ICS 35.240
CCS L70

团　体　标　准

T/CESA 1217—2022

计算机基本输入输出系统（BIOS）测试方法 第 2 部分：服务器

Test methods for computer basic Input output system

The Part 2：Server

22-07-21 发布　　2022-08-20 实施

中国电子工业标准化技术协会　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。

本文件由中国电子技术标准化研究院提出。

本文件由中国电子技术标准化研究院、中国电子工业标准化技术协会归口。

本文件起草单位：中国电子技术标准化研究院，华为技术有限公司、天津飞腾信息技术有限公司、龙芯中科技术股份有限公司、上海兆芯集成电路有限公司、无锡先进技术研究院、中电科技（北京）有限公司、南京百敖软件股份有限公司、阿里巴巴技术有限公司、统信软件技术有限公司、同方股份有限公司 腾讯科技(深圳)有限公司、浪潮电子信息产业股份有限公司、海光信息技术股份有限公司、中国长城科技集团股份有限公司。

本文件主要起草人：李雪莲、钟伟军、任翔、赵鑫、尹航、宋博伟、齐筱、宋东匡、沈莉梅、聂永丰、刘勇鹏、舒奕棋、李超、李强、刘景龙、牛彦奎、苏卫强，沈金祥、陈小春 任彤、吴平、高杰、李羿，常琳、张磊、占俊、耿成山 杨蔚才、李志高 蒋增增、张炳会，李道童、樊青松、何治平、黎建根、成联国。

计算机基本输入输出系统（BIOS）测试方法 第2部分：服务器

1 范围

本文件规定了服务器BIOS的设备支持要求、一般功能要求、接口要求、安全要求、能效要求、可靠性与可用性要求以及人机配置界面要求等方面的测试环境、测试项和测试方法。

本文件适用于服务器的设计和选型。

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。

高级配置与电源管理接口规范（ACPI Specification Version 6.3）

智能平台管理接口规范（IPMI Spefification V2.0 ）

DSP0266 Redfish规范 （Redfish Specification Version 1.11.0）

系统管理输入输出系统规范（SMBIOS Reference Specification, Version 3.3.0 ）

统一可扩展固件接规范（UEFI Specification Version 2.8）

3 术语和定义

下列术语和定义适用于本文件。

3.1

固件 firmware

固化到计算机中的非易失性存储器中的一组程序或软件。

3.2

基本输入/输出系统 basic input/output system

存于计算机主板上的固件，负责计算机开机时的硬件检测和初始化、操作系统安装和引导，并向操作系统提供计算机主板信息和服务接口。

3.3

统一可扩展固件接口 unified extensible firmware interface

当前应用最广泛的一种 BIOS 固件接口标准，描述操作系统和固件之间的接口。

3.4

基板管理控制器 baseboard management controller

部署于服务器主板上的具有独立供电、独立处理器、独立 I/O 接口的控制单元。

3.5

热键 hot key

BIOS 启动过程中能够响应的特定功能按键。

3.6

安全启动根 root of secure boot

安全启动的起点，是安全启动第一个被执行的程序，从它开始建立安全启动的可信链，保证整个

系统安全。

4 缩略语

下列缩略语适用于本文件。

ACPI：高级配置与电源管理接口（Advanced Configuration and Power Interface）

BIOS：基本输入输出系统（Basic Input Output System）

BMC：基板管理控制器（Baseboard Management Controller）

CPU：中央处理单元（Central Processing Unit）

ECC：错误检查和纠正技术（Error Checking and Correcting）

HDD：机械硬盘 （Hard Disk Drive）

HTTPS：安全超文本传输协议（Hypertext Transfer Protocol Secure）

IPMI：智能平台管理接口（Intelligent Platform Management Interface）

JEDEC：联合电子设备工程委员会 （Joint Electron Device Engineering Council）

KB：千字节 （Kilobyte）

OS：操作系统（Operating System）

PXE：预加载执行环境（Preboot eXecution Environment）

SMBIOS：系统管理基本输入/输出系统（System Management BIOS）

SPD：串行存在检测 （Serial Presence Detect）

SPI：串行外接口（Serial Peripherial Interface）

SSD：固态硬盘 （Solid State Drive）

TCM：可信加密模块（Trusted Cryptography Module）

UEFI：统一可扩展固件接口（Unified Extensible Firmware Interface）

USB：通用串行总线（Universal Serial Bus）

5 测试环境

5.1 测试辅助设备

测试辅助设备见表 1。

表 1 测试辅助设备

序号	类型	分类/说明
1	测试机	通过网线、串口线连接被测机，用于串口信息测试，PXE、HTTPS 启动测试等
2	VGA 显示器	用于连接被测机 VGA 输出
3	电/光口交换机	用于网络交换
4	USB 设备	闪存盘、USB 键盘、USB 光驱带商用 OS 安装光盘，用于 USB 相关特性测试
5	功率计	用于功耗测试
6	网线	网络连接

