Accident Analysis of Equipment System Based on the Event Sequence Diagram and Fault Tree

Ren xin[1,2], Li yuan[3], Tie-ying WU[4], Zhang kan[5], Ma li[1,*] Corresponding author

1. Naval Medical Research Institute, Shanghai, 200433, China

2. Graduate School, National Defense University, Beijing, 100091, China

3. Maintenance Management Teaching-research Office, Equipment Academy, Beijing, 101400, China

4. Oncology Department, The 264th-Hospital of PLA, Taiyuan, 030000, China

5. Department of Equipment Economics and Management, Naval Univ. of Engineering, Wuhan, 430033, China

Keywords: event sequence diagram; FT; equipment system; internal fault tree

Abstract. The application of ESD_FT (Event Sequence Diagram and Fault Tree) method in accident analysis of equipment system was discussed in this paper, a new ESD basic event launched by internal fault tree was proposed, and the ESD_FT analysis model of the equipment system coolant loss accident was established. According to the analysis results, it can be concluded that the ESD_FT comprehensive analysis method is very effective and practical for accident analysis.

1 Introduction

ESD (event sequence diagram) is a kind of intuitive graphical description method, but the ESD method has many disadvantages in model control, event processing, graphic modeling and so on. For the complex system, the model produced by pure ESD is often too large, complex and not intuitive. The model produced by ESD_FT comprehensive analysis model is simple and intuitive and it can make full use of the fault tree analysis technique advantages, and the ESD_FT comprehensive analysis model is a very effective for accident analysis.

2 ESD and ESD_FT method introduction

The basic unit of ESD includes event, condition, logic gate, and constraint. When the dynamic system is described, ESD introduces a variety of dynamic logic symbols, such as competition, restriction, etc.

ESD_FT comprehensive analysis is the method in which all the ESD events are constructed through the fault tree based on ESD modeling of the system, the fault tree taking ESD event for top event is named as internal fault tree. In order to make the ESD_FT comprehensive analysis method more concise and intuitive, a new symbol is introduced so as to represent the ESD basic events expanded by the internal fault tree, as shown in figure 1, and the basic process of the ESD method combined with the fault tree can be shown in figure 2.

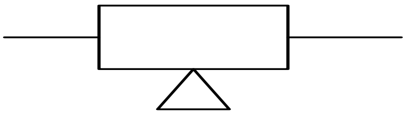

Fig.1 ESD event expanded by the internal fault tree

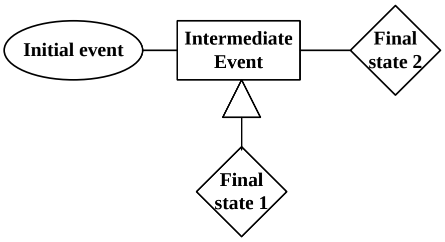

Fig.2 Basic flow diagram of ESD method combining fault tree

Copyright © 2017, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

3 Water replenishment system of equipment system

The working process of the equipment system includes two phases: feed water preparation and replenishment. Assume that these two phases are two subsystems of the feed water system, respectively named as subsystemIand subsystemII. The subsystemIis composed of water, replenishment pump barge, deoxygenation/salt ion exchanger, all kinds of valves. The subsystem IIis composed of water supply pumps, heat exchangers, filters and valves, etc. The principle diagram of the water replenishment system is shown in figure 3.

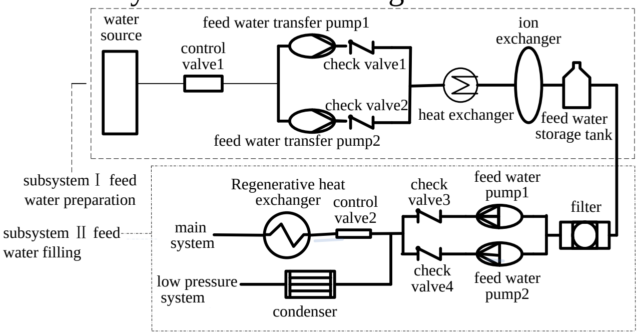

Fig.3 Principle diagram of water replenishment system

4 ESD analysis of equipment system coolant loss accident

4.1 Assumption and boundary condition

If the coolant loss accident of equipment system happens during the operation, the water replenishment system can also be used as the high pressure injection system. The responding flow diagram of equipment system after water loss accident is shown in figure 4. SP is the pressure sensor which is used to monitor the pressure of equipment system, and when the pressure reaches the minimum limit value (P<Pmin), the corresponding controller of the system will be started. SW is the water level sensor which is used to monitor the water level, and when the water level reaches the limit value of Wmin, the corresponding controller of the system will be started. CP is the pressure controller, and when the equipment system pressure reaches the limit, the pressure controller will be started to close the equipment system. CW is the water level controller, and when the water level sensor detects that the water level reaches the limit, the water level controller will be started to close the equipment system. SDL is the logic of closing the equipment system, SCM is the device of closing the equipment system, and R is the equipment system.

