

ASSESSMENT OF HIGH INTEGRITY INSTRUMENTED PROTECTIVE ARRANGEMENTS†

Alan G King
Hazard & Reliability Specialist, ABB Engineering Services, Billingham, Cleveland UK. TS23 4YS

To comply with the requirements of Functional Safety standards such as IEC 61508 and IEC 61511, it is a requirement that end users undertake calculation of the probability of failure: "The probability of failure on demand of each safety instrumented function shall be equal to, or less than, the target failure measure as specified in the safety requirement specifications. This shall be verified by calculation".

In many instances, this sort of calculation is straightforward and presents relatively few challenges. However, there are other situations where the design of the safety function aims for high reliability and its consequent complexity demands a different approach.

This paper describes as a case study an assessment of the probability of failure of a typical high integrity high pressure trip system for a "top tier" COMAH site in UK. The site had decided to replace the original pressure switches with new pressure transmitters and also replace some of the trip logic with a new safety PLC. The reminder of the trip system remained the same. They required a calculation to demonstrate that the probability of failure was still acceptable – below the target value for this function.

The calculation method for this high integrity safety function required the identification of string sets – success paths through a block diagram of the safety function, and then the minimum cut sets – failure groupings. Once the minimum cuts sets have been listed, the independent failure probability for each of these groupings can be calculated. Additionally, the dependent common cause failure probabilities are calculated. These can be summed to give the overall failure probability for the whole safety function.
The practical method discussed in this paper works for the sort of more complex of arrangements often found in many SIL 2 and SIL 3 safety functions and which cannot be assessed with the simple approaches used for single channel SIL 1 loops.

KEYWORDS: IEC 61511, IEC 61508, Functional Safety, Risk Reduction, Minimum Cut Sets

INTRODUCTION

It has always been the case that the management of high hazard plants has needed to demonstrate the application of suitable means to manage the risks associated with their

operations. In many countries across the world, this has become a legal requirement for operating in those regions. This is the case across Europe, in North America, and in many industrial countries across the world. However, this generally implies that there is not only a need to demonstrate appropriate risk management but also a demonstration of the use of current industry good practice. This in turn involves the use of and compliance with relevant national and international standards.

The use and management of instrumented protective functions such as trips, alarms and interlocks are of key importance in the effective management of risks on many sites. These fall into the category of functional safety[1]. The standards representing current good practice for functional safety using electrical, electronic or programmable electronic means are IEC 61508 [1] and IEC 61511 [2][2], together with the other sector standards that have been generated from IEC 61508. These standards are generally agreed across the world to represent current good practice in this field. These standards have been in the public domain for several years now, and the regulators in many countries are looking for compliance now with these standards, or at the least a programme of action leading towards compliance, as a means of demonstrating the use of current good practice.

These standards cover the whole of the safety lifecycle – from the initial concept through to operation and maintenance[3]. Within the requirements relating to design and operation of instrumented safety functions, there is the demonstration that each safety instrumented function achieves a necessary target performance. This is the performance needed for effective management of the level of risk. The focus for this paper is the specific requirement in the standards that end users undertake a calculation of the probability of failure: "The probability of failure on demand of each safety instrumented function shall be equal to, or less than, the target failure measure as specified in the safety requirement specifications. This shall be verified by calculation"[4]. Calculation is therefore a mandatory requirement for compliance with the standard. In many instances, such calculations of failure probability are simple and straightforward. This is true for single channel safety instrumented functions with probabilities of failure in the range for Safety Integrity Level 1 (SIL 1)[5]. However, for safety functions designed for higher reliability, for example those aiming to achieve SIL 2 or SIL 3, the consequent complexity can demand a different approach.

[1]Functional Safety here refers to those systems that rely on the correct functioning of electrical or other systems to achieve the required level of safety.

[2]IEC 61511 is the Process Sector standard derived from the generic standard IEC 61508 on instrumented Functional Safety.

[3]And through to the eventual decommissioning of the systems.

