(19)中华人民共和国国家知识产权局

(12)实用新型专利

(10)授权公告号 CN 205249258 U
(45)授权公告日 2016.05.18

(21)申请号 201521086256.5

(22)申请日 2015.12.23

(73)专利权人 深圳市祈飞科技有限公司
地址 518048 广东省深圳市福田区新洲路深圳国际商会大厦(B座)1705、1706单元

(72)发明人 阮仕涛

(74)专利代理机构 深圳市顺天达专利商标代理有限公司 44217
代理人 李琴

(51)Int.Cl.
H04L 12/46(2006.01)

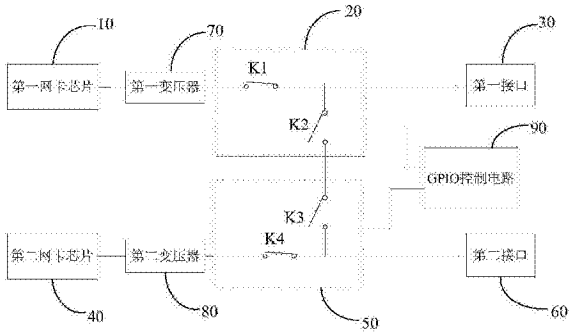
权利要求书1页 说明书3页 附图1页

(54)实用新型名称

一种BYPASS系统

(57)摘要

本实用新型公开了一种BYPASS系统，包括依次连接的第一网卡芯片、第一继电器开关电路和第一接口，依次连接的第二网卡芯片、第二继电器开关电路和第二接口，第一继电器开关电路包括第一继电器开关、第二继电器开关，第二继电器开关电路包括第三继电器开关和第四继电器开关；第一继电器开关连接在第一网卡芯片和第一接口之间，第四继电器开关连接在第二网卡芯片和第二接口之间，第二继电器开关和第三继电器开关依次连接在第一继电器开关和第一接口的连接点和第四继电器开关和第二接口的连接点之间。实施本实用新型的有益效果是，在网络安全设备断电或关机情况下能够实现自动关闭BYPASS功能。



CN 205249258 U

1.一种BYPASS系统，用于在网络安全设备处于断电或关机情况下时能够自动关闭BYPASS功能，其特征在于，包括依次连接的第一网卡芯片、第一继电器开关电路和第一接口以及依次连接的第二网卡芯片、第二继电器开关电路和第二接口，所述第一继电器开关电路包括第一继电器开关、第二继电器开关，所述第二继电器开关电路包括第三继电器开关和第四继电器开关；

所述第一继电器开关连接在所述第一网卡芯片和所述第一接口之间，所述第四继电器开关连接在所述第二网卡芯片和所述第二接口之间，所述第二继电器开关和第三继电器开关依次连接在所述第一继电器开关和第一接口的连接点和所述第四继电器开关和第二接口的连接点之间；其中：所述第一继电器开关和所述第四继电器开关在初始状态时处于导通状态，所述二继电器开关和第三继电器开关在初始状态时处于断开状态。

2.根据权利要求1所述的BYPASS系统，其特征在于，所述BYPASS系统还包括分别与所述第一继电器开关电路和第二继电器开关电路连接的GPIO控制电路，所述GPIO控制电路用于在网络安全设备上电时控制打开或关闭BYPASS功能。

3.根据权利要求1所述的BYPASS系统，其特征在于，所述BYPASS系统还包括连接在所述第一网卡芯片和所述第一继电器开关之间的第一变压器，所述第一变压器用于调节由所述第一网卡芯片接收的第一输入网络信号的电压。

4.根据权利要求3所述的BYPASS系统，其特征在于，所述第一变压器的型号为GST5009。

5.根据权利要求1所述的BYPASS系统，其特征在于，所述BYPASS系统还包括连接在所述第二网卡芯片和所述第四继电器开关之间的第二变压器，所述第二变压器用于调节由所述第二网卡芯片接收的第二输入网络信号的电压。

6.根据权利要求5所述的BYPASS系统，其特征在于，所述第二变压器的型号为GST5009。

7.根据权利要求1所述的BYPASS系统，其特征在于，所述第一接口和所述第二接口为RJ45接口。

一种BYPASS系统

技术领域

[0001] 本实用新型涉及网络通讯领域，更具体地说，涉及一种在网络安全设备断电或关机情况下能够实现自动关闭BYPASS功能的BYPASS系统。

背景技术

[0002] 工控电脑主机和网络安全设备通常设有多个网口，用于与局域网端的多个网络进行连接，从而实现多网络段之间的同时通信。但是如果主机和设备发生故障，比如异常断电或者关机，那通过这台设备所连接的所有网络都会终止，并且设备的网口之间也会失去联系。为了在断电和关机情况下还能实现内部网络之间的互通，大多数主机和设备都会采用BYPASS功能。

[0003] 一般网络安全设备在断电或关机情况下会打开BYPASS功能，即内部网路之间是连通的。但在工业领域的某些应用中，为了提高局域网络中设备运行的安全性，要求设备在断电或关机后能关闭系统的BYPASS功能，即内部网络之间不再互通。

