Functional Safety Assessment of the Safety Protection System Based on Petri Net

Peng Wang*, Mengyuan Hu

College of Electronic Information and Automation, Tianjin University of Science and Technology, 300222, China

*E-mail: *1090465299@qq.com*

www.tust.edu.cn

Abstract

In this paper, the functional safety evaluation of the safety protection system of gasoline hydrogenation unit was carried out using Petri net. Firstly, the principle and framework of the gasoline hydrogen refueling unit was described. Secondly, the safety integrity level was introduced, and the influencing factors of the safety integrity level were summarized. Thirdly, the Petri net model and the Markov model are compared and the Petri net model is used to verify its security integrity level. Finally, the calculation result demonstrated that the SIL did not reach the target level, and then reached the target level after improvement. This analysis method can provide reference for the safety integrity level evaluation of similar devices.

Keywords: Gasoline hydrogenation, Petri net, Functional safety assessment

1. Introduction

With the passage of time, modern science and technology continue to develop, the number of vehicles climbed. The sulfides produced by automobile exhaust have a great impact on air quality. Therefore, the production of clean gasoline is very important for environmental protection. In response to this problem, we have proposed the hydrogenation of gasoline. The purpose of gasoline hydrogenation is to desulfurize at a small octane loss. Gasoline hydrogenation equipment is a device used for filling the car fuel tank, which includes liquid level sensors, flowmeters, valves and other equipment. Because it is usually operated in high temperature, high pressure and hydrogen environment, there are safety risks, which requires us to do a good job of safety protection, equipped with safety instrument system. Safety instrument system is composed of sensor logic controller and actuator, it can perform one or more absolute safety control instrument functions. Petri networks, which can intuitively describe the relationship between system states and events, are widely applied in many fields. Therefore, the functional safety assessment of the safety protection system of the gasoline hydrogenation unit based on Petri network is a topic worth discussing.

The rest of this article is organized as follows. The second section introduces the research status at home and abroad about the gasoline hydrogenation technology and the safety analysis. In the third part, the gasoline hydrogenation unit is presented. In the fourth section, a example is given to analysis the risk of facility. In the fifth part verifies and improves the safety integrity level of gasoline hydrogenation unit. The sixth part summarizes the main content of this paper.

2. Research Status at Home and Abroad

2.1. Research status of gasoline hydrogenation technology

At present, most of the catalytic raw materials selected by the manufacturers in China have the problem of excessive metal content, as well as excessive sulfur content and non-hydrocarbon components. These problems will not only cause the decline of product quality in the gasoline production process, but also cause the problem of environmental pollution in view of the existence of many

sulfur and other elements in the production process. In the production process, using diolefin saturation treatment can effectively reduce the occurrence of olefin coking phenomenon; in addition, in the relatively mild reaction environment, the influence of impurities can be further reduced, so as to reduce the octane value factors and losses, and better meet the relevant national technical standards and production requirements.

2.2. Research status of safety analysis

The gasoline hydrogenation equipment of a chemical plant in China uses a set of independent safety instrument system (SIS) for safety control. Its process is complex, and the operating environment is high temperature and high pressure, involving flammable and explosive gases, which requires close monitoring. Since its launch, the application of SIS system has significantly improved the stability and reliability of the equipment, realized safe, stable and efficient operation, avoided the occurrence of equipment shutdown and failure problems, at the same time brought economic benefits to the enterprise, but also guaranteed the personal safety of workers.

2.3. Application of petri network in system security analysis

Petri was first proposed by Kal Adam Peri. Petri network represents the system model in the form of a mesh structure model. Petri network is a visual mathematical modeling tool that contains elements such as place, transition, arc and token, which can represent the static function and structure of the system. In addition, Petri networks combine data flow, control flow, and various logical relationships to support a more rich and complex system modeling, allowing for a better analysis of the dynamic behavior of a specific system.

