ISBN: 978-981-18-7950-0
2023 the 13th International Workshop on Computer Science and Engineering (WCSE 2023)
doi: 10.18178/wcse.2023.06.056

Probabilistic Risk Assessment and Its Application in Complex Integrated Task Risk Assessment

Qi Yang [1, 2], Lingjie Zhang [1, 2], Hongqi Yang [1, 2 +], Yujie Liu [1, 2], Ning Hu [1, 2] and Jieyi Zhang [1, 2]

[1] China Electronic Product Reliability and Environmental Testing Research Institute, Guangzhou, China

[2] Key Laboratory of Industrial Equipment Quality Big Data, MIIT, Guangzhou, China

Abstract. In view of the characteristics of complex integration tasks such as launch tasks, such as complex processes, many systems involved, and frequent human-computer interaction, the probabilistic risk evaluation (PRA) method is introduced to realize the quantitative risk assessment of complex integration tasks. In this paper, the development and application status of PRA method are analyzed, and key technologies such as comprehensive modeling analysis of human factors reliability based on human error rate prediction (THERP) and human cognitive reliability (HCR) models, importance ranking, and uncertainty analysis based on Monte Carlo simulation are studied. Taking the propellant leakage in the launch tasks as an example, the PRA method is applied to quantitatively evaluate the risk of this scenario, and the results show that the PRA method has good applicability in the risk assessment of complex integration tasks, and can provide decision-making support for institutional risk management and control of complex integration tasks.

Keywords: probabilistic risk assessment; complex integration task; human reliability

1. Introduction

With the continuous development of China's aerospace industry and the shortening of the complex integrated tasks cycle, the demand for the use of the launch site and the requirements for tasks success have been continuously improved. The launch site system is an important guarantee for the completion of the launch tasks, responsible for completing the assembly, testing, refueling, transfer and launch of various systems at the launch site, so ensuring the safety of the launch site is of great significance to ensure the success of the launch tasks. Due to the complex system structure, diverse failure modes, and close personnel participation involved in the implementation process of such complex integrated tasks as launch tasks, there are many uncertainties, and traditional system safety analysis methods, such as Fault Tree Analysis (FTA) [1], Failure Mode and Effects Analysis (FMEA) [2], Hazard and operability analysis (Hazard). and Operability, HAZOP) [3] and other methods focus on static analysis of single faults, it is difficult to accurately construct a dynamic risk assessment model of system operation, and it is impossible to give the importance ranking of risk events and their uncertainty effects and the cumulative risk value of the system. Probabilistic Risk Assessment (PRA) is a comprehensive method for constructing risk event chain models using event sequence diagrams and fault trees, which can effectively solve the problems of insufficient risk quantitative assessment, importance ranking of risk influencing factors, risk uncertainty analysis, and description of risk accident evolution process in complex integration tasks.

2. PRA Technology Development and Application Status

PRA method was first proposed and applied by the United States Nuclear Regulatory Commissions in 1975 in the Probabilistic Risk Assessment Report of the United States Commercial Light Water Reactor Nuclear Power Plant [4], and the correctness of PRA was confirmed in the Three Mile Island nuclear Power Plant leakage accident in 1979. Since then, PRA has been gradually popularized and applied in industrial fields such as petrochemical industry and equipment development. From 1988 to the present, the National Aeronautics and Space Administration (NASA) applied PRA to space models such as the International Space

+ Corresponding author.
E-mail address: yhqceprei2021@163.com.

Station, alien probes, and satellites. The European Space Agency (ESA) also applies PRA technology to tasks reliability and safety risks of manned or unmanned spacecraft [5].

In China, in the 1980s, the Aerospace Standardization Institute, the first Aerospace Institute, the Fifth Aerospace Institute and other institutions successively carried out PRA research and applied it in the nuclear industry, aerospace, aviation and other industrial fields, and achieved phased research results. In 1998, the First Aerospace Academy and other institutions carried out PRA analysis on the fault detection and analysis system of carrier rocket. In 2005, the Fifth Academy of Astronautics established the PRA model of manned spacecraft to verify the safety index requirements of manned spacecraft. In 2009, the Aerospace Standardization Institute and other institutions conducted PRA application research on the docking mechanism of the space station.

