SIL loop: certified or non certified equipment - the way to go!

I P Parry and P R Smith
Hima Sella Ltd

Introduction

Presumably, having started to read this article, you have heard of, been involved with or been panicked by IEC61508 and need to either understand the process of SIL assessment of safety related instrument loops or even perform such calculations. A safety instrumented loop is any loop whose failure to operate could realize a hazard to life, the environment or to Asset Management.

Hopefully, you will be fully aware that the new standard consists of seven parts. Parts 1 to 4 are normative and as such constitute the main requirements whilst parts 5 to 7 provide guidance and supporting information. Of specific importance to the assessment of instrument loops are parts 2, 3 and 6. Part 2 addresses the requirements for assessment including both qualitative and quantitative, the LOWEST of these two assessments will apply!

Part 3 addresses the issue of software in programmable electronic systems (PES) and part 6 provides formulae and guidance to support the quantitative analysis.

However, don't forget Part 1 as this lays down the requirements for documentation, responsibility and competence.

OK that's the background, so what is the best way to set about designing safety loops to IEC 61508? Is it possible to just use any instrument that satisfies the functional specification, OR is there an advantage in choosing certified components from accredited companies?

Lets look at a typical basic safety loop.

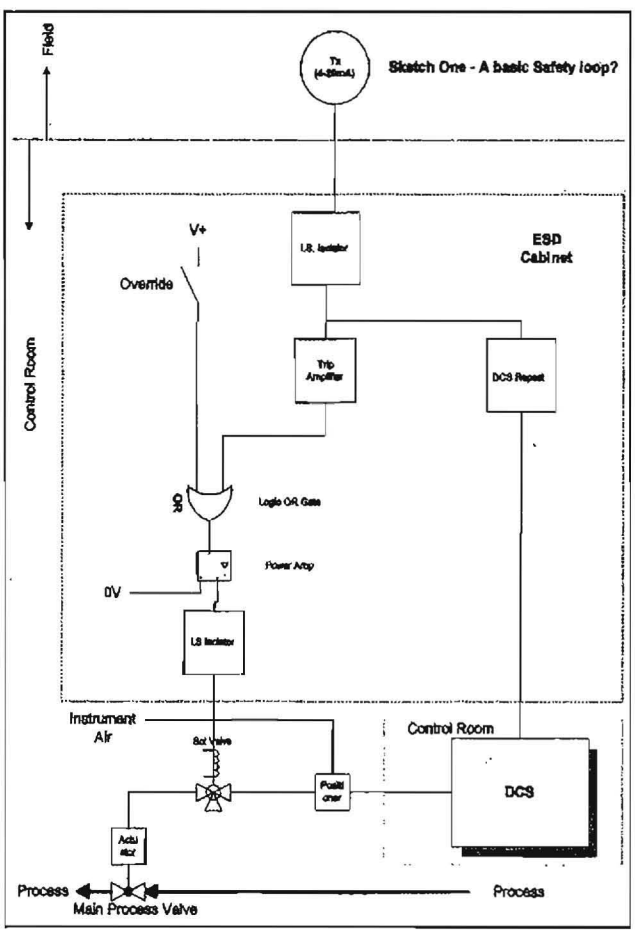

Figure 1: A Basic safety loop?

A Basic Safety Loop?

First Question: is it a safety loop?

A HAZOP will have determined the consequences of the process valve NOT closing when required and these may be:

- ❒ Safety - The degree of risk to personnel ranging from minor injuries to several deaths.
- ❒ Environment - Minor to severe pollution of the local environment.
- ❒ Commercial - Damage to equipment or loss of valuable product.

Second question: what happens when potential component failures occur? For instance:

1. The DCS repeat interface, which is not part of the safety loop, could fail such that the trip amplifier function is inhibited and the whole loop integrity is compromised.

   Result: the safety loop will never trip.
2. The single contact presented by the Override could weld closed resulting in a permanent override which, in the absence of any form of alarm, would not be detected.

   Result: the safety loop will never trip.
3. The main process valve is required to close to fulfil the safety function. The characteristics of a control valve may not be compatible with the required characteristics of a reliable ESD valve.

