Introduction

A growing level of attention has recently been given to the automated control of potentially hazardous processes such as the overpressure or containment of dangerous substances. Several independent protection methods provide measures to reduce the risk from such hazards to personnel, the environment and assets. A significant level of this risk reduction is allocated to *safety instrumented functions* (SIF). The integrity of the *safety instrumented system* (SIS) to perform these functions (known as *functional safety*) is therefore critical and the requirements for determining and achieving functional safety are given in IEC 61511-1[REF 1]. This standard is now adopted as the predominant worldwide standard for such systems in the process industry.

The integrity requirements of the SIS have implications on all the elements that comprise the system such as sensors, interfaces, controllers, logic solvers, actuators and valves. All the connections that make up the complete control loop are also taken into consideration. One of the key instruments in this loop is the logic solver (decision maker), which initiates the final element to make the process safe if the need arises.

The aim of this paper is to explore some of the possibilities available to the SIS designer of a tank overfill protection system for the logic solver and to show examples of straightforward system topologies and their associated *safety integrity level* (SIL) calculations.

A general step-by-step procedure to define and evaluate an SIS is suggested in the Appendix. The examples used in this paper illustrate how the procedure is applied in specific cases.

Tank Overfill Protection System

A tank overfill protection system is a SIS that provides an additional layer of protection over the basic tank gauging (control) system. As with all SIS, the actual SIL needs to be established for the particular tank at the storage facility, taking into account all the operational risk factors, but typically these functions are SIL 1 or 2. It is important that the instrumentation used in the SIS is totally independent from that used in the tank gauging system so that it does not suffer interference from the latter or be subjected to common points of failure. It is expected that the overfill protection function automatically shuts off the input feed to the tank by isolating the pump and closing the input valve (ensuring that any resulting pipeline pressure surges are suitably dealt with). Tank level sensors can be degraded over time due to their exposed position both inside and outside the tank, and it is advantageous to use devices that have diverse technologies from the tank gauging sensors.

Factors Leading to the Choice of a Logic Solver

People can often assume the logic solver has to be a safety PLC. But in many cases a discrete logic device for each loop, which avoids the complications and expense of a programmable solution, is a sensible option. One of the objectives of functional safety is to engineer the protection layers so that the complexity of safety-related functionality is minimized. This includes designing the overall concept for the minimum number of safety instrumented loops, avoiding the unnecessary use of more complex technology and reducing interdependency between loops and keeping safety and non-safety functionality separate. IEC 61508-2[REF 2] and related standards demand a higher burden on the architectural design, which can often be avoided using less complex discrete logic solver technologies.

Apart from the obvious savings in cost from a simpler architecture, perhaps the biggest gains with this approach are unseen. Consider that this straightforward approach avoids the development cost of application programming (plus associated costs such as software maintenance, upgrades, configuration management and back-ups) and the need for specialist competence in operation and maintenance of the programmable platform. Installation, validation and commissioning of

complex programmable systems also require specific competence and procedures, which can make the functional safety management (FSM) system more onerous to set up and maintain.
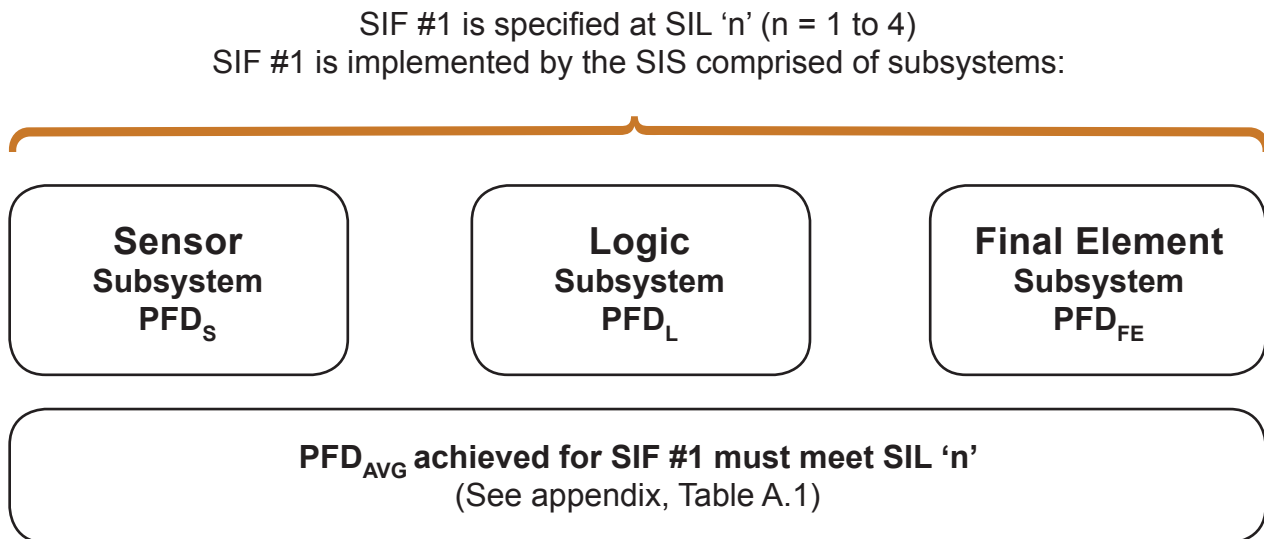
Many safety-related applications in the process industry are ideally suited to one or more single loop logic solvers because they are small scale, isolated or located in remote areas. As mentioned, the simpler architectural demands using this approach can reduce the cost of hardware, software and procedural overheads.

