MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

22nd Annual International Symposium
October 22-24, 2019 | College Station, Texas

Fault Tree Uncertainty Analysis

Raymond "Randy" Freeman*
S&PP Consulting
12303 Lake Shore Ridge
Houston, TX 77041
*Presenter E-mail: Rafree@yahoo.com

Abstract

Fault tree analysis (FTA) is a widely used methodology in the process industries. FTA is used for the development of failure mechanisms, computation of failure frequencies and the determination of the probability of failure on demand of safety systems. Much of the data used in a FTA study are uncertain. For example, the failure rate of a pump is often not known with great precision. Likewise the failure rates of instrumentation are often known only within some defined limits. The common practice, used by analysts in the quantification of a fault tree, is to use the most likely or best guess as to the needed failure rate data. The use of best guess values as data inputs to the quantification of a fault tree creates uncertainty in the computed results.

This paper presents a general methodology for the determination of the impact of uncertainty on the results of a fault tree study. The general methodology is based on the mathematics of propagation of error and variance contribution analysis. An example is presented to illustrate the application of the fault tree uncertainty analysis methodology to a real world problem.

Keywords: Quantitative Risk Assessment, Fault Tree Analysis, Uncertainty Analysis

1. Background

Fault tree analysis is a widely used method for representation of failure mechanisms in chemical plants. The methodology is described in the CCPS CPQRA guideline book [Ref. 1] and is extensively discussed in Chapter 9 of Lees [Ref. 2]. Lacking in these discussions is a systematic method to quantify the uncertainty of the results of the fault tree calculations.

Fault tree analysis has also been used in the aircraft and aerospace industries, nuclear power plant review and is recognized by the OSHA Process Safety Management (PSM) standard [Ref. 3] as a method for process hazards analysis.

2. Review of Error Propagation and Variance Contribution Analysis (VCA) Methodology

The mean and variance of a function of random variables can be approximated using the method described by Haugen [Ref. 4] and applied by Freeman [Ref. 5, 6, 7]. Define an arbitrary function of a set of random variables, x_i, as:

Let

$$Y = F(x_i) \quad \text{(Eq 1)}$$

The mean of Y can be estimated using the following approximation:

$$E(Y) = F[\, E(x_i)] \quad \text{(Eq 2)}$$

Where:

E(Y) = expected value of random variable Y = mean of Y

$E(x_i)$ = expected value of random variable x_i = mean of x_i

The variance of Y can likewise be estimated as:

$$V(Y) = \sum_{i=1}^{n} \left[\frac{\partial Y}{\partial x_i} \right]^2 V(x_i) \quad \text{(Eq 3)}$$

Where:

V(Y) = variance of random variable Y as defined above in Equation 1

$V(x_i)$ = variance of random variable x_i as defined above in Equation 1

Note that the variance is simply the square of the standard deviation. Using the variance will simplify the mathematics that is described below. The contribution of each independent random variable to the overall variance in the function is:

$$V(Y \text{ from } x_i) = \left[\frac{\partial Y}{\partial x_i} \right]^2 V(x_i) \quad \text{(Eq 4)}$$

The relative contribution of each term to the overall variance V(Y) is a measure of the importance in the uncertainty in the particular random variable, x_i. In effect, this is a sensitivity analysis combined with a uncertainty evaluation. The variance contribution combines the sensitivity in the answer to changes in the uncertain random variable, x_i, with a measure of the uncertainty in the random variable, x_i. The overall variance in Y is found by summing the sensitivity weighted variances from each random variable.

Numerical Estimate of the Sensitivity

Let us return to the fundamental definition of the derivative.

As before, set y = F(xi)

$$\frac{\partial y}{\partial x} = \lim_{\Delta xi \to 0} \left[\frac{F(xi + \Delta xi) - F(xi)}{\Delta xi} \right] \quad \text{(Eq 5)}$$

We are interested in a numerical estimate of the derivative. Therefore, we will make the following approximation.

$$\frac{\partial y}{\partial x} \sim \left[\frac{F(xi + \Delta xi) - F(xi)}{\Delta xi} \right] \quad \text{(Eq 6)}$$

Linear Functions

Let us examine the approximation for a simple linear function.

Let Y = AX + B (Eq 7)

What is the sensitivity of Y to a change in variable X? By simple calculus:

$$\frac{\partial y}{\partial x} = A \quad \text{(Eq 8)}$$

We can also find the sensitivity using the numerical approximation as:

$$\frac{\partial y}{\partial x} \sim \left[\frac{F(xi + \Delta xi) - F(xi)}{\Delta xi} \right] \quad \text{(Eq 9)}$$

$$\frac{\partial y}{\partial x} \sim \left[\frac{(A(xi + \Delta xi) + B) - (A(xi) + B)}{\Delta xi} \right] \quad \text{(Eq 10)}$$

$$\frac{\partial y}{\partial x} \sim \left[\frac{\big(A(xi + \Delta xi)\big) - (A(xi))}{\Delta xi} \right] \quad \text{(Eq 11)}$$

$$\frac{\partial y}{\partial x} \sim \left[\frac{\big((A\,xi + A\,\Delta xi)\big) - (A(xi))}{\Delta xi} \right] \quad \text{(Eq 12)}$$

$$\frac{\partial y}{\partial x} \sim \left[\frac{A\,\Delta xi}{\Delta xi} \right] \quad \text{(Eq 13)}$$

$$\frac{\partial y}{\partial x} = A \quad \text{(Eq 14)}$$

Note that for a simple linear equation the numerical result for the sensitivity is exactly the same as the analytical expression. There is no restriction on the size of the perturbation (Δxi) used in the

calculations. Previously, Freeman [Ref 7] has suggested using a 10% perturbation in xi to do the sensitivity calculations. However any size of perturbation will work and generate the correct sensitivity.

This is a general result. As long as the function can be expressed as a linear function of a number of variables, xi, the sensitivity can be directly calculated by a simple perturbation of the function. The resulting sensitivity will be exactly the same as would be obtained using analytical methods.

Non-Linear Expressions

In the quantification of a fault tree, the top event frequency is computed using failure rates of the component devices and time that measures the interval between system validations. In a minimal cut set of two or more basic events, the time variable may be the same. For example the test interval for a valve may be the same for a pressure transmitter. A minimal cut set involving both the valve and the pressure transmitter would create a 2rd order term in the test interval. If the test interval is uncertain, how do we compute the sensitivity of the top event frequency with respect to the test interval? We will now explore how to deal with this type of problem when completing the uncertainty analysis.

As before, let

$y = F(xi) = Axi^n + B$ (Eq 15)

What is the sensitivity of Y to a change in variable X? By simple calculus:

$\frac{\partial y}{\partial x} = nAxi^{n-1}$ (Eq 16)

Let us evaluate the numerical approximation for this case. If n=2, the function of interest is:

$y = F(xi) = Axi^2 + B$ (Eq 17)

From basic calculus, the exact analytical expression for the sensitivity is:

$\frac{\partial y}{\partial x} = 2\ A(xi)$ (Eq 18)

If xi = 1

$\frac{\partial y}{\partial x} = 2\ A$ (Eq 19)

Again the approximation of the derivative is:

$\frac{\partial y}{\partial x} \sim \left[\frac{(A(xi+\Delta xi)^2+B)-(Axi+B)}{\Delta xi}\right]$ (Eq 20)

$\frac{\partial y}{\partial x} \sim \left[\frac{F(xi+\Delta xi)-F(xi)}{\Delta xi}\right]$ (Eq 21)

Inserting the equation for F(xi) we obtain:

$\frac{\partial y}{\partial x} \sim \left[\frac{(A(xi+\Delta xi)^2+B)-(Axi+B)}{\Delta xi}\right]$ (Eq 22)

$$\frac{\partial y}{\partial x} \sim \left[\frac{(A\,(xi^2+2\Delta xi+\Delta xi^2)+B)-(Axi+B)}{\Delta xi}\right] \quad \text{(Eq 23)}$$

$$\frac{\partial y}{\partial x} \sim \left[\frac{A\,(xi^2+2\Delta xi+\Delta xi^2)-Axi}{\Delta xi}\right] \quad \text{(Eq 24)}$$

$$\frac{\partial y}{\partial x} \sim A\left[\frac{(xi^2+2\Delta xi+\Delta xi^2)-xi}{\Delta xi}\right] \quad \text{(Eq 25)}$$

Setting xi =1, and using a 10% perturbation as $\Delta xi = 0.1\ xi$ = 0.1

$$\frac{\partial y}{\partial x} \sim A\left[\frac{(1^2+(2)(0.1)1+0.1^2)-1}{0.1\ (1)}\right] \quad \text{(Eq 26)}$$

$$\frac{\partial y}{\partial x} \sim A\left[\frac{(2)(0.1)+0.01}{0.1}\right] \quad \text{(Eq 27)}$$

$$\frac{\partial y}{\partial x} \sim A\left[\frac{0.21}{0.1}\right] \quad \text{(Eq 28)}$$

$$\frac{\partial y}{\partial x} = 2.1\ \text{A} \quad \text{(Eq 29)}$$

Note that the numerical estimate (Eq 29) is approximately 5% greater than the analytical value (Eq 19). As shown in Table 1, for higher order equations the error will increase as the size of the perturbation becomes more important. Table 2 shows the impact of reducing the perturbation size to 1%. For 10th order variables (say a minimal cut set with 10 basic events) the error is 5%. For almost all engineering evaluations, a maximum error of 5% should be adequate.

