International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 6 Issue 4 Ver. I ǁ 2018 ǁ PP. 42-46

Industrial Ethernet Communication Network Design

Xu Pengfei[1], Zhang Jing[2], Yin Tengfei[3], Qian Xiaoxiao[4], Yang Yong[5]
[1](College Of Electronic And Electrical Engineering, Shanghai University Of Engineering Science, Shanghai, 201620, China)
Corresponding Author: Xu Pengfei

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

Date of Submission: 24-03-2018 Date of acceptance: 09-04-2018

I. Introduction

Industrial Ethernet is widely used in industrial production because of its high performance and high interoperability. Its security and redundancy have become two core issues of industrial networks. Ethernet redundancy is generally divided into two categories: One is to provide line and switch redundancy, mainly STP, RSTP and MSTP, etc. They use a ring topology to prevent the emergence of a logical ring network, but the failure recovery time is longer [1-3]. However, the Media Redundancy Protocol (MRP) can quickly detect ring network link failures and establish a new network topology to restore the network [4]. The other type is to connect two independent Ethernets through a node, mainly PRP and so on. PRP does not lose packet data, but it increases the number of network packets, and clock synchronization is difficult to implement [5]. In addition, VRRP(Virtual Router Redundancy Protocol) technology is a reliable technology designed for network interruption. It can automatically switch the network to fault-free network to ensure the continuity and reliability of network communication [6-7].

In order to solve the enterprise's requirement for secure and stable information and data from the field level to the management level, this paper comprehensively uses VRRP and MRP protocols based on the analysis of relevant technology requirements, and designs a communication network solution that the two switches become hot backups to each other. It realizes network communication with strong self-healing and enhances the stability of the system. In addition, the use of security module functions and technologies such as Internet Group Management Protocol Snooping (IGMP Snooping) and iPCF enables data to be transmitted between the internal and external networks in isolation, as well as ensuring the fast and secure wireless transmission. Based on technical analysis and structural design, the plant's network communication system is built.

II. Network communication technology requirements

Factory production department has features such as reproducibility and substitutability, and different workshops only establish communication with the control center. With the increasing industrial network architecture, how to ensure the fast and secure network transmission and the stability of the system through technical means have become necessary functional requirements. This section focuses on the analysis of various communication technologies related to Industrial Ethernet.

2.1 Channel Division and iPCF Fast Roaming

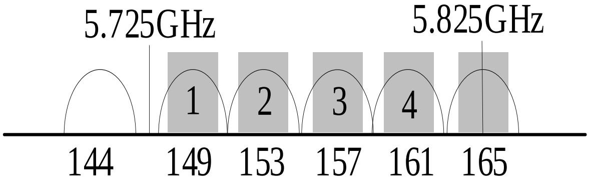


Fig.1 Channel selection

In wireless communication, in order to enhance the anti-jamming of wireless communication, the IEEE 802.11r mode is used to work. The work area is set in the 5.725-5.825 GHz frequency band and divided into four channels, as shown in Fig.1. In order to avoid being in the same coverage area, the adjacent omnidirectional antenna AP (Access Point) causes congestion due to the shared channel, resulting in increased load. Therefore, the AP's channel is set to 1-2-3-4-1.

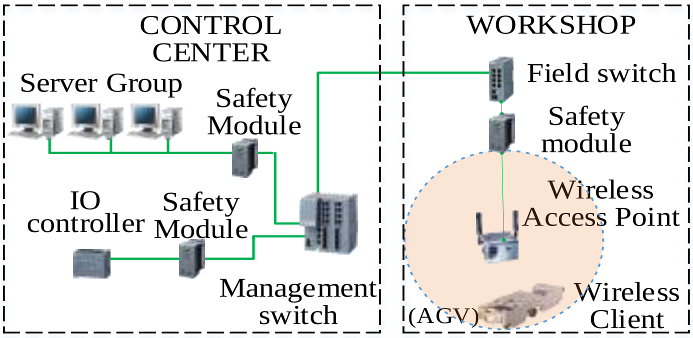


Fig.2 Wireless communication control system

Automatic Guided Vehicle (AGV) is a kind of simple mobile robot integrating sound, light, electricity and computer. It is mainly used in flexible processing systems and flexible assembly systems. As shown in Fig.2, when the AGV moves quickly in different workshops, the client on the car quickly switches in different wireless zones. At this point, each AP access point polls the client for connection in a fixed channel order. When the contact with the AP is lost, the client scans the next channel from its allowed channel list and selects the nearest AP connection. When setting the access point mode and client mode, start the device PNIO support function and select an update time of more than 32ms. This ensures that multiple access points in the system can communicate on different channels, reducing roaming time to less than 50ms.

