Safety Science 48 (2010) 580–597

Contents lists available at ScienceDirect

Safety Science

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

An integrated method for safety pre-warning of complex system

Jinqiu Hu [a,*], Laibin Zhang [a], Lin Ma [b], Wei Liang [a]

[a] *Faculty of Mechanical and Electronic Engineering, China University of Petroleum, Beijing 102249, China*
[b] *Cooperative Research Centre for Integrated Engineering Asset Management, Queensland University of Technology, Brisbane, QLD 4001, Australia*

ARTICLE INFO

Article history:
Received 4 September 2009
Received in revised form 29 December 2009
Accepted 8 January 2010

Keywords:
Integrated method for safety pre-warning
Dynamic Bayesian networks
Complex system
Gas turbine compressor system

ABSTRACT

In large-scale and complex industrial systems, unplanned outages and hazardous accidents cause huge economic losses, environmental contamination, and human injuries, due to component degradation, exogenous changes, and operational mistakes. In order to ensure safety and increase operational performance and reliability of complex system, this study proposes an integrated method for safety pre-warning to analyze the current safety state of each component and the whole system indicating hidden hazards and potential consequence, and furthermore predict future degradation trends in the long term.

The work presented here describes the rationale and implementation of the integrated method incorporating HAZOP study, degradation process modeling, dynamic Bayesian network construction, condition monitoring, safety assessment and prognosis steps, taking advantage of the priori knowledge of the interactions and dependencies among components and the environment, the relationships between hazard causes and effects, and the use of historical failure data and online real-time data from condition monitoring.

The application of the integrated safety pre-warning approach described here to the specific example of the gas turbine compressor system demonstrates how each phase of the presented method contributes to completion of the safety pre-warning system development in a systematic way.

1. Introduction

In complex industrial systems (e.g., pipeline system, mechanical system, and auto-control system), operating, regulating, maintenance activities, and external incidents take place and multiple entities (e.g., persons, subsystems, components, and environment) interact in a complex manner. Failures of complex systems have huge negative impacts on business, environment, and society. The growth in awareness of safety pre-warning of complex system has imposed a need on industrial companies to integrate into their safety management strategy not only the present running states, but also the future condition trends under dynamic operational and environmental changes, which is further used for proactive maintenance scheme.

However, no systematic method has yet been established for developing an advanced safety assessment and prognosis for safety pre-warning of the complex systems, such as those, in an industrial gas turbine compressor system. Conventionally, failure modes and effects analysis (FMEA) (or failure modes and effects criticality analysis (FMECA)) and Hazard and Operability (HAZOP) study have provided tools for determining appropriate static (as opposed to dynamic) safety-related maintenance. As system complexity and the number of the interrelationships of subordinate components and of observable variable sets grow, they have proven to be inadequate for dealing with the complex interrelationships and high level reasoning required for analyzing such complicated system features.

Thus, these situations motivate us to develop an integrated approach for dynamic safety assessment and prognosis needed for improving the operational availability and reliability of complex target systems, such as those significantly responsible for system risk. This new method is required for analyzing aspects of the complex target system's performance, incorporating HAZOP, Markov process, and dynamic Bayesian networks (DBN), aiming to foresee how a system (or component) will evolve from its current degraded state until its failure and then until the system's breakdown (performance level), analyzing the impact of degradation on the component itself and on the other entities of the system to predict system failures and remaining useful life (RUL). The work reported here is concerned with use of all historical failure data, on-line monitoring data and also the priori knowledge of system structure and function as an integrated manner, in order to finally determine whether and when the underlying system is in need of maintenance or risk control and improve its operational safety and availability.

This new integrated method is introduced in general terms here, and then applied in order to illustrate its practicality. Specifically, we use the example of the gas turbine compressor

* Corresponding author. Tel.: +86 13401021372.
E-mail address: hjqcup@hotmail.com (J. Hu).

0925-7535/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ssci.2010.01.007

Notation

BN	Bayesian network	FB	forwards-backwards (algorithm)
CPD	conditional probability distribution	FMEA	failure modes and effects analysis
CPT	conditional probability table	FMECA	failure modes and effects criticality analysis
DAG	directed acyclic graph	GTCS	gas turbine compressor system
DBN	dynamic Bayesian network	HAZOP	hazard and operability (study)

system as a field case study presenting how to apply the proposed approach to a real industrial system for safety pre-warning, and the results are utilized to determine proper safety inspection measurements and proactive maintenance plan, when the predicted performance falls within the warning region (or beyond warning threshold). This provides adequate time for safety engineers to inspect the hardware of a system, conduct a repair on the defect, and even make a contingency plan before the catastrophic failure occurs, without any unplanned outages.

