Case Study: Building a reliable system (Solution)

System Description:

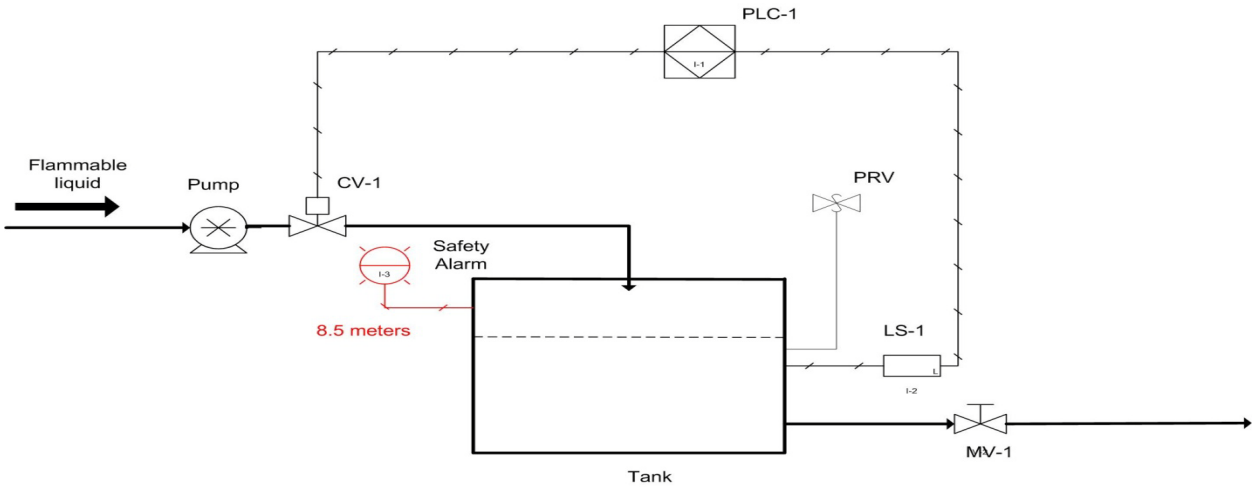

Figure 1. Tank system diagram

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 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) 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 the 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 shut down the pump to stop the liquid going into the tank. Assume this operator has only about 10 minutes to response the alarm.

The site engineer worries about this situation and hopes to increase the reliability of this system (decrease the failure probability). Furthermore, the site engineer wants to decrease the possibility of potential explosion hazard. 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
Level sensor	Spurious operation (shift in calibration)	3E-5
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	Fail to open	1E-5
Pressure relief valve PRV	Spurious operation	2E-6
Manual valve MV-1	Failure to remain open	4E-6
Safety alarm	Fail to run	2E-4
Tank	Structure failure	3E-9

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

Step 1: System reliability analysis

The purpose of this step is to improve the reliability of the system. What is probability of the malfunction of the system ? During this step, the site engineer does not need consider the operator.

