Journal of Health and Safety at Work 2024; 14(2): 244-271

ORIGINAL RESEARCH PAPER

Safety Integrity Level (SIL) Determination and Verification for Gas Turbine and Generator in a Combined Cycle Power Plant

Behzad Gholami[1], Mousa Jabbari[1,2*], Davood Eskandari[3]

[1]Department of Occupational Health and Safety Engineering, School of Public Health and Safety, Shahid Beheshti University of Medical Sciences, Tehran, Iran
[2]Workplace Health Promotion Research Center, Shahid Beheshti University of Medical Sciences, Tehran, Iran
[3]Department of Occupational Health and Safety Engineering, School of Public Health, Shahrekord University of Medical Sciences, ChaharMahal and Bakhtiari, Iran

Received: 22 - 10 - 2023 Accepted: 16 - 6 - 2024

ABSTRACT

Introduction: One of the ways to produce electricity in power plants is to use gas turbines and generators. Due to the use of methane gas as the fuel of the burners and the high rotation speed, this equipment has a high DOW index level, therefore, if the hazardous conditions in the gas turbine are not controlled by the safety instrumented system and the process is not directed to a safe state, Catastrophic events will occur such as fire and explosion and damage to property and people as well as interruption of the power generation process will happen in the long term, so gas turbine safety instrumentation systems can be considered as "critical safety systems". Therefore, the reliability and availability of their function should be evaluated. The purpose of this research is to determine and verify the safety integrity level (SIL) related to the safety instrumented function (SIF) of the gas turbine and generator in a combined cycle power plant.

Material and Methods: In this study, the safety integrity level was determined by using two methods, Calibrated Risk Graph (CRG) and Independent Protection Layer Analysis (LOPA), and to verify the safety integrity level, the requirements related to random hardware failure, hardware failure tolerance, and systematic capability are considered according to IEC 61511 and IEC 61508 standards.

Results: The results of a case study in gas turbine and generator showed that the LOPA method is more quantitative than CRG and provides more details of independent protective layers, so it is a more suitable method for determining SIL. The SIL verification results show the SIL2 level, closer to the LOPA results.

Conclusion: The obtained results show that the function of the studied gas turbine safety instrumentation system has a suitable level of reliability and availability and is well responsive to risky conditions and possible deviations. The present approach helps safety engineers and instrumentation engineers to calculate the reliability and availability of the Function of the safety instrumentation systems of their process equipment and ensure its acceptability or not

Keywords: *Safety Instrumented Level (SIL), Layer of Protection Analysis (LOPA), Calibrated Risk Graph (CRG), Probability Failure on Demand (PFD), Hardware Fault Tolerance (HFT), Systematic Capability (SC)*

HOW TO CITE THIS ARTICLE

Gholami B, Jabbari M, Eskandari D. Safety Integrity Level (SIL) determination and verification for gas turbine and generator in a combined cycle power plant. J Health Saf Work. 2024; 14(2): 244-271.

1. INTRODUCTION

Understanding the safety process is the first step in reducing the risk level, and in to reduce the risk level, it is necessary to calculate the existing risk level and compare it to the organization's tolerable risk level. Each independent protection layer (IPL) plays an effective role in reducing the level of risk. Gas turbines and generators are used to generate electricity in power plants, in these turbines, natural gas is used to fuel the burners, these turbines have a high rotation speed, and in case of dangerous conditions such as overspeed,

* Corresponding Author Email: *jabbarim@sbmu.ac.ir*

Copyright © 2024 The Authors.
Published by Tehran University of Medical Sciences

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International license (https://creativecommons.org/licenses/by-nc/4.0/). Non-commercial uses of the work are permitted, provided the original work is properly cited.

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

vibration, lube oil high temperature, natural gas high pressure in the gas turbine is not controlled by the safety instrumented system and the process is not directed to a safe state, catastrophic events such as fire and explosion and damage to property and people will occur, Therefore, safety instrument systems (SIS) of gas turbines are considered as "critical safety systems", so their level of reliability and availability of function should be evaluated (Figure 1). This study was conducted to determine and verify the safety integrity level related to the safety instrumented function of the gas turbine and generator in a combined cycle power plant. The stage of risk assessment and determining and verifying the safety integrity level has been carried out according to IEC 61511 Part-3 and IEC 51508 Part-2&6 standards.

2. MATERIAL AND METHODS

Since the gas turbine has specific process flows, therefore, by the IEC 61511 Part-3 standard, the HAZOP study method was used to identify process risks. Process flow paths of gas turbine and generator include cooling oil flow system, cooling and sealing air system, hydraulic oil path for gas turbine trip, fuel gas system, hydraulic oil supply system to inlet guide vane control ring, which HAZOP studies on They were carried out and using the safety risk matrix method and the 5 ××5 probability and severity table, the level of risk related to each scenario was determined.

In the next step, the required SIL safety integrity level related to a safety instrumented function was determined by the methods of calibrated risk graph and independent layers of protection analysis (LOPA) based on the IEC 61511 Part-3 standard and the CCPS Handbook on LOPA. In the calibrated risk graph method, a decision tree is used to determine SIL, which contains consequence parameter (C), exposure time parameter (F), probability of avoiding the hazard event (P), and the absence of SIF under hazardous conditions (W). In the LOPA analysis method, the existing risk level was calculated by multiplying the

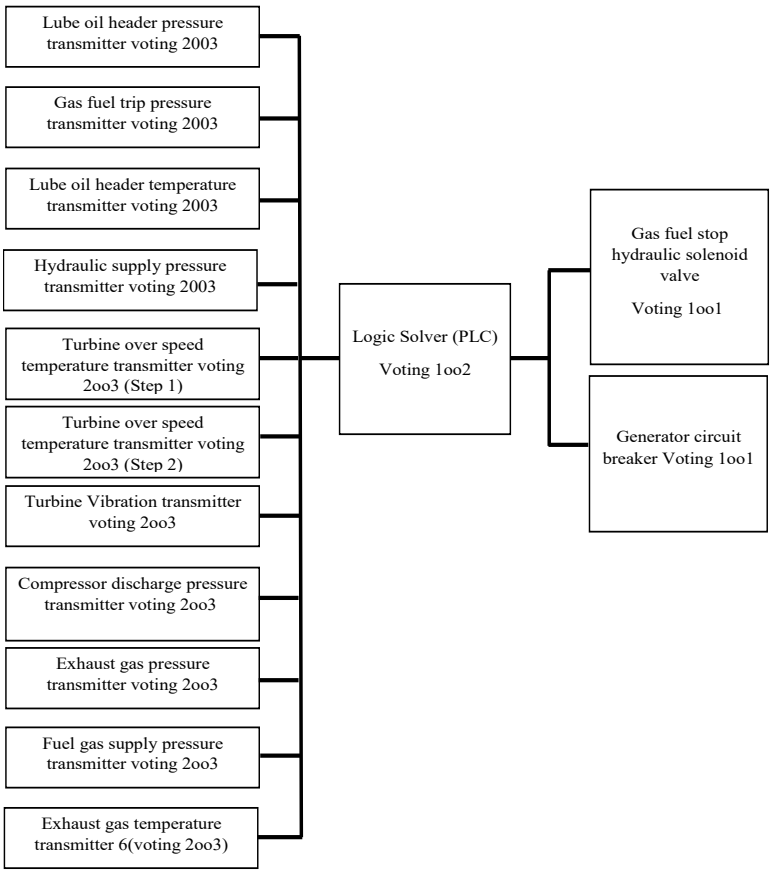


Fig. 1: Gas turbine and generator safety instrumentation system under study

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

Table 1: Comparison of SIL determination results using CRG and LOPA methods

No.	Scenario	Risk Reduction Factor (RRF) with LOPA	SIL determination with CRA	SIL determination with LOPA
1	Low lube oil pressure	1000	SIL2	SIL2
2	Lube oil header high temperature	1000	SIL2	SIL2
3	Gas fuel hydraulic low pressure	1000	SIL2	SIL2
4	Hydraulic supply low pressure	1000	SIL2	SIL2
5	Turbine over speed 1	1000	SIL2	SIL2
6	turbine over speed 2	1000	SIL3	SIL2
7	High vibration	1000	SIL3	SIL2
8	Loss of compressor discharge pressure	1000	SIL2	SIL2
9	Fuel gas supply low pressure	1000	SIL2	SIL2
10	Exhaust gas high pressure	1000	SIL3	SIL2
11	Exhaust high temperature	1000	SIL3	SIL2

probability of failure on demand (PFD) related to the existing Independent protection layers and the frequency of the initial event. Then the calculated risk value was compared with the tolerable level of the organization. In cases where the risk level is higher than the organization's tolerable risk level, independent protection layers are suggested to reach tolerable levels. It can be said that if there is a safety instrumented system as an independent protection layer, what should be the numerical value of PFD and SIL level, to make the system safe and bring the risk level to a tolerable level.

The IEC 61508 standard specifies the SIL verification requirements for any SIF used in process industries. Achieving the target safety integrity level depends on the following parameters, all of which are considered in this research: 1) Random hardware failures, which are obtained by calculating the average probability of failure on demand (PFD) and considering the rate of dangerous failures. In this research, the formulas in the IEC 61508 Part-6 standard and Jahanian's general formula (GPFD), and the formulas in the ISA 84.00.02 Part-2 technical report were used to calculate the PFD_{ang}. 2) Hardware reliability, which is a function of two parameters: hardware fault tolerance (HFT) and safe failure fraction (SFF). 3) Systematic Capability, which is achieved by considering systematic failures (software failures, electronic interference, usage methods different from design requirements, etc.). To ensure that a SIF can meet the requirements related to the target SIL, all three of the above limitations must be considered (Table 2).

3. RESULTS AND DISCUSSION

The results of the calibrated risk graph to determine the required SIL on 11 consequences showed that 7 consequences require SIL2 level and 4 consequences require SIL3 level. The analysis of 11 scenarios using the LOPA method and based on the number and type of existing protection layers showed that SIL2 level is required for all consequences (Table 1). To verify SIL, first the numerical value of PFD_{ang} was calculated using the standard formulas of IEC 61508 Part-6 and Jahanian's general formula (GPFD), the formulas of ISA 84.00.02 Part-2 technical report, which was confirmed in all three sources of SIL2 level for all scenarios. then according to the structure of the composition (Architecture) of the subsystems of the safety instrument system, the numerical value (HFT) was calculated and then the safe failure fraction (SFF) was calculated based on the IEC 61508 Part-2 standard and using the tables in this standard, the value of the SIL level was determined based on the two parameters HFT and SFF, which shows the SIL2 level for all scenarios. And finally, the numerical value of systematic capability was extracted from manufacturer certification. The result showed that based on the numerical value of systematic capability, the level of safety integrity is equal to SIL2 (Table 2).

Therefore, it can be concluded that the level of

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

Table 2: SIL verification results considering requirements for hardware fault tolerance, random hardware failures, and systematic capability

Sub-System	Element Function	voting	SIL of sub-system					
			For achieved Hardware Fault Tolerance		For Random hardware failure and calculation PFD_{avg}		For Systematic Capability	
Sensor	Lube oil low pressure	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4	SIL 4	$PFD = 1.58 \times 10^{-5}$ SIL= 4	$PFD = 5.66 \times 10^{-4}$ SIL 3	SIL=3 capable	SIL= 3
	Lube oil header high temperature	2oo3	HFT=1 , Route 1H, SFF=%93, SILL= 4		$PFD = 2.76 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	Gas fuel hydraulic low pressure	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 1.58 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	Hydraulic supply low pressure	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 1.58 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	Turbine over speed 1	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 7.36 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	Turbine over speed 2	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 7.36 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	High vibration	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 7.36 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	Loss of compressor discharge pressure	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 1.58 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	Fuel gas supply low pressure	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 1.58 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	Exhaust gas high pressure	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 1.58 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	Exhaust high temperature	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 2.76 \times 10^{-5}$ SIL= 4		SIL=3 capable	
Logic Solver	DCS	1oo2	HFT=1 , Route 1H, SFF=%95, SILL= 3	SIL 3	$PFD = 2.3 \times 10^{-4}$ SIL= 3	SIL 3	SIL=3 capable	SIL2
Final element	Hydraulic Solenoid Valve	1oo1	HFT=0 , Route 1H, SFF=%79 , SILL= 2	SIL 2	$PFD = 3.5 \times 10^{-3}$ SIL= 2	$PFD = 4.8 \times 10^{-3}$ SIL 2	SIL=2 capable	SIL= 2
	General Vacuum Circuit	1oo1	HFT=0 , Route 1H, SFF=%66 , SILL= 2		$PFD = 1.3 \times 10^{-3}$ SIL= 2		SIL=2 capable	
SIL of SIF(Gas Turbine and Generator Trip)			SIL 2		SIL 2		SIL 2	
SIL 2 Safety Instrument Function (Gas Turbine and Generator Trip)								

safety integrity related to the performance of the safety instrumented system for the trip function of the gas turbine and generator in dangerous conditions for all scenarios is equal to SIL2, which is equal to the SIL level required based on LOPA.

4. CONCLUSIONS

In this study, IEC 61511 and IEC 61508 standards have been used to assess risk and determine and verify the trip performance of gas turbine and generator in a combined cycle power plant under dangerous and abnormal operating conditions. The present approach helps safety engineers and instrumentation engineers to calculate the reliability and availability of the safety instrumentation function of their process equipment and ensure its acceptability. To increase the level of safety and reliability, the following suggestion is presented as one of the results of the research: installing a spare oil cooler, installing the F&G system in the natural gas route, using the 1oo2 architecture instead of 1oo1 for the final element and discharge hydraulic oil pressure and then closed natural gas main control valve.

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

فصلنامه بهداشت و ایمنی کار
جلد ۱۴/ شماره ۲/ تابستان ۱۴۰۳ صفحات ۲۴۴-۲۷۱

تعیین و تایید سطح یکپارچگی ایمنی (SIL) توربین گازی و ژنراتور در یک نیروگاه سیکل ترکیبی

بهزاد غلامی[۱]، موسی جباری[۱،۲*] ، داود اسکندری[۳]

[۱]گروه مهندسی بهداشت حرفه ای و ایمنی کار، دانشکده بهداشت و ایمنی، دانشگاه علوم پزشکی شهید بهشتی، تهران، ایران
[۲]مرکز تحقیقات ارتقای سلامت محیط کار، دانشگاه علوم پزشکی شهید بهشتی، تهران، ایران
[۳]گروه مهندسی بهداشت حرفه ای و ایمنی کار، دانشکده بهداشت، دانشگاه علوم پزشکی شهرکرد، چهارمحال و بختیاری، ایران

تاریخ دریافت: ۱۴۰۲/۷/۳۰، تاریخ پذیرش: ۱۴۰۳/۳/۲۷

چکیده

مقدمه: یکی از راه های تولید برق در نیروگاهها استفاده از توربین های گازی و ژنراتور های همراه می باشد. این تجهیزات به علت استفاده از گاز متان به عنوان سوخت مشعل ها و سرعت دوران بالا، دارای سطح شاخص DOW بالایی می باشند، بنابر این درصورتی‌که شرایط مخاطره‌آمیز در توربین گازی توسط سیستم ابزار دقیق ایمنی کنترل نگردد و فرآیند به حالت ایمن هدایت نشود، وقایع فاجعه باری مانند آتش‌سوزی و انفجار و آسیب به اموال و افراد و همچنین قطع فرآیند تولید برق در طولانی مدت رخ خواهد داد، بنابراین می‌توان سیستم‌های ابزار دقیق ایمنی توربین‌های گازی را به‌عنوان «سیستم‌های ایمنی بحرانی» در نظر گرفت، لذا بایستی سطح قابلیت اطمینان و دسترسی عملکرد آن‌ها مورد ارزیابی قرار گیرد. هدف از این تحقیق، تعیین (Determination) و تایید (Verification) سطح یکپارچگی ایمنی مربوط به عملکرد سیستم ابزار دقیق ایمنی جهت از سرویس خارج کردن توربین گازی و ژنراتور در یک نیروگاه سیکل ترکیبی می‌باشد.

