Replacement of SIS Logic Solvers Whilst the Process Remains Operational

Clive Timms
C&C Technical Support Services

Introduction

With increasing global demand for oil and gas driving prices higher and higher, the focus of oil and gas producers is to maintain and maximise production from every available facility. Older unreliable facilities are being upgraded and this often includes the replacement of Safety Instrumented Systems (SIS) such as emergency shutdown (ESD) systems, process shutdown (PSD) systems, Emergency Depressurisation (EDP) systems and fire and gas (F&G) systems due to obsolescence or reliability issues.

Traditionally, the replacement of such safety critical systems is undertaken during a plant shutdown opportunity to ensure that process integrity was maintained and the replacement systems could be fully commissioned and validated without the presence of the process hazards. However, in this era of high oil and gas demand we are now seeing more and more SIS replacement projects being undertaken whilst the process is still fully operational, and this can lead to potential compromises during commissioning and validation of functionality.

The live replacement of SIS creates two main issues:

- Maintaining process integrity during the SIS replacement;
- Avoiding the significant potential for spurious trips whilst transferring safety functions to the replacement system.

The decision to maintain production during the SIS change out process is driven by avoidance of production losses sustained when the process is shut down. Thus the focus of project management is also, unfortunately, all too often on the avoidance of spurious trips during installation at the expense of maintaining integrity. In some cases little or no attempt is made to undertake a hazard analysis to identify the project related hazards created by a live change over.

A SIS change out, whilst the process remains operational, will always be more costly in terms of project time and manpower compared to doing it whilst the process is shut down. This additional cost is easily offset by avoiding production shut down.

Operators often use the argument that a SIS change out is ‘simply a like-for-like modification’ and, as a consequence, projects may not budget for any validation testing following change over. This is often without any consideration that:

- they are completely replacing the logic solver, which has an impact on every safety instrumented function (SIF);
- they are most probably rationalising the cause and effect logic configuration;
- the I/O interface architecture may also be significantly different;
- they may be taking the opportunity to upgrade field fitted devices as well.

So the argument of like-for-like may have little foundation.

The life-cycle phases of IEC 61508 and IEC 61511 require commissioning and validation completed before hazards are introduced, and they were not developed or structured for SIS related projects to be implemented on live process plant whilst hazards are present. Thus it is always going to be difficult, if not impossible, to fully comply with the life-cycle framework.

Following the SIS Safety Life-cycle phases

Upgrading and changing out the logic solver is of far more significance than making a 'modification' to the functionality. It will be necessary to progress the project by following the SIS safety life-cycle phases but certain phases need to be further developed to embrace projects contemplating SIS replacements on live process plant. Many of the objectives remain the same but the approach taken, with a live change out, will be somewhat different from that of a new build SIS.

Figure 1 is the standard overview of the IEC 61511[1] life-cycle phases, and the main phases concerning a SIS replacement project, that has a shutdown opportunity for the change over, are 1 through to 6.