[4]IEC 61511-1 Clause 11.9.1

[5]See References [1] and [2] for definitions of SIL 1 through to SIL 4.

BACKGROUND

This paper describes as a case study an assessment of the calculation of probability of failure of a typical high integrity high pressure trip system for a "top tier" COMAH site in UK. The site had decided to replace their original pressure switches with new pressure transmitters and also replace some of the trip logic with a new safety PLC. The remainder of the trip system remained the same. They required a calculation to demonstrate that the probability of failure was still acceptable – below the target value for this function.

The original configuration of the safety instrumented function is shown in Figure 1.

The safety instrumented function is initiated by high pressure and acts to stop the flow of both reactants (A & B). For high pressure protection, the critical requirement is to stop the flow of Reactant B. Thus, the safety function can be seen as limited to that part which senses high pressure and stops the flow of Reactant B. The sensors are both pressure switches and for the action to stop the flow of Reactant B the pressure switches operate on a 1 out of 2 basis – either pressure switch sensing high pressure is sufficient to trigger successful operation of the function.

The plant wished to improve the system by replacing the pressure switches with pressure transmitters, so that the analogue value of pressure from each could be made available to the operators. Additionally, they decided that they would purchase a safety PLC for the plant trip system as a whole. This safety PLC would then provide the interface to the new pressure transmitters and also provide a means of relaying the analogue values to the plant control system for display to the operators. The new arrangement is shown in Figure 2.

From this it can be seen that the changes only affect the part of the trip system upstream of the two original relays R5 and R6. The remainder of the system is unchanged. There are two new relays R1 and R2. These are part of the output arrangement for the safety PLC.

