Process Safety and Environmental Protection

Learning (and Unlearning) from Failures: 30 Years on from Bhopal to Fukushima an Analysis through Reliability Engineering Techniques

Ashraf Labib, University of Portsmouth, UK.

Email: ashraf.labib@port.ac.uk

Abstract:

Reliability engineering techniques such as failure mode effect analysis (FMEA), fault tree analysis (FTA), and reliability block diagrams (RBD) have been used to analyse the case of the Bhopal disaster (Labib and Champaneri, 2012), and subsequently used in the analysis of other disasters (Labib, 2014b), where it has been shown how such techniques can help in building a mental model of describing the causal effects of the disaster. The same case study of Bhopal was also investigated (Ishizaka and Labib, 2014) and a new logic gate in the fault tree method was proposed for analysing disasters and the benefits of using hybrid techniques of multiple criteria and fault analysis to evaluate and prevent disasters were demonstrated.

In this paper an analysis of learning, and un-learning, from failures is carried out using a comparison between Bhopal and Fukushima, although they occurred in different industries, by comparing them we observe many similarities. This is followed by a compilation of different models based on FTA and RBD analysis of the Bhopal disaster which were an outcome of a series of workshops that were carried out to investigate the Bhopal disaster. This approach shows how the same case study can be viewed from different perspectives although the same modelling techniques were used. The paper then explores few interesting research questions such as how to evaluate different models? Do multiple models lead to better understanding of the case study? And are there any practical guidance to follow when studying root cause analysis?

Keywords: Learning from failures; Unlearning; Bhopal; Fukushima; Fault tree analysis; Reliability block diagram

1. Introduction:

Bhopal, Minamata, Deepwater Horizon, and Fukushima are examples of disasters that have common features. They all show that in their struggle to maximize their profits, major companies and industries have tended to compromise safety. They also demonstrate an attempt from those responsible to initially hide the extent of the impact of the disaster and in doing so, many lives have been lost due to late response. They also illustrate how man-made disasters can have a far reaching impact on the neighbouring communities and the environment. Finally, they remind us, as also proposed by others (Mohagheg and Mosleh 2009; Taniguchi and D'Agostino 2012 a, b; Taniguchi 2012), that disasters are not just a technological problem but there is a need to study socio-technical factors, and to adopt a trans-disciplinary approach that incorporates social and natural scientists, practitioners, and policy makers.

Bhopal occurred 30 years ago, before many of today's engineers were born, and so it may be worth summarizing the incident. In the midnight of December 2, 1984, the tank 610 (one of three tanks) containing methyl isocyanate (MIC), which is an intermediate compound in the production of a highly toxic pesticide called cevine, got contaminated with water. The source of contamination whether intended

or un-intended is still questionable. This led to the initiation of an 'exothermic reaction' (a type of chemical reaction where the energy needed for the reaction to occur is less than the total energy released, so heat is generated as an output which in turn is used as an input to speed the chemical reaction and generates more heat). This reaction turned into a violent 'runaway' which is a term used to describe an accelerated and uncontrollable chemical reaction. This leaked to the atmosphere by-passing safety barriers such as the vent gas scrubber (VGS) which is a device designed to serve as the last line of defence in the eventuality of this deadly gas leak. Apparently the VGS was not well designed to be capable of handling such mount of leak, and to make matters worse, it was unavailable as it was under maintenance during the incident. There was also a catalogue of safety breaches through operational errors such as shutting the refrigeration unit which was designed to keep the temperature below 5 degrees centigrade and the unavailability of the flare tower. The process at Bhopal can be illustrated as shown in Figure 1. The consequence of this disaster was the killing of around 3,400people, and injuring around 200,000. It is also reported that 3,000 cows were killed and vegetation died over an area of 40 km^2.

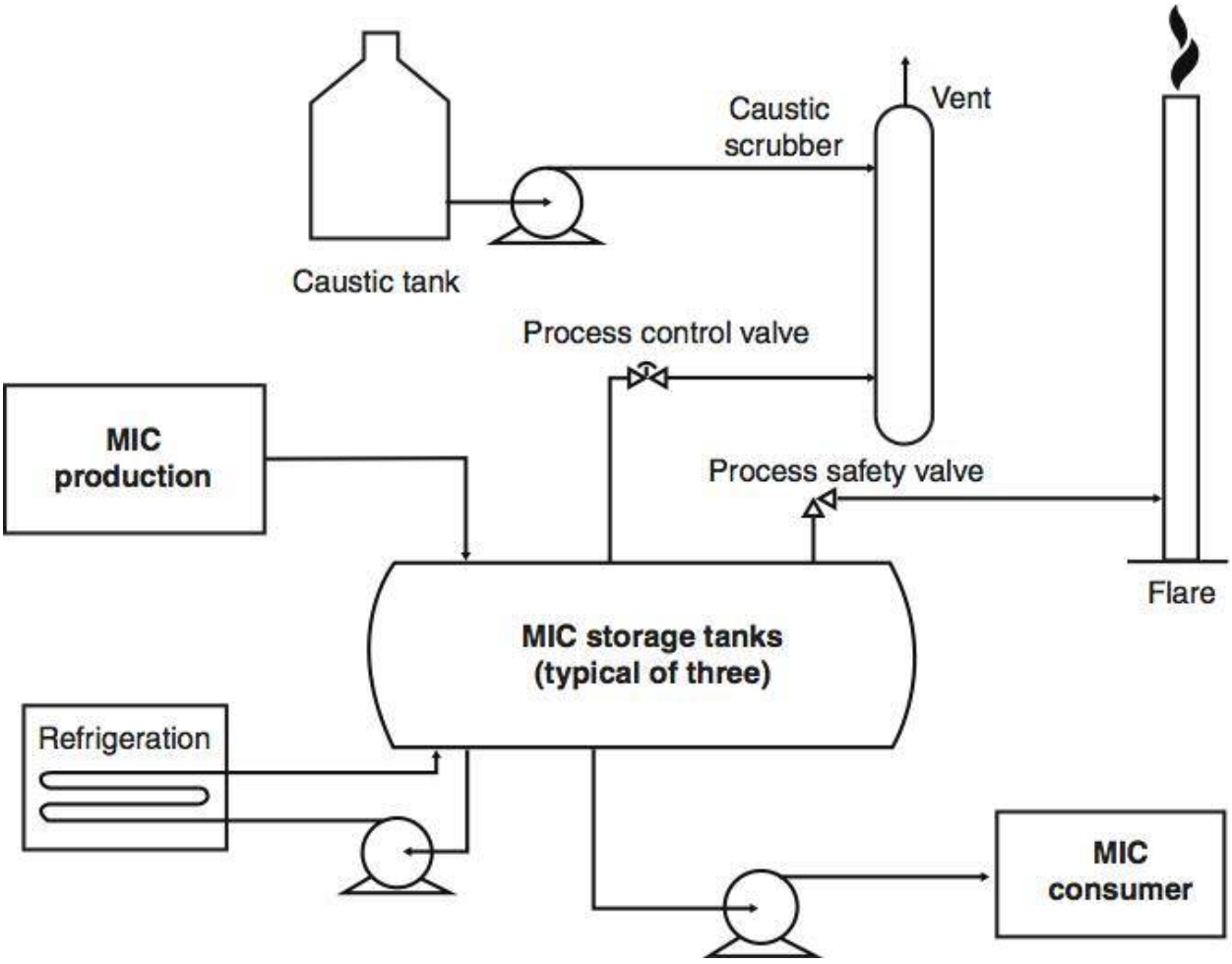


Figure 1: The Process at the Bhopal Plant -Ref: Adapted from SPE (http://www.spe.org/news/article/what-caused-the-deadliest-industrial-accident-in-history)

Fukushima disaster occurred on March 11th, 2011, when Japan suffered from one of its worst ever recorded earthquakes of magnitude 9.0 Richter scale, known as the Great East Japan Earthquake. This was then followed by a massive tsunami, which swamped the Fukushima site and took out the AC electrical power capability. Due to these two double jeopardy events, the cooling capability of the four nuclear reactors at the nuclear power plant was lost, a phenomenon known as the 'ultimate heat sink'. This together with hydrogen built up caused an ignition that led to a nuclear melt-down. This disaster was classified as a level 7 of the International Nuclear and Radiological Event Scale (INES), the highest severity level which is only shared with the Chernobyl disaster. For more details about the analysis of Fukushima, the reader can consult Labib (2014 a, b), and Labib and Harris (2015).