In recent years, domestic scholars have carried out a lot of research on PRA technology and application. X. Li et al. applied PRA technology to a certain lunar exploration mobile subsystem [6].B. Cui et al. studied a launch site risk analysis system based on PRA and built a risk analysis model [7]. J. Liu et al. applied PRA method to evaluate the reliability and safety of the connection mechanism for the docking and separation process of spacecraft [8]. Y. Wu proposed a PRA based quantitative risk analysis and decision method for ship equipment [9]. Wang Xin et al. used probabilistic risk assessment technology to carry out reliability modeling and evaluation methods for a certain missile weapon system [10]. T. Zeng et al. proposed a probabilistic risk assessment method based on Bayesian networks for the assembly process of satellite antenna, used Bayesian networks to build an intermediate event reliability model considering human-machine loop coupling, and used human factor reliability and other methods to conduct quantitative analysis of the model [11].

From the above PRA development and application status, PRA technology has been widely used in nuclear industry, aerospace, aviation and other industrial fields. There are few studies on the application of PRA methods to risk assessment of complex integrated tasks such as launch tasks. Once there is a problem, it will not only endanger the safety of astronauts, spacecraft and launch site personnel and equipment, but also have a serious impact on related industries. Therefore, this paper applies the PRA method to evaluate the risk level of complex integration tasks such as launch tasks, and provides effective technical means for risk identification, risk assessment, risk control and decision-making of complex integration tasks.

3. Key Techniques for PRA Modeling and Analysis

Combined with the implementation process of the complex integration tasks, the following technologies involved in the PRA work are further studied, which lays a foundation for the quantitative risk assessment of PRA applied to the complex integration tasks.: (1) Human reliability modeling and analysis technology; (2) Uncertainty Analysis Technique; (3) Importance ranking technology.

3.1. Comprehensive modeling of human factor reliability based on THERP+HCR

Human mistakes are usually caused by the combination of cognitive and operational factors. Human Cognitive Reliability (HCR) model can be used to quantify cognitive errors. The Technique for Human Error Rate Prediction (THERP) model can be used to quantify operational errors. The two models have good applicability in terms of effectiveness, availability, engineering, etc., and are widely used in the nuclear industry, aviation, aerospace and other fields [12].

3.1.1. Construction of a comprehensive model of THERP+HCR

The human handling of accidents is divided into three stages: observation awareness, diagnostic decision-making, and operational processing, as shown in Fig. 1.

P_1, P_2, and P_3 in the Fig. 1 represent the failure probabilities of the observation stage, the diagnostic stage, and the operational stage, respectively. The calculation method for the failure probability P of the entire response action sequence is shown in Equation (1).

$$P = p_1 + (1 - p_1) p_2 + (1 - p_1)(1 - p_2) p_3 \tag{1}$$

In the formula, p_1, p_2, and p_3 are the probability of errors in observation awareness, diagnostic decision-making, and operational processing. P_1 and p_3 are calculated using the THERP model, and p_2 is calculated using the HCR model. Detailed modeling methods are given in the following chapters.

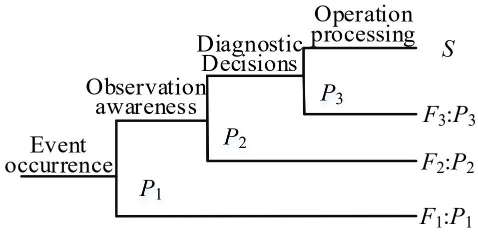

Fig. 1: Human error probability quantification process

3.1.2. THERP model construction

Using the THERP model to quantify the probability of human operational errors is mainly divided into the following two steps:

(1) HRA event tree construction

The Human Reliability Analysis (HRA) event tree divides the process of a task completed by a person into several subtasks in chronological order, and uses a binary event tree to describe it. There are two possibilities for failure or success on each branch node. Fig. 2 shows an example of a process for determining the success probability of a task composed of two subtasks (subtask 1 comes first and subtask 2 comes second) using an HRA event tree.

