Evaluation of Uncertainty in Safety Integrity Level (SIL) Calculations

Raymond “Randy” Freeman
S&PP Consulting
12303 Lake Shore Ridge
Houston, TX 77041
Voice: 713 856 7143
EMAIL: rafree@yahoo.com

Angela Summers
SIS-Tech
12621 Featherwood Dr., Suite 120
Houston, TX 77034
EMAIL: asummers@sis-tech.com

Presented at 2015 Spring Meeting of the AIChE 11 Global Congress on Process Safety Austin, TX. Published in Process Safety Progress, December 2016.

Keywords: Uncertainty, SIL Evaluation, Variance Contribution Analysis, VCA

Abstract

The evaluation of the safety integrity level of a new or existing safety instrumented system (SIS) requires detailed calculations based on the failure rates of the device and the planned maintenance-testing cycle for the system. The failure rates of the devices are taken from standard failure rate tabulations of equipment. The maintenance and testing plans are developed based on plant experience. The quantitative evaluation determines the probability of failure on demand (PFD) for a demand mode SIS and yields the safety integrity level (SIL) of the SIS. All of the data used in the SIL calculations are uncertain. This paper explores the impact of uncertainty on the PFDcalculation fora SIS. The “70%” rule of thumb from IEC 61508 is compared to results obtained using probability theory such as variance contribution analysis (VCA). A proposed methodology for handling the uncertainty in the PFD calculations is presented based on the application of the VCA method. An example is worked to demonstrate the methodology.

1. Background

The calculation of the probability of failure on demand (PFD) is a common engineering task when designing an interlock in compliance with IEC 61511 [1]. The calculation of the PFD is often done using approximate equations defined in the ISA TR84.00.02 technical report [2]. Reliability block diagrams are often used to determine the PFD of an interlock implemented as a SIS, where the PFD of the individual field sensors, logic solver and final control elements are considered independently of each other in the sense that the failure of one device is not conditional on the failure of another. The PFD is then calculated using the failure rates of the devices, planned test intervals, vendor supplied estimates on diagnostic coverage of the devices and an allowance for the potential for common cause failures. The PFD corresponds to one of four safety integrity levels (SILs), where each level possesses a PFD that is one order of magnitude less than the next, for example, SIL-1 has a PFD < 0.1, while SIL-2 has a PFD < 0.01. Almost all of these parameters are uncertain. The failure rate data are often taken from generic data sources which show wide ranges in the observed values.

Because of the uncertainty in the parameters, the design engineer makes allowances in the design by the use of safety factors or rules of thumb to improve the chances that the final interlock installation will work as intended. Since each engineer has a different set of safety factors and rules of thumb, two designs may differ significantly in the way a hazard is controlled.

A more formal method for handling the underlying uncertainty in the PFD calculation of an interlock is needed. This article will demonstrate two approaches available for the uncertainty calculations:

- Direct determination by use of the Monte Carlo Simulation Method
- Use of the Variance Contribution Analysis approximation.

The easiest way to demonstrate the applicability of the variance contribution analysis to interlock uncertainty is via a worked example. The remainder of this article demonstrates these two uncertainty analysis methods using a typical PFD calculation.

2. Example Interlock

Consider the process system shown in Figure 1. The process uses a compressor to increase the pressure of a process stream prior to additional processing. The gas being compressed is toxic and flammable. Of concern is a slug of liquid being sent to the compressor. If a liquid slug is sent to the compressor, significant damage to the compressor is expected with probable seal damage and a subsequent release of flammable and toxic material into the work area. A large fire and/or explosion could result if the release were to be ignited. If the release is not ignited, the nearby workers could be exposed to the toxic gas resulting in death or injury. A Layer of Protection

Analysis (LOPA) review of this system has been completed. Among several recommendations, the LOPA team recommended the installation of a SIL-2 high level interlock in the compressor knockout drum to stop the compressor prior to liquids entering the system.

Figure 1 shows a simplified diagram for the interlock. Three level sensors are provided in the Compressor Knock Out Drum. The SIS logic solver will use 2oo3 voting to detect high level in the compressor knockout drum. The SIS logic solver will also monitor the difference in the level signal from each of the three level sensors and will activate an alarm if the deviation is excessive. Two independent methods of stopping the compressor are provided. The SIS will directly signal the motor controller on the compressor to stop. In addition, the SIS logic solver will also signal two additional relays to open the power supply to the compressor motor.

