**An innovative application of the Advanced Recursive Operability Analysis to the Bhopal Accident Reconstruction**

Federico Florit1, Marco Barozzi2, Martina Silvia Scotton2, Sabrina Copelli2\*

*1 Politecnico di Milano, Dipartimento di Chimica, Materiali ed Ingegneria Chimica “G. Natta”, via Mancinelli 7, Milano (MI), IT*

*2 Università degli Studi dell’Insubria, Dipartimento di Scienza e Alta Tecnologia, via Valleggio 9, Como (CO), IT*

*\* Corresponding author E-Mail: sabrina.copelli@uninsubria.it*

**1. Introduction**

Nowadays chemical industry plays a leading role in our daily life, satisfying the needs of a large portion of the world population. The safety of chemical products is guaranteed by rigorous standards and control systems, which lead the chemistry sector to be one of the most prepared and equipped industrial sectors in terms of safety and health at work. Nevertheless, it is important to remember that the current success in terms of awareness and perception of chemical hazards owes much of its development to the lessons learned, at great cost, after the occurrence of catastrophic accidents.

The 70s and 80s were the scene of some of the biggest industrial accidents in the world, among which we can find the disasters of Flixborough, Seveso and Pasadena. But historically, the most serious accident is undoubtedly the Bhopal disaster. We will never know the precise number of people who died that terrible night; however, more than 25,000 victims were estimated and more than 120,000 people still suffer today from discomfort due to MIC exposure.

Aim of this work was to demonstrate, using an Advanced Recursive Operability Analysis (AROA)[1,2], that the dynamics of whatever accidental scenario can be always traced whether a non-standard Hazard Identification (HI) procedure is carried out on the final operative plant. The terms “non-standard” refers to an analysis carried out under operative conditions which deviate from the normal plant operations (with respect to all process variables deviations are normally computed), e.g. during a temporary shut-down.

In the Bhopal case study, the presence of such non-standard operative conditions had led to multiple losses of safety at very different levels: plant equipment operations, control systems efficiency, presence of active protective measures and ad hoc procedures to be followed by the operators in case of emergency. Such losses of safety could not be traced carrying out a standard HI procedure.

**2. Methods**

Quantitative Risk Analysis (QRA) is a complex task performed to either quantify or minimize the hazards associated with the operation of potentially dangerous installations. A QRA procedure can be ideally subdivided into four main phases: 1) Hazards Identification (HI); 2) Frequency Estimation (FE); 3) Accident Consequence Evaluation (ACE); 4) Individual and Societal Risk Calculation (I&SRC). This work considers only the first two phases. Hazard identification represents a fundamental activity: not identified hazards will remain hidden until the occurrence of the related accidents. Among the various available methodologies, HazOp is the most known and widely applied. On the other hand, the probabilistic quantification of the hazardous states frequency is usually done using a Fault Tree Analysis (FTA). Unfortunately, FTA is a time-consuming task because of the general difficulty of extracting the necessary information from HazOp tables. To make FTA less expensive, an Advanced Recursive Operability Analysis (AROA) was applied to the portion of the plant involved in the Bhopal accident. AROA is based on a procedure which allows collecting plant perturbations data in a structured way. At the end of the AROA study, it is possible to systematically construct all fault trees of interest.

A typical AROA format presents the following fields to be correctly compiled:

1. Node – Process variable – Deviation

2. Causes

3. Consequences due to failure of safety functions

4. Plant state following the correct intervention of safety functions

5. Protections, made up by: a. Alarms; b. Operator actions; c. Automatic safety systems

6. Remarks

The AROA format must be used exclusively to collect information on the relationships between process variables deviations. Indeed, with the aim of simplifying the work of the HazOp team (i.e. to reduce the cost of HazOp analysis), the information to be collected will concern mainly plant perturbations (i.e. the relationships among cause-consequences of process variables deviations) leaving out the construction of fault trees of protection and control systems, as well as the analysis of spurious failures.

