLAN 或 VxLAN 隔离二层流量，通过 VRF 隔离三层流量，按需部署互访策略。

2. 虚拟机隔离：为了保护虚拟机不同租户的数据安全性，需做好虚拟机之间各种资源的隔离来避免数据干扰，包括 vCPU 隔离、内存隔离和网络 I/O 隔离等。

3. 虚拟防火墙：采用虚拟防火墙技术可以过滤有害访问流量并支持控制列表访问，从而保护虚拟机及用户数据。

4. 业务安全软件：通过部署 Web 应用防护、云堡垒、云防火墙、数据安全系统、云安全中心等系统提供业务安全保障。

5. 数据安全：从数据采集安全、数据存储安全、数据传输安全、数据使用安全、数据共享安全、数据销毁安全等维度保障数据安全。

6. 运维安全：通过部署集中日志管理平台来实现审计和检测层面的安全性，同时部署 DPI 等软件来实现运维监控安全。

5.5.3 管理安全

1. 口令管理：口令设置应满足一定复杂性要求，定期更换，且口令保存的过程中应使用加密存储方式。

2. 用户认证：利用多因素认证、单点登录、认证日志记录等方式，保障用户认证安全。

3. 访问控制：基于权限最小化原则，根据用户的角色分配不同的权限，制定严格的访问控制策略。

4. 数据安全：对敏感数据进行加密存储和传输，定期对系统数据进行备份，对显示给用户的数据进行脱敏处理，保护数据安全。

5. 网络安全：在系统与外部网络之间设置防火墙，对不同安全级别的网络进行隔离，部署入侵检测与防御系统，实时监测网络流量，保障网络安全。

6. 安全审计：记录系统的各种安全事件和操作行为，定期对审计日志进行分析，对安全事件进行跟踪调查，确定事件的责任人，并采取相应的措施进行问责。

6 智算系统集成对接要求

6.1 项目实施对接要求

智算集成单位需参与工程整体流程，涉及到与设计单位、施工单位、监理单位、设备厂家等多方合作，全面负责组织与协调设备供应商完成智算集成工作，组织协调本项目各硬件设备集成过程中出现的问题，各软件安装联调过程中出现的问题，并作为整体系统产生任何问题时的第一响应方。智算集成单位主要负责内容及分工如下：

