

# Comprehensive Analysis of Safety Risk Assessment HRSG: PT. “X” Indonesia with the Combination Method of HAZOP, LOPA and SIL

Anton Irawan<sup>1\*</sup>, Indar Kustiningsih<sup>1</sup>, Sayid Jakfar<sup>2</sup>

<sup>1</sup>Department of Chemical Engineering, Faculty of Engineering, Universitas Sultan Ageng Tirtayasa, Indonesia

<sup>2</sup>Magister Study Program of Chemical Engineering Universitas Sultan Ageng Tirtayasa, Indonesia.

\*Corresponding author. Email: [antonirawan@untirta.ac.id](mailto:antonirawan@untirta.ac.id)

## ABSTRACT

Gas turbine cogeneration or combined heat and power is an efficiency in generating electricity while utilizing hot exhaust gases to generate steam in HRSG. The facility has significant risk in operation, need to comprehensively risk analysis and carry out of mitigation. Comprehensive risk analysis of these unit with the combined method of HAZOP, LOPA, SIL, by initiating hazard identifying and continued analysis with the HAZOP method and obtained 23 scenarios of deviation HAZOP were acceptable risk, 20 scenarios were significant risk and 1 scenario was as high risk. The safeguard on combination of HAZOP and LOPA analysis to medium and high risk scenarios is not required, because the initiating event frequency are smaller than the target mitigation likelihood, an increasing of SIL is required in the analysis of the combination of HAZOP and SIL. Existing protection has been met but still of a possibility of the instrumentation system opening failure such as the opening of diverter valve of the hot exhaust gases from the exhaust diffuser to gas stack and the HRSG unit, failure of BFW level control in HRSG unit and reduced supply of air demand to gas turbine unit due to dirty of air filter. Recommendations, for adding SIL for diverter valve, install safeguard alarm of HRSG level and install auto cleaning of intake air filter to gas turbine.

**Keywords:** HAZOP, LOPA, SIL, Risk Matrix, Risk Mitigation.

## 1. INTRODUCTION

Gas turbine cogeneration or combined heat and power is a combination of Heat Recovery Steam Generator and Electric power gas turbine units, which are very important supporting units in the chemical industry for the availability of electricity and steam supply [1, 2]. This industrial facility is expected to always operate normally, so that only normal operation control is needed such as temperature, pressure, flow rate, and so on, but in reality there are always abnormal conditions and emergency conditions, in this condition it is possible that things will not happen, such as the occurrence of over pressure, high temperature, leakage, so that it will have consequences and impacts on safety, production, financial, environmental. In abnormal and emergency conditions, safety devices such as relief valves, pressure switches, and others are required as well as supporting systems such as

emergency shutdown systems, fire detection systems and so on.

Abnormal conditions will have consequences and impacts, such as the combined heat and power 620-megawatt Kleen Energy-Siemens combined cycle natural power plant in Middletown which left 6 peoples dead and 50 injured [3], steam turbine explosions and fires. Pittsburgh's 880 megawatt power plant that shuts down more than 800,000 households and industries around the area [4]. Rupture and leak of HRSG boiler pipe PT. X after being operated for 5 years resulted in delays in the production process and financial losses.

High temperature 700°C in the combustion chamber of the turbine gas unit and hot exhaust gases from the turbine gas output are utilize HRSG boiler to produce 16 tons/hour of steam with a pressure of 30 kg/cm<sup>2</sup>. These condition have safety risk that have occurred, namely

leaks due to ruptured boiler pipes, and it need to be analyzed. A comprehensive analysis by combining the HAZOP, LOPA and SIL methods will provide accurate risk analysis results and risk mitigation so that the safety of operations and the adequacy of instrumentation tools installed in the HRSG unit have appropriate reliability. Safety risk analysis using only a single method such as HAZOP, LOPA or SIL has its own advantages and disadvantages, in the analysis to see the relationship between events that have occurred previously, the LOPA method is inadequate in viewing the guide word as a variable that will have consequences on each layer of protection [5]. In the worst-case scenario analysis of possible failures in each layer of protection, the single LOPA method can provide good analytical conclusions [5]. The combined method still has weaknesses, especially in mitigation analysis, because it only takes into account the safety of people as a mitigation target [6]. SIL analysis and calculation only takes into account the test interval of instrumentation equipment, even though the equipment is used for a long time in the operation process.

