Software Tools for the Lifecycle Support of Safety Instrumented Systems

Author: Clive Timms
C&C Technical Support Services Limited

Abstract

Since the publication of IEC 61508 (1) and IEC 61511 (2) there has been a steady increase in the number of PC based software tools developed to aid compliance. These come with a wide range of both capability and price, but carefully selected tools are considered the most appropriate way forward for ensuring lifecycle support of safety instrumented systems (SIS). Software tools are not just the realm of the design engineer, and this paper draws on experiences to demonstrate the benefits that can be realised by SIS engineering practitioners and end users. This paper will also discuss configuration aids for programmable logic controllers (PLC) but it will not cover PLC software or computer aided design (CAD) software.

The range of available tools

Tools are now available to support all phases of the lifecycle and it is important to note that the phases that usually attract the most focus range from Hazard and Operability (HAZOP) through to SIS design, but these only represent 25% of the complete lifecycle. The remaining 75% of the lifecycle phases, as shown in Figure 1, need just as much care and consideration for achieving compliance.

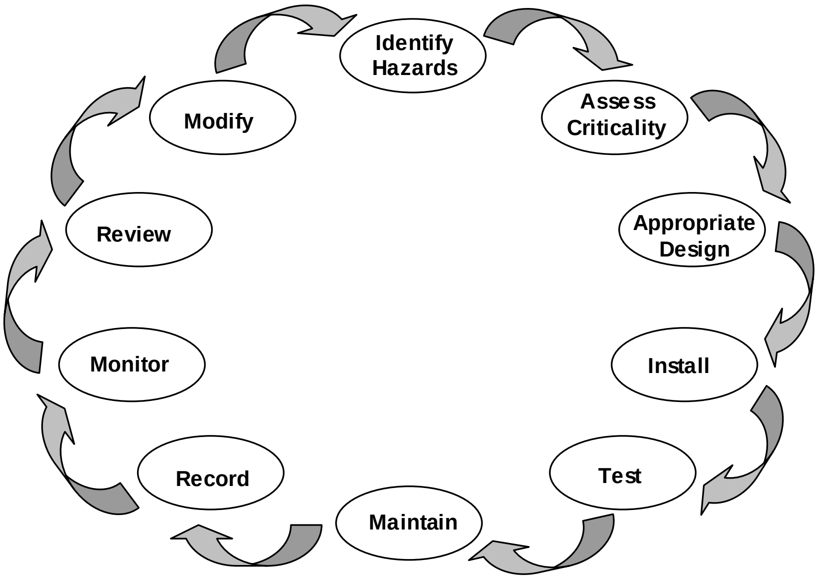

Figure 1 – SIS Lifecycle

Just like in any other form of engineering, those involved in the SIS lifecycle including development, design, installation and ongoing support need to have an appropriate set of tools to help the whole process and to aid compliance with the IEC 61508 and sector specific standards such as IEC 61511 for the process sector. It should also be incumbent on these key people to produce their respective deliverables with the most efficient use of their time. The reality is that designers seldom embrace the benefits of using software tools or pass these benefits on to the end user. End users should be aware of the benefits that can be achieved with the aid of a good suite of software tools including:

- A more efficient approach HAZOP;
- Significant reduction in the time taken for SIL determination exercises;
- Greater visibility of recorded data for audit and regulation compliance purposes;
- Interactive and simplified design processes;
- Optimal selection of the design elements
- Greatly reduced design time;
- Validation and security of design calculations;
- Optimisation of design against test and maintenance strategies;
- More effective risk reduction for identified hazards;
- Easier design control and change control;
- High integrity data handling and recording;
- Improved test and maintenance recording for ongoing review;
- Feedback from test and maintenance to reliability data collection;
- Improved life cycle management of SIS.

Examination of some of the main activities in the lifecycle will reveal more information about what is required from the different phases of the lifecycle and how these can be improved with the appropriate software aids.

Identifying Hazards- HAZOP Review

HAZOP reviews and a number of variances have been widely introduced since the early seventies and the HAZOP review process is the key to achieving compliance with the European Union Seveso II Directive [(3)] as this requires an operator to identify all hazards.

A HAZOP review is undertaken to systematically analyse every part of a process by lines and nodes to determine if deviations from design intent could result in undesirable consequences. The objectives and prime deliverables from a HAZOP review are the identification of safeguards and actions (Figure 2) which will reduce the risk of an occurrence of the undesirable event.