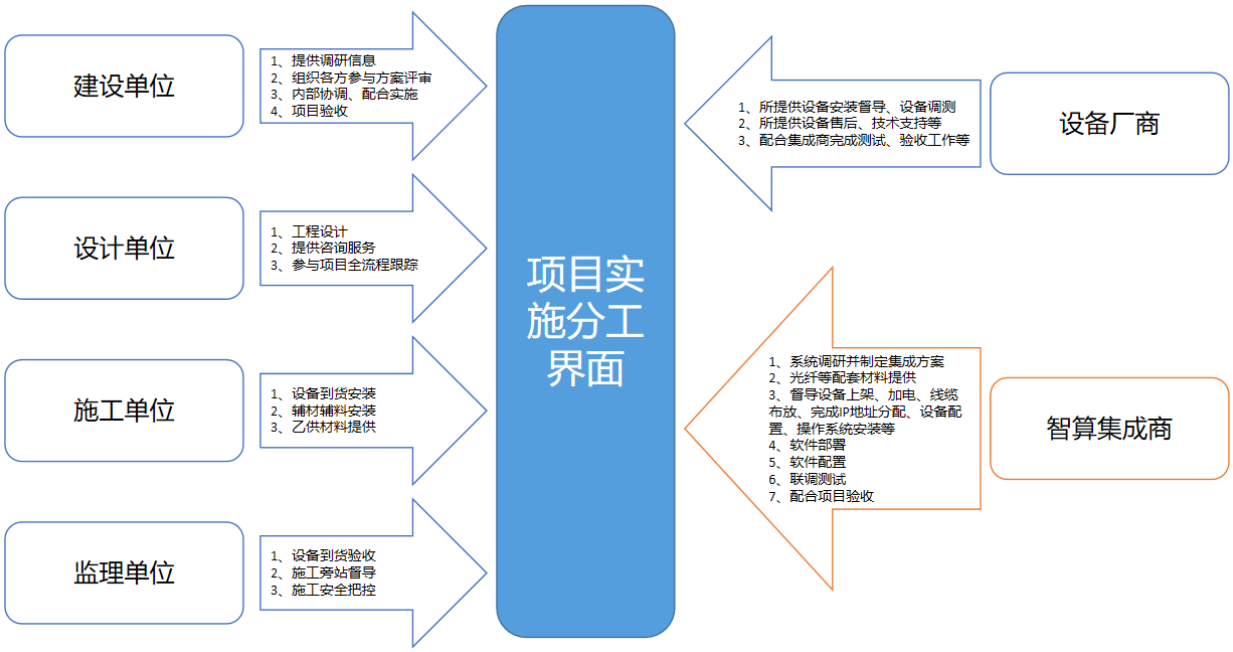

图 6.1 工程分工界面

1. 与建设单位分工界面

建设单位负责：提供项目基本情况信息，组织各方参与方案评审，项目进行过程中内部协调、配合实施，项目完成后进行验收确认。

智算集成单位负责：建立干系人通讯录，参与设计方案评审，完成进度计划分析与排期，确认主设备到货进度计划等。

2. 与设计单位分工界面

设计单位负责：机柜与设备布置图，硬件资源池划分，线缆布放计划，电力/地线，信号线端口互

联设计，协助完成周边端口资源分配。

智算集成单位负责：依据设计单位提供的工程设计方案进行集成方案详细设计。

3. 与施工单位分工界面

施工单位负责：设备到货安装、辅材辅料安装、设计规定的乙供材料的提供。

智算集成单位负责：配合督导设备安装、综合布线、线缆整改等关键施工节点。提供尾纤、网线、标签等工程所需的一切辅料。

4. 与监理单位分工界面

监理单位负责：设备到货接收查验、机房施工安全把控、施工整体督导。为施工督导主导方。

智算集成单位负责：督导施工队完成设备的安装上架、加电、加固、接地、线缆布放，为施工督导配合方。

5. 与设备厂家分工界面

设备厂家负责：将所提供设备（含设备自带配件、电源线等）运送到指定地点，负责提供安装督导、设备模块组装、设备调测；负责所提供设备的相关售后服务、保修、技术支持等；负责配合智算集成单位完成系统联调及验收测试等。

智算集成单位负责：设备联调规划、设备 IP 地址分配，负责对设备提供商提出设备初始化配置要求；负责完成全网设备、链路、协议功能的连通性、稳定性、安全性测试以及网络性能测试等；确保工程中所有硬件设备的可用性；负责解决各硬件设备安装和调测出现的问题；负责本工程服务器操作系统的安装及配置，确保达到本项目对相关设备的规范和功能要求。

6.2 智算平台部署与系统对接要求

6.2.1 智算平台部署要求

1. 云基础平台部署

(1) 智算云平台

采用高可用架构部署云管理平台，实现计算/存储/网络虚拟化资源池化管理。平台部署智能调度引擎，支持 GPU/FPGA 等异构资源动态分配。同时具备分布式资源监控模块，支持多维资源展示、定位、查询等能力。

(2) 网络管理平台

平台部署 SDN 控制器，支持 VxLAN、智能无损网络协议，实现网络自动化配置。支持网络可视化管理、网络策略管理，实现端到端流量监控、QoS 动态调整等能力。

(3) 资源管理平台

平台部署资源编排系统，支持容量预测功能，实现资源利用率智能预测。支持多租户配额管理，实

现分级资源配额策略。

2. 容器化平台部署

通过资源管理平台 API 实现 Kubernetes 集群自动化部署，配置容器网络插件，支持 SR-IOV、DPDK 加速方案，部署持久化存储驱动，对接分布式文件存储系统。

3. AI 平台部署

采用 Operator 模式部署 AI 训练框架，如 TensorFlow/Kubernetes，支持 GPU 共享调度组件，如 NVIDIA vGPU，配置模型推理服务网格。

