CHEMICAL ENGINEERING TRANSACTIONS
VOL. 48, 2016

A publication of
AIDIC
The Italian Association
of Chemical Engineering
Online at www.aidic.it/cet

Guest Editors: Eddy de Rademaeker, Peter Schmelzer

ISBN 978-88-95608-39-6; **ISSN** 2283-9216

DOI: 10.3303/CET1648001

Reliability Analysis and Risk Analysis: Integration between Hazop, FMEDA and Fault Tree Analysis for SIL Assessment

Franco Antonello[a], Davide DeDominicis[b], Alessandro Ivaldi, Graziano Fiocca[a] , Loris Tomiato[b]

[a]ARTES S.r.l. Via Battisti 2/A 30035 MIRANO (VE) Italy
[b]ARPAV Dpt Treviso Via S.Barbara 5a 31100 TREVISO Italy
franco.antonello@artes-srl.org

In the field of risk analysis regarding major accidents, the most commonly adopted techniques of analysis and evaluation are the HazOp and Fault Tree, which have various software for the application and available established procedures.

The integration between these two methods is known by the exposure of Lihou and others, but is infrequently applied.

In more recent years methodologies for assessing the level of protection (LOPA - Level Of Protection Analysis) provided by components and instrumentation systems have also been formalized, it's possible through them to determine the SIL (Safety Integrity Level); mainly the technique called FMEDA, further analysis of failure modes, formalized by IEC regulation and most commonly applied especially in the field of process automation. Tools that facilitate the application of these techniques are available, although a specific training is nevertheless required for their use.

Systems reliability is a key element in risk analysis, along with human error, for the evaluation of which various methods are available as well; in general, however, for human error a simplified criterion is often used which combines a generic error probability with the number of chances on which the error may occur.

Here there's a software that provides for the integration of some techniques, allowing a saving of time and also ensuring the congruence between them: by applying HazOp application the fault tree, in graphical and quantified form, is automatically obtained, with the possibility to calculate MCS and define the SIL.

The application of the HazOp is done using a spreadsheet with the help of drop-down menus that can be customized by the user. The selection and input of reliability data is performed using a collection of data systematized in the same form.

Once the worksheet has been filled out and the reliability data have been selected, the program builds the fault trees, calculates combinations of data, provides the Minimal Cut Sets and graphically represents the fault trees that derive from the analysis.

1. Introduction

The software has a double purpose: it is used to identify and assess the risks of accidents on chemical processes, and at the same time can also be used for the evaluation of the reliability of systems or installations, or to identify anomalies that may affect product quality. The described method incorporates in a single software, with the use of a single data input, all the steps typical of risk analysis: the division of the system into nodes for HazOp application, the calculation of the frequencies of TopEvents and Minimal CutSets, and the construction of fault trees and event trees, as well as evaluation of the system SIL.

To ensure proper operation the software requires the application of some conventions in order to limit the discretion of the user, for which the following table provides some concepts related to the HazOp theory.

Please cite this article as: Antonello F., Dedominicis D., Ivaldi A., Fiocca G., Tomiato L., 2016, Reliability analysis and risk analysis:integration between hazop and fault tree analysis, Chemical Engineering Transactions, 48, 1-6 DOI:10.3303/CET1648001

2. General criteria

2.1 Analysis set-up and conventions

When examining a system, process or machinery, it is necessary to first identify the points, called nodes, on which apply the analysis; that is, to which nodes variation in parameters are referred.

A node can consist of a tube, an apparatus or an instrumentation circuit, depending on the level of detail that is to be obtained. For example a tank or a reactor can form a single node or can be analyzed referring to all of its input and output lines; a distillation column can be examined with one or two nodes, because the correlation between top and bottom parameters is more complex, etc.

Likewise, in a system constituted by a regulation instrumental circuit or by a PLC or DCS, the nodes could be defined by sets of components that perform the same function or that share common characteristics.

To be able to share a single data entry across various types of analysis, like for example LOPA, Hazop review or a Process Hazard Analysis, predefined terms are used to identify nodes and parameters on a table-shaped worksheet. These terms are pre-inserted in the application to identify a set of key elements like guiding words and parameters, the events that mark causes, the effects and the safety measures.

