CHEMICAL ENGINEERING TRANSACTIONS
VOL. 53, 2016
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Valerio Cozzani, Eddy De Rademaeker, Davide Manca

ISBN 978-88-95608-44-0; **ISSN** 2283-9216
DOI: 10.3303/CET1653019

Comparison of Classical and "Cause Consequence Diagrams" Recursive Operability Analysis: the T2 Laboratories Accident

Sergio Contini[a], Paolo Mario Contini[a], Vincenzo Torretta[b], Carlo Sala Cattaneo[c], Massimo Raboni[d], Sabrina Copelli*[a]

[a] Università degli Studi dell'Insubria - Dip. di Scienza e Alta Tecnologia, Via G.B. Vico 46 - 21100 Varese – Italy
[b] Università degli Studi dell'Insubria - Dip. di Biotecnologie e Scienze della Vita, Via G.B. Vico 46 - 21100 Varese – Italy
[c] Artyll – Società Lombarda di Ingegneria, Via Poerio 10 – 20025 Legnano (MI) – Italy
[d] Università LIUC – Cattaneo, Scuola di Ingegneria Industriale, Corso Matteotti 22 - 21053 Castellanza (VA) - Italy
sabrina.copelli@uninsubria.it

On December 19, 2007, a powerful explosion and fire killed four employees and destroyed T2 Laboratories, Inc., a chemical manufacturer in Jacksonville, Florida. In the accident 32 people were injured, including 4 employees and 28 members of the public who were working in the surroundings. Debris was found up to one mile away, and the explosion damaged buildings within one quarter mile of the facility. After the accident, the question which arose was: could an even simplified risk analysis prevent such a tragedy?
It is widely accepted that performing a detailed Quantitative Risk Analysis (QRA) is a complex and time consuming task because of all the steps which must be carried out: 1) hazards identification; 2) frequency estimation; 3) accident consequence evaluation; 4) individual and societal risk calculation.
Specifically, Hazard Identification (HI) and Frequency Estimation (FE) represent two fundamental activities since: 1) not identified hazards can remain hidden until the occurrence of the related accidents; 2) the probabilistically quantification of the hazardous plant states frequencies, e.g. through Fault Tree Analysis (FTA), helps to support decisions making on risk reduction. Particularly, since generating FTs is a time consuming task, the Recursive Operability Analysis (ROA) has been ideated. ROA, both in its classical and revised version (called Recursive Operability Analysis – Cause Consequence Diagrams, ROA-CCD), is based on a procedure which allows collecting plant perturbations data in a structured way.
The aim of this work is to apply both the classical and the new ROA-CCD analysis on the T2 Laboratories chemical plant (with particular reference to the reactor node) in order to identify all the possible top events and states of plant unavailability. In this way, it has been evidenced that even a simplified but reliable risk analysis could have been unearthed clearly all plant criticalities. Moreover, the results concerning the risk quantification have been critically analyzed showing that ROA-CCD achieves the same results, in terms of Minimal Cut Sets, of its classical version with a lower effort. This goal is fulfilled by avoiding the unnecessary subdivision of the plant into nodes prior to perform the analysis; in this way, considering only the process variables related to the "key piece of equipment" (in this case, the reactor), records in the ROA format are drastically reduced.

1. Introduction

Recently, the problem of the risk associated with chemical plants has strongly increased whilst, simultaneously, the threshold of the population risk acceptability has decreased. In order to face such a criticality, both stakeholders and competent authorities have developed a series of methodologies aimed at managing risk prevention and protection (Tixier et al., 2002).
Specifically, in order to prevent major accidents, a Risk Assessment (RA), defined as "a process, which includes both qualitative and quantitative determination of risks and their social evaluation" (Khan and Abbasi, 2001), prior of the realization of a new industrial site has been made mandatory. Unfortunately, a forward-looking risk analysis requires strong efforts since both an exhaustive identification of potential hazards and an

