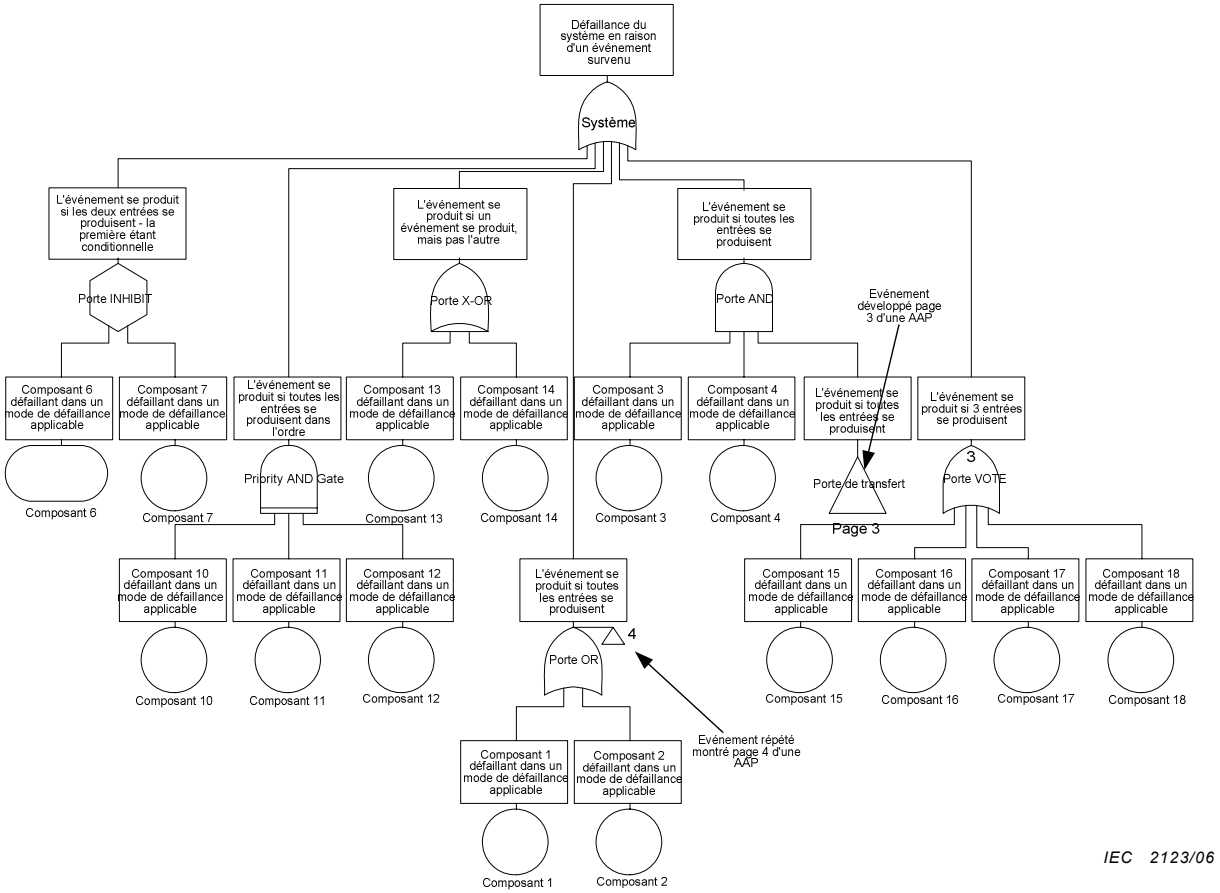


Figure 6 – Exemple d'arbre de panne contenant un événement de transfert et un événement répété

Un exemple d'arbre de panne rectangulaire montrant un événement de transfert extérieur ou de cause commune est visible Figure 7. L'événement B est un événement qui est analysé de manière plus poussée sur un autre arbre de panne. L'événement D est un événement de base.

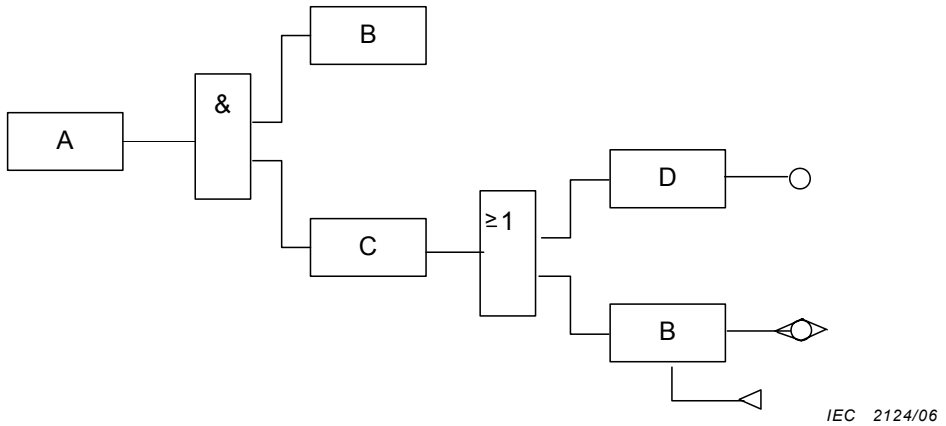


Figure 7 – Exemple présentant des indications se rapportant à une cause commune dans une représentation de porte rectangulaire

