

工业生产线通讯网络方案设计与分析

徐鹏飞, 张菁, 李志伟, 戎自强

(上海工程技术大学 电子电气工程学院, 上海 201620)

摘要: 针对工业以太网信息交换过程中, 无线传输不安全和因系统故障导致网络通讯不稳定等问题, 在分析通讯网络技术需求的基础上, 完成了结构设计和网络构建, 提出了更为合理的方案; 基于交换机互为热备份的方式, 综合利用虚拟路由器冗余协议 (Virtual Router Redundancy Protocol, VRRP) 和介质冗余协议 (Media redundancy protocol, MRP), 实现了可容忍宕机和链路失效的冗余传输通讯, 提高了系统的稳定性; 同时, 利用快速漫游和组播监听技术并结合使用了安全模块功能, 实现了数据快速无线传输并与外部网络隔离, 保障了数据传输的安全性; 所提出的方案在工业生产与控制领域有较好的应用前景。

关键词: 交换机; MRP; VRRP; 组播监听

Design and Analysis of Communication Network Scheme for Industrial Production Lines

Xu Pengfei, Zhang Jing, Li Zhiwei, Rong Ziqiang

(School of Electrical and Electronic Engineering, Shanghai University of Engineering Science, Shanghai 201620, China)

Abstract: For the problem of unsafe wireless transmission and instability of network communication in the industrial Ethernet, this paper completed the structural design and network construction based on the analysis of the related technical requirements. Based on the mutual hot backup mode, the VRRP protocol and MRP protocol are combined to realize the communication which can tolerate downtime and link failure, and improve the system stability. With iPCF, IGMP Snooping and security module functions, it realizes the fast data transmission and data security. The scheme proposed in this paper has a good application prospect in the industrial field.

Keywords: switch; MRP; VRRP; IGMP snooping

0 引言

以太网凭借高性能、高互用性等特点, 被广泛用于工业生产领域, 其安全性和冗余度成为工业网络的两大核心^[1-2]。通常以太网冗余分为两大类: 一类是提供线路和交换机冗余, 主要有 STP、RSTP 和 MSTP 等, 它们采用环形拓扑结构防止逻辑环网的出现, 但故障恢复时间较长^[3-5], 而 IEC62439 标准定义的介质冗余协议 (MRP) 能快速检测环网链路故障并建立新的网络拓扑来恢复网络错误! 未找到引用源。; 另一类是节点连接两个独立的以太网, 主要有 PRP 等, PRP 不会丢失报文数据, 但会增加网络报文的数量, 而且时钟同步难以实现^[9-10]。虚拟路由器冗余协议 (VRRP) 技术是一种针对网络中断的可靠性设计技术, 可以使网络自动切换至无故障网络, 确保了通讯的连

续性和可靠性^[11]。

从现场设备到操作系统、驱动设备以及人机接口, 没有通讯网络, 机器管理控制、生产区域协调和监测等复杂任务很难实现。随着“互联网+”的提出和智能终端的普及, 工业网络相关技术将不断推进, 使生产朝着智能化、网络化和数字化方向发展。为了解决企业从接入层到管理层能实现安全稳定的信息传递的要求^[12], 本文在对相关技术需求进行分析的基础上, 将 VRRP 和 MRP 等协议综合利用, 设计了交换机互为热备份的通讯网络方案, 实现了具有较强自愈性的通讯网络, 增强了系统的稳定性。此外, 通过使用安全模块功能以及组播监听和快速漫游等技术, 实现了数据在内部与外部网络间隔离传输, 保证了无线传输的快速安全。根据技术分析与结构设计, 对工厂通讯系统进行网络构建。

1 网络通讯技术需求

工厂生产单元具有可复制性与可替换性等特点, 不同车间只与控制中心建立通讯。随着工业网络架构越来越大, 如何通过技术手段确保网络传输的快速安全和系统的稳定成为必要的功能需求。本部分着重对工业以太网相关的各种通讯技术进行分析。

