CNEA (CAUSAL NETWORK EVENT ANALYSIS): PROPOSAL OF A RISK ANALYSIS TECHNIQUE

Luís Fernando Peres Calil, calil@emc.ufsc.br
Acires Dias, acires@emc.ufsc.br
Centro de Engenharia da Mobilidade (CEM) / Universidade Federal de Santa Catarina (UFSC)
Rua Paulo Malschitzki, 10 - Campus universitário Bom Retiro (UNIVILLE), 89219-710 Joinville / SC

Abstract. *This paper presents a new risk analysis technique called CNEA (causal network event analysis), which is being developed to meet the needs of users in safety and reliability management - or even in continuity management. The technique consists of a causal network that allows a visual analysis of a particular event (an incident, for instance), improving the representation of the linkage between failures. With that, consequently, the annalist has a more detailed view of possibles measures to prevent the occurrence of the central event and / or mitigate their effects. Was observed, during the applications, that CNEA fits perfectly in both modeling of faults in equipment and in procedures for operation / maintenance. Additionally, it was possible to perceive an improvement in the interaction with other failure analysis techniques – such as failure modes and effects analysis (FMEA), fault tree analysis (FTA) and bayesian networks.*

Keywords*: Risk analysis, CNEA, FMEA, FTA, Bayesian network.*

1. INTRODUCTION

During a risk analysis, either to improve security or to improve equipment reliability and processes continuity, techniques are used to structure and organize information, such as FMEA (failure mode and effect analysis), FTA (fault tree analysis), ETA (event tree analysis), among others. The emphasis on CNEA technique is due to the need to integrate outcomes in order to identify more clearly the causal chains of events of failure (an incident, for instance).

Thus, in CNEA (causal network event analysis) the event of study is highlighted at the centre of the diagram, showing its causes on the left and its effects on the right. Links characterize the causal chains, and it is possible to include barriers on these links between causes, incident and effects – as presented in sections 3 and 4.

Note that, this approach of present the event of analysis on the centre, its causes and its effects in the same diagram is also adopted by other techniques, especially by the BTA (bow-tie analysis). The BTA is seen as an evolution of the cause and consequence diagrams of the 70's and barriers diagrams of the 80's. Currently, this technique is used in several areas, such as: Trbojevic (2001) in the management of shipping and other port operations; Ramzan (2006) in risk management at nuclear power plants; Iannacchione, Tadolini and Esterhuizen (2007) in mitigating risk of structural instability and fires in mines; Trbojevic (2004) to analyse passenger train derailment; the ARAMIS project (Accidental Risk Assessment Methodology for Industries), which aims to develop a methodology for risk assessment (Delvosalle et al. 2006), among others.

However, the BTA summarize a list of causes and consequences, but it does not structure them in a network and do not allow to use barrier as a pivotal event of scenarios – which will be detailed in Section 5.2 of this article. These aspects, in addition to helping the iteration of others techniques, are important for modelling an incident (what is briefly discussed in Section 2), which is crucial to risk analysis and subsequent communication.

The need to develop a technique that is more akin to risk analysis has emerged in research activities at Post-graduate Program of the Department of Mechanical Engineering, Universidade Federal de Santa Catarina (UFSC), prominently in the project that analysed the risk of loss of SF_6 (sulfur hexafluoride) in high voltage circuit breakers (Calil, 2009). One of the outcomes was the publication of the research methodology used in the project in a book (Dias et al., 2011), which is the main reference of this article.

2. INCIDENT MODELING

Incidents can be represented by a number of models. The model used in this paper is the Mosleh and Dias (2003) one, shown in Figure 1, in which the incident is the result of a hazard condition coupled with a triggering event (or event triggers), crossing the barriers. This sequence of events is often called the causal chain.

In order to reduce the probability of occurrence of an incident, or even mitigate its consequences, we implement barriers along the causal chain. These may be physical barriers, procedures, manuals, education, training, motivation or thing to interfere in the causal chain by avoiding the incident or mitigating its consequences.

A maintenance procedure can work for a system that does not go down, or does not evolve into a hazard condition. A wall-fire is, for instance, a physical barrier used to mitigate the incident and intended to keep the fire in a restrict area, which minimizes the consequences of that incident.