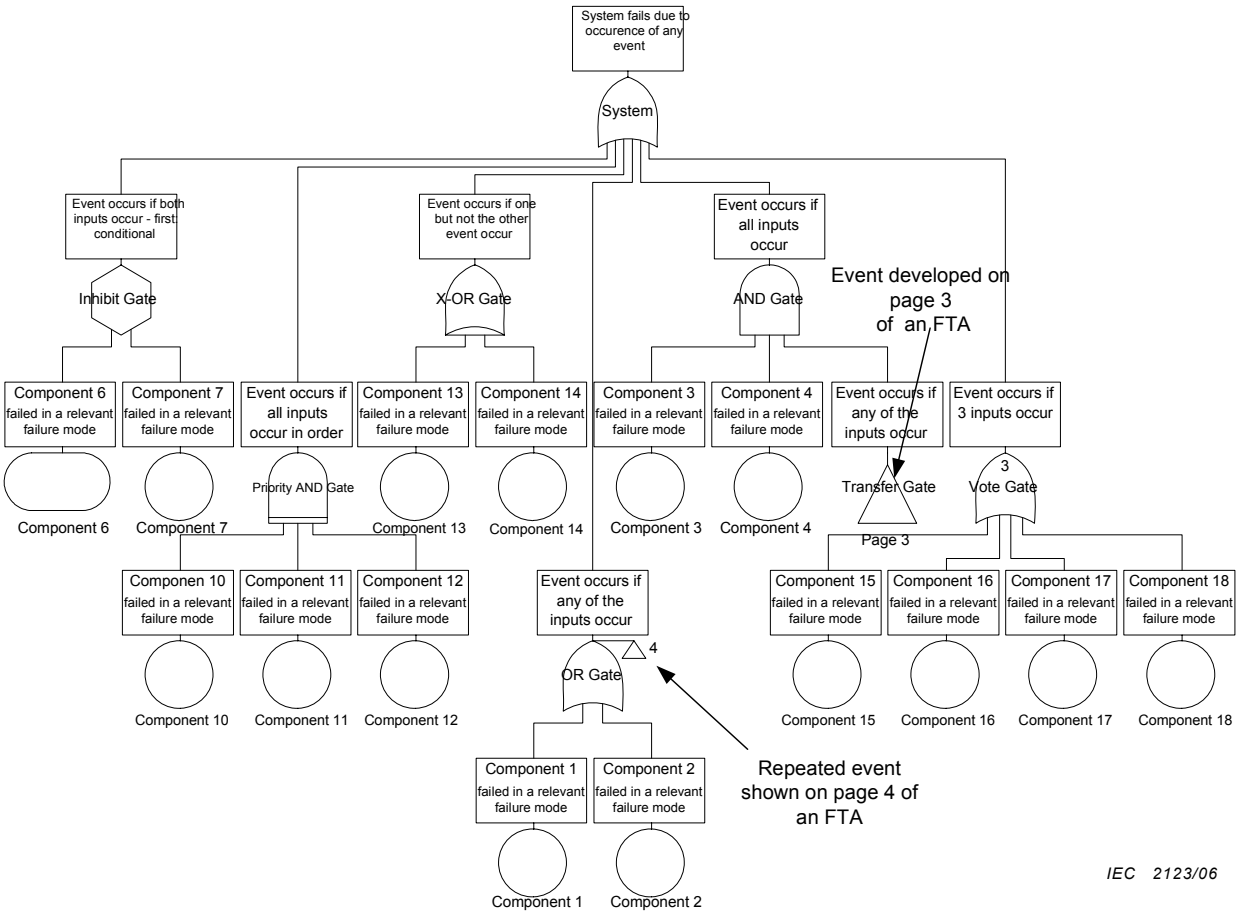


Figure 6 – Example fault tree containing a repeated and a transfer event

An example of a rectangular fault tree showing transfer out repeated or common cause event is shown in Figure 7. Event B is an event, which is analysed further on another fault tree. Event D is a basic event.