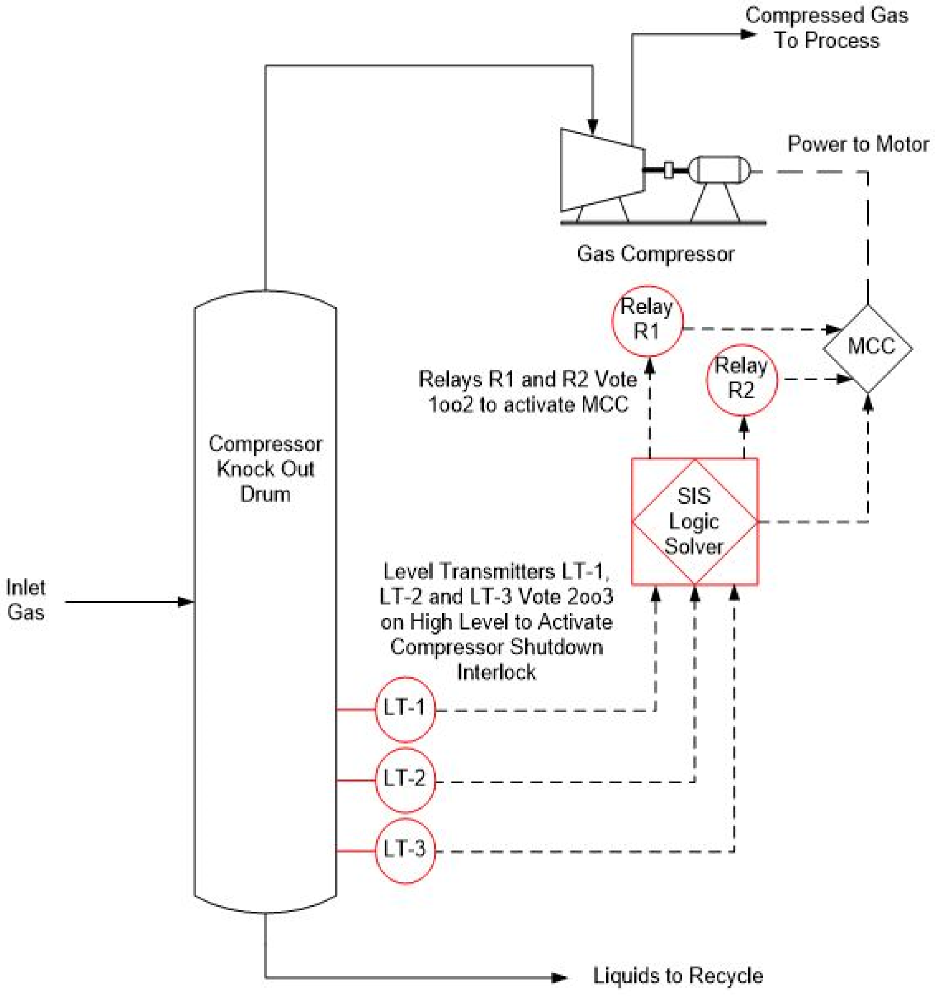
Compressed Gas
To Process
Power to Motor
Gas Compressor
Relay R1
Relay R2
MCC
Relays R1 and R2 Vote 1oo2 to activate MCC
Compressor Knock Out Drum
SIS Logic Solver
Inlet Gas
Level Transmitters LT-1, LT-2 and LT-3 Vote 2oo3 on High Level to Activate Compressor Shutdown Interlock
LT-1
LT-2
LT-3
Liquids to Recycle

Figure 1 P&ID Sketch for Example Interlock

These two output actions will both be activated in the event of high level in the compressor knockout drum. Either one of the two output actions is capable of stopping the compressor by turning off the electric power supply to the motor.

3. Models

The first step in the calculation of the “goodness” of an interlock is to establish the model to be used in the calculations. Figure 2 presents the Reliability Block Diagram for the example. Note that the sensors are 2oo3 voting and the final control elements are each 1oo1. Supporting Information Appendix A presents the equations for various models that can be used for describing this system.

The overall probability of failure on demand (PFD) of the interlock is given as:

$PFD = PFD_{s} + PFD_{sis} + PFD_{fce}$ (Eq 1)

Where:

PFD is the probability of failure on demand of the interlock as a whole

PFD_{s} is the probability of failure on demand of the sensors (voting as 2oo3)

PFD_{sis} is the probability of failure on demand of the SIS logic solver

PFD_{fce} is the probability of failure on demand of the final control elements.

Since there are two final control elements arranged in series, the PFDfce is composed of the probabilities of failure of the control elements (Relay and MCC). As:

$PFD_{fce}= PFD_{r} + PFD_{mcc}$ (Eq 2)

Where:

PFD_{r} = Probability of failure on demand of the two relays voting as 1oo2 to shutdown gas compressor.

PFD_{mcc} = Probability of failure on demand of the MCC to shutdown the gas compressor

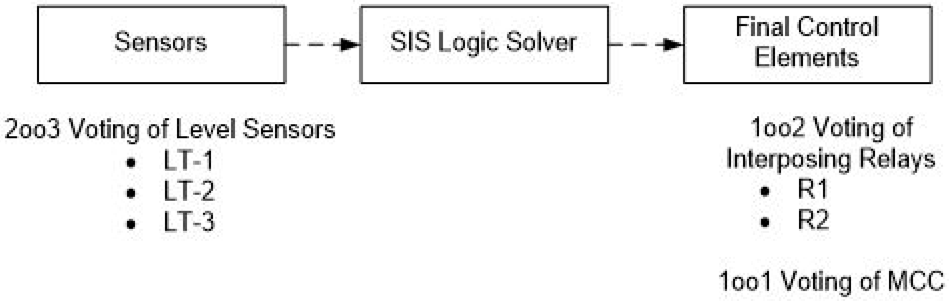

Figure 2 Reliability Block Diagram for Example Interlock

For this example, the following selections are made to model the performance of the interlock.