For cases where the test frequency, repair time, or mission time appears in a minimal cut set 3 or more times, I suggest that the following perturbation in time be used to compute the sensitivity of the top event:

$$\Delta time = 0.01\ time \quad \text{(Eq 30)}$$

The sensitivity of the top event frequency to all uncertain variables can be computed using a perturbation of 1%.

$$\Delta xi = 0.01\ xi \quad \text{(Eq 31)}$$

3. Fault Tree Analysis

Fault trees are often used to analyze potential failures of an engineered system. A fault tree is a failure logic diagram that shows the relationship of device or system failures leading to an accident. Fault tree analysis is covered in detail in the CCPS CPQRA book [Ref. 1]. A fault tree is constructed by starting with a top event or condition and asking the question:

What conditions lead to this outcome?

Each condition in the next layer down is then analyzed by asking the same question. What conditions lead to this outcome? The logic of how these intermediate conditions (termed intermediate events) are related is expressed using AND and OR logic gates. An AND gate output is true if and only if (iff) all of the inputs to the AND gate are all true simultaneously. An OR gate output is true iff one of the inputs to the OR gate is true.

Once the fault tree logic structure is created, numerical data can be used to calculate the frequency or probability of the top event of concern occurring. For fault trees where a basic event is found in multiple branches of the tree, such as power failure, the logic structure of the tree must be simplified to remove the impact of the repeated events on the top event of concern. This simplification is done using Boolean Algebra. Each resulting grouping of basic events can cause the top event to occur. These groupings of basic events are called minimal cut sets. As a simple example consider the the Boolean Algebra representation of a fault tree :

T = BE11 + BE1 • BE2 + BE1 • BE3 + BE2 • BE9 + BE3 • BE7 (Eq 32)

Where:

T = Fault Tree Top Event

BE11 = Basic Event 11

BE1 = Basic Event 1

BE2 = Basic Event 2

BE3 = Basic Event 3

BE7 = Basic Event 7

BE9 = Basic Event 9

+ = Boolean Algebra Addition Symbol

• = Boolean Algebra Multiplication Symbol

For this example the top event T, the minimal cut sets are:

BE11

BE1 BE2

BE1 BE3

BE2 BE9

BE3 BE7

For example the existence of basic events BE1 and BE3 guarantees that the top event T will occur. Publically available standard computer software such as SAPHIRE [Ref. 8] may be used to find the minimal cut sets of a large fault tree.

The representation of the top event in equation 32 can now be used to compute the probability or frequency of occurrence of the top event. If the devices describe by the basic events are non-repairable and are tested after a period of time TI, the probability of top event, T, may be calculated as:

$$\text{Prob (T)} = \lambda_{11} TI/2 + (\lambda_1 TI/2)(\lambda_2 TI/2) + (\lambda_1 TI/2)(\lambda_3 TI/2) + (\lambda_2 TI/2)(\lambda_9 TI/2) + (\lambda_3 TI/2)(\lambda_7 TI/2) \quad \text{(Eq 33)}$$

Where:

λ_{11} = failure rate of device 11 in basic event BE11, failures per unit time

λ_1 = failure rate of device 1 in basic event BE1, failures per unit time

λ_2 = failure rate of device 2 in basic event BE5, failures per unit time

λ_3 = failure rate of device 3 in basic event BE3, failures per unit time

λ_7 = failure rate of device 7 in basic event BE7, failures per unit time

λ_9 = failure rate of device 9 in basic event BE9, failures per unit time

TI = test interval, time

Equation 33 assumes that the device failure rates are small and the product λ TI < 0.1. The other major assumption is that the values of all of the failure rates and test intervals are known. In reality the failure rate data are not known exactly with only a range or probability distribution representing the state of knowledge.

4. Example Problem

The following example is taken from the ISA technical report on fault tree analysis [Ref. 9]. This example should not be considered as a recommendation by either ISA or AIChE. The example is presented to allow for the demonstration of the methods that can be used in a fault tree study to quantify the uncertainty in the resulting calculated failure frequency or failure probability.

Consider the interlock on the intermediate storage tank T101 shown on Piping and Instrument Diagram in Figure 1. The interlock block diagram is shown in Figure 2. The interlock is intended to prevent an abnormal condition in the tank which could lead to a uncontrolled release of the tank contents. The process hazards analysis team has recommended that the interlock be designed to safety integrity level 2 (SIL 2) with a target probability of failure on demand (PFD) of no greater than 1E-2 or a risk reduction factor (RRF) of 100. Does the proposed interlock shown on Figure 1 meet the SIL 2 target? What is the uncertainty in the predicted PFD of the interlock?

A fault tree for the failure of this interlock is shown in Figure 3. A minimal cut set analysis has been completed and the resulting minimal cut sets are presented in Table 3. We can now write the Boolean Algebra equation that represents this fault tree as:

$$T = PE + TS1 \bullet TS2 + LS1 \bullet LS2 + FT1 \bullet FT2 + FT2 \bullet FT3 + FT1 \bullet FT3 + BV1 \bullet BV2 + BV1 \bullet SOL1 + BV2 \bullet SOL2 + SOL1 \bullet SOL2 + PT1 \bullet PT2 \quad \text{(Eq 34)}$$

Assuming that the interlock is non-repairable until tested at time TI and using lamda-time (λT) approximation of the failure rate, the Boolean representation of the fault tree may now be converted to a failure probability model as:

$$\text{Prob}(T) = \text{Prob}(PE) + (\lambda_{TS1}\,TI/2)(\lambda_{TS2}\,TI/2) + (\lambda_{LS1}\,TI/2)(\lambda_{LS2}\,TI/2) + (\lambda_{FT1}\,TI/2)(\lambda_{FT2}\,TI/2) + (\lambda_{FT2}\,TI/2)(\lambda_{FT3}TI/2) + (\lambda_{FT1}\,TI/2)(\lambda_{FT3}\,TI/2) + (\lambda_{BV1}\,TI/2)(\lambda_{BV2}\,TI/2) + (\lambda_{BV1}\,TI/2)(\lambda_{SOL1}TI/2) + (\lambda_{BV2}\,TI/2)(\lambda_{SOL2}\,TI/2) + (\lambda_{SOL1}\,TI/2)(\lambda_{SOL2}\,TI/2) + (\lambda_{PT1}\,TI/2)(\lambda_{PT2}\,TI/2) \quad \text{(Eq 35)}$$

Where:

Prob(PE) = failure probability of electronic logic solver, assumed to be constant at 5E-3.

λ_{TS1} = failure rate of temperature switch 1, failures per unit time

λ_{TS2} = failure rate of temperature switch 2, failures per unit time

λ_{LS1} = failure rate of level switch 1, failures per unit time

λ_{LS2} = failure rate of level switch 2, failures per unit time

λ_{FT1} = failure rate of flow transmitter 1, failures per unit time

λ_{FT2} = failure rate of flow transmitter 2, failures per unit time

λ_{FT3} = failure rate of flow transmitter 3, failures per unit time

λ_{BV1} = failure rate of block valve 1, failures per unit time

λ_{BV2} = failure rate of block valve 2, failures per unit time

λ_{SOL1} = failure rate of solenoid valve 1, failures per unit time

λ_{SOL2} = failure rate of solenoid valve 2, failures per unit time

λ_{PT1} = failure rate of pressure transmitter 1, failures per unit time

λ_{PT2} = failure rate of pressure transmitter 2, failures per unit time

TI = test interval, time

The electronic logic solver PE is assumed to have a constant failure probability of 5E-3.