Please cite this article as: Contini S., Contini P.M., Torretta V., Sala Cattaneo C., Raboni M., Copelli S., 2016, Comparison of classical and "cause consequence diagrams" recursive operability analysis: the t2 laboratories accident, Chemical Engineering Transactions, 53, 109-114
DOI: 10.3303/CET1653019

assessment of the potential damages affecting human, environmental and equipment targets must be performed in order to propose effective mitigation actions.
In a recent review, Tixier (Tixier et al., 2002) has identified at least sixty risk analysis methodologies capable of analyzing and managing different safety aspects linked to an industrial site. As a common point, all these methodologies include up to three main phases:
- identification of hazards and accidental scenarios (in terms of cause – consequence analysis). Such a phase is based on the industrial site description in terms of performed activities, managed products and installed equipment. Moreover, it comprises the evaluation of the magnitude of the incidents outcomes.
- evaluation of the risk. This phase enables to take into account the impacts of the previously found consequences of incidental scenarios on the industrial site or on its vicinity.
- hierarchical ordering of the results obtained through the two previous phases. This phase is carried out in order to plan some mitigation interventions for the highest detected risks.
Particularly, on one side, the phase of Hazard Identification (HI) is essential because it establishes the bases of the risk analysis by providing input data for the successive Risk Evaluation (RE) phase; on the other side, the phase of RE, realized through either a deterministic (evaluation of damage consequences) or a probabilistic (evaluation of accident frequency, that is, Frequency Estimation - FE) approach (of course a combined approach is always possible), is fundamental for the hierarchical ordering phase, where modifications or corrective actions on the most severe risks are effectively implemented.
Historically, for chemical plants, the phase of HI has been mainly performed using a Hazard and Operability (HazOp) analysis, sometimes complemented by a Failure Mode and Effects Criticality Analysis (FMECA). The HazOp study is used to identify hazardous scenarios (the so-called Top Events, TEs) and operability problems by using logical sequences of cause-deviation-consequence of process parameters. Unfortunately, because of its structure, it is not capable of either ranking properly the effects of failures of individual components or studying the relative effectiveness of the proposed corrective actions, even if it is possible to insert, in the standard HazOp modules, a criticality analysis of the effects of failures (Contini et al., 2015). Particularly, to face in a more structured way the criticality evaluation problem, FMECA is often used for integrating properly the HazOp study. Since, the HazOp analysis remains a complex and lengthy hazard identification method, some attempts to provide suitable software tools for HazOp “quasi-automatic” compilation have been done (Khan and Abbasi, 1997, 2000). But, despite of these efforts, the results of the analysis remained too poorly structured to be used for the successive evaluation phase, particularly for the part related to the FE that, commonly, it is carried out using Fault Trees Analysis (FTA). In order to face such a problem, the Recursive Operability Analysis (ROA) has been developed in the ‘80s by Snamprogetti (ENI group) and then, it has been improved and diffused by the research group led by Norberto Piccinini (Piccinini et al., 1994). ROA uses a format which expresses, in a structured way, the relationship between the variations of process variables and their causes and consequences, also highlighting the logical link with protection systems (both automatic and manual). Therefore, it can be said that ROA modules have been realized precisely to facilitate the automatic construction of fault trees, according to a simple and systematic procedure (Piccinini and Demichela, 2008). Recently, such a technique has been revised and a more compact (precisely, in terms of required efforts) procedure, called ROA - Cause Consequence Diagrams (ROA-CCD), has been ideated (for a comparison of the two techniques, see paragraph 2) (Contini et al., 2015).
The main aims of this work have been to demonstrate that: 1) the classical ROA and the ROA-CCD analysis are perfectly equivalent in terms of results provided for the frequency estimation of a given top event (that is, they calculate the same list of Minimal Cut Sets – MCS); 2) whether applied to a chemical plant where an accident has occurred, they are able to identify (in the aftermath) and insert the occurred accident cause – consequence path among the identified Top Events, showing that even a simplified but complete risk analysis (performed previously) is able to identify the main criticality of a plant, providing useful information for the implementation of the required mitigation actions (during the plant design phase). Particularly, for what concern the second aim, the relevant case study of the T2 Laboratories accident has been referred to since it represents a key example of both incomplete kinetic study of a process and deficient process control design. The results obtained by the ROA and the ROA-CCD procedure, which have been carried out by two independent groups of the authors, are in perfect agreement with the detailed reconstruction provided by the report of the Chemical Safety Board (CSB, 2009), which investigated the accident in 2008.

