Stochastic SIL Verification for Complex Safety Instrumented Systems

Sara Shahidi and Dr. Mehran Pourzand, Monaco Engineering Solutions Limited

To ensure a Safety Instrumented System (SIS) is capable of delivering its function with the required Safety Integrity Level (SIL), it is necessary for end users to conduct a SIL verification analysis. The Probability of Failure on Demand (PFD) is known as the main parameter for verifying SIL.

There are two main approaches for modelling of PFD for a Safety Instrumented Function (SIF). The first one is based on deterministic approach using steady-state availability equations. This approach is the most commonly used technique for simple standard systems with constant failure rates. The second approach is based on the application of Monte Carlo (MC) method, as a stochastic approach, to the determination of reliability and availability of complex system configurations with non-constant failure patterns.

This paper examines the stochastic approach as opposed to the deterministic approach for a low demand SIF. It is demonstrated that using the stochastic approach can give more realistic verification results in a SIL study. Using the MC technique gives the flexibility to the end user to ensure that the required SIL level is achieved considering both the input data uncertainties and system complexity.

Keywords: SIL, Verification, SIS, PFD, Monte Carlo, Stochastic, Input data uncertainties.

Introduction

Following a risk assessment study such as Hazard Identification (HAZID) or Hazard and Operability (HAZOP), it is necessary to evaluate the reliability of safety systems and ensure that they can deliver the required functions. This can be performed using assessment tools such as Risk Matrix, Risk Graph or Layers of Protection Analysis (LOPA). As a result of using these tools, the target reliability for the safety systems can be identified. The next step is to verify whether the safety system is capable of delivering the target reliability within the scope of design and operation.

This paper focuses on Safety Instrumented Systems (SIS) which are broadly used in process plants as highly reliable safety systems. They can be used to deliver the following three functions:

- Shutdown Function: Automatically take the process to the safe state;
- Permissive Function: Permit the process to move forward in a safe manner; and
- Mitigation Function: Take action to mitigate the consequence of an industrial hazard.

Based on above a SIS can be comprised of several Safety Instrumented Functions (SIF). The following are some simple examples of safety functions that a SIS can deliver:

- The level of condensate in a Knock Out Drum (KOD) upstream of a gas compressor is very high; the level transmitter initiates compressor shutdown upon a high high level of condensate in KOD;
- The main flame in a furnace fails. A flame detector in the furnace initiates Emergency Shutdown Valve (ESDV) to close feed fuel gas line upon failure of flame; and
- The water flow in a cooling system on a reactor goes down; the flow transmitter initiates the blowdown valve on the reactor to depressurise it upon low flow of the cooling water line.

Usually, SIFs are very effective in protecting plants from major accidents, however they are not perfect. Reliability assessments should be performed to ensure they SIFs are capable of meeting their target reliability level. This is often known as Safety Integrity Level (SIL) verification.

Safety Integrity is defined as the “probability of a safety related system satisfactorily performing the required function under all stated conditions within a stated period of time” [Ref. 1]. The level of safety integrity of a SIF is classified by four main categories as shown in Table 1. The SIL verification methodology aims to link the reliability of a SIF to the required Risk Reduction Factor (RRF) using its Probability of Failure on Demand (PFD). SIL 1 to 4 are mainly based on the range of RRF and PFD depending on demands rate.

Table 1 SIL Definition based on RRF and PFD for a low demand SIF[1]

SIL	RRF	PFD
4	10,000 to 100,000	$\geq 1x10^{-5} < 1x10^{-4}$
3	1,000 to 10,000	$\geq 1x10^{-4} < 1x10^{-3}$
2	100 to 1,000	$\geq 1x10^{-3} < 1x10^{-2}$
1	10 to 100	$\geq 1x10^{-2} < 1x10^{-1}$

1. This paper aims to focus on the requirements of low demand SIFs, a different methodology can be utilised for high demand SIFs which is not in scope of this study.

PFD is defined as the likelihood that a component will fail to perform its design function when required. This term is used to quantify loss of safety due to random hardware failures. Deterministic and stochastic approaches are two main approaches that can be used to quantify PFD for SIF's basic components. Either of these approaches can be applied for SIL verification; however selection of approach is strongly dependent on the level of accuracy and confidence required. The overall PFD of a SIF then can be defined using Fault Tree Analysis (FTA).

SIL Verification Methodology

The SIL verification methodology includes:

- Step 1: Identification of each SIF components such as initiator(s), logic solver(s) and final element(s);
- Step 2: Development of a fault tree using "AND", "OR" and "Voting" logics to represent each component within a SIF and the links between components. Reliability data can be used for each component using databases e.g. Failure Mode, Effect and Diagnostics Analysis (FMEDA) reports, Exida SIL Reports [Ref. 2] or Functional Safety Certificates and Offshore Reliability Data which is known as OREDA [Ref. 3 and 4]; and
- Step 3: An assessment to verify whether the SIL target can be achieved for each SIF.