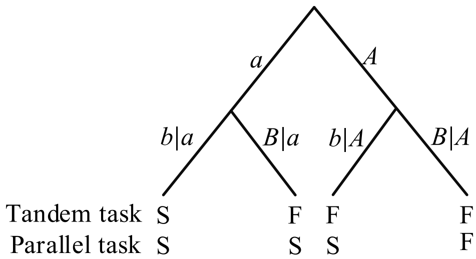

Fig. 2: Example of HRA event tress for string and parallel tasks

(2) Calculation of personnel error probability

The personnel error probability in Fig. 2 is divided into two categories: non-conditional probability and conditional probability. The calculation method is as follows.

①The non-conditional probability, taking A as an example, is calculated as Equation (2).

$$A=BHEP\times PSF \tag{2}$$

In the formula, BHEP is the basic error probability of personnel, which is determined by referring to the THERP manual; PSF is a correction factor, which is determined by consulting the THERP manual in combination with factors such as personnel stress and operating proficiency.

②Conditional probability, taking B|A as an example

First, use the non-conditional probability calculation method to calculate B, and then use the correlation calculation formula between A and B to calculate B|A. The correlation classification and corresponding calculation formula between A and B are shown in Table 1.

Table 1: Task correlation calculation formula

Correlation Category	Calculation formula
Full correlation	$B\|A=1$
High correlation	$B\|A=(1+B)/2$
Medium correlation	$B\|A=(1+6B)/7$
Low correlation	$B\|A=(1+19B)/20$
zero correlation	$B\|A=B$

Since the correlation only exists between task success and success, and between task failure and failure, the conditional probabilities B|A and $b|a$ are applicable to the above methods. Other conditional probabilities such as $b|A$ and $B|a$ are determined based on $b|A=1-B|A$, $B|a=1-b|a$.

3.1.3. HCR model construction

The HCR model is used to evaluate the probability that personnel fail to complete diagnostic decisions within a limited time. The human error probability follows a three-parameter Weibull distribution [13], as shown in Equation (3).

$$p(t)=e^{-\left(\frac{t/T_{1/2}-\gamma}{\eta}\right)^{\beta}} \tag{3}$$

In the formula, t is the allowable time of the task; $T_{1/2}$ is the actual execution time of the task; γ, η, β is a distribution parameter whose value is related to human behavior, as shown in Table 2 [14].

Table 2: The value of parameter γ, η, β

Behavior Type	γ	η	β
Skill type	0.29	0.87	1.79
Regular type	0.3	0.88	1.63
Knowledge type	0.2	1.18	0.94

The actual task execution time $T_{1/2}$ is corrected according to Formula (4).

$$T_{1/2}=T_{1/2}^{'}\left(1+K_1\right)\left(1+K_2\right)\left(1+K_3\right) \tag{4}$$

In the formula, $T_{1/2}'$ is the task execution time under normal conditions; K_1 is the personnel experience correction factor, K_2 is the personnel psychological stress correction factor, and K_3 is the human-machine interface correction factor [15].

3.1.4. Uncertainty simulation based on monte carlo

Using Monte Carlo simulation to determine the probability of occurrence of consequence states at different percentile levels, the following two steps are included:

Step 1: Uncertainty propagates from the bottom event to the top event along the fault tree, as shown in Fig. 3.

