



PLANNING AND IMPLEMENTATION OF FF-SIS WITHIN THE PROCESS INDUSTRY

Gordon Stevenson

MIEAust CPEng

Abstract:

This paper discusses the planning and implementation of FF-SIS within the process industry. The approval of fieldbus for use on SIL 3 rated systems has opened the door to manufacturers, system designers and production companies to incorporate the many benefits of FF into the IEC 61511-1 safety lifecycle model. How to realise the benefits of FF and its impact on the specification, design, validation, verification and maintenance of an SIS are addressed. The risks associated with FF-SIS are examined and practical risk reduction/mitigation steps proposed.

Keywords: Fieldbus, Process Industry, Safety Lifecycle, Safety Instrumented System

1. Introduction.

For the last three years Control System engineers have applied the requirements of IEC-61511 to the analysis, realisation and operation of Safety Instrumented Systems (SIS) throughout the process industry.

In parallel, many Mining & Metals and Oil & Gas Operating companies, Design Contractors and System Integration Companies have adopted Foundation™ Fieldbus (FF) as the preferred process instrumentation protocol.

Since 2002, Foundation™ Fieldbus Users and the Foundation™ have been developing FF for SIS (FF-SIS). TÜV approval of the overall FF-SIS system concept was gained in 2003 and protocol type approval earlier this year.

The FF-SIS Safety Rollout Team (SROT) is currently working on the formal release of the specification, due to hit the street in 2007. Also, many SIS and Instrument manufacturers are developing FF-SIS hardware and system solutions in conjunction with the SROT. With Beta SIS devices scheduled for delivery to selected end users this year and FF-Registered Safety-Certified SIS products becoming available in 2008.

In the very near future, Control System Engineers throughout the process industry will be called upon to specify, design, validate and commission FF-SISs. The challenge is to successfully merge these two areas of expertise, FF and Functional safety, deliver the full benefits of FF within the framework laid out by IEC-61511 and the boundaries of regulatory requirements, corporate risk policies and technical requirements.

The majority of companies have developed detailed and robust technical specifications and guidelines that define requirements for SIS hardware, programming, system integration, physical design, along with verification processes, Factory Acceptance Testing (FAT), construction, commissioning and documentation needs. They also have detailed lifecycle guidelines and documented work processes that span the analysis, realisation and operation phases of the safety lifecycle.

Companies have also developed technical specifications and guidelines for FF instrumentation on Basic Process Control Systems (BPCS) based on the published Foundation™ engineering and application guidelines, AG-140, AG-163 and AG-181.

2. Benefits of FF-SIS

There are many potential benefits from utilising FF-SIS in relation to traditional hardwired architecture. The challenge is to turn this potential into tangible results that can be measured against the way in which current systems are designed and operated.

Increased sensor and final element diagnostics, reduced CAPEX, reduced OPEX, construction / commissioning / operational savings have all been highlighted as potential benefits.

This is not an unreasonable stance given the experience gained from implementing FF on the BPCS platform. However, upfront investment is required to review and modify the applicable documents and processes utilised in the Safety Lifecycle to ensure that the implementation of FF-SIS can live up to its potential.

3. Risk, Risk Reduction and Mitigation

It is a given that FF-SIS or traditional SIS shall supply the nominated level of Functional Safety when applied in accordance with IEC-61511. There is though, an inherent risk in adopting a new technology to replace a tried and proven solution. That risk is compounded when it applies to Functional Safety and risk reduction on a potentially dangerous industrial process.

So, what are the risks? Lack of competent staff, FF-SIS equipment still under development, potential to not implement the technology correctly, failure to realise the true benefits (financial risk) of FF, increased reliance on Limited Variable Language (LVL), lowering redundancy and reliability by utilising more diagnostics to meet SIL requirements, and increased risk of common cause failure are all potential of adding additional risk.

