EP500 EP600 NVMe PCIe SSD

技术白皮书

文档版本	01
发布日期	2022-06-01

超聚变数字技术有限公司

版权所有 © 超聚变数字技术有限公司 2022。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

XFUSION 和其他超聚变商标均为超聚变数字技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受超聚变数字技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，超聚变数字技术有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

超聚变数字技术有限公司

地址： 河南省郑州市郑东新区龙子湖智慧岛正商博雅广场 1 号楼 9 层 邮编：450046

网址： https://www.xfusion.com

目 录

前言.....v

1 产品简介.....7

1.1 概述.....7

1.2 系统设计.....8

2 产品特点.....10

2.1 性能特点.....10

2.2 可靠性特点.....10

2.3 可维护性特点.....11

3 外观结构.....12

3.1 外观.....12

3.2 结构.....13

4 产品规格.....14

4.1 基本规格.....14

4.1.1 EP500.....14

4.1.2 EP600.....16

4.2 容量.....18

4.3 QoS.....18

4.4 IOPS 一致性.....19

4.5 热插拔.....20

4.6 NVMe 特性.....21

4.7 环境条件.....21

4.8 温度监控和过温保护.....21

5 信号管脚.....23

5.1 2.5 寸盘信号管脚定义.....23

6 管理.....26

6.1 带内管理.....26

6.2 带外管理.....26

7 安全.....27

7.1 安全架构 27
7.2 安全威胁及攻击 28
7.3 安全策略及措施 29
8 认证 30

前言

概述

本文档详细介绍 NVMe PCIe 固态硬盘 EP500、EP600 的系统设计、产品特点和产品规格等，让用户对 EP500、EP600 NVMe PCIe SSD 有一个深入细致的了解。

读者对象

本文档（本指南）主要适用于以下工程师：

- 技术支持工程师
- 维护工程师
- 用户

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	表示如不避免则将会导致死亡或严重伤害的具有高等级风险的危害。
警告	表示如不避免则可能导致死亡或严重伤害的具有中等级风险的危害。
注意	表示如不避免则可能导致轻微或中度伤害的具有低等级风险的危害。
须知	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。
说明	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

修改记录

文档版本	发布日期	修改说明
01	2022-06-01	第一次正式发布。

1 产品简介

1.1 概述

1.2 系统设计

1.1 概述

EP500、EP600 系列是支持高达 7.68TB 的企业级 SSD，搭载最新的 128 层 3D eTLC NAND 和专业的企业级控制器。在数字转型和数据爆炸的时代，企业级用户的各种业务场景中，对性能的需求越来越高，需要更高 IOPS、更低的延时，且高一致性来满足快速的数据访问。例如在线事务处理（OLTP），需要对实时的原始数据进行处理，力求通过并行查询和最小化响应时间来提高单位时间内交易的数量；在线分析处理（OLAP），需要通过复杂的数据查询分析，为商业决策起辅助作用；此外还有高性能计算，云计算，VDI 等越来越多的应用对服务器的存储性能提出了更高的要求。为企业和数据中心客户提供更高性能、更低功耗及更容易维护的完整解决方案。

EP500、EP600 系列是企业级高性能的存储及加速部件，具有性能高、响应快、可靠性高等特点，极大的提升存储 IO 性能。兼容业界主流操作系统和虚拟化系统，可以提升数据库、虚拟化、HPC、搜索等多种应用的业务性能，帮助客户降低系统 TCO。

EP500、EP600 的数据接口是 PCIe 4.0 x4，包含 2 个系列的产品，分别是：

- EP500 系列：标准的 2.5 寸盘，接口形态是 SFF-8639。
  适合于读密集型的业务场景。
- EP600 系列：标准的 2.5 寸盘，接口形态是 SFF-8639。
  适合于读写混合的业务场景。

EP500、EP600 提供丰富的单品容量和规格，满足不同应用场景需求。

- EP500 读密集型系列提供单盘容量：1920GB、3840GB、7680GB
- EP600 读写混合型系列提供单盘容量：1600GB、3200GB、6400GB

