Assessment of two accidents involving safety devices

Jean-François Lechaudel, Sylvie Bauchet

ASSESSMENT OF TWO ACCIDENTS INVOLVING SAFETY DEVICES

J.F. Lechaudel, S. Bauchet

INERIS

Verneuil-en-Halatte, France.

ABSTRACT

This paper mainly aims at describing and analysing two accidents : an ammonia leakage and an explosion in a chemical unit. These accidents are in connection with safety equipment failures. Lessons are pointed out for each accident and, finally, conclusions are drawn about possible requirements for safety devices and the interest of testing them.

1. INTRODUCTION

In relation to the real or supposed risks, the actions currently carried out generally consist in setting up devices known as «safety devices» to reduce the occurrence or the gravity of potential accidents.

These devices are sometimes passive (walls, retention) but generally active, in the sense that they require at least a source of energy or a sequence of activation.

These devices are frequently described as « safe », proof of the confidence which is primarily granted to them, but these qualities are not always related to explicitly defined criteria.

INERIS, BP N°2 60550 VERNEUIL-EN-HALATTE

9th International Symposium Loss Prevention and Safety Promotion
in the Process Industries, Barcelone, 4-8 mai 1998

The application of prescriptions associated with the regulations resulting from the « SEVESO Directive » (/1/) also tends to multiply the recourse to such devices, the risk being « to collect them » and to expose themselves to their own failures. To a certain extent, the failure of these « safety devices », on sites where modifications have been undertaken, makes it possible to qualify some recent accidents as « post-SEVESO accidents ».

This paper presents briefly hereafter two of these accidents. An ammonia leakage on a rail tank cars unloading installation and an explosion in a chemical unit. In addition to the lessons which can be drawn directly from those, this article reminds, in conclusion, important requirements for the qualification of these « safety devices ».

2. AMMONIA LEAKAGE (DECEMBER 16, 1994)

2.1 SUMMARY OF THE EVENT

The diagram (see Figure 1) hereafter represents the installation concerned.

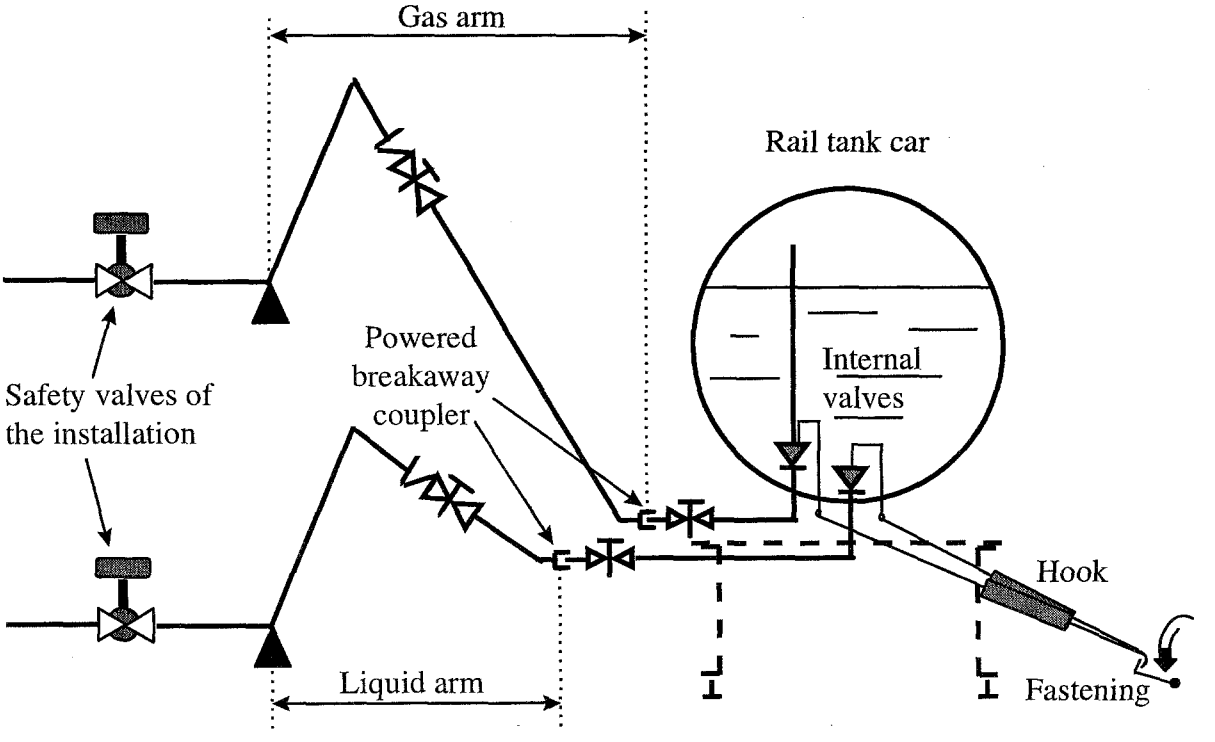

Figure 1: Diagram of the rail tank cars unloading installation .