2.2 Multicast Snooping Controls the Priority of Data Processing

The switch implements restrictions on multicast data (black arrows) through multicast snooping and multicast routing. By snooping the IGMP control message (white arrows), the switch parses the current group member status and creates a multicast forwarding table, and updates the status of the group member hosts in real time, so as to achieve dynamic registration of IP multicast.

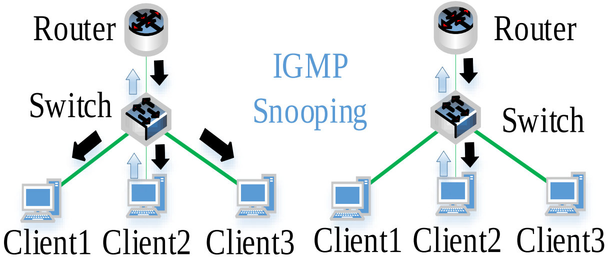


Fig.3 IGMP Snooping function

As shown in Fig.3, when listening to Client 2 sends a report message (Client 1 and Client 3 are not sent), the switch adds the port which connected to Client 2 to the multicast address table, thus forming a mapping with the MAC multicast address. After multicast data is sent from Layer 3 devices, Layer 2 multicast devices enable IGMP snooping and send data only to Client2 to implement priority control on data processing. This reduces bandwidth usage and improves transmission rates.

The switch periodically sends IGMP Query messages from all hosts. If the host wants to continue receiving this address table group message, it should respond to the IGMP Report message. If the switch does not receive IGMP Report messages from any host, the switch will be reorganized and logged out.

2.3 Security Module Function Protects the Device

On the production line, some data cannot be disclosed to the public. The transmission of the communication is filtered in the same way as the MAC address and communication protocol. Network Address Translation (NAT) translates a protected internal network address into an external network address, thereby establishing a controlled connection. The security module acts as a firewall and NAT route to isolate the internal network from the external network.

In addition, the role of the firewall integrated into the security module is to protect IO devices from unauthorized access. Configure it to only allow access to virtual stations and set communication overload limits. The security module saves the data in a log file. The logging function supports monitoring access and records those attacks that are accessed and attempted, so that preventive measures can be taken. The security module only allows communication between authenticated and authorized devices. This prevents operators from making mistakes. Preventing unauthorized access can avoid interference and communication overload.

III. Plant layout and network structure design

Considering some characteristics which the industrial system's high requirements for network redundancy self-healing, low tolerance to downtime, and so on. The approach adopted in this article is to combine the VRRP and the MRP, while allowing the two switches (A and B) to be hot backups of each other. It reduces the impact of switch failures and avoids problems such as network cycles and broadcast storms.

3.1 Plant Layout Design

Industrial communication network structure is divided into three parts: management network, field layer network and wireless transmission network. The management layer is located in the control center and is responsible for the transmission of data flows and the control of access to network resources. The field layer is located at the production line and is responsible for the collection and transmission of production data. The wireless transmission network is responsible for the command and data acquisition and transmission processing between the AGV system and the control center

.

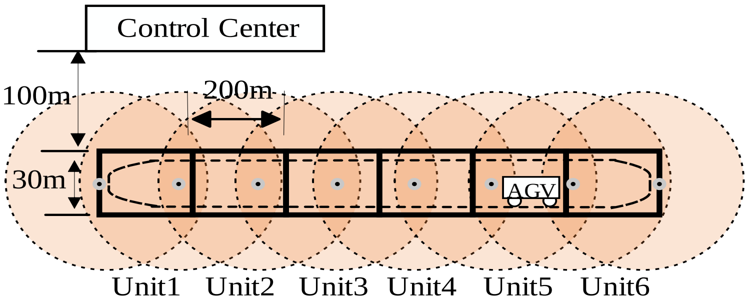


Fig.4 Factory workshop layout

A plant area is mainly composed of a control center and a workshop. As shown in Fig.4, the workshops are arranged in a straight line, each with a length of 200 meters and a width of 30 meters. The AGV runs along the circular track from the unit 1 to 6. The control center conducts wired communication with the production line. The AGV signal is connected to the main network in a wireless manner to realize communication with the control center.

