SENSITIVITY ANALYSIS IN SUPPORT TO DESIGN ACTIVITIES

S. Contini and L. Fabbri
European Commission, Joint Research Centre
IPSC, Ispra, VA, 21027, Italy

ABSTRACT

A system may present different potentially dangerous failure states (Top-event), which are identified through the application of systematic methodologies, as for instance HAZOP, FMEA The analysis of system failure states via Fault Tree allows determining the accident failure frequency and the importance measures of components' failure modes. The combination of Importance and Sensitivity Analysis (ISA) constitutes a very powerful tool to improve the design of critical systems or to prove that the design satisfies the safety requirements. In current applications, the different Top-events are *sequentially analysed* to identify the weakest parts of the system which require further design considerations. This procedure, refereed to as Sequential ISA (SISA), has some limitations, among which the significant cost of the analysis. The present paper describes a new method, named "Concurrent Importance and Sensitivity Analysis (CISA)", aiming at overcoming the limitation of SISA and extending its application to the identification of "over-reliable" system functions (if any) on which the reliability / maintainability characteristics of the involved components can be relaxed with consequent cost saving. The result is a *uniformly protected* system satisfying the predefined design goals.

1. INTRODUCTION

The different failure modes associated with the system's components, referred to as primary or basic events (BE), might have a different impact on the occurrence probability of the system's failure states, referred to as Top-events. Each relevant Top-event, representing an accident scenario, can be scrutinized using the fault tree analysis (FTA) technique. The fault tree is the most popular system analysis technique allowing to systematically describing the logical relationships between the failure at components level with the failure at subsystem and system levels. Besides the probabilistic parameters at system level, FTA provides the importance measures (or indexes) of each BE and the so-called Minimal Cut Sets (MCS), i.e. the minimum set of basic events whose failure causes the system failure. The components' importance indexes are normally classified into two categories: (*i*) structural and (*ii*) probabilistic, depending on whether they are directly associated with (*i*) the BE structure function (i.e. how the BE combines within the MCS) or (*ii*) with the BE failure probability. Once the most "sensitive" failure modes are identified, some system improvements can be produced 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, as e.g. parallel, stand-by, K out of N. Generally, the design modifications involve components of the system safety functions.

Complex systems are usually characterised by a set of potential failure states (Top-events), whose associated Fault Trees could contain some common BEs. For design improvement purposes the Importance and Sensitivity Analysis is applied to all fault trees, independently and sequentially, starting from those associated with system failure states with the heaviest consequences. In this paper this approach is referred to as Sequential Importance and Sensitivity Analysis (SISA). This approach present some practical limitations: (*i*) the analyst cannot fully realise the actual impact on the overall system safety of a modification following the sensitivity analysis conducted on a single Fault Tree at a time; (*ii*) it may happen that the result of the sensitivity analysis requires some deeper modification (e.g. the use of redundancies, implying a modification of more Fault Trees; (*iii*) the cost of the overall analysis may be significant because of repetitions and overlapping. As a matter of fact, any system modification resulting from the analysis of any Fault Tree would require updating and re-analysing all previously-analysed Fault Trees, containing the modified components. 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. Due to the extensive use of fail-safe components, the improvement of the system from the safety viewpoint may jeopardise the system availability target. This means that the fault trees for system unavailability should be constructed and analysed concurrently with the fault trees of the safety functions.

A possible way forward to overcome these limitations is to perform the Sensitivity Analysis on all Fault Trees concurrently (CISA). This is the subject of the present paper, which describes a significant improvement of the method for on-line Importance and Sensitivity Analysis implemented in the past within ASTRA [1, 2], which has been applied with success to a real system [3]. The proposed method offers two significant advantages over the previous one: *(i)* it removes the subjective parameter in the calculation of the global importance index of components and *(ii)* it considers also the components with the lowest importance indexes that may be associated with "over-reliable" functions. In particular, this method allows obtaining a uniformly protected system, i.e. not only without "weak functions", causes of system failure, but also without uselessly "over-reliable functions", causes of major costs. Hence, the additional cost for reducing the Top-events occurrence frequency could be partially compensated by relaxing the reliability / maintainability characteristics of those functions that are uselessly reliable.

2. BASIC CONSIDERATIONS

2.1 Definition of Top-event Goals

Methodologies such as FMEA and HAZOP are commonly applied to identify the potential adversary events leading to accidents or production loss (accident scenarios). As it is well known, the quantitative definition of risk associated with the failure of a system is given by a set of triplets [4]:

$$R = < S_i \ f_i \ C_i > \qquad i=1,2,\ldots.$$

where S_i is a possible accident scenario for the system (Top-event), f_i is its frequency, and C_i its consequence. The overall risk of the system can be represented on a log-log scale as depicted in Figure 1 where for each accident scenario (squared points) the values of occurrence probability and consequence are reported. Three zones can be defined in the graph, which are divided by two straight lines representing the risk acceptance criteria. The area above the bold straight line is considered as the area in which the risk is unacceptable, whilst the area below the dotted line is where the risk is acceptable. The area in between is the ALARP region (As Low As Reasonably Practicable) in which efforts must be done to possibly reduce the risk further by decreasing the failure likelihood of occurrence and / or reducing the consequences to an extent that is practically feasible. The task of the system designer is to "move" the risk points towards the acceptable risk area through the improvement of the system safety and/or the mitigation measures.