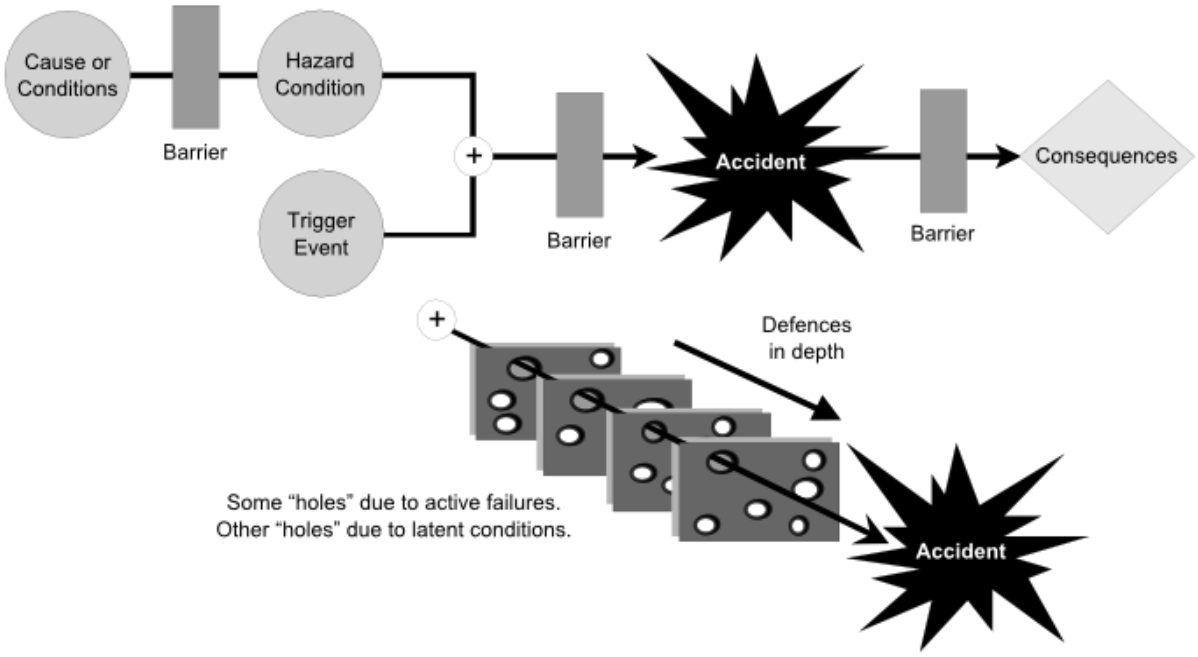


Figure 1. Causal chain of an incident and its trajectory through barriers.
Adapted from Mosleh and Dias (2003) and Reason (1997).

However, barriers are not perfect and their "holes" – either by an active failure, or by a latent condition – may allow the incident to occur, as is depicted in the bottom of Figure 1. In order to reduce the risk of the incident or mitigate its consequences, we can implement more then one barrier, which is called "defences in depth". This model is specially important to guide the risk analysis. It is used to guide researches on methodologies, analysis techniques, situations already studied, lessons learned, etc. In short, the cause or condition of Figure 1 is the one who guides to the survey of all hazards of the technical system under analysis. Moreover, it is assumed that every technical system has its own hazards. Then the barrier that lies after the cause or condition aims not to leave the danger to become the hazard condition. Not every hazard condition becomes incident. However, the hazard condition when combined with the trigger event can result in an incident, if there are no barriers to prevent this risk – that was evident because of the combination: hazard condition plus trigger event. What is a trigger event, so? It is an event that can trigger hazard condition for potentiating the risk of the incident. Trigger events are, for example, of atmospheric nature, lack of training, lack of procedure, lack of quality in operations and maintenance, among others.

Once the model of the causal chain has become suitable for risk analysis, the CNEA to be akin to the causal analysis, making easier the analysis and synthesis of results derived from techniques that typically focus on specific aspects of failure events.

3. ASPECTS ABOUT CNEA

The CNEA technique is used for analysis of events (e.g., incidents), causes, effects and barriers that can be implement to reduce the chance of causes trigger the central event, or mitigate its effects – as is present in Figure 2. In Table 1, in its turn, presents the syntax that was established in order to structure the representation of the technique in a very simplified way, to facilitate understanding and use.

In Figure 2, the incident under analysis may occur in result of either Cause 4 or Cause 3, and the latter happening due to Cause 1 or 2. In the proposed syntax, existing barriers, such as that aims to prevent the occurrence of the incident due to Cause 3 (or at least reduce the likelihood) are shown in white, and proposed barriers are highlighted in grey. With regard to the effects, it is also possible to include intermediaries ones in its scenarios, such as Effect 3. Stands out even the possibility of doing a ramification on the barriers. These ramifications (which are pivotal events) allows modelling scenarios that the barrier was effective or not – in Figure 2, the Effect 2 will occur when the Proposed Barrier 2 is effective, or the Effect 1, when not.

Note that the CNEA is akin to models of representation of incidents based on causal chains, as proposed by Mosleh and Dias[1] – shown in Figure 1. However, in a CNEA we can model several causal chains for a particular incident, as illustrated in Figure 3.

[1] The possibility of using CNEA with other types of incident models, such as STAMP (Systems-Theoretic Model and Processes Accidents) proposed by Leveson and colleagues (Leveson et al., 2003), should evaluate.

