Proceedings of the 13th International Forum of Automotive Traffic Safety, 2016, pp 212- 217
No. ATS.2016.314

Application ofFunctional Safety Theories in Furnace Safety Supervisory System

Peng Wang[1],Xiaoyan Chen[1], Lei Yu[2]
[1]*College of Electronic Information and AutomationTianjin University of Science&Technology*
Tianjin300222, China
[2] *Tianjin Railway Technical and Vocational College, Tianjin300240, China*

Abstract: Furnace safety supervisory system (FSSS)plays an important role in protecting the boiler of thermal power plant from danger. In order to evaluate the performance of FSSS itself, functional safety theoriesare applied in this papertoachieve hazard and risk analysis, target safety integrity level (SIL)determinationand functional safety evaluation. The most important safety instrumented function (SIF) of FSSS --master fuel trip (MFT) is considered, and the probability of failure on demand (PFD) is calculated based on the method of fault tree analysis (FTA). According to the analysis result,target SILfor FSSS is 2,but the actual system does not meet the requirement. Through corrective measures of making one-out-of-two (1oo2) redundant configuration for each actuator and compressing the functional testing cycle, the safety index of MFT ultimately reaches the target value.

Keywords:furnace safety supervisory system(FSSS); master fuel trip (MFT); safety instrumented system (SIS); safety integrity level (SIL); functional safety evaluation

1 Introduction.

The rapid industrial development has brought enormous benefit, butmeantime caused a lot of disasters. In the process industry, safety instrumented system (SIS) has been widely used for secure protection and disaster mitigation[1-4]. To ensure the effective implementation of safety functions for SIS, functional safety analysis techniques emerged. In2000, the international electrotechnicalcommission (IEC) published IEC61508 standard [5], which is a breakthrough in functional safety studies. After that, international safety standards for specificapplication areaswerereleasedin succession[6-8]. The development and application of SISare mainly around two themes-- safety instrumented function (SIF) and functional safety. SIF means the protective measure to prevent froma potential hazardous event. Functional safetyrepresents the ability of executing the SIF.

Furnace safety supervisory system (FSSS) is an interlocking protection system in thermal power plant, whichcan effectively reduce deflagration, explosion and other destructiveaccidents [8-10]. However, safety analysis and evaluationrequirements of FSSSare not includedin related design standards or regulations,which lead to great security risk. In view of this, functional safety theories are applied to evaluate FSSS in this paper. Firstly, the working principleand basic constructionof FSSS are introduced; Secondly,the target Safety Integrity Level (SIL)of FSSS is determined by conducting a hazard and risk analysis; Thirdly, according to a specific safety instrumented function-- master fuel trip (MFT), reliability analysis model is established, and the safety performance indexes are calculated; Finally, in contrast with the target SIL, reasonable corrective measures are proposed[11-12].

2. Working principle of FSSS.

FSSS plays an important rolein automatic protection and controlforthermal power plant.FSSS integrates combustion controlandsecurity protection functions,and monitors the boiler at all stages. Once dangerous situations emerge, FSSS will take measures to ensure the normal operation of combustion equipments and the safety of operators.

Combustion control system (CCS), as the basic process control system (BPCS), is used toensure the continuous and stable

combustionstate; FSSS, as the safety instrumented system (SIS), is used toobtain security protection.Therelationship between the two systems is shown in Figure 1.