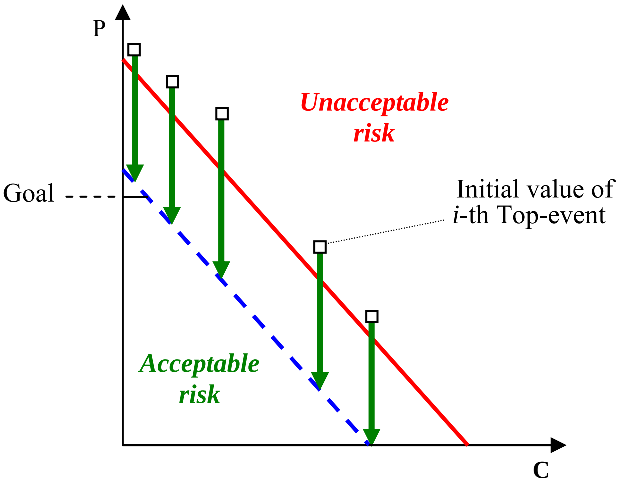

Figure 1: Example of a Probability-Consequence plot showing unacceptable Top events

In this paper we consider the problem of reducing the risk by reducing the accident's probability, i.e. by improving the protection systems. Hence, for each accident, a goal can be defined, i.e. a probability value that must be achieved through selected design changes. In Figure 1 the green arrows represent the probabilistic reduction that is necessary in order to make the risk acceptable.

2.2. Importance and Sensitivity Analysis

The Importance and Sensitivity Analysis (ISA) is a consolidated procedure applied during the system's design phase to identify the weakest parts of the system, i.e. those components giving the greatest contribution to the likelihood of occurrence of the most relevant Top-events, and to identify and evaluate the suitable design modifications aiming at improving the system safety level. Essentially, the ISA procedure is based on three main steps:

1. Ranking of components according to their importance to system failure (importance indexes).
2. Having identified the weakest system points (i.e. components with the highest importance indexes), the design can be improved by adopting one or more design strategies (design alternatives).
3. Following the design modification the Fault Tree is updated and re-analysed to assess the effects of the improvement made, that is the impact of the adopted design alternatives to the system failure probability and the selection of the most convenient alternative by taking into account the existing constraints (e.g. cost, space, and weight)

ISA is conducted on all Fault Trees describing all possible failure of the associated system. In practice the fault trees are analysed independently, and sequentially, starting from those having more severe consequences. This approach is referred to as "Sequential ISA" (SISA) in this paper. Figure 2 gives a schematic diagram of SISA for a system with N=3 fault trees.

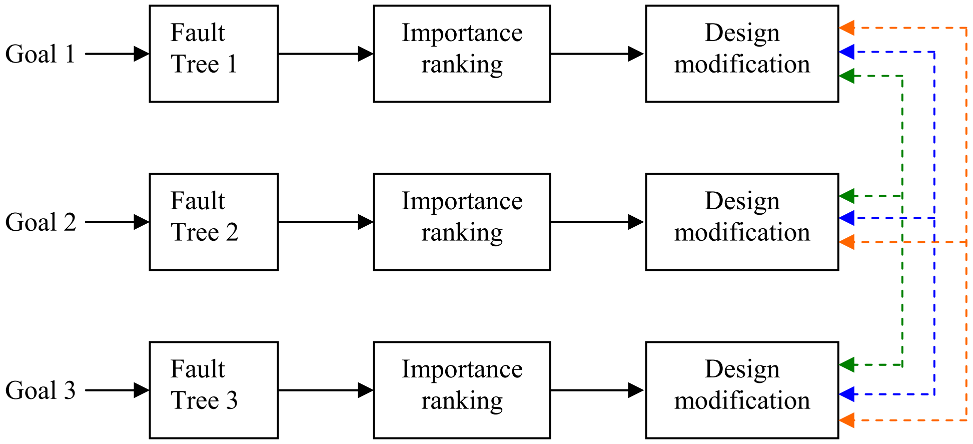

Figure 2. Schematic diagram of the Sequential Importance and Sensitivity Analysis (SISA)

According to the SISA approach a single fault tree is analysed at a time. At the generic *i*-th step of the ISA process, the probabilistic quantification provides the Top-event occurrence probability $Q^{(i)}$ and the components importance indexes. Since these indexes are determined on a single Fault Tree they are referred to as "Local Importance Indexes" (LII) in this paper. The component with the maximum LII value is selected and considered for design improvement. If a potentially useful design modification is identified then the Fault Tree under consideration is analysed to decide 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 component, then it is necessary to properly modify it before analysing it. Moreover, a system modification following the analysis of e.g. the *j*-th Fault Tree should lead to the updating of all Fault Trees previously analysed (i.e. from 1 to *j*-

1), which contain the modified component. This process is represented in Figure 2 by the arrows with dotted lines. In the current practice, this "backwards" re-analysis is not performed very often for two main reasons: (*i*) the increase of the overall costs of the analysis, and (*ii*) the coherency of the Fault Trees, which implies that a component modification that leads to a failure probability reduction of the *j*-th Top-event cannot increase the failure probability of the other Top-events. It is rather evident that the Sequential ISA might lead to over protect some system functions.