2. Description of the Classical and CCD ROA

In the following, a comparison between Classical and CCD ROA will be briefly presented. A more detailed description is beyond the aim of this work but it can be found elsewhere (Contini et al., 2015).
Starting from the comparison between the classical HazOp format (usually employed for the HI phase) with that of the ROA, it can be noticed that the information contained in the first three columns of the standard

HazOp module (that is, guide words, process variables and deviations) have been condensed in only one column. Moreover, information required on protections are more detailed and split up between optical/acoustic alerts (able to activate the action of the operator) and automatic protections (such as bursting discs, relief valves, interlocks, etc..). Finally, a last column, which contains the progressive number of the events (that is, the Top Events) for which the team decides that the consequences are such as to require the quantification of probability of the associated risk, has been inserted.
From the information contained in a single row of a ROA module, a graphical representation of the relationships between process variables (or events), called Incidental Sequences Diagram (ISD), can be directly derived in order to verify the completeness and correctness of the analysis, before moving on to the completion (analyzing the protection systems) and the analysis of the fault trees (FTs). Particularly, a FT corresponding to a single TE is obtained by direct combination of the ISDs derived for each row of the ROA module which is linked to it.
Given its simplicity, the classical ROA has been widely used, in the last thirty years, to analyze chemical plants. But, recently, some criticalities have been underlined so that a revised version of this technique has been proposed. Such a new procedure, called ROA – Cause Consequences Diagram (ROA-CCD), exhibits some main differences with respect to the classical ROA, that they can be summarized in the following: 1) the new module allows registering consequences not only due to failure of protective functions, but also to their correct intervention; this additional information can be then used to determine a probabilistic contribution to plant unavailability; 2) human errors can be modeled in a simpler and more effective way with respect to previous efforts (Colombo and Demichela, 2008), since it has been inserted a column where it is specified the physical component on which the operator can/must act to realize the protection action; 3) the content of a single row of the ROA format is represented in the form of a Cause Consequence Diagram (CCD), instead of an ISD, from which fault trees can be easily extracted to quantify both top events accident frequencies and plant shut down frequencies for unavailability calculation; 4) the analysis of the spurious failure of the protective systems is performed using a FMECA-like format in order to better explicit the contribution of the single components to plant unavailability; and, finally, 5) ROA-CCD does not requires the preliminary identification of nodes on which the causes and consequences of process variables deviations are examined, leading to a much lower number of nodes to be examined. Indeed, nodes are generally associated only to the main plant components (e.g. separators, vessels,…) and not to their connections. This last feature is of particular importance since the efforts required for the analysis are strongly reduced, making ROA-CCD cheaper and easier than its classical version. Anyway, as some nodes are omitted in the ROA-CCD procedure, it is necessary to prove that they are not strictly necessary for the computation of the occurrence frequencies of all TEs and contributions to plant unavailability. In this project the two procedures (ROA and ROA-CCD), implemented independently (that is, by two different working teams), allowed generating fault trees exhibit the same list of Minimal Cut Sets.

3. Description of the T2 Laboratories Plant and the Accident

T2 Laboratories Inc. was a small privately-owned corporation located in Jacksonville, Florida, which began operations in 1996. Mainly, T2 blended and sold solvents for printing industry but, starting from 2004, it has started to produce Methylcyclopentadienyl manganese tricarbonyl (MCMT), an organomanganese compound used as an octane-increasing gasoline additive. Such a compound is synthesized through a three steps recipe: in the first step (called metalation), molten metallic sodium was reacted with methylcyclopentadiene (MCPD) in the presence of a diethylene glycol dimethyl ether (diglyme) to form sodium methylcyclopentadiene and hydrogen (gas). This was accomplished by adding metallic sodium to a mixture of MCPD dimer and diglyme, then heating the mixture (CSB, 2009). The heating operation melted the sodium and split the MCPD dimer molecules into two MCPD molecules that reacted with the sodium. T2 vented the hydrogen gas produced by this step to the atmosphere. In the second step (called substitution), T2 added manganese chloride (dry powder) to the reactor. The manganese chloride reacted with the sodium methylcyclopentadiene in the reactor to form manganese dimethylcyclopentadiene and sodium chloride. In the final step (called carbonylation), T2 added carbon monoxide gas to the bottom of the reactor, bubbling the gas through the manganese dimethylcyclopentadiene under pressure. In this step, one of the methylcyclopentadiene molecules on each manganese dimethylcyclopentadiene molecule was replaced with three carbon monoxide molecules, forming the MCMT.
The MCMT dedicated plant was very simple; particularly, it consisted of a jacketed reactor also equipped with a warming internal coil. Figure 1 reports a sketch of the plant, also showing the control systems available at that time. As it can be seen, the reactor had got: two automatic liquid loading circuits (MCPD and diglyme, controlled by FIC-01 and FIC-02); a manhole for the manual addition of the solids (Na); a temperature controller circuit (TIC-04) that, through the measure of the internal reactor temperature (TT-03 and (TT-04),

