Safety of Nuclear Power Plants
Tutorial - FTA/DF/HRA
Date: May 15th, 2012 (Solution)

System Description:

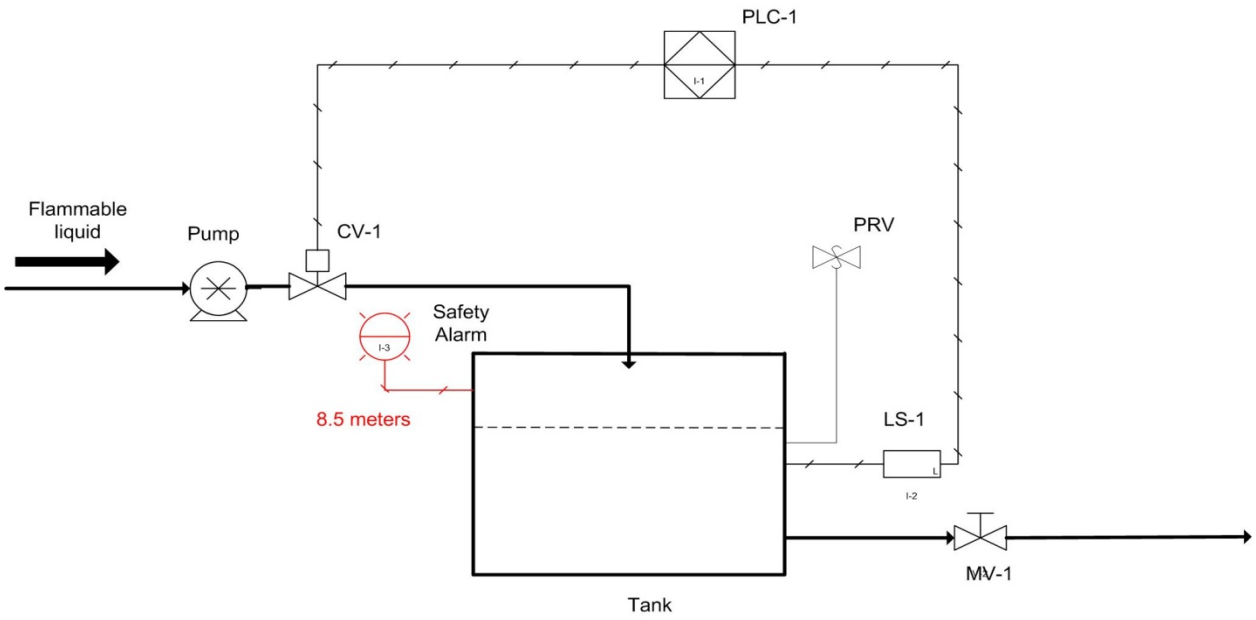


Figure 1. Tank system diagram

The flammable liquid is drawn from a process source and pumped into a sealed tank. The height of tank is 10 meters. A typical level control system including a level sensor (LS-1), a control valve (CV-1) and a programmable logic controller (PLC-1) is installed to maintain the tank level below 8 meters. One manual valve (MV-1) is also installed to enable to liquid out of the tank to other equipment. In the normal operation situation, this valve is 30 percent open. The tank is contained in an environment with the possibility of sparks such as an electricity spark. The site engineer worries that if the tank becomes full, it will rupture and become a potential explosion hazard. For this reason, a pressure relief valve (PRV-1) is installed to relieve the liquid pressure. An alarm system is also installed for the safety reason. If the level control system fails and the level of liquid in the tank reach to 8.5 meters, then the alarm will be triggered to notify the operator. The operator can fully open the manual valve (MV-1) and manually release the liquid from the tank. The operator can also close the pump to stop the liquid going into the tank. Assume this operator has only about 10 minutes to response the alarm. In this case, you can ignore the possibility of the break of the tank.

Below is the reliability data table he can use for the analysis. It is assumed that power supply for all the components always work.