实用新型内容

[0004] 本实用新型要解决的技术问题在于，针对现有技术的上述在网络安全设备断电或关机情况下会打开BYPASS功能的缺陷，提供一种在网络安全设备断电或关机情况下能够实现自动关闭BYPASS功能的BYPASS系统。

[0005] 本实用新型解决其技术问题所采用的技术方案是：一种BYPASS系统，用于在网络安全设备处于断电或关机情况下时能够自动关闭BYPASS功能，包括依次连接的第一网卡芯片、第一继电器开关电路和第一接口，依次连接的第二网卡芯片、第二继电器开关电路和第二接口，所述第一继电器开关电路包括第一继电器开关、第二继电器开关，所述第二继电器开关电路包括第三继电器开关和第四继电器开关；

[0006] 所述第一继电器开关连接在所述第一网卡芯片和所述第一接口之间，所述第四继电器开关连接在所述第二网卡芯片和所述第二接口之间，所述第二继电器开关和第三继电器开关依次连接在所述第一继电器开关和第一接口的连接点和所述第四继电器开关和第二接口的连接点之间；其中：所述第一继电器开关和所述第四继电器开关在初始状态时处于导通状态，所述第二继电器开关和第三继电器开关在初始状态时处于断开状态。

[0007] 在上述BYPASS系统中，所述BYPASS系统还包括分别与所述第一继电器开关电路和第二继电器开关电路连接的GPIO控制电路，所述GPIO控制电路用于在网络安全设备上电时控制打开或关闭BYPASS功能。

[0008] 在上述BYPASS系统中，所述BYPASS系统还包括连接在所述第一网卡芯片和所述第一继电器开关之间的第一变压器，所述第一变压器用于调节由所述第一网卡芯片接收的第一输入网络信号的电压。

[0009] 在上述BYPASS系统中，所述第一变压器的型号为GST5009。

[0010] 在上述BYPASS系统中，所述BYPASS系统还包括连接在所述第二网卡芯片和所述第

四继电器开关之间的第二变压器，所述第二变压器用于调节由所述第二网卡芯片接收的第二输入网络信号的电压。

[0011] 在上述BYPASS系统中，所述第二变压器的型号为GST5009。

[0012] 在上述BYPASS系统中，所述第一接口和所述第二接口为RJ45接口。

[0013] 实施本实用新型的BYPASS系统，具有以下有益效果：因第一继电器开关和第四继电器开关在初始状态时处于导通状态，而第二继电器开关和第三继电器开关在初始状态时处于断开状态，在网络安全设备出现断电或关机等异常情况时，由于继电器开关本身的特性，所有的继电器开关会恢复至初始状态，而此时BYPASS功能自动关闭，这样可以使得内部网络之间不再互通，提高了局域网络中设备运行的安全性。

附图说明

[0014] 下面将结合附图及实施例对本实用新型作进一步说明，附图中：

[0015] 图1是本实用新型一种BYPASS系统实施例的电路示意图。

具体实施方式

[0016] 为了对本实用新型的技术特征、目的和效果有更加清楚的理解，现对照附图详细说明本实用新型的具体实施方式。

[0017] 如图1所示，为本实用新型一种BYPASS系统实施的电路示意图，该BYPASS系统能够实现在网络安全设备处于断电或关机情况下时能够自动关闭BYPASS功能。在本实施例中，其包括依次连接的第一网卡芯片10、第一继电器开关电路20和第一接口30以及依次连接的第二网卡芯片40、第二继电器开关电路50和第二接口60，第一继电器开关电路20和第二继电器开关电路50连接，第一网卡芯片10和第二网卡芯片30用于接收输入的两路网络信号，分别为第一输入网络信号和第二输入网络信号，而第一接口30和第二接口60为内部网络设备的两个接口，优选为RJ45接口。

[0018] 特别地，第一继电器开关电路20又包括第一继电器开关K1、第二继电器开关K2，第二继电器开关电路50包括第三继电器开关K3和第四继电器开关K4，第一继电器开关K1连接在第一网卡芯片10和第一接口30之间，第四继电器开关K4连接在第二网卡芯片40和第二接口60之间，第二继电器开关K2和第三继电器开关K3依次连接第一继电器开关K1和第一接口30的连接点和第四继电器开关K4和第二接口60的连接点之间。

[0019] 其中：第一继电器开关K1和第四继电器开关K4在初始状态时处于导通状态，而第二继电器开关K2和第三继电器开关K3在初始状态时处于断开状态，而根据继电器开关本身的特性，在网络安全设备断电或关机时，所有继电器开关会恢复至初始状态，也就是说，在网络安全设备断电或关机时，第一继电器开关K1和第四继电器开关K4在初始状态时处于导通状态，而第二继电器开关K2和第三继电器开关K3在初始状态时处于断开状态，内部网络之间并没有连通，从而实现自动关闭BYPASS功能。

[0020] 上述BYPASS系统还包括第一变压器70和第二变压器80，在本实施例中，第一变压器70和第二变压器的型号优选为GST5009。第一变压器70连接在第一网卡芯片10和第一继电器开关K1之间，第二变压器80连接在第二网卡芯片40和第四继电器开关K4之间，第一变压器70和第二变压器80分别用来调节两路网络信号的电压和强度。

