High Availability Fieldbus Networks in Hazardous Areas

Phil Saward
MTL Instruments

Automation 2011, Mumbai
21st September 2011
In this presentation...

- Foundation Fieldbus ‘physical layer’ failure modes
- Keys to achieving high network availability
- Some simple reliability theory!
- Does redundancy really improve availability?
- Redundancy as applied to practical FF networks
What could possibly go wrong?

Control Room:
- Host H1 Card
- Power Supply / Conditioner

Field:
- Device Coupler
Well, there are a few things…

- Short-circuit or open-circuit in trunk cable causes loss of whole segment.

  - Control Room
  - Power Supply / Conditioner

- H1 card: Single point of failure

- FF power supply: Single point of failure

- Open-circuit in spur causes loss of single device

- Short-circuit in spur causes loss of single device

- Wiring hub: Single point of failure

- Single point of failure
Spur short-circuit protection

Current limit set at approx 40-60mA, depending on type of Device Coupler

Some types turn off spur completely until short-circuit is removed

Potential short-circuit
Keys to achieving High Availability

- Avoid unnecessary complexity!
- Choose inherently reliable apparatus
  - Long “Mean Time Between Failures”
- Repair faults as quickly as possible
  - Short “Mean Time to Repair”
- Use redundancy, where available
- Design systems to be inherently resilient to faults
  - Fall back to reduced accuracy/functionality with loss of PV
  - Partition critical processes, eg separate fieldbus segments
Is specifying redundancy a ‘hang-over’ from early days of electronics?
- Electrolytic capacitors with short life-times?
- Failure of semiconductors at high operating temperatures?

Most operators still elect to use redundancy for critical applications
- “Peace of mind”

Financial impact of down-time vs. cost of redundancy
Simple availability theory

\[ \text{Availability, } \%, = 100 \times \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \]

- MTTF = Mean Time to Failure = “Up Time”
- MTTR = Mean Time to Repair = “Down Time”

\[ \text{Unavailability, } \%, = 100 - \text{Availability} \]
A simple example…

- I have a car
- It breaks down on average once every 3 years
  - MTTF = 26,280 hours
- Repair shop takes on average 3 days to fix it
  - MTTR = 72 hours

\[
\text{Availability, } \% = 100 \times \frac{26,280}{26,280 + 72} = 99.73\%
\]

\[
\text{Unavailability, } \% = 100 - \text{Availability} = 0.27\%
\]

\[
\text{Unavailability} = 0.0027 \times 365 = 1 \text{ day per year}
\]
Does Redundancy really improve availability?

- What if I have a second car with same (un)reliability?
- A simple redundant scheme!

\[
Unavailability_{\text{new}} = Unavailability_1 \times Unavailability_2
\]

\[
= 0.27\% \times 0.27\% = 0.00075\%
\]

\[
Unavailability = 0.0000075 \times 365 \text{ days}
\]

\[
= 4 \text{ minutes per year}
\]
Random and Systematic faults

- Calculated MTTF figures
  - Based on component reliability databases
  - Predict *random* failures

- However, experience suggests....
  - Some (most?) equipment failures are due to *systematic* faults
    - Faulty component batches
    - Manufacturing errors
    - Inherent design faults

- Systematic faults will affect identical items of apparatus
  - Both channels in a redundant system!
  - *Complete failure could occur, but only if both channels fail within MTTR period*
In our example, 4 minutes per year unavailability is absurdly low!

Common cause failures will reduce the availability of redundant systems and are often overlooked.

Common cause failures are difficult to quantify, but typically 5% of single-channel failure rate.

Common-cause failures in our car example:
Diagnostics in redundant systems

- Need periodic checking and annunciation of faults for standby channels in a redundant system
- Interval between checks influences the availability
- Diagnostic information must be unambiguous

- In our example….
  - Battery of standby car may have gone flat
Catastrophic failure of a ‘redundant’ system

8th January 1989: East Midlands Airport, nr. Leicester, UK

Left-side engine failed

Flight crew mis-interpreted cockpit diagnostic information and shut down right-side engine

Attempted landing without power & crashed 500m short of runway

Highlights need for accurate failure indication in redundant systems
Fix it Quick!

- **Time to Repair** is crucial and wholly in the hands of the user, but redundancy helps!

