

Foundation Fieldbus End Users Council Australia Inc.

9 Corcoran St Duncraig, WA 6023

P.O. Box Z5546 Perth, WA 6831

## **A TRULY REDUNDANT WIRING SOLUTION FOR FOUNDATION FIELDBUS SEGMENTS**

**Mike O'Neill**

Director, International **MooreHawke** Sales

Moore Industries-International, Inc

A restricting factor in the uptake of FOUNDATION Fieldbus technology is that the physical layer used does not naturally allow for redundancy. Power supplies and interface packages can provide redundant connections to higher level networks, but all device communications within individual segments are absolutely dependent upon the performance and integrity of a single twisted-pair cable.

This paper introduces a completely new and secure solution for fieldbus segment cabling which, when used in conjunction with redundant DCS system interfaces and redundant segment power supplies, is the final piece necessary to overcome objections to the reliability and vulnerability of fieldbus systems. The paper describes the technology used to allow segment-powered H1 interfaces to communicate on redundant media, and outlines the software changes necessary for those DCS designs with independently powered H1 interfaces. The paper shows how the technology builds on current expertise in wiring practices for Manchester-encoded bus-powered 2-wire systems, and requires no changes to the design and operation of field devices.

Finally, the paper describes the impact of such a redundant wiring system on the choices for hazardous area protection technology, predicting that intrinsically-safe techniques will be completely overshadowed by a return to non-incendive and flameproof solutions.

Keywords: **Fieldbus Redundant Wiring**

## 1. Fieldbus Systems

Fieldbus uses modern low-power electronics to add computational and communications functionality to process measurement & control instruments. Many such devices can be connected together onto multi-drop networks (fieldbus segments) where power is supplied along a main connecting cable (trunk) and split down to individual devices by drop cables (spurs). These devices can provide multi-variable data and a large measure of self-diagnostics. They are also bi-directional; technicians and engineers in the maintenance shop can interrogate these devices, revising parameters and reconfiguring devices to suit changing process requirements. Fieldbus is growing in popularity as systems designers discover the advantages in distributed processing and advanced diagnostics, and many end-users have made statements that new system implementations will automatically be specified with fieldbus technology as first choice.

Common versions of fieldbus for process control are Profibus-PA and FOUNDATION™ Fieldbus, which are both based on the same physical layer implementation of IEC61158; a two-wire power and signal connection, with Manchester-encoded digital communications at 31.25kHz on a nominal 9–32VDC bus. Sometimes called a Manchester-encoded Bus Powered (MBP) system, this physical layer implementation is serial and linear; there is no physical layer redundancy built into the system.

This raises reliability issues over the security of communications, some of which are addressed by additional hardware such as duplicated power supplies and system-end interfaces. In FOUNDATION Fieldbus systems, it is common to see redundant H1 interfaces and duplex power supplies. In Profibus-PA systems, Segment Couplers combine the DP/PA data conversion with power 'conditioning' (filtering to prevent the high frequency digital signal disappearing into the DC power supply) and so redundant communications is more difficult to implement. Even with these duplicated components, the entire segment still hangs on a single twisted-pair cable and so some suppliers and users restrict the number of devices on individual segments to minimise the potential consequences of segment failure.

## 2. Control in the Field

One of the most under utilised aspects of fieldbus is the ability to perform Control-In-The-Field (CITF) which is available with FOUNDATION Fieldbus right now, and will certainly become available in Profibus networks (since Profibus always seems to follow FF developments). CITF offers a return to the classical control systems design; that is, truly distributed control where PID processing is performed either at the primary measurement device or within the final actuator device. The DCS (Digital or Distributed Control System) is then primarily used for process monitoring, trending, alarming and optimisation of the control strategy to meet changing business demands. Fieldbus provides the communications technology to bring the measured value(s) to the control block (software within the device). The PID block may be enhanced to various degrees, either by specific software in devices or downloadable software (if devices support block instantiation).

