KUWAIT SECTION

December
NEWSLETTER 2009

INSIDE THIS ISSUE

FROM SECTION PRESIDENT'S DESK

I am pleased to release the December 2009 Newsletter of ISA - Kuwait Section.

We invite ISA Members and other Automation Professionals to contribute articles to be published in this newsletter.

Please send your feedback about your expectations of ISA - Kuwait Section to

kuwait-section@isa-online.org

Best Regards

Ali H Al Hashemi
President
ISA - Kuwait Section

ISA KUWAIT SECTION OFFICE

Ali H Al Hashemi
President
Kuwait National Petroleum Co
a.hashemi@knpc.com

Ali H. Alawadhi
Vice President
Kuwait National Petroleum Co

ah.awadhi015@knpc.com

PP Muthu
Secretary
Rezayat Trading Co Ltd
Office 24816836 Ext. 146
Cell 9437119
muthu@rezayatkwt.com

C. Dakshinamurthy
Treasurer
Kuwait Oil Co
Office 23822713
dakshinamurthy@kockw.com

Chandra Sekhar, S
Membership Chair
Kuwait Oil Co
chandras@kockw.com

Editorial Board

Invitation to Members

We invite interested ISA members to write anything about Automation to be published in this monthly Newsletter.	We invite IA&C Manufacturers and their representatives to use this newsletter to advertise their product offerings.

When is a Safety Integrity Level (SIL) Rating of a Valve Required?

Riyaz Ali
Director, Instruments Unit, MEA
Emerson Process Management – Fisher Divn,
Dubai - UAE

KEYWORDS

Random Failures, Systematic Failures, Failure data, Safety Instrumented System (SIS), Basic Process Control System (BPCS), Probability of Failure on Demand (PFD), Safety Integrity Level (SIL), Safe Failure Fraction (SFF)

ABSTRACT

Final Control Elements (Control valves or Safety Shut Down Valves) are the key components of any close loop control system, whether it is used for Basic Process Control System (BPCS) or for Safety Instrumented System (SIS). Financial constraints derive different constructions of valves suitable for throttling vs On-Off applications. However, due to past accidents, reliability has become key criterion for valve selection process. Many of process industries based on their plant specific experience are tempted to use Control Valves for Safety shut down applications, specifically smaller size valves, which may not be cost prohibitive. This paper will provide clarity on when to assign the SIL suitability for valves used in different scenarios (process control vs safety shut down) and establish criterion to assign SIL applicability for "Final Element".

INTRODUCTION

Safety integrity Level (SIL) is the discrete level for specifying the safety integrity requirements of the safety instrumented functions. It is a quantifiable measurement of risk used as a way to establish safety performance targets of SIS systems. An SIL level can be expressed in terms of Probability of Failure on Demand (PFD) or Risk Reduction Factor (RRF). Risk reduction factor is simply a reciprocal of PFD (1/PFD). SIL levels are designated in terms of PFD or RRF as a range of numbers.

PFD is a value that indicates the probability of a system failing to respond to a demand. PFD is a function of test interval time and failure rate of the equipment under control.

In short, to establish an SIL suitability rating for a Safety Instrumented Function (SIF) loop, a PFD value needs to be computed for components of loop (SIF loop consists of Sensor, Logic Solver, Final Element) To calculate PFD, an equipment failure rate number is required.

FAILURE MECHNAISM

Failures are categorized so that failure data can be organized in a consistent way. ISA Technical report ISA-TR84.00.02-2002 – Part 1 talks about two failure modes - physical (random) failures and functional (systematic) failures.

Physical or random failures result from the degradation of one or more hardware mechanisms. It is often permanent and attributable to some component or module. For example, when a control valve is at the end of travel and not moving with the change in the control signal due to a broken shaft, the failure has occurred because of a physical failure of the component in the valve.

On the other hand, functional or systematic failures are failures related in a deterministic way to a certain cause, which can be eliminated by a modification of the design or manufacturing process, operational procedures, or other relevant factors. For example, a computer program has crashed and there is no physical damage, but the system has failed. The end result is that the program is not working and a failure has occurred due to a systematic error in programming code.