EP500、EP600 外观如图 1-1 和图 1-2 所示。

图1-1 EP500 外观

图1-2 EP600 外观

1.2 系统设计

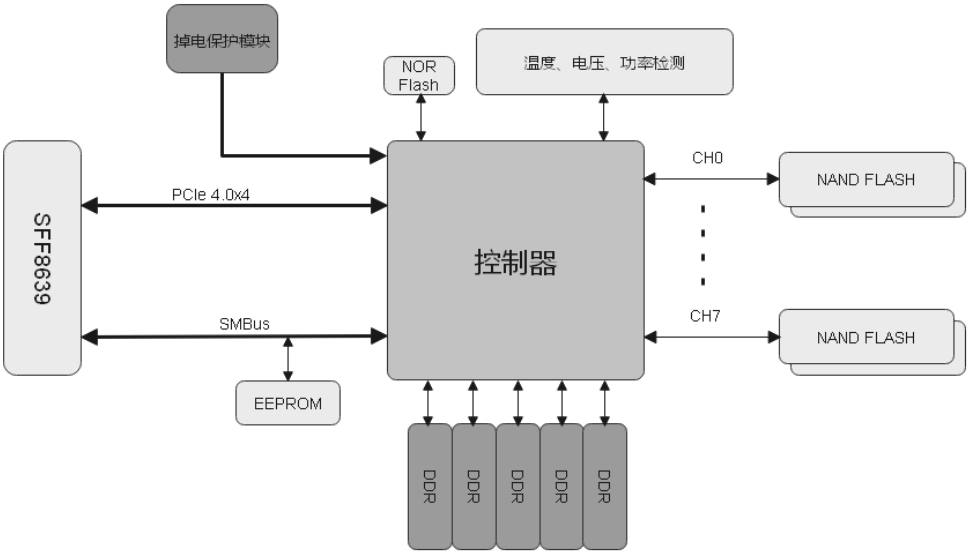
EP500、EP600 的系统设计特点如下：

- 采用企业级 SSD 控制器，能充分发挥控制器和 NAND 的性能潜力。是一款基于 SSD FTL 算法、LDPC 纠错算法而设计的 ASIC 控制器，支持 1.4 版本 NVMe 标准，主要特点是高性能、低功耗。

- 增强的设备管理功能。标准的 NVMe 接口特性，可以满足操作系统免驱，可做 OS 盘。提供完善的热插拔功能，满足用户简单维护的需求。满足 NVMe 盘标准的带外管理功能，与服务器配合，让在网设备健康状态监测更智能。

EP500、EP600 的系统架构如图 1-3 所示。

图1-3 EP500、EP600 系统架构



2 产品特点

2.1 性能特点
2.2 可靠性特点
2.3 可维护性特点

2.1 性能特点

- 采用高性能、低功耗的企业级 SSD 控制器。
- 支持 NVMe 1.4 标准，多队列 IO 技术提升 SSD 性能及 QoS 表现。

2.2 可靠性特点

- 端到端数据保护：支持用户通过 DIF 域进行数据保护，数据在盘片内部各模块间传输时均有校验保护。
- 内置类 RAID 算法：基于 Flash die 级的类 RAID 算法，当介质数据出现错误后，可以通过冗余计算恢复数据。
- 增强的 LDPC 纠错算法：提供比 Flash 颗粒要求更高的纠错能力，为设备的可靠性带来有效的保证。
- 高级 Flash 访问技术：组合应用 NAND 颗粒的读重试和自适应电压调节 read 技术，有效保证数据的可靠性。
- 数据巡检技术：周期性的巡检数据，提前预防错误的发生。
- 智能磨损平衡技术：智能均衡 Flash 颗粒磨损压力，有效延长设备的使用寿命。
- 元数据多备份：对于启动固件、NAND 等关键的元数据都采用双备份和数据一致性校验保证。
- 掉电保护：当设备异常下电时，确保硬盘内的数据不丢失。
- 温度控制：通过监控多个温度传感器，综合 CPU、NAND 等温度，调控读写速度来保护数据。
- 数据加密：数据在写入时进行加密，读出时进行解密的机制。控制器支持 AES-256 硬件加密。

- 八级功耗管理：精确到每瓦都有对应的性能档位，6~14W，通过简单的设置命令即时调整即时生效。
- 固件在线升级：FW 在线升级不断业务，秒级处理，即时生效。
- NAND 接口速率可达 1600MT/S。