The Safety Integrity Level

The performance of a SIF is defined by the *safety integrity level* (SIL 1 to SIL 4). All elements that form the SIS must be designed or selected in accordance with the IEC 61508 or IEC 61511 standards. In practice, each SIF in an SIS typically consists of three subsystems that include one or more sensor elements, logic solver elements and final control elements, as required to meet the (highest) target SIL for the function(s) being performed (Figure 1).

Figure 1. *Subsystem of a SIF.*

SIF #1 is specified at SIL 'n' (n = 1 to 4)
SIF #1 is implemented by the SIS comprised of subsystems:

Sensor Subsystem PFD_S	**Logic** Subsystem PFD_L	**Final Element** Subsystem PFD_{FE}

PFD_{AVG} achieved for SIF #1 must meet SIL 'n'
(See appendix, Table A.1)

The three basic attributes of the SIS that require design consideration and evaluation in order to achieve the SIL are:

1) The **architectural constraints** for each subsystem are at least SIL 'n'

2) The **systematic capability** of each subsystem is at least SC 'n'

3) The **probability of failure on demand**, PFD_{AVG} is within (or <) the range for SIL 'n'

Each one of these attributes places requirements on the elements used in each subsystem.

Example Failure Data and Methodology

For the purposes of the examples in this paper, we shall assume that the elements included in these example SIFs have the following functional safety data available:

Table 1. SIF Device Safety Data.

Parameter	Level Sensor	Safety Trip Alarm	Actuated Valve
Dangerous Detected Failure Rate, λ_{DD} (per hr)	1.4E-07	1.7E-07	5.6E-07
Dangerous Undetected Failure Rate, λ_{DU} (per hr)	2.5E-08	8.6E-08	2.8E-07
Safe Failure Rate, λ_S (per hour)	1.36E-07	6.6E-07	4.5E-07
Safe Failure Fraction, SFF	90% to <99%	90% to <99%	60% to <90%
Type, A/B	Type A	Type B	Type A
Systematic Capability, SC	SC2	SC3	SC2

NOTE: The failure rates (and hence SFF) in the table above are indicated for the failure mode of the element that affects the SIF (e.g., closing of a feed valve if a tank overfill condition is detected). This is always a critical point for the system designer to note.

A simplified methodology to define and evaluate a SIS from element data that satisfies the three necessary attributes mentioned above is given in the Appendix of this paper, including the reference information needed from IEC 61508. (The reader might wish to study that first before looking at the examples of how it is implemented in the examples that follow).

NOTE: For the purposes of this paper, it shall be assumed that the system engineering from start to finish is performed in accordance with an appropriate functional safety management (FSM) system in accordance with [REF 4], clause 6.

SIL 1 Tank Overfill Protection System

Suppose the requirement is for a SIL 1 tank overfill protection system. We shall follow the steps shown in the methodology in the Appendix for this example.

