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

19th Annual International Symposium
October 25-27, 2016 • College Station, Texas

General Method for Uncertainty Evaluation of 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

Abstract

The IEC 61511 standard requires a verification calculation that a proposed design for a safety instrumented function (SIF) achieves the desired safety integrity level (SIL). The evaluation of the safety integrity level of a new or existing safety instrumented system 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 often taken from standard failure rate tabulations of equipment. The maintenance and testing plans are developed based on plant experience. All of the data used in the SIL calculations are uncertain. This paper develops a general method for uncertainty analysis of the SIL calculations. The general method is based on the application of probability theory - variance contribution analysis (VCA) – to the equations presented in ISA TR 84.00.02-2115. An example is worked to demonstrate the methodology.

Background

The calculation of the probability of failure on demand (PFD) is a common engineering task when designing an interlock or safety system that is to be in compliance with IEC 61511 [Ref. 1]. The calculation of the PFD is often done using approximate equations defined in the ISA TR84.00.02 technical report [Ref. 2]. The simplified equation method in the ISA report is commonly used and is based on the use of reliability block diagrams where the field sensors, Safety Instrumented System (SIS) logic solver and final control elements are considered independent of each other in the sense of not sharing common devices or systems. 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. Almost all of these parameters are uncertain. The failure rate data is 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 calculation of the PFD of an interlock is needed. Previously, Freeman and Summers [Ref. 3] published an uncertainity analysis of the PFD of an interlock. Two different methods were used in this analysis:

- Monte Carlo Simulation
- Variance Contribution Analysis (VCA)

Monte Carlo Simulation requires that the engineer build a model of the interlock using specialized computer software. The use of VCA requires that the sensitivity of the interlock model be determined either by numerical methods or by direct analytical calculations. The Freeman paper demonstrates that VCA can be used for the uncertainty analysis. However, the paper does not present a complete analysis method that can be applied to any system defined in the ISA technical report TR84.00.02. The goal of this paper is to develop a general set of analytical equations that will allow VCA to be used in uncertainty analysis of any interlock developed per the IEC 61511 standard.

Review of Interlock Design

The IEC standard looks at an interlock as a series of three major components (see Figure 1). First is the sensor set which sends an indication of an abnormal event to a logic solver. The logic solver determines is the signal from the sensor meets the conditions required to activate (trip) the interlock. If the interlock is to be activated, a signal is sent to the final control elements to take action (stop flow, close valve, etc) to prevent a process safety event from occurring.

Based on the devices selected the design engineer then evaluates whether the proposed interlock design meets the design criterion for probability of failure on demand. Typically, the design engineer is given the target PFD as a statement such as “provide a SIL-2 interlock to stop flow on high level in a vessel.” A SIL-2 interlock requires a PFD of at most 0.01 or a risk reduction factor of at least 100. The needed risk reduction is often determined in a Layer of Protection Analysis (LOPA) [Ref. 4] and represents the managements decision on how risk is to be managed in a system. The resulting SIL-2 interlock design must have a high likelihood of achieving the target risk reduction as the LOPA team may be relying on it to be part of an overall risk reduction plan to prevent a process safety incident.

The ISA technical report (TR 84.00.02) [Ref. 2] provides shortcut methods for the evaluation of the PFD of an interlock design. Tables 1 and 2 are taken from the ISA technical report [Ref. 2]. Typical parameters need to compute the PFD include:

- DC is the diagnostic coverage;
- DI is the diagnostic interval;
- TI is the proof test interval,
- λ^D is the dangerous failure rate;
- MTTR is the mean time to restore the system to operation
- β is the common cause failure parameter that is always is between 0 and 1

In practice most if not all of these parameters are uncertain. Using parameter values obtained from plant records, vendor data or generic data bases the design engineer proceeds to develop the model for the interlock.

What is needed is a means to rapidly evaluate the impact of parameter uncertainty on the interlock PFD. The remainder of this paper applies the methods of variance contribution analysis (VCA) to determine the mean (expected value) and the standard deviation of the interlock PFD for a given design.

Table 1. Simplified PFD_{avg} formulas for Non-Repairable System without considering CCF, Diagnostics or MTTR.			
Configuration	**Function**	**PFD based on "Average before" failure rate**	**Appendix A Equation Number**
1oo1	F_1 =	$\left[\lambda^D \times \frac{TI}{2}\right]$	A-1
1oo2	F_2 =	$\left[(\lambda^D)^2 \times \frac{TI^2}{4}\right]$	A- 2
1oo3	F_3 =	$\left[(\lambda^D)^3 \times \frac{TI^3}{8}\right]$	A-3
2oo2	F_4 =	$\left[\lambda^D \times TI\right]$	A-4
2oo3	F5 =	$\frac{3}{4} \times \left[(\lambda^D)^2 \times TI^2\right]$	A-5
3oo3	F6 =	$3 \times \left[\lambda^D \times \frac{TI}{2}\right]$	A-6

Where TI is the proof test interval, λ^D is the dangerous failure rate.

Table 2. Simplified PFD_{avg} Formulas for Repairable System considering CCF, Diagnostics and MTTR			
Configuration	**Function**	**PFD based on "Average before" failure rate**	**Appendix A Equation Number**
1oo1	F_7 =	$\left[\frac{(1-DC)\times\lambda^D\times TI}{2}+\frac{DC\times\lambda^D\times DI}{2}+\lambda^D\times MTTR\right]$	A-24
1oo2	F_8 =	$\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2}+\frac{DC\times(1-\beta)\times\lambda^D\times DI}{2}+(1-\beta)\times\lambda^D\times MTTR\right]^2+\left[\frac{(1-DC)\times\beta\times\lambda^D\times TI}{2}+\frac{DC\times\beta\times\lambda^D\times DI}{2}+\beta\times\lambda^D\times MTTR\right]$	A- 25
1oo3	F_9 =	$\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2}+\frac{DC\times(1-\beta)\times\lambda^D\times DI}{2}+(1-\beta)\times\lambda^D\times MTTR\right]^3+\left[\frac{(1-DC)\times\beta\times\lambda^D\times TI}{2}+\frac{DC\times\beta\times\lambda^D\times DI}{2}+\beta\times\lambda^D\times MTTR\right]$	A-26
2oo2	F_{10} =	$2\times\left[\frac{(1-DC)\times\lambda^D\times TI}{2}+\frac{DC\times\lambda^D\times DI}{2}+\lambda^D\times MTTR\right]$	A-27

Table 2. Simplified PFD_{avg} Formulas for Repairable System considering CCF, Diagnostics and MTTR			
Configuration	**Function**	**PFD based on "Average before" failure rate**	**Appendix A Equation Number**
2oo3	F_{11} =	$3\times\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2}+\frac{DC\times(1-\beta)\times\lambda^D\times DI}{2}+(1-\beta)\times\lambda^D\times MTTR\right]^2+\left[\frac{(1-DC)\times\beta\times\lambda^D\times TI}{2}+\frac{DC\times\beta\times\lambda^D\times DI}{2}+\beta\times\lambda^D\times MTTR\right]$	A-28
3oo3	F_{12} =	$3\times\left[\frac{(1-DC)\times\lambda^D\times TI}{2}+\frac{DC\times\lambda^D\times DI}{2}+\lambda^D\times MTTR\right]$	A-29

Review of 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. 5] and applied by Freeman [Ref. 3, 6, 7]. Define an arbitrary function of a set of random variables, x_i, as:

Let

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

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

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

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:

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

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:

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

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.

Recommended Interlock PFD Uncertainty Analysis Method

Previously, Freeman and Summers [Ref. 3] suggested a framework for the inclusion of uncertainty analysis in the calculations completed for a new interlock per the ISA TR [Ref. 2]. The following uncertainty analysis method has been expanded to incorporate critical decisions that the process management must make in the design process.