روش کار: در این مطالعه سطح یکپارچگی ایمنی با استفاده از دو روش نمودار ریسک کالیبره شده (CRG) و آنالیز لایه های حفاظتی مستقل (LOPA) تعیین گردید و جهت تایید سطح یکپارچگی ایمنی الزامات مربوط به خرابی های تصادفی سخت افزار (Random Hardware Failure)، تحمل خطای سخت افزاری (Hardware Fault Tolerance) و قابلیت سیستماتیک (Systematic Capability)، مطابق با استاندارد IEC 61511 و IEC 61508 در نظر گرفته شده است.

یافته ها: نتایج مطالعه موردی در توربین گازی و ژنراتور نشان داد که روش LOPA نسبت به CRG روش کمی‌تری می‌باشد و جزئیات بیشتری از لایه‌های حفاظتی مستقل را فراهم می‌کند، لذا روش مناسب‌تری برای تعیین SIL می‌باشد. نتایج تایید سطح یکپارچگی ایمنی مربوط به عملکرد سیستم ابزاردقیق ایمنی نصب شده، سطح SIL2 را تایید می کند، که به نتایج حاصل از LOPA نزدیک تر است.

نتیجه گیری: نتایج حاصله نشان داد که عملکرد سیستم ابزار دقیق ایمنی توربین گازی مورد مطالعه دارای سطح قابلیت اطمینان و دسترسی مناسبی است و به‌خوبی پاسخگوی شرایط مخاطره‌آمیز و انحرافات احتمالی می‌باشد. رویکرد حاضر به مهندسین ایمنی و مهندسین ابزاردقیق کمک می کند، قابلیت اطمینان و قابلیت در دسترس بودن عملکرد سیستم های ابزار دقیق ایمنی تجهیزات فرآیندی خود را محاسبه کرده و از قابل قبول بودن یا نبودن آن اطمینان حاصل کنند.

کلمات کلیدی: *سطح یکپارچگی ایمنی (SIL)، آنالیز لایه های حفاظتی مستقل (LOPA)، نمودار ریسک کالیبره شده (CRG)، احتمال خرابی در زمان تقاضا (PFD)، تحمل خطای سخت افزار (HFT)، قابلیت سیستماتیک (SC).*

* پست الکترونیکی نویسنده مسئول مکاتبه: *Jabbarim@sbmu.ac.ir*

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

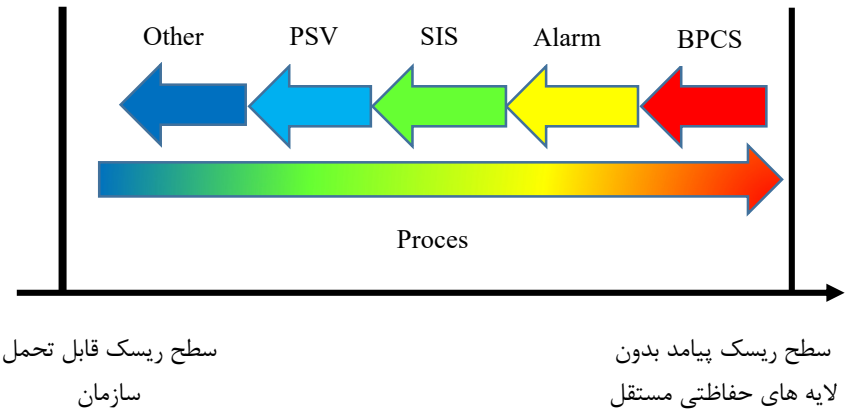
مقدمه

ارزیابی سطح ایمنی مشابه کیفیت، تولید و بهره‌وری بخش مهمی از استراتژی شرکت‌ها محسوب می‌شود. درک فرآیند ایمنی اولین قدم در کاهش سطح ریسک می‌باشد و جهت کاهش سطح ریسک نیاز به محاسبه سطح ریسک موجود و مقایسه آن با سطح ریسک قابل‌تحمل سازمان می‌باشد. هر لایه حفاظتی مستقل (Indipendent Protection Layer) نقش مؤثری در کاهش سطح ریسک دارد. شکل ۱ لایه‌های حفاظتی مستقل را نشان می‌دهد که برای جلوگیری از وقوع حوادث (Prevention) یا به حداقل رساندن اثر حوادث (Mitigation) به کار گرفته می‌شوند. برای این که یک تجهیز، سیستم یا عمل به عنوان IPL شناخته شود بایستی سه ویژگی موثر بودن، مستقل بودن و قابل ممیزی بودن را داشته باشد. هر کدام از لایه‌های حفاظتی در یک مرحله از زنجیره‌ی رخداد حادثه وارد عمل شده و وظیفه قطع زنجیره حادثه را دارد و به این ترتیب مانع ازتبدیل شدن رخداد اولیه به حادثه پایانی می‌شوند. با توجه به این که هر کدام از لایه‌های حفاظتی مستقل دارای یک احتمال خرابی در زمان تقاضا (Probability Failure on Demand) می‌باشند، بنابر این ممکن است در لحظه‌ای که به عملکرد درست آن‌ها نیاز است، به درستی عمل نکرده و زنجیره تشکیل حادثه قطع نگردد، بنابراین نیاز به چند لایه حفاظتی مستقل جهت اطمینان از قطع زنجیره حوادث می‌باشد. همان طور که در شکل ۲ نشان داده شده است، هر کدام از لایه‌های حفاظتی مستقل، سطح ریسک را به مقدار مشخصی کاهش می‌دهند، لذا رسیدن به سطح ریسک قابل تحمل سازمان، تعداد و نوع لایه‌های حفاظتی مستقل را تعیین می‌کند (۱-۳).

سیستم کنترل فرآیند پایه‌ای (Basic Process

لایه های حفاظتی مستقل	کاهنده اثر پیامد	لایه هفتم: تیم واکنش در شرایط اضطراری منطقه ای (Community emergency response)
		لایه ششم: واکنش در شرایط اضطراری داخلی (Plant emergency response)
	پیشگیری کننده از وقوع پیامد	لایه پنجم: محافظت کننده های فیزیکی مانند شیراطمینان ((Physical Protection (Relief Device)
		لایه چهارم: سیستم ابزاردقیق ایمنی (Safety Instrumented System)
		لایه سوم: آلارم های حیاتی همراه با دخالت اپراتور (Critical Alarms and Human Intervention)
		لایه دوم: سیستم کنترل فرآیند (Basic Process Control System)
		لایه اول: طراحی فرآیند ذاتا ایمن (Inherently Process Safe Design)

شکل ۱: لایه های حفاظتی مستقل در واحد های صنعتی (۲,۴).



شکل ۲: لایه های حفاظتی مستقل در واحد های صنعتی (۲, ۴).

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]
[DOI: 10.18502/jhsw.v14i2.17136]

Control System) و سیستم ابزار دقیق ایمنی (Safety Instrumented System) دو نوع از لایه‌های حفاظتی مستقلی هستند که جهت محافظت از تأسیسات در برابر شرایط فرآیندی نامطلوب مورد استفاده قرار می‌گیرند. این تجهیزات را سیستم‌های کنترلی قابل برنامه‌ریزی (Programabe Control System) نیز می‌نامند زیرا توسط یک واحد پردازشگر مرکزی که قابلیت برنامه‌ریزی دارد کنترل می‌شوند. سیستم‌های ابزار دقیق ایمنی (SIS) ترکیبی از حس‌گر(S)، حل‌کننده منطقی(LS) و عملگر پایانی(FE) می‌باشند که یک یا چند عملکرد ابزار دقیقی (SIF) را در جهت حفظ ایمنی فرآیند انجام می‌دهند(۵). سیستم‌های کنترل فرآیند پایه‌ای (BPCS) فرآیند را در حالت نرمال نگه می‌دارند ولی سیستم‌های ابزاردقیق ایمنی فرآیندی که از حالت نرمال خارج‌شده را به حالت نرمال برمی‌گردانند یا آن را از سرویس خارج می‌کنند(۴، ۶، ۷).

در مطالعه‌ای که صادقی، جباری و همکاران (2020) بر روی خطرات آتش‌سوزی و انفجار در یک نیروگاه سیکل ترکیبی با استفاده از شاخص آتش‌سوزی و انفجار DOW انجام دادند، به این نتیجه رسیدند که توربین گازی با سوخت متان بیشترین مقدار شاخص DOW را دارد که برابر ۳۲۱ می‌باشد و حداکثر واقعی خسارت احتمالی به دارایی‌ها برابر 4.12 میلیون دلار محاسبه گردید. حداکثر قطعی احتمالی ۵۰ روز تخمین زده شد و درنهایت ضرر ناشی از توقف واحد برابر 3.03 میلیون دلار آمریکا محاسبه گردید(۸، ۹). نتایج این مطالعه نشان می‌دهد درصورتی‌که شرایط مخاطره‌آمیز در توربین گازی توسط سیستم ابزار دقیق ایمنی کنترل نگردد و فرآیند به حالت ایمن هدایت نشود، حوادث فاجعه باری مانند آتش‌سوزی و انفجار و آسیب به اموال و افراد رخ خواهد داد، بنابراین می‌توان سیستم‌های ابزار دقیق ایمنی توربین‌های گازی را به‌عنوان "سیستم‌های ایمنی بحرانی" در نظر گرفت، لذا بایستی سطح قابلیت اطمینان و دسترسی عملکرد آن‌ها مورد ارزیابی قرار گیرد. یکی از روش‌های این که مشخص شود سیستم ابزاردقیق ایمنی (SIS) می‌تواند به عنوان یکی از لایه‌های حفاظتی مستقل (IPL) موثر عمل کند و در شرایطی که به آن نیاز است در دسترس باشد، تعیین سطح یکپارچگی ایمنی (Safety Integrity Level) می‌باشد.

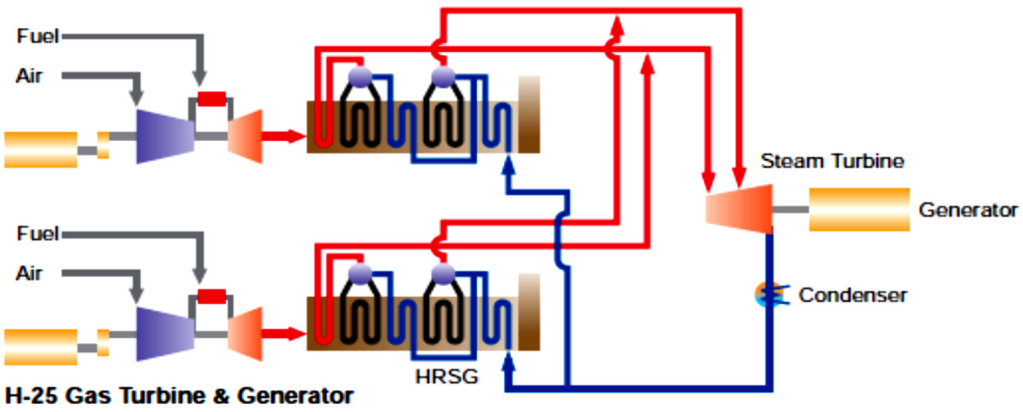
سطح یکپارچگی ایمنی(SIL)، مطابق تعریف IEC 61511 به‌طور گسترده‌ای برای ارزیابی دسترسی عملکرد سیستم‌های ابزار دقیق ایمنی استفاده می‌شود. استاندارد IEC 61511 Part-3 محدوده‌ای از روش‌های کاملاً کیفی تا روش‌های کاملاً کمی را برای تعیین سطح یکپارچگی ایمنی معرفی می‌کند(۱۰). دو روش پرکاربرد در صنعت نفت و گاز برای تعیین SIL وجود دارد که عبارت‌اند از: آنالیز لایه‌های حفاظتی (LOPA) و نمودار ریسک کالیبره شده(۱۱).

استاندارد IEC 61511 و استانداردهای خاص مربوطه مبتنی بر ریسک هستند، به این معنی که الزامات مربوط به ارزیابی قابلیت اطمینان عملکرد سیستم‌های ابزار دقیق ایمنی (SIF) باید از نتایج ارزیابی ریسک فرآیندی استفاده کنند(۱۱). جهت شناسایی خطرات احتمالی و اثرات آن‌ها در مراحل مختلف فرآیند، می‌توان از بسیاری از تکنیک‌های تجزیه‌وتحلیل خطرات استفاده کرد. روش مطالعه خطر و عملیات (HAZOP) یکی از متداول‌ترین روش‌های کیفی تجزیه‌وتحلیل خطرات فرآیندی می‌باشد (۱۲، ۱۳). جهت تعیین سطح یکپارچگی ایمنی مورد نیاز، ریسک‌های فرآیندی به‌وسیله روش‌های ارزیابی ریسک نیمه کمی مانند LOPA و نمودار ریسک کالیبره شده ارزیابی می‌گردند (۱۱، ۱۴).

ازآنجاکه توربین گازی دارای جریان‌های فرآیندی مشخصی می‌باشد بنابراین در این تحقیق مطابق استاندارد IEC 61511، از روش HAZOP جهت شناسایی خطرات فرآیندی استفاده‌شده است. سپس جهت شناسایی سناریوهای خطرناک روش ماتریس ایمنی ریسک (Risk Safety Matrix) به‌کاربرده شده است. در مرحله بعد سطح SIL مورد نیاز مربوط به عملکرد سیستم ابزاردقیق ایمنی، توسط روش‌های نمودار ریسک کالیبره شده و آنالیز لایه‌های حفاظتی مستقل از IEC 61511

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]



شکل ۳: نیروگاه سیکل ترکیبی (۱۷).

Part-3 تعیین گردید. و درنهایت جهت تایید سطح یکپارچگی ایمنی مربوط به عملکرد سیستم ابزاردقیق ایمنی نصب شده از سه روش خرابی‌های تصادفی سخت‌افزار (Random Hardware Failure)، تحمل خطای سخت افزاری (Hardware Fault Tolerance) و قابلیت سیستماتیک (Systematic Capability) استفاده شده است(۱۰، ۱۵، ۱۶).