A Truly Redundant Wiring Solution for Foundation Fieldbus Segments.

C.I.T.F. brings an immediate reduction in communications traffic on the segment and hence an overall reduction in macro-cycle times. For example, a conventional fieldbus control strategy sends the measured value (AI) from a measurement device to the segment controller, where it is processed as a PID block. This commands an output (AO) from the actuator, which returns a confirmation back to the controller – 3 external links are required. By contrast, execution of PID and AO within the actuator only requires 1 external link – the measured value (AI). Figure 1 (courtesy of Endress+Hauser, Switzerland) shows the external links required depending on the location of the PID function block.

Reducing the communications overhead in any segment also allows for more devices on the segment, with a consequent reduction in systems hardware costs (fewer cables, fewer power supplies, fewer segment interface cards). <sup>(1)</sup>

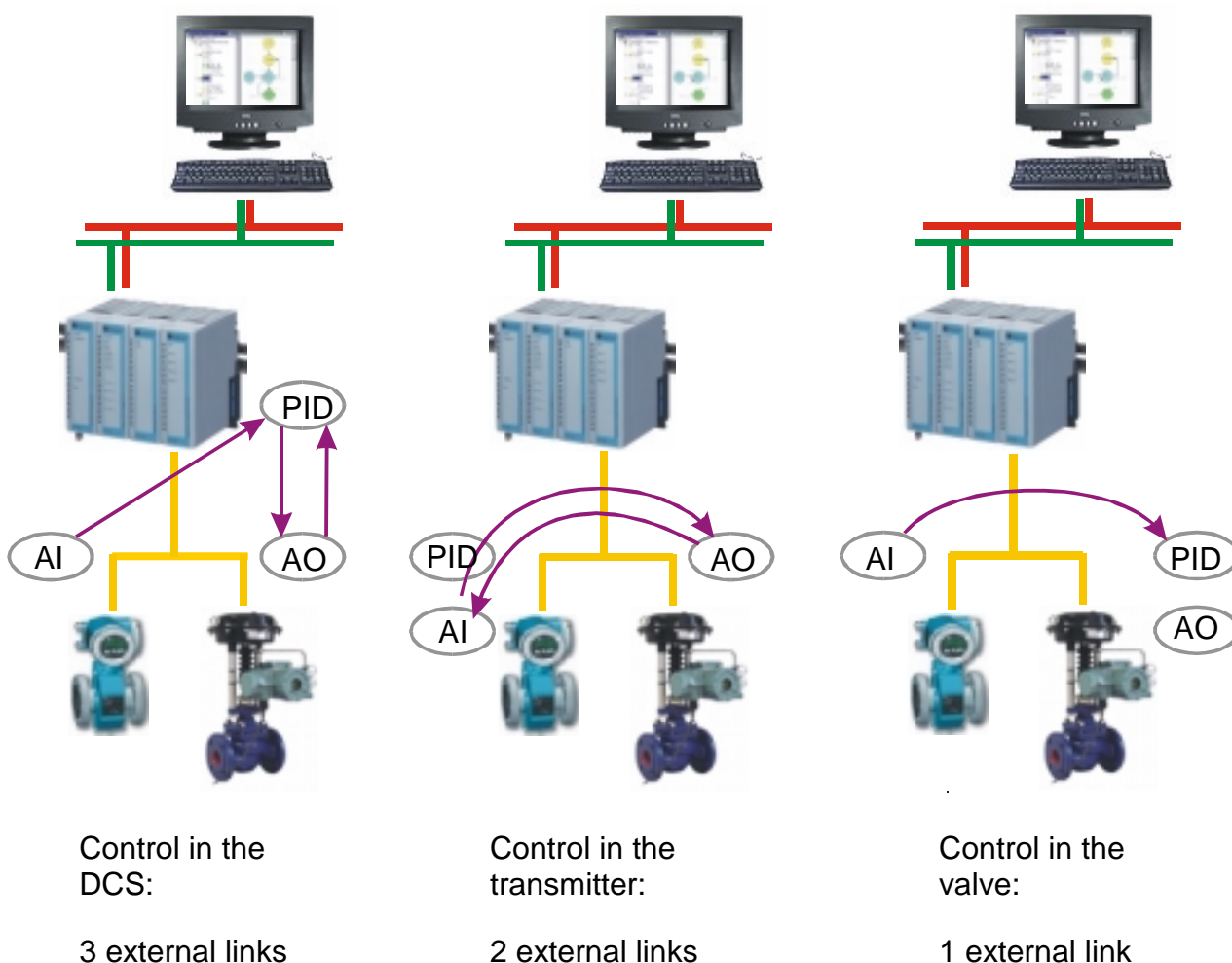


Fig 1: External communications links, depending on location of PID function

### 3. Redundant fieldbus wiring solutions

Currently, fieldbus segments may be protected from failure by redundant power supplies, redundant segment couplers and the ability to automatically transfer the Link Active Scheduler (FF) / Bus Master Controller (PA) functionality to alternative devices. Such a configuration is shown as figure 2. A break in the the segment cable will completely disrupt communications & power to field devices.

A possible solution is to make the fieldbus segment a ring. After all, fieldbus MBP communications is token-passing and ring configurations seem to work in Ethernet applications. However, the ring connection fails for two reasons;

- (1) Timing discrepancies between the long path & the short path leading to data corruption.
- (2) The location & function of the terminator.

Another solution may be to place a fieldbus power supply in the field, driving the segment from the far end (figure 3). This would work in the sense that devices in the field would be powered after an upstream break, but there is no communications path back to the DCS. The exact location of the cable break within the segment determines if any control loop is connected to its measured value and continues, or if the loop is forced into a failsafe state, which may be quite comprehensively designed in a variety of ways (last known good value, hold position, move to open, or to close, or to a pre-defined set value, etc), but is still failsafe and not active control. The costs of providing a duplicate fieldbus power supply in the field (one per segment) are also likely to be prohibitive for most fieldbus implementations, unless there were definite and predictable benefits to that plant operation.