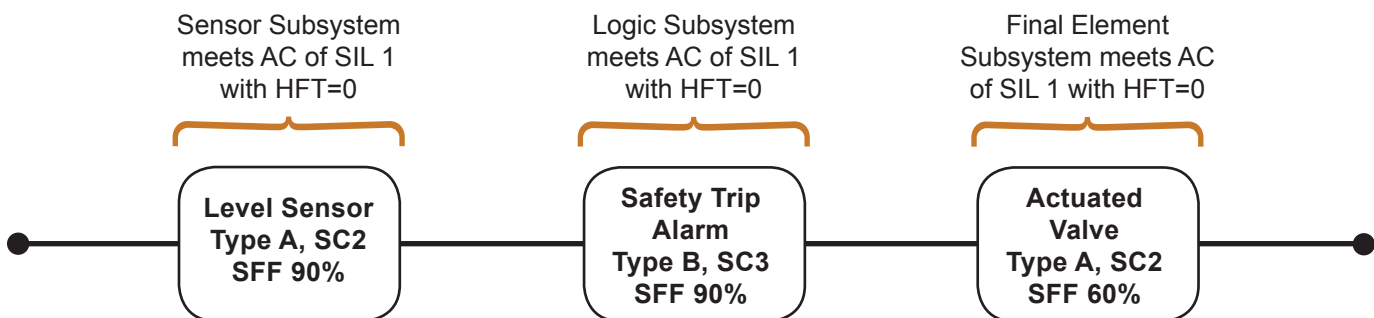### 1. Architectural Constraints (AC)

Subsystem	Comments Regarding Element Failure Data Provided in Table 1
Sensor	The level sensor is Type A and has SFF of 90-99%. With reference to Table A.2 in the Appendix, when used on its own (HFT = 0), the input subsystem has AC that (more than) meets SIL 1.
Logic	The STA logic solver is Type B and has SFF of 90 - 99%. With reference to Table A.2 in the Appendix, with HFT = 0, the logic subsystem has AC that (more than) meets SIL 1.
Final Element	The actuated valve is Type A and has SFF of 60-90%. With reference to Table A.2 in the Appendix, with HFT = 0, the output subsystem has AC that (more than) meets SIL 1.

2. Systematic Capabilities (SC)

Subsystem	Comments Regarding Element Failure Data Provided in Table 1
Sensor	The level sensor is SC2 which (more than) meets the requirements for SIL 1 when used on its own.
Logic	The STA logic solver is SC3 which (more than) meets the requirements for SIL 1 when used on its own.
Final Element	The actuated valve is SC2 which (more than) meets the requirements for SIL 1 when used on its own.

Figure 2. Reliability Block Diagram for the SIF Showing the AC and SC for Each Element.

Sensor Subsystem meets AC of SIL 1 with HFT=0

Logic Subsystem meets AC of SIL 1 with HFT=0

Final Element Subsystem meets AC of SIL 1 with HFT=0

Level Sensor Type A, SC2 SFF 90%

Safety Trip Alarm Type B, SC3 SFF 90%

Actuated Valve Type A, SC2 SFF 60%

The outcome of steps 1 and 2 above mean that a SIL 1 architecture for the system can be achieved with a single element in each subsystem. This is reflected in the reliability block diagram (RBD) in Figure 2 for the system:

3. Probability of Failure on Demand (PFD$_{AVG}$)

All three subsystems are based on a 1-out-of-1 (1oo1) voting architecture, for which the equation is:

$$PFD_{AVG} = (\lambda_{DU} + \lambda_{DD}) \, t_{CE}$$

Where the channel equivalent down time (t_{CE}) which is given by:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \, MTTR$$

For this example we shall will assume the following values:

Proof Test Interval, T$_1$ = 8,760 hrs (= 1 yr)	This must be confirmed by the operator and the PFD calculation re-performed if different from this assumption.
Mean time to repair, MTTR = 8 hrs	The a user parameter, so the comment about applies.

Now we need to calculate the PFD_{AVG} for each subsystem by referring to the failure data in Table 1 (above), the assumptions listed above for T1 and MTTR and the equations in the Appendix.

Sensor Subsystem (Level Sensor, 1oo1)

EQUATION	CALCULATION		RESULT
$\lambda_D = \lambda_{DD} + \lambda_{DU}$	1.4E-07 + 2.5E-08	=	1.65E-07
$t_{CE} = \dfrac{\lambda_{DU}}{\lambda_D}\left(\dfrac{T_1}{2} + MTTR\right) + \dfrac{\lambda_{DD}}{\lambda_D} MTTR$	(1.4E-08/1.65E-07)(8760/2+8)+(2.5E-07/1.65E-07)8	=	674
$PFD_{AVG} = (\lambda_{DU} + \lambda_{DD}) t_{CE}$	(2.5E-08 + 1.4E-07)674	=	1.11E-04

Logic Subsystem (Safety Trip Alarm, 1oo1)