3. Analysis of the Gasoline Hydrogenation Unit

The raw oil is introduced into the filter through an external device, and the purpose of the overall filtration is to separate the particles in the raw material. Among them, after the large particles are removed, they enter the selective hydrogenation feed equipment. The feed can be used as a way to select the hydrogenation reactor feed pump to control the flow rate to achieve a reasonable effect, and then use the supplementary hydrogen mixing mode to form a mixed feed. First, the mixture is sent to the selective hydrogenation reaction device, and the heat exchange is carried out by means of the hydrodesulfurization reaction. The heating is stopped after the temperature is repeatedly raised to a suitable temperature. Next, the diene to olefin reaction is carried out to meet the requirements. In order to ensure the smooth progress of the whole reaction process, we introduce the catalyst under suitable catalytic conditions for the reaction. After the reaction is completed, we will use a tandem selective hydrogenation reactor to reprocess the product. Through the hydrogenation static desulfurization treatment, and the selective hydrogenation reaction redox reaction, the heat exchange is finally realized through the heat exchanger, and then after the treatment of the catalyst, the saturated state of the olefin product is successfully obtained.

During this process, the reactant is reinjected into the heat exchanger for heat exchange. When it reaches a certain extent, the subsequent reaction of the reactants can be continued. By adjusting the temperature and the interaction of the catalyst, they enter the second reactor for desulfurization treatment, and the catalyst can efficiently achieve the requirement of complete desulfurization. The product of hydrodesulfurization reaction enters the heat separation tank after heat exchange, and the gas phase is added to the product cold separation tank and circulating cleaning equipment after air cooling and cooling of the desulfurization reaction. After the treatment of desulfurization and hydrogenation reaction, the obtained product will be transported to the separation tank after gas phase cooling. In the separation tank, part of the oil phase material will be separated. After it is stable, the non-condensable gas will be transported to the liquid separation tank for further treatment. The separated liquid is discharged after condensation treatment through the condenser, and some of the gas is sent to the gas-liquid separator to mix with water vapor and return to the heat exchanger to continue heating. Then, the product after pressure stabilization treatment is transported to the absorption tower, and then processed again by the liquid separation equipment of the circulating hydrogen compressor. After the mixed hydrogen treatment, it meets the needs of desulfurization production.

4. Device Risk Analysis

4.1. Confirmation of the SIL level

Safety Integrity Level is a measure of the safety of safety instrument system and enterprise safety instrument system management level, its value represents the order of risk

reduction level. The three foundations for determining the level of security integrity are: structural constraints, system capabilities, and hardware security integrity. The safety integrity of hardware mainly depends on the reliability of hardware in the case of dangerous failure. The influence of these factors mainly includes the failure model, system structure, functional test cycle and component reliability level. In the IEC61508 standard, the safety integrity level is divided into four levels, and the operation mode of the system is divided into low requirement operation mode and high requirement operation mode. In the low requirement operation mode, the SIL level is based on the average failure probability, while in the high requirement or continuous operation mode, the SIL level is based on the average failure probability per hour. The requirements for SIL levels for different operating modes, which are shown in Table 1and Table 2.

Table 1 The SIL level for the low-requirement operation mode

Low-required operation mode		
Safety integrity level （SIL）	Average probability of failure on demand （PFD_{avg}）	Risk reduction factor （RRF）
4	10^{-4}~10^{-5}	10000~100000
3	10^{-3}~10^{-4}	1000~10000
2	10^{-2}~10^{-3}	100~1000
1	10^{-1}~10^{-2}	10~100

Table 2 The SIL level for the high requirement operation mode

The SIL level for the high requirement operation mode	
Safety Integrity Level （SIL）	Meverage hourly failure probability PFH_{avg}
4	10^{-8}~10^{-9}
3	10^{-7}~10^{-8}
2	10^{-6}~10^{-7}
1	10^{-5}~10^{-6}

The SIS system is more focused on monitoring whether there are risk conditions in the production process and reducing the possibility of risk occurrence. The scheme is a passive system, which is generally in a non-dynamic state. Only when necessary, it will play a role and will not actively participate in the normal operation of the basic process control system. The safety life cycle covers the entire period from the conceptual design of the project to the discontinuation of SIF. Under certain time and conditions, the possibility of safety-related systems performing their prescribed safety functions can be called safety integrity level (SIL), which represents the level of reducing the risk of safety instrumented systems. It is very important to select the appropriate SIL level. If the selection is too high, it will cause cost waste, and if it is too low, it will bring unacceptable risks. According to the IEC61508 standard, SIL4 level is the highest and SIL1 level is the lowest.