The rest of this paper is organised as follows. In Section 2, the limitations of conventional safety-related methods are described. In Section 3, the proposed integrated safety pre-warning method is introduced and then algorithms and major steps with particular examples are also presented. In Section 4, an application of gas turbine compressor system is provided to illustrate the validation of this research in detail. Conclusions are given in Section 5.

2. Limitations of conventional methods

Many of the safety assessment and prognosis methods used in current industrial system have been incorporated into safety pre-warning scheme. Their associated hidden variables, such as corrosion, leakage and wear, and monitoring parameters, such as temperature, pressure and flow, indicate some important process behaviors of the system under consideration.

Basically, as a conventional safety assessment method, FMEA and HAZOP approaches answer to the questions "what if" as dictated by the concerns of interest. It is concerned with the manner of failure, the effects of such failures, and other required information. These approach has been useful both for straightforward reasoning for purposes of safety-related inspection or maintenance and for problem solving in well-understood, simple systems.

However, either FMEA or HAZOP offers little insight concerning complex system features and performance. Also, it cannot be used easily to explain the complex interrelationships inherent among numerous subordinate components. It is also poor in use with advanced condition monitoring techniques, which can provide more detailed information concerning system performance, based upon deep understanding of system features. Consequently, insufficient understanding of system characteristics, for example, due to its complexity, usually renders safety assessment method difficult to realize efficiently (Kang and Golay, 2000).

On the other hand, an effective and efficient system safety prognosis is also essential for appropriate inspection and maintenance strategy making, and has become a major concern in the field of industrial safety pre-warning. Nevertheless, prognosis has been a difficult task and has attracted much attention of researchers in the field (Jardine et al., 2006; Heng et al., 2008, 2009; Kothamasu et al., 2006; Sutherland et al., 2003; Liu et al., 2007). The approaches to prognosis fall into three main categories: statistical approaches, artificial intelligent approaches, and model-based approaches (Jardine et al., 2006). Iung et al. (2008) and Muller et al. (2004, 2008) further include maintenance policies in the consideration of the machine prognostic process integrating of statistical approach, data-driven approach and model-based approach, in order to provide decision support for maintenance actions.

All above-mentioned methods have advanced the development of system prognostics. In summary, however, several aspects need to be further investigated when they are applied to complex industrial systems:

(1) In most safety pre-warning scheme, the safety assessment and prognosis are usually two independent processes. In this situation, system prognosis merely takes into account the historical failure data and condition monitoring data to predict future performance of systems without considering the results of safety assessment. The main disadvantage of such prognostic approaches is that they ignore the impact of external incidents, dynamic changes of exogenous environment, operating and regulating adjustment of the system, which can be analysed by safety assessment. Such ignorance makes prognosis inaccurate, especially under variable operating conditions and dynamic environments. On the other hand, safety assessment without prognosis is prone to be static, such as HAZOP or FMEA, failing to foresee the future hazards which need to be removed by proactive maintenance.
(2) Considering the conventional safety assessment approaches (e.g. HAZOP), not all of the compatible hazard propagation pathways derived from hazard analysis would happen in the real world, since a considerable part of them have a very low occurrence probability. Especially during the safety assessment of large-scale complex system, such approaches would result in large numbers of hazard outcomes or even "combinational explosion", which may lead the safety engineer taking inappropriate safety measurements, missing the best maintenance time, or even a catastrophic result (Zhang et al., 2008).
(3) When predicting the system reliability in the long term, the existing literature (Huang et al., 2007; Heng et al., 2009; Lee et al., 1999) largely focuses on the degradation mechanism and remaining useful life from the component or single equipment deterioration point of view; for example, ball bearing, pump, and steam generator. Very few models have taken into account not only the interdependencies among the components and subsystems, but also the impact of degradations and the influence of exogenous variables on the degradation processes. The main reason for this is that, to decrease the model's complexity and avoid combinational explosion, two hypotheses according to which there is no simultaneous occurrence of failure and the statistical independence between events are assumed (Weber and Jouffe, 2006). However, such hypotheses are no longer valid when components have common causes or when components have several failure modes.

3. An integrated method

3.1. Overview

The method presented here utilizes the combination of HAZOP analysis, degradation process modeling, dynamic Bayesian networks development, condition monitoring scheme, safety