CHEMICAL ENGINEERING TRANSACTIONS Volume 19, 2010
Editor Simberto Senni Buratti
 ISBN 978-88-95608-11-2 ISSN 1974-9791
DOI: 10.3303/CET1019037

Sensitivity Analysis Applied to Multiple Fault-trees

Sergio Contini, Luciano Fabbri, Vaidas Matuzas
European Commission, Joint Research Centre
Via E. Fermi 2749, 21020 Ispra (VA), Italy

Fault-tree analysis is applied to technological systems to determine the probability of system's failure modes with unacceptable consequences, called "critical states". As many Fault-trees as the number of system's critical states are constructed and analysed; when their probabilities are deemed not acceptable, the Importance and Sensitivity Analysis (ISA) is applied to improve the system safety through design modifications.
This paper describes a novel approach based on the ISA method aiming at supporting the designer in achieving the objective of obtaining a uniformly protected system satisfying the predefined design goals in a cost-effective way. It is based on the concurrent analysis of all relevant system's Fault-trees. This approach aims at overcoming the limitations of the current approach, which is based on the sequential analysis of Fault-trees. In addition, it extends the ISA application also to "over-reliable" or "over-protected" system functions on which the reliability/maintainability characteristics of the involved components can be relaxed with consequent cost saving.

1. Introduction

Fault-tree Analysis (FTA) is one of the most popular techniques for studying the system failure states (Top-events) with unacceptable consequences. Fault-trees allow describing systematically the cause-effect relationships amongst failure events from system to components, at different levels of detail. FTA allows studying the role played by the different failure modes associated with the system's components (hereafter referred to as Basic-events).
The quantification of the Fault-tree allows determining the reliability parameters of interest for the system design improvement. In particular, this analysis provides the so-called Minimal Cut Sets (minimum sets of basic events that verify the Top-event), their occurrence probability and the system failure probability P_{top}. Depending on the severity of the consequences defined by the Top-event a probabilistic goal P_G is defined. If P_{top} is considered as not-acceptable, i.e. $P_{top} > P_G$, a design review process has to be performed with the specific objective of reducing P_{top} so that $P_{top} < P_G$.
Hence, given the situation in which $P_{top} > P_G$, it is necessary to answer to the following questions:
- How can the system be improved?
- On which basis a better design solution can be identified?
- How is it possible to make the system uniformly protected against accidents?
- Are there functions over protected or over reliable?

Please cite this article as: Contini S., Fabbri L. and Matuzas V., (2010), Sensitivity analysis applied to multiple fault-trees, Chemical Engineering Transactions, 19, 225-230 DOI: 10.3303/CET1019037

- What about if more design alternatives could be adopted?

A possible way forward to address these questions is to apply the Importance and Sensitivity Analysis.

2. Importance and Sensitivity Analysis

The Importance and Sensitivity Analysis is a consolidated procedure applied during the system's design phase to identify the weakest parts of the system, i.e. those components whose failure modes give the greatest contribution to the likelihood of occurrence of the Top-event. Once these components are identified, suitable design modifications can be considered aiming at reducing the system failure probability. Essentially, the ISA procedure applied to a given Fault-tree for which $P_{top} > P_G$ is based on three steps:

1. Identification of the most critical components by using importance indexes (see e.g. Rausand and Hoyland, 2004 for a survey of importance indexes);
2. Application of possible design alternatives to the weakest system points (i.e. components with the highest importance indexes) by taking into account the existing constrains (e.g. cost, space, weight);
3. Following the design modification the Fault-tree is updated and re-analysed to assess the effect of the improvement made.

These three steps are iteratively applied until $P_{top} < P_G$.

In practice the ISA process is conducted on all Fault-trees constructed for all critical system's states.

2.1 Current practice: Sequential Importance and Sensitivity Analysis

When two or more fault trees are of concern, practitioners analyse them sequentially, generally starting from those having more severe consequences. If different Fault-trees are associated with the same level of consequence, the choice of the Fault-tree from which to start the analysis is simply based on subjective considerations. In this paper this approach is referred to as "Sequential ISA" (SISA). Figure 1 gives a schematic diagram of SISA for a system with N=3 Fault-trees.