توربین گازی و ژنراتور

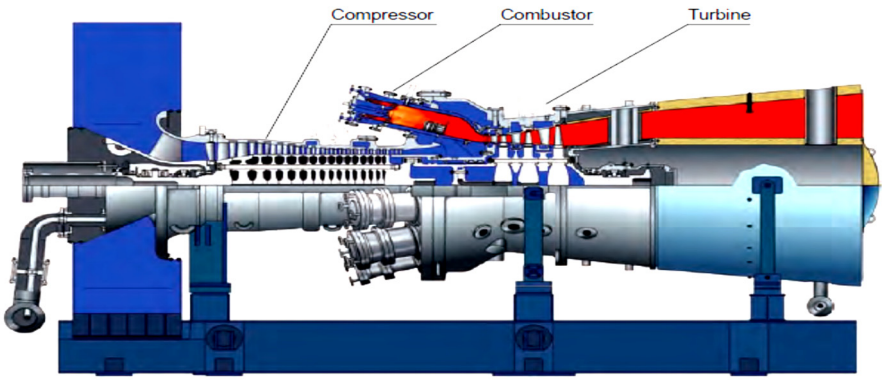
نیروگاه سیکل ترکیبی درواقع ترکیبی از توربین بخار و توربین گازی می‌باشد به‌نحوی‌که توربین گازی و ژنراتور برق را تولید می‌کند، درعین‌حال انرژی حرارتی تلف‌شده از توربین گازی (توسط محصولات احتراق) برای تولید بخار موردنیاز توربین بخار مورداستفاده قرار می‌گیرد و به این طریق برق مضاعف تولید می‌شود. شکل ۳ یک نیروگاه سیکل ترکیبی را نشان می‌دهد(۱۷).

در صورت اختلال در سیستم توزیع برق در پالایشگاه‌های نفت و گاز و پتروشیمی‌ها، واحدهای فرآیندی از سرویس خارج‌شده و خطراتی همچون افزایش ناگهانی فشار و نشت مواد قابل اشتعال و حتی آتش‌سوزی را در پی دارد، بنابراین اختلال در سیستم توزیع برق با هزینه‌های هنگفتی همراه می‌باشد، لذا در این تأسیسات تولید مداوم برق از اهمیت خاصی برخوردار می‌باشد.

توربین‌های گازی و ژنراتور دارای اجزای ژنراتور، کمپرسور هفده مرحله‌ای، محفظه احتراق، توربین سه مرحله‌ای، مسیر جریان گاز طبیعی به‌عنوان سوخت، مسیر جریان هوای ورودی به کمپرسور، مسیر جریان روغن خنک‌کننده و روغن هیدرولیک می‌باشد(۱۸). مسیرهای جریان فرآیندی توربین گازی و ژنراتور شامل مسیر جریان روغن روان‌کننده و خنک‌کننده (Lubeoilsystem)،مسیر تأمین‌هوای‌خنک‌کننده‌وپرژینگ (Cooling and sealing air system)، مسیر روغن هیدرولیک مخصوص از سرویس خارج کردن توربین گازی (Trip oil system)، مسیر تأمین خوراک گاز طبیعی مشعل‌ها (Fuel gas system)، مسیر جریان روغن هیدرولیک تنظیم‌کننده شیر ورودی هوا به کمپرسور (Hydraulic supply system to inlet guide vane control ring) می‌باشند. حسگرهای مربوط به دمای روغن خنک‌کننده، مقدار دور توربین بر دقیقه، لرزش، دمای گازهای حاصل از احتراق، فشار گاز ورودی به مشعل‌ها و فشار هوای ورودی به کمپرسور و غیره، هرگونه شرایط غیر نرمال فرآیندی را شناسایی کرده و سیگنال مربوطه را به واحد پردازشگر مرکزی یا حل‌کننده منطقی (Logic Solver) ارسال کرده، و حل‌کننده منطقی فرمان از سرویس خارج کردن توربین را به شیر قطع گاز ورودی به مشعل‌ها(Gas fuel stop solenoid valve) می‌دهد (۱۷).

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]



شکل ۴: توربین گازی متشکل از کمپرسور ۱۷ مرحله‌ای، مشعل‌ها و توربین سه مرحله‌ای(۱۷).

شدت پیامد / احتمال وقوع		خیلی کم	کم	متوسط	زیاد	خیلی زیاد
		۱	۲	۳	۴	۵
غیر محتمل	۱	۱	۲	۳	۴	۵
بندرت	۲	۲	۴	۶	۸	۱۰
گاهی	۳	۳	۶	۹	۱۲	۱۵
بعضی مواقع	۴	۴	۸	۱۲	۱۶	۲۰
مکرر	۵	۵	۱۰	۱۵	۲۰	۲۵

سطح ریسک		توضیح
غیر قابل قبول	۱۸ - ۲۵	ریسک غیر قابل قبول است و نیاز به اقدامات کنترلی جدید جهت کاهش سطح ریسک می باشد
قابل تحمل (ALARP)	۸ - ۱۷	ریسک قابل تحمل است
قابل قبول	۱ - ۷	ریسک جزئی و قابل‌قبول است

شکل ۵: ماتریس ایمنی ریسک (۲۰)

روش کار

در این تحقیق شناسایی خطرات توربین گازی موردمطالعه با استفاده از روش HAZOP و ارزیابی ریسک سناریوها با استفاده از روش ماتریس ایمنی ریسک انجام گردیده است. جهت تعیین SIL از دو روش نمودار ریسک کالیبره شده و LOPA و جهت تایید SIL از سه روش خرابی‌های تصادفی سخت‌افزار (Random Hardware Failure)، تحمل خطای سخت افزاری (Hardware Fault Tolerance) و قابلیت سیستماتیک (Systematic Capability) استفاده شده است.

شناسایی خطرات و ارزیابی ریسک توربین گازی با استفاده از روش HAZOP و ماتریس ارزیابی ریسک

روش شناسایی خطر HAZOP یک تکنیک شناسایی خطر کیفی است که می‌تواند در هر زمان در طول چرخه عمر فرآیند تا از سرویس خارج شدن تأسیسات و برای

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]
[DOI: 10.18502/jhsw.v14i2.17136]

جدول ۱: سطح احتمال وقوع پیامد (۲۰)

توصیف احتمال وقوع	اعداد احتمال	طبقه‌بندی
غیرمحتمل- هرگز اتفاق نمی‌افتد	0.00001	
به‌ندرت – یک‌بار در هر 100 تا 1000 سال	0.0001	
گاهی – یک‌بار در هر 10تا 100 سال	0.001	
بعضی مواقع – یک با در هر 1 تا 10 سال	0.01	

جدول ۲: شدت وقوع پیامد (۲۰)

توضیح	شدت پیامد	طبقه بندی
بدون آسیب و صدمه، تأثیر خیلی جزئی بر محیط‌زیست، کمتر از 20،000 دلار خسارت.	خیلی جزئی	1
جراحت یک نفر یا کمترین جراحت، یک تأثیر قابل‌شناسایی و مشخص روی محیط‌زیست، کمتر از 200،000 دلار خسارت.	جزئی	2
چندین نفر مجروح یا یک نفر جراحت شدید، اثر جدی بر محیط‌زیست و خسارت زیر 2میلیون دلار.	متوسط	3
مرگ یک نفر و جراحت شدید چند نفر، اثرات شدید روی محیط‌زیست و خسارت زیر 20 میلیون دلار.	شدید	4
مرگ یک نفر و جراحت شدید چند نفر، اثرات شدید روی محیط‌زیست و خسارت زیر 20 میلیون دلار.	خیلی شدید	5

هرگونه اصلاح فرآیند که نیاز به ارزیابی ریسک دارد، مورداستفاده قرار گیرد. فرآیند تجزیه‌وتحلیل HAZOP یک روش سیستماتیک است، که از آن برای تعیین هرگونه انحراف از حالت نرمال عملیاتی و بررسی این‌که آیا حفاظ‌های ایمنی مناسب به‌درستی برای کاهش و یا جلوگیری از وقوع حوادث انتخاب‌شده است، استفاده می‌شود. برای ارائه یک ارزیابی جامع از فرآیند، از کلمات راهنما مانند: زیاد / کم / قطع جریان/ برگشت جریان، همراه با پارامترهای عملیاتی متفاوتی مانند فشار / دما / دبی جریان سیال / ارتفاع سطح مایع، استفاده می‌شود و برای هر لوله، ظرف یا مخزن مربوط به فرآیند به‌صورت سیستماتیک اعمال می‌شود (۱۳، ۱۹). در این تحقیق توربین گازی به ۱۱ گره (Node) تقسیم‌بندی شد و ضمن تعیین انحرافات موجود در هر گره، دلایل وقوع انحرافات و حفاظ‌های ایمنی موجود ثبت گردید.

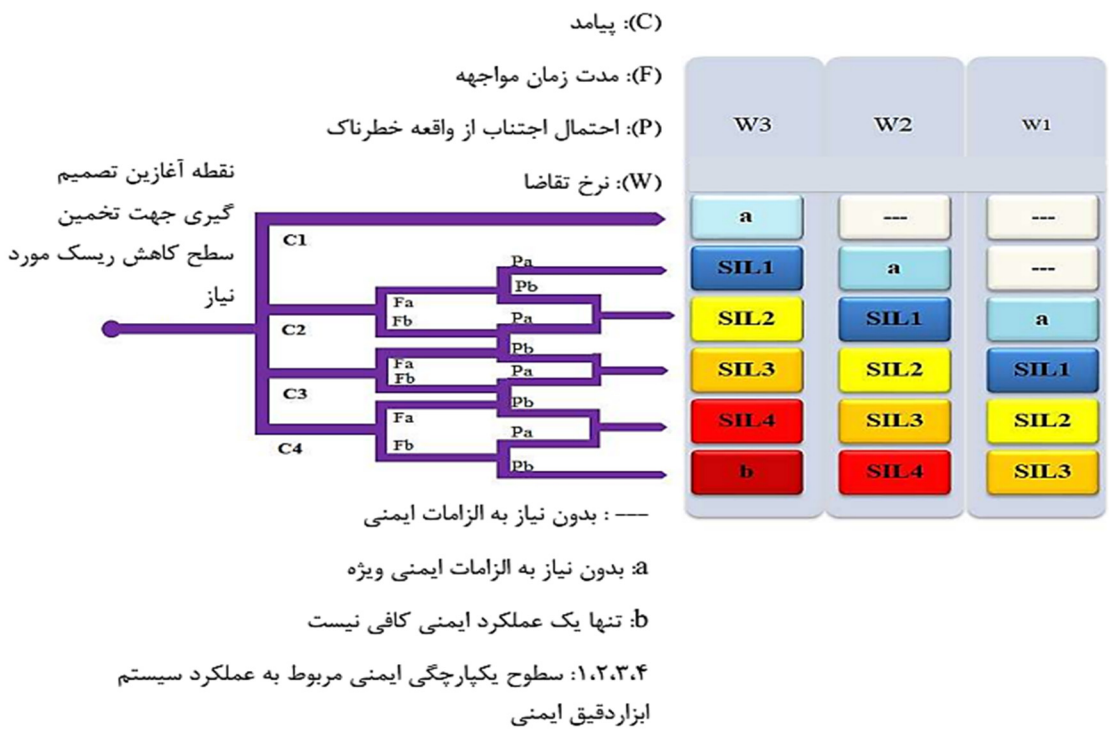
جهت تعیین سطح ریسک هر حادثه پایانی از روش ماتریس ریسک ایمنی استفاده گردید. شکل ۵ ماتریس ریسک ایمنی با پنج سطر جهت شدت حادثه پایانی و پنج ستون جهت احتمال وقوع حادثه پایانی را بر اساس جدول ۱ و ۲ نشان می‌دهد. با توجه به خطرات شناسایی‌شده سطح ریسک تعیین می‌شود. یک ماتریس ریسک دارای سه منطقه است: در سطح اول، ریسک به حدی کم است که می‌توان آن را نادیده گرفت، در این منطقه از ریسک هیچ اقدام کنترلی اضطراری لازم نیست و به آن ریسک قابل‌قبول می‌گوییم، در سطح ریسک دوم ریسک نامطلوب و تنها در صورتی قابل تحمل (Tolerable) است که کاهش ریسک غیر عملی باشد یا هزینه‌ها جهت کاهش سطح ریسک به قدری زیاد است که با بهبود بدست آمده نامتناسب باشد (ALARP)، سطح ریسک سوم در منطقه غیرقابل‌قبول قرار دارد و در این منطقه طراحی فرایند باید تغییر داده شود یا اقدامات ایمنی قابل‌توجهی برای کاهش سطح ریسک لازم و ضروری است (۱۳، ۲۰).

تعیین سطح یکپارچگی ایمنی

سطح یکپارچگی ایمنی (SIL) از ۱ تا ۴ رتبه‌بندی می‌شود و جهت توصیف سطح قابلیت اطمینان و در درسترس بودن یک عملکرد سیستم ابزاردقیق ایمنی (SIF) استفاده می‌شود. سطح SIL1 کمترین میزان

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]



شکل ۶: نمودار ریسک کالیبره شده (۱۰).

حفاظت ایمنی و SIL4 بالاترین میزان حفاظت ایمنی را دارد که برای صنایع هسته‌ای استفاده می‌شود(۱۳). در این تحقیق جهت تعیین سطح یکپارچگی ایمنی از نمودار ریسک کالیبره شده و آنالیز لایه‌های حفاظتی مستقل استفاده گردیده است.

نمودار ریسک کالیبره شده

نمودار ریسک کالیبره شده یک روش نیمه کمی است که سطح یکپارچگی ایمنی را با آگاهی از عملکرد عوامل خطر مرتبط با فرآیند و سیستم کنترل آن تعیین می‌کند. در این روش از چهار پارامتر مختلف استفاده شده است که در کنار هم ماهیت وضعیت خطرناک را در زمان خرابی سیستم ابزار دقیق یا زمانی که سیستم ابزار دقیق عمل نکند توصیف می‌کنند. (۱۰، ۲۱).

نمودار ریسک یک ارزیابی درجه‌بندی‌شده از یک حادثه پایانی را بر اساس مجموعه‌ای از عوامل خطر و عدم وجود SIF نشان می‌دهد. در شکل ۶ نمونه‌ای از نمودار ریسک کالیبره شده از استاندارد IEC 61511 Part-3 نشان داده‌شده است (۱۰، ۱۱، ۲۰).

برای تعیین SIL از یک درخت تصمیم استفاده گردید که حاوی عواقب وضعیت خطرناک (C)، احتمال وجود خطر (F)، احتمال اجتناب از وضعیت خطرناک (P) و میزان تقاضا (W) می‌باشد، که در شکل ۶ نشان داده‌شده است. پارامترهای جدول ۳ برای رسیدن به SIL مورد نیاز، در درخت تصمیم منعکس‌شده‌اند. سطح SIL هدف با دنبال کردن مسیر با توجه به عوامل خطر انتخاب‌شده تعیین می‌شود. درجه‌بندی، به فرآیند اختصاص مقادیر کمی (عددی) به هر یک از عوامل خطر در نمودار خطر اشاره دارد، این مقادیر از استاندارد IEC 61511 Part-3 انتخاب گردیده است (۴، ۲۰، ۲۱).

آنالیز لایه‌های حفاظتی مستقل (LOPA)

یکی دیگر از روش‌های تعیین SIL که در صنایع نفت و گاز کاربرد گسترده‌ای دارد روش آنالیز لایه‌های

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]
[DOI: 10.18502/jhsw.v14i2.17136]

جدول ۳: درجه‌بندی کمی عوامل خطر در نمودار ریسک درجه‌بندی‌شده (۴، ۱۰).