2.3 可维护性特点

- 支持带内的在线升级，方便进行日常维护。
- 完备的命令行管理功能，用户可以通过各种命令进行日常的设备管理。支持通过访问带外通道进行设备管理，设备信息中包含型号、容量、固件版本、磨损度和健康状态等相关信息。
- 支持日志查询，用户可以通过日志监控产品的健康状况。
- 通过标准 NVMe CLI 工具带内便捷获得深入失效分析的相关日志。

3 外观结构

3.1 外观

3.2 结构

3.1 外观

EP500 EP600 包含有标准的 2.5 寸硬盘的产品，适合安装在机架服务器等通用服务器内。

图3-1 EP500、EP600 硬盘框拉手条前视图

EP500 EP600 通过拉手条提供工作状态指示灯功能。图 3-1 中的琥珀色/蓝色指示灯是故障指示灯，绿色指示灯是工作指示灯。灯的颜色跟硬盘框指示灯设计强相关。当盘工作在服务器中的时候，指示灯定义如表 3-1 所示。

表3-1 SSD 盘状态指示灯定义

Activity 指示灯（绿色灯）	Fault 指示灯（琥珀色/蓝色灯）	状态
Off	Off	NVMe SSD 盘不在位
On	Off	NVMe SSD 盘在位且无故障
2Hz 闪烁	Off	NVMe SSD 盘正在进行读写操作
Off	2Hz 闪烁	NVMe SSD 盘正处于热插过程中

Activity 指示灯（绿色灯）	Fault 指示灯（琥珀色/蓝色灯）	状态
Off	0.5Hz 闪烁	NVMe SSD 盘已完成热拔流程，允许被拔出
On/Off	On	NVMe SSD 盘故障