This requires large numbers of records and significant effort to manage through to close out.

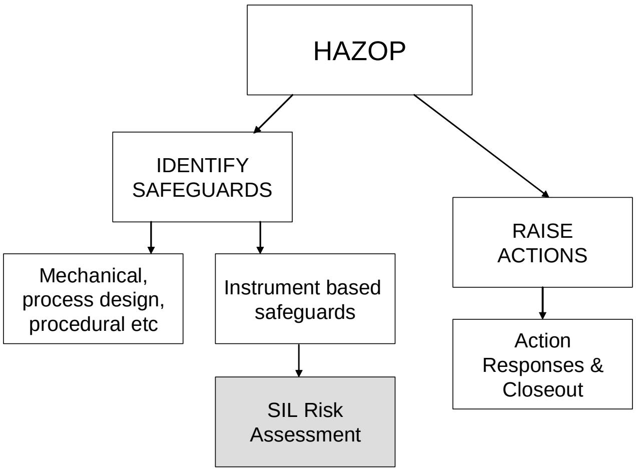
HAZOP
IDENTIFY SAFEGUARDS
RAISE ACTIONS
Mechanical, process design, procedural etc
Instrument based safeguards
SIL Risk Assessment
Action Responses & Closeout

Figure 2 – HAZOP Deliverables

Traditionally handled as a paper exercise it can produce shelf after shelf of documents which are often difficult to reference, hard to manage and tiresome to update, whilst producing HAZOP reports can be very time consuming. However, significant improvements can be made to reduce the effort involved providing the right kind of HAZOP tool is selected. This should then aid the flow of information from the review input to the output deliverables. The market for HAZOP orientated software tools is extremely competitive and there are some good tools around and some very poor examples as well, so what should the practitioner be looking for?

The following bullet points list some of the primary functionality that should be available in good HAZOP tool:

- The ability to capture the HAZOP team for each assessment;
- Preformatted Worksheets and the ability to clone them;
- Line , node and adjacent line/node tracking;
- Assigned severity by 'cause/consequence pairs';
- The ability to assign different types of safeguards;
- The ability to cross reference common safeguards between lines/nodes;
- The ability to flag instrument based safeguards for SIL determination;
- The raising of actions during HAZOP (a direct e-mail option is very useful);
- Facilities to manage action responses and HAZOP close-out;
- Facility to assess the criticality of safeguards using a (configurable risk matrix;
- Modular reporting structure to allow different levels of user defined reporting;
- Export of HAZOP findings to spreadsheet or through database exchange.

HAZOP can be very tedious for all concerned, but there are many opportunities to make the whole process far more effective and less time consuming for the both the chairperson and the review team. Experienced chairpersons who have adopted software tools have seen a 50% reduction in the time taken to undertake a typical HAZOP.

This can be achieved right from the outset by dramatically improving preparation time by having configurable parameter glossaries which then form drop down selections for fluids, guidewords, causes, consequences, measurement types, measurement units, parameters, priorities etc. Using these configurable parameter sets for each line or node removes unnecessary review work. Having pull down glossary selections incorporated into structured worksheets significantly reduces data input time. The ability to clone worksheets to another line or node is another major advantage. In reality, very few HAZOP chairpersons are good typists and a HAZOP secretary is often used to take records. Feedback from HAZOP chairpersons who have adopted a software tool indicates that they can be far more focused on the actual detail of the assessment when the data input is made easier. It also removes the need for a secretary. Data input is enhanced if the laptop, used for the recording process, is linked to a projector so that the whole team can view the worksheets.

Raising actions during the HAZOP review meeting is the one of the main activities. If the software facilitates the emailing of actions, directly from the HAZOP review, by use of an automatically formatted action form, then this significantly reduces the burden on the chairperson and further reduces the need for a HAZOP secretary. In addition the action party knows exactly what to expect in his/her email inbox. Action responses also need to be managed for formal close out and this is far more effective and easier to track within a tool.

Allocating risk reducing safeguards which can be mechanical, instrument and procedural is another main activity and a database platform will make searching and cross referencing simpler and quicker, especially for those safeguards allocated to multiple lines/nodes. The instrument based safeguards, or Safety Instrumented Functions (SIF) as they will become, will need to be risk assessed by a Safety

Integrity Level (SIL) determination process. The user should look for tools which offer a direct exchange or export of SIF data between HAZOP and SIL determination.

Producing HAZOP reports can be a gargantuan and time consuming task, but this can be virtually eliminated if the tool has a modular reporting feature.