An alternative way of carrying out the sensitivity analysis is to perform it concurrently on the whole set of system's Fault Trees. This approach is referred to as "Concurrent ISA" (CISA) in this paper. Figure 3 provides a schematic diagram of CISA for N=3 fault trees.

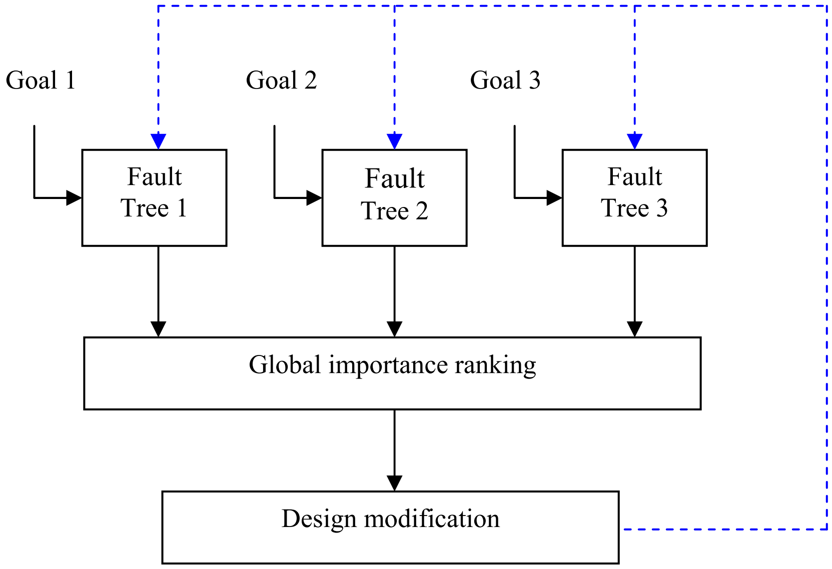

Figure 3. Schematic diagram of the Concurrent Importance and Sensitivity Analysis (CISA)

The substantial difference between SISA and CISA is the determination of the Global Importance indexes (GII) of basic events, i.e. indexes determined on the basis of LII in all Fault Trees. The GII ranking coincides with the LII ranking only if all Fault Trees are independent, i.e. if they do not share any basic event. 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 concurrently re-analysed. It is clear that the CISA approach is particularly suitable also to face problems of conflicting requirements.

In Figure 2 and 3 each Fault Tree has an associated goal. This is the aim of the ISA procedure: each Top-event probability must be lower than the corresponding goal. This allows selecting the proper probabilistic reduction to be attained depending on the Top-event position in the risk curve.

From what has been said, the following considerations can be drawn:

- SISA and CISA are equivalent if:
    - only one fault tree is involved in the analysis;
    - all fault trees are independent, i.e. if there are no common events.
- CISA is superior to SISA when there are common events, since:
    - the designer can immediately see the impact on all Top-events of each adopted design modification;
    - the determination of components criticality, by means of GII, takes into account the probabilistic dependence between Top-events;
    - the cost of the analysis is lower.

3. THE PROPOSED CISA METHOD

Within the CISA method proposed in the past [1] a subjective definition of importance for each Top-event was required. To get rid of this clear drawback, the present paper proposes an alternative approach, which consists of determining the global importance indexes (GII) of basic events in more objective terms. Another important aspect, not considered in the past, is that the current ISA focuses only on the identification of the weakest components of the system in terms of safety. By contrast, it does not address the identification of functions that are uselessly reliable the examination therewith might contribute to a clear reduction of the total cost for system's improvement. Thus, together with the "Goal Achievement" phase, which aims at reducing the risks of the system, the present approach incorporates a "Cost Reduction" procedure. This new approach is described in the following sections: firstly with reference to a single fault tree and then to multiple fault trees. A simple example is also provided in order to show how the method works.

3.1 Goal Achievement Phase

Let $Q_0(t)$ be the occurrence probability of the Top event under consideration at the mission time t. To simplify the notation throughout the paper the reference to the time will be omitted.

Let $P_G < Q_0$ be the assigned probabilistic goal to be achieved.