During an operation of unloading ammonia from a tank car, an arm of transfer is disconnected brutally a few minutes after the beginning of the operation. An escape on the liquid phase occurs.

Several actions on the emergency stops remain ineffective and the hook fastening, maintaining the valve of the car, does not open. The formed cloud prevents any access to the chemical protection suits located near the unloading installation.

A foreman of the installation back turn to the wind, equipped with a simple mask, makes profit from the immobility of the arm and a momentary transfer of the aerosols cloud to approach at ten meters from the car. He then succeeds in launching a wheel block on the hook. This one unhooks from its housing and makes fall the valve from the car, thus stopping the ammonia escape.

The quantity of ammonia rejected is approximately 27 tons, in 37 minutes. Nobody was wounded. Ammonia odours are perceived up to 8 km downwind.

2.2 ANALYSIS (/2/)

This installation was equipped with an automatic device of disconnection for the transfer arm (loading or unloading), called « powered breakaway coupler ». The breakaway sequence was engaged as soon as a movement of car was detected on the track. The objective was to put the installation in a secure state, with respect to the potential consequences of a collision between the car being unloaded and another car. This device was an additional one compared to the traditional safety arrangements at the time of unloading operations.

The analysis of this accident showed that the detection device for the approach of a car on the track was the initiating event of this accident. An order (output signal) was generated by this device, following probably some operations on the track.

As much the initiating event has an unspecified cause, as much the induced events occurred according to the programmed sequence. They correspond to an awaited response of the automatism.

In particular, the electronic control system started the automatic procedure of disconnection of the transfer arms. The gas phase safety valves of the arm were well closed. The same applies to the safety valves isolating the units. Unfortunately, on car side, the liquid phase valve of the powered breakaway coupler remained wedged by a nut. Moreover, the hook which was to jump automatically at the time of an emergency procedure remained hung in its fastening.

According to the research undertaken by the company, the nut (standard M16HH) which blocked the liquid phase valve of the arm, on car side, does not originate from the material used in the factory. Its origin remains unknown to date. It should be noted that the presence of nuts, preventing the dissociation of two elements of a loading arm, had already been observed a few months earlier.

During the analysis of this accident, several anomalies could be highlighted. In particular, it is possible to point out :

- the order of tilting the pneumatic hook fastening was maintained only during the safety valve closing. The detection of the end of the safety valve closing annihilated any order of tilting the fastening ;
- In addition, at the electronic control system level, the sequence setting in safety, started by the emergency stops, should have rocked open the fastening of the hook. In fact, this sequence of setting in safety was activated only when someone pressed on the button. It was stopped in the event of relaxation of this button. The order given by the action on the emergency stop was thus fugitive or not maintained ;
- the hook position on its fastening could give a mechanical jamming, even in the event of effective fastening tilting.

2.3 LESSONS

This accident results from a double failure : non releasing of the hook and wedging by a nut in partially open position of the liquid phase valve arm, on car side.

The principal lessons of this accident within the framework of this article are :

- the possible mechanical failures should be taken into consideration, whether they are specific to the system such as mechanical jamming or resulting from an external event (for example, presence of foreign bodies in the installation) ;
- A validation, using in particular tests of the actions performed by the « safety loop » would probably have made it possible to detect several anomalies ;
- Lastly, the ultimate barrier, consisting in the intervention of equipped personnel, must be organised : adequate equipment for the personnel out of the accident potential effect zone and devices on the installation facilitating the approach and the operations.

3. EXPLOSION IN A CHEMICAL UNIT (MAY 18, 1996)

3.1 SUMMARY

At 5 :34, the lightning causes an important decrease of voltage during 140 ms on the 90 kV power supply network of a chemical plant. As a result, for one chemical unit, a switch occurs between the power alimentation and the emergency power unit. After this voltage variation, the normal voltage input does not change anything, because of an emergency power unit internal 16 minutes time lag programmation.

For this installation, in these conditions, the emergency power unit tries to take over, without success.