   Result: the safety loop may not trip.
4. None of the sub-systems identified are stated to be 'fail safe' by design so we must assume that normal commercial equipment is used.

   Result, in the event of a sub-system failure the failure mode of the loop is unpredictable and hence safety is not optimised.

So that wasn't a safety loop after all. So, what is a safety loop?

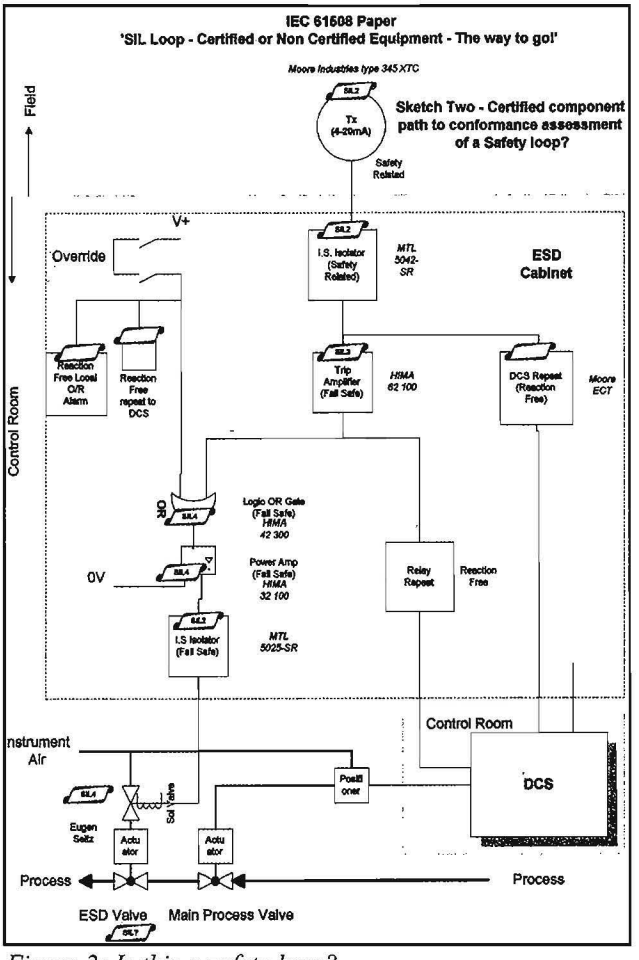

Figure 2: Is this a safety loop?

Is this a Safety Loop?

We now have a loop that introduces the concepts of :

❒ Reaction free - The device is designed so that it cannot influence the loop into which it is connected.

❒ Fail Safe - The device has been designed to 'fail safe', in the event of a failure, with a high degree of assurance. The output will be forced 'low' in the event of an internal component failure. The reliability of devices purposely designed to be 'fail safe' is of the order 99.5% or better. Using the terms of EC 61508 this would equate to 'Safe Failure Fraction' of 99.5% or better.

In addition several extra safety features have been introduced:

1. The Override has dual independent contacts connected in series so that some insurance against contact weld is provided.
2. The override signal is alarmed by local indicator light and DCS signal.
3. A dedicated ESD valve is incorporated to isolate the process in the event of control valve failure or leakage.

Now that we have a safety loop which is defendable, how do we assess its conformance with IEC 61508?

Following the HAZOP performed to identify the likely process hazards, and therefore establish the requirement for a safety loop, a SIL determination procedure is performed.

This procedure uses a 'Risk analysis' methodology to determine practical design considerations including the safety loop, required to reduce the risk of the hazard actually developing. This review will identify additional or alternative measures capable of reducing the risk.

The extent of risk reduction employed on a particular process is determined largely by the ALARP (As Low As Reasonably Practicable) principle and is dominated by the hazard consequence. Due to practical design issues the identified hazard may be expected to occur once every 'x' years, this is the 'demand' placed on the safety loop. The safety loop function is to recognise the onset of the process condition which might result in the identified hazard and to act immediately (within the 'safety time' of the process) to implement strategies designed to stop the hazardous process condition occurring, such as by closing valves, switching off heaters etc.

Note that the 'Safety Time' is the time required for the conditions to develop to a point where the 'hazard' is inevitable.