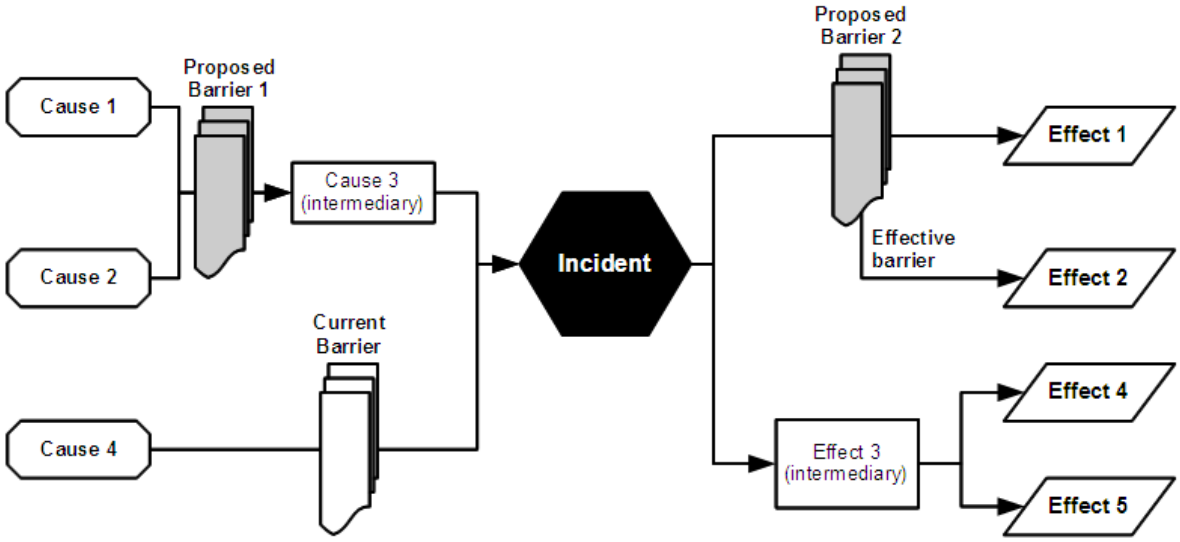


Figure 2. Diagram of a causal network events analysis (CNEA)

Table 1. Taxonomy of the CNEA.

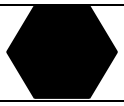
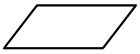
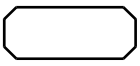
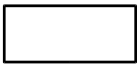
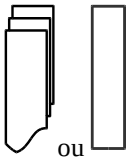
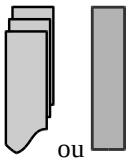
FIGURE	DESCRIPTION
	Event under analyse, for example, an incident.
	Final effect that the central event can generate, within the scope of analysis.
	Root cause for the occurrence of the event centre, within the scope of analysis.
	Intermediary cause or effect, i.e., necessary causes for the root cause drive to the central event, or potential effects arising from this event that must occur before the final effects.

FIGURE	DESCRIPTION
	Preventive barriers already implemented that aim to prevent the occurrence of the central or mitigate its effects.
	Preventive barriers that shall be implemented.

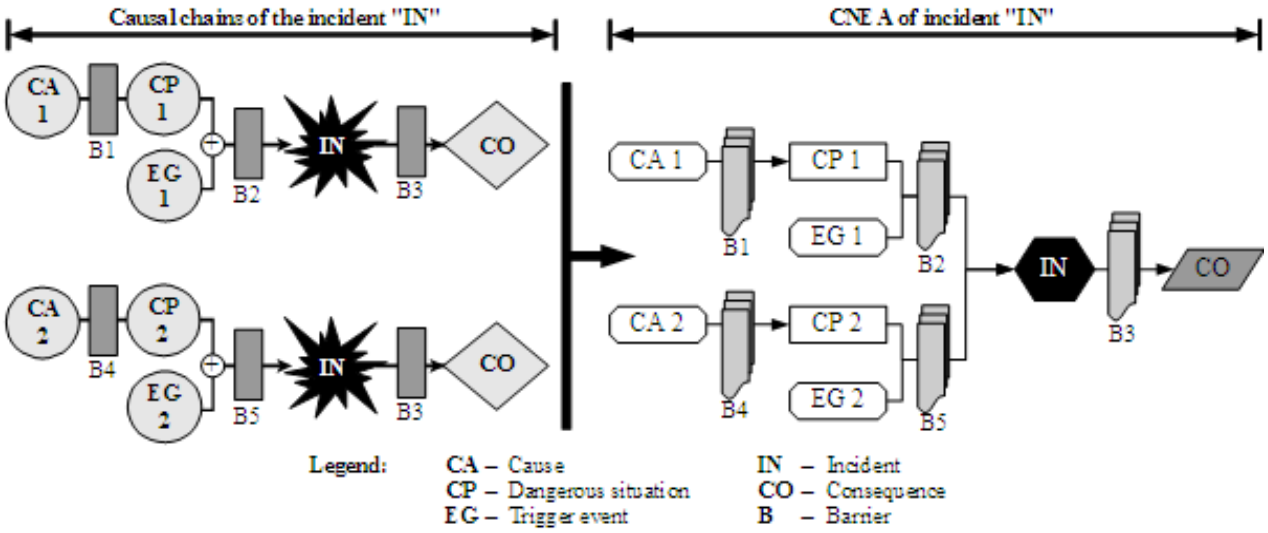


Figure 3. Causal chains, modelled as Mosleh and Dias, combined in a causal network CNEA

To be able to group multiple causal chains, the effects of the incident should be identical. If there a particularity of an incident, when triggered by a specific condition, this causal chain should be treated separately. Moreover, in some cases it is possible to simplify the network by grouping some elements of CNEA – for example, when the same event trigger trigger more than a dangerous condition.

