Reliability Engineering and System Safety 95 (2010) 806–815

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

The development and application of dynamic operational risk assessment in oil/gas and chemical process industry

Xiaole Yang, M. Sam Mannan *

Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University System, College Station, TX 77843-3122, USA

ARTICLE INFO

Article history:
Received 2 August 2009
Received in revised form
6 March 2010
Accepted 10 March 2010
Available online 23 March 2010

Keywords:
Dynamic operational risk assessment
Discrete event simulation
Probabilistic simulation
Dynamic simulation
Stochastic model
Process dynamics model

ABSTRACT

A methodology of dynamic operational risk assessment (DORA) is proposed for operational risk analysis in oil/gas and chemical industries. The methodology is introduced comprehensively starting from the conceptual framework design to mathematical modeling and to decision making based on cost–benefit analysis. The probabilistic modeling part of DORA integrates stochastic modeling and process dynamics modeling to evaluate operational risk. The stochastic system-state trajectory is modeled according to the abnormal behavior or failure of each component. For each of the possible system-state trajectories, a process dynamics evaluation is carried out to check whether process variables, e.g., level, flow rate, temperature, pressure, or chemical concentration, remain in their desirable regions. Component testing/inspection intervals and repair times are critical parameters to define the system-state configuration, and play an important role for evaluating the probability of operational failure. This methodology not only provides a framework to evaluate the dynamic operational risk in oil/gas and chemical industries, but also guides the process design and further optimization. To illustrate the probabilistic study, we present a case-study of a level control in an oil/gas separator at an offshore plant.

1. Introduction

The oil/gas and chemical process systems exhibit complicated and dynamic behavior. Various time-dependent effects such as season changes, aging of process equipment, physical processes, stochastic processes, operator response time, etc. are involved in such dynamic processes. With the accumulated experience of quantitative risk assessment and the progressive awareness of dynamic characteristics of reliability and safety, conventional approaches lack the ability to address these issues in quantitative risk assessment for dynamic processes [1,2]. For instance, fault tree/event tree analysis (FTA/ETA) [3], initially applied in nuclear power plants, collects a set of logical expressions to represent static relationship between a component output event and component failure or another component output event in the process system. FTA is a good implementation tool using logic to identify output deviations due to input deviations or internal failures, but withdraws the system dynamic response to time, process variables, and human behavior [4].

The review by Siu regarding the research on reliability and safety assessment of dynamic process systems is an important summary of the work already performed in this field of study [5]. Dynamic probabilistic risk assessment (DPRA) was first proposed by Amendola to study the likelihood of accident sequences in a nuclear reactor [6]. Upgrades in the conventional event tree analysis have resulted in two alternates methods: continuous dynamic event tree (C-DET) [7] and discrete dynamic event tree (D-DET) [8]. Which method used is dependent on how the branching times are selected. Monte Carlo sampling from the distribution of stochastic variables is the basis for event time selection in the C-DET approach. Whereas, branching time selection in the D-DET approach follows a set of rules, such as a discrete approximation of the corresponding C-DET [9]. Computer code, MSAS (Monte Carlo simulation for accident sequences) [10], is designed to implement C-DET, and codes DYLAM [6], DETAM [11], as well as ADS [9], are designed for D-DET. However, deficiencies exist in all these approaches. For example, DYLAM does not consider dependency between component failure and the inspection as well as maintenance of equipment [12]. It is also limited by underestimating the failure probability due to cutoff probability laws [13]. Another widely used approach in dynamic reliability and safety analysis is the application of the Markov theory [14]. The Markov theory is applicable to describe the stochastic behavior of a chemical process if the process has Markov properties. Several approximate applications of the Markovian method for dynamic safety analysis are published

* Corresponding author. Tel.: +1 979 862 3985; fax: +1 979 865 6446.
E-mail address: mannan@tamu.edu (M. Sam Mannan).

0951-8320/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2010.03.002

[12,15–17]. However, these methods overlook the impact of inspection on the system-state transitions and the subsequent process variable evolution. When testing or inspection comes into play, the time between *component abnormal event occurring but undetected* and *component abnormal event detected* is not essentially an exponential distributed random variable. The distribution of system-state sojourn time could be arbitrary. This will introduce a derivative to the conventional Markovian process. Even though the semi-Markovian process is valid for a non-exponential distribution case, the system-state transition does not essentially have Markovian property. The evolution of system-state is not necessarily either a Markovian process or a semi-Markovian process. Additionally, the process variable evolution has to be discretized in the Markovian approximation approaches. Within these approaches, process variables are considered as well as the component performance indicators to define the states in a Markov chain. On the one hand, the discretization must be exclusive enough to simulate the actual continuous and dynamic behavior of the process variable; on the other hand, adequate discretization will introduce computational burden.