عوامل خطر	مقادیر کمی	توضیحات
شدت پیامد (C)		پیامد: حاصل‌ضرب تعداد افراد در آسیب‌پذیری
	C_A: حداقل خسارت	آسیب‌پذیری (Vulnerability):
	C_B: بین 0.01 تا 0.1	0.01 : نشتی کم از مواد قابل اشتعال و سمی
	C_C: بین 0.1 تا 1.0	0.1 : نشتی زیاد از مواد قابل اشتعال و سمی
	C_D: بالاتر از 1.0	0.5 : میزان نشتی مانند بالا اما قابلیت اشتعال و سمیت بالاتر است
		1.0 : ترکیدگی و انفجار
احتمال وجود خطر (F)	F_A: کمتر از 0.1	
	F_B: بیشتر از 0.1	
احتمال اجتناب از واقعه خطرناک (P)	P_A: اگر تمام شرایط ایمنی مناسب و رضایت‌بخش باشد.	احتمال حضور در موقعیت خطرناک به‌ندرت است.
	P_B: اگر تمام شرایط ایمنی نامناسب باشد	احتمال حضور دائمی در موقعیت خطرناک.
نرخ تقاضا (نیاز به عملکرد سیستم ابزار دقیق ایمنی) (W)	W_1: کمتر از 0.1 بار در سال	برای W بالاتر از 10 بار در سال، یکپارچگی بالایی موردنیاز است.
	W_2: بین 0.1 تا 1.0 بار در سال	
	W_3: بین 1.0 تا 10 بار در سال	

جدول ۴: سطح یکپارچگی ایمنی جهت سیستم ابزار دقیق ایمنی با تقاضای کم (۷، ۲۳).

سطح یکپارچگی ایمنی	احتمال خرابی در زمان تقاضا (PFD_{avg})	فاکتور کاهش ریسک (RRF)
SIL4	$0.00001 \le PFD_{avg} < 0.0001$	$100000 < RRF \le 10000$
SIL3	$0.0001 \le PFD_{avg} < 0.001$	$10000 < RRF \le 1000$
SIL2	$0.001 \le PFD_{avg} < 0.01$	$1000 < RRF \le 100$
SIL1	$0.01 \le PFD_{avg} < 0.1$	$100 < RRF \le 10$

حفاظتی مستقل (LOPA) می‌باشد. روش LOPA یک روش آنالیز ریسک نیمه کمی می‌باشد(۲۲)، این روش در هر دو استاندارد IEC 61508 Part-5 و IEC 61511 Part-3 بیان‌شده است. روش LOPA به‌طور جامع در کتاب‌های راهنمای CCPS نیز توضیح داده‌شده است (۱۱).

اطلاعات ورودی LOPA از روش کیفی شناسایی و ارزیابی مخاطرات فرآیندی (HAZOP) تأمین می‌گردد(۲). ریسک حادثه پایانی با توجه به مقدار عددی تکرارپذیری رخداد اولیه و احتمال خرابی لایه‌های حفاظتی موجود محاسبه می‌گردد. سپس مقدار ریسک محاسبه‌شده با سطح ریسک قابل تحمل سازمان مقایسه می‌شود. در مواردی که سطح ریسک بالاتر از سطح ریسک قابل تحمل سازمان باشد، لایه‌های حفاظتی مستقل لازم جهت کاهش سطح ریسک، و رسیدن به سطح ریسک قابل‌تحمل ارائه می‌گردد. فاکتور کاهش ریسک (Risk Reduction Factor) از تقسیم سطح ریسک واقعی بر سطح ریسک قابل‌تحمل به دست می‌آید (۲، ۱۱).

$$RRF = \frac{\text{Actual Risk}}{\text{Tolerable Target Risk}} \qquad (۱)$$

فاکتور کاهش ریسک با میانگین احتمال خرابی لایه‌های حفاظتی در زمان تقاضا (PFD_{avg}) رابطه عکس دارد (۱۱، ۱۳).

$$RRF = \frac{1}{PFD_{avg}} \qquad (۲)$$

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

جدول۵: انواع خرابی سیستم ابزار دقیق ایمنی و ارتباط بین آن‌ها (۵).

	خرابی های ایمن (λ_S :Safe failure rates)	λ_D :Dangerous failure rates
قابل شناسایی (Detected)	قابل تشخیص ایمن (λ_{SD} :Safe detected)	قابل تشخیص خطرناک (λ_{DD} :Dangerous detected)
غیر قابل شناسایی (Undetected)	غیر قابل تشخیص ایمن (λ_{SU} :Safe undetected)	غیر قابل تشخیص خطرناک (λ_{SU} :Dangerous undetected)
مجموع خرابی ها	$\lambda_{TOT}=\lambda_{DD}+\lambda_{DU}+\lambda_{SD}+\lambda_{SU}$	

در جدول ۴ ارتباط بین سطح یکپارچگی ایمنی (SIL) و مقدار کمی PFD_{avg} و فاکتور کاهش ریسک به‌دست‌آمده از روش LOPA نشان داده‌شده است(۵، ۷، ۲۳-۲۵).

حفاظ‌های ایمنی که دارای سه مشخصه مؤثر بودن، مستقل بودن و قابل ممیزی بودن باشند، به‌عنوان لایه حفاظتی مستقل (IPL) شناخته می‌شوند. هر لایه حفاظتی مستقل یک دستگاه، سیستم یا اقدامی (device، system، or action) است که قادر است از پیشروی زنجیره حادثه و تبدیل شدن به حادثه پایانی جلوگیری کند. عملکرد هر لایه حفاظتی مستقل از رخ داد اولیه و عملکرد هر لایه حفاظتی دیگر می‌باشد.

پس از شناسایی لایه‌های حفاظتی مستقل، ریسک مربوط به حادثه پایانی از حاصل‌ضرب فرکانس مربوط به رخداد اولیه در احتمال خرابی لایه‌های حفاظتی مستقل موجود در لحظه تقاضا محاسبه می‌گردد(۲). فرمول‌های ۳ و ۴ محاسبه سطح ریسک موجود برای هر حادثه پایانی را نشان می‌دهد.

$$f_i^C = f_i^I \times \prod_{j=1}^{J} PFD_{ij} \qquad (۳)$$

$$f_i^C = f_i^I \times PFD_{i1} \times PFD_{i2} \times \ldots \times PFD_{ij} \qquad (۴)$$

f_i^C: فرکانس پیامد برای سناریو i

f_i^I: فرکانس رویداد اولیه i

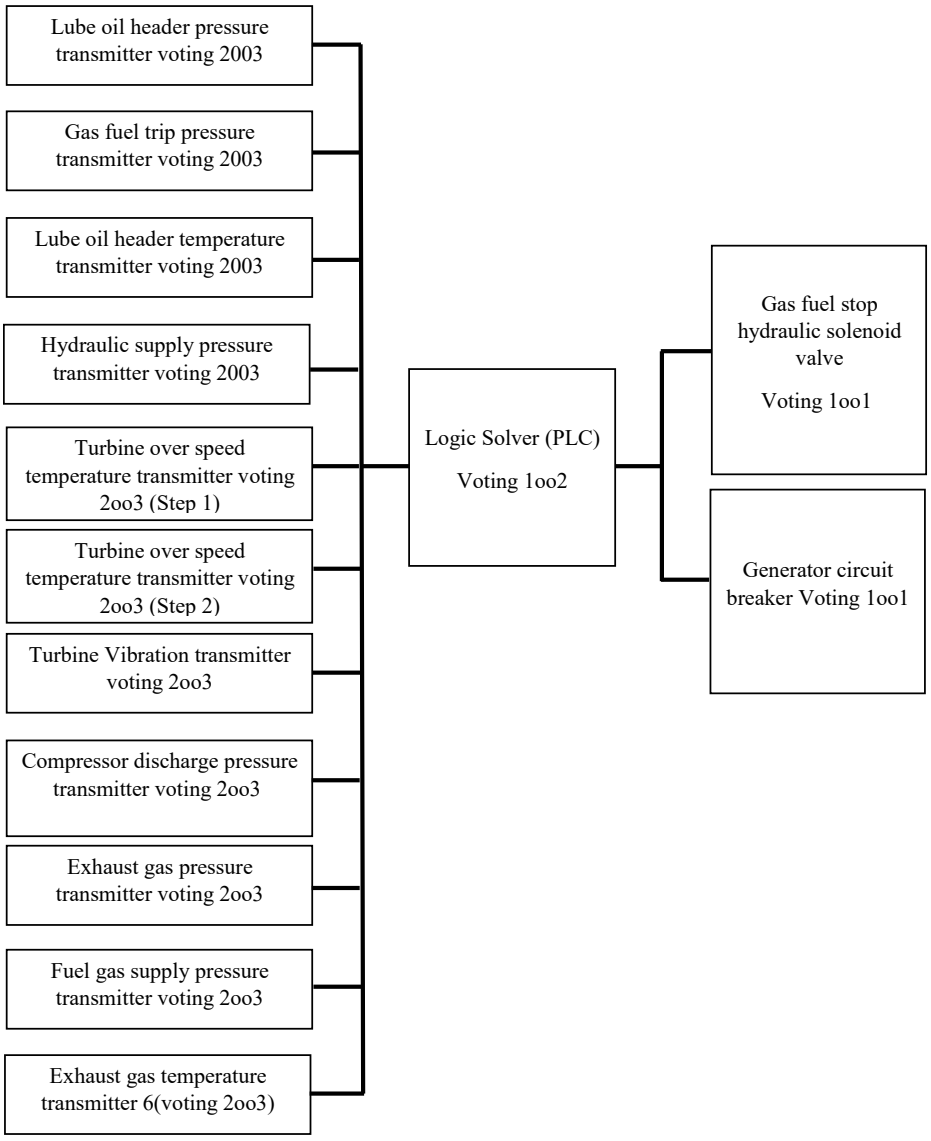
PFD_{ij}: احتمال عمل نکردن لایه حفاظتی ژام در لحظه‌ای که به آن نیاز است.

تایید و راستی آزمایی سطح یکپارچگی ایمنی (SIL) (Verification

استانداردهای IEC 61508 و IEC 61511 الزامات یکپارچگی ایمنی را برای سیستم‌های ابزار دقیق ایمنی که در صنایع فرآیندی استفاده می‌شوند بیان می‌کنند. دستیابی به سطح یکپارچگی ایمنی هدف برای یک عملکرد سیستم ابزاردقیق ایمنی، به پارامترهای زیر بستگی دارد: ۱) خرابی‌های تصادفی سخت‌افزار که با محاسبه میانگین احتمال خرابی در زمان تقاضا PFD_{avg} و در نظر گرفتن نرخ خرابی‌های خطرناک بدست می‌آید، ۲) قابلیت اطمینان سخت‌افزار که تابع دو پارامتر تحمل خطای سخت افزاری (HFT) و نسبت خرابی‌های ایمن (SFF) می‌باشد، ۳) قابلیت سیستماتیک که با محاسبه خرابی‌های سیستماتیک (خرابی‌های ناشی از نرم‌افزار، تداخل الکترونیکی، روش استفاده متفاوت با طراحی و ...) بدست می‌آید. در واقع برای اطمینان از این که یک عملکرد سیستم ابزار دقیق ایمنی بتواند الزامات مربوط به SIL هدف را برآورده کند هر سه محدودیت فوق بایستی در نظر گرفته شود(۱۵، ۲۵، ۲۶). در این مطالعه عملکرد سیستم ابزاردقیق ایمنی شامل از سرویس خارج کردن ناگهانی توربین گازی و ژنراتور می‌باشد، جهت انجام این عملکرد حسگرهای سیستم ابزاردقیق ایمنی بایستی شرایط غیر نرمال (مانند افزایش دمای روغن خنک‌کننده، سرعت دوران بالای توربین و یا لرزش بیش از حد توربین و ژنراتور) را شناسایی کرده و مرکز کنترل (DCS) فرمان

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]



شکل ۷: سیستم ابزار دقیق ایمنی توربین گازی و ژنراتور مورد مطالعه

قطع گاز ورودی به مشعل‌ها را از طریق بستن ناگهانی شیر کنترل اصلی گاز ورودی به مشعل‌ها صادر کند، با بسته شدن ناگهانی شیر کنترل اصلی گاز، توربین از سرویس خارج می‌شود.

خرابی‌های تصادفی سخت‌افزار (Random Harware Failure)

خرابی‌های تصادفی سخت‌افزار جهت محاسبه میانگین احتمال خرابی در زمان تقاضا (PFD_{avg}) بکار می‌روند. استاندارد IEC 61508 Part-6 تعدادی فرمول را برای محاسبه مربوط به برخی از ساختارهای معماری MooN ارائه داده است. هر سیستم ابزار دقیق ایمنی دارای چند زیرسیستم و هر زیرسیستم دارای یک یا چند گروه با اکثریت رأی (Voting) می‌باشد و هر گروه با اکثریت رأی دارای یک ساختار معماری M-out-of-N مانند 1oo1، 1oo2، 1oo3، 1oo2D، 2oo2 یا 2oo3 می‌باشد(۲۷). سطح دسترسی عملکرد سیستم ابزاردقیق ایمنی به مواردی همچون نرخ خرابی‌های ایمن و خطرناک، نرخ خرابی‌های

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

جدول۶: اطلاعات مربوط به محاسبه زیرسیستم‌های سیستم ابزار دقیق ایمنی توربین گازی

زیر سیستم	سازنده	ساختار معماری	λ_D	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	DC	β	TI
سنسور فشار روغن	**Yokogawa**	2oo3	0.376	0.000	0.055	0.338	0.036	90%	٪5	2سال
سنسور دمای روغن	**Yokogawa**	2oo3	0.663	0.193	0.04	0.06	0.063	٪90	٪5	2سال
سنسور سرعت دوران	**SHINKAWA**	2oo3	0.242	0.00	0.012	0.089	0.153	٪40	٪5	2سال
سنسور لرزش	**SHINKAWA**	2oo3	0.242	0.00	0.012	0.089	0.153	٪40	٪5	2سال
پردازشگر مرکزی (LS)	**Yokogawa**	1oo2	4.800	1.000	3.800	4.320	0.480	٪90	٪5	2سال
شیر کنترلی تخلیه فشار روغن (Hydraulic Solenoid Valve)	**MULER coax**	1oo1	1.100	1.100	1.700	0.300	0.800	٪30	٪3	2سال
سنسور قطع جریان برگشتی (Circuit breaker)	**Siemens**	1oo1	0.300	0.000	0.500	0.000	0.300	٪30	٪3	2سال

نکته 1: تمامی نرخ های خرابی بر اساس **0.000001** ساعت می باشد. برای ساختار ترکیب بندی **1oo1** (یک از یک) مقدار فاکتور β تاثیری بر مقدار PFD_{avg} ندارد.

نکته 2: $DC = \frac{\lambda_{DD}}{\lambda_D}$ ، $MTTR = MRT = 8h$ ، **A:** در دسترس بودن

قابل‌شناسایی و غیرقابل‌شناسایی، میانگین زمان تعمیر تا در سرویس قرار گرفتن مجدد (MTTR)، نوع معماری یا ساختار ترکیب‌بندی اجزاء (Architecture)، قابلیت پوشش تشخیصی (Diagnostic Coverage)، مدت‌زمان آزمودن‌های دوره‌ای (Test Time Interval) و فاکتور بتا â برای خرابی‌های با علت مشترک (CCF) بستگی دارد(۲۴، ۲۵، ۲۷-۲۹). در جدول ۵ ارتباط بین انواع خرابی‌هایی که برای سیستم ابزار دقیق ایمنی رخ می‌دهد نشان داده‌شده است.

اگر هر زیرسیستم برای (مثال زیرسیستم سنسور) شامل بیشتر از یک گروه با اکثریت رأی باشد، احتمال خرابی در زمان تقاضا برای هر زیرسیستم از حاصل جمع احتمال خرابی همه گروه‌ها به دست می‌آید(۵، ۲۸).