Identification of SIF's Components

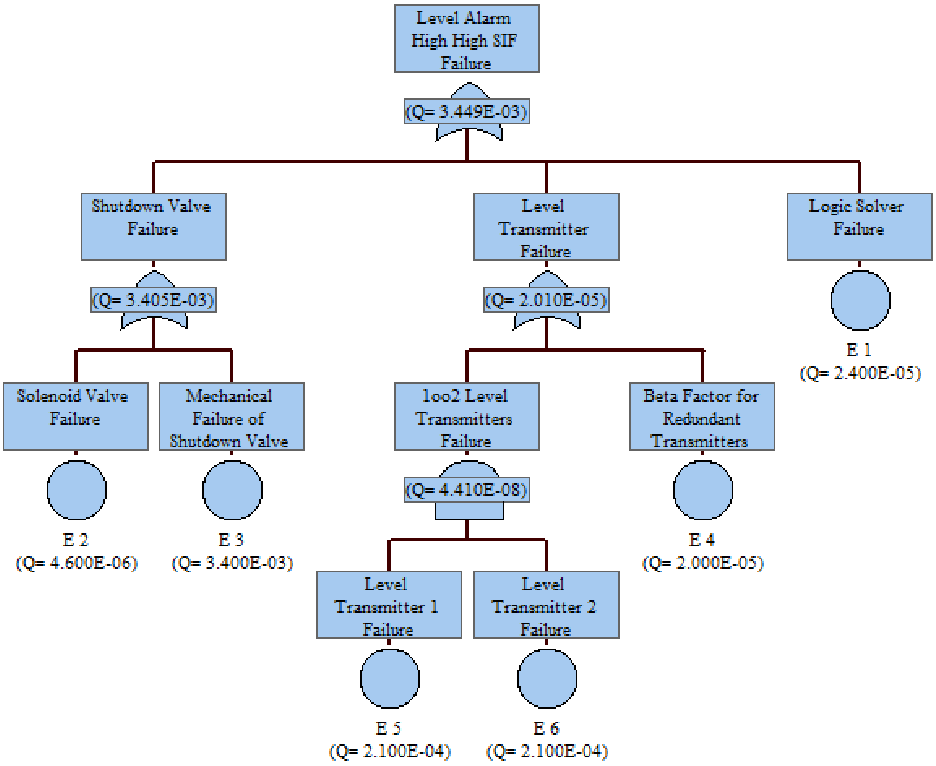
The SIF Loops can be defined from available SISs based on their operating functions. For the purposes of SIL verification, a SIF loop is defined as an individual input device and all its associated outputs. Usually a SIF loop is comprised of:

- Transmitter(s): such as level transmitter, temperature transmitter or pressure transmitter;
- logic solver(s): an automatic controller dedicated to the safety system; and
- Final element(s): such as shutdown valves, pump/compressor trip systems.

Fault Tree Development

A fault tree graphically represents the interaction of failures within a system. Basic events at the bottom of the fault tree are linked via logic symbols (e.g. gates) to the top event. The top event represents an identified hazard or a system failure mode for which predicted reliability or availability data is required. Figure 1 shows an example Fault Tree for a typical SIF.

Figure 1 FTA Example for a SIF



Each fault tree shows the components that could cause a failure of the safety critical function. Where there is redundancy designed into the system, an “AND” gate is used. Where one single item could cause failure, an “OR” gate is used. For a SIL study, the top event will be the PFD of an identified SIF loop. The following sections discuss the inputs required in constructing a fault tree.

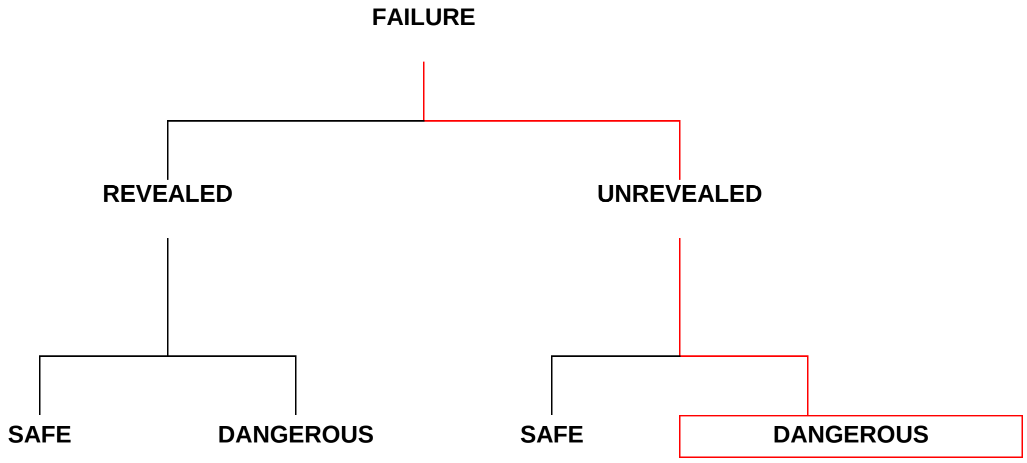
Reliability Data

One of the most important inputs into a fault tree is the failure rate data. The outcomes of the analysis are significantly influenced by the source of data that are used in the model. The most relevant reference is Failure Modes Effects and Diagnostics Analysis (FMEDA) for specific sub-systems. In the absence of FMEDA, there are a number of reliability data sources available such as Exida SIL Reports, OREDA Handbooks and Non-Electronic Parts Reliability Data (NPRD-95) [Ref. 5].