activates or deactivates the heating (internal coil, fluid: oil, V-04) or the cooling (external jacket, fluid: water, V-03) system according to pre-determined set point values; a pressure control circuit (that regulates the pressure inside the reactor by relieving directly into the atmosphere, PIC-10) equipped with an emergency relief system (BD-10): a bursting disc set to 400 psig. All control operations are automatic but the operator can always act on specific components to make required instructions.
It is important to notice that the refrigeration action is particularly critical, since cool water is introduced into the jacket and, then, it is evaporated to remove the reaction heat and vented directly into the atmosphere. Moreover, only a high temperature alert (TAH-04) and a high pressure alert (PAH-10) have been installed.

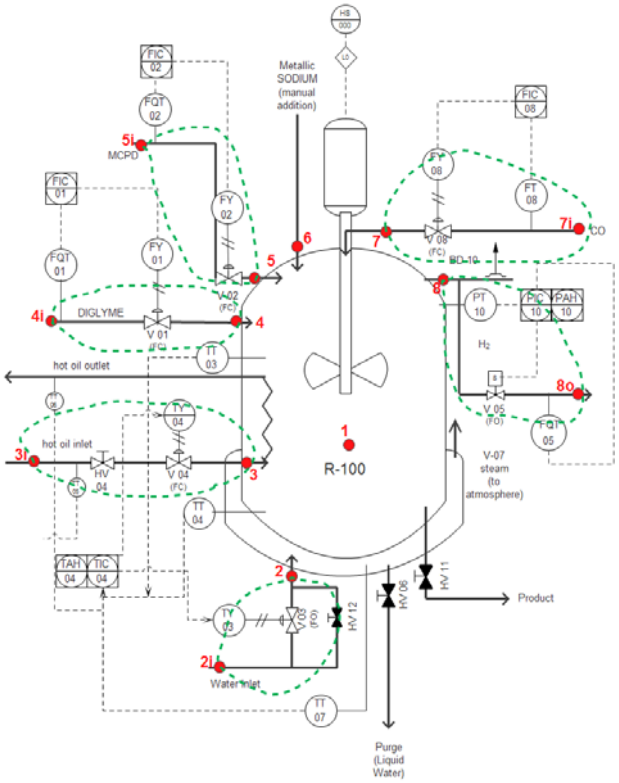

Figure 1: Simplified P&ID of the reactor dedicated to the production of MCMT. Nodes for ROA have been added.

The cause – consequence path leading to the accident at T2 Laboratories was very simple: during the run of the 175° batch of MCMT, the process operator reported a cooling problem and request the intervention of one of the owners. As one of the owners approached the control room, the reactor burst and its contents exploded, killing the owner and the process operator in the control room and two outside operators who were exiting the reactor area. The CSB, which investigated the accident, found that a runaway exothermic reaction had occurred during the first (metalation) step of the MCMT process. In order to determine the most likely failure scenario, the CSB tested the T2 batch recipe using a VRSP apparatus. As a conclusion, an insufficient cooling during the process resulted in a runaway reaction which led to an uncontrollable pressure and temperature rise in the reactor. The pressure burst the rupture disk and, then, the reactor itself; the reactor's contents (hydrogen) ignited, creating an explosion equivalent to 1,400 pounds of TNT. The CSB identified the following root cause: T2 did not recognize the runaway reaction hazard associated with the MCMT it was producing. Moreover, it identified the following contributing causes: 1) the cooling system employed by T2 was susceptible to single-point failures due to a lack of design redundancy; 2) the MCMT reactor relief system was incapable of relieving the pressure from a runaway reaction (since it has been wrongly designed).

4. Results

As previously stated, the authors have been divided into two independent groups in order to perform both classical ROA and ROA-CCD on the T2 plant sketched in Figure 1.