3.2 结构

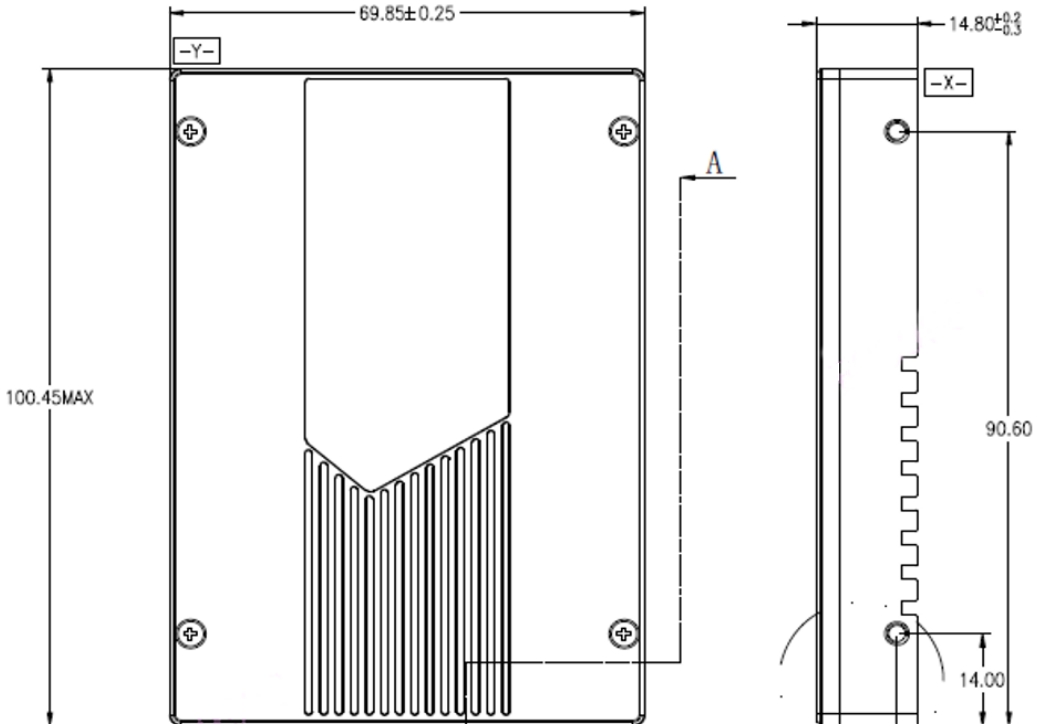
说明

所有的尺寸量度都是毫米。

表3-2 长宽高信息

X － Length	Y － Width	Z － Height
100.2±0.25	69.85±0.25	14.8+0.2 或者 14.8-0.3

图3-2 硬盘尺寸



4 产品规格

4.1 基本规格
4.2 容量
4.3 QoS
4.4 IOPS 一致性
4.5 热插拔
4.6 NVMe 特性
4.7 环境条件
4.8 温度监控和过温保护

4.1 基本规格

4.1.1 EP500

表4-1 EP500 规格[a]（LBA[b] format：512B）

特征	规格		
型号	XFSP4151T90000N	XFSP4153T80000N	XFSP4157T60000N
容量	1920GB[c]	3840GB	7680GB
形态	2.5 寸盘	2.5 寸盘	2.5 寸盘
接口	PCIe 4.0	PCIe 4.0	PCIe 4.0
Flash 颗粒类型	X2 TLC	X2 TLC	X2 TLC
顺序读带宽（MB/s）[d]	6,000	6,000	6,000

特征	规格		
随机 4KB 读 IOPS（稳态）[e]	700,000	1000,000	1000,000
平均读延时 @1QD（μs）[f]	85	85	85
顺序写带宽（MB/s）	2,600	4,500	4,500
随机 4KB 写 IOPS（稳态/最大）[g]	90,000	180,000	190,000
平均写延时 @1QD（μs）	15	15	15
写操作寿命[h]（PBW）	3.504PB	7.008PB	14.016PB
DWPD（JESD219）[i]	1	1	1
功耗（Idle, Active）[j]	5W，12W	5W，14W	5W，14W
重量（g）	<120		
掉电保护	是		
颗粒失效保护	是		
Trim	是		
平均无故障时间（MTBF）	200 万小时		
年失效率（AFR）	≤0.44%		
误码率（UBER）	10^{-17}		
数据保存时间（掉电）[k]	40℃3 个月		
新盘做备件时数据保存时间（掉电）[l]	40℃12 个月		
备注：			

特征	规格
a：性能规格是在最大功耗条件下测试的值。 b：LBA（Logical Block Addressing，逻辑块寻址）是描述存储设备上数据所在区块的一种通用机制，一般用在硬盘上。LBA 是一种特殊简洁的线性寻址机制，地址块被用一个整数来索引，比如第一个块表示为 LBA 0，第二个为 LBA 1，等等。 c：GB = 1,000,000,000 Byte。 d：MB/s = 1,000,000 Bytes/second。性能是使用 FIO 工具在 CentOS 7.0 系统上用 1 线程 512QD 128KB（131,072 bytes）顺序读的结果。顺序写带宽类似。 e：使用 FIO 工具用 8 线程 128QD 4KB 随机读在稳定态的结果。 f：μs = Microsecond。1 线程 1QD 随机 4KB 读的平均延迟。平均写延迟类同。 g：使用 FIO 工具用 4 线程 64QD 4KB 随机写在稳定态的结果。 h：1PB = 10^{15} Bytes。写操作寿命是在 4KB IO size 和 4KB 对齐的测试条件下的结果。 i：DWPD：JESD219 标准下驱动器每天全盘写入次数，当用户每天全盘写入次数不超过规格值时，可持续使用 5 年，否则将影响 SSD 使用寿命。 j：Activity 功耗是在最大顺序写带宽测试条件下的结果。 k：生命周期范围内，SSD 掉电后数据保存时间。 l：前 3%生命周期范围内，SSD 掉电后数据保存时间。	

4.1.2 EP600

表4-2 EP600 规格[a]（LBA[b] format：512B）

特征	规格		
型号	XFSP4161T60000N	XFSP4163T20000N	XFSP4166T40000N
容量	1600GB[c]	3200GB	6400GB
形态	2.5 寸盘	2.5 寸盘	2.5 寸盘
接口	PCIe 4.0	PCIe 4.0	PCIe 4.0
Flash 颗粒类型	X2 TLC	X2 TLC	X2 TLC
顺序读带宽（MB/s）[d]	6,000	6,000	6,000
随机 4KB 读 IOPS（稳态）[e]	700,000	1000,000	1000,000
平均读延时@1QD（μs）[f]	85	85	85

特征	规格		
顺序写带宽（MB/s）	2,600	4,500	4,500
随机 4KB 写 IOPS（稳态）[g]	200,000	350,000	380,000
平均写延时@1QD（μs）	14	14	14
写操作寿命（PBW）[h]	8.76PB	17.52PB	35.04PB
DWPD（JESD219）[i]	3	3	3
平均功耗（Idle, Active）[j]	5W，12W	5W，14W	5W，14W
重量（g）	<120g		
掉电保护	是		
颗粒失效保护	是		
Trim	是		
平均无故障时间（MTBF）	200 万小时		
年失效率（AFR）	≤0.44 %		
误码率（UBER）	10^{-17}		
数据保存时间（掉电）[k]	40℃ 3 个月		
新盘做备件时数据保存时间（掉电）[l]	40℃ 12 个月		
备注参考 EP500			