در این تحقیق، ابتدا سیستم ابزار دقیق ایمنی که دارای اجزای زیرسیستم سنسور (ورودی)، زیرسیستم حل‌کننده منطقی، و اجزای زیرسیستم عملگر نهایی (خروجی) است، ترسیم گردید(۵). در شکل ۷ اجزای سیستم ابزار دقیق ایمنی توربین گازی موردمطالعه نشان داده‌شده است. سپس اجزای هر زیرسیستم، که دارای یک یا چند گروه با اکثریت رأی (گروه‌های با اجزای چندتایی یا M عنصر از N عنصر) می‌باشد شناسایی گردید.

بر اساس نظر خبرگان، مدت‌زمان آزمایش اثبات (TI) برای سنسورها و حل‌کننده منطقی دو سال و برای عملگرهای پایانی ۱ سال در نظر گرفته شده است. همچنین یک مدت‌زمان هشت‌ساعته برای میانگین زمان تعمیر (MRT) و میانگین زمان در سرویس قرار گرفتن مجدد (MTTR) هر یک از خرابی‌ها در نظر گرفته شده است. سپس نرخ خرابی‌های خطرناک قابل‌شناسایی و غیرقابل‌شناسایی و نرخ خرابی‌های ایمن قابل‌شناسایی و غیرقابل‌شناسایی از منابعی مانند Exida، TUV و شرکت سازنده (Yokogawa، SHINKAWA، MULLER coax)، استخراج گردید. مقدار عددی فاکتور β برای خرابی‌های با دلایل مشترک از کتاب راهنمای PDS DATA HANDBOOK استخراج گردید(۳۰). داده‌های مربوط به متغیرهای محاسبه PFD_{avg} برای زیرسیستم‌های سیستم ابزار دقیق ایمنی توربین گازی موردمطالعه در جدول ۶ نشان داده‌شده است.

مقدار PFD_{avg} از حاصل جمع میانگین احتمال خرابی در زمان تقاضای سه زیرمجموعه سنسور، حل‌کننده منطقی و عملگر پایانی محاسبه گردید. سپس سطح دسترسی عملکرد سیستم ابزار دقیق ایمنی با استفاده از فرمول ۱۰ محاسبه گردید(۲۸).

$$PFD_S = \sum_i PFD_{Gi} \qquad (۵)$$

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE} \quad (۶)$$

$$PFD_{1oo1} = \left(\lambda_{DU} + \lambda_{DD}\right) t_{CE} \quad (۷)$$

$$PFD_{1oo2} = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{TI}{2} + MRT\right) \quad (۸)$$

$$PFD_{2oo3} = 6\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{TI}{2} + MRT\right) \quad (۹)$$

$$\text{Safety Availability} = 1 - PFD_{avg} \quad (۱۰)$$

فرمول‌های ۷، ۸ و ۹ محاسبه PFD_{avg} برای حالت‌های با تقاضای کم، از استاندارد IEC 61508-2010 Part-6 برای ساختارهای معماری 1oo1، 1oo2 و 2oo3 که در سیستم ابزار دقیق ایمنی توربین گازی موردمطالعه وجود دارد را نشان می‌دهد. زمانی که زیرسیستم از چند جزء تشکیل‌شده است، و نیاز به محاسبه PFD با نرخ خرابی ترکیبی از اجزاء می‌باشد، لازم است که یک مقدار ثابت برای میانگین زمان از سرویس خارج شدن تجهیز (MDT) در نظر گرفته شود(۲۸). مقادیر t_{CE} و t_{GE} مدت‌زمان از سرویس خارج شدن معادل تجهیز را نشان می‌دهند که با استفاده از فرمول‌های ۱۱ و ۱۲ محاسبه‌شده‌اند:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{TI}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MRT \quad (۱۱)$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{TI}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MRT \quad (۱۲)$$

t_{CE}: میانگین زمان از سرویس خارج شدن معادل برای ساختارهای معماری 1oo1، 1oo2 و 2oo3

t_{GE}: میانگین زمان از سرویس خارج شدن معادل برای ساختارهای معماری 1oo2 و 2oo3

استاندارد IEC 61508 Part-6 فرمول‌های محاسبه PFD را برای تعداد خاصی از ساختارهای معماری (MooN) پیشنهاد می‌کند (1oo1، 1oo2، 1oo2D، 2oo2، 1oo3، 2oo3). این فرمول‌ها تنها شش حالت ترکیبی را شامل می‌شوند و به‌راحتی نمی‌توان آن‌ها را به حالت‌های ترکیبی دیگر تعمیم داد، برای مثال برای ساختارهای 2oo4 و 3oo5 فرمولی ارائه نداده است. در سال ۲۰۱۴ حمید جهانیان، از بخش انرژی شرکت زیمنس، مطالعات گسترده‌ای را بر روی فرمول‌های IEC 61508 Part-6 برای ساختارهای MooN مربوط به SIS انجام داد و بر اساس یک تجزیه‌وتحلیل دقیق توانست یک فرمول کلی برای به دست آوردن PFD مربوط به تمام ساختارهای MooN ارائه دهد. فرمول GPFDF خرابی‌های با دلایل مشترک، خرابی‌های خطرناک قابل‌شناسایی و غیرقابل‌شناسایی، میانگین زمان در سرویس قرارگیری مجدد، مدت‌زمان آزمودن تشخیص، و میانگین زمان مورد نیاز برای تست تشخیص را شامل می‌شود(۲۷). در این تحقیق مقدار احتمال خرابی در زمان تقاضا برای عملکرد سیستم ابزار دقیق ایمنی توربین گازی و ژنراتور مورد مطالعه با فرمول GPFDF نیز انجام گردید و نتایج به‌دست‌آمده با نتایج حاصل از استاندارد IEC 61508 مقایسه گردید. فرمول ۱۳ فرمول کلی جهانیان را نشان می‌دهد، فرمول‌های ۱۶، ۱۷ و ۱۸ فرمول‌های محاسبه PFD_{avg} برای ساختارهای معماری 1oo1، 1oo2 و 2oo3 می‌باشند که از فرمول GPFDF استخراج‌شده‌اند.

$$PFD_{koon} = \prod_{i=1}^{n-k+1} N_i \lambda_D D_i + PFD_{CCF} \quad (۱۳)$$

$$PFD_{CCF} = \beta \lambda_{DU}\left(\frac{\tau}{2} + PPT + MRT\right) + \beta_D \lambda_{DD} MRT \quad (۱۴)$$

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

$$D_i = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{i+1} + PPT + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (۱۵)$$

$$PFD_{1oo1} = \lambda_D D_i + PFD_{CCF} \quad (۱۶)$$

$$PFD_{1oo2} = 2(\lambda_D)^2 D_1 D_2 + PFD_{CCF} \quad (۱۷)$$

$$PFD_{1oo2} = 6(\lambda_D)^2 D_1 D_2 + PFD_{CCF} \quad (۱۸)$$

قابلیت اطمینان سخت افزار (Hardware safety integrity)

قابلیت اطمینان سخت‌افزار با روش Route 1H براساس تحمل خطای سخت‌افزار (HFT) و کسر خرابی‌های ایمن (Safe Failure Fraction) تعیین می‌شود. تحمل خطا توانایی سیستم ابزاردقیق ایمنی برای انجام اقدامات مورد نظر (و یا عدم انجام اقدامات ناخواسته) در صورت خرابی یک یا چند جزء از سیستم ابزاردقیق ایمنی است. تحمل خطا معمولا از طریق یک یا چند مولفه اضافی تامین می‌شود که اصطلاحا به آن "گروه با اکثریت رأی" گفته می‌شود و بر اساس عملکرد سیستم ابزار دقیق ایمنی تنظیم می‌شود. هر زیر سیستم مربوط به عملکرد سیستم ابزاردقیق ایمنی از یک یا چند گروه با اکثریت رأی تشکیل شده است که ممکن است معماری‌های مشابه یا متفاوت داشته باشند. تحمل خطا بیانی از تعداد خطاها یا خرابی‌هایی است که یک "گروه با اکثریت رأی" می‌تواند تحمل کند و عملکرد سیستم ابزاردقیق ایمنی در صورت بروز چنین خطایی به درستی اجرا شود. میزان تحمل خطا برای هر گروه با اکثریت رای تابعی از معماری آن می‌باشد. که در جدول ۷ نشان داده شده است(۱۵، ۲۶).

کسر خرابی‌های ایمن (SFF) برای هر تجهیز، جزء یا زیر سیستم مورد استفاده در عملکرد سیستم ابزاردقیق ایمنی محاسبه می‌شود. هر تجهیز از n جزء ساخته شده است و هر یک از آن‌ها داری نرخ شکست مخصوص به خود (λ) است. کسر خرابی‌های ایمن با استفاده از فرمول ۱۹ محاسبه می‌شود(۱۵، ۲۶):

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{Dd}}{\sum \lambda_S + \sum \lambda_{Dd} + \sum \lambda_{Du}} \quad (۱۹)$$

استاندارد IEC 61508 Part-2 حداقل تحمل خطای سخت افزاری را برای سطح SIL مورد نیاز تعریف می‌کند. دستگاه‌های نوع B به هر وسیله‌ای که به نحوی ریز پردازنده (حل‌کننده منطقی) است توصیف می‌شود، دستگاه‌های نوع A همه دستگاه‌های دیگر (حسگر، عملگر پایانی و حل‌کننده منطقی غیر قابل برنامه ریزی) را شامل می‌شود. اگر الزامات IEC 61508 Part-2 برای تحمل خطا برآورده شود، طراحی مفهومی مناسب است و می‌توان ادعا کرد که SIL مورد نیاز به دست آمده است. اگر حداقل تحمل خطای سخت افزاری مورد نیاز با روش بالا برآورده نشود، ممکن است توصیه‌ای برای افزایش تحمل خطای سخت‌افزار و دست یابی به SIL مورد نیاز ضروری باشد(۱۵، ۲۵، ۲۶). جدول ۸ تعیین SIL را بر

جدول ۷: تحمل خطای سخت افزاری مربوط به هر معماری (گروه با اکثریت) (۲۶)

ساختار معماری زیر سیستم (Sub-system Architecture (Voting))	تحمل خطای سخت افزاری (Hardware Fault Tolerance)
1oo1	0
1oo2	1
2oo2	0
2oo3	1
1oo3	2

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

جدول ۸: حداقل SIL مجاز برای یک عملکرد ایمنی که توسط یک عنصر یا زیر سیستم نوع A و یا B انجام می شود (۱۵, ۲۶)

کسر خرابی های ایمن (SFF) برای هر عنصر یا زیرسیستم	تحمل خطای سخت افزار (HFT)		
	0	1	2
Type A			
< 60%	SIL 1	SIL 2	SIL 3
60% – < 90%	SIL 2	SIL 3	SIL 4
90% – < 99%	SIL 3	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4
Type B			
< 60%	Not Allowed	SIL 1	SIL 2
60% – < 90%	SIL 1	SIL 2	SIL 3
90% – < 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

اساس تحمل خطای سخت افزاری و کسر خرابی‌های ایمن نشان می‌دهد:

قابلیت سیستماتیک (Systematic Capability)

بدیهی است که برآورده شدن الزامات یکپارچگی ایمنی سخت‌افزار جهت دستیابی به SIL مورد نیاز بسیار مهم است. اما این تا حد زیادی خرابی‌های مرتبط با خرابی‌های تصادفی سخت‌افزار بر اساس یک محیط کاری مشخص را پوشش می‌دهد. عوامل دیگری نیز وجود دارد که ممکن است باعث عدم اجرای عملکرد ایمنی شوند، به عنوان مثال یک خطا در فرآیند طراحی سخت‌افزار می‌تواند باعث شود که سخت‌افزار زودتر از زمان مورد انتظار از کار بیافتد، یا ممکن است یک عضو در شرایطی متفاوت از آنچه که در شرایط طراحی توصیه شده استفاده شود و تحت تنش فرآیندی قرار بگیرد. علاوه بر این خرابی‌های ناشی از نرم‌افزار و خرابی‌های تداخل الکترونیکی نیز ممکن است باعث عدم اجرای عملکرد ایمنی شوند. شناسایی تعداد خرابی‌های این نوع دشوار است و توسط محاسبه PFD_{avg} پوشش داده نمی‌شود، چنین خرابی‌هایی را خرابی‌های سیستماتیک می‌نامند(۱۵، ۱۶).

استاندارد IEC 61508 Part-2 جداولی را ارائه می‌دهد که اقدامات لازم برای کنترل خرابی‌های سیستماتیک در حین عملیات را پوشش می‌دهد، به طوری که اگر یک خطای سیستماتیک رخ دهد، شناسایی شود و اقدام مناسب انجام شود. هر چه سختی اقدامات اعمال شده در طول چرخه عمر سیستم بالاتر باشد، و دستورالعمل‌های مربوط به تعمیر و نگهداری تست‌های دوره‌ای به درستی اجرا شود، سطح اطمینان بیشتری وجود دارد که عملکرد سیستم ابزاردقیق ایمنی بدرستی انجام شود، این سطح اطمینان در واقع قابلیت سیستماتیک نامیده می‌شود. به عنوان مثال اگر یک حسگر تمام نیازهای PFD برای SIL3 و تمام الزامات تحمل خطای سخت افزاری (HFT) برای SIL3 را به عنوان یک دستگاه ساده (HFT=0، Voting=1oo1) برآورده کند، اما قابلیت سیستماتیک فقط الزامات SIL2 را برآورده کند، در نتیجه این حسگر در نهایت فقط الزامات SIL2 را برآورده خواهد کرد. در این تحقیق برای هر عضو، اعداد مربوط به قابلیت سیستماتیک که الزامات مربوط به سطح SIL را بر اساس طراحی و ساخت سازنده بیان می‌کند، از گواهی سازنده استخراج شده است(۱۵، ۱۶).

یافته ها

در این بخش نتایج حاصل از انجام مطالعات HAZOP، تعیین سطح SIL با استفاده از روش نمودار ریسک کالیبره شده و LOPA و نتایج حاصل از تایید سطح SIL مربوط به عملکرد سیستم ابزار دقیق ایمنی توربین گازی موردمطالعه مطابق با الزامات مربوط به

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

خرابی‌های تصادفی سخت‌افزار، تحمل خطای سخت‌افزار و قابلیت سیستماتیک آورده شده است.

یافته‌های حاصل از مطالعات HAZOP

در این تحقیق مطالعات عملیات و خطر (HAZOP) بر روی مسیرهای فرآیندی روغن روان‌کننده و خنک‌کننده (Lube oil system)، سیستم تأمین هوای خنک‌کننده و پاکسازی محفظه احتراق (Cooling and sealing air system)، سیستم روغن هیدرولیک مخصوص از سرویس خارج کردن توربین گازی (Trip oil system)، سیستم تأمین خوراک گاز طبیعی مشعل‌ها (Fuel gas system)، سیستم روغن هیدرولیک تنظیم‌کننده شیر ورودی هوا به کمپرسور (Hydraulic supply system to inlet guide vane control ring) در توربین گازی موردمطالعه انجام شد.