2.2 Guide words and parameter

The analysis takes place by considering, for each node, the causes and effects of deviations of operating parameters, such as temperature, pressure, intensity of the signal, etc. To systematize the examination is used to refer to guide words that are dependent on the analyzed system, linking them to the type of applicable variation or deviation identified by a symbol: in case of chemical plants, for example, at least the following guide words are always used:

Table 1: obligatory deviations used in the software

symbol	deviation	parameter
+	higher than expected	temperature pressure flow level
-	lower than expected	temperature pressure flow level
≠	different than expected	composition
><	opposite than expected	flow or stream
NO	complete absence	flow

The software allows the recording of used process parameters in a database, with the possibility to specify further the deviation, for example, specifying "+ FLOW feed or – FLOW water," etc. or " ≠COMPOSITION +air or ≠COMPOSITION -water", so as to describe the event more accurately possible.

2.3 Causes and effects of deviations

For every deviation of the considered parameter, the analysis team (usually led by an expert in risk analysis and composed by process experts, such as process engineer plant manager, instruments technician, etc.) evaluates the possible causes of the event.

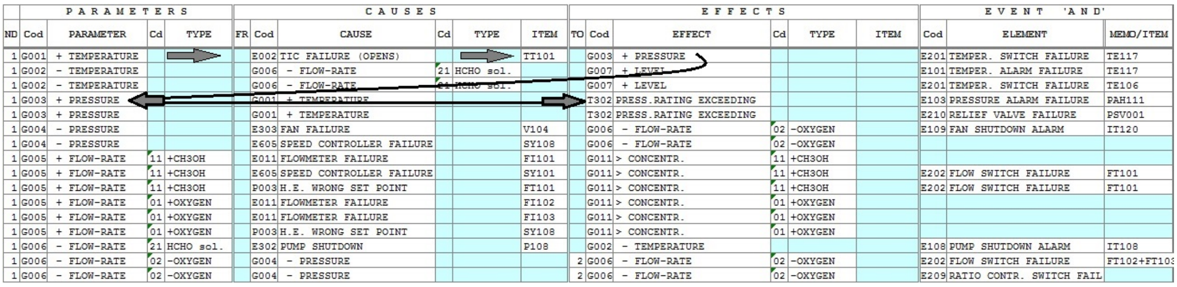
The causes must correspond to elementary events, i.e. failures, anomalies, human errors, ..., which can be associated to an expected frequency. The software includes a database with over 1000 reliability data taken from international databases related to mechanical, instrumental, electronic or human errors which may be automatically associated to the single event on the basis of a choice made by the user, or which can be used by the expert as an aid in the choice of failure rate or error probability.

For each event the user can specify the symbol that distinguishes the considered item, and this will later permit to obtain a list of critical components with the frequency of required maintenance and inspections.

The system includes standard abbreviations such as A.O. (Abnormal Operation), O.F. (Operational Failure), etc. with a series of predefined terms which can anyway be customized by the user.

For each identified cause is described an effect or consequence, which may consist of a deviation of another parameter in the same node or in another node, or the ultimate consequence (Top Event).

In case a sequence of events may involve one or more nodes, the guide words can be used to describe a sequence of effects, each of which will become cause of a further effect, as exemplified in Figure 1.



