

The new trend in industrial communications and industrial automation applications—Industrial Ethernet

Vincent Liu, MOXA Product Manager

Redundancy is currently one of the hottest topics for many industries and business information backup systems, particularly in light of the fact that more types of industrial equipment now comes with an Ethernet interface. In fact, the rapid development of hardware and software for Industrial Automation has forced administrators responsible for network monitoring and management to think more carefully about the different kinds of requirements for backing up systems in an unstable environment.

In this paper, we discuss different recovery requirements for redundant solutions, as well as approaches to keeping redundant hardware and software architectures running reliably and at peak performance. The technology related to redundant solutions will also be considered.

Redundant Ethernet Applications in Industrial Automation

Before looking in detail at the different levels of redundancy required for control systems in industrial automation, we should first point out that dual connections between LAN switches (at the information level) and the enterprise backbone are a must. Of course, there are some plant floors where no type of redundancy application has been established, but saving money by not setting up redundancy can very easily result in lax control and vulnerability to disasters. In the following sections, we will focus on what is practical, effective,

Released on August 10, 2003, First modification on July 2, 2007

Copyright © 2003 The Moxa Group. All rights reserved.

MOXA manufactures one of the world's leading brands of device networking solutions. Products include industrial embedded computers, industrial Ethernet switches, serial device servers, multiport serial cards, embedded device servers, and remote I/O servers. Our products are key components of many networking applications, including industrial automation, manufacturing, POS, and medical treatment facilities.

How to contact MOXA

Tel: 1-714-528-6777
Fax: 1-714-528-6778
Web: www.moxa.com
Email: info@moxa.com

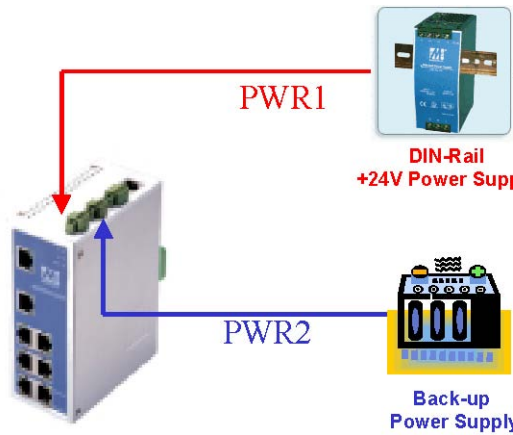


This document was produced by the Moxa Technical Writing Center (TWC). Please send your comments or suggestions about this or other Moxa documents to twc@moxa.com.

and important for redundancy in automation control.

Power Redundancy

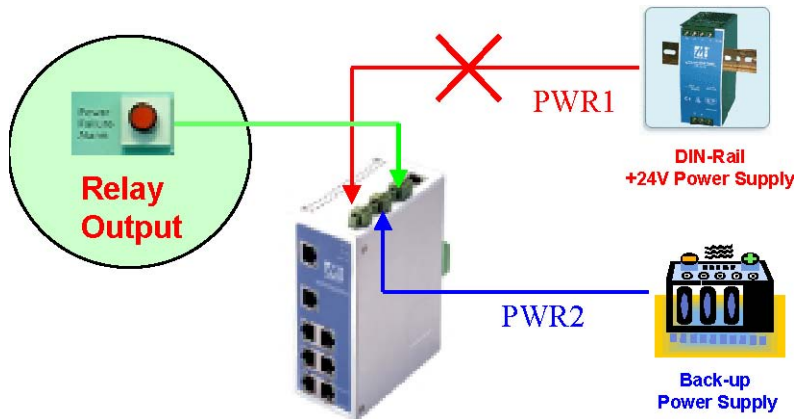
Unlike the “comfortable” environment of office automation, control systems used in industrial automation must be able to withstand harsh environmental conditions. For this reason, a basic redundancy requirement for control systems is that every part of the communication network should be hooked up to a backup power supply in case of a power outage. The backup power supply takes over as soon as the electricity fails, minimizing the possibility of damage caused by the system shutting down.