The objective of this study is provide an overview of the significant risks in the operation of the combined heat and power so that the mitigation can be carried out and the operation is safer.

## 2. METHODS

### 2.1 Hazard identification, hazard and operability study

The HAZID and HAZOP methodology are used to identify major process hazards or operability issues related to the process design [7]. HAZID is a first step of hazard identification of facility process and the significant hazard is continued to proceed in HAZOP methodology to identify all probable deviations far from initial design intentions and determine the possible abnormal causes and the consequences of each those deviations. Deviation analyzing, it is to consider the worse-case scenario, so it should be assumed that no safeguard is installed in the facilities. The most severe consequences must be taken into account also.

### 2.2 Layers of protection analysis

The LOPA analysis is a tool for assessing the adequacy of protection layers used to mitigate process risk. It includes simplified methods to characterize the consequences and estimate the frequencies of an incident [7]. The layers of protection are the following: basic process design, basic process control systems, critical alarms, safety instrumented functions, relief devices, additional mitigation. The steps to carry on a LOPA analysis are: 1 choose the scenarios that are of significant risk or high risk from HAZOP, 2 estimate the potential risk, 3 define the tolerable risk, 4 analyze the layers of protection and establish the independent protection layers, 5 risk reduction factor, 6 estimate the event frequency to compare with acceptable risk criteria.

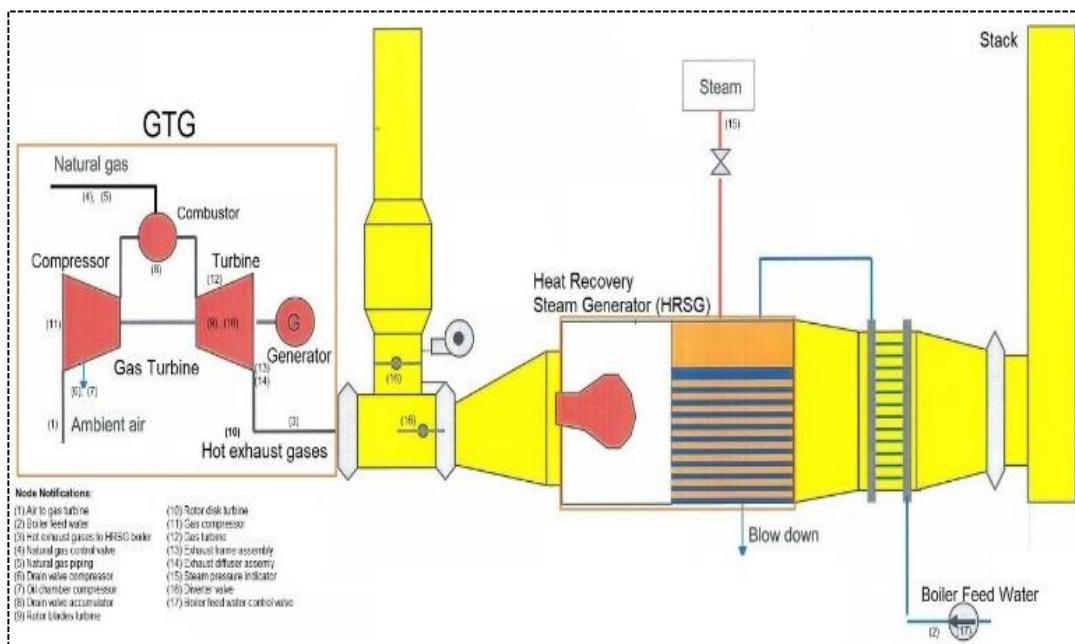


Figure 1. Flow diagrams Process of the study

### 2.3 Safety integrity level analysis

A SIL is a measure of safety system performance or probability of failure on demand for a Safety Instrumented Function or a Safety Instrumented System [7]. There are for levels of SIL consist of SIL1, SIL2, SIL3, SIL4. The higher the SIL level, the lower the probability of failure on demand for the safety system, and the better the system performance, IEC 2002 [8, 9].

