Best Practice For Network Design

Mark Cooksley.
Hirschmann Automation and Control GmbH
Contents

• Case Studies
• General Aims and Requirements
• Structured Cabling
• Topology and Redundancy
• VLANs
• Multicast Control
• Device Replacement
• Security
• Network Management
• Conclusion
LISTEN.
THINK.
SOLVE™

Case Studies

Mark Cooksley.
Hirschmann Automation and Control GmbH
Automotive Sector
Military Sector
LISTEN. THINK. SOLVE.™

General Aims & Requirements

Mark Cooksley.
Hirschmann Automation and Control GmbH

Copyright © 2007 Hirschmann Automation and Control GmbH.
Investing in operational safety pays (1)

Network failure can be expensive!

Result of a study by Infonetics, USA, among 100 of the top 1000 US companies:

- Average down days: 24 days per year
- Average failure duration: 4.86 hours per year
- Average failure cost: 32,000 $ per hour

Failure cost according to an ICL survey:

- 34 % below 1,000 $
- 34 % 1,000 - 10,000 $
- 20 % 10,000 - 100,000 $
- 12 % above 100,000 $

Network failures cost major corporations 2% to 16% of their sales revenue

(Infonetics Research 2005)
Around two thirds of all failures are caused by faults in network components.

Source: Datacom, Network Management Special
Total Cost of Ownership of a network over 5 years

Source: Gartner Group
Requirements of a modern industrial network

- Robust with high availability
- High performance
- Future proof
- Security policy
- Industrial-grade products
- Compliance with standards
Requirements of a modern industrial network

- Real-time capability
- Expandability during operation
- Training concept
- Support concept
- User-friendly commissioning and operation
- Management solution
Structured Cabling

Mark Cooksley. Hirschmann Automation and Control GmbH
Advantages of Structured Cabling

- Simplifies design
- Large choice of components
- Compatibility
- Increased availability
- Ease of maintenance
Standards

ISO/IEC 11801  EN50173  ANSI/TIA/EIA 568-B
Revised DIN EN 50173

EN50173-1  Generic Cabling System General Requirements (Basics)

EN50173-2  Generic Cabling System Office Premises

EN50173-3  Generic Cabling System Industrial Premises

EN50173-4 / 5 / 6 / 7  Residential / Data Centres / Hospitals / Airport Premises
Terminology

• CD = Campus Distributor
• BD = Building Distributor
• FD = Floor Distributor
• MD = Machine Distributor (new: Intermediate Distributor (ID))
• TO = Telecommunication Outlet
• CP = Consolidation Point
Cabling Structure Office ↔ Industry

Layer 1

Layer 2

(Layer 3)

Layer 4

Primary cabling

Secondary cabling

Tertiary cabling

Office building
**Physical Cabling Structure**

**Office:**
```
Primary: CD  Secondary: BD  Tertiary: FD
```
- **FO (1500m)**: E9...10/125, G50(62,5)/125
- **FO (500m)**: E9...10/125, G50(62,5)/125
- **TP (90m + 2 * 5m)**: FO, G50(62,5)/125

**Industry (3 or 4 layers):**
```
```
- **FO (1500m)**: E9...10/125, G50(62,5)/125
- **FO (500m)**: E9..10/125 or G50(62,5)/125
- **TP (90m + 2 * 5m)**: FO, G50(62,5)/125
- **Bus cable**: TP, HCS/POF

**Transmission media**
Available Bandwidth

- Office networks
  - Overbooking
  - Traditional estimation

- Industrial networks
  - Non-blocking
  - Different approaches
Industrial Bandwidth Availability

- Industrial network:
  - No overbooking of the network
  - Non-blocking from edge to core
Calculating Bandwidth Requirements

Example: 100 pps
100Mb/s link

Number of bytes per packet 64
Add 20 for header and Inter-Frame Gap 84
Multiply by 8 for bits 672
Multiply by number of packets per second 67,200
Calculate % of line speed 0.067%