Each Fault-tree, FT_j (j=1,N) has an associated goal P_{Gj}. Consider the generic j-th fault tree. The first quantification gives $Q^{(0)}_j$ and the ranking of importance indexes. $Q^{(0)}_j$ is the Top-event probability of the j-th fault tree at step zero of the analysis. The comparison between $Q^{(0)}_j$ and P_{Gj} gives an indication about the effort needed to improve the system. Obviously, if $Q^{(0)}_j \leq P_{Gj}$ no further improvement is needed. By contrast, when $Q^{(0)}_j > P_{Gj}$, the goal P_{Gj} can be reached after one or more improvement steps which are associated with system modifications.

At the generic i-th step of the SISA process, the probabilistic quantification provides the Top-event probability $Q^{(i)}_j < Q^{(i-1)}_j$ and the components importance measures at step i. Since these measures are determined on a single Fault-tree they are hereafter referred to as "Local Importance Indexes" (LII). The components with the higher LII values are selected and considered for design improvement. Depending on the functions carried on by these components, possible improvements may consist of:

- Modifying their reliability/maintainability parameters (failure rate, repair time, time between tests, etc.);
- Introducing redundant elements (e.g. parallel, stand-by, k/n);
- Modifying the testing policy.

If a potentially useful design modification is identified then the Fault-tree under consideration is analysed to verify whether to retain it or not. In the positive case, i.e. the modification is retained, if the next Fault-tree to be examined contains the modified components then it is necessary to properly modify it before proceeding with its analysis. This is represented in Figure 1 with the connection lines between "Design modification" and "Fault-tree" blocks.

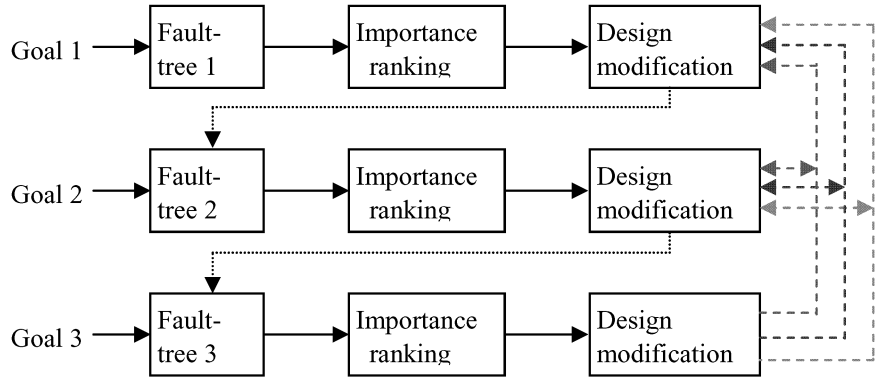

Figure 1. Schematic diagram of the Sequential Importance and Sensitivity Analysis

The SISA approach has a number of disadvantages when the N Fault-trees are not independent (i.e. contain common Basic-events). Some of them are:

- Any proposal for a modification of the system resulting from the analysis of the j-th Fault-tree would require (but in practice is not carried out) the analysis' update of all the Fault-trees previously analyzed (i.e. from 1 to j-1), which contain the modified component; this process is represented in Figure 1 by the arrows with dotted lines.
- The resulting design modification could not be the best cost-effective one, since it depends on the order in which Fault-trees are examined; for instance the best cost-effective design solution obtained considering the sequence FT1-FT2-FT3 can be different from the solution obtained considering e.g. FT2-FT3-FT1. In other words it is not possible to state that the identified design modification, which achieves the goal, is the best cost-effective one, since it depends on the order in which Fault-trees are analysed. A numerical example is given in (Contini et al., 2009).
- The coherency of the Fault-trees, which implies that a component modification leading to the failure probability reduction of the j-th Top-event may further decrease the failure probability of the Top-events previously analysed; consequently, one or more system functions may become more reliable than needed.

