

网络安全

网络安全的实现 需借助防护措施

随着自动化模块的网络化，“安全危机”成为了关键所在。在联网的情况下，网络的安全性及重视设备进行远程信息存取的安全性非常重要。文 | Jörg Neumann

在这里所概括的“功能安全”只涉及及为了实现全天安全系统而采取和实施的平行测量安全措施。如在维护人员对控制装置进行错误操作，或对外部信息截取产生强大负荷，而让时间界限内的程序产生损失，也能保证喷漆机器人不会对工作人员的人身安全造成威胁。与生产关系密切的 IT 系统会出现可

能危及到工作人员安全的情况，通常的解决方法仅是将安全措施限制在安全范围内，即限制在避免对工作人员造成伤害或对机械和成本较高的材料产生重大损失的方面。过去，连接工厂 LAN 或仅是临时性接近机械设备进行保养和维护并非人们的关注点，尤其是对那些较小型的机械设备。

多年来，无数 MSR 结构组件和控制装置都已包含 Ethernet 接口、Modbus 界面和用于用户接口的嵌入式 Web 服务器。这样，HMI 系统便于用于组态和除 Modbus 存取外，基于网络的输入信号读取及输出值的书写。而几乎所有的生产厂商对于安全的重视都不够。开始时，他们中大多数人认为通过登陆名和密码

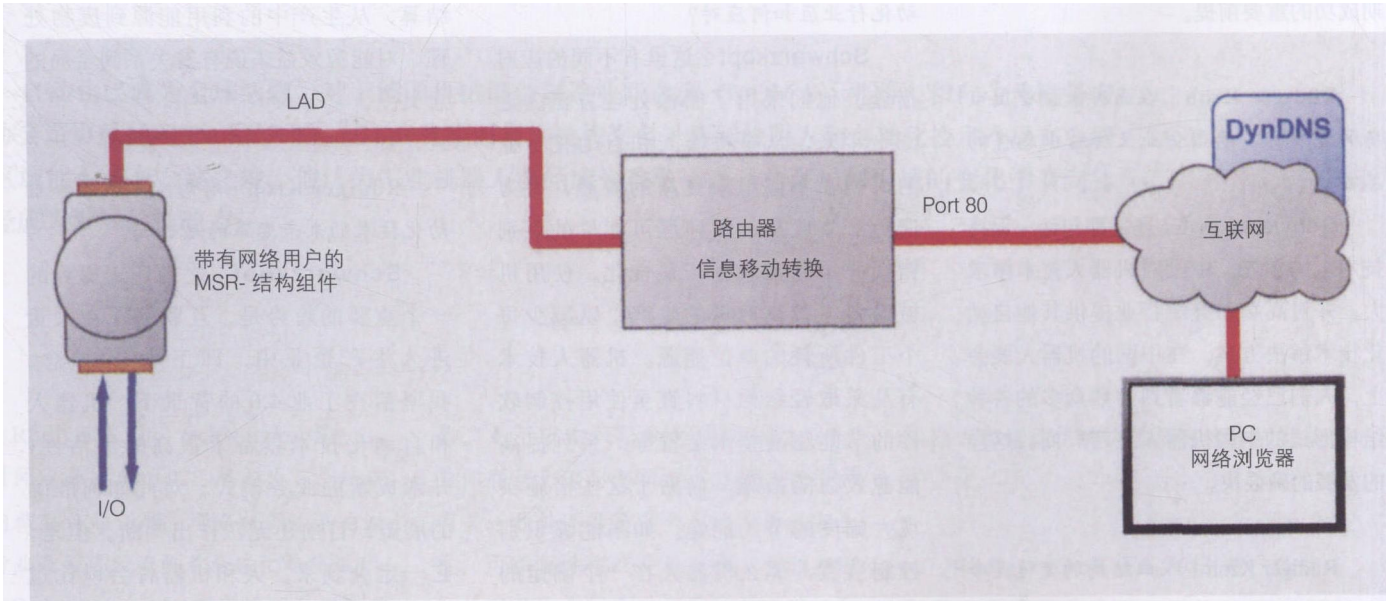


图 1 带有 LAN 界面和集成化网络服务的 MSR 结构组件拥有一个功能性的弱点。通过一个信息进一步移动、动态的 DNS 或固定的 IP 地址网络互连，外部的信息存取者不需花费较大精力便可通过互联网接触到 MSR 结构组件并可对其进行使用。用户名和密码通常并未设定阻碍

