

# Hirschmann Network Systems

## *White Paper*

*High Availability Industrial Automation Networks*

**The evolution of Industrial Automation networks .....3**

**Assessing the cost of downtime.....4**

Minimising the Impact of downtime ..... 4

**The need for an Architecture .....5**

Architecture for high availability Industrial networking ..... 5

Key technology positions for the IA network ..... 5

**High availability & resiliency requirements.....6**

Use of high availability systems ..... 6

Reliability/resiliency ..... 6

Resiliency Features..... 7

Manageability ..... 8

Supportability..... 8

An insurance policy ..... 8

**Hirschmann high availability IA Ethernet solutions .....9**

So when is a ring not a loop? ..... 9

Building high availability Industrial networks with Ethernet ..... 12

Evaluation criteria..... 12

**Network design guidelines for High Availability IA Networks ..... 13**

**Conclusion ..... 16**

# High Availability & Resilience

According to International Data Corporation, "A system is considered to be highly available if, when failure occurs, data is not lost, and the system can recover in a reasonable amount of time." Therefore keeping the network available is one of the top priorities for IT professionals today. It also is one of the largest contributors to system costs.

To determine the value of high availability services, IT managers are forced to weigh the costs of downtime against the risks. It all comes down to one central question: How much should be paid to insure against downtime?

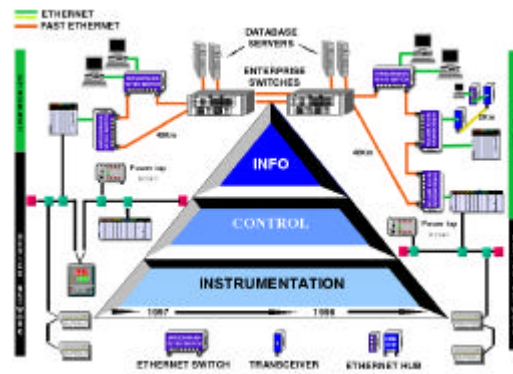
This white paper compliments Hirschmann's 'Distributed Communication Architecture' (DCA) White Paper, it aims to:

- ❑ Help you assess the cost and impact of downtime on your customer's business
- ❑ Develop the network resilience component of the overall IA architecture.
- ❑ Define your high availability & resiliency network strategy.
- ❑ Provide network design examples on building high availability, Ethernet field bus systems.

## The evolution of Industrial Automation networks

The seamless integration of the Office Automation and Industrial Automation networks will result in improved productivity and help to significantly reduce costs. The consequential 'information explosion' resulting from the deployment of intelligent 'web enabled' devices, Manufacturing execution systems (MES), computerised maintenance management systems (CMMS), decision support systems and more, will strain, beyond breaking point, the traditional approach to industrial networking.

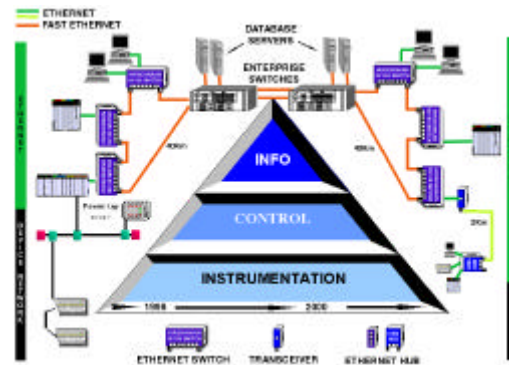
The traditional fieldbus network follows a structure that make the seamless integration of Office Automation (OA) and Industrial Automation (IA) impossible. The traditional multi-layered, hierarchical network deployed in the majority of Industrial networks today will not support the distributed intranet computing model that is set to dominate the IA Industry over the next 3 years. As can be seen from the diagram, a multi-layered approach introduces bottlenecks to the flow of data. Information gained from the intelligent sensors and devices connected at the instrumentation layer must traverse Controllers, HMI, or PC gateways before reaching the destination enterprise servers that serve management and decision support systems on the OA network.



Since Ethernet is already the network choice for business computing, its presence at the control level will make the visionary's goal of sensor to boardroom integration a much easier task for manufacturers. Issues that prevented Ethernet from being used in the design of real time control environments have now been overcome with standards based solutions. In terms of speed and data transfer rates, Ethernet comfortably exceeds those of high-speed fieldbus, such as Profibus and ControlNet. Whereas Profibus has a

maximum transfer rate of 12Mbps, while ControlNet is only 5Mbps, standard Ethernet has a transfer rate of 10Mbps, with 100Mbps Fast Ethernet rapidly replacing it. With Gigabit Ethernet, the prospects of a 1000Mbps control network backbone become a reality.

In its Industrial Line, Hirschmann brings to Ethernet levels of determinism and resilience



comparable to that found in today's fieldbus. The momentum behind Ethernet is unstoppable and its domination in the control and automation industry is certain. Nothing can surpass Ethernet as the lowest cost implementation of a transparent control network. For more information on this subject please refer to the Hirschmann 'Distributed Communication Architecture' White Paper.