It is the reliability of the safety loop performing its task that leads to a reduction in the risk. If the probability of loop failure is high then this will either result in 'spurious' (safe) trips which make the process expensive, or unrevealed (dangerous) faults which will impede the required function of the safety loop. IEC 61508 requires the failure mode and Rate of Dangerous failures to be quantified and the SIL rating provides a simple system of grading according to risk reduction capability. Eg SIL 1 is an average probability of failure to perform its function on demand of $\geq 10^{-2}$ to $<10^{-1}$ and this may be interpreted as at least 9 out of 10 trip demands will result in a safe outcome - a risk reduction.

We might conclude that the loop shown in *Figure 1* was based on an inadequate specification and was not properly assessed.

We should now have an adequate SIL requirement for the safety loop and Sketch Two illustrates an improved loop using certified 'sub-systems'.

But - do we need to use certified 'sub-systems'?

Qualitative Assessment

The standard requires each component in the loop (called a sub-system) to be assessed against the IEC 61508 requirements for Safety Integrity (IEC 61508 Part 2, para 7.4.3).

Each loop component means the field sensor and its installation, all interfacing equipment, the ESD components and all field output devices including final valves, actuators, positioners, solenoid valves and whatever else may be required to implement the safety function.

The requirement is to determine that each component is suitable for its intended function and this includes the application of existing standards such as EMC. It is not my intention to pursue this part of the assessment, suffice it to say that any such complementary standards which might be involved must be considered and complied with. A very important example would be those for hazardous area working.

The standard identifies two parameters, 'Hardware Fault Tolerance' and 'Safe Failure Fraction'. Two tables within the standard (part 2, para 7.4.3.1.4) are applicable.

For Hardware Fault Tolerance, two cases are considered:

Type A - Effectively simple devices which may or may not include software.

have to consider the use of generic information. Many companies such as the old ICI do collect and publish data for their own use but this is frequently limited to failure rates ie quantitative data.

Some generic data bases such as Oreda provide good typical failure rates and information from operator experience. Relevant text books such as 'Reliability Maintainability and Risk' (by Dr D J Smith, ISDN 0-7506-5168-7) also provides some useful guidance on both typical failure rates and failure modes. This can be used to produce a rough assessment of Safe Failure Fraction which might be usefully compared with other sources of data to support an overall conclusion. However, this is a risky approach and should be used with care for SIL1 and possibly SIL2. The requirement for supporting evidence certainly excludes its use for a SIL greater than 2 and arguably for SIL2 also.

Quantitative Assessment

Part 6 of IEC 61508 provides the methodology required to calculate the Probability of Failure to Danger (PFD) that is required to enable a quantitative SIL to be assessed. The IEC 61508 calculation uses fail to danger rates combined with a mean down time assessment to derive a figure for the PFDsys (Average Probability of Failure on demand of a safety function for the E/E/PES safety related system).

A fail to danger rate must be obtained for each sub-system involved in the safety loop. In our example the safety loop consists of:

- 4-20mA Tx, the field sensor
- I.S. Isolator (input)
- Fail Safe Trip Amplifier
- Fail Safe Logic OR gate
- Fail Safe Output Driver Amplifier
- I.S Isolator (output)
- Safety Related Solenoid Valve
- ESD Valve

Note that the other sub-systems are not part of the safety loop.

Reference - Override Circuits

The override circuit is not involved in the SIL calculation BUT it must be considered as it potentially degrades the availability figure if used to override part of a running process (A procedure which is NOT recommended) eg SIL 4 requires the PFD to be between 10^{-4} and 10^{-5} per year. This figure may be transformed into an availability time per year. ie available to perform its trip function. 10^{-4} equates to 99.99% available, 10^{-5} equates to 99.999% available per year. So, if an override is applied for more than 52.6 minutes per year then by definition the protected system was not available to fulfil its safety function consistent with a SIL 4 requirement. Note that this is simplified because in practice the total loop SIL will fall somewhere in between the limit figures. Consequently the actual time that an override may be applied without compromising the loop SIL is somewhere in between the limit figures.