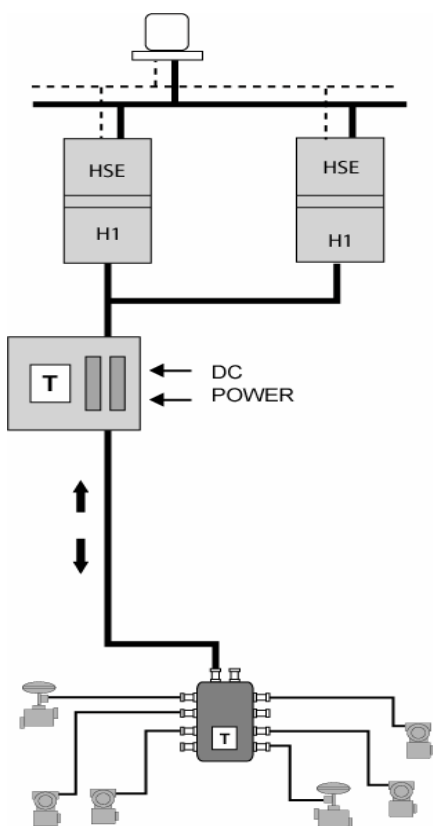


Fig 2: Conventional MBP segment

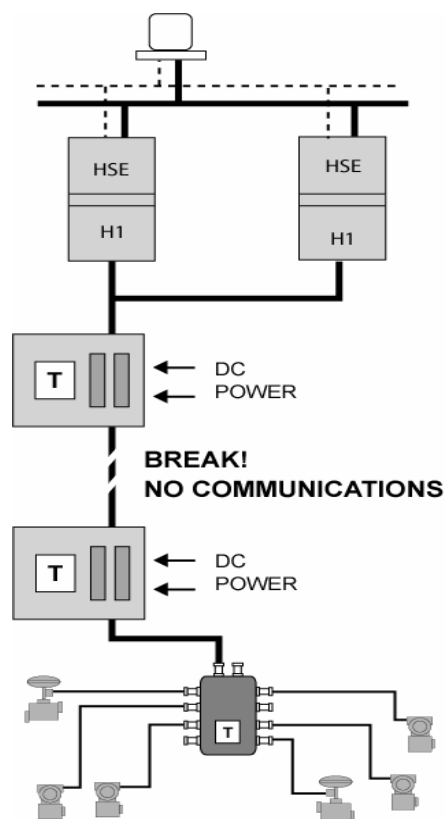


Fig 3: Field-powered MBP segment

#### 4. Automatic segment termination

A newly available and practical solution for redundant fieldbus wiring is to make the segment a long U-shape, where each end of the segment is terminated normally and connected to a local (not field-mounted) H1 interface. Each end is powered but since both ends are within the systems marshalling cabinet, this is easy to achieve. This configuration is indicated in figure 4. Note that the field device coupler does not have a terminator.

This configuration therefore meets nearly all the requirements necessary for a redundant segment solution; duplicated power, duplicated H1 interfaces and two installed cables. However, in the event of a cable failure on either side, only one terminator would be present on the remaining segment and it is very unlikely that device communications could proceed normally.

The key development to make this U-shaped segment redundant is the availability of an automatically-terminating device coupler. In normal operation, the fieldbus devices are connected to the segment and therefore connected to both H1 interfaces. Typically, one H1 is designated as the primary unit and the other is secondary, only monitoring communications. The auto-termination network within the device coupler detects that communications is active on each leg of the segment cable, and normal segment termination is at each end of the U-shape i.e back-of-panel