A major distinguishing feature between a random failure and a systematic failure is that failures arising from a random failure can be predicted with reasonable accuracy, while systematic failures, by their very nature, can not be accurately predicted.

With a basic understanding of failure mechanisms, it is clear that with mechanical items like control valves, failures can be classified under the physical or random failure category, which is simpler by nature.

Systematic failures are typical characteristics of programmable electronic systems or microprocessor-based devices. The reliability concept has been around the industry for a long time but due to advancements in electronics and control systems, this concept is more crucial than ever before. Because a final control element is part of the control loop, its reliability data is also being questioned by end-users.

This leads to a basic question –

DOES A "FINAL CONTROL ELEMENT" REQUIRE A SIL SUITABILITY RATING?

To understand the exact need, let us discuss control systems used in process sector industries. Control systems are frequently separated into two categories: systems that protect the equipment, classified as "Safety Instrumented System" and systems that control the equipment, known as "Basic Process Control System." Final control elements are part of both systems.

According to IEC 61511 part 1, 3.2.3, Basic Process Control System has been defined as:

Basic Process Control System (BPCS)
A system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1.

This definition leads us to conclude that a BPCS is any system that has a SIL<1. Therefore, SIS systems employing Safety Instrumented Functions with a specified safety integrity level, which is necessary to achieve safety function, need to have a SIL rating equal to or above 1.

This above conclusion raises some interesting questions:

1. Why are control valves to be SIL certified?

Industry practices and routines generally define which valve design need to be used for a safety versus control applications.

However, due to reliability attributes of control valves, especially on smaller sizes, make them suitable for safety applications.

Financial considerations and maintenance aspects (using same valve design for both control and safety) are making control valves attractive for safety applications. We can categorize in three different scenarios as below, where control valves can be used as safety shut down valves.

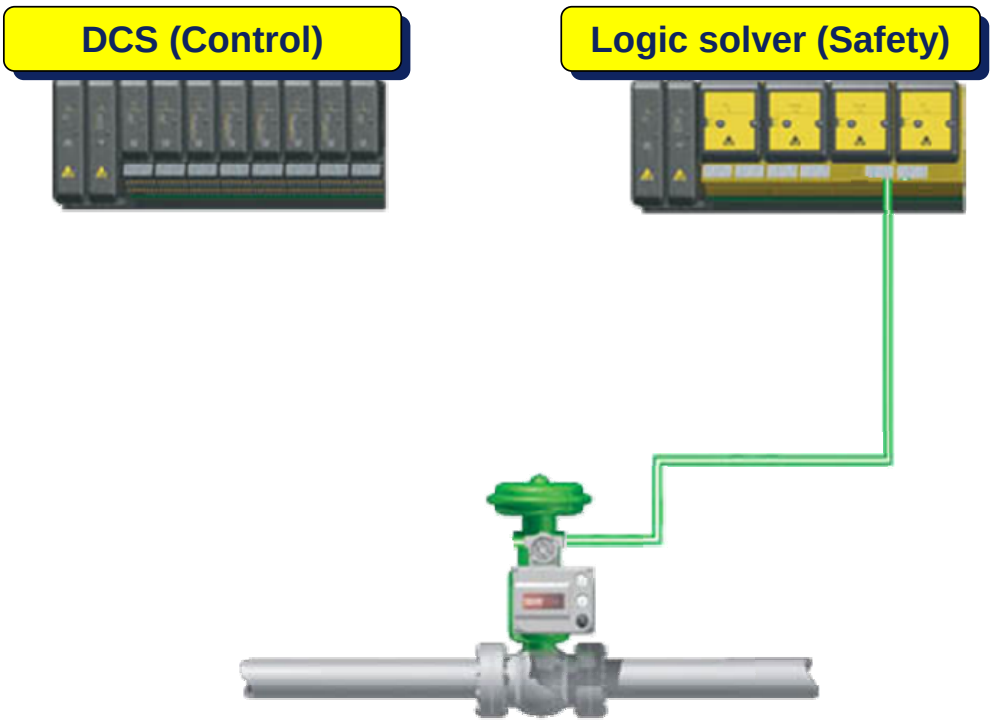
CASE 1: Control valves which are used only as an on/off single final element

CASE 2: Control valves which are used in a dual purpose context (both for control and safety)

CASE 3: Control valves which are used in a dual purpose context in addition (redundancy) to an on/off valve

Illustration for Case1:

A control valve is used for Safety Applications. In this case Control Valve is “Final Element” of Safety Instrumented Function (SIF) Loop needs to have SIL rating equal to or above 1.