3.1 Model for Sensors (2oo3)

There are three sensors that will be used in a 2oo3 voting system. From Supporting Information Appendix A, using Equation A-7, the model for the sensors becomes:

PFDsavg =

$$3\times\left[\frac{(1-DCs)\times(1-\beta s)\times\lambda^{Ds}\times TIs}{2}+\frac{DCs\times(1-\beta s)\times\lambda^{Ds}\times DIs}{2}+(1-\beta s)\times\lambda^{Ds}\times MTTRs\right]^{2}+$$

$$\left[\frac{(1-DCs)\times\beta s\times\lambda^{Ds}\times TIs}{2}+\frac{DCs\times\beta s\times\lambda^{D}\times DIs}{2}+\beta s\times\lambda^{Ds}\times MTTRs\right]\qquad\text{(Eq 3)}$$

Where:

PFD_{savg} is the average probability of failure on demand of the sensors

DC_s is the diagnostic coverage for sensor failure

DI_s is the diagnostic interval for the sensors

$MTTR_s$ is the mean time to restore the sensors to functionality given a sensor failure

TI_s is the test interval for the sensors

β_s is the common cause failure parameter

λ^{Ds} is the failure rate to a dangerous condition for the sensors

3.2 Model for SIS Logic Solver

Use a fixed PFD as specified by the vendor. Unless detailed design information is provided by the SIS logic solver vendor, this will be the normal default condition for most studies. For this problem, a typical PFD of 1.30 x 10^{-4} was selected to represent the SIS Logic Solver.

3.3 Model for Final Control Elements

There are two separate paths to shutdown the gas compressor. First is by the SIS logic solver commanding the MCC to shutdown power to the gas compressor motor. The second is for the SIS logic solver to issue a shutdown command to two interposing relays (R1 and R2) which will cause the power to the gas compressor motor to stop.

3.3.1 Model for Interposing Relays (1oo2)

There will be two interposing relays (R1 and R2 in the interlock). From Supporting Information Appendix A, use Equation A-3 for the interposing relays, the model becomes:

$$\text{PFDravg} = \left[\frac{(1-\beta r)\times\lambda^{Dr}\times TIr}{2}+\right]^2 + \left[\frac{\beta r\times\lambda^{Dr}\times TIr}{2}+\right] \qquad \text{(Eq 4)}$$

Where:

PFD_{ravg} is the average probability of failure on demand of the relays voting 1oo2 to shutoff the gas compressor.

TI_r is the test interval for the relays

$\beta_r$is the common cause failure parameter

$\lambda^{Dr}$is the failure rate to a dangerous condition for the relays

3.3.2 Model for MCC (1oo1)

From Supporting Information Appendix A and using equation A-1 for the MCC, the model becomes:

$$\text{PFDmccavg} = \frac{\boldsymbol{\lambda^{Dmcc} * \text{TImcc}}}{\mathbf{2}}$$

(Eq 5)

Where:

PFD_{mccavg} is the average probability of failure on demand of the MCC to shutoff the gas compressor.

TI_{mcc} is the test interval for the MCC

λ^{Dmcc} is the failure rate to a dangerous condition for the MCC

4. Data

The calculation of the PFD of the interlock requires a set of data to be used to represent the system. Tables 1 - 3 presents the data used to represent the interlock system. Note that these data are taken from generic data sources and do not represent any particular device or system.

Table 1. Sensor Failure Rate Data for Example Interlock

Variable	Units	Value	Notes
λ^{Ds}- Fail Dangerous Rate	1/Yr	$5.0x10^{-3}$	
DC_s – Diagnostic Coverage	Unit Less	0.9	
DI_s – Diagnostic Interval	Yr	$5.71x10^{-5}$	0.5 hours
TI_s – Test Interval	Yr	5	
β_s- Common Cause Failure Fraction	Unit Less	0.02	
$MTTR_s$ - Mean Time to Restore	Yr	$8.22x10^{-3}$	72 hours

Table 2. Relay Failure Rate Data for Example Interlock

Variable	Units	Value
λ^{Dr}- Fail Dangerous Rate	1/Yr	2x10-3
DC_r – Diagnostic Coverage	Unit Less	0
DI_r – Diagnostic Interval	Yr	0
TI_r – Test Interval	Yr	1
β_r- Common Cause Failure Fraction	Unit Less	0.02
$MTTR_r$- Mean Time to Restore	Yr	0

Table 3. MCC Failure Rate Data for Example Interlock

Variable	Units	Value
λ^{Dmcc}- Fail Dangerous Rate	1/Yr	1.31E-03
DC_{mcc} – Diagnostic Coverage	Unit Less	N/A
DI_{mcc} – Diagnostic Interval	Yr	N/A
TI_{mcc} – Test Interval	Yr	1
β_{mcc}- Common Cause Failure Fraction	Unit Less	N/A
$MTTR_{mcc}$ - Mean Time to Restore	Yr	N/A

Given the data in Tables (1–3) with the Equations (1–5), the PFD of the system may be calculated.