Furthermore, the system’s hardware should at least be compatible with unregulated DC and have reverse power protection. As discussed next, the two most common ways to send power failure alarms to network administrators is by e-mail or relay output.

Alarms by Relay Output

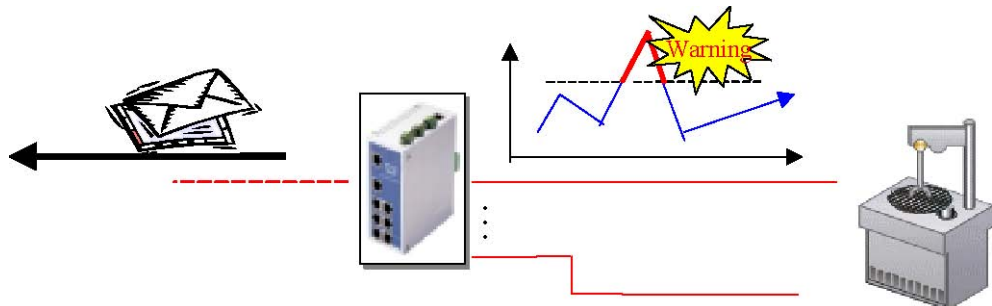
When one of the power supplies fails, the relay output will send an alarm to the administrator automatically.



Exception Report by Email

An e-mail with warning message will be sent to the administrator automatically when an exception/event is detected.

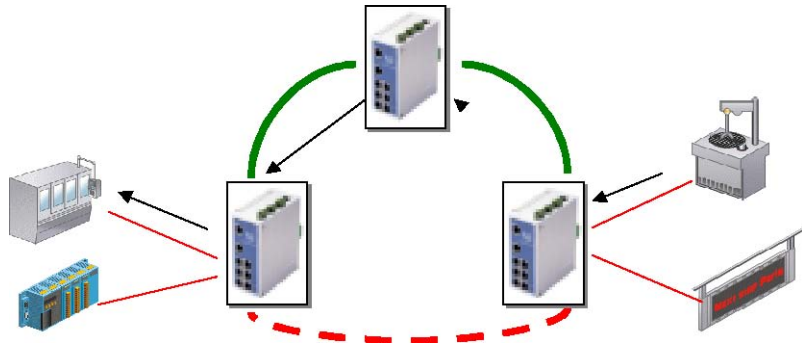
Switch Events		Port Events
Cold Start	Warm Start	Link On
Power On/Off	Authentication Failure	Link Off
Topology Change	Configuration Change	Traffic Overload



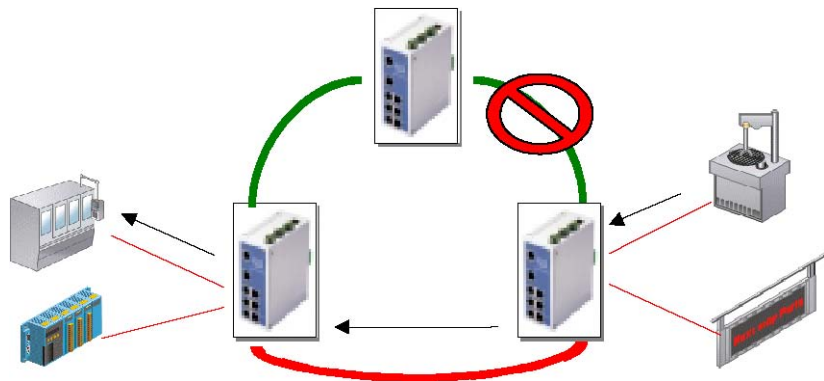
Media Redundancy

Media redundancy, which involves forming a backup path when part of the network becomes unavailable, is a basic requirement for automation. The technology developed recently for media redundancy—called IEEE 802.1D Spanning Tree Protocol, or STP for short—uses an Ethernet ring topology with backup paths. In the early years, it was not possible to create an Ethernet ring topology since loops in an Ethernet network are not allowed. In addition, using a dual-star topology to create an automation system network that is readily available and also reliable is one option, but the cost of

creating such a network is high. What IEEE 802.1D does is to identify one of the switches in the network as the “root switch” of the network, and then automatically block packets from traveling through any of the network’s redundant loops.