The Goal Achievement Phase (GAP) aims at identifying possible design modifications such that $Q \leq P_G$

Starting from Q_0 the goal P_G is reached in one or more steps, where at each step a system modification is made. The Top-event probability Q changes from Q_0 at step 0 (initial condition) to $Q^{(i)} < Q^{(i-1)}$ at the *i*-th step. At each step, the difference between the Top-event failure probability and the goal P_G is a measure of the effort needed to improve the system. The Total Gain percentage at the generic *i*-th step, indicated as $G^{(i)}$ (i.e. referring to the initial situation where $Q = Q_0$) and the percentage effort still to be done to reach the goal are given by:

$$G^{(i)} = \frac{Q_0 - Q^{(i)}}{Q_0 - P_G}100; \qquad E^{(i)} = 100 - G^{(i)} \tag{1}$$

The goal is satisfied when $Q^{(i)} \leq P_G$, which means that $G^{(i)} \geq 100$.

All these quantities are graphically shown in Figure 4.

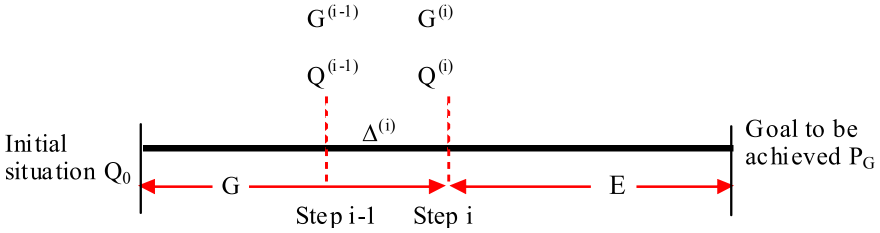

Figure 4. Main parameters of the system improvement process at a generic step

The gain at the generic *i*-th step, referred to as Step Gain percentage and represented as $\Delta^{(i)}$, is given by:

$$\Delta^{(i)} = \frac{Q^{(i-1)} - Q^{(i)}}{Q_0 - P_G}100 \tag{2}$$

The component to consider at each step is the one with the highest Criticality index I_k^C [5]. In this context the Criticality index is interpreted as a measure of the relative variation of the top-event probability due to a given relative variation of the component failure probability. In Appendix the following equation is proved:

$$\frac{Q^{(i-1)} - Q^{(i)}}{Q^{(i-1)}} \cong I_k^{C(i-1)} \frac{(q_k^{(i-1)} - q_k^{(i)})}{q_k^{(i-1)}}$$

Note that the value of $Q^{(i)}$ can be obtained without analysing the fault tree. Indeed, from the above equation, after a little algebra, we have:

$$Q^{(i)} \cong Q^{(i-1)}[1 - I_k^{C(i-1)} \frac{(q_k^{(i-1)} - q_k^{(i)})}{q_k^{(i-1)}}] \qquad (3)$$

This expression gives the new value of the Top-event occurrence probability $Q^{(i)}$ at the i-th step of the ISA procedure, that we would obtain if we operated on the *k*-th BE (component). The reduction in the failure probability of the selected component, $q_k^{(i)} < q_k^{(i-1)}$, can be obtained in different ways, as e.g.:

1) Changing the reliability/maintainability parameters through:
- Reduction of the failure rate (use of a component of better quality);
- Reduction of the mean down time (use of a component of better maintainability);
- Modification of test intervals and/or of testing policy.

2) Use of redundant configurations consisting in substituting the component with two or more components of the same type. The configurations that can be used, without changing the fault tree structure (already implemented in ASTRA-SAM [2]), are of various type (parallel; cold and warm stand-by with perfect switch; K/N of active components; K/N of tested components with different testing policy: simultaneous, sequential, and staggered).

If the gain $G^{(i)}$ corresponding to the chosen design modification is acceptable, then the fault tree can be effectively updated and analysed, otherwise another modification can be identified and tested in the same way. Considerations on constraints such as volume, weight, cost, etc, should be taken into account to further help identifying the best design alternative to implement.

It may happen that, at a given step, two or more components have similar importance indexes, leading to the consideration of design alternatives with similar step gain. These alternatives can be managed by means of a decision tree, where each node has as many descendants as the number of identified potentially acceptable alternatives, as schematically shown in Figure 5, where the root represents the initial design configuration.

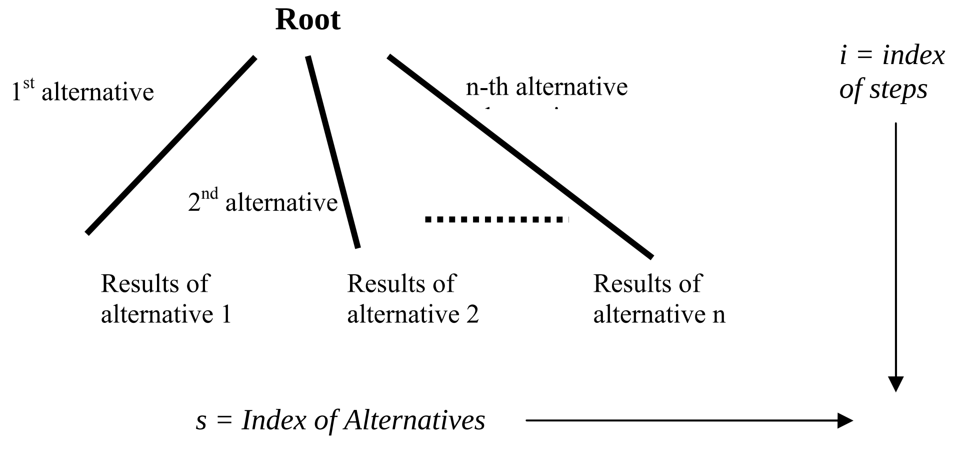

Figure 5. Schematic representation of different potentially acceptable alternatives (decision tree)