Hirschmann's DCA provides the means for Vendors to deliver a future-proof open Ethernet fieldbus family with all the resilience, reliability and deterministic benefits which in the past have only been found in proprietary legacy fieldbus solutions.

### Assessing the cost of downtime

Hirschmann research shows about 20 per cent of downtime problems are caused by network-related errors. Knowing the cost of system downtime to your business operations is key to running a successful business. It becomes even more important for Industrial Automation applications, where manufacturing depend on intelligent control system being continuously online.

To help you assess the cost of downtime to the business, Hirschmann has drawn on its experience in mission critical networks to provide you with a simple method for estimating your cost of downtime. The simple method of calculating the cost of downtime to look at the cost to the business due to the business-critical application not being available and then add the sum of the human cost of employees idled by the downtime. What this does not address is the consequential loss of that failure, this is much more difficult to quantify. Imagine for a moment that in a water treatment or chemical plant a network failure made it impossible to shut off a valve discharging untreated sewerage or residues into a local river. The cost of a cleanup operation, the negative PR and the environmental damage caused would result in a massive cost.

$$\text{Downtime Cost} = (\text{Business Loss} + \text{User cost}) \times \text{downtime}$$

$$(\text{cost/hour} + \text{cost/hour}) \times \text{hours}$$

### Minimising the Impact of downtime

Businesses are unable to eliminate downtime, but they can take steps to minimise its impact and reduce the risk of outage. There are two basic techniques to prevent unscheduled outages: fault avoidance and rapid recovery.

**Fault avoidance** prevents faults from occurring. It encompasses the right process and people and as well as the right technology. **Rapid recovery**, the second technique, minimises downtime when outages or system failures do occur. Redundant components can maintain operations in the event of a failure, while online repairs will allow the faulty component to be repaired without incurring further downtime.

## The need for an Architecture

By adopting a network architecture today Automation and Control companies will set out a statement of direction for Industrial Networking that customers can have confidence in. The architecture will define the strategic direction and desired state of customer's IA network in a timeframe of 3 years.

### Architecture for high availability Industrial networking

Before digging down too deep into Industrial Automation (IA) network design considerations it is first necessary to understand those high level statements that tie back into a customer's business goals. By so doing, the resilience strategy adopted will incorporate the customer's values and give recognition to their organisational culture.

Such statements might include:

- Only stable and proven and standards based technologies will be implemented in the next generation IA network.
- The next generation IA network must transparently, yet securely integrate with the Office Automation (OA) and enterprise network.
- Where business cost-justified, the next generation IA network must be optimised for high availability.
- The next generation IA network must provide multiple service quality levels to ensure that mission-critical processes are not impacted by lower-priority applications.

These simple statements show how an organisation wants to use networking over the long term. Consequences of these statements provide guidance for network planning and allow decisions to be made on specific technology adoption criteria.

Without such statements an organisation risks that its IA network will not be 'in sync' with its business and global market trends. These principles form the foundation of the network architecture.

### Key technology positions for the IA network

With the architecture principles adopted it becomes easier to make decisions on issues of technology.

Some key technology areas are listed below. This white paper covers the area of **High availability & resiliency**.

- Ethernet switching
- Quality of Service (QoS)
- Legacy fieldbus integration and migration
- Sensor bus integration
- High availability & resiliency**
- Security
- Long distance communication
- System and Network management
- Electro magnetic immunity
- Intrinsic safety systems

## High availability & resiliency requirements

### Use of high availability systems

The strength of an IA system is limited by the strength of its weakest link. If any one component is weak, regardless of whether it is hardware, the operating system, the network, controller or application— the whole system can collapse.

The need to optimise the network for maximum uptime forces us to look at high availability systems. To maintain and improve systems without disruption requires a strong combination of reliable technology, strong support and a flexible infrastructure.

High availability doesn't just happen, nor is it provided by hardware alone. It must be built, managed and measured. High availability in the network is built upon:

- ❑ Reliability/resiliency
- ❑ Manageability
- ❑ Supportability.

### Reliability/resiliency

Reliability/resiliency applies to the technology. It is designed into products, both hardware and software, and is available upon purchase of those products. For clarity, the reliability/resiliency of the network can be further segmented into:

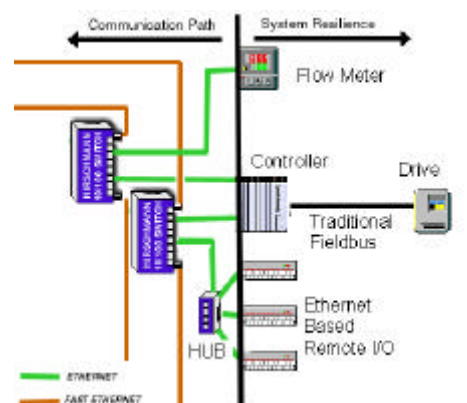
- ❑ **Communication path** reliability/resiliency
- ❑ **System** reliability/resiliency

Communication reliability/resiliency manifests itself in path redundancy. A network can be designed to detect a particular path is no longer able to pass data and will automatically switch to the backup path within 1 second. The different path redundancy techniques range from 100% proprietary to fully standards based solutions. The benefits of each are discussed later.

