Determine the lower and upper bounds of prevention barriers failure probabilities to predict the accident causation probability

Nurul Fatin Amalina Binti Irham, Dr. Sherif Abdulbari Ali

Faculty of Chemical Engineering, Universiti Teknologi Mara Shah Alam

***Abstract*—Any institutions or industries may have their own internal guidelines in order to reduce the risk of accidents and controlling the hazards surround the area. But, the current available guidelines might be to general and not able to give the probability of failure for the equipment. This study is focusing on reactor in Pilot Plant building located at Universiti Teknologi MARA (UiTM) Shah Alam which is Continuous Stirred Tank Reactor (BP 100). The objectives of this research are to determine the boundaries of prevention barriers failure probabilities and directly predict the accident causation probability and also to provide a software those can easy the risk assessment. The Fault Tree Analysis Diagram has been used as the risk assessment method. Then, the Fault Tree Analysis has been done to the Continuous Stirred Tank Reactor (BP 100) in order to predict the condition that may happen if it is undergo overheating (more than 50℃). Fault Tree Analysis Software of Continuous Stirred Tank Reactor (BP 100) has been constructed using Microsoft Visual Basic 6.0. Resulting from the constructed software, it is shows that overheating of Continuous Stirred Tank Reactor does not lead to the failure of overall equipment because the reliability value is 0.9991 compared to probability value which is 8.0108×10^{-4}.**

Keywords— Accident causation, Barriers failure, Fault tree analysis, Prevention method, Safety barrier, Safety function, Safety system, Hazard Identification

INTRODUCTION

In recent years, safety becomes a demanding issue and important to all institutions and industries. Many of academic institutions started to the research about safety. Safety in Malaysia becomes better day by day since there is developing of technology. Safety is required in order to protect from loss of life and properties. In Malaysia, the occupational safety and health had started since 1896 (DOSH, 2016).

In Malaysia, Department of Occupational Safety and Health Malaysia (DOSH) is responsible over the safety and health of the workers at the workplace by evaluating the risk in industrial area including machineries and reports. The sectors that include in DOSH responsibility or the place that should performing safety are manufacturing, mining and quarrying, construction, hotels and restaurant, agriculture, forestry and fishing, transport, storage and communication, public services and statutory authorities, any industries that using all types of utilities (such as gas, electricity, water, and sanitary services), finance, insurance, real estate and business services, wholesale and retail trades (DOSH, 2016).

The performance of safety can be measured by identification of hazard, risk assessment, and risk analysis (Covello and Merkhofer, 1993). Identification of hazard can be done by observing the area of workplace for the machinery or working area and referring to safety data sheet for the chemical. Risk assessment is a tool that helps to identify the specific counter measure for the specific hazardous material or situation (Covello and Merkhofer, 1993). Then, the risk analysis should be done after the risk assessment in order to analyze the result form risk assessment in order to improve the current performance of safety.

There are many ways to performing the safety and reducing the tendency of accident in workplace such as follow and never skip the standard operating procedure, wear the personnel protective equipment, and many more. The management of the company should provide the personnel protective equipment to the workers. The safety barrier also one of the methods that can reduce the possibility of accident by protecting the human life and properties. Snorre Sklet (2006) once states that the meaning of safety barrier is the prevention method against the unwanted event. The management of company should provide safety barriers in order to protect the workers from the accident. Theoretically, there are three types of safety barriers which are personnel barriers, organizational barriers, and technological barriers (Jian K. et al, 2015). However, some of barriers are suitable to be performed in industries and some are not. Thus, management should evaluate the working area before performing the safety barriers.

Accident can be caused by many factors. Accident would be happen because safety is not being performed. Performing of safety required money but loss of human life and properties need a lot of money to recover from the accident. Because of this, Malaysia started to perform safety and implement some regulations that related to safety in order to protect the workers and company's properties. Manikam Pillay (2015) states that there are five ages of accident causation which are starting by leak of technological system, human behaviors, socio-technical, culture, and resilience.

The prevention method of barriers failure and method to predict the accident causation are two major studies for this research. Barriers failure can be prevented by constructing the fault tree diagram or event tree analysis diagrams and determines the probability values (Daniel A. C. and Joseph F. L., 2002). While, for the prediction of accident causation should be based on the theory of accident causation such Domino's theory, human factor theory, and many more (Manikam Pillay, 2015). Thus, two major studies in this research are prevention method of the barriers failure and prediction method of accident causation.