Before starting with the analysis, it has been necessary to adopt some assumptions because of the unavailability of the complete P&ID of the reactor system, namely: 1) availability of support systems (e.g., water, electric energy, air supply); 2) availability of input substances (MCPD, Diglyme, Na, CO); and, 3) availability of oil in the heating system. Then, the systematical compiling of the ROA modules has been carried out according to the procedure detailed in Contini et al. (2015).
The hazard identification performed according to both classical ROA and ROA-CCD methodologies has given the same sequences of events leading to the physical explosion of the reactor and the subsequent ignition of the flammable mixture released in the atmosphere, which is the main top event arising from the analyses. However, if the classical ROA is compared with its new version, ROA-CCD has been found much faster to be carried out, also requiring a less number of records (8 for ROA-CCD and 16 for classical ROA).
The fault trees based on the content of the results arisen from both ROA and ROA-CCD, although graphically different, were logically equivalent: that is, they gave the same list of Minimal Cut Sets. For the sake of simplicity, only the Cause Consequence Diagram and the Fault Tree for the TE = “Reactor explosion” (derived from the ROA-CCD) have been reported in Figure 2.

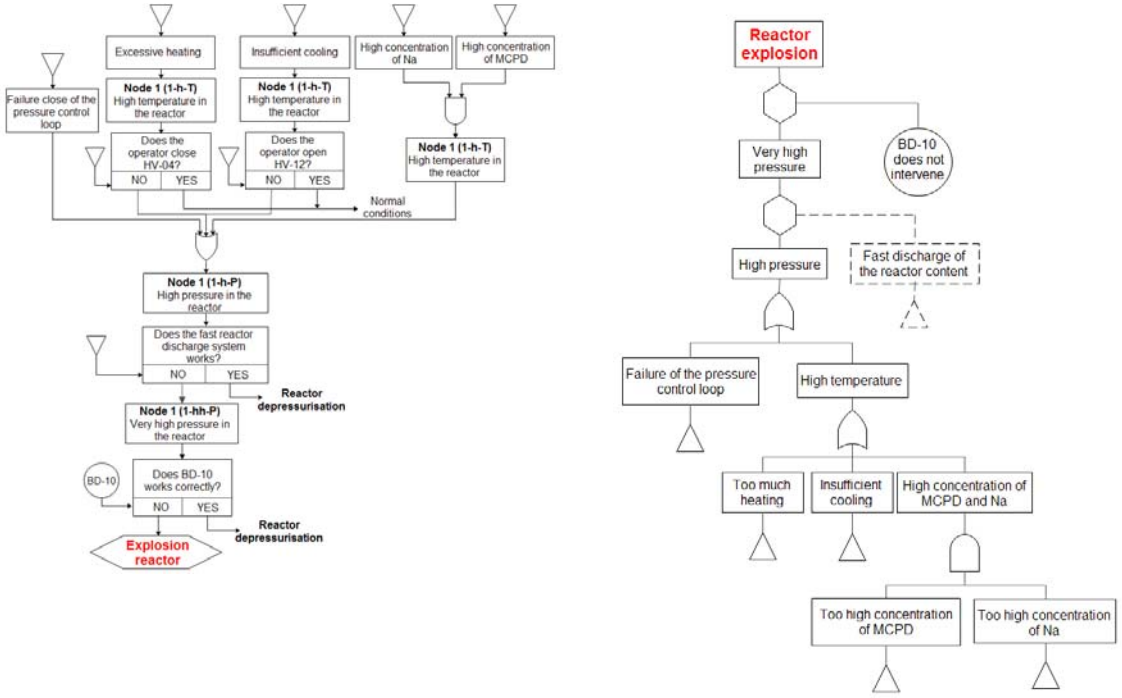

Figure 2: CCD (a) and Fault tree (b) for the TE “Reactor explosion”, derived by a ROA-CCD. Sub-trees are indicated as white triangles.

Of course, concerning the FT, given the complexity of the sub-trees (indicated in the figure as triangles), only the global structure has been depicted. The analysis of the “Reactor explosion” fault tree has provided the results shown in Table 1. Particularly, the analysis has been performed by calculating the Expected Number of Failures (ENF), which represents a good unreliability upper bound. The result of 1.28e-5 stands for the probability of explosion during the run of a single batch.