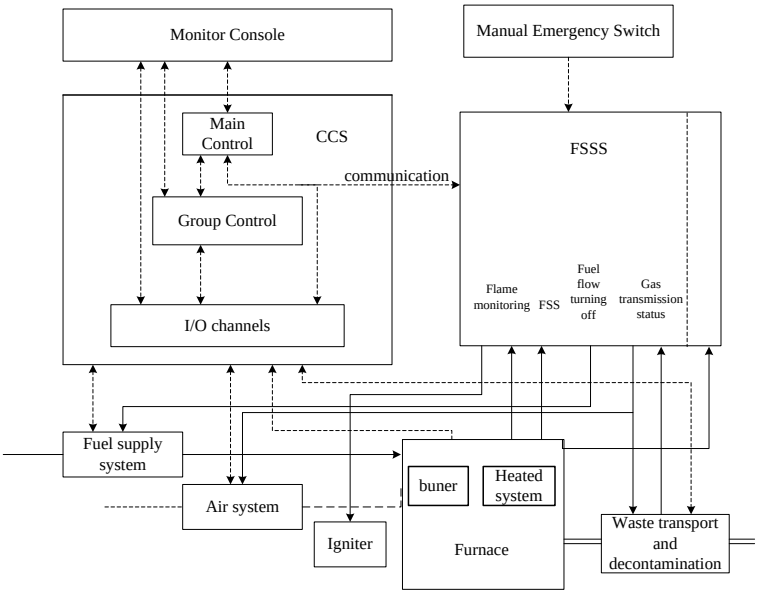

Figure 1.Configuration of FSSS

3.Hazard and risk analysis.

The unsafe working conditionsof furnace are deflagration or explosion. Deflagration is the phenomenon that combustible materials accumulated in the furnace, flue, and ventilation ducts are ignitedsimultaneously, causinga significant increase of the furnace pressure.Serious deflagration is explosion.

Power industry internal data shows thatfurnace explosion occurred two times in the last 10 years, causing economic losses between1 million yuan and5 millionyuan, and no casualties. According to the accident consequences and occurrence likelihood classifications, shown in Table 1 and Table 2, consequenceand occurrence likelihood of furnace explosionare light and high, respectively.Based on the above analysis results and the risk matrix, shown in Figure 2, thetargetSIL of FSSS is 2.

Table 1.Classifications of accidents consequences

Severity	Description
Lighter	Impact is only restricted in the local area at the beginning,if don't take appropriate protective measures, it may lead to serious consequences.
Serious	Maybe result in serious injury or death.Economic losses is between1 million yuan and5 millionyuan around the accident place.
Particularly serious	Five times more than "serious" level.

Table 2. Classifications of accidents probabilities

Possibility	Description
low	Accident frequency is smaller than 10^{-4} per year.
medium	Accident frequency is between 10^{-4}per year and 10^{-2} per year
high	Accident frequency is above 10^{-2} per year

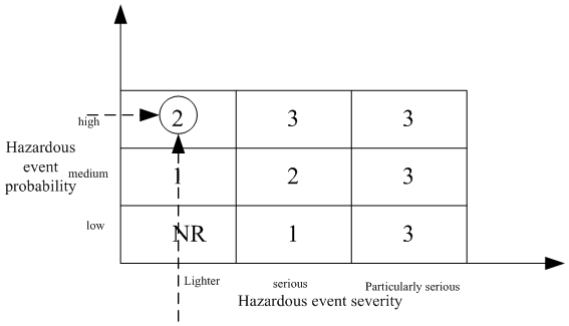

Figure 2.Risk matrix

4. Functional safety evaluation of safety instrumented functions.

Take the most important safety instrumented functionof FSSS-- Master fuel trip (MFT)for example, and functional safety evaluation of FSSS is carried out.

4.1.Function realization of MFT.

MFT is the core safety function of FSSS.When hazardous cases which may result in serious consequences occur, it is necessary to cut off all fuel into the furnace to achieve MFT function, shown in Figure 3. MFT triggering signal is input DCS logic processing unit and logic operations are implemented. On the one hand, equipment outage signal is sent directly to the field device through corresponding interlock system, achieving"soft" control;on the other hand, trip commandsaresent to MFT hard trip circuit to stop related equipments, achieving "hard" control. By this way,the reliability of MFT is improved.