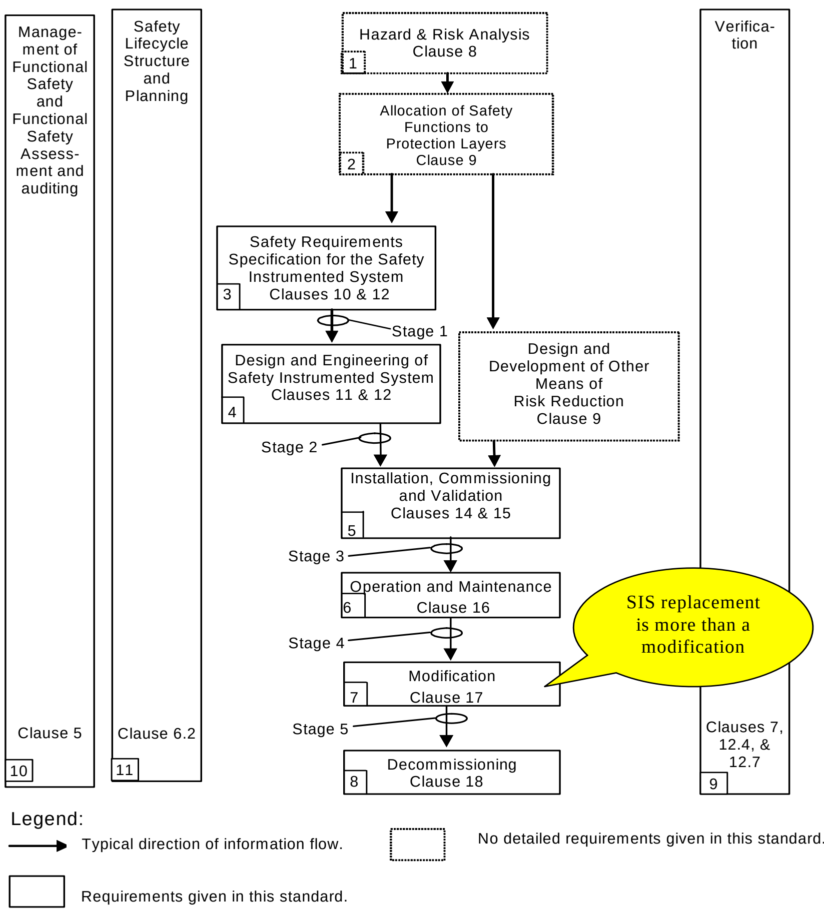

Figure 1 IEC 61511 Life-cycle Phases

There are many additional considerations that need to be applied when the process is running. Figure 2 suggests a more pragmatic 'route map' for the management of a project of this nature.

In this route map activities that are required to satisfy each stage of the project are shown as square 'activity' boxes which input into project progression phases shown as AND gates. The darker shaded activities indicate where specific considerations need to be developed for a live process. It can be seen that different types of risk assessments are embedded in the majority of the activities. Training starts early in the project as a large number of operational people need to be familiarised with the changes and these people are likely to work on complex shift patterns.

The main gated progression phases still follow the IEC 61511 life-cycle as follows:

- Hazard identification and risk assessment *(IEC 61511 phases 1-3;*
- Design, engineering and FAT *(IEC 61511 phase 4);*
- Training;
- Installation of replacement SIS *(IEC 61511 phase 5);*
- Commence cut over to new SIS *(IEC 61511 phase 5);*
- Plant daily meetings *(IEC 61511 phase 5);*
- Permit to work (PTW) *(IEC 61511 phase 5;)*
- Control Room Operator (CRO) interfaces *(IEC 61511 phase 5);*
- The cut over work *(IEC 61511 phase 5);*
- Testing and sign off *(IEC 61511 phase 5);*
- *Ongoing operations and maintenance (IEC 61511 phase 6);*