4.2. Influencing factors of safety integrity level

- Failure mode
- Redundant structure
- Common cause failure
- Diagnostic coverage rate
- Periodic function test
- Maintenance mode

4.3. Safety integrity level verification

Hardware security integrity is a part of the overall security integrity of SIS, and its influencing factors include failure mode, component failure rate and detection cycle. When evaluating an interlocking circuit, it is necessary to determine its failure probability to determine its SIL level. Finally, the SIL verification results are compared with the grading analysis results to verify whether the circuit meets the requirements. In order to meet the requirements of SIL grading analysis, it is necessary to reset the layout structure, component selection, redundant design and maintenance plan of the interlocking loop. IEC standard provides a variety of methods to verify SIL level, including simple formula method, reliability block diagram method, fault tree analysis method and Markov model method.

For the transition of the system state, the Markov model is represented by a circle and an arrow, which represent the state of the system and the transition between states, respectively. The Markov model of the 1oo1 structure is shown in Fig. 1.

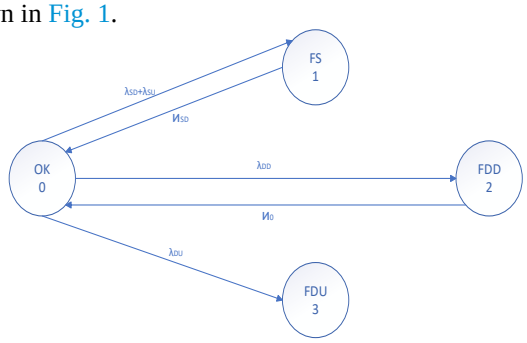

Fig.1. 1oo1 redundant structure Markov model

The state transition matrix of 1oo1 redundant structure is P [1].

$$P=\begin{bmatrix} 1-(\lambda_s+\lambda_D) & \lambda_{SD}+\lambda_{SU} & \lambda_{DD} & \lambda_{DU} \\ \mu_{SD} & 1-\mu_{SD} & 0 & 0 \\ \mu_0 & 0 & 1-\mu_0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (1)$$

To calculate the mean time between failures, you can use the system state transition diagram, the system state transition diagram is shown in Fig. 2.

Fig.2 1oo1 structure Markov model (MTTFS)

The corresponding matrix is:

$$Q'=1-(\lambda_{SD}+\lambda_{SU}) \quad (2)$$

And because:

$$N=\left[I-Q'\right]^{-1} \quad (3)$$

Therefore:

$$N=\frac{1}{\lambda_{SD}+\lambda_{SU}} \quad (4)$$

The sum of the elements of the N rows of the matrix is the result of MTTFS:

$$MTTF=\frac{1}{\lambda_{SD}+\lambda_{SU}} \quad (5)$$

The formula of system dangerous failure probability is:

$$PFS=S_0P^{8760}\begin{bmatrix}0 & 1 & 0 & 0\end{bmatrix}^T \quad (6)$$

The formula of system safety failure probability is:

$$PFD=S_0P^{8760}\begin{bmatrix}0 & 0 & 1 & 1\end{bmatrix}^T \quad (7)$$

Markov model is a model that can represent the dynamic behavior of the system. It can consider multiple reliability factors, and multiple reliability indexes can be obtained by one modeling. However, it will face problems such as space explosion. Especially when the complexity of the system increases, the difficulty of this method will increase greatly.

The stochastic Petri net is used to analyze the hardware failure probability, which solves the problem of Markov state explosion, reveals the dynamic characteristics of the system, and can evaluate the hardware safety integrity of the safety instrumented system.

5. Verification of safety integrity level of gasoline hydrogenation unit

In this section, SIL is evaluated for one of the dangerous scenarios SIF5 of the gasoline hydrogenation unit. The main fuel gas of the fractionator reboiler F9101 of SIF5 is selected to set low pressure and low PSLL6049 A / B / C (2oo3) interlock shutdown XV6011 as a representative. In this process, the components to be considered are as follows.

- SIF serial number:SIF5
- Accident scenario： The pressure of F9201 fuel gas in the hydrodesulfurization heating furnace is too low, which leads to the extinction of the main nozzle. If the fuel gas continues to enter the furnace, the furnace explosion accident may occur.
- Consequence description:The pressure of F9201 fuel gas in the hydrodesulfurization heating furnace is too low, which leads to the extinction of the main nozzle. If the fuel gas continues to enter the furnace, the furnace explosion accident may occur.
- SIF function description:F9101 main fuel gas setting pressure is low PSLL6049A / B / C (2oo3) interlock closed XV6011.
- SIL target: SIL2

In this process, the components to be considered include as shown in Table 3.