Failure rate data for the other devices are present in Table 4. The mode (most likely value) of the failure rate is set equal to the point value taken from the ISA example [Ref. 9]. The triangular probability distribution (Appendix A) was assumed to represent the failure rate data for the equipment items. The upper and lower limits are based on the failure rate data of Appendix 4 of Smith [Ref. 10].

Using the device failure rates represented by the Table 4 column labeled as the mode and the minimal cut sets presented in Table 3, the ISA technical report [Ref.9, page 35] computes an interlock PFD as 7.5E-3 (RRF of 133). This would satisfy the requirement for a SIL 2 interlock {PFD of 1E-2 or a RRF of 100}. Now what is the uncertainty in the interlock PFD?

The first thing to remember is that the PFD should be calculated based on the mean value of the failure rate lambda (λ), not the mode of the failure rate. For a data set, the mean is the best single point representation of the data set. Table 5 presents the PFD of each minimal cut set using the mean of the device failure rate lambda (λ). The total of the PFD becomes 1.47E-2 (RRF of 68). This would not satisfy a SIL 2 interlock requirement.

Now we will compute the variance of the predicted probability of top event, T. To compute the variance of the probability of the top event, T, we will need to compute the sensitivity of the top event to each of the variables.

Sensitivity Using Numerical Perturbation Calculation

We will use the ISA interlock example previously analyzed by Freeman (Ref. 7). Using public data sources Freeman found that the probability of failure on demand (PFD) was 1.49E-2. To use the

perturbation method for the evaluation of the sensitivities requires evaluating the impact of small changes in the uncertain input parameters. To enable these calculations to be completed numbers using 8 significant digits were used. The calculations were completed using Microsoft Excel which uses double-precision floating-point arithmetic compliant with IEEE 754 specification. Excel nominally carries 15 significant figures in calculations. We will complete the calculations with Excel displaying 5 significant digits and round the result at the end of the calculations to 4 significant digits. We will illustrate the calculations by looking at the Flow Transmitter, FT1.

a. First we recalculate the PFD of the example and find it to be 1.4594E-02. This is the base number that we will use in the perturbation calculations.
b. We now make a small change in mean failure rate of FT1. The mean failure rate is 8E-6 failures/hour. A 1% perturbation is used or an increase of 0.08E-6 failures/hour.
c. The perturbed value of the failure rate of FT1 becomes (8 + 0.08) * 1E-6 failures/hour or 8.08E-6 failures/hour.
d. The perturbed value of the failure rate of FT1 is now used to re-calculate the PFD of the interlock. The resulting re-calculation finds that the PFD is 1.4618E-02
e. The change in the PFD from the base number due to the perturbation of the failure rate of FT1 is now computed as:

   delta PFD = 1.4618E-02 - 1.4594E-02 = 2.4556E-05

f. The sensitivity of the PFD to a change in the failure rate of FT1 is now computed by dividing the change in the PFD by the change FT1 failure rate as:

   sensitivity = (2.4556E-05)/(0.08E-6 failures/hour) = 307.0 hours
   Result is rounded to 4 significant digits.

We now note that in the paper by Freeman (Ref. 7) that equation 32 presents the sensitivity for FT1 as:

$$\frac{\partial Prob(T)}{\partial \lambda \mathrm{FT1}} = \text{ 307.0 hr} \qquad \text{(Eq 32 of Ref 7)}$$

The answers are exactly the same. The sensitivity calculations for all of the devices are presented in Table 6. Note that in every case the sensitivity found using the analytical expression and the numerical estimate are the same. This is a general result which will be true for all basic event equipment failure rates found in a fault tree minimal cut set.

Once found, the sensitivities can now be used to compute the variance contribution of each particular device to the overall variance of the top event PFD in the same manner as Freeman previously presented.

The sensitivities of the top event probability are summarized in Table 6. We may now compute the variance contribution of each uncertain variable using Equations 1 – 4 in the methodology section of this paper. The relative variance contribution is expressed as a percent of the total variance of the top event probability. The top event variance is found to be 8.24E-6 (failures per hour)^2 or equivalently the top event standard deviation is 2.78E-3 failures per hour.

In this example the variance (measure of uncertainty) is dominated by the flow transmitters. The flow transmitters account for almost 2/3 of the uncertainty in the top event probability. Failures of the flow transmitters appear in 3 of the minimal cut sets. Since the uncertainty in the transmitter

failure rates is large, the flow transmitters should contribute a significant amount to the variance of the fault tree top event.

We can use the variance in the top event to define the likelihood of achieving SIL 2 performance of the interlock. The calculations are done using the normal probability distribution. The normal distribution is tabulated as the standard normal distribution using a normalization factor Z.

The standard normal factor, Z, [Ref. 11] is defined as:

$$Z = \left[\frac{xi - E(x)}{\sigma}\right] \quad \text{(Eq 36)}$$

Where:

σ = standard deviation. Note that the variance of a random variable is the square of the standard deviation of the random variable.

E(x) = Expected value of the random variable x_i

For the example, the expected value of the probability of the top event of concern was calculated as

$$E[Prob(T)] = 1.47E\text{-}2 \quad \text{(Eq 37)}$$

From Table 4, the standard deviation in the probability of the top event is

$$\sigma_T = 2.78E\text{-}3 \quad \text{(Eq 38)}$$

The target PFD for a SIL 2 interlock must not be worse than 1E-2 (RRF of 100).

We compute the normal distribution Z factor at the SIL 2 target value as

$$Z = (0.01 - 0.0147)/2.78E\text{-}3 \quad \text{(Eq 39)}$$

$$Z = -1.69065 \quad \text{(Eq 40)}$$

Tabulations of standard normal distribution are presented in most statistics books such as Meyer [Ref. 11]. For this value of Z, the corresponding probability that the interlock will achieve SIL 2 performance is 4.55 percent. We can also compute the risk reduction that the proposed interlock design will achieve.

What is the interlock probability of failure on demand (PFD) that we can be 95% certain that the interlock will provide? At the 95% level, the corresponding Z factor is 1.65 [Ref 11]. We now compute the corresponding PFD of the interlock that corresponds to this Z factor.

$$Z = \left[\frac{x95\% - E[Prob(T)]}{\sigma}\right] \quad \text{(Eq 41)}$$

In this case:

$x_{95\%}$ = the PFD that we can be confident that the interlock will achieve

$$\sigma_T = 2.78E\text{-}3 \quad \text{(Eq 42)}$$

$$E[Prob(T)] = 1.47E\text{-}2 \quad \text{(Eq 43)}$$

$$Z = 1.65 \quad \text{(Eq 44)}$$

Rearranging equation 40 to find $x_{95\%}$we obtain:

$$x_{95\%} = E[Prob(T)] + Z\,\sigma_T \quad \text{(Eq 45)}$$

$$x_{95\%} = 1.47E\text{-}2 + (1.65)\,(2.78E\text{-}3) = 0.0193 \quad \text{(Eq 46)}$$

or a 95% certain risk reduction factor of

$$RRF = 1/PFD = 1/0.0193 = 52 \quad \text{(Eq 47)}$$

By the same logic there is 5% chance that the risk reduction is a PFD of 0.01 or an RRF of 99. In summary, this interlock is likely to perform as a mid-range SIL 1 interlock, not the SIL 2 interlock desired by process hazards analysis team.

5. Methodology for Fault Tree Uncertainty Analysis

We can now generalize the methods used in the above example to a proposed method for the evaluation of the uncertainty in a fault tree. The following step-by-step procedure is modified from that that previously published by Freeman (Ref 7) to indicate the use of numerical methods to compute the sensitivity. Step 8 shown in *italics* indicates the modification..

