LOPA

1. Safety related system consists of:

Mechanical protection system

Passive protection system

Basic process control system

Alarms

Safety instrumented system (SIS)

1. The function of SIS is called SIF. More than one SIF could be allocated to a SIS.
2. A SIS consists of a sensor, logic solver and final element.
3. The ability of a SIS is to carry out the actions necessary to achieve a safe state in process.
4. IEC-60508 for general industry and IEC-60511 for oil and gas industry.
5. Important to notice table below.



1. A Risk is the amount of harm that can be expected to occur during a given time period due to specific harm event.

Risk = Frequency times Severity

Remember prevention and mitigation.

1. Safety Integrated Level or SIL is allocated to SIF not SIL. SIL is a measurement of performance required for a Safety Instrumented Function (SIF).
2. Calculate the risk and then divide it by 10^-5 or 10^-6 to achieve Risk Reduction Factor or RRF.
3. Failure Rate or λ is defined by (no. of faults)/(total working time of all items). In calculation we use OREDA handbook for generic date of mean λ. We suppose just constant failure rate.

11. Pavg equals to λ times TI divided by 2 if λ.TI<<1. It is assumed that after each time interval the equipment is as new as first day. Time interval is really important when regarding sil target.

12. LOPA stages:

A. Estimate consequence and its severity

B. Create a scenario by putting together a cause and a consequence.

C. Determine initial frequency based on table bellow:





D. Identifying related IPL and calculate PFD for each IPL



E. Calculate scenario frequency based on following formula:

 10^-5 = fi x PFD1 x PFD2 x …. x P1 x P2 x …

F. Determine the SIL

HAZOP EXAMPLE 1

**HAZOP Example 1**

|  |
| --- |
| Node: Crude Fired Furnace H-1001 |
| **Deviation** | **Cause** | **Consequence** | **Safeguard** | **Recommendation** |
| No/Less flow of crude | 1. No level in storage tank | 1. Damage pump due to dry run |  | 1. Install LSLL on crude storage tank to trip crude pumps. |
| 2. Damage to heater coils due to over-temperature | 1. FSLL that will shut-off furnace burners |
| 2. Pump failure or trip | 1. Damage to heater coils due to over-temperature | 1. FSLL that will shut-off furnace burners2. Standby pump |  |
| 3. Control valve (FV-2311) close more due to any failure in its control loop |  |  |  |
| 4. Plugging of line |  |  |  |

**HAZOP Example 2**

|  |
| --- |
| Node: Hexane Surge Tank |
| **Deviation** | **Cause** | **Consequence** | **Safeguard** | **Recommendation** |
| High Level | 1. Pump failure or trip | 1. Overfilling of tank and overflow from vent that may lead to fire and fatality2. No flow to next process | 1. Control loop will close LV-902. LAH-903. LSHH-10 will close SDV4. Dike*5. Vibration switch on pump* |  |
| 2. LV-90 open more due to any failure in its control loop | 1. Overfilling of tank and overflow from vent that may lead to fire and fatality | 1. LAH-90 (dependent)2. LSHH-10 will close SDV3. Dike |  |

Worst Probable scenario

S1 = pump failure + Overfilling…fatality

~~S2 = pump failure + no flow to next process~~

S3 = LV-90 open + overfilling…fatality

**LOPA Calculations for Scenario: S1**

Step 1: Consequence and severity

Consequence: Overfilling of tank and overflow from vent that may lead to fire and fatality

Severity:

based on approach 1: Category 4 >>>> fc = 10-5 /year

based on approach 2: single fatality >>>> fc = 10-5 /year

based on approach 3: (conditional modifiers/enabling conditions)

single fatality >>>> fc = 10-5 /year

condition 1: ignition probability P1 = 5%

condition 2: exposure probability P2 = 50%

condition 3: fatal injury due to exposure (based on probit) P3 = 50%

Step 2: Scenario = 1 cause + 1 consequence

**S1 = pump failure + Overfilling…fatality**

**condition 1: ignition probability P1 = 5%**

**condition 2: exposure probability P2 = 50%**

**condition 3: fatal injury due to exposure (based on probit) P3 = 50%**

Step 3: initial event frequency

Pump failure >>>> fi = 1/year

Step 4: IPL (independent protection layer)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Safeguard | Independent | Specific | Effective | Auditable | IPL | PFD |
| LIC-90 | √ | √ | √ | √ | **√** | **0.1** |
| LAH-90 + Operator | × | √ | × | × | **×** | **-** |
| Dike | √ | √ | √ | √ | **√** | **0.01** |

RRF >= 10 , PFD <=0.1

Step 5: Calculate scenario frequency

fc = fi x PFD1 x PFD2 x …. x P1 x P2 x …

10-5 = 1 x 0.1 x *x* x 0.01 x 0.05 x 0.5 x 0.5

PFD(SIF) = 0.8

Step 6: Making decision

PFD=0.04 >>>> SIL(SIF) = SIL1

**LOPA Calculations for Scenario: S3**

**Step 1: Consequence and severity**

Consequence: Overfilling of tank and overflow from vent that may lead to fire and fatality

Severity:

based on approach 2: single fatality >>>> fc = 10-5 /year

**Step 2: Scenario = 1 cause + 1 consequence**

S3 = LV-90 open + overfilling…fatality

**Step 3: initial event frequency**

Control loop failure >>>> fi = 0.1/year

**Step 4: IPL (independent protection layer)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Safeguard | Independent | Specific | Effective | Auditable | IPL | PFD |
| LAH-90 + Operator | × | √ | × | × | **×** | **-** |
| Dike | √ | √ | √ | √ | **√** | **0.01** |

**Step 5: Calculate scenario frequency**

fc = fi x PFD1 x PFD2

10-5 = 0.1 x 0.01 x *x*

PFD(SIF) = 0.01

**Step 6: Making decision**

PFD=0.01 >>>> SIL(SIF) = SIL1

If 0.1=<PFD<1 SILa : no special safety requirement

If 1=<PFD non-SIL : no safety requirement

13. Risk matrix



At first we estimate the probability for instance for BPCS is medium and then we estimate severity for this example it is high then SIL 3 is selected and since we have dike in the example as other protection system and it has 2 credits in depth, it then becomes SIL1.



14. Graph matrix

15. In order to verify the selected SIL in a loop, 3 components should be taken into account.

A. SIL capability stated in the certificate

B. Calculate PFD for each and then sum them and find the corresponding SIL

C. Check architectural constrains by checking first rout:



HFT (Hardware Fault Tolerance): maximum number of failures that can be tolerated in a SIS component

HFT for the following systm:

1001#0

1002#1

1003#2

2002#0

2003#1

2004#2

SFF (Safe Failure Fraction): fraction of safe failures

SFF = (Ysd + Ysu + Ydd)/ (Ysd + Ysu + Ydd+ Ydu)