Reliability Analysis of Operations in the DCS of a Nuclear Power Plant Based on Accident Simulation

Wenjie Lu and Licao Dai(✉)

Human Factor Institute, University of South China,
Hengyang City 421001, People's Republic of China
lujj94@qq.com, dailicao@sina.com

Abstract. With the development of computer technology, the operation environment of main control rooms in modern nuclear power plants (NPP) has considerably changed over the years, namely the use of advanced Digital Control System (DCS). In this paper, the accident of steam generator tube rupture (SGTR) of a DCS in a nuclear power plant is simulated and the task analysis method is used to explore the reliability of the secondary side cooling and depressurization operation of the operators. The effect of the man-machine interface changes on operators is studied on the basis of SGTR accident simulation. An event tree is built to model the operators' activities of handling the accident. Operators' behaviors in a DCS are determined and a quantitative calculation of operators' reliability is then conducted.

Keywords: Digital control system · Steam generator tube rupture
Mission analysis method · Quantitative calculation

1 Introduction

Compared with the traditional control system, the flexibility of the operation of nuclear power plants are more advantageous and DCS is getting more and more widely used in the nuclear power plants. DCS operators monitor the plant system and perform operations mainly through the mouse on the computer screens instead of manual activities on instrument panels, signal lamps, buttons and switches in an old control room. The new man-machine interface may bring changes to operators on cognition, resulting in new human errors. The reliability of DCS has a significant impact on the safety and availability of nuclear power plants. Therefore, the safety impact of nuclear power plant DCS must be systematically evaluated and verified. Human reliability analysis plays an important role in the safety analysis of NPP operation. With the application of the digital control system in modern nuclear power plants, the operating environment of the main control room has undergone major changes, thus changing the operator's cognitive process, behavior patterns and task characteristics, mainly on the information display, man-machine interface interaction and management, operating procedures, control and input facilities, as well as alarm systems, operator decision-making and

P. M. F. M. Arezes (Ed.): AHFE 2018, AISC 791, pp. 264–271, 2019.
https://doi.org/10.1007/978-3-319-94589-7_26

support systems. DCS has many technical advantages, but the combination of potential human factors and DCS will produce new human error.

2 DCS Control Process Error Mode

2.1 DCS Control Features

The traditional main control room has a very large work space, with a space-specific man-machine interface. Alarms, display and control, man-machine interface components have their own unique and easy-to-see spatial location. Operators walk to the panels with different functions to perform tasks. In the DCS, the information is displayed on the video display unit (VDU) and the large display system (LDS), with the controls being operated by the mouse and the keyboard. Man-machine interfaces on DCS tend to lack physical sense of space. Operators work before computers. All these lead to the change of the cognitive process of the operators. New human error should be considered in the human reliability analysis of DCS.

The primary tasks of nuclear power plant operators are monitoring and control, such as monitoring flow, starting pumps and switching valves. The primary tasks involve four cognitive processes: monitoring and testing, situation assessment, response planning and response implementation [1]. Operators in the DCS perform the appropriate auxiliary tasks to complete the primary tasks. These auxiliary tasks are called "interface management tasks." NUREG/CR-6690 states the general interface management tasks include the following items [2] :

(1) Configuration: Set the man-machine interface of the computer workstation to the desired arrangement, for example by assigning software functions on the multi-purpose display.
(2) Browse: Accessing and retrieving specific aspects of man-machine interfaces on computer workstations, such as monitors or controllers.
(3) Arrangement: Adjust the operator's perception of the information. It can happen on several levels, inside and inside the display, such as arranging items within a display page or window.
(4) Access: Access the human-machine interface to determine information about its status, such as the current display's relationship to the rest of the display network or the most recent file date. This category also includes the use of help systems.
(5) Automation: Set shortcuts to simplify interface management tasks.

In a DCS, operators can only see part of the information at any time through the VDU on the DCS. The limited viewing area is a feature called "keyhole effect" [3]. Operators must perform interface management tasks to accessing information through the limited windows. Interface management tasks may affect the cognitive reliability of the operator. When operators conduct primary tasks, they need some attention resources to perform interface management task. Due to limited attention resources, the performance of the primary tasks maybe impaired. Slips and lapses may occur. In addition, the primary task is interrupted in a way of selection of wrong pictures, slow execution and missing steps.

