

ANALYSIS OF INDEPENDENT PROTECTION LAYERS AND SAFETY INSTRUMENTED SYSTEM FOR OIL GAS SEPARATOR USING BAYESIAN METHODS

G. Unnikrishnan^{1*}, Shrihari², Nihal A. Siddiqui³

¹Department of Health, Safety & Environment, University Of Petroleum and Energy Studies, Dehradun, India

²Department of Chemical Engineering, University Of Petroleum and Energy Studies, Dehradun, India

³Department of Health, Safety & Environment, University Of Petroleum and Energy Studies, Dehradun, India

*email: ukrishnan77@yahoo.com

ABSTRACT

Process and Nuclear industries use Independent Protection Layers (IPLs) to prevent initiating abnormal events from becoming accidents. They form layers of protection that acts to prevent an abnormal situation from escalating. IPLs can be hardware (Basic Control System-BPCS) or operator actions, active (Safety Instrumented System-SIS) or passive (Dike walls) or a combination of all these factors. Safety Instrumented System (SIS) is the protection layer that comes in to action in case of failure of BPCS and operator action. Therefore reliability and ability of the SIS to respond should be higher than that of the layer like the BPCS. Reliability of SIS is usually specified in terms of Safety Integrity Level (SIL). The required SIL is calculated by analyzing the Probability of Failure of Demand (PFD) of all the IPLs in the case of an Initiating Event (IE) and comparing the Mitigated Consequence Frequency with a pre-established Tolerable Frequency (TF). The calculations involve probability of failure of each of layers and are usually done through spreadsheet or proprietary software. Bayesian methods are suited to handle these calculations due the nature of conditional probabilities inherent in the system. Further Bayesian methods can analyze the influencing factors affecting the PFD of the IPLs. This paper will present analysis of IPLs and its influencing factors using Bayesian methods including application of Common Cause Failures (CCF) and NoisyAnd distribution to Conditional Probability Tables (CPTs).

1. INTRODUCTION

Independent Protection Layers (IPLs) form the safety barriers that prevent Initiating Events (IE) from becoming hazardous consequences (accidents) and are used extensively in Nuclear and Process industries. The concept and methodologies of such layers are described in Center for Chemical Process Safety's (CCPS) book Layers Of Protection Analysis (2001) [1]. Layers Of Protection Analysis (LOPA) is a formalized procedure used to assign Safety Integrity Levels (SIL) to the Safety Instrumentation Systems (SIS) in accordance with the International Electro-technical Commission's standard (IEC) 61511 meant for process industries. SIL levels involve calculation of the Mitigated Consequence frequency using the Probability of Failure on Demand (PFDs) of each of the IPLs and comparing the value with Tolerable Frequency for the events. If the calculated Mitigated Consequence frequency is higher than the Tolerable Frequency, the reliability of the SIS layer has to be increased. The calculations are usually implemented through spreadsheet or proprietary software. Due it probabilistic nature such calculations can be easily done through Bayesian Networks (BN). BN models can offer easy inclusion of several influencing factors that affect the IPLs PFDs. Common Cause Failure (CCF) and other uncertainties or noise in the system can also be modelled with BN. This paper will describe the usage of BNs to model the IPLs including CCF and other uncertainties in the system through NoisyAnd distribution.

2. LAYERS OF PROTECTION.

Figure 1 illustrates the concept of successive layers that protect personnel, environment and assets from the harmful consequences of a loss of containment in a process system. The failures of protection layers are considered in series. Except for the Design & BPCS rest of the protection layers act only on demand. (Demand mode operation).

