PCI 总线接口芯片 CH365

硬盘和网络安全隔离卡方案

（第一版 1A）

南京沁恒电子有限公司
www.winchiphead.com

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测试版，用于制作更低成本的单网卡、单硬盘的网络安全隔离卡。

2、最终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，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 总线通用接口芯片 CH365，因为：

① CH365 支持扩展 ROM，并且可以使用厂家免费授权使用的 BRM 程序库，包括 80 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。

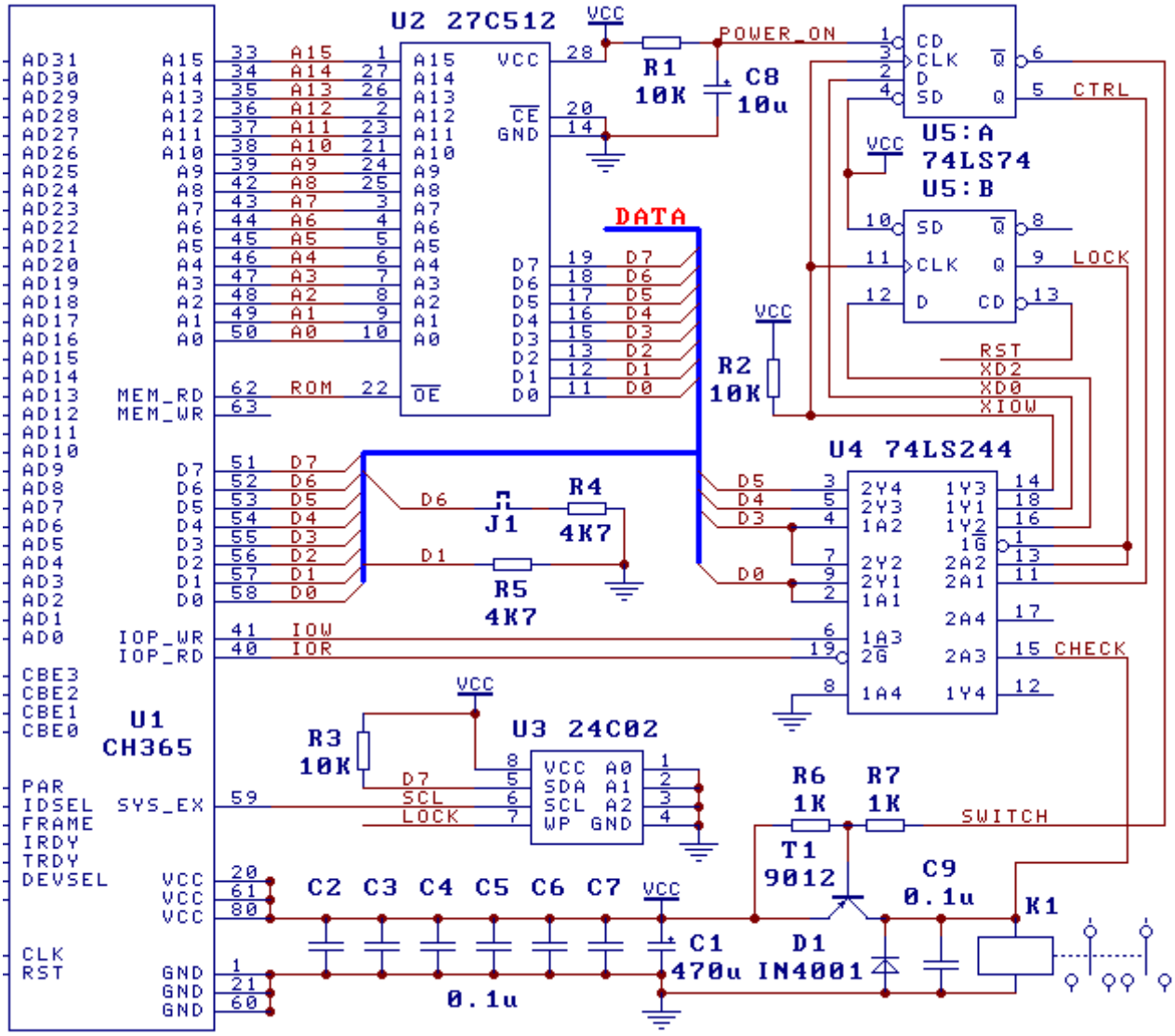
② CH365 具有 I/O 端口读写功能，可以在标准的 PCI 总线上获得扩展 ROM 发出的切换

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，另外还可以通过扩展外围电路实现切换锁定。

③ CH365 支持 I²C 接口，如果连接一个低成本的串行 EEPROM，则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 CH365 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（详细的物理切换电路请参考隔离卡评估板的技术资料光盘）