The basic methodology to develop the HAZOP, LOPA and SIL analysis, the first stage was studied comprehensive of every nodes to be developed, in this case is with concerning to the gas turbine generator unit and heat recovery steam generator unit, to identify the operating principles of both units as the main combined heat and power facilities, and also to select the nodes to be evaluated. To do this, it was needed to systematically carry on node a review of the process flow diagram as shown in Figure 1, piping and instrument diagrams, operation manuals, and multi-expertise personal of the team [10]. Sixteen nodes that are distributed among two units facility were considered for this this study, as it is shown in Table 1.

**Table 1.** Unit facility and nodes of the study

Unit facility	Nodes
Gas Turbine Gen-erator	Natural gas control valve, Natural gas piping, Drain valve compressor, Oil chamber compressor, Drain valve accumulator, Rotor blades turbines, Rotor disk turbine, Gas compressor, Gas Turbine, Hot exhaust gases to boiler HRSG, Exhaust frame assembly, Exhaust diffuser assembly
Heat Recovery Steam Generator	Steam pressure indicator, Diverter valve, Boiler feed water control valve, Steam generation

For each node, deviations were analyzed, regarding guide words and the relevant process variables of flow, temperature, and pressure. Each association between a guide word and a variable represented a hazard scenario.

Each hazard scenario was categorized as affecting to human injury is given the symbol as I, delay of production is given the symbol as D, financial loss is given the symbol as F, effecting to environmental is given the symbol as E, these hazards are represents as average in scenario analysis. Each scenario was ranked according to its estimated severity and likelihood of probability or frequency has assigned criteria levels, P1 Very unlikely, P2 Small chance, P3 Occasionally, P4 occurrence, to determine the risk ranking. The severity level is each a category, S1 Very Little, S2 Minor, S3 Medium/Significant, S4 Critical, S5 Catastrophic was assigned to each scenario, according to the effects to the Probable, P5 Frequent. The risk ranking as a result of the relation between the severity and the probability or frequency of each every hazard scenario, the result of scenario can consist of following levels: low is given symbol as L, medium is given symbol as M high is given symbol as H, as it is shown in Figure 2.

## 3. RESULTS AND DISCUSSIONS

### 3.1 HAZOP analysis

There are relevant analysis variables are Flow, Temperature, Pressure. For each variable, the guide words applied, Flow: guide words were “None”, “Less”, “More”, Temperature and Pressure: guide words were “Low”, “High”. Eight scenarios were found to be of medium hazard on HAZID analysis, for HAZOP, there are twelve scenarios were found to be of medium risk and one scenario high risk in sixteen nodes in both of the unit, GTG unit and HRSG unit, as it is shown in Table 2.

		Probability / Frequency Code					Risk Ranking	Definition and criteria
		P1	P2	P3	P4	P5		
Severity Code	S1	1(L)	2(L)	3(L)	4(L)	5(L)	1.0 (L) - 7.9 (L)	Acceptable Risk (L), subject to application of the principle of ALARP
	S2	2(L)	4(L)	6(L)	8(M)	10(M)	8.0 (M) - 14.9 (M)	Operation can be executed after efficient measures are implemented and the analyses team has found the risk satisfactory (M), principle of ALARP to be followed
	S3	3(L)	6(L)	9(M)	12(M)	15(H)		
	S4	4(L)	8(M)	12(M)	16(H)	20(H)	15.0 (H) - 25.0 (H)	High Risk: if the undesired event after mitigating measures is evaluated to unacceptable risk (H) the operation shall not be carried out.
	S5	5(L)	10(M)	15(H)	20(H)	25(H)		