[0021] 此外，上述BYPASS系统还包括分别与第一继电器开关电路20和第二继电器开关电路50连接的GPIO控制电路90，该GPIO控制电路90主要用于在网络安全设备上电时控制第一继电器开关电路20和第二继电器开关电路50中所有继电器开关的导通和断开，即用来输出GPIO控制信号，以控制第一继电器开关K1、第二继电器开关K2、第三继电器开关K3以及第四继电器开关K4的导通和断开状态，以实现灵活打开或关闭BYPASS功能。

[0022] 另外，在本实施例中，在网络安全设备上电时，可通过GPIO控制电路90输出GPIO控制信号对继电器开关电路中的所有继电器开关进行控制，控制其导通或断开，实现灵活打开或关闭BYPASS功能。具体地，当输出的GPIO控制信号为低电平时，控制第二继电器开关K2和第三继电器开关K3导通，第一继电器开关K1和第四继电器开关K4断开，打开BYPASS功能；而当输出的GPIO控制信号为高电平时，控制第一继电器开关K1和第四继电器开关K4导通，第二继电器开关K2和第三继电器开关K3断开，关闭BYPASS功能。这里，需要说明的是，通过操作系统对GPIO控制电路进行控制，以输出GPIO控制信号来控制继电器开关的导通和断开是比较常用的功能，在此不再赘述。

[0023] 相较于现有技术，本实用新型的BYPASS系统，因第一继电器开关K1和第四继电器开关K4在初始状态时处于导通状态，而第二继电器开关K2和第三继电器开关K3在初始状态时处于断开状态，在网络安全设备出现断电或关机等异常情况时，由于继电器开关本身的特性，所有的继电器开关会恢复至初始状态，而此时BYPASS功能自动关闭，这样可以使得内部网络之间不再互通，提高了局域网络中设备运行的安全性。另外，当网络安全设备上电时，可以通过GPIO控制电路输出不同的GPIO控制信号，以根据需要实现灵活控制打开或关闭BYPASS功能。

[0024] 上面结合附图对本实用新型的实施例进行了描述，但是本实用新型并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本实用新型的启示下，在不脱离本实用新型宗旨和权利要求所保护的范围情况下，还可做出很多形式，这些均属于本实用新型的保护之内。

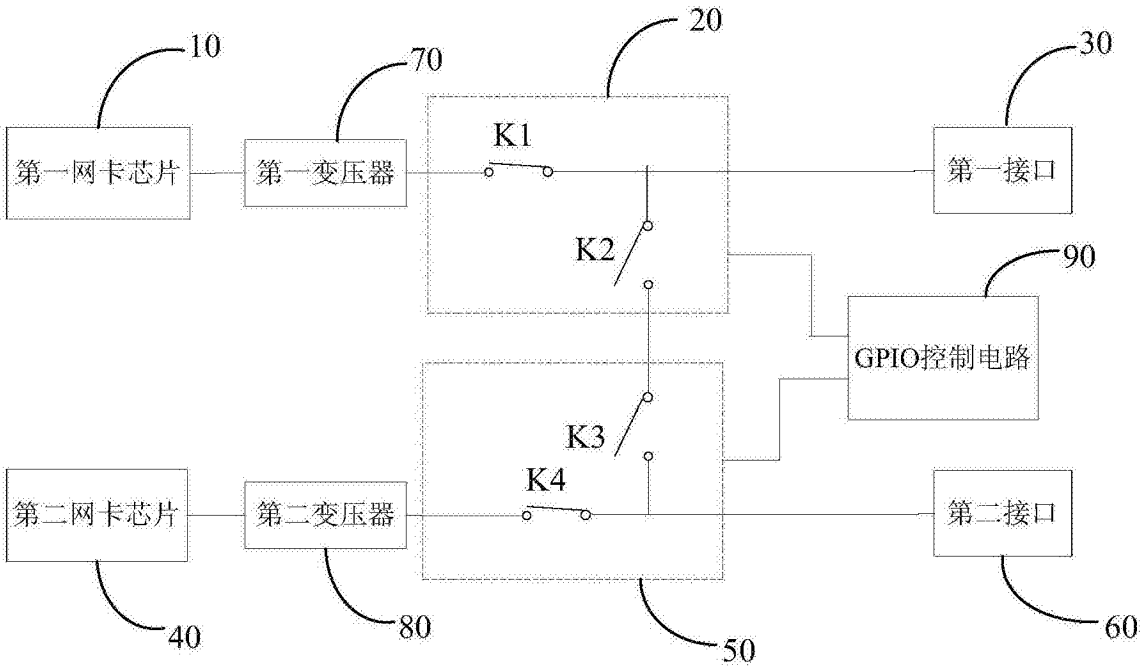

10
70
20
30
第一网卡芯片
第一变压器
K1
第一接口
K2
90
GPIO控制电路
K3
K4
第二网卡芯片
第二变压器
第二接口
40
80
50
60

图1