CASE 1

Illustration for Case2

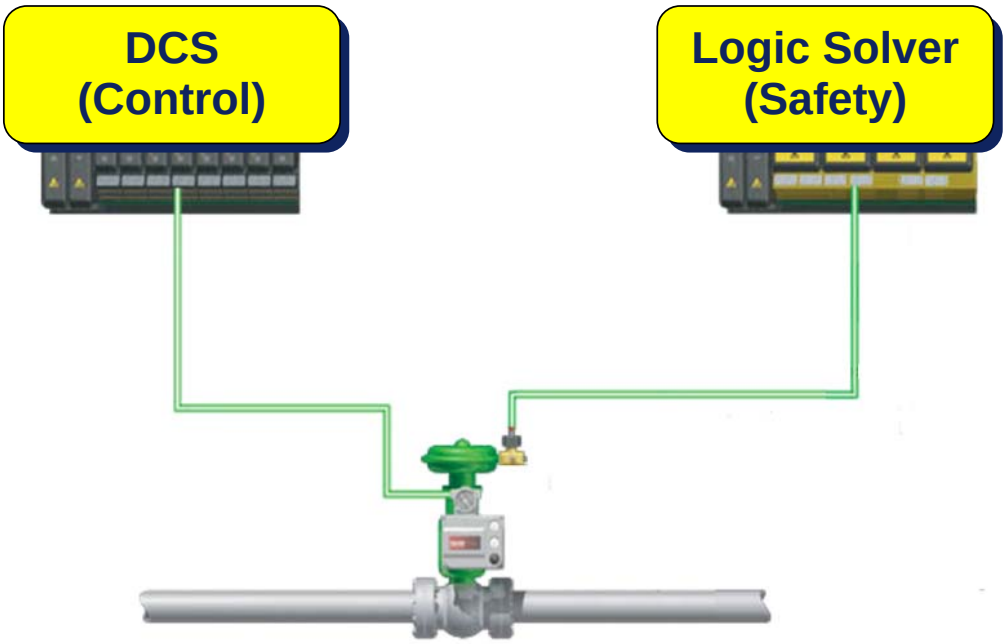
Is it possible to use single control valve common for both Safety and Control?

According to IEC61511 part 1 clause 11.2.10, it states that a device used to perform part of a safety instrumented function shall not be used for basic process control purposes, where a failure of that device results in a failure of the basic process control function which causes a demand on the safety instrumented function, unless an analysis has been carried out to confirm that overall risk is acceptable.

This may possibly lead to following interpretation;

- YES: If all possible failures of the control valve **do not** place a demand **on any** SIF than control valve may be used with no further analysis. In this case, Control Valve is “Final Element” of Safety Instrumented Function (SIF) Loop, needs to have SIL rating equal to or above 1.
- NO: If failure of the control valve will place a demand **on a SIF** than it may not be used as the only final element in that SIF.
- If failure of the control valve will not place a demand on SIF, for which it is intended but may place demand **on any other associated SIF** than the control valve may be used in a SIF only after detailed analysis. An additional step to