BARRIERS AND ACCIDENT CAUSATION

Barriers

There are three components that related to barrier which are barrier function, barrier system, and barrier elements. Barrier itself can be defined as a model that functions as the protector to the asset by protecting it from hazard (Snorre Sklet, 2006). By

focusing directly to the safety matter, below is the categories of safety barrier, safety function, and safety element.

Categories of safety barrier

There are three categories of safety barriers which are personnel barriers, organizational barriers, and technological barriers (Jian K. et al, 2015). The personnel barrier is the application of human knowledge in safety areas to prevent the accident or undesired events by applying the right response over the safety system (Jian K. et al, 2015). The organizational barrier is the management agenda or activities conducted by the management of the respective company in order to give the awareness to the workers about the important of safety accomplishment at the workplace (Jian K. et al, 2015). Technological barrier divided into three types of barriers which are passive barrier, positive barrier, and detection barrier (Jian K. et al, 2015). The passive barrier is something that fix such as wall, it is call as passive barrier because it does not need any human work and energy transformation (Jian K. et al, 2015). The positive barrier need software for it to be functioned and it can be functioned manually or automatically (Jian K. et al, 2015). One of the examples of positive barriers is automatic sprinkler system (Jian K. et al, 2015). The detection barrier cannot prevent and control accident, but it can detect and monitor the potential risk by sending the information to the control system in order to alert that the risk is detected (Jian K. et al, 2015).

Categories of safety function

There are four phases of safety function which are normal condition, initial phase, conducting phase, and injury phase (Snorre Sklet, 2006). During the normal condition, the accident can be avoided or prevent. Besides that, if there are undesired events at normal condition it may cause by the lack of system control. Next, the initial phase is where the accident sequence is started to begin. The starting of accident may due to loss of control at normal condition, but still the undesired event has potential to be prevented from further worst situation (Snorre Sklet, 2006). Next, the concluding phase can be defined as the end of accident which the action that can be taken at this situation is protection needed for the people that may injured or the balance of the properties left after the accident (Snorre Sklet, 2006). Lastly, the injury phase is the phase where the mitigating process can be done (Snorre Sklet, 2006). At this situation, the serious effect by the accident can be treated by doing the recovery session in order to protect the current effect from further worst effect.

Categories of safety system

Snorre Sklet (2006) stated that passive and active system is based on behavior or response of the system. The passive systems do not need any action to protect the situation, fix firmly, and do not affected by the process that operate surround it. The example of the passive system is brick wall that does not any action in order to protect the human or material. Next, the active system is a system that needs an action in order to decrease the risk potential (Snorre Sklet, 2006). The example of active system is lamp switch which need an action to push the button in order to make it functioned (Snorre Sklet, 2006). In addition, usually the active system is affected by the process surround the area whether by human action or technical system (Snorre Sklet, 2006).

Criteria of measuring the performance of the safety barrier

The first criterion in measuring the performance of the safety barrier is evaluation. The evaluation is needed in order to ensure that the safety barrier working as expectation (Hollnagel, 1995). Second criterion is resource required (Hollnagel, 1995). The resource required is important in order to ensure the resources used for performing and maintaining the barrier is available (Hollnagel, 1995). Third criterion is reliability. Reliability is the probability of the component will not fail (Hollnagel, 1995). The reliability also helps to identify the resistance of the barrier (Hollnagel, 1995). The adequacy is function as the criteria that help to identify the efficiency of safety barrier in order to achieve the safety barriers' objective (Hollnagel, 1995). The availability criterion can be considered as the availability of the safety barrier during the needs. The sixth criterion is time required for implementation (Hollnagel, 1995). This criterion indicates that the time required starting from designing the barrier until the implementation of the barrier. The last criterion needed is applicability to safety critical task (Hollnagel, 1995). This criterion indicates that the ability of safety barrier playing an important role in safety and become one of the important things in socio-technical framework.

Accident Causation

Accident may cause by action or condition. Basically accident causation can be defined as the causes or reasons of accident to be happen either towards human or properties. Below are the theories for the accident causation.