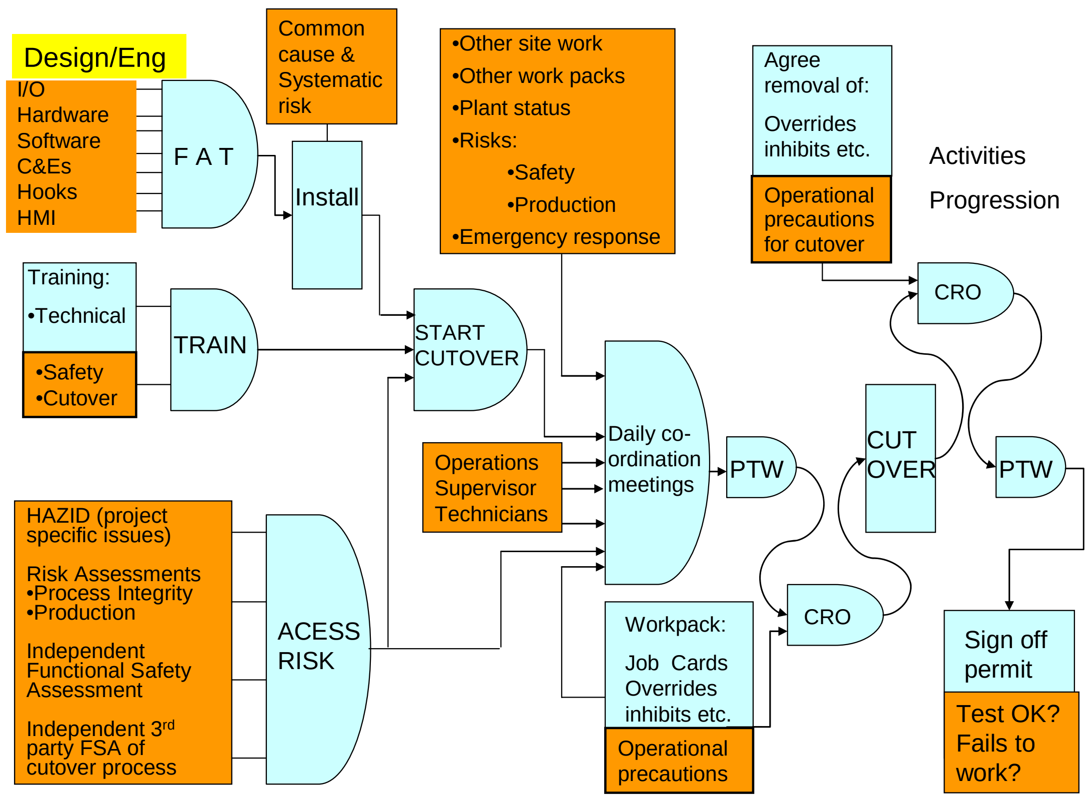

Figure 2 – Live SIS Replacement Project Route Map

The following sections highlight some of the difficulties, pitfalls and issues surrounding the most significant life-cycle phases when changing out a SIS whilst the process remains operational.

1. Hazard and risk assessment

The opportunity may be taken to add functionality for outstanding plant changes and this will require specific hazard analysis and risk assessment to establish the functional requirements for additional SIF.

During the project development phase the risks involved in undertaking a live change out of a SIS must be clearly defined. This should involve a detailed hazard analysis to look into the impact that the project could have on the integrity of the facility due to systematic errors with respect to the SIS replacement specification, design and implementation.

Some of the typical systematic errors that have been encountered include failure to check that the secure power supplies can cope with two ESD/PSD and F&G systems running concurrently, during the time it takes to transfer all the functionality from the old to the new SIS, and failure to check that HVAC systems can cope with the additional heat dissipation load in the equipment rooms during the changeover period. The latter having the potential for significant electronic component temperature stress related issues that could cause problems later.

Hazard analysis should also highlight specific hazards and associated risks during the physical transfer of I/O from the old systems to the new systems, as transfer will result in the repeated loss of ‘key’ safety functionality for periods of time. This may require the project to use special risk reducing measures during the physical transfer.

Thus there are some significant assessments that should be made as follows:

- Whether the integrity of the facility is compromised and, if so, how;
- Whether the SIS functionality is identical or if changes to the Cause and Effects are proposed;
- Whether like-for-like functional testing/comparison is going to be possible;
- Whether the I/O transfer is true like-for like;
- Any changes to the actual I/O interfaces;
- The physical constraints for moving I/O such as terminal connectivity;
- The risks involved with the physical disconnection and reconnection such as the implications of a spurious closure of a primary process valve;
- The risks due to the unavailability of functionality during the physical changeover;
- How to avoid loss of functionality whilst moving physical I/O;
- How to keep operations informed about what functionality is on which system;
- What to do in the event of a real facility emergency if work is in progress.

Unfortunately many of the above issues are often not considered, due to the misty like-for-like approach, or they are only considered at the last minute giving no time to plan any strategy.

2. <u>Allocation of Safety Functions to Protection Layers</u>

In theory the majority of the SIS functions should already be defined from the existing system, and only those functions that are added at the upgrade opportunity as part of plant change requirements, should need to be considered.

Even though the bulk of the functionality will most likely be identical, the opportunity may well be taken to rationalise the complexity of the cause and effect logic. This should only be done following a proper assessment of the changes, and all simplification needs to be backed up with SIL studies to determine the extent and suitability. Hazard analysis may also be required to ratify the changes for a complete audit trail. All too often the SIL determination has not even been completed for the original system configuration before the rationalisation is undertaken. In driving a project to satisfy timescales and deadlines, the audit basis for changes can be easily lost, and this is a major concern.

As discussed, SIS change out is often argued as a like-for-like replacement basis of the SIL requirements of the system/s. Thus the like-for-like could simply be re-implementing inadequate SIF design. Even where SIL studies may have been previously implemented, experience has revealed that few SIS change out projects are prepared to review or undertake the PFD or hardware fault tolerance calculations for the new systems, even though the whole logic solver will change, filed elements may be changed and very often the I/O interfaces are modified as well.

Rationalisation of SIS functionality within the replacement SIS also impacts greatly on the application software configuration, making it difficult, if not impossible, to check functionality of the old and replacement SIS configurations on a like-for-like basis. The whole configuration must therefore be checked by comprehensive factory acceptance testing (FAT).