EQUATION	CALCULATION		RESULT
$\lambda_D = \lambda_{DD} + \lambda_{DU}$	1.7E-07 + 8.6E-08	=	2.6E-07
$t_{CE} = \dfrac{\lambda_{DU}}{\lambda_D}\left(\dfrac{T_1}{2} + MTTR\right) + \dfrac{\lambda_{DD}}{\lambda_D} MTTR$	(8.6E-08/2.6E-07)(8760/2+8)+(1.7E-07/2.6E-07)8	=	1457
$PFD_{AVG} = (\lambda_{DU} + \lambda_{DD}) t_{CE}$	(8.6E-08 + 1.7E-07)1457	=	3.8E-04

Final Element Subsystem (Actuated Valve, 1oo1)

EQUATION	CALCULATION		RESULT
$\lambda_D = \lambda_{DD} + \lambda_{DU}$	5.6E-07 + 2.8E-07	=	8.4E-07
$t_{CE} = \dfrac{\lambda_{DU}}{\lambda_D}\left(\dfrac{T_1}{2} + MTTR\right) + \dfrac{\lambda_{DD}}{\lambda_D} MTTR$	(2.8E-07/8.4E-07)(8760/2+8)+(5.6E-07/8.4E-07)8	=	1468
$PFD_{AVG} = (\lambda_{DU} + \lambda_{DD}) t_{CE}$	(2.8E-07 + 5.6E-07)1468	=	1.2E-03

As explained in the Appendix, the PFD_{AVG} for the system is calculated from the sum:

$$PFD_{SYSTEM} = PFD_S + PFD_L + PFD_{FE}$$
$$= 1.1E-04 + 3.8E-04 + 1.2E-03$$
$$= \mathbf{1.7E-03}$$

Referring to Table A.1 (Appendix) shows this is comfortably in the **SIL 2** range (10^{-3} to $< 10^{-2}$).

> Note: That due to the relatively large uncertainties in the source values of component failure data, the results of failure analysis do not yield figures with high precision. Therefore, this means expressing results to more than two significant figures is of little value (and the implied precision could be misleading).

SIL 2 Tank Overfill Protection System

Now, suppose the requirement is for SIL 2. We will refer to the same element failure data and follow the same steps as above for the SIL 1 example and as given in the Appendix. For this example, we shall also assume that the user requirements specification has an additional requirement from the operator's functional safety policy that any SIL 2 applications shall use 1oo2 voting in the sensor subsystem for maintenance purposes.

1. Architectural Constraints

Subsystem	Comments Regarding Element Failure Data Provided in Table 1
Sensor	The level sensor is Type A and has SFF of 90-99%. With reference to Table A.2 in the Appendix it (more than) meets the AC requirements for SIL 2 on it's own. However, note that there is an additional requirement for 1oo2 voting due to the operator's policy for SIL 2 systems so HFT = 1 will be used.
Logic	The STA logic solver is Type B and has SFF of 90 - 99%. With reference to Table A.2 in the Appendix it meets the AC requirements for SIL 2 on it's own. However, because there are 2 sensors, each one needs to an STA, so HFT = 1.
Final Element	The actuated valve is Type A and has SFF of 60-90%. With reference to Table A.2 in the Appendix, with HFT = 0, it meets the AC requirements for SIL 2 on it's own.

2. Systematic Capability

Subsystem	Comments Regarding Element Failure Data Provided in Table 1
Sensor	The level sensor is SC2 which meets the requirements for SIL 2.
Logic	The STA logic solver is SC3 which (more than) meets the requirements for the SIL 2.
Final Element	The actuated valve is SC2 which meets the requirements for SIL 2.

