A Hybrid Process Coupling Hazard Analysis Method based on PFMEA and BN

Yang Wu, Tingdi Zhao, Jiayun Chu
School of Reliability and Systems Engineering
Beihang University
Beijing, China
barry@buaa.edu.cn

***Abstract*—The coupling of man-machine-environment is one of the important hazardous causes in complex processes, which is currently lack of effective analysis methods on the subsequent impacts. In this paper, a hybrid coupling hazard analysis method applying the core ideas of Process Failure Mode and Effects Analysis (PFMEA) and Bayesian Network (BN) is proposed to decompose and describe the complex processes, and to determine the boundary conditions. Coupling hazard model is proposed to analyze the impact on the subsequent processes. BN method is used to model the accident process and evaluate the probability of the accident. Finally, the feasibility and effectiveness of the proposed models and methods are illustrated using a product case.**

Keywords-hazard analysis; coupling hazard; PFMEA; Bayesian network

I. INTRODUCTION

System safety has anessentially dynamic feature, and likewise accidents always occur in the dynamic running process[1]. It isthe transmission and coupling of hazard elementsin the system and mission flow that cause the accident[2][3]. With the increasing of complexity in modern large-scale physical systems, unintended design interaction and the coupling relationship have been the main reasons of accidents[4]. Currently,there have been abundant researches on the static coupling relationship between the system units, while research on the coupling hazard analysis in the dynamic interaction process is insufficient [5]-[7]. Except the coupling hazard feature, the hazard transmission is another important feature of the accident. Currently, researches on the hazard transmission mostly focus on the transmission mechanism of the failures hazard factors and the network hazard factors [8]-[9]. On the other hand, researches on the hazard transmission are aimed at the physical structure and the hazard factortransmission path [10]. With the development of the modern accident causation theory, the hazard transmission behavior gradually attracts attention [11][12]. But the current research is mostly limited to description without sufficient analysis. Process Failure Mode and Effects Analysis (PFMEA) is a relatively mature process hazard analysis method, so it is valid to analyze the hazard transmission [13]. To solve several problems such as multi-state, failure dependency and uncertainty in the modeling of accident causation logic in complex systems, Bayesian Network (BN) is a valid method [14]-[16].

This paper attempts to propose a hybrid process coupling hazard analysis method based on Process Failure Mode and Effects Analysis (PFMEA)and Bayesian Network (BN). By exploring the coupling mechanism of man-machine-environment and analyzing the relationship between the upstream and downstream events, this method can provide a way to identify the event chain and the accident causation logic relationship between the events in the accident evolution process. Finally, corresponding measures can be recommended to improve the process safety.

II. HYBRID PROCESS COUPLING HAZARD ANALYSIS

A. Process Coupling Hazard

Process is the development program ofsystem events. A step in the program can be defined as an event, which contains three aspects of factors, man, machine and environment. For normal execution process, man-machine-environment factors change in their admissible parameter intervals (regarded as normal states) respectively, and thencontinuously outputin accordance with relevant regulations until the process finished safely. But in the actual process, any factor can present various abnormal states except the normal state. All the abnormal states, combined with their coupling influences, usually leave the process in dangerous condition, and eventrigger an accident.

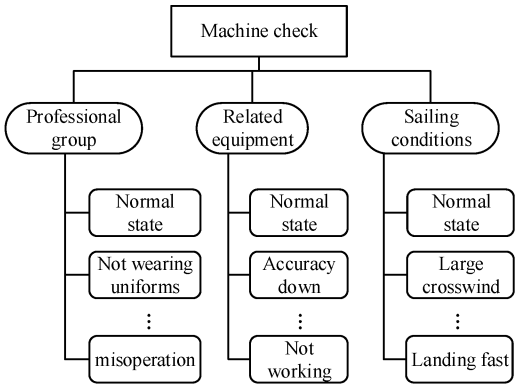

Figure 1. Different states of man- machine-environment.