Heinrich's Domino Theory

There are five elements that involve in Domino's Theory timeline which are social environment and ancestry, fault of the person, unsafe act or condition (mechanical and physical hazards), accident, and lastly injury (Rohana Hassan et al., 2014, Yvonne Toft et al., 2012). In order to prevent the unwanted event (accident) from happen, one of the element in Domino's Theory should be eliminated. From H.W. Heinrich Domino's Theory, the unsafe act or condition is the central contributor to the undesired event (Yvonne Toft et al., 2012). By removing the unsafe act or condition factor, the other factor could be stop or inefficient based on Domino's Theory (Yvonne Toft et al., 2012). Yvonne et al., (2012) states that over 75000 reported insurance regarding on accidents, the most contributor is come from unsafe acts of person which cover 88% from the total reports. The balance percentage goes to unsafe mechanical or physical conditions and bad lack (unpreventable accidents) at 10% and 2% respectively (Yvonne Toft et al., 2012).

Human Factor Theory

David L. Goetsch (2010) states that human factor theory is regarding on accident that happen due to human error. There are three types of human error which are inappropriate activities, inappropriate response and overload (Daniel A. Crowl and Joseph F. Louvar, 2002, David L. Goetsch, 2010). The first types of error which is inappropriate activities is all about the actions that should not be done by the person at the workplace which may has the tendency for the accident happen (Daniel A. Crowl and Joseph F. Louvar, 2002). The inappropriate activities can be included under unsafe act proportion. One of the examples for inappropriate activities is putting the flammable material near to the heating process. The second type of human error theory is inappropriate response. The inappropriate response also can be classified as unsafe act. One of the examples for inappropriate response is using unsuitable extinguishing media during firefighting which may cause for larger fire and another worse undesired event. The last element in human factor theory is overload. Overload is causes by carrying a heavy load that over the human ability (Daniel A. Crowl and Joseph F. Louvar, 2002). Overload may cause backache or injury to human body.

Accident/Incident Theory

The next theory is Accident/Incident Theory. Basically, this theory is the continue theory from human factor theory (B.S. Dhillon, 2003). The decision to err inside accident/incident theory indicates the wrong decisions that have been decided by the person in charge during the critical situation (B.S. Dhillon, 2003). Besides that, the incorrect estimation over the risk also include under decision to err (B.S. Dhillon, 2003). Overload of the system can cause the systems failures which are one of the accident/incident theories. Next, the last element in accident/incident theory is ergonomic traps. The ergonomic traps may cause by unsuitable height of workstation. Same as elements in human factor theory, it may cause backache or other discomfort condition for long time period to the respective worker.

Fault Tree Analysis

The advantage of models of accident causation in safety industry is helping in identification of causes of the accident (Mark Lehto and Gavriel Salvendy, 1991). Besides that, the model also has the tendency to eliminate or reduce the probability and possibility of accident to happen (Mark Lehto and Gavriel Salvendy, 1991). The Fault Tree Analysis is one of the models of accident causation that have been used for study in reliability, safety and risk in industry or education level. Fault Tree Analysis has been developed starting from 1960s in order to help the safety evaluation in industry. However, the Fault Tree Analysis might take a longer time to be solved if there are too many of equipment involve (Ahmad Ali Baig et al., 2013). Besides that, Fault Tree Analysis is a "top-down" analysis which the analysis is started with the top event and continues to the more specific or causes of top event. There are two terms that will be used in Fault Tree Analysis which are reliability and probability. Reliability is the probability of the component will not fail (Hollnagel, 1995). While, the definition of probability in safety point of view is the probability of failure (Daniel A. C. and Joseph F. L., 2002):

METHODOLOGY

Chosen of equipment.

The Continuous Stirred Tank Reactor (BP 100) has been chosen as the studied equipment for this research. Compared to other equipment in Chemical Engineering Pilot Plant, this reactor was the equipment that often faced a problem. Formerly, this equipment undergo overheat until the heater was burned. The barrier failure probabilities and accident causation of this equipment were studied.

Designed of Fault Tree Analysis Diagram

Fault Tree Analysis is one of the risk assessment methods used by the industries to predict the accident causation. Thus, this method has been chosen to be applied to the equipment in Chemical Engineering Pilot Plant, UiTM Shah Alam. Fault Tree Analysis Diagram was designed according to the schematic diagram of Continuous Stirred Tank Reactor (BP 100).