The outcome of steps 1 and 2 above mean that voting is required in the sensor and logic subsystems to achieve the requirements for the system. This is reflected in the reliability block diagram (RBD) in Figure 3 for the system.
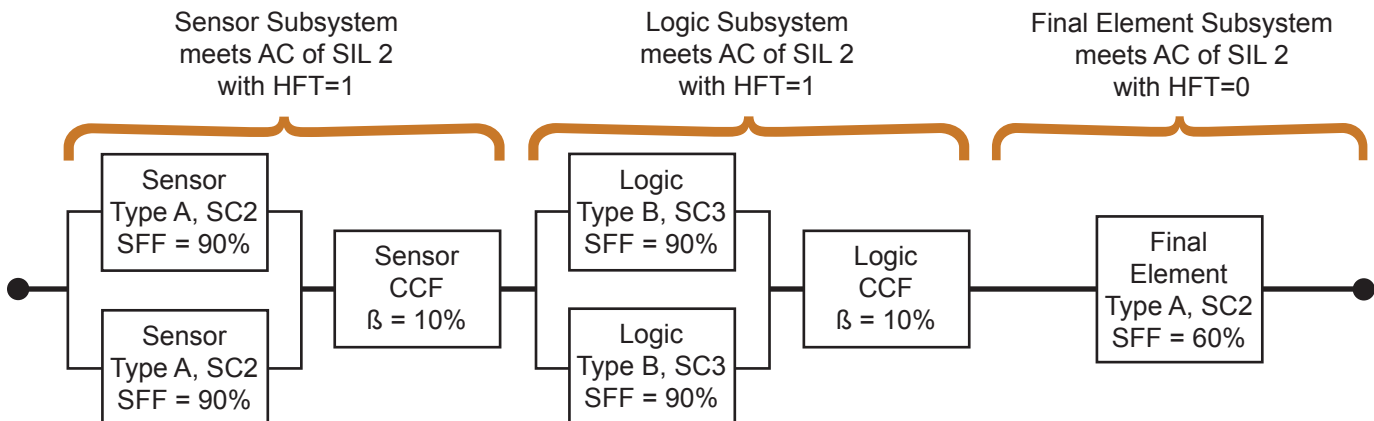
3. Probability of Failure on Demand

The equations to use for 1oo2 (sensors and logic) and 1oo1 (final element) architectures are shown in the Appendix.

For this example we will assume the following values:

Proof Test Interval, T_1 = 8,760 hrs (= 1 yr)	This must be confirmed by the operator and the PFD calculation re-performed if different from this assumption.
Mean time to repair, MTTR = 8 hrs	A user parameter - as comment above.
Common cause factor for undetected failures, ß = 10%	Typically this is in the range 3-10%. The strategies and justification are outside the scope of this paper (refer to IEC 61508 Part 2, clause 7.4.3.4 and 7.4.5.2d and Part 6 Annex D) hence a worst case of 10% is assumed for each instance in this example.
Common cause factor for detected failures, $ß_D$ = 10%	As comment above (a worst case figure is used).

As before, we need to calculate the PFD_{AVG} for each subsystem by referring to the failure data given in Table 1 (above), the assumptions listed above for T_1, MTTR, ß, $ß_D$ and the appropriate equation in the Appendix for the voting arrangement used.

Sensor Subsystem (Level Sensor, 1oo2)

EQUATION	CALCULATION		RESULT
$\lambda_D = \lambda_{DD} + \lambda_{DU}$	= $\quad$ 1.4E-07 + 2.5E-08	=	1.65E-07
$t_{CE} = \dfrac{\lambda_{DU}}{\lambda_D}\left(\dfrac{T_1}{2} + MTTR\right) + \dfrac{\lambda_{DD}}{\lambda_D}MTTR$	= (1.4E-08/1.65E-07)(8760/2+8)+(2.5E-07/1.65E-07)8	=	674
$t_{GE} = \dfrac{\lambda_{DU}}{\lambda_D}\left(\dfrac{T_1}{3} + MTTR\right) + \dfrac{\lambda_{DD}}{\lambda_D}MTTR$	= (2.5E-08/1.65E-07)(8760/3+8)+(1.4E-07/1.65E-07)8	=	452
$PFD_{AVG} = 6((1-ß_D)\lambda_{DD} + (1-ß)\lambda_{DU})^2 t_{CE}t_{GE}$ $+ ß_D\lambda_{DD}MTTR + ß\lambda_{DU}(T_1/2+MTTR)$	2((0.9x1.4E-07)+(0.9x2.5E-08)^2 674x452 + (0.1x1.4E-07x8) + (0.1x2.5E-08)((8760/2)+8)	=	1.11E-05

Logic Solver for Tank Overfill Protection

Logic Subsystem (Safety Trip Alarm, 1oo2)