2.2 Control Process of Human Error

In the past a large number of documents on human error have different definitions and classification, there are some people in the DCS error pattern and the traditional main control room the same, and because DCS has different characteristics, the need for other human error mode. The error is usually divided into error of omission (EOO) and error of commission (EOC) [4]. EOO said he forgot to carry out the task, but EOC said the wrong mission. Rasmussen classifies staff behaviors into three categories (SRK models): skill-based, rule-based, knowledge-based [5]. The form of information content in skill-based behavior is signal, and the performance of personnel behavior is mainly influenced by the schema of pre-memory and is represented by the similar structure in the space-time region. The content of the information content in the rule-based behavior is a sign, Personnel behavior is guided by pre-existing rules (IF-THEN rules); knowledge-based behavior in the face of the new scene action plan to be made in real time. The classification of human error caused by human behavior in SRK model is based on the difference of cognitive behavior between different behaviors. It is also based on the view that cognitive failure is the main failure mode of complex human-machine interface. Skill-based behavior basically requires no awareness, including two types of mistakes, lapse and slip. Knowledge-based personnel behavior requires relatively high cognitive behavior, rule-based second, the error caused by these two kinds of personnel actions is a mistake. From the error mechanism point of view, slip and lapse is the main attention or memory problems, and mistake mainly decision-making problems. This shows that the prevention of human factors caused by the behavior of skilled and regular personnel is mainly to prevent the operator's memory and attention problems in order to avoid slip and lapse, reduce the slip and lapse can also reduce the possibility of mistake. In addition, it is in the accident conditions to reduce the operator's decision-making errors, reduce the operator's mistake in the accident. Since the main cause of errors is not the DCS design, but the operator's misjudgment, the interface between the traditional master control room and the DCS may be the main cause of lapse and slip in the operator's operation [6]. Swain and Guttmann [7] Six patterns of human error are proposed, including omission of operation, wrong object, incorrect operation, confusion of modes, improper operation and delayed operation.

2.3 DCS Cognitive Behavior Model

The cognitive process of human includes sensory, perception, memory, thinking, imagination and other cognitive activities. Through these cognitive activities, we can understand the characteristics, the nature and the interrelationships of objective things. Cognitive load has a great impact on the cognitive reliability of people, cognitive overload may make people's cognitive process may be mistakes. However, the increase of cognitive load of operators on DCS is caused by the bottleneck of human cognitive resources (memory and attention, etc.) [8]. When the operator in the implementation of operational tasks cognitive resource needs and cognitive resource supply to match, cognitive tasks are likely to be better implemented, if the cognitive resource needs more

than the supply or lack of cognitive information, the operator Cognitive performance will decline, resulting in errors.

In Budley-Hitch's working memory model [9], Proposed that there are two independent short-term memory buffers, one is a voice loop used to process voice information and store numbers, the other is an air-space drawing board used to process the air-space information to determine the spatial relationship, and the central actuator is responsible for completing Coordinate the work and exchange information rapidly between the two memories. Operators in the DCS in the same form (oral or visual space) encoded information easily interfere with each other, while in the traditional master control room operators can form the object and the system of spatial separation, which will enable operators to form more in the operation Lasting, more reliable, clearer and more meaningful "Skyshield." In terms of long-term memory, traditional control rooms are more "coherent" and "ecological" than DCS, and operators are able to form a "mental model" that is stronger than DCS. In terms of attention, Wickens's SEEV model [10] four factors of concern were raised: the saliency of the signal, the effort to note the signal, the operator's expectations of the signal, and the task's relevance or value of the signal.

3 Simulation Experiment

The simulator in the experiment was designed and researched by China Guangdong Nuclear Power Group Co., Ltd. with reference to the Daya Bay PWR nuclear power plant so that the environment of the simulation experiment is similar to that of the nuclear power plant. The experiment is based on the accident of heat transfer tube rupture (SGTR) in the steam generator of a nuclear power plant. The task analysis method is used to explore the reliability of the secondary side cooling and depressurization operation of the operator on the DCS. Steam generator heat transfer tube rupture (SGTR) refers to the rupture of the heat transfer tube between the primary side and the secondary side. When the reactor is in a power operating condition, the pressure on the primary side is much higher than the pressure on the secondary side. When the heat pipe breaks, the primary coolant leaks through the breach to the secondary side. The experiment mainly analyzed the rupture of the heat transfer tube of a steam generator and recorded the secondary side cooling and depressurization operation of the operator on the DCS in the simulation experiment.

