Study on Human Reliability Assessment for MCR and RSS Switching Switch Configuration Scheme

Zhihui Xu[1], Siqi Jin[1], Huaqing Peng[1], Peng Wang[2]

1.State Key Laboratory of Nuclear Power Safety Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen, Guangdong, 518172, China
2.Taishan nuclear power joint venture Co., Ltd., Taishan, Guangdong,529200, China

ABSTRACT

In order to avoid the failure of MCR/RSS switching function caused by the failure of single MCR/RSS switch, MCR/RSS switch usually adopts redundant design and multi-position arrangement. This paper presents a specific case of human reliability assessment of nuclear power plant task, and systematically evaluates whether the operator can quickly evacuate to RSS and complete the switching operation from the perspective of human engineering. This paper provides a beneficial attempt for the overall assessment of human risk of specific personnel tasks, and puts forward reasonable opinions on the improvement of design scheme, which is convenient for modeling and iterative consideration with PSA model.

Keywords: Main control room, Remote shutdown station, Human reliability analysis, Human Factor Engineer

I. INTRODUCTION

The Main Control Room (MCR) provides centralized and effective supervision of the nuclear power plant under all operational conditions. It ensures the safe operation of nuclear power plant and can take measures to maintain its safety or return it to a safe state after experiencing a design basis accident. The Remote Shutdown Station (RSS) is an auxiliary control point that is physically and electrically separated from the MCR. The RSS is equipped to offer sufficient monitoring signals and operational capabilities, allowing the nuclear power plant to achieve a safe shutdown state and monitor key parameters in case the MCR is unavailable, such as during a fire. Operations from the MCR and RSS cannot occur simultaneously; they are interlocked with each other. The control functions switch and interlock between the MCR and RSS are achieved through the MCR/RSS transfer switch.

II. MCR/RSS SWITCHING SWITCH CONFIGURATION SCHEME

II.A. MCR/RSS Switching Switch Configuration

The MCR/RSS switching switch adopts mutually independent multi-contact models, ensuring that a single MCR/RSS switching switch signal can be independently connected to instrumentation and control systems and remain consistent with their total number of columns. To prevent the failure of a single MCR/RSS switching switch from causing the MCR/RSS switching function to fail, the MCR/RSS switching switch adopts a redundant design. Configuration is designed with three MCR/RSS switching switches, using a 3-out-of-2 voting logic. The MCR/RSS control function switch can be completed as long as any two or all three MCR/RSS switching switches function properly, as shown in Figure 1. The nuclear power plant normally operates in MCR mode. If an operator completes the MCR/RSS switching operation, the system enters RSS mode, and personnel in both MCR and RSS are informed through specific alarm signals.

II.B. MCR/RSS Switching Switch Configuration

Three MCR/RSS switching switches are arranged at three different locations, both inside and outside the RSS. These switches are non-keyed toggles and can be operated directly. Switch 1 is positioned on the panel surface inside the RSS room, covered by a protective shield to prevent inadvertent operations.

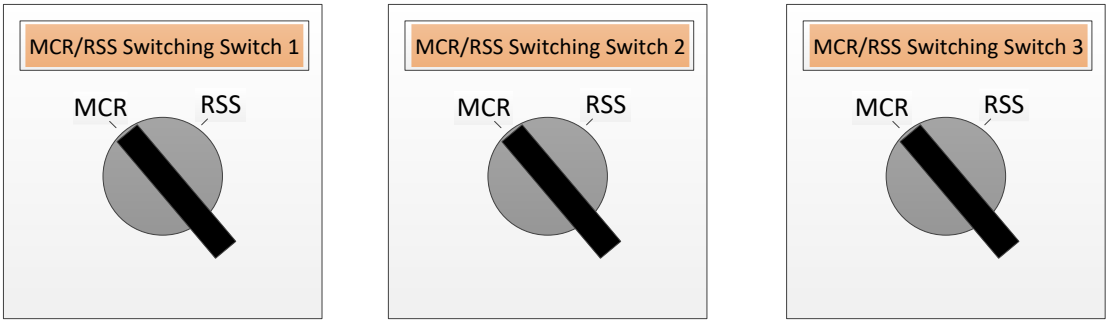

FIGURE 1. Schematic Diagram of MCR/RSS Switching Switch

II.C. MCR/RSS Switching Switch Environment

Adequate operating space is maintained around the three MCR/RSS switching switches, and the rooms they are situated in are ventilated by a ventilation system to provide suitable ventilation conditions, temperature, and humidity. Under normal circumstances, normal lighting is provided by the nuclear island lighting system. In special emergency situations, backup lighting is supplied by the nuclear island emergency lighting system.

