[工业以太网]

工业以太网安全应用研究

工业以太网在工业自动化领域内受重视的程度越来越高，严苛的工业环境不仅要求工业以太网技术不断创新，而且要求能够保持优秀的稳定运行性能。目前，工业以太网技术已经可以整合现场设备与上层信息网络，达到无缝集成的效果。在技术不断发展的同时，也应该重视到工业以太网是否能够具备足够的安全稳定性能。

文 / 黄桂苹、赵国祥 • 研华自动化

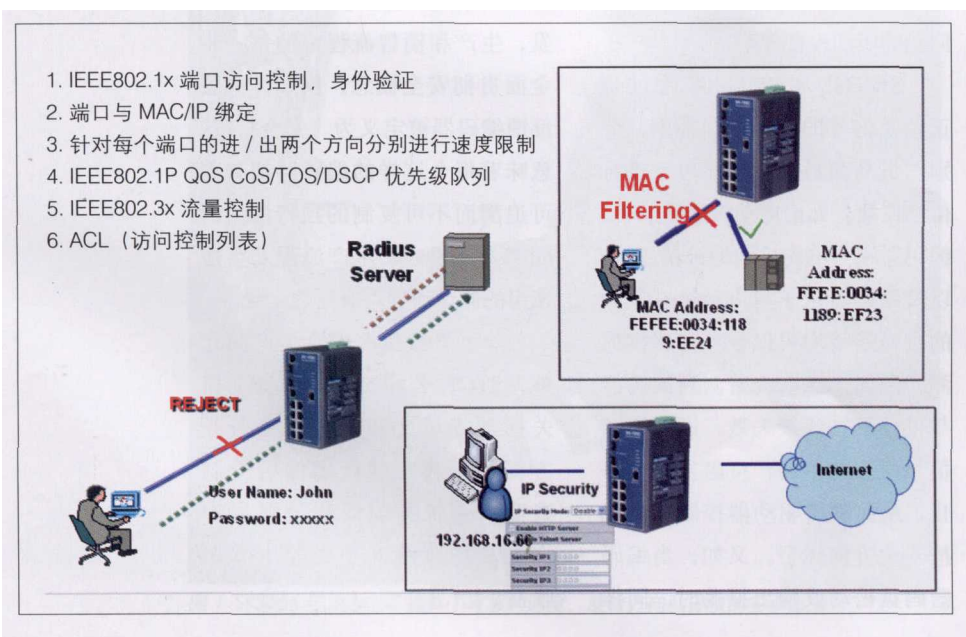
工业以太网交换机是组建强大的工业以太网的核心设备，而硬件设备能否安全运行，是保证整个网络能够安全稳定运行的基础。以往在工业环境中，用户选择商用交换机来构建以太网络时，常常会遇到由商用交换机本身故障而引起的种种问题，如风扇温度过高导致死机、电磁干扰环境下无法正常工作等。为达到在严苛工作环境下仍能保持安全稳定运行的功能要求，工业交换机在硬件方面与商用交换机存在着很大的差异。表格所示为工业交换机和商用交换机的硬件指标对比。

以上硬件的设计及防护特点，保障了工业交换机能够进行长期稳定的运行，这也是各工业交换机厂家对外宣传的主要卖点之一。随着各行业应用的深入，硬件安全要求也不断提高，例如，针对电力市场的高 EMC 干扰，工业交换机要求全部达到 EMC4 级以上防护等级；针对交通行业车载交换机的防振动、高低温等特殊要求，传统的 FJ45 接口都通过 M12 接头来实现其防护性能；针对纯室外工作环境，要求工业交换机达到 IP67 以上的防护等级。

综上研究，工业交换机的硬件设备能否安全运行是与各行业应用环境密切相关的。如果产品性能参数达到使用要求，生产质量标准符合相关规定，则硬件上的故障就可以得到有效避免，工业以太网就可以在一定程度上保证其安全性和稳定运行状态。

下面来研究基于软件层面的安全应用现状。工业以太网长期致力于实时性、可靠性和安全性的研究和改进；同时工业以太网也在防御网络病毒攻击、防御针对 MAC 地址攻击等方面不断深入研究。这些来自于网络本身的问题在工业以太网中是如何得到解决的呢？常规来讲，杀毒软件的使用必不可少，且通常采用双层防火墙来抵抗网络攻击：第一层防火墙用于阻止来自外部的非法访问，第二层防火墙用于屏蔽来自内部的非法访问，并分配给合法用户不同权限。此外，还可利用日志记录来调整过滤和登陆策略。