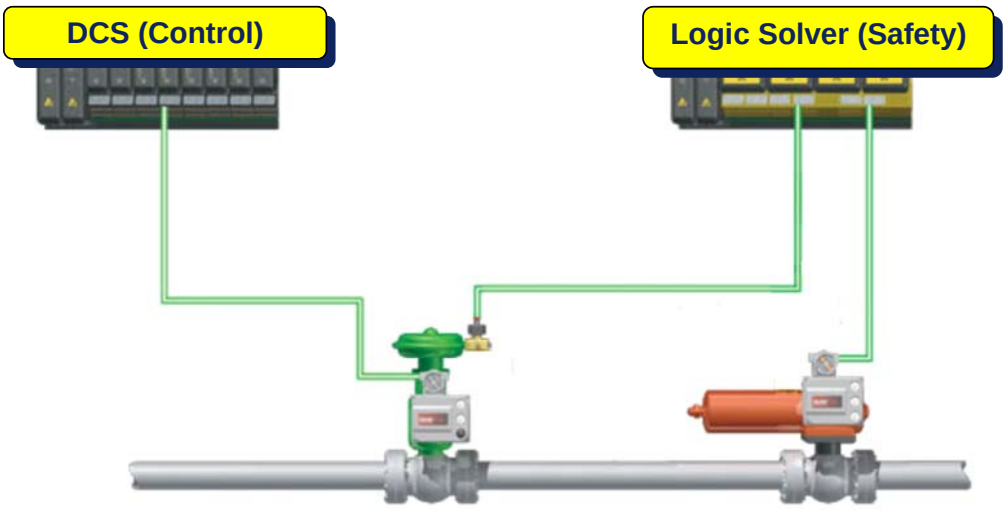
further analysis will be necessary in these cases to ensure that the dangerous failure rate of the shared equipment is sufficiently low. In this case, Control Valve is “Final Element” of Safety Instrumented Function (SIF) Loop, needs to have SIL rating equal to or above 1.



CASE 2

Illustration for Case 3

In this scenario a control valve is used to provide additional hardware fault tolerance for higher SIL application, which is similar to using a control valve for safety but with the added burden of justifying and verifying the SIF design and its final SIL value.



CASE 3

2. Why are control valves that are used in a BPCS required to be SIL certified?

As per IEC definition, a SIL rating is not required but it is possible that reliability data for a valve may be required. Industry or end user may require failure rate data of equipment or in loose term MTBF (Mean Time Between Failure).

Essentially MTTF (mean time to fail) is the right term to define product reliability. It is usually furnished in units of hours. This is more common for electronic components, but trends are seen even for mechanical items.

3. How can MTTF provide useful data for the calculation of PFDavg (probability of failure upon demand)?
MTTF can be simplified to 1/(sum of all failure rates) or equal to 1/λ. In general, components of MTTF can be categorized in the following categories:

Safe Detected (λ^{SD})
Safe Undetected (λ^{SU})
Dangerous Detected (λ^{DD})
Dangerous Undetected (λ^{DU})

This data leads to useful information:
MTTFs (Mean time to Fail Safe) and
MTTFd (Mean time to fail Dangerous)
SFF (Safe Failure Fraction)

MTTFs can be computed by adding ($\lambda^{SD} + \lambda^{SU}$) and reversing the number
MTTFd can be computed by taking λ^{DU} and reversing the number

SFF can be computed using the equation = $1 - (\lambda^{DU}) / (\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU})$ or $(\lambda^{SD} + \lambda^{SU} + \lambda^{DD}) / (\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU})$.

PFD_{AVG} can be calculated using simplified equation of failure rate of equipment under control (EUC) times test interval divided by two.

MTTFs calculations provide plant availability, which is a very important measurement of process plant up-time capability. A spurious trip that is considered a safe but unplanned trip may be too strenuous for piping and other equipment. Not only are production and quality affected, profits may be as well. Also, it is important to consider the higher risk associated with plant start up. IEC 61508 stresses more on "safety event", in case of demands, which relates to dangerous undetected failures and are used to compute PFDavg.

As such, mechanical equipment like valve bodies and actuators do not have any diagnostics capabilities. According to IEC 61508 part 2, table 2, with a hardware fault tolerance (HFT) of zero, they can only be used in SIL 1 applications. A digital valve controller mounted on a "Final Control Element" improves the diagnostic coverage factor, which in turn improves the SFF number, allowing the possible use of higher SIL rated applications (Per IEC 61508 part 2, table 3) by use of the Partial Stroke Test.

CONCLUSION

If control valve is designated to carry out a safety function then it should meet the SIL level of the Safety Instrumented System Function loop. In this case, failure rate numbers will be required to compute the total PFD_{AVG} of the loop. The end user may possibly ask for third party certification to comply with IEC 61508 requirements to meet certain SIL suitability. However, if a control valve is designated for normal process control than as per IEC61511-3 part 1, section 3.2.3, Basic Process Control System, definition does not designate control valves to have SIL suitability.