4.2 容量

表4-3 EP500 容量

EP500	User Addressable Sectors in LBA Mode
1920GB	3,750,748,848
3840GB	7,501,476,528
7680GB	15,002,931,888

表4-4 EP600 容量

EP600	User Addressable Sectors in LBA Mode
1600GB	3,125,627,568
3200GB	6,251,233,968
6400GB	12,502,446,768

说明

- 由于容量的一小部分用于 NAND 介质管理和维护，SSD 的总可用容量可能小于总物理容量。使用 JESD218B 标准。用户可寻址逻辑块计数= 21168 + (1953504 x SSD Capacity in Gbytes)。
- 1GB=10^9 bytes，1 sector=512 bytes，显示的 LBA 计数表示总的用户存储容量，并将在盘使用寿命期间保持相同。

4.3 QoS

表4-5 EP500 服务质量（LBA format：512B）

规格	单位	EP500		
		QD = 1		
		1920GB	3840GB	7680GB
服务质量（99%）				
随机 4KB 读 [a]	μs	95	95	95
随机 4KB 写 [a]	μs	32	32	32
随机 4KB 读 [b]	ms	0.48	0.48	0.48

随机 4KB 写 [b]	ms	8.2	5	5
服务质量（99.99%）				
随机 4KB 读 [a]	μs	100	100	100
随机 4KB 写 [a]	μs	55	60	60
随机 4KB 读 [b]	ms	0.7	0.7	0.7
随机 4KB 写 [b]	ms	14	9	9
a：使用 FIO 工具在 1 线程 1QD 下测试 4KB 随机 IO 的结果。 b：使用 FIO 工具在 1 线程 128QD 下测试 4KB 随机 IO 的结果。				

表4-6 EP600 服务质量（LBA format：512B）

规格	单位	EP600		
		QD = 1		
		1600GB	3200GB	6400GB
服务质量（99%）				
随机 4KB 读 [a]	μs	95	95	95
随机 4KB 写 [a]	μs	14	14	14
随机 4KB 读 [b]	ms	0.48	0.48	0.48
随机 4KB 写 [b]	ms	4.4	0.8	0.8
服务质量（99.99%）				
随机 4KB 读 [a]	μs	100	100	100
随机 4KB 写 [a]	μs	26	55	55
随机 4KB 读 [b]	ms	0.7	0.7	0.7
随机 4KB 写 [b]	ms	9	2	2
备注参考 EP500				

4.4 IOPS 一致性

表4-7 EP500 IOPS 一致性（LBA format：512B）

规格 [a, b]	单位	EP500

		1920GB	3840GB	7680GB
随机 4KB 读（最大）c	%	95	95	95
随机 4KB 写（最大）c	%	90	90	90

表4-8 EP600 IOPS 一致性（LBA format：512B）

规格 a，b	单位	EP600		
		1600GB	3200GB	6400GB
随机 4KB 读（最大）c	%	95	95	95
随机 4KB 写（最大）c	%	90	90	90

说明

a：性能测试过程中每秒采样一次 IOPS，将采样数据从大到小依次排序，取前 99.9%数据中的最小 IOPS 与整个测试过程中的平均 IOPS 进行比较；性能数据是在整盘 LBA 范围内进行测试待 IO 到达稳定态后统计的。

b：使用 FIO 工具在 LINUX*CentOS 7.5 操作系统上以 8 线程 128QD*4KB (4096 bytes)对随机读/写 IOPS 一致性进行测量。当工作负载达到稳态时，在整盘 LBA 范围内执行测量。