1. Complete the interlock design using the methods outlined in IEC 61511 [Ref. 1].

2. Review with the process system management and determine if the proposed interlock should be considered repairable or non-repairable. A simple flow chart for this decision making is presented in Figure 2. The basic question is: "can the interlock be repaired safely while the process operates." This is a management question and management should be the one that decides the answer to this important question.

3. 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 report (TR84.00.02) [Ref. 2]. For non-repairable systems, Table 3 can be used. For more complex systems such as non-repairable redundant systems with the potential for common cause failures, use the repairable equations of Table 4 and set DI, DC, and MTTR all equal to zero. For systems where common cause failures (DCF), Diagnostics and repair are to be considered, use the recommendations of Table 4.

Table 3. Roadmap for Mean and Variance of Non-Repairable System Without Considering CCF, Diagnostics and MTTR			
Configuratio n	**Function**	**Mean PFD Using Appendix A Equation**	**PFD Variance Using Appendix A Equation**
1oo1	F_1 =	A-9	A-18
1oo2	F_2 =	A- 10	A- 19
1oo3	F_3 =	A-11	A-20
2oo2	F_4 =	A-12	A-21
2oo3	F_5 =	A-13	A-22
3oo3	F_6 =	A-14	A-23

Table 4. Roadmap for Mean and Variance of Repairable System Considering CCF, Diagnostics and MTTR			
Configuratio n	**Function**	**Mean PFD Using Appendix A Equation**	**PFD Variance Using Appendix A Equation**
1oo1	F_7 =	A-30	A-44
1oo2	F_8 =	A- 31	A- 86
1oo3	F_9 =	A-32	A-94
2oo2	F_{10} =	A-33	A-48
2oo3	F_{11} =	A-34	A-102
3oo3	F_{12} =	A-35	A-50

Note that in all of the calculations indicated by the equations referenced in Table 4, the expected value of any the random variables is used to complete the calculations.

4. 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 safety instrumented system interlocks.

5. 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 [Ref. 8]. The example interlock calculations used a triangular distribution to represent the uncertainty in the parameters.

6. Compute the expected value or mean of the interlock PFD using the mean value of each of the variables in Step 5. See Tables 4 and 5 for recommended equations.

7. Compute the sensitivity of the result from the interlock performance equation by use of the partial derivative of the basic interlock performance equation with respect to each of the variables as presented in Appendix A.

8. Compute the variance of the interlock performance equation PFD by use of the variance contribution using equations from Tables 3 or 4. 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 7), as evaluated at the variable mean. Sum the resulting terms to obtain the overall variance of the PFD in the interlock performance equation. See Tables 4 and 5 for recommended equations.

9. Determine the level of risk that the owner/operator wishes to take that the final interlock will not work. Note that this is a management decision not an instrument engineer decision! In this paper, the 95% level of risk reduction has been used:
   - 5% chance of failure or a 95% chance of the interlock achieving the desired risk reduction

10. 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, [Ref. 9] as:

$$Z = \left[\frac{xi - E(x)}{\sigma}\right] \qquad \text{(Eq 5)}$$

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 = 1.645. Rearranging Eq. 5 allows for the direct calculation of the corresponding value of the 95% upper confidence limit on the PFD as:

$$X95\% = 1.645\ \sigma + E(x) \qquad \text{(Eq 6)}$$

Where:

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

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.

Example Interlock Problem

Previously, Freeman and Summers [Ref. 3] published an example in the use of VCA to determine the likelihood that the interlock would provide the risk reduction desired by the management and the LOPA team. The process system is shown in Figure 3. 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 Knock Out 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 Knock Out Drum. The SIS logic solver will also monitor the difference in 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. These two different shutdown will both be activated in the event of high level in the Compressor Knock Out Drum. Either one of the two shutdowns is capable of stopping the compressor by turning off the electric power supply to the motor.

Models

The first step in the calculation of the "goodness" of an interlock is to establish the model to be used in the calculations. Note that the sensors are 2oo3 voting and the final control elements are each 1oo1. 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 = PFDs + PFDsis + PFDfce (Eq 7)

Where:

PFD = Probability of failure on demand of the interlock as a whole

PFDs = Probability of failure on demand of the sensors (voting as 2oo3)

PFDsis = Probability of failure on demand of the SIS logic solver

PFDfce = Probability of failure on demand of the final control elements.

Since there are two final control elements arranged in series, the PFDfce = sum of the PFDs of the final control elements (Relay PFD and MCC PFD).

PFDce = PFDr + PFDmcc (Eq 8)

Where:

PFDr = Probability of failure on demand of the two relays voting as 1oo2 to shutdown gas compressor.

PFDmcc = Probability of failure on demand of the MCC to shutdown the gas compressor

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

Model for Sensors (2oo3)

The sensors are considered repairable as one sensor can be replaced while the other two function and provide continuous functionality of the interlock. There are three sensors that will be used in a 2oo3 voting system. From Appendix A, using Equation A-7, the model for the sensors becomes:

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

$$\left[\frac{(1-DCs)\times\beta s\times\lambda^{Ds}\times TIs}{2}+\frac{DCs\times\beta s\times\lambda^{D}\times DIs}{2}+\beta s\times\lambda^{Ds}\times MTTRs\right] \qquad \text{(Eq 9)}$$

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

MTTR is the mean time to restore the system from the time that failure occurs

Model for SIS Logic Solver

Use a fixed probability of failure on demand 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 1.30×10^{-4} was selected to represent the SIS Logic Solver.

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 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. Two different models are needed to the final control elements. These two subsystems are considered non-repairable in this analysis,

Model for Interposing Relays (1oo2)

There are two interposing relays (R1 and R2 in the interlock). From Appendix A, use Equation A-25 setting parameters DC=DI=MTTR=0 for the non-repairable interposing relays, the model becomes:

$$\text{PFDravg} = \left[\frac{(1-\beta r)\times\lambda^{Dr}\times TIr}{2}+\right]^2+\left[\frac{\beta r\times\lambda^{Dr}\times TIr}{2}+\right] \qquad \text{(Eq 10)}$$

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

β_r is the common cause failure parameter

λ^{Dr} is the failure rate to a dangerous condition for the relays

Model for MCC (1oo1)

From Appendix A and using equation A-1 for the non-repairable MCC, the model becomes:

$$\boldsymbol{PFDmccavg} = \frac{\lambda^{Dmcc} * \mathbf{TImcc}}{\mathbf{2}} \qquad \text{(Eq 11)}$$

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

$\lambda^{Dmcc}$is the failure rate to a dangerous condition for the MCC

Data

The calculation of the PFD of the interlock requires a set of data to be used to represent the system. Tables 5, 6, and 7 are taken from the Freeman-Summers paper [Ref. 3] and presents the data used to represent the interlock system. Note that these data were originally taken from generic data sources and do not represent any particular device or system.

Table 5. 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	2.84×10^{-3} Yr^{-1}	5×10^{-3} Yr^{-1}	8.5×10^{-3} Yr^{-1}	5.45×10^{-3} Yr^{-1}	1.36×10^{-6} Yr^{-1}
DC_s – Diagnostic Coverage *	0.8	0.9	0.99	0.897	1.51×10^{-3}
DI_s – Diagnostic Interval **	5.71×10^{-5}	5.71×10^{-5}	5.71×10^{-5}	5.71×10^{-5}	0
TI_s – Test Interval	4 Yr	5 Yr	6 Yr	5 Yr	5.56×10^{-2} Yr^{2}
β_s- Common Cause Failure Fraction *	0	0.02	0.1	0.04	4.67×10^{-4}
$MTTR_s$ - Mean Time to Restore ***	1.37×10^{-3} Yr	8.22×10^{-3} Yr	1.92×10^{-2} Yr	9.59×10^{-3} Yr	1.34×10^{-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 6. 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	0.056 Yr^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 7. 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	$1.74x10^{-4}$ Yr^{-1}	$1.31x10^{-3}$ Yr^{-1}	$3.00x10^{-2}$ Yr^{-1}	$1.05x10^{-2}$ Yr^{-1}	$4.76x10^{-5}$ 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	$5.6x10^{-2}$ 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

Uncertainty Analysis Results

Using the VCA method to estimate the PFD of the interlock design yields the results shown in Table 8.