表 1 测试辅助设备（续）

7	串口线	串口连接
8	PCIe 网卡	用于相关测试项执行
9	PCIe RAID 卡	用于相关测试项执行
10	SAS 硬盘	用于相关测试项执行
11	SATA 硬盘	用于相关测试项执行
12	PCIe GPU 卡	用于相关测试项执行
13	PCIe SSD	用于相关测试项执行

5.2 测试工具

测试工具见表 2。

表 2　测试工具

序号	名称	用途	工具状态
1	ACPICA	在 OS 下进行 ACPI 解析	开源工具

6 测试方法

6.1　设备支持

6.1.1 内存

6.1.1.1 测试内容

测试 BIOS 对内存的支持情况。

6.1.1.2 测试方法

内存测试方法见表 3。

表 3　内存测试方法

序号	测试项	测试方法
1	BIOS 能正确识别和初始化处理器所能支持的内存模组类型（Level1）	1)　准备被测计算机支持的内存模组列表 2)　逐一安装所支持的内存模组，启动计算机至 BIOS 配置界面或者 OS 下，确认内存信息与实际一致，执行内存测试，正常通过测试； 3)　内存无法替换的情况下（如颗粒贴片），仅测试计算机自带内存。 4)　全部支持的内存模组测试正常表示通过，否则表示不通过

表 3　内存支持测试方法（续）

序号	测试项	测试方法
2	内存工作频率默认初始化成 CPU、内存共同支持且不高于 BIOS 配置界面设置的最高频率（Level1）	进入 BIOS 配置界面，分别设置内存频率大于、等于、小于内存模组标称频率，重启计算机，检查内存实际工作频率是 CPU、内存共同支持的最高频率，且执行内存测试能够正常通过测试表示通过，否则不通过。

6.1.2　存储设备支持

6.1.2.1　测试内容

测试 BIOS 对存储设备的支持情况。

6.1.2.2　测试方法

存储设备支持测试方法见表 4。

表 4　存储设备支持测试方法

序号	测试项	测试方法
1	BIOS 能正确识别和初始化不同接口或不同总线协议的存储设备（Level1）	1）　计算机连接有操作系统安装镜像的源存储设备（包含 USB 光驱、闪存盘），连接 SAS、SATA、PCIe 等接口的目标存储设备（包含 HDD 和 SSD），测试是否能从源存储设备向目标存储设备正常安装操作系统 2）　安装完成后重启计算机，验证是否能从目标存储设备正常启动步骤 1 安装的操作系统 3）　安装操作系统和启动操作系统都成功表示通过，否则不通过
2	BIOS 能从源存储设备将操作系统安装至目标存储设备中（Level1）	

6.1.3　输入输出设备支持

6.1.3.1　测试内容

输入输出设备支持测试 BIOS 对输入输出设备的支持情况。

6.1.3.2　测试方法

测试方法说明见表 5。

表 5　输入输出设备支持测试方法

序号	测试项	测试方法
1	BIOS 支持 USB 键盘（Level1）	计算机连接 USB 键盘，启动至 BIOS 配置界面，可通过 USB 键盘进行 BIOS 配置界面操作表示通过，否则不通过
2	BIOS 支持串口和 VGA 输出（Level1）	计算机连接串口线和 VGA 显示设备，启动计算机到 BIOS 配置界面，验证可通过串口输入输出、可通过 VGA 显示表示通过，否则不通过