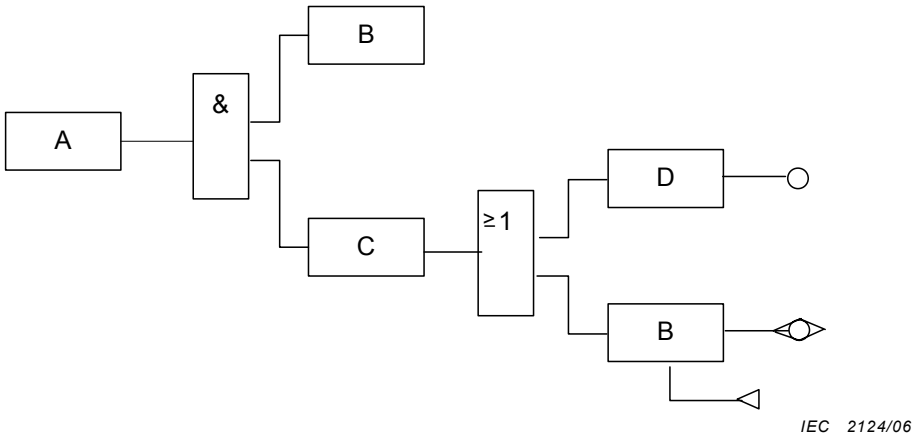


Figure 7 – Example showing common cause considerations in rectangular gate representation

7.5.3 Technique de construction

La première étape dans la construction d'un arbre de panne est de définir clairement l'événement de tête, le domaine d'application et l'objectif de l'arbre de panne, les limites du système ou de l'objet de l'analyse et la résolution de l'analyse. Il convient que cet objectif soit défini en termes de définition de l'événement de tête.

Il faut que l'événement de tête décrive un problème qui doit être analysé pour en déterminer les causes. Dans l'application AAP pour l'amélioration de la fiabilité d'un système en développement, l'événement de tête est une défaillance du système et l'objectif de l'analyse est de déterminer ce qui contribue à cet événement et d'identifier les faiblesses de la conception ou les composants non fiables. Dans l'analyse quantitative la probabilité d'apparition de l'événement de tête et toutes ou la plupart des entrées seront déterminées. Dans l'analyse qualitative, Méthode A, les entrées de l'événement de tête seront examinées afin d'identifier les causes de leur apparition (autres événements ou pannes). Dans l'analyse quantitative, Méthode B, pour l'amélioration de la conception, les entrées de l'événement de tête sont analysées pour identifier les principaux éléments contribuant à l'événement de tête, et améliorer la conception par une élimination systématique de ces faiblesses ou réduction de ces modes de défaillances.

Le domaine d'application de l'analyse définit les événements ou les modes de défaillance qui seront inclus dans l'arbre de panne. Le domaine d'application couvre aussi les détails du problème analysé, le niveau de révision de la conception du système analysé, le profil d'utilisation du système et autres conditions fonctionnelles et environnementales, alors que les limites définissent ce qui est inclus et ce qui est exclu de ce système (par exemple, les connections internes, les enveloppes mécaniques, etc.).

Il convient de construire un arbre de panne de façon à ce qu'il représente clairement le flux d'événement qui ont mené à l'apparition de l'événement de tête.

Une fois l'événement de tête clairement défini de même que les limites du système et de l'analyse, alors la construction de l'arbre de panne en découle de haut en bas. L'événement de tête a des entrées et leur combinaison est modélisée et représentée par la porte appropriée. Les entrées dans l'événement de tête sont alors développées systématiquement pour être des résultats de leur propre événement d'entrée. Chacune des entrées, en descendant l'arbre de panne est développée séparément et ce développement est complété lorsque les événements primaires sont atteints.

La résolution spécifiera dans quelle mesure le système doit être analysé. A titre d'exemple, un système électronique peut être analysé jusque dans ses composants et leurs causes et modes de défaillances, ou à un niveau supérieur dans son assemblage (par exemple, processeur de signal, amplificateur de puissance, régulateurs de tension d'alimentation spécifique, etc.) Parfois, la résolution peut être une combinaison d'analyse de niveau détaillé et d'assemblage, liée à la disponibilité de la probabilité d'information de l'apparition.

Si l'on ne respecte pas strictement le concept de «cause immédiate» (événement d'entrée), on risque d'omettre des modes de défaillance en croyant les avoir déjà inclus.

Le concept d'«unité de base» permet à l'analyste de ne pas élaborer des branches d'arbre de panne qui n'apportent pas d'informations nouvelles ou utiles. Une unité de base n'est pas développée plus avant. Elle est traitée comme si elle était une unité ou un composant unique ou comme si elle était examinée séparément.

Pour qu'une unité ou un événement soit considéré(e) comme étant «de base», il faut et il suffit que les trois exigences suivantes soient satisfaites:

– les limites fonctionnelles et matérielles sont clairement définies;

7.5.3 Construction procedure

The first steps in construction of a fault tree is to clearly define the top event, the scope and the objective of the fault tree, the boundaries of the system or object of analysis and the resolution of the analysis. This objective should be defined in terms of the definition of the top event.