A 100Mb/s link can support 150,000 (148,809) 64 byte pps
Topology and Redundancy

Mark Cooksley.
Hirschmann Automation and Control GmbH
Star / Bus Topology
Mesh Topology
Recovery Mechanisms

- HIPER Ring
  - De facto standard (Rockwell, Siemens, Schneider, Mitsubishi, ABB, Emerson, Invensys)
  - Ring topology – simple wiring structure
  - Very fast recovery time ~ 50ms

Inactive link, activated when another fails
Recovery Mechanisms

- Spanning Tree and Rapid Spanning Tree Protocol
  - Standardised – IEEE802.1w and IEEE802.1d
  - Mesh topology – more complex wiring

Some links deactivated so as not to cause loop
VLANs

Definition of a VLAN:

• Connection of data terminal equipment to closed, logical LANs within a physical infrastructure

Why use VLANs?

• Broadcast limitation
• Security
Physical LAN
Virtual LANs
Multiple VLANs per Switch
Management VLAN
VLAN Types

- VLANs layer 1: port based (IEEE 802.1Q)
- VLANs layer 2: MAC address based
- VLANs layer 3: network address based or protocol based (IEEE 802.1v)
- VLANs layer 4-7: application based → future
VLAN Rules

• Ingress Rules
  – Which VLAN ID should a frame be given?

• Egress Rules
  – Which VLAN IDs should be allowed out of a port?
  – Should the VLAN Tag be removed?
VLANs: Tagging

<table>
<thead>
<tr>
<th>Ingress Station</th>
<th>Port</th>
<th>PVID</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>D</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Uplink</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Static/Current (Egress) VID</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>M</td>
</tr>
<tr>
<td>2</td>
<td>U U U M</td>
</tr>
<tr>
<td>3</td>
<td>U U M</td>
</tr>
<tr>
<td>4</td>
<td>U U U U M</td>
</tr>
</tbody>
</table>

Copyright © 2007 Hirschmann Automation and Control GmbH. All rights reserved.
Multicast Control

Mark Cooksley.
Hirschmann Automation and Control GmbH
IPv4 Address Types

• Unicast - transmitting a message to a single destination node

• Broadcast - transmitting a message to all nodes in a subnetwork

• Multicast - transmitting a message to a group of nodes that are not necessarily in the same subnetwork.
Why Use Multicasts?

• Multicasting delivers traffic to multiple receivers without adding any additional burden on the source

• Multicasting is a bandwidth-conserving technology
Where Are Multicasts Used?

• General
  – Video Conferencing
  – Video Surveillance
  – Distance Learning
  – Software Distribution
  – Ticker Tape

• Industrial
  – Producer / Consumer
  – Publisher / Subscriber
And the issue is?

- Ethernet was not designed to support multicasts
- Ethernet processes multicasts like broadcasts
  - First bit
  - Learned Address Table
- Additional protocols are required to correctly handle multicasts
The multicast problem

Ethernet A:
Data_A = 15%  Multicast_A = 2%

Ethernet B:
Data_B = 35%  Multicast_B = 4%

Ethernet C:
Data_C = 45%  Multicast_C = 5%

Ethernet D:
Data_D = 25%  Multicast_D = 3%

Multicast load:
→ 14 %
Overcoming the multicast problem

• Ensure multicasts are only sent to relevant ports

• Two methods:
  • IGMP
    • Internet Group Management Protocol
    • Layer 3 – designed for routers, so controls multicasts between routers
  • GMRP
    • GARP (Generic Attribute Registration Protocol) Multicast Registration Protocol
    • Layer 2 – designed for switches, so controls multicasts on Ethernet
EtherNet/IP Adaptation of CIP Specification – CI & ODVA
Volume 2 Chapter 9

All EtherNet/IP devices shall at a minimum support:

- Internet Protocol (IP version 4) (RFC 791)
- User Datagram Protocol (UDP) (RFC 768)
- Transmission Control Protocol (TCP) (RFC 793)
- Address Resolution Protocol (ARP) (RFC 826)
- Internet Control Messaging Protocol (ICMP) (RFC 792)
- Internet Group Management Protocol (IGMP) (RFC 1112 & 2236)
- IEEE 802.3 (Ethernet) as defined in RFC 894
**IGMP**

- End devices register with local router ("Querier") that they wish to receive multicasts from multicast source
- Router directs multicasts to end device
- Result – broadcasts on Ethernet network
IGMP Snooping

- Switches eavesdrop (snoop) on the IGMP conversation between end device and querier
- Switches are able to learn which end devices want the multicast data
IGMP Limitations

- IGMP Snooping requires a Querier
  - Some switches can act as a Querier
  - Multiple queriers can exist

- In some cases, multicasts can still “flood” onto other parts of the network

- For correct configuration of IGMP queriers and snooping download the Hirschmann white paper
  - “Hirschmann Interoperability to Industrial/Process and Ethernet/IP environments”
Five Ways To Solve The Flooding Issue

• Producer registers for its own multicast stream
• Use IGMP v1 and activate multiple Queriers
• Use Static Querier ports
• Manually enter multicast addresses in the Learned Address Table
• Redirect unregistered multicast streams
Device Replacement

Mark Cooksley
Hirschmann Automation and Control GmbH
Device Replacement

• Rapid rectification of failures required
• The “Midnight Maintenance Man”
• Device replacement techniques
  – Standardized / Proprietary
  – Exchangeable memory media
  – Topology-dependent configuration
Removable Memory Media

• Benefits
  – No technical knowledge required to replace a switch
  – No possibility for error
DHCP Option 82

• Benefits
  – No technical knowledge required
  – Minimised hardware costs
  – Manufacturer-independent
Address Conflict Detection

- Duplicate IP addresses destroy communication
- Every device should check its address before use

```
192.168.0.54
```

```
192.168.0.54
```
EtherNet/IP Default Factory Settings

• Order Code “E”
• Settings:
  – EtherNet/IP protocol: Enabled
  – IGMP Snooping: Enabled
  – IGMP Querier: Enabled
  – Unknown multicasts: Send to Query ports
  – DHCP: Enabled
  – Address Conflict Detection: Enabled
  – System Name: Product name + 3 bytes MAC address

• Benefits
  – Plug & Play EtherNet/IP solution
  – No technical knowledge required
Security

Mark Cooksley.
Hirschmann Automation and Control GmbH
“IT personnel in particular must be made aware that inadvertent intrusions resulting from system maintenance and housekeeping, network upgrades, or broadcast storms can disrupt the control system”

– EtherNet/IP Media Planning and Installation Manual

“Intrusions into the control network from other networks could cause processing delays and loss of control”

– EtherNet/IP Media Planning and Installation Manual
What percentage of network security attacks do you believe originate from inside or outside of your company?

- **83%** inside
- **13%** outside
- **4%** don't know
Firewall Techniques

- Hard perimeter
- Defence in depth
Stateful Inspection

Insecure → Secure

Ping → Reply

Reply → Ping

X

Ping → X → Reply
Packet Filtering

- Accept or discard data based on IP address or protocol
Management

LISTEN.
THINK.
SOLVE™

Mark Cooksley.
Hirschmann Automation and Control GmbH
ISO Network Management Classification

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Accounting Management</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration**

**Supervision**
SNMP Management

• The standard for Ethernet switch management
Profile Communication Structure

- PC
- PanelView
- CompactLogix
- Flex I/O
- CIP Switch
RSLogix5000 v16 with Add-On Instructions
PanelView Screens Designed By Rockwell
Available Resources

- Sample files
  - http://samplecode.rockwellautomation.com
  - Catalog Number 9701

- Author
  - Vivek Hajarnavis
Conclusion

- A simple and clear design, following international cabling standards, will result in a robust network

- Segment office, production, and test environments (firewall, router, VLANs)

- Create and test a device replacement concept

- Design in security right from the start

- Network management is critical for availability