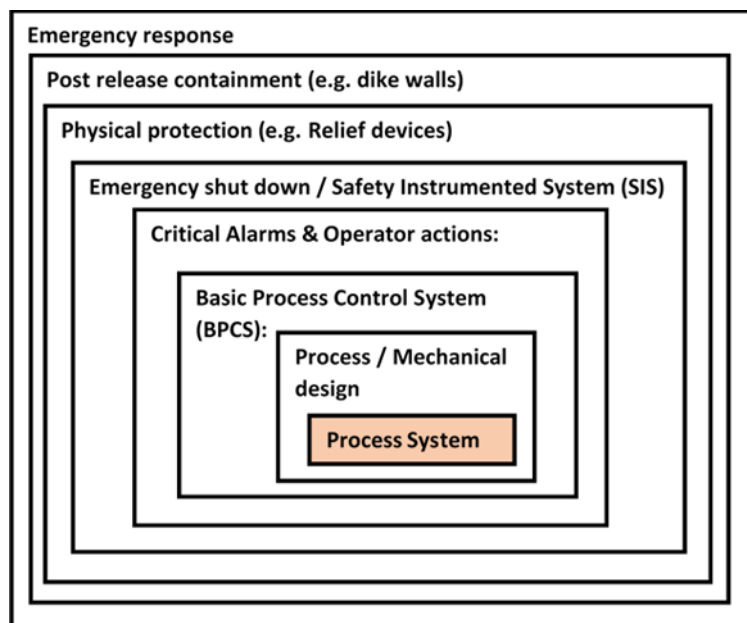


Figure 1: Layers Of Protection for a Process System

3. CALCULATIONS FOR DETERMINING SAFETY INTEGRITY LEVEL (SIL)

Calculations to determine SIL for the Safety Instrumented System (SIS) involve the following steps.

Step 1: Each of the layers of protection has a PFD associated with it. The sequential failure of the IPLs can be readily put in the equation 1 below:

$$PFD_{IPLs} = \prod_{n=1}^N PFD_n \quad (1)$$

N is the total number of IPLs.

In calculations for SIL, the PFD of SIS layer is set to 1; that is no credit is taken for the SIS already provided

Step 2: If the probability of Initiating Event is IE, then the probability of Mitigated Consequence is given by

$$\text{Mitigated Consequence} = IE * \prod_{n=1}^N PFD_n \quad (2)$$

Sometimes the probability of Initiating Events are modified by enabling conditions (EC) (for example presence of operators) and conditional modifiers (CM) (example: probability of gas cloud ignition) and the same can be included in the above equation 2 to give equation 3.. Center for Chemical Process Safety's (CCPS) Criteria for evaluating Enabling Conditions and Conditional Modifiers in Layers Of Protection Analysis (2014) [2] gives details on the above.

$$\text{Mitigated Consequence} = IE * EC * CM * \prod_{n=1}^N PFD_n \tag{3}$$

Step 3: This step is the comparison with established Tolerable Frequencies. (TF). Table 1 below shows the commonly used values for TFs. These values could vary depending upon the country and nature of loss. Some companies use more categories and tolerable frequencies. Lewis (2007) [3] summarizes the subject.

Category	Tolerable Frequency (TF)
Multiple Personnel fatality	$1 * 10^{-6}$
Environment	$1 * 10^{-4}$
Property (Assets)	$1 * 10^{-4}$

Table 1: Category of Consequences & Tolerable Frequencies

The required PFD of the SIS is obtained by dividing the TF by the total PFDs of IPLs (excluding SIS) and is given by the following equation.

$$PFD \text{ required for SIS} = \frac{TF}{\text{Mitigated Consequence}} \tag{4}$$

Equation 4 is repeated for each category of loss and corresponding Tolerable Frequency in Table 1 and the highest value of SIL obtained is taken for implementing the SIS.

Step 5: The PFD required for SIS is categorized as per IEC 61511 shown on Table 2.

Range of failures. Average Probability of Failure on Demand	Risk Reduction Factor	Category of Safety Integrity Level SIL
$\geq 1 * 10^{-5}$ to $< 1 * 10^{-4}$	$>10,000$ to $\leq 100,000$	SIL 4 ^{**}
$\geq 1 * 10^{-4}$ to $< 1 * 10^{-3}$	>1000 to $\leq 10,000$	SIL3
$\geq 1 * 10^{-3}$ to $< 1 * 10^{-2}$	>100 to ≤ 1000	SIL2
$\geq 1 * 10^{-2}$ to $< 1 * 10^{-1}$	>10 to ≤ 100	SIL1
$\geq 1 * 10^{-1}$ to $< 1 * 10^1$	>10	SILa [*]

** SIL4 is not normally used in Process industries

*SILa denotes that there is no need to assign a SIL level to the SIS under consideration.