The DORA methodology proposed in this study is similar to the ones introduced above in that the probabilistic modeling integrates process dynamic behavior and system stochastic behavior due to component performance permutation. The resulting improvements with this study include the following:

- The DORA probabilistic modeling is entirely independent of the conventional quantitative risk assessment tools such as fault tree or event tree analysis. It considers dynamic effect of the oil/gas and chemical processes as the research in the literature review does but not follows the same logic relationship among different scenarios in the process.
- The component performance permutation is not limited to component failure. Component abnormal event is also considered so that this methodology is applicable to scenarios with either system shutdown due to component failure or system remaining in process in the presence of component abnormal event.
- Component states are not only limited to ‘up’ and ‘down’ to study the system stochastic behavior. Testing/inspection intervals and component repair times are important parameters to define the component states. It provides insights for testing/inspection interval optimization.
- The system-state trajectory is simulated upon Monte Carlo sampling from the distribution of stochastic variable. The restriction to apply Markov chain is removed.
- The demand of large simulation numbers is decomposed appropriately in this study.

Section 2 explains, in detail, the framework of DORA and elements of the methodology. In Section 3, level control in an oil/gas separator is presented as a case-study for the probabilistic modeling part of DORA. Finally, the conclusion and future work are presented in Section 4.

2. Methodology

2.1. DORA framework

The proposed DORA framework is shown in Fig. 1.

Scope identification and system description plays an important role in DORA as a foundation and starting point for further hazard identification and mathematical model development. The scope of a DORA project has to be defined for the study to be better managed, controlled, verified, and communicated to the stakeholders or customers. According to the demand of the stakeholders/customers, the analysis scope varies from a small scale of system, for instance a liquid storage tank, to a middle size of system, say, a cracker unit, to a large scale of system (perhaps the whole refinery plant) and so forth. Regardless of the size of the study scope, the system will be broken down into several subsystems, further components. Each component or a group of components within the same subsystem has its own fashion of failure mode.

Generally, hazard identification by itself can be performed at any stage during the initial design or ongoing operation of a process. However, it is required to be performed before the mathematical modeling for probabilistic safety analysis in the DORA framework. The DORA mathematical modeling is scenario and failure mode specific. *Hazard identification* is the step directing to the discovery of the scenario and component failure mode. Therefore, *hazard identification* and the subsequent *scenario identification*, and *component failure mode identification* steps are necessary in the early stage of the operational risk assessment in a DORA study. The hazard identification methods for DORA are adapted from general hazard identification.

There could be several scenarios that lead to the same consequence in a process. For example, for fire hazard in a fuel storage tank system, multiple scenarios might be identified as the direct causes coincided with an ignition source: overflow of the storage tank, leakage at the tank bottom, leakage at piping, etc. The process dynamics modeling and incident consequence analysis are scenario specific. In each scenario, a unique dynamics model is developed to characterize the physical features of the process. It is important to identify the component failure mode in a DORA study. The reasons are, firstly, any scenario identified in the last step has resulted from certain component failures or abnormal events. In this study, the term ‘failure mode’ is used for both actual equipment failure mode and abnormal event mode. An explicit DORA study is dependent on identifying all the possible hazards, scenarios, and component failure mode combinations. There are usually multiple components in the same system. Different component failure mode combinations could lead to the same scenario. The relationship among *scope identification and system description*, *hazard identification*, *scenario identification*, and *component failure mode identification* is shown in Fig. 2. For any one of the a hazards identified, b scenarios need to be analyzed. In each of the b scenarios, there could be c possible component failure mode combinations driving the scenario. Secondly, this step connects the previous qualitative steps and the following quantitative assessment steps. The reliability data needed for further system performance analysis are failure mode specific. For the same piece of equipment, reliability data for different failure modes are totally different. The component failure mode identification will determine what component reliability data to be used as the input of the quantitative analysis steps.

DORA probabilistic modeling integrates process dynamics modeling and stochastic modeling to analyze the behavior of process variables in the presence of component failure/abnormal event. The evolution of incidental sequences in a process system is a combination of deterministic and stochastic events. The physical behavior of a process is a set of deterministic events, and the system component performance determines the stochastic events. The linkage between the two is that the stochastic system-state trajectory is the driven force of the process physical variable trajectory. In this step, attention is confined to developing a systematic DORA probabilistic modeling for computing the probability of process variables exceeding the operational safety boundaries using considerable computational space storage and time consumption. This step will be explained in further detail in next section.