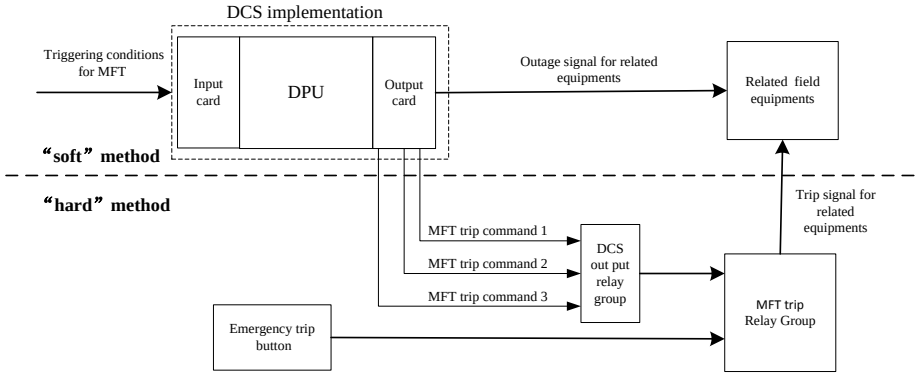

Figure 3.Trip principle of MFT

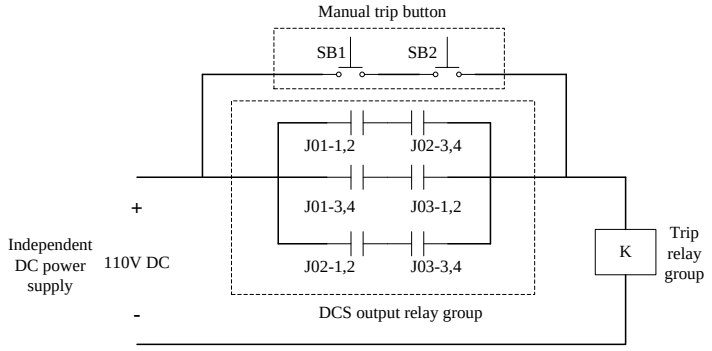

Figure 4.MFT trip circuits in positive logic mode

MFT hard trip circuit consists of DCS output relay group, MFT trip relay group and manual trip buttons, and supplied by DCS power or separate power. DCS output relay group adopt 2 out of 3connecting mode, driven by three MFT trip signal from DCS.According to the actual design of a certain power plant, MFT hard trip circuits in positive logic mode are shown in Figure 4.

4.2.Constitution of SIS.

SIS is an instrumented system used to perform one or more SIFs, consisting ofsensors, logic controllers and actuators. SIF is performed by SIS, and each SIF has a certain Safety Integrity Level (SIL).

TakingMFT triggeredwhen the wind is Less than 30% for example, signal flow diagram of the SIF is shown in Figure 5.

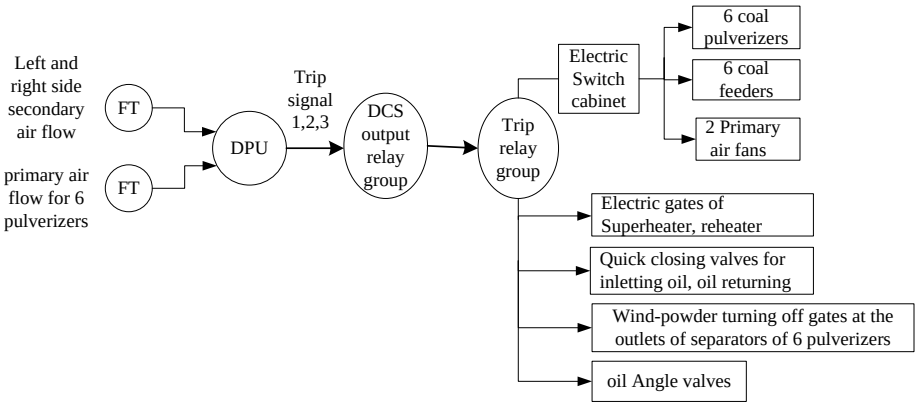

Figure 5.Signal flow diagram of low air trip MFT

4.3. Determination of SIL.

Safety Integrity Level (SIL) refers to the probability that SISsuccessfully implements required safety functions under specified conditions, and during specified time.There are clear descriptionsabout the target failure probability corresponding to different SILsin two operating modes in IEC 61508, as shown in Table 3.