	PARAMETERS				CAUSES						EFFECTS						EVENT 'AND'		
ND	Cod	PARAMETER	Cd	TYPE	FR	Cod	CAUSE	Cd	TYPE	ITEM	TO	Cod	EFFECT	Cd	TYPE	ITEM	Cod	ELEMENT	MEMO/ITEM
1	G001	+ TEMPERATURE				E002	TIC FAILURE (OPENS)			TT101		G003	+ PRESSURE				E201	TEMPER. SWITCH FAILURE	TE117
1	G002	- TEMPERATURE				G006	- FLOW-RATE	21	HCHO sol.			G007	+ LEVEL				E101	TEMPER. ALARM FAILURE	TE117
1	G002	- TEMPERATURE				G006	- FLOW-RATE	21	HCHO sol.			G007	+ LEVEL				E201	TEMPER. SWITCH FAILURE	TE106
1	G003	+ PRESSURE				G001	+ TEMPERATURE					T302	PRESS.RATING EXCEEDING				E103	PRESSURE ALARM FAILURE	PAH111
1	G003	+ PRESSURE				G001	+ TEMPERATURE					T302	PRESS.RATING EXCEEDING				E210	RELIEF VALVE FAILURE	PSV001
1	G004	- PRESSURE				E303	FAN FAILURE			V104		G006	- FLOW-RATE	02	-OXYGEN		E109	FAN SHUTDOWN ALARM	IT120
1	G004	- PRESSURE				E605	SPEED CONTROLLER FAILURE			SY108		G006	- FLOW-RATE	02	-OXYGEN				
1	G005	+ FLOW-RATE	11	+CH3OH		E011	FLOWMETER FAILURE			FI101		G011	> CONCENTR.	11	+CH3OH				
1	G005	+ FLOW-RATE	11	+CH3OH		E605	SPEED CONTROLLER FAILURE			SY101		G011	> CONCENTR.	11	+CH3OH		E202	FLOW SWITCH FAILURE	FT101
1	G005	+ FLOW-RATE	11	+CH3OH		P003	H.E. WRONG SET POINT			FT101		G011	> CONCENTR.	11	+CH3OH		E202	FLOW SWITCH FAILURE	FT101
1	G005	+ FLOW-RATE	01	+OXYGEN		E011	FLOWMETER FAILURE			FI102		G011	> CONCENTR.	01	+OXYGEN				
1	G005	+ FLOW-RATE	01	+OXYGEN		E011	FLOWMETER FAILURE			FI103		G011	> CONCENTR.	01	+OXYGEN				
1	G005	+ FLOW-RATE	01	+OXYGEN		P003	H.E. WRONG SET POINT			SY108		G011	> CONCENTR.	01	+OXYGEN				
1	G006	- FLOW-RATE	21	HCHO sol.		E302	PUMP SHUTDOWN			P108		G002	- TEMPERATURE				E108	PUMP SHUTDOWN ALARM	IT108
1	G006	- FLOW-RATE	02	-OXYGEN		G004	- PRESSURE				2	G006	- FLOW-RATE	02	-OXYGEN		E202	FLOW SWITCH FAILURE	FT102+FT103
1	G006	- FLOW-RATE	02	-OXYGEN		G004	- PRESSURE				2	G006	- FLOW-RATE	02	-OXYGEN		E209	RATIO CONTR. SWITCH FAIL	

Figure 1: Hazop worksheet

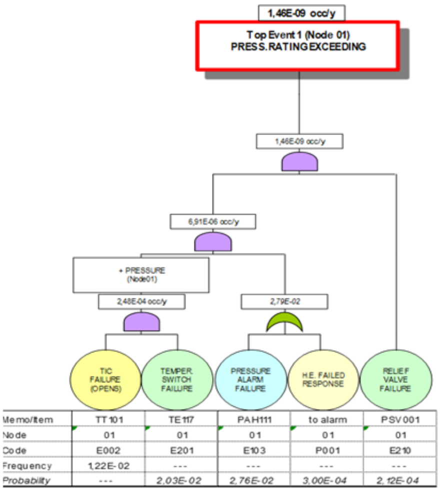
One of the advantages for the user, especially in cases of complex analysis with many causes / effects sequences involving multiple nodes, is the possibility built in the application to carry out an automatic check that there are no repetitions or duplications, reporting the user with possible inconsistencies.

2.4 Safety measures and Top Event

In the sequences of events that originate Top Event (also called final events), next to the causes must be considered the possible presence of elements or components that can prevent the occurrence of unwanted events or through which it is possible to minimize their impact. These elements consist in warning or blocking systems or safety components such as PSV or rupture discs or also of controlling measures and actions entrusted to man or computer systems that are able to timely detect the occurrence of events or faults and prepare appropriate measures of prevention or protection.
These elements are considered or expected as a result of the analysis and it’s possible to assess the likelihood of intervention and ponder the influence they may have towards the final result, that is, the expected frequency of the Top Event.
This analysis is in fact often carried out at the design stage of a system, in order to avoid accidental events with not acceptable frequency of occurrence, and, in a limited resources environment, also serves to check the cost / benefit of different solutions, so as to ensure maximum security with minimum cost.
These elements are not always simple components, but may be also composed of complex systems of which it is possible to assess the reliability and, therefore, the probability of failure.
The software allows this evaluation through the definition of UNAVAILABILITY. In the following, these elements are also defined as "AND Events " (AE).