Constructed a Fault Tree Analysis Software

Conducted a design of software to determine the lower and upper bounds of prevention barriers failure probabilities to predict the accident causation probabilities. Microsoft Visual Basic was used to develop the software of Fault Tree Analysis for Continuous Stirred Tank Reactor (BP 100).

Validation regarding on the constructed software

The theoretical equation from Daniel A. Crowl and Joseph F.Louvar (2002) had been used for coding in order to ensure that this software was based on theory of Fault Tree Analysis.

RESULT AND DISCUSSION

The Fault Tree Analysis Software has been used to calculate the reliability and probability value of the overheated Continuous Stirred Tank Reactor (BP 100). The purpose of this software is to predict the situation that may happen with the respective basic causes of accident. Four basic causes that have been chosen were failure of temperature sensor (TIC 1), failure of control valve V3, failure of control valve V5, and failure of control valve V4.

For this research, the time interval and the failure rate were depended on 1 year period of time. The common failure rate data of components from the Chemical Process Safety Fundamentals with Applications (Daniel A. C. and Joseph F. L., 2002) and Reliability Estimates for Selected Sensors in Fusion Applications (Blanton and Eide, 1993) have been used as the references. Table 1 shows that each of the component got the reliability value higher than probability. This result proved that the Continuous Stirred Tank Reactor (BP 100) was reliable even though it was undergo overheated.

The top event of the Fault Tree Analysis was "overheating of CSTR". The causes of top event was then studied by referred to the schematic diagram of Continuous Stirred Tank Reactor (BP 100).Figure 1 shows the overall Fault Tree Analysis Diagram constructed by using Microsoft Visual Basic and the schematic diagram of Continuous Stirred Tank Reactor (BP 100).

Components	Failure Rate (Faults/year)	Reliability	Probability
Temperature Sensor, TIC 1	0.00876	0.9912783	0.0087217
Control Valve, V3	0.6	0.5488116	0.4511884
Control Valve, V5	0.6	0.5488116	0.4511884
Control Valve, V4	0.6	0.5488116	0.4511884
Control Valve, V1	-	0.9960649	0.0039351
Control Valve, V2	-	0.7964290	0.2035710
Overheating of Continuous Stirred Tank Reactor (BP 100)	-	0.9991989	8.0107821×10^{-4}

Table 1: The results collected from the Fault Tree Analysis Software for Continuous Stirred Tank Reactor BP 100 (Blanton and Elde, 1993, Daniel A.C. and Joseph F.L., 2002).