REFERENCES

i) International Electrotechnical Commission, "Functional Safety - Safety instrumented systems for the process industry sector" - IEC61511
ii) International Electrotechnical Commission, "Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems" - IEC61508
iii) Control Systems Safety Evaluation & Reliability – William M Goble
iv) ISA Technical report ISA-TR84.00.02-2002 – Part 1

ISA Kuwait Section with association with HONEYWELL arranged a Technical Presentation on *"Plant Wide Manufacturing Execution Systems for Refineries and Petrochemical Plants"* on November 5th, 2009

ISA Meeting Notice
Thursday, December 10th , 2009
Hilton Resorts – Mangaf

The Kuwait Section of ISA is pleased to invite all the ISA Members in Kuwait to the Technical Presentation on **December 10th, 2009** sponsored by Yokogawa Middle East .

M r . Govind Raju Seshadri - Marketing Manager, **Yokogawa Middle East, Bahrain**

Will present on :

" Benefits of True Integration of DCS / SIS / SCADA "

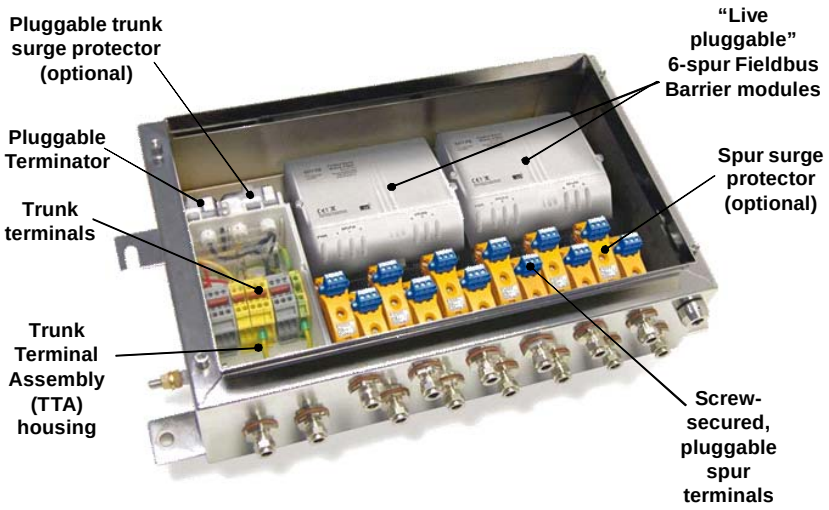
Attendance is free of charge for all ISA members. The meeting registration and reception will begin at 6:00 P.M. and the presentation will start at 6:30 P.M. The presentation and dinner will be held at the **BURGAN ROOM, Hotel Hilton Resorts, Mangaf.** Please confirm you attendance to muthu@rezayatkwt.com

New 9370-FB Series Fieldbus Barriers – A Value Proposition

Serviceability – Safety – Size – Scalability

Introduction

MTL's 9370-FB Series Fieldbus Barrier establishes a new benchmark for FOUNDATION™ Fieldbus networks in hazardous areas. As a Zone 1-mounted wiring hub with spur connections to intrinsically safe fieldbus instruments, the 9370-FB retains the major benefits of the *High Energy Trunk* technique while removing the drawbacks associated with existing Fieldbus Barrier implementations. The result is lower cost, safer operation and higher reliability throughout the life-cycle of the fieldbus network, with benefits not only for the plant operator but also for all parties involved in the design and installation process.



The new 12-spur 9373-FB Fieldbus Barrier in Stainless Steel enclosure with Trunk and Spur surge protection fitted

The *High Energy Trunk* technique provides a valuable means of connecting fieldbus instruments in Zone 1 or Zone 0 hazardous areas to the host control system. The Fieldbus Barrier is field-mounted and provides the interface between the trunk connection and intrinsically safe spurs, allowing heavily loaded segments and long cable lengths irrespective of the Gas Group. The spur connections are compatible with any IS-certified fieldbus devices complying with 'Entity' or 'FISCO' specifications.