3. Fault Tree and Minimal Cut Set

Setting the analysis and respecting the conventions described above allows to obtain directly the fault trees from hazop or from another executed analysis. In fact the software, after checking automatically the formal correctness of the input settings, proceeds to graphically draw and calculate the fault trees as in Figure 2.



Memo/Item	TT101	TE117	PAH111	to alarm	PSV001
Node	01	01	01	01	01
Code	E002	E201	E103	P001	E210
Frequency	1,22E-02	---	---	---	---
Probability	---	*2,03E-02*	*2,76E-02*	*3,00E-04*	*2,12E-04*

Figure 2: Fault Tree

To facilitate the processes of control of congruence of the conventions and of calculation and graphical representation of fault trees, the software associates to each event or each component an alphanumeric code that allows to apply the rules of algebra for solving equations descriptive of fault trees and for the calculation of the MCS.

3.1 The solving equations

Conceptually the HazOp can be represented by a set of equations of the type:

$$E_{\lambda} = \sum_{i=1}^{L_{\lambda}} C_i \prod_{j=1}^{M_i} EA_{i,j} \tag{1}$$

Where
Eλ = λ-th effect
Ci = i-th cause of the λ-th effect
EAj,j = j-th event of the i-th cause.
The (1) should be read as: "the Event λ-th takes place by the L causes Ci if for each of them occur Mi concauses EAi, j with an expected frequency equal to the sum of the expected frequencies of the L causes, each multiplied by the probability that occur at the same time the Mi contributing causes."
In other words the summations correspond to OR logic gates, while the multiplications correspond to AND logic gates.
The expression is thus both in terms of qualitative illustration of the phenomenon, and in quantitative terms. Substituting the equations of the Effects to the Causes give general equations of the type:

$$TE_{\mu} = \sum_{i=1}^{L\mu} EE_i \prod_{j=1}^{M_i} \left(\sum_{k=1}^{N_j} EE_{k,j} \prod_{l=1}^{O_k} EA_{l,k} \right)_{i,j} \tag{2}$$

where EEi = i-th elementary event or Ci

Each term in the first sum of the equation (2), is a Minimal Cut Set (MCS), i.e. the contribution of each elementary cause to the primary TopEvent.
It should also be considered that the writing mode adopted does not require a Boolean analysis of the FaultTree. In fact, the elementary events (EE) appear only and always as expected frequency, while safety measures appear always as unavailability.

4. Criteria for calculating reliability

The software has a database with failure rates or error probability referred both to individual components and to circuits or systems as well as to human errors; data are derived from reliability databases commercially available, but can be integrated with specific data obtained or calculated by the user.
The choice of data to be used is carried out at the request of the software once the tests of consistency and completeness are positively completed. The calculation criteria are given below.

4.1 Expected frequency and probability of failure on demand (PFD)

The software is typically used for the estimation of frequencies derived from sequences of events, but may also represent single event resulting from a single cause such as, for example, the rupture of a pipe. Given the variability of the units of the base failure rates available on the market and given the multiplicity of possible situations, it’s used the convention to represent the Top Event with an annual frequency, and the unavailability is provided as probability.
Given:
f = expected frequency [occ/y]
L = pipe length [m]
MT = Mission Time or working time in the year [h/y]
MTBT = Mean Time Between Test [h]
MTTR = Mean Time To Repair [h/occ]
N = occ/year or number of operations for each of which is possible an error
P = probability [-]
PFD = probability of failure on demand [p]
λ = base failure rate [occ/h] or [occ/(h·m)]

$f=\lambda\cdot MT$ or, in case of pipes $f=\lambda\cdot MT\cdot L$ (3)

If the base failure rate is provided in probability (sometimes also it is used to indicate the relationship between the number of unsuccessful operations and the number of requests for intervention)

$$f=p\cdot\frac{MT}{MTTR} \quad (4)$$

For human errors is used to consider the opportunities for error, so

$$f=p\cdot N \quad (5)$$

In case of unavailability or PFD must distinguish between systems on stand-by and systems whose failure is autodetected (such as control loops whose failure automatically causes a deviation of controlled parameter or other parameters, or in the case of stop a pump which results in the lack of flow).
In the case of on stand-by components (typically blocking systems):

$PFD=\left[1-\frac{(1-e^{-\lambda\cdot MTBT})}{\lambda\cdot MTBT}\right]$ which for λ·MTBT<0,1 approximates to $\lambda\frac{MTBT}{2}$ (6)