Today, 'the network' reaches into the very core of the attached devices, which could be anything from I/O blocks to Controllers. Network hardware connect internal system buses to the outside world, whilst software drivers provide the necessary logical paths for data to reach the application or process.

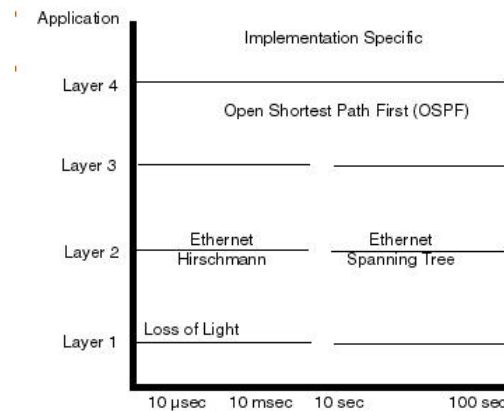
This closely coupled integration of system and network makes reliability/resiliency a central design consideration for Industrial Automation vendors. For high availability systems a single network interface, represents a Single Point of Failure (SPOF) that can bring a system to its knees. To counter this, a vendor will often offer a high availability systems that implements redundant network interfaces that detect path failure and activate a redundant interface as required.

With redundancy implemented, the next question is the speed a network failure can be detected by the attached system and then bypassed. This speed will determine whether or not the network interruption will impact the application.



In general terms, the speed of switch over can be correlated to the layer in the ISO protocol stack where the failure is initially flagged and bypassed.

Systems detecting 'loss of light' on a fibre optic link (ISO Layer 1) can typically detect and switch in 7-100 microseconds. Ethernet based Layer 2 implementation provides detect and switch anywhere from 4ms to 60 seconds. At Layer 3 (IP) and Layer 4 (TCP), detect and switch times are heavily dependent upon configured timers within the Internet (IP) and Transmission Control (TCP) protocols. Above the TCP/IP protocol the application or process itself could potentially manage this resiliency function, in which case detect and switch time would be by specific vendor design.



**Resiliency Features**

Like all other aspects of the Hirschmann DCA architecture, a base requirement is that network resiliency is a scalable function. It is the application needs that should dictate the level of resiliency a network should offer not the topology of a particular network technology. Resiliency costs money, therefore a scalable solution will start with no resiliency characteristics and scale up to a solution that can cope with multiple points of failure, with no disruption.

The DCA implements 4 levels of resiliency that meets the needs of most, if not all applications. Resiliency is not just a function of the network nodes and communication paths. As previously discussed, the network extends all the way into the attached system via the network interface and driver software, therefore the higher levels of resiliency are dependent upon the combined capabilities of the networked devices and the infrastructure.

Resiliency	Redundancy	Network Topology	Networked Devices
LEVEL 1	NONE	BUS, STAR SINGLE NODE	Single network i/f
LEVEL 2	COMMUNICATION PATH	SINGLE RING SINGLE NODE	Single network i/f
LEVEL 3	+ NODE or I/F FAILURE	SINGLE RING DUAL NODE	Dual network i/f
LEVEL 4	+ SECOND PATH BREAK	DUAL PATH/RING DUAL NODE	Dual network i/f

### Manageability

Manageability is one of the greatest concerns of a high availability system. System and Network management in the enterprise has become a scalable and powerful tool. Vendors are only slowly moving away from proprietary systems towards Open Systems based upon standards such as SNMP and Web based management, often Java based.

In the IA network today, management and monitoring of the manufacturing process is performed from the Human Machine Interface (HMI). The HMI is vendor specific, providing a management interface to the plant. In this environment a SNMP manager will be implemented as a separate and independent system which is not integrated into the HMI.

Networking products that have been specifically designed for industrial application will provide physical alarm indication (Open Circuit/Closed Circuit) when an alarm condition arises. The benefit of these products is that they will seamlessly integrate with the existing HMI and control network management applications.

As for the future, a convergence on SNMP and Web based management of controllers, instrumentation and the network will bring the HMI and network management platform together in a consolidated and integrated management system.

Also included under manageability are the proactive processes for performance management, configuration management and change management.

### Supportability

Supportability encompasses both preventive and reactive efforts.

Preventive efforts include:

- ❑ A high availability design
  - Topology (bus / star / ring) dual homing,
  - Redundancy (fibres / power / nodes / network interfaces),
  - Hot swap
  - Online diagnostic tools or diagnostic software to avert problems *before* they occur.
  - Reactive efforts to restore availability in the event of a failure, and get the system functioning again *before* solving the technical problem.
- ❑ System robustness

**System robustness** deals with the fit for purpose of a product in a particular environment. This may be intrinsic safety for environments with explosive potential. Alternatively the environment may be considered harsh with extreme high or low operating temperatures or excessive electromagnetic noise caused by large motors or conductors affecting the transmission characteristics of the communication path.