4. CNEA MODELING

The modelling process involves, usually, query the parties who may be affected (stakeholders) by risk and who has knowledge of either the technical or safety issues. From this knowledge you can get: scenarios, implemented controls to reduce risk, identification of potential barriers to be implemented to reduce the risk; etc. Throughout the application of the technique CNEA, it is recommended to follow five main steps, as shown in the following sections, videlicet: defining the scope of analysis, Incident identification, identification of causes, identification of effects, and identification of barriers.

4.1. Defining the scope of analysis

It is the definition of the limits of the analysis, both with regard to the deployment of causes and effects. So, before starting the modelling of events to be studied, it should be clear how much causes will be investigated (what is the level of detail) and how far the impact of this incident will be examined. In the processes of defining the scope of analysis is very important to be clear what results it wants to get from the analysis, and how to explicit the outcomes. Also what other techniques will be used to help the organization and updates about the analysis performed.

4.2. Incident identification

The second step of CNEA is the incident (IN) identification, for that, one should answer questions like:

- Which functions the system under analysis (or component) must meet?
- What are the conditions of operation of this system / component?
- How can we characterize the incident?

So it is possible to identify clearly how could occurs the event that you want to avoid. The incident (IN) is then represented in the central position of the CNEA diagram, characterized, for example, as a non-function or a function beyond project limits.

4.3. Identification of causes

Cause (CA) is the event that is the source of the problem. In any risk analysis, the analyst always looks for the elimination of the cause, or reduce their probability of occurrence. The causes are the reasons that lead to the occurrence of the central event, and therefore they are located on the left side of the CNEA diagram (Figure 2). Note that the objective of the analysis team is to identify all the causes that lead to the incident. They should characterize the immediate causes (which are more directly related to the perception of the operator of the item) and the intermediary causes (which require more detailed analysis of the incident). However, greater attention should be given at the root causes, once the better the study of root causes the greater the possibility of success of the analysis process. To this end, one wonders what the possible causal chains that lead to occurrence of the incident (the way it was characterized).

4.4. Identification of effects

In the CNEA diagram (Figure 2) the effects are arranged on the right side of the central event, and can therefore also be called consequences (CO) (Figure 3), depending the approach of the risk analysis. Whatever approach is adopted, the analysis team should identify all possible scenarios to reach the final effects, within the scope of analysis. For that, all the intermediary conditions should be outlined and establishes the possible connections between them.

4.5. Identification of barriers

The barriers are divided into those that aim to eliminate, reduce or monitor the incident (IN), acting on the causes, and barriers to eliminate, mitigate or prepare for the effects / consequences (CO), acting on the incident – as shown in Figure 2 and Figure 3. To identify these barriers, the following questions should be asked:

- How the incident or its causes could be prevented? What are possible ways of monitoring and control?
- How can mitigate the effects, if the central event occurs? Is it possible to maintain the function of the system active even during the incident?

At this point it is interesting to do an analysis of how barriers can fail and what the effects of failures. It is noteworthy that this analysis must be done separately, in a FTA, for example.

From the identification of barriers to prevention and contingency, we can define an action plan for managing risk. To do so, you should ask questions like:

- What tasks are performed to ensure that barriers were implemented?
- What tasks are performed to ensure that barriers remain active?
- Who is responsible for each task?
- How to know when the task should be performed?
- How to know exactly what should be done? Is there a procedure?
- What is the training required to implement the tasks?
- How to check if the task was performed correctly and if it is effective?

Once the action plan is set, it is possible to feed back the CNEA with the new information.

Thus, it is recommended to evaluate several issues:

- There is sufficient control over the risk? What more can be done?
- Can one increase the effectiveness of control over the risk?
- Is it feasible to increase the number of barriers to reduce the probability of occurrence of the centre event?
- There is a possibility of removing any barriers?
- The action plan is feasible?

4.6 Trigger event

The trigger event (EG) of Figure 3 is an event that triggers the hazard condition in such a way that results in an incident. In matter of reliability, trigger events are usually external events, such as high pressure, dust, humidity, temperature, impact, etc., that drives to a failure mode that, for example, was hidden during the life cycle of the item. In risk analysis, in general, the trigger event is also related to external events coming from the environment, from the human or from the technical system itself, such as: storms, cyclones, tornadoes, floods, traffic accidents, fires, riots, or any disturb that make a hazard condition leads to an incident, in terms of discontinuity of a function as non-supply of electricity, leakage of chemical, etc.

Triggers event are very much present in the human condition throughout the life cycle of work and the work process. For example, in the life cycle of an activity, the start times of activity and the end are more prone to errors. Studies of safety at work emphasize the chance of operational failures occur are grater due to inattention or fatigue. In these situations, the causes are organizational and barriers to prevent the occurrence of the trigger event are strongly related to training and teamwork.