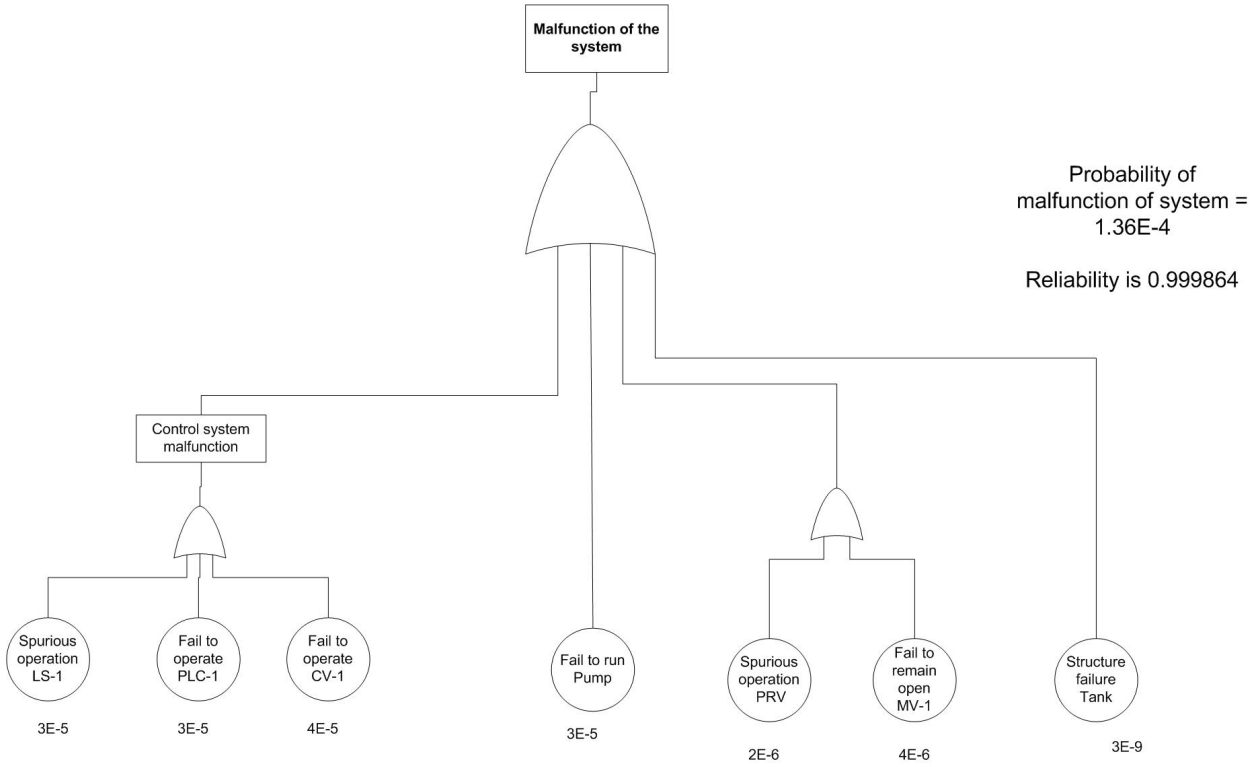

Figure 2. Fault tree for the reliability analysis of the system

After the calculation from constructed fault tree, the reliability of the system is 0.999864

<u>Adding redundant pump</u>

The site engineer can certainly improve the reliability of the system, for example, a redundant pump can be introduced to the system. Observing from the fault tree above, both control system and pump play important role on the system reliability analysis. Assume that the site engineer would like to install a redundant pump instead of control system. In the fault tree, one AND gate will be added, shown below. After the calculation, the reliability of the system is 0.999894.