Failure Types

Failures may occur as “revealed” or “unrevealed”. Revealed failures will raise a signal to warn the operator of a component or equipment fault. Unrevealed failures are only determined once a demand is placed on a component or equipment to perform a specific function. These failures can also be further categorised as “safe” or “dangerous” failures. Both types should be considered carefully in the design and operability of an asset. The failure types are shown in Figure 2. Determination of the correct PFD is highly dependent on the appropriate identification/utilisation of failure category within the fault tree. Unrevealed” failures which are “dangerous” are considered to be most detrimental to an asset, particularly if that failure is associated with a protective device or safety system.

Figure 2 Failure Types for a Component



The failure of components may be random hardware or systematic failures. Random hardware failures are failures occurring at a random time which results from one or more of the possible degradation mechanisms in the hardware. Systematic failures are failures related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing procedures, documentation or other relevant factors.

Common Cause Failure

There is the potential for a Common Cause Failure (CCF) for systems with some degree of redundancy or a voting system. The β-Factor method was used to account for CCF [Ref. 7]. This method allows for CCF to be added onto the component’s PFD. Therefore, it limits the improvement in system PFD due to redundant components.

It is important to represent CCFs correctly as they often make a substantial contribution to the unavailability of redundant systems. A numerical value for β -factor can be determined using a checklist methodology based on the following criteria [Ref. 7]:

- Separation;
- Similarity (e.g. Redundancy/Diversity);
- Complexity;
- Analysis;
- Operating Procedures;
- Training;
- Environmental Control; and
- Environmental Testing.

Failure to determine the above factors may lead to an uncertainty in the value of CCF for the voting system.

Testing Interval

It is likely that unrevealed failures will occur within systems which are not in continuous operation. This may lead to undesirable consequences particularly if a system is classified as safety critical and is required to function on demand. Therefore, in order to protect against these potential consequences, it is necessary to reduce the number of unrevealed failures e.g. by periodic testing. These regular tests highlight safe and dangerous unrevealed failures prior to commissioning relevant corrective repairs. Periodic testing is fundamental to operations and it is widely understood that by increasing test frequency the PFD of the overall system can be reduced. Without an adequate testing regime in place, systems would continue to operate and become less reliable over time until reaching a state of failure. In fact, testing enhances the performance of a system or component during its "useful life" and avoids early replacement. However, it should be acknowledged that an increased testing regime will have a detrimental impact on plant availability due to increased planned downtime, which require a greater maintenance effort and increase operational expenditure.

SIL Verification

The verified SIL rating for each safety system is mainly based on the required PFD. There are two other factors for SIL verification: Hardware Fault Tolerance and Reponses Time. However, these factors have not been discussed in this paper.

The PFD term is used to quantify loss of safety due to random hardware failures and calculated using FTA. This value is then compared to the required SIL for the SIF stated in Section 0.This parameter includes the contribution from both Revealed and Unrevealed failures. The Revealed part of the PFD (PFDR) quantifies the loss of safety due to dangerous failures, during the period when it is known that the function is unavailable (with failure rate,λ_r). The average duration of this period is the MTTR or restoration time. The Unrevealed part of the PFD (PFDU) quantifies the loss of safety due to dangerous failures, during the period when it is not known that the function is unavailable (with failure rate, λ_u). The average duration of this period is the T/2, where T is test interval. Therefore PFD is PFDR + PFDU.

PFD calculation approaches

The following section discusses two main approaches of PFD calculations: deterministic and stochastic.

Deterministic Approach

Exact Approach

Markov chain has been used to estimate the PFD for critical safety systems based on the deterministic approach. It assumes that the probabilities of the system transitioning from one state to another are constant and that all failures rates and repair rates are constant. Firstly, Cycle Time which is the time from completion of one inspection to the start of the next one can be estimated as following:

$$\mathbf{Cycle\ Time = T + t_i + MTTR(1 - R(t)})\qquad\text{Equation 1}$$

Where:

R(t) is reliability of the failure distribution

t_i is inspection time

T is proof test interval (hours), which is the length of time that the item needs to last, before it is replaced.