In the event that one of the paths in the network is disconnected from the rest of the network, the STP automatically readjusts the ring and uses the redundant path. The actual topology of the redundant ring—that is, which segment will be blocked—is determined by the number of switches that make up the ring.

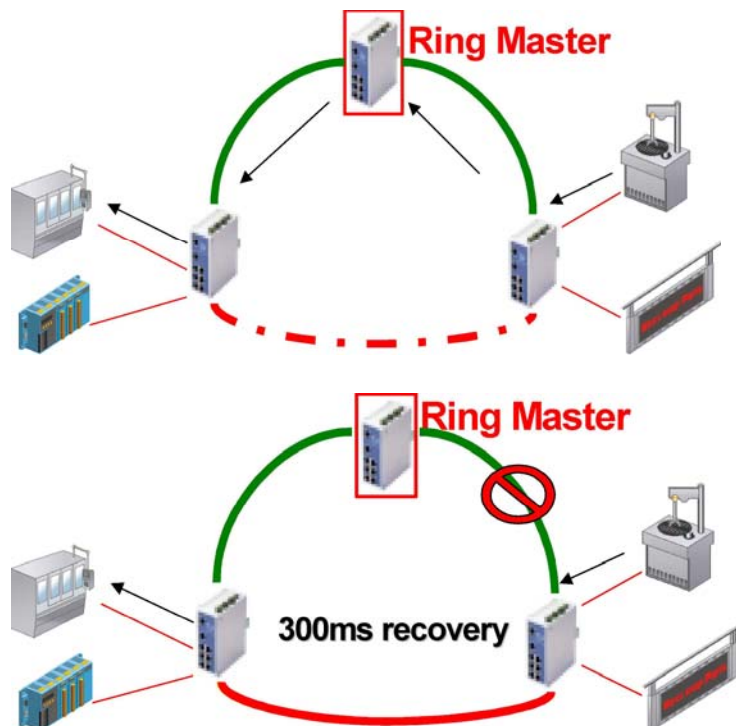


Although IEEE 802.1D STP has solved some limits of Ethernet network technology, it also has limitations, including lower convergence speed, constraints of bridge diameter, VLAN insensitivity, and link blockage (when the bandwidth is not enough for all traffic). For this reason, IEEE 802.1W Rapid Spanning Tree Protocol (RSTP) was developed. This newer protocol has all the advantages of IEEE 802.1D, but in addition provides higher performance, as well as the correct behavior

for mis-ordering and duplication in RSTP Bridges.

