Most system designers and project managers look at the project procurement, installation and deployment costs when they price a project.

However, the costs of an automation system spread over the life cycle of the plant and should include maintenance, fault-finding and health-checking.

Perhaps most important is the cost in terms of loss of production should faults develop during the lifetime of the plant. Spending a little more at procurement time can repay many times over.

Good fault tolerant design need not be more expensive. Sometimes fault tolerance can be achieved with just a little thought at no additional cost.
Life cycle costs

- The procurement, installation and commissioning costs are only incurred at the start of the project.

- Costs from device failures increase as equipment gets older.

When system overhaul is undertaken this can partially reset the increasing cost of failures.
Control system design

- Control system design normally proceeds by building on the experience obtained from previous designs.
  - But, designs which are based on badly designed systems will be bad!
  - Only by using experience from operations and maintenance staff can we develop good system designs.
  - In my experience it is rare for such feedback mechanisms to be present. Particularly when design is carried out by sub-contractors.
- Designers need to know about mistakes that have been made in the past.
  - Feedback from operations and maintenance is essential.

System costs

- Maximising plant availability is critical in reducing the total costs of the system. It is essential that the System Designer understands:
  - That minimising plant down time when faults inevitably occur (i.e. maximising plant availability) is a key requirement.
  - The impact of the network layout on plant reliability.
  - That the incorporation of network health checking and fault finding facilities are essential.
  - How to appropriately use features such as redundancy and network monitoring and rapid fault location and repair to improve plant availability.
The parts of a control system will fail whilst in service.

The consequences of failures are often predictable, but the failures themselves are unpredictable.

The design of a reliable control system is not simple.

... and should be accompanied by analysis of how parts fail and of the consequences of these failures.

Cost of failures

Minimising the failure footprint

A good network design will minimise the effect on production when inevitable failures occur.

We can speak of minimising the “failure footprint”.

There are three basic ways to minimise the impact of faults:

1. Make failures less likely – Minimise the Fault Frequency.
2. Restrict the Fault Effect when failures inevitably occur.
3. Minimise the Fault Duration – Provide for rapid fault location and repair.
Minimising the failure footprint

1. How can we minimise **Fault Frequency**?

- Understand and implement the design and installation rules.
- Improve reliability - use good quality well tested (certified) and reliable devices, connectors and network components.
- Use manufacturers who carry out burn-in testing on devices.
- For PROFIBUS use the lowest possible bit rate that gives the required performance.

2. How can we minimise the **Fault Effect**?

- Analyse the effects of failures on plant operation.
- Use well thought out network layout and design.
- Think about:
  - Using separate networks or different masters (distributed control),
  - Using different segments for different parts of the process,
  - Dealing with common cause failures.
3. How can we minimise the *Fault Duration*?

- Provide facilities in the design for rapid fault diagnosis and fault location.
- Provide in the design for device hot swapping without reconfiguration.
- Use designs that allow for a quick fix.
- Provide redundancy when appropriate. Needs to be well thought out!
- Use standardised, vendor independent solutions rather than being locked into manufacturer specific solutions.

---

Minimising fault impact in design

- Use pluggable devices that can be removed/replaced without impinging on network operation.
- Use appropriate network layout and segmentation so that physical layer faults allow critical plant operation to continue in the event of failure or device replacement.
- Provide for rapid troubleshooting and simple fault isolation.
- For PROFIBUS systems use:
  - Connector systems and layouts that do not break the bus or loose termination when disconnected.
  - Termination solutions that allow devices to be removed or replaced.
- Use appropriate solutions for redundancy.
Reliability and availability

Reliability is a measure of how a component, assembly or system will perform its intended function, without failure, for the required duration when installed and operated correctly in a specified environment.

Availability is a measure of reliability indicating the fraction of time in which a device or system is expected to operate correctly.

It is important to remember that reliability and availability are statistical measures: they will not predict when a particular device will fail, only the expected rate based on average performance of a batch of test devices or on past performance.