c：4KB = 4,096 bytes。

4.5 热插拔

热插拔分为以下两种：

- 通知式热插拔：用户可以带电直接插入 SSD 设备。拔出设备前，需先完成相应的操作准备步骤。
- 暴力热插拔：用户可以直接插入、拔出 SSD 设备。

  EP500、EP600 系列的 2.5 英寸 SSD 支持通知式热插拔和暴力式热插拔。

须知

进行暴力热插拔操作前，请先确认以下条件：

- 硬盘所在服务器支持暴力热拔插。
- BIOS 已开启 VMD 功能。

4.6 NVMe 特性

EP500、EP600 SSD 支持 NVMe 1.4 协议。除了支持基本特性和强制命令，还支持命名空间管理，支持最高 32 个命名空间。

4.7 环境条件

表4-9 应用环境条件

环境指标项	说明
产品	EP500，EP600
温度	存储温度：-40℃~+85℃（-40℉～+185℉） 工作温度：0℃~70℃[a]（32℉～+158℉）
海拔	• 工作状态：-305m~+4572m • 非工作状态：-305m~+12192m 说明 海拔从 1800m 开始每升高 220m，工作温度降低 1℃。超过 3048m 工作会影响可靠性。
湿度	• 工作状态：5%~95% • 非工作状态：5%~95%
冲击	• 工作状态：1000G 加速（最大），时长 0.5ms • 非工作状态：1000G 加速（最大），时长 0.5ms
振动	• 工作状态：最大 3.1GRMS（5Hz-800Hz） • 非工作状态：最大 3.1GRMS（5Hz-800Hz）

4.8 温度监控和过温保护

EP500 EP600 系列 SSD 配备 3 个温度传感器：控制器温度传感器、板温度传感器和 Nand 传感器。

EP500 EP600 系列 SSD 遵循复合温度方案，作为 NVMe 健康日志（日志标识符 02h，字节 1 和字节 2）的一部分，考虑了控制器、电路板、NAND 温度传感器，并提供复合值。

管理系统的重点是利用集成在整个 SSD 关键点上的 3 个温度传感器。允许在不同的环境中监测 key 组件的温度，从而实现更精确的热管理。

此外，设备将通过 SMBUS 读取 SMART 信息里面保存的 0X6Ah 地址来提供带外的温度访问。

NVMe 1.4 规范建议警告复合温度阈值（WCTEMP）为 70°C。

EP500 EP600 系列 SSD 采用热节流机制，以在发生故障或偏移时保护设备，从而防止设备温度超过其最高规定温度。

在带内，EP500 EP600 的固件使用了 2 级预警机制：

第一级告警阈值是 70℃。当温度达到该值，设备性能将被限制，直到温度再次低于 70℃。

第二级告警阈值是 77℃。设备 IO 将被停止，以避免不可逆转的损坏，当温度再次低于 77℃时，设备 IO 将缓慢恢复。

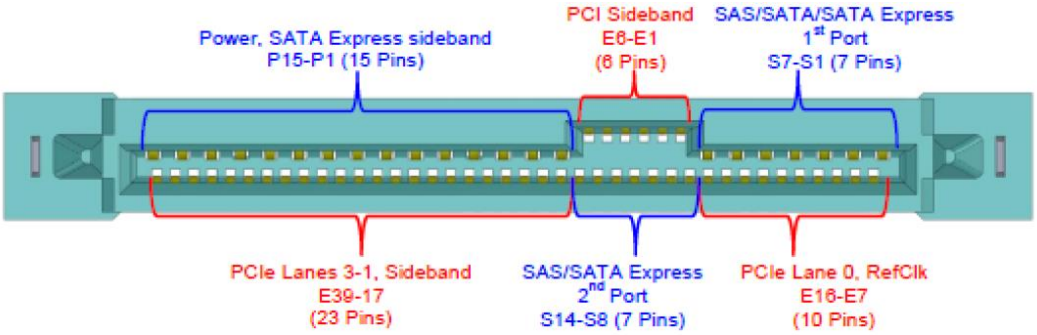
5 信号管脚

5.1 2.5 寸盘信号管脚定义

5.1 2.5 寸盘信号管脚定义

2.5 寸盘接口是标准的 SFF-8639，PCIe 信号分配如下。

图5-1 PCIe 信号分配



接口的管脚定义如下。

表5-1 管脚定义

引脚	名称	描述	引脚	名称	描述
S1	GND	接地	E7	PCIE_REFCLK0_P	PCIe Primary Reference Clock signals
S2	-	NC	E8	PCIE_REFCLK0_N	
S3	-	NC	E9	GND	接地
S4	GND	接地	E10	PETp0	ePCIe 0 传送正极