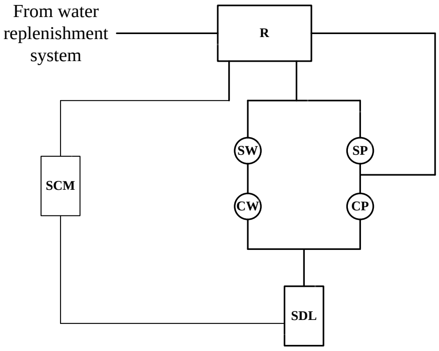

Fig.4 Responding flow diagram of equipment system after water loss accident

4.2 ESD analysis process

The water loss of the equipment system occurs during the operation, and the ESD method is used to analyze accident scene of the equipment system. The establishment process of the ESD model is described as shown in figure 5. The regulator pressure of the equipment system and the water level will drop when the coolant loss accident occurs, and reaching the lower limit of the regulator pressure and reaching the lower limit of water level become the competing events. If the pressure firstly reaches the lower limit, it is needed to firstly confirm whether the pressure sensor SP is in normal or not. If the SP is in normal, after the delay, the pressure controller CP starts, and if the CP can normally start and work, the system will develop towards the expansion door II. The SDL starts after the delay, and if the SDL can normally start and work, the SCM will start after a delay; if SCM can normally start and work, the equipment system is safe. If SDL or SCM is in failure, whether the fault can be found depends on the operator, and if the fault can be found timely, the equipment system will be safe.