3. Safety Requirements Specification for the SIS

The safety requirements specification for a replacement SIS will depend on a number of factors such as:

- How close the replacement system design is to the original;
- Te as built status of the cause and effects
- Whether the cause and effects are to be replicated;
- Whether the cause and effects have been rationalised;
- Whether the field elements will remain the same;
- The suitability of the current measured values and ranges;
- The suitability of the current set points;
- Changes to the basic process control system (BPCS) and its interfaces;
- Whether a SIL determination study was done for the original system;
- Whether the design calculations exist for original system;
- The basis on which the existing system test strategy was developed.

If there are genuinely no changes to the SIS safety requirements specification then the replacement system can adopt the same functionality and specification as the original system, providing all the points listed above are covered.

In reality though, there will most likely be some functional differences, and the main issues that can cause problems in defining these will be the availability of the most up-to-date cause and effects, and configuration details for the measured variable settings.

In some cases, the as built status of the cause and effects may be suspect, particularly if there has not been tight change control during the operation of the original SIS. There may well have been significant changes to the cause and effects, over the operating life of the original system, which are not well documented. In addition, there are likely to be changes that have been waiting to take advantage of the opportunity afforded by the replacement SIS. Thus configuration of the replacement SIS could be significantly different from the original.

Examination of the measured variable ranges and set point settings all too often reveal some very suspicious data such as rising set points that are set 100% full scale or falling set points that are set at 0% full scale. Where set points have been set at extreme range values it is a clear indication that there has probably been a lack of configuration control and that they were set like this to avoid nuisance trips with little regard to the integrity issues.

SIS replacement project teams are usually only interested in replicating the current calibration and set points. By simply copying the configuration in this way all bad settings will also be replicated. It is essential that all measured variable ranges and set points are checked and validated as being appropriate with input from the site process engineering group. However, experience shows that this is seldom in the ‘project’ scope.

Replacement SIS projects often take the attitude that ‘we are only replacing the logic solver’ when they lack the fundamental SIL requirements information to determine if the capability of the logic solver is adequate. SIS replacement projects seldom include SIL determination studies in their work scope so that this situation can be recovered. There are other projects where they make no reference to existing SIL studies.

More close examination of a replacement SIS project scope may also reveal that a number of initiating devices or final elements are also to be replaced or upgraded, and are not in fact like-for-like. These changes can also introduce significant modifications to the communications architecture between the SIS CPU and the field.

4. Design and Engineering of the SIS

The extent and detail of the design and engineering scope will also be dependant on the bulleted factors highlighted in Section 3 above.

A replacement SIS is often undertaken simultaneously with a significant upgrade to the basic process control system (BPCS) and this can have a significant impact on the human machine interface (HMI), graphics and communications. All of these factors must be fully detailed and understood. The operators of the BPCS and SIS need to be fully involved in the design and development of the HMI and the project must be prepared to provide training as part of their scope.

A difficult situation will develop with the design of the specific safety instrumented functions connected to the new logic solver if the SIL information is not made available. The adequacy and requirements of the architecture for the field elements cannot be determined and the probability of failure on demand (PFD) calculations and hardware fault tolerance checks cannot be performed.

So many projects that use the 'like-for-like' arguments have no intention of revisiting or undertaking the required design calculations and yet there may be fundamental differences.

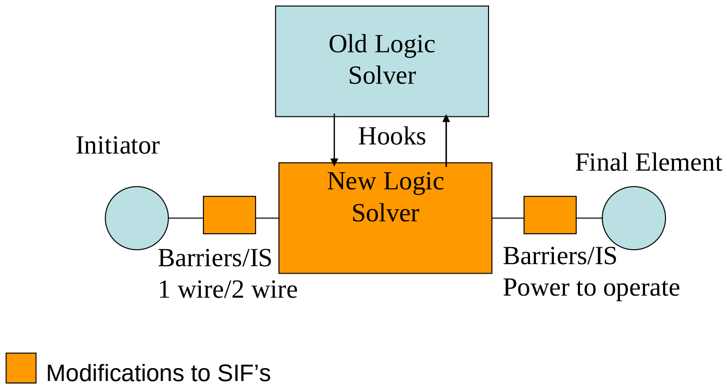

Figure 3 - Example (1) of I/O Issues

Figure 3 shows an example where a project was introducing some fundamental I/O interface modifications by changing the SIS logic solver. Not only was the most significant element being the logic solver changed, which impacts on every SIF, but the old SIS used barrier diodes, power off to operate, and 1 wire connections whilst the replacement SIS was to use intrinsically safe (IS) interfaces, power on to operate and 2 wire connections.