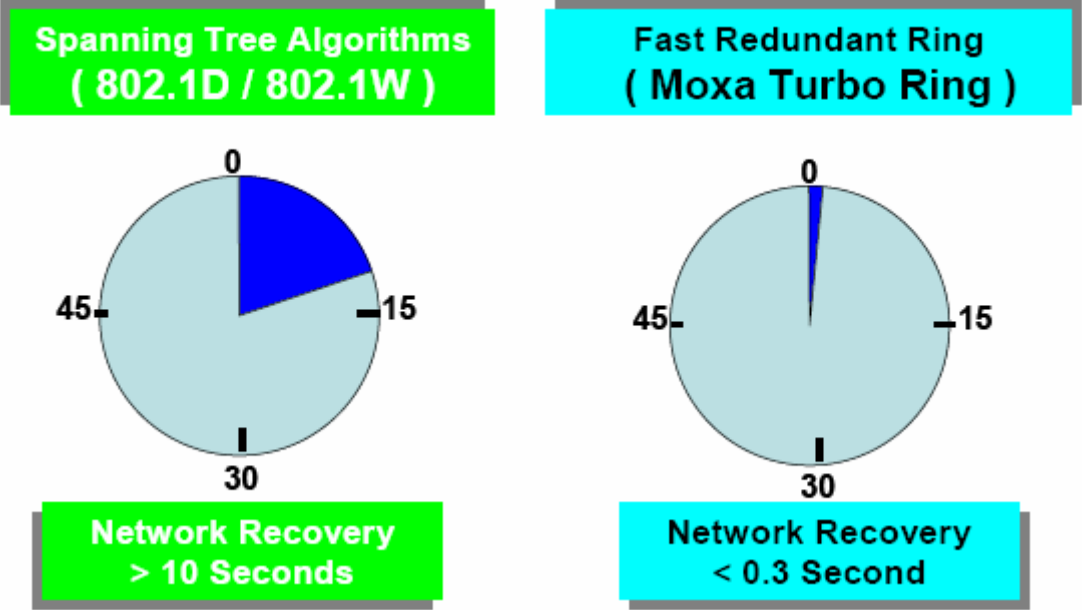
RSTP can also work with legacy STP protocols, and start a migration delay timer of 3 seconds. It reduces the convergence time for the physical media to signal link failure, and the six-link “propose-sync-agreement,” which is based on a maximum diameter of 7 for the Bridge LAN handshakes, is decreased to the ms range for failures that involve point-to-point links. The technologies mentioned above made media redundancy with high performance not only possible, but also feasible.

For this reason, many Ethernet device manufactures are developing proprietary protocols based on 802.1W to meet the fast recovery time required in industrial automation. Moxa has recently joined this movement by presenting customers with Moxa Turbo Ring, which has a recovery time of under 300 ms at 20 nodes with 120 devices. (Note: Turbo Ring has been upgraded to provide a recovery time of under 20 ms, at a full load of 250 devices.)



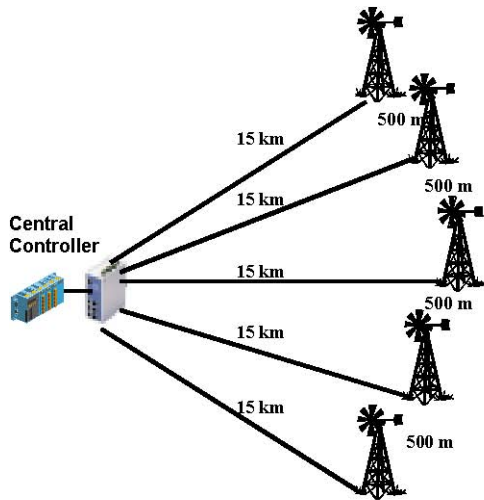
(Note: Turbo Ring has been upgraded to provide a recovery time of under 20 ms, at a full load of 250 devices.)

If guaranteeing a recovery time of less than 1 second is the most critical media redundancy issue, then Moxa Turbo Ring is certainly the best choice. (Note: Turbo Ring has been upgraded to provide a recovery time of under 20 ms, at a full load of 250 devices.)



In addition, media redundancy by ring topology also reduces the cost when it comes to long distance wiring. In some applications, such as windmill monitoring and management, the wiring distance is quite long. But with ring topology, you can decrease the cost of wiring by quite a bit, making the wiring much more cost-effective.