3.2 MRP Protocol Reduces Reconfiguration Time

By establishing a ring topology, a single failure of a switch or line in a ring Ethernet can be compensated by MRP. Through the WEB page configuration of the switch, all ring ports are set to full duplex and 1000 Mbps. The management switches A and B are set as media redundancy managers (MRM) and the field switches as media redundancy clients (MRC). Both form a ring network, and the ring network is managed by MRM.

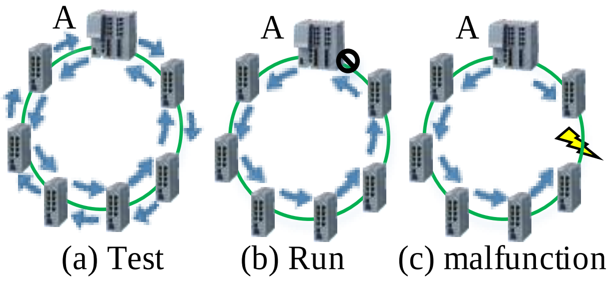


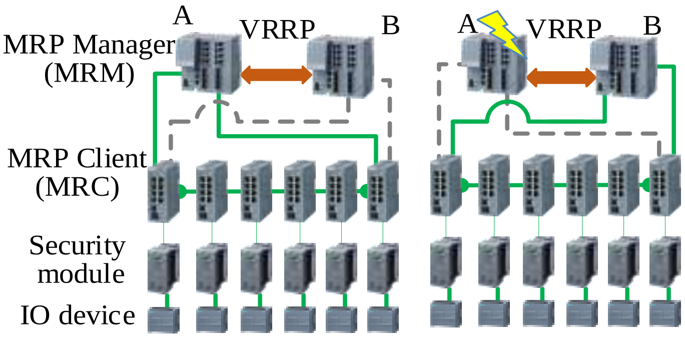
Fig.5 MRP working status in different situations

As shown in Fig.5, the MRM sends test messages on two ports at regular intervals. If the test message can be transmitted from one port to another, it indicates that the ring network is unblocked. At this point, the MRM blocks one port to avoid infinite loops. If the MRM does not receive subsequent test messages, the MRM will reconstruct and connect through its blocked port. The maximum reconfiguration time of MRP is 200ms. In order to ensure that IO does not fall during network reconfiguration, the watchdog time of the IO device needs to be set to 200ms or more. MRP is expandable. It can quickly detect network errors and establish redundant network paths in milliseconds, reducing the time it takes to reconfigure the network.

3.3 VRRP Protocol Reduces Single Faults

The Virtual Router Redundancy Protocol (VRRP) solves the static configuration problem by grouping a set of routers into virtual routers (VR). Layer 3 switches A and B have routing and VLAN functions. A and B form VR in logical groups and use the same virtual ID. When setting up the network, set A as the primary virtual router with a priority of 255. The entire VR uses the IP address of the physical Ethernet interface of A. A is responsible for forwarding messages that are sent to that IP address. B acts as a backup router and its priority is arbitrarily set in the range of 1-254.

A assigns a virtual IP address and MAC address to its network interface. Meanwhile, A sends VRRP messages to B at a certain interval to explain its operating status to B. In Fig.6, when A fails, the higher priority B becomes the primary virtual router. B replaces A for processing messages from the control center and the client. This ensures that the link is in an uninterrupted state. VRRP reduces the possibility of switch failures in the network.



(a) Normal Status (b) Fault Status

Fig.6 VRRP working status in different situations

IV. Network Construction and Implementation Detection

4.1 Distribution and Connection of Devices

In order to reduce the number of equipment, combined with the actual situation, the entire plant area uses an omnidirectional antenna covering a radius of 200 meters. They are arranged along the track at an interval of 170 meters ,as shown in Figure. 4. At the same time, it ensures seamless transmission of data and signals when the car moves at high speed. When an AP fails, the transmission range of the failed AP can still be covered by neighboring APs, and signals and data can still be transmitted continuously throughout the entire network.