**Figure 2.** Risk Matrix.

**Table 2.** Medium and high-risk scenarios

Equipment	Total number of scenarios	HAZID		HAZOP	
		Number of Medium hazard scenarios	Number of High hazard scenarios	Number of Medium risk scenarios	Number of High risk scenarios
Natural gas control valve	2	0	0	-	-
Natural gas piping	1	0	0	-	-
Drain valve compressor	1	1	0	-	-
Oil chamber compressor	1	1	0	-	-
Drain valve accumulator	1	0	0	-	-
Rotor blades turbines	1	1	0	-	-
Rotor disk turbine	1	1	0	-	-
Gas compressor	7	-	-	0	0
Gas Turbine	10	-	-	3	0
Hot exhaust gases to boiler HRSG	7	-	-	6	1
Exhaust frame assembly	1	1	0	-	-
Exhaust diffuser assembly	1	1	0	-	-
Steam pressure indicator	1	0	0	-	-
Diverter valve	1	1	0	-	-
Boiler feed water control valve	1	1	0	-	-
Boiler feed water	7	-	-	3	0
Natural gas control valve	2	0	0	-	-

### 3.2 LOPA and SIL analysis

Based on the HAZOP analysis for medium and high risk result, and this paper, the GTG unit and HRSG unit were chosen to explain the LOPA and SIL. Nine scenarios for both units were evaluated as medium and high risk, as it is shown in Table 3.

Referring to Table 3, the eight medium risk scenarios and one high risk scenario with risk number between 8 - 16 in node scenario the boiler feed water and node scenario hot exhaust gases to HRSG boiler, these scenarios are explained detail as follows.

#### 3.2.1 Node: Air flow to gas turbine "Less", "More"

As it is shown in Table 3, for this scenario was considered severity of 2.25, this value severity level between low to medium, and a probability or frequency of 4 as probable level, so this event represents a risk of  $2.25 \times 4 = 9$ , this value as medium risk level.

The possible cause of this scenario is air filter clogging or a failure in the governor actuator, this condition would make it stay open, resulting in continue air feeding to gas turbine. This failure would no significant consequences, it would significant consequences to gas turbine interlock only. The existing safeguard that would control of this scenario, considering that initiating event frequency is 1E-01.

- "Less" flow, and the PFD for each of the IPLs was: BPD: 1E-01, BPCS: 1E-01, alarm: 1E-01, the overall event frequency:  $1E-01 \times 1E-01 \times 1E-01 \times 1E-01 = 1E-04$ .
- "More" flow, and the PFD for each of the IPLs was: BPD: 1E-01, BPCS: 1E-01, PSV: 1E-01, the overall event frequency:  $1E-01 \times 1E-01 \times 1E-01 \times 1E-01 = 1E-04$ .

Based on both of these value, it is observed that the hazard generated by this deviation is mitigated with the safeguards that exist already.

#### 3.2.2 Node: Flow boiler feed water "None", "Less"

As it is shown in Table 3, for this scenario was considered severity of 3, this value severity level is medium, and a probability or frequency of 4 as probable level, so this event represents a risk of  $3 \times 4 = 12$ , this value as medium risk level. The possible cause of this scenario is control valve clogging or a failure in the flow control valve due to instrument air supply fails, this condition would make it stay closed, resulting in a decrease or no water feeding to boiler. This failure would no significant consequences in the short term, for long period it would significant consequences to overheat and cracked as pin-hole of HRSG-Shell and Tube heat exchanger.