1.1 信道规划与 iPCF 快速漫游

对于信道的规划, 在共同覆盖区域选择不同频段的信

收稿日期:2018-07-13; 修回日期:2018-08-21。

基金项目:国家自然科学基金(61705127)。

作者简介:徐鹏飞(1993-),男,江苏南通人,硕士研究生,主要从事工业通讯网络安全分析方向的研究。

李志伟(1982-),男,河南沈丘人,博士,硕士生导师,主要从事工业自动化控制与分析方向的研究。

张菁(1969-),女,上海人,硕士生导师,副教授,电气设计与楼宇智能化专业教学团队负责人,主要从事学科及专业电气工程及其自动化方向的研究。

道, 在不同的区域可以选择相同的信道; 同一 AP (Access Point) 管理信道可以相同, 数据信道要不同, 所以相邻的 AP 之间选用不同信道来防止互相产生干扰。为了避免由多个站点共享和竞争信道引起的冲突, 同时考虑到无线安全性和数据传输可靠性, 使用全双工交换式以太网进行数据传输。

自动导引车 (AGV, Automatic Guided Vehicle) 是一种集声、光、电、计算机为一体的简易移动机器人, 主要应用于柔性加工系统、柔性装配系统。车内的网络设备按 VLAN 的功能划分为虚拟交换机, 属于不同的 VLAN 设备, 不能直接连接。整个系统中 AGV 小车上 IP 摄像头的高清视频, 应传输到控制中心。将 I/O 设备与摄像头分别接入不同的 VLAN, 避免视频数据对控制系统的影响。为了降低带宽占用, 通过组播方式将视频信号与控制数据子网隔离。

小车在环形轨道上运送物料时, 会在无线区域快速切换, 客户端的退出和重新登录发生得非常快。如图 1 所示, 当 AGV 小车在不同车间内快速移动时, 车上的客户端在不同的无线区域内快速切换, 此时每个 AP 接入点以固定的信道顺序依次轮询客户端是否连接。当失去与 AP 的联系时, 客户端会从其允许的通道列表中扫描下一通道, 并选择最近的 AP 连接。在设置接入点模式和客户端模式时, 启动设备 PNI0 支持功能, 选择大于 32 ms 的更新时间, 确保系统中的多个接入点在不同的通道中均能通信, 进而将漫游时间缩短至 50 ms 以下。

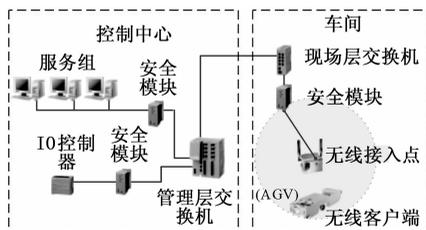


图 1 无线通讯控制系统示意图

1.2 组播侦听功能控制数据优先处理

交换机通过组播侦听和组播路由实现对组播数据 (黑色箭头) 的限制, 通过侦听 IGMP 控制帧 (白色箭头), 解析当前组成员状态并创建组播转发表, 并实时更新组成员主机的状态, 实现 IP 组播的动态注册。

图 2 为 IGMP Snooping 功能图, 当侦听到主机 Client2 发出报告帧 (Client1 和 Client3 未发出) 时, 交换机把与 Client2 相连的端口添加到组播地址表, 从而与 MAC 组播地址形成映射。当组播数据从三层设备发出后, 二层组播设备启动 IGMP Snooping 功能, 将数据只发送到 Client2, 从而对控制数据进行优先级处理, 降低带宽占用, 提高传输速率。