Table 2: Range of Average Probability of Failures on Demand & Safety Integrity Levels.

4. APPLICATION TO IPLS OF OIL AND GAS SEPARATOR

The calculations described under 3 are illustrated for a typical industrial Oil and Gas Production separator shown in Figure 2.

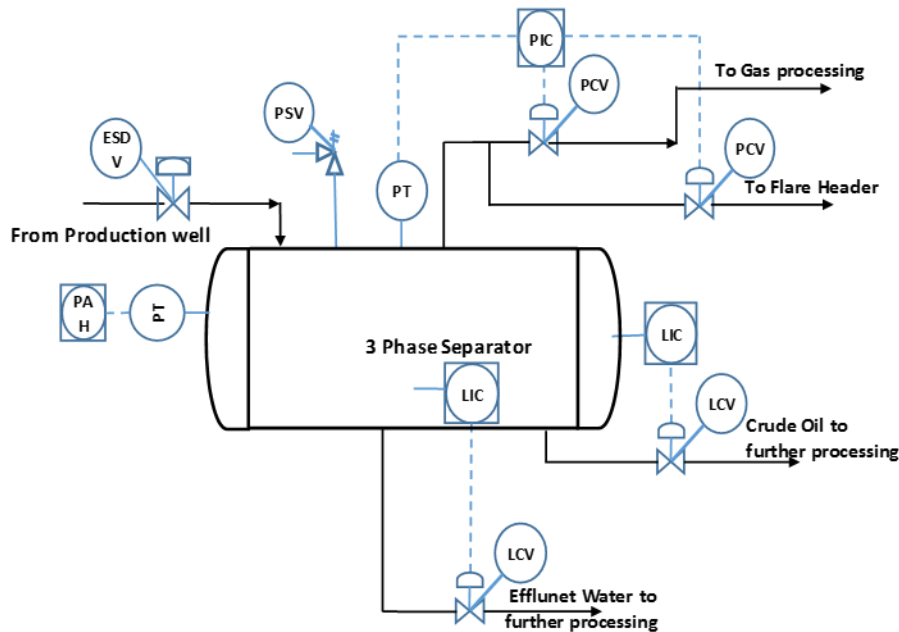


Figure 2: Typical Oil & Gas separator showing the Independent Protection Layers

The Initiating Events for an overpressure scenario in the separator are:

- Pressure surge from upstream well which suddenly raises the pressure inside the Separator vessel. Frequency 0.1 per year.
- Fail to open situation for the Pressure Safety Valve (PSV). PFD =0.000212 (Based on CCPS & HSE UK database)

The hazardous consequences are vessel failure, loss of containment, fire and explosion which are of highest severity.

The IPLs are:

IPL1: Adequate process and mechanical design of the separator vessel is the first layer of protection, which is not usually considered in SIL calculations (PFD=1.0)

IPL2: Basic Process Control Systems-here there are two, the Pressure Control Valve PCV for controlling the vessel pressure (BPCS1) and the other PCV for letting the gas out to the flare in case the pressure goes up beyond the set point (BPCS2). They are not independent and therefore PFD of both the control systems together are taken as 0.10.

IPL3: The SIS forms the next IPL; namely the Emergency Shutdown Valve (ESDV) that comes into action independently once the BPCS and Operator action has failed. PFD is taken as 0.0008 from CCPS & HSE UK database. SIL calculations are done without considering this. PFD is set to 1.

The (PAH) alarm coming from the control system is meant to initiate Operator action to control the sudden rise in pressure. However Operator action is not considered as an IPL in this paper. Depending on company's policies this IPL may be included in SIL calculations.