The top event must describe a problem that has to be analysed in order to determine contributing causes. In FTA application for reliability improvement of a system under development, the top event is a system failure and the objective of analysis is to determine contributors to this event and identify design weakness or unreliable components. In quantitative analysis the probability of occurrence of the top event and all, or most, inputs will be determined. In qualitative analysis, Method A, the inputs to the top event will be investigated in order to identify the causes of its occurrence (other events or faults). In quantitative analysis, Method B, for design improvement, the inputs to the top event are analysed to identify the major contributors to the top event and to improve design by systematic elimination of those weaknesses or mitigation of contributing failure modes.

The scope of analysis defines the events or the failure modes that will be included in the fault tree. The scope also covers the details of the problem being analysed, the revision level of the system design under analysis and the use profile of the system and other operational and environmental conditions, while the boundaries define what is included and what is excluded from that system (e.g., internal connections, mechanical enclosures, etc.).

A fault tree should be constructed in such way that it clearly represents the flow of events that cause occurrence of the top event.

Once the top event is clearly defined as well as the system boundaries or analysis extent, then the fault tree construction flows from the top down. The top event has inputs and their combination is modelled and represented by the appropriate gate. Inputs into the top event are then developed systematically to be results of their own input events. Each of the inputs, going down the fault tree, is developed separately and this development is completed when the primary events are reached.

The resolution will specify to what extent the system is to be analysed. As an example, an electronic system can be analysed down to its components and their failure modes and causes, or to a higher level of its assemblies (e.g., signal processor, power amplifier, specific supply voltage regulators, etc.). At times, the resolution can be a combination of detailed and assembly level analysis, dependent on availability of probability of occurrence information.

Strict adherence to the concept of "immediate cause" is necessary to ensure that failure modes are not omitted by reason of the assumption that such modes have been included previously.

The concept of "basic units" can be used to save the analyst the effort of developing fault tree diagrams that do not yield new or useful information. A basic unit is not developed further. It is treated as if it were a single unit or component or dealt with separately.

In order for the unit or event to be considered "primary", it is necessary and sufficient that the following three requirements be satisfied:

– both the functional and physical boundaries are clearly defined;

– le fonctionnement de l'unité ne dépend d'aucune fonction auxiliaire ou bien tous les événements se rapportant à l'unité sont exprimés par une seule porte OR dont l'une des entrées représente une panne de l'unité, alors que les autres entrées représentent des incapacités à remplir les fonctions auxiliaires correspondantes;

– aucune cause immédiate ne peut être déterminée pour l'apparition de l'événement.

Il convient que la nomenclature utilisée dans un arbre de panne soit normalisée pour réduire la confusion et indiquer clairement ce que sont les événements de manière organisée.

La construction réelle d'un arbre de panne suit la logique analytique du flux des événements.

– Le concept de «cause immédiate» nécessite que l'analyste détermine les causes immédiates nécessaires et suffisantes à l'apparition d'une issue de tête. Il convient de noter qu'il ne s'agit pas des causes de base de l'issue de tête ou de l'événement de tête, mais des causes immédiates ou des mécanismes immédiats qui ont conduit à l'événement de tête. Ceux-ci peuvent être les événements (intermédiaires) de niveau inférieur.

– Les causes immédiates, nécessaires et suffisantes pour l'issue de tête sont maintenant traitées comme des événements intermédiaires, et l'analyse se poursuit pour déterminer les causes immédiates (événements d'entrée) nécessaires et suffisantes de ces événements.

– La construction progresse vers le bas de l'arbre de panne, en passant sans cesse du mécanisme au mode et en approchant continuellement le niveau inférieur du mécanisme et des modes, jusqu'au moment où le niveau approprié ou défini de résolution est atteint. Les événements de base individuels ou primaires (initiaux) sont ceux qui représentent les causes individuelles de défaillances ou de pannes potentielles.

7.5.4 Evaluation de l'arbre de panne

7.5.4.1 Investigation et analyse

L'investigation comprend l'étude de la structure de l'arbre de panne, par comparaison à des informations disponibles telles que des schémas, des dessins, des schémas fonctionnels, des commandes de logiciels, l'identification des événements de cause commune et la recherche des branches indépendantes. Il convient que l'investigation permette de dépister des événements de cause commune, mais qu'en aucune façon elle suppose que leur présence est insignifiante. De telles conclusions ne peuvent être tirées qu'après une analyse approfondie par réduction booléenne ou détermination de coupes minimales lorsque les portes statiques sont présentes, les coupes n'existant pas dans les portes dynamiques, à moins de faire une approximation pour ignorer la séquence. Comme la difficulté de l'analyse croît rapidement avec la taille de l'arbre de panne, l'investigation de l'arbre de panne aide l'analyste à savoir quelles branches sont indépendantes du reste de l'arbre et peuvent donc être analysées séparément si nécessaire.