These are reviewed below:

Competent Staff	This risk can be reduced by investment in training and ensuring staff are exposed to the applicable technologies early in the realisation and operations phases. Utilising both Vendor and Foundation™ certified training programs. Also, SIS competency must be assured by verification that all personnel have met appropriate competency unit requirements.
FF-SIS equipment	Don't try and use proven-in-use analysis of existing FF sensors, valve positioners and auxiliary equipment. Restrict usage to TÜV approved equipment, as it becomes available.
Technology	Learn from experience gained on implementing FF on BPCS. Adopt what worked and document what didn't. Involve FF End Users Council (FFEUC) in set up of site guidelines and standards. Spend the time up front to incorporate FF-SIS into applicable standards, guidelines and procedures.
Benefits	Set targets in terms of reduced capital and operational costs. Set targets in terms of saved construction and commissioning man hours. Record any benefits realised in proof testing intervals, availability and reliability realised from FF-SIS.
LVL	Understand and document how LVL is used to configure FF segments and FF-SIS IO.

Reliability	The added diagnostics that FF-SIS offers should not be utilised to meet SIL requirements at the expense of redundancy and reliability.
Common Cause Failures	Understand what additional common cause failures FF-SIS introduces and ensure that it is considered during verification of conceptual design.

4. Develop Implementation Strategy and Plan

There is inherent risk when any new technology is introduced into an operational facility. This risk must be understood and managed through careful planning and investment in a detailed implementation strategy and schedule.

The implementation strategy must address all of the following points in detail.

FF-SIS Strategy	Document outlines the strategy and schedule under which FF-SIS shall be introduced to site. Includes a description of each phase and its required inputs and outputs. Outlines all organisation/entities and their roles and responsibilities throughout the process. Sets out Key Performance Indicators (KPIs) in which to measure the success of the implementation.
Risk Management	Introduction of a new functional safety solution must be addressed with the company risk management group. Get them up to date and on board as early as possible. Understand their requirements and address them in the plan and strategy.
Technology Review	A detailed review of FF-SIS must be undertaken. Has it the potential to deliver the desired results for the company. What does it offer that the current technologies do not?
Product review	Review of manufacturing development programs and product release dates is required. Do product testing and release dates compliment the project schedule? Can a trial be conducted on site? What logic solver architectures and Safety Integrity Levels (SILs) will be available? What local support will be available from vendors? What certified FF sensors and valve positioners are going to be available? If possible, trial sensor and valve positioners on site.

Product Selection	<p>The introduction of a new technology has the potential to challenge existing equipment supply agreements in place on site. Product selection criteria must be established in terms of technical, financial and operational considerations.</p> <p>Technical specifications need to be developed to cover FF-SIS and associated sensors and valve positioners</p>
Justification	<p>Company policy may dictate that a formal approval process be followed before FF-SIS can be considered for Functional Safety. Justification is typically based on risk management, financial, technical and operational merits. A project must allow the necessary time and resources to ensure that internal approval processes are followed.</p>
Documentation	<p>Analysis and realisation phase documents should be updated in line with FF-SIS prior to the start of project Process Hazard Analysis (PHA). Ample time and resources must be allowed for this activity to be implemented correctly.</p>
3 rd Party Vendors	<p>The plan must allow time for aligning 3rd party vendors to supply FF-SIS. Contracts, technical specifications and preferred equipment listings must be updated prior to issuing bid documents to 3rd parties. Reluctance to adopt FF-SIS needs to be addressed during negotiations prior to award. Detailed specifications and project requirements are key to winning over companies that would prefer to stick with traditional SIS solutions.</p>
Upgrading SIS	<p>It should be the ultimate goal, where possible, to utilise one SIS solution on site. Standardisation on equipment and technology has many benefits in terms of verification and validation, maintenance, proof testing, documentation, training, spares, on-going analysis and gathering of failure data and statistics.</p> <p>Once sufficient experience has been gained on the correct implementation of FF-SIS plans should be drawn up for the migration of existing systems to the new technology. Long term plans should be drawn up to upgrade systems as hardware becomes redundant or no longer supported by vendors, or in conjunction with plant/operational modifications that call upon changes to the existing SIS.</p> <p>Migration may entail the wholesale replacement of the existing system, or retaining the logic solver and only upgrading IO, field sensors and valve positioners to the FF platform. Upgrading options will become more</p>

defined as FF-SIS products are released and backward compatibility with existing systems is better understood.