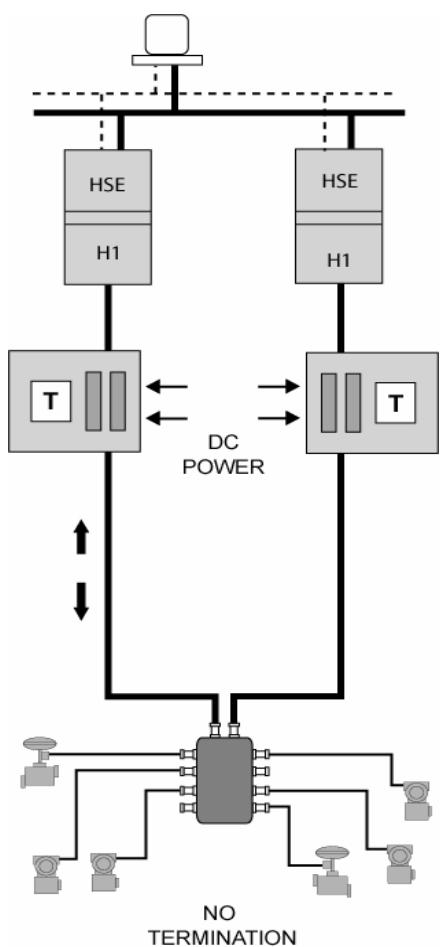


Fig 4: Looped MBP segment

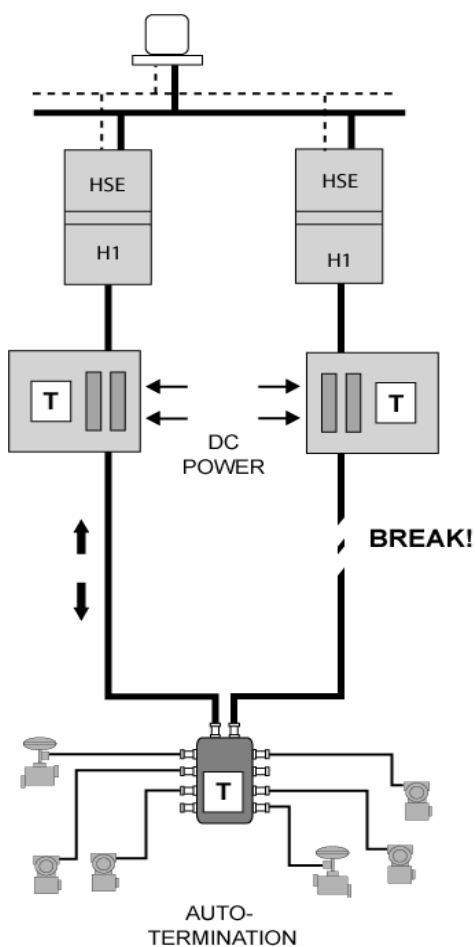


Fig 5: Auto-terminator activated

Under cable break conditions, see figure 5, the auto-terminating device coupler detects that communications cannot take place through one leg of the segment, and if it also establishes that it is at the end of a functioning leg, it activates a local terminator. The U-shaped segment has now split into 2 pieces, one connected to a H1 interface and the other properly constituted with an interface card, a fieldbus power supply plus the correct number of terminators. The auto-terminator technology is patent-protected.

No changes to individual field devices are necessary, but there may be revisions necessary to DCS software or firmware in order to reliably switch between the populated segment and the unpopulated segment. For example, DCS packages normally provide redundancy by simply lodging 2x H1 interfaces on the same segment. The H1 interface with the lowest address becomes the primary LAS, and the other H1 interface assumes the role of secondary. Both H1 interfaces are operational and remain so even if the segment cable breaks in the field. This could mean that in some circumstances, all the devices can 'drop off' the live list as far as the primary LAS is concerned (cable break in leg connected to the primary LAS), but the secondary LAS is not enabled to report on their data, even though they are still connected to it and able to communicate.

Luckily, many DCS vendors have designed their H1 interfaces to draw operation power from the segment itself, and the same technology that enables auto-termination (active signal detection & switching) can also be used to switch off the H1 interface via the local fieldbus conditioned power supply. This is all that is necessary to force the DCS to switch over to the other (active) H1 interface. The complete solution has a specific power conditioner design which reacts to cable short-circuits and cable open-circuits, switching off the H1 interface and forcing all power & communications through the remaining healthy leg. (*Complete details are still under review by patent authorities at the time of writing*).

Where H1 interfaces are more akin to linking devices and have separate power, this technique does not work. Here, internal firmware changes are required in order for the H1 interfaces to detect that one leg of the segment has effectively gone offline.

## **5. Hazardous area instrumentation**

Many industrial processes use or generate potentially explosive materials and measures must be taken to bring down the risk of unwanted ignitions. There are many techniques available for the protection of electronic instrumentation, based on a variety of concepts. There are mechanical methods such as flameproof and sand-filling which seek to contain any explosions and also to prevent propagation of ignition, and other separation techniques such as pressurisation and oil-filling, which aim to prevent hazardous materials and ignition capable sources co-existing.

Intrinsic Safety (I.S.) is a technique which controls available energy (sparks and hot surfaces), under both normal and fault conditions, to levels below which ignition of any particular material may take place. I.S. systems are considered to be among the safest of all forms of electrical protection, and the concept is only limited in application because the available power within an I.S. circuit is very small. However, instrumentation systems (pre-fieldbus) used low levels of power in individual instrument circuits, and so I.S. became the favoured technique for instrumentation.

A Truly Redundant Wiring Solution for Foundation Fieldbus Segments.

The first I.S. systems used pre-defined and verified loops described by 'systems certificates' issued by independent third parties. Systems certificates were holding back the general deployment of intrinsic safety in hazardous areas and it was with some relief that the Entity Concept was proposed and made acceptable.