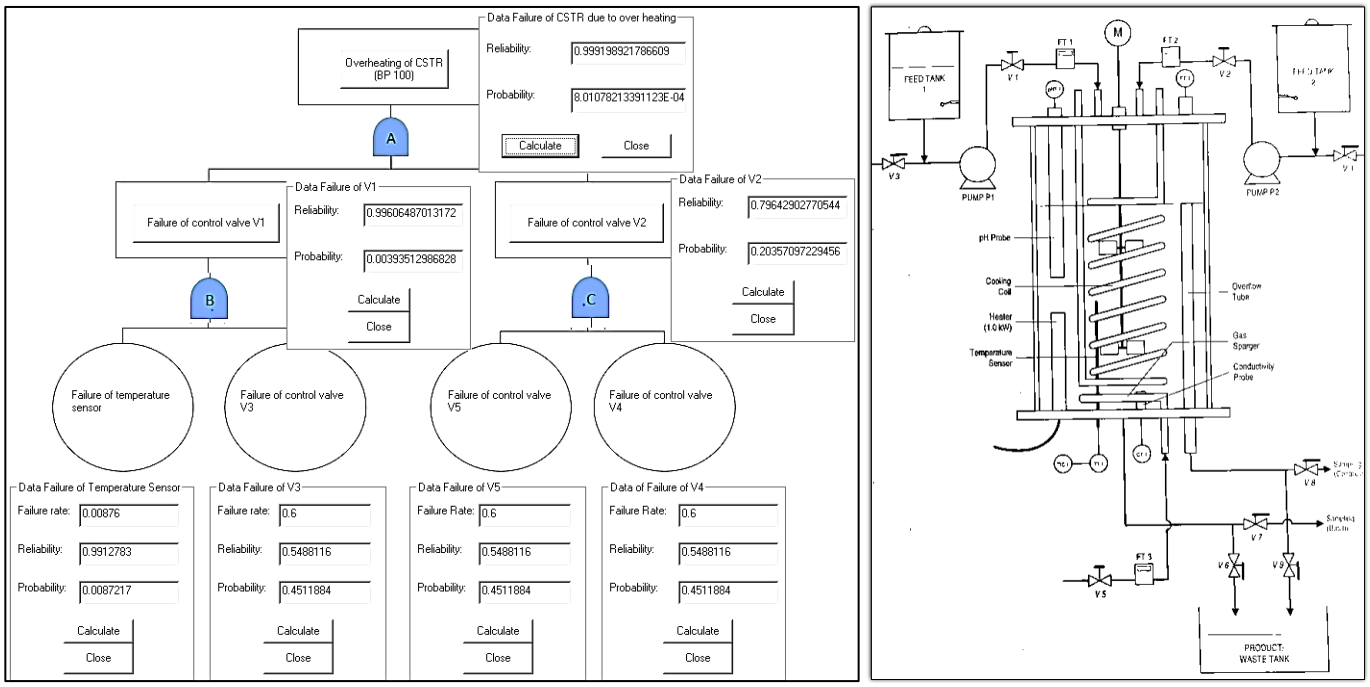

Figure 1: The overall Fault Tree Analysis Software constructed by using Microsoft Visual Basic and the schematic diagram of Continuous Stirred Tank Reactor (BP 100).

Compared to other equipment, Continuous Stirred Tank Reactor (BP 100) was the equipment that usually faced a problem in pilot plant but it took quite some times for the equipment to fail. The problem was occurred only two times in a year but, the failure of the reactor would not happen every year. The often problem that Continuous Stirred Tank Reactor (BP 100) faced was overheated. This problem caused by the heater inside the reactor. During the experiment, sometimes students did not aware that the level of chemical inside the reactor was below the heater placement. The heater should be immersed inside the chemical in order to avoid the overheated problem. Besides that, the element inside the heater also may be broke if it was overheated. The insufficient amount of chemical inside the reactor was caused by the error made by the students during the experiment. For example, there were some errors during the experiment, the students will take the sample a few times for each sample and thus it caused to the insufficient of chemical inside the reactor. Another reasons that caused heater to burn was drained the excess chemical without shut down the heater. This caused the heater to burn or the column to be cracked.

Furthermore, the usual temperature of the reactor should be less than or equal to 40℃ in order to ensure that the heater was not burned due to overheat. The reactor can be considered overheated when the temperature indicator shows 50℃ or more.

The four basic causes overheating of Continuous Stirred Tank Reactor (BP 100) were failure of temperature sensor (TIC 1) and failure of valves (V3, V5, and V4). The type of link between components for BP 100 reactor was Parallel Link. The fault tree diagram for parallel link need both components to fail in order to make the system fail. If control valve V1 was fail, the reactant from feed tank 1 cannot enter the reactor and it was the same if the control valve V2 was fail, the reactant from feed tank 2 cannot enter the column. The Continuous Stirred Tank Reactor would not undergo overheating if there was sufficient chemical inside the reactor. Even though only one reactant was entered the reactor, still the equipment would be fine. This was because, back to the principle of Parallel Link of fault tree analysis, both components need to be failed in order to make the system to fail.

All the four basic causes V3, V4, V5, and TIC 1 were the main effect to the overheated of Continuous Stirred Tank Reactor. Then, all three valves, V3, V4, and V5, each of valve would stopped the chemical or cooling water from enter the reactor. Thus, overheated of reactor might happen and caused the heater to burn. While temperature sensor, TIC 1 was important because it would notified people the temperature inside the reactor. If the sensor was failed, thus overheated problem of the reactor cannot be detected. According to Daniel A.C. and Joseph F.L. (2002), event in Fault Tree Analysis are not limited to the failure of the machines or hardware only, the human and the environment surround the equipment also can be included as the event.

CONCLUSION AND RECOMMENDATION

In conclusion, the constructed Fault Tree Analysis Software was helped to determine the barrier failure probabilities of Continuous Stirred Tank Reactor (BP 100) and Continuous Stirred Tank Reactor was not failed due to overheat because the reliability value was 0.9991 which was higher compared to probability value which was 8.0108×10^{-4}. It is recommended to upgrade the Fault Tree Analysis Software in order to be able to determine the failure rate data of all basic causes for Continuous Stirred Tank Reactor (BP 100).