This maximum override time must be stated on the SIL calculation so that the end user may construct appropriate operating procedures.

Reference - Architecture

By system architecture we mean the degree of robustness built into the loop. For instance, a perfectly acceptable safety loop may be constructed using the loop example shown. The architecture is considered to be '1oo1 to trip', ie if the single sensor output exceeds the trip value then the ESD valve WILL be closed to fulfil the safety function. Unfortunately the ESD valve will also be closed if any of the loop components fails 'safe' due to an internal fault a so called spurious trip.

It is worth a quick word about what we mean by 'Reliability'. A safety loop can be 'available' so that the associated process experiences little down time - but it might not be safe. When specifying architectures we must always consider 'to trip' ie 1oo1 to trip.

The aim of IEC 61508 is to ensure that the availability of the safety loop to perform its function is optimised first of all and then the spurious trip rate may be considered.

The spurious trip rate can be optimised by careful consideration of various architectures,1oo1, 1oo2D, 2oo2D, 1oo3, 2oo3 etc. A common choice is 2oo2 which provides security against spurious trips because two identical loops are constructed to do the job of one, and both channels have to demand a trip before the ESD valve will close.

The problem with 2oo2 is that a single component failing to danger WILL destroy the integrity of the safety loop unless or until the loop is 'proof' tested. It will destroy the integrity because a dangerous fault will remain hidden until a demand occurs at which time the protective loop will fail to operate with some consequence.

So, '2oo2' will cut the spurious trip rate but increase the risk of a hidden fail to danger. A '1oo2' architecture will increase the spurious trip rate but remain safe under a single component failure to danger.

The trick is to recognise the weak points in a loop, these are generally the field sensor and actuator. Most ESD components are well specified and documented so that their likely performance is predictable to a high degree and consequently do not significantly contribute to loop failure. Some data which is often presented indicates that the contributions to loop failure are typically: Sensor 35%, Logic Solver 15% and Final Actuator 50%.

Probably the optimum configuration is '2oo3 sensors' with '1oo1' or '1oo2' logic and a '1oo2' final actuator, as both spurious trips and hidden fail to danger are minimised.

This can only be a very brief introduction to the subject of architectures and is consequently incomplete. For further guidance on architectures please reference Part 6 of the IEC61508.

The example case illustrated in *Figure 1* should be interpreted as 1oo1 for sensors, input isolator, logic, output isolator, solenoid valve and ESD valve.

Once the components of the safety loop and the architecture are clearly understood then the fail to danger rates for each sub-system must be determined. It is possible that the supplier will be able to provide such data but this is currently the exception rather than the rule. Generally, it is necessary to obtain and collect sources of 'generic' data so that a particular device can be assessed. This situation is non ideal because such data is rarely given with reference to the local environment and, in the case of field components, the process fluid.

Generic data should be used with care and should utilise more than one source in order to obtain a worst case representative figure. There are many such sources and the greater your reference database the better your assessment will be.

Safe Failure Fraction	Hardware fault tolerance		
	0	1	2
<60%	SIL1	SIL2	SIL3
60% - <90%	SIL2	SIL3	SIL4
90% - <99%	SIL3	SIL4	SIL4
>=99%	SIL3	SIL4	SIL4

Simplified Representation of IEC 61508 Type A (IEC 61508 Table 2)

Safe Failure Fraction	Hardware fault tolerance		
	0	1	2
<60%	Not allowed	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - <99%	SIL2	SIL3	SIL4
>=99%	SIL3	SIL4	SIL4

Simplified Representation of IEC 61508 Type B (IEC 61508 Table 3)

Note:
A Hardware Fault tolerance of 'N' means that 'N+1' faults could cause a loss of the safety function. The 'safe failure fraction' of a sub-system is defined as the ratio of the average rate of safe failures plus dangerous detected failures of the sub-system to the total average failure rate of the sub-system. Mathematically: $\frac{LSD+LSU+LDD}{LSD+LSU+LDD+LDU}$

Type B - Effectively complex devices which often do include software.

Simply, we are required to decide whether we have intimate understanding of the device concerned, for example, the failure modes of all constituent components; its behaviour under fault conditions, and whether it provides extensive, reliable field failure data in support of claimed failure rates.