For events whose failure autodetect:

$$PFD=\frac{\lambda\cdot MT\cdot(MTTR+TR)}{8760} \quad (7)$$

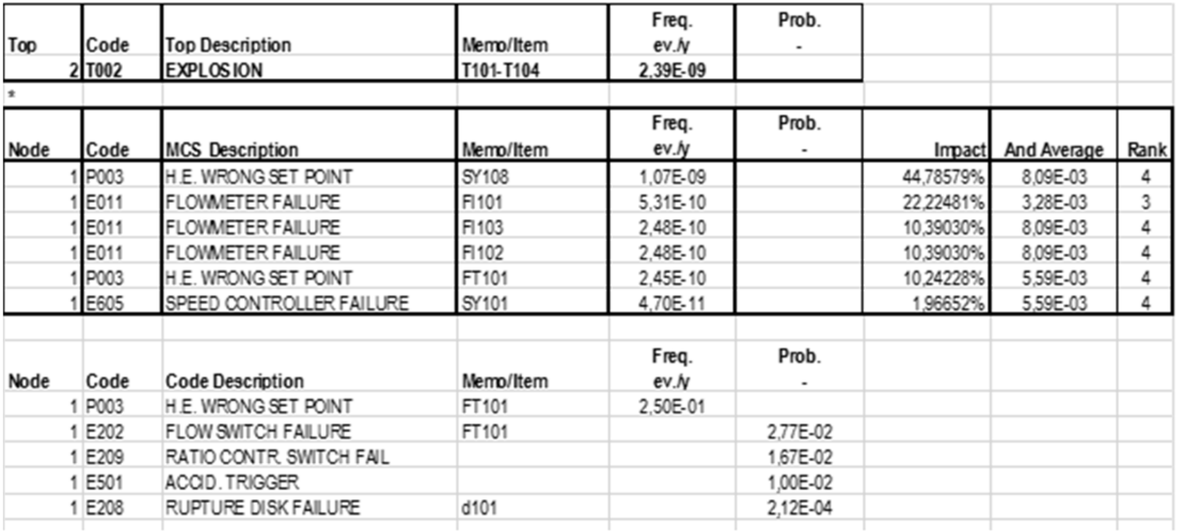
Where can also be considered the time of detection TR (in hours)
In case of redundant systems composed of identical items (no common causes of failure, to be considered separately) that don't auto detect, the calculation is performed by:

$$\mathrm{PFD}=\frac{\mathrm{n}!}{r!\cdot(\mathrm{n}\text{-}\mathrm{r})!}\cdot\frac{(\lambda\cdot MTBT)^{r}}{r+1} \quad (8)$$

Where:
m = number of components required for the operation
n = number of components existing in the system
r = n-m+1

4.2 Minimal Cut Set (MCS)

The software allows to obtain the MCSs for each identified Top Event, by providing a summary of the causes (elementary events) with the percentage contribution of each to the frequency of TOP Event, so as to make explicit the contribution of each event, and provide a useful tool for evaluating cost / benefit and on which elements act on a priority base.
It is also provided the average PFD of the "AND Events " (safety measures), and their number (corresponding to the number of barriers or components that must fail to cause the undesired occurrence). In this way there is also the representation of the security level, i.e. of the barriers provided to stop the sequence of dangerous events. The example of the representation of MCS is reported in Figure 3.



				Freq.	Prob.
Top	Code	Top Description	Memo/Item	ev./y	-
2	T002	EXPLOSION	T101-T104	2,39E-09	

*

				Freq.	Prob.			
Node	Code	MCS Description	Memo/Item	ev./y	-	Impact	And Average	Rank
1	P003	H.E. WRONG SET POINT	SY108	1,07E-09		44,78579%	8,09E-03	4
1	E011	FLOWMETER FAILURE	FI101	5,31E-10		22,22481%	3,28E-03	3
1	E011	FLOWMETER FAILURE	FI103	2,48E-10		10,39030%	8,09E-03	4
1	E011	FLOWMETER FAILURE	FI102	2,48E-10		10,39030%	8,09E-03	4
1	P003	H.E. WRONG SET POINT	FT101	2,45E-10		10,24228%	5,59E-03	4
1	E605	SPEED CONTROLLER FAILURE	SY101	4,70E-11		1,96652%	5,59E-03	4