6.1.4　板卡

6.1.4.1　测试内容

测试 BIOS 对板卡设备的支持情况。

6.1.4.2 测试方法

板卡测试方法说明见表 6。

表 6 板卡测试方法

序号	测试项	测试方法
1	BIOS 能正确地识别常见的 PCIe 板卡，正确分配资源（Level1）	1) 确定被测板卡列表，如网卡、RAID 卡、显卡等 2) 计算机接入 PCIe 板卡，启动计算机至 OS 下，检查对应的板卡的 PCIe 资源分配是否与需求相符，相符表示通过，否则不通过
2	BIOS 支持加载及运行板卡 UEFI 驱动（Level1）	1) 关闭安全启动 2) 准备自带 UEFI 驱动的 PCIe 板卡，UEFI 驱动所采用指令集属于被测计算机支持范围（下同） 3) 接入 PCIe 板卡，启动计算机，检查驱动是否可正常加载和运行，运行无错误表示通过，否则不通过
3	在安全启动使能的情况下，BIOS 支持对板卡的 UEFI 驱动做签名认证（level2）	1) 开启安全启动 2) 准备 UEFI 驱动经过正确签名和未经正确签名（包括未签名、签名错误、密钥不匹配等，下同）的 PCIe 板卡 3) 重复“板卡测试项 2 步骤 3”，经过正确签名的 PCIe 板卡驱动正常运行，未经正确签名的 PCIe 板卡驱动不被运行表示通过，否则不通过

6.1.5 BMC 支持

6.1.5.1 测试内容

测试 BIOS 对 BMC 支持情况，无 BMC 可跳过此项测试。

6.1.5.2 测试方法

BMC 支持测试方法说明见表 7。

表 7 BMC 支持测试方法

序号	测试项	测试方法
1	BIOS 能正确的初始化 BMC 中的显示和串口（Level1）	启动计算机，观察 BMC 的显示或串口设备，确认是否有 BIOS 启动的信息显示，有表示通过，否则不通过
2	BIOS 能识别和初始化 BMC 端虚拟输入设备（Level1）	参照“表 5 中序号 1”
3	BIOS 能识别和初始化 BMC 端虚拟媒体设备（Level1）	参照“表 4 中序号 2”，以 BMC 虚拟媒体设备作为源存储设备

表 7　BMC 支持测试方法（续）

序号	测试项	测试方法
4	BIOS 和 BMC 通信接口初始化，通信协议符合 IPMI 或 Redfish （Level1）	1）　在支持 IPMI 或 Redfish 协议的 BMC 界面，可获取（或查看）BIOS 相关信息，信息正确表示通过，否则不通过 2）　IPMI、Redfish 支持其一即可

6.2　一般功能

6.2.1　启动操作系统

6.2.1.1　测试内容

测试 BIOS 是否满足启动操作系统要求。

6.2.1.2　测试方法

启动操作系统的测试方法见表 8。

表 8　启动操作系统的测试方法

序号	测试项	测试方法
1	BIOS 加载启动操作系统的方式符合 UEFI 规范定义（Level1）	准备支持 UEFI 的商用发行版操作系统，在被测计算机上采用 UEFI 方式安装，能够正常完成操作系统安装，安装后能正常启动表示通过，否则不通过 可与“表 4 中序号 2”合并测试
2	BIOS 按启动项的先后顺序依次尝试启动项（Level1）	1）　准备计算机所支持的多种启动设备，包括网络（如 PXE）、USB 介质（如闪存盘、USB 光驱等）、硬盘（如 SAS、SATA 等）等，分别满足可启动和不可启动两种要求 2）　通过组合验证，检查是否满足按启动项顺序完成操作系统启动的要求，即当启动项不可启动时，能够跳到下一个启动项继续尝试，直到成功启动操作系统或持续循环则表示通过，否则不通过