We have only looked at a few of the main areas in which a well structured HAZOP tool can bring improvements but, to safety engineers engaged in the detail of a large HAZOP review, many additional advantages soon become obvious.

Risk Assessment - SIL Determination

SIL determination is a risk assessment process and it is not the intention of this paper to bore readers by taking them through the whole process but, as with HAZOP, it will look at the areas where software based tools can bring advantages. There are numerous ways of undertaking SIL determination and examples include Fault Tree Analysis (FTA), Risk Graphs, Risk Matrices and Layers of Protection Analysis (LOPA). Whatever the favoured method, the objective of SIL determination is to assign an actual integrity level to an instrumented protective function.

Since the IEC 61508 standard provides a direct correlation between an assigned integrity level and the risk reduction that must be achieved by the instrumented protective function the practitioner needs to determine if this reduction is sufficient. This also has implications within European legislation for demonstrating that risk has been reduced to as low as reasonably practicable (ALARP).

Risk assessment is in many ways a more detailed hazard assessment and considers the consequences of an unwanted hazardous event and the likelihood that it will occur. It makes a detailed analysis of the causes and consequences and requires records to be made of the whole thinking process. It will need also to reference the HAZOP findings, meet the corporate tolerable risk objectives and provide an audit trail for the outcome.

This can all be achieved as a paper exercise, but it can be a very unwieldy and less than efficient approach that produces a mass of documentation which is then hard, if not impossible, to maintain. Practitioners who have used both paper and suitable database based risk assessment software tools will know that the effort involved in SIL determination can be reduced by more than 50% (N.B. the author includes spreadsheets as a type of paper approach due to their low integrity and ease of corruption). In addition, if the application runs on a database platform, it should be possible to sort the data on any stored parameter or combination of parameters which can then be cross referenced by useful attributes such as equipment type or plant area. By their nature, database files are easy to maintain and offer high integrity data by following the simple backup formalities.

So where does a software application provide the gain? The user should look for the following features:

- The ability to capture the team for each risk assessment;
- The ability to set user defined tolerable risk criteria;
- Client configurable FTA, risk graphs, matrices or LOPA;
- Calibration of the preferred risk assessment method;
- Facilities to handle safety, asset and environmental assessments;
- Records of drawing references;

- Functional description recording;
- Design purpose recording;
- Consequences of failure recording;
- Records of risk reduction measures;
- Comparison of risk reduction with tolerable risk criteria;
- Narrative record keeping to support all risk reduction claims;
- Cloning facilities to reduce input for similar assessments;
- Facilities to raise actions (a direct e-mail option is very useful);
- Facilities to manage action responses and close-out;
- Data exchange with HAZOP;
- Data sorting;
- User configurable reporting options;
- Export of findings to spreadsheet or through database exchange.

LOPA deserves a special mention as it is rapidly becoming a popular and often the preferred method for undertaking a SIF risk assessment. It is a relatively thorough process which links perfectly with HAZOP by analysing scenarios based on every possible cause for a specific undesired consequence (i.e. cause/consequence pairs) and then determines what risk reduction and mitigation can be claimed for each cause.