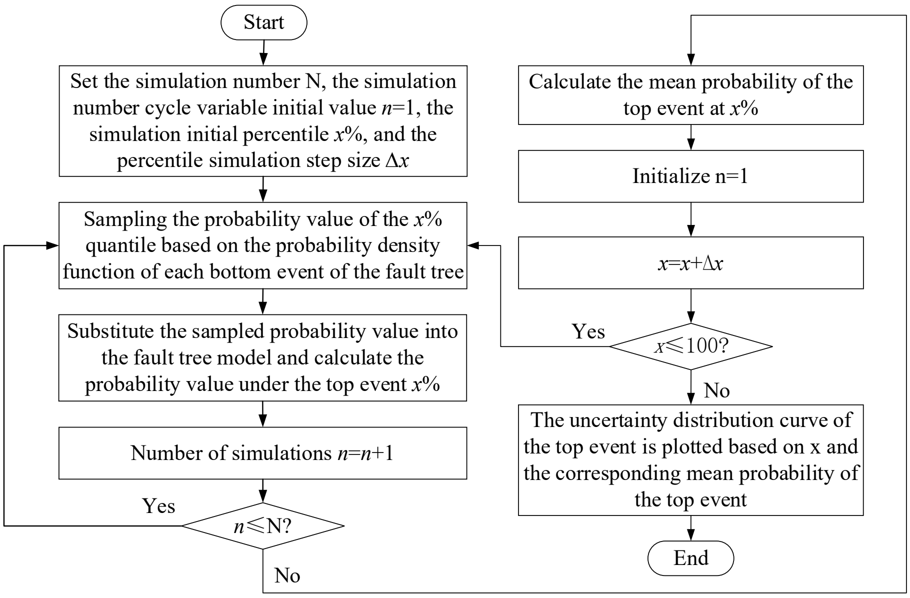

Fig. 3: Monte carlo simulation process

Step 2: Uncertainty propagates from left to right along the event tree from the middle event to the consequence state, and the uncertainty propagation process is similar to step 1, changing the bottom event in the process of Figure 5 to the intermediate event, the fault tree to the event tree, and the top event to the consequence state.

3.1.5. Basic event importance analysis

Calculating the importance of basic events and sorting them according to their relative size can find the weak links that cause systemic risks, and provide reference for risk decision-making and risk control. The importance includes F-V (Fussell-Vesely) importance, Risk Achievement Worth (RAW), Risk Reduction Worth (RRW), calculated as follows.

(1)F-V importance

The F-V importance of the basic event i is calculated as Equation (5).

$$I_i^{F-V} = \frac{P_{FS}\left(M_i\right)}{P_{FS}} \tag{5}$$

where $P_{FS}(M_i)$ is the probability of the occurrence of the final state in the minimum cut set containing the basic event i, P_{FS} is the probability of a consequence state occurring.

(2)RAW importance

The RAW importance of the basic event i is calculated as Equation (6).

$$I_i^{RAW} = \frac{P_{FS}\left(P_i = 1\right)}{P_{FS}} \tag{6}$$

where P_{FS} (P_i=1) is the probability of the occurrence of the final state when the probability of occurrence of the basic event i is set to 1;

(3)RRW importance

The RRW importance of the basic event i is calculated as Equation (7).

$$I_i^{RRW} = \frac{P_{FS}}{P_{FS}\left(P_i = 0\right)} \tag{7}$$

where $P_{FS}(P_i$=0) is the probability of a consequence state occurring when the probability of occurrence of the basic event i is set to 0.

4. Case Analysis

Taking propellant leakage in complex integration tasks as an example, the PRA method is applied to quantitatively evaluate the risk of this scenario.

4.1. Construction of probabilistic risk assessment model

Combined with the characteristics of the complex integration tasks, the event tree is used to construct a risk event chain model with "propellant leakage" as the initial cause, as shown in Fig. 4.