$PFD = PFD_s + PFD_{sis} + PFD_r + PFD_{mcc}$ (Eq 6)

$PFD_s = 3.06x10^{-5}$ (Eq 7)

$$PFDsis = 1.34x10^{-4} \qquad \text{(Eq 8)}$$

$$PFDr = 2.1x10^{-5} \qquad \text{(Eq 9)}$$

$$PFDmcc = 6.75x10^{-4} \qquad \text{(Eq 10)}$$

$$PFD = PFD_s + PFD_{sis} + PFD_r + PFD_{mcc} = 8.39x10^{-4} \qquad \text{(Eq 11)}$$

The Risk Reduction Factor (RRF) is 1/PFD or 1/8.39x10^{-4} = 1,192. This calculation indicates that the interlock can perform as a SIL-3 capable system. The original goal was a SIL-2 system. Therefore, the proposed design and test frequencies appear to be adequate to provide at least a SIL-2 protection of the gas compressor. The direct calculation of the interlock PFD ignores all of the uncertainty in the data used to complete the calculations. What is the impact on the results if uncertainty is included in the calculations? What are the chances that the system will perform at least as a SIL-2 capable system with an RRF of 100? These questions are addressed in the following uncertainty analysis.

5. PFD Uncertainty Analysis

Almost every variable in Equations (1-5) are uncertain. Typical values are tabulated in generic sources such as IEEE 500 [3] , OREDA [4] , Smith [5] and others. All of these generic data sources present a range from low to high with some recommended value for the parameter falling somewhere in the range. Tables (4-6) present the ranges for each of the uncertain variables considered in this analysis. The data in Tables (4-6) are representative of those to be found in the generic data sources. Note that the numbers in tables used in this example are expressed using enough significant figures that will allow the reader to reproduce the calculations. In a real problem, the number of significant figures reported should be consistent with the data used in the calculations.

Table 4. Uncertainty Data for Level Sensors Used in Example Interlock

(All variable probability distributions assumed to be triangularly distributed)

Variable	Min	Mode	Max	Mean	Variance
λ^{Ds}- Fail Dangerous Rate	2.84x10^{-3}Yr^{-1}	5x10^{-3}Yr^{-1}	8.5x10^{-3}Yr^{-1}	5.45x10^{-3} Yr^{-1}	1.36x10^{-6} Yr^{-1}
DC$_s$ – Diagnostic Coverage *	0.8	0.9	0.99	0.897	1.51x10^{-3}
DI$_s$ – Diagnostic Interval **	5.71x10^{-5}	5.71x10^{-5}	5.71x10^{-5}	5.71x10^{-5}	0
TI$_s$ – Test Interval	4 Yr	5 Yr	6 Yr	5 Yr	5.56x10^{-2}Yr^{2}
β_s- Common Cause Failure Fraction *	0	0.02	0.1	0.04	4.67x10^{-4}
MTTR$_s$ - Mean Time to Restore ***	1.37x10^{-3}Yr	8.22x10^{-3}Yr	1.92x10^{-2}Yr	9.59x10^{-3}Yr	1.34x10^{-5}Yr^{2}

* Unit less ** 0.5 hours, assumed to be deterministic ***Min of 12 hr, Mode of 72 hours, Max of 168 hrs

Table 5. Uncertainty Data for Relays Used in Example Interlock

(All variable probability distributions assumed to be triangularly distributed)

Variable	Min	Mode	Max	Mean	Variance
λ^{Dr}- Fail Dangerous Rate	8.76x10^{-9} Yr^{-1}	2.00x10^{-3} Yr^{-1}	4.73x10^{-2} Yr^{-1}	1.64x10^{-2} Yr^{-1}	1.19x10^{-4} Yr^{-2}
DC$_r$ – Diagnostic Coverage *	NA	NA	NA	NA	NA
DI$_r$ – Diagnostic Interval*	NA	NA	NA	NA	NA
TI$_r$ – Test Interval	1 Yr	1 Yr	2 Yr	1.33 Yr	0.056Yr^{2}
β_r- Common Cause Failure Fraction	0	0.02	0.1	0.04	4.67x10^{-4}
MTTR$_r$ - Mean Time to Restore*	NA	NA	NA	NA	NA

* Not used in relay model

Table 6. Uncertainty Data for MCC Used in Example Interlock

(All variable probability distributions assumed to be triangularly distributed)