3.1 Task Analysis

The control tasks in the DCS consist of the primary tasks and the interface management tasks. One or more secondary tasks in the execution of the tasks fail. If the recovery is timely, the final major tasks can also be successful. If the recovery of the secondary task fails is unsuccessful, the failure or failure of the relevant secondary task causes the primary task to fail. In order to study the reliability of the operator's secondary cooling and depressurization operation on the DCS in the background of SGTR accident, the primary tasks and interface management tasks in the DCS are analyzed and divided into observable sub-tasks to control the tasks. Human error in the primary tasks may lead to

the implementation of inappropriate controls, and human error in the secondary tasks is likely to delay access control and display, hinder the operation of the operator, or select the wrong controls and displays [11]. There is no interface management task in the operation of the traditional main control room, but DCS interface management tasks occupy a large part. Analyze the primary tasks and interface management tasks in the DCS and model them as unit tasks for control tasks so that basic human error probabilities for unit tasks can be observed and calculated in simulator-based experiments or field operations studies. Unit tasks include: Operation selection, screen selection, control device selection and operation execution [12]. In this paper, the establishment of an event tree model approach, the primary tasks and interface management tasks into the event tree model, based on the results of the event tree analysis to quantify the results obtained operator DCS on the secondary side of the cooling step-down operation the reliability.

3.2 Establish the Event Tree Model

Under the background of experimental simulation of SGTR accident, the most important function of the operator in DCS is to obtain information and search information. Then according to the state parameter display on the VDU, combined with his own mental model to evaluate the status of the power plant, accordingly, Strategy and response to the implementation of behavior, need to develop a clear strategy. The establishment of the event tree model shown in Fig. 1.

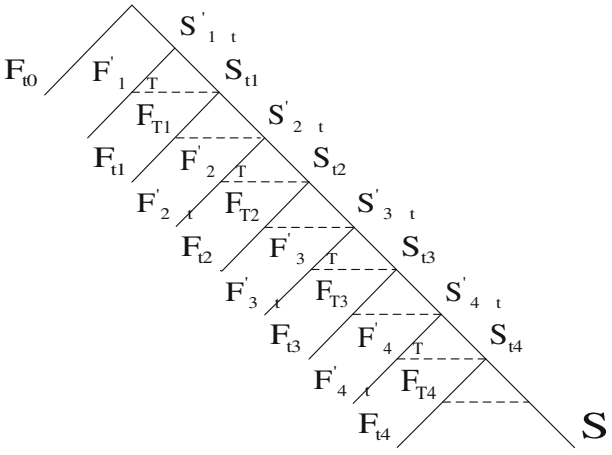

Fig. 1. The event tree model

Name	Content	Task category
S'_{tA}	Operator successfully completed the A interface operation management tasks	Interface management tasks
F'_{tA}	The operator did not complete the pre-A interface management tasks	Interface management tasks
S_{tA}	The operator successfully completed A operation	Primary tasks
F_{tA}	The operator did not complete the A operation successfully	Primary tasks
F'_{TA}	The operator successfully corrected the error and completed the pre-A interface management tasks	Interface management tasks
F_{TA}	The operator successfully corrected the error and completed the A operation	Primary tasks

The value of A in the table is 1, 2, 3, and 4, corresponding to the symbols in the figure, where A = 1 indicates the operation of reverting to safety injection, A = 2 means the operation of reversion of the accidental evaporator, A = 3 means A circuit cooling operation, A = 4 indicates the stability of the accident evaporator pressure operation.

for F'_{t1}, Check the "THERP Manual", the operator failed to complete the security before the return of the interface management tasks before the error probability of the nominal value 1×10^{-3}, Consider the impact of stress factor, amended as $5 \times 1 \times 10^{-3} = 5 \times 10^{-3}$; for F'_{T1}, Check the "THERP Manual", the operator failed to complete the security before the return of the interface management tasks before the error probability of the nominal value 1×10^{-3}, Consider the impact of stress factor, amended as $5 \times 1 \times 10^{-3} = 5 \times 10^{-3}$.

Similarly, consult "THERP Manual" F'_{t1}, F'_{t2}, F'_{t3} The error probability correction value is 5×10^{-3}, F'_{T2}, F'_{T3}, F'_{T4} The error probability correction value is 5×10^{-3}.

F_{t0} for operators failing to detect SGTR alerts, the probability is very small in simulations and can be ignored.