6.2.2 系统对接要求

智能计算系统集成重点关注参数网平面和数据网平面，传统通算各平面对接建议按照现有行业标准和规范执行。

1. 计算与存储对接要求

运用 NVMe 协议，按需通过 RDMA（RoCE/InfiniBand）实现高速无损传输或传统 TCP/IP 传输。计算节点支持直接并发访问多个存储节点，满足负载均衡和可靠性要求。计算节点部署读写缓存，减少数据搬运延迟，提升 GPU 利用率。小规模场景下，可使用计算存储融合节点，提升资源利用率。

2. 计算与网络对接要求

采用胖树（Fat-Tree）网络拓扑，实现无阻塞带宽、多路径路由。使用 RDMA 高速网络，实现计算节点间高吞吐、低延迟通信，支持分布式训练。运用 GPU Direct 通信技术，支持 GPU 显存直接跨节点访问，提升集群扩展效率。按需部署智能网卡，卸载网络协议栈、安全、存储管理功能，释放 CPU 资源，提供硬件级隔离。

3. 存储与网络对接要求

运用 iSER/SRP 协议实现高速传输，降低延迟。分布式对象存储通过 25G/100G 以太网对接，支持三副本或 EC 纠删码。采用无损以太网技术（PFC/ECN），实现链路级反压避免丢包和端到端拥塞通知，保障 RoCEv2 在以太网上的无损传输。

4. 安全与相关系统对接要求

通过 VLAN/VRF 实现东西向流量隔离，出口方向配置防火墙、抗 DDOS、WAF、IPS 等安全设备实现南北向流量安全隔离。通过流量监控平台进行智能流量识别，加强数据安全管理，对敏感信息实施传输加密和存储加密。安全设备应与云平台安全组策略同步，网络 ACL 与容器网络策略联动，日志审计系统与各平台日志采集对接，达到智算级安全可控要求。

7 智算系统集成系统调测技术要求

7.1 计算子系统配置调测

7.1.1 硬件安装与检查

设备安装需要依据设计图纸及集成方案进行。设备安装前需要做好机房内走道部分地面防护，提前完成设备出库、拆包装等工序；安装过程中要做好设备及配套材料的保护，确保设备的承重、散热和通风等满足设计及集成方案要求；设备安装后，需要检查硬件设备的物理连接，确保线缆连接牢固，布局合理，检查电源连接，确保设备供电安全可靠。

7.1.2 软件安装与配置

1. 操作系统与软件环境配置
   (1) 操作系统安装：安装指定版本的操作系统，确保系统内核、CPU 架构等满足集成方案要求；配置系统分区、Swap 空间、设备名、设备网卡等，关闭不必要的服务，优化系统性能；硬件驱动安装，为包括网卡、GPU 等硬件设备安装与操作系统及业务需求匹配的驱动包；
   (2) 软件环境配置：安装计算框架工具包，如 CUDA、CANN 等；配置环境变量，安装依赖库和工具链，确保 AI 框架或上层业务能够正常运行。
2. 计算资源初始化与配置
   (1) 资源池化配置：安装、配置容器化平台或虚拟化平台组件，便于上层管理平台调用；配置计算资源云化或容器化管理平台，便于 CPU、GPU、内存等资源的动态分配和管理；
   (2) 资源调度配置：配置资源调度系统，如 OpenStack、Kubernetes 等，设置任务优先级和资源分配策略，配置动态资源伸缩机制，根据任务负载自动调整资源分配。

7.2 存储子系统配置调测

7.2.1 硬件安装与检查

1. 开箱验货与登记

核对设备清单（服务器节点、硬盘、网卡、线缆、导轨等）与采购订单一致性。检查设备外观是否完好，序列号记录备案。验证硬件规格（如 SSD 型号、容量、网卡速率、网卡类型等）是否符合技术规范要求。

2. 机房环境确认
   (1) 供电：检查机柜 PDU 冗余供电（A/B 路）、电压稳定性；
   (2) 空间与承重：确认机柜 U 位、深度、承重（≥设备重量×1.5）；
   (3) 散热：冷通道温度（18-27℃）、设备间距（预留前后散热空间）；
   (4) 网络：光纤/网线预布线完成，标签清晰。
3. 物理安装：