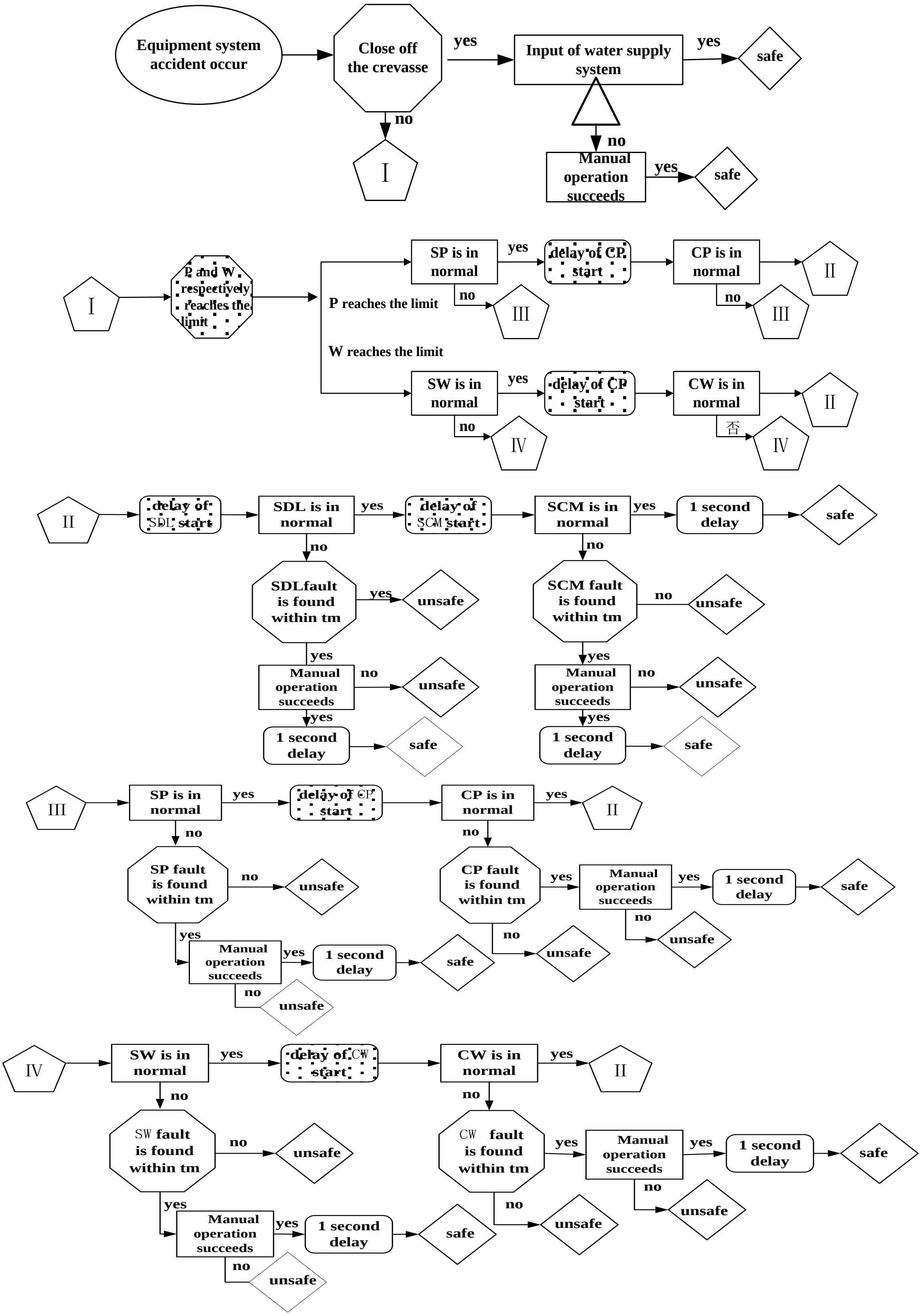

Fig.5 ESD model of equipment system water loss accident

5 Fault tree analysis

5.1 Construction of the fault tree

It is assumed that the success probability of the water source is 1, that is to say, the fault of water source does not occur in the task time. Through the analysis of the whole water supply system and the response of each part after the water loss accident, the failure tree of the equipment system can be built as shown in figure 6.