5. Impact on Company Safety Lifecycle and supporting Documentation

5.1. Clause 5 – Management of Functional Safety

Company SIS management procedures must be reviewed and updated to cover any changes as a result of FF-SIS.

A clear understanding of the skills and knowledge required to deliver a FF-SIS should be identified and development, training and recruitment plans put in place to ensure that personnel with the correct competencies are available to support the safety lifecycle, *clause 5.2.2*.

FF-SIS also introduces change to the way in which SIS configuration can be managed, *clause 5.2.7*. The management program must be modified to address the specific issues relating to the configuration of FF devices and segments. Instrument models, ITK, DD and EDDL, CFF file revisions all need to be recorded and controlled through out the entire safety lifecycle. Segment communication configuration and how field devices are configured (via the host or via separate configuration tools) needs to be identified and documented.

5.2. Clause 6 – Safety Lifecycle Requirements

During the preliminary design, the company systematic safety lifecycle will have to be reviewed, and modified if necessary, to incorporate the unique requirements of FF-SIS.

Availability of FF-SIS equipment and systems is an important consideration in the early years of FF-SIS. This may have to be factored into the lifecycle until a broad base of certified equipment and support is available.

Changes to the content of FAT, SIS validation and personnel competency/training may have to be highlighted in the requirements.

High level guidance on usage of safety buses should also be considered.

5.3. The Realisation Phase – Clause 11 - SIS Design and Engineering

This clause defines the requirements that must be met to design a SIS to provide the Safety Instrumented Function (SIF) and meet the specified SIL(s).

The major input for this phase is the Safety Requirements Specification (SRS), in which the detailed requirements for SIFs are documented.

SIS Design Criteria or Basis of Design Document

The Design Criteria, or Basis of Design, is key to defining how the safety management system, auditing, life-cycle methodology plan and the verification process interacts with delivery of a SIS that meets the requirements of the SRS.

The Design Criteria sits above, and links, a number of more detailed documents that are necessary to implement the realisation phase of the SIS. Typically, a Hardware Specification, Software Guideline, Physical Design Guideline, Verification Procedure, Procurement Strategy, FAT Procedure, Installation Guidelines/Procedures, Detailed Pre-commissioning, Commissioning Procedures and System Validation Procedure are utilised during the realisation phase.

Once the decision has been made to pursue FF-SIS one of the first documents to be updated must be the Design Criteria. The update must address the higher level issues of implementing a new functional safety solution and be a platform in which to identify what other supporting documents, processes and/or procedures need to be modified. It should also define a suitable timetable that supports a successful implementation of the technology.

Particular emphasis must be placed on the changes FF-SIS is likely to have on the conceptual design process.

The Design Criteria must layout the approach an Engineer must take when selecting equipment and redundancy levels and define the way in which the probabilistic performance of the conceptual design is determined.

The Design Criteria shall identify the preferred method of equipment selection and identify the limitations of each method and the minimum requirements to correctly implement each one, *clause 11.5*.

Out of the available analysis methods, the full IEC 61508 assessment is the most comprehensive. This assessment method best addresses the issue of systematic faults and recognises the fault control and fault avoidance methods adopted by the instrument manufacturer. As a result, full IEC 61508 assessment may end up being the preferred way in which to select FF-SIS sensors and final elements.