Coupling refers to the dependency among time, space, function, structure, communication and organization.The abnormal and normal states and their combinations make the

978-1-5386-0918-7/17/$31.00 ©2017 IEEE

events chain execute wrongly, and thus lead to an accident, this phenomenon is namely thecoupling hazard. At present, the PFMEA used in process hazard analysis only considers abnormal states of one factor, and then identifies safety consequences one by one. Although the independency assumption makes it convenient to conduct process hazard analysis, there is a certain gap with actual situations. Coupling of several factors usually result in serious consequences. For example,considering the situation that the armament switchfails to turn off because of a failure or a wrong operation of the pilot, it is possible to lead to an excepted firingif the plane lands too fast, which may cause serious losses including people injuryand machine damage. There are two types of coupling hazard in the case above. One is the coupling relationship between the upstream and downstream events, namely the failing turn-off of armament switch leading the excepted firing.The other is the space coupling relationship, namely the excepted firing can cause people injury and machine damage nearby. Because the coupling hazards can be hardly identifiedbased on the previous methods, it is necessary to improve the PFMEA in order to analyze the process coupling hazard.

B. Process Coupling Hazard Identification Based On Improved PFMEA

1) Process Decomposition And Coupling Hazard Mode Recognition

Process is made up by a series of events according to specific logic order. Every complex process can be divide into several subprocess, and every subprocess contains a series of events. The function or target of the specific process is implemented with events combined in time order.

While dividing process into basic events, every event should be clear about its target and specified output, which is reflected by the corresponding constraints of man-machine-environment. The constraint of man is generally defined as the correct complement of specific action within specific time; the constraint of machine is generally defined as quantitative requirements of function and performance; the constraint of environment is generally defined as the boundaries of one or several kinds of factors impacting current operations. All the constraints determine the man-machine-environment states, and the combinations of different states correspond to different event states.

As shown in the Fig. 2, if all the states of the event are expressed in the form of matrix section columns,then each area represents a state of the event, and the time line through all the matrix section represents an execution trace of the process. Only the system trace through the normal area of each section can ensure the system in the safe state. It is the corresponding state of man-machine-environment that determines the timeline path.

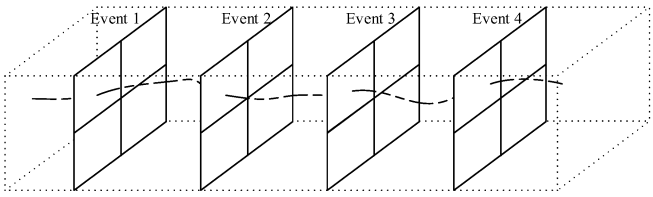

Figure 2. The execution of the process.

As shown in Fig. 3, there are three kinds of states for man and machine and two kinds of states for environment. Man, machine and environmentare represented as H, M, and E respectively, and the event is represented as S. For event 1, man, machine and environment are in the state of H3, M1, and E2 respectively, thus the event is in the state of S106 which representsa normal state; for event 2, man, machine and environment are in the state of H1, M1 and E1 respectively, thus the event is in anothernormal state S201. When the process progresses through the time line path S106 and S201, the process is safe; when the process progresses in any other combination, such as S106 and S213, or S117 and S214, it may cause an accident. Man-machine-environment states determine the event state, and further determine whether the process is executed safely.

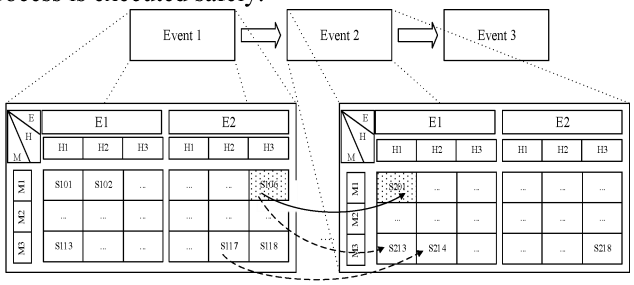

Figure 3. The coupling influence of man-machine-environment.

In order to analyze the coupling hazard of man-machine-environment, it is requested to confirm the possible states corresponding to constrains and identify the state of each event one by one. Sometimes, one or two factors can determine the event state, so the results can be combined. The process coupling hazard analysis method of man-machine-environment is shown in Table. I. The event is in the state of S1 when man and machine are in H1 and M1 while the environment is inwhatever state.

TABLE I. MAN-MACHINE-ENVIRONMENT COUPLING ANALYSIS TABLE

Stage	Event	Man	Machine	Environment	State
Stage1	Event1	H1	M1	E1	S1
		H1	M1	E2	S1
		H1	M2	E1	S2
		…			
	…				

2) Hazard TransmissionTrace Identification In The Process

Despite the single event variation in man-machine-environment, the coupling in complex process also contains the coupling between different events. Since the process is executed for specific target or output, there must be certain associations between the events contained in the