If the answers are 'no' then the device would be 'Type B', if 'yes' then the device would be 'Type A'.

Note that these tables limit the claimed SIL for any 'sub-system' based on its architecture irrespective of how good the calculated failure rate is. This avoids too much reliance on very low calculated failure rates without the support of fault tolerance in the design.

Easy? I don't think so. It is rarely possible to obtain supporting information when using non-certified components but sometimes you have no choice if certified components are unavailable. It is most often necessary to move into the dark side of available data to see if sufficient information can be obtained to allow a defendable decision with adequate 'evidence'. Such an assessment may be considered for a simple device such as a relay or a solenoid valve, but what about a 'ph' sensor? If a decision has to be made then it must be worst case but 'safe', so the inevitable conclusion is that the device is 'Type B' and this means that you may have to convince a jury why you conclude that the Safe Failure fraction is reasonable at 60-<90% just to achieve the lowest SIL of '1'. I assume, of course that no commercially available sensor will be designed with a hardware fault tolerance of >0.

Remember that this is just part of the assessment and it has to be done for 'each' loop sub-system. However, the science of ESD controllers has progressed so far that you will not have a problem obtaining the correct data from such suppliers. I am also happy that the more informed manufacturers of loop components are now actively complying with the standard. So, if you have chosen wisely then you should be left with the dilemma of how to assess only one or two sub-systems. If you are unlucky then you may also be struggling to assess your field sensor if the measurand is other than pressure or temperature.

To assess a device of unknown pedigree the first port of call will be the supplier. You will need to request information on 'fault tolerance', 'safe failure fraction', PFD_G (average probability of failure on demand) and FTD. (failure to danger rate - per hour or per year)

The latter two are required for the 'Quantitative' part of the assessment. This is your first piece of evidence even if the answer is negative.

Next, you will need to assess your own competency to proceed further. If you are not experienced in sensor technology or at least comfortable with electronics then you will need the services of a consultant. If you consider yourself to be capable then it will be necessary to review all the information that you can get from the supplier and then use this to make a valued judgment on the first aspect of fault tolerance.

Safe failure fraction can be approached in several ways but assuming that the manufacturer has not produced a 'failure mode and effects analysis' for his product then this reduces to two:

If the supplier can (and will) provide data from his Quality Department regarding warranty returns then this may provide a clue to the approximate value of safe failure fraction. This will not be adequate alone, especially if the component is a relatively low cost one where the client is more than likely to throw the device away and simply order another. IF he is aware that it has failed! Of course, as the nature of safety systems is that the demand on them is low by requirement, then it is a matter of conjecture as to how many devices are installed but non- operational and in a dangerous state. With a badly designed loop the fault will only become visible when a test is performed or when a demand is made.

A better approach is to obtain end user data directly if the end user's maintenance department keeps records of such failures. It is a little early in the life of IEC 61508 for this to be common, but it is a necessary requirement of IEC61508 and an enquiry might prove fruitful.

OK, so you have failed in the easy approach. Now you

Sub-System	Data Source (failures per million hours)		
	A	B	C
4-20mA Tx, the field sensor	Sensor 2-10	110	1.43+2.85 = 4.28
I.S. Isolator (input)	-Transmitter 10 - 20	-	-
Trip Amplifier	-Transmitter 10 - 20	-	-
Logic OR gate	-Transmitter 10 - 20	-	-
Output Driver Amplifier	-Transmitter 10 - 20	-	-
I.S Isolator (output)	-Transmitter 10 - 20	-	-
Solenoid Valve	General Solenoid De-energise to trip 1 - 8	-	-
ESD Valve	Valve (Butterfly Worst case) '*' 20	ESD Gas - 19.72	ESD/PSD 33.8
Main Process Valve (For Information Only)	Valve (Butterfly Worst case) 20	Butterfly - 22.83	Butterfly 137.0

Table 1: Overall failure rates (for this example I have used three data sources A, B and C for each sub-system).