				Freq.	Prob.
Node	Code	Code Description	Memo/Item	ev./y	-
1	P003	H.E. WRONG SET POINT	FT101	2,50E-01	
1	E202	FLOW SWITCH FAILURE	FT101		2,77E-02
1	E209	RATIO CONTR. SWITCH FAIL			1,67E-02
1	E501	ACCID. TRIGGER			1,00E-02
1	E208	RUPTURE DISK FAILURE	d101		2,12E-04

Figure 3: Minimal Cut Set example

4.3 Event tree

The software include also a scenario analysis using the technique of the event tree, whose origin can be defined separately from hazop or depend from hazop and / or FTA. The reliability data for the event tree valuations are obtained from the software database. The example is provided in Figure 4.

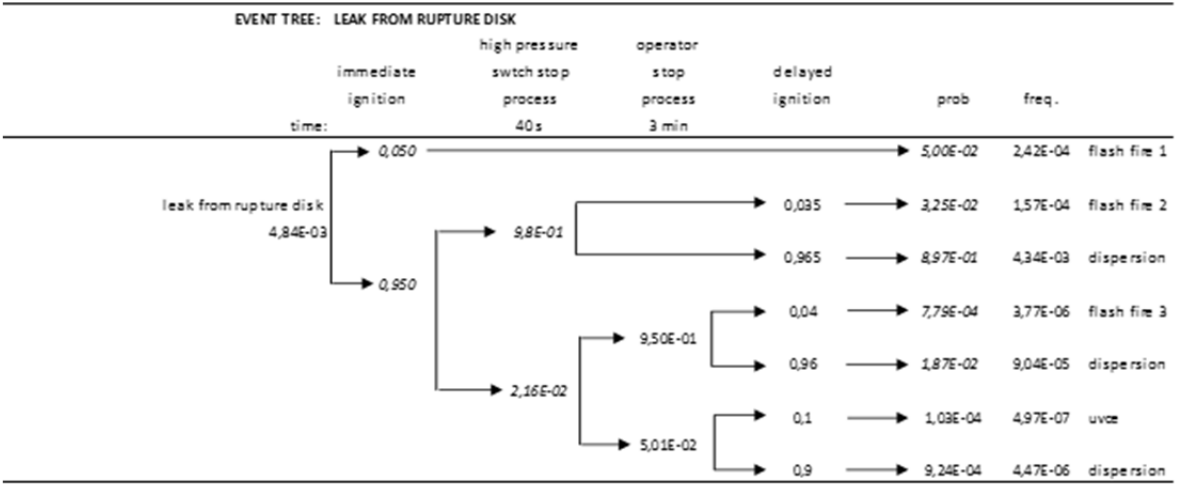


Figure 4: Event tree example.

5. Conclusions

The software allows, through a write-assisted HazOp analysis, to obtain directly the draw of fault trees associated identified Top Event or unwanted occurrences. Using reliability data included in a dedicated database, which can be supplemented and enriched by the user, it is possible to obtain automatically the calculation of expected frequencies or the unavailability of systems by means of the FTA technique, with the evaluation of MCSs associated with each Top Event.

In addition, by applying the analysis to a set of components and conducting the examination in order to promptly identify dangerous failures it is possible to obtain directly the SIL (Safety Integrity Level - EN IEC 62061) or PL (Performance Level - EN ISO 13849-1) that represents the degree of reliability ensured by a set or system with aimed to control, which can be a DCS or PLC.

The integration of different analysis techniques, which are usually carried out in different steps, in a single environment, and specially with a single data entry, is one of the main benefits of the software, which reduces analysis time and costs.

The future development of the software is aimed, in addition to the constant updating of the internal reliability database, to the integration of additional analysis tools in order to be able to compare different techniques on the same system.

Reference

Goble W. et al. , 2003, Failure Mode, Effects and Diagnostic Analysis. Report 02/08-01 Exida <exida.com>

Lihou D.A., 1980, Efficient Use of Operability Studies. Safety Promotion and Loss Prevention in the Process Industries

Lihou D.A. , 1980, Fault Trees from Operability Studies. Safety Promotion and Loss Prevention in the Process Industries

Piccinini N. et al. , 2002, How to avoid the generation of loops in the construction of fault trees. Reliability and Maintainability Symposium Proceeding IEEE, vol. 2.