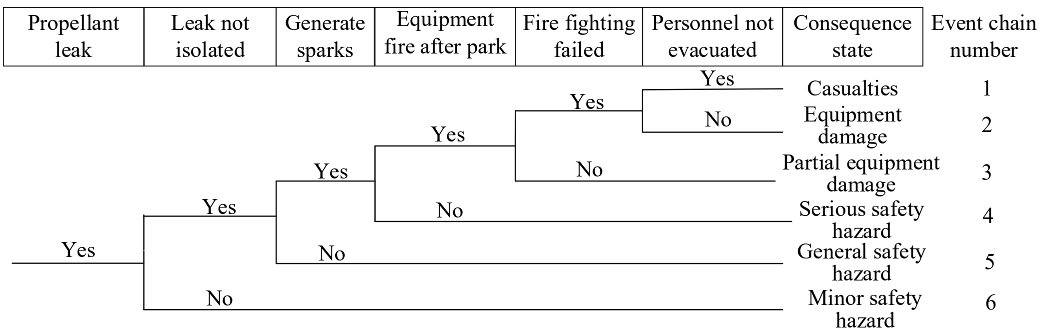

Fig. 4: Propellant leak event tree

In Fig. 4, leakage without isolation is a typical human error event, and it is difficult to directly give the probability of occurrence, and THERP+HCR is used to model and analyze it to obtain its probability of occurrence, and the process is as follows.

The THERP+HCR model is used to calculate the probability of leakage not isolated in the event tree. The operator completes the three steps of leakage isolation observation, diagnosis and operation.

①Observation error probability p_1: According to the training of personnel and the obviousness of the alarm signal, p_1 can be considered very small, assuming 1.0e-4.

②Diagnostic error probability p_2: Combined with the characteristics of the filling system and the personnel operation procedures, p_2 is calculated from formula (2), p_2=3.28e-2.

③Operation error probability p_3: Leak isolation involves the operator versus the operator, who completes the specific operation, and the person in charge supervises the operator and corrects his errors. The specific steps are as follows: (i) whether the operator successfully closed the pipeline isolation valve (a_1/A_1), and whether the person in charge successfully corrected the operator to close the pipeline isolation valve (a_2/A_2); (ii) whether the operator closes the filling flap (b_1/B_1), and whether the person in charge successfully corrects the operator's failure to close the filling flap (b_2/B_2); (iii) Whether the operator turns off the filling pump (c_1/C_1), and whether the person in charge successfully corrects whether the operator does not turn off the filling pump (c_2/C_2). The HRA event tree for the operator to implement leak isolation is shown in Fig. 5.

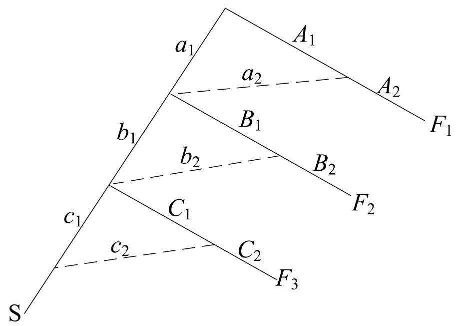

Fig. 5: Operator implements leak isolation HRA event tree

The probability of operation error p3=F1+F2+F3, by checking the THERP manual [14], combined with the correlation between personnel characteristics and personnel operation behavior, F_1=0.00116, F_2=3.881e-4, F_3=1.936e-3, p_3=1.936e-3 were calculated.

④ The probability of leakage not isolated is P: $P=p_1+(1-p_1)\times p_2+(1-p_1)\times(1-p_2)\times p_3$=3.477e-2。

4.2. Model quantification and integration

For the primary cause event and other intermediate events in the event tree, the probability is given with reference to similar equipment and complex integration tasks characteristics as follows: propellant leakage probability=6.98e-5, generate sparks probability=5.4e-3, equipment fire after spark probability=0.85, fire extinguishing failure probability=4.5e-4, personnel not evacuated probability=1.0e-4. The probability of the consequence state of the event tree species is calculated as shown in Table 3.

Table 3: Probability of consequence state

Consequence state	Probability	Proportion %	Consequence state	probability	Proportion %
Casualties	5.0081e-15	7.1749e-9	Serious safety hazard	1.9658e-9	2.8163e-3
Equipment damage	5.0031e-12	7.1678e-6	General safety hazard	2.4138e-6	3.4582
Partial equipment damage	1.1134e-8	1.5951e-2	Minor safety hazard	6.7373e-5	96.5231

The results showed that the probability of occurrence was 6.7373E-5, the largest proportion of safety hazards was 96.5231%, the total proportion of all safety hazards was 99.9841%, and the probability of occurrence of other consequence states was relatively small, totaling 0.01588%.