6.2.2　文件系统支持

6.2.2.1　测试内容

测试 BIOS 是否满足文件系统支持要求。

6.2.2.2　测试方法

通过“6.2.1 启动操作系统要求”测试即表示此项测试通过。

6.2.3　BIOS 升级

6.2.3.1　测试内容

测试 BIOS 是否满足 BIOS 升级要求。

6.2.3.2 测试方法

BIOS 升级测试方法见表 9。

表 9 BIOS 升级测试方法

序号	测试项	测试方法
1	BIOS 升级操作与提示（Level1）	1) 执行 BIOS 升级操作，能够在无人工干预下完成升级，显示升级进度，并存在醒目提示信息，提示用户切勿断电或重启机器； 2) 升级完成后重启，BIOS 版本升级成功表示通过，否则不通过。 BIOS 升级方式满足带内升级、带外升级其一即可
2	用户设置的 BIOS 配置升级后保持不变（只适用新旧 BIOS 版本配置项相互兼容的情况）（Level1）	进入 BIOS 配置界面修改配置并保存，之后完成新 BIOS 版本升级，重启进入新 BIOS 配置界面，升级后用户配置与升级前相同表示通过，否则不通过。 新 BIOS 版本需与原 BIOS 版本 BIOS 配置项数据格式兼容
3	BIOS 升级应具备签名校验功能（Level1）	1) 分别升级正确签名和未经正确签名的 BIOS 镜像 2) 只有经正确签名的 BIOS 镜像能完成升级表示通过，否则不通过
4	带内安全升级，升级 BIOS 操作在 BIOS 下完成（Level2）	符合“6.4.7 BIOS 代码区域保护测试”情况下，成功完成带内 BIOS 升级表示通过，否则不通过

6.2.4 网络引导

6.2.4.1 测试内容

测试 BIOS 是否满足网络引导要求。

6.2.4.2 测试方法

网络引导测试方法说明见表 10。

表 10 网络引导测试方法

序号	测试项	测试方法
1	PXE 引导（Level1）	1) 在测试机搭建 PXE 引导环境，确保与被测机之间网络连接正常 2) 执行 BIOS PXE 启动，能够正常启动远程服务器上的 OS 表示通过，否则不通过
2	HTTPS boot（Level2）	1) 在测试机搭建 HTTPS boot 环境，确保与被测机之间网络连接正常 2) 执行 BIOS HTTPS 启动,能够正常启动远程服务器上的 OS 表示通过，否则不通过

6.2.5 诊断功能

6.2.5.1 测试内容

测试 BIOS 是否满足诊断功能要求。

6.2.5.2 测试方法

诊断功能测试方法说明见表 11。

表 11 诊断功能测试方法说明

序号	测试项	测试方法
1	BIOS 诊断信息输出方式（Level1）	测试 BIOS 诊断信息输出方式，进行信息收集或观察，只要支持调试端口、串口日志和内存日志中一种即表示通过，全部不支持表示不通过
2	BIOS 基础诊断信息：无内存（level2）	构造无内存，启动计算机，BIOS 诊断信息有正确体现表示通过，否则不通过
3	BIOS 基础诊断信息：内存初始化失败（Level1）	构造内存初始化故障，启动计算机，BIOS 诊断信息有正确体现表示通过，否则不通过
4	BIOS 基础诊断信息：无显示输出设备（level2）	构造无显示输出设备，启动计算机，BIOS 诊断信息有正确体现表示通过，否则不通过
5	BIOS 基础诊断信息：无启动设备（level2）	构造无启动设备场景，启动计算机，BIOS 诊断信息有正确体现表示通过，否则不通过

6.2.6 电源管理

6.2.6.1 测试内容

测试 BIOS 是否满足电源管理要求。

6.2.6.2 测试方法

电源管理测试方法见表 12。

表 12 电源管理测试方法

序号	测试项	测试说明
1	S0、S5 模式支持（Level1）	在不改变外接电源的情况下，进行开机、关机测试，覆盖所有支持的开关机操作，能够正常开机和关机表示通过，否则不通过

6.2.7 主板管理

6.2.7.1 测试内容

测试 BIOS 是否满足主板管理要求，无 BMC 可跳过此项测试。

6.2.7.2 测试方法

主板管理测试方法说明见表 13。

表 13　主板管理测试方法说明

序号	测试项	测试说明
1	BIOS 支持从 BMC 端的远程媒体挂载设备进行操作系统的安装（Level1）	参考“6.1.5 BMC 支持测试项 3”
2	BIOS 支持 BMC 端进行设备启动顺序的修改（Level1）	通过 BMC 修改 BIOS 启动项顺序，重启计算机，BIOS 启动顺序与 BMC 下发的一致则通过，否则不通过。至少测试 2 组不同的启动项顺序

6.3　接口

6.3.1　SMBIOS 测试

6.3.1.1　测试内容

测试 BIOS 是否满足 SMBIOS 要求。

6.3.1.2　测试方法

SMBIOS 测试方法见表 14。

表 14　SMBIOS 测试方法

序号	测试项	测试方法
1	BIOS 支持 SMBIOS 信息上报（Level1）	启动操作系统，通过 dmidecode 命令查看 BIOS 上报 SMBIOS，内容匹配实际则通过，否则不通过