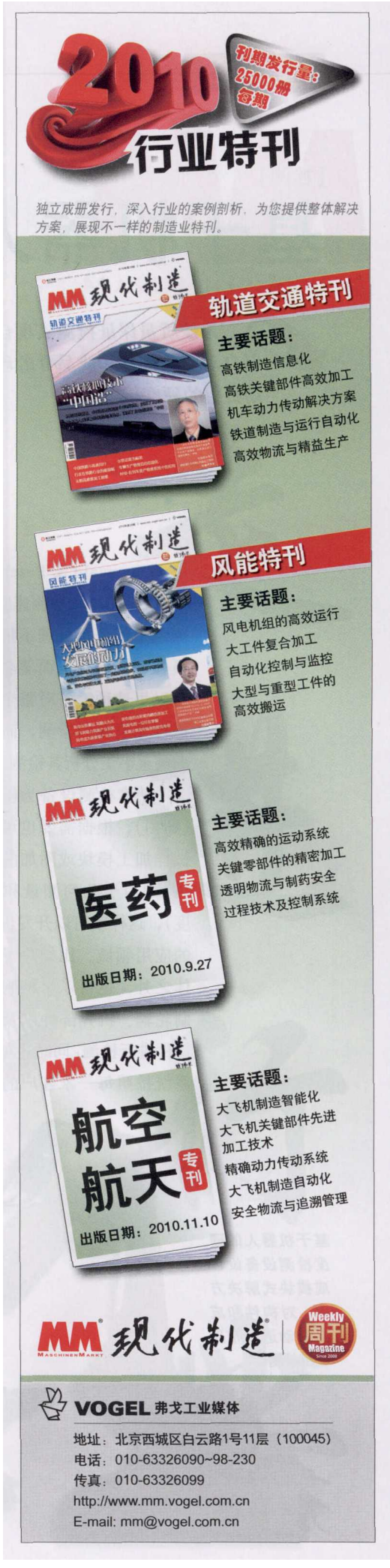
除了使用杀毒软件、防火墙等防御手段之外，通过对大量的工业交换机现场应用进行总结，研华总结出如下安全经验（如图）。



工业以太网交换机与商用交换机的区别		
对比项目	工业以太网交换机（以研华工业交换机为例）	一般商用交换机
设计及元器件制造标准	工业级别	民用级别
工作电压	12 ～ 48 VDC	220 VAC
电源冗余	双电源	单电源，一般没有冗余
安装方式	DIN 导轨，机架等安装方式	桌面，机架
工作温度	-40 ～ +75℃	0 ～ +40℃
散热方式	外壳散热	风扇
外壳材料	高强度金属外壳	塑胶外壳，强度低
防尘性	全封闭结构，防尘性较好	有散热风扇，防尘性差
附加报警触点	有	无
各端口工作方式自定义	有	一般没有
电源掉电报警	有	无
链路故障报警	有	一般没有
符合标准	工业级	OFFICE 级
支持容错冗余光纤环网	完全支持	一般不可以做环网
环网切换时间	毫秒级	30 ～ 90 s
MTBF	大于 200 000 h（20 年以上）	取决于不同厂家
EMC 等级	3 ～ 4 级	一般不要求
防护等级	IP30-67	一般不要求

其中，用到了当下流行的安全技术和应用技巧：

- 流量控制技术：把流经端口的异常流量限制在一定的范围内；
- 访问控制列表（ACL）技术：ACL 通过对网络资源进行访问输入和输出控制，确保网络设备不被非法访问或被用做攻击跳板；
- 安全套接层（SSL）为所有 HTTP 流量加密，允许访问交换机上基于浏览器的管理 GUI；
- 802.1x 和 RADIUS 网络登录控制基于端口的访问，以进行验证和责任明晰，源端口过滤只允许指定端口进行相互通信；
- Secure Shell（SSHv1/SSHv2）加密传输所有的数据，确保 IP 网络上安全的 CLI 远程访问；
- 安全 FTP 实现与交换机之间安全的文件传输，避免不需要的文件下载或未授权的交换机配置文件复制。

应该注意到，在应用以上安全技术时，将面临实时性和成本的困难。目前工业以太网的应用和设计主要是基于工程实践和经验，随着系统集成和扩展方面的需求、IT 技术深入至自动化系统组建的需求以及 B/S 监控方式的普及等已成为工业以太网的必然发展趋势，在网络安全因素下，工业以太网的可用性研究是非常必要的。工业以太网必须从自身体系结构入手来更好地应对安全问题。

综合全篇所述，工业以太网的安全应用在软硬件都有着更高的要求，同时还要兼顾应用环境需求特征。为获得安全稳定的工业以太网应用，要在满足网络负载与平衡、满足实际应用要求的同时，将更好地解决并提升网络安全作为长期探讨的课题。MM