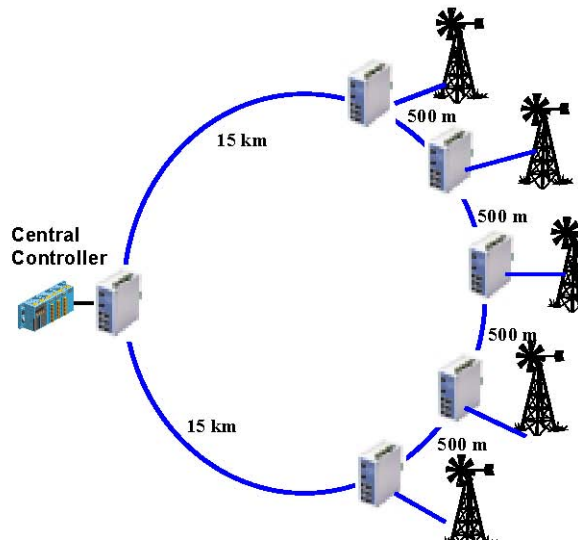
Start Topology Cabling



Cable Length=15+15+15+15+15=75 km

Network Node
Redundancy

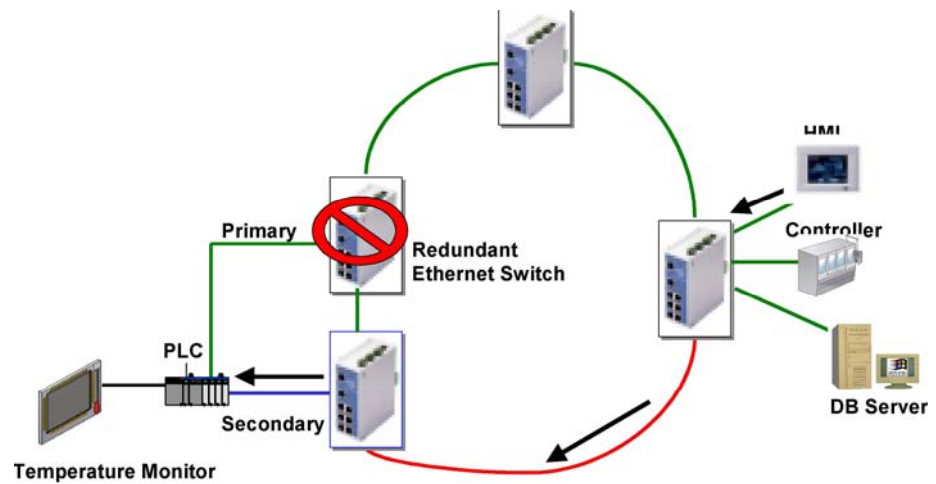
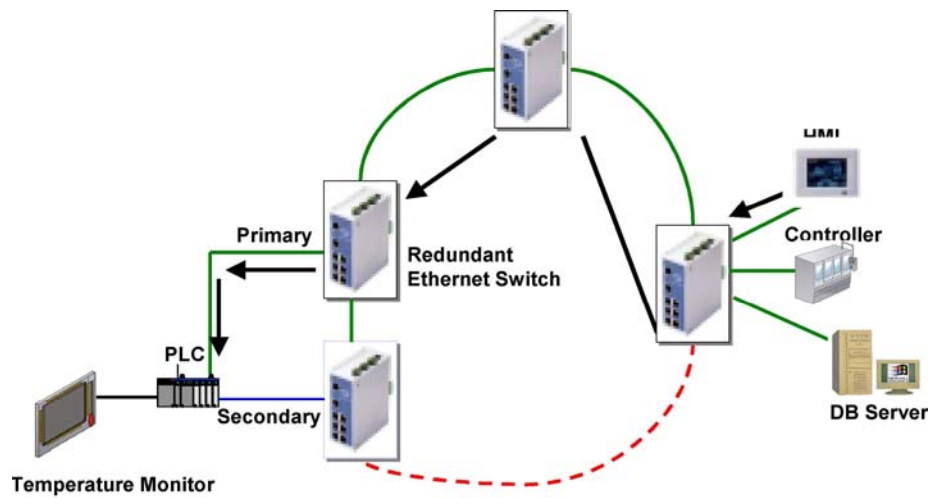
Ring Topology Cabling



Cabling=15+15+0.5+0.5+0.5+0.5=32 km

After successfully implementing media redundancy in an industrial Ethernet network, another problem is how to include every point in the entire control system. For this reason, switches that are connected to critical devices need to set up dual network nodes, one of which is the second Ethernet switch. Both of these network nodes should connect to a dual-homing controller.

To keep the system running normally when a network disaster occurs, a controller that supports two Ethernet interfaces to connect both redundant switches, and which has the capability to select the most suitable homing path, must establish connections with certain critical end devices. In this case, the cost of redundant equipment would be less than buying an exact duplicate of the network switch, and part of the critical system would still be running if a network failure occurs.