6.3.2　ACPI

6.3.2.1　测试内容

测试 BIOS 是否满足 ACPI 要求。

6.3.2.2　测试方法

ACPI 测试方法说明见表 15。

表 15　ACPI 测试方法

序号	测试项	测试方法
1	BIOS 支持 ACPI 信息上报(level2)	启动操作系统，例如从/sys/firmware/acpi/tables 查看 BIOS 上报 ACPI，通过 ACPICA 工具解析上报信息正确则通过，否则不通过

6.3.3　内存映射

6.3.3.1　测试内容

测试 BIOS 是否满足内存映射要求。

6.3.3.2　测试方法

内存映射测试方法见表 16。

表 16　内存映射测试方法

序号	测试项	测试说明
1	BIOS 应向操作系统提供系统的内存布局和属性等信息（Level1）	1）　通过 UEFI 方式启动操作系统 2）　在 OS 下可以导出或查看 BIOS 上报的内存映射信息则通过，否则不通过
2	内存映射中运行时保留内存满足按 64KB 对齐（Level2）	1）　通过 UEFI 方式启动操作系统 2）　在 OS 下导出 BIOS 上报的内存映射信息，检查运行时保留的内存满足同一个 64KB 地址空间内只有一种页表属性则通过，否则不通过

6.3.4　运行时服务

6.3.4.1　测试内容

运行时服务测试 BIOS 是否满足运行时服务要求。

6.3.4.2　测试方法

测试方法说明见表 17。

表 17　运行时服务测试方法

序号	测试项	测试说明
1	GetTime/SetTime（Level1）	在 UEFI 方式启动的 Linux 中，可调用 GetTime 和 SetTime 进行时间获取和设置则通过，否则不通过
2	GetVariable/SetVariable（Level1）	1）　UEFI 方式启动的 Linux，通过 efivar 和 efimgr 命令查询和设置变量，分别覆盖有无 runtime 属性、有无 non-volatile 属性的变量 2）　只有 runtime 属性的变量才能访问（包括 get、set），且 non-volatile 属性的变量修改后重启计算机其值与前次设置值一致表示通过，否则不通过。注：non-volatile 属性变量测试选择 BIOS 配置界面可观测变量，在 OS 下设置，在 BIOS 配置界面检查
3	ResetSystem（Level1）	在 UEFI 方式启动的 Linux，通过 reboot 命令进行计算机重启，重启正常则通过，否则不通过

6.4　安全

6.4.1　BIOS 口令测试

6.4.4.1　测试内容

测试 BIOS 是否满足密码设置、管理及安全要求。

6.4.4.2 测试方法

BIOS 口令测试方法见表 18。

表 18 BIOS 口令测试方法

序号	测试项	测试方法
1	BIOS 支持管理员密码和普通用户密码两种密码（Level1）	可设置管理员密码和普通用户密码表示通过，否则不通过
2	BIOS 密码验证功能（Level1）	在设置密码后尝试进入 BIOS 配置界面，分别采用管理员密码、普通用户密码、错误密码（包括空密码），BIOS 能够做出正确响应表示通过，否则不通过
3	管理员密码权限（Level1）	1） 采用管理员密码登录 BIOS 配置界面 2） 所有操作无权限限制表示通过，否则不通过
4	普通用户密码权限（Level1）	1） 采用普通用户密码登录 BIOS 配置界面 2） 只能查看配置项和修改普通用户密码，其他操作受限，表示通过，否则不通过
5	密码复杂度校验（Level2）	分别构造满足和不满足长度、字符组合要求的密码进行密码设置（长度、字符组合相互独立），分别用于管理员密码和普通用户密码设置，同时观察密码不满足时原因信息提示，正确拦截不符合要求的密码且提示信息正确表示通过，否则不通过
6	密码非明文存储（Level1）	密码设置后，对存储介质（如 Flash）进行扫描，不存在密码明文表示通过，否则不通过
7	管理员密码历史密码不重复（Level2）	分别对管理员密码和普通用户密码进行测试，采用最近使用过的若干密码作为新密码进行设置，覆盖次数限制的边界 对管理员密码具备重复拦截功能，对普通用户密码无拦截功能表示通过，否则不通过
8	首次登录设置模式（Level2）	检查出厂不存在缺省密码，首次登录 BIOS 配置界面时强制要求设置管理员密码表示通过，否则不通过
9	密码防暴力破解（Level2）	分别对管理员密码和用户密码进行测试，分别执行连续使用错误密码登录测试、错误密码和正确密码混合使用测试，当连续错误次数超过次数限制后会锁定登录功能，测试达到要求的分钟数能正常登陆表示通过，否则不通过
10	密码操作记录日志（Level2）	经过历次密码测试后，日志信息能正确展示实际密码操作过程表示通过，否则不通过