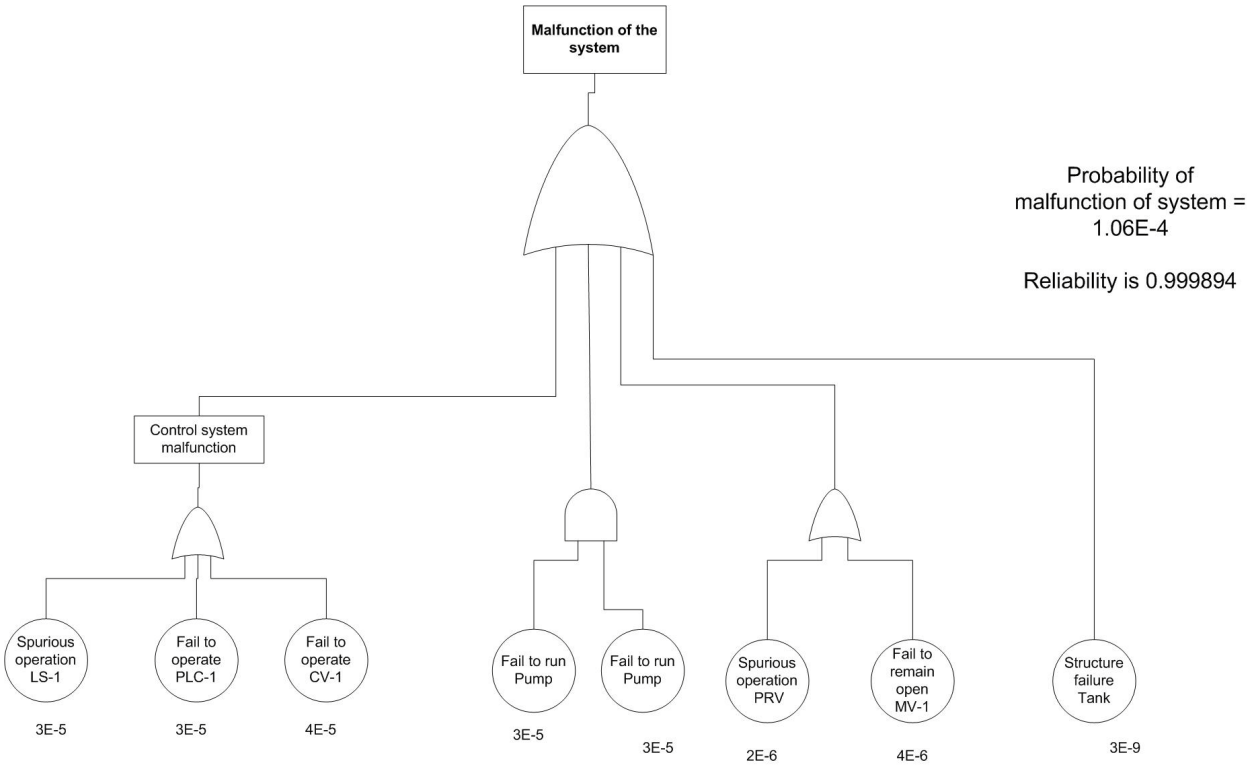

Figure 3. Fault tree after introducing redundant pump

Dependent failure

In order to improve the reliability of the system, the site engineer decides to add more redundant components such redundant pump or redundant safety alarm. Is this alright ? If redundant component is introduced in the system, then dependent failures need also to be considered. Dependent failure in this case could be calculated using β-factor model.

Assume β factor is 0.02. The engineer recalculate the probability of malfunction of the system after taking dependent failure into account, shown below. After the calculation, the reliability of the system is 0.999893.

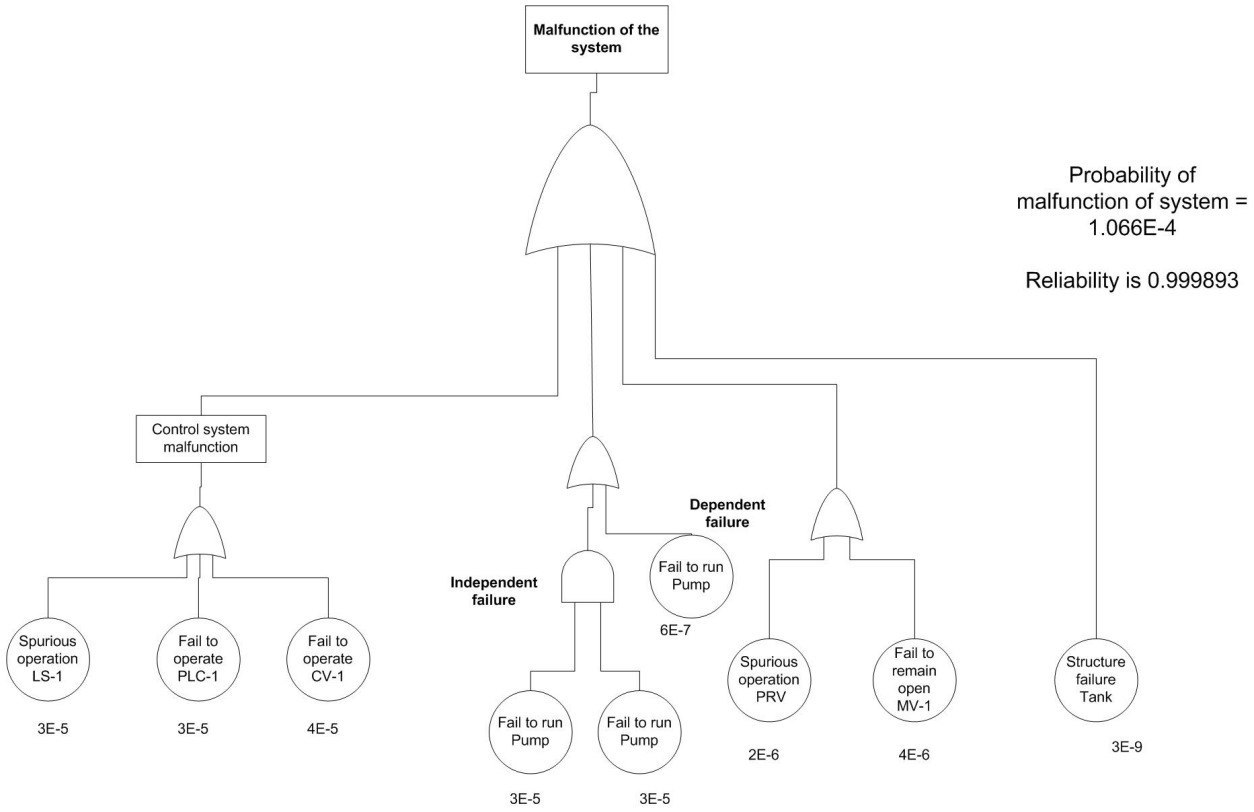

Figure 4. Fault tree after considering dependent failure

Step 2: Top event analysis

The site engineer needs to analyze the probability of explosion hazard. In order to do so, the engineer needs to redefine the top event and build the fault tree using different failure mode of corresponding components. The reliability of human operator needs to be considered as well.