Table 3.Safety integrity levels in two modes

	Low demand operation mode	High demand or continuous operation mode
SIL	Probability of failure on demand (PFD_{avg})	Probability of failure per hour (PFH)
4	$10^{-4}\sim10^{-5}$	$10^{-8}\sim10^{-9}$
3	$10^{-3}\sim10^{-4}$	$10^{-7}\sim10^{-8}$
2	$10^{-2}\sim10^{-3}$	$10^{-6}\sim10^{-7}$
1	$10^{-1}\sim10^{-2}$	$10^{-5}\sim10^{-6}$

Failure modescan be classifiedinto safe failure and dangerous failure, considering self-diagnosis capability and common cause failure, can also be further divided. Establish dangerous failure fault tree for MFT triggered when the wind is Less than 30%, shown in Figure 6. Failure rates (unit:10-9h^{-1}) of different componentsare shown in Table 4,including safe detected failure rateλSD, safe undetected failure rateλSU, dangerous detected failure rateλDD, dangerous undetected failure rate λDU.For redundant structures,the corresponding common cause failure factorβ are listed,and the average probabilities of failure on demand of different components are calculated.Assume that the functional testing cycle TI is one year,and average repair time RT is 8 hours.

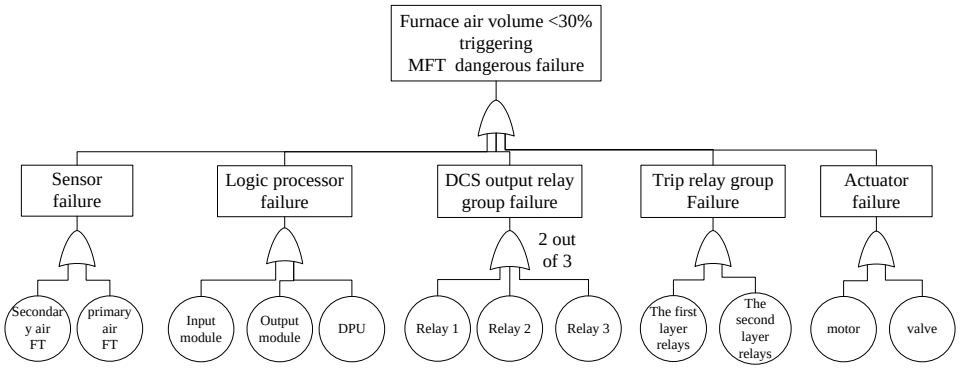

Figure 6.Dangerous failure fault tree of low air trip MFT

Table 4. Failure rates of components

components	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	β	PFD_{avg}
Secondary air flow transmitter (FT)	0	593	1886	172	0.1	2.324×10^{-4}
Primary air flow transmitter (FT)	0	593	1886	172	0.1	7.747×10^{-5}
Analog Input (AI) Module	31	45	20	0.006		1.863×10^{-7}
Digital Output (DO) Module	16	12	17	0.3		1.45×10^{-6}
Distributed processing unit (DPU)	1091	694	1251	4		2.753×10^{-5}
DCSoutput relay group	0	8	0	1	0.035	6.57×10^{-7}
First layer trip relay	21	93	10	40		1.752×10^{-4}
Second layer triprelay	6	6	10	11		4.826×10^{-5}
Shutoff valve	0	201	144	224		9.823×10^{-4}
Electric actuator	461	905	2510	388		1.719×10^{-3}

According to the above results,obtain the average probability of failure on demand of sensor, logic and actuator, resulting in the average probability of failure on demand of the entire SIF.