Component	Failure mode	Failure probability
Level sensor LS-1	Fail to operate	1E-6
Control valve CV-1	Fail to operate	4E-5
Programmable logic controller PLC-1	Fail to operate	3E-5
Pump P	Fail to run	3E-5
Pressure relief valve PRV-1	Fail to open	1E-5
Manual valve MV-1	Failure to remain open	4E-6
Safety alarm	Fail to run	2E-4

(All the data in this table are referred from the book " Loss Prevention in the Process Industries " by Frank P. Lees (1986))

Task 1: Your task is to help the site engineer to analyze the probability of the explosion hazard using the approach of FTA. The probability of the hazardous event "ignitable source sparks" is assumed to be 0.05. In this task, you can assume that all the failures of corresponding components are independent and failures of the pump P and manual valve MV-1 can be ignored. Human operator failure can also be ignored

Hint: During two cases, there will be the possibility of the explosion. First, the tank become full and then rupture. Secondly, the pressure relief valve fails and pressure in the tank is too high.

Task 2: In order to decrease the possibility of the explosion hazard, the site engineer decides to add a redundant pressure relief valve (PRV-2), which is exactly as same as the PRV-1. Your task is to help the site engineer to modify the fault tree. In this task, dependent failures of pressure relief valves need to be considered. Human operator failure can be ignored

Hint: You can use β factor model to handle DF issue.

Task 3: The site engineer decides to include the human operator into the current fault tree. Your task is to help the site engineer to perform human reliability analysis and calculate the failure probability of the human operator. Furthermore, you need to modify the fault tree. In this task, you can assume that the probability of failing to open the manual valve by the human operator is 0.05.

Hint: You can use the approach THERP to calculate the failure probability of the human operator.

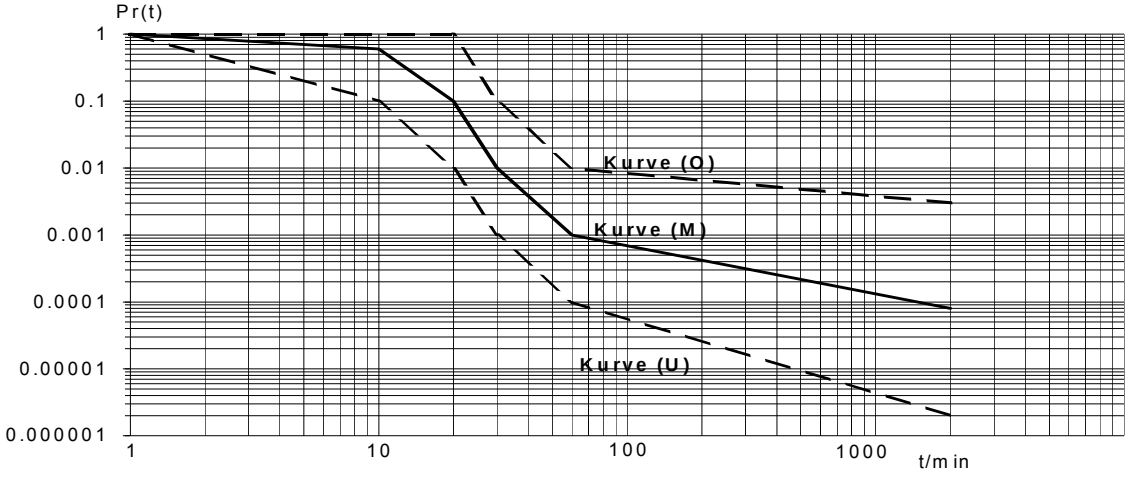
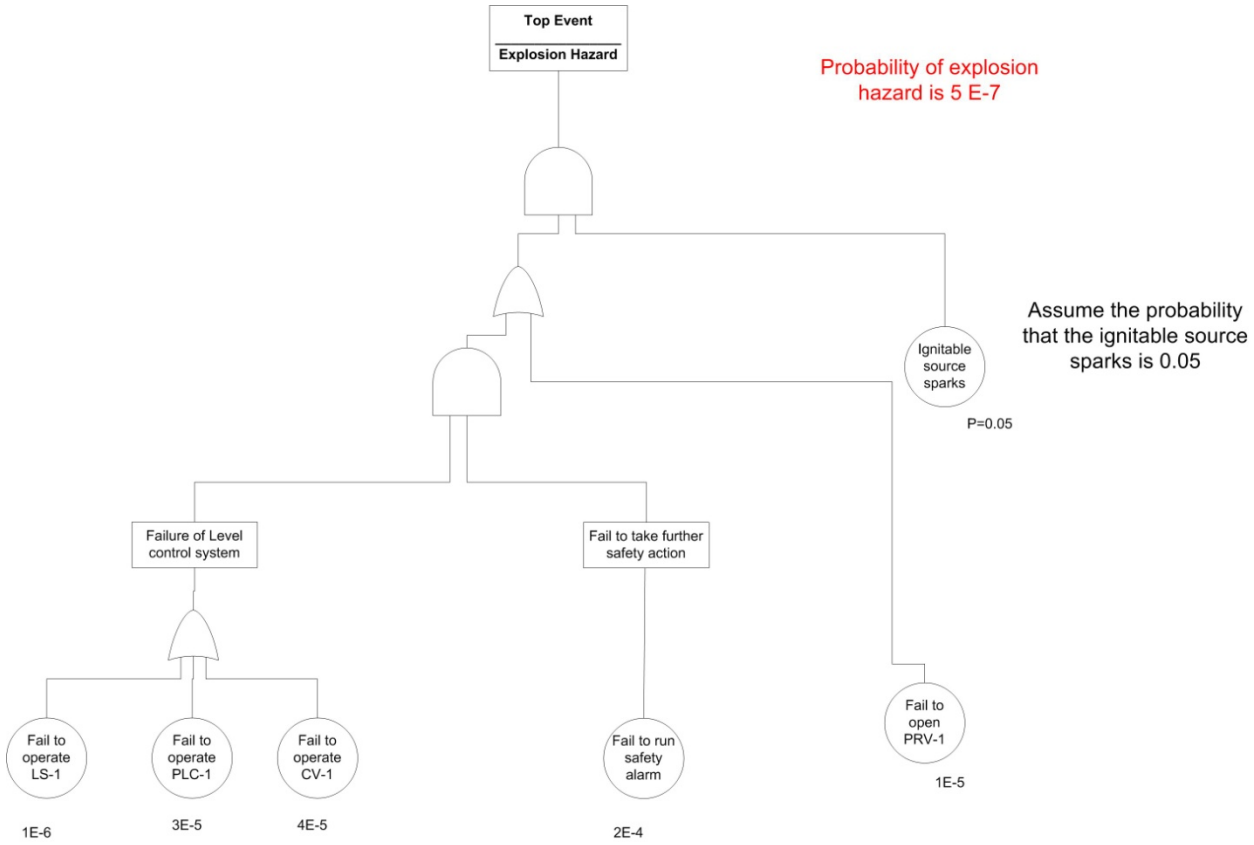


