PCI 扩展 ROM 控制芯片 CH364

硬盘和网络安全隔离卡方案

版本： 1

http://wch.cn

1、概述

安全隔离卡用于将普通计算机分为安全环境（内网）和开放环境（外网），内网和外网使用不同的硬盘并且连接到不同的网络，从而能够避免硬盘中的重要数据通过网络等方式泄露。一般的双网卡方案、多重引导卡或者多用户管理卡只是在逻辑层提供硬盘数据隔离，而硬盘和网络安全隔离卡的特点主要是在物理层提供硬盘数据隔离，确保更高的数据安全性。技术方案有：

A、 单网卡、双硬盘物理切换隔离；

B、 通过外部硬件在 IDE 接口拦截硬盘命令实现的单硬盘物理隔离；

C、 利用硬盘特性“Address Offset Mode”和“Set Max”实现的单硬盘物理隔离。

方案 B 偏重于硬件设计，硬件设计不佳就容易导致硬盘数据传输速度下降或者产生主板兼容性问题，所以技术难度较大。方案 C 充分利用了硬盘自身的技术特性，偏重于软件设计，硬件成本最低，但是部分硬盘还不支持“Address Offset Mode”特性。方案 A 的技术最简单，也最可靠，是真正的物理隔离。无论哪一种技术方案，通常都需要在启动时选择内网或者外网，这些选择界面和切换操作通常由扩展 ROM 中的启动程序完成。

这里主要讨论技术方案 A，大多数内容也适用于技术方案 B 和 C。另外，专门针对方案 C 的技术方案可以向合作厂家提供参考版源程序，用于制作更低成本的单网卡、单硬盘的网络安全隔离卡。

2、用户的功能需求分析

① 用户需要在开机后选择将使用内网的安全环境，还是外网的开放环境，所以安全隔离卡应该能够在开机时向用户提供选择界面。通常可以由安全隔离卡自身提供的扩展 ROM 程序实现，该程序运行于 DOS 或者 Windows 等操作系统引导之前。

② 当用户选择完后，安全隔离卡需要执行内外网的环境切换，也就是说，扩展 ROM 程序能够根据用户的选择通知隔离卡进行切换。如果更智能些，隔离卡应该能够判断当前的网络环境，如果已经是所需要的网络环境则不必切换。

③ 当启动时切换选择后，必须确保不能在 Windows 等操作系统的运行过程中被无意或者恶意的切换，否则将导致硬盘数据不完整以及数据通过外网泄露，所以安全隔离卡需要一个切换锁定装置。当隔离卡在启动时切换完成后，必须有一个锁定装置保证不会再执行其它任何切换，而在重新开机或者重新启动后，锁定装置自动解除，从而可以由隔离卡自身的扩展 ROM 程序根据用户的选择重新进行切换。

④ 美观需求。早期产品是从计算机后壳引出电线接一个电器开关到桌面，由用户随时拨动开关，所以就很难做到美观，也不完全，容易无意中碰到，完全不象一个高科技的 IT 产品。

⑤ 方便性和智能化，体现在软件功能上。新式的隔离卡通常采用扩展 ROM 程序，根据用户的使用习惯提供仿 Windows 中文界面和智能提示，以及个性化的启动图片。

⑥ 软硬件的兼容性，由所采用的技术方案而定。例如，IDE 接口只用于硬盘和光驱产品，当前的 UDMA133 硬盘工作在 133MHz 高频上，如果通过拦截硬盘 IDE 接口获取扩展 ROM 发出的切换指令，那么就会增加 IDE 接口的负载，从而很容易产生主板兼容性问题，或者影响硬盘数据的传输速度，好的技术方案应该尽量采用成熟的标准化技术，例如通过 PCI 总线的 I/O 端口获取扩展 ROM 发出的切换指令。

3、我们的技术方案

根据上述分析，可以采用 PCI 扩展 ROM 专用控制芯片 CH364P，因为：

① CH364 支持扩展 ROM，并且可以使用厂家随芯片提供的免费授权使用的 BRM 程序库，包括约 120 个通用子程序，基于 BRM 程序库和参考样例，设计扩展 ROM 程序将非常容易。