The percentage of the probability of elementary events occurring as a percentage of the sum of all elementary event probabilities for this minimum cut set is shown in Table 4.

The results show that equipment fire and leakage are not isolated in the minimum cut concentration accounted for a relatively large proportion, and it is recommended that relevant measures be taken at the complex integration tasks to reduce the probability of equipment fire after sparking, and strengthen the monitoring of leakage isolation measures, including the monitoring of relevant personnel and equipment that implement leakage isolation operations.

Table 4: Proportion of the probability of occurrence of basic events in the minimum cut set

Consequence state	Minimum cut set	Proportion%	Consequence state	Minimum cut set	Proportion%
Casualties	Propellant leak Leak not isolated Generate sparks Equipment on fire Fire fighting failed Personnel not evacuated	7.828e-3 3.899 0.606 95.324 5.047e-2 0.113	Equipment damage	Propellant leak Leak not isolated Generate sparks Equipment on fire Fire fighting failed	7.837e-3 3.904 0.606 95.431 5.116e-2
			/	/	/
Partial equipment damage	Propellant leak Leak not isolated Generate sparks Equipment on fire	7.841e-3 3.906 0.607 95.48	Serious safety hazard	Propellant leak Leak not isolated Generate sparks	0.174 86.493 13.333
			/	/	/
General safety hazard	Propellant leak	0.200 6	Minor safety hazard	Propellant leak	100
	Leak not isolated	99.799 4			

4.3. Uncertainty analysis

In Fig. 4, there is uncertainty in the failure of fire extinguishing in the event tree, and the uncertainty research event chain propagates to the consequence state. Casualties are the consequence state that is the focus of complex integration tasks. Based on Monte Carlo simulation, the probability distribution curve of casualties is shown in the Fig. 6.

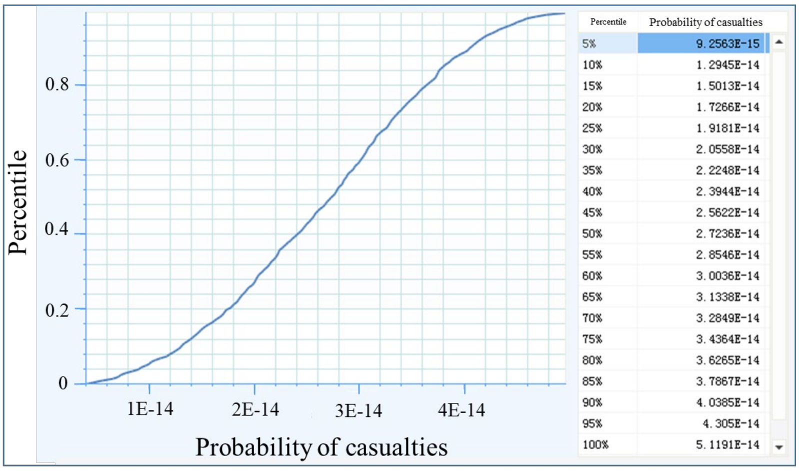

Fig. 6: Human casualty uncertainty distribution

4.4. Event importance analysis

RAW is used to calculate the importance of basic events, and the results are shown in Table 5.

Table 5: RAW importance ranking of base events

Basic event	probability	RAW	sort	Basic event	probability	RAW	sort
Propellant leak	6.98e-5	1.43e4	1	Generate sparks	0.005 4	1.85e2	4
Fire fighting failed	4.5e-4	2.22e3	2	Leak not isolated	0.034 77	28.76	5
Personnel not evacuated	0.001	1.00e3	3	Equipment on fire	0.85	1.18	6

The results show that the RAW of propellant leakage is the largest, which contributes the most to increasing the probability of occurrence of the consequence state, followed by fire extinguishing failure, personnel not evacuated, sparks generated, leakage not isolated, and equipment fire RAW is the smallest. Therefore, the complex integration tasks should focus on the prevention of propellant leakage, reduce the probability of its occurrence through relevant prevention and control measures, and carry out risk prevention and control from the initial cause of the accident.