The above SISA limitations are even amplified when considering problems with conflicting requirements, as for instance safety and production loss, or fail-safe trip vs. spurious trip of safety systems, i.e. those problems in which the improvement of a requirement implies the worsening of another requirement.

2.2 Proposed approach: Concurrent Importance and Sensitivity Analysis

A possible way forward to overcome the limitations of the SISA approach is to perform the Sensitivity Analysis on all Fault-trees concurrently. This approach is called

Concurrent Importance and Sensitivity Analysis (CISA) and is performed in two phases:
- Goal Achievement Phase (GAP);
- Cost Reduction Phase (CRP).
A schematic diagram of the CISA method is presented in Figure 2.

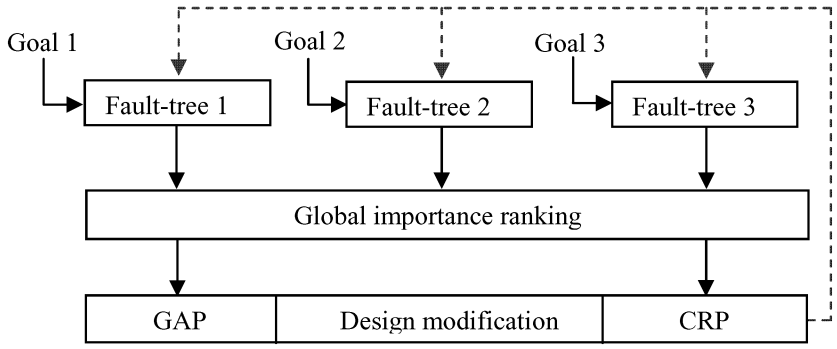

Figure 2. Schematic diagram of the Concurrent Importance and Sensitivity Analysis

The CISA approach applied for multiple Fault-trees is based on the determination of Global Importance indexes (GII) of basic events, i.e. importance referred to the system as a whole and not to a particular Fault-tree. Within the CISA method proposed in the past (Contini et al., 2000) a subjective definition of importance for each Top-event was required. This drawback is eliminated with the definition of the GII indexes determined from the LII indexes of basic events in all fault trees.
In case of Birnbaum or Criticality indexes it can be proved that, by assuming the rare event approximation:

$$Q_T = \sum_{i=1}^{N} Q_i \tag{1}$$

the following relationships holds true (Contini et al., 2009):

$$I_k^B = \sum_{j=1}^{N} I_{kj}^B \tag{2}$$

$$I_k^C = \frac{1}{Q_T} \sum_{j=1}^{N} I_{kj}^C Q_j \tag{3}$$

where:
N - Total number of Fault-trees;
I_k^B - Global Birnbaum importance index of the k-th event;
I_{kj}^B - Local Birnbaum importance index for the k-th event in the j-th Fault-tree;

I_k^C - Global Criticality importance index of the k-th event;

I_{kj}^C - Local Criticality importance index for the k-th event in the j-th Fault-tree;

Q_j - Top-event probability of the j-th Fault-tree.