III. ANALYSIS OF MCR/RSS SWITCHING OPERATION TASKS

If the environment in the main control room deteriorates for some reason, the operating shift decides to evacuate from the MCR to the RSS. The operator and coordinator simultaneously evacuate from the MCR to the RSS. The operator first switches the three MCR/RSS switchers at three different locations to the "RSS" position according to the guidance of the accident procedure. The coordinator confirms that the three MCR/RSS switchers at three different locations have been switched to the "RSS" position according to the guidance of their own accident procedure. After completing the operation and confirmation of the MCR/RSS switchers, the operator and coordinator also need to log in to the operator workstation in the RSS and activate its control function. The detailed task analysis is shown in Table 1.

Table 1. Main steps of the task and time consumption analysis

No.	Operation steps	Specific actions	Time required (minutes)	Possible failures	Failure consequences	Key steps	Recovery measures
1	Confirm RT	Use RPS0300TO1/0300TO2 (ECP panel)	0.8	1. Forgot to execute 2. Execution failure	RT failure	No	-
2	Carry materials	Take necessary materials and bring them to RSS	0.25	1. Forgot to take out 2. Took wrong materials	-	No	-
3	Decide to evacuate	Based on the deterioration of MCR, decide to evacuate MCR and go to RSS	1.6	1. Insufficient decision-making time	Failed to evacuate in time	No	-
4	Execute switch operation	Go to the chief's office to get the key of the switch protection box	2	1. Forgot to bring the key 2. Took the wrong key	Omitted carrying	Yes	Return to the chief's office to get the key
		Walking to the RSS room	3	-	-	Yes	-
		Open the protection box and put switch 1 in the "RSS" position	0.25	1. Forgot to take the switch	Switching fails	Yes	-

No.	Operation steps	Specific actions	Time required (minutes)	Possible failures	Failure consequences	Key steps	Recovery measures
		Open the protection box and put switch 2 in the "RSS" position	0.25	1. Switching is not in place 2. Forgot to bring the key	Switching fails	Yes	-
		Open the cover and put switch 3 in the "RSS" position	0.25	Switch is not turned on Forgot to take the switch	Switching fails	Yes	-
		OP logs in to the RSS workgroup and confirms activation	0.2	1. Forgot the login password and failed to log in	Failed login	No	Ask colleagues for help

Note: The time required was measured onsite.

IV. MCR/RSS Switching Switch Environment

IV.A. Failure analysis of switching operation

Based on the main task steps in Table 1, the key steps leading to failure in the MCR/RSS switchover are:
a) Taking the keys of the RSS small box (forgetting to take the keys or taking the wrong ones);
b) The switch was not turned in place (the operation was not carried out properly or the switch was missed).
Based on this, an event tree model as shown in Figure 2 and a fault tree model as shown in Figure 3 can be constructed.

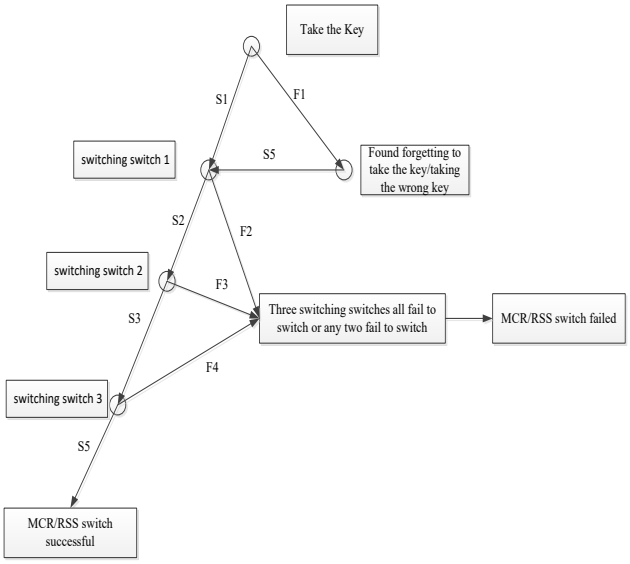

FIGURE 2.MCR/RSS Switching Event Tree

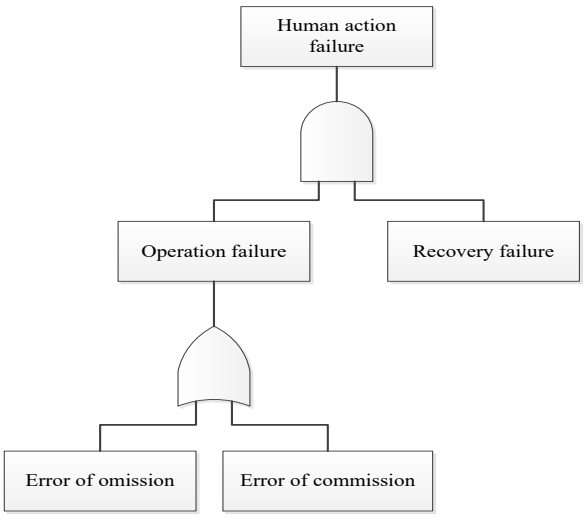

FIGURE 3.The Fault Tree

IV.B. Calculation of switching operation failure

This calculation is based on the failure data in the NUREG/CR 1278 Basic Failure Data Table, as shown in Table 2.