The Entity Concept allows (i) devices to be approved as being intrinsically safe as long as they are not exposed to excess voltage, current and power (input) entity parameters and separately, (ii) I.S. interfaces to be approved with maximum (output) entity parameters. This makes it quite easy to select an I.S. interface to match any particular device without requiring third-party expert assistance, and allows tremendous flexibility in matching devices and I.S. interfaces. A further complication arises through cable parameters - cables represent potential sources of energy-through inductance and capacitance, and *in-situ* values of inductance and capacitance must also be shown to be below specific limits.

There are many inconvenient aspects to the use of intrinsic safety:

- restrictions on available power
- costly approval process
- management of approval certificates for devices and interfaces
- cable calculations for individual loops
- premium prices for I.S. devices
- overall increase in systems cost through necessary barriers/isolators

However, I.S. users are allowed the tremendous advantage of 'live working'; the ability to open up I.S. field instruments and make adjustments without removing power to that instrument and without having local gas detection or gas clearance certificates.

Alternative methods of explosion protection all required that loops be properly isolated or otherwise be demonstrated to be safe. After all, if the method of protection was solely that the enclosure could contain any internal ignition and quench any flame to prevent it propagating to cause a larger explosion, then that protection could not apply when the enclosure was opened. I.S. technology prospered because instrumentation *could* be made to work with I.S. levels of power and 'live working' was worth the 'hassle' and extra costs.

## 6. Hazardous area fieldbus systems

Within hazardous areas, fieldbus devices are subject to the same sort of technical constraints as conventional 4/20mA instruments, with the additional burden of multi-dropping many devices on the same network. The previously preferred solution of intrinsic safety has now become a problem; it was never easy (nor cheap) to put together individual I.S. loops - trying to deliver the same limited power to multiple loads has proven very difficult using conventional technology.

For example, inserting a conventional entity-type I.S. interface into a fieldbus segment (with suitably-approved devices) enables around 80mA or so to be made available. A low number of devices per segment poses problems for economic arguments in support of fieldbus implementation. Various solutions to this problem have been put forward, such as split-architecture systems where a field-mounted device coupler acts as an associated I.S. interface and greater power can be supplied as part of the trunk (2), and the complete revision of standard Entity systems into the **Fieldbus Intrinsically Safe CO**ncept (**FISCO**).

The alternative hazardous area technologies have not been previously favoured for other reasons. Exd systems, for example, always seem to suffer from a problem of maintenance – flameproof junction boxes are big, heavy and expensive, and while using increased safety (Exe) junction boxes is easier, they also cannot be opened ‘live’ without shielding all the non-intrinsically safe live parts. Even once the junction box is open, the wiring cannot be touched without de-powering the loop or otherwise demonstrating that field maintenance work will be safe.

### 7. Practical I.S. fieldbus systems

Split-architecture systems are available from a number of suppliers (P&F, **MooreHawke**) and these make a good combination of high-power trunk and low-power (I.S.) spurs, see figure 2. Sometimes the Trunk is I.S. for a lower Gas Group, or the Trunk may be mechanically protected by non-intrinsically safe wiring systems. In both cases, Trunk capacities are much higher than conventional IIC solutions, with around 350mA being typical. The downside is that the Trunk cable and the field interface (commonly called a device coupler) cannot be located in IIC (if the Trunk is only rated for IIB) or cannot be located in Zone 0 (if the Trunk cable is not intrinsically safe). Of course, the spurs are IIC-approved and so the field devices can be located in any Gas Group, any Zone.