4.7 Hazard condition

The hazard condition (CP) of Figure 3 is a condition characteristic of all the technical system in working, since every technical system has its own hazards. Thus, at extreme work, or before critical events, these hazards are more likely to initiate a incident. This also happens when the operation or maintenance programs are not adequately prepared to handle the concerns of operators and maintainer, in the circumstances of normal operation and, more important, in special operation and maintenance. A hazards condition is best identified in the scenario design. May be evidenced in the process of reliability analysis and risk analysis, using techniques such as brainstorming, functional analysis, FMEA with criticality analysis (which many authors call FMECA). An example of hazard condition cold be a hidden failure.

5 RELATIONSHIP BETWEEN CNEA AND OTHER TECHNIQUES

The CNEA is a technique for modelling cause–effect relationships and therefore can be used to replace or complement techniques for this type of analysis. In the following sections, it is presented some considerations about the relationship between CNEA and FTA, ETA, FMEA, BTA and bayesian networks.

5.1 CNEA and FTA

In CNEA is possible to deployment the causes of the central event until the desired resolution (in the limit the scope of analysis), keeping the representation of intermediary events and how they relate. It is interesting to note that the network structure allows us to represent causal links without having to specify how causes interact, providing a graphical model to facilitate experts to understanding the causal chains of the central event under analysis.

For example, in Figure 4, the causal chain is represented by an FTA. However, to establish the relationship between events, it is necessary to know which gate would be used, "AND" or "OR". In other words, it required specific knowledge regarding the cause-effect relationships in the context of the function of systems: if there is dependence between functions, if items are operating in series or if there is any redundancy, etc.

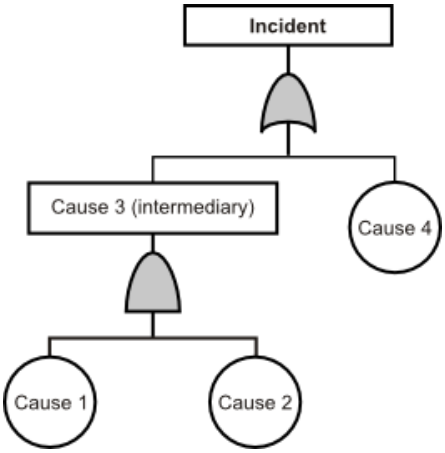


Figure 4. Example of FTA

The same model presented in Figure 4, in the context of the FTA, is represented in Figure 2, in the context of CNEA (excluding barriers). In the last case, however, there is no logic gates OR (typical in FTAs), but only the nomenclature of the events described in the taxonomy.

The preponderant for the CNEA is in fact that it evidences the barriers that are in themselves, actions to be taken to prevent the progress of causes. Sometimes, the barriers may even be ways to eliminate causes.

5.2 CNEA and ETA

Regarding the analysis of the effects, CNEA allows design scenarios outlining the potential future states, considering the occurrence of the centre event. Just as the causes, effects are also represented in the form of network, showing the chain until they reach the final effects (defined by the scope of analysis). On the other hand, ETA design pivotal events but show only the final states (results of the scenarios).

Pivotal events are those that alter the sequence of the causal chain. In an ETA all analysed events are pivotal, as is shown in Figure 5. In CNEA, the effects are considered as states and barriers are pivotal events. Thus, the CNEA allows highlighting the intermediary effects, and also the barriers that may act as pivotal events.

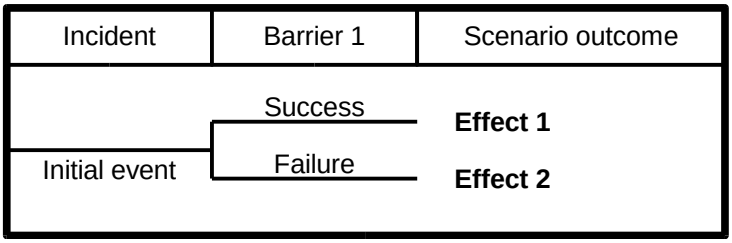


Figure 5. Representation of a pivotal event (Barrier 1) in an ETA

In the CNEA, pivotal event is modelled considering that the barrier may or may not be successful. This consideration is more relevant in the analysis of effects, that the success of a barrier results in a "smaller" consequence, but that should not be overlooked. Figure 6 illustrates this situation. The effectiveness of the barrier indicated by the thick line below the barrier, result to the occurrence of Effect 3. So this will prevent the occurrence of Effect 1 and the effects thereafter. That is, the Effect 3, in fact, may mean, for example, a warning signal, a security mechanism or disabling a function that prevents the incident result in the Effect 1, and a subsequent effect. Thus, the barrier acts as a pivotal event in the same manner as in the ETA model illustrated in Figure 5.

Note that it is possible, in one diagram, visualize the relationship of causes (which can also be modelled in an FTA) and the effects (which can be modelled in an ETA), without having to determine the type of relationship between its elements – such as in a FTA – and the effects can be listed without the need to understand all the events that influence the causal chain (i.e., all pivotal events), as in ETA.