EQUATION		CALCULATION		RESULT
$\lambda_D = \lambda_{DD} + \lambda_{DU}$	=	$1.7E\text{-}07 + 8.6E\text{-}08$	=	$2.6E\text{-}07$
$t_{CE} = \dfrac{\lambda_{DU}}{\lambda_D}\left(\dfrac{T_1}{2} + MTTR\right) + \dfrac{\lambda_{DD}}{\lambda_D} MTTR$	=	$(8.6E\text{-}08/2.6E\text{-}07)(8760/2+8)+(1.7E\text{-}07/2.6E\text{-}07)8$	=	1480
$t_{GE} = \dfrac{\lambda_{DU}}{\lambda_D}\left(\dfrac{T_1}{3} + MTTR\right) + \dfrac{\lambda_{DD}}{\lambda_D} MTTR$	=	$(8.6E\text{-}08/2.6E\text{-}07)(8760/3+8)+(1.7E\text{-}07/2.6E\text{-}07)8$	=	992
$PFD_{AVG} = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}(T_1/2+MTTR)$	=	$2((0.9\times1.7E\text{-}07)+(0.9\times8.6E\text{-}08)^2\ 1480\times992 + (0.1\times1.7E\text{-}07\times8) + (0.1\times8.6E\text{-}08)((8760/2)+8)$	=	$3.80E\text{-}05$

Final Element Subsystem (Actuated Valve, 1oo1)

EQUATION		CALCULATION		RESULT
$\lambda_D = \lambda_{DD} + \lambda_{DU}$	=	$5.6E\text{-}07 + 2.8E\text{-}07$	=	$8.4E\text{-}07$
$t_{CE} = \dfrac{\lambda_{DU}}{\lambda_D}\left(\dfrac{T_1}{2} + MTTR\right) + \dfrac{\lambda_{DD}}{\lambda_D} MTTR$	=	$(2.8E\text{-}07/8.4E\text{-}07)(8760/2+8)+(5.6E\text{-}07/8.4E\text{-}07)8$	=	1468
$PFD_{AVG} = (\lambda_{DU} + \lambda_{DD})\,t_{CE}$	=	$(2.8E\text{-}07 + 5.6E\text{-}07)1468$	=	$1.2E\text{-}03$

The PFD_{AVG} for the system is calculated from the sum:

$$PFD_{SYSTEM} = PFD_S + PFD_L + PFD_{FE}$$

$$= 1.11E\text{-}05 + 3.80E\text{-}05 + 1.2E\text{-}03$$

$$= \mathbf{1.3E\text{-}03}$$

Referring to Table A.1 (Appendix) shows this is comfortably in the **SIL 2** range (10^{-4} to $< 10^{-2}$)

Design, Installation and Operational Considerations

In the case where redundant channels are used to support a voting configuration (1oo2 in the SIL 2 overfill protection system), the voting is implemented by simply wiring the relay contacts from the two STA. This ensures that a trip from either STA will de-energize the solenoid, as shown in Figure 4.

Figure 4. *1oo2 STA Contact Wiring.*

Vs (Hot)   0V (Neutral)

1-A   2-A   Solenoid

STA1	STA2	TRIP
0	0	0
0	1	1
1	0	1
1	1	1
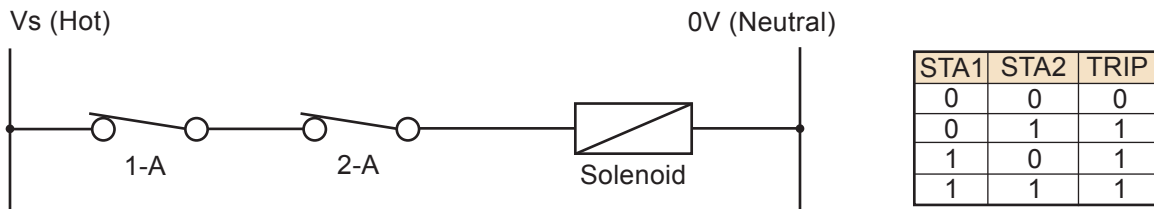
Conclusion

While the safety PLC approach offers advantages for installations where there are a high number of field I/O safety loops, in many plants the number of such loops is small. (Keeping the number to a minimum is an objective of safety engineering anyway). The benefits of avoiding software programming and all the related support and competence aspects (at the highest safety function SIL on the site) have already been mentioned. For the majority of plants where the safety functions may be few and/or physically widespread, discrete logic solutions are advantageous, (for example, savings in cable costs). The STA is easy to install with it's wide range of power supply options and it's small package that helps to keep it separate from the non-safety instrumentation. In the event of maintenance due to transients or failure, it can be readily swapped out at low unit and operational cost without interfering with the other processes in the plant. Local indication gives reassurance that the status of safety loops is reported directly.

This paper shows that design of Safety Instrumented Systems does not necessarily have to be based on an expensive and complex safety PLC system. Discrete logic devices such as the STA offer flexible, low- cost and user- friendly advantages which will be welcomed by many plant operators. While Safety Instrumented Systems design is for competent practitioners, this paper shows a straightforward approach to selecting the most suitable devices and performing the analysis to demonstrate the achievement of the required safety integrity level.