2. Learning (and Unlearning) From Failures - Bhopal versus Fukushima:

2.1 Bhopal Vs. Fukushima:

Although there are similarities between Bhopal and Fukushima nuclear power plant disaster as mentioned above, there are also subtle differences. Bhopal was a perfect storm (Pate-Cornell, 2002) or an accident waiting to happen (Chouhan, 2005), whereas Fukushima is claimed to be a 'Sotegai' (a Japanese word that means beyond hypothetical expectations) or a black swan (Taleb, 2010).

So, why was Bhopal a perfect storm? In all, or most, major accidents, we see a similar pattern of multiple things going wrong simultaneously. The list of things that went wrong at Bhopal is striking, including:

- Many safety related devices where not well designed to handle such major gas leak, with no redundancy, and to make things even worse, most of these devices (such as the VGS, flare tower, and cooling refrigerator) were not available at the time of the disaster.
- The plant was losing money, which resulted in staff and maintenance budget cutbacks.
- A social system that dismissed safety culture and created extreme tension between management and workers to the extent that one disgruntled worker was willing to intentionally ruin a batch of MIC(SPE, 2014)..
- The plant was to close permanently, which, no doubt, significantly affected operator morale and contributed to the lack of maintenance and the bypassing of safety systems.
- The complete failure or lack of an emergency response program.
- Ineffective treatment of the injured.
- The people outside and inside the fence had no idea how hazardous the plant was. There was no siting or any awareness of the dangers of this plant.

However, there are also striking similarities between Bhopal and Fukushima. Both occurred in the so-called high reliability organizations (HRO). HRO is a term that refers to industries such as oil and gas, process, nuclear and aviation, where they possess a high degree of reliability despite their hazardous environment. Both incidents had a long term impact and effect on the environment. Both incidents are attributed (as in many disasters) to socio-technical reasons. Both incidents were attributed to bad design and bad operation. Both disasters are considered the worst in their own industry, where Bhopal is considered the worst disaster in chemical process industry and Fukushima (together with Chernobyl) is considered the highest severity (level 7) in nuclear power plants (using the IAEA INES scale of severity).

What we have learned from Bhopal that it led the industry to the incorporation of inherit safe design concepts (Kletz, 2006), which led to many companies to reduce, or eliminate if possible, their stock of

hazardous intermediates. On the other hand, Fukushima led the industry to embrace (Sorensen etal 1999), and re-examine (Weightman , 2013) defence-in-depth concept and beyond design research. Unfortunately, it seems that what we have not learned yet is the effect of routines, sense making and culture (operation) in the case of Bhopal (Weick, 2010). It also seems that what we have not learned yet from Fukushima is the effect of culture (Kurokawa, 2012) and the need for a global regulation with licencing powers in nuclear power plants (Labib, 2014a).

2.2 **The Unlearning Process:**

After Bhopal Qi et al (2012) outlined a set of regulations and measures that took place to improve process safety. They then made an important observation and posed a fundamental question: *'since the Bhopal tragedy in 1984, it is embarrassing that questions such as – "Has the industry become safer?" can still not be answered positively*' (Qi et al, 2012).

After Bhopal, process industries have instituted new regulations, standards and routines as remedial measures intended to reduce likelihood or consequences of accidental chemical releases. Despite all these abundant precautions and stringent regulations, the number of reported incidents continues to plague our society. (Qi et al, 2012).

Kletz (1993) provided examples of how similar types of incidents keep occurring. Accordingly, he hypothesised that repeated incidents occur because organisations have no memory since there are plenty of personnel changes that result into a 'brain drain'. It is then recommended that there is a need to study retrospectively serious incidents through investigations of root cause analysis and also to give attention to near-misses and early warning signals with the aim to incorporate effective learning through development of knowledge retention tools.

Qi et al (2012) provided three challenges and a possible way forward to address each of them. First, organisational memory loss, and this can be addressed by continuous learning and improved communication. Second, insufficient attention to accident warnings, and this can be addressed through effective integration of process hazard analysis and decision making. Third, increasing complexity of process operation, and this can be addressed through scientific research based consequence modelling and training.

Therefore, the aim of the paper is to demonstrate how a study of Bhopal case through a retrospective in-depth root cause analysis can provide a mental model that can be considered as both a knowledge retention and a decision support tool. This is because knowledge can be retained and communicated through an effective problem structuring method. It can be argued that formulating a problem would normally solve 80% of the problem. This is in line with the argument posed by Einstein and Infeld (1938) "*The formulation of a problem is often more essential than its solution, which may be merely a matter of mathematical or experimental skill*". Therefore, in the next section a compilation of different models based on fault tree analysis (FTA) and reliability block diagram (RBD) analysis of the Bhopal disaster are provided. This was an outcome of a workshop that was carried out to investigate the Bhopal disaster. The basic intention of this work is to demonstrate how such modelling can be a valuable asset in the intellectual tool box of practitioners, and hence can contribute to the prevention of the unlearning phenomena. Although some can argue that these techniques are 'tools of the trade' in industries such as process or nuclear industry, there are evidents from many investigation reports in the wake of the

Fukushima disaster, which claimed that such tools were under-utilized, and often miss-used (Labib, 2014 a, b).

3. Models of the Bhopal Disaster based on FTA and RBD:

A series of workshops were held at the Universities of Portsmouth, Manchester and Glasgow Caledonian in the UK to study the Bhopal disaster. This was part of a series of masters classes in programmes related to the topic of learning from failures, which formed a part of MBA and maintenance engineering master courses. The participants were mainly practitioners with a background in engineering or business and management. The author first provided a framework of the concept of learning from failures similar to the one proposed afterwards by Labib and Read (2013) which relies on three principles: 1) feedback to design, 2) use of advanced techniques for analysis, and 3) extraction of interdisciplinary generic lessons.This was followed by provision of techniques that can be used for analysis such as FMEA, FTA, and RBD. A brief narrative of the disaster was then provided followed by the display of a video describing the sequence of events and consequences. The participants were then divided into groups in order to act as an investigation team with the aim of conducting in depth analysis using tools learned and then tasked to prepare an investigation report that contains analysis and recommendations. Each group provided an oral presentation. Finally, the author provided feedback and where possible revised and extended the models. The FTA model in Figure (2) shows a revised and extended model provided by the investigation of one of the groups.