Variable	Min	Mode	Max	Mean	Variance
λ^{Dr}- Fail Dangerous Rate	$1.74\text{x}10^{-4}\text{Yr}^{-1}$	$1.31\text{x}10^{-3}\text{Yr}^{-1}$	$3.00\text{x}10^{-2}\ \text{Yr}^{-1}$	$1.05\text{x}10^{-2}\text{Yr}^{-1}$	$4.76\text{x}10^{-5}\text{Yr}^{-2}$
DC_r– Diagnostic Coverage*	NA	NA	NA	NA	NA
DI_r – Diagnostic Interval*	NA	NA	NA	NA	NA
TI_r – Test Interval	1 Yr	1 Yr	2 Yr	1.33 Yr	$5.6\text{x}10^{-2}\text{Yr}^{2}$
β_r- Common Cause Failure Fraction*	NA	NA	NA	NA	NA
$MTTR_r$ - Mean Time to Restore*	NA	NA	NA	NA	NA

* Not used in MCC model

The information contained in the ranges on the variables in Tables (4-6) contain the information needed to evaluate the uncertainty in the PDF of the interlock. All of the uncertain variables are considered to be distributed per the triangular probability distribution. Properties of the triangular probability distribution are presented in Supporting Information Appendix B of this paper.

5.1 Method 1 - Monte Carlo Analysis of PFD

The RiskAMP Monte Carlo software package [6] was used to simulate the PFD of the example interlock. The models presented above for the sensor and final control elements along with the probability distribution data of Tables (4-6) were used to complete the Monte Carlo simulation. The Monte Carlo simulation used the same probability distribution (triangular) to represent the uncertain parameters. A total of 100,000 random trials were completed using the Latin Hypercube sampling method to speed the convergence of the simulation.

Figure 3 presents the resulting frequency count histogram of frequency of example interlock PFD. The histogram plot represents a count of the number occurrences of the PFD as a result of the 100,000 Monte Carlo trials. Also shown in Figure 3 is the SIL-2 criterion of a PFD of 1 x 10^{-2}. Those outcomes to the right of the SIL-2 criterion represent designs that would not achieve needed SIL-2 performance for risk reduction. Those outcomes to the left of the SIL-2 criterion represent successful designs. The resulting mean, standard deviation and 95% upper limit of the example interlock PFD determined from the simulation are as follows:

Mean PFD = 7.8 x 10^{-3} or an RRF of 128

Standard Deviation of PFD = 4.8 x 10^{-3}

95% upper limit on PFD = 1.70 x 10^{-2} or an RRF of 59

70% upper limit on PFD = 10 x 10^{-3} or an RRF 100

These interlock performance indicators will be used as the basis for judging other methods of analysis. These performance indicators are the best estimates of how the final system will actually perform given the input data used in the interlock design.

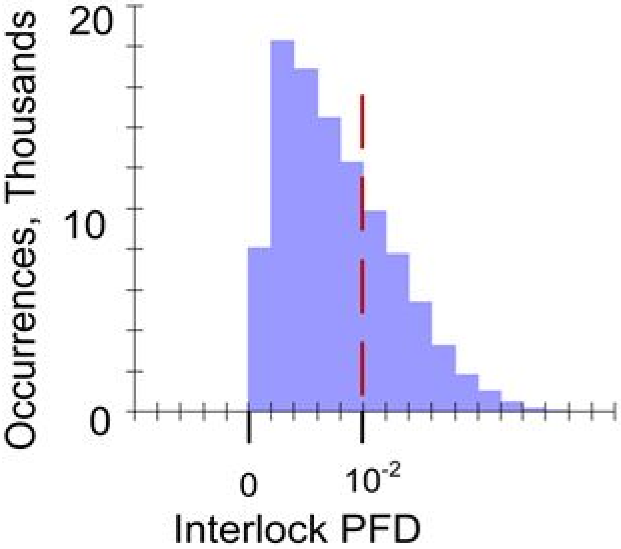

Figure 3. Monte Carlo Simulation Frequency Count for Example Interlock Probability of Failure on Demand (PFD)

5.2 Method 2 - Variance Contribution Analysis (VCA) of PFD

5.2.1 Review of VCA Methodology

Each of the variables used to compute the PFD is uncertain. Therefore, the PFD is a mathematical function of a number of random variables. The mean and variance of the PFD is required to understand the uncertainty in the PFD estimate. The mean and variance of a function of random variables can be approximated using the method described by Haugen [7] and applied by Freeman [8, 9]. An arbitrary function, $F(x_i)$, of a set of independent random variables, x_i, is defined as:

Let

$$Y = F(x_i) \qquad \text{(Eq 12)}$$

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

$$E(Y) = F[E(x_i)] \qquad \text{(Eq 13)}$$

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:

$$V(Y) = \sum_{i=1}^{n} \left[\frac{\partial y}{\partial x_i}\right]^2 V(x_i) \qquad \text{(Eq 14)}$$

Where:

V(Y) = variance of random variable Y as defined above in Equation 14

$V(x_i)$ = variance of random variable x_i as defined above in Equation 14

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:

$$V(Y\ from\ X_i) = \left[\frac{\partial y}{\partial x_i}\right]^2 V(x_i) \qquad \text{(Eq 15)}$$

The relative contribution of each term to the overall variance V(Y) is a measure of its importance with regard to the uncertainty in the particular random variable, x_i. In effect, this is a sensitivity analysis combined with an uncertainty evaluation. The variance contribution combines the sensitivity of the answer to changes in the uncertain random variable x_i, with a measure of the uncertainty in the random variable, $V(x_i)$.