Table 1: Results of the fault tree analysis for the Top Event “Reactor explosion”

Top Event	ENF (single batch)	Number of MCS	Relative importance	
			Criticality index	Structural index
Explosion	1.28e-5	37 (2 – 5)	BD10 PIC10, FQT05 PT10, V05	BD10 PIC10, FQT05, PT10, V05
Explosion + fast discharge	7.64e-10	72 (3 – 7)	BD10, V11 PIC10, FQT05 PT10 V05	BD10 V11 PIC11, PT11 PIC10, FQT05, PT10, V05

Could this value be acceptable? The answer may be negative since: 1) generally the value of the individual acceptable risk is considered equal to 1.00e-6; and 2) this concerns only one batch.
Hence taking into account the fact that in one-year time N batches are carried out (the real value for T2 batches has not been reported anywhere), the probability of having an explosion can be roughly calculated by the ENF multiplied by N. Of course this is valid only if the charged operators, whenever starting a new batch, perform a complete check of the working condition of all components.
By looking at the other results, the number of MCS is 37 of order ranging between 2 and 5. Particularly, two importance indexes have been considered in the analysis of the MCS, that are: 1) the Criticality index, which gives the percentage variation of the Top Event for a given variation of the component failure probability; and, 2) the Structural index, where the importance of a component depends on its location in the set of MCS; hence this index does not consider the failure probability. Observing Table 1, it can be seen that the most important items (i.e. related to the relatively weak system functions) are the rupture disk and the pressure control system components. In the “importance of the components” columns, components are ranked in decreasing order; components on the same line have comparable importance.
Based on the above importance indexes and recognizing the fact that the system is protected against the explosion only by a rupture disk (BD-10), as a proposed mitigation action, a new safety function, that is the fast discharge of the reactor content in a dedicated quench pool, has been added (in fault tree reported in Figure 2, this new safety system has been represented by dotted lines). The results of the analysis of the new fault tree are also provided in Table 1. As it is possible to note, the reduction of the ENF is very significant (7.64e-10!); the number of MCS has increased from 37 to 72, of order ranging between 3 and 7.

5. Conclusions

In this work it has been demonstrated that even a simple but reliable Risk Analysis can underline all the main criticalities of a plant, making its omission an unjustified dangerous way to save money when a new plant is realized. In this case, the ROA-CCD methodology has been employed to perform the RA of the T2 laboratories plant (with particular reference to the reactor node). Results arising from such an analysis (which is very low time consuming) has been compared with those of a more detailed one, the classical ROA, demonstrating that the two methodologies provide the same list of MCS: this means that they are logically equivalent (even if the structure of the related Fault Trees is different). Moreover, on the basis of the ROA-CCD, it has been possible to propose mitigation actions (such as the fast discharge of the reacting mixture when it is in runaway conditions) simply by looking at the structure of the FT corresponding to the analyzed TE.

References

Colombo S., Demichela M., 2008, The systematic integration of Human Factors into safety analyses: an integrated engineering approach, Reliability Engineering & System Safety 93, 1911-1921.

Contini P. M., Contini S., Copelli S., Rota R., Demichela M., 2015, Document From HazOp study to automatic construction of cause consequence diagrams for frequency calculation of hazardous plant states, Safety and Reliability of Complex Engineered Systems - Proceedings of the 25th European Safety and Reliability Conference, ESREL 2015, 347-355.

CSB (U.S. Chemical Safety Board), 2009, Runaway: Explosion at T2 Laboratories report < http://www.csb.gov/videos/runaway-explosion-at-t2-laboratories/> accessed 15.03.2016

Khan F. I., Abbasi S. A., 1997, TOPHAZOP: a knowledge-based software tool for conducting HAZOP in a rapid, efficient yet inexpensive manner, Journal of Loss Prevention in the Process Industries 10, 333-343.

Khan F. I., Abbasi S. A., 2000, Towards automation of HAZOP with a new tool EXPERTOP, Environmental Modelling & Software 15, 67-77.

Khan F. I., Abbasi S. A., 2001, Risk analysis of a typical chemical industry using ORA procedure, Journal of Loss Prevention in the Process Industries 14, 43-59.

Piccinini N., Ciarambino I., Scarrone M., 1994. Probabilistic analysis of transient events by an event tree directly extracted from operability analysis. Journal of Loss Prevention in the Process Industries 7, 23-32.

Piccinini N., Demichela M., 2008, Risk based decision-making in plant design, Canadian Journal Of Chemical Engineering 86, 316-322.

Tixier J., Dusserre G., Salvi O., Gaston D., 2002, Review of 62 risk analysis methodologies of industrial plants, Journal of Loss Prevention in the Process Industries 15, 291-303.