Figure 4 shows an example where the change of SIS logic solver required significant changes to the I/O communications interfaces between the CPU and the field elements.

In both these examples the respective project teams considered the replacement of the SIS logic solver to be like-for-like and in neither case had they any intention of undertaking any SIF PFD calculations to determine if the changes had any impact.

As far as the client was concerned, the SIS shown in Figure 4 was certified to a SIL 3 capability. They failed to appreciate that this was only for the logic solver and did not include the serial and Ethernet communications network which had no certification or any available reliability data. In addition no thought had been given to the implications on SIF PFD, the speed of response, systematic failures, common cause or random failures that might have been imposed by the I/O communications interface.

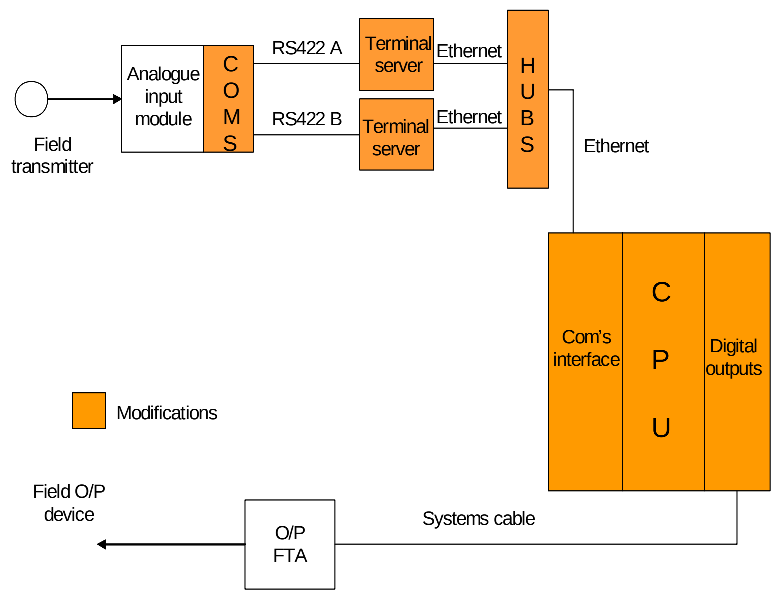

Figure 4 – Example (2) of I/O Issues

4.1 Factory Acceptance Testing (FAT)

The objectives of FAT for a project intending to implement the live replacement of a SIS must be far more comprehensive and extend much further than the testing of logic solver and associated software as indicated in Part 1, Section 13 of IEC 61511. When site installation is undertaken this will involve connecting directly with existing field elements while the process is live. So FAT must also embrace elements of validation, site acceptance testing, testing of all the HMI and I/O interfaces, testing of I/O and should include simulation or physical tests for all interfaces and field element types.

The boundaries and content of FAT must be planned to cover:

- All interfaces with other systems such as BPCS and Fire and Gas systems;
- All human machine interfaces;
- Content and accuracy of all graphic displays;
- Checks for compatibility of input field element types with measurements, ranges and set points;
- Checks for compatibility for all output field element types such as solenoids, switch gear etc.;
- A full check of the cause and effects for every initiator and associated final element/s;

- Clock synchronisation of multiple clocks;
- Logic solver performance;
- Input to output performance;
- Application software testing.

FAT must be comprehensively completed if the replacement SIS logic solver is to dovetail into a live process without compromising the integrity or production.

In Figure 5 a simple outline of the FAT boundaries is shown for a typical ESD/PSD related SIS replacement and shows how the scope of FAT should extend right out to the I/O field interfaces with simulations for the field devices.