Logic Solver for Tank Overfill Protection

References and Bibliography

[REF 1] IEC 61511-1:2003 Functional safety – safety-instrumented systems for the process sector – framework, definitions, system, hardware and software requirements

[REF 2] IEC 61508-2:2010 Functional safety of E/E/PE safety-related systems – system requirements

[REF 3] IEC 61508-6:2010 Functional safety of E/E/PE safety-related systems – Guidelines on the application of IEC 61508-2 and IEC 61508-3

[REF 4] IEC 61508-1:2010 Functional safety of E/E/PE safety-related systems – general requirements

Useful Links

|	
Moore Industries Website	http://www.miinet.com
Functional Safety Poster	http://www.miinet.com/SafetySeries
The STA Data Sheet	http://www.miinet.com/InterfaceSolutionDownloadCenter/PopularProducts.aspx
IEC Functional Safety Website	http://www.iec.ch/functionalsafety/

Appendix - A General Procedure to Define a Safety Instrumented System

This appendix is intended to offer a simple methodology to design a SIS for a specific application that uses safety functions in the low demand mode. For further information IEC 61508-6[REF 3] should be consulted.

Figure A.1. SIS Subsystem Framework.
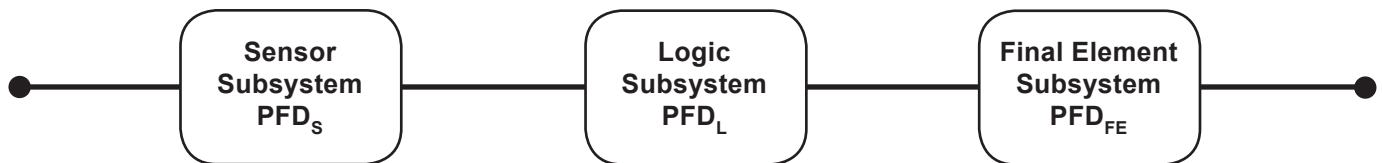
The 3-stage subsystem framework for a SIS, as described in IEC 61508, is shown in Fig A.1 above.

This representation can also be seen as a *Reliability Block Diagram* (RBD) model. As the model consists of three series blocks, the simple rule can be applied that the PFD (or failure rate, for that matter) for each block can be summed to establish the relevant parameter (PFD or λ) for the system. Hence:

$$PFD_S \ + \ PFD_L \ + \ PFD_{FE} \ = \ PFD_{SYSTEM}$$

When there are redundant elements in a subsystem (depicted as parallel blocks in the RBD), things are more complicated and this is covered later in this procedure.

The average PFD of the system that performs the safety function is one of the key parameters that define the SIL for the safety function, as given in IEC 61508-1[REF 4] Table 2:

Table A.1. SIL Ranges for Low Demand Safety Instrumented Functions.

Safety Integrity Level (SIL)	Average Probability of Failure on Demand (PFD$_{AVG}$) for a Low Demand Safety Function
SIL 4	$\geq 10^{-5}$ to $<10^{-4}$
SIL 3	$\geq 10^{-4}$ to $<10^{-3}$
SIL 2	$\geq 10^{-3}$ to $<10^{-2}$
SIL 1	$\geq 10^{-2}$ to $<10^{-1}$

The system PFD$_{AVG}$ will need to be divided between the three subsystems shown in Fig A.1. Although not in the Standard, a reasonable division that seems to be widely accepted is 35% : 15% : 50% to the sensor, logic and final element subsystems respectively. These provide realistic PFD targets for the subsystems to meet.

Logic Solver for Tank Overfill Protection

The other important reference information from the Standard that we shall need to refer to is the *architectural constraints* (IEC 61508-2 Tables 2 and 3):

Table A.2. Architectural Constraints of Type A and B Elements or Subsystems.

Safe Failure Fraction (SFF)	Type A Element or Subsystem (IEC 61508-2 Table 2) Hardware Fault Tolerance (HFT)			Type B Element or Subsystem (IEC 61508-2 Table 3) Hardware Fault Tolerance (HFT)		
	0	1	2	0	1	2
< 60%	SIL 1	SIL 2	SIL 3	NO SIL	SIL 1	SIL 2
60% - < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% - < 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

Unlike PFD, architectural constraints only apply to subsystems and elements (not systems); the SILs in the table are effectively the limit that the subsystem or element can be used in (unless further architectural measures are used).