5.2.2 VCA of Example Interlock

The best estimate of the example interlock PFD is determined by using the mean value of the uncertain parameters rather than the mode (most likely). Only when the probability distribution is symmetric about the mean (such as the uniform or normal distributions) will the mean and mode correspond to the same value. Substituting the mean values (given in Tables 4, 5, and 6) for the uncertain parameters into the equations for that describe the example interlock, mean interlock PFD is found as:

PFD = 7.72 x 10^{-3}

RRF = 1/PFD = 130

The error in the relative mean RRF is found as:

Relative error = (VCA estimate – Monte Carlo estimate)/Monte Carlo estimate

Relative error = (130 – 128)/128 = 2/128 => 1.6%

The variance of the PFD can be found by use of the parameter sensitivity weighted contribution of the various uncertain parameters. Previously, Freeman [Ref 9] found that a perturbation of 10 percent about the mean to determine the sensitivity resulted in an error of no more than 16% in the resulting uncertainty calculations. Thus, for this example interlock, the sensitivity of each uncertain variable was determined by a numerical perturbation of 10 percent about the mean of the uncertain variable. Table 7 presents the results of the calculations. In addition, the sensitivity weighted contribution of each of the random variables is also presented in Table 7. See Appendix B of the on-line supplementary information for variance and sensitivity calculation details.

Using the VCA method for estimation of the variance:

Variance of PFD = 3.18 x 10^{-5}

Standard Deviation of PFD = 5.64 x 10^{-3}

For comparison, the Monte Carlo method found the standard deviation to be:

Standard Deviation of PFD from Monte Carlo = 4.8 x 10^{-3}

Once again, the relative error is:

Relative error = (VCA estimate – Monte Carlo estimate)/Monte Carlo estimate

Relative error = (5.64 x 10^{-3}- 4.8 x 10^{-3})/ 4.8 x 10^{-3}

Relative error => 17.5 %

Haugen [7] found that the normal probability distribution may often be used to compute the confidence limits on the random variable found as a function of other random variables. The standard normal distribution has a mean of zero and a standard deviation of one. Tabulations of the cumulative standard normal distribution are presented in every statistics text (for example, Meyer, [10]) using a normalization function to convert the actual distribution to the standard normal distribution.

Table 7. Sensitivity, Variance and Variance Contribution to Example Interlock Uncertainty

Random Variable	Mean	Mean Units	Variance	Variance Units	Sensitivity	Variance Contribution	Variance Contribution %
LT Sensor Failure Rate	5.45x10^{-3}	Event/yr	1.36x10^{-6}	(Event/yr)^{2}	1.30x10^{-2}	2.30x10^{-10}	0.00%
MCC Failure Rate	1.05x10^{-2}	Event/yr	4.76x10^{-5}	(Event/yr)^{2}	6.65x10^{-1}	2.11x10^{-5}	66.11%
Relay Failure Rate	1.64x10^{-2}	Event/yr	5.58x10^{-3}	(Event/yr)^{2}	4.07x10^{-2}	9.23x10^{-6}	28.98%
Beta1 - LT	0.04	Unit less	4.67x10^{-5}	Unit less	1.45x10^{-3}	9.77x10^{-11}	0.00%
Beta2 - Relays	0.04	Unit less	4.67x10^{-5}	Unit less	-1.07x10^{-2}	5.35x10^{-9}	0.02%
Diagnostic Coverage (DC)	0.897	Unit less	1.5x10^{-3}	Unit less	-6.08x10^{-4}	5.57x10^{-10}	0.00%
LT MTTR	9.59x10^{-3}	Years	1.34x10^{-5}	Years^{2}	2.62x10^{-4}	9.18x10^{-13}	0.00%
MCC Test Interval	1.33	Years	0.056	Years^{2}	5.25x10^{-3}	1.54x10^{-6}	4.84%
Relay - Test Interval	1.33	Years	0.056	Years^{2}	5.03x10^{-4}	1.41x10^{-8}	0.04%
LT Sensor Test Interval	5	Years	0.1667	Years^{2}	1.36x10^{-5}	3.10x10^{-11}	0.00%
Total Variance						**3.18x10^{-5}**	
Std Dev						**5.64x10^{-3}**	

By convention this normalization function is referred to as Z and is given by:

$$Z = \left[\frac{x_i - E(x)}{\sigma}\right]$$

(Eq 16)

Where:

x_i is a particular value of the random variable x

E(x) is the expected value of the random variable x

$\sigma$is the standard deviation of the normal distribution for the random variable x

For example, with Z equal to 1.64, the cumulative normal distribution is 0.95 [Ref. 10]. Stated differently, 95% of the values of the random variable will be below that found when Z is 1.64. The value of Z equal to 0.52 corresponds to the cumulative normal distribution value of 0.70.