MTTR is the Mean Time to Repair

The expected available time (uptime) during a cycle is given by:

$\text{Availability}=\int_0^T \mathrm{R(t)dt}$

Steady-state availability can be expressed as the ratio of the uptime to the cycle time:

$$A_m = \frac{\int_0^T R(t)dt}{T + t_i + MTTR[1 - R(T)]}$$

Where A_m is Mean availability

For the exponential distribution of Reliability: $R(t) = e^{-\lambda_U t}$,

Where:

λ_U is Unrevealed Dangerous Failure Rate (failures per hour)

Then,

$$A_m = \frac{1 - e^{-\lambda_U T}}{T + t_i + MTTR[1 - e^{-\lambda_U T}]}$$

Therefore, the mean unavailability of single Component is given by:

$$\mathbf{Q_m} = 1 - \mathbf{A_m} = \frac{\boldsymbol{\lambda_U T - (1 - e^{-\lambda_U T}) + \lambda_U\, t_i + \lambda_U . MTTR, (1 - e^{-\lambda_U T})}}{\boldsymbol{\lambda_U [T + t_i + MTTR(1 - e^{-\lambda_U T})]}}\qquad\text{Equation 2}$$

Where Q_m is mean unavailability

For the voting systems, if there are n identical equipment of which m must survive for the system to survive and r must fail for the system to fail:

$r = n - m + 1$

The probability of failure of this system, ${Q_m}/{n}$, within the proof test interval is:

$$Q_m/_n = \sum_{k=r}^{n} \binom{n}{k} . q.(t)^k \left(1 - q(t)\right)^{n-k}$$

Where q is mean unavailability of each equipment

The average probability of failure, $\emptyset_m/_n$ of the m-out-of-n system is:

$$\emptyset_m/_n = \frac{\int_0^T \sum_{k=1}^{n} \binom{n}{k} . q(t)^k \left(1-q(t)\right)^{n-k} dt}{T + t_i + MTTR.[1 - R(T)]}$$

For the exponential distribution, $q(t) = 1 - e^{-\lambda t}$, then

$$\emptyset_m/_n = \frac{\int_0^T \sum_{k=1}^{n} \binom{n}{k} \left(1 - e^{-\lambda t}\right)^k \left(e^{-\lambda t}\right)^{n-k} dt}{T + t_i + MTTR.[1 - e^{-\lambda T}]}$$

Critical Safety Unavailability (CSU) can be obtained from Equation 2 considering revealed and unrevealed failures:

$$CSU = \frac{-\lambda_R}{\lambda_R + \mu} e^{-(\lambda_R + \mu)t} + \frac{\lambda_R}{\lambda_R + \mu} + \frac{\lambda_U T - \left(1 - e^{-\lambda_U T}\right) + \lambda_U t_i + \lambda_U MTTR(1 - e^{-\lambda_U T})}{\lambda_u [T + t_i + MTTR(1 - e^{-\lambda_U T})]}$$

Where,

λ_R is Revealed Dangerous Failure Rate (failures per hour);

For the steady state availability (t → ∞) the above equation becomes:

$$CSU = \frac{\lambda_R}{\lambda_R + \mu} + \frac{\lambda_U T - \left(1 - e^{-\lambda_U T}\right) + \lambda_U t_i + \lambda_U MTTR(1 - e^{-\lambda_U T})}{\lambda_U [T + t_i + MTTR(1 - e^{-\lambda_U T})]}$$

$\mu = {1}/{MTTR}$, then

$$CSU = \frac{\lambda_r MTTR}{1 + \lambda_r MTTR} + \frac{\lambda_U T - \left(1 - e^{-\lambda_U T}\right) + \lambda_U t_i + \lambda_U MTTR(1 - e^{-\lambda_U T})}{\lambda_U [T + t_i + MTTR(1 - e^{-\lambda_U T})]}$$

Now for small values of $\lambda_U . T$ and $\lambda . MTTR$, CSU will be:

$$CSU = \lambda_R . MTTR + \frac{\lambda_U T}{2} + \frac{t_i}{T} + \lambda_U . MTTR$$

Or:

$$CSU = \lambda_D . MTTR + \frac{\lambda_U T}{2} + \frac{t_i}{T}$$

Now, as PFD does not include unavailability due to systematic failures i.e. t_i=0, so from above equations:

$$\mathbf{PFD} = \frac{\boldsymbol{\lambda_R} \mathbf{MTTR}}{\mathbf{1} + \boldsymbol{\lambda_R} \mathbf{MTTR}} + \frac{\boldsymbol{\lambda_U} \mathbf{T} - \left(\mathbf{1} - \mathbf{e}^{-\boldsymbol{\lambda_u} \mathbf{T}}\right) + \boldsymbol{\lambda_U} \mathbf{MTTR}(\mathbf{1} - \mathbf{e}^{-\boldsymbol{\lambda_U} \mathbf{T}})}{\boldsymbol{\lambda_U} [\mathbf{T} + \mathbf{MTTR}(\mathbf{1} - \mathbf{e}^{-\boldsymbol{\lambda_U} \mathbf{T}})]} \qquad \text{Equation 3}$$

and for small values of $\lambda_U . T$ and $\lambda . MTTR$, PFD will be:

$$PFD = \lambda_D . MTTR + \frac{\lambda_U T}{2} \qquad \text{Equation 4}$$

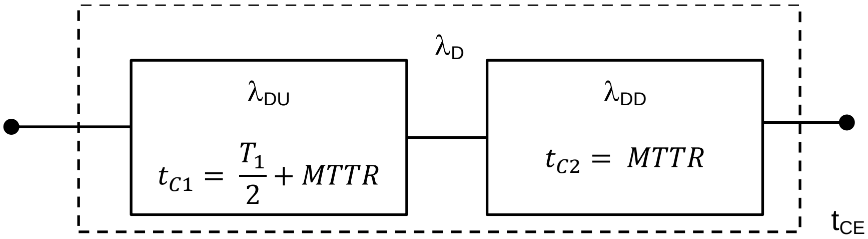
Where,

λ_D is Dangerous Failure Rate (failures per hour);

Simplified Approach

IEC 61508 and 61511 [Ref. 7 and 8] suggests a simplified version of the exact deterministic approach. Based on this, a channel equivalent mean down time t_{CE} is calculated for the 1oo1 (one-out-of-one) architecture consists of a single channel as shown in Figure 3.

Figure 3 1oo1 Architecture of a Safety Component



$$t_{CE} = \frac{\lambda_U}{\lambda_D}\left(\frac{T}{2} + \text{MTTR}\right) + \frac{\lambda_R}{\lambda_D}\text{MTTR}$$

The PFD is calculated from the channel mean down time and the dangerous failure rate as shown below.

$$\text{PFD} = 1 - e^{-\lambda_D t_{CE}}$$

Where,

$$\lambda_D = \lambda_U + \lambda_R$$

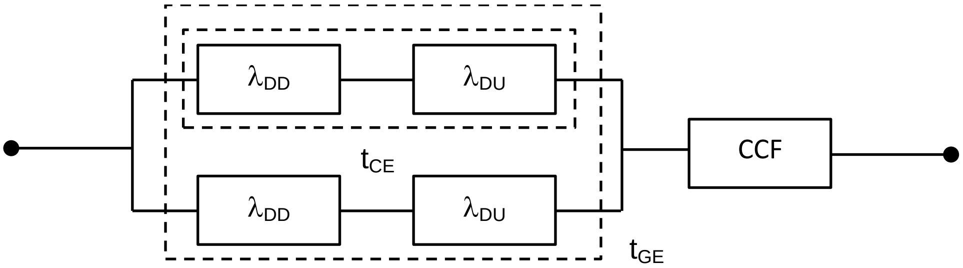
The above formula can be simplified for failure rates values of much smaller than 1 as below:

$$\mathbf{PFD} = \frac{\lambda_U \mathbf{TI}}{\mathbf{2}} + \lambda_D \ \mathbf{MTTR} \qquad \text{Equation 5}$$

This is same with Equation 4.

In 1oo2 architecture, as shown in Figure 4, two channels are connected in parallel and dangerous failures in both channels will have to occur at the same time for the whole configuration to fail on demand. These channels may also fail due to a single common cause failure.

Figure 4 1oo2 Architecture of a Safety Component



In addition to the t_{CE} defined earlier, IEC also considers a system equivalent down time, t_{GE}, in a 1oo2 architecture. t_{GE} and the average PFD are calculated using the following equations:

$$t_{GE} = \frac{\lambda_U}{\lambda_D}\left(\frac{TI}{3} + \text{MTTR}\right) + \frac{\lambda_R}{\lambda_D}\text{MTTR}$$

$$\mathbf{PFD} = \mathbf{2}\left((\mathbf{1} - \beta_D)\lambda_{DD} + (\mathbf{1} - \beta)\lambda_{DU}\right)^{\mathbf{2}} \mathbf{t_{CE} t_{GE}} + \ \beta\lambda_U\left(\frac{\mathbf{TI}}{\mathbf{2}} + \mathbf{MTTR}\right) + \beta_D\lambda_R \ \mathbf{MTTR} \qquad \textbf{Equation 6}$$

Where,

β is CCF factor for undetectable dangerous faults; and

β_D is CCF factor for detectable dangerous faults.

IEC also demonstrated simplified formulas for restricted numbers of voting systems such as 1oo3 and 2oo3.

Limitations of the Deterministic Approach

Regardless of whether the exact or simplified approach is used, there are some limitations using the deterministic method as it is not suitable for complex systems or dealing with input data with uncertainties. Basically, the deterministic approach is only suitable when steady-state availability is considered. Although it is reasonable to assume that repair rates are effectively constant over a long period of time, it is difficult to justify these for failure rates that increase with time. This can cause uncertainties in the final PFD results which cannot be resolved with deterministic approach.

Stochastic Approach

The stochastic approach has been used to consider uncertainties and complexities by using a range of input values for the PFD calculation. The methodology presented in this paper is based on the Monte Carlo (MC) technique and is capable of considering uncertainties for limiting factors such as test intervals, Mean Time to Failure (MTTF) and MTTR which all define the PFD.