At a given step each branch represents a potentially acceptable system design modification; its acceptability is based on the reliability characteristics of the selected component and on considerations about existing constraints. This procedure leads to the development of a tree. A path from the root to a terminal node represents a set of design modifications, which is a potentially acceptable solution for system design improvement. In other words a path is a set of design modifications compatible with all constraints. The Total Gain provides information on “How good” the *k*-th path is. In order to speed up the process, all alternatives at step *i* could be compared to continue only with those that seem to be the most promising, i.e. having comparatively higher Total Gain. Hence, potential alternatives recognised as less significant, can be removed to avoid developing branches that cannot give useful solutions.

3.2 Cost Reduction Phase

The Cost Reduction Phase (CRP) 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. The identification of these functions could allow reducing the cost of the final design solution by relaxing the reliability/maintainability characteristics of the involved components without compromising the achievement of the overall goal P_G. Hence the “cost” necessary for improving safety in the GAP phase could be partially compensated by the solutions adopted in the CRP phase.

The selection of the components to be examined is based on the minimum values of the importance indexes. It is important to outline the fact that if the fault tree probabilistic analysis were based on the disjunction of MCS (i.e. the classical FTA approach), the determination of the criticality indexes would necessarily require the calculation of all MCS. Frequently, the number of MCS is so high that makes such determination impractical. This is probably the main reason why the CRP phase has never been proposed in the past.

The quantification method based on the newer approach of Binary Decision Diagrams (BDD), which allows performing the exact quantification of fault trees without the need to determine the MCS [2, 4], helps a lot to determine the minimum BE importance indexes and, in turn, to implement correctly the CRP procedure.

Some strategies can be adopted for those components characterised by lower importance indexes. For instance, depending on the type of component:

- increase of failure rate (change with a component of worst quality);
- increase of down time (allowing a larger repair time interval, e.g. delaying the repair activity, avoiding to keep a spare part in the plant store);
- increase the time between test (reduce the test frequency);
- change the testing policy (e.g. from staggered to sequential).

Thus, the component with the *minimum* Criticality index [7] can be examined to check whether a modification can be adopted by changing q_k with a greater value that still satisfies the goal P_G.

The following equation provides the increase of $Q^{(i)}$ at the generic step (i) with respect to the previous step ($i-1$), $Q^{(i)} > Q^{(i-1)}$, following a modification (increase) of the failure probability of the selected component from $q_k^{(i-1)}$ to $q_k^{(i)}$:

$$Q^{(i)} \cong Q^{(i-1)}[1 + I_k^{C(i-1)} \frac{(q_k^{(i)} - q_k^{(i-1)})}{q_k^{(i-1)}}] \tag{4}$$

If the new value is acceptable, then the fault tree is quantified with the new $q_k^{(i)}$ value, otherwise another modification is examined.

In summary, the following steps, which can be repeated until $Q < P_G$, implement the procedure:

1. Select the event with minimum I^C
2. Identify the possible modification according to the type of component;
3. Determine the consequent variation of Q using equation (4);

4. If Q is acceptable then confirm the decision: the fault trees are modified and the new values are calculated, otherwise go to step 1.

As for the previous case (GAP) a decision tree helps managing the different design alternatives.

3.3 Extension of the methodology to multiple fault trees

The two phases previously described with reference to a single fault tree can easily be extended to cover the case of the set of *N* fault trees associated with the same safety level or with different safety levels. In the first case the unique goal for frequency reduction (P_G) is defined, whereas in the second case each *j*-th fault tree has its own goal P_G^j. The effect of any design modification adopted on the component(s) of (one or more) fault tree at a given safety level, can be assessed also on all the other fault trees belonging to different safety levels.