(1) 按设计图纸安装节点到机柜，紧固导轨；

(2) 连接电源线（A/B 路分接不同 PDU）；

(3) 连接网络线缆：

- RDMA 网络：接入 IB 交换机或 RoCE 交换机指定端口；
- 管理/IP 网络：接入管理网交换机。

(4) 接地线安装。

7.2.2 软件安装与配置

1. 存储系统环境配置

(1) 操作系统与依赖安装：安装指定 OS，如 CentOS7.9、Ubuntu 20.04 等；

(2) 安装驱动及系统环境配置：如 RDMA 驱动（OFED）、NVMe 驱动、网卡驱动等，完成系统名称、网卡、时间同步等系统环境配置。

2. 存储软件部署

部署分布式存储软件（如 Ceph/WeKA/Lustre/厂商方案）：通过 Ansible/SaltStack 或厂商管理平台批量安装。配置软件仓库、安装核心组件（MON/OSD/MDS 等）。

3. 集群初始化与配置

创建存储集群，加入所有节点。配置核心参数：

(1) 网络分区：RDMA 网络用于数据面，IP 网络用于管理面；

(2) 冗余策略：根据冗余策略配置副本数或 EC 算法；

(3) 池划分：创建对应硬件的存储池，如 NVMe_pool、SSD_HDD_pool 等。

7.3 网络子系统配置调测

7.3.1 通用网络配置

1. 设备固件与驱动版本检查：检查设备固件/软件版本进行是否符合设计要求；

2. 应根据设计对基础网络参数进行配置包括 IP 地址、VLAN、路由、VRF、访问控制列表等进行配置；

3. 应对根据业务需求路由路径、协议参数、QoS 策略、MTU 等进行优化。

7.3.2 参数网络配置

1. RoCE v2 协议配置

(1) 应配置 RoCE v2 协议，检查是否 RoCE v2 协议激活（ibstat、rdma system 命令）；

(2) 应对 PFC 与 ECN 配置进行配置，启用流量控制（Priority Flow Control）和显式拥塞通知（ECN），避免 RoCE 丢包；

(3) 应为 RoCE 流量分配专用 DSCP（Differentiated Services Code Point）值，并在网络设备上配置优先级队列；

(4) 应进行 MTU 进行设置，确保端到端一致（需交换机、网卡、OS 均支持）；

(5) 交换机与 HCA 的链路速率应匹配；

(6) 应对服务器 RoCE 网卡进行配置，启用 RoCE v2 模式，设置正确的优先级、ECN 等参数；

(7) 操作系统内核或用户态驱动应支持 RoCE v2。

2. IB 协议配置配置

(1) 应选择支持目标带宽的 HCA 卡，HCA 卡驱动兼容操作系统；

(2) 应启用子网管理器 SM：SM 可在 IB 网络管理服务器、交换机或是服务器上启用。每个 IB 网络应为一个独立子网（Subnet），配置 SM 的 polling_interval（轮询间隔）为较低值（如 1 秒），稳定拓扑中应禁用动态路由更新，减少 SM 的计算开销；