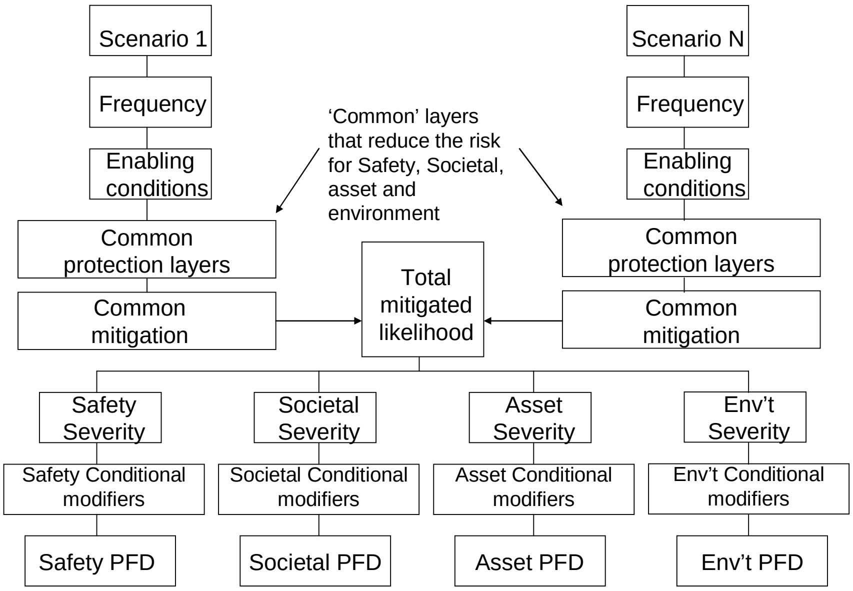

Figure 3 – LOPA Flow Diagram

LOPA practitioners will know from experience that the number of worksheets rapidly increment when multiple cause/consequence pairs are analysed for on site safety, societal, asset loss and environmental consequences. In addition, as the risk reduction is quantified for each layer and there will often be different risk reduction and/or mitigation associated with site safety, societal, asset loss and the environment. A typical LOPA flow diagram is shown in Figure 3 and this demonstrates the complexity of analysing and calculating risk reduction along the different parallel assessment paths.

This complexity constitutes a reasonably high risk of confusion for manual assessments on paper, in word or on spreadsheets, and is a prime example where available software tools can help to avoid errors in the SIL determination.

Like HAZOP, SIL determination can be a very tedious process due to its detailed analysis and record keeping. Engaging with a good risk assessment tool will make the whole process much slicker and quicker whilst actually improving the integrity, quality and presentation of the data.

The concerns and conflicting views expressed by some, from within the functional safety community, about over simplifying Safety Integrity Level (SIL) determination through the use of software aids are not founded, provided they are only used by practitioners competent in the application of IEC 61508. The risk assessment process will be as thorough and comprehensive as the practitioner makes it irrespective of software aids.

Realisation - Undertaking Safety Instrumented Function Design

Without being over simplistic, there are two types of Safety Instrumented Function (SIF) design types that most SIF design engineers will come up against. These are the simple SIF and the complex SIF. The simple SIF is the straight forward initiator, logic solver and final element as shown in Figure 4. It may contain MooN (i.e. M out of N) identical multiple devices for any of the three elements.

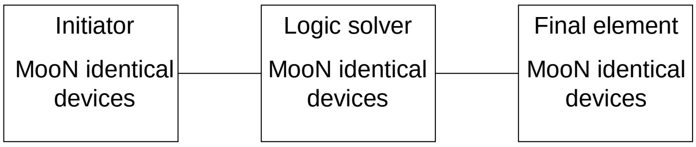

Figure 4 – Simple SIF

Where there are multiple devices for any of the elements then the effects of common mode failure will need to be considered. The simple SIF will constitute about 90-95% of the functions that have to be designed on an average process plant.

The complex SIF will probably constitute about 5-10% of the functions that have to be designed but calculating their probability of failure on demand (PFD) and optimising an appropriate test and maintenance strategy can prove very difficult. A complex SIF will most likely take the form of Figure 5.

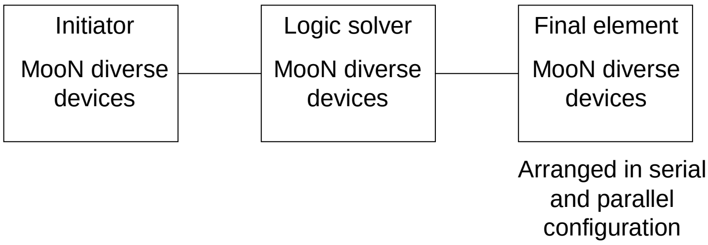

Figure 5 – Complex SIF

In a complex SIF the initiator may comprise a number of diverse measurement devices that are then voted MooN; so the reliability data will be different for each of the initiator types and the simple PFD calculation formula will no longer apply. Similarly, the logic solver may also be comprised of multiple and diverse unit logic. The most common problem area is usually the final element which may have multiple and diverse devices configured in a combination of serial parallel paths (e.g. in order to shut off flow to a vessel there may be a number of feed lines in parallel with a combination of valves in series as well as pumps).

For all types of SIF design the expectations of the end user will be:

- Minimal design time;
- An optimal design that meets the SIL requirements;
- Low cost design;
- Optimal test strategy;
- Low maintenance costs.

In order to meet the above expectations a basic software tool should incorporate the modules shown in Figure 6.