6.4.2 安全启动

6.4.2.1 测试内容

测试 BIOS 是否满足安全启动要求，除特殊说明，安全启动测试中默认在开启安全启动的情况下进行。

6.4.2.2 测试方法

安全启动测试方法见表 19。

表 19 安全启动测试方法

序号	测试项	测试方法
1	BIOS 安全启动中只有签名校验通过的程序才能被运行（Level1）	对 BIOS 运行中每一个镜像构造正确签名和未经正确签名的情况，启动计算机，只有正确签名的镜像能被运行表示通过，否则不通过 注：测试中每一级镜像相互独立，覆盖每一个从外部（指 CPU 和内存之外，如 Flash）加载的边界
2	BIOS 支持 UEFI 规范定义的 Secure Boot 功能（Level1）	构造由 UEFI 变量中证书正确签名和未经正确签名镜像，BIOS 加载并启动正确签名的正确签名，而拒绝启动未经正确签名的镜像表示通过，否则不通过
3	BIOS 配置界面中支持对第三方证书的注册、删除（Level1）	通过第三方证书签名的镜像执行本表格测试项 1 测试，当第三方证书通过 BIOS 配置界面注册后，签名校验正确，删除后签名校验不正确，表示通过，否则不通过
4	安全启动应从安全启动根开始（Level2）	参考本表格测试项 1，安全启动根之外首个镜像只有签名校验通过才能被运行表示通过，否则不通过
5	管理员可以通过 BIOS 配置界面设置安全启动关闭或开启（Level1）	参考本表格测试项 1，登录 BIOS 配置界面关闭安全启动后，未正确签名的镜像可被运行表示通过，否则不通过

6.4.3 可信度量

6.4.3.1 测试内容

测试 BIOS 是否满足可信度量要求。

6.4.3.2 测试方法

可信度量测试方法见表 20。

表 20　可信度量测试方法

序号	测试项	测试方法
1	BIOS 自动识别、初始化可信模块（Level1）	具备可信模块的计算机，启动到 BIOS 配置界面，可见可信模块表示通过，否则不通过
2	BIOS 向 OS 报告可信模块信息（Level1）	进入 OS，能够识别和使用可信模块表示通过，否则不通过
3	BIOS 对关键部件进行度量，记录度量事件（Level1）	设置可信模块正常可用，启动到 OS，由 OS 收集度量结果和度量事件，可以通过度量事件重现度量过程和结果表示通过，否则不通过
4	BIOS 管理员配置界面支持可信模块的可用性配置（Level1）	以管理员身份登录 BIOS 配置界面，进行可信模块可用性配置，修改配置后参照本表格测试项 1、2、3 的测试方法，验证行为与可用性配置匹配表示通过，否则不通过
5	BIOS 管理员配置界面对可信模块度量值清除，及清除前的告警和确认（Level1）	以管理员身份登录 BIOS 配置界面，支持可信模块度量值清除，清除前的告警信息准确且必须经过确认表示通过，否则不通过

6.4.4　密码算法强度

6.4.4.1　测试内容

测试 BIOS 所采用的密码算法是否满足强度要求。

6.4.4.2　测试方法

密码算法强度测试方法见表 21。

表 21　密码算法强度测试方法

序号	测试项	测试方法
1	密码算法强度（Level1）	1)　由被测对象提供使用的密码算法（含相关参数）清单，对于非推荐算法，由被测对象同时提供具备与推荐算法同等安全性的证据 2)　清单中不存在私有算法，且通过白盒测试验证实际应用的算法与清单匹配表示通过，否则不通过