Some definitions

Mean Time Between Failures (MTBF) is the expected or average time that a device will be free of failure.

Typical MTBF for a well designed and manufactured electronic device might be 10 to 20 years.

Mean Time To Repair (MTTR), is the time taken to repair a failed device.

In an operational system, MTTR generally means time to detect the failure, diagnose and locate the problem and replace the failed part.
Availability

- Availability can be calculated from MTBF and MTTR:

\[
\text{Availability, } A = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}
\]

- Remember that availability is a statistical measure and represents an average probability of being in operation.

- There is little point in trying to be accurate with these figures since actual failures are unpredictable.

- Availability is typically specified in “nines notation”. For example, 3-nines availability corresponds to 99.9% availability. A 5-nines availability corresponds to 99.999% availability.

Availability, \(A\) = (1 - \(D\)) = \(\frac{\text{MMTR}}{\text{MTBF} + \text{MTTR}}\)

<table>
<thead>
<tr>
<th>Availability, (A)</th>
<th>(D = (1 - A))</th>
<th>Downtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.9 = 90% (1-nine)</td>
<td>0.1 (10^-1)</td>
<td>36.5 days/year</td>
</tr>
<tr>
<td>0.99 = 99% (2-nines)</td>
<td>0.01 (10^-2)</td>
<td>3.7 days/year</td>
</tr>
<tr>
<td>99.9% (3-nines)</td>
<td>0.001 (10^-3)</td>
<td>8.8 hours/year</td>
</tr>
<tr>
<td>99.99% (4-nines)</td>
<td>0.0001 (10^-4)</td>
<td>53 minutes/year</td>
</tr>
<tr>
<td>99.999% (5-nines)</td>
<td>0.00001 (10^-5)</td>
<td>5 minutes/year</td>
</tr>
<tr>
<td>99.9999% (6-nines)</td>
<td>0.000001 (10^-6)</td>
<td>5 minutes/10years</td>
</tr>
<tr>
<td>99.99999% (7-nines)</td>
<td>0.0000001 (10^-7)</td>
<td>Not feasible!</td>
</tr>
<tr>
<td>99.999999% (8-nines)</td>
<td>0.00000001 (10^-8)</td>
<td>Impossible!</td>
</tr>
</tbody>
</table>
Availability and downtime

- Note that the availability of a device can be improved by decreasing the MTTR.
- This can be accomplished in several ways:
  - Faster detection and location of faults. (Accomplished by diagnostic reporting facilities, availability of fault finding tools and training of maintenance personnel).
  - Faster repair of the fault. (Accomplished by availability of spares and all of the above).
  - Fault tolerant design.

Example

- Consider a remote IO unit with a MTBF of 10 years.
- When the device fails, it could take several days to recognise, diagnose and locate the fault. And then, if not held as a spare, several more days to obtain a replacement. The MTTR could be one week, giving an availability of:

\[
A = \frac{MTBF}{MTBF + MTTR} = \frac{10 \times 365}{10 \times 365 + 7} = \frac{3650}{3650 + 7} = 0.998
\]

- That is approximately 3-nines availability, or a downtime of about 16 hours/year.
- Consider the availability when the MTTR is reduced to ½ day:

\[
A = \frac{10 \times 365}{10 \times 365 + 0.5} = 0.99986
\]

- The availability is now 4-nines and the downtime has reduced to about 1 hour/year.
Reliability modelling

- The system designer must understand the methods of modelling and analysis of reliability and availability in systems.
- In particular how system availability can be predicted from the individual parts.
- Also understand how standby systems, redundant solutions and common cause failures impact the overall system reliability.
- We often find that redundancy is inappropriately used and sometimes results in no real improvement in system availability.
- Careful network layout can have a major effect on the fault footprint and significantly improve the overall availability of the plant.