Sub-System	Data Source (failures per million hours)		
	A	B	C
4-20mA Tx, the field sensor	Sensor 1 - 5	55	2.14
I.S. Isolator (input)	-10	-	-
Trip Amplifier	-10	-	-
Logic OR gate	-10	-	-
Output Driver Amplifier	-10	-	-
I.S Isolator (output)	-10	-	-
Solenoid Valve	General Solenoid De-energise to trip 0.5 - 4	-	-
ESD Valve	Valve (Butterfly Worst case) 10	ESD Gas - 19.72	ESD/PSD 16.9
Main Process Valve	Valve (Butterfly Worst case) 10	Butterfly - 11.42	Butterfly 67.5

Table 2 : Fail to danger rates (assumed worst case)

Sub-System	Estimated Dangerous Failure Rate (failures per million hours)
4-20mA Tx, the field sensor	55
I.S. Isolator (input)	10
Trip Amplifier	10
Logic OR gate	10
Output Driver Amplifier	10
I.S Isolator (output)	10
Solenoid Valve	4
ESD Valve	19.72
Main Process Valve	67.5

Table 3: summarises the available fail to danger rates.

These failure rates are for all failures including both 'dangerous' and 'safe'. We now need to determine a dangerous failure rate for each! In the absence of any reliable data the only reasonable assessment must be that 50% fail to 'danger' and 50% fail 'safe', though this may not be 'safe' because some devices may have a fail to 'danger' rate which is higher than 50%! Hence the need for evidence.
'' Note that a Butterfly Valve would not be used in an ESD application but data is used to determine a worst case position.*

What next?

Well, to perform the calculations required by IEC 61508 it will be necessary to determine a practical proof test interval, a mean down time for each subsystem and a beta factor for cases where the architecture is other than '1oo1'.

Proof Test Interval (T1)

The minimum time between loop tests designed to ensure that all loop components are functioning correctly.
The starting point for Proof Test Interval is one year, but the final value is determined PRIMARILY by the loop SIL target or, assuming the loop SIL is easily achievable, the process requirement, eg it could be necessary to demand a weekly test on particularly critical loops though operational experience may subsequently allow the end user to justify a less onerous period.

Mean Time to Restoration (hour) (MTTR)

The maximum time required to determine the cause of loop failure and restore it to operation by replacing faulty sub-systems.
The figure used here should be an accurate reflection of the worst case restoration time taking into account spare parts availability, accessibility and availability of competent personnel.

Beta Factor (b)

The fraction of undetected failures that have a common cause.
This factor may be estimated but it requires a consideration of many factors such as independence of power supplies, routing of cables, siting of valves etc. This is not a trivial task and will not be addressed here. I would refer you to a textbook on the subject.

Conclusion

Our quantitative assessment does not achieve even the lowest SIL of 1 (PFD$\geq 10^{-2}$ to $<10^{-1}$ per year). Our qualitative assessment may have claimed a shaky SIL1 but the result overall is unacceptable because though it met the architectural constraints for SIL1 the PFD is too high.

Generic data is useful where no alternative source exists and where the available generic data is for equipment which is very similar to the actual equipment being used.

In our case we could find no generic data for I.S. Isolators or ESD Logic Solver components so we used the nearest 'similar' generic data. The result is conservative because it does not lead to a SIL claim but unacceptably pessimistic because SIL1 is probably achievable. To improve the data used such that it is defendable will require a great deal of further research.

SILCalc

Component	Type/ Quantity	No of Ch	A_{SD} per year	A_{DU} per year	Architecture	β e	T1 (j) in years	MTTR(g) in hours	PFD_{AVG}
Sensor	a	1	4.82E-01	4.82E-01	1oo1		1	8	2.413E-01
I.S Isolator *	b	1	8.76E-02	8.76E-02	1oo1		1	8	4.388E-02
Trip Amp	c	1	8.76E-02	8.76E-02	1oo1		1	8	4.388E-02
							1	8	
							1	8	
Logic modules							1	8	
							1	8	
							1	8	
Logic 'OR'	d	1	8.76E-02	8.76E-02	1oo1		1	8	4.388E-02
							1	8	
							1	8	
							1	8	
							1	8	
Driver Amplifier	e	1	8.76E-02	8.76E-02	1oo1		1	8	8.776E-02
							1	8	
							1	8	
							1	8	
							1	8	
Output I.S. Isolator	f	1	0.00E+00	0.00E+00	1oo1		1	8	0.000E+00
							1	8	
Solenoid valve	g	1	3.60E-02	3.60E-02	1oo1		1	8	1.755E-02
ESD Valve	h	1	1.73E-01	1.73E-01	1oo1		0.33	8	2.868E-02