Table 8. Results of VCA on Example Interlock Design		
Subsystem	**Mean PFD**	**Variance of PFD**
Sensors	6.41E-5	1.7657E-9
Logic Solver	1.34E-4	0
Relays	5.46E-4	2.0333E-7
MCC	6.98E-3	4.52E-5
Totals	**7.73E-3**	**4.54E-5**

Note: Calculations are carried to an adequate number of places to allow for the resulting PFD to be determined. Rounding to significant number of figures is done at the end.

The mean PFD of 0.00773 implies a mean risk reduction factor of:

RRF = 1/PFD = 1/0.00773 = 129 (Eq 11)

The variance of 4.54E-5 implies a standard deviation in the PFD of

Std Dev = (Variance)$^{1/2}$ = 0.006737 (Eq 12)

The corresponding 95% level of confidence in the PFD:

X95% = 1.645 std Dev + Mean PFD (Eq 13)

X95% = 1.645 (0.006737) + 0.00773= 0.01881 (Eq 14)

The RRF for 95% certain PFD is

RRF95% = 1/0.01881 => 53 (Eq 15)

This is essentially the same result previously reported by Freeman and Summers [Ref. 3] using either Monte Carlo Simulation or numerical approximation methods for the VCA sensitivities. The calculated PFD at the 95% level of 0.01881 indicates that there is only a 5% chance that the interlock will provide an RRF worse that 53. Since this level is only SIL-1 capable and not

SIL-2 capable as desired by management, a revised design will be needed to achieve the desired risk reduction or a different protective measure will be needed to control risk.

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. (2015).

3. Freeman, R. and Summers, A, "Evaluation of Uncertainty in Safety Integrity Level Calculations," Process Safety Progress, Published Wiley Online Library (wileyonlinelibrary.com). DOI 10.1002/prs.11805, 23 January 2016

4. Center for Chemical Process Safety, *Layer of Protection Analysis – Simplified Process Risk Assessment*, AmericanInstitute of Chemical Engineers, New York, 2001

5. Edward B. Haugen, Probabilistic Approaches to Design, John Wiley, New York, 1968

6. R.A. Freeman, "Quantifying LOPA Uncertainty," Process Safety Progress, Vol 31, No. 3, pp 240-247, 2012

7. 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

8. David Vose, Risk Analysis – A Quantitative Guide, 3rd Edition, John Wiley, 2008

9. Paul L. Meyer, Introductory Probability and Statistical Applications, John Wiley, New York, 1972

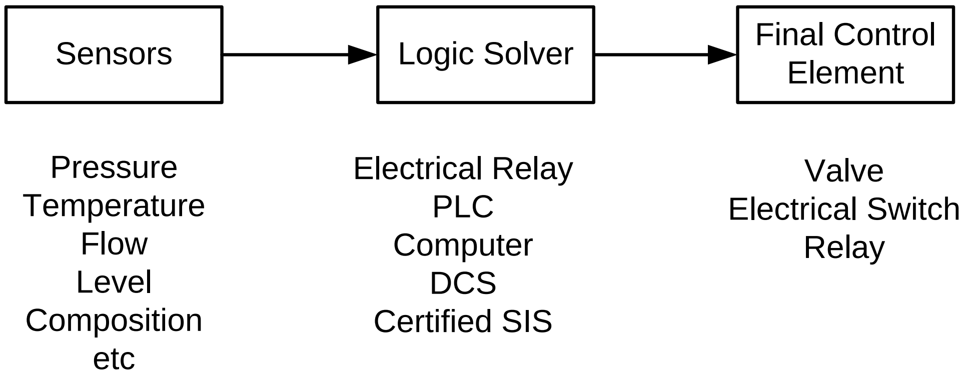


Figure 1. Typical Components of an SIS Interlock

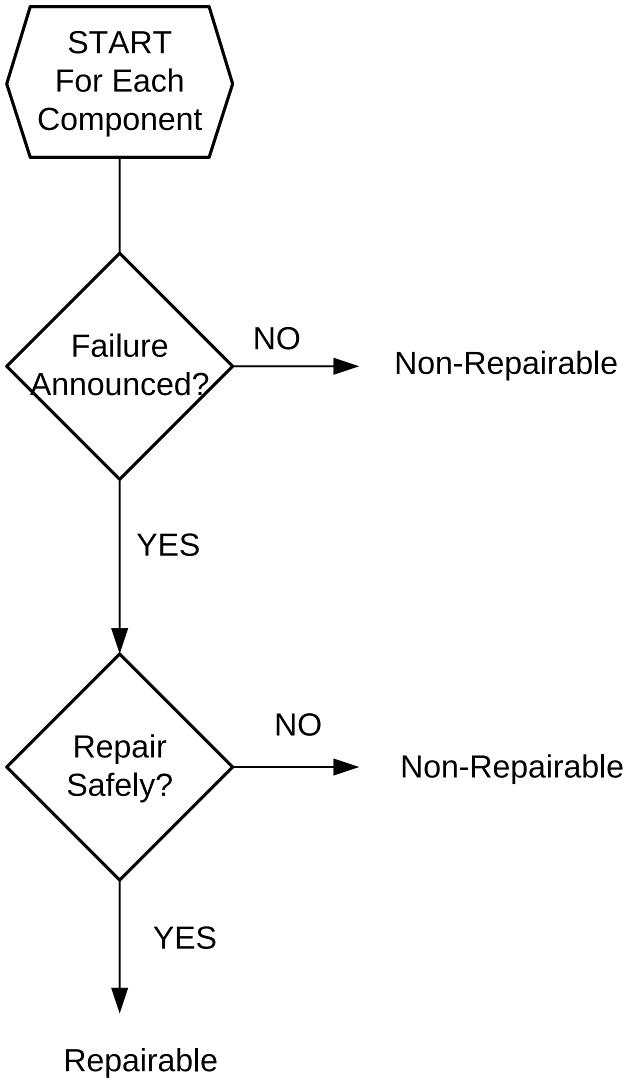
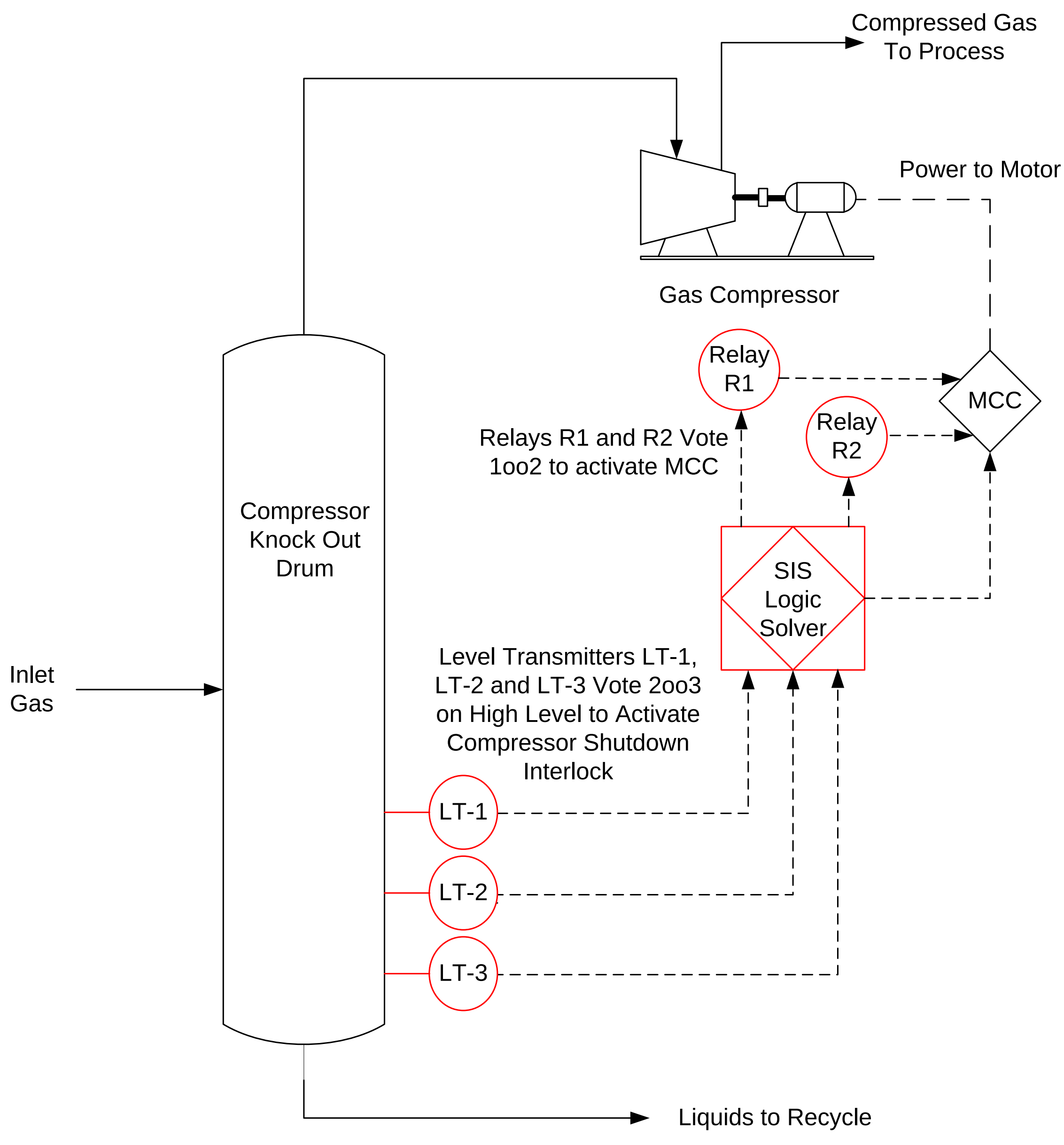