Essentially, the procedure involves selecting elements from their failure modes and failure data that can be formed into the subsystems in the generic SIS shown in Figure A.1 above.

> NOTE: For the purposes of this simplified procedure, we shall assume that:
>
> -the elements being considered have already been preselected in terms of all their specifications to fulfill the functional, environmental and any other requirements of the system
>
> -the Safety Requirements Specification (IEC 61508 Phase 9 - which derives system requirements from the hazard and risk studies for the specific application) is being implemented by the system designer

Each step in the approach relates to each of the three basic attributes of the SIS that were listed earlier on page 2 of this paper.

1) First of all, consider the **architectural constraints** of each subsystem which need to meet the target SIL. Start by comparing the failure data of each element with the requirements in Table A.2 above for the target SIL with a HFT of 0 (i.e., the element on its own). If the type (A/B) and SFF indicate the target SIL is achieved, then no redundancy/voting for that element is required. If it is not achieved, then redundancy/voting of the element will be needed (HFT = 1 or 2 columns apply). Use the results of this step to form a *reliability block diagram* (RBD) model of the SIS (in the form shown in IEC 61508-2 Fig 6). Remember that if redundancy is required (shown as parallel blocks in the RBD), a series block should be added to model the common cause failure (CCF).

2) Check the **systematic capability** number for each subsystem is at least the same as that of the target SIL. If this cannot be achieved using the single or redundant elements as selected in step 1, it will be necessary to use redundant elements in such a manner that they will not suffer from common cause systematic failures.

> NOTE: From the two steps above, it should now be possible to determine the architecture of the SIS

3) Calculate the **PFD$_{AVG}$** of each subsystem from the dangerous failure rate of the element(s) to check it meets the proportion (35, 15 or 50%, as explained above) of the target SIL. This requires knowledge (or a conditional assumption at this stage) of the proof test interval (T_1) and the mean time to repair (MTTR) that will be used by the operator, both in hours. Here we shall use the PFD equations from IEC 61508-6[REF 3].

For the simple case where the subsystem is comprised of only one element (voting is 1oo1), the equation is:

$$PFD_{AVG} = (\lambda_{DU} + \lambda_{DD})\, t_{CE}$$

Where tCE (the channel equivalent down time) is:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

For a 1oo2 voted architecture, where the safety function is performed if at least one of the channels indicates a dangerous state in the EUC, the equation to use is:

$$PFD_{AVG} = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2\, t_{CE}\, t_{GE} + \beta_D\, \lambda_{DD}\, MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$$

Where ß is the common cause factor (CCF) for dangerous undetected failures, ß$_D$ is the CCF for dangerous detected failures, t_{CE} is as defined above and t_{GE} (the group equivalent down time) is:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

For a 2oo3 voted architecture, where the safety function is only performed if at least two of the channels indicate a dangerous state in the EUC, the equation to use is:

$$PFD_{AVG} = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2\, t_{CE}\, t_{GE} + \beta_D\, \lambda_{DD}\, MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$$

Where ß, ß$_D$, t_{CE} and t_{GE} are as defined above.

Once the PFD$_{AVG}$ quantities are established for each subsystem, the PFD$_{AVG}$ for the system is calculated from the sum:

$$PFD_{SYSTEM} = PFD_S + PFD_L + PFD_{FE}$$

If the resultant PFD$_{AVG}$ for the system does not meet the SIL, it may be possible to reduce the proof test interval until it does, assuming that this concludes with a realistic interval for the operator (otherwise further redundancy or diagnostics to produce lower failure rates and hence lower the PFD$_{AVG}$ may be an option).

Logic Solver for Tank Overfill Protection

Demand Moore Reliability • **www.miinet.com**

MOORE INDUSTRIES

United States • info@miinet.com	**Belgium • info@mooreind.be**	**China • sales@mooreind.sh.cn**
Tel: (818) 894-7111 • FAX: (818) 891-2816	**Tel: 03/448.10.18 • FAX: 03/440.17.97**	**Tel: 86-21-62491499 • FAX: 86-21-62490635**
Australia • sales@mooreind.com.au	**The Netherlands • sales@mooreind.nl**	**United Kingdom • sales@mooreind.com**
Tel: (02) 8536-7200 • FAX: (02) 9525-7296	**Tel: (0)344-617971 • FAX: (0)344-615920**	**Tel: 01293 514488 • FAX: 01293 536852**

www.miinet.com   - 14 -   *Moore* Industries-International, Inc.