**Table 3.** Summary of HAZOP, LOPA, and SIL for Gas Turbine Generator and Heat Recovery Steam Generator

Node	P.P.	Dev	F	S	R	F <sub>i</sub>	IPLs PFD			EF (fi)	RL	TML	PFD <sub>ave</sub> [ $\frac{TML}{EF}$ ]	RRF [ $\frac{1}{PFD_{ave}}$ ]	Ratio LOPA	SIL for SIF	SIL
							BPD	BPC S	ALA	PSV							
Air to Gas Turbine	Flow	Less	4	2.25	9	1 E-1	1 E-1	1 E-1	1 E-1	-	M	3 E-3	30	3.33 E-2	> 1	0	-
Air to Gas Turbine	Flow	More	4	2.25	9	1 E-1	1 E-1	1 E-1	-	1 E-1	M	3 E-3	30	3.33 E-2	> 1	0	-
Boiler Feed Water	Flow	None	4	3	12	1 E-1	1 E-1	1 E-1	1 E-1	-	M	3 E-3	30	3.33 E-2	> 1	0	-
Boiler Feed Water	Flow	Less	4	3	12	1 E-1	1 E-1	1 E-1	-	-	M	3 E-3	1	1	> 1	1 E-1	SIL <sub>1</sub>
Boiler Feed Water	Temperature	Low	4	2.5	10	1 E-1	1 E-1	1 E-1	-	-	M	3 E-3	3	3.33 E-1	> 1	1 E-1	SIL <sub>1</sub>
Hot exhaust gases to HRSG Boiler	Flow	More	4	4	16	1 E-1	1 E-1	1 E-1	1 E-1	-	H	3 E-4	3	3.33 E-1	> 1	0	-
Hot exhaust gases to HRSG Boiler	Temperature	High	4	2	8	1 E-1	1 E-1	1 E-1	-	-	M	3 E-2	30	3.33 E-2	> 1	1 E-1	SIL <sub>1</sub>
Hot exhaust gases to HRSG Boiler	Pressure	Low	4	2	8	1 E-1	1 E-1	1 E-1	-	-	M	3 E-2	30	3.33 E-2	> 1	1 E-1	SIL <sub>1</sub>
Hot exhaust gases to HRSG Boiler	Pressure	High	4	2	8	1 E-1	1 E-1	1 E-1	-	1 E-1	M	3 E-2	300	3.33 E-3	> 1	0	-

Abbreviations: P.P = Process Parameter, Dev = Deviation, F = Frequency, S = Severity, R = Risk, Fi = Initial frequency / likelihood, BPD = Basic Process Design, ALA = Alarm, PSV = Process Safety Valve, EF = Event Frequency, RL = Risk Level (M: Medium, H: High), TML = Target Mitigation Likelihood, PFDave = average of Probability of Failure on Demand, RRF = Risk Reduction Factor, SIL = Safety Integrity Level, SIF = Safety Instrumented Function.

Recommendation to avoiding of this scenario is need to additional safeguard to install HRSG LL level alarm. The existing safeguard that would control of this scenario, considering that initiating event frequency is  $1E-01$ ,

- a. "None" flow, and the PFD for each of the IPLs was: BPD:  $1E-01$ , BPCS:  $1E-01$ , alarm:  $1E-01$ , the overall event frequency is  $1E-01 \times 1E-01 \times 1E-01 \times 1E-01 = 1E-04$ . Based on this value, it is observed that the hazard generated by this deviation is mitigated with the safeguards that exist already
- b. "Less" flow, and the PFD for each of the IPLs was: BPD:  $1E-01$ , BPCS:  $1E-01$ , the overall event frequency is  $1E-01 \times 1E-01 \times 1E-01 = 1E-03$ . Based on this value, to reach the overall event frequency of  $1E-04$ , it is necessary a SIL 1 of PFD  $1E-01$  must be implemented. Installing LL level alarm together with a low-temperature indicator PFD  $1E-01$  would reduce the overall event frequency to  $1E-04$ .