3.1 Model by 1st Group:

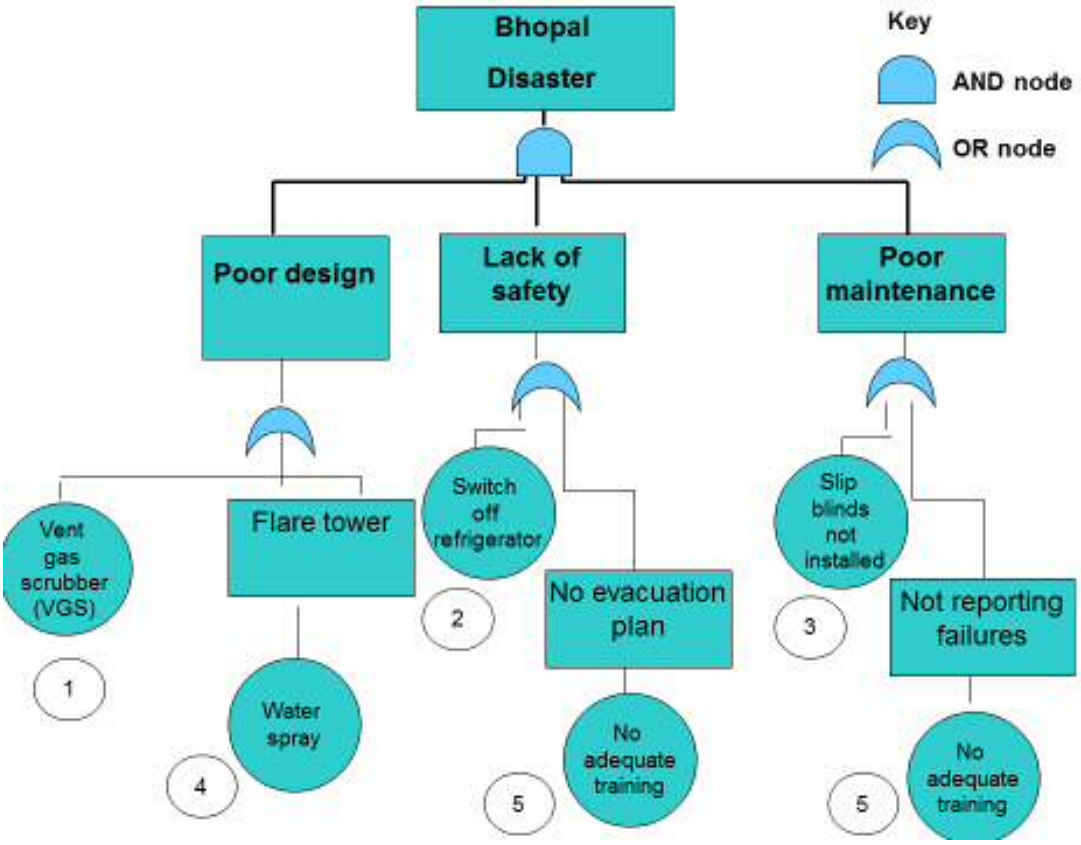


Figure 2: The first model of FTA.

The FTA model was extended to provide a demonstration of how the concept of cut sets can be applied as a numerical method for fault trees which can further enhance the analysis.

A 'cut set' is any group of fault tree initiators which, if all occur, will cause the TOP event to occur.
A 'minimal cut set' is a least group of fault tree initiators which, if all occur, will cause the TOP event to occur.

To derive 'cut sets', we need first revise Boolean Algebra rules. Note in Boolean: Plus "+" represents "OR" gate, whereas multiplication "**.**" represents "AND" gate.

Axioms of Boolean algebra:

[A1] ab = ba (Commutative Law)
[A2] a+b = b+a (Commutative Law)

[A3] (a+b)+c= a+(a+b) = a+b+c (Associate Law)
[A4] (ab)c = a(bc) = abc (Associate Law)

[A5] a(b+c) = ab + ac (Distributive Law)

Theorems of Boolean algebra

[T1] a + 0 = a
[T2} a + 1 = 1
[T3] a . 0 = 0
[T4] a . 1 = a

[T5] a . a = a (Idempotent Law)
[T6] a + a = a (Idempotent Law)
[T7] a +ab = a (Law of Absorption)
[T8] a (a + b) = a (Law of Absorption)

Thus, the logic expression for Top event Bhopal Disaster (BD) is:
BD = (1 + 4).(2 + 5).(3 + 5)
BD = (1 + 4).{2.3 + 5.3 + 2.5 + 5.5}
BD = (1 + 4).{2.3 + 5.3 + 2.5 + 5} [Applying T5: a.a = a]
BD = (1 + 4).{2.3 + 5.3 + 5} [Applying T7: a + a.b = a]
BD = (1 + 4).{2.3 + 5} [Applying T7: a + a.b = a]

This is simplest possible and can be used to redraw an equivalent fault tree.
BD = (1 + 4).{2.3 + 5} = {1.2.3 + 2.3.4 + 1.5 + 4.5}

Therefore, Minimal Cut Sets are: 1.2.3; 2.3.4; 1.5; 4.5 i.e.

- Vent gas scrubber**.** Switch off refrigerator**.** Slip blinds not installed.
- Switch off refrigerator**.**Slip blinds not installed**.** Water spray.
- Vent gas scrubber**.** No adequate training.
- Water spray **.**No adequate training.

Any of the above combinations will result in the top event occurring. This can easily be shown from the equivalent RBD. The RBD in Figure (3) is a natural extension of the FTA in Figure (2) and one can easily be trained to draw it guided by the following rules as explained by Labib (2014b):

1. Every **OR** in an FTA is a **Series** configuration in the equivalent RBD.
2. Every **AND** in an FTA is a **Parallel** configuration in the equivalent RBD.
3. Start from the **Top** of the Tree.
4. Only model **Basic events**.
5. The **order** in an RBD does NOT matter.
6. Look for a **real** root cause.
7. Both FTA and RBD are mental models for **risk analysis** rather than risk assessment.

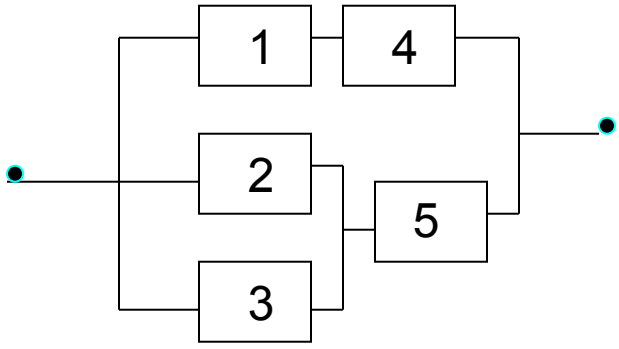


Figure 3: The equivalent RBD.

In order to illustrate the benefit of using RBD, suppose that one was given resources to spend on improving the plant, it can be observed from the RBD that box 5 (No adequate training) is a crucial issue because it controls two boxes (2 and 3). This finding that relates to the significance of the impact of lack of training is very much in line with what Chouhan (2005) has identified. Chouhan who carried out an extensive analysis of Bhopal, was one of the workers at Bhopal and hence had a first-hand experience of the disaster. In his account of the disaster, he presented three figures where one relates to the consistent decline in the number of workforce, followed by a second figure which illustrates a consistent decline in training months per year over time at the Bhopal plant prior to the accident, and a third figure that shows how the composition of the existing workforce at Bhopal was predominantly trainees just prior to the accident, as compared to a majority of experienced staff in the earlier years of its production. These three figures provided by Chouhan (2005) highlighted the problem of no adequate training, which was captured in the analysis of the FTA and RBD models provided by the 1st group.

3.2 Model by 2nd Group:

The second group developed an FTA model that is shown in Figures 4, 5, 6 and 7. This model is more comprehensive. Its equivalent RBD is then shown in Figure 8.

There was however a considerable debate among the members of the group and the author on whether the top event of Figure 4 should be an OR gate or an AND gate. The author provided the following feedback. In an FTA if the intention is to use it as a design tool for a prospective analysis - for example for a new design of a system, then it is better to be pessimistic and assumes an OR gate as the rationale here is any one of the factors can cause the accident to happen. Whereas in a retrospective analysis of the causal factors of an accident, it is clear that at Bhopal all the factors – of inadequate work force, failure of plant due to diminished design specification, poor management decisions, and poor maintenance of the plant, have been combined simultaneously to cause the disaster. So, in short, for the top gate: use OR gate for a prospective analysis, and use an AND gate for a retrospective analysis. This is in line with the Swiss cheese model as proposed by Reason (1997) which implies a domino effect, where all barriers were peached simultaneously; alignment of holes in the slices of the Swiss cheese.