1. Create the fault tree using standard methods outline in the CPQRA book [Ref 1].
2. Determine minimal cut sets by hand or using standard computer software such as SAPHIRE [Ref 12].
3. Define the needed failure rate data for each basic event.
4. Define those basic events that are considered to be uncertain.
5. For the basic events that are uncertain, define the probability distribution and associated parameters needed to numerically define the probability distribution. Appendix B of this paper presents the needed description of 4 commonly used probability distributions. In many cases the triangular distribution will be selected. The minimum, maximum and mode (most likely) parameters will be needed for the triangular distribution.
6. Compute the mean of each of the uncertain variable
7. Compute the probability or frequency of the fault tree top event of interest using the mean value for each uncertain variable.
8. *Compute the sensitivity of the top event probability or frequency using the numerical methods outlined in this paper.*
9. Compute the variance of each of the uncertain variables
10. Compute the variance contribution of for each of the uncertain variables to the top event probability or frequency using equation 6.
11. Compute the total variance of the top event of interest probability or frequency by summing all of the contributions determined in Step 10.
12. Compute the variance contribution percent of each uncertain variable by dividing the variable contribution (Step 10) by the total variance of the top event of interest (Step 11).
13. Define the level of risk the project is willing to take. What chance will the project management accept for potential failure of the interlock to achieve the desired risk reduction? In the above example, I have used a 5% risk of failure or a 95% certainty that the interlock will achieve a risk reduction factor of 52. In the example, there is a very low probability that the interlock will achieve a SIL 2 PFD of 0.01 or an RRF of 100.

Alternately you can report the 90% range for the top event of interest. For the example the 90% range starts at the 5% RRF of 99 and there is a 95% certainty that that an RRF of at least 52 will be achieved. The expected risk reduction for this interlock is an RRF of 68.

6. Conclusions

A general procedure has been presented to quantify the uncertainty in calculations of failure frequencies using the fault tree methodology. The uncertainty analysis procedure is based on the application of propagation of error and variance contribution analysis techniques to the minimal cut sets created during a fault tree study. The procedure is simple and can be incorporated into standard fault tree analysis programs such as SAPHIRE [Ref 8]. This procedure is based on perturbation calculation of the frequency of the top event from changes in the uncertain variables. Incorporation of a numerical perturbation method into standard fault tree software such as SAPHIRE would be easy to implement and would provide the means for evaluation of the uncertainty in the quantified fault tree results.

For the example interlock presented in this paper, the uncertainty in the device failure rates degrades the predicted interlock SIL from meeting SIL 2 requirements to becoming a mid range SIL 1 interlock. This is a general result. Uncertainty in design parameters will reduce the likelihood that the equipment will achieve desired results. The design engineer has two choices:

- Accept the conclusion that the interlock will not perform as SIL 2
- Re-design the interlock using more reliable components to achieve the SIL 2 target

The variance contribution analysis shown in Table 7 indicates that the major contributor to the uncertainty in the interlock performance is the Flow Transmitters. Flow transmitters certified to SIL-2 or SIL-3 performance with lower failure rates could improve the calculated PFD of the interlock.

7. References

1. Center for Chemical Process Safety , *Guidelines for Chemical Process Quantitative Risk Analysis – 2rd edition*, American Institute of Chemical Engineers, New York, 2000.
2. Frank P Lees, Loss Prevention in the Process Industries – 2rd Edition, Butterworth, ISBN 0-7506-1547-8, Oxford, UK, 1996
3. US Department of Labor, Occupational Safety and Health Administration, CFR 1910.119 - Process Safety Management of Highly Hazardous Chemicals, 1910.119(e)(2)(vi).
4. Edward B. Haugen, *Probabilistic Approaches to Design*, John Wiley, New York, 1968
5. Raymond. Freeman and Angela Summers, "Evaluation of Uncertainty in Safety Integrity Level Calculations," *Process Safety Progress*, Published online in Wiley Online Library (wileyonlinelibrary.com) DOI 10.1002/prs. 11805, 2016
6. Raymond. Freeman, "General Method for Uncertainty Evaluation of Safety Integrity Level Calculations – Part 2 Analytical Methods," *Process Safety Process*, Published online in Wiley Online Library (wileyonlinelibrary.com) DOI 10.1002/prs 111915, October 2017

7. Raymond. Freeman ,“Error Propagation and Uncertainty Analysis: Application to Fault Tree Analysis”, Process Safety Progress, Published Wiley Online Library (wileyonlinelibrary.com/journal/prs) DOI: https://doi.org/10.1002/prs.12080, June 29, 2019
8. US Nuclear Regulatory Commission, “Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) – Version 8,” NUREG/CR-7039, Vol 3, June 2011.
9. ISA, “Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques Part 3: Determining the SIL of a SIF via Fault Tree Analysis, ISA Technical Report ISA-TR-84.00.02-2002 – Part 3, Approved 17 June 2002.
10. David J. Smith, *Reliability Maintainability and Risk – 8th Edition*, ISBN 978-0-08-096902-2, Elsevier, London, 2011
11. Paul L. Meyer, Introductory Probability and Statistical Applications, John Wiley, New York, 1972

Table 1. Comparison of Analytical Sensitivity with Numerical Approximation with Perturbation of 10% in xi for the equation: $y = F(xi) = Axi^n + B$

Order of Equation n	Equation for Analytical Sensitivity $\frac{\partial y}{\partial x} = nAxi^{n-1}$	Sensitivity with xi = 1 and A=1	Numerical Sensitivity with $\Delta xi = 0.1\ xi$	Error %
1	$\frac{\partial y}{\partial x} = 1A(xi)^0$	1	1	0
2	$\frac{\partial y}{\partial x} = 2A(xi)^1$	2	2.1	5
3	$\frac{\partial y}{\partial x} = 3A(xi)^2$	3	3.31	-10%
4	$\frac{\partial y}{\partial x} = 4A(xi)^3$	4	4.64	-16%
5	$\frac{\partial y}{\partial x} = 5A(xi)^4$	5	6.11	-22%
6	$\frac{\partial y}{\partial x} = 6A(xi)^5$	6	7.72	-29%
7	$\frac{\partial y}{\partial x} = 7A(xi)^6$	7	9.49	-36%
8	$\frac{\partial y}{\partial x} = 8A(xi)^7$	8	11.44	-43%
9	$\frac{\partial y}{\partial x} = 9A(xi)^8$	9	13.58	-51%
10	$\frac{\partial y}{\partial x} = 10A(xi)^9$	10	15.94	-59%

Error = (Analytical- Numerical)/Analytical

Table 2. Comparison of Analytical Sensitivity with Numerical Approximation with Perturbation of 1% in xi for the equation: $y = F(xi) = Axi^n + B$

Order of Equation n	Equation for Analytical Sensitivity $\frac{\partial y}{\partial x} = nAxi^{n-1}$	Sensitivity with xi = 1 and A=1	Numerical Sensitivity with $\Delta xi = 0.1\ xi$	Error %
1	$\frac{\partial y}{\partial x} = 1A(xi)^0$	1	1	0
2	$\frac{\partial y}{\partial x} = 2A(xi)^1$	2	2.01	-1%
3	$\frac{\partial y}{\partial x} = 3A(xi)^2$	3	3.03	-1%
4	$\frac{\partial y}{\partial x} = 4A(xi)^3$	4	4.06	-2%
5	$\frac{\partial y}{\partial x} = 5A(xi)^4$	5	5.10	-2%
6	$\frac{\partial y}{\partial x} = 6A(xi)^5$	6	6.15	-3%
7	$\frac{\partial y}{\partial x} = 7A(xi)^6$	7	7.21	-3%
8	$\frac{\partial y}{\partial x} = 8A(xi)^7$	8	8.29	-4%
9	$\frac{\partial y}{\partial x} = 9A(xi)^8$	9	9.37	-4%
10	$\frac{\partial y}{\partial x} = 10A(xi)^9$	10	10.46	-5%

Error = (Analytical- Numerical)/Analytical

Table 3. Basic Events in Minimal Cut Sets For Example

Cut Set No	BE 1	BE 2
1	PE	-
2	TS1	TS2
3	LS1	LS2
4*	FT1	FT2
5*	FT2	FT3
6*	FT1	FT3
7*	BV1	BV2
8*	BV1	SOL1
9*	BV2	SOL2
10*	SOL1	SOL2
11	PT1	PT2

* Minimal cut Set with same basic event as another cut set

Table 4. Lamda (λ) Failure Rate Data With Uncertainty Limits

Device	Minimum Failures per 1E6 Hours	Mode Failures per 1E6 Hours	Maximum Failures per 1E6 Hours	Mean Failures per 1E6 Hours	Lamda Variance (Failures per 1E6 Hours)^2
Flow Transmitters FT1, FT2 and FT3	1.0	2.9	20.0	8.0	18.3
Pressure Transmitters PT1 and PT2	1.0	2.3	20.0	7.8	18.8
Temperature Switch TS1 and TS2	3.0	7.6	20.0	10.2	12.9
Level Switch LS1 and LS2	2.0	4.6	20.0	8.9	15.8
Block Valves BV1 and BV2	0.2	2.3	10.0	4.2	4.4
Solenoid Valves SOL1 and SOL2	1.0	2.3	8.0	3.8	2.3