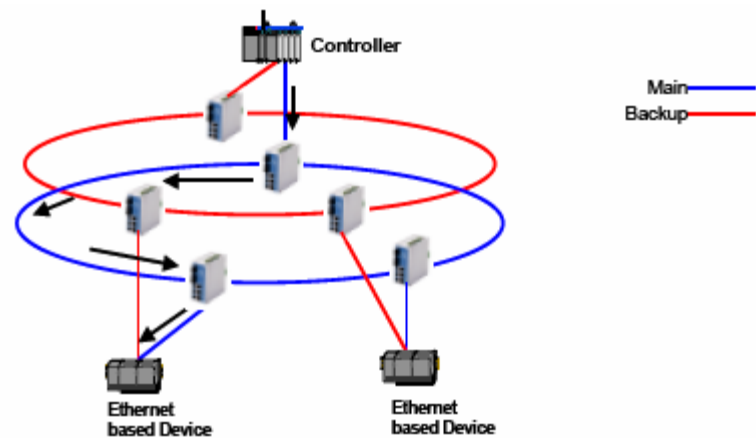
Each node represents a switch, and the duplicated switch must connect with the same critical devices under these circumstances. This means that not all of the devices in the system will be able to connect to this Ethernet redundant switch because of certain concerns, such as cost. Besides, implementation of network node redundancy depends on the actual needs of each industrial automation application.

Network Redundancy

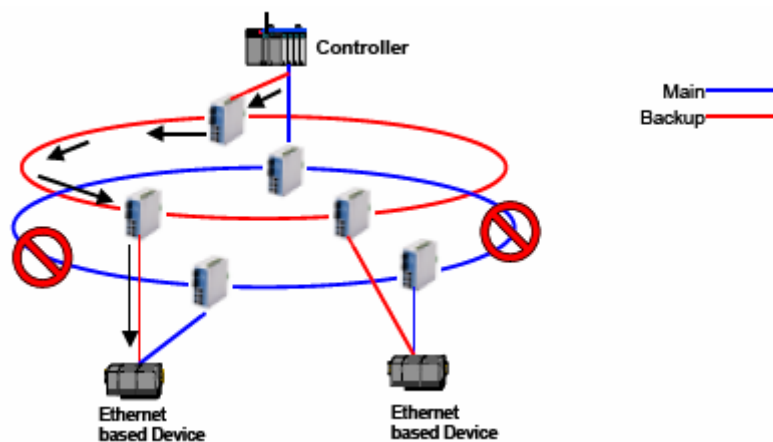
When a network disaster occurs, companies often suffer great loss. For this reason, all network administrators in industrial automation need to establish a network that is available 100% of the time to let all network nodes continue to operate once an accident occurs.

Once media redundancy is implemented successfully, network node redundancy will perform better to help reduce system downtime. If every node of a network is to have network node redundancy, the advanced redundancy management of Ethernet networks has to be taken into consideration, as well as two completely independent networks and two communications ports on connected devices. There are two ways to get two communication ports on your connected devices. If your device already has 2 Ethernet ports, you can label them Port A and Port B. If you use 1-port devices, the devices need to be upgraded to two Ethernet ports for the purpose of determining the primary and secondary homing paths. The shift in the controller of a network must be obstacle-free and transparent in order to determine the safest path for data flow.