引脚	名称	描述	引脚	名称	描述
S5	-	NC	E11	PETn0	ePCIe 0 传送负极
S6	-	NC	E12	GND	接地
S7	GND	接地	E13	PERn0	ePCIe 0 接收负极
E1	REFCLK1+	参考时钟接口 B（未使用）	E14	PERp0	ePCIe 0 接收正极
E2	REFCLK1-	参考时钟接口 B（未使用）	E15	GND	接地
E3	3.3Vaux+	为 SM bus 供应 3.3V 电压	E16	-	NC
E4	-	NC	S8	GND	接地
E5	-	NC	S9	-	NC
E6	-	NC	S10	-	NC
P1	-	NC	S11	GND	接地
P2	-	NC	S12	-	NC
P3	-	NC	S13	-	NC
P4	IfDet#	界面检测（旧接地预充）	S14	GND	接地
P5	GND	接地	S15	-	NC
P6	GND	接地	S16	GND	接地
P7	-	NC	S17	PETp1	ePCIe 1 传送正极
P8			S18	PETn1	ePCIe 1 传送负极
P9			S19	GND	接地
P10	PRSNT#	在位（硬盘类型）	S20	PERn1	ePCIe 1 接收负极
P11	Activity	活动（输出）/旋转	S21	PERp1	ePCIe 1 接收正极

引脚	名称	描述	引脚	名称	描述
P12	GND	热插拔 接地	S22	GND	接地
P13	12V	预充电 全部 12V 只给 ePCIe SSD 供电	S23	PETp2	ePCIe 2 传送正极
P14			S24	PETn2	ePCIe 2 传送负极
P15			S25	GND	接地
-	-	-	S26	PERn2	ePCIe 2 接收负极
-	-	-	S27	PERn2	ePCIe 2 接收正极
-	-	-	S28	GND	接地
-	-	-	E17	PETp3	ePCIe 3 传送正极
-	-	-	E18	PETn3	ePCIe 3 传送负极
-	-	-	E19	GND	接地
-	-	-	E20	PERn3	ePCIe 3 接收负极
-	-	-	E21	PERp3	ePCIe 3 接收正极
-	-	-	E22	GND	接地
-	-	-	E23	SMClk	SM-Bus 时钟
-	-	-	E24	SMDat	SM-Bus 数据
-	-	-	E25	TBD	TBD

6 管理

EP500、EP600 提供了功能丰富的维护管理功能，包括运行在 OS 中的带内管理命令集和通过 BMC 提供的带外管理功能。

6.1 带内管理

6.2 带外管理

6.1 带内管理

带内管理的功能有：

- 全盘数据清除功能，方便用户报修设备时保障数据的保密性。
- 在线升级功能，而且升级 firmware 不需要重启 OS，方便用户的设备维护。
- 资产管理功能，提供生产日期、序列号等信息，方便用户进行资产管理。
- 标准 SMART 统计功能，用户可以查询设备的健康状态、寿命、读写数据量等。
- SNMP 代理功能，用户可以对 NVMe 设备进行集中式管理。
- 日志查询功能，运维人员用来进行问题分析。

6.2 带外管理

EP500、EP600 基于 SMBUS 接口实现了《NVM Express Management Interface Revision 1.0》规范的《NVM Express Basic Management Command》部分的带外管理功能。BMC 软件能通过 SMBUS 接口访问存储在 EEPROM 里的 VPD 信息和读取 NVMe SSD 盘的管理信息。EP500、EP600 产品的 VPD 信息遵循《NVM Express Management Interface Revision 1.0》规范的要求。