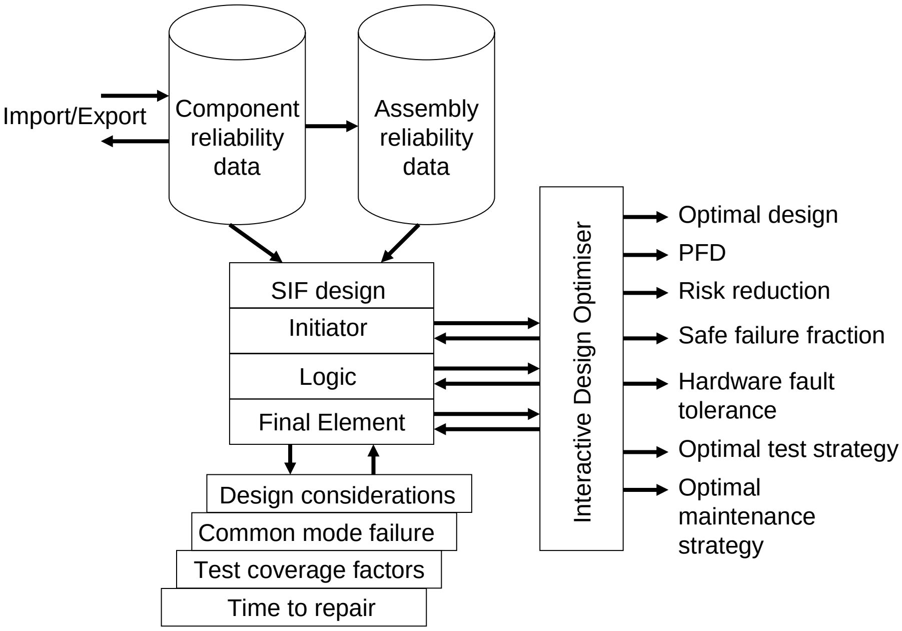

Figure 6 –SIF Design Tool Modules

Whatever the type of function, manually undertaking the calculations, even using a spreadsheet, can be time consuming particularly since a large number of iterations will need to be performed to establish the most optimal design along with corresponding test and maintenance strategies and this can often be displayed graphically to show available the degrees of freedom for the PFD to achieve optimum testing.

Avoiding miscalculations or data errors is of paramount importance for functional safety and this is an area of particular concern. The risk of error in manually performed calculations, particularly when large numbers of calculations have to be performed, is always going to be far greater than using of software tools specifically designed for the task. In order to add extra assurance, the practitioner should look for tools that have been independently verified to perform their calculations. Validated software will perform the calculations repeatedly and consistently. The question then arises of who will have verified hand calculations or a spreadsheet with embedded calculations?

To minimise the effort with hand calculated PFD computations the temptation to use an approximations such as:

$PFD_{avg} = 1/2 (\lambda \times T)$ for a single element (i.e. 1oo1)

Where: λ = dangerous failure rate, T = Test interval

Indeed, there are a number of commercial software applications only facilitate simple approximations for PFD calculations. A more appropriate and accurate calculation is the full exponential distribution:

$$\text{PFD} = 1 - \frac{1}{\lambda t}\sum_{j=0}^{r-1}\left\{ \frac{1}{(n-j)}\sum_{k=j+1}^{n} {}^{n}C_{k}\left[F(t)\right]^{k}\left[\overline{F(t)}\right]^{n-k} \right\}$$

Where: r = (n – m +1), n = total units, m = number of units required to operate

If PFD by approximation and full exponential distribution are plotted over a range of test intervals, as shown in the example in Figure 7, a significant discrepancy will be seen.

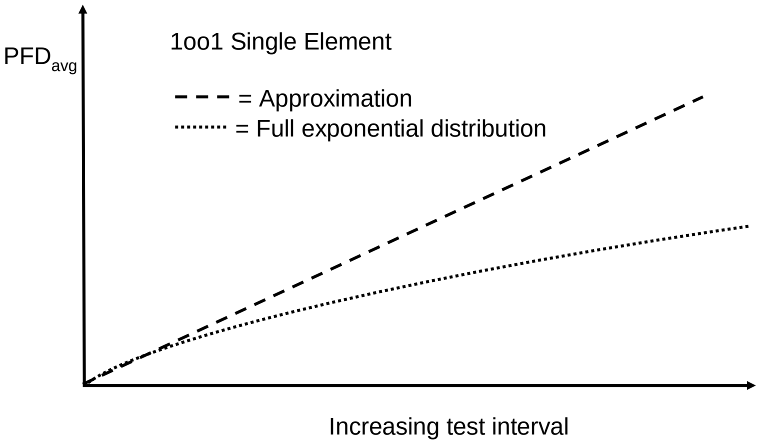

Figure 7 –PFD Comparison

This is because the ‘approximation’ is only valid when Lambda X T <<1. Voted elements e.g. 2oo3 result in even larger discrepancies. Producing large quantities of calculations by hand, or even by spreadsheet, involving the comprehensive exponential distribution is an onerous task with multiple opportunities for error, but it becomes a simple task using a well appointed software application.