RESULTS			
	Overall PFDg	=	5.070E-01
	Overall Fail to Danger Rate	=	
	IEC 61508 SIL	=	not SIL classifiable!
			NOTE: WHEN WARNING DISPLAYED SIL

Table 4 presents the SIL calculation result determined by using the figures of Table 3. Note that for a simple architecture such as 1oo1, PFD approximates to (LDU) MDT. To obtain the loop PFD the individual sub-system PFD's are merely summed.

Where to now?

IEC 61508 Part 1 demands that 'evidence' is provided in support of all safety loop design work. Our first attempt is unhelpful because though the conclusions are safe they are neither realistic nor useful. We now have a choice. To cut the costs of loop SIL assessment and optimise safety, evidence and integrity we must use equipment manufactured by responsible companies who are well versed in the requirements of IEC 61508 and who can provide a documentation path in support of their equipment. If we take this path early enough in a contract and use sub-system suppliers who either have accredited certification of their sub-systems or of their design systems then project cost and timescale will be optimised and due diligence clearly documented.

In our example *Figure 2* shows the most cost effective route to compliance:

Sub-System	Supplier	SIL Certified ?	Failure to Danger Rate (per hour)
Field Transmitter	Moore Industries	Self Certified under	144.0E-9
Temperature inc RTD	Type SPA	CASS FSCA to SIL2	
Field Transmitter Pressure	Moore Industries Type 345 XTC	TÜV Certified SIL2	29.2E-09
I.S.Isolator (Input)	MTL 5042-SR	Baseefa Certified SIL2	1.6E-08
Fail SafeTrip Amp	Hima 62 100	TÜV Certified SIL3	7.9E-10
Fail Safe Logic 'OR' gate	Hima 42 300	TÜV Certified SIL4	1.10E-13
Fail Safe Driver Amplifier	Hima 32 100	TÜV Certified SIL4	6.2E-09
I.S. Isolator (Output)	MTL5025	Baseesfa Certified SIL3	0
Solenoid Valve	Eugen Seitz	TÜV Certified AK7	2E-08 (TBC)
ESD Valve (option 1)	Mokveld Valves	Independent 3rd	2.79E-07
		Party Review	
ESD Valve (option 2)	Bell Valves	TBC	3.82E-07 (1/3 yr Proof Test)
Sub-System	**Supplier**	**Fault Tolerance**	**Safe Failure Fraction**
Field Transmitter	Moore Industries type 345 XTC	0	96%
I.S.Isolator (Input)	MTL 5042-SR	0	92.5%
Fail SafeTrip Amp	Hima 62 100	1	90%-99%
Fail Safe Logic 'OR' gate	Hima 42 300	2	90%-99%
Fail Safe Driver Amplifier	Hima 32 100	2	90%-99%
I.S. Isolator (Output)	MTL5025	0	100%
Solenoid Valve	Eugen Seitz	TBC	TBC
ESD Valve (option1)	Mokvel Valves	TBC	TBC
ESD Valve (option2)	Bell Valves	TBC	TBC

Table 5 illustrates the generally accredited information now available on request (Note that the ESD Valve information is not accredited but it is based on comprehensive reports on the operational experience either independent or internal. The data therefore has a high degree of credibility).