Fault Tree Analysis of Bhopal Disaster:

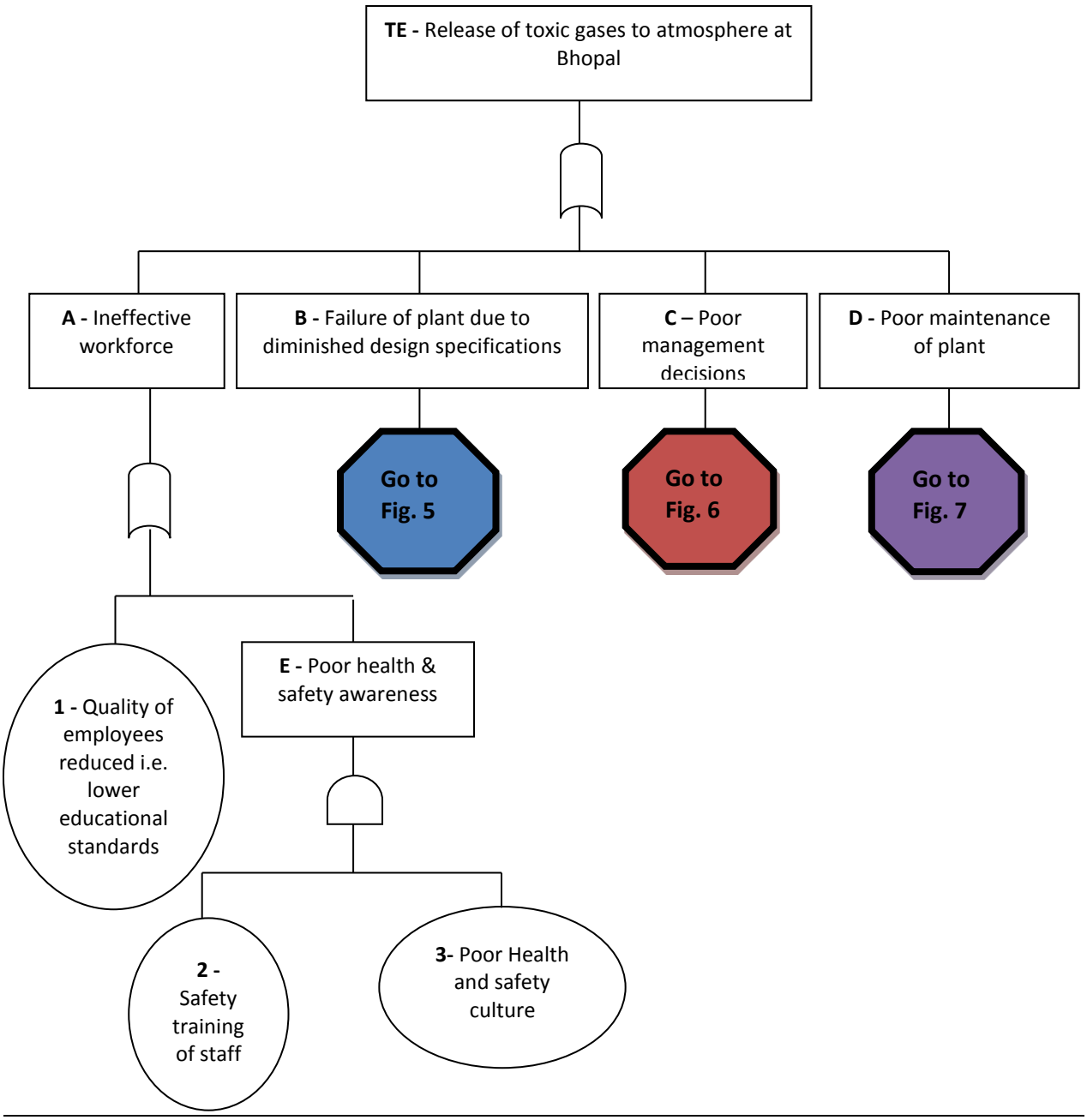


Figure 4: The second model of FTA (a) (adapted from Labib and Champaneri, 2012).

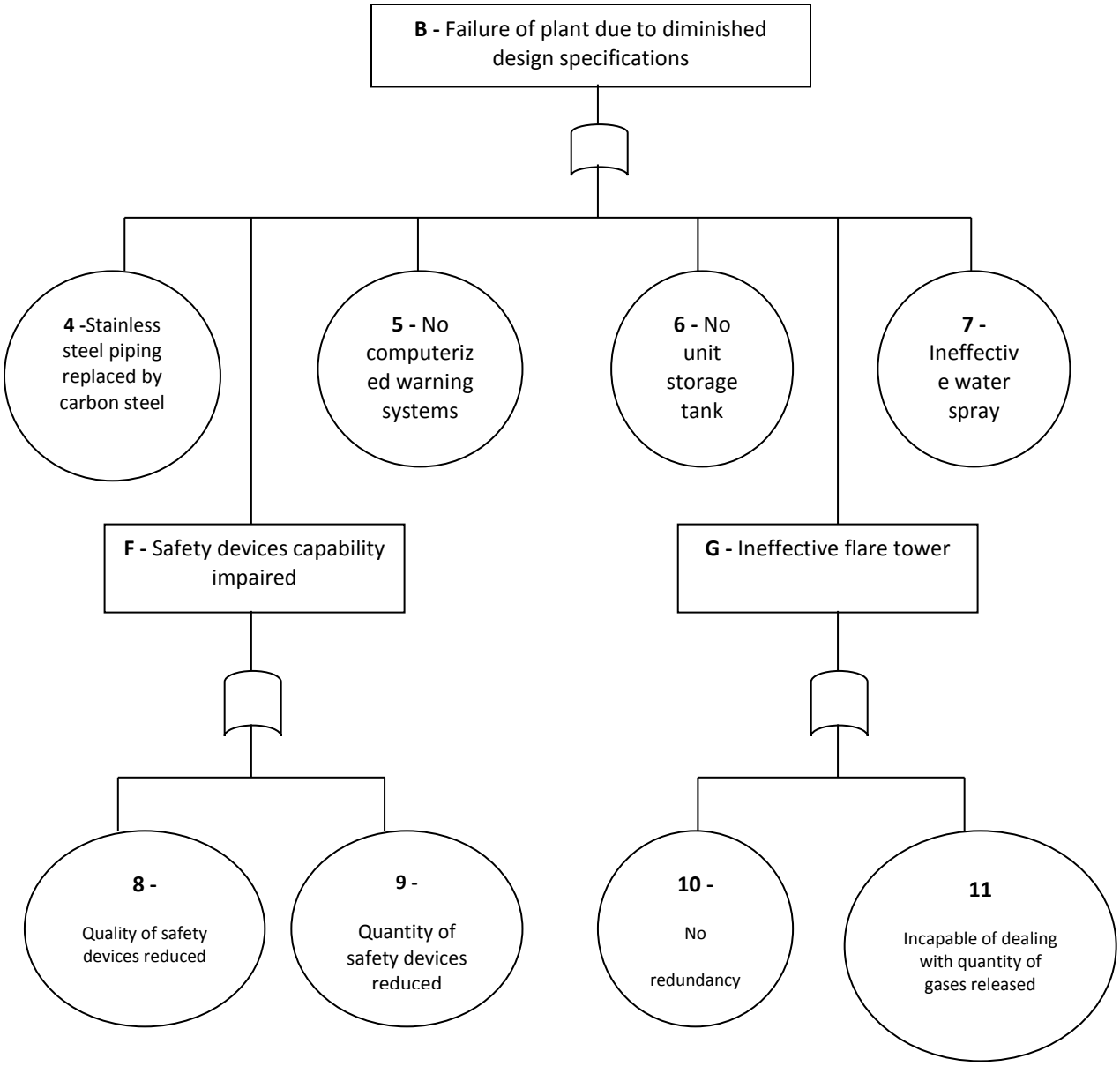


Figure 5: The second model of FTA (b) (adapted from Labib and Champaneri, 2012).