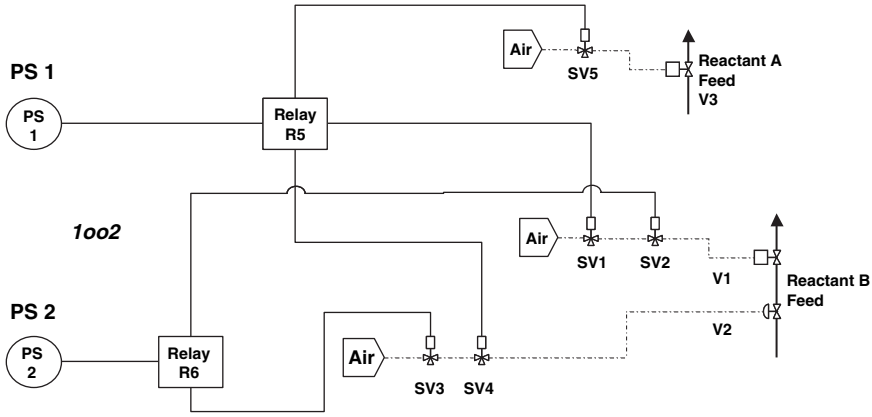

Figure 1. Original trip system

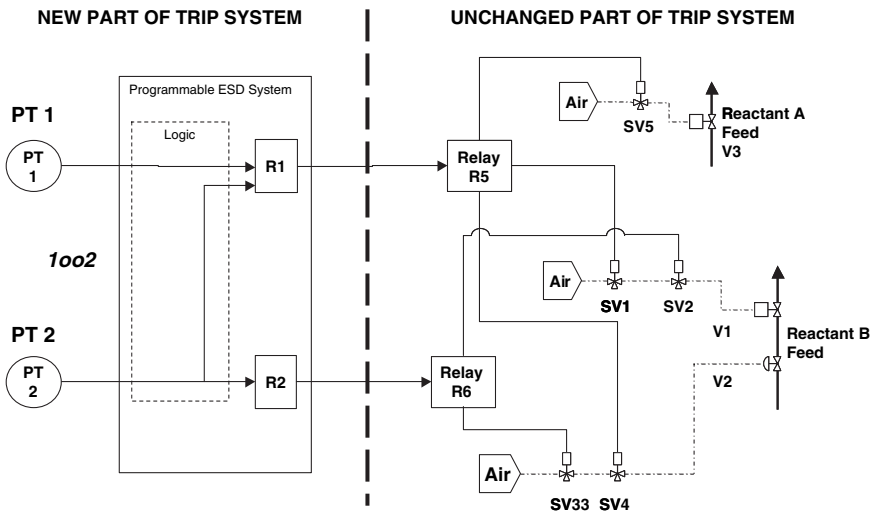

Figure 2. Proposed modification

DESCRIPTION OF THE METHOD

BLOCK DIAGRAM

The diagram in Figure 2 is too detailed as a basis for calculation. The first stage is therefore to simplify the function into a block diagram, showing only the parts of the safety function that are essential for high pressure protection. This is illustrated in Figure 3 and shows the sensors and logic block (representing the safety PLC). The two new relays R1 and R2 have been combined with their corresponding relays from the original system R5 and R6 respectively. This is to simplify calculations. Furthermore, the output side of the safety function only shows the routes through to the trip valves V1 and V2, which are the two valves that can block the flow of Reactant B. Closure of either of these valves represents success for the safety function.

From this diagram, we can identify the success paths through the function. There are six of these success paths:

1. PT1 – Logic – R1 & R5 – S1 – V1
2. PT1 – Logic – R1 & R5 – S3 – V2
3. PT2 – Logic – R1 & R5 – S1 – V1
4. PT2 – Logic – R1 & R5 – S3 – V2
5. PT2 – Logic – R2 & R6 – S2 – V1
6. PT2 – Logic – R2 & R6 – S4 – V2

These are known as string sets. However, what we are interested in for the probability calculations are not the success paths but the failure groups known as minimum cut sets.

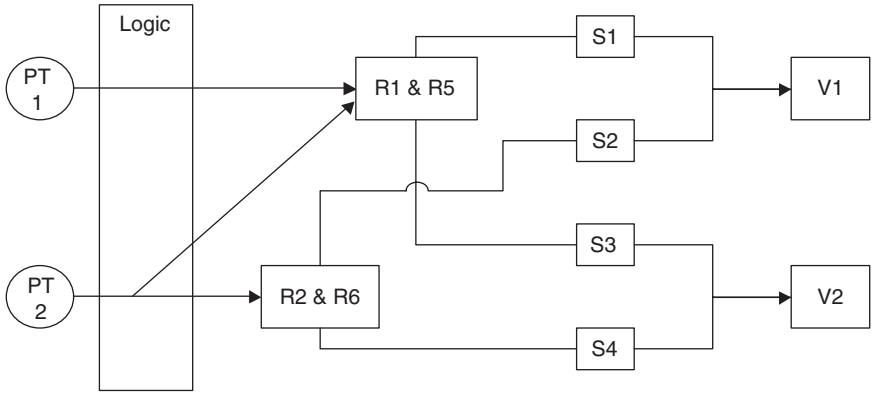

Figure 3. Block diagram of trip function

It is possible to generate the minimum cut sets for the function from the string sets but it is not straightforward. In practice, it is easier to identify the minimum cut set groups for functions of limited complexity, such as Figure 3, by inspection.

MINIMUM CUT SETS

A cut set is a group of items in the safety function whose failure will cause the function to fail. A minimum cut set is a group of items whose failure is just sufficient to cause failure of the overall function. Restoration of any one of the items from failed to working will cause the overall function to work successfully. For the function shown in Figure 3 there are 17 identifiable minimum cut sets. These are shown in Table 1 below.

