Journal of Loss Prevention in the Process Industries 29 (2014) 144–154

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

An extension of Multiple Greek Letter method for common cause failures modelling

Živa Bricman Rejc*, Marko Čepin

University of Ljubljana, Faculty of Electrical Engineering, Tržaška 25, 1000 Ljubljana, Slovenia

ARTICLE INFO

Article history:
Received 20 August 2012
Received in revised form
10 December 2013
Accepted 17 February 2014

Keywords:
Reliability
Common cause failures
Multiple Greek Letter method
Safety injection system

ABSTRACT

Common cause failure describes a condition where several components share the same source of failure that causes them to fail or become unavailable simultaneously. The objective of this paper is to present an improved approach to common cause failure modelling within reliability analyses. The currently used methods allow one component to share common characteristics with only one group of components, which may be affected by the same source of failure. Therefore, an improved method was developed, where components can be assigned to several groups of components that are susceptible to faulty operation with respect to their similar characteristics. A mathematical derivation of the method is presented and the theory is applied to smaller theoretical samples and to a simplified real example. The results show that the new method enables a more detailed reliability analysis. The results prove that consideration of common cause failures using the improved method may decrease the system reliability compared to traditional common cause failure consideration. The system reliability decreases more, if the redundant components have more similarities and are therefore assigned to several common cause failure groups.

1. Introduction

With the increasing desire to reduce costs and outages in complex industrial processes, risk and failure analysis has been receiving greater attention in order to forecast accidents, analyse the consequences of likely accidents and develop strategies for emergency situations in order to minimize the damage caused by accidents in different industrial processes (Khan & Abbasi, 1998). Additionally, in the nuclear industry high safety demands require extensive risk and failure analysis to ensure the safety of nuclear facilities. The probabilistic risk assessment (PRA) has become the most widely accepted procedure for risk and failure analysis in the nuclear industry (Cepin, 2011), with event tree and fault tree analysis being the two main methods applied. PRA also provides information about the event sequences that contribute significantly to risk and is a standard tool for the safety assessment of nuclear power plants (NPPs), strategic facilities and technological processes. PRA is therefore used for upgrading existing systems, improving systems operation and reliability. This can be additionally improved with preliminary risk assessment during the early design phases. The preliminary risk assessment provides potential risk areas in the system during the early design stages, when risk mitigation is the least expensive costs (Lough, Stone, & Tumer, 2008, 2009). Preliminary risk assessment can be combined with PRA techniques such as the fault tree analysis, which can prevent accidents from occurring or can encourage the engineers to redesign the observed system to reach the higher level of system reliability (Lough et al., 2009).

PRA is also used in various other industries, such as gas and oil, chemical, aircraft and aerospace industries (Shahrair, Sadiq, & Tesfamariam, 2012). Various other procedures also exist and are widely used. For example, in the gas and oil industry, fractography, chemical analyses, tensile, hardness and corrosion tests (Kim, An, Lee, & Lee, 2009) are used. Within the oil and gas industry historical data analysis, conformance test and scoring system of hazard assessment and various quantitative techniques are also applied for risk assessments of fuel pipelines (Dziubiński, Frątczak, & Markowski, 2006). Another example of the procedures in use are optimum risk analysis (Khan & Abbasi, 2001), failure mode effect analysis and what-if analysis, which are widely applied in the chemical industry.

In this paper, the focus is on PRA, specifically on fault tree analysis for NPPs, where component and sub-component failures are considered.

Fault tree analysis is used for the analysis of a single system within the observed NPP. The redundancy and diversity of

* Corresponding author. Tel.: +386 1 4768 954; fax: +386 1 4768 710.
E-mail addresses: ziva.bricman@fe.uni-lj.si (Ž.B. Rejc), marko.cepin@fe.uni-lj.si (M. Čepin).

http://dx.doi.org/10.1016/j.jlp.2014.02.009
0950-4230/

components contribute to greater system reliability, not only in the nuclear industry but also in other fields. Component failures are usually considered as mutually independent in reliability analyses. However, this may not be completely true, as some common mechanisms or characteristics may exist and may potentially affect more than just one component.

This has led to the use of common cause failures (CCFs), which are based on distinct criteria and refer to a specific group of failures that may potentially occur due to a shared cause of failure, e.g., the fault of the same manufacturer, or due to a coupling mechanism that creates a condition causing several components to fail, e.g., a fault caused by a similar maintenance process. Such failures can greatly endanger the benefits of redundancy in highly reliable systems, if the diversity of components is not properly adjusted. CCFs are therefore an important part of a fault tree analysis (Cepin, 2010).

As CCFs can greatly impact the reliability of the observed systems, their consideration is also increasing in the early design phases (Lough et al., 2009). If CCFs are considered, the systems, sub-systems, or components, whose operation is endangered by the CCFs, can be located in the early-design phase, which increases the reliability of the observed system and reduces the costs of risk mitigating. Several methods for treating CCFs are described in the literature. The most commonly used methods for CCF definition are the Beta factor method, the Alpha factor method and the Multiple Greek Letter method (Mosleh et al., 1988, 1989; Mosleh, Rasmuson, & Marshall, 1998). Additionally, the uncertainty of the CCF failure rates was investigated (Vaurio, 2002) along with external CCF events in redundant systems (Vaurio, 1995) and the dependencies regarding different system testing schemes and intervals (Vaurio, 2003).