MC is often used to calculate the expected outcome from a complex system and in some cases the probability distribution around that outcome where normal mathematical methods break down. MC works by generating several different samples of input parameters based on predefined probability distributions, calculating the outcome from each sample and calculating the average outcome from these samples. In complex systems, it is often necessary to run thousands of samples to find the true average due to the many combinations of possible inputs. The calculation of the PFD of the SIF not considering steady-state failure rates can be too complex for normal mathematical methods. An MC method is ideally suited to deal with this problem.

Generating random failure times

In order to calculate the average PFD using an MC method, a large number of samples must be run. The inputs to each sample are the failure times of each component. Each component has a known failure rate, λ, and this failure rate is assumed to be either constant or within a range of data.

Event sequencing and calculation of PFD

Once the failure time of each component has been calculated for a particular sample, the next step is to calculate the sequence in which events occur. This sequence of events will be dependent on the testing frequency and Diagnostic Coverage (DC) of the component. Determining when a failure of that component will be detected and the maintenance policy for the equipment e.g. is the component repaired immediately, is there a mobilisation time associated with the repair, does the system continue operating during the mobilisation for repair, etc.

Once the sequence of events is known, the amount of time that the system would fail to operate on demand can be calculated. This has already been defined as cycle time (Equation 3) and it is known here as $T_{C,i}$ for a particular sample, i.

The probability of failure on demand can be calculated for the particular sample, i:

$$PFD_i = \frac{T_{U,i}}{Tc,i}$$

To calculate the average PDF, thousands of samples must be run. The average PFD, for N samples, can be calculated using either of the following equivalent equations.

$$\boldsymbol{PFD_{avg}} = \frac{\sum_{i=1}^{N} \boldsymbol{PFD_i T_i}}{\sum_{i=1}^{N} \boldsymbol{T_i}} \qquad \text{Equation 7}$$

The calculation of the PFD for systems with more components is complicated by the fact that the order of failure and detection of the components determines and the time that the system would be in an unsafe condition. For these more complex systems diagrams have been constructed to illustrate all the possible sequences of events. More details will be described in Section 0.

In order to run the Monte Carlo simulation a macro is used to generate random numbers for a specified number of samples. The time spent in an unsafe condition and the cycle time is calculated and recorded for each sample and the average PFD is calculated using Equation 6.

Uncertainties in SIL Assessment

Uncertainty is defined in literatures as something “not definitely ascertainable or fixed” [Ref. 1]. Uncertainties in SIL assessment can reduce the validity of the results and the confidence in the achievable risk reduction level. The main contributors to uncertainty are model uncertainty, completeness uncertainty and data uncertainty. The main effect of the above uncertainties is on the estimation of PFD for the Safety Function due to the limitations of modelling real life systems and environment.

Model Uncertainty

SIL Assessment uses both architectural and reliability models in order to model a system’s characteristics. The architectural models represent the logic of the system and it is deterministic. However, reliability models are mainly based on probabilistic properties of the system. The uncertainty of the model depends on the validity of the model assumptions.

The system structure can be analysed and simplified into fault tree models which define the logic of system as series, parallel or voting systems. The uncertainty occurs when one system is a mixture of the named logics and separation of the components, to model system logic accurately, is not possible.

Precautions on modelling of a system depend on a trade-off between accuracy and simplification. More accurate system modelling may lead to undesirable complications which can increase the likelihood of mistakes and errors.

On the other hand, system structuring is also function of analyst competency, regulations, standards, guidelines and internal company policies. The model uncertainty is dependent on the validity of assumptions, approximation formulae and the software available. Although the above factors can be reduced by increasing engineering standards, some uncertainties always remain in models.

Completeness Uncertainty

This type of uncertainty is either not including part of the system in assessment or not considering unknown factors. One example is not considering different failure modes of a component or an incomplete scope of work.

Data Uncertainty

Insufficient failure related data in SIS causes statistical uncertainties in SIL assessment. The other reason for data uncertainty is when analysis is required for new technologies and early life of the system. To overcome data shortage in such assessments, assumptions are required to perform the assessment.

Generic databases are established to provide data for reliability assessment but they also introduce uncertainties due to lack of relevance. Difference in plant specific conditions like operational environment, maintenance procedures, collection methods and change in technology may result in inaccurate data usage. Such uncertainties can be overcome using MC methods.

Case Study

Example SIF

This section presents a case study where an FTA for PFD calculation has been examined based on deterministic and stochastic approaches. The SIF is comprised of Shutdown Valve (SDV), Logic Solver (LS) and sets of transmitters with 2oo3 voting system. The input data for failure rate, test intervals and structure of the model is available, but there are uncertainties in few of the input data as shown in Table 2. Fixed failure rate values (Most Likely) have been used for the deterministic approach whereas a range of failure rates (between Min and Max) have been used for the stochastic approach.