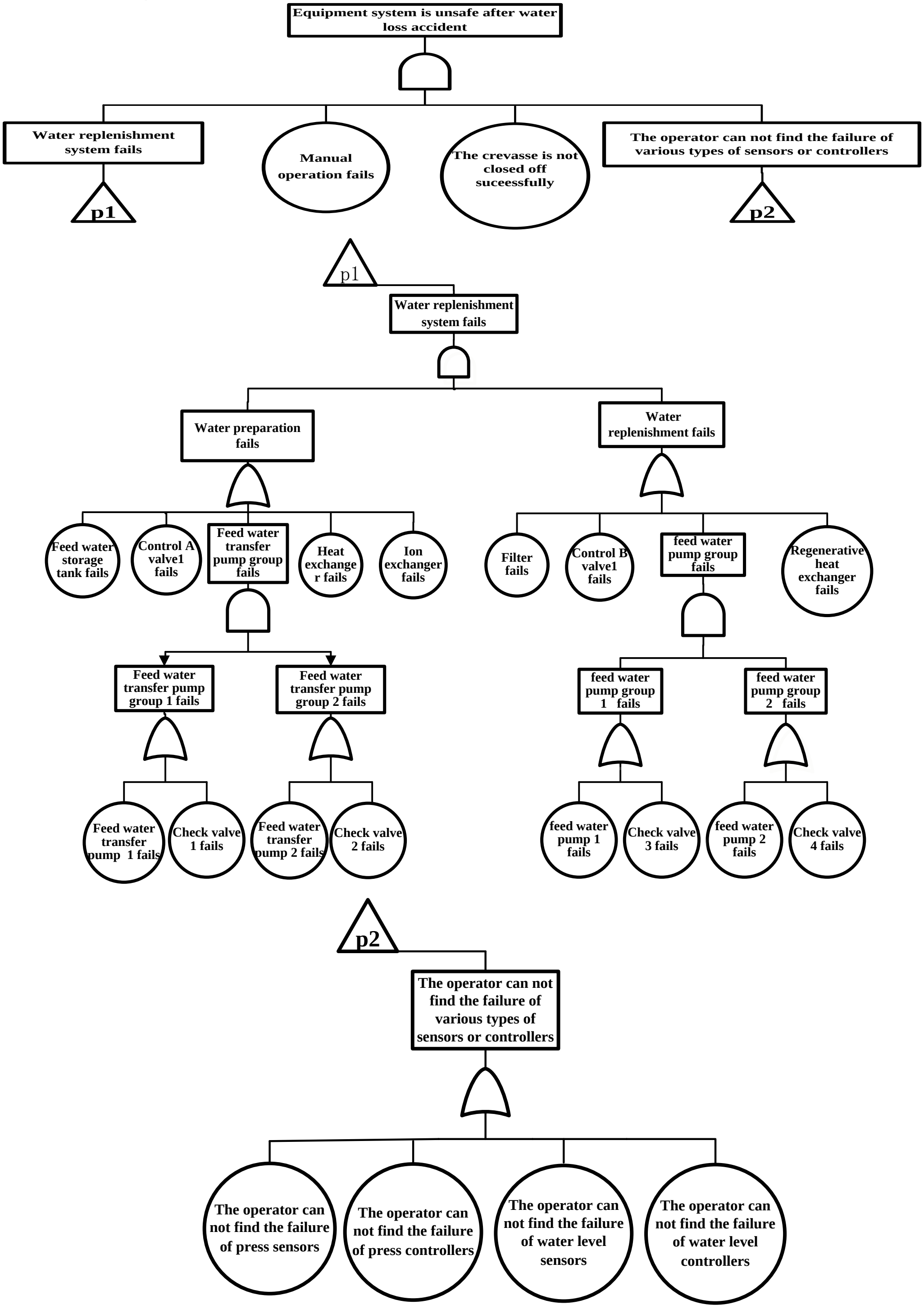
Equipment system is unsafe after water loss accident
Water replenishment system fails
Manual operation fails
The crevasse is not closed off suceessfully
The operator can not find the failure of various types of sensors or controllers
p1
p2
p1
Water replenishment system fails
Water preparation fails
Water replenishment fails
Feed water storage tank fails
Control A valve1 fails
Feed water transfer pump group fails
Heat exchanger fails
Ion exchanger fails
Filter fails
Control B valve1 fails
feed water pump group fails
Regenerative heat exchanger fails
Feed water transfer pump group 1 fails
Feed water transfer pump group 2 fails
feed water pump group 1 fails
feed water pump group 2 fails
Feed water transfer pump 1 fails
Check valve 1 fails
Feed water transfer pump 2 fails
Check valve 2 fails
feed water pump 1 fails
Check valve 3 fails
feed water pump 2 fails
Check valve 4 fails
p2
The operator can not find the failure of various types of sensors or controllers
The operator can not find the failure of press sensors
The operator can not find the failure of press controllers
The operator can not find the failure of water level sensors
The operator can not find the failure of water level controllers

Fig.6 Fault tree in which equipment can not work normally after water loss accident

5.2 Qualitative and quantitative analysis of fault tree

It is assumed that all kinds of sensor fails and the operator can not find the fault and the probability is 0.01. The success probability of each component of the replenishment system is shown in table1.

Table 1 Success probability of water replenishment system component

Component	Success probability	Component	Success probability
Water replenishment storage tank	0.999	Filter	0.995
Ion exchanger	0.995	Heat exchanger	0.995
Control valvel A and B	0.99	Water replenishment pump 1 and 2	0.99
Check valve 1,2,3 and 4	0.99	Water replenishment transfer pump 1 and 2	0.99

6 Conclusion

The application of ESD_FT method in the coolant loss accident analysis of equipment system is discussed in this paper. Compared with the traditional event tree and the independent fault tree analysis method, the ESD gives a lot of dynamic information of the system and it is more suitable for the study of equipment system accident, and ESD_FT synthesis analysis is a very effective dynamic probabilistic safety analysis method.

References

[1] Jaroslav Holy. Some insights from recent applications of HRA methods in PSA effort and plant operation feedback in Czech Republic[J]. Reliablity Engineering and System Safety, 2006, 83： 169-177.

[2] Senthil Kumar C, John Arul A, Om Pal Singh, Suryaprakasa K. Rao Reliability analysis of shutdown system[J]. Annals of Nuclear Energy 2005, 32: 63-87.

[3] Yuko Mizuno, Hisashi Ninokata, David J Finnicum. Risk-informed design of IRIS using a level-1 probabilistic risk assessment from its conceptual design phase[J]. Reliability Engineering and System Safety, 2005, 87：201-209.