As shown above, the response time for the operator after receiving the alarm signal is about 10 minutes. The THERP method can be used to conduct this analysis. (Figure A in the class note can used to calculate the failure of the diagnosis and middle curve of figure A is first used). Following the procedure of the THERP method :

Success of the diagnosis is 0.4 , on the other side, failure is 0.6

Success of opening the manual valve or shut down the pump is 0.95 (we assume), failure is 0.05

Therefore, the probability of the operator failure in this case study is Pr=0.6+0.4*0.05=0.62

After this, the engineer can combine this HEP data with other reliability data and build the corresponding fault tree. It should be noted that different failure mode of level-sensor is used in this step. The result for the probability of explosion hazard is 1.5E-10

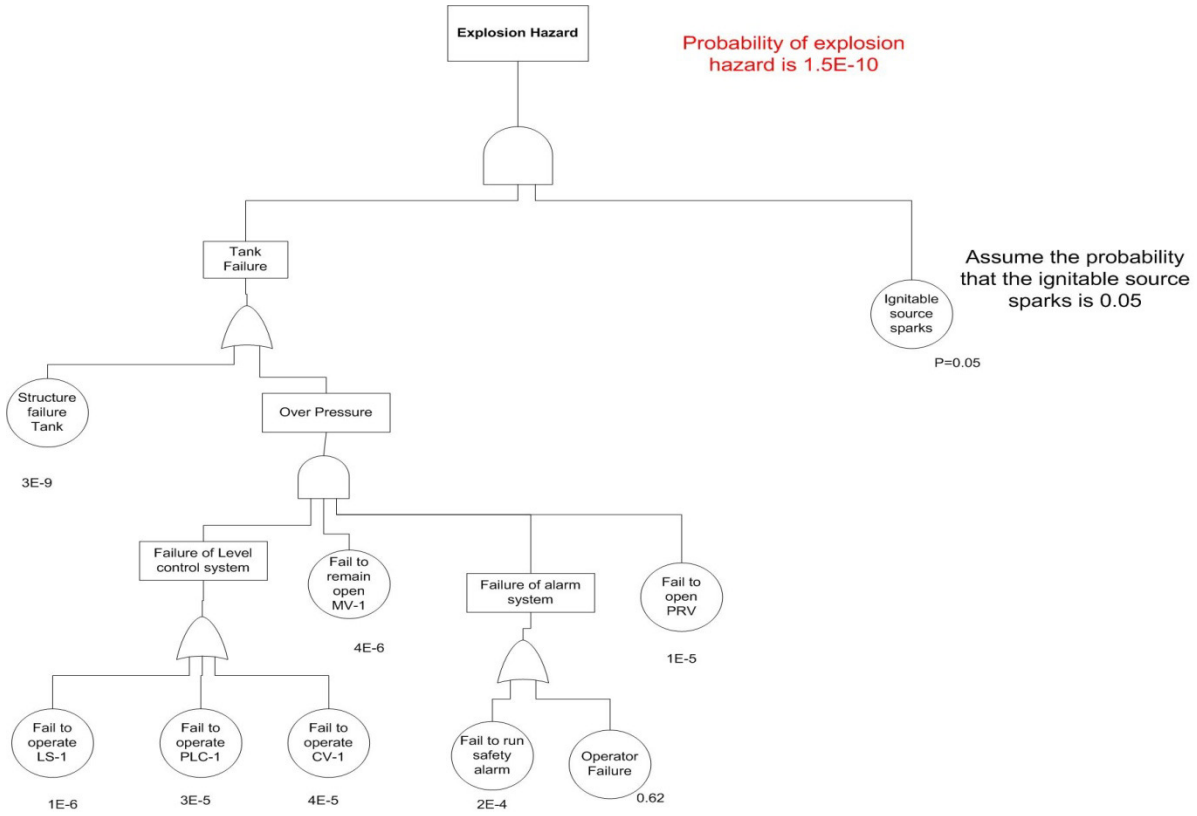

Figure 5 Fault tree for top event analysis

Training the operator

Now assume the operator has been trained for this type of safety action. Therefore, lower curve of THERP figure can be selected.