Table 2. Failure probability calculation of key steps

Human-induced events	Potential failures	Omission failures	Execution failures	Recovery failures	HEP
Step 1: Operator retrieves key	Key not retrieved or wrong key retrieved	Probability of key not retrieved: 0.001, according to NUREG/CR 1278, Table 20-8: Item 1	Probability of wrong key retrieved: 0.001, according to NUREG/CR 1278, Table 20-9, analogous to Item 2	Probability of recovery: 0.5 , according to NUREG/CR 1278, Table 20-22 (Item 8)	HEP1 = (0.001 + 0.001) * 0.5 = 1.0E-3
Step 1 recovery: Discovers forgotten key, returns to retrieve it	N/A	N/A	N/A	S5=1, recovery is successful	Opening of protective box reveals forgotten key; time analysis indicates sufficient time to return and retrieve it
Step 2: Executes switch operation 2201CC-	Switch operation fails	Probability of switch operation forgotten: 0.003 , according to NUREG/CR	Switch operation fails to reach target position: 0.003. According	Probability of recovery: 0.1, according to NUREG/CR 1278, Table 20-22 (Item 1)	HEP2 = (0.003 + 0.003) * 0.1 = 6.0E-4

		1278, Table 20-7, Item 1 (procedure with >10 steps)	to NUREG/CR 1278, Table 20-12 (Item 10)		
Step 3: Executes switch operation 3201CC-	Switch operation fails	Probability of switch operation forgotten: 0.003, according to NUREG/CR 1278, Table 20-7, Item 1 (procedure with >10 steps)	Switch operation fails to reach target position: 0.003, according to NUREG/CR 1278, Table 20-12 (Item 10)	Probability of recovery: 0.1 , according to NUREG/CR 1278, Table 20-22 (Item 1)	HEP3 = (0.003 + 0.003) * 0.1 = 6.0E-4
Step 4: Executes switch operation 1201CC-	Switch operation fails	Probability of switch operation forgotten: 0.003, according to NUREG/CR 1278, Table 20-7, Item 1 (procedure with >10 steps)	Switch operation fails to reach target position: 0.003, according to NUREG/CR 1278, Table 20-12 (Item 10)	Probability of recovery: 0.1, according to NUREG/CR 1278, Table 20-22 (Item 1)	HEP4 = (0.003 + 0.003) * 0.1 =6.0E-4

Note: The HEP maintains its original value in table 2, and will be transformed into a median by PSA analysts when introduced into the PSA model.

In the calculation process, NUREG/CR 6883 is referred to, and 1.0E-5 is adopted as the lower limit of human failure probability. Based on the relatively severe fire scenario in the main control room, from the time of discovering fire in the main control room, a total time window of 30 minutes without intervention is taken for the entire evacuation and switch task. The experienced time of about 12 minutes for the temperature or smoke in the main control room to exceed the environmental conditions for people to continue residing due to fire combustion is deducted, i.e., the effective time window from MCR evacuation to RSS is about 30-12=18 minutes. According to the evaluation in Table 1, the whole evacuation task takes about 9 minutes, so the surplus time is 18-9=9 minutes, while the time for returning to take the keys again due to forgetting is 3+2+3=8 minutes. Therefore, after forgetting to take keys, it is allowed to return and take keys again before continuing to perform switch operation.

IV.C. Calculation of switching operation failure

Since the failure of step 1 can be completely recovered, the correlation between steps 2, 3, and 4 is considered for the failure of switching from MCR to RSS. Since the operations of steps 2, 3, and 4 are performed sequentially, the correlation factors and analysis results are shown in Table 3.

Table 3. Correlation analysis between steps

Correlation	Personnel	Time	Location	Clues	Relevance
Step 2 and Step 3	Same	Similar	Different	Different	High
Step 3 and Step 4	Same	Similar	Different	Different	High

Note: In order to quickly interface the HRA calculation results with the PSA model, this table conducted correlation analysis based on the commonly used SPAR-H method's correlation calculation formula, aiming to further examine the HRA calculation results that are more in line with reality.

