

电信基站/移动基站专用 门禁管理系统

产品名称	电信基站/移动基站专用 门禁管理系统
公司名称	深圳视沃电子有限公司
价格	面议
规格参数	
公司地址	深圳市宝安区龙华民治大道(民康路口)民泰大厦 9楼908室
联系电话	0755-29481228

产品详情

SW102-JZ电信基站/移动基站专用 门禁管理系统 电信基站门禁管理的特点

通常无人值守，需要维修的时候才派技术人员过去。

数量多，一般一个城市的电信基站少则数百个，多则数千个。

分布范围广，各基站很分散，分布在城市的各个角落。每个基站需要的门禁数量少。

每个基站有价值昂贵的电信设备。

电信单位对无人值守基站门禁管理的需求 不能再采用传统的机械钥匙来管理各个基站。机械锁和钥匙不适合基站这样的对安全、稳定、可靠要求高的场合。 由于分布范围广，专门为门禁系统布线是不可能的。单独布线不仅成本极度高昂，而且施工有难度。而采用无线设备用于门禁，性能会相当不稳定。 ADSL设备是电信基站得天独厚的资源，成本较低，是电信部门的自有资源。所以可以优先考虑使用ADSL进行组网控制门禁系统。

虽然已经有了专门的基站监控系统，但是由于在门禁方面不够专业，还是存在安全隐患或者功能缺陷。

要有灵活的权限管理，能及时且灵活地对基站的进出人员进行授权。授权指定人员对指定门有进出权限。因为基站往往是在派遣工作人员前才对工作人员对该门授权的。所以，电信管理部门今天打算派 张三和李四去 某个基站，就当天授权他们可以通过该基站的门，张三和李四就可以前往维护，其他时间他们是不能随便出入该基站的门的。电信管理部门只可能在管理中心授权，不可能到基站现场授权，所以必须远程控制。有的门禁系统采用将权限写在卡上面，这样虽然也可以实现管理中心集中临时授权，但无法解决及时挂失问题。 能实时监控各基站门的状况，当有意外发生时，能及时报警。因为电信基站无人值守，里面陈列了价值数十万的甚至数百万的电信设备，所以管理中心一定要能及时了解各基站门的开启情况，当有意外发生时，根据报警信息，及时采取措施，减少损失。采用联网型门禁系统后，有问题的离职人员利用套配的钥匙或者未来得及注销的当地的卡，或者私自授权的卡 盗取或者破坏电信设备或其他不法分子破门而入盗取电信设备的事情发生时，管理中心可以实时监控到这

些信息，对非法闯入予以报警，可以实时通知公安部门擒拿罪犯。

本解决方案相对于其他无人值守门禁系统解决方案的优缺点分析

门禁系统对于基站无人值守门禁功能上没有太大区别,主要的重点和难点在于联网通讯模式上,市面上常见的通讯模式解决方案有以下几种:

方式一: 通过固定IP,用TCP/IP 互联网进行通讯

该方式和我们的方案的模式是类似的,缺点是 固定IP的电信越来越稀缺的资源,即使固定IP是电信的自有资源,也会舍不得用,一个固定IP的年租金达数千元.如果门禁系统每个点都占用一个固定IP费用太高,如果只是总部占用一个固定IP,分部采用主动上报的方式进行通讯,这信息如果并发的话容易引起冲突,使得出现通讯故障. 我方提供的方案无需固定IP,国内 国外 有许多网络服务商提供免费的动态域名,如果一家停止服务了,也可以方便地换另外一家.而且这些网络服务商都是知名的网络公司,运营相当稳定.

方式二: 通过485-TCP/IP 转换器,将普通的RS485或者RS232控制器转换成可以支持TCP/IP的方式进行联网.

这种通讯模式在某种意义上是假的TCP/IP通讯模式,这种方式从原理上好像是是可以实现的,测试一下好像也能通,实际存在以下隐患.这种转换在软件和硬件上都存在一定的延时,对于通讯速度要求高,或者门禁指令长的情况,就有可能通讯不上. 这种通讯质量和通讯延时,更不适合internet广域网的数据通讯.