The more complex the SIF, then the more reasons there are to look for tools which help reduce the likelihood of configuration or computational errors. Tools that can model a complex SIF using the architecture shown in Figure 5 provide designers with enormous flexibility at every stage of the process. Tools are now available that can start at a basic component level and solve the probability of failure for complex functions through simple modelling techniques. The architecture of a modelling tool for solving extremely complex Safety Instrumented Functions is shown in Figure 8.

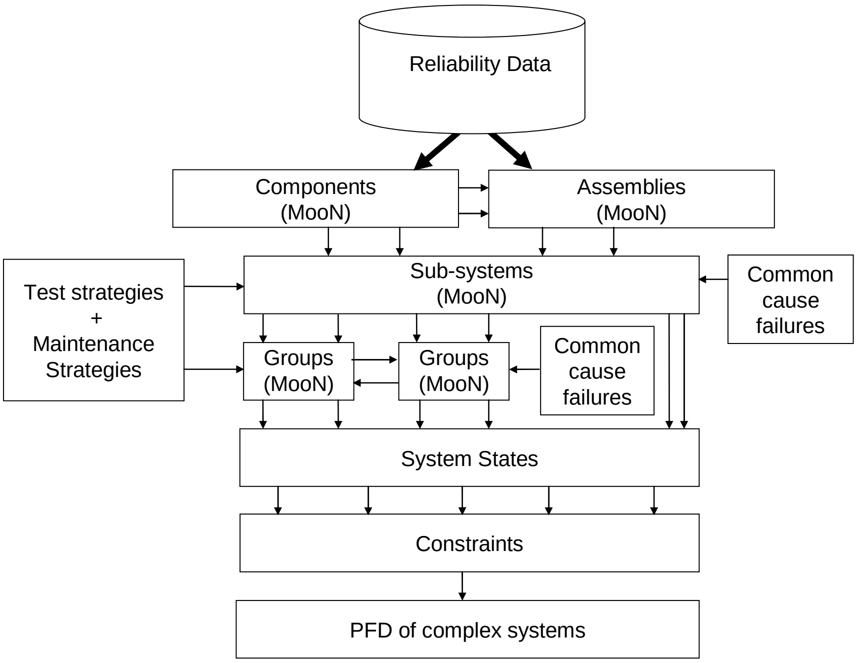

Figure 8 – Architecture of a modelling tool for complex SIF's

The tool facilitates the construction of a SIF from component level with MooN full exponential distribution, including separate common cause failure calculations, for multiple components, subsystems or groups of subsystems. This particular modelling application resolves the probability of failure on demand by analysing the success or failure of the subsystem states. Logical constraints can be applied for success or failure modes to automatically resolve the state table.

There are concerns and conflicting views within the functional safety community, about the 'dumbing down' or over simplifying of the approach to design through the use of tools. The fact is that competent practitioners will do a good job with or without tools. Nuclear scientists use computers as a routine for their design and analysis so it is not unreasonable for functional safety engineers to take full advantage of tools that can improve their performance and accuracy.

Optimal design can result in significant savings on fitted hardware and even the specification of the PLC which needs to be sourced. Experience with many design projects shows that these savings will normally offset the whole cost of the SIL determination exercise and the software tools by a large factor. In addition if it is not necessary to install certain hardware the ongoing operational burden of testing and maintenance is removed, making further savings throughout the life of the facility.

Configuration, Verification and Validation

Configuration is concerned with implementation of the safety instrumented functionality into the Programmable Logic Controller (PLC). Validation is about demonstrating that the end product meets the original design requirements. This is not the same as verification which is more about demonstrating that the design has been progressed through each stage in the appropriate manner.

Some interesting tools are emerging at a Safety Instrumented System (SIS) level that will now facilitate PLC configuration directly from a SIL determination and validate all the logical functionality from initiation through activation of the required final elements. Figure 9 shows how the system definition can be undertaken directly from a SIL determination to define accurate functional requirements removing the need for the time consuming and potentially inaccurate manual configuration. The defined functionality can be directly transferred or translated into IEC-61131 function block code where output drivers can then automatically generate vendor specific application code for the target PLC.