With Initiating Event frequency of 0.1 per year and Enabling Event probability of 0.1, calculation for the SIS is put in a spread sheet given below in Figure 3:

Tolerable Risk	1E-06
----------------	-------

Initiating event description	Initiating Event Frequency / Year	Enabling Event Probability	Probability of Conditional modifiers	INDEPENDANT PROTECTION LAYERS						Mitigated Consequence Frequency without SIS
				IPL1 Process / Mechanical Design	IPL2 BPCS1	IPL3 Operator Response to Alarm-NotConsidered	IPL4 Independent SIF	IPL5 F & G Detection	IPL6 Others-None	
U/S OR D/S DISTURBANCE	1.00E-01	0.1	1.0	1.0	0.1	1.0	1.0	1.0	1.0	1.00E-03
Pressure Safety Valve	2.12E-04									2.12E-04
TOTAL CAUSE FREQUENCY	1.00E-01						F (event - without SIS)		TOTAL	1.21E-03

PFD Required For SIS	8.25E-04
Risk Reduction Factor	1212
Required SIL for SIS	3

Figure 3: Spreadsheet calculations for determining the Safety Integrity Level of the ESDV

In this case the Mitigated Consequence frequency is 1.00 E-03, whereas, based on the severity, the TF of consequences is placed at 1.00 E-06, (see Table 1) which is lower. Therefore the SIL level of the SIS is arrived by substituting the above values in to equation 4.

$$PFD \text{ required for SIS} = \frac{1 * E - 06}{1 * E - 03} = 1 * E - 03$$

The above value is in category of SIL3 (See Table 2) and thus the SIS has to designed with SIL3 reliability.

5. BAYESIAN NETWORKS

A detailed description of Bayesian Network (BN) is not attempted in the paper. Interested readers can go through any of the several books on the subject e.g. Pourret et al (2008) [4], Kjærulf et al (2005) [5], Neapolitan (2003) [6]. Briefly BN is a directed acyclic graph (DAG) in which the nodes represent the system variables and the arcs symbolize the dependencies or the cause–effect relationships among the variables. A BN is defined by a set of nodes and a set of directed arcs. Probabilities are associated with each state of the node. The probability is defined, a priori for a root (parent) node and computed in the BN by inference for the others (child nodes). Each child node has an associated probability table called Conditional Probability Table (CPT).

The computation of the net is based on the Bayes Theorem which states that if P (B) is probability of B happening, then P (A/B) is probability of A happening given that B has happened, given P (B) not equal to zero

Following gives the most common form of Bayes equation

$$P(A|B) = \frac{P(B|A)*P(A)}{P(B)} \tag{5}$$

$$\text{Where } P(B) = P(B|A) * P(A) + P(B|A') * P(A') \tag{6}$$

A' stands for A not happening

The equation 5, right hand side represents the prior situation –which when computed gives the left hand side –called posterior values. The value P (A) is the prior probability and P (B | A) is the likelihood function –which is data specific to the situation. P (B) is the probability of B- which is calculated from equation 6.

6. USING BAYESIAN NET (BN) FOR SIS CALCULATIONS

6.1 Kannan [7] used BN to calculate the PFD of the IPLs specifically for a separator using BN. He described the failure IPLs consisting of Level Control Valve and 2 Emergency Shutdown Valves (ESDVs) in series including the components; Level Transmitter (LT) and Programmable Logic Controller (PLC). Common cause failure due to cold weather of the LT was illustrated in the paper. SIL calculations were not given.

The spreadsheet calculations given in Figure 3 are mapped to BN using Netica software. See Figure 4.