In addition, it must be noted that instrumentation must be registered with the FoundationTM as compliant with the applicable Interoperability Test Kit (ITK). Where applicable, instrument – SIS interoperability tests must be carried out in accordance with the FoundationTM Host Interoperability System Test (HIST).

The Design Criteria shall also outline the required system availability and fault tolerance against false trips, dangerous failures and multiple failure modes in terms of preferred system architectures and redundancy models. In addition, it must identify how the FF-SIS shall handle dangerous faults detected by diagnostic tests, *clause 11.3*.

The Criteria shall identify if hardware fault tolerance levels of FF-SIS sensors or final elements can be reduced, *clause 11.4.4*. Can prior use of a standard FF be applied to the equivalent FF-SS device? If this approach is to be used then the minimum evidence of suitability that is acceptable needs to be defined.

The preferred approach to proof testing of FF-SIS must be identified with clear reference to the appropriate testing guidelines and processes. In addition, it must identify how the engineer approaches and documents the estimation of proof test diagnostic coverage for each FF device.

The Design Criteria shall identify the probabilistic calculation methods to be employed to determine if the conceptual design meets the requirements of the SRS. The Criteria defines what methods shall be utilised based on the demand mode of operation and give guidelines on when to treat high demand mode as continuous mode to simplify modelling. Clear details on the preferred method of FF redundancy must be provided.

The Criteria should identify the preferred probabilistic calculations to be used to calculate the PFDavg. If applicable, the criteria should nominate where simplified equations can be used i.e. Block Diagram, Markov Model or Fault Tree analysis. If a commercially available software package is to be used the applicable software version should be nominated.

Control in the Field (CITF) has gained more acceptance in the Process industry, with many BPCS systems utilising it to good effect. Advantages of CITF are that it provides true distribution of control and reduces FF segment communication, macro cycle times and Host loading. The Design Criteria must identify when, where and how CITF functionality can be utilised for Functional Safety.

The use of FF-SIS also introduces the ability to have an SIF distributed across more than one segment or have one segment associated with more than one SIF. The Criteria should identify how allocation and segregation of SIFs on segments is to be handled.

The Design Criteria should clearly identify where safety logic in the field can be utilised, the preferred way in which to allocate sensors and final elements to segments, limitations placed on segment loading and macro cycle times and execution sequence. Where a segment contains more than one SIF, shared or common hardware and software must conform to the highest applicable SIL, *clause 11.2.3*.

The criteria must identify how on-line testing, by-pass facilities, manual actuation and trip resets shall be implemented on FF-SIS, *clauses 11.2.5*,

11.2.7 and 11.2.8. Particular attention must be given to SIF that utilise CITF to deliver Functional Safety.

SIS Hardware Specifications

Hardware specifications have been developed to ensure that the physical construction of the SIS logic solver and peripherals utilised by a given company or plant meet the requirements of IEC-61511, regulatory codes and the company's internal technical specifications.

A robust specification identifies the desired architecture, layout, performance, and redundancy requirements of the logic solver, IO systems and power supplies. In addition it,

- defines the operational environment that the equipment shall be expected to perform in. It defines the minimum operational life requirements, reliability, availability and failure statistics, the company maintenance requirements and requirements for hardware compatibility (retrospectively and in the future).
- identifies the interface points and utilities provided.
- nominates the maintenance, testing and inspection criteria and applicable regulatory/certification requirements that the system must support and/or conform to.
- identifies physical layout requirements for the panel, racks, wiring systems that address construction, interfacing and maintenance access issues.
- defines component labelling, segregation, and isolation issues.
- defines the company's requirements for installed spare capacity, expansion capability, hardware redundancy and diagnostics.

When a company has a preferred equipment supply agreement with a SIS manufacturer the technical specification tends to be very detailed in hardware requirements. Where there is no agreement, the specification tends to be more general in an attempt not to be overly onerous in its requirements and preclude suitable equipment from compliance.