如果加载的门禁控制器设备超过几十台,就有可能不堪负担,即存在负载数量少的问题,在较大的门禁系统中根本无法实施.这种方案很多厂家是采用虚拟串口的方式,将IP地址虚拟为本机的一个串口,虚拟串口是个很不稳定的软件状态,一旦后台的虚拟程序运行出现问题,或者无意中没有运行,门禁软件就无法和门禁系统进行通讯.TCP/IP转换器是通用型设备,而每家门禁厂家的通讯格式都有不同,这样就存在兼容性的问题,同样一个TCP/IP转换器对某家门禁系统没有大问题,但有可能对另外一家门禁系统就存在兼容性问题.转换器公司也绝不会单独为某家门禁公司产品做个性化的设计.同时,门禁公司一般大致测试一下,觉得可以用,就推给客户了,这样是很不负责的.两个产品之间好的兼容特性,必须通过大量的测试,局部的修改和调整,大量的市场反馈才能够获得的.所以这种实施方式,只适合原有的485/232门禁系统要简易改造成局域网门禁,而且门禁点的数量不能太多,笔者不建议您这样做,因为因此带来的不稳定性会增加更多的麻烦.这个方式的优点有两个:其一 门禁开发商方便了,任何普通的门禁系统加上个转换器就可以实现TCP通讯了,免去了开发新设备的麻烦,或者在真正TCP控制器开发出来之前先对付一下销售,但这个有点对消费者来说是不利的,只是对厂家有利.其二:可以多台控制器共用一个转换器,可以节约一点成本,但是其实意义不大,一般无人值守基站就一两个门需要门禁控制,况且我方的方案可以有八个端口可以使用,每个端口可以接一台单门 双门 或者 四门控制器,最多可以控制一个基站的32道门,如果还需加大还有解决方案. 而我方的方案采用了自带TCP/IP接口(注意:不是TCP/IP模块,有些产品带了一个TCP模块,TCP模块多半是第三方的产品,核心技术在模块供应商,出现兼容性问题,门禁设备的开发商无法彻底分析和解决问题.),就好像自带了网卡一台计算机一样,通讯数据直接通过中央处理器和存储芯片就行数据处理和交换存储,没有转换延时.确保通讯数据处理的直接 快速 稳定.

方式三: 通过GPRS或者短信 进行联网

这个方式的最大优点是 可以免布线,通过无线传输,只要手机信号可以覆盖到的地区都可以进行联网.这个优点对其他行业的无人值守门禁有意义,但对电信无人值守基站意义不大,因为电信基站电话网络是肯定有且很富裕的.电信基站不太关注是否需要无线来联网.但同时无线联网带来一系列的问题是值得三思的,无线相对于有线毕竟是不稳定的,无线的信号经常会收到干扰甚至屏蔽,例如我们的手机经常会出现通讯质量不好,或者收不到信号的情况,如果通讯不稳定,如果临时要派人去某个基站,但无法进行授权,工作人员就无法顺利进入基站,耽误工作和处理故障的时间.如果某个基站被非法闯入,如果这个时候通讯不通,总部就无法实时获得报警信息,而无法采取措施.如果非法进入者进入后 掐断或者 断电 GPRS或者短信通讯设备,总部更是永远无法获得报警信息,犯罪者可以有足够的时间从容作案.此外,GPRS和短信模式是通过流量计费的,如果要实时进行通讯,费用巨大,如果不实时处理,就会无法判断是通讯是否中断,刷卡信息和报警信息就无法及时传到总部,有些厂家采用了变通的做法,就是基站有刷卡或者报警的时候才发出信息给总部以节约流量费用,这个模式存在三个缺点:其一 如果无线通讯被干扰或者中断,信息无法及时传到总部,其二 如果多个地点同时发生信息,总部未必可以处理好大量数据并发的情况.可能会因为数据拥挤丢失数据.其三:通讯接通速度慢,操作员等待行累,数据信息获取流量小而有限. 而我方采用的ADSL或者其他宽带上网,采用的ADSL月租上网,而且是电信自有资源,费用不高,且可控制,信息流量大,且可以实时监控所有门禁,所有刷卡信息和报警信息几乎可以实时传达到总部,操作员操作方便轻松快捷,系统通讯稳定可靠,随时可以发现被中断的线路,且门禁系统具备自动拨号功能,如果停电后来电等都可以自动拨号上网.

方式四: 通过电话线MODEN拨号联网.

这个是TCP/IP方式流行前,普遍采用的远程通讯模式,优点是 也是利用电信资源电话线,缺点是: MO DEN拨号方式不稳定,经常中断,接入联通速度慢,操作员操作等待时间长,传输数据信息量不大,该通讯模式已经趋于淘汰,不适合产品以后的升级和扩展.如果长期联通,电话费用高,如果不长期联通,缺乏信息反馈和报警反馈的实时性.

方式五: 通过可读可写卡存储门禁信息进行联网

这个实现方式是,员工如果要派去某个基站执行工作任务,在总部通过发卡机将这个员工的权限(何时可以合法进入那些基站)写在卡里,该员工持该卡到相应的基站进门工作.进入的时间记录存贮在卡里,下次拿回时将进门信息(时间和地点记录)提取到电脑里备查. 优点是:无需联网,无其他任何通讯费用.缺点是:不方便临时调度,员工只有回到总部重新授权后,才能去临时要去的基站.信息没有实时性,无报警功能,挂失不方便,不及时,挂失麻烦,需要将该卡号到所有点就行挂失,不能在总部统一挂失.

而我方采用的方案,可以实时处理报警信息,授权和挂失卡权限. 如果基站有非法闯入,报警信息会第一时间反馈到总部控制室的电脑屏幕上,并驱动电脑音响提醒值班人注意,采取措施,通知附近的公安执勤人员迅速看到现场,捉拿罪犯.也可以驱动现场的警报器,威吓犯罪人员. 可以灵活机动快速地处理临时调度,例如工作人员现在正在A基站工作,总部得到通知,需要其马上赶往B基站,这样总部管理人员就可以通知其马上赶往B基站,并通过系统对其授权其可以进入B基站,并随时可以监控 该人员是否及时赶到了B基站.