5、电路说明

- U1 是 CH365 芯片，但不宜使用不支持 I/O 端口写的 CH362。如果使用 CH362 则需要另外加一个至少 44 脚的 CPLD 芯片，总成本至少增加二十元。
- U2 是 ROM 芯片，用于存放扩展 ROM 程序。由于内外网络切换和锁定指令只需要两条 I/O 指令，加上启动选择界面等部分后，扩展 ROM 程序仍然很小，通常为 8KB 至 64KB，所以可以使用 27C512、27C256、27C128 甚至 27C64 等 ROM 芯片。如果需要支持在线程序升级等附加功能，也可以使用 Flash 闪存 29C512、29C010 或者

29F010 等，并且闪存的 WR 或者 WE 引脚连接到 CH365 的 MEM_WR 引脚。

- U3（24C01A 或者 24C02 芯片）是可选元器件，可以用于记忆用户的使用习惯，保存进入内网时的安全密码等，隔离卡厂家也可以用其保存产品序列号、扩展 ROM 的启动模式、工作模式等，由于其成本很低，建议使用该器件。
- 如果使用 CH365 的单芯片扩展 ROM 方案，则可以省掉 U2 的 ROM 芯片，而将 U2 和 U3 合二为一。采用单芯片方案后，扩展 ROM 程序可以放在 U3 中，从而也可以支持在线升级，当然，U3 的容量就要更大，例如 24C08 或者 24C16 等芯片。
- 跳线 J1 和电阻 R4 是可选器件，由用户根据需要设定跳线，从而使扩展 ROM 卡采用不同的启动模式、工作模式等。如果不插跳线，则数据线 D6 默认为高电平；如果插上跳线，则数据线 D6 默认为低电平。扩展 ROM 中的程序可以随时读取由跳线设定的默认电平，作为程序中的参数。如果使用 U3，则通常可以省掉 J1 和 R4。
- 电阻 R5 是可选的，用于设定 PCI 板卡也就是隔离卡的厂商 ID 和设备 ID，不用 R5 时隔离卡使用 CH365 的默认 ID 值。建议使用，如果使用 R5，则需要在 ROM 中 PCI 配置空间映象区域（ROM 的 0040H～007FH 地址范围）设置相应的数据。
- U4 和 U5 实现切换寄存和切换锁定，U4 是 74LS244 芯片，U5 是 74LS74 芯片，都是很普通的 TTL 芯片，本方案不建议使用 CMOS 芯片。详细工作原理见后。
- 电容 C1 和 C2 至 C7 是电源退耦电容，C1 是容量不小于 100uF 的电解电容，C2 至 C7 是容量为 0.1uF 的高频贴片电容。实际电路应该对继电器 K1 独立供电以减少干扰，所以继电器 K1 的电源电路中还需要一个电解电容和一个高频贴片电容。
- 电阻 R1 和电容 C8 用于向 U5A 提供上电复位，C8 是电解电容。
- 电阻 R2 用于在 U4 的 1G 三态输出关闭后保持 XIOW 也就是 U5 的 CLK 的稳定，如果 U5 是 TTL 芯片，则 R2 可以省掉。
- 电阻 R3 用于向 I^2C 接口的 SDA 信号线提供上拉，如果没有抗干扰的要求，则 R3 可以省掉，而 SDA 可以使用 CH365 内置的弱上拉。
- 三级管 T1 和电阻 R6 及 R7 是继电器 K1 的功率驱动电路，二级管 D1 和电容 C9 是针对继电器等电感性负载的安全保护和抗干扰措施。如果实际需要切换的网络线和硬盘线比较多，那么可以采用多个双刀双掷的继电器，其驱动控制端并联后由 T1 进行驱动。T1 是 PNP 三级管 9012 或者 8550，T1 和 D1 的驱动电流都不能小于所有继电器吸合所需驱动电流的总和。

6、切换和锁定的工作原理

D 触发器 U5A 用于保存切换状态，D 触发器 U5B 用于保存锁定状态。

4 位三态缓冲 U4 的 1G 用于缓冲或者锁定切换指令，4 位三态缓冲 U4 的 2G 用于查询切换状态和锁定状态等。

开机后，U5A 由 R1 和 C8 复位为低电平，其 Q 端输出低电平，T1 不驱动，继电器选择内网。U5B 由 PCI 总线复位 RST 复位，其 Q 端输出低电平，对应于没有锁定状态，隔离卡进入准备状态。

当扩展 ROM 接收到用户的选择后，首先通过 I/O 读取当前切换状态，不匹配则通过 I/O 端口向 U5A 发出切换选择，U5A 控制 T1，由 T1 驱动继电器选择内外网。

当内外网切换和对 U3 的写操作完成后，扩展 ROM 程序通过 I/O 端口向 U5B 发出锁定指令，U5B 输出高电平，所以 U4 的 1G 输出禁止，XIOW、XD0、XD2 保持不变，从而使 U5A 和 U5B 中的数据保持不变，隔离卡进入锁定状态。