交换机定时发送所有主机的 IGMP Query 报文, 若主机要继续接收该地址表组报文, 则应回应 IGMP Report 报

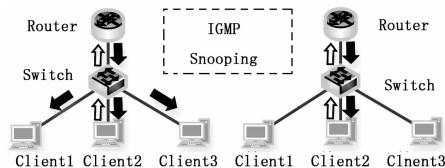


图 2 IGMP Snooping 功能示意图

文, 若交换机收不到任何主机的 IGMP Report 报文, 则将改组注销。

1.3 安全模块功能对设备进行保护

在生产线上, 有些数据不能对外公开, 安全模块可用作防火墙来过滤数据包。通信的传输采用与 IP 和 MAC 地址以及通信协议相同的方式进行过滤。网络地址转换 (NAT) 能将受保护的内部网络翻译成外部网络地址, 建立一种受控的连接, 安全模块作为防火墙和 NAT 路由使内部网络隔离于外部网络。这种将较多的私有 IP 地址由较少的公有 IP 地址代表的方式, 在一定程度上减缓了可用的 IP 地址空间的枯竭。

此外, 集成到安全模块的防火墙用于保护 IO 设备免受未经授权的访问, 配置成仅允许访问虚拟站, 设置通信过载限制。安全模块将数据保存在日志文件中, 日志记录功能支持访问监控, 并记录访问和尝试的攻击, 以便采取预防措施。安全模块只允许经过身份验证和授权的设备之间的通信。这样能防止操作员出现错误, 防止未经授权的访问, 并避免干扰和通信过载。此外, 可以通过安装防病毒软件和网管软件, 对系统进行监控、报警和阻断。通过使用安全模块设置的防火墙、数据加密和安全监控管理系统, 维护工程师可以通过外部网络与内部生产网络建立安全连接, 对车间内部程序进行维护, 确保传输数据的安全性和保密性。

2 厂区布局与网络结构设计

结合工业系统对网络冗余自愈的高要求、对宕机的低容忍度等特点, 这里采用虚拟路由器冗余协议 (VRRP) 和介质冗余协议 (MRP) 相结合的方式, 使三层交换机 (A 和 B) 互为热备份, 不仅降低了交换机的故障影响, 也避免了网络循环、广播风暴等问题出现。

2.1 厂区布局设计

工业通信网络结构分为管理层网络、接入层网络、无线覆盖接入网络和 AGV 小车终端网络 4 部分。管理层包含控制中心和生产主交换机, 设在控制中心, 负责传输数据流和控制网络资源访问。接入层设在生产线, 用以连接无线接入点 AP 设备, 负责生产数据的采集传输。无线覆盖接入网络是由不同信道的 AP 所组成的网络; AGV 小车终端网络则负责 AGV 系统与控制中心间指令以及数据的采集传输处理。

某工厂厂区主要由控制中心和车间两部分构成。如图 3 所示, 车间按直线排列, 每个长度约 200 米, AGV 小车从

车间 1 到 6 沿环形轨道运行。控制中心与车间生产线进行有线通讯，AGV 小车信号以无线形式接入主网络，实现与控制中心的通讯。

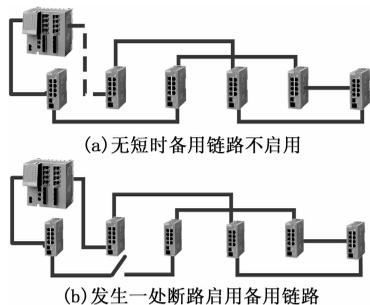


图 3 工厂车间布局示意图

2.2 利用 MRP 协议减少链路故障重组时间

介质冗余协议是对环型以太网进行状态监控与控制实现冗余度的环网协议。通过建立环形拓扑，环型以太网中的交换机或线路的单个故障可以由该 MRP 协议补偿。通过交换机的 WEB 页面配置，将所有环网端口的连接设为全双工和 1000 Mbps。管理层的三层交换机 A 与 B 设为冗余管理器，与作为冗余客户端的交换机组成环网，环网由冗余管理器进行管理。

图 4 为交换机 A 在不同情况下 MRP 工作状态。冗余管理器在两个端口上每间隔一定时间发出测试帧，当测试帧每次都顺利到达另一环口，冗余管理器就会认为环网畅通。此外，冗余管理器会阻塞一个环口中除测试帧以外的所有报文，从而将环网转换为线型网络，避免无线循环的广播。