جدول ۹ خلاصه نتایج مطالعات HAZOP را برای ۷ انحراف نشان می‌دهد. با توجه به استفاده از گاز طبیعی به‌عنوان سوخت مشعل‌ها و سرعت دوران بالای توربین گازی، شدت پیامدها در سطح بالایی تخمین زده شد، اما با توجه به حفاظ‌های موجود، احتمال وقوع پیامدها

جدول ۹: شناسایی خطرات فرآیندی (HAZOP) توربین گازی و ژنراتور مورد مطالعه

انحراف	دلیل	پیامد پایانی	حفاظهای ایمنی	L	S	RR
1) کاهش فشار روغن خنک کننده و روان کننده	1-1) پمپ اصلی روغن خراب شود	1) افزایش دمای روغن و آسیب به یاتاقان ها و سیستم های دوار 2) کاهش فشار روغن هیدرولیک و بسته شدن شیر کنترل اصلی گاز و از سرویس خارج شدن توربین گازی و ژنراتور	1) در سرویس قرار گرفتن اتومات پمپ روغن اضطراری با برق باتری(DC) 2) سنسور کاهش فشار روغن (PIT-L&LL) 3) آلارم کاهش فشار و آلارم افزایش دمای روغن 4) سیستم ابزاردقیق ایمنی (SIS)	2	4	8
	1-2) قطع برق AC و از سرویس خارج پمپ AC		1) سنسور کاهش فشار روغن (PIT-L&LL) 2) آلارم کاهش فشار و آلارم افزایش دمای روغن 3) سیستم ابزاردقیق ایمنی (SIS)	2	5	10
2) افزایش دمای روغن خنک کننده و روان کننده	2-1) خرابی مبدل خنک کننده روغن	1) آسیب به گیربکس، یاتاقان‌ها و شفت	1)سنسور و آلارم افزایش دمای روغن خنک کننده 2) سنسور دما بر روی یاتاقان‌ها و گیربکس	3	4	12
3) کاهش فشار روغن هیدرولیک، تنظیم کننده شیر کنترل هوای ورودی به کمپرسور	3-1) خرابی پمپ اصلی روغن هیدرولیک	1) کاهش فشار روغن هیدرولیک و بسته شدن شیر کنترل اصلی گاز و از سرویس خارج شدن توربین گازی و ژنراتور 2) بسته شدن شیر کنترل تنظیم هوای ورودی به کمپرسور، افزایش دمای کمپرسور و توربین، آسیب به کمپرسور و توربین، بد سوزی مشعل ها	1) سیستم کنترل فرآیند BPCS بصورت خودکار پمپ دوم را در سرویس قرار می‌دهد 2) سیستم ابزاردقیق ایمنی (SIS)، توربین گازی را از سرویس خارج می کند 3) آلارم کاهش فشار روغن هیدرولیک	2	4	8
	3-2) فیلترهای روغن هیدرولیک مسدود شوند		2) سیستم ابزاردقیق ایمنی (SIS)، توربین گازی را از سرویس خارج می کند 3) آلارم کاهش فشار روغن هیدرولیک 4) سنسور تشخیص اختلاف فشار روغن در دو طرف فیلتر(Pressure difference transmitter)	2	4	8
4) کاهش فشار هوای خنک کننده و پاک کننده محفظه احتراق	4-1) گرفتگی فیلترهای مسیر هوای ورودی به کمپرسور	1) تجمع گاز در محفظه ی احتراق و احتمال انفجار در زمان جرقه زدن 2) افت فشار هوای خنک کننده، و سوختگی پره های توربین و کمپرسور 3) افت فشار هوا در محفظه احتراق و کاهش دور توربین	سیستم مدیریت مشعل‌ها (BMS) (BPCS for Burner Management System) 1) سیستم ابزار دقیق ایمنی، سنسور خطی (LVDT)، میزان بسته شدن IGV را تشخیص می‌دهد و PLC فرمان بسته شدن SRV را صادر می‌کند 2) سیستم پاک‌سازی خودکار فیلترها 3) سنسور 2oo3 فشار هوا بر روی کمپرسور 4) طراحی ذاتاً ایمن تیغه‌های IGV ، این تیغه‌ها در کمترین حالت به میزان 27 درجه باز می‌باشند. 5) آلارم افت فشار هوا	2	4	8
	4-2) خرابی کمپرسور					
	4-3) افت فشار روغن هیدرولیک که باعث بسته شدن IGV می شود					
	4-4) بد عمل کردن IGV، و بسته شدن مسیر هوا					

L:Likelihood (احتمال) , R: Severity (شدت) , RR: Risk Ranking (سطح ریسک)

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

ادامه جدول ۹: شناسایی خطرات فرآیندی (HAZOP) توربین گازی

انحراف	دلیل	پیامد پایانی	حفاظهای ایمنی	L	S	RR
5) افزایش فشار گاز طبیعی	5-1) افزایش فشار گاز طبیعی از بالادست مانند بدعمل کردن رگلاتور گاز.	1) نشت گاز قابل اشتعال از محل فلنج ها و آتش سوزی و انفجار 2) افزایش دما در خروجی گازهای حاصل از احتراق و آسیب دیدن پره های توربین 3) افزایش بیش از حد سرعت دوران و لرزش توربین و ژنراتور و کمپرسور و آسیب به پره های توربین، پره های کمپرسور و آسیب به شفت و یاتاقان ها	1) دو عدد شیر کنترل فشار بر روی ظرف جدا کننده گاز از مایع همراه (K.O.Drum) 2) سنسور افزایش فشار گاز (PIT) و دستورالعمل عملیاتی جهت اقدام اپراتور 3) سنسور دما در خروجی حلقه مانند مشعل ها 4) دوازده عدد سنسور دما در مراحل 1 تا 3 توربین 5) هجده عدد سنسور دما در داکت خروجی گازهای حاصل از احتراق 6) سنسور کنترل افزایش سرعت توربین (Over Speed sensor)	2	3	6
	5-2) بد عمل کردن شیر کنترل اصلی گاز طبیعی به مشعل ها (SRV)		1) سنسور خطی LVDT، باز شدن بیش از حد SRV را در اثر افزایش فشار گاز ثبت و کنترل می کند 2) سنسور دما در خروجی حلقه مانند مشعل ها 3) دوازده عدد سنسور دما در مراحل 1 تا 3 توربین 4) هجده عدد سنسور دما در داکت خروجی گازهای حاصل از احتراق 5) سنسور کنترل افزایش سرعت توربین (Over Speed sensor)			
6) کاهش فشار گاز طبیعی	6-1) مسدود شدن فیلتر های گاز در اثر آلودگی	1) کاهش فشار و یا قطع گاز ورودی به توربین و از سرویس خارج شدن توربین، ژنراتور و قطع تولید برق	1) سنسور خطی LVDT، میزان باز یا بسته بودن شیر کنترل اصلی گاز ورودی SRV 2) سنسور دما در خروجی حلقه مانند مشعل ها 3) هجده عدد سنسور دما داکت خروجی گازهای حاصل از احتراق 4) دوازده عدد سنسور دما در مراحل 1 تا 3 توربین 5) سنسور های ثبت اختلاف فشار (Differential Pressure) در دو طرف فیلتر	2	3	6
	6-2) بد عمل کردن شیر کنترل اصلی فشار گاز و بسته شدن آن					
	6-3) کاهش فشار از تامین کننده گاز					
7) افزایش لرزش در اجزای ژنراتور و توربین	7-1) جدا شدن یک قطعه از روتور و آسیب به اجزای سیم پیچ در استاتور	1) شکستگی در اجزای توربین و ژنراتور مانند شکسته شدن شفت	1) سنسور های ثبت لرزش بر روی شفت 2) قطع گاز ورودی توسط بسته شدن شیر کنترل گاز اصلی (SRV)	3	3	9

جدول ۱۰: کار برگ تعیین SIL با روش نمودار ریسک کالیبره شده جهت کاهش فشار روغن خنک کننده

توصیف انحراف و پیامد پایانی	دلیل	C	F	P	W	SIL
کاهش فشار روغن روان کننده و خنک کننده، آسیب به ژنراتور و توربین و قطع برق واحد های پایین دست	خرابی پمپ اصلی روغن	C3	F1	P2	W2	**SIL2**
	قطع برق AC و در سرویس قرار نگرفتن پمپ اضطراری	C3	F1	P2	W2	**SIL2**
افزایش دمای روغن در هدر روغن، گیربکس و یاتاقان‌ها، خرابی یاتاقان‌ها و گیربکس و خرابی ژنراتور و توربین و قطع برق	خرابی کولر روغن و یا قطع آب‌خنک کننده	C3	F2	P1	W2	**SIL2**
	افزایش فشار بخار روغن در مخزن روغن (افت خلأ)	C3	F1	P1	W2	**SIL1**

کاهش‌یافته و سطح ریسک بیشتر پیامدها در محدوده قابل‌قبول و سطح ریسک برخی از پیامدها در محدوده ALARP قرار می‌گیرد. این بدان معنی است که بر اساس مطالعات ارزیابی ریسک کیفی HAZOP، توربین گازی مورد مطالعه دارای حفاظهای ایمنی کافی برای پاسخگویی به وضعیت‌های خطرناک می‌باشد.

یافته‌های حاصل از تعیین SIL

با استفاده از خروجی ارزیابی ریسک به روش HAZOP سناریوهای خطرناک شناسایی شد و با روش نمودار ریسک کالیبره شده و مطالعات LOPA جهت تعیین سطح SIL مورد ارزیابی قرار گرفت. شکل ۲ نمودار ریسک کالیبره شده از IEC 61511 Part-3 را نشان می‌دهد. برای هر سناریو سطح SIL با دنبال کردن هر شاخه و انتخاب هر یک از پارامترها در عدم وجود SIF به دست آمد. کاربرگ نمودار ریسک کالیبره شده برای سناریو کاهش فشار روغن خنک‌کننده و روان‌کننده در جدول ۱۰ نشان داده‌شده است (۱۱). نتایج نمودار ریسک کالیبره شده بر روی ۱۱ انحراف از حالت نرمال عملیاتی نشان داد که ۷ انحراف نیاز به سطح SIL2 و ۴ انحراف

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

جدول ۱۱: کار برگ تعیین SIL با روش LOPA جهت کاهش فشار روغن خنک کننده

پیامد حادثه	واقعه اولیه			IPLs				
	توصیف واقعه اولیه	IEL (Freq. per year)	TRL	نوع لایه حفاظتی	توصیف لایه حفاظتی	PFD	IRL	SIL
کاهش فشار روغن روان کننده و خنک کننده، آسیب به ژنراتور و توربین و قطع برق واحد های پایین دست	پمپ اصلی روغن خنک کننده خراب شود	10^{-1}	10^{-6}	سیستم کنترل فرآیند (BPCS)	PIT, TCP, DCS	10^{-1}	10^{-3}	SIL2
				آلارم و دخالت نفر اپراتور (Alarm & Process intervention)	آلارم کاهش فشار و دستورالعمل بهره برداری	10^{-1}		
	قطع برق AC و در سرویس قرار نگرفتن پمپ اضطراری	10^{-1}	10^{-6}	سیستم کنترل فرآیند (BPCS)	PIT- TCP, DCS.	10^{-1}	10^{-3}	SIL2
				آلارم و دخالت نفر اپراتور (Alarm & Process intervention)	آلارم کاهش فشار و دستورالعمل بهره برداری	10^{-1}		

IEL: Initiating Event Likelihood, TRL: Tolerable Risk Likelihood, IRL: Intermediate Risk Likelihood

نیاز به سطح SIL3 دارد. این نتایج در جدول ۱۲ نشان داده‌شده است.

روش آنالیز لایه‌های حفاظتی مستقل (LOPA) نسبت به روش نمودار ریسک کالیبره شده کمی‌تر است. جهت انجام مطالعات LOPA در ابتدا تمامی لایه‌های حفاظتی مستقل (IPL) مربوط به دلیل و پیامد شناسایی و ثبت گردید. هر لایه حفاظتی مستقل دارای یک احتمال شکست در زمان تقاضا (PFD_{avg}) می‌باشد که از کتاب‌های راهنمای CCPS استخراج گردید(۳۱). در این تحقیق سطح ریسک قابل‌پذیرش سازمان برابر 10^{-6} در نظر گرفته‌شده است(۳۲، ۳۳). روش LOPA یک تصویر واضح از لایه‌های حفاظتی مستقل و واقعه اولیه را نشان می‌دهد. با استفاده از فرمول‌های ۳ و ۴ سطح ریسک موجود از حاصل‌ضرب احتمال شکست در زمان تقاضا برای هر IPL و تکرارپذیری واقعه اولیه به دست آمد. از تقسیم سطح ریسک موجود بر سطح ریسک قابل‌پذیرش، فاکتور کاهش ریسک محاسبه گردید سپس تعیین SIL با توجه به مقدار فاکتور کاهش ریسک انجام شد. کار برگ LOPA برای انحراف کاهش فشار روغن خنک‌کننده و روان‌کننده در جدول ۱۱ نشان داده‌شده است(۱۱).

آنالیز ۱۱ سناریو با استفاده از روش LOPA و بر اساس تعداد و نوع لایه‌های حفاظتی موجود، نشان می‌دهد برای تمامی سناریوها سطح SIL2 موردنیاز می‌باشد (جدول ۱۲). برای انحراف کاهش فشار روغن، به دلیل خرابی پمپ اصلی روغن و آسیب به توربین، محاسبه فاکتور کاهش ریسک و تعیین SIL در زیر آورده شده است:

$$\text{Actual Risk} = f_i^C = f_i^1 \times \prod_{j-1}^{J} PFD_{ij} = 10^{-1} \times 10^{-1} \times 10^{-1} = 10^{-3}$$

$$RRF = \frac{10^{-3}}{10^{-6}} = 1000 \quad \text{if} \quad 1000 \le RRF < 100 \quad \rightarrow \quad SIL = 2$$

نتایج حاصل از تعیین SIL با استفاده از دو روش LOPA و نمودار ریسک کالیبره شده در جدول ۱۲ آورده شده است.

یافته‌های حاصل از تایید سطح یکپارچگی ایمنی (SIL Verification)

جهت تایید حداکثر سطح یکپارچگی ایمنی برای عملکرد سیستم ابزاردقیق ایمنی در رابطه با خرابی‌های سخت افزاری تصادفی خطرناک ابتدا می‌بایست احتمال خرابی در زمان تقاضا (PFD_{avg}) محاسبه گردد. سیستم ابزار دقیق توربین گازی، برای از سرویس خارج کردن توربین گازی (Gas Turbine and Generator Trip)، دارای زیرسیستم سنسور با ۱۱ گروه با اکثریت رأی،

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

جدول ۱۲: مقایسه نتایج تعیین SIL با استفاده از دو روش نمودار ریسک و آنالیز لایه‌های حفاظتی

انحراف از حالت نرمال	فاکتور کاهش ریسک با استفاده از روش LOPA	تعیین سطح SIL با استفاده از روش نمودار ریسک کالیبره شده	تعیین سطح SIL با استفاده از روش LOPA
کاهش فشار روغن (Low lube oil pressure)	1000	SIL2	SIL2
افزایش فشار در هدر روغن (Lube oil header high temperature)	1000	SIL2	SIL2
کاهش فشار روغن هیدرولیک (Gas Fuel Hydraulic Low Pressure)	1000	SIL2	SIL2
کاهش فشار روغن ساپلای تنظیم کننده میزان هوای ورودی (Hydraulic supply low pressure)	1000	SIL2	SIL2
افزایش سرعت دوران توربین (Turbine over speed 1)	1000	SIL2	SIL2
افزایش سرعت دوران توربین (Turbine over speed 2)	1000	SIL3	SIL2
لرزش بالا (High vibration)	1000	SIL3	SIL2
کاهش فشار هوا در خروجی کمپرسور (Loss of compressor discharge pressure)	1000	SIL2	SIL2
کاهش فشار گاز ورودی (Fuel gas supply low pressure)	1000	SIL2	SIL2
افزایش فشار در خروجی توربین گازی (Exhaust gas high pressure)	1000	SIL3	SIL2
افزایش دما در خروجی توربین گازی (Exhaust high temperature)	1000	SIL3	SIL2

زیر سیستم منطق حلال با یک گروه با اکثریت رأی و زیرسیستم عملگر نهایی با دو گروه با اکثریت رأی می‌باشد، شکل ۵ سیستم ابزار دقیق ایمنی توربین گازی را نشان می‌دهد. در جدول ۱۳ نتایج حاصل از محاسبه PFD_{avg} برای زیرسیستم‌های سیستم ابزار دقیق ایمنی توربین گازی موردمطالعه با استفاده از فرمول‌های استاندارد IEC 61508 Part-3، گزارش فنی ISA-84.00.02 Part-2 و فرمول کلی جهانیان GPFDF آورده شده است.