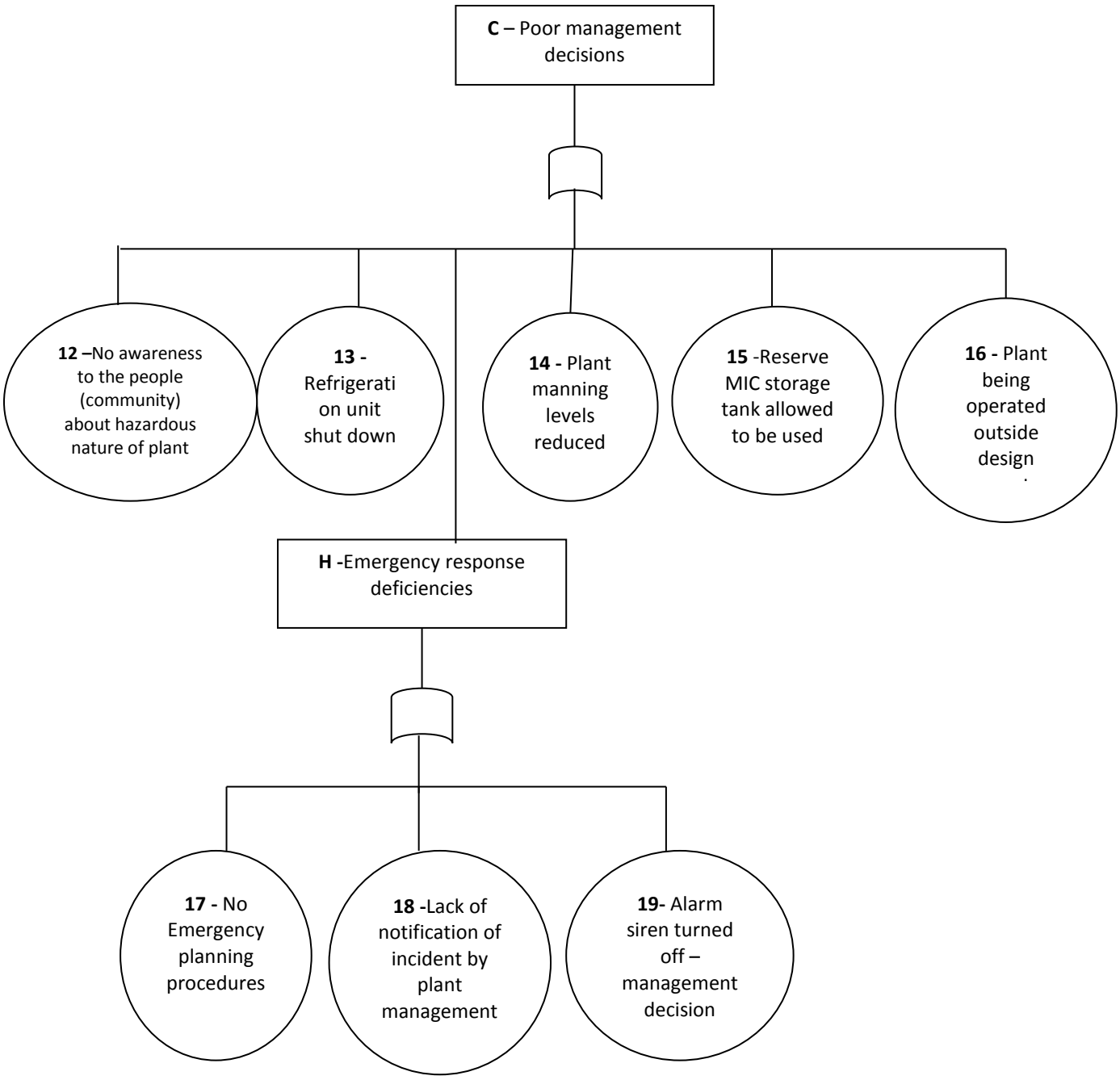


Figure 6: The second model of FTA (c) (adapted from Labib and Champaneri, 2012).

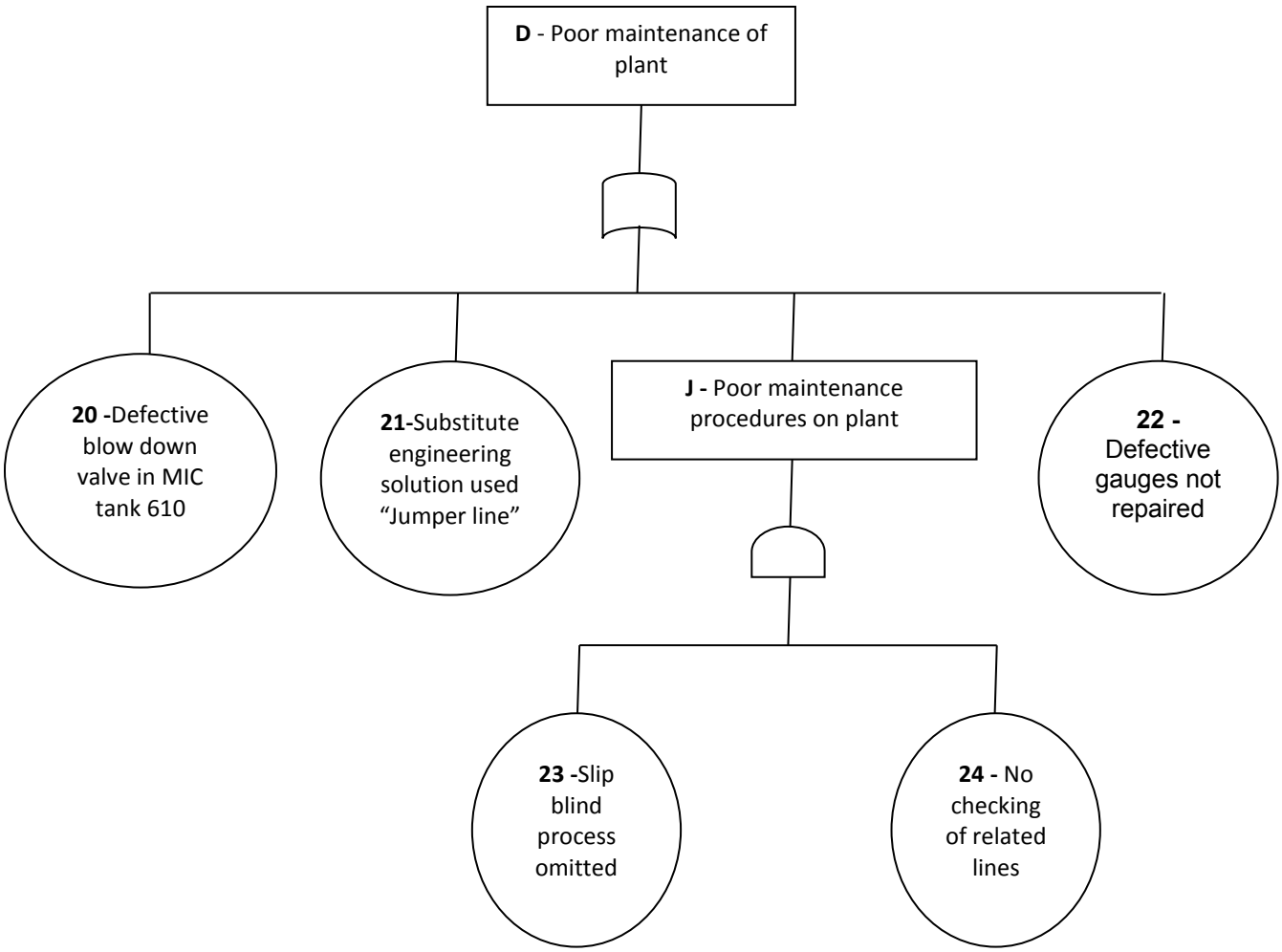
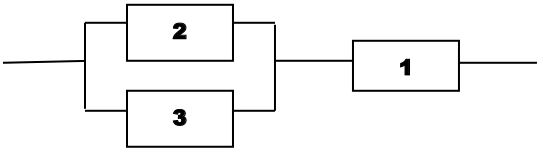
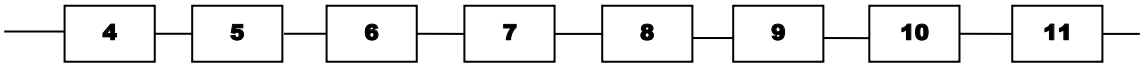


Figure 7: The second model of FTA (d) (adapted from Labib and Champaneri, 2012).