### An insurance policy

In many ways, high availability is like an insurance policy: the smaller the exposure to the risk of downtime and the greater the need for mission-critical uptime, the more the user is likely to invest to minimise the risk. Similar to buying insurance, the IA customer must be convinced of the risk and understand the cost of downtime before he agrees to buy it.

## Hirschmann high availability IA Ethernet solutions

All Hirschmann products are fully compliant to Ethernet standard 802.3. Where further standards apply which are essential for IA network design, for example in delivering QoS and security, Hirschmann adopt standards such as IEEE 802.1p&Q. Where implementation issues or standards fall short of IA networking requirements, Hirschmann lead the world in the development of value added features that make the *IndustrialLine* products unique.

These features include:

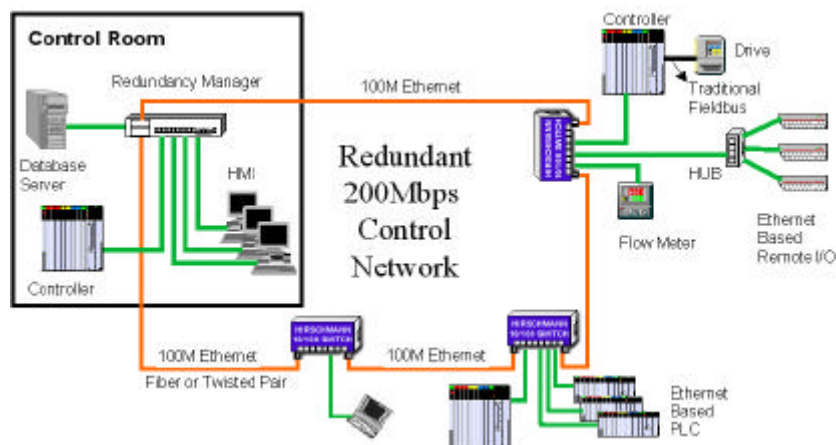
- ❑ Fast Path Recovery time -
  - 300msec maximum
- ❑ Multiple levels of Redundancy tailored to application requirements
- ❑ Dual 24VDC power inputs
- ❑ Single mode fibre for distances up to 40Km
- ❑ DIN Rail mounting
- ❑ Robust design for harsh conditions
- ❑ Extended operating temperature (0°C - 60°C) without fan

Path recovery times in less than one second are not achievable with 'Spanning Tree', the Ethernet 802.1d standard for layer 2 link recovery. Typically Spanning Tree will take in the order of 30 - 60 seconds to detect and bypass a communication path failure, whilst doing so all networked devices will be isolated. This solution is acceptable for applications within an Office Automation environment but not for a mission critical industrial solution.

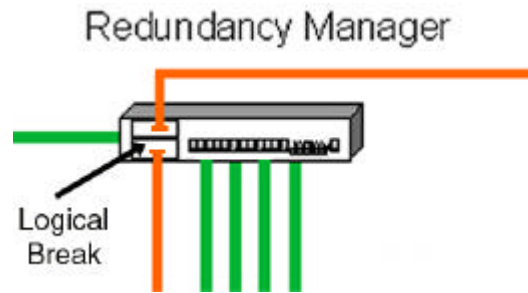
In recognition of this Hirschmann developed the 'Ethernet Ring'. Ring topologies are used to provide network path resilience in many traditional fieldbus systems. However, creating an Ethernet ring is a very new proposition. Ethernet is a bus architecture that uses broadcast messages to resolve addresses of connected devices. If a ring or more importantly a loop is created any Ethernet broadcast frame will be sent around the loop, eventually bringing the network to its knees.

### So when is a ring not a loop?

Hirschmann have developed the 'Redundancy Manager', a Ethernet switch that has added capabilities that overcomes the architectural limitation of Ethernet described above.