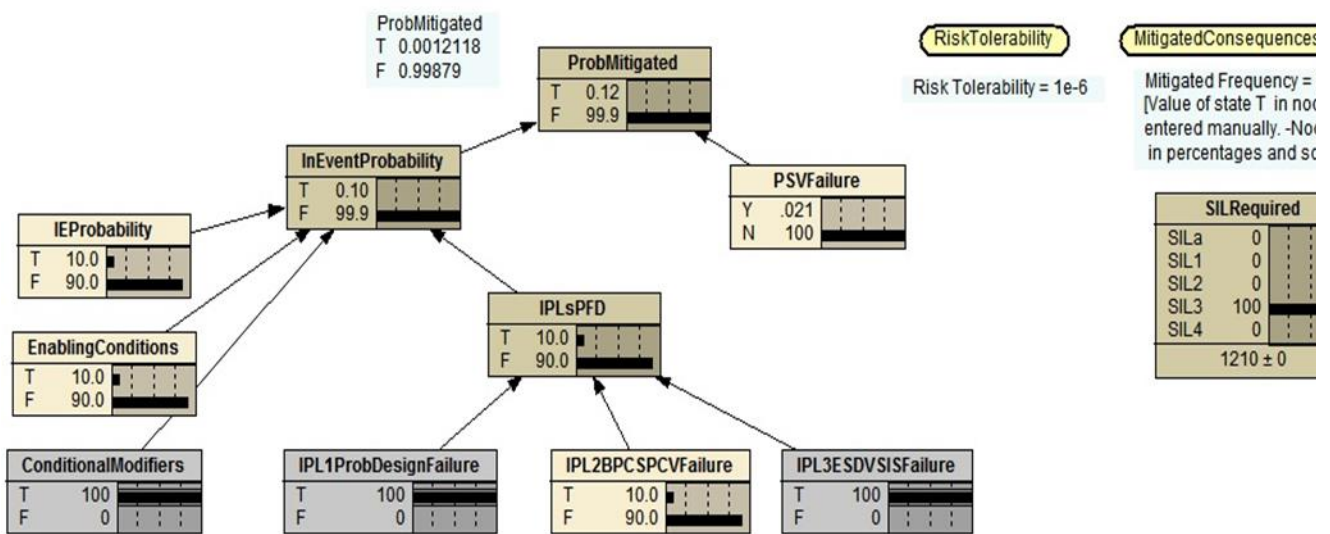


Figure 4: Bayesian Network for IPLs for Oil & Gas Separator

Note: Netica nodes do not display decimals beyond 4 digits. Higher decimals are obtained through the Report feature in the Menu and added in the Figure.

The BN in Figure 4 is equivalent to the spreadsheet including the SIL calculations.

Initiating Events are InEventProbability from upstream disturbance and PSV failure. InEventProbability is the child node of IEProbability, EnablingConditions and ConditionalModifiers nodes. IPLsPFD is the child node for the parents of IPL1 to IPL3 nodes. The nodes are parameterized with the probability values used in the spreadsheet. The PFD calculation in the node IPLsPFD is implemented using the AND Gate feature in Netica. No credit is taken for the SIS layer (PFD =1).

Once the probability for consequences is calculated by the BN (value of state T in node ProbMitigated), the value is input manually into the constant node named MitigatedConsequences. The SIL is calculated and presented in the node SILRequired. The values in Netica nodes are in percentage probability and so when entering the value manually the same has to be divided by 100 to match with the probability values in which the Risk Tolerability is expressed. This BN represents a general structure of network for any IPLs with a SIS.

The probability values of any of the nodes can be changed and the resultant change in the Mitigated Consequence node can be seen easily, including backward propagation of probabilities when a child node is changed.

6.2 Adding Influencing Factors

Unlike that in spreadsheet calculations, influencing factors that affect the BN can be easily added to the BN. For example testing affects the PFD of PSV. Adding of the influencing factor of PSV testing for the node PSVFailure is given in Figure 5. The states are OnSchedule and NotOnSchedule. The input probabilities for this node are the initial or prior states, which can be updated based on actual data. For BN in Figure 5, the PSV failure data given earlier (PFD = 0.00021) is assumed to be when the testing is as per schedule. When testing is not as per schedule the PFD is taken as 0.0007. These values are entered in CPT for node PSVFailure.