General Flow Control



Network Failed



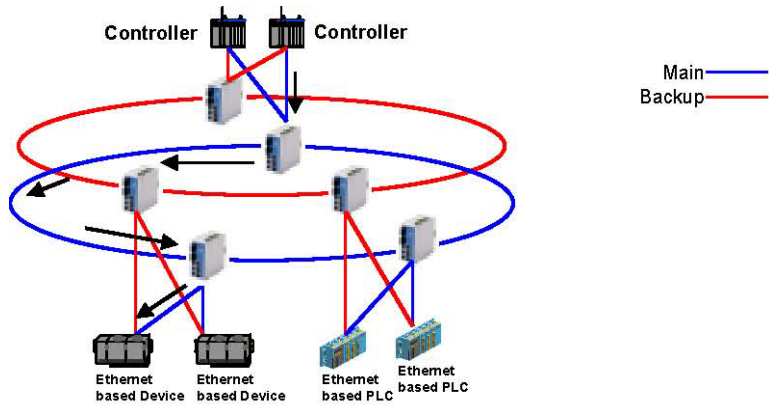
The bottom line is that the redundant network should be able to replace the failed network when a network disaster occurs, meaning that the network continues to function, even though many faults have occurred.

Complete System Redundancy

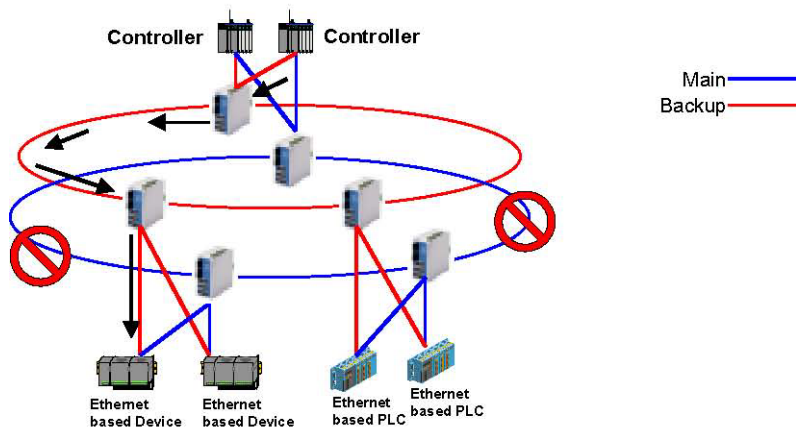
Although you might decide not to establish redundancy for all devices of a network due to budget and space limitations, it is still good to know how to create a system that is completely redundant. A completely redundant system consists of redundant switches, redundant communication ports, and redundant device pairs. All Ethernet devices and workstations are connected to both independent ring network architectures. Depending on the circumstance, there are two possibilities that fit this redundancy application. One of the possibilities uses devices that have two ports, with one of the ports utilized for the primary path, and the other port serving as the secondary path. The other possibility uses devices that have only one port. In this case, the devices must be upgraded to two Ethernet ports, in order to form the primary and secondary paths.

Complete system redundancy can form an extremely reliable network that minimizes data loss and has fast recovery time. There must be a dual homing controller that is able to distinguish which Ethernet device is active—the primary path or secondary path. The diagnostics can ensure that active devices are fully functional and ready to take over at any time. IEEE 802.1p/Q can perform a wide range of diagnostics, keeping track of the status of the network, as well as all devices that make up the networks. Some fieldbus devices from different manufacturers exchange packets with each other periodically over the networks through diagnostic messages, serving as an indication of “signs of life.” These devices usually have a complete picture of the network so that they can select intelligently which network, device, and port to communicate with. A failure detection function can detect late and lost messages and duplication.