The Beta factor model is the simplest and the first derived model for CCF estimation, which is described only with one parameter. Recently the method was upgraded to take into account different shared failure causes (Kancev & Cepin, 2012). On the other hand, the Alpha factor and the Multiple Greek Letter model are multi-parameter models, which enable more detailed CCF modelling. The existing Multiple Greek Letter (MGL) method (Mosleh et al., 1988, 1989) allows one component to be considered only in one group of components that may fail due to a shared cause, i.e., a common cause failure group. Consequently, the possibility that one component may share a different common characteristic with more than just one group of similar components is absent.

Therefore, the objective of this paper is to develop an advanced MGL method for CCF estimation that allows a more detailed system reliability analysis and assessment. The advanced method was developed for cases where one component shares several common characteristics with more than just one group of similar components, which was previously impossible. This enables the use of more detailed system failure models (e.g., fault trees), which enable the consideration of more root causes and coupling mechanisms between the components. The method is very useful for highly redundant systems, where CCFs play a significant role. The method enables more detailed CCF modelling compared to previous methods. The developed method is applied to a safety injection system of an NPP with an Advanced Pressurized Water Reactor (US-APWR) by using the fault tree analysis.

The paper is organized as follows: Section 2 provides the background and is divided into subsections 2.1–2.3. Subsection 2.1 presents the existing method, i.e., fault tree analysis, which is used for assessing and improving the reliability of the observed systems. Subsection 2.2 presents the common cause failure analysis, which is an important part of the fault tree analysis, and subsection 2.3 presents a method for common cause failure estimation, i.e., Multiple Greek Letter method. Section 3 presents the new method for common cause failure estimation, i.e., an advanced Multiple Greek Letter method. Section 4 presents the results of the case studies, where the presented method has been tested, and the concussions are given in Section 5.

2. Background

2.1. Fault tree analysis

For the purpose of this paper the reliability analyses were performed using fault tree analysis. Fault tree analysis (FTA) is one of the most significant methods within probabilistic risk assessment (PRA) (Stamatelatos et al., 2002; Vesely, Goldberg, Roberts, & Haasl, 1981). It is a standard method for assessing and improving the reliability of systems, where system failures are analysed according to component failures. In general, a component's working state can be described with two elementary states: the operational state and the fault state. The evaluation of the failure probability for each component is performed with a probability model that is selected according to the component's function and operation. Therefore, the failure rate can be defined as a relation between the number of failures and the operating time. The failure rate can also be defined as an inverse value of the mean time to failure. The failure probability per demand can be defined as a relation between the total number of failures and the number of all demands (IAEA, 1992).

FTA is an analytical approach where an undesired top event is primarily defined, i.e., a system failure, and the system is then analysed in the context of its environment and operation to find all possible ways in which the undesired top event can occur (Cepin & Mavko, 2002). A fault tree is a graphical diagram of the combinations of basic events that can result in an undesired top event connected through logical gates. The more gates and events the tree consists of, the more complex its evaluation is. The undesired top event is defined at the top of the fault tree and describes the inability of the system to perform its proper function. The basic event is evaluated as a fault of one component in the system, e.g., power generator, valve, power line, bus, power transformer, storage tank, in a particular failure mode (Vesely et al., 1981). All the operations between the basic events are based on Boolean algebra.

Fault trees can be evaluated either qualitatively or quantitatively. A qualitative evaluation contains a minimal cut set (MCS) evaluation, a qualitative importance evaluation, a common cause failure evaluation, while a quantitative evaluation contains probability estimation, a quantitative importance evaluation and sensitivity analyses (Vesely et al., 1981). The probability of a top event occurrence Q_{TOP} can be evaluated quantitatively using minimal cut sets, which are combinations of the smallest number of components that may cause a system failure. The probability of each MCS is calculated as a product of the probabilities of all the contained basic events. The top event probability can be calculated as follows (Cepin, 2011; Vesely et al., 1981):

$$\begin{aligned}Q_{TOP} = & \sum_{l=1}^{L} Q_{MCS_l(BE_1,\ldots,BE_X)} - \sum_{l<m} Q_{MCS_l(BE_1,\ldots,BE_X)\cap MCS_m(BE_1,\ldots,BE_X)} \\ & + \sum_{l<m<n} Q_{MCS_l(BE_1,\ldots,BE_X)\cap MCS_m(BE_1,\ldots,BE_X)\cap MCS_n(BE_1,\ldots,BE_X)} \\ & - \ldots + (-1)^{L-1} Q_{\cap_{l=1}^{L} MCS_l(BE_1,\ldots,BE_X)}\end{aligned} \tag{1}$$

where MCS_l is the minimal cut set l, L is the number of all MCS, $Q_{MCS_l(BE_1,\ldots,BE_X)}$ is the probability of the occurrence of the l-th MCS containing X basic events.

If the mutual dependences between the basic events within the minimal cut set are not considered, Q_{MCS_l} can be calculated as follows (Cepin, 2011; Vesely et al., 1981):