With the mean and variance of the PFD of the example interlock estimated above, it is possible to estimate the confidence limits. At the 95% limit, the value for Z is 1.64 [Ref. 10]. The value for the interlock PFD mean and standard deviation are:

Mean of example interlock PFD = E(x) =7.80 x 10^{-3}

Variance of example interlock PFD = 3.18 x 10^{-5}

The standard deviation of the example interlock PFD is the square root of the example interlock variance or:

Std Dev = $[3.18 \times 10^{-5}]^{1/2}$ = SQRT[3.18 x 10^{-5}] = σ = 5.64 x 10^{-3}

The 95 percent upper limit on the example interlock PFD is found by solving Equation 16 for X95% as:

X95% = 1.64 σ + E(x) (Eq 17)

Where:

X95% is the upper 95% limit on the computed PFD of the interlock of interest .

σ is the Standard Deviation of the interlock PFD based on uncertainty in the data

E(x) is the Mean frequency of the interlock PFD

Substituting the values for E(x) and σ determined above, the corresponding 95% upper limit on the frequency of the example interlock PFD is 1.70 x 10^{-2} or an RRF of 59. Likewise, the 70% upper limit is calculated with Z set at 0.52 as 1.07 x 10^{-2} or an RRF of 93.

6. Discussion

Two different methods (Monte Carlo Simulation and Variance Contribution Analysis) have been used above to calculate the performance of the example interlock. The results of the above calculations are summarized in Table 8.

Table 8. Summary of Example Interlock Results by Method of Calculations

Calculation Basis Description	By Monte Carlo Simulation		By Variance Contribution Analysis (VCA)	
	PFD	RRF	PFD	RRF
Based on generic data recommended values	8.39x10^{-4}	1192	8.39x10^{-4}	1192
Based on mean values of uncertain parameters	7.80x10^{-3}	128	7.72x10^{-3}	130
Based on 70% chance interlock will work	1.07x10^{-2}	93	1.07x10^{-2}	93
Based on 95% chance interlock will work	1.70x10^{-2}	59	1.70x10^{-2}	59

For this example interlock, the use of the generic database recommended values will yield a PFD value that is significantly less conservative than those that consider uncertainty. Using the recommended data, the design calculates out to be in the low range SIL-3 performance. Using the parameter means instead of the recommended value, results in the interlock performance dropping to low range SIL-2. When we look at the chances that the example interlock will achieve at least a specified level of confidence of working, we find that the interlock is midrange SIL-1 for a 95% chance of working. If only a 70% chance of working is established by the designer, the calculated example interlock performance is near the division line between SIL-1 and SIL-2 (RRF=100).

From Table 7, it can be seen that only three of the uncertain variables contribute to the uncertainty in the variance of interlock PFD. These are:

MCC Failure Rate (66% of variance contribution)

Relay Failure Rate (29% of variance contribution)

MCC Test Interval (5% of variance contribution)

All of the other variables contribute a negligible amount to the uncertainty in the interlock performance. By reducing the uncertainty in these variables by data collection, talks with equipment suppliers or firmly fixing test intervals on equipment, the uncertainty in the PFD can be reduced. The resulting interlock performance confidence limits will be closer to the mean RRF of 130. However, the confidence limits will always be BELOW or worse than the performance based on calculations using the mean value of the parameters. This fact requires that the interlock designer understand that there is a difference between the desired RRF as determined by a LOPA team and the design target RRF that the designer must achieve. The desired RRF is used to define the design target RRF. The design target RRF will ALWAYS be higher than the desired RRF. That the design and target RRF are different is best illustrated by giving their definitions.

- Desired RRF – Risk reduction factor needed to manage the calculated risk from a process scenario to an acceptable level within a company's risk management program. Alternately, the desired risk reduction could be expressed as the desired PDF for the interlock.
- Design Target RRF – Risk reduction factor used by control and design engineers to select the equipment and logic for an interlock that will achieve the Desired RRF. Alternately, the design target could be expressed as the design target PDF.

For good design, there should be a high probability of success of the final interlock design. The probability of success needs to be specified by the owner/operator of the final system. In the above interlock example two probabilities of success (70% and 95%) were used to illustrate the calculation methods.

7. Recommended Interlock PFD Uncertainty Analysis Method

Based on the above example interlock, the following general method may be used in the evaluation of the uncertainty in the performance of a new interlock system.

1. Complete the interlock design using the methods outlined in IEC 61511 [1].
2. Create interlock performance equation as the mathematical model for the combination of sensor, logic solver and final control elements using the methods outlined in ISA Technical Reports ([2], TR84.00.02). An example of this step is given in Equations (1-5) for the example interlock.