The procedure for multiple fault trees is similar to the one described in the previous section. The difference relies mainly on the determination of the Global Criticality index of basic events and the total failure probability Q_T. It can be easily proved that for the present case, by assuming the rare event approximation:

$$Q_T = \sum_{j=1}^{N} Q_j \tag{5}$$

the following relationships holds true [6]:

$$I_k^B = \sum_{j=1}^{N} I_{kj}^B \tag{6}$$

$$I_k^C = \frac{1}{Q_T} \sum_{j=1}^{N} I_{kj}^C \, Q_j \tag{7}$$

where:

N Total number of fault trees.
$I^B{}_k$ Global Birnbaum importance index of the *k*-th event in the *N* fault trees in which it appears.
$I^B{}_{kj}$ Local Birnbaum importance index for the *k*-th event in the *j*-th fault tree;
$I^C{}_k$ Global Criticality importance index of the *k*-th event in the *N* fault trees in which it appears.
$I^C{}_{kj}$ 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, due to the low probability values of Top-events, the approximation of eq. (5) is acceptable, i.e. the probability of the intersection of two fault trees is negligible. At each step of the analysis equation (7) allows to determine the global criticality which is used to select the event to examine.

Therefore, once the global criticality indexes and the total unavailability have been determined, the Concurrent ISA described in the previous section can be applied as if the *N* fault trees were the *N* descendants from an OR gate of the fictitious Top-event defined as: "*Occurrence of any accident in the plant*". When a given design modification is adopted, then from the *N* fault trees those containing the involved component are analysed to determine the impact on all Top-events occurrence probability.

3.4 Application Example

3.4.1 Problem Definition

The methodology described in the previous section is applied to a case of three fault trees, which are supposed to be associated with the same safety level and having the same goal $P_G = 10^{-5}$ for frequency reduction. The logical functions of the three fault trees are given by:

$TOP_1 = A\,B + A\,C$; $TOP_2 = A\,D + E$; $TOP_3 = B\,F\,H + H\,K$

TOP_1 and TOP_2 contain the common event A; TOP_1 and TOP_3 contain the common event B.
The basic events data are given in Table 1 where λ is the failure rate and τ the repair time. The last column contains the failure probability at the mission time T = 10,000 hours.

BE	*A*	*B*	*C*	*D*	*E*	*F*	*H*	*K*
λ (h^{-1})	10^{-5}	10^{-4}	10^{-6}	10^{-5}	10^{-5}	10^{-4}	10^{-5}	10^{-5}
τ (h)	100	50	-	-	200	100	-	50
q(T)	$9.99 \cdot 10^{-4}$	$4.97 \cdot 10^{-3}$	$9.95 \cdot 10^{-3}$	$9.51 \cdot 10^{-2}$	$1.99 \cdot 10^{-3}$	$9.90 \cdot 10^{-3}$	$9.51 \cdot 10^{-2}$	$4.99 \cdot 10^{-4}$

Table 1: Main parameters associated with the BE of the reference system (initial design configuration)

3.4.2 Goal Achievement

The exact values of the three Top-events, describing the failure logic of the initial design configuration, are as given below. As the rare event approximation holds true, their sum (Q_T) provides the total system's probability of failure.

$Q_1 = 1.48 \times 10^{-5}$; $Q_2 = 1.19 \times 10^{-3}$; $Q_3 = 5.22 \times 10^{-5}$ $Q_T = 1.27 \times 10^{-3}$.

None of these fault trees satisfy the goal P_G. For each Top-event the LII are given in Table 2. The importance measures are used to rank the events in decreasing order. The last row contains the global value obtained using equation (9).

TOP	***A***	***B***	***C***	***D***	***E***	***F***	***H***	***K***
1	1	0.665	0.331					
2	0.84			0.159	0.159			
3		0.089				0.089	1	0.91
Global	0.798	0.011	0.0038	0.149	0.149	0.003	0.041	0.037

Table 2: Local and Global Criticality indexes of the BE for the reference system

The BE with highest importance index is A. Let's suppose that two possible modifications could be conceived for this event representing the failure mode of a repairable component:

Alternative 1: Reduce the repair time of A from 100 h to 50 h
Alternative 2: Use the parallel redundancy (A1 and A2 substitute A)

With these alternatives new values for Q_1 and Q_2 can be obtained (Q_3 does not change, since it does not contain A):

Alternative 1: $Q_1 = 7.43 \times 10^{-6}$ $Q_2 = 6.89 \times 10^{-4}$ $Q_3 = 5.22 \times 10^{-5}$ $Q_T = 7.48 \times 10^{-4}$
Alternative 2 : $Q_1 = 1.48 \times 10^{-8}$ $Q_2 = 1.90 \times 10^{-4}$ $Q_3 = 5.22 \times 10^{-5}$ $Q_T = 2.42 \times 10^{-4}$

Both alternatives deserve to be retained; however, as expected, the second one is more effective. For illustration purposes we will proceed with the second alternative only. So far TOP_1 is the only fault tree satisfying the goal condition ($Q<10^{-5}$), therefore, it has not to be considered for improvement anymore. However, the variation of Q_1 is still considered in order to see how it changes as a result of the subsequent design alternatives. In order to proceed with the analysis, the new importance indexes for the newly designed system have to be calculated. They are given in Table 3.