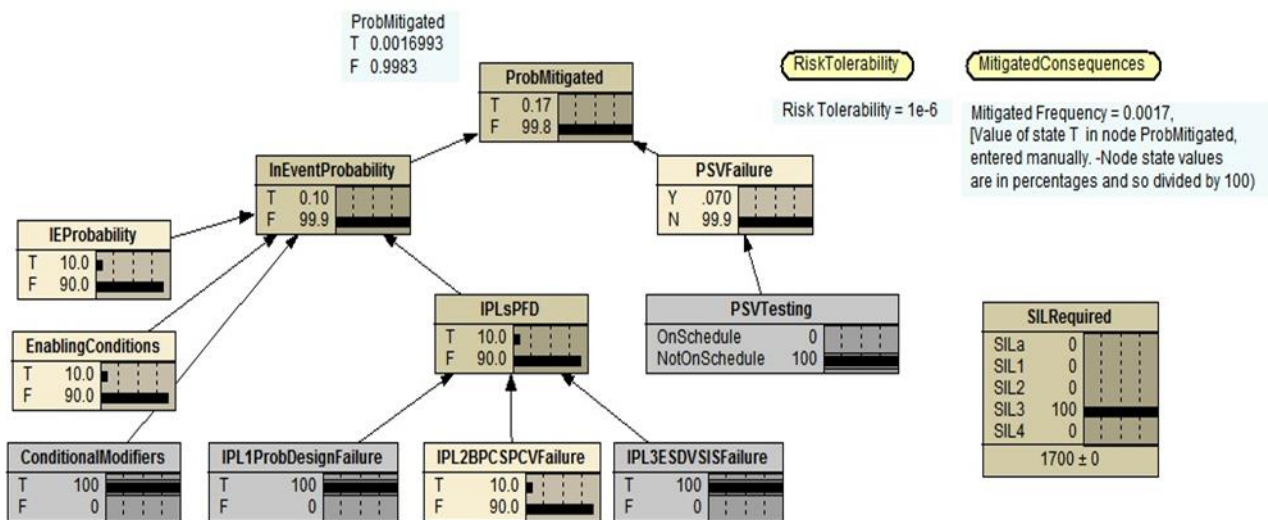


Figure 5: BN for IPLs with addition of influencing factor for PSV failure.

6.2.1 Changing influencing factors

The influencing factors can be changed based on actual situation. For example, if the PSV testing is not as per schedule the state in NotOnSchedule can be set 100, to see the effect of the same on other nodes. See Figure 5. The PFD for the PSV goes up to 0.0007 and the probability of Mitigated Consequence goes up to 0.0017 from 0.0010. Though the SIL rating is not affected in this case, visualizing such influencing factors gives better insight into the state of the IPLs.

6.3 Common Cause Failures (CCF)

CCFs can be implemented quite easily in BN. See the Figure 6, where a CCF for the Control Valve & ESDV failure has been added to the BN. The CCF is based on a scenario of fire. If there is fire, there is a probability that the instrument air piping and cables could be damaged rendering both the valves ineffective. In the node for Fire, probability of Fire is entered as 0.02 & in CCF node CPT, the probability of CCF being true when there is fire is entered as 0.80. It be seen that there is slight increase in the PFD for BPCS (goes up to 0.105 from 0.10) resulting in an increase of Mitigated Consequence to 0.0013 from 0.0012.

Though the change in the probability is very minor, it may impact the SIL level sometimes.