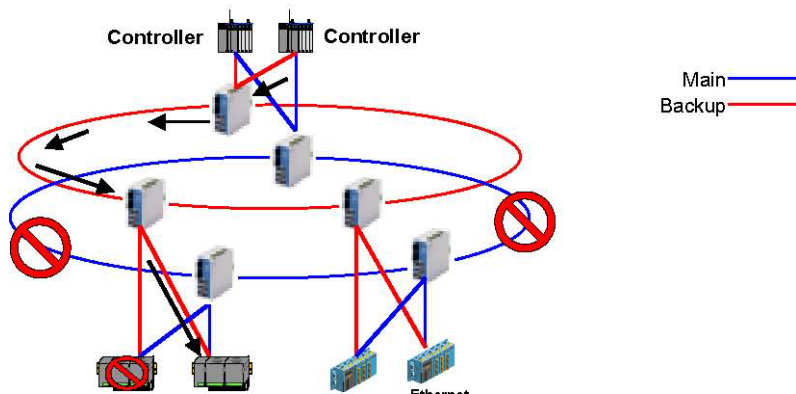
General Flow Control



Network Failed



Network and Device Failed



On the other hand, diagnostics in control applications of the network can detect failures, allowing end devices to respond with a notification to the administrator. When managing distributed redundancy, the problem of heavy traffic on a centralized system can be avoided. Communication ports and pairs of devices, and redundancy management of the entire architecture will select the most suitable route to communicate

with other devices based on the health of network segments. In this way, the complete system redundancy can survive and keep running, even if many faults crop up.

What to consider when constructing a 100% reliable redundant architecture for an Ethernet network in industrial automation

To ensure 100% system availability of the plant floor for industrial automation, many vendors have proposed different criteria for redundant network systems. To prevent your networks from being damaged by power failure, you should establish power redundancy in every component of the entire network. As far as reestablishing a backup path is concerned, 802.1D/W makes it both possible and feasible. Some Ethernet switches are connected with several critical devices whose data transmission to the central controller cannot afford breakdowns. For this reason, you will need node redundancy instead of media redundancy, since backing up paths is no longer enough to satisfy higher demands. Will a dual network solve the problems met in all industrial automation applications with high availability and efficient recovery? Where can you report the control status of a gas chromatograph or burner management? These are some of the reasons why people wish to establish complete system redundancy.

After understanding more about the several topologies and related methods of redundancy needed by current control systems for industrial automation, we need to emphasize again the importance of availability. In the early days, newly-developed equipment in industrial automation did reduce the need for workers. But it was common for administrators to work long hours in the field collecting monitoring data, fixing transmission problems, and dealing with network disasters.

The redundancy we have been talking about is divided into several levels in terms of device, and is displayed in the following table:

Level	Redundancy	Applied Situation	Device port
1	Power Redundancy	The basic issue for any sort of redundancy	1
2	Media Redundancy	+ Keeping backup path	1
3	Network Node Redundancy	+ Consideration of single failed switch	2
4	Network Redundancy	+ Consideration of multiple failed switches	2
5	Complete System Redundancy	+ Consideration of multiple failed end devices	2

This table can be used to analyze, and serve as a reference for system redundancy. Companies can select the most suitable option based on their needs and budget.

What to consider when selecting transmission media

After understanding the different kinds of needs for redundancy in industrial automation, the next thing we need to consider seriously is transmitting media. In this regard, the following constraints have to be taken into consideration:

Constraint	Solution
Electrical Isolation	Fiber in the communication path
Noise Immunity	Fiber in the communication path
Security	Fiber in the communication path
Distance > 2 km	Single mode fiber in the communication path
2 km > distance > 100 m	Multi-mode fiber in the communication path
Distance < 100 m with environmental influence	Shielded Cat 5 copper wire in the communication path
Distance < 100 m without environmental influence	Unshielded Cat 5 copper wire in the communication path

The following table lists the necessary connections and speeds.

Connection	Speed
Backwards compatible	1000BaseT full-duplex
	1000BaseT
Auto-negotiation—lowest speed will be chosen	100BaseT2 full-duplex
	100BaseTX full-duplex
Half duplex works in shared Ethernet (HUB) only	100BaseT2
	100BaseTX
Full duplex works in a switching environment. Double performance of Ethernet.	10BaseTX full-duplex
	10BaseTX

Summary

Since Ethernet now penetrates the automation hierarchy, and Industrial Ethernet switches have started playing a key role in setting up Ethernet LANs, we can expect the technology available for plant floor systems in industrial automation to keep improving. The power, media, node, network, and complete system redundancy mentioned above certainly help create a more convenient kind of industrial automation control. In short, we should pay careful attention to the redundancy concept, and include it as a central part of the design of industrial automation networks.

Disclaimer
This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form for any purpose, without our prior written permission.