Serviceability

The time taken to repair failed instrumentation is crucial in many process applications. At worst there is the risk of lost production. Even temporary loss of process visibility can lead to compromises in product quality or manufacturing efficiency. If, in addition, there is the risk of fire and explosion or exposure to toxic hazards it is even more important to minimise the time an operator spends in the process area. Any activity in an area where flammable or toxic materials are present is complex and expensive to organise, so the repair of field mounted equipment should be as straightforward as possible. In some cases, extreme environmental conditions – such as high or low temperatures – provide an additional incentive to shorten any time spent outside the control room.

A guiding principle during the design of MTL's 9370-FB was to make it quick and easy to repair in the event of failure. As a result, the parts of the system containing complex electronic circuits are housed in "pluggable" modules that are "hot-swappable" in the presence of explosive atmospheres and, due to this design, they can be easily removed and replaced in the field. This crucially leads to less time spent on this maintenance activity in the field.

Easy removal of 9377-FB Fieldbus Barrier modules

This is in sharp contrast with conventional Fieldbus Barrier implementations, where serviceability is impaired by the hard-wired nature of the field enclosure. As a result, some attempts are usually made in existing installations to allow some degree of maintainability in hazardous areas. For example, explosion-protected isolating switches may be incorporated in the fieldbus trunk circuit, to allow a failed Fieldbus Barrier module to be removed from the enclosure while other barrier modules remain energised and operating. However, this adds significantly to the amount of internal wiring and hardware, and threatens to reduce the overall reliability of the network. During the replacement, interconnecting cables that are temporarily removed from the failed barrier module must be prevented from shorting to other circuits inside the enclosure and then correctly re-inserted into the trunk and spur terminals on the replacement module.

As an example, the table below describes the steps required to replace a failed Fieldbus Barrier module in both a conventional installation and in the new 9370-FB Series. This highlights two important areas:

1. The time taken to affect the repair, ie. The Mean Time To Repair. This will depend on factors such as accessibility and environmental conditions, but plant operators will have their own assessment of the relative times. Repairing the conventional system is likely to take tens of minutes, compared with less than five minutes for the 9370-FB.

2. That a new fault could be introduced inadvertently. The relative complexity of repairing the conventional system adds a new risk – such as misplacing the wiring when it is re-connected to the replacement Fieldbus Barrier module. This kind of fault may not become evident until after the operator has completed the initial repair and returned from the field.

Maintenance activity	Conventional Fieldbus Barrier enclosure	9370-FB Series Fieldbus Barrier enclosure
Remove and replace Fieldbus Barrier module	• Remove main enclosure cover • Select and operate appropriate isolating switch • Open trunk terminal cover on barrier module • Remove trunk wiring from terminals and secure • Remove spur wiring from terminals and secure • Remove and replace barrier module • Reinstate trunk and spur wiring and close trunk terminal cover • Operate isolating switch • Replace enclosure cover	• Remove main enclosure cover • Loosen barrier securing screws • Remove and replace barrier module • Tighten barrier screws and replace enclosure cover

Comparison of module replacement procedure for conventional FBB and new 9370-FB

Safety

Any electrical apparatus located within a hazardous area presents a possible source of ignition for flammable materials, so the selection process should identify and – as far as is practically possible – minimise the risk of personal injury or damage to plant and equipment. The design and construction of electrical equipment intended for hazardous area use is governed by international standards, and the user has an implied obligation not only to comply with minimum requirements, but also to select apparatus that uses the latest technology to achieve safety. There are two important considerations:

1. To reduce the risk associated with routine maintenance that is properly carried out accordance to the manufacturer's guidelines and national codes of practice, and
2. To reduce the risk that any inadvertent or unauthorised activity could cause an unsafe condition.

Since Fieldbus Barriers are intended to be installed hazardous areas, careful attention should be paid to the risks of operating and maintaining them throughout their life cycle.

By definition in a 'High Energy Trunk' network, the voltage and current levels in the fieldbus trunk circuit are above those permitted by Intrinsic Safety and are therefore capable of causing an incendive arc if the circuit is broken or shorted. MTL's 9370-FB Fieldbus Barrier is constructed so that the fieldbus trunk connections are contained within a separate compartment that has its own cover. Once the trunk cables have been installed into the terminals within this compartment, it should not be necessary to open it until the unit is taken out of service.