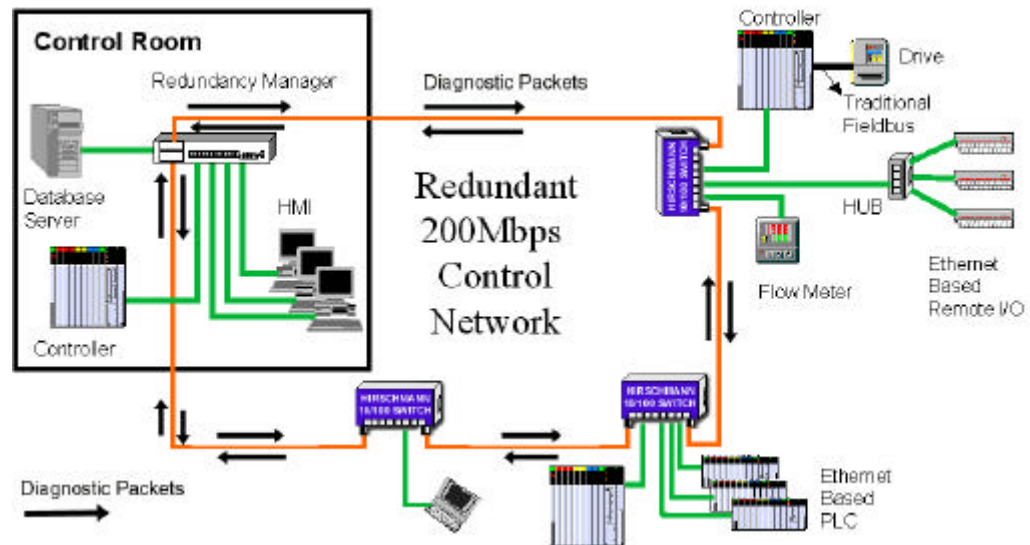


In addition to performing all the standard Ethernet switching functions, the Redundancy Manager allows a physical 200Mbps ring to be created by terminating both ends of the traditional Ethernet Bus (Fibre or Copper).

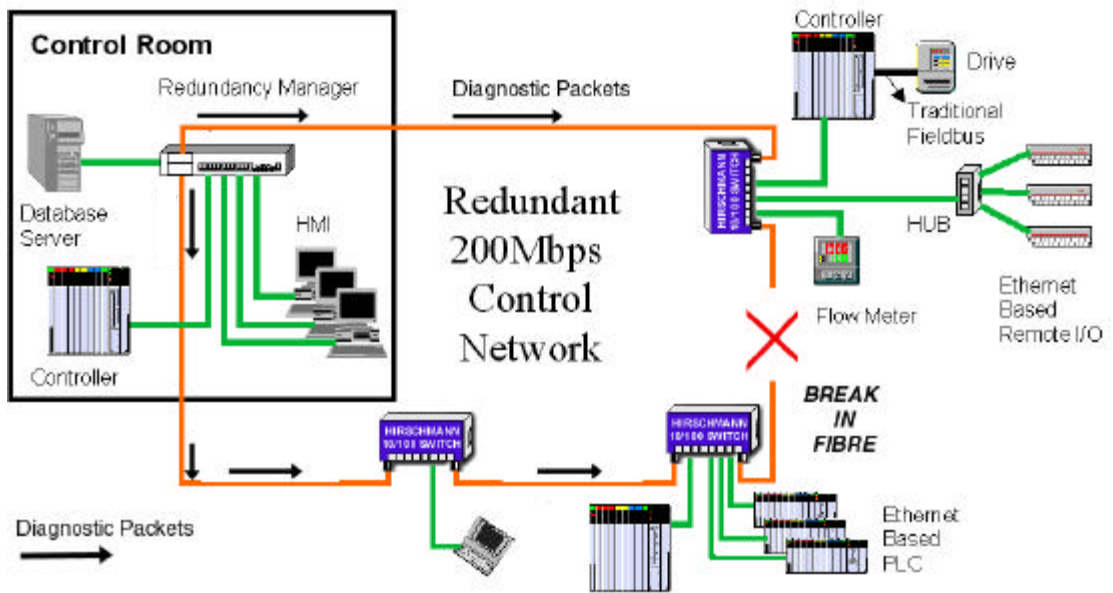


**Although the Ethernet bus is physically terminated the Redundancy Manager logically breaks them.** The result of this break is broadcast frames will not experience the implications of a loop, in fact the Redundancy Manager is effectively transparent to the networks operation, even if the Redundancy Manager was taken out of the ring altogether there would be no impact on the networks ability to pass data.

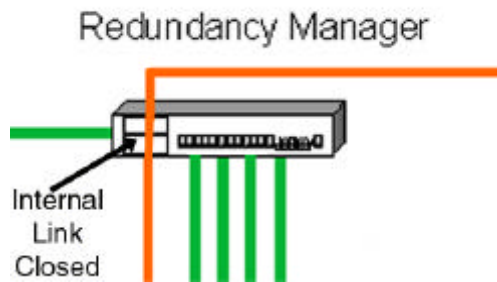
Logically there are two sides to the Redundancy Manager, each is continuously transmitting and receiving real time diagnostic messages to the other around the ring. As the messages are sent they are given both identifier and a standard 802.1p/Q priority. The identifier allows the distant receiving port to 'count' them in, the high priority allows the frames to take a deterministic path through any 802.1p/Q compliant switches (up to 50) in the ring. The result is a real time report on the actual state of the network at any instant.