Table 5. Probability of Minimal Cut Sets Based on Mean Failure Rates

Cut Set No	BE 1	BE 2	PFD based on mean λ
1	PE	-	5.00E-03
2	TS1	TS2	2.00E-03
3	LS1	LS2	1.52E-03
4	FT1	FT2	1.23E-03
5	FT2	FT3	1.23E-03
6	FT1	FT3	1.23E-03
7	BV1	BV2	3.38E-04
8	BV1	SOL1	3.38E-04
9	BV2	SOL2	3.38E-04
10	SOL1	SOL2	2.77E-04
11	PT1	PT2	1.17E-03

Table 6. Sensitivity of Example System PFD to Basic Event Failure Rates Based on a 1% Perturbation

Basic Event Label	Device Type	Mean Failures per 1E6 Hours	Failure Perturbation of 1% of Mean Failures per 1E6 Hours	Perturbed Failure Rate Failures per 1E6 Hours	Total System PFD Using Peturbed Failure Rate of Basic Event	Change in Total System PFD	Sensitivity of PFD to Change in Failure Rate Hours
FT1	Flow Transmitter	8	0.08	8.08	1.461848E-02	2.455603E-05	307.0
FT2	Flow Transmitter	8	0.08	8.08	1.461848E-02	2.455603E-05	307.0
FT3	Flow Transmitter	8	0.08	8.08	1.461848E-02	2.455603E-05	307.0
PT1	Pressure Transmitter	7.8	0.078	7.878	1.460560E-02	1.167179E-05	149.6
PT2	Pressure Transmitter	7.8	0.078	7.878	1.460560E-02	1.167179E-05	149.6
TS1	Temperature Switch	10.2	0.102	10.302	1.461389E-02	1.995945E-05	195.7
TS2	Temperature Switch	10.2	0.102	10.302	1.461389E-02	1.995945E-05	195.7
LS1	Level Switch	8.9	0.089	8.989	1.460912E-02	1.519596E-05	170.7
LS2	Level Switch	8.9	0.089	8.989	1.460912E-02	1.519596E-05	170.7
BV1	Block Valves	4.2	0.042	4.242	1.460037E-02	6.445958E-06	153.5
BV2	Block Valves	4.2	0.042	4.242	1.460037E-02	6.445958E-06	153.5
SOL1	Solenoid Valves	3.8	0.038	3.838	1.459976E-02	5.832058E-06	153.5
SOL2	Solenoid Valves	3.8	0.038	3.838	1.459976E-02	5.832058E-06	153.5

Table 7. Variance of Top Event Probability Due to Uncertain Device Failure Rates

Device No	Device Type	Label	Sensitivity of Top Event Probability to Device Failure Rate $Hour^{-1}$	Variance of Device Failure Rate (Failures per 1E6 $Hour)^2$	Variance Contribution to Top Event Variance	Contribution to Top Event Variance %
1	Logic Solver	PE	-	0	0.00E+00	0%
2	Temperature Switch	TS1	195.7	12.9	4.94E-07	6%
3	Temperature Switch	TS2	195.7	12.9	4.94E-07	6%
4	Level Switch	LS1	170.7	15.8	4.60E-07	6%
5	Level Switch	LS2	170.7	15.8	4.60E-07	6%
6	Flow Transmitter	FT1	307	18.3	1.72E-06	21%
7	Flow Transmitter	FT2	307	18.3	1.72E-06	21%
8	Flow Transmitter	FT3	307	18.3	1.72E-06	21%
9	Block Valve	BV1	153.5	4.4	1.04E-07	1%
10	Block Valve	BV2	153.5	4.4	1.04E-07	1%
11	Pressure Transmitter	PT1	149.6	18.8	4.21E-07	5%
12	Pressure Transmitter	PT2	149.6	18.8	4.21E-07	5%
13	Solenoid valve	SOL1	153.5	2.3	5.42E-08	1%
14	Solenoid valve	SOL2	153.5	2.3	5.42E-08	1%