Standby and redundant systems

- We often see standby or redundant systems used to try to improve plant availability.
- Here we have two or more devices working in parallel.
- Should a fault occur in the operational device then the standby device can take over.
- The switch over can be manually activated or can be automatic. The switching time should be considered when estimating the overall system availability.
- This scheme achieves high availability because the system function is maintained whilst repairing the failed device.
Multiple controller systems

- Multiple PROFIBUS masters or PROFINET controllers with automatic duty-standby switching are available from a number of suppliers.

- These can drive different networks to provide redundancy down to the field level. However, separate power supply and network cable routing are advisable to minimise common-cause failures.

- Sometimes dual slaves can be used in the field with a simple “wired-OR” voting system driving the final actuator or connecting two redundant sensors.

- However, more often we find such redundant controllers are using the same field devices and actuators.

- Such systems must be carefully designed, taking account of the consequences of all possible failures.

Redundancy solutions for PROFIBUS

- Solutions for redundant PROFIBUS cabling are available from many manufacturers:

  - Siemens Y-Link
  - PROCENTEC ProfiHubs
  - COMbricks modules
  - Moor-Hawke Redundancy for PA
  - ABB Redundancy Link Module
Properly designed redundant solutions can provide robustness against a wide selection of faults and conditions.

PROFINET systems can be laid out in a number of ways:
- Star and tree topologies using switches:
- Line topology using two-port devices:
- Or a combination of both.
PROFINET system layout

There is a clear advantage of the star topology in terms of system availability in that any device can be replaced without affecting the other devices.

However, the system cost will be significantly greater because of the number of switches required.

The line topology is much lower cost, because separate switches are not required.

But removal or replacement of any device will cause all downstream devices to fail.

Redundancy solutions for PROFINET

One of the big advantages of PROFINET is that it incorporates a specification for media redundancy.

The standardised Media Redundancy Protocol (MRP) provides manufacturer independent redundancy which can be used over copper or fibre cables.

PROFINET redundancy can provide:

- Controller redundancy.
- Transmission media and switch redundancy.
- IO device redundancy.

Redundant PROFINET systems are relatively easy to implement and can be used across different manufacturers.
PROFINET redundancy

- Standardised Media Redundancy Protocol (MRP) can be used on PROFINET systems to give media redundancy.

- But the system must still be properly designed, considering all possible failures and their likelihood. Common cause failures must be properly dealt with.

Other ways to improve availability

- The careful design of networked systems can improve their availability.
- In particular by organising the system so that selected parts of the system can be independently shut down for maintenance without affecting the remaining production.
- A simple example of this is seen with streamed production.

- A stream can be taken out of service without affecting the other stream.
- But only if the system design allows this.
The concept of dividing the plant into Automation Islands or Automation Units is well established.

Each automation unit is considered as being functionally separated from the rest of the plant so allowing it to operate (and to be shut down) independently.

A good network design will facilitate the isolation of these automation units using:
- Different controllers;
- Different networks or subnetworks;
- Segmentation.

Careful choice of various architectures for automation units is a key stage in the design process which can impact on the overall reliability and maintainability of the control system.

A new Certified PROFIBUS System Design course was developed last year and is fully accredited by PI.

This 3-day training course is suitable for managers, designers and engineers who are involved in the planning, specification, design and procurement of PROFIBUS systems.

The course covers the optimum design both DP and PA systems for availability and maintenance.

The 1-day Certified PROFIBUS Installer course is an essential pre-requisite which is normally run together with the design course making 4-days of training.

The course is also available for cost-effective on-site delivery for between 6 and 12 people.
Certified PROFIBUS and PROFINET training including the new Certified PROFIBUS System Design course is available from the UK’s accredited training centres:

- PROFIBUS International Competence Centre
  - Manchester Metropolitan University.
    - in Manchester, or a location of your choice.
    - (www.sci-eng.mmu.ac.uk/ascent/).
- PROFIBUS International Training Centre
- Verwer Training & Consultancy Ltd
  - in Manchester or on-site.
  - (www.VerwerTraining.com)