<table>
<thead>
<tr>
<th>Fieldbus Barrier type</th>
<th>Mean Time to Repair (MTTR)</th>
<th>Availability, %</th>
<th>Predicted unavailability, minutes per year</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-spur Simplex</td>
<td>8 hours</td>
<td>99.99276</td>
<td>38</td>
</tr>
<tr>
<td>6-spur Redundant</td>
<td></td>
<td>99.99905</td>
<td>5</td>
</tr>
</tbody>
</table>

- **Redundant systems can tolerate longer MTTR**

| 6-spur Simplex             | 72 hours                   | 99.93486        | 342                                       |
| 6-spur Redundant           |                            | 99.99626        | 20                                        |
Conclusions so far...

- Practical redundancy schemes are imperfect but do offer a significant improvement in network availability
  - Most random and many systematic faults are captured
  - Periodic monitoring of standby channel is important in active/standby schemes
  - Common cause failures reduce the theoretical maximum availability
  - Repair time is important, especially in simplex systems

- In our example, unavailability contribution due to common cause failures would be 70 minutes per year (average)
Alternative redundancy schemes

- 1+1 redundancy typically assumed
- N+1 redundancy can offer improvements in hardware ‘footprint’ and installation cost
N+1 redundancy – simplex power at 250mA

Module A
powers 4 segments
at 250mA
N+1 redundancy – redundant power at 250mA

Module A
powers 4 segments at 250mA

Module B
powers 4 segments at 500mA or provides redundancy at 250mA
N+1 redundancy – redundant power at 500mA

Module A
powers 4 segments at 250mA

Module B
powers 4 segments at 500mA or provides redundancy at 250mA

Module C
Provides redundancy for 4 segments at 500mA
N+1 redundancy: complete system

6 modules provide redundant power at 500mA for 8 segments
Fieldbus Barrier redundancy

- Fieldbus Barriers (Isolated Segment Couplers) are widely adopted for connection to IS-certified fieldbus instruments in Zone 1 hazardous areas in FOUNDATION™ Fieldbus networks.
- In conventional installations the complex, field-mounted barrier module is not protected by redundancy.
- Introduction of redundant Fieldbus Barriers allows users to protect critical segments.
Typical Fieldbus Barrier application

- Fieldbus control system (DCS)
- Increased safety (Ex e) ‘High Energy’ trunks
- 24V dc Bulk power input
- Redundant Fieldbus Power Supply

CONTROL ROOM

Simplex Fieldbus Barrier

- Intrinsically Safe spurs

FIELD Zone 1

Non-critical fieldbus segment

Critical fieldbus segment

Intrinsically safe FISCO or Entity Fieldbus Devices
Fieldbus Intrinsically Safe Concept (FISCO)

- Fieldbus control system (DCS)
- 24Vdc Bulk power input
- Redundant 4-segment FISCO power supply
- Intrinsically Safe trunk and spurs (1 segment of 4)
- FIELD Zone 1 IIB Hazardous area
- Intrinsically Safe Field wiring hub
- Intrinsically safe FISCO Fieldbus devices
FISCO Power Supply Redundancy

**Scheme includes Monitoring of Standby FISCO Power Supply and Supply Arbitration Module**
## Availability analysis

<table>
<thead>
<tr>
<th>Ex technique</th>
<th>System Component</th>
<th>Availability</th>
<th>Unavailability per year, minutes</th>
<th>Total system unavailability per year, minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FISCO</td>
<td>910x-22 FISCO power supply (redundant)</td>
<td>99.99972%</td>
<td>1.5</td>
<td>3.8</td>
</tr>
<tr>
<td></td>
<td>F259 Intrinsically Safe Megablock (10-spur)</td>
<td>99.99956%</td>
<td>2.3</td>
<td></td>
</tr>
<tr>
<td>High Energy Trunk (Fieldbus Barrier)</td>
<td>Typical Redundant FF power supply</td>
<td>99.999%</td>
<td>1.0 (approx)</td>
<td>11.0</td>
</tr>
<tr>
<td></td>
<td>Typical Fieldbus Barrier</td>
<td>99.998%</td>
<td>10.0 (approx)</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**

1. Calculated figures should be taken as guidance only.
2. Power supply availability figures are per segment.
3. Ambient operating temperature is assumed to be 20°C for the power supplies (conditioned control room environment) and 45°C for the Megablock (field environment).
4. Mean Time to Repair (MTTR) assumed as 8 hours in all cases.
5. Megablock availability figure calculated according to the formula: Availability, % = 100*MTTF/(MTTF+MTTR).
6. Unavailability is 1-Availability, where 1 year = 525,600 minutes.
In summary…

- Hardware redundancy can play an important role in maintaining high availability in Foundation Fieldbus networks.
- New product enhancements extend the scope and capability of redundancy.
- An intelligent approach to reliable networks should consider external factors, not only the physical hardware.