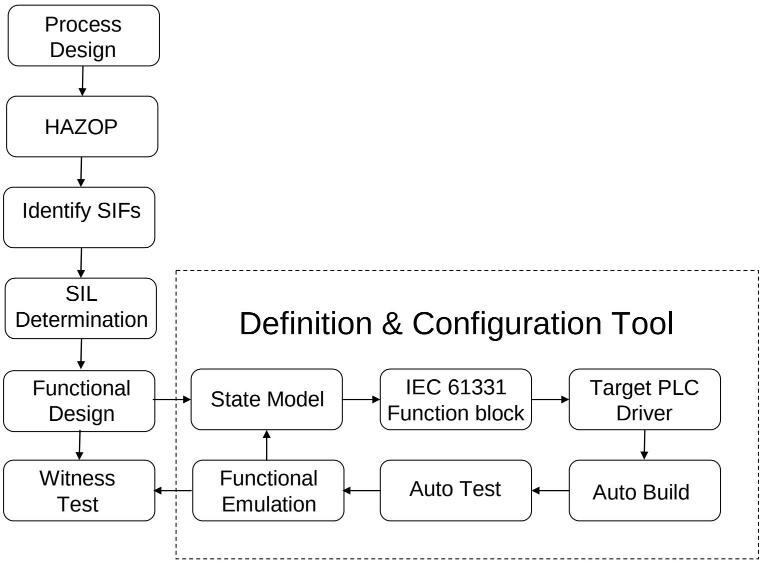

Figure 9 – Definition and Configuration Tool

Since the kind of tool shown in Figure 9 works on a state model concept it is very effective in emulating the functional logic for validation purposes.

Many older or as often called 'legacy systems' are based on relay ladder logic. When it is time to upgrade legacy systems then definition and configuration tools also offer distinct advantages of a manual re-configuration by incorporating a translation engine to convert the legacy system relay ladder logic. This will avoid the manual process of taking the existing cause and effect charts, which depends on them having been maintained to the as-built status, and the corresponding many hundreds of man-hours re-configuring the replacement PLC. The source relay ladder logic in the legacy system can be translated into IEC 61331 function block format and configured automatically to the host PLC as shown in Figure 10. As a bonus, a new set of documentation can be produced representing the actual as-built status.

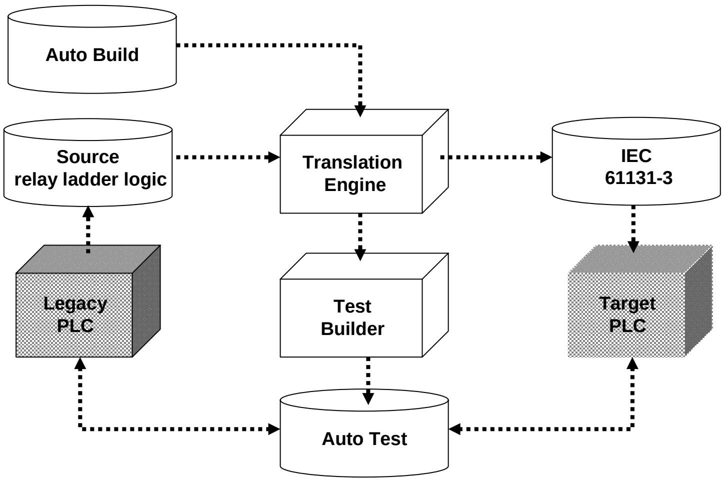

Figure 10 – Auto Upgrade for a Legacy System

Tools are also available that keep designers in touch with the Cause and Effect representation for the logic functionality which are so familiar to the SIF design fraternity. These also facilitate a direct automatic interface between SIL determination tools for PLC configuration and will generate active Cause and Effect matrices. These can be viewed on the target PLC and will actually activate dynamic graphical Cause and Effect responses to indicate the states of initiating 'causes' with the corresponding 'effects' or outputs to the final elements. These are extremely user friendly and equally useful for engineers and operations people, not just for a SIS build and validation but for ongoing operations.

Operations and Maintenance

Operations and maintenance tend to be the Cinderella phases of the lifecycle with all the glory going to risk analysis and design, but if a SIF is allocated an inappropriate proof test regime, and if testing is not properly carried out, or the equipment is not maintained correctly, then the probability of failure will increase and it is likely that it will fail much sooner than expected.