L'analyse d'un arbre de panne suit le flux d'événements et identifie les causes de ces événements vers le bas. L'évaluation de l'arbre de panne peut être logique (qualitative) ou numérique (quantitative) ou les deux. L'analyse d'un arbre de panne quantitatif utilisée dans le développement de produit pour l'amélioration de la fiabilité identifie les facteurs qui contribuent fortement à la probabilité d'apparition de l'événement de tête, et les causes de celles ayant une probabilité d'apparition élevée. A titre d'exemple, si la probabilité de défaillance d'un assemblage d'un système contribue fortement à la probabilité de défaillance du système, la cause est recherchée et une fois identifiée, cette défaillance peut être atténuée. Pour illustrer cet exemple, un facteur contribuant à la probabilité de défaillance d'une alimentation électrique d'un système peut être identifié comme un condensateur sous contrainte excessive. Le remplacement d'un condensateur par un autre condensateur de tension plus élevée diminue considérablement la probabilité de défaillance de l'assemblage et, par la suite, du système.

– operation of the unit does not depend on any supporting function, or all events related to the unit are expressed by a single OR gate having one of the inputs representing a fault of the unit, the remaining inputs representing inability to perform the corresponding support functions;

– no immediate causes can be determined for the occurrence of that event.

The nomenclature used in a fault tree should be standardized so as to minimize confusion and to clearly label and explain what the events are in an organized manner.

The actual construction of a fault tree follows the analytical logic of the flow of events.

– The "immediate cause" concept requires that the analyst determine the immediate necessary and sufficient causes for the occurrence of the top event. It should be noted that these are not the basic causes of the top outcome or top event, but the immediate causes or immediate mechanisms for the top event to occur. These may be the lower level (intermediate) events.

– The immediate, necessary and sufficient causes of the top event are now treated as intermediate events, and the analysis continues to determine their immediate and sufficient causes (input events) to determine their necessary and sufficient causes.

– The construction proceeds down the tree, transferring attention from mechanism to mode, and continually approaching a lower level of mechanism and mode, until ultimately the appropriate or defined level of resolution is reached. The individual basic events or primary (bottom) events are those that represent individual causes of potential failures or faults.

7.5.4 Fault tree evaluation

7.5.4.1 Investigation and analysis

Investigation includes a review of the fault tree structure by comparison with available information such as schematics, drawings, functional diagrams, software commands, identification of common events and a search for independent branches. Investigation should identify common cause events, but should not assume that their presence is benign. Such conclusions can be drawn only after a thorough analysis, using Boolean reduction or determination of minimal cut sets when the static gates are present, as the cut sets do not exist in dynamic gates, unless approximation is applied to ignore sequencing. As the difficulty of the analysis increases rapidly with the size of the fault tree, inspection of the fault tree allows the analyst to identify which branches of the fault tree are independent and can thus be analysed separately if needed.

Analysis of a fault tree follows the flow of events and identifies the causes of those events downward. Fault tree evaluation may be either logical (qualitative) or numerical (quantitative) or both. Analysis of a quantitative fault tree used in product development for reliability improvement identifies the high contributors to the probability of occurrence of the top event, and the causes for those with a high probability of occurrence. As an example, if the probability of failure of an assembly of a system is a high contributor to the probability of system failure, the cause is investigated and once identified, that failure mode can be mitigated. To illustrate this example, a high contributor to the probability of a failure of a system power supply can be identified as an overstressed capacitor. Replacement of that capacitor with another, with higher voltage rating, considerably reduces probability of failure of the assembly and subsequently of the system.

Il convient que les documents fournis à l'appui des analyses soient présentés de sorte que l'on puisse revoir les résultats et incorporer toute modification jugée utile du fait de changements dans la conception, dans les procédures d'exploitation ou dans la meilleure compréhension des caractéristiques physiques de la défaillance. Pour cela, il est nécessaire que la construction puisse être effectuée de façon systématique. Une approche systématique implique la compréhension de deux concepts et leur emploi cohérent. Il s'agit des concepts de «cause immédiate» (événements d'entrée) et d'«unité de base».

Les analyses logiques (qualitatives) et numériques (quantitatives) d'un système ont essentiellement pour but:

– d'identifier les événements ou les pannes qui peuvent provoquer directement une défaillance du système, et contribuent à la probabilité de tels événements; et de cette manière, d'améliorer la sûreté de fonctionnement (fiabilité) d'un système;
– de réduire les pannes pouvant entraîner des conséquences qui peuvent être des dangers potentiels pour la sécurité;
– d'évaluer le niveau de défaillance toléré du système (capacité du système à continuer de fonctionner après la survenue d'un nombre donné de défaillances ou d'événements mineur(e)s conduisant à une défaillance du système);
– d'évaluer les données afin de pouvoir mettre en évidence les composants critiques et les mécanismes de défaillance;
– d'identifier les diagnostics de défaillance des dispositifs, les stratégies de réparation et de maintenance, etc.