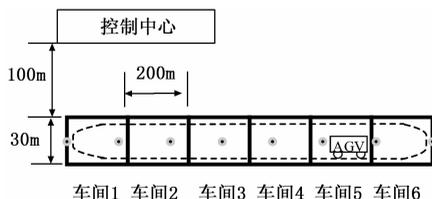


图 4 交换机在不同情况下 MRP 工作状态示意图

当冗余管理器未接收到随后的测试帧时，冗余管理器将会重构，通过其阻塞的端口进行连接通讯。MRP 最大重构时间为 200 ms，为了保证网络重构期间 IO 不会掉站，需要将 IO 设备的看门狗时间设置为 200ms 以上。MRP 具有拓展性，能在毫秒级内快速检测网络错误并建立冗余的网络路径，减少重新配置网络的时间，为小型和超大型网络实施并具有拓展性。

2.3 使用 VRRP 协议降低单点故障

整个通讯链路中，在数据传输过程中，除了要避免网络循环外等链路引起的故障外，更需要考虑作为传输关键节点的交换机的故障排除问题。虚拟路由器冗余协议 (VRRP) 可以解决静态配置问题，能将一组路由器组成虚拟路由器 (VR)。三层交换机 A 和 B 具有路由选择和 VLAN 功能，A 和 B 以逻辑组的形式组成 VR，并使用相同的虚拟

ID，二者互为热备，互相监测着彼此的运行状态。

为防止交换机自主选举根桥的资源开销及不确定性，在网络搭建时，设置端口优先级，将交换机 A 设为主虚拟路由器即根桥交换机，优先级为 255。整个 VR 使用交换机 A 的物理以太网接口的 IP 地址，A 负责转发发送到该 IP 地址的数据包。交换机 B 为备用路由器，优先级在 1—254 中任意设置。在非根桥交换机上依据最低根路径开销，选举出根端口和最优路径。

图 5 为不同情况下 VRRP 工作状态。交换机 A 将虚拟的 IP 地址和 MAC 地址分配给其网络接口，同时交换机 A 间隔一定时间将 VRRP 数据包发送给交换机 B，向交换机 B 说明自己的运行状态。当交换机 A 发生故障，优先级较高的交换机 B 迅速启动成为主虚拟路由器，代替交换机 A 成为主虚拟路由器，负责处理来自控制中心和客户端的数据包，确保链路不间断的工作。VRRP 降低了网络中交换机单点故障的可能性。

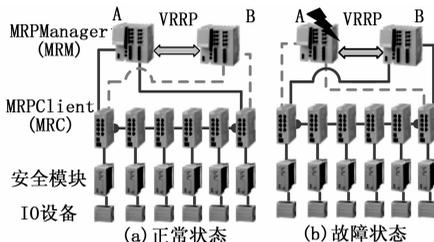


图 5 不同情况下 VRRP 工作状态示意图

2.4 故障检测与远程维护

环网冗余采用循环检测和故障报警两种故障检测机制，目的是收集链路及故障数据以及警报检测。冗余管理器每间隔 T 时刻收发环状态检测报文，冗余客户端依次接收并转发，实现循环检测^[13]。

当冗余客户端接收的状态检测报文不能转发到下一个副节点，即检测到链路故障，有故障的 IO 设备就在控制器生成诊断报警。随即冗余客户端发送链路告警报文给冗余管理器；冗余管理器收到两个及以上链路告警报文后，将备用端口变成转发状态。一定时间内，冗余管理器通过是否收到绕回的环状态检测报文，判断环网是否恢复正常。此报警控制机制启用程序中相应出错子程序的调用，从而确保 IO 控制器对错误有序处理。

远程维护实现集中管理和控制设备，跨越长距离的访问各生产单元的组件，科实现等同于现场编程和诊断的功能；不仅可以快速地解决设备和生产单元间出现的问题，还可以缩短现场较长的服务时间。本方案通过建立外网对办公网络的端对端的 VPN 通道，通过安全模块 ACALANCE S 的 VPN 隧道来实现远程操作。