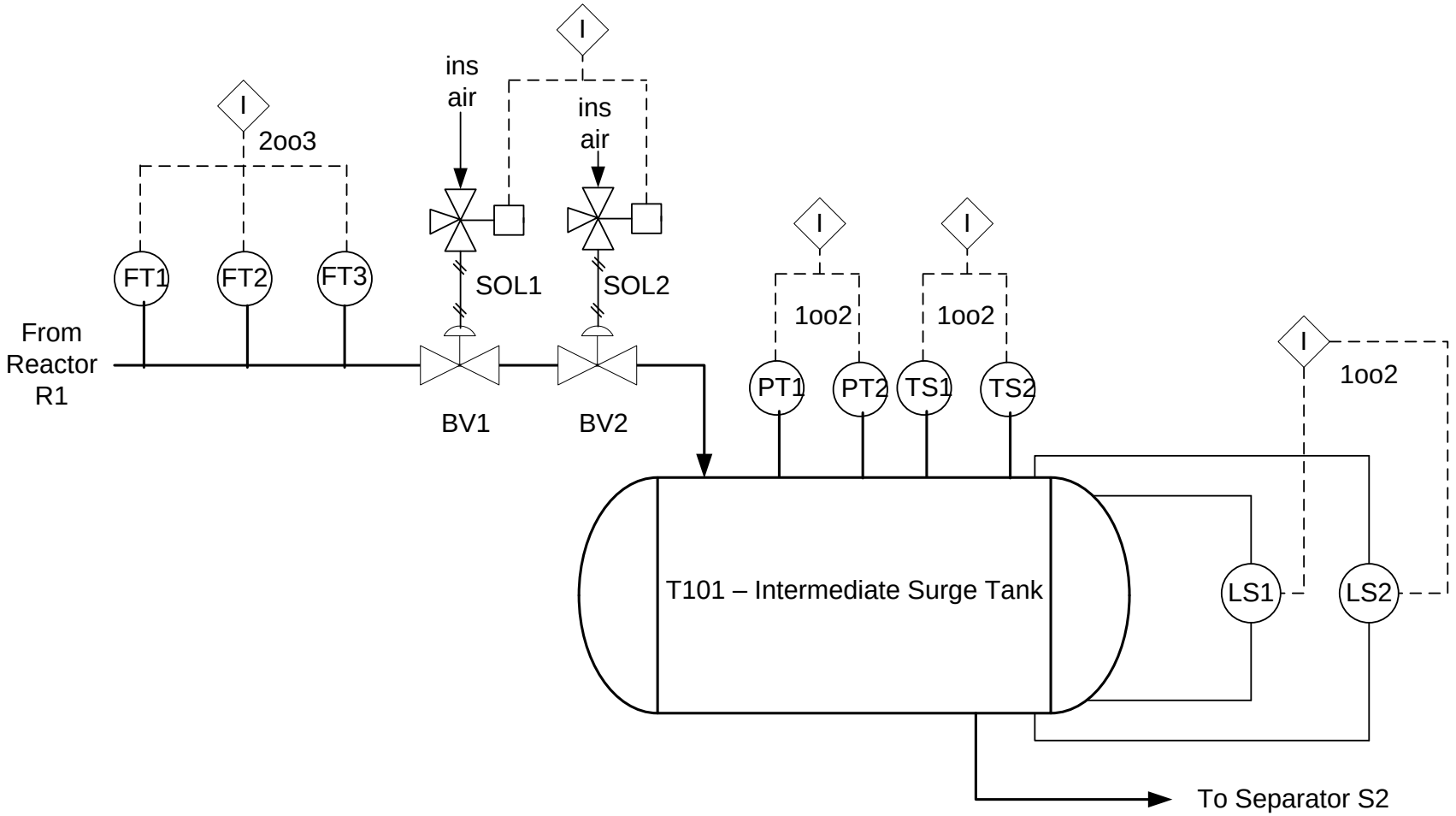

Figure 1. P&ID Diagram for Example

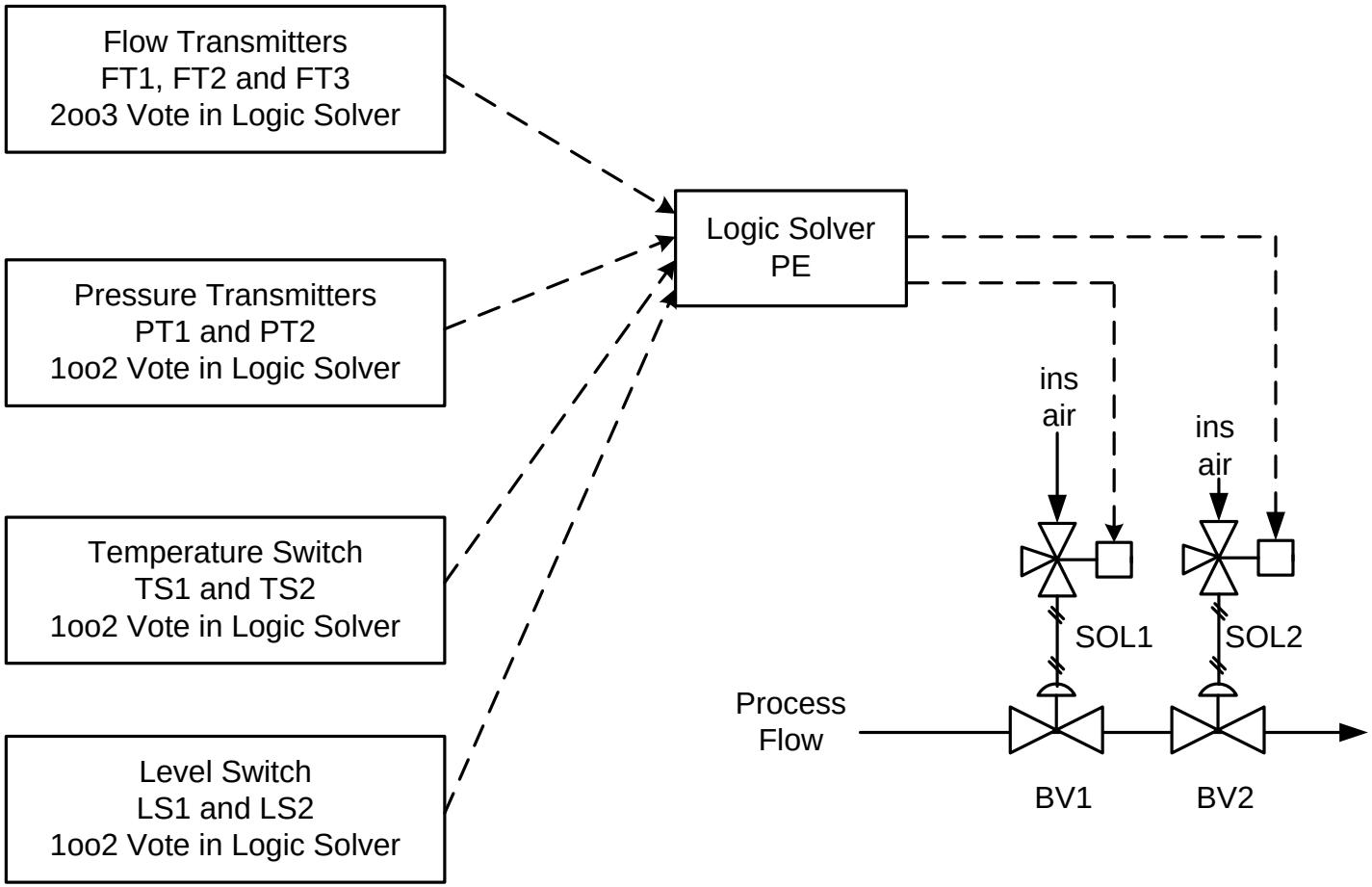

Figure 2. Interlock Block Diagram

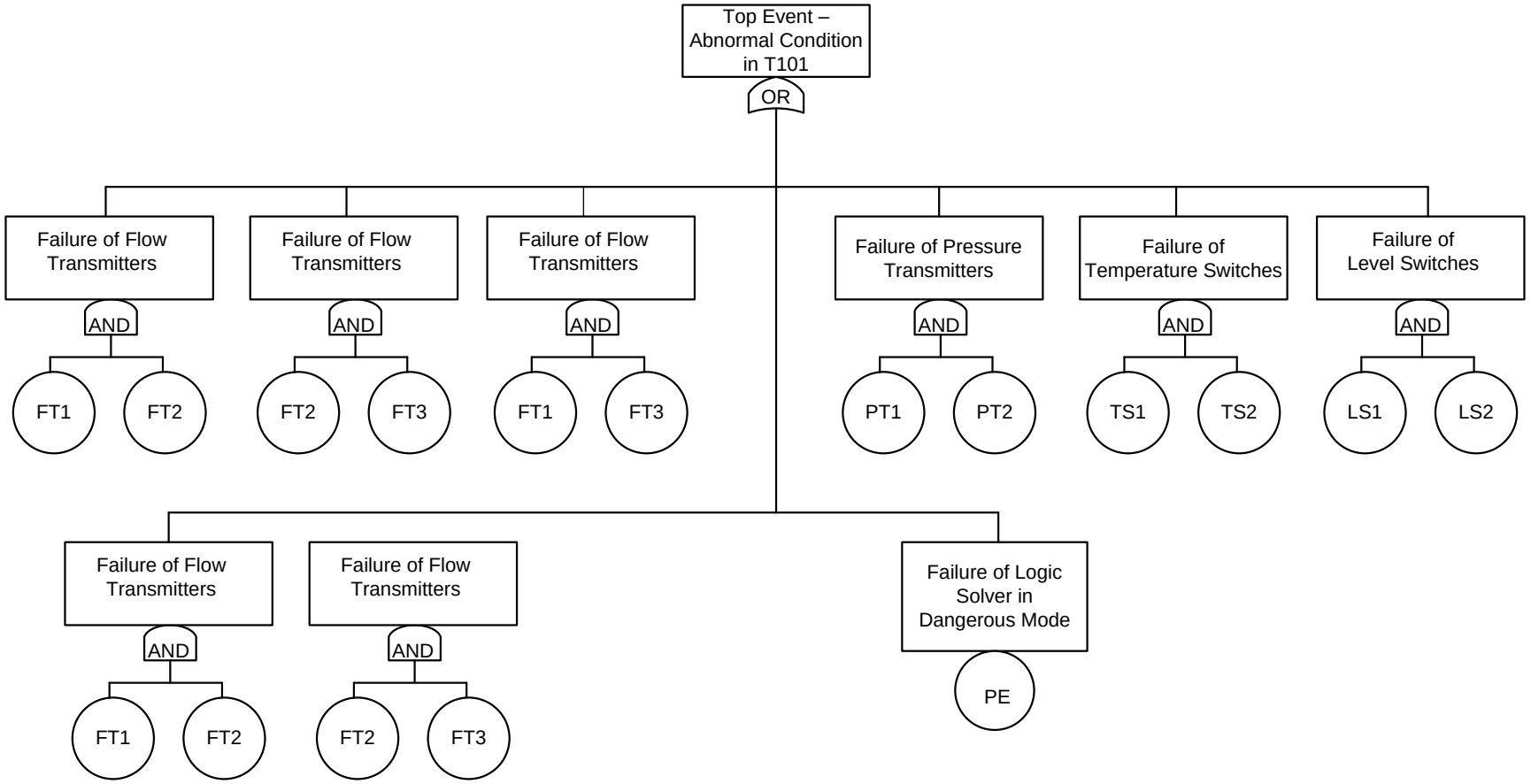

Figure 3. Fault Tree for Example Interlock

Appendix A – Commonly Encounter Probability Distributions

There are four probability distributions used to represent the failure rate of equipment items. These are:

1. Uniform Distribution
2. Triangular Distribution
3. Normal Distribution
4. Log-Normal Distribution

This appendix reviews the properties of these four probability distributions.

1. Uniform Distribution

The uniform distribution [Ref. A-1, pg 74; A-2, pg 687-688] is used when a variable is only known within a defined range. Figure A-1 presents a plot of the probability density function (pdf) for the uniform distribution. The distribution is defined using two parameters, A and B.