② CH364 具有 I/O 端口读写功能，可以在标准的 PCI 总线上获得扩展 ROM 发出的切换指令以及当前网络环境，用于实现内外网络环境切换和判断。

③ CH364 具有支持锁定的控制输出引脚，可以实现切换锁定，具有重启时自动加载的控制信号，方便在 WINDOWS 下进行切换。

④ CH364 提供 Flash-ROM 闪存，支持在线擦写，便于在用户端远程升级，容量从 64KB 到 1MB，可以记忆用户上次的选择，也可以记忆进入内网时所需的密码，或者保存产品序列号等。

另外，真正的安全性必须是在公开技术方案后仍然保持原来的安全性，基于 CH364P 设计的安全隔离卡，由于通过 I/O 端口获取切换指令并且采用切换锁定技术，所以，在公开技术方案的情况下，依然能够保持原来的安全性，而不怕任何恶意的程序和病毒。

4、基本原理图

与 CH365 方案相比，由于 CH364P 是专用的扩展 ROM 控制芯片，所以除了 CH364 芯片组之外，无需其它任何芯片，只要外加物理切换器件即可，不但提高了性能，而且综合成本更低。

完整的物理切换电路请参考隔离卡评估板的技术资料光盘。

5、扩展 ROM 程序设计

以下是与硬件相关的切换和锁定等部分 C 语言程序，IO_BASE_ADDR 由 BRM 提供。

```
ctrl_port = IO_BASE_ADDR + CH363_CFG_CTRL;
lock_port = IO_BASE_ADDR + CH363_CFG_DOUT;
```

① 读取当前切换状态和锁定状态（假定继电器不吸合为内网）

```
s = inportb ( ctrl_port )
if ( s & 0x02 ) { 正在外网 }
else { 正在内网 }
if ( inportb ( lock_port ) & 0x10 ) { 正在锁定状态 }
else { 正在准备状态，没有锁定状态 }
```

② 设定新的切换状态和锁定状态（假定继电器不吸合为内网）

```
if ( 需要选择外网 ) { s = 0x0A; }
else { s = 0x00; }  /* 选择内网 */
outportb ( ctrl_port, s );  /* 设定切换状态 */
if ( 需要锁定状态 ) { outportb ( lock_port, inportb ( lock_port ) | 0x10 ); }
```

③ 读写 I^2C 接口的串行 EEPROM 芯片 24Cxx

请参考 BRM 子程序_CH363_I2C7_BYTE_R 和_CH363_I2C7_BYTE_W 及 CH363_I2C7_BLK_R 等

④ 读写 Flash-ROM 闪存

请参考 BRM 子程序_CH364_FLASH_READ 和_CH364_FLASH_WRITE 及_CH364_FLASH_ERASE 等

为了加速和简化扩展 ROM 程序设计，CH364 还可以提供与之配套的 BRM 应用子程序库，其中包括 640x480x16 色或者 800x600x256 色仿 Windows 中英文图形界面程序库、图片显示程序库、硬盘文件读写操作程序库、Boot-ROM 启动程序库、数据解压缩程序库、字符串处理程序库、杂项程序库，这

些子程序都能够在 BIOS 环境下运行，无需 DOS 等操作系统，另外，还可以提供与之配套的多国语言字库提取工具等。基于专业的 BRM 程序库设计隔离卡的扩展 ROM 程序将非常简单，可以不需要考虑主板兼容性，不需要考虑硬盘存取、中英文图形显示等各种底层 I/O 操作。相关说明也可参考 CH36x 通过 Boot-ROM 进行 BIOS 扩展的方案。

6、隔离卡评估板

双硬盘隔离卡评估板套件包括：

一块隔离卡样品，默认支持 PATA 并口硬盘切换，可以另选 SATA 串口硬盘切换小板。

技术资料光盘，包括成本预算及简单中文说明；

隔离卡样板的电路原理图和 PCB 印制板图；

BRM 子程序库 V2.2 和 V3.X（支持 800x600x256 色）；

隔离卡扩展 ROM 源程序；

WINDOWS 环境下的切换工具的源程序。

单硬盘隔离方案主要依赖于硬盘自身安全特性和 BRM 程序库中提供的相关子程序，而其硬件更为简单，当然也可以直接使用双硬盘隔离卡的硬件，单硬盘隔离方案主要包括另外一套扩展 ROM 源程序。

关于批量产品的成本预算，请联系业务人员。