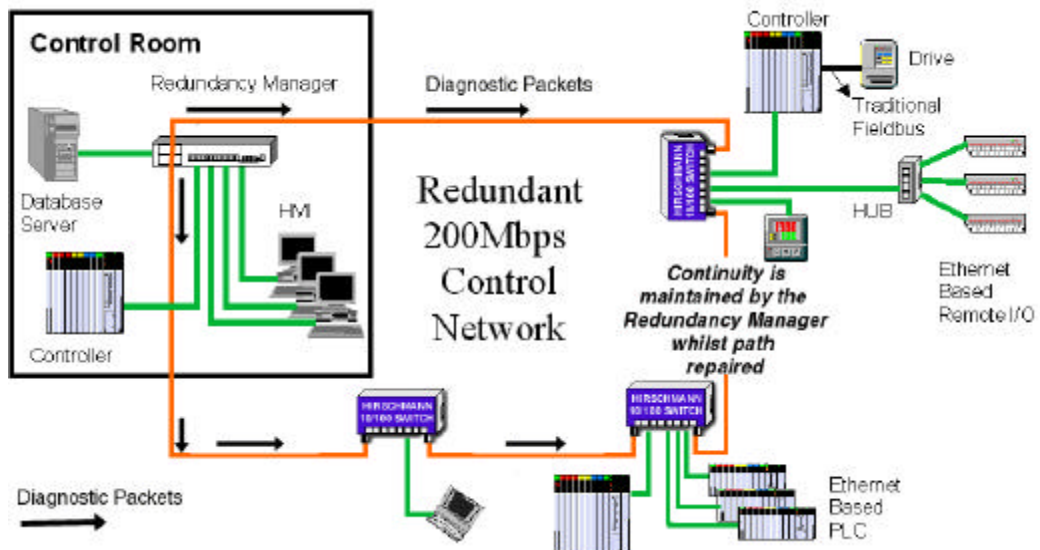
In the case of a failure in the ring i.e. either a node or a link has been lost, the Redundancy Manager will still be transmitting on both ring ports, however, because of the failure in the network the diagnostic messages will not reach all around the ring. Both sides of the Redundancy Manager are now able to interpret this loss of diagnostic data as a network failure.



When the network failure is detected, the Redundancy Manager connects the two interfaces internally. This will return the network to full operational status. The detection and network healing process will be complete in between 20 and 300msec, depending on the size of the ring.



The Hirschmann 'Ethernet Ring' solution is orders of magnitude faster at link recovery than 802.1d Spanning Tree which takes up to 60 seconds for path recovering. Monitoring of the data stream, it does not only protect one link between two switches but also the whole ring. The reduced cost of a ring infrastructure compared to dual buses makes the 'Ethernet Ring' solution economical viable. Clear and efficient redundancy structures also provide the flexibility to expand or extend the network without impacting network traffic.



## Building high availability Industrial networks with Ethernet

Traditionally the choice of resilience attributes in an IA network has been dictated by the network topology. The choice of topology is often dictated by the vendor, followed by influencing factors such as long distances, environmental conditions, cost, performance etc. It has not, therefore, always been possible to implement resilient networking practises by design, more often by what is available within a particular network topology that was chosen for altogether different reasons.

Using Ethernet in the IA network fundamentally changes this approach. Ethernet is not vendor specific, it can drive information over extremely long distances using fibre optics, which are immune to electromagnetic noise. Ethernet is cost-effective for 95% of Industrial applications and it offers levels of performance 100 x greater than its nearest traditional rival. Ethernet networks can be designed to meet the application or process requirements for resilience without compromising any of the design considerations mentioned before.

The decision to design resilience into a network from the beginning has additional benefits, such as flexibility to expand and extend the network without causing downtime and general piece of mind whilst working close to cabling routes.

### Evaluation criteria

Using Ethernet fieldbus technology has the added benefit of delivering scalable resilience features. Scalability enables cost-effective IA networks to be built that fully meet the high availability & resilience requirements of the specific application.

With such flexibility comes choice. Pre-defined evaluation criteria can be used to aid the network design process by applying standard rules that, if followed, will result in the availability levels required.

Often, evaluation criteria will be specific to a vendors target market, but typically they will include:

- Size of device population affected by an outage
- Mission-criticality of the manufacturing process
- Special site considerations
- High availability vendor product features

**Network design guidelines for High Availability IA Networks**

Based upon these criteria the following rules allow IA network templates to be created that will simplify and standardise high availability network design.