In the present work, an AROA was applied considering the deviations of the different process variables with respect to the non-standard state of the plant (that was, for the Bhopal plant, a shutdown state before plant dismissing). This is an important difference with respect to all the already presented applications of the ROA, which consider deviations from standard (or normal) operative conditions of the plant. Such a modification was necessary to correctly describe the dynamics of the Bhopal accident.

**3. Results and discussion**

Figure 1 reports the simplified P&ID of the portion of the Bhopal plant involved in the accident.



**Figure 1.** Simplified P&ID of the Bhopal plant (portion involved in the accident).

Referring to the P&ID reported in Figure 1, the system can be divided into 2 nodes:

* Node 1: identifies all the lines and equipment belonging to the E-610 tank. Process variables considered and their deviations (between square brackets) are reported in the following:

1. (L) MIC level [h]
2. (T) Temperature [h]
3. (P) Pressure [h, hh, hhh]

* Node 2: identifies all the lines and instrumentation belonging to the safety devices (Vent Gas Scrubber - VGS and torch). Process variables considered and their deviations (between square brackets) are reported in the following:

1. (FSC) Flow rate of caustic soda [l]
2. (FMIC) MIC Flow rate [h]
3. (CMIC) MIC concentration in atmosphere [h]

The deviations indicated by the letters in the square brackets stand for high (h) and low (l). The repetition of the letter expresses an intensification of the deviation. For example (hh.P) symbolizes a very high pressure, while (hhh.P) corresponds to an even greater pressure. The information is represented using a classic AROA model in Table 1.