(3) 宜通过分区（Partition Key, PKEY）PKEY 划分逻辑网络，隔离不同租户或应用流量；

(4) 应根据网络拓扑设置路由算法；

(5) 应进行 MTU 进行设置，确保端到端一致（需交换机、网卡、OS 均支持）；

(6) 所有交换机和 HCA 应被 SM 正确识别，交换机与 HCA 的链路速率应匹配；

(7) 宜启用链路层信标（Link Beaconing），快速感知物理链路故障。

7.3.3 网络调测

1. 应进行连通性测试，包括不限于：

(1) 端到端测试：使用 ping、traceroute 验证设备间连通性；

(2) 跨网段通信：测试不同 VLAN、子网间的路由是否正常。

2. 应进行性能测试括不限于：

(1) 带宽与延迟：通过工具（如 iperf、perfstat）测试吞吐量、时延、抖动是否符合要求；

(2) 负载测试：模拟高并发流量，验证设备（如交换机、防火墙）的转发能力；

(3) QoS 验证：测试优先级流量是否优先保障。

3. 应进行冗余与容灾测试，包括不限于：

(1) 链路聚合：拔掉一条链路，测试冗余链路是否自动切换；

(2) 路由冗余：模拟主路由失效，验证备份路由（如 HSRP/VRRP）能否接管；

(3) 设备故障转移：测试主备防火墙、负载均衡器的切换时间。

7.4 安全子系统配置调测

7.4.1 系统基础安全

1. 使用系统漏扫工具、资产安全检测等工具检测以下内容：
   (1) 执行系统漏洞检查任务，发现权限许可和访问控制漏洞。
   (2) 对虚拟化平台、容器平台漏洞进行扫描，包括安全绕过、目录遍历等风险。
   (3) 探测互联网资产（如 IP、端口），减少未授权访问的风险。
2. 使用基线检测工具、系统漏扫工具检测以下内容：
   (1) 执行安全基线检查任务，关闭不必要的服务和端口。
   (2) 定期扫描主机漏洞，及时修补已知问题。
   (3) 启用实时防护和入侵检测功能，提升主机整体安全性。
3. 安全域隔离与部署，利用防火墙等设备完成安全域的设置与策略部署：
   (1) 根据集成方案规划设置不同安全域，并配置安全等级。
   (2) 根据业务系统访问需求，配置安全域间访问控制策略。

7.4.2 业务安全

1. 使用内容安全检测工具、代码审计工具检测以下内容：
   (1) 执行内容合规检查任务，识别敏感数据并防止泄露。
   (2) 动态调整关键页面数量，定期检测内容违规情况。
   (3) 检查源代码中是否存在硬编码密码或不安全的对象引用问题。
   (4) 识别开源组件是否包含已知漏洞，提供 CVE 编号及修复建议。
2. 使用代码扫描工具检测以下内容：
   (1) 对未经编译的源代码、开源组件的安全检查能力，能够在未部署时对代码中存在的问题、漏洞进行扫描和处理，降低正式部署之后的问题风险。
   (2) 别源代码中引用的开源组件，包括开源组件的名称、版本、是否存在漏洞、漏洞对应的 CVE 编号及漏洞描述。
   (3) 组件安全性测评，检测非登录状态下的页面是否能被第三方程序调用、检测程序是否具有后台运行提醒功能。
3. 利用 IPS/IDS 保护业务安全：
   (1) 配置 IPS/IDS 互联端口，定义可信区域与非可信区域。
   (2) 定义安全策略模板，并在系统中调用，保障业务系统安全。
   (3) 设置系统日志、安全日志配置，保障安全事件可回溯。

7.4.3 管理安全

1. 使用弱口令检测工具检测以下内容：
   (1) 执行弱口令检查任务，确保密码策略符合安全规范（如复杂度、有效期等）。

(2) 满足平台合规项弱口令字典规范要求，避免用户使用易被破解的密码。

(3) 支持对网络可达资产进行在线非暴力检查，避免明文存储或传输密码。

2. 使用互联网暴露资产安全检测工具、Web 漏扫工具检测以下内容：

(1) 探测互联网资产，创建资产发现任务，动态收集资产信息。

(2) 防止公网直接访问安全评估与检测平台，确保网络安全域划分。

(3) 支持多路扫描，满足不同网段 Web 站点同时检测需求。

(4) 提供 SSL 加密模式传输，保障网络通信安全。

8 智算系统集成验收技术要求

8.1 智算验收测试方案

8.1.1 测试范围与目标

1. 硬件验收

(1) 测试内容：包括 CPU、GPU、内存、存储设备、网络设备的配置、性能基线及稳定性验证。例如，CPU 需测试单核/多核性能，GPU 需验证 AI 加速能力。

(2) 测试工具：验收测试应具备自检测试工具并能根据验收标准生成自检报表，自检工具包括不限于连通性检测、设备状态采集、路由状态检测、可靠性测试、端口检测、安全检查等。