当计算机重新开机或者重新启动时，由于 RST 信号线将 U5B 复位，导致隔离卡解除锁定状态，而进入准备状态，从而可以由扩展 ROM 程序重新选择网络环境。重新启动不会影响 U5A 中的数据，所以重新启动本身不会导致网络环境改变或者恢复为默认值。

当隔离卡进入锁定状态后，U3 的 WP 引脚由 LOCK 驱动为高电平，所以 U3 中的数据也将被写保护，只能读取而不能写入，从而确保 U3 中的数据不会被意外或者恶意改写。

当内外网的硬盘参数不同时，切换网络环境后必须重新启动。为了防止重启后扩展 ROM 程序再次要求用户进行选择，可以在 U3 中设置一个标志，当重启后扩展 ROM 检测到这个标志则在锁定状态后直接引导操作系统，而不必再出现选择界面。

从 I/O 端口读取的字节数据中：位 0 是当前切换状态；位 3 是当前锁定状态；位 4 在正常情况下也是当前切换状态，准确地说，是继电器工作状态；位 5 暂未使用，可以用于检测硬盘是否工作等。

向 I/O 端口写入的字节数据中：位 0 是设定切换状态；位 3 是设定锁定状态。当进入锁定状态后，隔离卡将保持当前状态，不再接受新写入的数据。

7、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。

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 ( IO_BASE_ADDR )
if ( s & 1 ) { 正在外网，必要时可以再复查( s & 0x10 ) }
else { 正在内网，必要时可以再复查 s 的位 4 }
if ( s & 8 ) { 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 = 1; }
else if ( 需要选择内网 ) { s = 0; }
outportb ( IO_BASE_ADDR, s );                /* 设定切换状态 */
if ( 需要锁定状态 ) { outportb ( IO_BASE_ADDR, s | 8 ); }
```

③ 读写 I^2C 接口的串行 EEPROM 芯片 24Cxx

请参考 BRM 子程序 CH36_READ_I2C 和 CH36_WRITE_I2C

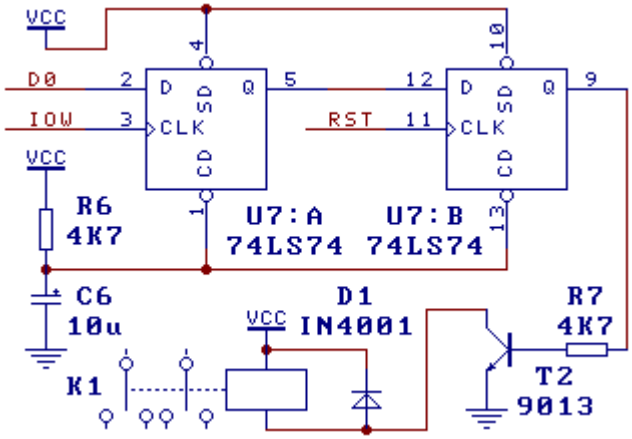
为了加速和简化 ROM 程序设计，CH365 还可以提供与之配套的 BRM 应用子程序库，包括 640x480x16 色或者 800x600x256 色仿 Windows 中英文图形界面程序库、硬盘文件读写操作程序库、Boot-ROM 启动程序库、数据解压缩程序库、字符串处理程序库、杂项程序库，这些子程序都能够在 BIOS 环境下运行，无需 DOS 等操作系统，另外，还可以提供与之配套的多国语言字库提取工具等。基于 BRM 程序库设计隔离卡的扩展 ROM 程序将非常简单，更多相关说明请参考 CH36x 通过 Boot-ROM 进行 BIOS 扩展的方案。

8、另一种不需要切换锁定的硬盘和网络切换方法

参考下图，电阻 R6 和电容 C6 用于在刚打开电源时复位 D 触发器 U7A 和 U7B。当用户作出切换选择后，应用程序将用户的选择通过 I/O 写指令送给 U7A 保存。D 触发器 U7B 的时钟线连接到 PCI 总线的复位信号线 RST，当复位完成后，RST 由低变高，其上升沿将来自 U7A 的选择保存到 U7B 中，U7B 控制三极管 T2 进行物理切换。无论用户在什么时候做出选择，真正的物理切换总是在复位期间进行的，并且扩展 ROM 程序还可以在引导操作系统前对切换状态结果进行校验，防止恶意的物理切换，所以技术上也比较安全。

如果不考虑切换的安全性，继电器还可以由 CH365 的 A15 引脚控制的三极管直接进行驱动。在任何时候需要进行切换时，只要在程序中发出一个 I/O 指令，使 CH365 的 A15 改变一下电平就可以了。A15 引脚在系统复位时为低电平，在系统复位后默认是高电平，也可以设定工作模式修改为默认是低电平。A15 引脚是锁存输出引脚，引脚电平一直保持

不变，直到 CH365 被系统复位或者应用程序再通过 I/O 指令对其进行重新设置。



9、安全隔离卡评估板

双硬盘隔离卡评估板套件包括：

一块隔离卡样品。

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）；

一个隔离卡扩展 ROM 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。