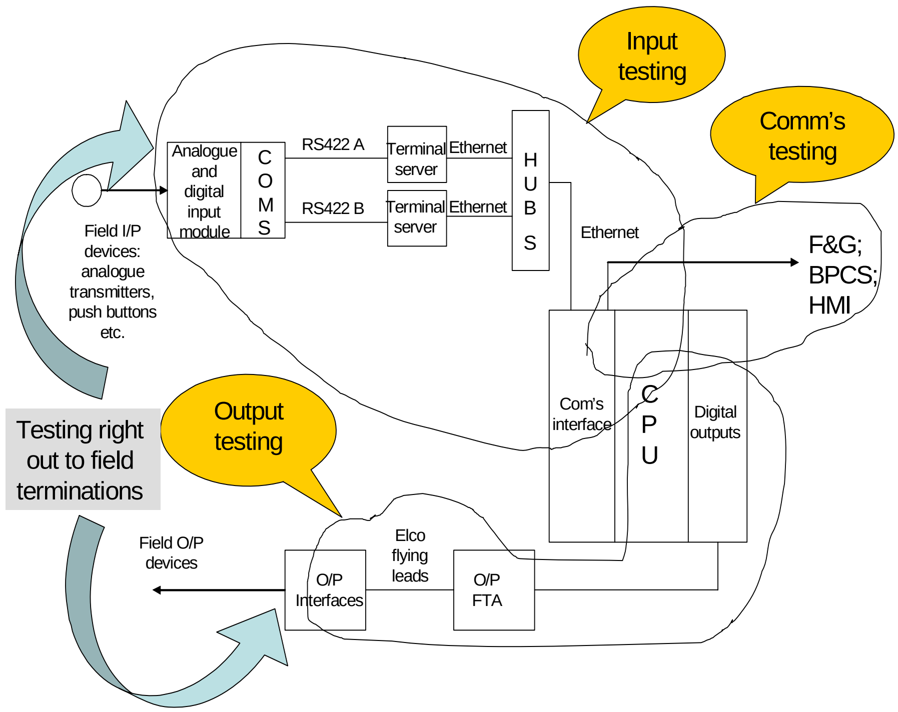

Figure 5 – FAT Boundaries for a Typical ESD/PSD Replacement SIS

A similar approach is required for Fire and Gas systems or any other functional safety related unit of logic.

Taking testing out to the extremity of the I/O boundaries as shown in Figure 5 will ensure as seamless as possible integration with the field elements, which are all that remain of the old SIS in this example.

All faults detected during FAT must be logged and cleared before the system is shipped.

5. Installation, Cutover, Commissioning and Testing

The project should have checked that secure power supplies and HVAC are capable of supporting both the old and the replacement system for the changeover period. In addition there has to be sufficient space to install the replacement SIS before the old system is destructed. Fundamental points but all too often missed by some projects that then run into power supply issues, for example, when it is far too late in the project.

Another fundamental item that is often overlooked is whether the actual terminals (e.g. Klippon terminals), associated with the SIS outputs for all normally powered field elements, can support the connection of a 24 Volt temporary supply to hold the field element in the powered state whilst the wires are physically moved (i.e. cutover) to the new system.

5.1 Installation

The replacement SIS is therefore initially installed along side the old system but without any I/O connections to the field elements. This will probably require special software programs or ‘hooks’ to be installed to transfer data between the two systems.

5.2 Cutover

The process of cutover is divided up into specific work packs which need to take cognisance of the following:

- Other site work in progress;
- Other work packs associated with cutover;
- The plant status i.e. stability and operational plans for the period;
- The associated risks with respect to safety and production;
- The required emergency response procedures specific to each work pack;
- The overrides/inhibits that are required to perform the work;
- Specific operational precautions required during the work.

The work packs form part of the daily site meetings which are held to discuss operational, maintenance and construction plans for the day. These meetings must examine the work content, the safety risks, the production risks and make proposals for any special operational precautions that will need to be put in place e.g. additional diligence with alarm monitoring, the permanent display of specific graphics for the area and what communications is to be established between the CRO and the technicians undertaking the cut over work.

The safety integrity risks should be readily established from the risk analysis undertaken as part of SIL determination, since the consequences of the function failing to work after cutover are the same as the consequences of failure used in the SIL determination analysis. Unfortunately, as stated earlier in this paper, there are projects that do not have this information to hand.

All cutover work should form part of the permit to work (PTW) process and the control room operator (CRO) must be fully involved in the cutover process since he/she must agree to an override/inhibit being put in place and then removed at the end of the job. The override/inhibit status must be logged by the CRO and form part of shift handover information.

There is a serious potential for loosing site of which SIF is functionality connected to which system. With many hundreds of I/O to change over, the cutover process will take a number of weeks and must have detailed planning and regular status updates. It is important to have operations representatives on the project team to act as co-ordinators between the project and operations on a continuous basis.