Existing SIS hardware specifications shall need to be modified / expanded to address the specific requirements of FF-SIS. The main points that shall have to be addressed are:

Interoperability of Equipment

The specification needs to identify how conformance and interoperability of the host and FF instruments is to be realised. This takes the form of nominating the applicable versions of Conformance Test System and Interoperability Test Systems to be followed along with the supporting documentation and minimum level of verification required during the realisation phase.

Diagnostic Requirements

It is important that the full benefit of diagnostic is released when calculating the SIF probability of failure, *clause 11.9*.

FF Instrument Diagnostics

One of the main advantages FF brings to SIS will be the increased Diagnostic Coverage (DC) provided by the FF instrument and the associated impact on the detected failure rate, refer to equation 1.

$$\lambda_{\text{detected}} = \text{DC} \times \lambda_{\text{total failure rate}} \quad \text{equ. 1}$$

More advanced sensors on the market offer extensive diagnostic capabilities like memory integrity checks, electronic fault detection, watch dog timer, and element degradation monitoring. Some also provide predictive diagnostics where sensor life expectancy and performance degradation is monitored. Transmitters are also available with advanced process monitoring capabilities which detect drift, noise, bias, spikes, plugged sensing lines, coated electrodes, coil and electrode faults, ground or shielding/wiring faults etc.

Smart valve positioners also provide extensive diagnostics on the health and operation of the valve and individual valve components. Valve stroke signatures, testing capabilities and component degradation diagnostics can be used for predictive maintenance of a valve.

Communication Diagnostics

There are products available that monitor noise, jitter, unbalance and other physical layer physical parameters. Some even provide visualisation of communication signals, data logging and proactively detect degradation before communication failures.

The SIS specification should identify what level of segment diagnostics should be provided, whether it shall be an integral part of the SIS or on a separate diagnostic system. In addition, it should identify where

and how diagnostic data should be stored and retrieved and what the data can be used for. There are options to store the data on a stand alone system, or integrated into the BPCS historian. What data is to be stored and what benefit from a SIS operations and maintenance point of view should also be addressed. As a minimum, historical data should be gathered to allow re-evaluation of the frequency of proof testing and if necessary used to validate quoted failure data and allow support for proven-in-use analysis for future projects.

Standard segment circuit monitoring requires loss of power monitoring, *clause 11.2.11.*

Network Wiring Schemes

The specification needs to define the desired FF network wiring schemes to be utilised. There are four main schemes to choose from; Point to Point, Bus with Spurs, daisy chain and tree topology. Each has its advantages and disadvantages with tree topology the most popular choice for FF segments on a BPCS.

Due to the various advantages of a tree topology it would be understandable to assume that this trend would also apply to FF-SIS. But additional considerations need to be addressed before choosing the most suitable wiring scheme for FF-SIS. SIF grouping and segregation, response times, control/logic location, HOST architecture and tradition/FF wiring mix and policy on use of repeaters and couplers need to be addressed.

FF Redundancy

The specification must also address the use of redundancy in FF IO. When and where redundancy Host IO cards, use of multiple Backup Link Active Schedulers (BLAS), power supplies, conditioners, and/or fully redundant segment wiring can and can't be used must be addressed.

Diversity

Limitation in credited diversity when utilising FF-SS sensors and final elements with traditional hardwired equipment must be considered.

Power Supplies and Conditioners	The specification must have detailed requirements on the FF segment power supply system power conditioners and redundancy requirements. Note that these should be supplied as an integral part of the SIS, regardless of who manufactures them, as they are a key component of the FF segment.
Maint./Eng. Interface	The specification must identify how the M/E interface fits into the overall system architecture. Are the FF segment and devices maintain through a separated M/E interface or does the chosen system offer a combine logic solver and FF-SIS M/E interface, <i>clause 11.7.2</i> .
Maint./Testing Requirements	Requirements for FF-SIS testing and on-line proof testing should be identified, <i>clause 11.8</i> .
Password Protection/Access	The specification must define the security or special procedural requirements to maintain integrity of segment, sensor and final element configuration.