Figure 2. Decision Tree for Determination
of Repairable or Non- Repairable

Figure 3. P&ID Sketch for Example Interlock



APPENDIX A -- DEVELOPMENT OF UNCERTAINTY EQUATIONS

NON-REPAIRABLE SYSTEMS

For systems that are considered non-repairable, the simplified equations of Table A.1 (taken from the ISA Technical Report [Ref. 2]) are used for the analysis.

Table A.1 Simplified PFD_{avg} formulas for Non-Repairable System without considering CCF, Diagnostics or MTTR.

Configuration	Function	PFD based on "Average before" failure rate	Equation Number
1oo1	F_1 =	$\left[\lambda^D \times \frac{\mathrm{TI}}{2}\right]$	A-1
1oo2	F_2 =	$\left[(\lambda^D)^2 \times \frac{\mathrm{TI}^2}{4}\right]$	A- 2
1oo3	F_3 =	$\left[(\lambda^D)^3 \times \frac{\mathrm{TI}^3}{8}\right]$	A-3
2oo2	F_4 =	$\left[\lambda^D \times \mathrm{TI}\right]$	A-4
2oo3	F5 =	$\frac{3}{4} \times \left[(\lambda^D)^2 \times \mathrm{TI}^2\right]$	A-5
3oo3	F6 =	$3 \times \left[\lambda^D \times \frac{\mathrm{TI}}{2}\right]$	A-6

Where TI is the proof test interval, λ^D is the dangerous failure rate.

The expected value of the probability of failure on demand is found by calculating the PFD using the expected value (mean) of the random variables.

Let y a function of some random variables, x_i, as:

$$y = F(x_i) \qquad \text{(Eq A-7)}$$

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

$$E(y) = F[E(x_i)] \qquad \text{(Eq A-8)}$$

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

For the configurations defined in Table A.1, the corresponding expected PFD are presented in Table A.2.

Table A.2 Expected Value of PFD_{avg} formulas for Non-Repairable System without considering CCF, Diagnostics or MTTR.			
Configuration	**Function**	**Expected PFD based on "Average before" failure rate**	**Equation Number**
1oo1	$E(F_1)$ =	$\left[E(\lambda^D)\times\frac{E(\mathrm{TI})}{2}\right]$	A-9
1oo2	$E(F_2)$ =	$\left[(E(\lambda^D))^2\times\frac{E(\mathrm{TI})^2}{4}\right]$	A- 10
1oo3	$E(F_3)$ =	$\left[(E(\lambda^D))^3\times\frac{E(\mathrm{TI})^3}{8}\right]$	A-11
2oo2	$E(F_4)$ =	$\left[E(\lambda^D)\times E(\mathrm{TI})\right]$	A-12
2oo3	$E(F_5)$ =	$\frac{3}{4}\times\left[(E(\lambda^D))^2\times E(\mathrm{TI})^2\right]$	A-13
3oo3	$E(F_6)$ =	$3\times\left[E(\lambda^D)\times\frac{E(\mathrm{TI})}{2}\right]$	A-14

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

The variance of the PFD is found by taking the weighted sum of the variance of the random variables. The weighting function is the sensitivity of the PFD with respect to random variable. In mathematical terms the variance of a function may be found in terms of the variance of the random variables as:

Once again let

$y = F(x_i)$ (Eq A-15)

The variance of Y can likewise be estimated as:

$$V(y) = \sum_{i=1}^{n} \left[\frac{\partial y}{\partial x_i}\right]^2 V(x_i) \qquad \text{(Eq A-16)}$$

Where:

$V(y)$ = variance of random variable y as defined above

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

The sensitivity of y with respect to a random variable x_i is:

$$\text{Sensitivity of y with respect to } x_i = \left[\frac{\partial y}{\partial x_i}\right] \qquad \text{(Eq A-17)}$$

For the configurations defined in Table A.1, the corresponding variance of the PFD are presented in Table A.3.

Table A.3 Variance of PFD_{avg} formulas for Non-Repairable System without considering CCF, Diagnostics or MTTR.			
Configuration	**Function**	**Variance in Function F_i based on "Average before" failure rate**	**Equation Number**
1oo1	$V(F_1) =$	$\left[\frac{E(\mathrm{TI})}{2}\right]^2 V(\lambda^D) + \left[\frac{E(\lambda^D)}{2}\right]^2 V(TI)$	A-18
1oo2	$V(F_2) =$	$\left[E(\lambda^D)^2 \frac{E(\mathrm{TI})^2}{2}\right]^2 V(\lambda^D) +$ $\left[E(\lambda^D)^2 \frac{E(TI)}{2}\right]^2 V(TI)$	A- 19
1oo3	$V(F_3) =$	$\left[3\times E(\lambda^D)^2 \frac{E(\mathrm{TI})^3}{2}\right]^2 V(\lambda^D) +$ $\left[\frac{3}{8} E(\lambda^D)^3 E(TI)^2\right]^2 V(TI)$	A-20
2oo2	$V(F_4) =$	$E(TI)^2 V(\lambda^D) + E(\lambda^D)^2 \times V(\mathrm{TI})$	A-21
2oo3	$V(F_5) =$	$\left[\frac{3}{2}\times E(\lambda^D)\times E(\mathrm{TI})^2\right]^2 V(\lambda^D) +$ $\left[\frac{3}{2}\times E(\lambda^D)^2 \times E(\mathrm{TI})\right]^2 V(TI)$	A-22
3oo3	$V(F_6) =$	$\left[\frac{3}{2}\times E(\mathrm{TI})\right]^2 V(\lambda^D) +$ $\left[\frac{3}{2}\times E(\lambda^D)\right]^2 V(TI)$	A-23

Note that for the calculation of the variance functions, V(Fi), the random variables are evaluated at the expected value (mean).