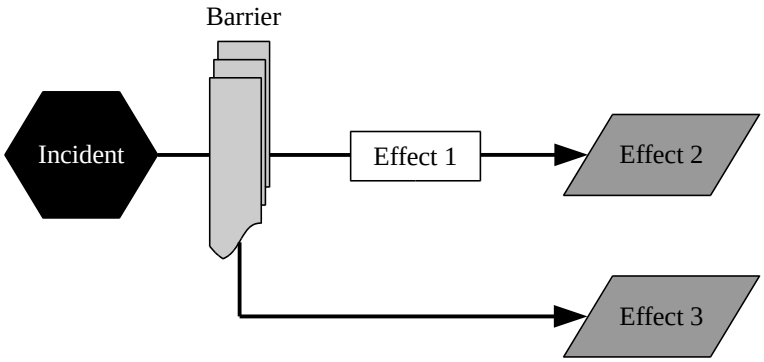


Figure 6. Representation of an effective barrier (pivotal event) in a CNEA

5.3 CNEA and FMEA

In a FMEA the knowledge is structured regarding the name of the item, its function, possible failure modes, causes, effects, priorities for analysis and action to mitigate or eliminate failures. The technique have some issues, outstanding: time required for analysis, cost analysis, amount of information, updating information, repetition of approach, continuity problems and difficulty to see the main failures.

CNEA, on the other hand, aims to analyse incidents in the context of risk analysis. The technique proved to be adequate to represent the events of FMEA in graphical way, highlighting barriers that interfere in each scenario. For the most critical events the graphic representation makes easer the communication with anyone who works or interacts with the technical system under analysis. However, if CNEA is the unique technique used, the analyst could have difficulty to understand a complex system as a whole.

Figure 7 illustrates the adaptation of a CNEA diagram for analysis of failure modes with a FMEA. To this end, we identified the central event – usually defined as an incident – as a failure mode. Note that the degree of severity "S" refers to all effects, then, the severity is associated with the failure mode – since it is the origin of the effects.

On the left side of the failure mode is presents its causes. They are deployed into root causes, intermediary, or immediate, defined according to the depth of the FMEA analysis. Risk Priority Number (RPN) is attached to each cause, with its respective rate of occurrence "O" and the difficulty of detection "D". The difficulty of detection, for example, refers to all the existing controls over the scenario, from causes to effects.

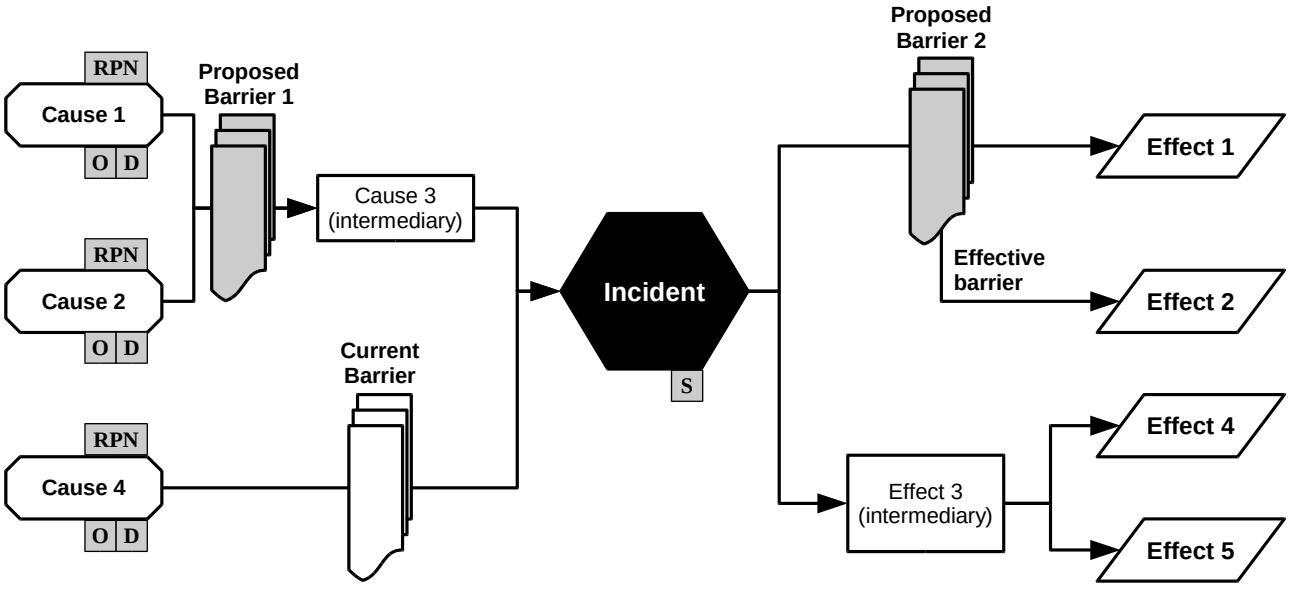


Figure 7. CNEA diagram adapted to represent a FMEA

Additionally, the adequacy of CNEA diagram to the information present in the FMEA worksheet, some adjustments were made. As shown in Figure 7, it was made a differentiation between barriers in the following conditions: barriers in white are "current control", i.e., already exist in the system; grey barriers define "proposed action", i.e., to be determined from the analysis performed. And Risk Priority Number (RPN), indicating the severity (S), Occurrence (O)

and Detection (D), can also be included in the CNEA analysis. They are used to help the analysis team to set priorities for detailed analysis, implementation barriers and funding resources to improve the technical system.

