SIL Determination is the key activity for assessing whether instrumented protection is needed to achieve the required level of safety. It includes determination of the Safety Integrity Level (SIL) that a specific safety instrumented function needs to achieve within the context.

There is a wide variety of methods available for SIL Determination. The standards IEC 61508 and the draft of IEC 61511 provide a selection of methods from which the reader may choose. These methods are found within the “informative” sections of the standards and are therefore not mandatory - you can choose a method from those listed in the standard or choose a suitable alternative from elsewhere.

However, no matter what method you select, there are certain issues and problems that are common to the application of all methods. This brief note aims to highlight some of them and offer suggestions related to them.

Hazardous Event

The starting point is identifying the potential hazardous event - what can happen should the safety function fail to operate correctly on demand. We are interested in assessing the benefit derived from the safety function. For SIL Determination, the consequence is regarded as the difference between the safety function working and not working. In most situations, the cost of the safety function working compared with when it fails to operate on demand will be small. Just occasionally, however, there can be significant cost associated with the safety function operating as intended - lost production or contaminated product. This needs to be considered in the assessment of the benefit from the safety function and reflected in the SIL. The difference between the SIS function working and not working is the true benefit of it, in terms of risk reduction.

Existing Safety Functions

When assessing existing instrumented safety functions, the key question to answer is “What exactly is the safety function for?” In most instances, the purpose will be well-known - but not always. It is important to get a full understanding of the true reason the safety function is required.

We need to know whether its primary purpose is protecting people, asset or production loss or protecting the environment. Where there is more than one purpose we need to be sure which requires the higher reliability safety function. We
must use that for assessing the Safety Integrity Level (SIL).

When considering an instrumented safety function the question may be, "Is it reducing the frequency of relief valve lifting (environmental protection) or is it protecting a vessel from rupture (safety)?" The answer will be key to assessing the consequence of failure on demand

**Speed of Response**

Can the instrumented safety function act quickly enough? This is not strictly an issue for SIL Determination. It is really a matter of proper design. Nevertheless, it is valuable to use the opportunity to raise the question and check that there is appropriate supporting documentation. Some large gate valves can take a minute to close. Even large trip valves can take up to 10 seconds to move to the fully closed position.

**Demand Frequency**

Working out what the demand frequency is likely to be is always difficult. Clearly, the more frequent the demands, the greater the awareness of the plant operators as to how often demands occur.

It is important to include all potential sources of demand in any SIL Determination. To do this, it is vital to have a systematic approach that covers normal operation, abnormal operation, start-up, shutdown and demands initiated from outwith the plant (loss of services, power, etc.). Many of these may not be frequent, but when added together they become significant. Demand trees are a good way of being systematic.

Estimation of infrequent demands is difficult. This is especially so when the interval between demands is more than about 10 years. There may be no member of staff who has worked on the plant for that length of time.

**Team Competencies**

Effective SIL Determination requires input from many disciplines. It is certainly not something for the instrument engineer to do as a solo exercise!

It can be done in a manner similar to a Hazop, as a meeting with a leader (preferably a trained safety & reliability professional) and an appropriate group of other relevant disciplines present. These would include instrument and control engineers, process engineers and plant operations representation. This latter representation could be plant management or supervision but for preference would be actual plant operators.

Careful choice of people for such meetings is required to ensure that all relevant disciplines are present but also to ensure that the group will work well together. Sometimes the presence of more senior management can inhibit the discussion of what really happens on the plant.

Such meetings can work well for initial screening purposes and may provide sufficient detail to justify SIL 1 safety functions.

For the higher safety integrity levels (SIL 2 and above) more detail would be appropriate and for this it is better to appoint someone independent from the design team to carry out the assessment.

**Alarms**

When doing SIL Determination there is often a need to include a claim for risk reduction from operator response to alarms. However, there is a tendency to do this without sufficient thought!

Will the operator be "available" to respond? There may be insufficient time in which to respond. There may be too many other alarms at the time. It may be difficult for the operator to decide what to do. How do you know the operator will take the correct action on the initiation of an alarm? Is there a clear, well defined documented response for each critical alarm? Is the means of response still available to the operator? If the alarm has occurred because a control valve has stuck open, then an operator response "close control valve" using the same valve is not going to be effective!