ACKNOWLEDGMENT

Grateful thanks to Dr. Sherif Abdulbari Ali, my final year project supervisor for the encouragement, guidance, critics, and friendship. I am very lucky and thankful to have a very supportive and helpful supervisor that always guide me along my final year project journey. My thankful also goes to Mr. Jamil, the pilot plant technician for the guidance during my research. Lastly, thank you to all lecturers and friends that help me throughout my degree life.

REFERENCES

[1] Ahmad Ali Baig et al. (2013). Reliability Analysis Using Fault Tree Analysis: A Review. *International Journal of chemical Engineering and Applications.* 4(3): 169-173

[2] Arnljot Hoyland and Marvin Rausand (2004) *SYSTEM RELIABILITY THEORY Models and Statistical Methods.* Canada: John Wiley & Sons Inc.

[3] B.S. Dhillon (2003) *Engineering Safety*. Singapore: World Scientific Publishing Co.Pte.Ltd.

[4] C. H. Blanton and S. A. Eide (1993), Reliability Estimates for Selected Sensors in Fusion Applications. *Idaho National Engineering Laboratory*. 2-8

[5] Daniel A. Crowl and Joseph F. Louvar (2002) *Chemical Process Safety Fundamentals with Applications*. 2nd ed. Upper Saddle River: Prentice Hall.

[6] Duijm, N.J., Madsen, M. D., Andersen. H. B., Hale. A., Goossens, L., Londiche, H., et al. (2003). Assessing the effect of safety management efficiency on industrial risk. In *ESREL 2003.* Maastricht: Balkema.

[7] Daniel A. Crowl and Joseph F. Louvar (2002) *Chemical Process Safety Fundamentals with Applications*. 2nd ed. Upper Saddle River: Prentice Hall.

[8] David L. Goetsch (2010) *Occupational Safety and Health for Technologist, Engineers, and Managers.* 7th ed. Pearson

[9] DOSH (2016) The Role and Development. Department of Occupational Safety and Health Malaysia. (Website) http://www.dosh.gov.my/index.php/en/about-us/dosh-profile

[10] DOSH (2016) DOSH Profile. Department of Occupational Safety and Health Malaysia (Website) http://www.dosh.gov.my/index.php/en/about-us/dosh-profile

[11] Dr.Liew Voon Kiong (2008) Introduction to Visual Basic 6.0 (Website) Retrieved from http://www.vbtutor.net/lesson1.html.

[12] Hollnagel E., (2004). Barrier and accident prevention. Hampshire, UK: Ashgate.

[13] Hollnagel E., (1995). The art of efficient man-machine interaction: Improving the coupling between man and machine. In J.-M. Hoc, P.C. Cacciabue, & E. Hollnagel (Eds.), *Cognition & Human-Computer Cooperation.* Hilssdale, NJ: Lawrence Erlbaum Associates Inc.

[14] Jian K, Jixin Zhang, and Jianchun G. (2016) Analysis of the safety barrier function: Accidents caused by the failure of the safety barriers and quantitative evaluation of their performance. *Journal of Loss Prevention in the Process Industries*, 43: 361-371

[15] Manak Bavan (2006) HAZARD IDENTIFICATION AND RISK ANALYSIS-CODE OF PRACTICE. *Indian Standard*

[16] Manikam Pillay (2015) Accident Causation, prevention and safety management: a review of the state-of-the-art. *Procedia Manufacturing*, 3: 1838-1845

[17] Rohana Hassan et al., (2014) *InCIEC 2014 Proceedings of the International Civil and infrastructure Engineering Conference 2014* Singapore: Springer

[18] Rohana Hassan et al., (2014) *InCIEC 2014 Proceedings of the International Civil and Infrastructure Engineering Conference 2014* Singapore: Springer

[19] Sklet S., and Hauge S., (2003). *SINTEF-Memo discussion of the term safety barrier*. Trondheim: SINTEF (in Norwegian).

[20] Snorre Sklet (2006) Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries*, 19(5): 494-506.

[21] Syuhada Bte Ismail (2013) *Development of risk matrix analyzer in Chemical Engineering Pilot Plant building via HIRARC Methodology*. Universiti Teknologi Mara: Degree Thesis

[22] Yvonne Toft et al., (2012) *Model of Causation: Safety.* Australia: Safety Institute of Australia.