در این تحقیق جهت محاسبه PFD_{avg} از فرمول‌های استاندارد IEC 61508 Part-6 استفاده‌شده است. میانگین احتمال خرابی در زمان تقاضا برای عملکرد سیستم ابزار دقیق ایمنی توربین گازی موردمطالعه از حاصل جمع سه زیرمجموعه سنسور، حل‌کننده منطقی و عملگر پایانی محاسبه گردید. بر اساس محاسبات زیر مقدار کمی (عددی) PFD_{avg} برابر ۰,۰۰۵۵۹۶، و سطح یکپارچگی ایمنی عملکرد سیستم ابزار دقیق ایمنی توربین گازی برابر SIL2 به دست آمد:

$$PFD_S = PFD_{PT(Lube\ oil)} + PFD_{PT(Fuel\ gas\ trip)} + PFD_{TT(Lube\ oil\ header)} + PFD_{PT(Lube\ oile\ hydraulic\ supply)} + 2PFD_{Over\ speed} + 2PFD_{Vibration} + PFD_{PT(Exhaust\ gas} + PFD_{PT(Ful\ gas\ supply)} + 6PFD_{TT(Exhaust\ gas)}$$

$$PFD_S = 1.58\times10^{-5} + 1.58\times10^{-5} + 2.76\times10^{-4} + 1.58\times10^{-5} + 2\left(1.8\times10^{-5}\right) + 2\left(7.36\times10^{-5}\right) + 2\left(7.36\times10^{-5}\right) + 1.58\times10^{-5} + 6\left(2.76\times10^{-4}\right) = 5.66\times10^{-4} = 0.566\times10^{-3}$$

$$PFD_{LS} = 2.3\times10^{-4} = 0.23\times10^{-3}$$

$$PFD_{FE} = PFD_{Hyraulic\ solenoid\ valve} + PFD_{Circuit\ breaker} = 3.5\times10^{-3} + 1.3\times10^{-3} = 4.8\times10^{-3}$$

$$PFD_{avg} = PFD_S + PFD_L + PFD_{FE}$$

$$PFD_{avg} = 0.566\times10^{-3} + 2.3\times10^{-4} + 4.8\times10^{-3} = 5.596\times10^{-3}$$

$$SIL_{Gas\ Turbine\ Generator\ Trip} = SIL2$$

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

جدول ۱۳: نتایج محاسبه زیرسیستم‌های مربوط به سیستم ابزار دقیق ایمنی توربین گازی

زیر سیستم	PFD_{avg} with IEC 61508-2010 Part-6 Formulas(28)	Jahanian Formulas (GPFDF)(27)	ISA-84.00.02 Formulas(34)
سنسور فشار روغن	1.58×10^{-5}	1.58×10^{-5}	$\mathbf{1.6 \times 10^{-5}}$
سنسور دمای روغن	2.76×10^{-5}	2.94×10^{-5}	$\mathbf{2.88 \times 10^{-5}}$
سنسور سرعت دوران	7.36×10^{-5}	7.42×10^{-5}	$\mathbf{7.42 \times 10^{-5}}$
سنسور لرزش	7.36×10^{-5}	7.42×10^{-5}	$\mathbf{7.42 \times 10^{-5}}$
حل کننده منطقی (LS)	2.3×10^{-4}	2.3×10^{-4}	$\mathbf{2.3 \times 10^{-4}}$
شیر کنترلی تخلیه فشار روغن (Hydraulic Solenoid Valve)	3.5×10^{-3}	3.5×10^{-3}	$\mathbf{3.5 \times 10^{-3}}$
سنسور قطع جریان برگشتی (Circuit breaker)	1.31×10^{-3}	1.31×10^{-3}	$\mathbf{1.31 \times 10^{-3}}$

$$\text{Safety Availability} = 1 - PFD_{avg} = 1 - \left(5.596 \times 10^{-3}\right) = 0.9940 = \%99.40$$

با استفاده از فرمول ۱۰ قابلیت دسترسی سیستم ابزار دقیق ایمنی برابر ٪۹۹/۴۰ محاسبه گردید که سطح قابلیت اطمینان و دسترسی مناسبی را نشان می‌دهد(۷). همانطور که در جدول ۱۳ مشاهده می‌شود نتایج محاسبه PFD_{avg} برای هر سه فرمول بسیار به هم نزدیک می‌باشد و سطح یکپارچگی ایمنی برای هر سه فرمول برابر با SIL2 می‌باشد.

همان طور که گفته شد جهت تایید سطح یکپارچگی ایمنی برای عملکرد سیستم ابزاردقیق ایمنی جهت از سرویس خارج کردن توربین گازی و ژنراتور در شرایط غیر نرمال عملیاتی، می‌بایست الزامات مربوط به خرابی‌های خطرناک سخت افزاری تصادفی، تحمل خطای سخت افزاری و خرابی‌های سیستماتیک در نظر گرفته شود.

جدول ۱۴ نتایج تایید SIL برای عملکرد سیستم ابزار دقیق ایمنی را با در نظر گرفتن تمامی الزامات فوق نشان می‌دهد. نتایج تحمل خطای سخت افزاری (HFT) و قابلیت سیستماتیک (SC) نیز حداکثر سطح SIL2 را برای عملکرد از سرویس خارج کردن توربین گازی و ژنراتور نشان می‌دهد.

بحث

شناسایی خطرات به روش HAZOP بر روی توربین گازی تحت مطالعه نشان می‌دهد که شروع یک انحراف از حالت نرمال فرآیندی می‌تواند زنجیره‌ای از حوادث را در پی داشته باشد که در صورت عدم کنترل و قطع زنجیره‌ی بروز حوادث، می‌تواند منجر به حوادث فاجعه باری گردد. برای مثال افزایش فشار گاز طبیعی به دلیل بدعمل کردن شیرهای کنترلی گاز طبیعی می‌تواند باعث افزایش دما در خروجی گازهای حاصل از احتراق و درنتیجه سوختگی پره‌های توربین، افزایش سرعت دوران توربین، و در بدترین حالت پرتاب قطعات و آتش‌سوزی و انفجار و قطع برق تولیدی شود. روش HAZOP نشان می‌دهد که توربین گازی تحت مطالعه، دارای حفاظ‌های ایمنی کافی در برابر خطرات و حوادث احتمالی می‌باشد و احتمال بروز حوادث را کاهش می‌دهد. ارزیابی ریسک خطرات شناسایی‌شده با استفاده از ماتریس ایمنی ریسک نشان می‌دهد که در بیشتر سناریوها سطح ریسک در محدوده قابل‌قبول و برخی در محدوده ALARP قرار دارد، لذا حفاظ‌های ایمنی موجود می‌تواند پاسخگوی خطرات و انحرافات احتمالی باشد. اما به دلیل اینکه روش شناسایی خطر HAZOP و ارزیابی ریسک به روش ماتریس ایمنی ریسک روشی کیفی می‌باشد، نمی‌تواند اطلاعات دقیقی از مقدار کمی (quantitative) سطح ریسک موجود را جهت تعیین سطح یکپارچگی ایمنی ارائه دهد.

در این تحقیق از روش نمودار ریسک کالیبره شده و آنالیز لایه‌های حفاظتی مستقل از استاندارد IEC61511-2016 Part-6 جهت تعیین سطح یکپارچگی ایمنی مورد نیاز استفاده شده است. مقایسه دو روش تعیین SIL همانند نتایج یونگون و همکارانش نشان می‌دهد که

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

جدول ۱۴: نتایج تایید SIL با در نظر گرفتن الزامات تحمل خطای سخت افزاری، خرابی های تصادفی سخت افزار و خرابی های سیستماتیک

زیر سیستم	اساس عملکرد زیر سیستم	گروه با اکثریت رای	سطح SIL مربوط به SIF برای هر زیر سیستم					
			بر اساس الزامات تحمل خطای سخت افزاری (HFT)		بر اساس الزامات خرابی تصادفی سخت افزار (Calculation (PFD_{avg})		بر اساس الزامات قابلیت سیستماتیک (SC)	
حسگر	کاهش فشار روغن	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4	SIL 4	$PFD = 1.58 \times 10^{-5}$ SIL= 4	$PFD = 5.66 \times 10^{-4}$ SIL 3	SIL=3 capable	SIL 3
	افزایش فشار در هدر روغن	2oo3	HFT=1 , Route 1H, SFF=%93, SILL= 4		$PFD = 2.76 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	کاهش فشار روغن هیدرولیک	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 1.58 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	کاهش فشار روغن ساپلای تنظیم کننده میزان هوای ورودی	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 1.58 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	افزایش سرعت دوران توربین 1	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 7.36 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	افزایش سرعت دوران توربین 2	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 7.36 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	لرزش بالا	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 7.36 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	کاهش فشار هوا در خروجی کمپرسور	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 1.58 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	کاهش فشار گاز ورودی	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 1.58 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	افزایش فشار در خروجی توربین گازی	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 1.58 \times 10^{-5}$ SIL= 4		SIL=3 capable	
	افزایش دما در خروجی توربین گازی	2oo3	HFT=1 , Route 1H, SFF=%92, SILL= 4		$PFD = 2.76 \times 10^{-5}$ SIL= 4		SIL=3 capable	
واحد پردازنده مرکزی	واحد پردازنده مرکزی	1oo2	HFT=1 , Route 1H, SFF=%95, SILL= 3	SIL 3	$PFD = 2.3 \times 10^{-4}$ SIL= 3	SIL 3	SIL=3 capable	SIL 2
عملگر پایانی	شیر کنترلی تخلیه فشار روغن Hydraulic Solenoid) (Valve	1oo1	HFT=0 , Route 1H, SFF=%79 , SILL= 2	SIL 2	$PFD = 3.5 \times 10^{-3}$ SIL= 2	SIL 2	SIL=2 capable	SIL=2
	سنسور قطع جریان برگشتی (Circuit breaker)	1oo1	HFT=0 , Route 1H, SFF=%66 , SILL= 2		$PFD = 1.3 \times 10^{-3}$ SIL= 2		SIL=2 capable	
سطح SIL جهت عملکرد از سرویس خارج کردن توربین گازی و ژنراتور:			SIL2		SIL2		SIL2	
سطح یکپارچگی ایمنی کل جهت عملکرد از سرویس خارج کردن توربین گازی برابر با SIL2 می باشد.								

روش نمودار ریسک کالیبره شده به دلیل تعیین سطح SIL بر اساس پیامد، روشی محافظه‌کارانه‌تر بوده و سطح SIL را بالاتر نشان می‌دهد (۲۰)، بنابراین می‌تواند هزینه‌های مالی قابل‌توجهی را به دنبال داشته باشند زیرا تجهیزات دارای سطح SIL بالاتر پرهزینه هستند و نیاز به هزینه‌های ساخت، نگهداری و بازرسی بیشتری دارند. روش LOPA جزئیات بیشتری از لایه‌های حفاظتی موجود و مقدار عددی سطح کاهش ریسک موردنیاز را فراهم می‌کند و تصمیم‌گیری در مورد سطح SIL به واقعیت نزدیک‌تر می‌باشد و ازآنجاکه نسبت به نمودار ریسک کمی‌تر (quantitatively) است، با دقت بیشتری می‌توان نشان داد که سطح ریسک توسط SIL تعیین‌شده به‌اندازه‌ای کاهش‌یافته است که می‌تواند معیارهای ریسک قابل‌پذیرش را فراهم کند.

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

از ۱۲۷ دلیل-پیامد که در مطالعات HAZOP شناسایی شد، تعداد ۵۲ دلیل-پیامد با روش نمودار ریسک کالیبره شده و ۲۴ دلیل-پیامد با استفاده از روش LOPA، مورد ارزیابی قرار گرفت. بنابراین همانند نتایج آلنجدورو و تورس می‌توان نتیجه گرفت که سادگی نسبی نمودار ریسک کالیبره شده آن را برای غربالگری تعداد زیادی از عملکردهای ایمنی مناسب‌تر می‌سازد(۱۱). روش LOPA دارای مزایای مهمی همچون آنالیز دقیق تعداد و نوع لایه‌های حفاظتی و ثبت احتمال خرابی لایه‌های حفاظتی در لحظه تقاضا (PFD_{avg}) و محاسبه مقدار سطح ریسک موجود بر اساس لایه‌های حفاظتی موجود می‌باشد، با این وجود در مقایسه با روش نمودار ریسک کالیبره شده می‌تواند وقت‌گیرتر و کندتر باشد و گروه ارزیابی نیاز به منابع بیشتری برای به دست آوردن داده‌های دقیق‌تر داشته باشند. روش LOPA نیاز به مهارت ویژه‌ای برای تهیه اعداد احتمال دارد و برای تفسیر این اعداد مهارت خاصی لازم است. نمودارهای ریسک و LOPA هر دو محدودیت‌های مشابهی را در رابطه با عدم توانایی در تعیین خرابی‌های با علت‌های مشترک (CCF) دارند.

جهت تایید سطح یکپارچگی ایمنی عملکرد سیستم ابزاردقیق ایمنی تمامی الزامات مربوط به خرابی‌های تصادفی سخت‌افزار، قابلیت اطمینان سخت‌افزار، و قابلیت سیستماتیک در نظر گرفته شد. در بحث الزامات مربوط به خرابی‌های تصادفی سخت‌افزار، محاسبه PFD_{avg} با استفاده از فرمول‌های ارائه شده از سه منبع IEC 61508 Patr-6، ISA 84.00.02 Part-2 و فرمول کلی آقای جهانیان (GPFDF) انجام گردید. مقایسه نتایج حاصل از محاسبه PFD_{avg} با استفاده از فرمول‌های استاندارد IEC 61508 Part-6 با نتایج حاصل از فرمول کلی جهانیان (GPFDF) نشان می‌دهد (جدول ۱۳) که همان‌طور که جهانیان نیز نتیجه گرفته بود، از هر دو روش نتایج تقریباً یکسانی از محاسبه PFD_{avg} به دست می‌آید(۲۷). جهانیان محاسبه مقدار PFD_{avg} را برای ساختارهای معماری 2oo3 و 3oo5 مربوط به سنسورهای شعله (Flame detector) یک توربین گازی، با استفاده از فرمول GPFDF و IEC 61508 Part-6 انجام داد و به نتایج یکسانی رسید. بنابراین درصورتی‌که محققان ارزیابی سطح SIL به برخی از ساختارهای معماری برخورد کنند که فرمول‌های محاسبه PFD_{avg} آن در استاندارد IEC 61508 Part-6 وجود نداشته باشد، می‌توانند از فرمول GPFDF آقای جهانیان استفاده کنند.