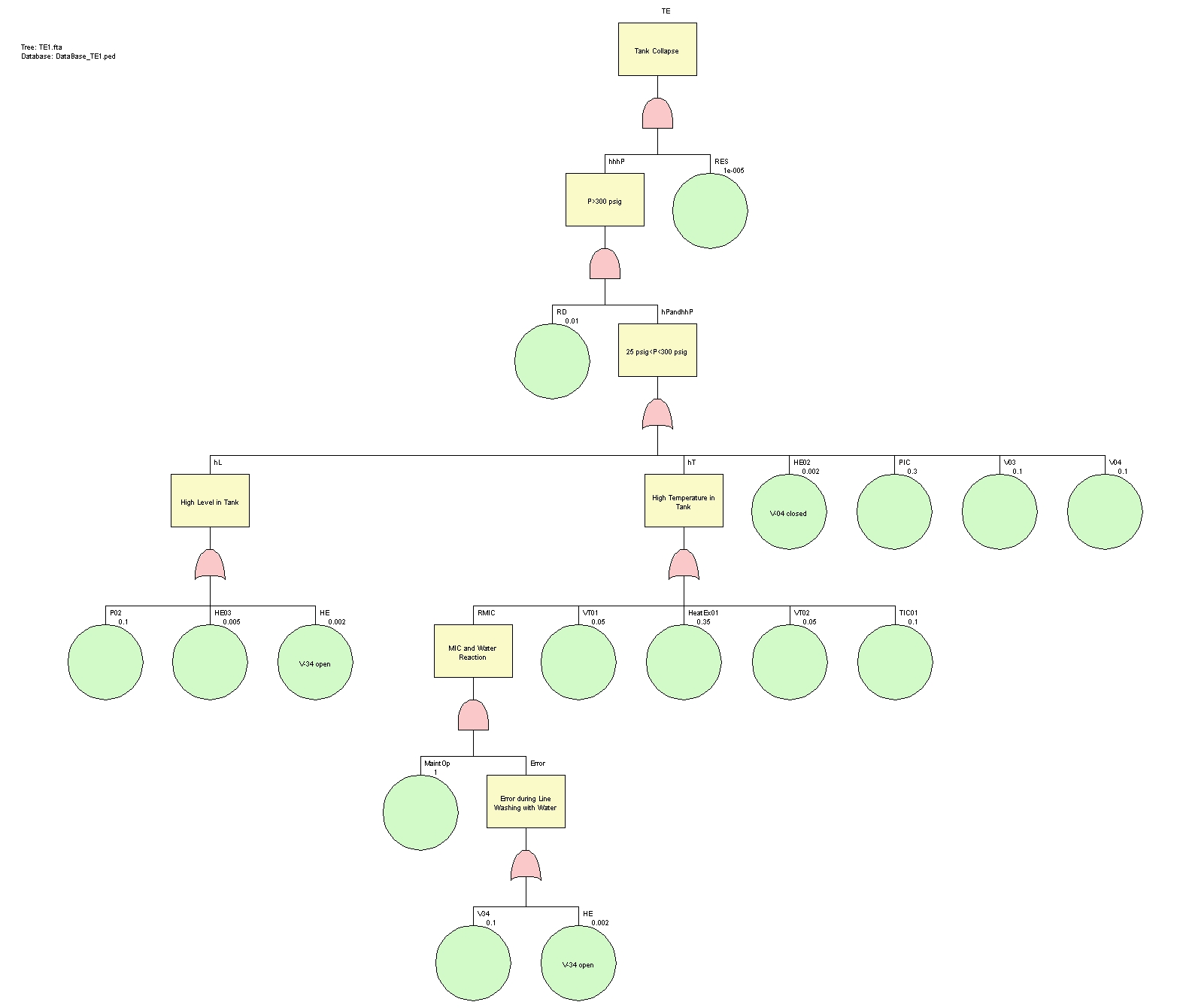
**Table 1.** AROA of the Bhopal plant (accident section)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Node 1: Tank E-610** | | | | | | | | |
| **REC** | **Node-Deviation-Variable** | **Causes** | **Consequences due to protections failure** | **Plant state following the correct intervention of safety functions** | **Alarms** | **Operator Actions** | **Automatic safety systems** | **Top Event** |
| 1 | 1.h.L  [%]  (L>50) | P-02 fail to operate  OR  Human Error (Excessive MIC Loading or V-34 open) | 1.h.P | Normal Level State due to Human Action | LIAH-01 | Manual intervention on V-34 | - | No |
| 2 | MIC reaction with water | Water (from cleaning operations)  AND  Human Error (V-34 open) | 1.h.T | 1.h.T | - | - | - | No |
| 3 | 1.h.T  [°C]  (T>11) | **REC 2**  OR  HE-01 no cooling  OR  P-01 fail to operate  OR  VT-01 fail closed  OR  VT-02 fail closed  OR  TIC-01 fail low | 1.h.P | 1.h.P | TAH-01 | Check on HE-01 | - | No |
| 4 | 1.h.P  [psig]  (25<P<40) | 1.h.L  OR  1.h.T  OR  PIC-01 fail low  OR  V-03 fail closed  OR  V-04 closed (fail closed OR HE) | 1.hh.P  2.h.FMIC | 1.hh.P | - | - | **-** | No |
| 5 | **1.hh.P**  **[psig]**  **(40<P<300)** | 1.h.P | 1.hhh.P | Discharge to VGS  (**2.h.FMIC**) | - | **-** | RD-01  **SRV-01** | **No** |
| 6 | 1.hhh.P  [psig)]  (P>300) | 1.hh.P | **Tank collapse** | **Tank Damaged but not collapsed** | - | **-** | **Resistance to Rupture** | **TE1** |
| **Node 2: Vent Gas Scrubber and Node 3: Torch** | | | | | | | | |
| **REC** | **Node-Deviation-Variable** | **Causes** | **Consequences due to protections failure** | **Plant state following the correct intervention of safety functions** | **Alarms** | **Operator Actions** | **Automatic safety systems** | **Top Event** |
| 7 | 2.l.FSC | P-03 fail to operate  OR  VT-27 fail closed | 2.h.FMIC | 2.h.FMIC | FAL-02 | - | - | No |
| 8 | 2.h.FMIC | **REC 4**  OR  2.l.FSC  OR  **REC 5\*** | 3.h.FMIC | CMIC<TLV (atm) | - | - | FL-01 | No |
| 9 | 3.h.FMIC | 2.h.FMIC | CMIC>>TLV  (**Toxic Release)** | CMIC>>TLV  (**Toxic Release)** | - | - | - | **TE2** |