In practice, for safety-related studies the approximation of equation (1) is acceptable. At each step of the analysis equation (3) allows to determine the Global criticality index which is used to select the events associated with the weakest points of the system.
The GII ranking coincides with the LII ranking if all Fault-trees are independent, i.e. if they do not share any basic event. If fault-trees are not independent then, for a generic event x_k, $GII_k > \max(LII_k)$.
As represented in Figure 2 the CISA method is made up of two phases.
1) Goal Achievement Phase. This phase aims at reducing the occurrence probability of all systems' Top-events to acceptable values. During the GAP phase the component with the maximum GII value is selected and considered for design improvement. If a useful design modification is identified, then all Fault-trees containing the selected component are accordingly modified and re-analysed.
It is clear that the CISA approach is particularly suitable also to face problems of conflicting requirements (e.g. unavailability vs. safety; no-intervention on demand vs. spurious intervention for protective systems) and to find suitable trade-offs. Once all Top-events have reached the predefined goal, the second phase is applied.
2) Cost Reduction Phase. This second phase aims at verifying whether the design configuration, resulting from the previous GAP phase, may contain safety/control functions that present a failure probability which is unjustifiably low compared to the requirements. Contrary to the GAP phase, the selection of the components to be examined for cost reduction is based on the minimum values of the GII. In this way the CISA approach is not solely used to address the most critical components in terms of their contribution to risk, but it also focuses on those less critical components carrying out functions that may be "over-reliable" or "over-protected". The identification of these components may provide a contribution to costs reduction during the design phase, satisfying, at the same time, the probabilistic goals. Indeed on these components it is possible to relax their reliability characteristics (e.g. longer repair time or time between tests, higher failure rate using components of lower quality, etc.), but still satisfying the relationship $P_{top} < P_G$.
It should be outlined that the Cost Reduction Phase is applicable only if the Fault-tree analyser is able to calculate the importance indexes based on all MCS. As the number of MCS is often very high, the probabilistic analysis is limited to the most important ones. By ignoring indeed the less significant MCS, it is evident that the contribution of components with low importance indexes is automatically neglected. This is probably the main reason why in practice the CRP phase was never proposed in the past.
The new analysis approach based on Binary Decision Diagrams allows performing the exact analysis considering all MCS. Hence the importance indexes canbe determined for all components.
The final objective of CISA is to support the analyst in obtaining a uniformly protected system by removing not only the "weaker functions", causes of system failure, but also the uselessly "over-protected functions", causes of major costs. Hence, the additional

cost for reducing the failure probability of certain functions could be partially compensated by relaxing the reliability / maintainability characteristics of functions that are uselessly over protected.
The detail description of the CISA probabilistic model, together with a numerical example, can be found in (Contini et al., 2009).

3. The CISA software

The CISA methodology has been implemented in a software tool which allows the user to immediately verify, on line, the effects of the different actions (modification of reliability/maintainability parameters of a basic events; or the use of redundant configurations such as parallel, stand-by, k/n; or the modification of the system failure logic) applied to the selected critical components. The CISA software makes use of ASTRA 3.0 as the Fault-tree analysis engine. ASTRA is based on the Binary Decision Diagrams approach which offers several advantages, among which – what is important for the CISA model - the exact probabilistic analysis performed on all MCS stored in the compact form of Directed Acyclic Graph (Contini et al., 2006).

4. Conclusions and further developments

This paper presented the use of the Importance and Sensitivity Analysis for the design review of systems with multiple critical states, i.e. multiple fault trees After presenting the drawbacks of the sequential approach currently applied, referred to as in this paper as SISA, the new CISA approach has been presented, characterised by the concurrent analysis of all fault trees. The analysis procedure is composed of two phases: Goal achievements and Cost reduction, the former is based on the basic events with the highest importance indexes, whether the latter is based on the basic events with the lowest importance indexes. In this way the reliability/maintainability characteristics of components of “over-reliable” or “over-protected” system functions can be relaxed with consequent cost saving. The CISA approach overcomes the drawbacks of the currently applied SISA approach. The methodology described in this paper has been implemented in the CISA software. The current version has to be completed with the implementation of the top-event uncertainty module. Indeed, it is not sufficient to prove that, for each fault tree the mean Top event probability $P_{top} < P_G$, but that it is necessary to determine the associated probability, i.e. $Pr\{P_{top} < P_G\}$.

References

Contini S., Sheer S. and Wilikens M., 2000, Sensitivity Analysis for System Design Improvement, Proceedings of DSN 2000, New York.

Contini S., Cojazzi G.G.M. and De Cola G., 2006, On the exact analysis of non coherent fault trees: the ASTRA package, PSAM 8, New Orleans, USA.

Contini S., Fabbri L. and Matuzas V., 2009, Concurrent Importance and Sensitivity Analysis Applied to Multiple Fault Trees, JRC IPSC report, EUR 23825 EN, Ispra.

Rausand M. and Hoyland A., 2004, System Reliability Theory, Second edition, Wiley Series in Probability and Statistics, ISBN 0-471-47133-X.