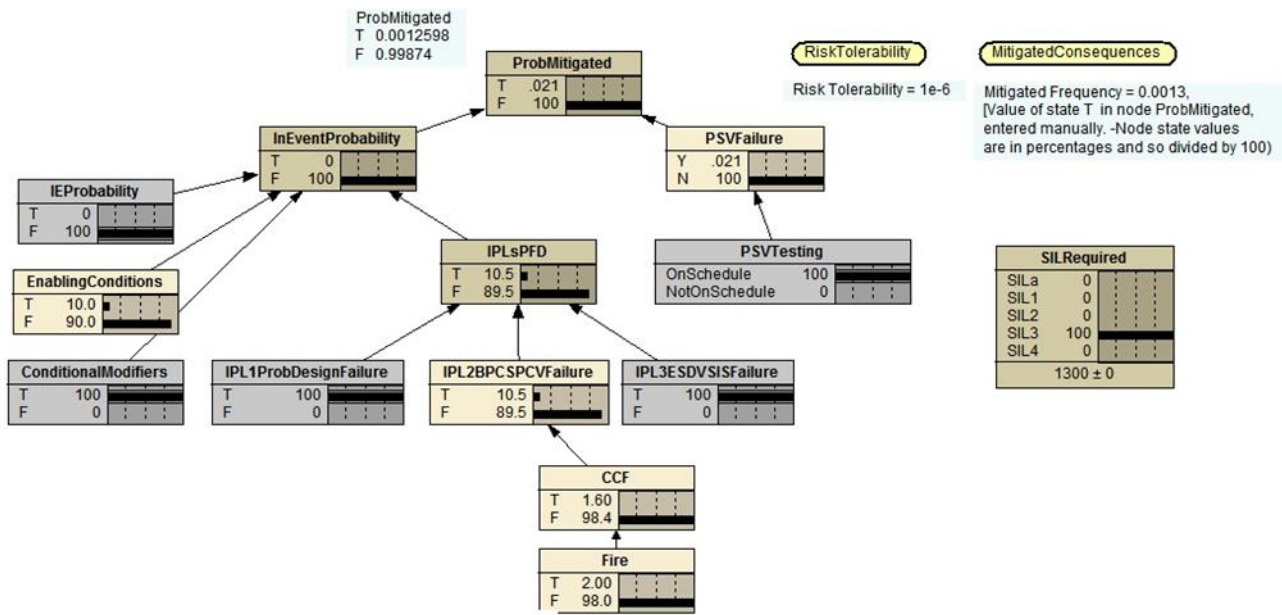


Figure 6: BN showing addition of Common Cause Failure of control valves due to fire

6.4 Noisy-And Distribution

Netica has a facility to use Noisy-OR or Noisy-And distribution. This can be used to model the PFD of failure of IPLs more realistically. Noisy-(logical) distribution essentially represents the noise in the system, which cannot be adequately modelled since in reality all causes to an event or consequence cannot be identified. Further if there are many causes (parent nodes), the entries in the CPT rises exponentially.

Noisy-OR distribution can be used when there are several possible causes for an event, any of which can cause the event by itself, but only with a certain probability. Also, the event can occur spontaneously (without any of the known causes being true), which can be modelled with probability 'leak'. (This can be zero if it cannot occur spontaneously).

Noisy-And distribution is used when there are several possible requirements for an event, and each of which has a probability that will actually be necessary. Each of the necessary requirements must pass for the event to occur. Noisy-And can also model a situation where the event may not occur even when all requirements are passed.

In the case of IPLs for Oil & Gas separator, Noisy-And distribution is appropriate since all the IPLs have to fail necessarily for event to occur.

The equation for NoisyAnd is written in Netica as

$$P(IPLsPFD | IPL1ProbDesignFailure, IPL2BPCSPCVFailure, IPL3ESDVSISFailure) = \text{NoisyAndDist}(IPLsPFD, 0.0, IPL1ProbDesignFailure, 0.6, IPL2BPCSPCVFailure, 0.6, IPL3ESDVSISFailure, 0.6)$$

(7)

The probability values in equation 7 are assumed values and are not based on actual data. No probability leak is assumed; that is, for combined IPLs given by node IPLsPFD, the condition T=100 is possible only when all IPLs have failed.

Netica Help file at Norsys [8] provides further details of the syntax for the above distribution.