3 网络构建与实施检测

3.1 设备的分布与连接

为了减少设备数量和安装维护成本，同时确保小车高

速移动时保持不间断的数据和信号无缝传输, 结合实际情况, 全厂区采用覆盖半径为 200 米的全向天线, 以 170 米的间距沿轨道交叠布置, 如图 6 所示。

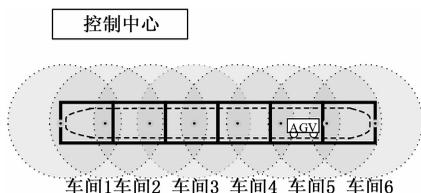


图 6 工厂车间布局示意图

在无线通讯中, 为了增强无线通讯的抗干扰性, 采用 IEEE802.11r 的模式工作。此外, 5 GHz 频段的信道速度快而且比 2.4 G 更加抗干扰, 所以将工作区定在 5.725~5.825 GHz 频段, 并分成四个信道, 如图 7 所示。为了避免在相同覆盖区域内, 相邻全向天线 AP 因共享信道引起冲突导致负荷增加, AP 的信道依次设定为 1-2-3-4-1…。当个别全向天线 AP 故障时, 故障 AP 的传输范围仍能被相邻的 AP 覆盖, 信号和数据仍能在全网范围内不间断传输。

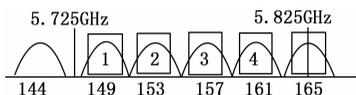


图 7 信道选择示意图

结合工厂布局, 为满足大量的数据传输需求, 选择标准传输距离不得超过 750 米的 1000 Mbps 多模光纤传输。为了节约设备成本, 考虑到实际接线环境与方式, 采用跨接方式实现多站点、长距离的光纤连接, 如图 8 所示, 跨接顺序为: 1-3-5-6-4-2。

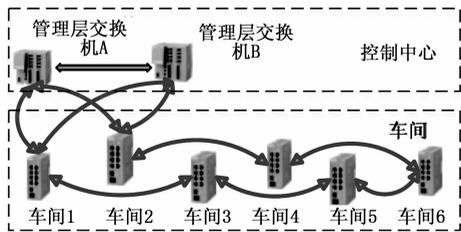


图 8 交换机跨接方式连接示意图

3.2 安全模块功能的应用实现

由于安全机制, 如认证数据加密或访问控制, SCALANCE S 模块能够保护自动化单元免受数据间谍、未经授权的访问和不必要的通信负载。即使在外部网络发生干扰的情况下, 自动化小区内的数据流量仍然不受影响。SCALANCE S 模块独立于所使用的应用协议保护通信。所有基于 IP 的协议和仍然广泛使用的自动化工程二层协议可以轻松地以这种方式进行保护, 而不会限制允许的生产数据流量。SOFTNET 安全客户端允许对受 SCALANCE S 保护的设备进行安全访问。

在使用该组态时, 允许从内部子网发送到外部网络中 PC1 节点的所有数据包通过防火墙转发到外部网络的数据

包包含有安全模块的 IP 地址以及动态分配的端口号。只允许对这些数据包的回复从外部网络通过。

在工业生产过程中, 为了确保生产数据的安全可靠性, 需要考虑将工厂生产网络与工厂办公网络分离。在使用该组态时, 只能从内部网络发起 IP 流量的传输; 仅允许外部网络的响应, 防止未授权的设备 and 流量进入。

3.3 组态的参数设定与激活

利用西门子 SCALANCE S 安全模块作为防火墙与 NAT 路由器。为了测试通信网络是否正常, 首先需要对 PC 进行 IP 设置。在外部网络上位机中安装并启动安全组态工具, 在创建新项目过程中, 用一个用户名和相应的密码创建一个新用户。

表 1 PC 的 IP 设置

PC	IP 地址	子网掩码	网关
PC1	192.168.1.100	255.255.255.0	192.168.1.1
PC2	192.168.2.100	255.255.255.0	192.168.2.1