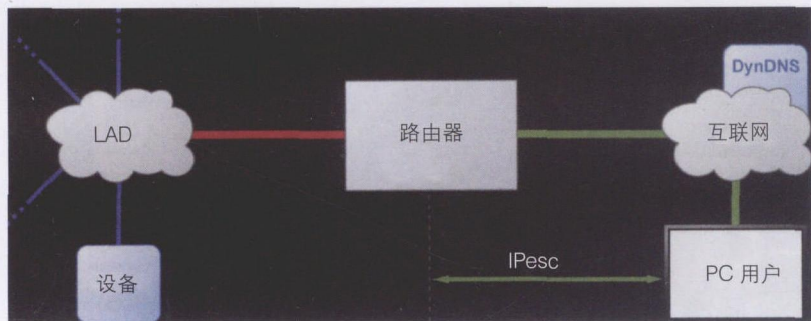


图2 有些技术解决方案也使用集成路由器 IPsec。在这种情况下,不存在终端对终端的编成密码,因为路由器中的 IPsec 结束,装置便可在不需要密码的情况下进行数据传递。因为在这样的远程信息存取技术解决方案中用预共享密钥进行工作,所以对于每个密钥的拥有者来说,均可进入 VPN

便能够进行网络存取。当时,组件的提供者认为这些组件的使用处于安全的局域网络中,在该网络中的用户所使用的 PC 均不会受到恶意软件的影响,且不会连接至互联网中。但是一些实例已经证实,这种观念是错误的。

施工现场的互联网连接

过去,在使用自己的网络服务器时,或是在互联网上进行远程存取时,使用者受到了没有充分安全性保障的困扰。

任意一个 MSR 结构组件的 LAN 界面均与一个路由器相连。在路由器中,接通 TCP 端口 80 启动“向前移动”(端口转发),这激活了 Dyn DNS 服务(动态 DNS 服务),并建立了一个相应的账号。由此便能够在途中或任意的一个地点从 MSR 结构组件的网络服务器上很容易发现的主机名来进行信息存取。这样便能够始终动态的与互联网中处于变化的路由器 IP 地址相适配。这种技术方案,实际上每个知道用户名和密码的用户均能够通过互联网来读写组件中的数据。因为作为名字/密码的组合可以由生产厂商多重进行标准调整或是可以进行很简单的组合(如“管理员/管理员”)便可运用,这样就启动了连接混乱使用的阀门。

动态的 DNS 服务,更加具有实际意义的是使用了进入互联网的固定 IP 地址,在这种情况下,总是使用相同的地址通过互联网接触到相应的组件。专用搜寻装置,如整个互联网适应可达到的装置和设备的 Shodan,结果是可提供带有超级链接的网页,能够在一定的时间范围内找到 MSR 组件和打开相应的链接。时间上的问题需要及时破解,而这样的问题几乎处处都能够出现。

未通过许可但能对网络中的薄弱环节进行远程攻击在实际工作中是真实存在的。2013 年初,一家在业内处于领先地位的德国高科技暖气设备生产厂商获悉,公司所生产的暖气设备中使用的一家瑞士著名企业提供的控制装置被人为侵入(图 1)。因为可靠程度不高的使用者或是由外部进入到设备内部的非使用者得到控制器,和其设备路由器之间的线路连接上明确的文字 LAN 交流,甚至通过这种方法获取了设备维护技术人员的姓名和密码,通过互联网自由接通和断开其他厂商的暖气设备,因为所涉及到的高科技暖气设备也作为微型发电厂向公共网络中进行馈电,并由此涉及到公共基础设施,在这种情况下,还有可能会接通 BSI(德国联邦信息技术安全局)。电视与广播中的节目均

专注工业互联
引领总线通讯



2015.3.9 SIAF·广州 2.2馆H01号

高性价比协议转换器

- 产** 超薄设计,硬币厚度;
- 品** 硬件封装,系统稳定;
- 特** 三防处理工艺,防潮隔湿;
- 色** 金属外壳,坚硬更轻巧;
- 工作温度: -40~85°C。



四川零点自动化系统有限公司
Sichuan Odot Automation System Co.,Ltd.

总部: 四川绵阳市科创区创业中心C328
电话: 0816-2530577
传真: 0816-2538289
技术支持: 13778119619
E-mail: sales@odot.com.cn
http://www.odot.com.cn
邮编: 621000



24小时热线: 400-1024-485

▲反馈服务编码M5248

报道过这样的实例。过去涉及到这样事情的生产厂商需要向用户与大众解释出现问题的原因，并说明应如何防止这样的问题在今后出现。

无人打算建立防火墙

与上述问题相似的疑问还表现在，对基于互联网的设备远程存取需要使用一些广泛推广的标准路由器的集成化 VPN 性能上。这样的性能通常会涉及到一个植入的 IPSec 服务器，通过预共享钥匙（预先指定的关键）的用户便可使用该服务器。为了随时通过互联网到达路由器，这里也重新使用了 Dyn-DNS。对于所有在远程的设备或在独立的 MSR 组件上存取的计算器系统，将建立一个 IPSec 用户，并用相应的预共享钥匙进行配置（图 2）。

这种技术解决方案的难点在于，加密路由器 IPSec 会被放置在距离工厂非常远的距离。在一个局域网内，通常情况下在路由器后面没有 VPN 作为保护。此外，IPSec 用户无法在设备上信息进行存取，而是在 LAN 中的其他计算功能设备上信息进行存取。而最大的问题是，在结构组件和控制器上使用互联网远程信息存取的预共享钥匙。由于失去了远程维护备忘部分，所以每个拥有此把钥匙的用户在进行远程信息存取时将不受限制，不仅不会失去使用者权益和被使用者的权力，也不会屏蔽每个使用者。