Pour évaluer le niveau de défaillance toléré d'un système, il faut déterminer le degré de redondance dans le système et vérifier que des événements communs (événements de cause commune) ne nuisent pas à cette redondance. Bien que l'on n'ait pas besoin d'utiliser de données numériques pour ce type d'analyse, celles-ci sont nécessaires pour trouver les combinaisons d'événements qui ont le plus de chance de se produire et de provoquer une panne du système.

7.5.4.2 Analyse logique

7.5.4.2.1 Généralités

Il existe trois techniques fondamentales pour effectuer l'analyse logique: l'investigation, la réduction booléenne et la détermination de coupes minimales. La base de l'analyse logique est la modélisation, qui fournit une représentation d'arbre de panne d'une structure, fonctionnelle, architecturale, ou une combinaison des deux. Une modélisation correcte signifie une représentation des fonctions ou des composants d'un système, de manière à établir leurs interactions, dépendances, les causes immédiates d'issues défavorables, etc.

7.5.4.2.2 Réduction booléenne

La réduction booléenne peut être utilisée pour évaluer les effets des événements de cause commune (événements identiques apparaissant dans des branches différentes) dans les arbres de panne où l'événement de tête est indépendant de l'instant et de la séquence des événements. Pour procéder à une réduction booléenne, on peut résoudre les équations booléennes se rapportant à l'arbre de panne. La réduction booléenne peut également être utilisée pour identifier les coupes minimales.

7.5.4.2.3 Identification des coupes minimales

Il existe plusieurs méthodes permettant de définir les coupes minimales, mais elles peuvent être difficiles à appliquer à des arbres très ramifiés et, dans ce cas, elles risquent d'être à l'origine de lacunes. C'est pourquoi il existe divers programmes informatiques pour aider l'analyste dans sa tâche.

Analyses should be documented in such a way that results can be reviewed and any changes needed can be incorporated in order to reflect changes in design, operating procedures or improved understanding of the physics of failure. In order that this may be done, a systematic approach to the construction is required. To implement this systematic approach, two concepts have to be understood and used consistently. These are the concepts of "immediate cause" (input events) and of "basic unit".

The primary purposes of logical (qualitative) and numerical (quantitative) analyses of a system can be summarized as follows:

– identification of events or faults which can directly cause a system failure, and contribute to the probability of such events and, in that manner, improve dependability (reliability) of a system;
– mitigation of faults that may be contributors to the outcomes that may be potential safety hazards;
– assessment of fault tolerance of the system (ability to function even after a specified number of lower level failures or events contributing to the occurrence of a system failure have happened);
– assessment of information to locate critical components and failure mechanisms;
– identification of device failure diagnostics, inputs to repair and maintenance strategies, etc.

The assessment of fault tolerance of the system includes a determination of the degree of redundancy in the system and a verification that the redundancy is not impaired through common events. Although the major part of fault tolerance assessment does not require the use of numerical data, such numerical data are required to evaluate which combinations of events causing a system fault are the most likely to occur.

7.5.4.2 Logical analysis

7.5.4.2.1 General

Three basic techniques are used for logical analysis: investigation, Boolean reduction and determination of minimal cut sets. The basis of logical analysis is modelling which provides fault tree representation of a structure, be it functional, architectural, or a mixture of the two. Correct modelling means representing the functions or components of a system in such a way as to establish their interactions, dependencies, immediate causes of unfavourable outcomes, etc.

7.5.4.2.2 Boolean reduction

Boolean reduction can be used for the evaluation of the effects of common events (identical events occurring in different branches) in fault trees where the occurrence of the top event does not depend on timing or sequencing of events. Boolean reduction can be carried out by solving Boolean equations for the fault tree. Boolean reduction can also be used to identify minimal cut sets.

7.5.4.2.3 Identification of minimal cut sets

There are several methods of determining minimal cut sets, but application of larger trees may be difficult and incomplete. For this reason, various computer programs are available to assist the analyst.

Une coupe est un groupe d'événements qui, lorsqu'ils se produisent conjointement, sont à l'origine de l'événement de tête. Une coupe minimale est le plus petit de ces groupes dont tous les événements doivent se produire pour que l'événement de tête ait lieu. Si l'un de ces événements dans une coupe minimale ne survient pas, l'événement de tête ne se produira pas. La définition peut être étendue à des arbres de panne qui dépendent de la séquence des événements. Dans ces cas, la coupe minimale définit le groupe d'événements qui peut être à l'origine de l'événement de tête. Quand l'apparition de l'événement de tête dépend de la séquence des événements d'entrée, cet événement est analysé en utilisant les techniques de Markov qui sont décrites dans la CEI 61165.