It can be seen from Table 1 that some minimum cut sets have one member, some have 2 members, some 3 members and some 4 members. For calculation of independent failure probability, the minimum cut sets may be thought of as voting groups on a basis of 1 out of 1, 1 out of 2, 1 out of 3 and 1 out of 4 respectively. If we assume that the duration of any proof testing is short compared with the interval between tests then we can use the simplified formulae for the average probability of failure on demand (PFDavg), where θ is the dangerous failure rate and T is the test interval:

$$\text{PFDavg (1oo1)} = 0.5 \times \theta T$$
$$\text{PFDavg (1oo2)} = \frac{4}{3} (0.5 \times \theta T)^2$$
$$\text{PFDavg (1oo3)} = 2 (0.5 \times \theta T)^3$$
$$\text{PFDavg (1oo4)} = 16/5 (0.5 \times \theta T)^4$$

These formulae for the independent failure probability are shown for minimum cut sets with identical types of members. For example, Minimum Cut Set No 2 with four solenoid valves (S1, S2, S3, S4), or Minimum Cut Set No 5 with two trip valves (V1, V2). Where a minimum cut set has members of different types, for example, No 6 with a pressure

Table 1. Minimum cut sets

No	Minimum cut set	No	Minimum cut set	No	Minimum cut set
1	PT1, PT2	7	PT2, S1, V2	13	R2&R6, S1, V2
2	S1, S2, S3, S4	8	PT2, S3, V1	14	R2&R6, S3, V1
3	PT2, R1&R5	9	R1&R5, S2, S4	15	S1, S2, V2
4	R1&R5, R2&R6	10	R1&R5, S2, V2	16	S3, S4, V1
5	V1, V2	11	R1&R5, S4, V1	17	PLC Logic
6	PT2, S1, S3	12	R2&R6, S1, S3		

transmitter and two solenoid valves (PT2, S1, S3) the formulae have to be modified – the exponent is removed and the single bracketed part is replaced with the product of the PFDavg for each member of the cut set. Additionally, calculation of dependent failure probability is required, where a cut set contains a number of similar or identical items[6].

CALCULATIONS

For the safety instrumented function described above, calculation was carried out for each minimum cut set. The site had their own preferred failure rates for use in PFDavg calculations and the proof test interval was set at 3 months. The calculation summary is shown in Table 2. It shows the calculation spreadsheet for independent failure. The figures in brackets in the "Formula" column are the PFDavg results for the cut set items. These were based on the site preferred failure rates and test interval using the formula:

$$\text{PFDavg (item)} = 0.5 \times \theta \times T$$

where θ is the dangerous failure rate and T is the test interval

It should be noted that whilst the spreadsheet calculates to many decimal places the input data is only good to two significant figures (if that). Thus, the total Independent PFDavg comes to 5.0×10^{-5}. However, many of the cut sets have potential for dependent failure. The PFDavg for this must be calculated and added to the value for independent failure. Dependent failure probability has been calculated using the beta factor method and the formula:

$$\text{PFDavg (Dependent)} = \beta \times 0.5 \times \theta \times T$$

Where θ is the dangerous failure rate for the item in question, T is the proof test interval and β is the Beta Factor. A value of 15% has been used for the Beta Factor as a conservative figure for identical items in close proximity.

[6]The process valves were designed to fail to the safe position on loss of instrument air. Consequently, failure of instrument air has not been included in the consideration of common cause failure. Common cause failure of the valves due to contaminated instrument air adversely affecting their performance is covered by the dependent failure assessment.

