



Sharing Control & Safety Instruments Are your layers overlapping?

Dirk Schreier
Functional Safety Consultant
HIMA Australia Pty Ltd
L3, 37 St Georges Terrace
Perth WA 6000
Australia

INTRODUCTION

Since its release as an Australian standard in July of 2004, AS61511 is rapidly being accepted and applied on Safety Instrumented Systems throughout the process industry. Principles such as independence between control and protective instruments have existed for many years, however they continue to often be overlooked even with the introduction of this standard.

Older prescriptive standards particularly in burner / boiler applications recognize the need for independence between control & safety. With older technology it was more difficult to share signals. Separate switches were often used to provide the shutdown function and alarming function.

Today's improved technology has made it easier to share signals. Signal isolators and splitting devices are often used to share transmitter signals between control and safety instrumented systems (SIS). Splitters are also available with certain SIL ratings thereby giving the impression that signals can be safely shared.

AS61511 requires an assessment to be made that considers the independence of protection layers. This is particularly important when a failure in the control function can cause a demand on the safety function. This is the critical aspect often overlooked; a further examination of the problem will clarify the issue.

WHAT'S THE PROBLEM?

The problem is generally not so much the splitting device itself, as we are able to obtain failure data for these devices and include them in our calculations. The problem is generally the lack of understanding the methods used and the assumptions made during the Layer Of Protection Analysis (LOPA) and SIL Assignment.

Simplistically, two aspects are considered during this analysis; (1) Consequence and (2) Likelihood. A Consequence analysis will estimate the damage that will be done should the hazardous event occur. Likelihood analysis will estimate how likely it is that this event might take place given the current controls that are in place. The product of these two aspects is effectively the risk.



The next step is to compare the risk with the tolerable risk. If the risk is higher than the tolerable risk, further risk reduction is required. The magnitude of this difference is represented by a Safety Integrity Level (SIL).

TRANSMITTERS

Consider the following scenario. A pressure transmitter provides a BPCS (basic process control system) with a process variable, which is used for control purposes. The BPCS along with the transmitter keeps the process under control.

A SIL selection team considers this control loop during a layer of protection analysis, and gives credit for reducing the likelihood of the hazardous occurrence. The SIL selected for this loop demonstrates a requirement for further risk reduction, and a Safety Instrumented System is suggested to achieve this. A signal splitter is introduced to provide the ESD system with a repeat of this variable, in order for it to detect and act upon pressure excursions beyond the process limits.

The layer of protection analysis is repeated, now considering also the SIS protection, the required risk reduction *appears* to have been met however credit for the pressure transmitter has been taken *twice*, once in the BPCS, and once in the SIS protection layer. A failure of the transmitter circumvents the control provided by the BPCS and the protection layer provided by the SIS; a serious common mode failure!

This problem is not isolated to the use of splitters, but also when re-transmitting a signal from a SIS analogue output for use in the control system. Separate pressure transmitters must be provided to ensure independent layers of protection.

VALVES

The independence criterion is also just as important when considering final elements such as valves. Consider the scenario where a protective function removes the air supply from a control valve. Once again the SIL Selection team considers the control loop when estimating the likelihood and is thereby taking credit for the valve.

A stuck open control valve causing a hazard will produce a demand on the safety function. However, in this scenario the safety function will fail to protect against the hazard as it only has the same 'stuck' valve available to remove the hazard.

Once again credit has been taken for the valve twice. Once as reducing the likelihood by controlling the process and thereby the demand on the safety function and secondly as reducing the likelihood as part of the SIS protection layer.

Separate control and shutdown valves must be provided to ensure independent layers of protection.



OPERATORS

Another common mistake made with regards to independent layer of protection deals with taking credit for operator intervention. Operator intervention is often considered during a LOPA. The operator acts on an alarm generated by the process control system and performs some action to get the process back into control. The problem here is that the signal, from which the alarm is generated, could be the same signal that is used for controlling the process.

Credit is taken for the transmitter twice. Once for reducing the likelihood by controlling the process and thereby the demand on the safety function, and once as a layer of protection provided by the operator alarm. A dangerous failure of the transmitter circumvents the control provided by the BPCS and the layer of protection provided by the operator intervention.

If the transmitter is stuck at a healthy value then control is lost, and an alarm would never be raised.

CONCLUSIONS

It is therefore very important to understand the assumptions made during the LOPA before introducing these devices. Double dipping is a common mistake made when applying these methods and may contribute heavily to common cause failures.

Following AS61511 will ensure your layers don't overlap because it includes a balance of processes and competence, however companies regularly overlook the competence element hence jeopardizing the possibility of compliance to the standard. Following just the processes laid down in the standard is not enough to comply, nor is a strategically placed CFSE at defined intervals.

The biggest issue that leads to instances such as the "double dipping" scenario is a lack of competence in the project. This is not to be confused with age or general experience of the instrument or control engineer in charge. More importantly it is the specific safety systems experience and knowledge the engineer has with the application, the consequences, legal & regulatory framework and acumen for considering the pessimistic view of "what could possibly go wrong"

This is why 44% of errors occur in the specification stage of a project and is a major factor why independence is overlooked by double dipping.