### 3.2.3 Node: Temperature boiler feed water "Low"

As it shown in Table 3, for this scenario was considered severity of 2.5, this value severity level is between low to medium, and a probability or frequency of 4 as probable level, so this event represents a risk of  $2.5 \times 4 = 10$ , this value as medium risk level. The possible cause of this scenario is the economizer fouling increased, this condition would make heat transfer process in economizer to boiler feed water decrease. This failure would no significant consequences, it would significantly to decrease of steam produced. The existing safeguard that would control of this scenario, considering that initiating event frequency is  $1E-01$ , and the PFD for each of the IPLs was: BPD:  $1E-01$ , BPCS:  $1E-01$ , the overall event frequency is  $1E-01 \times 1E-01 \times 1E-01 = 1E-03$ . To reach the overall event frequency EF of  $1E-04$ , it is necessary a SIL 1 of PFD  $1E-01$  must be implemented. The recommendation to avoiding this scenario consider to installing LL temperature alarm together with a low-temperature indicator PFD  $1E-01$  would reduce the overall event frequency to  $1E-04$ .

### 3.2.4 Node: Flow hot exhaust gases to HRSG boiler "More"

As it is shown in Table 3, for this scenario was considered severity of 4, this value severity level is critical, and a probability or frequency of 4 as probable level, so this event represents a risk of  $4 \times 4 = 16$ , this value as high risk level. The possible cause of this scenario is diverter valve fails to open or a failure in the diverter valve operation due to stucked of very hot gases, this condition

would make it stay closed, resulting in all hot exhaust gases feeding to boiler. This failure would no significant consequences in the short term, for long period it would significant consequences to overheat and cracked as pinhole of HRSG-Shell and Tube heat exchanger. Recommendation to avoiding of this scenario is need consider to installation of diverter valve with high performance to keep reliability.

The existing safeguard that would control of this scenario, considering that initiating event frequency is  $1E-01$ , and the PFD for each of the IPLs was: BPD:  $1E-01$ , BPCS:  $1E-01$ , alarm:  $1E-01$ , the overall event frequency is  $1E-01 \times 1E-01 \times 1E-01 \times 1E-01 = 1E-04$ . Based on this value, it is observed that the hazard generated by this deviation is mitigated with the safeguards that exist already.

### 3.2.5 Node: Temperature hot exhaust gases to HRSG boiler "High"

As it shown in Table 3, this scenario was considered severity of 2, this value severity level is minor, and a probability or frequency of 4 as probable level, so this event represents a risk of  $2 \times 4 = 8$ , this value is as medium risk level. The possible cause of this scenario is gas turbine in maximum load operation in long period, resulting the excess of exhaust gases feeding to boiler. This failure would no significant consequences in the short term, for long period it would significant consequences to overheat and cracked as pinhole of HRSG-Shell and Tube heat exchanger.

The existing safeguard that would control of this scenario, considering that initiating event frequency is  $1E-01$ , and the PFD for each of the IPLs was: BPD:  $1E-01$ , BPCS:  $1E-01$ , the overall event frequency is  $1E-01 \times 1E-01 \times 1E-01 = 1E-03$ . Based on this value, to reach the overall event frequency of  $1E-04$ , it is need a SIL1 of PFD  $1E-01$  must be implemented. Installing HH temperature indicator and alarm with PFD  $1E-01$  would reduce the overall event frequency to  $1E-04$ .

### 3.2.6 Node: Pressure hot exhaust gases to HRSG boiler "Low" High"

As it is shown in Table 3, this scenario was considered severity of 2, this value severity level is minor, and a probability or frequency of 4 as probable, so this event represents a risk of  $2 \times 4 = 8$ , this value as medium risk level.

- a. The first of possible cause of this scenario "Low" pressure hot exhaust gases to HRSG boiler is too low load operation of gas turbine, this condition would make turbine blades very slow spin, the resulting is low pressure steam generated.