$$PFD_{Sensor} = 2PFD_{Secondary\ air\ flow\ transmitter\ FT} + 6PFD_{Primary\ air\ flow\ transmitter\ FT} = 9.296 \times 10^{-4}$$

$$PFD_{Logic\ unit} = 18PFD_{AI\ module} + 3PFD_{DOmodule} + PFD_{DPU} + PFD_{DCS\ output\ relay\ group} = 3.589 \times 10^{-5}$$

$$PFD_{Actuator} = 6PFD_{First\ layer\ trip\ relay} + 30PFD_{Second\ layer\ trip\ relay} + 16PFD_{Electr\ ic\ actuator} + 69PFD_{Shutoff\ valve} = 9.778 \times 10^{-2}$$

$$PFD_{SIF} = PFD_{Sensor} + PFD_{Logic\ unit} + PFD_{Actuator} = 9.874 \times 10^{-2} > 10^{-2}$$

4.4 Revision.

SIL of MFT triggered when the wind is Less than 30%does not meet the target value. Corrective measures include:

1) Adopt actuators withredundant configuration;
2) Reduce the functional testing cycle of the actuators;
3) Select actuatorswith smallfailure rates.

Constitute1out of 2 (1oo2) redundancy structures for valves and electric actuators.Common cause failure rateis 0.1, functional testing cycle is shortened to 0.5 years. Results after revision are shown in Table 6.

Table 6.Probabilities of failure on demand after revision

	Shutoff valve	Electric actuator	Actuator	SIF
PFD_{avg}	4.943×10^{-5}	8.778×10^{-5}	1.372×10^{-4}	1.103×10^{-3}

5. Conclusions.

FSSS has been widely usedin thermal power plant, but there is a lack of safety evaluation on FSSS.A hazard and risk identification for FSSSis conducted,and the target SIL is determined in this paper.SIS consists of sensor, logic controller and actuator, and actuator and sensor have greater effects on SIL.In thepractical application of FSSS in thermal power plants, sensors are usually inredundant configurations, but actuators are on the contrary, mainly due to the high cost, and limited installation space. However, to improve the level of functional safety of FSSS,greater attention to actuatorsmust be payed, and the choice of instruments and functional testing cycle must be given enough consideration.

References

[1] Application of Safety Instrumented Systems for the Process Industry[S]. ANSI/ISA 84.1-1996, 1996.
[2] William M. Goble. Control system safety evaluation and reliablity [M]. US: ISA, 1998.
[3] ZHANG Jian-guo. The application of safety instrumented systems for the process industry sector [M]. Beijing: China electric power press, 2010.
[4] Lohmann, S.,Henkel, K., Jorling, F.Control and safety instrumented system as joint solution for safe power plant operation [J]. VGB Powertech,v 93, n 6,p 93-7,2013.
[5] International Electrotechnical Commission, Functional safety of electrical/ electronic/programmable electronic safety-related systems, IEC-61508, Parts 1-7, 2ed Ed., Geneva, Switzerland, 2010.
[6] International Electrotechnical Commission, Functional safety–safety instrumented systems for the process industry sector, IEC-61511, Parts 1-3, 1st Ed., Geneva, Switzerland, 2003.
[7] Nuclear power plants-instrumentation and control for systems important to safety-general requirements for systems[S]. IEC61513-2001,2001.
[8] Safety of machinery: functional safety of safety-related electrical, electronic, programmable electronic safety-related systems. IEC62061-2005, 2005.
[9] WANG Yong-jian, SHI Xi-gen, XU Hong-bin, etc. Protection principle and application in thermal power plants [M]. Beijing: China electric power press, 2009.
[10] YANG Jin-ping, BAI Jian-yun. Security monitoring and protection system [M]. Beijing: China electric powerpress, 2006.
[11] WEI Gen-yuan. Sequence control and protection in large thermal power plant [M]. Beijing: China electric powerpress, 2008.
[12] DENG Chao，DUAN Chaoqun，WU Jun.Economic optimization model for phased sequential preventive maintenance based on equipment reliability[J].Computer Integrated Manufacturing Systems,2016,29(2):568-575(in Chinese)