Table 2. Independent PFDavg calculations

	Minimum cut set	Formula	Independent PFDavg
1	PT1, PT2	= 4/3 (0.001663)^2	= 3.69E-06
2	S1, S2, S3, S4	= 16/5 (0.004167)^4	= 9.64506E-10
3	PT2, R1&R5	= 4/3 (0.001663) × (0.000448)	= 9.93344E-07
4	R1&R5, R2&R6	= 4/3 (0.000448)^2	= 2.67755E-07
5	V1, V2	= 4/3 (0.004167)^2	= 3.47222E-05
6	PT2, S1, S3	= 2 (0.001663) × (0.004167)^2	= 5.77257E-08
7	PT2, S1, V2	= 2 (0.001663) × (0.004167) × (0.004167)	= 5.77257E-08
8	PT2, S3, V1	= 2 (0.001663) × (0.004167) × (0.004167)	= 5.77257E-08
9	R1&R5, S2, S4	= 2 (0.000448) × (0.004167)^2	= 1.55599E-08
10	R1&R5, S2, V2	= 2 (0.000448) × (0.004167) × (0.004167)	= 1.55599E-08
11	R1&R5, S4, V1	= 2 (0.000448) × (0.004167) × (0.004167)	= 1.55599E-08
12	R2&R6, S1, S3	= 2 (0.000448) × (0.004167)^2	= 1.55599E-08
13	R2&R6, S1, V2	= 2 (0.000448) × (0.004167) × (0.004167)	= 1.55599E-08
14	R2&R6, S3, V1	= 2 (0.000448) × (0.004167) × (0.004167)	= 1.55599E-08
15	S1, S2, V2	= 2 (0.004167) × (0.004167)^2	= 1.44676E-07
16	S3, S4, V1	= 2 (0.004167) × (0.004167)^2	= 1.44676E-07
17	Safety PLC[7]		= 1.0000E-05
		Total Independent PFDavg	= 5.0225E-05

The calculation in Table 3 has only been done for those cut sets with all items identical, as these will be the ones most susceptible to dependent failure. It is possible to calculate and include contributions for those cut sets where some items are the same but one is different. However, the size of the contribution from this would be much smaller and may be neglected.

The overall PFDavg for the system is therefore:

$$\begin{aligned} \text{PFDavg (System)} &= \text{Independent PFDavg total} + \text{Dependent PFDavg total} \\ &= 0.00005 + 0.00157 \\ &= 0.00162 \end{aligned}$$

It is worth noting that the PFDavg in this example is dominated by the dependent failure contribution and were it to have been omitted the result would have been around 1.5 orders of magnitude out.

[7]A notional illustrative probability has been used in these calculations for a Safety PLC suitable for SIL 3 safety functions. In any actual calculations, the probability used should be based on assessment of the actual Safety PLC architecture and its predicted performance.

Table 3. Principal dependent failure PFDavg

	Minimum cut sets	Principal dependent PFDavg
1	PT1, PT2	0.000249
2	S1, S2, S3, S4	0.000625
3	PT2, R1&R5	
4	R1&R5, R2&R6	0.000067
5	V1, V2	0.000625
6	PT2, S1, S3	
7	PT2, S1, V2	
8	PT2, S3, V1	
9	R1&R5, S2, S4	
10	R1&R5, S2, V2	
11	R1&R5, S4, V1	
12	R2&R6, S1, S3	
13	R2&R6, S1, V2	
14	R2&R6, S3, V1	
15	S1, S2, V2	
16	S3, S4, V1	
17	Safety PLC	
	Total dependent failure PFDavg	0.001567

RESULTS

The above calculation shows that the overall PFDavg is in the range for SIL 2. It is at the higher performance end of the range for SIL 2. The operating site was looking for an overall PFDavg that would be at least as good as the previous system and therefore allow them to meet their target. The previous arrangement had a PFDavg of 0.00268 and so the site could demonstrate that the changes would be an improvement and the new system would meet the requirements for the plant.

CONCLUSIONS

Whilst the calculation of the failure probability for a single channel safety function is relatively simple to do, safety functions with the type of architecture described in this paper present more of a challenge. This is often the case with safety functions aiming to achieve performance in the range for SIL 2 or SIL 3. This paper has demonstrated that

there is a systematic way to approach calculation of the PFDavg of these more complex arrangements and to show that in this respect the requirements of IEC 61508 and IEC 61511 to show by calculation can be met.

REFERENCES

IEC 61508: "Functional safety of electrical/electronic/programmable electronic safety-related systems", International Electrotechnical Commission, Geneva, 1998 & 2000

IEC 61511: "Functional safety – Safety instrumented systems for the process industry sector", International Electrotechnical Commission, Geneva, 2003