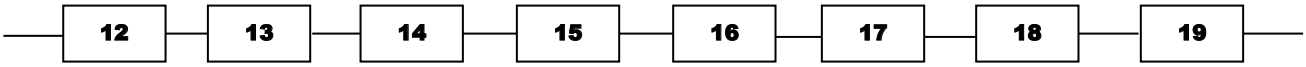
Reliability Block Diagram - Ineffective workforce



Reliability Block Diagram - Failure of plant due to diminished design specifications of



Reliability Block Diagram – Poor management decisions



Reliability Block Diagram – Poor maintenance of

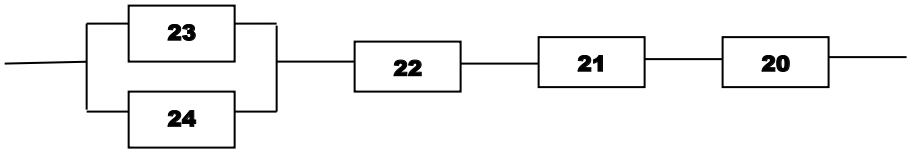


Figure 8: The equivalent RBD of the second model (adapted from Labib and Champaneri, 2012).

In the previous section it has been shown that the same case study can be viewed from different perspectives although the same modelling techniques were used. In the next section we explore few interesting research questions such as how to evaluate different models? And do multiple models lead to better understanding of the case study? And are there any practical guidance to follow when studying root cause analysis?

4. Discussion, feedback and evaluation:

FTA and RBD are considered valuable techniques that can be incorporated in the intellectual toolbox of engineers and decision makers. Constructing a model using these techniques is considered a sort of a design issue, where it involves iterations and it has been observed that experience plays a significant role.

But early management of these problems [safety, procedural and technological] is dependent on mental models that are consensually valid, experience-based, and informed by activity that clarifies puzzling cognitions. (Weick, 2010).

The idea of learning and then unlearning is of particular interest as the concept of unlearning has received relatively little attention in the literature. It can be argued that unlearning happens when a disaster is repeated. A disaster is by definition high impact low frequency. So unlearning occurs when both impact and frequency starts to be considered as 'high'. When such phenomena occurs it requires considerable restructuring and re organization and in some cases stopping the project altogether. For example, NASA experienced two accidents (Challenger and Columbia space shuttles) which led to the abandonment of the space shuttle programme (Handberg, 2014). Nuclear power generation experienced two major accidents (Chernobyl and Fukushima). As a result, some countries such as Germany, Denmark, and Italy decided to abandon this source of energy (Franchino, 2015). Air Malaysia had two major accidents within less than a year which led to a huge drop in sales and subsequently considerable restructuring (Lee, and Han, 2014).

According to Mahler (2009), there are three categories of lessons that organizations can derive from disasters: (1) not learned, (2) learned only superficially, or (3) learned and then subsequently unlearned. Using the same theoretical lens we can observe the three categories. The first one related to 'not leant' can manifest itself in the form of an organisation not aware about, or not capable of applying or willing to apply a mental modelling technique such as FTA or RBD. The second category of explaining the unlearning process relates to 'learned only superficially', which can be illustrated when an analysis based on a tool such as FTA is conducted but not followed or conducted without identification of the 'real' root cause. For example, recommendations could have been too general. The BP case can serve as a good example here. The BP Texas City refinery experienced a disaster when a flammable liquid caused an explosion and major fire. The CSB and the Baker's panel reports (Baker, 2007) concluded among many other findings that "BP emphasized personal safety, but not process safety". So it was this 'tick the box' mentality, which was a recipe for unlearning that can cause a drift to another disaster. So, five years after the Texas City disaster we had the Deepwater Horizon event at the Gulf of Mexico and BP was again held responsible for. The key issue about learning is not just admitting that learning has occurred but how this accident has been fed back to routines within the organization in a continuous adaptive way. The third category which relates to 'learned and then subsequently unlearned' can perhaps be illustrated by observation of the case of Bhopal itself. According to Abbasi and Abbasi (2005): '*the Vishakhapatnam disaster of 1997 reveals that most of the lessons of Bhopal seemed to have been forgotten'*. Another example of the 'unlearning' occurred at NASA which concerns its organizational structure. According to the Rogers report (1986), among the reasons for the Challenger disaster were the existence of rivalry among centres, different organizational cultures, lack of responsibility and accountability, and cross-centre communication issues which created information and coordination problems. After the disaster, the shuttle program was restructured into a centralized configuration which continued until the 1990s, but then reorganization occurred and the system was decentralized, to improve efficiencies; a policy of 'faster, better, and cheaper' according to Woods (2006). This policy of coping with pressures created the

conditions favouring the Columbia disaster which occurred after the Challenger disaster (CAIB, 2003). More details about NASA can be found in Labib (2014b).

An additional dimension of root cause of technological disasters is what Mansion and Evan (2002) call socio–cultural in nature. This refers to attitudes and values that are widely accepted by people in a society and which penetrate the attitudes and values of the corporate culture of various firms. Mansion and Evans (2002) make an observation that in designing the Union Carbide plant in Bhopal, management could not help but know of the pervasive poverty in that city of approximately two million people. In all likelihood, they observed in the local government the absence of concern with, and resources for, protecting the health and safety of its citizens. Hence, when designing the plant, engineers and planners paid little heed to the importance of building in fail-safe devices to protect Bhopal residents against gas leaks. After all, life in Bhopal was deemed not quite as valuable as in Institute, West Virginia, where Union Carbide had already built a comparable plant, making sure to provide additional redundant systems (Mansion and Evan, 2002). So, in short, in order to understand the causal factors of a man-made disaster, four factors have to be analysed: human, design, organizational and socio-cultural factors.

5. Methods to evaluate different models and practical guidance to follow when studying root cause analysis:

'*Any description should be two-faced, looking simultaneously to the world of data and to that of concepts*' (Cartwright, 1959, p. 13). Hence there will be an attempt here to utilise the lessons gained from the analysis of a specific disaster such as Bhopal to extract a higher level of learning of the techniques used. This will be achieved through the utilization of the concept of single and double loop learning which were defined by Argyris and Schon (1978). So using this theoretical lens, the analysis of Bhopal will be considered in term of an action and its consequence as single loop learning, whereas the governing tools used in terms of FTA and RBD as double-loop learning, where the emphasis will be on examining what generally makes a good analytical tool such as FTA. The main focus will be on FTA rather than RBD since the RBD is a natural outcome of the FTA.

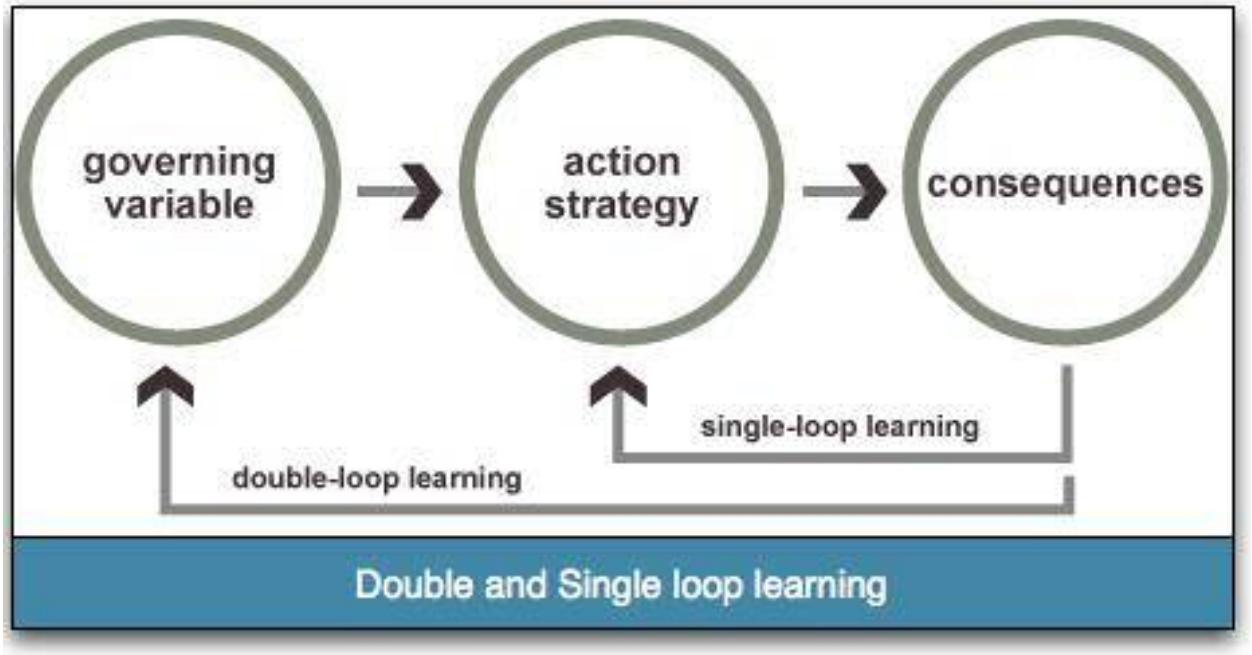


Figure 9: Double and Single Loop Learning - adapted from Argyris and Schon (1978).