REPAIRABLE SYSTEMS

For systems that are considered repairable, the simplified equations of Table A.4 are used for the analysis. The expected value of the probability of failure on demand (PFD) is found by substituting the expected value of each of the random variables into the corresponding equation. The expected value of the PFD for each of the system configurations is presented in Table A.5

Table A.4 Simplified PFD_{avg} Formulas for Repairable System considering CCF, Diagnostics and MTTR			
Configuration	**Function**	**PFD based on "Average before" failure rate**	**Equation Number**
1oo1	F_7 =	$\left[\frac{(1-DC)\times\lambda^D\times TI}{2}+\frac{DC\times\lambda^D\times DI}{2}+\lambda^D\times MTTR\right]$	A-24
1oo2	F_8 =	$\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2}+\frac{DC\times(1-\beta)\times\lambda^D\times DI}{2}+(1-\beta)\times\lambda^D\times MTTR\right]^2+\left[\frac{(1-DC)\times\beta\times\lambda^D\times TI}{2}+\frac{DC\times\beta\times\lambda^D\times DI}{2}+\beta\times\lambda^D\times MTTR\right]$	A- 25
1oo3	F_9 =	$\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2}+\frac{DC\times(1-\beta)\times\lambda^D\times DI}{2}+(1-\beta)\times\lambda^D\times MTTR\right]^3+\left[\frac{(1-DC)\times\beta\times\lambda^D\times TI}{2}+\frac{DC\times\beta\times\lambda^D\times DI}{2}+\beta\times\lambda^D\times MTTR\right]$	A-26
2oo2	F_{10} =	$2\times\left[\frac{(1-DC)\times\lambda^D\times TI}{2}+\frac{DC\times\lambda^D\times DI}{2}+\lambda^D\times MTTR\right]$	A-27
2oo3	F_{11} =	$3\times\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2}+\frac{DC\times(1-\beta)\times\lambda^D\times DI}{2}+(1-\beta)\times\lambda^D\times MTTR\right]^2+\left[\frac{(1-DC)\times\beta\times\lambda^D\times TI}{2}+\frac{DC\times\beta\times\lambda^D\times DI}{2}+\beta\times\lambda^D\times MTTR\right]$	A-28

Table A.4 Simplified PFD_{avg} Formulas for Repairable System considering CCF, Diagnostics and MTTR			
Configuratio n	**Function**	**PFD based on "Average before" failure rate**	**Equation Number**
3oo3	F_{12} =	$3\times\left[\frac{(1-DC)\times\lambda^{D}\times TI}{2}+\frac{DC\times\lambda^{D}\times DI}{2}+\lambda^{D}\times MTTR\right]$	A-29

Where:

DC is the diagnostic coverage;

DI is the diagnostic interval;

TI is the proof test interval,

λ^D is the dangerous failure rate;

MTTR is the mean time to restore the system to operation

β is the common cause failure parameter that is always is between 0 and 1

Table A.5 Expected PFD Formulas for Repairable System considering CCF, Diagnostics and MTTR			
Configuration	**Function**	**PFD based on "Average before" failure rate**	**Equation Number**
1oo1	$E(F_7)$ =	$\left[\frac{(1-E(DC))\times E(\lambda^D)\times E(TI))}{2}+\frac{E(DC)\times E(\lambda^D)\times E(DI)}{2} + E(\lambda^D)\times E(MTTR)\right]$	A-30
1oo2	$E(F_8)$ =	$\left[\frac{(1-E(DC))\times(1-E(\beta))\times E(\lambda^D)\times E(TI)}{2}+ \frac{E(DC)\times(1-E(\beta))\times E(\lambda^D)\times E(DI)}{2}+ (1-E(\beta))\times E(\lambda^D)\times E(MTTR)\right]^2 + \left[\frac{(1-E(DC))\times E(\beta)\times E(\lambda^D)\times E(TI)}{2}+ \frac{E(DC)\times E(\beta)\times E(\lambda^D)\times E(DI}{2})+ E(\beta)\times E(\lambda^D)\times E(MTTR)\right]$	A- 31
1oo3	$E(F_9)$ =	$\left[\frac{(1-E(DC))\times(1-E(\beta))\times E(\lambda^D)\times E(TI)}{2}+ \frac{E(DC)\times(1-E(\beta))\times E(\lambda^D)\times E(DI)}{2}+ (1-E(\beta))\times E(\lambda^D)\times E(MTTR)\right]^3 + \left[\frac{(1-E(DC))\times E(\beta)\times E(\lambda^D)\times E(TI)}{2}+ \frac{E(DC)\times E(\beta)\times E(\lambda^D)\times E(DI)}{2}+ E(\beta)\times E(\lambda^D)\times E(MTTR)\right]$	A-32

Table A.5 Expected PFD Formulas for Repairable System considering CCF, Diagnostics and MTTR

Configuration	Function	PFD based on "Average before" failure rate	Equation Number
2oo2	$E(F_{10}) =$	$2\times\left[\begin{array}{l}\frac{(1-E(DC))\times E(\lambda^D)\times E(TI))}{2}+\\ \frac{E(DC)\times E(\lambda^D)\times E(DI)}{2}\\ +E(\lambda^D)\times E(MTTR)\end{array}\right]$	A-33
2oo3	$E(F_{11}) =$	$3\times\left[\begin{array}{l}\frac{(1-E(DC))\times(1-E(\beta))\times E(\lambda^D)\times E(TI)}{2}+\\ \frac{E(DC)\times(1-E(\beta))\times E(\lambda^D)\times E(DI)}{2}+\\ (1-E(\beta))\times E(\lambda^D)\times E(MTTR)\end{array}\right]^2 + \left[\begin{array}{l}\frac{(1-E(DC))\times E(\beta)\times E(\lambda^D)\times E(TI)}{2}+\\ \frac{E(DC)\times E(\beta)\times E(\lambda^D)\times E(DI)}{2}+\\ E(\beta)\times E(\lambda^D)\times E(MTTR)\end{array}\right]$	A-34
3oo3	$E(F_{12}) =$	$3\times\left[\begin{array}{l}\frac{(1-E(DC))\times E(\lambda^D)\times E(TI))}{2}+\\ \frac{E(DC)\times E(\lambda^D)\times E(DI)}{2}\\ +E(\lambda^D)\times E(MTTR)\end{array}\right]$	A-35

The variance of the PFD of the repairable systems is found in the same manner as that in the non-repairable cases. Once again let:

$y = F(x_i)$ (Eq A-36)

The variance of Y can likewise be estimated as:

$$V(y) = \sum_{i=1}^{n} \left[\frac{\partial y}{\partial x_i}\right]^2 V(x_i) \quad \text{(Eq A-37)}$$

Where:

$V(y)$ = variance of random variable y as defined above

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

The sensitivity of y with respect to a random variable x_i is:

In the case of the repairable systems, there are several more potentially uncertain or random variables:

- DC is the diagnostic coverage;
- DI is the diagnostic interval;
- TI is the proof test interval,
- λ^D is the dangerous failure rate;
- MTTR is the mean time to restore the system to operation
- β is the common cause failure parameter that is always is between 0 and 1