Where:

A = minimum value of the random variable

B = maximum value of the random variable

The mean or expected value of a random variable, x, that follows the uniform distribution is:

$$\text{Mean} = \text{Expected Value} – E(x) = (A+B)/2 \qquad \text{(Eq A-1)}$$

The variance of a random variable, x, that follows the uniform distribution is:

$$\text{Variance} = V(x) = (B-A)^2/12 \qquad \text{(Eq A-2)}$$

The standard deviation of a random variable, x, that follows the uniform distribution is:

$$\text{Standard Deviation} = (\text{Variance})^{1/2} = (B-A)/(12)^{1/2} \qquad \text{(Eq A-3)}$$

2. Triangular Distribution

The triangular distribution [Ref. A-2, pg 686-687] is used when a variable is known to lie within a defined range and a “best guess” or estimate can be made as to the most likely value to the variable. Figure A-2 presents a plot of the probability density function (pdf) for the triangular distribution. The distribution is defined using three parameters, A. B and C.

Where:

A = minimum value of the random variable

B = maximum value of the random variable

C = most likely (mode) of the random variable

The mean or expected value of a random variable, x, that follows the triangular distribution is:

$$\text{Mean} = \text{Expected Value} – E(x) = (A+B+C)/3 \qquad \text{(Eq A-4)}$$

The variance of a random variable, x, that follows the triangular distribution is:

Variance = $V(x) = [A^2 + B^2 + C^2 - AB - AC - BC]/18$ (Eq A-5)

The standard deviation of a random variable, x, that follows the triangular distribution is:

Standard Deviation = $(\text{Variance})^{1/2} = \{[A^2 + B^2 + C^2 - AB - AC - BC]/18\}^{1/2}$ (Eq A-6)

3. Normal distribution

The normal distribution [Ref A-2, pg 665-666] is used when a variable when data analysis finds the normal distribution is the best model to describe the spread in the measured variable. Figure A-3 presents a plot of the probability density function (pdf) for the normal distribution. The distribution is defined using two parameters, μ and σ.

Where:

μ = mean of the measured data for variable

σ = standard deviation of the measured data for variable

The expected value of a random variable, x, that follows the normal distribution is:

Expected value = mean = $E(x) = \mu$ (Eq A-7)

The variance of a random variable, x, that follows the normal distribution is:

Variance = square of standard deviation = $V(x) = \sigma^2$ (Eq A-8)

The standard deviation of a random variable, x, that follows the normal distribution is:

Standard deviation = σ (Eq A-9)

4. Lognormal Distribution

The lognormal distribution [Ref. A- 2, pg 658-659] is used when a variable when data analysis finds the lognormal distribution is the best model to describe the spread in the measured variable. Figure A-4 presents a plot of the probability density function (pdf) for the lognormal distribution. Many variables in nature are lognormally distributed (for example the height of people). The log normal distribution is used when the variable of interest has a known physical lower limit of zero. A variable, x, is lognormally distributed if ln(x) is normally distributed. The lognormal distribution is defined using two parameters, μ_y and σ_y.

Let the original data be defined by the variable x with mean and standard deviation as:

μ_x = mean of the measured data for variable x

σ_x = standard deviation of the measured data for variable x

Define a new variable y as:

$y = \text{Ln}(x)$ (Eq A-10)

Then variable x is said to be lognormally distributed if y is normally distributed. We can now write the mean and standard deviation of y (μ_y and σ_y.) [Ref. A-3, A-4 and A-5] as

$$\mu_y = Ln[\mu_x^2 / ((\sigma_x^2 + \mu_x^2)^{½})] \quad \text{(Eq A-11)}$$

$$\sigma_y = [Ln(\sigma_x^2 / \mu_x^2 + 1)]^{½} \quad \text{(Eq A-12)}$$

Where:

Ln is the natural logarithm (base e) of the argument

Appendix A References:

A-1. P. L. Meyer, *Introductory Probability and Statistical Applications*, 2nd Edition, Addison-Wesley, Reading Mass, Library of Congress Catalog no. 75-104971, 1972, pp. 74

A-2. D. Vose, *Risk Analysis–A Quantitative Guide*, 3rd edition, Wiley, Chichester, West Sussex, England, ISBN 978-0-470-51284-5, 2008, pp. 686-687

A-3. "Lognormal mean and variance - MATLAB lognstat". www.mathworks.com. Retrieved 27 December 2018

A-4. M. Mood, F. A. Graybill, and D. C. Boes. *Introduction to the Theory of Statistics.* 3rd ed., New York: McGraw-Hill, ISBN 0-07-042864-6, 1974. pp. 117.

A-5. E.L. Crow and K. Shimizu, Lognormal Distributions – Theory and Applications, Marcel Dekker, New York, ISBN 0-8247-7803-0, 1988, pp. 9