创建模块时, 按照设置要求输入 MAC 地址、外部 IP 地址 (192.168.2.1) 和外部子网掩码 (255.255.255.0)。在组态 NAT 路由器时, 选择路由模式并激活 NAT, 同时为内部接口添加相应的 IP 地址 (192.168.1.1) 和子网掩码 (255.255.255.0)。经过参数设置组态 NAT 规则, 允许组态的地址转换方向上的通信。

在分配规则集过程中, 可以通过打开用于设置属性的对话框并选择“防火墙”选项卡来检查分配情况。用户特定的 IP 规则集保存在“IP 规则”子选项卡里。经过设置并分配用户特定的 IP 规则集, 使得离线组态已完成。

此外, 通过添加发往 PC2 的 IP 地址的帧的目标 IP 地址 (192.168.2.100) 进一步指定此防火墙的规则, 同时在整个过程中可以通过设置, 记录适用所定义规则的数据包。将组态成功地下载到安全模块中, 安全模块将自动重启并激活新组态, 使设备处于工作状态。

3.4 ping 命令测试防火墙

最后使用 ping 测试来测试防火墙功能。由于组态, ping 数据包可以从内部网络传递到外部网络, 外部网络中的 PC 已回复 ping 数据包。安全模块作为防火墙具有状态检查功能, 可以使用从内部到外部的 IP 数据流量来测试。在 PC1 中调用“命令提示符”, 输入 PC1 对 PC2 执行的 ping 命令“ping 192.168.2.100”。如果 ping 通, 测试结果显示为 Lost=0 (0% loss), 这说明 IP 数据包已到达 PC2, 网络通信正常。此外, 将安全组态切换到在线模式进行在线诊断, 从安全模块中查看数据包过滤日志条目。当从 PC1 到 PC2 的数据包 IP 地址以安全模块的外部 IP 地址 (192.168.2.1) 显示在外部网络接口上, 则证明网络连接良好。

4 总结

工业通讯网络已经成为当今自动化过程应用中的重要

内容,从现场设备到操作系统、人机接口等,已深入到工业自动化的各个层次。本文对工业以太网通讯进行了需求分析、技术选择和网络构建,以交换机互为热备份的设计为基础,综合利用了虚拟路由器冗余协议和介质冗余协议,提升了系统对宕机的容忍度和网络的稳定性。在当前的大数据时代,如何保护网络,确保数据不丢失是整个生产线的重点。本文通过设置安全模块功能,对内部网络和数据进行保护,并利用了组播监听和快速漫游等技术,不仅提升了信息交换速率,更确保传输数据的安全性,最终制定出兼容经济性、技术拓展性和可复制性的方案。

参考文献:

[1] 张慧明. 工业以太网技术在建材工业的应用 [J]. 建材技术与应用, 2016 (6): 31-32.

[2] 朱永东, 李 彬. 浅析提高工业以太网的可靠性和稳定性 [J]. 电子技术与软件工程, 2013 (18): 37.

[3] 张国庆. 工业以太网交换机数据链路层安全分析与设计 [D]. 上海: 上海交通大学, 2014.

[4] Chen W, Yu Q, Yu P F, et al. Research of Ethernet Ring Protection Technology [J]. Applied Mechanics and Materials, 2014, 3207 (556): 6026-6029.