SIS Programming Guidelines

Programming guidelines have been developed to ensure that there is a standard approach to programming/configuration of SIS logic solvers and that it has been conducted in accordance with the requirements of IEC-61511.

Guidelines nominate how LVL is to be utilised by the software developer in conjunction with the Application Software Safety Requirements Specification (ASSRS) to achieve consistent SIS software safety.

As a minimum, the guideline nominates the preferred syntax, terminology, programming notation, preferred software architectures, hardware and software architecture relationships, use of embedded software, use of compliant logic and library functions and module linking and tools (configuration/testing/compiler programmes).

The guidelines need to be expanded to cover the unique aspects of FF-SIS including but not limited to configuration of segment communication, CITF, handling of FF diagnostics and default alarms.

Physical Design Guidelines

The implementation of FF requires an entirely different work process when compared to hardwired IO. Guidelines need to be modified to cover the unique requirements of FF segment design.

Physical design must take into consideration the limitations of segment loading and macro cycle times, segregation of SIFs, physical limitation on segment wiring, limitation of FISCO and FNICO, mix of hardwired and FF sensors and final elements.

Most companies already have design guidelines developed for BPCS segments and it should be a simple process of expanding upon this ground work to cover FF-SIS.

5.4. The Realisation Phase – Clause 13 - Factory Acceptance Testing

The use of FF instruments on BPCSs has altered how FATs are conducted and how extensive they are.

Traditionally, all inputs would be simulated from a test console comprising of switches, pushbuttons, current sources/sinks, resistor banks, pulse generators, transmitters etc. with outputs monitored by using lamps/LEDs, current meters, DVMs etc. Therefore, the comprehensive testing of a simple indicating loop or a complex multiple IO loop was a relatively easy process.

To conduct a comprehensive test of a loop on a FF segment, the full segment should be constructed so that the full macro cycle is tested and the interaction between instruments and with the host is verified.

Imagine that you have a SIF distributed across three segments with each segment having eight devices on it. The time and hardware needed to conduct a full test to prove SIF maximum response time meets the requirements of the SRS would preclude it from the FAT.

This would not be an issue if unlimited time and resources were available to conduct a comprehensive FAT. However, generally the project schedule, construction schedules and timeframes, and project management are always aligned when it comes to minimising the time period allowed for a FAT.

It is unrealistic to construct a full SIF including whole segments in order to conduct a comprehensive test. It is more efficient to conduct this test during commissioning of the installed system and restrict the FAT to testing specific sections of the SIF.

Testing procedures and documentation needs to identify FAT tests, test limitation boundaries and limitations and how they relate to the validation tests carried out during SIS commissioning.

5.5. The Realisation Phase – Clause 14 – Installation and Commissioning

Installation Guidelines/Procedures

Installation guidelines should be expanded to include a segment wiring test. FF segment testing devices are available that measure and record the electrical properties of a full segment. These parameters should be recorded and used as reference data for future segment testing, *clause 14.2.4*.

If segment diagnostics are not provided by the SIS it would be good practice to recheck and record the segment wiring parameters as part of the proof tests. The recorded data would allow prediction of segment failure due to deterioration of cable insulation, termination, conductor etc.

Pre-commissioning and Commissioning Procedures

Pre-commissioning procedures require to be expanded to include FF. These should be written to maximise the benefits that FF offers.

On some BPCS hosts it is possible to download the field instrument configuration from host to instrument. The instrument only has to be installed with the tag number configured and the balance of data is downloaded from the host. If available, this functionality should be adopted into the design of FF-SIS.

Commissioning of all primary and auxiliary FF-SIS devices should be done on fully loaded segments. Where possible it is preferred by testing operation by simulating the process variable and verifying the loop all the way through to the SIS and HMI.