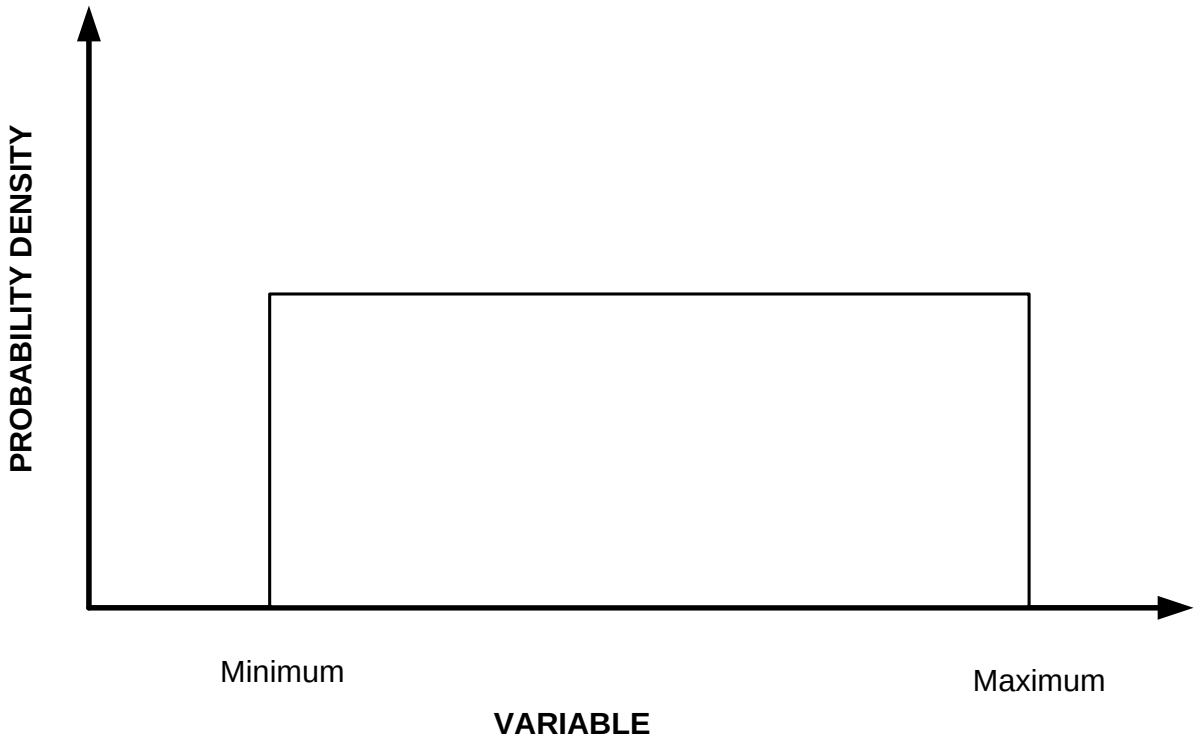

Figure A-1. Uniform Probability Distribution

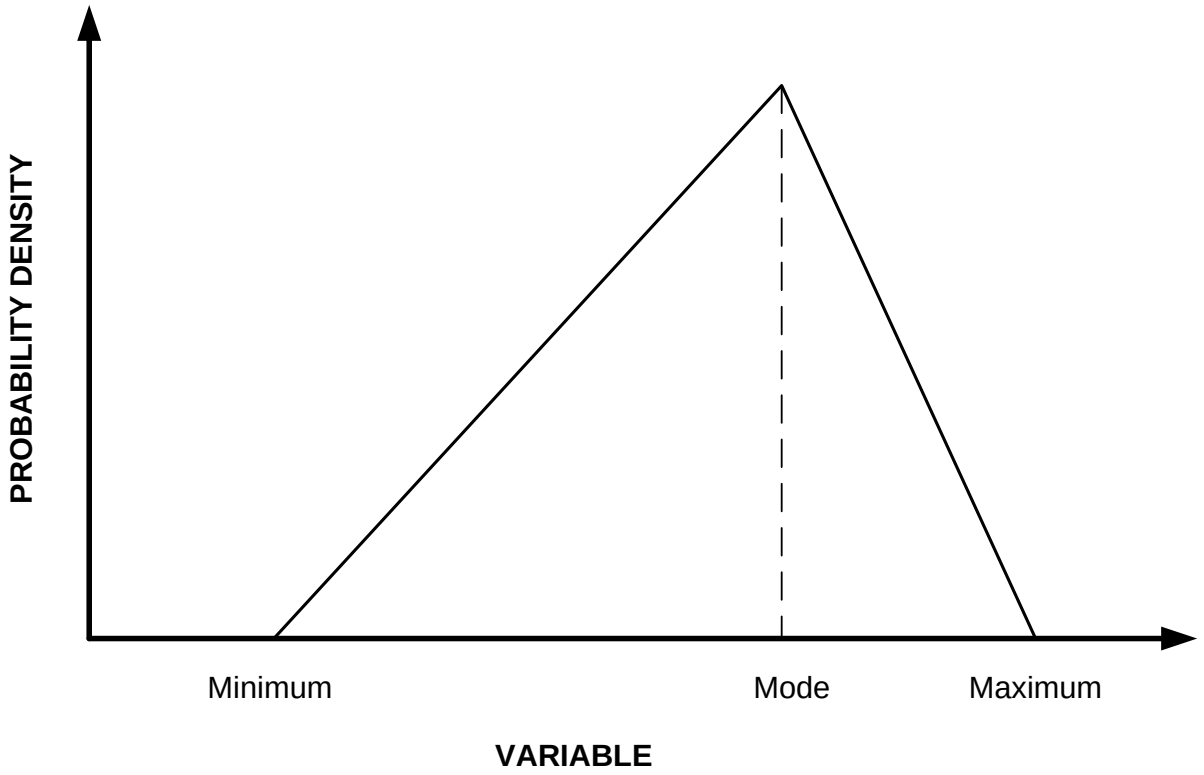

Figure A-2. Triangular Probability Distribution

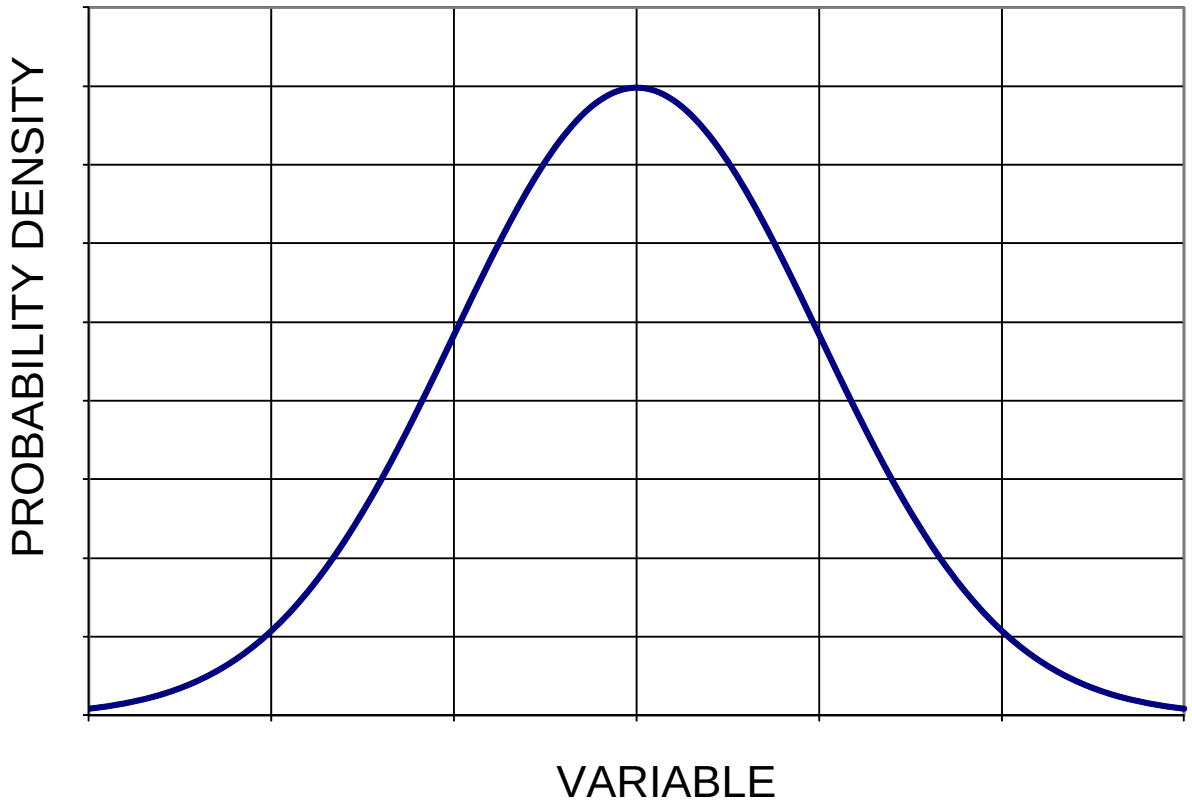

Figure A-3. Normal Probability Distribution

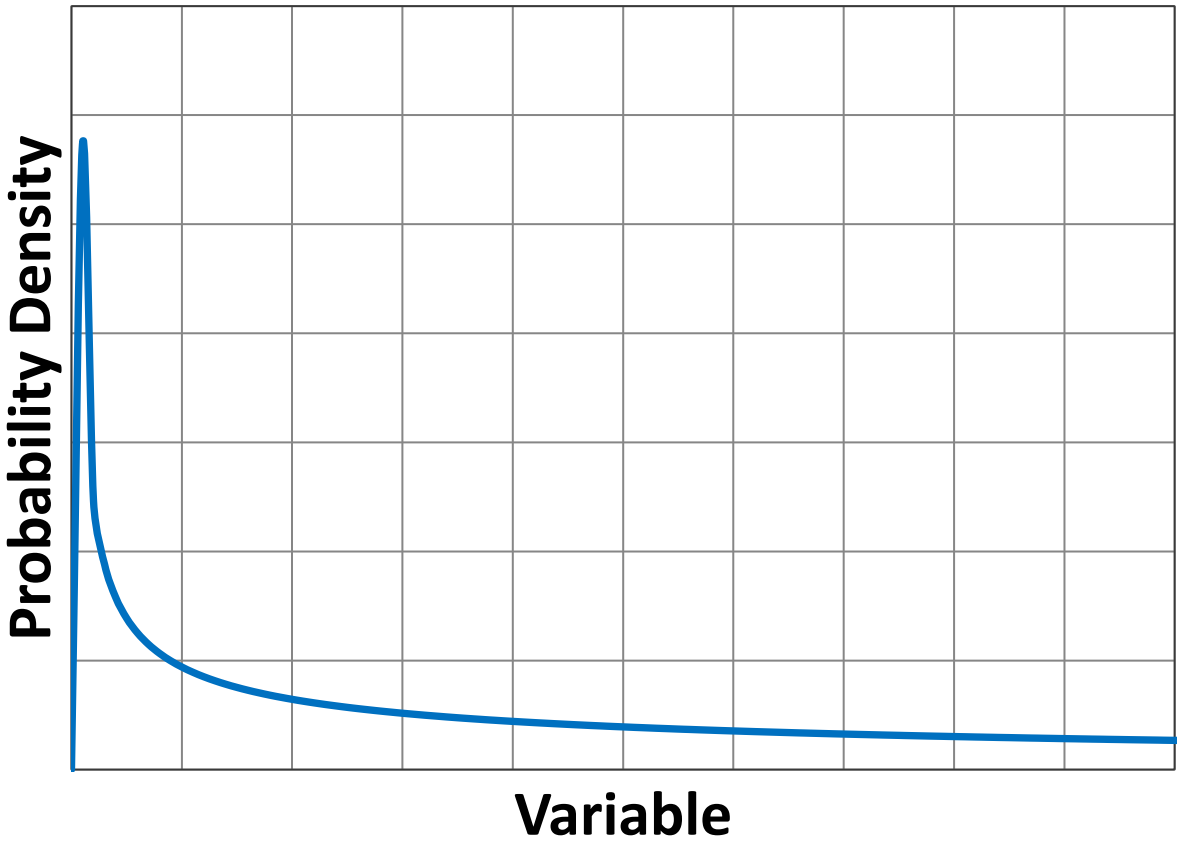

Figure A-4. Lognormal Probability Distribution