Journal of Loss Prevention in the Process Industries 23 (2010) 574–584

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

A novel method to apply Importance and Sensitivity Analysis to multiple Fault-trees

Sergio Contini, Luciano Fabbri*, Vaidas Matuzas

European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen, Ispra Establishment, via Enrico Fermi, 21020 Ispra, VA, Italy

ARTICLE INFO

Article history:
Received 21 December 2009
Accepted 7 May 2010

Keywords:
Sensitivity analysis importance measures
Fault-trees
Design improvement
Process safety

ABSTRACT

The unavailability/frequency analysis of critical failure states of complex industrial systems is normally conducted by using the Fault-tree methodology. The number of Fault-trees describing the system is given by the number of system's failure states (i.e. Top-events). For each Top-event characterised by unacceptable occurrence probability, some design improvements should be made. Importance and Sensitivity Analysis (ISA) is normally applied to identify the weakest parts of the system. By selecting these parts for design improvement, the overall improvement of the system is made more effective. In current practice, ISA is normally applied sequentially to all Fault-trees. The sequence order is subjectively selected by the analyst, based on several criteria as for instance the severity of the associated Top-event. This approach has the clear limitation of not ensuring the identification of the most cost-effective design solution to improve safety. The present paper describes an alternative approach which consists of concurrently analysing all relevant system's Fault-trees with the objective of overcoming the above limitations and to identify the most cost-effective solution. In addition, the proposed method extends the ISA application to "over-reliable" system functions, if any, on which the reliability/maintainability characteristics of the involved components can be relaxed, with a resulting cost saving. The overall outcome of the analysis is a uniformly protected system, which satisfies the predefined design goals. A point to note is that the overall cost of the analysis of the proposed approach is significantly lower if compared with the sequential case.

1. Introduction

Complex systems are normally characterised by a number of dangerous failure states, which are directly associated with possible accident scenarios. The study of these states, by including the determination of their occurrence probability/frequency can be performed by means of various system analysis techniques. The most popular is the Fault-tree Analysis (FTA) (Kumamoto & Henley, 1996; Vesely, 1970), which allows describing in a systematic way the cause-effect relationships amongst failure events from single components to system. In particular, FTA allows studying the role played by the different failure modes associated with any system's components, which might have a different impact on the occurrence probability of the system failure state, hereafter indicated as the Top-event. In addition, the quantification of Fault-trees allows the analyst to obtain the information of interest for design improvement. When the estimated failure probability of the Top-event is deemed not acceptable, a design review has to be made with the specific goal of reducing it to an acceptable predefined value. This is normally done by using Importance and Sensitivity Analysis (ISA) (Rausand & Hoyland, 2004) which, combined with the results of FTA, represents a very powerful tool to improve the design of critical systems. ISA is a methodology addressed to envisage the output behaviour of a model as a consequence of the variation of the input variables, with the purpose of identifying input variables that are more significant in term to their contribution to the model output. Referring to FTA, the model's output is the probability of occurrence of the Top-events. The input variables are all possible failure modes of the system's components, which, in FTA, are indicated as primary or basic events (BEs). For the purpose of this paper we will refer to component failure modes or BE without distinction. The identification of the weakest components in the system in term of their contribution to risk is the final objective of such an analysis, as it allows identifying those elements that require further design improvement. In general, the definition of importance measures (IMs) (Van der Borst & Schoonakker, 2001) for each BE allows the analyst to assess the relative risk-significance of the associated component in terms of its contribution to the

* Corresponding author. Tel.: +39 0332 785801; fax: +39 0332 789007.
E-mail address: luciano.fabbri@jrc.ec.europa.eu (L. Fabbri).

0950-4230/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jlp.2010.05.004

occurrence probability of the Top-event. In particular the failure modes (i.e. BEs) with highest IMs are those most sensitive, giving the maximum increase (or decrease) of the Top-event probability for a given increase (or decrease) of the associated BE probability. These BEs are clearly associated with system functions that are more critical. Once the most "sensitive" failure modes are identified, some system improvements can be made by modifying the design of the associated components. More specifically, a critical component can be substituted either with another component of better quality and/or better maintainability and/or better testing strategy, or with a subsystem where the component has a redundant part (e.g. parallel, stand-by, K out of N).