It is a simple fact of life that the large planning and accounting systems such as SAP do not readily facilitate the SIF requirements for testing, maintaining, monitoring and analysing results. Many operators have only small/moderate sized SIS requirements or they cannot afford the cost of something like SAP. SIS require structured reporting to record the testing and maintenance results to provide empirical reliability data. The resulting data should then be compared with the data used at the time of design to ensure that the SIF continues to meet the required SIL. This should be a continuous process right up until decommissioning. SAP users will know that the provision of customised features tends to be a very specialist and expensive exercise.

Some of the major safety systems suppliers have developed their own specific facilities for SIS operations and maintenance requirements as bolt-on features to their safety systems. These may be suitable, providing an end user wishes to be tied down to a major vendor. Low cost test and maintenance applications are now emerging to bridge the gap and help low budget operators fulfil compliance with testing and maintenance requirements and management.

The main objectives for managing testing and maintenance for any SIS user are:

- The ability to decide how which of the functionality is required for their business;
- That the design of any system is flexible enough to enable it to complement any existing maintenance systems or to provide a total maintenance management capability if required;
- The management of test and maintenance routines for any equipment (i.e. not just SIS);
- Provision of records and an audit trail of test and maintenance history;
- Reliability analysis based upon historical test results;
- The system can be operated stand-alone or can integrate seamlessly with other maintenance or design tools.

As part of the process the additional details required also include:

- A user defined library of test routine procedures and maintenance procedure methods;
- Assignment of appropriate test/maintenance procedures to any routine;
- Application of float and priority to routines;
- Base date for scheduling for individual routines;
- Defined 'look-ahead' scheduling time for maintenance planning purposes;
- The ability to 'roll up' multiple test types on the same equipment which are scheduled for the same date.

Any testing and maintenance will need to be carried out to a set of user defined Performance Standards for the equipment so as to ensure that the success or failure can be clearly determined. When these performance standards set up and embedded within the software they automatically flag all deviations from the performance requirements. If this is only monitored manually, then there is a high risk that the integrity of the safety functions will be compromised, particularly when the numbers start to run into hundreds and perhaps thousands. When a software based test and maintenance system is adopted then it can also aid strategy by incorporating pre-defined operational 'contingency plans' or risk assessments may be defined and reviewed by maintenance and operations staff to help decide the course of action on test failure.

Maintenance requirements are often risk assessed to provide operators with an appropriate strategy for maintenance effort and sparing. There are tools available for undertaking risk based maintenance (RBM) assessments, but these should not take precedence over the test and maintenance strategies calculated as part of the PFD for safety instrumented functions.

Conclusions

Hopefully, this paper will have highlighted some of the main areas where using software tools can aid compliance with IEC 61508, improve SIS integrity and confidence in the lifecycle management, whilst opening up opportunities for capital and operating expenditure savings. Many of the tool types discussed are very low budget in price and the payback can easily be achieved before the completion of one relatively small project.

It is up to the user to make their choice of which tools to adopt. However, the best in class tools are those that have been developed by engineers who are experienced practitioners of the standards.

There are concerns and conflicting views expressed by some, from within the functional safety community, about ‘dumbing down’ Safety Integrity Level (SIL) determination and design through the use of tools, but tools are only an aid and they should only be used by practitioners competent in the application of IEC 61508.

Questions have also been raised about the integrity of PC based software for functional safety based applications due to the considered low integrity of standard PC based applications. This is totally misguided when compared with the risks involved with manually performed calculations, and avoiding miscalculations or data errors is of paramount importance for functional safety. Tools are emerging which offer seamless data exchange and integrity from HAZOP, through risk assessment, design, PLC configuration and operating and maintenance, thus avoiding the errors that so easily occur in the manual transfer of data and configuration.

Software tools are not just the realm of the design engineer. There are extensive benefits that can be realised throughout the lifecycle by using tools as an integral part of safety management systems (SMS) to help improve the focus on regulation compliance, risk reduction and profitable safety.

References

1. BS IEC 61508: 1998. Functional Safety of electrical/electronic/programmable electronic safety-related systems.

2. BS IEC 61511: 2003. Functional safety - Safety Instrumented Systems for the process industry sector.

3. European Seveso Directive, 1982 (Council Directive 81/501/EEC) reviewed 1996 and adopted as Seveso II Directive.

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