5. Conclusion

In this paper, PRA-related technologies are studied and applied to risk assessment for complex integration tasks. Taking propellant leakage in complex integration task flow as an example, the PRA method is applied to quantitatively evaluate the risk of this scenario.

The PRA method has good applicability in the risk assessment of the complex integration tasks, and the evaluation results are consistent with the actual situation. The PRA method can not only quantify the total risk value of dangerous consequences, but also rank the relative risks of primary cause events and intermediate events, find out the weak links in system design, make up for the lack of quantitative risk assessment at the complex integration tasks, and provide opinions and suggestions for the risk management personnel of the complex integration tasks to formulate risk control measures.

6. References

[1] PEETERS J F W, BASTEN R J I, TINGA T. Improving failure analysis efficiency by combining FTA and FMEA in a recursive manner[J]. Reliability Engineering & System Safety, 2018, 172: 36-44.

[2] W. Wang, X.Lin, Y. Qin, et al. A risk evaluation and prioritization method for FMEA with prospect theory and Choquet integral [J]. Safety Science, 2018, 110(A): 152-163.

[3] L. Zhu, H. Ma, Y. Huang , et al. Analyzing Construction Workers' Unsafe Behaviors in Hoisting Operations of Prefabricated Buildings Using HAZOP[J]. International Journal of Environmental Research and Public Health, 2022, 19(22).

[4] N. Paltrinieri, V. Cozzani Assessment and comparison of two early warning indicator methods in the perspective of prevention of atypical accident scenarios [J]. Reliability Engineering and System Safety, 2012, 5(102): 21-31.

[5] N. Kakzad, F. Khan, P. Amyotte. Quantitative risk analysis offshore drilling operations: a Bayesian approach [J]. Safety Science, 2013, 2(57): 108-117.

[6] X. Li, H Huang, F Li. PRA based reliability analysis of complex space phased-tasks system [J]. Systems Engineering and Electronics, 2019. 41(9), 2141-2147.

[7] B. Cui, J. Zhao, J. Chen, et al. Research on Risk Analysis System of Launch Site [J]. Safety and Environmental Engineering, 2014, 21(4), 152-158.

[8] J. Liu, H Zheng, Q Zheng, et al. Reliability assessment of docking mechanism based on probabilistic risk assessment [J]. Manned Spaceflight, 2012, 18(03): 41-45.

[9] Y. Wu. Risk analysis and decision making in ship research & design with probabilistic risk-based assessment [J].Ship & Boat. 2010, 21(01): 57-59.

[10] X. Wang, J. Chen, Z. Yang, et al. Reliability Modeling and Analysis of Missile Weapon System Based on PRA [J]. Tactical Missile Technology, 2020(06): 112-119.

[11] T. Zeng, S. Gao, F. Sun, et al. Probabilistic risk analysis of satellite antenna assembly considering man-machine-environment coupling effect [J]. Systems Engineering and Electronics, 2023(02): 606-613.

[12] L. Zhang. Human factor reliability analysis technology in probabilistic safety evaluation [M]. Beijing: Atomic Energy Press, 2006.

[13] L. Zhang, X. He, L. Dai, et al. The simulator experimental study on the operator reliability of Qinshan nuclear power plant. Reliability Engineering System Safety, 2007, 92(2): 252~259.

[14] X. He, X. Huang. Human reliability analysis in industrial systems: principles, methods and applications [M]. Beijing: Tsinghua University Press, 2007.

[15] Y. Yi, J. Li, Z. Huang. Reliability data collection and processing of PSA equipment in operational nuclear power plants [M]. Beijing: Atomic Energy Press, 2015.