7.5.4.3 Analyse numérique

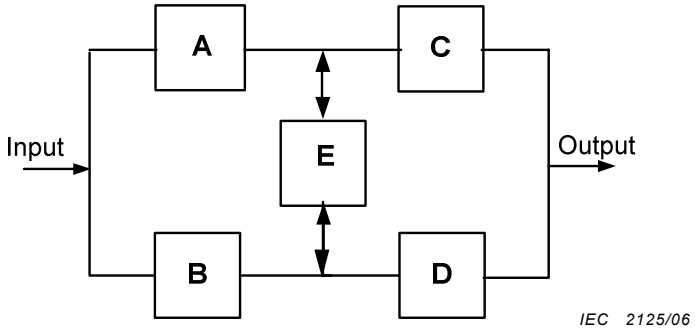
Cette analyse a pour but de parvenir à une estimation quantitative de l'apparition d'un événement de tête ou d'un ensemble choisi d'événements. L'analyse numérique peut également être utilisée comme aide et comme complément lorsqu'on effectue une analyse logique. Pour procéder à l'évaluation numérique d'un arbre de panne, on a besoin de données probabilistes sur les composants. Les techniques de prévision de fiabilité et de disponibilité, les résultats des essais ou les données recueillies en exploitation peuvent servir à déterminer les valeurs quantitatives.

7.5.5 Exemples d'une évaluation simple de matériel utilisant algèbre de Boole et sa représentation par un arbre de panne

7.5.5.1 Exemple de circuit à embranchement

L'arbre de panne avec l'algèbre de Boole peut simplifier l'analyse de fiabilité. Comme le montre cet exemple, les expressions mathématiques très complexes qui devraient être écrites si l'analyse était réalisée en utilisant un bloc-diagramme de fiabilité sont remplacées par l'algèbre de Boole considérablement plus simple. Bien entendu, l'utilisation de l'AAP est particulièrement adaptée aux circuits plus complexes où il existe également une interdépendance entre le logiciel et le matériel, et l'analyse est réalisée en utilisant un des nombreux progiciels.

Un exemple d'utilisation de l'analyse par arbre de panne pour la représentation d'un circuit à embranchement est représenté à la Figure 8.



NOTE Voir les Figures 11 et 12 pour les arbres de panne équivalents.

Figure 8 – Exemple de circuit à embranchement à analyser par arbre de panne

Dans le circuit à embranchement ci-dessus, le signal doit passer de l'entrée **'Input'** à la sortie **'Output'**. Il peut passer par le bloc E dans les deux directions. L'une des façons de réaliser l'analyse serait de modéliser le système selon deux circonstances possibles, tout d'abord en supposant que le bloc E est correct, puis en supposant que le bloc E est incorrect. Dans le premier cas, le signal passerait par les blocs A ou B et C ou D, comme s'il s'agissait de blocs parallèles, respectivement. Dans le cas où le bloc E est incorrect, (condition de défaillance de E) les blocs A et C sont en série, parallèles aux blocs B et D également en série. Cela est représenté par l'équation suivante:

A cut set is a group of events which, when occurring together, cause the top event to happen. A minimal cut set is the smallest such group in which all events have to occur for the top event to occur. If any of the events in a minimal cut set does not occur, the top event will not occur. The definition can be extended to fault trees dependent on sequencing of events. In such instances, the minimal cut set determines the group of events with the potential to cause the top event. When the occurrence of the top event depends on the sequence of the input events, this event is analysed using Markov techniques which are described in IEC 61165.

7.5.4.3 Numerical analysis

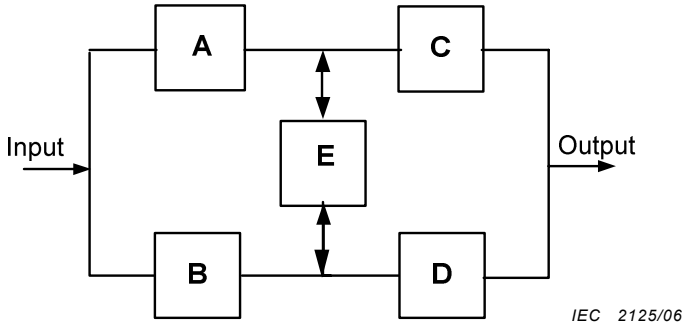
The purpose of numerical analysis is to provide a quantitative assessment of the probability of occurrence of the top event or a selected set of events. Numerical analysis can also be used to support and supplement logical analysis. In order to perform a numerical evaluation of a fault tree, probabilistic data at the component level are required. Reliability and availability prediction techniques, actual test or field use data may be used to establish the quantitative values.

7.5.5 Examples of a simple hardware evaluation using Boolean algebra and its representation by a fault tree

7.5.5.1 Bridge circuit example

Fault tree with Boolean algebra can simplify reliability analysis. As shown in this example, the very complex mathematical expressions that would have to be written if the analysis was done using the reliability block diagram, are substituted by considerably easier Boolean algebra. Understandably, the use of FTA is especially convenient for the more complex circuits where there is also interdependency of software and hardware, and analysis is done using one of many available software packages.