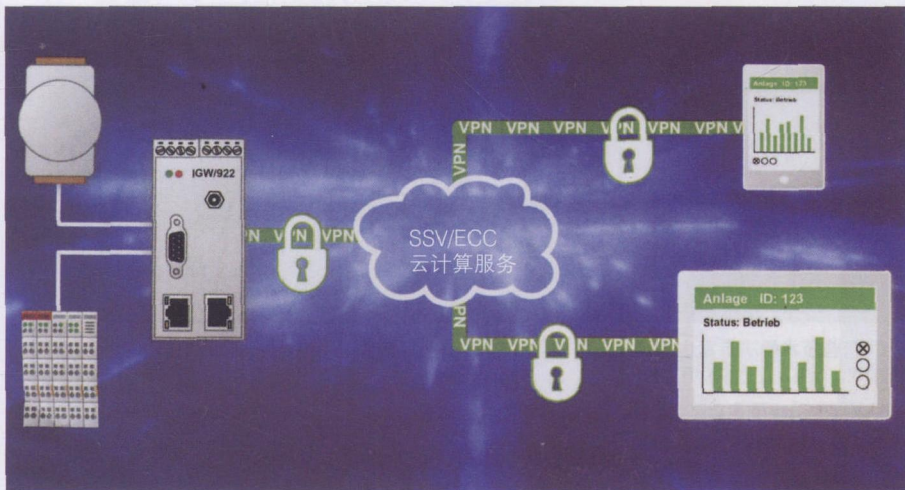


图 4 为了使自动化装置达到长期以来未达到的安全，必须对安全防护观念予以和在装置结构安全防护同样的重视

而所存在的风险还在继续升高，之前存在的漏洞所发生的问题，路由器的经营者还是需要远程存取控制。在 M2M 应用和远程主动技术情况下，甚至于还存在 IPSec-VPN 的应用，此时通过一个移动无线电提供者便可以管理和控制整个虚拟个人网络。而使用只能对这种技术解决方案中的移动无线电提供者无条件信任（图 3）。

移动无线电提供者的安全机制并非具备完全的可靠性，这一事实已在 2013 年 9 月得到了证实。那时，人们不得不安装语音电话，而一个黑客盗走了 200 万个语音电话用户的个人信息。这些个人信息外泄的用户中的自动化系统拥有者只是希望，接近他们程序装

置自动化系统维护的信息或是他们的信号技术信息不属于泄露范围。自从多数装置设备与互联网或其他系统交换数据，又有了一个可能操纵自动化系统的全新入侵点。

一旦出现自动化系统被入侵造成可以接受或不被接受的操控所造成的损失时，各安全系统便出现故障（或是这些安全系统反应延缓），很显然没有防护安全不可行。即使是无人遭受损失，被入侵的自动化网络的损失也是巨大的，一个 OEM 的损失被称作几乎是不可避免的“销量在大幅下降”。

挑战和任务

多个实例表明，人们必须对设备联网和远程存取的安全防护提高重视（图 4）。如 SSV 软件系统公司所提供的安全防护平台。长期以来不只需要重视对重要结构组件或独立系统的安全防护，还必须重视整个自动化装置基础设施的安全防护。为此，自动化装置会在结构上繁复冗余，一方面在结构上要确保自动化装置的安全，另一方面还涉及到安全防护措施，必须考虑到在自动化装置的结构上将这两方面的观点结合起来，并将在安全部分落实 ISO 标准模拟看作为随着时间要求会提高且要求会“随之增长”的程序。

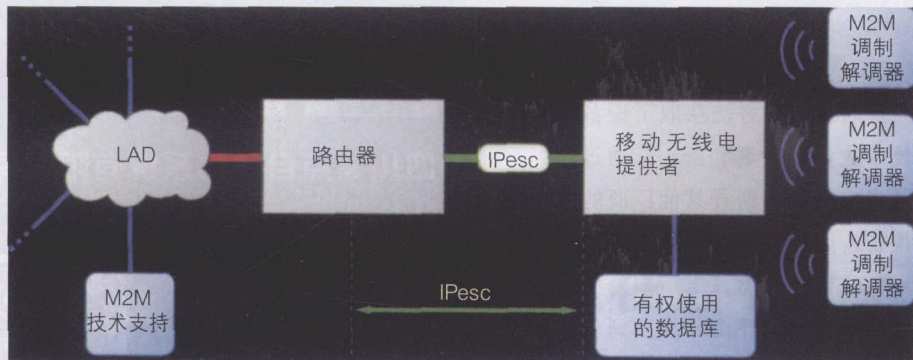


图 3 当由一个移动无线电提供者的基于 IPsec 的 VPN 基础设施可供使用时，问题不仅是缺少终端对终端的密码，还缺少虚拟的私人网络范围内的安全检验证实。对于要求功能安全的自动化应用而言，做到一个这样的技术解决方案是不成问题的