2. 软件验收

(1) 适配性测试：验证操作系统、AI 框架与硬件的兼容性，确保驱动、库版本匹配。

(2) 集群管理工具：测试 Slurm/Kubernetes 的任务调度效率与资源利用率。

3. 网络与通信

(1) 性能测试：带宽、延迟及丢包率指标需满足设计中的要求，验证跨节点分布式通信的稳定性。

(2) IB/RoCE 网络测试：确认子网管理器配置正确，无重复分区或冲突。大规模 Allreduce 操作时，吞吐量无明显下降，延迟符合集群规模预期。

(3) 冗余测试：模拟链路中断场景，验证网络自愈能力。

4. 稳定性测试

智算集群稳定性：测试被测设备在 PyTorch 框架下，使用 LLaMA2/GPT-3 等模型在 64 节点进行训练的稳定性能。

5. 安全性验收

(1) 访问控制：测试防火墙、权限管理及数据加密机制的有效性。

(2) 灾备能力：验证数据备份恢复流程及冗余系统切换效率。

8.1.2 测试流程与阶段

1. 分项测试执行

(1) 单节点测试：验证硬件单体性能及软件基础功能。主要测试内容包括：allreduce 带宽性能、单卡物理算力测试和单机模型训练测试。每项测试需明确测试目的，测试前条件确认，测试详细步骤，预期结果和测试结果。

(2) 集群联调测试：模拟多节点协同任务，评估通信效率与负载均衡策略。主要测试内容包括：参数面集合通信性能测试、参数面集合通信稳定性测试、集群训练稳定性测试、参数面网络性能测试和集群性能测试。每项测试需明确测试目的，测试前条件确认，测试详细步骤，预期结果和测试结果。

2. 数据分析与优化

(1) 性能瓶颈定位：使用性能分析工具识别算力、内存或网络瓶颈，提出调优建议。

(2) 问题闭环：针对测试中发现的异常，结合日志与调试工具进行根因分析。

3. 验收评审

(1) 验收标准：依据验收规范标准要求进行验收，相关方签字确认。

(2) 文档交付：测试结束后输出测试报告、测试脚本、问题清单及优化方案，作为验收通过的依据。

8.2 智算验收测试能力要求

8.2.1 测试团队能力要求

1. 硬件能力

熟悉AI芯片的算力评估方法（如FP16/TFLOPS性能指标），能通过MLPerf等基准测试工具验证理论性能与实际表现的偏差。掌握服务器硬件（如存储RAID配置、液冷系统）的故障模拟与诊断技术，需通过设备供应商认证。

2. 软件与算法能力

具备主流框架（MindSpore、PyTorch）的部署调优经验，能解决CUDA驱动版本冲突、算子兼容性等典型问题。熟悉多机多卡通信协议，能通过AllReduce算法测试验证通信带宽利用率。

3. 网络与安全能力

掌握RoCEv2、InfiniBand等协议的配置优化，能通过延迟和吞吐量测试验证网络性能。具备CISP或CISSP认证，能执行漏洞扫描及数据加密合规性审计。

4. 人员素质能力

验收测试应严格按照验收测试规范标准执行，并记录测试日志和结果，确保全面覆盖测试需求。测试人员应理解业务流程，熟练掌握测试工具的使用方法，并记录操作步骤形成测试文档。具备良好的缺

陷沟通能力，包括缺陷的记录、跟踪、修复和验证。验收测试过程中投入人数不少于施工阶段投入的人员数量。

8.2.2 测试流程能力要求

1. 全栈覆盖能力

支持从单设备（如单台AI服务器）到集群（如超千节点）的逐级扩展测试，确保系统线性扩展比≥80%。覆盖数据预处理、训练、推理全流程，例如ResNet-50训练任务需在指定硬件下达到每小时2000张/卡的吞吐量。

2. 标准化与自动化

遵循验收规范（如硬件配置核对表、性能基线表）进行逐项验收。使用Ansible或Python编写自动化测试脚本，实现测试用例执行、结果采集与报告的自动化。

3. 问题闭环能力

通过日志和Profiling工具定位性能瓶颈或故障点。针对问题提出调优方案（如调整Kubernetes资源分配策略），并复测验证改进效果。

参 考 文 献

索　引