Figure 1

Task 1: The developed FTA

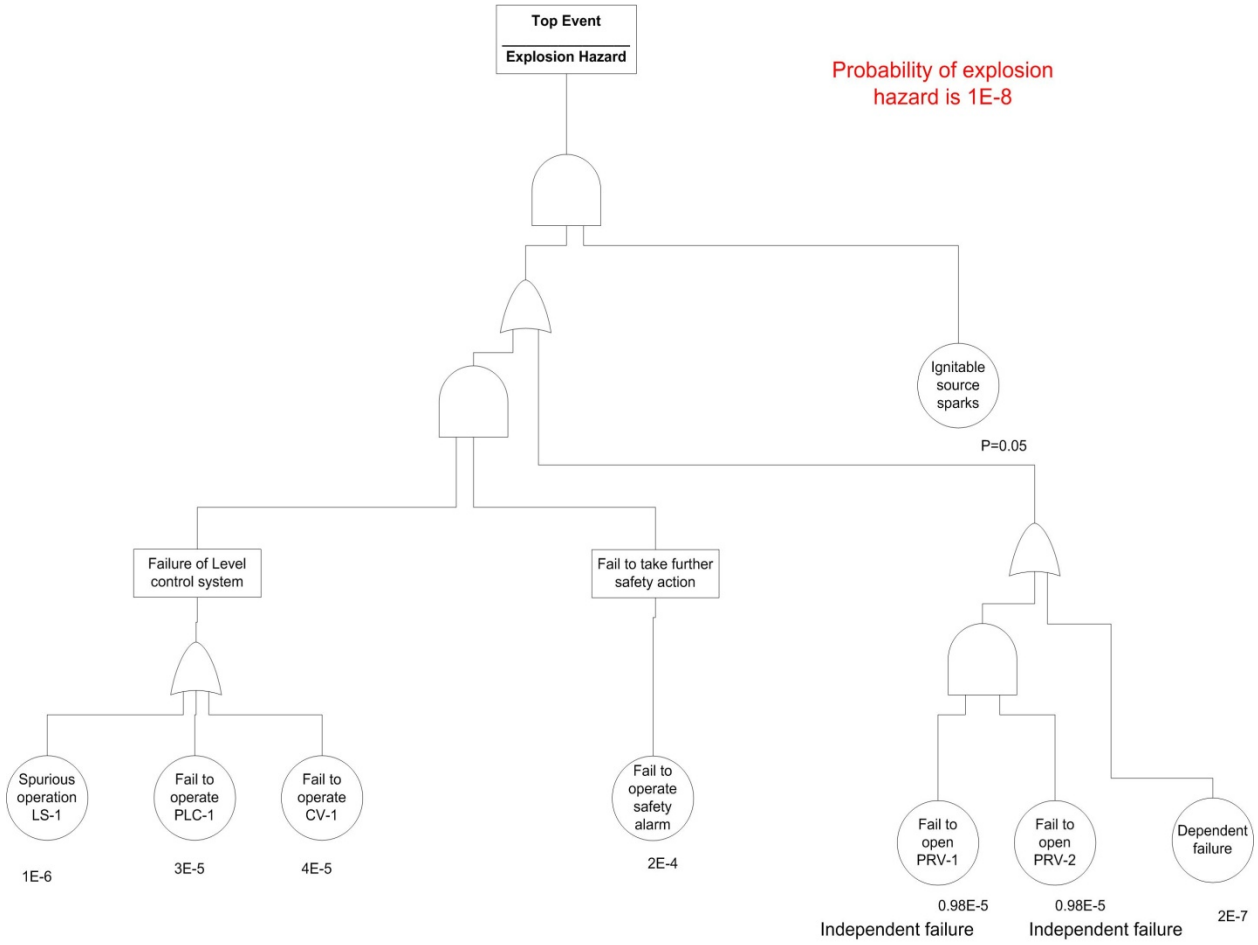


Task 2 :

// Redundant components and dependent failures

In order to decrease the possibility of the explosion hazard, the site engineer decides to add redundant components pressure relief valve (PRV-2). **If redundant component is introduced in the system, then dependent failures need to be considered**. In this case, Fault tree analysis is not enough. We can use β factor more to calculate it.

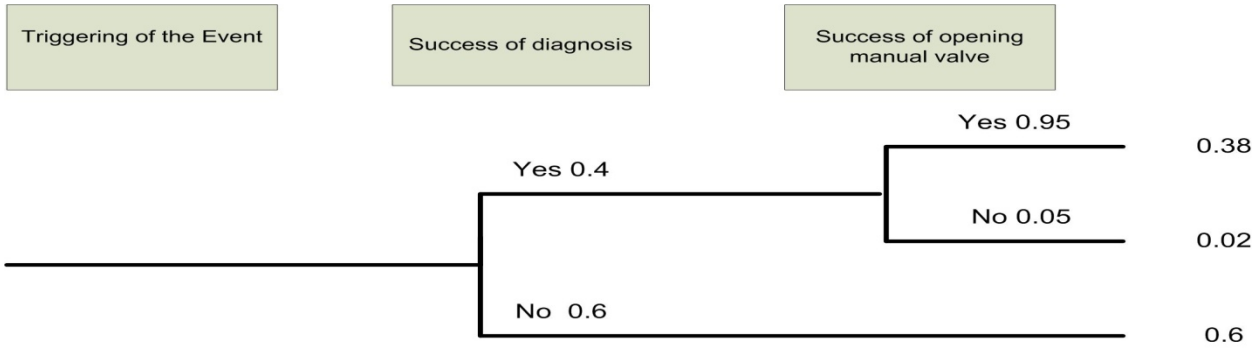
Assume β factor is 0.02. The engineer recalculate the probability of malfunction of the system after taking dependent failure into account.