All alarm points, failure actions and where possible diagnostics should be simulated and results recorded.

5.6. The Realisation Phase - Clause 15 – SIS Safety Validation

Once the associated commissioning activities are complete a full validation of a SIF can be performed. Validation test should encompass all primary components within the SIF.

Validation test procedures must be developed to test that a SIF utilising FF-SIS delivers the safety function as defined in the SRS. As nominated in IEC 61151 the validation test must show that the SIF performs under normal and

abnormal situations, performs on invalid process variable, diagnostic alarms perform as required and on loss of utilities, *clause 15*.

Any tests not carried out during the FAT due to the limitations previously mentioned must be covered during validation.

5.7. The Operation Phase - Clause 16 – SIS Operation and Maintenance

Before handover of a SIS to operations it is imperative that operations and maintenance staff have the competency required to maintain the SIL of each SIF implemented utilising FF. With the introduction of FF-SIS it is imperative that the applicable technicians/engineers are formally trained, familiar with the technology involved and have their competency assessed.

Both parties should document the handover process in advance to clearly define accountability and division of responsibilities, handover packages, handover documentation, timetable/schedule, applicable tagging and lockout processes, define equipment energisation status at handover, change management process etc.

It is advisable to have maintenance technicians and engineers gain formal accreditation by completing Foundation™ certified training programs. They should also receive formal training from the SIS manufacturer on the operation and maintenance of the logic solver inclusive of auxiliary equipment and sub-systems supporting the SIS. It is also recommended to have maintenance personnel actively involved in the pre-commissioning, commissioning and validation of the SIS.

In addition, maintenance staff and operators should receive a formal handover of the SIS from the design engineers which includes a summary review of the design intent and criteria, analysis phase, SRS, design and verification process, proof testing, design documentation and procedures developed for use during the operations phase, *clauses 16.2.4 and 16.2.5*.

It is imperative that operations do not take full ownership of the SIS until they are confident that the SIS has been designed, constructed and validated in accordance with the applicable regulations and standards. Any issues should be raised early and resolved with the design team.

5.8. The Operation Phase - Clause 17 – SIS Modification

FF-SIS introduces additional complexities that have to be considered when implementing a change on an operational system. The change management system employed by operations shall have to be modified to identify what processes must be followed when altering FF-SIS, *clause 17.1.1*.

The change management process must be structured in line with all foreseen permutations of change whilst allowing enough flexibility to cater for the unforeseen.

Some of the potential modifications unique to FF are:

- adding a SIF on a new segment
- adding sensors or final elements of a new SIF to an existing segment;
- modifying the configuration of sensors or final elements on an existing SIF
- introducing new types of sensor or final elements to an existing SIF
- separating SIFs on a common segment to improve response time.

Change management will have to address modification to macro cycle times, sensor and final element interoperability issues, downtime on SIFs on a common segment, use of common equipment like power supplies, access security, SIF re-verification and validation.

6. Conclusions

Successful implementation of FF-SIS will be realised in the not too distant future, 1-2 years.

Control System professionals working on projects currently in the planning or feasibility stages should be following the progress of this technology closely and preparing themselves for implementing it on their project if the opportunity arises.

Preparation must include: the monitoring and review of the FF-SIS solutions brought to the market by manufacturers, draft modifications to safety lifecycle processes and documentation to address FF-SIS, addressing competency issues within own organisation.

Preliminary work on the technical and financial justification for FF-SIS should be started. There is much data available from successful FF BPCS jobs that can be used as a basis for this justification.

In addition, definition of metrics to verify/quantify the benefits of FF-SIS are required.

There are challenges ahead, but nothing that cannot be addressed with good planning, a thorough understanding of the technology involved and the application of good functional safety engineering.

7. References

IEC-61511 parts 1, 2 and 3, *Functional Safety – Safety instrumented systems for the process industry sector*, Edition 1.0.