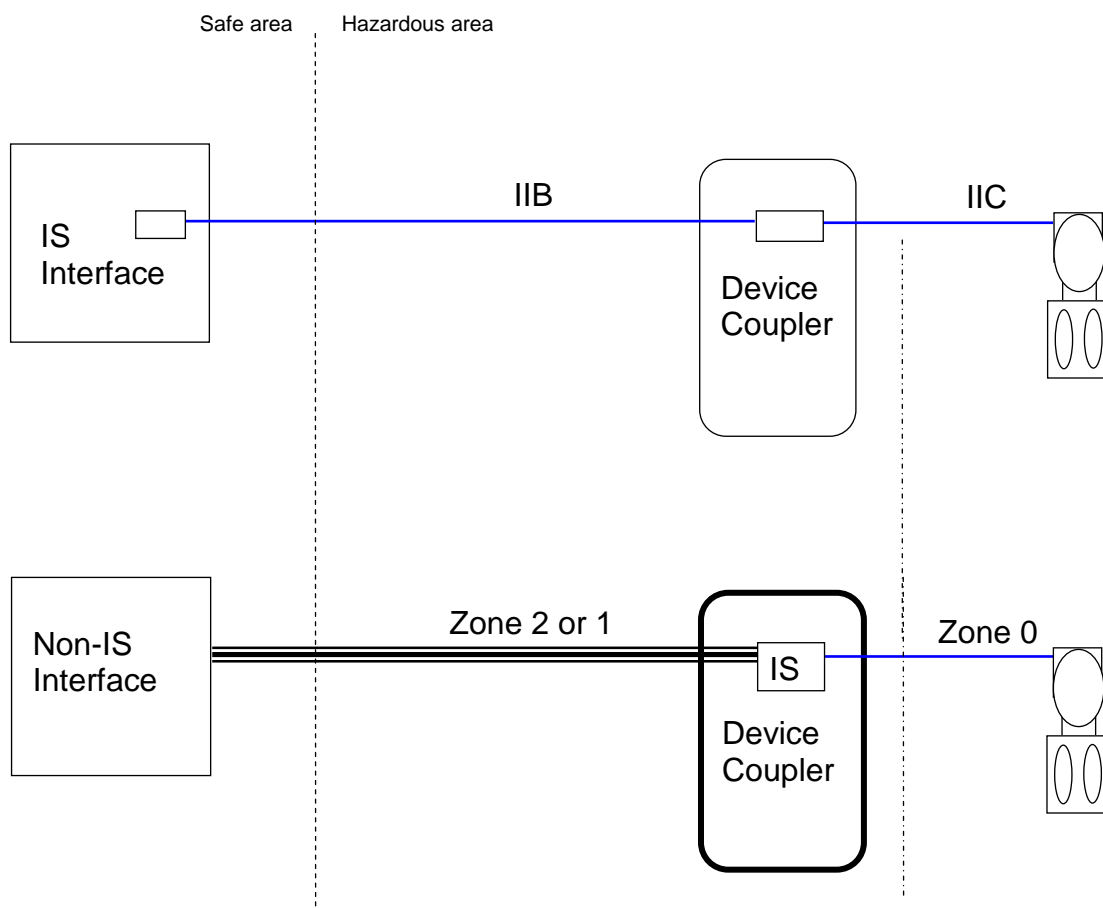


Figure 2: Split architecture systems

FISCO is a typical engineering solution to a sticky problem; if the conceptual design looks to be dangerous, build a few prototypes, test them out in a variety of situations and demonstrate by experiment that the proposed solution is actually safe,

irrespective of the applicable standard. In that way, FISCO was devised to assume a worst case set of cable parameters, takes a restricted view of what can be connected to a segment, and is tested empirically to demonstrate safety. The main deviation from the conventional standards on intrinsic safety is in the use of electronic current limiting networks as the safety element. The conventional standards assume that the current limiting component of a barrier (or other I.S. power source) is an infallible resistor, typically of wire-wound construction and substantially over-rated for its duty.

FISCO does away with the infallible resistor as the sole definition of maximum output current by incorporating electronic current limiting circuitry. Now the power supply design may have a rectangular current characteristic, or more commonly, a trapezoidal characteristic, and will be offered with higher predefined current output. This enables more current for fieldbus applications and typical FISCO power supplies offer 115mA for IIC and 250mA for IIB. The downside is the substantial cost of the power supply because of the greatly increased design complexity, and the impact of the electronic current-limiting network on the Mean-Time-To-Failure (MTTF). The overall MTTF is very much reduced compared to a conventional barrier; the single wire-wound component has to be replaced by an electronic circuit, which is not considered to be infallible for I.S. purposes, and so has to be duplicated or triplicated in series, see figure 3.