Table 3 Components to be considered for SIF5

Sensor Part Pressure Sensor	PSLL6049A / B / C (2oo3)
	Safety barrier (1oo2)
Logic controller part	PLC（2oo3）
	Relay 1 (1oo1)
Actuator	Emergency Shut-off Valve XV6011 (1oo1)
	Relay 2 (1oo1)

In order to evaluate random hardware failures, complete failure data of systems and components are required, considering functional test cycles and common cause failures. These factors will be included in the evaluation category in order to more accurately determine the random hardware failure probability of the system, and then evaluate its hardware security integrity level. The failure

probability of the system needs to meet the system requirements.

$$PFD_{avg} = PFD_{avg\ sensor} + PFD_{avg\ PLC} + PFD_{avg\ actuator} \quad (8)$$

The relay 1, relay 2, emergency cut-off valve and solenoid valve are all 1oo1 redundant structure, while the safety gate is 1oo2 redundant structure to ensure the stability and reliability of the system. Based on the Petri net model, the average failure probability of the emergency shut-off valve is calculated.

The state transition matrix Q is :

$$Q = \begin{bmatrix} -7.48\times10^{-6} & 2.34\times10^{-6} & 4.73\times10^{-6} & 4.13\times10^{-6} \\ 5.71\times10^{-5} & -5.71\times10^{-5} & & \\ 0.04167 & & -0.04167 & \\ 0.125 & & & -0.125 \end{bmatrix} \quad (9)$$

Equation solving:

$$\begin{cases} XQ = 0 \\ \sum_{i} Xi = 1, 1 \le i \le n \end{cases} \quad (10)$$

Solution:

$$PFD_{avg\ Cut\text{-}off\ valve} = 1.98\times10^{-2}$$
$$PFD_{avg\ Relay\ 1} = 2.455\times10^{-6}$$
$$PFD_{avg\ Solenoid\ valve} = 7.454\times10^{-4}$$
$$PFD_{avg\ Safety\ barrier} = 7.902\times10^{-4}$$
$$PFD_{avg\ Relay\ 2} = 2.5164\times10^{-6}$$

PLC,the system sensor is a 2oo3 redundant structure, and the reachability diagram of the 2oo3 structure Petri net is shown in Fig. 3.

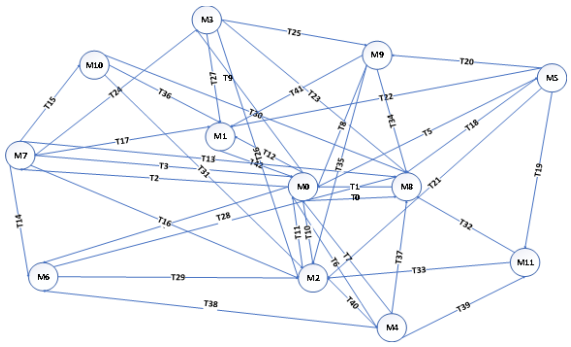

Fig. 3 2oo3 structure reachable graph

The state matrix is:

$$Q = \begin{bmatrix} -0.125 & 4.38\times10^{-7} & 6.54\times10^{-7} & 1.75\times10^{-6} & 2.62\times10^{-6} & 1.81\times10^{-6} \\ 5.71\times10^{-5} & -5.71\times10^{-5} & 0 & 0 & 0 & 0 \\ 0.125 & 0 & -0.125 & 0 & 0 & 0 \\ 0 & 1.31\times10^{-6} & 1.97\times10^{-6} & -6.66\times10^{-6} & 0 & 0 \\ 0.125 & 0 & 3.28\times10^{-6} & 0 & -0.125 & 0 \\ 0 & 1.46\times10^{-7} & 2.18\times10^{-7} & 0 & 0 & -6.66\times10^{-6} \\ 0 & 0 & 1.82\times10^{-6} & 0 & 0 & 0 \\ 2.71\times10^{-6} & 1.46\times10^{-7} & 2.18\times10^{-7} & 0 & 0 & 0 \\ 0.0417 & 0 & 0 & 0 & 0 & 0 \\ 0.125 & 7.28\times10^{-7} & 1.08\times10^{-6} & 0 & 0 & 0 \\ 0 & 7.28\times10^{-7} & 1.08\times10^{-6} & 0 & 0 & 0 \\ 0 & 0 & 1.82\times10^{-6} & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0.125 & 2.71\times10^{-6} & 1.13\times10^{-6} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1.80\times10^{-6} & 3.76\times10^{-6} & 1.20\times10^{-6} & 0 & 0 \\ 1.80\times10^{-6} & 0 & 3.76\times10^{-6} & 0 & 0 & 1.20\times10^{-6} \\ 0 & 0 & 3.38\times10^{-6} & 1.16\times10^{-6} & 0 & 1.75\times10^{-6} \\ -3.7\times10^{-6} & 0 & 1.88\times10^{-6} & 0 & 0 & 0 \\ 1.75\times10^{-6} & -9.37\times10^{-6} & 3.88\times10^{-6} & 0 & 1.16\times10^{-6} & 0 \\ 0 & 0 & -0.0417 & 0 & 0 & 0 \\ 0 & 0 & 1.88\times10^{-6} & -0.125 & 0 & 0 \\ 0 & 0 & 1.88\times10^{-6} & 0 & -3.69\times10^{-6} & 0 \\ 0 & 0 & 1.88\times10^{-6} & 0 & 0 & 3.7\times10^{-6} \end{bmatrix} \quad (11)$$