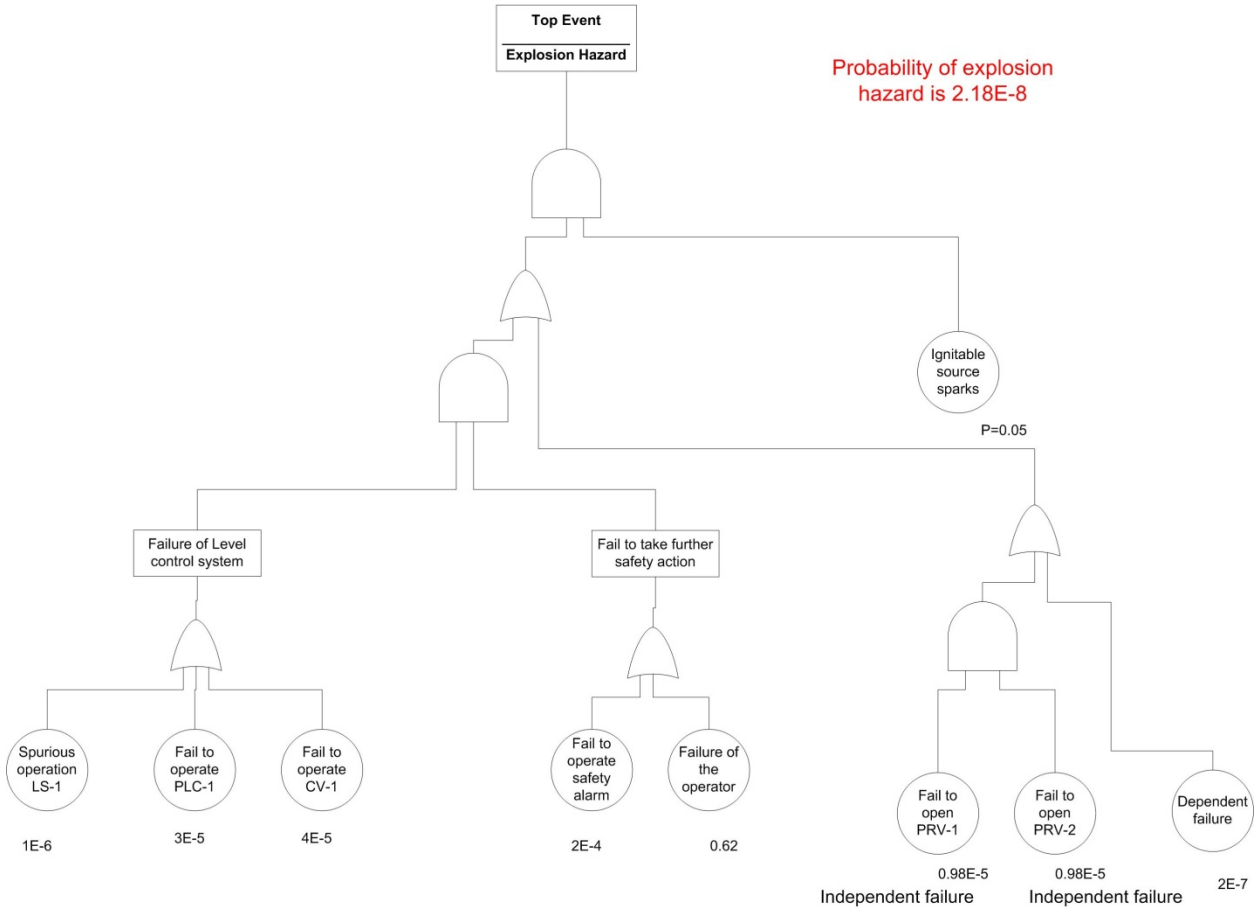
Task 3:

In this task, the human error probability (HEP) needs to be considered. We have assumed that the action time for the operator after receiving the alarm signal is about 10 minutes. We can use THERP method to conduct this analysis.

Figure 1 can be used to calculate the value of the HEP and middle curve (nominal) of figure 1 is first used. Following the procedure of the THERP method, we can calculate that the success of the diagnosis is 0.4 , on the other side, failure is 0.6. Success of opening the manual valve is 0.95 (we assume), failure is 0.05.



HEP in this case is 0.6+0.02=0.62



Now it can be assumed that he operator has been trained for this type of safety action and now if we continue to use THERP, lower curve can be used. Success of the diagnosis is 0.9 , on the other side, failure is 0.1. Success of opening the manual valve is 0.95 (we assume), failure is 0.05. Therefore, the probability of the operator failure in this case study is Pr=0.1+0.9*0.05=0.145