It is interesting to note that the graphical representation provides a better context and than the worksheet, and it looks more appropriate, both by providing a more efficient analysis and by better managing the knowledge generated, facilitating the viewing of the actions related to the failure mode.

Noteworthy are the following benefits in using the CNEA:

- improves communication between the analyst and other staff, assisting in the involvement of experts and the search for consensus on decision making;
- improves the representation and dissemination of knowledge, and it is indicated as a tool for empowerment;
- allows representation of immediate events and intermediaries – not only root causes and final effects;
- identifies where a current control is working at a causal chain and where would be implemented new controls in the future;
- shows, more clearly, the relationship between causes and between effects; and
- improve the formalization of knowledge and, consequently, the reuse of analysis information.

We also emphasize that the modelling of the incident in the CNEA diagram facilitates the task of identifying events and states to be analysed – once it allows visualizing the whole causal chain for each failure mode. Thus, the diagram also facilitates the elicitation of expert knowledge, as it acts as a communication tool.

The experience gained during the analysis indicated that CNEA is shown akin to FMEA, as the technique allows modelling the scenario resulting from the incident using states, which are the effects of FMEA.

5.4 CNEA and bayesian networks

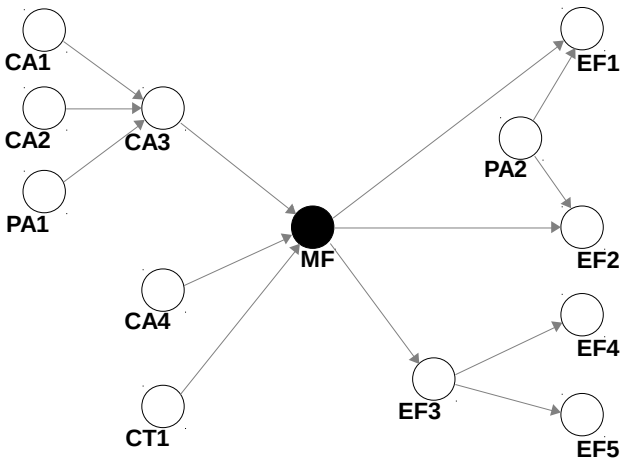
As the CNEA, the bayesian networks are also causal networks, which makes the use of the techniques together quite appropriate. The Table 2 shows the Bayesian network equivalent to the CNEA diagram illustrated in Figure 2, considering all events as independents.

It is interesting to note that we can verify the adherence of the model to reality, through a d-separation analysis.

Note that barriers – proposed actions and current controls – in this model, are in the same level of events that they intend to protect, as shown on the right side of the network (Table 2), which illustrates a table of relations (in this case deterministic) for node "CA3".

It is also possible to model – in a bayesian network – barriers that have a secondary effect, if it is successful, by modelling as a bridge (as illustrated in the case of nodes PA2, EF1 and EF2). So it is possible to design in a bayesian network every kind of relationships in a CNEA. Thus, one can see the consequences of either the effectiveness or not of a barrier to system behaviour. These rules define how a model developed using CNEA can be modelled in bayesian networks. This allows the user to outline the bayesian network, without having to worry about performance a d-separation analysis. In fact, a computational tool could do this automatically, and the bayesian network modelling would be transparent to the user.

Table 2. Bayesian network for the CNEA diagram of Figure 2, outstanding the relationship table of node "CA3".



Example of relationship table: node "CA3"			
CA1	**CA2**	**PA1**	**CA3**
Occur	Occur	Effective	Not occur
Occur	Occur	Not effective	Occur
Occur	Not occur	Effective	Not occur
Occur	Not occur	Not effective	Occur
Not occur	Occur	Effective	Not occur
Not occur	Occur	Not effective	Occur
Not occur	Not occur	Effective	Not occur
Not occur	Not occur	Not effective	Not occur

Legend:

MF – Failure mode
CA1 – Cause 1.
CA2 – Cause 2.
CA3 – Cause 3 (intermediary).
CA4 – Cause 4.
CT1 – Current Control 1.
PA1 – Proposed Action 1.
PA2 – Proposed Action 2.
EF1 – Effect 1.
EF2 – Effect 2.
EF3 – Effect 3 (intermediary).
EF4 – Effect 4.
EF5 – Effect 5.

It is interesting to note that the structure FTA / ETA is based on deterministic relationships (boolean logic), while bayesian networks can handle uncertainties in these relationships – but, the combination of CNEA and bayesian networks allows the analyst to make this deterministic analysis as well, as illustrated in Table 2. In this example, not occurring "CA1", occurring "CA2" and "PA1" not effective, certainly will occur "CA3". Thus, with the bayesian networks, the analyst can introduce uncertainty in this relationship and would model the occurrence of "CA3", for example, as 80% probability of occurring and 20% of not occurring. This allows to design a models with less epistemological uncertainty.