There is a need to think through the scenario and decide what the operator should do and then ensure that all operators are aware.

**Exposure**

When we are considering the potential consequences of the failure of a trip, we often need to look at the proportion of time that the person most at risk may be in the vicinity of the part of the plant where they could be injured.

Usually, for a high hazard area this will be intentionally quite small - less than 10% of the working day. However, before claiming benefit from this, it is important to ask the question as to whether the person is likely to be asked to go the
Hints and Tips

hazard area to investigate just at the time when the incident may occur? In this case the probability of the person being there is nearer to 100% than below 10%.

Safety Integrity Levels

On process plant, most instrumented protective functions will be SIL 1. Conversely, SIL 3 safety functions are normally very rare in the process industries. Furthermore, maintaining a SIL 3 system will call for a high level of testing and therefore maintenance cost.

For SIL 2 safety functions and above, do you have the correct formula for your reliability calculation? Have you included consideration of common cause failure? Do you have a method for selecting appropriate values for common cause factors?

How do you allow for physical blockages of connections to the plant process? Do you account for power supply failures, cabling and instrument manifold piping?

Have you included contributions from human error in your calculation of PFDavg?

Relevance of Safety Integrity Levels

SIL 1

On process plant, most instrumented protective functions will be SIL 1. Conversely, SIL 3 safety functions are normally very rare in the process industries. Furthermore, maintaining a SIL 3 system will call for a high level of testing and therefore maintenance cost.

For SIL 2 safety functions and above, do you have the correct formula for your reliability calculation? Have you included consideration of common cause failure? Do you have a method for selecting appropriate values for common cause factors?

How do you allow for physical blockages of connections to the plant process? Do you account for power supply failures, cabling and instrument manifold piping?

Have you included contributions from human error in your calculation of PFDavg?

Reliability Data

What reliability data are you using for your calculations? Are you using data that is based on your actual plant operating conditions? Where you have "difficult" process fluids - for example, ones that polymerise - do you adapt the failure rates to reflect this?

Are you depending on what reliability data the manufacturer offers for the equipment? Whist this may be reasonable for logic solvers, for items that contact the process fluid it is not so reasonable to expect that the manufacturer will be able to suggest appropriate data. Always question whether the data you are about to use is suitably realistic - reject any that seems overly optimistic.

Diagnoses

Are you relying heavily on diagnoses for achieving the required fail-to-danger values? If so, there are a number of questions you should be asking.

- What faults can actually be detected by the diagnostic facilities?
- How do you prove that the diagnoses are working?
- How often do you test the diagnostics - is it often enough?

Testing

Do you have a policy of testing once per year regardless of SIL rating? Can you justify the test interval needed to achieve the required SIL? If you do proper reliability calculations, you will be able to show that your test interval is appropriate.

We tend to assume that all proof tests are carried out perfectly on 100% of occasions. Proof testing errors do occur and particularly for SIL 2 and above, there should be some consideration of the possible errors and some contribution included in calculations.

Testing should verify the performance of the loop from end-to-end. That is from process fluid to process fluid. No section of the trip loop should be untested - even if it means testing different parts at different times.

Calibration and test equipment - how do you ensure that you are not utilising test or calibration equipment that in itself is incorrect or faulty. If the test equipment were to be incorrect, does your test regime use the same test kit on all the sensors in a l003 voting arrangement so that all three sensors are incorrectly calibrated? Are you creating opportunities for common cause failures or are your procedures designed to help prevent dependent failure?

Conclusions

These notes are intended to prompt those engaged in "SIL Determination" to consider some of the wider issues which may be relevant when conducting SIL assessments.

Dr Alan G King is a hazard and reliability specialist with ABB Eutech, PO Box 99, Belasis Hall Technology Park, Billingham, Cleveland. TS23 4YS. (Previously with ICI Technology, Wilton, Cleveland, England.)

E.mail: alan.g.king@gb.abb.com; agking@ieee.org