3. Define the uncertainty in the parameters and variables of the interlock model specified in step 2. The uncertainty can be given as the upper and lower range of the possible values (uniform probability distribution), as the upper, lower and recommended values (triangular distribution), or as a mean and standard deviation (normal distribution). See the example above for guidance in the evaluation of SIS interlocks.
4. Compute the expected value of each variable in the interlock performance equation. The equations for the mean and variance for the uniform, triangular and normal probability distributions are presented for various probability distributions in Vose [11]. The example interlock calculations used a triangular distribution to represent the uncertainty in the parameters.
5. Compute the expected value or mean of the interlock PFD using the mean value of each of the variables in Step 4.
6. Compute the sensitivity of the result from the interlock performance equation by estimating the partial derivative of the basic interlock performance equation with respect to each of the variables using a 10% perturbation about the mean or expected value of each random variable. See the interlock example problem worked above as an example of this step.
7. Compute the variance of the interlock performance equation PFD by use of the variance contribution using Equations 14 and 15. This entails multiplying the variance of each of the uncertain variables in the basic interlock performance equation by the square of its sensitivity (obtained in step 6), as evaluated at the variable mean. Sum the resulting terms to obtain the overall variance of the PFD in the interlock performance equation.
8. Determine the level of risk that the owner/operator wishes to take that the final interlock will not work. In this paper, two levels of risk have been used:
   - 5% chance of failure or 95% chance of success
   - 30% chance of failure or 70% chance of success
9. Assuming that the interlock owner operator wishes to take a low risk (5%) of the interlock failing to achieve its design target PFD, compute the 95% upper confidence limit on the computed PFD by use of the standard normal factor, Z, [10] as:

$$\mathrm{Z} = \left[\frac{x_i - E(x)}{\sigma}\right] \tag{Eq 18}$$

Where:

σ = standard deviation of the PFD of the interlock of interest from the interlock performance equation obtained from step 7. Note that the variance of a random variable is the square of the standard deviation of the random variable.

E(x) = the expected value of the PFD of the interlock of interest from the interlock performance equation obtained from step 5

For the 95% upper limit, Z = 1.64. Rearranging Eq. 10 allows for the direct calculation of the corresponding value of the 95% upper confidence limit on the PFD as:

$$X95\% = 1.64\ \sigma + E(x) \qquad \text{(Eq 19)}$$

Where:

X95% = the upper 95% limit on the computed PFD of the interlock of interest from the interlock performance equation.

10. Compare the 95% upper confidence limit on the PFD of the interlock of concern with that established as the desired PFD for risk reduction. If the 95% confidence of the RRF is greater than the desired RRF, the design is complete. If not, revise the design or change inspection test intervals to achieve the desired RRF. If it is not possible to achieve the desired target RRF economically, revisit the LOPA study accordingly to incorporate better information obtained in the uncertainty analysis. Improve the integrity of the LOPA IPLs or identify additional IPLs to drive the risk to a tolerable level. Continue this process until the computed RRFs are greater than the desired RRFs for risk reduction and risk management.

8. Supplementary Material Available On-Line

In the on-line version of this paper the reader will find a supplementary file that contains Appendices A and B to this paper. Appendix A includes the general equations used in interlock validation. Appendix B includes details on the calculation of the means and variances used in the body of this paper. The on-line version of *Process Safety Progress* materials may be found at:

http://onlinelibrary.wiley.com/journal/10.1002/(ISSN)1547-5913

9. Acknowledgement

This paper was presented at the 2015 Spring Meeting of the American Institute of Chemical Engineers 11th Global Congress on Process Safety in Austin, Texas held April 27-29, 2015. The authors thank the excellent technical reviewers who greatly improved the presentation of this paper.

10. References

1. International Society of Automation, Functional Safety: Safety Instrumented Systems for the Process Sector—Parts 1, 2, and 3, ANSI/ISA 84.00.01, 2004 [USA implementation of IEC 61511].
2. International Society of Automation, Safety Integrity Level (SIL)Verification of Safety Instrumented Functions, ISA TR84.00.02, Research Triangle Park, NC. (2002).
3. IEEE 500, *IEEE Guide to the Collection and Presentation of Electrical, Electronic Sensing Component and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations*, Wiley Interscience, New York, NY, 1983.
4. OREDA-97, *Offshore Reliability Data – 3rd Edition*, DetNotske Veritas (DNV), 1997.
5. David J. Smith, *Reliability Maintainability and Risk – 8th Edition*, Butterworth-Heinermann, Oxford, UK, 2011, ISBN: 978-0-08-096902-2.
6. Structured Data, LLC , RiskAMP Monte Carlo Add-In Library version 3.13. Professional Edition, Copyright © 2005-2010 , web site at http://www.RiskAMP.com.
7. Edward B. Haugen, *Probabilistic Approaches to Design*, Chapter 4, pp 145-157, John Wiley, New York, 1968.
8. R.A. Freeman, “Quantifying LOPA Uncertainty,”*Process Safety Progress*, Vol 31, No. 3, pp 240-247, 2012.
9. R. A. Freeman, “Simplified Uncertainty Analysis of Layer of Protection Analysis Results,”*Process Safety Progress*, Vol. 32, No 4, pp 351-360, December 2013, Published online in Wiley Online Library (wileyonlinelibrary.com) DOI 10.1002/ prs11585.pdf, 3 June 2013.
10. Paul L. Meyer, *Introductory Probability and Statistical Applications*, pp 342-343, John Wiley, New York, 1972.
11. David Vose, *Risk Analysis – A Quantitative Guide, 3rd Edition*, Appendix III, “A Compendium of Distributions,” pp 585-713, John Wiley, 2008.