Therefore, the intention of the first part of the analysis by the two models of Bhopal described in the previous sections was aimed to be 'efficient' in being able to identify causal factors of a specific case, whereas, by second loop learning, we generalise into being 'effective' in trying to identify best practice in using the tools in question (FTA, and RBD). Through the experience gained from being involved in the Bhopal workshops, one is able to provide an account of the following issues that are considered critical success factors for guidance in conducting analysis of future cases:

1 Multidisciplinary approach in the construction phase: For a good FTA analysis one needs a multiple disciplinary team. The saying of 'If you give someone a hammer, he will treat everything as a nail' is valid here. It was noticed that those groups who had multidisciplinary team members, generally, provided richer, and more comprehensive models than those teams who were not multidisciplinary in nature. This was evident especially in the brain storming phase of the analysis, where more possibilities of failure scenarios were generated from multidisciplinary team members.

2 Number of causal factors: When constructing a model fault tree the main challenge is the appropriate level of width and depth of the model. The trade-off involved is usually between simplicity and rigorous analysis. Regarding the width ie the number of nodes at each level, it is often suggested based on psychological studies (Miller, 1956) to limit the number of factors at any level of a hierarchical structure to 'the magic number seven plus or minus two'. The same guidance can be observed when constructing other decision models based on hierarchical structures such as the analytical hierarchy process (AHP) proposed by Saaty (1980) which also suggests to follow Miller's recommendations. As for the number of levels in an FTA hierarchical model the number of levels should be guided by the ability to reach a

'real' root cause, as described in the point below. It has been noticed from the two Bhopal models provided in the previous sections that the first model was on the threshold of simplicity, whereas the model provided by the second group was on the threshold of complexity.

3 Real root cause: The basic events of an FTA are considered to be the 'leaves' of the tree, the 'initiators' or 'root causes'. In an accident investigation, if a root cause is perceived as, for example, 'someone's behaviour' then it may be likely, as argued by Rasmussen (1997), that the accident could occur by another cause at another time. Such a root cause is superficial and should be regarded as a symptom rather than the real root cause which needs to be plan- and policy-related with respect to the current *status quo*. According to Labib (2014b) ideally the analysis should lead to initiation or modification of standard operating procedures (SOPs). Also, a root cause needs to contribute to the three features of how learning from failures is defined, as outlined by Labib and Read (2013), who argue that learning from failures means feedback to design of existing procedures, use of advanced techniques to analyse failures, and generation of interdisciplinary generic lessons.

4 When to use AND or OR Gates: It is generally accepted that the OR-gate indicates that the output event (top event) occurs only if one or more of the input events occur, and the AND-gate indicates that the output event occurs only if all the input faults occur at the same time. However, sometimes when analysing a disaster such as Bhopal, as compared to a certain machine failure, it was noticed that it is easily to confuse when to use a specific gate. Generally, in order to be in the safe side, the following rule applies: When in doubt use OR gate as it is better to assume a worst case scenario.

5 Tope event (An AND or an OR gate?) For the top gate of an FTA, one should follow the guidance offered to the second group of Bhopal as in the previous section which briefly states that for the top gate: use OR gate for a prospective analysis, and use an AND gate for a retrospective analysis. So if the analysis is intended to design a new system then we assume a pessimistic approach and hence an OR gate is preferable. Whereas if we are describing the event in a retrospective analysis (such as Bhopal), then it is expected that we use an AND gate where all the events occurred simultaneously and a domino effect has occurred where all safety barriers were breached. In the case of Bhopal, as it was 'an accident waiting to happen', and we were in doubt, we used an OR gate at the top of the tree.

6 Overcoming the interdependence limitation:. One of the limitations of any hierarchical structure such as the fault tree, which looks like a Christmas tree shape is that we implicitly assume, for simplicity, one linear direction. In other words, every child in the family tree belongs to one parent. In doing this we don't allow a node to be dependent on others; no child is allowed to belong to two fathers simultaneously. In order to overcome this limitation, one can repeat the interdependent basic elements. For example in the case of the first group model of Bhopal, it can be noticed that the basic event of 'no adequate training' is a causal factor for both branches; of 'lack of safety', and 'poor maintenance'. Hence the same basic node (number 5) in Figure 2, was repeated under both branches.

7 Challenge of being able to be succinct yet comprehensive. In other words ability to express a complicate phenomenon in few words that can fit in a box. Due to the limitation of the language (English Language or otherwise), it is often difficult to express an idea in a limited size box. Therefore one tend to use either abbreviation or be very selective in choosing small number of words to fit in the box. This filtering process might be a cause for confusion as different people might perceive the meaning of the contents in the box in different ways. The second group experienced such challenge especially because their model had plenty of boxes and it was difficult to limit the number of words used. It is a trade-off challenge and perhaps one way around it is to design software packages for such tools where a zooming facility is provided to give further explanation to the contents

6. Do multiple models lead to better understanding of the case study?

There is a school of thought which argues that using a model to analyze and investigate an accident may distract people who are carrying out the investigation, as they attempt to fit the accident to the model, which may limit free-thinking (Kletz, 2001). Whilst, in the view of the present author, this argument is valid, it can also be argued here that the use of a hybrid of models overcomes this issue as such an approach will lead to limiting the assumptions inherit in such models. Also, multiple models offer more views and hence enhances the richness of the understanding of the causal factors of the situation.

It is also argued here that safety is a system's feature and not a component property. Whilst reliability focuses on prevention of component failures, safety focusses on the 'total picture', and issues related to coupling and complexity of the whole system need to be analysed. Hence safety and reliability are not always positively correlated. A reliable system might be complex and coupled, for example due to the existence of redundancies involved and hence safety might suffer as a consequence. The analysis provided by FTA and RBD provides such system approach. This is to some extent in line with a school of thought who advocates a systems approach to technical and organizational safety which includes Rasmussen (1997), Hollnagel et al (2008), and Leveson et al (2009). The primary characteristics of this approach, according to Leveson et al (2009), are: 1) emphasis on top down systems thinking that emphasizes safety as whole system rather than a bottom-up approach that relies on reliability of components; 2) focus on the integrated socio-technical system as a whole; and 3) focus on modelling rather than try to specify general principles that apply to all organizations.

Although throughout this research work the tools used were found to be quite useful, but as with any other technique, one can also identify some limitations. The first main limitation is that the time element in terms of sequence of events is not captured in such analysis. The second limitation is the restrictive nature of the available optional gates which may over simplify the problem in question. The third limitation is the independence assumption. There are other reported methods in the literature which address some of these limitations, such as the Functional Resonance Accident Model (FRAM) by Hollnagel et al (2008), the Systems-Theoretic Accident Model and Processes (STAMP) method by Leveson et al (2009), and the by Socio-Technical Risk Analysis (SoTeRiA) Mohagheg and Mosleh (2009). These methods usually attempt to address a certain limitation in other methods but they themselves have their own limitations as well. Also there is always a trade-off between complexity of the proposed models and their inherit limitations. On the whole, our research shows that despite the existing limitation we were able to provide a mental model for understanding causal factors as well as provision of

guidance for constructing future models. We believe that such guidance may encourage researchers and practitioners to apply these techniques in other sectors as well.