TOP	*A1*	*A2*	*B*	*C*	*D*	*E*	*F*	*H*	*K*
1	1	1	0.331	0.665					
2	0.005	0.005			0.994	0.994			
3			0.089				0.089	1	0.91
Global	0.004	0.004	0.019	0.002	0.780	0.780	0.019	0.215	0.196

Table 3: Local and Global Criticality indexes of the BE for the system as modified via alternative 2

As results from the table, now the most important events are D and E, which both belong to TOP_2 only. Let's suppose that D can be made repairable with a small design modification. Suppose that the estimated mean repair time is 100 h. With this modification we find the following results:

$Q_1 = \mathit{1.48 \times 10^{-8}}$ $Q_2 = \mathit{2.99 \times 10^{-6}}$ $Q_3 = 5.22 \times 10^{-5}$ $Q_T = 5.52 \times 10^{-5}$

We notice that as far as the TOP_3 is concerned, the most important event is H. We now suppose that H could only be made repairable with a repair time of 100 h, whilst redundancy is not feasible due, for instance, to space problems. These assumption leads to:

$Q_1 = \mathit{1.48 \times 10^{-8}}$ $Q_2 = \mathit{2.99 \times 10^{-6}}$ $Q_3 = \mathit{5.48 \times 10^{-7}}$ $Q_T = \mathit{3.55 \times 10^{-6}}$

At this point the goal $P_G = 10^{-5}$ is achieved for all cases. This particular design solution foresees to make A redundant and to make D, H repairable. Clearly, the proposed modifications are not necessarily the most effective. A thorough analysis of all possible alternatives (decision tree) is very useful to select the best choice.

3.4.2 Cost Reduction

The previous section has shown how the system can be modified in order to achieve the attained goal. The results of the calculation of the BE critically indexes for the final system configuration are now given in Table 4.

TOP	*A1*	*A2*	*B*	*C*	*D*	*E*	*F*	*H*	*K*
1	1	1	0.331	0.665					
2	0.333	0.333			0.666	0.666			
3			0.089				0.089	1	0.91
Global	0.284	0.284	0.015	0.002	0.560	0.560	0.014	0.154	0.140

Table 4: Local and Global Criticality indexes of the BE for the current system configuration

As expressed in a previous section, the cost reduction phase is addressed to assess whether some of the less critical components are uselessly reliable and they can be worsened in order to reduce the costs of the aforementioned modifications. This means that $Q_1 = \mathit{1.48 \times 10^{-8}}$, which is far below the goal $P_G = 10^{-5}$, could be increased if suitable design modifications can be found. From Table 4, it is clear that the non-repairable component *C* is the less critical for the system. By considering a cheaper component with a higher failure rate (e.g. $\lambda = 10^{-4}$ h^{-1}), it is possible to show that the corresponding value of Q_T changes from $Q_T = \mathit{3,55 \times 10^{-6}}$ to $Q_T = \mathit{4.17 \times 10^{-6}}$, which is still within our goal.

To proceed further, it is necessary to focus on the next component with lowest importance (*F*). In particular, *F* is repairable with mean repair time of 100 h. If this is increased to 300 h, the corresponding value for Q_T is $\mathit{5.52 \times 10^{-6}}$, which is still acceptable. On this system configuration the least important components are *B* and *K*, which are both repairable. The decision to increase the repair time from 50 to 300 h is considered, giving $Q_T = \mathit{7.46 \times 10^{-6}}$. Continuing on this configuration the next component to consider is *E*, repairable. Changing its repair time from 200 to 300 the new value of Q_T is $\mathit{8 \times 10^{-6}}$, that is still within our goal range. The corresponding probabilities of the three Top-events have changed as follows:

$Q_1 = 6.59 \times 10^{-7}$ $Q_2 = 4.1 \times 10^{-6}$ $Q_3 = 3.8 \times 10^{-6}$ Q_T is 8×10^{-6},

which corresponds to one of the potential new system configurations obtained from the reference one by making a component redundant (*A*), two components reparable (*D* and *H*), C substituted with a component of worst quality, whilst for four other components the allowed down time has been extended to 300 h (*B, F, E,* and *K*).

4. CONCLUSIONS

In this paper we have briefly described the Concurrent Importance and Sensitivity Analysis (CISA) approach for system design improvements based on Fault tree analysis. Part of this approach has already been implemented in the past and applied with success to a real system. The proposed method overcomes the drawback of the previous implementation and extends its application to the consideration of safety functions whose availability can be lowered without compromising the requirements on the overall system safety level.

The CISA approach will be tested, and possible improved, on real systems before entering the software implementation phase.

5. REFERENCES

[1] S. Contini, S. Sheer, M. Wilikens, "Sensitivity Analysis for System Design Improvement", Proceedings of DSN 2000, New York

[2] S. Contini, G. Cojazzi, G. Renda, G. De Cola, " La metodologia ASTRA per l'analisi di affidabilita' di sistemi complessi", VGR 2004, Valutazione e Gestione del Rischio negli Insediamenti Civili ed Industriali, Pisa, 2004.

[3] A. Baietto, "Il ruolo dell'analisi di sensitivita' per l'integrazione dei requisiti di affidabilita' e sicurezza nella progettazione di sistemi di controllo per applicazioni energetiche" Tesi di laurea, Politecnico di Torino, 1997.