This feature is specially useful for modelling effects – once the occurrence of EF3, for example, does not necessarily imply in the occurrence of EF4. In this case, we can model the causal chain in a non-deterministic way.

Note that one of the difficulties of implementing a bayesian network – as any quantitative analysis, for example, an FTA – is to obtain statistics. For this, the analyst can make use of the database, simulations or other technique, based on experts' knowledge. One technique that can assist in estimates probabilities of occurrence (and relations of events / states) is the bayesian update, in which we can combine the subjective information with field data.

6. FINAL CONSIDERATIONS

CNEA (causal network event analysis) is a technique that allows design detailed models of incidents and thus facilitates the understanding of systems and communication in the analysis team. Furthermore, with the more detailed causal chain, it is possible to identify a greater number of points for taking action (barriers) and thus improve outcomes.

Since there is no need to know the deterministic relationships between the elements of the causal chain, as in the FTA, the inclusion of event in the causal chain has become greatly simplified.

The CNEA was initially designed to integrate with FMEA and thus facilitate its development, once on of the weakness of the FMEA is representation in table form. Both techniques are very complementary, i.e., while the FMEA shows together all failure modes, CNEA facilitate visualization of each failure modes of interest, explaining the relationship between causes, effects and barriers.

Systems usually have many failure modes (incidents). This problem is reduced by selecting only the failure modes in FMEA that are highlighted the greater NPR or the severity is above a predetermined limit.

In application in real systems, it was possible to see the great utility of CNEA, both for modelling failures in equipment and in processes. The representation of the causal chain by this technique is quite simple, which facilitated communication between team members – that usually are professionals from several areas such as maintenance engineers, electrical engineers, mechanical engineers, maintenance managers, among others.

The way information is organized makes possible to identify where a particular action can be implement to prevent the occurrence of a event within the causal chain or to mitigate its effects. Thus, the actions that will be taken by the organization, to manage the risks, can be taken. Moreover, the structure of the technique allows simulations to verify the impact of a barrier on the probability of effects. Through this kind of simulation we can assess the cost-risk-benefit of each barrier and justify either its implementation or not, considering the limit of as low as reasonably possible (ALARP).

Note that the concept of effective barrier allows to study conflicting situations, for example, reduced availability to increase safety.

It is noteworthy that, unlike the structure FTA / ETA, using CNEA it is possible to modelling a system in a more simplified way, which requires less knowledge. As will be gaining more knowledge, we can enhance (improve) the model by applying statistical treatment (with the possibility of use not deterministic relationships) based in the association with bayesian networks. You can also, if appropriate, to detail a specific item using a FTA. So it is possible to detail a model without the need to migrate for another analysis technique – once CENA allow integration of other techniques.

Finally, we point out that the CNEA (associated with other techniques or not) contributes to the knowledge management, especially with regard to their institutionalization, but also promotes the internalization. Thus, the training process becomes simpler, both in the implementation of action plans and employee training and dealing with changes in the context of team responsible for implementation of risk analysis.

8. REFERENCES

Calil, L. F. P., 2009, "Metodologia para gerenciamento de risco: foco na segurança e na continuidade", Tese (Doutorado em Engenharia mecânica) – universidade Federal de Santa Catarina (UFSC), Florianópolis, 231 p.

Delvosalle, C. et al., 2006, "Aramis project: a comprehensive methodology for the identification of reference accident scenarios in process industries", Journal of hazardous materials, Elsevier, v. 130, p. 200 – 219.

Dias, et al., 2011, "Metodologia para análise de risco: mitigação de perda de SF6 em disjuntores", Florianópolis, ISBN 978-85-98128-42-9.

Iannacchione, A. T., Esterhuizen, G. S., Tadolini, S. C., 2007, "Using major hazard risk assessment to appraise and manage escapeway instability issues: A case study", Proceedings of the International Conference On Ground Control In Mining, 26.

Leveson, N. et al., 2003, "A systems theoretic approach to safety engineering", Cambridge, MA.

Lewis, S.; Hurst, S., 2005, "Bow-tie anelegant solution", Strategic risk, p. 8, November.

Mosleh, A., Dias, A., 2003, "Towards an integrated framework for aviation hazard analysis", University of Maryland Report.

Ramzan, A., 2006, "The application of thesis bow-ties in nuclear risk management", The journal of the safety & reliability society, uK Safety and Reliability Society, v. 26, n. 1.

Reason, J., 1997, "Managing the risk of organizational accidents", Ashgate Publishing Limited.

Trbojevic, V., 2001, "Linking risk assessment of marine operations to safety management in ports", Proceedings of the Biennial Marine Transportation System Research and Technology Coordination Conference, 6., Washington.

Trbojevic, V., 2004, "Linking risk analysis to safety management", Proceedings of the International Conference On Probabilistic Safety Assessment And Management (PSAM), 7, Berlin.

9. RESPONSIBILITY NOTICE

The authors are the only responsible for the printed material included in this paper.