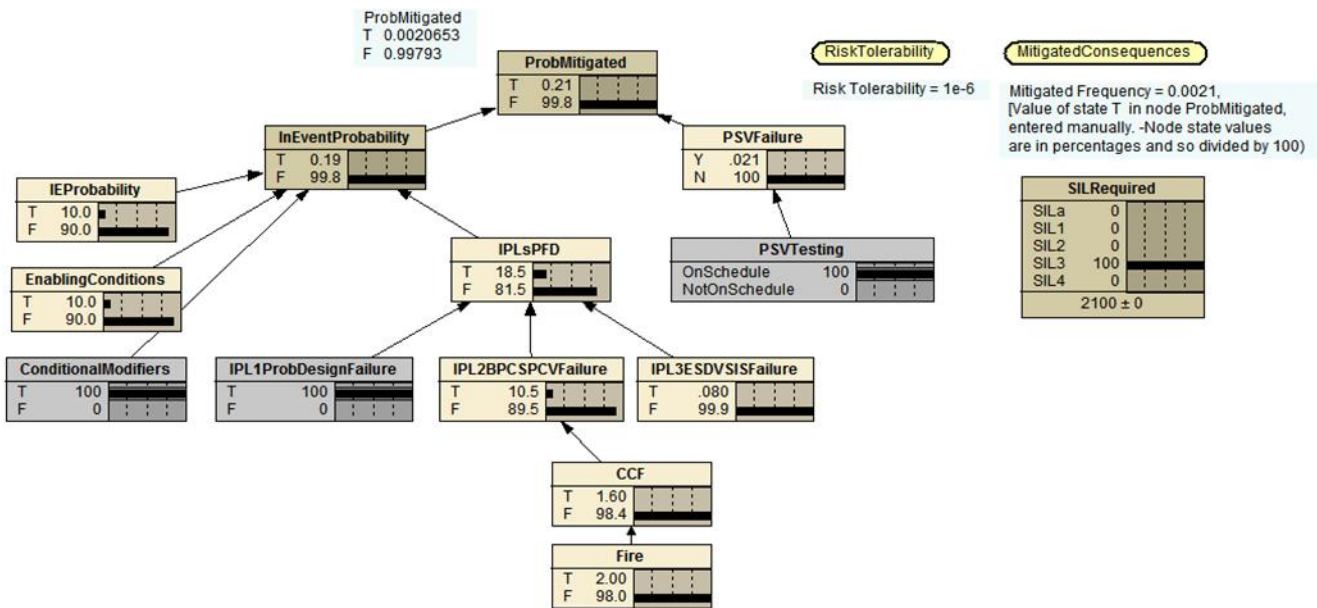


Figure 7: BN showing failure probabilities with NoisyAnd distribution

The equation populates CPT table for IPLsPFD with values based on the equation as given Table 3. The compiled BN given in Figure 7 shows that there is a small increase in the overall probability of Mitigated Consequence to 0.0021. Thus the NoisyAnd distribution offers a method to input probabilistic values to the IPLsPFD node instead of the AND feature that computes the CPT based on T & F only as used in BN shown in Figure 4.

T	F	IPL1ProbDesignFailure	IPL2BPCSPCVFailure	PL3ESDVSISFailure
1	0	T	T	T
0.4	0.6	T	T	F
0.4	0.6	T	F	T
0.16	0.84	T	F	F
0.4	0.6	F	T	T
0.16	0.84	F	T	F
0.16	0.84	F	F	T
0.064	0.936	F	F	F

Table 3: Probability values in Conditional Probability Table populated by NoisyAnd distribution

7. DISCUSSION

BN can model the IPLs, its influencing factors and failure rates in a visually easy and understandable way. SIL calculations can be implemented as a part of BN. Influencing factors and CCFs can be added to any node and its impact other nodes can be studied in detail. The ability to include probabilistic Noisy-And distribution to populate the CPTs increases the power of and applicability of the BN. Fine tuning the Noisy-And distribution based on site specific data is a challenge, and more work need to be done in this area. Application of Bayesian Methods to analysis of IPLs and SIL calculations will help improve the predictive & diagnostic power of the model.

REFERENCES

- [1] Center for Chemical Process Safety., “Layers of Protection Analysis, AIChE, New York. (2001)
- [2] Center for Chemical Process Safety., “Criteria for evaluating Enabling Conditions and Conditional Modifiers in Layers Of Protection Analysis, AIChE, New York. (2014).
- [3] Lewis, Steve., “Risk Criteria –When is low enough good enough?”, Risktec Solutions Limited, <http://www.risktec.co.uk/media/43520/risk> criteria when low enough good enough, (2007)
- [4] Pourret, Olivier., Naim, Patrick., Marcot, Bruce., Editors., “Bayesian Networks: A Practical Guide to Applications”, Wiley. (2008)
- [5] Kjærulf, U.B., and Anders M. L., “Probabilistic Networks -An Introduction to Bayesian Networks and Influence Diagrams, Springer. (2005)
- [6] Neapolitan, R.E., “Learning Bayesian Networks”, Prentice Hall. (2003)
- [7] Kannan, P. R., “Bayesian networks: Application in Safety instrumentation and risk reduction”, ISA Transactions, 46, pp 255-259 (2001).
- [8] Norsys Software Corporation, Netica, [www. norsys.com](http://www.norsys.com) (2015).