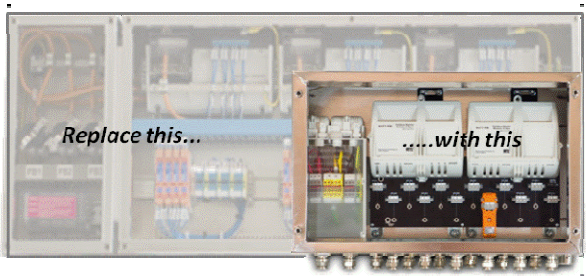
9373-FB (12-spur stainless steel enclosure) showing the pluggable components

Another contributor to safety is that all the user-accessible circuits and connections within the main enclosure compartment of a 9370-FB system are live-workable in a hazardous area. This eliminates any risk of an incendive spark from an unauthorised or inadvertent maintenance activity.

Size

Reducing the size of field-mounted apparatus such as junction boxes has advantages throughout the life of an installation. Right from the start, there can be savings in shipping and temporary storage costs. Smaller enclosures are also easier to install and maintain, and require less mechanical infrastructure to support them. Lids and covers are less likely to deform if they are smaller, reducing the risk of water or dust ingress.

The 9370-FB Series Fieldbus Barrier is significantly smaller than the conventional equipment it replaces. The 12-spur variant is as much as 70% smaller in terms of overall enclosure volume. This will be of particular benefit where space and weight are serious considerations, for example in restricted process areas or offshore installations.



The 9370-FB Fieldbus Barrier is up to 70% smaller than existing implementations

Scalability

It is an industry maxim that the later a problem emerges in a project, the more expensive it is to put right. In the extreme, replacing or modifying equipment that is already installed on the plant is many times more expensive than changing the design on paper. It is therefore imperative that decisions made about product selection during the 'Front End Engineering Design' stage of a project should survive through to completion. However, there are typically many uncertainties during the early design phases that introduce risk. For example, the area classification, field cable lengths, quantity and location of field instruments may only be known approximately when the apparatus needs to be specified.

The key to solving this problem is *flexibility*. The selected solutions must be able to accommodate changes right up until the design is frozen and, ideally, even during the commissioning stage.

Conventional Fieldbus Barrier enclosures do not lend themselves well to this process because they are 'customised' according to the project requirements and cannot be finalised until all requirements are fully defined. Two important considerations emerge:

1. Number of fieldbus spurs per field enclosure. This must be known within reasonable limits, so that the size and total number of enclosures can be established. Conventional Fieldbus Barriers are assembled using modules that are hard-wired into the enclosure. Subsequent expansion is problematic unless the space and dedicated internal wiring for an additional module have been provided during the initial construction. The addition of a module in the field can also be difficult because the trunk and spur wiring has to be correctly connected to its terminals.

   With the new 9730-FB Series, a 12-spur enclosure fitted with one 6-spur module can be specified instead of a 6-spur enclosure if there is any uncertainty. This attracts only a small price increment. Expansion to 12 active spurs is easily accomplished by plugging a second module into the enclosure. No other configuration is necessary, provided the fieldbus power supply is correctly sized and the full loading of the segment has been anticipated.

2. Surge protection. This may be specified for installations that are vulnerable to damage from electrical surges, either as a result of atmospheric activity or transients from heavy-current electrical apparatus. In order to reduce cost, normal practice would be to protect only those parts of the fieldbus network whose loss would cause serious operational problems, and parts that are most vulnerable. For example, fieldbus instruments that have a relatively long horizontal or vertical displacement from the field junction box are more likely to suffer damage from surge currents. Instruments in critical control loops may also warrant special protection.

   Again, these facts may still be uncertain when the design of the Fieldbus Barrier enclosures has to be finalised, in order for their supplier to begin manufacturing. In many cases, the full I/O schedule is not confirmed until much later in the project. As a result, the only options available are to provide surge protection within the Fieldbus Barrier enclosure for *all* spurs, or to manufacture different models with varying levels of protection. But these alternatives add cost and complexity.

   What is required is the ability to fit the surge protection components where and when they are required. The 9370-FB Series accomplishes this with pluggable protectors that can be fitted into the enclosure at any stage, even after installation. The basic enclosure design already anticipates the need to protect the fieldbus trunk and one or more spurs, without any additional wiring. This adds a great deal of flexibility.