BMC 通过带外管理功能，能获取 NVMe 盘的型号、健康状态、寿命、固件版本号等信息，方便客户对节点内的设备管理。

EP500、EP600 带外管理信息获取命令的 IIC 地址是 0x6A（不包含 R/W 位）。VPD 的 IIC 地址是 0x53（不包含 R/W 位）。

7 安全

7.1 安全架构

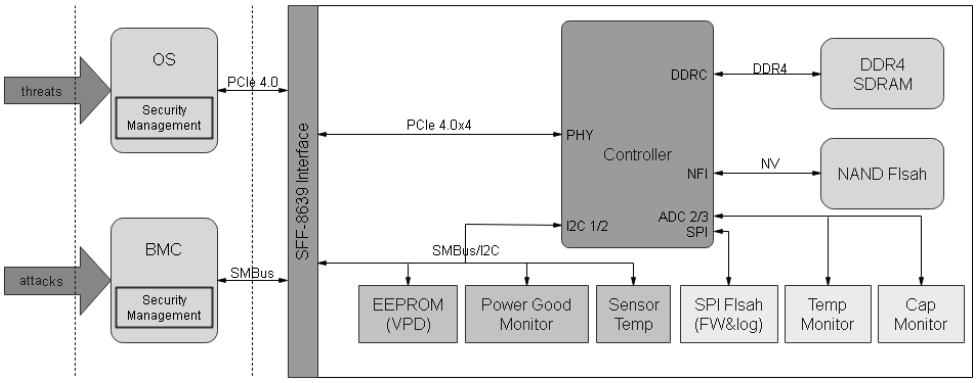
7.2 安全威胁及攻击

7.3 安全策略及措施

7.1 安全架构

根据 EP500、EP600 在系统中的逻辑位置，得出如下安全架构图。从图 7-1 可以看出，EP500、EP600 接口符合 NVMe 1.4 协议规范要求，各个操作系统平台通过标准磁盘 IO 接口进行数据读写。BMC 软件通过 SMBUS 接口进行带外管理操作，管理协议符合《NVM Express Management Interface Revision 1.0》规范的要求。标准磁盘 IO 接口和带外管理操作依托于 OS 和 BMC 两个系统的安全管理机制，产品本身涉及的安全风险相对很低。

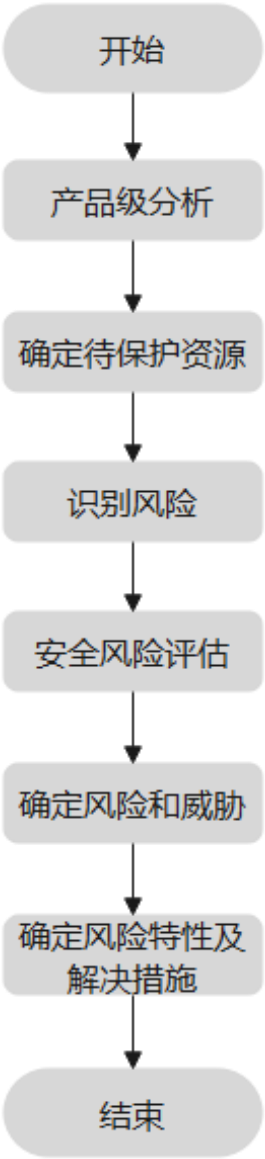
图7-1 安全架构图



7.2 安全威胁及攻击

通过图 7-2 识别 EP500、EP600 产品的安全威胁。

图7-2 风险评估流程



确定了涉及安全风险的产品元素及各自的风险评估如下。

主要元素	作用	有无风险	程度
NVMe Driver	SSD 的内核驱动，负责和块文件系统的	有	低

主要元素	作用	有无风险	程度
	交互和用户态的通信。		
CLI	用户态命令行接口，用以用户执行命令获取 SSD 的健康状态、温度等信息。	有	低
Firmware	NVMe 设备的前端协议处理模块，通过处理设备与主机之间的 I/O，实现对数据的传递和解析。	无	-
BMC interface	用户可以通过 BMC 对 SSD 设备进行管理，比如获取 SSD 的健康状态、温度信息等。	有	低

风险解决措施请参见 7.3 安全策略及措施。

7.3 安全策略及措施

一直理解，保障客户网络和业务的稳定安全运营是我们的首要责任。

作为服务器、存储等主机内部的一个存储设备，EP500、EP600 按着最小权限的安全准则做了安全增强措施，主要提供了如下功能：

- 权限控制：EP500、EP600 系列的设备控制工具都需要获得特殊的管理权限才能运行。用户不能随意修改盘内的设置。
- 操作日志：所有对 EP500、EP600 系列对所有的操作日志都做了记录。系统日志和关键日志分开存储。
- 端到端数据保护：EP500、EP600 系列采用端到端的数据校验，保证用户数据的一致性。并支持 T10 DIF 标准。
- 固件升级：EP500、EP600 系列对固件进行签名，只有能通过签名验证的固件才能正确激活。
- 带外管理：EP500、EP600 系列支持 I2C 的带外管理，提供查询功能。

8 认证

EP500、EP600 通过的各种准入认证 TBD。