*Integration with the Enterprise*

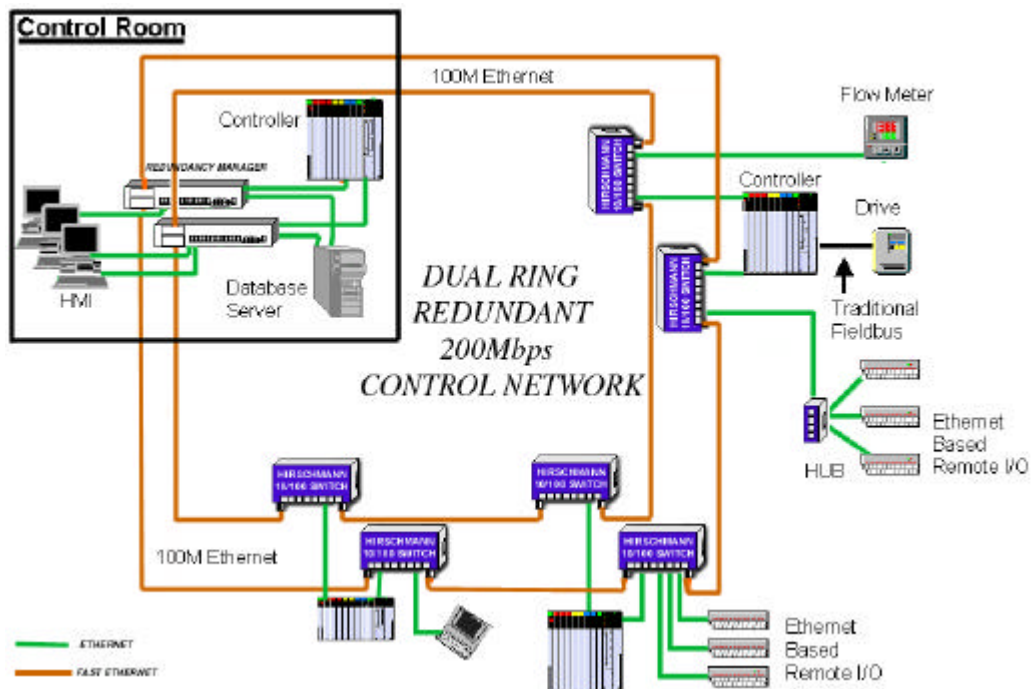
- Information level LAN switches should be dual connected to the enterprise backbone with resilient routing.

*Media Selection*

- **IF** environmental constraints (Electrical Isolation, Noise Immunity, Security) exist,  
**THEN** use Fibre Optics in the communication path.
- OTHERWISE IF** distances are <100m **AND** there are no environmental constraints,  
**THEN** use Shielded Category 5 copper wiring in the communication path,
- OTHERWISE IF** distances are >2Km  
**THEN** use single mode fibre in the communication path,  
**OTHERWISE** use multi-mode fibre in the communication path.

*Topology Selection*

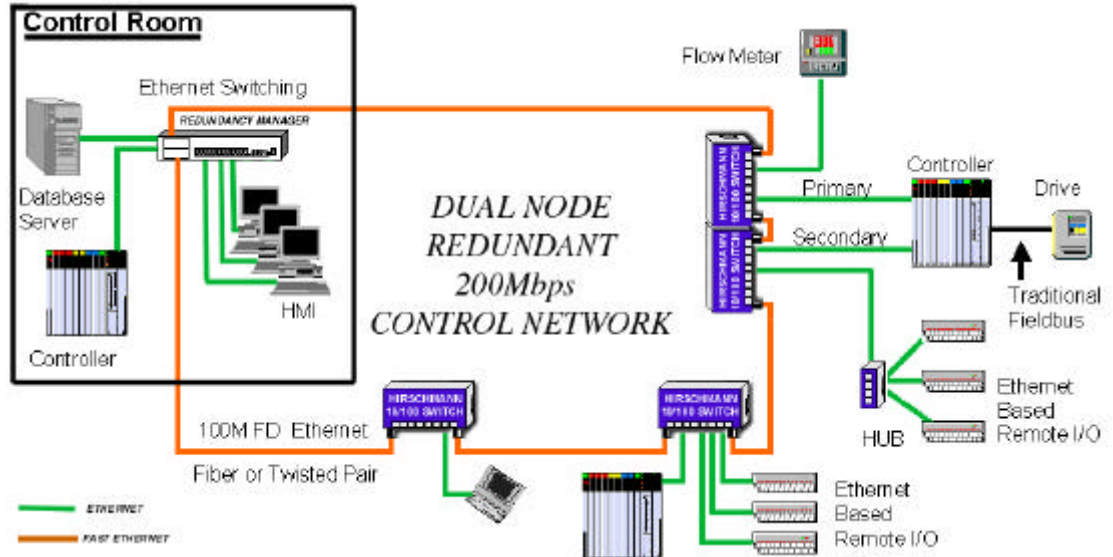
- **IF** an application requires 100% availability even after two points of failure.  
**THEN** use a dual ring with dual homing of controllers and critical devices.