Equation solving:

$$\begin{cases} XQ = 0 \\ \sum_{i} Xi = 1, 1 \le i \le n \end{cases} \quad (12)$$

Solution:

$$PFD_{avgPLC} = 1.21\times10^{-6}$$
$$PFD_{avg\ sensor} = 2.3\times10^{-4}$$

Then $PFD_{SIS} = PFD_{avg\ cut\text{-}off\ valve} + PFD_{avg\ relay1} + PFD_{avg\ solenoid\ valve} + PFD_{avg\ relay2} + PFD_{avg\ safety\ barrier} + PFD_{avg\ PLC} + PFD_{avg\ sensor} = 2.15\times10^{-2}$, which does not meet the SIL2 requirements and needs to be adjusted. It can be seen from Table 3-10 that the shut-off valve has the greatest influence on the total PFD of the equipment is the shut-off valve,which is shown in Table 4.

Table 4 The contribution of subsystem to system PFD

Systematic name	Proportion of impact on PFD
Cut-off valve	90%
Solenoid valve	3%
Pressure sensor	4%
Safety barrier	3%

Therefore, we can take the transformation of the emergency shut-off valve and increase the emergency shut-off valve group to realize the transformation from the 1oo1 structure to the 1oo2 redundant structure. After the transformation, the $PFD_{avg\ shut\text{-}off\ valve'} = 4.36\times10^{-3}$. After the transformation, $PFD_{SIS} = PFD_{avg\ shut\text{-}off\ valve'} + PFD_{avg\ relay1} + PFD_{avg\ solenoid\ valve} + PFD_{avg\ relay2} + PFD_{avg\ safety\ barrier} + PFD_{avg}$

$_{PLC}$ + $PFD_{avg\ sensor}$ = 6.13×10^{-3}, which meets the SIL2 safety requirements.

6. Conclusion

In recent years, China has paid more and more attention to production safety, and the government has also issued relevant policies and regulations for industries with high risks. In this context, the automation level of China 's petrochemical enterprises has been continuously improved, which provides good conditions for ensuring production safety. Driven by the policy, with the superposition of new facilities and demand and the increase in the demand for facilities upgrading, SIS system will be more widely used and play a vital role in today 's society and the country. The main conclusion of this paper is that the security level of the system depends on many factors, among which structural constraints, system capability and hardware security integrity level are crucial factors. In order to ensure the safe operation of the system, it is necessary to make reasonable analysis and judgment on these factors. Explore a variety of factors that affect the functional safety of safety instrumented systems, and use Petri net models to model and optimize them, so as to improve the level of safety instrumented systems.

References

1. Guo H, Yang X. Automatic creation of Markov models for reliability assessment of safety instrumented systems. Reliability Engineering & System Safety, 2008, 93(6):829-837.

Authors Introduction

Ms. Peng Wang

She is a postgraduate tutor of Tianjin University of Science and Technology. In 2014, she received a doctorate from North China Electric Power University. The research direction is the functional safety assessment of safety instrumented systems.

Ms. Mengyuan Hu

In 2023, she received her Bachelor of Engineering degree from the School of Electronic Information and Automation, Tianjin University of Science and Technology, China.She is pursuing a master's degree in engineering from Tianjin University of Science and Technology.