The incident tree has nine wrong paths F_1, F_2, F_3, F_4, The probability of their mistakes are:

$$P(F_1) = F'_{t1} \times F'_{T1} = 5 \times 10^{-3} \times 5 \times 10^{-3} = 2.5 \times 10^{-5}. \quad (1)$$

$$P(F_2) = F'_{t1} \times F'_{T1} = 5 \times 10^{-3} \times 5 \times 10^{-3} = 2.5 \times 10^{-5}. \quad (2)$$

$$P(F_3) = F'_{t3} \times F'_{T3} = 5 \times 10^{-3} \times 5 \times 10^{-3} = 2.5 \times 10^{-5}. \quad (3)$$

$$P(F_4) = F'_{t4} \times F'_{T4} = 5 \times 10^{-3} \times 5 \times 10^{-3} = 2.5 \times 10^{-5}. \quad (4)$$

The total probability of a mishap on an SGTR accident is:

$$P = P(F_1) + P(F_2) + P(F_3) + P(F_4) = 1 \times 10^{-4}. \quad (5)$$

4 Conclusion

Compared with the traditional control system, the change of digital control system of nuclear power plant will lead to the change of cognitive activity of the operator, resulting in the new human error, which will affect the human reliability. And new human error will affect the system Bring the risk. This paper studies the reliability of the secondary side cooling and depressurization operation of the operator on the DCS in the background of the rupture of the heat transfer tube of the steam generator of the nuclear power plant and reveals the cognitive process of the operator in the SGTR accident response and the interface management tasks And the primary tasks of human error prevention and control to provide technical measures to reduce the risk and improve the safety level of nuclear power plants.

Acknowledgements. The financial support by the National Natural Science Foundation of China (No. 51674145, 71771084), Postdoctoral Science Foundation of China (No. 2016M600 633), Natural Science Foundation of Hunan Province (No. 2017JJ2222) are gratefully acknowledged.

References

1. Barriere, M., Bley, D., Cooper, S., Forester, J., Kolaczkowski, A., Luckas, W., Parry, G., Ramey-smith, A., Thompson, C., Whitehead, D., Wreathall, J.: Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA), NUREG-1624, US Nuclear Regulatory Commission (2000)
2. O'Hara, J.M., Brown, W.S., Lewis, P.M., Persensky, J.J.: The Effects of Interface Management Tasks on Crew Performance and Safety in Complex, Computer-Based Systems, NUREG-6690, US Nuclear Regulatory Commission (2002)
3. Woods, D., Johannesen, L., Cook, R., Sarter, N.: Behind human error: cognitive systems, computers, and hindsight (CSERIAC SOAR 94-01). Wright Patterson Air Force Base. Crew Systems Ergonomics Information Analysis Center, Ohio (1994)
4. Stubler, W.F., O'Hara, J.M.: Soft Control: Technical Basis and Human Factors Review Guidance, NUREG/CR-6635, US Nuclear Regulatory Commission (2000)
5. Rasmussen, J.: Outlines of a hybrid model of the process operator. In: Sheridan, T.B., Johannsen, G. (eds.) Monitoring Behavior and Supervisory Control, pp. 371–383. Plenum Press, New York (1976)
6. Lee, S.J., Kim, J.H., Jang, S.C.: Human error mode identification for NPP main control room operations using soft controls. J. Nucl. Sci. Technol. **48**(6), 902–910 (2011)
7. Swain, A.D., Guttmann, H.E.: Handbook of Human-Reliability Analysis with Emphasis on Nuclear Power Plant Application. Sandia National Laboratories, NUREG/CR-1278, USNRC (1983)

8. Wang, Z., Gu, P., Zhang, J.: Human factor engineering analysis for computerized human machine interface design issues. Chin. J. Nucl. Sci. Eng. **12**(4), 367–368 (2010)
9. Baddeley, A.D., Hitch, G.J.: Working memory. In: recent Advances in Learning and Motivation, pp. 47–90. Academic Press, New York (1974)
10. Wickens, C.D., Goh, J., Helleburg, J., et al.: Attentional models of multi-task pilot performance using advanced display technology. Hum. Factors **45**, 360–380 (2003)
11. Janga, I., Kima, A.R., Al Harbib, M.A.S., Lee, S.J., Kanga, H.G., Seonga, P.H.: An empirical study on the basic human error probabilities for NPP advanced main control room operation using soft control. Nucl. Eng. Des. **257,** 79–87 (2013)
12. Ha, J.S.: A soft control model for human reliability analysis in APR-1400 advanced control rooms (ACRs). Procedia Eng. **100**, 24–32 (2015)