- b. The existing safeguard that would control of this scenario, considering that initiating event frequency is  $1\text{E-}01$ , “Low” pressure hot exhaust gases to HRSG boiler, and the PFD for each of the IPLs was: BPD:  $1\text{E-}0$ , BPCS:  $1\text{E-}01$ , the overall event frequency is  $1\text{E-}01 \times 1\text{E-}01 \times 1\text{E-}01 = 1\text{E-}03$ . Based on this value, to reach the overall event frequency of  $1\text{E-}04$ , it is necessary a SIL 1 of PFD  $1\text{E-}01$  must be implemented. Installing LL pressure alarm together with a high-temperature indicator and high-pressure indicator with PFD  $1\text{E-}01$  would reduce the overall event frequency to  $1\text{E-}04$ . The second of possible cause of this scenario “High” pressure hot exhaust gases to HRSG boiler is too high load operation of gas turbine, this condition would make turbine blades very fast spin, the resulting is high pressure steam generated.

The existing safeguard that would control of this scenario, considering that initiating event frequency is  $1\text{E-}01$ , “High” pressure hot exhaust gases to HRSG boiler, and the PFD for each of the IPLs was: BPD:  $1\text{E-}01$ , BPCS:  $1\text{E-}01$ , PSV:  $1\text{E-}01$ , the overall event frequency is  $1\text{E-}01 \times 1\text{E-}01 \times 1\text{E-}01 \times 1\text{E-}01 = 1\text{E-}04$

Based on this value, it is observed that the hazard generated by this deviation is mitigated with the safeguards that exist already.

Combined method risks analysis as above results almost was similar result on boiler HAZOP and SIL analysis [13]. It means the risks of operation of HRSG in the combined heat and power unit with operation of the standard heat exchanger boiler were found the similar phenomenon. The previous two similar cases study with method HAZOP, LOPA and SIL, the result mostly was medium level of risks and mitigation with PFD SIL 1 [11][12].

The basic process design of combined heat and power unit and heat exchanger boiler unit have installed the appropriate SIL on safety instrumented function, therefore even though the facility have operated in long service, the mitigated with safeguards that exist already. Considering of turbine blades very fast spin in gas turbine and the resulting of high pressure steam and hot exhaust gases temperature, SIL of SI in this facility requires to one step upgrade by additional with PFD SIL 1.

#### 4. CONCLUSION

The hazards and risks associated in gas compressor, accumulator, gas turbine generator, and economizer, in this paper summary had explained detail. The scenario represented a significant risks are medium and high risk level, it was necessary to reduce the overall frequency of the event. One scenario was found as high-risk, this scenario related to high temperature of hot exhaust gases to HRSG boiler. This high temperature can be mitigated by

installation HH temperature indicator and alarm to reach a lower overall event frequency for this scenario. Even though this scenario can be mitigated by installation of safety software system, temperature indicator alarm, but other safeguards is needed, it was include of response of operators in operations.

#### REFERENCES

- [1] Anson Elian dan Bambang Arip Dwiyanoro 2017 Perancangan Termal Heat Recovery Steam Generator Sistem Tekanan Dua Tingkat Dengan Variasi Beban Gas Turbin, Engineering, Jurnal Teknik ITS.
- [2] Vernon L. Eriksen 2017 Woodhead Publishing is an imprint of Elsevier Series in Energy, Heat Recovery Steam Generator Technology.
- [3] The U.S. Chemical Safety Board 2010 U.S. Chemical Safety and Hazard Investigation Board. <https://www.csb.gov/userfiles/file/final%20urgent%20recommendation%20small.pdf> Accessed 14 July 2014.
- [4] Aaron Davis 2017 Explosion shuts down Pittsburg power plant <https://www.eastbay-times.com/2017/01/30/explosion-shuts-down-pittsburg-power-plant/> Accessed 14 July 2014.
- [5] Ronny Dwi Noriyati 2018 Kombinasi Metode Layer of Protection Analysis and Fault Tree Analysis Berbasis Model Dinamika Process Plant: Case Study on Process Steam Drum Boiler, Disertasi, Teknik Elektro ITS.
- [6] Lassen, C A 2008 Layer of protection analysis for determination of safety integrity level. Norwegian: The Norwegian University of Science and Technology.