Classically the risk is expressed by a set of triplets (Kaplan & Garrick, 1981):

$$R = \langle Si\ Pi\ Ci \rangle \quad i = 1, 2, \ldots, N$$

where S*i* is a possible accident scenario for the system (Top-event), P*i* is its occurrence probability, C*i* is the associated consequence, and *N* is the number of Top-events. Normally, the risk is represented on a log-log diagram, where for each accident scenario an associated risk point is represented (i.e. its occurrence probability vs. consequence). The diagram is subdivided into three areas corresponding to acceptable risk, unacceptable risk and an area in between where risk reduction is desirable (e.g. the ALARP or ALARA regions). In general, if the system induced risk is not acceptable, the task of the system designer is to "move" the risk points out of the acceptable risk area through the improvement of the system safety and/or the mitigation measures. The present paper focuses on the control of risk through a reduction of the Top-events occurrence probability whilst the activity on consequence reduction, which involves the introduction of mitigation measures, is outside the scope of the present work. In order to reduce the Top-event occurrence probability it is necessary to introduce structural modifications in the production/control system and/or to improve the protection system functions. Normally, the second option is preferred for safety-related purposes, as the first is strictly linked to the production process and therefore any structural modification would impose a modification within the production line. In other words design modifications of the safety-related functions are generally much less expensive than modifications of the production/control functions. However any modification of the safety system should not compromise the plant availability requirements.

When risk reduction is deemed necessary, a specific probability goal has to be defined for each Top-event. The intent is to reduce the occurrence probability of each Top-event in such a way that the corresponding risk point on the log-log diagram is moved outside the unacceptable risk region. In general, the reduction of the Top-event occurrence probability can be obtained by intervening on the primary causes that can lead to the Top-event (i.e. BEs). The most effective approach is to operate on those BEs which contribute most to the probability of occurrence of the Top-event (i.e. those having highest IMs). However, it is important to note that for complex systems some BEs can be present in different Fault-trees and their modification can have different impacts on the Top-events probability.

Current approaches to Importance and Sensitivity Analysis are based on the Sequential analysis of the different Fault-trees i.e. given *N* Fault-trees they are independently analysed one after another. This approach is indicated in this paper as *Sequential Importance and Sensitivity Analysis* (SISA). The main complication of this approach arises when different Top-events contain common BEs. In such a case, it results that any proposal for the modification of a certain system's component, which results from the analysis of a certain Top-event, has to be reassessed when performing the analysis of other Fault-trees containing the same component. For this reason the analyst cannot fully assess the actual impact on the overall system safety from a modification resulting from the sensitivity study application conducted on a single Fault-tree at a time. In addition, when some major system's modification is required (e.g. the use of redundancy), this modification has to be implemented also on other Fault-trees. In general, the overall cost of the analysis might be significant because of repetitions, reiterations and overlapping. These limitations are amplified when considering problems with conflicting requirements, as for instance safety and production loss. Indeed, the reduction of the failure probability of Top-events is generally achieved through the improvement of the safety/control functions which, due to the extensive use of fail-safe components, could lead to a decrease of the system availability. For these reasons Fault-trees are independently analysed.

A better trade-off between these two conflicting situations would be the concurrent analysis on all Fault-trees of the system, in which both unavailability and safety functions are taken into account. Indeed, a possible way forward to overcome the limitations of the Sequential approach is to perform Sensitivity Analysis on all Fault-trees concurrently. This approach, which has been called *Concurrent Importance and Sensitivity Analysis* (CISA), is presented in this paper. The Concurrent Analysis was already implemented in the past (Contini, Sheer, & Wilikens, 2000). Although it was applied with success to a real system, that method was characterised by some of limitations. The approach here proposed overcomes the drawbacks of the previous implementation and it introduces a selective method to reduce the occurrence probability of each Top-event. In particular, different probabilistic goals are selected for different Top-events, depending on their specific contribution to risk. Another innovative aspect of the proposed approach is that the method is extended also to identify "over-reliable" system functions, if any, on which the reliability/maintainability characteristics of the involved components can be relaxed with consequent cost saving. The overall result of the analysis is a uniformly protected system satisfying the predefined probabilistic goals. Moreover the cost of the analysis is much lower than the cost from using the SISA approach. In order to implement the proposed approach a dedicated software tool was developed (JRC-CISA) which makes use of the JRC-ASTRA software for Fault-tree analysis (Contini, Fabbri, & Matuzas, 2009). The present paper describes the methodology, and provides a simple example of application.

2. Importance and Sensitivity Analysis (ISA)

2.1. Importance measures

The ISA methodology is based on the use of importance measures of BEs (also indicated as importance indexes). These are strictly associated with the risk-significance of related components. In particular, they are normally used to rank the system's components with respect to their contribution to the reliability and availability of the overall system. Importance measures of basic events have assumed a very important role in system reliability which is testified by the very rich literature; see e.g. Borgonovo and Apostolakis (2001), IAEA (1991), Rausand and Hoyland (2004), Van der Borst and Schoonakker (2001), and Zhang and Mei (1985)). The probabilistic importance measures that are currently in use for risk assessment purposes are summarised in Table 1.

2.2. Current approaches to ISA

As previously mentioned, the Importance and Sensitivity Analysis (ISA) is a procedure applied during the system's design phase to identify the weakest parts of the system, i.e. those components