Table 2 Input Data to Fault Tree

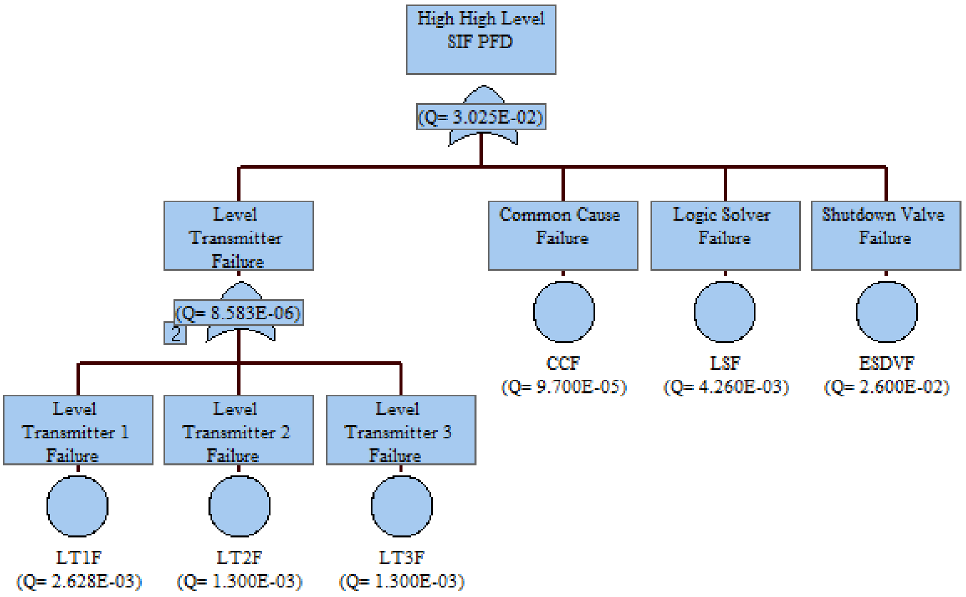
Component	Symbol	Parameter	Min	Most Likely	Max	T (hr)	MTTR (hr)
Level Transmitter 1	LT1	Failure Rate (per hour)	4.0E-07	6.0E-07	8.0E-07	8.8E+03	8
Level Transmitter 2	LT2	Constant Failure (PFD)	1.3E-03	1.3E-03	1.3E-03	-	-
Level Transmitter 2	LT3	Constant Failure (PFD)	1.3E-03	1.3E-03	1.3E-03	-	-
Common Cause Failure	CCF	Constant Failure (PFD)	6.4E-05	9.7E-05	1.3E-04	-	-
Logic Solver	LS	Failure Rate (per hour)	9.6E-07	9.7E-07	9.7E-07	8.8E+03	30
Shutdown Valve	SDV	Failure Rate (per hour)	1.0E-06	6.0E-06	1.1E-05	8.8E+03	30

Although the model is capable of handling uncertainty for all of the input data, the uncertainty has been considered for LT1, CCF and SDV. Other input data have been kept constant to avoid complication and to run the Monte Carlo model in a shorter period of time.

Deterministic Approach Results

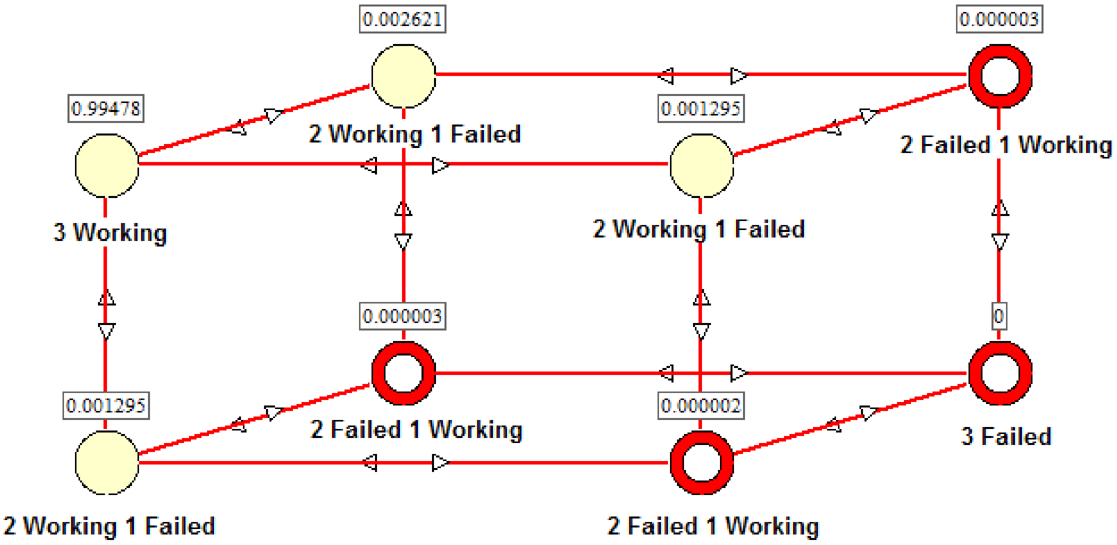
The deterministic approach has been used to perform the calculation for PFD of LT1, LS and ESDV. PFD for the rest is considered a constant value. The calculation for the voting system in level transmitters has also been done using the deterministic approach. The result for the deterministic approach is shown in Figure 5 and indicates that the PFD value is 3.03E-02. This means the SIF is capable of being a SIL 1 system.