[5] Aref Meddeb. On building multiple spanning trees and VLAN assignment in metro ethernet networks [J]. Networks, 2013, 61 (3): 263-280.

~~~~~

(上接第 169 页)

[5] 陈志宝, 丁 杰, 周 海, 等. 地基云图结合径向基函数人工神经网络的光伏功率超短期预测模型 [J]. 中国电机工程学报, 35 (3): 561-567.

[6] 丁 明, 刘 志, 毕 锐, 等. 基于灰色系统校正一小波神经网络的光伏功率预测 [J]. 电网技术, 2015, 39 (9): 2438-2433.

[7] 王继东, 宋智林, 冉 冉. 基于改进支持向量机算法的光伏发电短期功率滚动预测 [J]. 电力系统及其自动化学报, 28 (11): 9-13.

[8] Almonacid F, P Rez-Higuera P J, Fernandez E F, et al. A methodology based on dynamic artificial neural network for short-term forecasting of the power output of a PV generator [J]. Energy Conversion and Management, 2014 (85): 389-398.

[9] 王 飞, 米增强, 甄 钊, 等. 基于天气状态模式识别的光伏电站发电功率分类预测方法 [J]. 中国电机工程学报, 33 (34): 75-82.

[10] 谭 津, 邓长虹, 杨 威, 等. 微电网光伏发电的 Adaboost 天气聚类超短期预测方法 [J]. 电力系统自动化, 41 (21): 33-39.

[11] Shi J, Lee W J, Liu Y Q, et al. Forecasting power output of photovoltaic systems based on weather classification and support vector machines [J]. IEEE Transactions on Industry Applications, 2012, 48 (3): 1064-1069.

[6] Fernandes F A, Sestito G S, Luis D A, et al. Influence of network parameters on the recovery time of a ring topology PROFINET network [J]. IFAC Papers OnLine, 2016, 49 (30): 278-283.

[7] 周振凯, 刘晓磊. 基于工业以太网交换机的轨旁骨干网组网方案的研究 [J]. 铁道通信信号, 2015, 51 (11): 48-50, 62.

[8] 邹航宇. 工业以太网冗余协议研究 [D]. 上海: 上海交通大学, 2013.

[9] 张 涛. 冗余工业以太网时钟同步方法研究 [D]. 上海: 上海交通大学, 2014.

[10] Stefanka M. The parallel redundancy protocol over wide area networks [J]. Smart Grid and Renewable Energy, 2016, 07 (04): 147-153.

[11] 韩 保, 董 鹏, 张小龙. VRRP 技术对通信 IP 网网络性能的影响 [J]. 价值工程, 2014, 33 (33): 207-209.

[12] 薛百华, 王 奕. 测控网络安全与工业以太网 [J]. 中国仪器仪表, 2012 (05): 42-45.

[13] 吕金泉. 工业以太网分布式环网的设计与实现 [D]. 北京: 中国科学院大学, 2016.

[14] 徐 敏. 基于 802.11r 的无线局域网漫游技术的研究与实现 [D]. 西安: 西安电子科技大学, 2010.

[15] 邓昌建, 陈东义, 张 衡, 等. 工业无线网络 Krylov 子空间估计与动态信道选择 [J]. 计算机工程与应用, 2015, 51 (11): 62-66.

~~~~~

[12] 叶 林, 陈 政, 赵永宁, 等. 基于遗传算法模糊径向基神经网络的光伏发电功率预测模型 [J]. 电力系统自动化, 39 (16): 16-22.

[13] 王继东, 宋智林, 冉 冉. 基于改进支持向量机算法的光伏发电短期功率滚动预测 [J]. 电力系统及其自动化学报, 28 (11): 9-13.

[14] 王书舟, 伞 冶. 基于支持向量机的直升机建模 [J]. 计算机集成制造技术, 2008, 14 (3): 472-476.

[15] 杨纶标, 模糊数学原理及应用 [M]. 4 版. 广州: 华南理工大学出版社, 2006.

[16] 刘兴杰, 岑添云, 郑文书, 等. 基于模糊粗糙集与改进聚类的神经网络风速预测 [J]. 中国电机工程学报, 34 (19): 3162-3169.

[17] Radzikowska A M, Kerre E E. A comparative study of fuzzy rough set [J]. Fuzzy Set and Systems, 2002, 126 (1): 137-156.

[18] 戴 虹, 陈晋武, 张 震, 等. GRNN 在肌电预测踝关节运动中的应用 [J]. 仪器仪表学报, 34 (4): 845-852.

[19] Yan W Z H. Toward automatic time-series forecasting using neural networks [J]. IEEE Transactions on Neural Networks and Learning Systems, 2012, 23 (7): 1028-1039.

[20] 林 喆, 兰 生, 张宇航. 基于广义回归神经网络的油纸绝缘变压器的寿命预测 [J]. 高压电器, 2015, 51 (2): 125-130.