An example of use of the fault tree analysis for representation of a bridge circuit is shown in Figure 8.



NOTE See Figures 11 and 12 for equivalent fault trees.

Figure 8 – Bridge circuit example to be analysed by a fault tree

In the bridge circuit above, the signal has to flow from **Input** to **Output**. It can flow through block E in both directions. One way to perform analysis would be to model the system under two possible circumstances, first assuming that block E is good, and secondly assuming that block E is bad. In the first case, the signal would flow through blocks A or B and C or D, as if they were parallel blocks, respectively. When block E is bad (the condition that E failed), blocks A and C are in series, parallel to blocks B and D also in series. This is represented by the following equation:

$$R_S = (R_A + R_B - R_A \cdot R_B) \cdot (R_C + R_D - R_C \cdot R_D) \cdot R_E + (R_A \cdot R_C + R_B \cdot R_D - R_A \cdot R_B \cdot R_C \cdot R_D) \cdot (1 - R_E) \quad (7)$$

Si: $R_A = 0{,}78$; $R_B = 0{,}30$; $R_C = 0{,}15$; $R_D = 0{,}50$; $R_E = 0{,}40$

alors: $R_S = 0{,}344$

La probabilité de défaillance devient:

$$F_S = 0{,}656$$

La représentation de l'arbre de panne du circuit à embranchement (système) est montrée à la Figure 9.

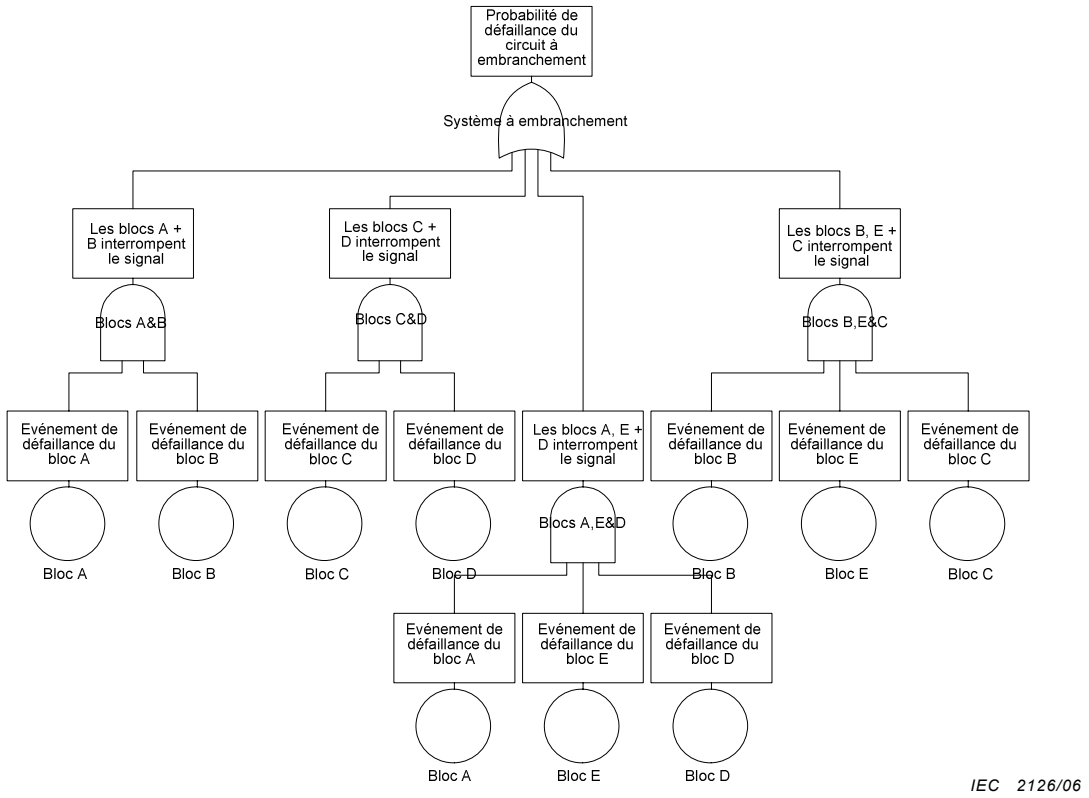


Figure 9 – Représentation de l'arbre de panne du circuit à embranchement

En utilisant l'algèbre de Boole et les coupes minimales (les cheminements qui empêcheraient le fonctionnement du système), le système de la Figure 9 devient le suivant:

Les coupes dans ce système seraient constituées des combinaisons d'événements suivantes de passage du signal d'arrêt:

– blocs A et B ($c_1 = F_a F_b = ab$);
– blocs C et D ($c_2 = cd$);
– blocs A, E et D ($c_3 = aed$);
– blocs B, E et C ($c_4 = bec$).