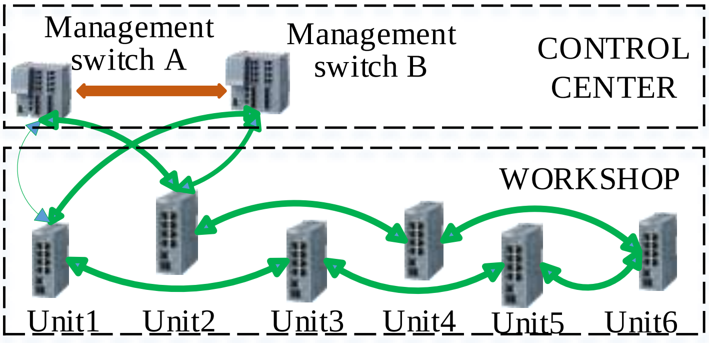


Figure.7 Switches connection method

In combination with the factory layout, 1000Mbps multimode fiber is selected as the transmission medium to meet a large number of data transmission requirements. Its standard transmission distance does not exceed 750 meters. Taking into account the actual wiring and environment, this paper uses crossover mode to achieve multi-site and long-distance optical fiber connections, as shown in Figure 9. This method saves equipment costs. The wiring sequence is 1-3-5-6-4-2.

4.2 Configuration of Security Module Functions

This article uses the Siemens SCALANCE S security module as a firewall and NAT router. In order to test whether the communication network is normal, it is necessary to set IP for the PC.

When creating the module, enter the MAC address, external IP address (200.1.1.1), and external subnet mask (255.255.255.0) as required. When configuring the NAT router, select the route mode and activate NAT. At the same time, the corresponding IP address (192.168.1.1) and subnet mask (255.255.255.0) are added to the internal interface. The configuration of the NAT rules is parameterized to allow communication in the configured address translation direction. In addition, the firewall's rules are further specified by adding the destination IP address (200.1.1.3) of the message addressed to PC2's IP address. At the same time record the data packet that applies this rule. The configuration is then downloaded to the security module so that the device is in operation.

Tab.1 PC's IP settings

PC	IP Address	Subnet Mask	Gateway
PC1	192.168.1.100	255.255.255.0	192.168.1.1
PC2	200.1.1.3	255.255.255.0	200.1.1.1

4.3 Ping Command Test Firewall

The security module has a status check function as a firewall, which can be tested by using IP data traffic from inside to outside. Then call "Command Prompt" in PC1 and enter the ping command that PC1 executes on PC2: "ping 200.1.1.3".If the ping is normal, the test result will be displayed as Lost = 0 (0% loss). This indicates that the IP packet has reached PC2 and the network communication is unblocked. In addition, the safety configuration is switched to online mode for online diagnostics. The packet filter log entries can be viewed from the security module. If the IP address of the packet from PC1 to PC2 is displayed on the external network interface as the external IP address of the security module (200.1.1.1), the network connection is proven to be good.

V. Summary

This article has carried on the demand analysis, the technical choice and the network construction to the industry ethernet communication. It is mainly based on the design that two switches mutually become hot backups, and comprehensively utilizes VRRP and MRP protocols to achieve a higher system tolerability and network stability. The internal network is protected by setting the security module function. The use of technologies such as IGMP Snooping and iPCF not only improves the rate of information exchange, but also ensures the security of transmitted data. The final formulation of the program is compatible with economics, reproducibility and technology development.

References

[1] M. Marchese, M. Mongelli. Simple protocol enhancements of Rapid Spanning Tree Protocol over ring topologies[J]. Computer networks, 2012, 56(4):1131-1151.

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

[3] Wei Chen, Qiang Yu, Peng Fei Yu, Research of Ethernet Ring Protection Technology, Applied Mechanics and Materials[J]. 2014, 3207(556): 6026-6029.

[4] Fábio Alves Fernandes, Guilherme Serpa Sestito, André Luís Dias, Influence of network parameters on the recovery time of a ring topology PROFINET network, IFAC PapersOnLine[J]. 2016, 49(30):278-283.

[5] Martin Stefanka, The Parallel Redundancy Protocol over Wide Area Networks, Smart Grid and Renewable Energy[J]. 2016, 07(04):147-153.

[6] Mr. Augustine Praveen Raja Ilango, Dr. T.V.U. Kiran Kumar, Ms. A. Geetha, Dynamic Time Sync Reference Load Balancing In Virtual Router Redundancy Protocol, International Journal of Engineering Sciences & Research Technology[J]. 2013, (5):1128.

[7] Hiroshi Matsuda, L2 Switch Feature for Virtual Router Redundancy Protocol Fast Convergence, International Journal of Computer Applications[J]. 2012, (11):1.

Xu Pengfei "Industrial Ethernet Communication Network Design" International Journal of Research in Engineering and Science (IJRES), vol. 06, no. 04, 2018, pp. 42–46.