We must evaluate the partial derivative of the PFD function with respect to each and then combine them using equation A-37. The partial derivatives of function F7 with respect to each random variable are found as follows

$$\frac{\partial F_7}{\partial DC} = \frac{-\lambda^D \times TI}{2} + \frac{\lambda^D \times DI}{2} \quad \text{(Eq A-38)}$$

$$\frac{\partial F_7}{\partial \lambda^D} = \frac{(1-DC)\times TI}{2} + \frac{DC \times DI}{2} + MTTR \quad \text{(Eq A-39)}$$

$$\frac{\partial F_7}{\partial TI} = \frac{(1-DC)\times \lambda^D}{2} \quad \text{(Eq A-40)}$$

$$\frac{\partial F_7}{\partial DI} = \frac{DC \times \lambda^D}{2} \qquad \text{(Eq A-41)}$$

$$\frac{\partial F_7}{\partial MTTR} = \lambda^D \qquad \text{(Eq A-42)}$$

We can now compute the variance of function F7 as:

$$V\left(F_7\right) = \sum_{i=1}^{n} \left[\frac{\partial F_7}{\partial x_i}\right]^2 V(x_i) \qquad \text{(Eq A-43)}$$

$$V\left(F_7\right) = \left[\frac{-\lambda^D \times TI}{2} + \frac{\lambda^D \times DI}{2}\right]^2 \mathrm{V(DC)} + \left[\frac{(1-DC)\times TI}{2} + \frac{DC \times DI}{2} + MTTR\right]^2 \mathrm{V}(\lambda^D) +$$

$$\left[\frac{(1-DC)\times \lambda^D}{2}\right]^2 \mathrm{V(TI)} + \left[\frac{DC \times \lambda^D}{2}\right]^2 \mathrm{(DI)} + \left[\lambda^D\right]^2 \mathrm{V(MTTR)} \qquad \text{(Eq A-44)}$$

Equation 44 represents the variance of the probability of failure on demand of the 1oo1 configuration when the system is repairable. We note the following relationships between the 1oo1, 2oo2 and 3oo3 configurations:

$F_{10} = 2\ F_7$ (Eq A-45)

$F_{12} = 3\ F_7$ (Eq A-46)

We can directly determine the variance of functions F_{10} and F_{12} from the properties of the variance operator, V(X).

$V(F_{10}) = V(2\ F_7)$ (Eq A-47)

$V(F_{10}) = 4\ V(F_7)$ (Eq A-48)

$V(F_{12}) = V(3\ F_7)$ (Eq A-49)

$V(F_{12}) = 9\ V(F_7)$ (Eq A-50)

The determination of the variance of functions F_8, F_{10}, and F_{11} is done in a similar manner. To simplify the presentation of the derivation of variance of functions F_8, F_{10}, and F_{11}, we introduce two functions H and Q as:

$$H = \left[\frac{(1-DC)\times(1-\beta)\times\lambda^D \times TI}{2} + \frac{DC \times (1-\beta)\times \lambda^D \times DI}{2} + (1-\beta)\times\lambda^D \times MTTR\right] \qquad \text{(Eq A-51)}$$

$$Q = \left[\frac{(1-DC)\times\beta\times\lambda^D\times TI}{2} + \frac{DC\times\beta\times\lambda^D\times DI}{2} + \beta\times\lambda^D\times MTTR \right] \quad \text{(Eq A-52)}$$

We note the following relationships:

$$F_8 = H^2 + Q \quad \text{(Eq A-53)}$$

$$F_9 = H^3 + Q \quad \text{(Eq A-54)}$$

$$F_{11} = 3\,H^2 + Q \quad \text{(Eq A-55)}$$

The variance of F_8, F_9 and F_{11} are found as:

$$V(F_8) = V(H^2 + Q) \quad \text{(Eq A-56)}$$

$$V(F_9) = V(H^3 + Q) \quad \text{(Eq A-57)}$$

$$V(F_{11}) = V(3\,H^2 + Q) \quad \text{(Eq A-58)}$$

We will need the sensitivity of F_8, F_9 and F_{11} to each of the potential random variables.

$$\frac{\partial F_8}{\partial x} = \frac{\partial(H^2 + Q)}{\partial x} = \frac{\partial(H^2)}{\partial x} + \frac{\partial(Q)}{\partial x} \quad \text{(Eq A-59)}$$

Likewise

$$\frac{\partial F_9}{\partial x} = \frac{\partial(H^3 + Q)}{\partial x} = \frac{\partial(H^3)}{\partial x} + \frac{\partial(Q)}{\partial x} \quad \text{(Eq A-60)}$$

$$\frac{\partial F_{11}}{\partial x} = \frac{\partial 3(H^2 + Q)}{\partial x} = 3\frac{\partial(H^2)}{\partial x} + 3\frac{\partial(Q)}{\partial x} \quad \text{(Eq A-61)}$$

Using the chain rule for partial derivatives, we now write:

$$\frac{\partial F_8}{\partial x} = 2H\frac{\partial(H)}{\partial x} + \frac{\partial(Q)}{\partial x} \quad \text{(Eq A-62)}$$

$$\frac{\partial F_9}{\partial x} = 3H^2\frac{\partial(H)}{\partial x} + \frac{\partial(Q)}{\partial x} \quad \text{(Eq A-63)}$$

$$\frac{\partial F_{11}}{\partial x} = 6H\frac{\partial(H)}{\partial x} + \frac{\partial(Q)}{\partial x} \quad \text{(Eq A-64)}$$

We now evaluate the derivatives of function H with respect to each potential random variables:

- DC is the diagnostic coverage;
- DI is the diagnostic interval;
- TI is the proof test interval,
- λ^D is the dangerous failure rate;
- MTTR is the mean time to restore the system to operation
- β is the common cause failure parameter that is always is between 0 and 1

$$\frac{\partial(\mathrm{H})}{\partial DC} = \frac{-(1-\beta)\times\lambda^D\times TI}{2} + \frac{(1-\beta)\times\lambda^D\times DI}{2} \qquad \text{(Eq A-65)}$$

$$\frac{\partial(\mathrm{H})}{\partial TI} = \frac{(1-DC)\times(1-\beta)\times\lambda^D}{2} \qquad \text{(Eq A-66)}$$

$$\frac{\partial(\mathrm{H})}{\partial \lambda^D} = \left[\begin{array}{l} \frac{(1-DC)\times(1-\beta)\times TI}{2} + \\ \frac{DC\times(1-\beta)\times DI}{2} + (1-\beta)\times MTTR \end{array}\right] \qquad \text{(Eq A-67)}$$

$$\frac{\partial(\mathrm{H})}{\partial MTTR} = (1-\beta)\times\lambda^D \qquad \text{(Eq A-68)}$$

$$\frac{\partial(\mathrm{H})}{\partial \beta} = \left[\begin{array}{l} \frac{(1-DC)\times(-1)\times\lambda^D\times TI}{2} + \\ \frac{DC\times(-1)\times\lambda^D\times DI}{2} + (-1)\times\lambda^D\times MTTR \end{array}\right] \qquad \text{(Eq A-69)}$$

$$\frac{\partial(\mathrm{H})}{\partial DI} = \frac{DC\times(1-\beta)\times\lambda^D}{2} \qquad \text{(Eq A-70)}$$

In a similar manner we evaluate the partial derivatives of function Q with respect to each potential random variables.

$$Q = \left[\frac{(1-DC)\times\beta\times\lambda^D\times TI}{2}+\frac{DC\times\beta\times\lambda^D\times DI}{2}+\beta\times\lambda^D\times MTTR\right] \qquad \text{(Eq A-71)}$$

- DC is the diagnostic coverage;
- DI is the diagnostic interval;
- TI is the proof test interval,
- λ^D is the dangerous failure rate;
- MTTR is the mean time to restore the system to operation
- β is the common cause failure parameter that is always is between 0 and 1

$$\frac{\partial(Q)}{\partial DC} = \frac{(-1)\times\beta\times\lambda^D\times TI}{2}+\frac{\beta\times\lambda^D\times DI}{2} \qquad \text{(Eq A-72)}$$

$$\frac{\partial(Q)}{\partial TI} = \frac{(1-DC)\times\beta\times\lambda^D}{2} \qquad \text{(Eq A-73)}$$

$$\frac{\partial(Q)}{\partial\lambda^D} = \left[\frac{(1-DC)\times\beta\times TI}{2}+\frac{DC\times\beta\times DI}{2}+\beta\times MTTR\right] \qquad \text{(Eq A-74)}$$

$$\frac{\partial(Q)}{\partial MTTR} = \beta\times\lambda^D\times MTTR \qquad \text{(Eq A-75)}$$

$$\frac{\partial(Q)}{\partial\beta} = \left[\frac{(1-DC)\times\lambda^D\times TI}{2}+\frac{DC\times\lambda^D\times DI}{2}+\lambda^D\times MTTR\right] \qquad \text{(Eq A-76)}$$

$$\frac{\partial(Q)}{\partial DI} = \frac{DC\times\beta\times\lambda^D}{2} \qquad \text{(Eq A-77)}$$