در این تحقیق مقدار PFD_{avg} مربوط به عملکرد سیستم ابزار دقیق ایمنی توربین گازی، با استفاده از فرمول‌های گزارش فنی ISA-84.00.02 Part-2 نیز محاسبه گردید (جدول ۱۳)، همان‌طور که اولیورا و آبراموویچ نیز در سال ۲۰۱۰ بیان کرده بودند، نتایج حاصل از استاندارد IEC 61508 Part-6 و گزارش فنی ISA-84.00.02 Part-2 تقریباً نزدیک به هم می‌باشند(۲۹). محاسبه PFD_{avg} با استفاده از فرمول‌های استاندارد IEC 61508 Part-6 به دلیل در نظر گرفتن نرخ خرابی‌های ایمن و خطرناک و خرابی‌های قابل‌تشخیص و غیرقابل تشخیص، تأثیر خرابی‌های با دلایل مشترک، و میانگین زمان تعمیر و در سرویس قرار گرفتن مجدد سیستم ابزار دقیق ایمنی، مقدار عددی دقیقی از احتمال عمل نکردن سیستم ابزار دقیق ایمنی در لحظه تقاضا را نشان می‌دهد. بر اساس این محاسبات مقدار عددی PFD_{avg} سیستم ابزار دقیق ایمنی جهت از سرویس خارج کردن توربین گازی برابر ۰،۰۰۵۵۹۵ و سطح یکپارچگی ایمنی عملکرد سیستم ابزاردقیق ایمنی برابر SIL2، و قابلیت در دسترس بودن عملکرد سیستم ابزار دقیق ایمنی (SIF Availability) برابر با ٪۹۹،۴۰ محاسبه گردید.

تایید (راستی آزمایی) سطح یکپارچگی ایمنی با در نظر گرفتن الزامات قابلیت اطمینان سخت‌افزار (Hardware Safety Integrity) با روش Route 1H براساس تحمل خطای سخت‌افزار (HFT) و کسر خرابی‌های ایمن (Safe Failure Fraction) نشان داد که در سیستم ابزار دقیق ایمنی تمامی حسگرها دارای ساختار معماری 2oo3 و تحمل خطای ۱، پردازشگر مرکزی دارای ساختار معماری

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

1oo2 و تحمل خطای ۱، و عملگر پایانی با ساختار معماری 1oo1 دارای تحمل خطای صفر می‌باشد. در این روش بیشترین سطح یکپارچگی ایمنی مربوط به حسگرها برابر با SIL4 و سطح یکپارچگی ایمنی مربوط به پردازشگر مرکزی و عملگر پایانی برابر با SIL2 محاسبه گردید. بنابر این سطح یکپارچگی ایمنی کلی مربوط به عملکرد سیستم ابزاردقیق ایمنی جهت ازسرویس خارج کردن توربین گازی برابر با SIL2 می‌باشد.

به‌منظور افزایش قابلیت اطمینان نیروگاه و تولید برق به‌صورت مداوم، پیشنهاد می‌شود چند توربین گازی به‌صورت موازی باهم نصب شوند، به‌طوری‌که در صورت از سرویس خارج شدن یک توربین گازی، توربین‌های گازی دیگر به‌صورت خودکار در سرویس قرارگرفته و مقدار برق موردنیاز را تأمین کنند. پیشنهاد می‌شود در مطالعات بعدی قابلیت اطمینان چند توربین که به‌صورت موازی باهم نصب‌شده‌اند محاسبه گردد.

پیشنهاد می‌شود در سناریو افزایش دمای روغن خنک‌کننده و روان‌کننده به دلیل خرابی کولر روغن، یک کولر روغن یدکی نصب گردد، و در صورت خرابی کولر روغن اصلی، کولر روغن یدکی به‌صورت خودکار در سرویس قرار گیرد و بدین‌صورت از Trip توربین گازی و قطع برق در اثر افزایش دمای روغن خنک‌کننده جلوگیری گردد.

بررسی‌ها نشان می‌دهد در مسیر جریان گاز طبیعی از ظرف جداکننده مایع از گاز (K.O.Drum) تا فیلترهای تصفیه گاز طبیعی، سیستم اعلان و اطفاء (F&G) وجود ندارد، با توجه به‌احتمال نشت گاز طبیعی و بروز حوادثی مانند اشتعال و انفجار، پیشنهاد می‌شود سیستم F&G در مسیر جریان گاز طبیعی تا فیلترهای تصفیه گاز طبیعی نصب گردد و سنسورها به سیستم ابزار دقیق ایمنی توربین گازی متصل گردد تا در صورت نشت گاز طبیعی فرمان بسته شدن شیر اصلی گاز طبیعی و از سرویس خارج شدن(Trip) توربین گازی از طرف مرکز کنترل (DCS) صادر گردد و از وقوع آتش‌سوزی و انفجار جلوگیری شود.

با توجه به این که در زیر سیستم عملگر پایانی (FE) از یک شیر کنترل (Solenoid valve) با معماری 1oo1 جهت تخلیه روغن هیدرولیک و در نتیجه بسته شدن شیر کنترل اصلی گاز طبیعی و قطع سوخت مشعل‌های توربین استفاده شده است، در صورت خرابی یا عمل نکردن عملگر پایانی، عملکرد از سرویس خارج کردن توربین گازی اجرا نمی‌شود، بنابر این پیشنهاد می‌شود جهت افزایش تحمل خطای سخت افزاری و افزایش در دسترس بودن زیر سیستم عملگر پایانی از معماری 1oo2 استفاده گردد.

استفاده از فرمول کلی جهانیان (GPFDP) در این تحقیق، می‌تواند راهنمای خوبی برای مهندسین ابزار دقیق و ایمنی جهت محاسبه PFD_{avg} مربوط به ساختارهایی از M-out-of-N باشد که در استاندارد IEC 61508 Part-6 و گزارش فنی ISA-84.00.02 Part-2 موجود نیست. برای مثال برای ساختار 3oo5 در استاندارد IEC 61508 Part-6 و ISA-84.00.02 Part-2 فرمولی ارائه نشده است ولی با فرمول GPFDF می‌توان به‌راحتی مقدار PFD_{avg} را محاسبه کرد.

نتیجه گیری

نتایج مطالعه نشان داد که روش LOPA نسبت به روش نمودار ریسک کالیبره شده، روشی کمی‌تر، دقیق‌تر و قابل اعتمادتر می‌باشد، زیرا محاسبات سطح ریسک بر اساس تعداد و نوع لایه‌های حفاظتی موجود و فرکانس وقوع واقعه اولیه و احتمال خرابی لایه‌های حفاظتی موجود در لحظه تقاضا صورت می‌گیرد.

نتایج محاسبه PFD_{avg} جهت تایید (راستی آزمایی) سطح یکپارچگی ایمنی با استفاده از فرمول‌های ارائه شده در استاندارد IEC 61508 Part-6، گزارش فنی ISA 84.00.02 Part-2 و فرمول کلی جهانیان (GPFDF) بسیار به هم نزدیک بوده و سطح یکپارچگی ایمنی برابر با SIL2 را نشان داد.

تایید (راستی آزمایی) سطح یکپارچگی ایمنی با در نظر گرفتن تمامی الزامات مربوط به خرابی‌های

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

تصادفی سخت‌افزار، قابلیت اطمینان سخت‌افزار و قابلیت سیستمالتیک نشان داد که عملکرد سیستم ابزاردقیق ایمنی جهت از سرویس خارج کردن توربین گازی در شرایط غیر نرمال عملیاتی، می‌تواند سطح یکپارچگی ایمنی برابر با SIL2 را برآورده کند که با نتایج حاصل از روش LOPA برابر است، لذا عملکرد سیستم ابزاردقیق ایمنی توربین گازی و ژنراتور مورد مطالعه از قابلیت اطمینان و دسترسی مطلوب و مناسبی برخوردار بوده و به‌خوبی می‌تواند پاسخ گوی خطرات احتمالی باشد.

رویکرد حاضر به مهندسین ایمنی و مهندسین ابزاردقیق کمک می‌کند قابلیت اطمینان و قابلیت در دسترس بودن عملکرد سیستم‌های ابزاردقیق ایمنی تجهیزات فرآیندی خود را محاسبه کرده و از قابل قبول بودن یا نبودن آن اطمینان حاصل کنند، زیرا هم روش‌ها و مراحل ارزیابی ریسک نیمه کمی و کیفی که مختص مهندسان ایمنی می‌باشد و هم ماهیت سیستم ابزاردقیق ایمنی، انواع خرابی‌ها، انواع ساختارهای معماری یا افزونگی (Voting) و فرمولهای محاسباتی مربوط به PFD_{avg} که مهندسین ابزاردقیق و بهره برداری اطلاعات جامعی از آن دارند به طور کامل توصیف و به کار برده شده است. لذا این تحقیق می‌تواند راهنمای کاملی جهت تعیین و راستی آزمایی سطح یکپارچگی ایمنی مربوط به عملکرد سیستم‌های ابزاردقیق ایمنی، هم برای مهندسین ایمنی و هم برای مهندسین ابزاردقیق باشد.

تعارض منافع

نویسندگان در این تحقیق اظهار داشته‌اند که هیچ‌گونه تضاد منافع یا روابط شخصی رقابتی که به نظر برسد در کار گزارش‌شده در این مقاله تأثیرگذار است، نداشته‌اند.

تصدیق

این تحقیق توسط دانشگاه علوم پزشکی شهید بهشتی پشتیبانی شده است.

REFERENCES

1. Ouache R, Kabir MN, Adham AA. A reliability model for safety instrumented system. Saf Sci. 2015;80:264-73.
2. CCPS of the AIChE. Layer of protection analysis: simplified process risk assessment. New York, New York 10016-5991: John Wiley & Sons; 2001.
3. Jafari MJ, Askarian A, Omidi L, Miri Lavasani MR, Taghavi L, Ashori A. The assessment of independent layers of protection in gas sweetening towers of two gas refineries. Saf Prom Injur Prev. 2014;2(2):103-12. [Persian]
4. G.M. International. Manual S. Safety instrumented systems. Plant Engineering and Maintenance According to IEC 61508 and IEC 61500 Standards. 4th edition.
5. Rausand M. Reliability of safety-critical systems: theory and applications: John Wiley & Sons; 2014.
6. Alizadeh S, Sriramula S. Unavailability assessment of redundant safety instrumented systems subject to process demand. Reliab Eng Syst Saf. 2018;171:18-33.
7. ANSI/ISA-84.00.01 Functional safety: safety instrumented systems for the process industry sector – Part 1; 2004.
8. Sadeghi A, Jabbari M, Rezaeian M, Alidoosti A, Eskandari D. Fire and Explosion Risk Assessment in a Combined Cycle Power Plant. Iran J Chem Chem Eng Research Article Vol. 2020;39(6).
9. Jabbari M, Kavousi A, editors. Consequence analysis of flammable chemical releases from a pipeline. 2011 Fourth International Joint Conference on Computational Sciences and Optimization; 2011: IEEE.
10. IEC 61511 Standard. Functional safety—safety instrumented systems for the process industry sector. Parts 1–3;2016.
11. Torres-Echeverria AC. On the use of LOPA and risk graphs for SIL determination. J Loss Prev Process Ind. 2016;41:333-43.
12. Hyatt N. Guidelines for process hazards analysis (PHA, HAZOP), hazards identification, and risk analysis: CRC press; 2018.
13. Darwish AS, Mansour MS, Farag H, Ezzat KH. Applying LOPA and fuzzy logic to identify SIL requirement for safety critical functions in a direct reduction iron

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]

industry. Alexandria Eng J. 2020;59(5):3575-85.
14. Gabriel A, Ozansoy C, Shi J. Developments in SIL determination and calculation. Reliab Eng Syst Saf. 2018;177:148-61.
15. IEC 61508 Standard. Functional safety of electrical/electronic/programmable electronic safety related systems. IEC 61508 Part 1-6. 2010.
16. Creech G. IEC 61508 Systematic Capability. Meas Control. 2014;47(4):125-8.
17. Kuba S, Yasuda EK, Katou Y, Kamino K. Hitachi H-25 Gas Turbine in Oil and Gas Market. Hitachi Rev. 2009;58(1):15.
18. HU J-q, ZHANG L-b, LIANG W, WANG Z-h. Quantitative HAZOP analysis for gas turbine compressor based on fuzzy information fusion. Syst Eng Theory Pract. 2009;29(8):153-9
19. IEC 60300-3-9. Guide to Risk Analysis of Technological Systems. IEC 60300-3-9 Part 3. IEC: Geneva, Switzerland. 1995.
20. Ahn J, Noh Y, Joung T, Lim Y, Kim J, Seo Y, et al. Safety integrity level (SIL) determination for a maritime fuel cell system as electric propulsion in accordance with IEC 61511. Int J Hydrogen Energy. 2019;44(5):3185-94.
21. Baghaei A. 3-Parameters SPW technique: a new method for evaluation of target safety integrity level. J Loss Prev Process Ind. 2013;26(6):1257-61.
22. Markowski AS, Mannan MS. ExSys-LOPA for the chemical process industry. J Loss Prev Process Ind. 2010;23(6):688-96.
23. IEC 61508. Functional safety of electrical/electronic/programmable electronic safety related systems. IEC 61508 Part 1. 2010.
24. Amicucci GL, Pera F, Tonti A. Reliability analysis of nuclear instrumentation and control systems. Instrumentation and Control Systems for Nuclear Power Plants: Elsevier; 2023. p. 887-956.
25. Clarke P. Chapter 8 - Safety instrumented system design. In: Clarke P, editor. Functional Safety from Scratch: Elsevier; 2023. p. 219-44.
26. Mitchell K, Longendelpher T, Kuhn M. Kenexis: Safety Instrumented System Engineering Handbook. CreateSpace Independent: Middletown, DE; 2010.
27. Jahanian H. Generalizing PFD formulas of IEC 61508 for KooN configurations. ISA Trans. 2015;55:168-74.
28. IEC 6108. Functional safety of electrical/electronic/programmable electronic safety related systems. IEC 61508 Part 6. 2010.
29. Oliveira LF, Abramovitch RN. Extension of ISA TR84. 00.02 PFD equations to KooN architectures. Reliab Eng Syst Saf. 2010;95(7):707-15.
30. Hauge S, Lundteigen MA, Hokstad P, Håbrekke S. Reliability prediction method for safety instrumented systems–pds method handbook, 2010 edition. SINTEF report STF50 A. 2010;6031.
31. CCPS of the AIChE. Guidelines for initiating events and independent protection layers in layer of protection analysis: John Wiley & Sons, Incorporated; 2015.
32. Gurjar BR, Sharma RK, Ghuge SP, Wate SR, Agrawal R. Individual and societal risk assessment for a petroleum oil storage terminal. J Hazard Toxic Radioact Waste. 2015;19(4):04015003.
33. Tchiehe DN, Gauthier F. Classification of risk acceptability and risk tolerability factors in occupational health and safety. Saf Sci. 2017;92:138-47.
34. ANSI/ISA-84.00.02 Functional safety: safety instrumented systems for the process industry sector – Part 2; 2002

[Downloaded from jhsw.tums.ac.ir on 2026-07-31]

[DOI: 10.18502/jhsw.v14i2.17136]