Transfer of field elements will usually start with the output field devices i.e. the SIS final elements, whilst all the inputs remain connected to the original system. This is why there needs to be software hooks between the two systems to ensure that both systems can operate all the final elements for any input initiation. The normally energised final elements for an ESD/PSD system have to remain powered by a temporary power source, whilst the wires are physically transferred. Thus the unavailability exposure time needs to be kept to an absolute minimum. It is also at this stage where any momentary loss of supply to a final element will result in a spurious closure. The risks associated with this should be assessed for each final element.

Wherever possible, offline or spared equipment should be transferred first, to minimise the risks, and then swapped over to become on line so that their partners can be transferred without risk.

Power on to initiate devices for systems such as fire and gas do not carry the risks of spurious initiation, and end of line monitoring facilities in the SIS should indicate a successful transfer.

The initiators are inhibited on both SIS prior to transfer and a simple check on measured value before and after transfer provides a preliminary indication that the transfer has been successful.

5.3 Commissioning and Validation Testing

Providing FAT was comprehensive, as discussed earlier, the project should have taken full advantage of the off line opportunities afforded at this stage to reduce on site validation. In any case, there will be significant difficulties in undertaking fully functional end-to-end testing of the majority of functions, with the process operational, so on site validation testing is most certainly going to be compromised and is forced to take a partitioned approach.

Starting with the field elements, operations need to be able to demonstrate that routine tests for ESD and Fire and Gas initiating devices and all final elements have been completed during the proof testing schedule for the original system. This will then have proven the functionality of all the field elements at the last test. The questions that remain are how comprehensive this has been and how dependable the records for this are?

FAT should have tested the SIS logic, all I/O communications and all the I/O using simulation up to the field termination.

Thus the purpose of validation for each field input and output is to ensure that they are connected to the correct I/O termination and that they remain functional. However there are significant differences between what can be achieved with validating Fire and gas and ESD/PSD systems on a live process plant.

5.3.1 Fire and Gas Systems

The compatibility of any replacement detectors, such as replacing catalytic type gas detectors with infra red (IR) gas detectors, should have been covered at FAT. All remaining original detectors, that are not replaced, should have been subject to routine testing, and FAT should have checked the new SIS with simulated inputs and ensured that all inputs have the appropriate engineering units, scaling, ranges and set points.

The objective of validation in the field is to ensure that the detectors are connected to their assigned input terminals and that they are being read correctly by the replacement SIS. Each detector should be tested, following changeover of the physical wiring, with simulated gas or smoke etc. Providing calibration was done at FAT, the site test does not have to be a full calibration routine, but should be designed to validate that the detectors are connected to the correct input, and that they are properly wired and operational.

Digital type inputs from break glass units and push buttons etc. should have been subject to routine testing. FAT should have checked the SIS with simulated digital inputs and ensured that all inputs activate appropriately. Thus the objective of validation is to ensure the initiating devices are connected to their assigned input terminals and that they are being read correctly by the replacement SIS. To confirm this, the line monitoring for each initiator should be checked, following changeover of the physical wiring. The test is intended to validate that the digital type inputs/initiators are connected to the correct input. Use of input inhibits can also aid confidence in validating digital inputs.

All Fire and Gas outputs in the replacement SIS should have been tested during FAT. The objective of validation is to ensure that the power-to-activate devices are connected to their assigned input terminals and that they are being line monitored correctly by the replacement SIS following transfer of the wiring. If it is possible to lock off deluge release and dispersant release devices, to prevent a release, then it is recommended that outputs tested by activation from within the replacement SIS HMI wherever possible. If F&G is being changed over during a shutdown, then it is recommended that all energise to activate output are tested.

5.3.2 ESD, PSD and EDP Systems

All transmitters and analogue measurement devices should have been subject to routine testing and calibration. FAT should have checked the replacement SIS with simulated inputs and ensured that all inputs have the appropriate engineering units, scaling, ranges and set points. The objective of validation is therefore to ensure that the transmitters and sensors are connected to their assigned input terminals and that they are being read correctly by the replacement SIS.

It is recommended that the measured value of each transmitter, sensor or analogue device is noted and recorded prior to changeover, and then checked against the replacement SIS reading following the physical changeover of the wiring. Wherever possible, it is recommended that operations move the process variable up or down by about 10% and that the measured value is checked to ensure that it tracks the change accordingly. Compare with process control variable. The input will have an override applied during this test. The test is intended to validate that the transmitters are connected to the correct input, and that they are properly wired and operational.

Digital inputs from normally closed contacts and push buttons etc. should have been subject to routine testing. FAT should have checked the replacement SIS with simulated digital inputs and ensured that all inputs activate appropriately. The objective of validation in the field, at the time of changeover, is to ensure the initiating devices are connected to their assigned input terminals and that they are being read correctly by the replacement SIS.