We can now determine the sensitivity of the functions F8, F9 , F11 to the random variables of interest. Restating equation A-62 for sensitivity of F8 with respect to the random variables.

$$\frac{\partial F_8}{\partial x} = 2H\frac{\partial(H)}{\partial x}+\frac{\partial(Q)}{\partial x} \qquad \text{(Eq A-78)}$$

For F_8 we find

$$\frac{\partial F_8}{\partial x} = 2\mathrm{H}\frac{\partial(\mathrm{H})}{\partial x} + \frac{\partial(\mathrm{Q})}{\partial x} \tag{Eq A-80}$$

$$\frac{\partial F_8}{\partial DC} = 2\left[\begin{array}{l}\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2}+\\ \frac{DC\times(1-\beta)\times\lambda^D\times DI}{2}+(1-\beta)\times\lambda^D\times MTTR\end{array}\right]\times \Bigg[$$

$$\left.\frac{-(1-\beta)\times\lambda^D\times TI}{2}+\frac{(1-\beta)\times\lambda^D\times DI}{2}\right]+$$

$$\frac{(-1)\times\beta\times\lambda^D\times TI}{2}+\frac{\beta\times\lambda^D\times DI}{2} \tag{Eq A-79}$$

$$\frac{\partial F_8}{\partial TI} = 2\left[\begin{array}{l}\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2}+\\ \frac{DC\times(1-\beta)\times\lambda^D\times DI}{2}+(1-\beta)\times\lambda^D\times MTTR\end{array}\right]\times\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D}{2}\right]+$$

$$\frac{(1-DC)\times\beta\times\lambda^D}{2} \tag{Eq A-81}$$

$$\frac{\partial F_8}{\partial MTTR} = 2\left[\begin{array}{l}\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2}+\\ \frac{DC\times(1-\beta)\times\lambda^D\times DI}{2}+(1-\beta)\times\lambda^D\times MTTR\end{array}\right]\times$$

$$\left[(1-\beta)\times\lambda^D\right]+\beta\times\lambda^D\times MTTR \tag{Eq A-82}$$

$$\frac{\partial F_8}{\partial \beta} = 2\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2} + \frac{DC\times(1-\beta)\times\lambda^D\times DI}{2} + (1-\beta)\times\lambda^D\times MTTR\right]\times \left[\left[\frac{(1-DC)\times(-1)\times\lambda^D\times TI}{2} + \frac{DC\times(-1)\times\lambda^D\times DI}{2} + (-1)\times\lambda^D\times MTTR\right]\right] + \left[\frac{(1-DC)\times\lambda^D\times TI}{2} + \frac{DC\times\lambda^D\times DI}{2} + \lambda^D\times MTTR\right] \quad \text{(Eq A-83)}$$

$$\frac{\partial F_8}{\partial DI} = 2\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2} + \frac{DC\times(1-\beta)\times\lambda^D\times DI}{2} + (1-\beta)\times\lambda^D\times MTTR\right]\times\left[\frac{DC\times(1-\beta)\times\lambda^D}{2}\right] + \frac{DC\times\beta\times\lambda^D}{2} \quad \text{(Eq A-84)}$$

$$\left[\frac{\partial F_8}{\partial \lambda^D}\right] = 2\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2} + \frac{DC\times(1-\beta)\times\lambda^D\times DI}{2} + (1-\beta)\times\lambda^D\times MTTR\right]\times\left[\frac{(1-DC)\times(1-\beta)\times TI}{2} + \frac{DC\times(1-\beta)\times DI}{2} + (1-\beta)\times MTTR\right] + \left[\frac{(1-DC)\times\beta\times TI}{2} + \frac{DC\times\beta\times DI}{2} + \beta\times MTTR\right] \quad \text{(Eq A-85)}$$

Using the sensitivities for F8 calculated above, the variance in F8 due to uncertain or random variables is found as:

$$V(F_8) = \left[\frac{\partial F_8}{\partial DC}\right]^2 V(DC) + \left[\frac{\partial F_8}{\partial TI}\right]^2 V(TI) + \left[\frac{\partial F_8}{\partial \lambda^D}\right]^2 V(\lambda^D) + \left[\frac{\partial F_8}{\partial MTTR}\right]^2 V(MTTR) + \left[\frac{\partial F_8}{\partial \beta}\right]^2 V(\beta) + \left[\frac{\partial F_8}{\partial DI}\right]^2 V(DI) \quad \text{(Eq A-86)}$$

Using the equation A-63, we now determine the variance of F_9.

$$\frac{\partial F_9}{\partial x} = 3\mathrm{H}^2 \ \frac{\partial(\mathrm{H})}{\partial x} + \frac{\partial(\mathrm{Q})}{\partial x} \qquad \text{(Eq A-87)}$$

$$\frac{\partial F_9}{\partial DC} = 3\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2} + \frac{DC\times(1-\beta)\times\lambda^D\times DI}{2} + (1-\beta)\times\lambda^D\times MTTR\right]^2 \times \left[\frac{-(1-\beta)\times\lambda^D\times TI}{2} + \frac{(1-\beta)\times\lambda^D\times DI}{2}\right] + \frac{(-1)\times\beta\times\lambda^D\times TI}{2} + \frac{\beta\times\lambda^D\times DI}{2} \qquad \text{(Eq A-88)}$$

$$\frac{\partial F_9}{\partial TI} = 3\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2} + \frac{DC\times(1-\beta)\times\lambda^D\times DI}{2} + (1-\beta)\times\lambda^D\times MTTR\right]^2 \times \left[\frac{(1-DC)\times(1-\beta)\times\lambda^D}{2}\right] + \frac{(1-DC)\times\beta\times\lambda^D}{2} \qquad \text{(Eq A-89)}$$

$$\frac{\partial F_9}{\partial MTTR} = 3\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2} + \frac{DC\times(1-\beta)\times\lambda^D\times DI}{2} + (1-\beta)\times\lambda^D\times MTTR\right]^2 \times \left[(1-\beta)\times\lambda^D\right] + \beta\times\lambda^D\times MTTR \qquad \text{(Eq A-90)}$$

$$\frac{\partial F_9}{\partial \beta} = 3\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2} + \frac{DC\times(1-\beta)\times\lambda^D\times DI}{2} + (1-\beta)\times\lambda^D\times MTTR\right]^2 \times \left[\left[\frac{(1-DC)\times(-1)\times\lambda^D\times TI}{2} + \frac{DC\times(-1)\times\lambda^D\times DI}{2} + (-1)\times\lambda^D\times MTTR\right]\right] + \left[\frac{(1-DC)\times\lambda^D\times TI}{2} + \frac{DC\times\lambda^D\times DI}{2} + \lambda^D\times MTTR\right] \qquad \text{(Eq A-91)}$$

$$\frac{\partial F_9}{\partial DI} = 3\left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2} + \frac{DC\times(1-\beta)\times\lambda^D\times DI}{2} + (1-\beta)\times\lambda^D\times MTTR\right]^2 \times \left[\frac{DC\times(1-\beta)\times\lambda^D}{2}\right] + \frac{DC\times\beta\times\lambda^D}{2} \qquad \text{(Eq A-92)}$$

$$\left[\frac{\partial F_9}{\partial \lambda^D}\right] = 3 \times \left[\frac{(1-DC)\times(1-\beta)\times\lambda^D\times TI}{2} + \frac{DC\times(1-\beta)\times\lambda^D\times DI}{2} + (1-\beta)\times\lambda^D\times MTTR\right]^2 \times \left[\frac{(1-DC)\times(1-\beta)\times TI}{2} + \frac{DC\times(1-\beta)\times DI}{2} + (1-\beta)\times MTTR\right] + \left[\frac{(1-DC)\times\beta\times TI}{2} + \frac{DC\times\beta\times DI}{2} + \beta\times MTTR\right] \qquad \text{(Eq A-93)}$$