Analyzing Table 1, two main potential Top Events (TEs) can be easily identified:

1. The physical collapse of E-610 tank due to an uncontrolled increase in pressure beyond the maximum tolerable value;
2. The release of toxic gas into the atmosphere if both VGS and flare fail to intervene.

Starting from the AROA Table, it was possible to automatically generate the related FTs. As the sake of example, Figure 2 reports the Fault Tree corresponding to TE1.



**Figure 2.** Fault tree for TE1.

From the calculation of the fault tree related to Node 1, we found the presence of 12 Minimal Cut Sets (MCS) 11 of order 3 and 1 of order 4, with respect to a total number of primary events which was equal to 15. The calculated TE probability was: 7.59 10-8; such a value can be considered as acceptable because it is lower than the usually adopted reference value of 10-6 (base: 1 year of mission time). Concerning the relative importance of the different components of the system in determining the TE (collapse of the tank), we found that the failure of the rupture disk (RD) and the exceeding of the resistance of the tank material are the most important components, followed by the heat exchanger (HE-01) and the tank pressure controller (PIC-01). All these components must receive more attention with respect to the others; this means that they must be subjected to frequent maintenance operations because they contribute heavily to the occurrence of the TE.

Regarding the tree related to Node 2, 13 MCS of order 2 and 1 of order 3 were calculated (over 17 total primary events). The calculated probability value obtained was 7.94 10-1 that, considering a risk acceptability value equal to 10-6, is a not acceptable value. The calculation showed that the flare together with the failure of the heat exchanger unit and the pressure controller constituted the most important components of the plant and, therefore, should have required greater attention and maintenance.

It is important to notice that, considering the state of “temporary shutdown” of the plant, the unavailability of the flare is 1; in case of normal operating conditions such a value would have been 2 or 3 order of magnitude lower. This is a very interesting point which highlights the importance of considering the deviations not only from normal plant state but also from upset plant state due to temporary operations.

**4. Conclusions**

This work highlighted how fundamental the contribution of a complete and adequate risk analysis is in the field of industrial prevention of potentially dangerous scenarios such as major accidents.

From the recursive operability analysis related to E-610 tank and associated equipment, it was found that the release of toxic gas into the atmosphere was to be considered as the worst unwanted event. Of course, it should be noted that the analysis carried out concerned only the E-610 system, which represented only a small part of a much larger and more complex plant. Assuming a detailed study of all the subsystems of the Bhopal chemical industry, countless TEs of similar nature to the one here analyzed could have been traced.

Using a modified version of the AROA it was possible to demonstrate that the dynamics of the Bhopal disaster was similar to that of all the major industrial chemical accidents: some deviations of the process variables have occurred when the plant was operating in a non-standard state as either a temporary shutdown or a maintenance, etc..

The lack of suitable procedures and protection devices specifically designed to operate when the plant is in a non-standard state is the first point of “no return” which foregoes the occurrence of an industrial accident: such evidence was demonstrated even in the case of Bhopal accident.

**References**

1. P.M. Contini, S. Contini, S. Copelli, R. Rota, M. Demichela, Safety and Reliability of Complex Engineered Systems - Proceedings of the 25th European Safety and Reliability Conference, ESREL 2015 (2015) 347-355
2. M. Barozzi, S. Contini, M. Raboni, V. Torretta, V. Casson Moreno, S. Copelli, Journal of Loss Prevention in the Process Industries 71 (2021) art. no. 104468