[4] S. Kaplan, B.J. Garrick, "On the quantitative definition of risk", Risk Analysis, Volume 1, Issue 1, Page 11-27, Mar 1981.

[5] A. Rauzy, "A brief introduction to Binary Decision Diagrams" RAIRO-APII-JESA, European Journal of Automation, Vol. 30-n.8/1996.

[6] S. Contini, L. Fabbri, "Concurrent Importance and Sensitivity Analysis as a Support to System Design Improvement", JRC Report under publication. JRC Ispra, 2008.

[7] M. Rausand, A. Hoyland, "System Reliability Theory. Models, Statistical Methods and Applications", Second Edition, Wiley Series in Probability and Statistics, 2004, ISBN 0-471-47133-X.

APPENDIX: Proof of equation (3)

Let $\Phi(\mathbf{x})$ be the structure function of the fault tree under examination. $\mathbf{x} = (\mathrm{x}_1, \mathrm{x}_2, \ldots \mathrm{x}_n)$ is the vector of the variables (basic events). It is known that, with respect to a given event x_k, the function $\Phi(\mathbf{x})$ can be written as follows:

$$\Phi(\mathbf{x}) = \mathrm{x}_k \ \Phi(1_k, \mathbf{x}) + \overline{\mathrm{x}_k} \ \Phi(0_k, \mathbf{x})$$

where:

$$\Phi(1_k, x) = \Phi(x_1, x_2, \ldots, x_k = 1, \ldots, x_n) \text{ and}$$

$$\Phi(0_k, x) = \Phi(x_1, x_2, \ldots, x_k = 0, \ldots, x_n)$$

Passing to probabilities:

$$\mathrm{P}(\Phi(\mathrm{x})) = q_k\, I_k^B + P(\ \Phi(0_\mathrm{k}, \mathrm{x})) \qquad \text{(A.1)}$$

where

$$I_k^B = \mathrm{P}(\Phi(1_\mathrm{k}, \mathrm{x})) - P(\ \Phi(0_\mathrm{k}, \mathrm{x}))$$

is the Birnbaum importance index (i.e. the probability of the critical state for the *k*-th basic event (BE), that is the Top- event occurs when x_k occurs [7]). Note that I_k^B does depend on the structure function and not on the *k*-th BE probability.

By indicating with $q_k^{(i-1)}$ the failure probability of the *k*-th BE at the (i-1)-th step corresponding to the system failure probability is $Q^{(i-1)}$, and with $q_k^{(i)}$ the value that corresponds to $Q^{(i)}$, the following relationships can be derived from (A.1):

$$q_k^{(i-1)}\mathrm{I}_\mathrm{k}^{\mathrm{B(i\text{-}1)}} + P(\Phi(0_\mathrm{k}, \mathrm{x})) = \mathrm{Q}^{(\mathrm{i\text{-}1})}$$

$$q_k^{(i)}\mathrm{I}_\mathrm{k}^{\mathrm{B(i\text{-}1)}} + P(\Phi(0_\mathrm{k}, \mathrm{x})) = \mathrm{Q}^{(\mathrm{i})}$$

Supposing that $q^{(i)} < q^{(i-1)}$, which implies that $Q^{(i)} < Q^{(i-1)}$, and subtracting the second equation to the first we get:

$$\mathrm{Q}^{(\mathrm{i\text{-}1})} - \mathrm{Q}^{(\mathrm{i})} = (\mathrm{q}_\mathrm{k}^{(\mathrm{i\text{-}1})} - \mathrm{q}_\mathrm{k}^{(\mathrm{i})})\ \mathrm{I}_\mathrm{k}^{\mathrm{B(i-1)}} \qquad \text{(A.2)}$$

From this equation the following can be derived:

$$\frac{\mathrm{Q}^{(\mathrm{i\text{-}1})} - \mathrm{Q}^{(\mathrm{i})}}{\mathrm{Q}^{(\mathrm{i-1})}} = \frac{\mathrm{I}_\mathrm{k}^{\mathrm{B(i-1)}}\mathrm{q}_\mathrm{k}^{(\mathrm{i-1})}}{\mathrm{Q}^{(\mathrm{i-1})}} \frac{(\mathrm{q}_\mathrm{k}^{(\mathrm{i\text{-}1})} - \mathrm{q}_\mathrm{k}^{(\mathrm{i})})}{\mathrm{q}_\mathrm{k}^{(\mathrm{i-1})}}$$

Note that $\mathrm{I}_\mathrm{k}^{\mathrm{C(i-1)}} = \dfrac{\mathrm{I}_\mathrm{k}^{\mathrm{B(i-1)}}\mathrm{q}_\mathrm{k}^{(\mathrm{i-1})}}{\mathrm{Q}^{(\mathrm{i-1})}}$ is the expression of the Criticality importance index of the *k*-th BE at the (i-1)-th step.