Figure 5 FTA for High High Level SIF PFD Calculation



Markov chain has been used to analyse the probability of failure of the voting system (2oo3). The State Transition Diagram (STD) for all of the failed and passed states is shown in Figure 6.

Figure 6 State Transition Diagram for 2oo3 Voting System

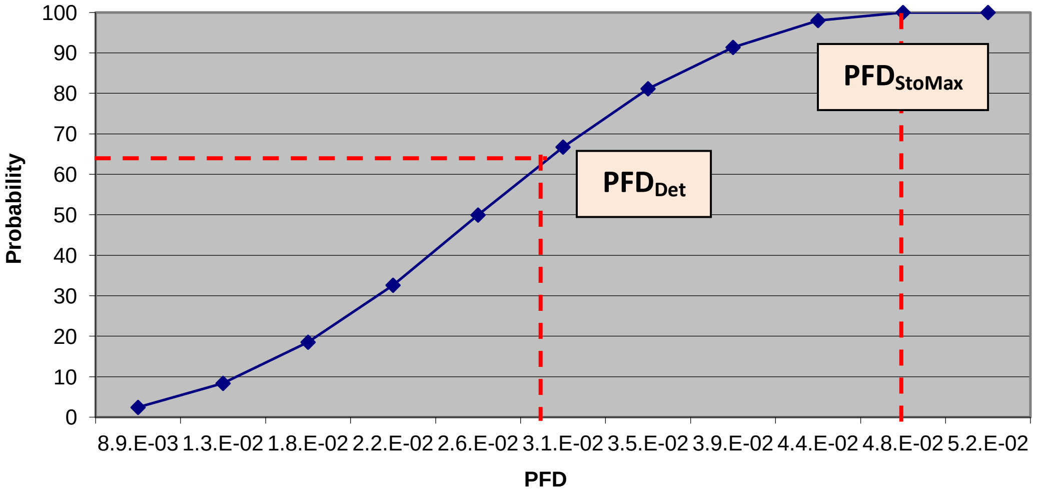


The yellow colour shows the states that the system will survive where the red colour shows the failure of system. The values above each circle show the system availability for that state.

Stochastic Approach Results

The MC method has been used to generate random numbers for failure rates and PFD of LT1, CCF and SDV using the triangular pattern. 7000 iterations have been run to generate more realistic results. The final PFD is not a constant number, but the calculation shows the probability of each PFD using cumulative approach as per Figure 7.

Figure 7 Probability of Cumulative PFD Results for High High Level SIF



The figure shows that, considering uncertainties, the probability of PFD being 3.05E-02 or less as per deterministic approach is only 65%. This means there is a possibility of 35% that PFD is greater than what has been calculated previously. It also demonstrates that the maximum value of PFD is 4.8E-02. This proves that, although the PFD value has been changed, the SIF is still capable of meeting SIL 1 requirement.

Conclusions

Two main approaches of PFD calculation for SIL verification have been explained in this paper: Deterministic and stochastic. It has been demonstrated that the deterministic approach is capable of handling typical systems with an acceptable level of accuracy. It is however, not capable of considering changes in input results due to uncertainties. The stochastic approach using the MC method, on the other hand, can be useful when a range of input data have been given instead of constant numbers. This will give flexibility in calculation of PFD for a variety of input data and ensure that SIL is verified with minimum simplifications and assumptions.

References

1. Webster, Webster's Encyclopedic Unabridged Dictionary, New York, Random House, 1989.
2. Safety Equipment Reliability Handbook, Exida, 3rd Edition, Volume 1, 2, and 3, November 2007.
3. OREDA 2009, Offshore Reliability Data Handbook, Published by OREDA Participants, Distributed by DNV Technica, Prepared by SINTEF Industrial Management, 5th Edition.
4. OREDA 2002, Offshore Reliability Data Handbook, Published by OREDA Participants, Distributed by DNV Technica, Prepared by SINTEF Industrial Management, 4th Edition.
5. Reliability Analysis Centre, Non-Electronic Part Reliability Data 1995, NRPD-95, PO Box 4700, Rome.
6. US Department of Defence Reliability Prediction of Electronic Equipment, MIL-HDBK-217F-2, 1995.
7. IEC standard 61508, Functional Safety of Electrical/Electronic/Programmable Electronic systems, 2010.
8. IEC standard 61511, Functional safety - Safety instrumented systems for the process industry sector, 2003.
9. Monaco Engineering Solutions Limited, Plant Simulation using Monte Carlo and Analysis Techniques (PLASMA) V 1.9.9.56, 2013.