6.4.5 BIOS 密码加密算法

6.4.5.1　测试内容

测试 BIOS 所采用的密码算法是否满足强度要求。

6.4.5.2　测试方法

BIOS 密码加密算法测试方法见表 22。

表 22　BIOS 密码加密算法测试方法

序号	测试项	测试方法
1	BIOS 密码加密算法（Level1）	同 6.4.4 密码算法强度测试

6.4.6　密码算法中使用到的随机数

6.4.6.1　测试内容

测试 BIOS 密码算法所采用的随机数是否满足要求。

6.4.6.2　测试方法

密码算法中使用到的随机数测试测试方法说明见表 23。

表 23　密码算法中使用到的随机数测试方法

序号	测试项	测试方法
1	BIOS 密码算法中随机数使用（Level1）	同 6.4.4 密码算法强度测试

6.4.7　BIOS 代码区域保护

6.4.7.1　测试内容

测试 BIOS 是否满足 BIOS 代码区域保护要求。

6.4.7.1　测试方法

BIOS 代码区域保护测试方法测试方法见表 24。

表 24　BIOS 代码区域保护测试方法

序号	测试项	测试方法
1	BIOS 代码区域保护（Level2）	OS 下进行 BIOS 代码所在 Flash 区域写、擦测试，BIOS 代码区域未被改变表示通过，否则不通过

6.4.8　敏感信息处理

6.4.8.1 测试内容

测试 BIOS 是否满足敏感信息处理要求。

6.4.8.2　测试方法

敏感信息处理测试方法见表 25。

表 25　敏感信息处理测试方法

序号	测试项	测试方法
1	敏感信息处理（Level1）	1)　由被测对象自举证敏感信息处理措施 2)　评估上述措施可达到清除敏感信息效果，且通过白盒测试验证实际与被测对象提供的信息相符表示通过，否则不通过

6.5　能效要求测试（Level2）

6.5.1　CPU 调频功能测试

6.5.1.1　测试内容

测试 BIOS 是否满足 CPU 调频功能要求。

6.5.1.2　测试方法

CPU 调频功能测试方法见表 26。

表 26　CPU 调频功能测试方法

序号	测试项	测试方法
1	CPU 调频功能（Level1）	1)　由被测对象提供调频规格范围：包括上限、下限、区间粒度、对象粒度（如单核、整体）等 2)　在 OS 下调用 BIOS 提供的调频接口进行规格覆盖测试，结果与调频预期相符表示通过，否则不通过

6.5.2　CPU 休眠功能

6.5.2.1 测试内容

测试 BIOS 是否满足 CPU 休眠功能要求。

6.5.2.2 测试方法

CPU 休眠功能测试方法说明见表 27。

表 27　CPU 休眠功能测试方法

序号	测试项	测试方法
1	CPU 休眠功能（Level1）	1)　由被测对象提供休眠规格范围，如单核、整体等 2)　在 OS 下调用 BIOS 提供的休眠接口进行规格覆盖测试，结果与休眠预期相符表示通过，否则不通过

6.5.3　功耗封顶

6.5.3.1 测试内容

测试 BIOS 是否满足功耗封顶要求。

6.5.3.2 测试方法

功耗封顶测试方法见表 28。

表 28　功耗封顶测试方法

序号	测试项	测试方法
1	功耗封顶（Level1）	1）　被测对象提供单板功耗可控范围，作为功耗封顶可设范围 2）　架设单板功耗测试仪器 3）　稳定运行的业务使功耗趋于稳定，通过带内或带外（支持一种即可）设置功耗封顶值，短暂静置（去抖）后，观察功耗测试仪器测试结果不超过封顶值（允许 5%误差）表示通过，否则不通过 4）　覆盖封顶前功耗大于封顶值、小于封顶值，封顶值越界等场景

6.6　硬件故障处理能力（Level2）

6.6.1　硬件故障处理与上报

6.6.1.1　测试内容

测试 BIOS 是否满足硬件故障处理与上报要求。

6.6.1.2　测试方法

硬件故障处理与上报测试方法见表 29。

表 29　硬件故障处理与上报测试方法

序号	测试项	测试方法
1	硬件故障处理（Level1）	1）　由被测对象提供的硬件故障处理特性清单，说明能够覆盖哪些硬件故障，分别做怎样的处理 2）　模拟硬件故障（可以是硬件模拟、软件注入故障模拟，软件注入故障方法由被测对象提供），观测并评估故障处理符合预期表示通过，否则不通过
2	BIOS 硬件故障上报（Level1）	本表格测试项 1 中每一条涉及上报的测试中，从 OS 和 BMC（如果涉及）输出接收到的故障上报信息，检查信息正确表示通过，否则不通过