Success of the diagnosis is 0.9 , on the other side, failure is 0.1

Success of opening the manual valve or shut down the pump 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

(Since tank structure failure is the dominant factor for the explosion hazard after fault tree analysis in this case study, training operator will not decrease the possibility of the hazard significantly. ***However, please keep it in mind that training operator could help to improve the situation, just not in this case study****)*

Adding automatic emergency shutdown system (ESD)

The site engineer still thinks this probability is too high and tries to decrease this number. An automatic emergency shutdown system (ESD) is installed in the tank. This system include a level sensor (LS-2), a control valve (CV-2) and a programmable logic controller (PLC-2). The purpose of this safety system is to prevent the explosion hazard by shutting down the input of the bank in case no response from the operator (10 minutes after the liquid level of the tank reach to 8.5 meters). Assume the failure probabilities for these new installed components are as same as the ones used in level control system.

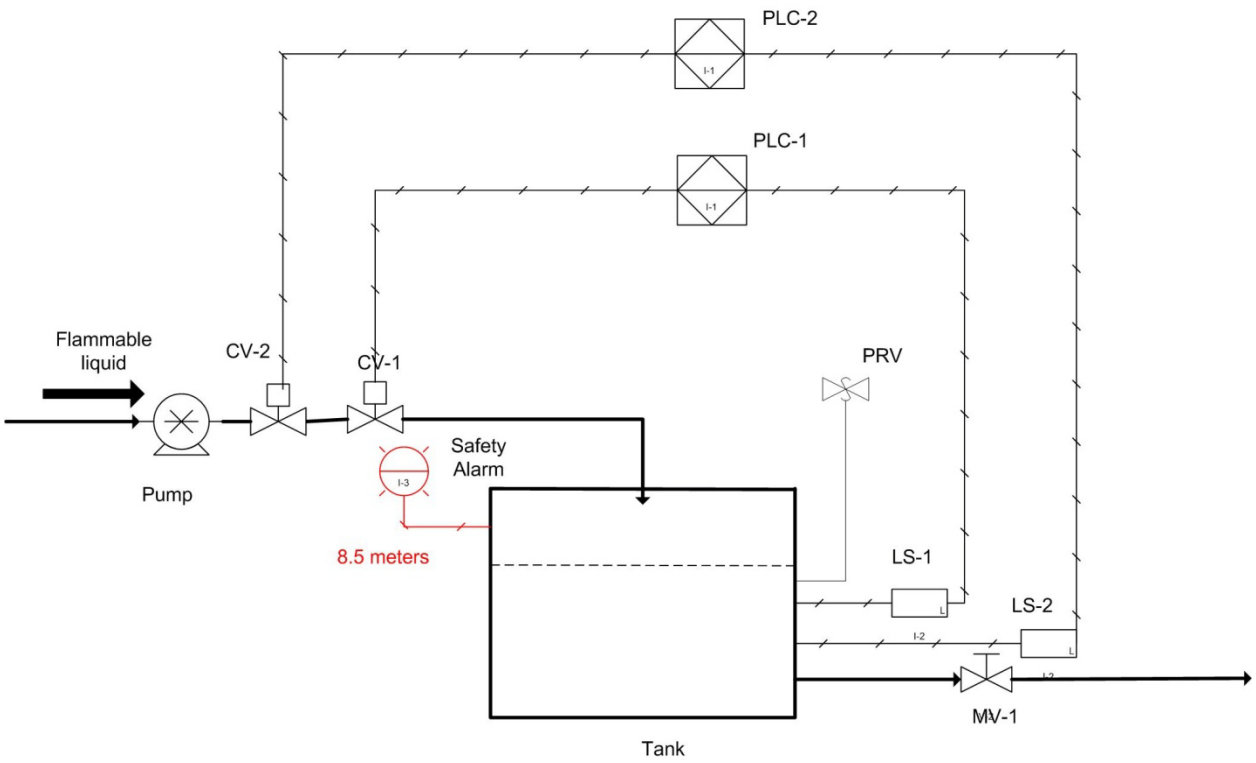

Figure 6. Tank system diagram after installing an automatic emergency shutdown system

Question :

Please re-build the fault tree and calculate the probability of explosion hazard. Compare this data with the previous data, can you be able to see the difference ??