**HIRSCHMANN RESILIENCE LEVEL 4**

**OTHERWISE IF** an application requires 100% availability with no single point of failure.

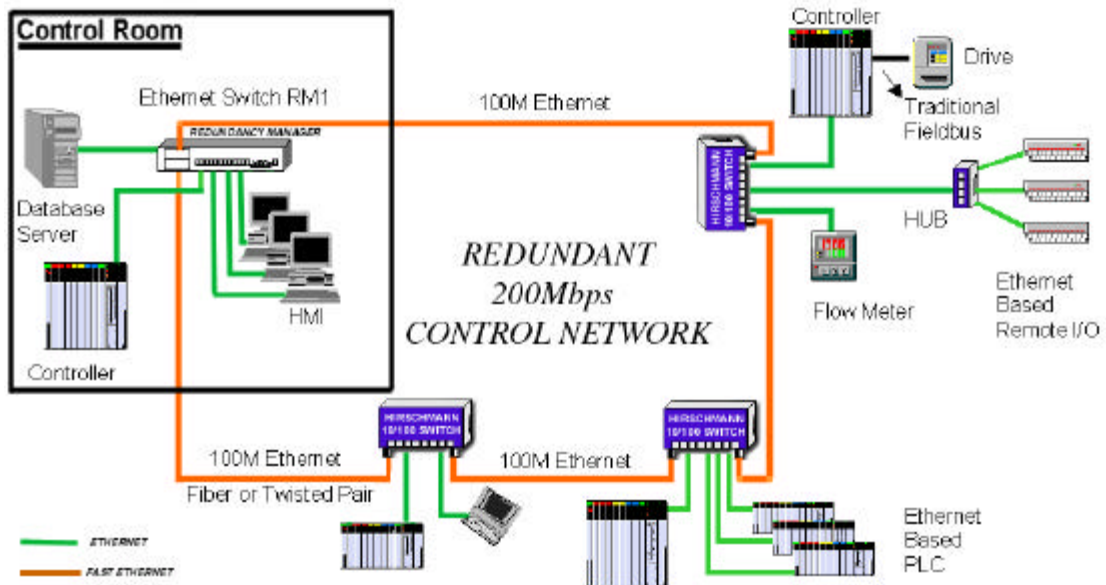
**THEN** use a single fibre ring with dual nodes and dual homing of controllers and critical devices.



**HIRSCHMANN RESILIENCE LEVEL 3**

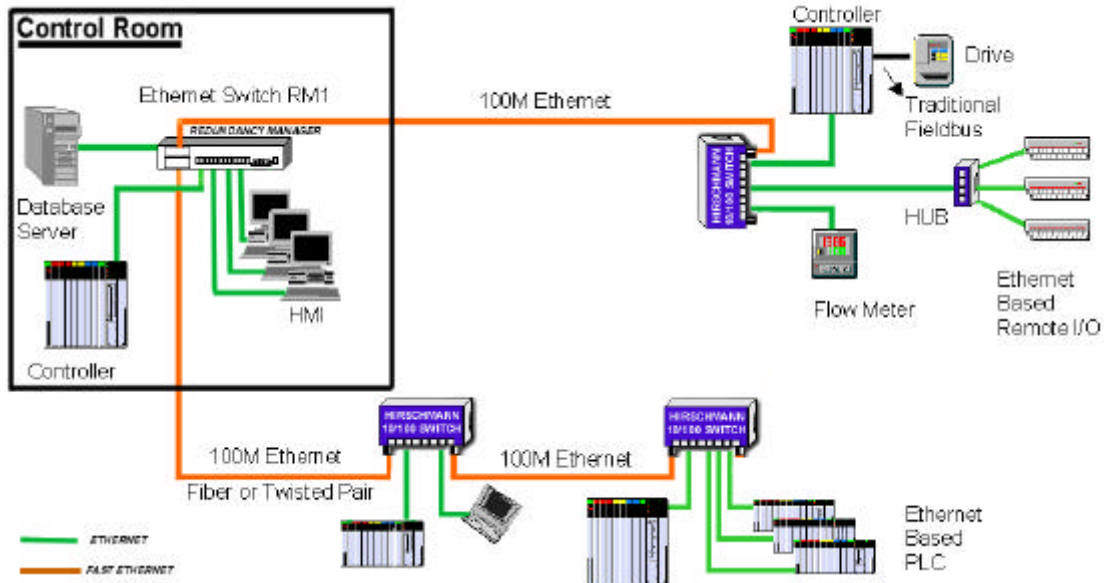
**OTHERWISE IF** an application requires a backup communication path

**THEN** use a single ring with single homing of controllers and devices



**HIRSCHMANN RESILIENCE LEVEL 2**

- ❑ **OTHERWISE** provide no communication path resiliency



**HIRSCHMANN RESILIENCE LEVEL 1**

***Device Attachment***

- ❑ **IF** the equipment supports Controllers or critical devices.  
  - THEN** implement System redundancy options that will ensure 100% uptime,
  - AND** provide full-duplex switched Ethernet network connection.
- OTHERWISE IF** equipment supports multiple HMI.  
  - THEN** protect against power failures and establish spares.
  - AND** provide Ethernet network connection.
- OTHERWISE** provide spares.

***Power Supply***

- ❑ **IF** the equipment supports business critical systems **OR** multiple devices,  
  - THEN** implement power supply redundancy
- OTHERWISE** provide spares.

## Conclusion

There is no doubt that Ethernet will become the next generation fieldbus that will provide the seamless communication between the worlds of Office and Industrial Automation, the remaining issues today are purely based upon implementation and price. Hirschmann believe that with it's Distributed Communication Architecture – DCA, they are in the unique position to work with automation vendors in creating a complete range of competitively priced, Ethernet based Industrial Networking products that either meet or exceed the needs of the market today. Further, DCA maps out a blueprint for future developments that will ensure Hirschmann partners always have access to market leading, Industrial strength solutions.

The resiliency examples described within this document show how Hirschmann's Industrial Ethernet products are being used to build scalable, highly resilient Ethernet fieldbus networks that are simple to design, build, implement and manage.