The criteria for correlation judgment based on NUREG/CR 6883 are considered. After correlation consideration, the failure probabilities of steps 2, 3, and 4 can be corrected as follows:

$$F_2=HEP_2=6.0E\text{-}4 \quad (1)$$

$$F_3=(1+6.04E\text{-}4)/2=0.5 \quad (2)$$

$$F_4=F_3=0.5 \quad (3)$$

The switch failure from MCR to RSS includes the failure of all three buttons to switch, or the failure of any pair of two buttons to switch. The failure probabilities for each sub-scenario are as follows:

a) The probability of all three buttons failing to switch is:

$$HEP_f=F_2*F_3*F_4=6.0E\text{-}4*0.5*0.5=1.5E\text{-}4 \quad (2)$$

b) The probability of steps 2 and 3 failing to switch, while step 4 switches successfully is:

$$HEP_{(2/3)}=F_2*F_3*(1-F_4)=1.5E\text{-}4 \quad (3)$$

c) The probability of steps 2 and 4 failing to switch, while step 3 switches successfully is:

$$HEP_{(3/4)}=(1-HEP_2)*HEP_3*F_4=6.0E\text{-}4*0.5=3.0E\text{-}4 \quad (4)$$

d) The probability of steps 3 and 4 failing to switch, while step 2 switches successfully is:

$$HEP_{(2/4)}=F_2*(1-F_3)*HEP_4=6.0E\text{-}4*0.5*6E\text{-}4=1.8E\text{-}8 \quad (5)$$

Which adopts the human factor failure probability value of HPLV=1.0E-5.
Therefore, the overall mission failure probability is:

$$HEP_t=HEP_f+HEP_{(2/3)}+HE_{P(3/4)}+HEP_{(2/4)}=1.5E\text{-}4+1.5E\text{-}4+3E\text{-}4+1.0E\text{-}5=6.1E\text{-}4 \quad (6)$$

V. CONCLUSIONS

According to the task analysis of the MCR/RSS switching scheme, it can be found that the configuration and layout of the MCR/RSS switch are reasonable. The operation team can refer to the procedures to check important operation steps, the operator evacuation path is clear and accessible, and the implementation location of the switching operation has good ventilation and lighting. The verbal communication between the operator and coordinator is not hindered, and the communication requirements of the operator and coordinator are met. Through the calculation of the probability of task error in switch switching, it can be found that the probability of task error is low, and the operator can reliably evacuate to RSS and complete the switching operation, which will not have an unacceptable impact on the overall safety of the nuclear power plant. At the same time, the improvement suggestions proposed in this article are as follows: it is necessary to add guidance in the operation rules that can clarify the evacuation rules and criteria under fire scenarios.

ACKNOWLEDGMENTS

This paper is supported by State Key Laboratory of Nuclear Power Safety Technology and Equipment.

REFERENCES

[1] Boring R., Boring L. and Gertman, D.I. Atomistic and Holistic Approaches to Human Reliability Analysis in the US Nuclear Power Industry[J]. Safety and Reliability, 2005, 25(2): 21 – 37.
[2] Lee S.W., Kim A.R., Ha J.S. and Seong, P.H. Development of a Qualitative Evaluation Framework for Performance Shaping Factors (PSFs) in Advanced MCR HRA[J]. Annals of Nuclear Energy, 2011, 38:1751-1759.
[3] Ma Zhanguo, Yoshikawa Hidekazu, Nawaz Amjad, Yang Ming. A human–machine interaction design and evaluation method by combination of scenario simulation and knowledge base. Journal of Nuclear Science and Technology, v 55, n 5, p 516-529, May 4, 2018.
[4] Gertman D., Blackman H., Marble J., Byers and Smith C. The SPAR-H Human Reliability Analysis Method, NUREG/CR-6883[R]. Idaho National Laboratory, Washington D.C.:USNRC, 2004.
[5] U.S Nuclear Regulatory Commission. Human Factors Engineering Program Review Model [R]. NUREG-0711, Rev 3, 2012.
[6] Zhihui Xu, Jiemei Zhang, Xuegang Zhang. Study for Reliability Analysis of Operator Response Process under IBLOCA Accident in Nuclear Power Plant [C]// International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection for Nuclear Power Plant. Springer, Singapore, 2020: 599-609.
[7] Swain A.D. Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772 [R]. Washington D.C.: USNRC,1987.
[8] International Electrotechnical Commission (IEC). Nuclear power plants - Design of control rooms - Functional analysis and assignment[S]. IEC 61839. Geneva: International Electrotechnical Commission, 2000.
[9] International Electrotechnical Commission (IEC). Design for control rooms of nuclear power plants[S]. IEC 60964. Geneva: International Electrotechnical Commission, 1989.
[10] Denham L. Phipps, George H. Meakin, Paul C.W. Beatty. Extending hierarchical task analysis to identify cognitive demands and information design requirements[J], Applied Ergonomics, 2011, 42(5): 741-748.
[11] Ormerod T.C., Shepherd, A. Using task analysis for information requirements specification: the sub-goal template (SGT) method[J]. Diaper, D., Stanton, N.A. (Eds.), The Handbook of Task Analysis for Human- Computer Interaction. Lawrence Erlbaum Associates, 2004, 16: 347-365.