## **8. Hazardous area redundant fieldbus wiring – impact on I.S. systems**

The configuration indicated in figure 2 has two power sources, one at each end of the U-shaped segment. If these power sources were to be intrinsically-safe, the resulting safety assessment of a potential hazard at a cable fault in the middle would be the same as if there were two isolated I.S. interfaces feeding the same device – the available fault current and voltage is doubled. Therefore, to achieve the same connectivity in whatever Gas Group (IIB or IIC) is required, those I.S. fieldbus interfaces would have to be re-designed for only half the capacity. Then the problem would be that the segment could not be guaranteed to operate with the full load, since the cable break may be very close to the marshalling cabinets and hence the entire remaining segment would be powered by only one interface. Avoiding the doubling of available fault voltage can be achieved by deliberately grounding one side of each isolated interface and making the system capable of achieving only one voltage. However, the system is then vulnerable to complete failure on a single ground fault from any cable.

## **9. Hazardous area redundant fieldbus wiring – new configurations**

With intrinsically safe systems at such a disadvantage, alternative methods of explosion protection would be required; Exn (non-incendive) and Exd (flameproof) devices would come back into vogue. There are still issues to address with each of those types of protection, but there is now a desire and a need to provide engineered solutions to gain the benefits of a truly redundant fieldbus system with the efficiencies of Control-in-the-Field.

Historically, the fundamental drivers for intrinsically-safe fieldbus against all of its associated disadvantages (cost, design problems, capacity issues) are that it enables;

A Truly Redundant Wiring Solution for Foundation Fieldbus Segments.

- (1) 'Live' working
- (2) Zone 0 connection (Ex ia systems)

However, the development of secure & reliable fieldbus communications eliminates the historical need for 'live' working – for example, the requirement to send someone (usually an apprentice/trainee) to the top of a distillation column to re-zero or re-span a transmitter or to get the serial number from that sump valve (purely for management purposes). This is now achievable through the Engineering workstation, lap-top or hand-held configurators.

In Zone 2, there are device couplers approved to allow live disconnection of Spurs and capable of Trunk connection to supplies up to 1.5A capacity. These units typically have approval with Ex nA (non-arcing) Trunk and Ex nL (energy-limited) Spurs. Spurs can be disconnected 'live', Trunks not, and Trunk terminals should be shrouded to meet IP30 in the hazardous area (not all are!).

In Zone 1, there are other device couplers approved using Ex me (encapsulation plus increased safety) techniques which, when used in Exe enclosures have individual magnetic interlocks to effectively isolate each spur and allow disconnection of Ex d wiring while the rest of the segment remains powered.

Most fieldbus devices are installed in Zone 2, with a much smaller number in Zone 1. Installation of any fieldbus device in Zone 0 is rare<sup>1</sup>. In practice, new controls over unregulated emissions and plant leakages are making Zone 1 areas smaller all the time, following similar pressures in the US to reduce Division 1 areas.

## 10. Conclusion

New developments in fieldbus wiring systems will introduce physical layer redundancy for the first time. This will encourage the adoption of Control-in-the-Field, further accelerating the requirement for this redundancy. The major consequence of making fieldbus wiring redundant in this way is that intrinsically safe fieldbus would be much more difficult from a certification point of view, and have far less capability at double the price. The conclusion must be that intrinsically safe fieldbus systems would be completely impractical where wiring redundancy is required, and alternative non-incendive and flameproof systems would become the norm, displacing current intrinsically safe systems.

## References

(1) da Silva Neto, E.F. and Berrie,P. "Who's afraid of Control in the Field", *Foundation Fieldbus General Assembly, Singapore, (2003)*

---

<sup>1</sup> None are actually known to the author – any reader able to demonstrate a Zone 0 fieldbus device requirement would be handsomely rewarded.