It is recommended that each digital input has an override applied and is then is activated from the field wherever this is possible. The test is intended to validate that the digital type inputs/initiators are connected to the correct input, and that they are properly wired and operational.

The transfer of normally energised outputs is perhaps the hardest of all transfers and this aspect has already been discussed. It is assumed that all final element devices such as valves and motors contactors will have been subject to routine testing. All outputs in the replacement SIS should have been tested during FAT. Thus the objective of validation in the field, at the time of changeover, is to ensure that de-energise to activate devices are connected to their assigned input terminals and that they are being correctly powered and can be de-energised by the replacement SIS.

It is recommended that all solenoid valves are trip tested, by de-energising them through the replacement SIS HMI if possible with:

- Prior risk assessment for each valve and instructions in the event of a platform emergency;
- Normally open ESD, PSD and EDP valves mechanically locked open;
- Normally closed ESD, PSD and EDP valves mechanically locked closed.

The test is intended to validate that the output devices are connected to the correct output termination, and that they are properly wired and operational.

For electrical drives it is recommended that off line spared equipment is tested such that:

- Each offline contactor is physically trip tested;
- The offline machine changed over to become on line;
- The contactor test is repeated for the drives that have just become offline.

Where electrical drives have no spared equipment then this will need more thought and the earliest shutdown opportunity should be taken to carry out the trip test.

6. Operations and Maintenance

Operators should form part of the project team and should play a key role in every phase of the project. Their training on the new SIS should begin at as early stage as possible so that they can appreciate the technology and add value to the design and development. They should be fully participant in the HMI interface development including the design of the graphics, FAT and co-ordination of installation and cutover.

Maintenance personnel should be trained in the new technology at an early stage to enable them to be involved in the installation commissioning and validation phases so that they become fully familiar with all aspects of the hardware and application software functionality.

The ongoing test and maintenance strategy should naturally formulate through the SIS design and SIF specific PFD calculations. However, projects are seen to proceed with no basis for setting test and maintenance strategies apart from the like-for like argument which is so often flawed.

Conclusions

Replacing a SIS is always going to be safer and less risky when the process is shut down. This removes most of the associated integrity and production issues as well as the additional stress related to working on integrity systems on a live process. The time taken and the project costs will also be considerably less. Full commissioning and validation will also be possible before the process starts up again.

The demand for oil and gas and current high prices drive operators to justify planned replacement of SIS without stopping production and this is always going to create integrity and production related issues. Projects must ensure that the risks are fully identified and evaluated and they should not shortcut the IEC 61508[2] and IEC 61511 standards by arguing like-for-like since this is so often far from the mark.

Providing projects follow the route map set out in Figure 2, it will be possible to achieve the replacement of a SIS on live process plant. By following these steps a replacement SIS can be seamlessly dovetailed into a live process plant with minimum loss of integrity and avoidance of lost production, but the required attention to detail will result in far more headaches for the project during the whole process.

However, SIS replacement while a process is shut down should always be the preferred option.

References

[1] BS IEC 61511, 2003, Functional Safety: Safety Instrumented Systems for the Process Industry Sector.

[2] BS IEC 61508, 1998-200, Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems.

Biography:

Clive has over 38 years experience in the petrochemical industry with offshore and onshore plants experience, and retired from Shell UK Exploration and Production in 2000 where he was Head of Automation and Control. He is now a Director of C&C Technical Support Services Ltd, which specialises in the application of the IEC 61508 and IEC 61511 standards, and was a founder Director of the CASS Scheme Ltd for conformity assessment to IEC 61508. He chaired the UK Offshore Operators Association (UKOOA) working group that produced the UKOOA Guidelines for Instrument-based Protective Systems, as an offshore sector interpretation of IEC 61508. He has a B.Sc. and M.Phil in Control Engineering, is a TÜV certified Functional Safety Expert, a Member of the IET and currently chairs the Institute of Measurement and Control Safety Panel.

Contact Details:

Clive Timms
C&C Technical Support Services Ltd
Strathayr
Rhu-Na-Haven Road
Aboyne
Aberdeenshire
AB34 5JB
U.K.

Tel: +44 (0) 1339 886618
Fax: +44 (0) 1339 885637
Email: c.timms@ifb.co.uk
Web: www.silsupport.com