6.6.2　启动阶段故障核隔离

6.6.2.1　测试内容

测试 BIOS 是否满足启动阶段故障核隔离要求。

6.6.2.2 测试方法

启动阶段故障核隔离测试方法说明见表 30。

表 30 启动阶段故障核隔离测试方法

序号	测试项	测试方法
1	启动阶段故障核隔离（Level1）	1) 被测对象提供的硬件故障处理特性清单包含此项，且通过“6.6.1 硬件故障处理与上报测试” 2) 启动到 OS，检查 OS 所获得的核信息，已排除故障核表示通过，否则不通过
2	BIOS 配置界面可开启和关闭（Level1）	BIOS 配置界面可配置核故障隔离开启核关闭，关闭后执行本表格测试项 1，无核隔离表示通过，否则不通过

6.6.3 内存 ECC

6.6.3.1 测试内容

测试 BIOS 是否满足内存 ECC 功能要求。

6.6.3.2 测试方法

内存 ECC 测试方法见表 31。

表 31 内存 ECC 测试方法

序号	测试项	测试方法
1	内存 ECC（Level1）	被测对象提供的硬件故障处理特性清单包含此项，且通过“6.6.1 硬件故障处理与上报测试”表示通过，否则不通过

6.6.4 启动阶段内存故障隔离

6.6.4.1 测试内容

测试 BIOS 是否满足初始化阶段内存故障隔离功能要求。

6.6.4.2 测试方法

启动阶段内存故障隔离测试方法见表 32。

表 32 启动阶段内存故障隔离测试方法

序号	测试项	测试方法
1	启动阶段内存故障隔离（Level1）	被测对象提供的硬件故障处理特性清单包含此项，且通过“6.6.1 硬件故障处理与上报测试”表示通过，否则不通过
2	启动阶段内存故障隔离功能配置（Level1）	BIOS 配置界面可配置此功能开启和关闭，关闭后，执行本表格测试项 1，BIOS 在检测到内存错误后停止继续运行表示通过，否则不通过

6.7 人机配置界面要求

6.7.1 支持热键操作

6.7.1.1 测试内容

测试 BIOS 是否满足热键操作要求。

6.7.1.2 测试方法

支持热键操作测试方法见表 33。

表 33 支持热键操作测试方法

序号	测试项	测试方法
1	热键操作（Level1）	由被测对象提供热键功能清单，分别验证热键功能符合预期表示通过，否则不通过

6.7.2 BIOS 配置界面要求

6.7.2.1 测试内容

测试 BIOS 是否满足配置界面功能要求。

6.7.2.2 测试方法

BIOS 配置界面要求测试方法见表 34。

表 34 BIOS 配置界面要求测试方法

序号	测试项	测试方法
1	系统基本信息（Level1）	BIOS 配置界面系统基本信息显示与实际一致表示通过，否则不通过
2	中英文显示（Level1）	1) 检查各界面显示，符合中文汉字或英文 2) 如果支持中英文切换，覆盖中英和英中切换，切换后显示正确表示通过，否则不通过
3	硬件相关配置（Level1）	1) 由被测对象提供 BIOS 配置界面硬件可配置特性清单 2) 可配置特性满足规范要求，并逐一进行测试验证 3) 全部符合表示通过，否则不通过
4	BMC 版本显示和 IP 配置（有 BMC 的情况下测试)(Level1)	进入 BIOS 配置界面，分别执行 BMC 版本信息查询、IP 查询和配置，与 BMC 界面查到的信息匹配表示通过，否则不通过
5	看门狗配置（Level1）	进入 BIOS 配置界面，分别进行看门狗开关配置、超时时间配置，看门狗超时后执行策略配置，配置后结果符合预期表示通过，否则不通过
6	BIOS 密码设置和清除（Level1）	通过“6.4.1 BIOS 密码测试”中测试项 3 管理员密码权限、测试项 4 普通用户密码权限中关于 BIOS 密码设置和清除时表示通过，否则不通过
7	启动项优先级配置（Level1）	修改启动项优先级，重复执行“6.2.1 启动操作系统要求 测试项 2 BIOS 按启动项的先后顺序依次尝试启动项覆盖”，符合预期表示通过，否则不通过

表 34　BIOS 配置界面要求测试方法（续）

序号	测试项	测试方法
8	恢复默认配置功能	通过 BIOS 配置界面修改配置并保存后，执行恢复默认配置，正常恢复表示通过，否则不通过，需覆盖每一个可配置项