Using the sensitivities for F_9 calculated above, the variance in F_9 due to uncertain or random variables is found as:

$$V(F_9) = \left[\frac{\partial F_9}{\partial DC}\right]^2 V(DC) + \left[\frac{\partial F_9}{\partial TI}\right]^2 V(TI) + \left[\frac{\partial F_9}{\partial \lambda^D}\right]^2 V(\lambda^D) + \left[\frac{\partial F_9}{\partial MTTR}\right]^2 V(MTTR) + \left[\frac{\partial F_9}{\partial \beta}\right]^2 V(\beta) + \left[\frac{\partial F_9}{\partial DI}\right]^2 V(DI) \qquad \text{(Eq A-94)}$$

Finally, in a similar manner the variance in F_{11} is computed as:

$$\frac{\partial F_{11}}{\partial x} = 6\mathrm{H}\frac{\partial(\mathrm{H})}{\partial x} + \frac{\partial(\mathrm{Q})}{\partial x} \qquad \text{(Eq A-95)}$$

$$\frac{\partial F_{11}}{\partial DC} = 6\left[\begin{array}{l}\frac{(1-DC)\times(1-\beta)\times\lambda^{D}\times TI}{2}+\\ \frac{DC\times(1-\beta)\times\lambda^{D}\times DI}{2}+(1-\beta)\times\lambda^{D}\times MTTR\end{array}\right]\times \Bigg[$$

$$\frac{-(1-\beta)\times\lambda^{D}\times TI}{2}+\frac{(1-\beta)\times\lambda^{D}\times DI}{2}\Bigg]+$$

$$\frac{(-1)\times\beta\times\lambda^{D}\times TI}{2}+\frac{\beta\times\lambda^{D}\times DI}{2} \qquad \text{(Eq A-96)}$$

$$\frac{\partial F_{11}}{\partial TI} = 6\left[\begin{array}{l}\frac{(1-DC)\times(1-\beta)\times\lambda^{D}\times TI}{2}+\\ \frac{DC\times(1-\beta)\times\lambda^{D}\times DI}{2}+(1-\beta)\times\lambda^{D}\times MTTR\end{array}\right]\times\left[\frac{(1-DC)\times(1-\beta)\times\lambda^{D}}{2}\right]+$$

$$\frac{(1-DC)\times\beta\times\lambda^{D}}{2} \qquad \text{(Eq A-97)}$$

$$\frac{\partial F_{11}}{\partial MTTR} = 6\left[\begin{array}{l}\frac{(1-DC)\times(1-\beta)\times\lambda^{D}\times TI}{2}+\\ \frac{DC\times(1-\beta)\times\lambda^{D}\times DI}{2}+(1-\beta)\times\lambda^{D}\times MTTR\end{array}\right]\times\left[(1-\beta)\times\lambda^{D}\right]+$$

$$\beta\times\lambda^{D}\times MTTR \qquad \text{(Eq A-98)}$$

$$\frac{\partial F_{11}}{\partial \beta} = 6\left[\begin{array}{l}\frac{(1-DC)\times(1-\beta)\times\lambda^{D}\times TI}{2}+\\ \frac{DC\times(1-\beta)\times\lambda^{D}\times DI}{2}+(1-\beta)\times\lambda^{D}\times MTTR\end{array}\right]\times \left[\vphantom{\frac{A}{2}}\right.$$

$$\left[\begin{array}{l}\frac{(1-DC)\times(-1)\times\lambda^{D}\times TI}{2}+\\ \frac{DC\times(-1)\times\lambda^{D}\times DI}{2}+(-1)\times\lambda^{D}\times MTTR\end{array}\right]\Bigg] +$$

$$\left[\frac{(1-DC)\times\lambda^{D}\times TI}{2}+\frac{DC\times\lambda^{D}\times DI}{2}+\lambda^{D}\times MTTR\right] \quad \text{(Eq A-99)}$$

$$\frac{\partial F_{11}}{\partial DI} = 6\left[\begin{array}{l}\frac{(1-DC)\times(1-\beta)\times\lambda^{D}\times TI}{2}+\\ \frac{DC\times(1-\beta)\times\lambda^{D}\times DI}{2}+(1-\beta)\times\lambda^{D}\times MTTR\end{array}\right]\times\left[\frac{DC\times(1-\beta)\times\lambda^{D}}{2}\right]+$$

$$\frac{DC\times\beta\times\lambda^{D}}{2} \quad \text{(Eq A-100)}$$

$$\left[\frac{\partial F_{11}}{\partial \lambda^{D}}\right] = 6\left[\begin{array}{l}\frac{(1-DC)\times(1-\beta)\times\lambda^{D}\times TI}{2}+\\ \frac{DC\times(1-\beta)\times\lambda^{D}\times DI}{2}+(1-\beta)\times\lambda^{D}\times MTTR\end{array}\right]\times$$

$$\left[\begin{array}{l}\frac{(1-DC)\times(1-\beta)\times TI}{2}+\\ \frac{DC\times(1-\beta)\times DI}{2}+(1-\beta)\times MTTR\end{array}\right]+$$

$$\left[\frac{(1-DC)\times\beta\times TI}{2}+\frac{DC\times\beta\times DI}{2}+\beta\times MTTR\right] \quad \text{(Eq A-101)}$$

Using the sensitivities for F_{11} calculated above, the variance in F_{11} due to uncertain or random variables is found as:

$$V(F_{11}) = \left[\frac{\partial F_{11}}{\partial DC}\right]^2 V(DC) + \left[\frac{\partial F_{11}}{\partial TI}\right]^2 V(TI) + \left[\frac{\partial F_{11}}{\partial \lambda^D}\right]^2 V(\lambda^D) +$$

$$\left[\frac{\partial F_{11}}{\partial MTTR}\right]^2 V(MTTR) + \left[\frac{\partial F_{11}}{\partial \beta}\right]^2 V(\beta) + \left[\frac{\partial F_{11}}{\partial DI}\right]^2 V(DI) \qquad \text{(Eq A-102)}$$

PROCEDURE FOR DETERMINATION OF VARIANCE FOR REPAIRABLE 1oo2, 1oo3 AND 2oo3 SYSTEMS

Based on the above derivations we may now write the formulas for the variance of various configurations of repairable equipment.

Step 1. Determine the configuration of equipment to be studied.

Step 2. Evaluate Function H using the expected value of all random or uncertain variables, equation A-51

Step 3. Evaluate Function Q using the expected value of all random or uncertain variables, equation A-52

Step 4. Evaluate the sensitivity of function H with respect to the random variables using equations A-65 thru A-70.

Step 5. Evaluate the sensitivity of function Q with respect to the random variables using equations A-72 thru A-77.

Step 6. Evaluate the variance as:

a. For 1oo2 systems use equation A-86 for $V(F_8)$
b. For 1oo3 systems use equation A-94 for $V(F_9)$
c. For 2oo3 systems use equation A-102 for $V(F_{11})$

The end result of the above calculations is the determination of the mean and variance of the configuration used in the sensor, logic solver or final control element systems. Table A.6 presents a cross reference roadmap for the determination of the mean and variance of various of the probability of failure on demand (PFD) of various hardware configurations. The mean and variance for the particular configuration is then returned to the overall calculations of the PFD of the interlock.