7. Conclusion:

In this paper we discussed in-detail the roots of the Bhopal disaster. Then, we compared the case of Bhopal and Fukushima and presented the similarities between both disaster cases. Then, we went onto examining, through the literature review, how the high reliability organisations got safer and whether they actually did. We cited several studies in which authors argue that despite additional precautions, the accidents keep occurring. Subsequently, we discussed the data collection and presented the different models based on FTA and RBD analysis of Bhopal disaster. We showed how the same case study can be viewed from different perspectives despite using the same modelling techniques.

Moreover, the article examined how different models can be evaluated. It investigated whether multiple models lead to better understanding of the case study. It attempted to present the practical guidelines that can help to follow the root cause of the problem.

The main contribution of this paper is the provision of a mental model that can serve both as knowledge retention and a decision support tool. It also contributes by providing practitioners with a guide to follow the root cause of the problem, equips them with the tool box leading to more effective decision-making practices, process safety and environment protection. Several lessons can be learnt from this research, some of which (among other ones) are i) multidisciplinary approach in the construction phase, ii) consideration of causal factors and provision an appropriate width and depth of the model, iii) discovery of the 'real' root cause, iv) correct application of AND or OR Gates.

Acknowledgement:

The author is grateful to the participants at Universities of Portsmouth, Manchester and Glasgow Caledonian. Specifically the author is grateful to the groups involved in the Bhopal, and Fukushima projects. The author is grateful to the anonymous reviewer for the valuable comments that have helped us to improve the paper.

References:

1. Abbasi, T and Abbasi, S.A. (2005)"The Expertise And The Practice Of Loss Prevention In The Indian Process Industry: Some Pointers For The Third World",*Process Safety And Environmental Protection*, 83(B5): 413–420.
2. Argyris, C.; Schön, D. (1978). *Organizational Learning: A theory of action perspective*. Reading MA: Addison-Wesley. ISBN 0-201-00174-8.
3. Baker Panel.(2007). *The Report of the BP U.S. Refineries Independent Safety Review Panel. The Baker Panel*, Washington, DC.
4. Cartwright, D. (1959). "Lewinian theory as a contemporary systematic framework". In Koch, S. (Ed.), *Psychology: A Study of a Science. New York*: McGraw-Hill, 2, 7–91.
5. Chouhan, T.R. (2005). "The unfolding of Bhopal disaster", *J. Loss Prevent. Proc. Ind.* 18, 4–8.
6. Einstein A., and Infield, L., (1938). *The evolution of physics*, Simon and Schuster, New York.

7. Franchino, F., The social bases to nuclear energy policies in Europe: Ideology, proximity, belief updating and attitudes to risk, European Journal of Political Research (forthcoming), pp1-140, 2015.
8. Handberg, R., Human spaceflight and presidential agendas: Niche policies and NASA, opportunity and failure, Technology in Society, 39, 31-34, 2014.
9. Hollnagel, E., Pruchnicki, S., Woltjer, R., Etcher, S(2008) "Analysis of Comair flight 5191 with the Functional Resonance Accident Model", *8th International Symposium of the Australian Aviation Psychology Association*, Sydney Australia.
10. Ishizaka A, Labib A. (2014)"A Hybrid and Integrated Approach to Evaluate and Prevent Disasters", *Journal of Operational Research Society (JORS)*, 65(10), pp 1475-1489.
11. Kletz, T.A., (1993). *Lessons from Disaster: How Organizations Have No Memory and Accidents Recur*. Gulf Professional Publishing.
12. Kletz, T, (2001). *Learning from Accidents*, Butterworth-Heinmann, Oxford.
13. Kletz, T.A. (2006)"Accident investigation: Keep asking "why?" ", *Journal of Hazardous Materials*, 1 30, 69-75.
14. Kurokawa, (2012) National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission (NAIIC).
15. Labib, A. and Champaneri, R. (2012). "The Bhopal Disaster – learning from failures and evaluating risk",*Journal of Maintenance & Asset Management*, 27 (3), 41-47.
16. Labib, A., and Read, M. (2013) "Not Just Rearranging the Deckchairs on the Titanic: Learning from Failures through Risk and Reliability Analysis", *Safety Science*, 51, 497-413.
17. Labib, A. (a). (2014) "Learning how to Learn from Failures: The Case of Fukushima Nuclear Disaster", *Probability and Safety Assessment Management (PSAM)*12, 22-27 Honolulu, Hawaii, USA.
18. Labib, A. (b) (2014), *Learning from Failures: Decision Analysis of Major Disasters*, Butterworth-Heinemann, Oxford, 450 p.
19. Labib, Ashraf, and Harris, John, Learning how to learn from failures: the Fukushima nuclear disaster, Engineering Failure Analysis, 47 (2015) 117–128.
20. Lee, C., and Han, L., Faith-based organization and transnational voluntarism in China: A case study of the Malaysia Airline MH370 incident, VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations, pp1-12, 2014.
21. Leveson N., Dulac N., Marais K., Carroll J. (2009) "Moving beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems" *Organization Studies*, 30 (2-3) , pp. 227-249.
22. Mahler, J.G. (2009). *Organizational Learning at NASA: The Challenger and Columbia Accidents*., Washington, DC: Georgetown UniversityPress.
23. Miller, G. (1956) "The magical number seven plus or minus two: some limits on our capacity of processing information", *Psychological Rev*., Vol 63, pp 81-97.
24. Mohagheg, Z, and Mosleh, A., (2009) Measurement techniques for organizational safety causal models: Characterization and suggestions for enhancements, Safety Science, Volume 47, Issue 10, Pages 1398–1409
25. Pate-Cornell, E., (2012) On "black swan" and "perfect storm": Risk analysis and management when statistics are not enough, *Risk Analysis*, Vol 32, No 11.
26. Qi, R., Prem, K.P., Ng, D., Rana, M.A., Yun, G., Mannan, M.S. (2012) "Challenges and needs for process safety in the new millennium", *Process Safety and Environmental Protection*, 9 0, 91–100.

27. Rasmussen, J., (1997), "Risk management in a dynamic society: a modelling problem", *Safety Science* 27/2, pp 183-213.
28. Reason JT. (1997) *Managing the risks of organizational accidents.* Aldershot, Hants, England; Brookfield, Vermont: Ashgate; USA.
29. Saaty, T.L. (1980). *The Analytic Hierarchy Process*. New York. NY. U.S.A.: McGraw-Hill International.
30. Sørensen, J. N., Apostolakis, G. E., Kress, T. S., & Powers, D. A. (1999). "On the role of defense in depth in risk-informed regulation". In Proceedings of the PSA '99. International topical meeting on probabilistic safety assessment, Washington, DC, August 22e26, (pp. 408e413). La Grange Park, Illinois: American Nuclear Society
31. SPE (2014) The Process at the Bhopal Plant -Ref: Adapted from SPE (http://www.spe.org/news/article/what-caused-the-deadliest-industrial-accident-in-history)- accessed 20/8/2014.
32. Taleb, N. N., (2010) The Black Swan: The Impact of the Highly Improbable, Penguin Books.
33. Taniguchi, K., and D'Agostino, C. (2012) The catastrophes and the combined failures of institutions, Part 1: A comparison of Fukushima and Minamata, Keio Business Review, No 47, pp 1-14.
34. Taniguchi, K., and D'Agostino, C. (2012)The catastrophes and the combined failures of institutions, Part II: A comparison of Fukushima and Minamata, Keio Business Review, No 47, pp 15-29.
35. Taniguchi, K. (2012), The Japanese capitalism and Fukushima: Institutional failures and dynamic capabilities. Tokyo: Keio University Press (in Japanese).
36. Weik, K.E. (2010) Reflections on enacted sensemaking in the Bhopal disaster, Journal of Management Studies, 47:3, 537-550.
37. Weightman, M. (2013) Fukushima – A failure of institutional defence in depth, International conference on topical issues in nuclear installation safety: defence in depth, 21-24 October, IAEA, Vienna.