SIL Calc

Component	Type/ Quantity	No of Ch	λ_{su} per year	λ_{du} per year	Architecture	β e	TI (j) in years	MTTR(g) in hours	PFD_{avg}
Sensor	a	1	2.56E-04	2.56E-04	1oo1		1	8	1.281E-04
I.S Isolator ^	b	1	1.40E-04	1.40E-04	1oo1		1	8	7.021E-05
Trip Amp	c	1	6.92E-06	6.92E-06	1oo1		1	8	3.467E-06
							1	8	
							1	8	
Logic modules							1	8	
							1	8	
							1	8	
Logic 'OR'	d	1	9.64E-10	9.64E-10	1oo1		1	8	4.827E-10
							1	8	
							1	8	
							1	8	
							1	8	
Driver Amplifier	e	1	5.43E-05	5.43E-05	1oo1		1	8	5.441E-05
							1	8	
							1	8	
							1	8	
							1	8	
Output I.S. Isolator	f	1	0.00E+00	0.00E+00	1oo1		1	8	0.000E+00
							1	8	
Solenoid Valve	g	1	1.75E-04	1.75E-04	1oo1		1	8	8.776E-05
ESD Valve	i	1	2.44E-03	2.44E-03	1oo1		0.33	8	4.055E-04

RESULTS			
	Overall PFDavg	=	7.495E-04
	Overall Fail to Danger Rate	=	
	IEC 61508 SIL	=	SIL 3

NOTE: WHEN WARNING DISPLAYED SIL

Table 6a: Pressure Measurement. Illustrates that a PFD consistent with SIL 3 is achievable using certified suppliers or suppliers with IEC 61508 experience. Remember that this is only part of the assessment and actually the SIL performance is limited to SIL 2 by the Hardware Integrity of several components ONLY the result of the LOWEST assessment applies.

SILCalc

Component	Type/ Quantity	No of Ch	A_{su} per year	A_{du} per year	Architecture	β e	TI (j) in years	MTTR (g) in hours	PFD_{avg}
Sensor	a	1	1.26E-03	1.26E-03	1oo1		1	8	6.319E-04
I.S Isolator *	b	1	1.40E-04	1.40E-04	1oo1		1	8	7.021E-05
Trip Amp	c	1	6.92E-06	6.92E-06	1oo1		1	8	3.467E-06
							1	8	
							1	8	
Logic modules							1	8	
							1	8	
							1	8	
Logic 'OR'	d	1	9.64E-10	9.64E-10	1oo1		1	8	4.827E-10
							1	8	
							1	8	
							1	8	
							1	8	
Driver Amplifier	e	1	5.43E-05	5.43E-05	1oo1		1	8	5.441E-05
							1	8	
							1	8	
							1	8	
							1	8	
Output I.S. Isolator	f	1	0.00E+00	0.00E+00	1oo1		1	8	0.000E+00
							1	8	
Solenoid valve	g	1	1.75E-04	1.75E-04	1oo1		1	8	8.776E-05
ESD Valve	h	1	2.44E-03	2.44E-03	1oo1		0.33	8	4.055E-04

RESULTS			
	Overall PFoDg	=	1.253E-03
	Overall Fail to Danger Rate	=	
	IEC 61508 SIL	=	SIL 2
			NOTE: WHEN WARNING DISPLAYED SIL

Table 6b: Temperature Measurement. Illustrates that a PFD consistent with SIL 2 is achievable using certified suppliers or suppliers with IEC 61508 experience. Hardware Integrity supports SIL 2.

Conclusion

Use accredited suppliers or equipment certified by an accredited body (or bodies).

Discussion

Reasons for using accredited suppliers or equipment:

1. Evidence is provided by the supplier in the form of either an accredited certificate or a formal report which documents the failure performance of the device. Hence, the task of the end user is minimised.
2. Typically, an assessment of a single sub-system (of the loop) will take 16-24 hours in the absence of supplier co-operation and this work will need documenting as evidence and the result may not be optimum or minimal risk.
3. Project costs and timescales are consequently significantly reduced.
4. Safety is optimised because subjectivity is removed.
5. Compliance with IEC 61508 is assured
6. Regulator concerns are minimised.
7. Assessment of embedded (or other) software has not been addressed in this article but it is a crucial part of the assessment as it was concerns about software reliability and safety which prompted the production of IEC 61508. A truly 'safe' assessment of such software as may be used in loop instruments is beyond the practical capability and competence of practising end user engineers. It is a specialist task which is being properly dealt with by the accredited bodies.

Note that this paper is intended to provide guidance only and is necessarily brief. None of the figures quoted here by example should be referenced without corroboration.