So the 220 volts and 24 volts tension (see Figure 3) delivered by the emergency power unit decreases gradually and various equipment are stop. The « double-effect » valves, normally staying in the same status, open and particularly the valves which allowed the decompression of the gas network for all reactors. It should be noted that, by design, the gas mixture is flammable in the gas network in connection with the reactors.

Consequently, a flammable mixture is evacuated by a chimney. Moreover, the opening of these valves allows a continuity between the sky of the reactors and the atmosphere at the exit of the chimney.

The available elements make it possible to locate the beginning of the process of explosion a few minutes later, when the release through the chimney is quite evanescent. At 5 :41, the lightning strikes the unit, ignites the flammable release and makes possible to a flame front to propagate through pipes and equipment in communication together. Three apparatus break successively : a cyclone, a tank and a reactor. As example, the photography hereafter (see Figure 2) represents the destroyed reactor.

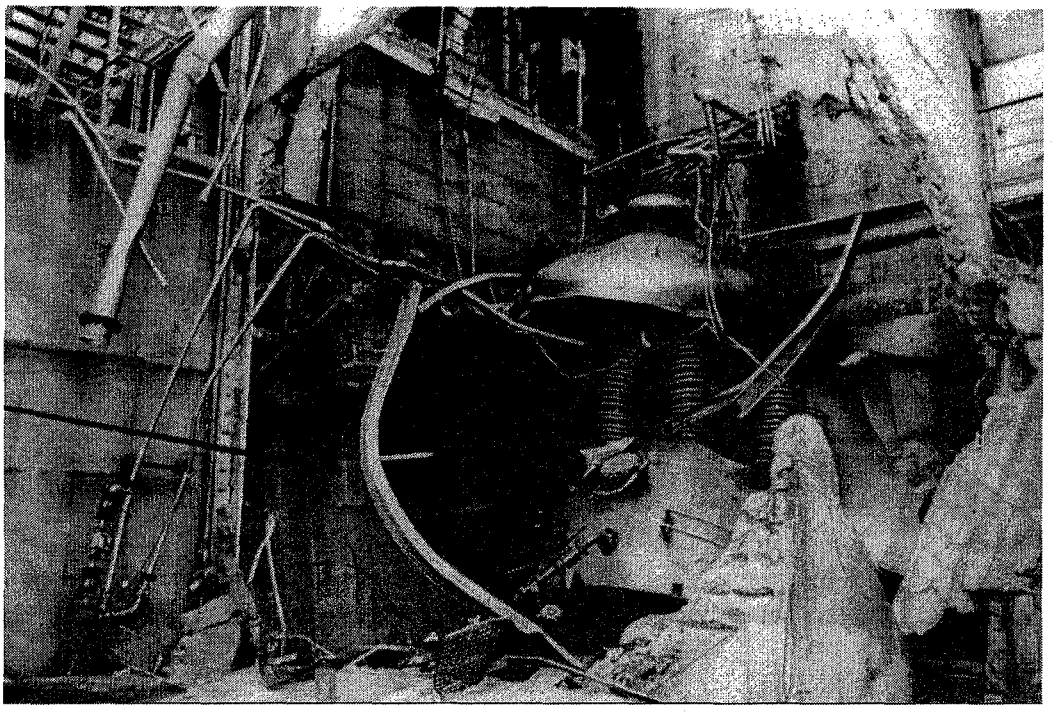

Figure 2: view of the destroyed reactor.

3.2 ANALYSIS (/3/)

This accidental sequence seems to have a low probability. In fact, this one was evaluated with less than 10^{-5}. It is mainly fixed by the probability of having an impact of the lightning on the installation while the gas sky of the reactors is in direct communication with the chimney.

Two elements come into view for this sequence :

- the malfunction of the emergency power unit ;
- the opening of the « double-effect » valves.

3.2.1 Emergency power unit

The first failure is associated with the malfunction of the emergency power unit (group called «time zero »). It can be noted that the control of this relatively old equipment was ensured by a group of electromechanical relays. The further analysis carried out underlined that the possible causes of its absence of operation were numerous (14 possibilities) and some of them could be random (for example, a defective contact). Beyond these elements, the principal point which can be retained for this equipment is the fact that such an electrical power variation was not taken into account in the design specifications of the material.

3.2.2 « Double-effect » valves.

The second failure or situation not dealt with, was the opening of the « double-effect » valves which were normally to be remained in their initial state. The figure hereafter (see Figure 3) represents the different parts of the control chain for these valves.

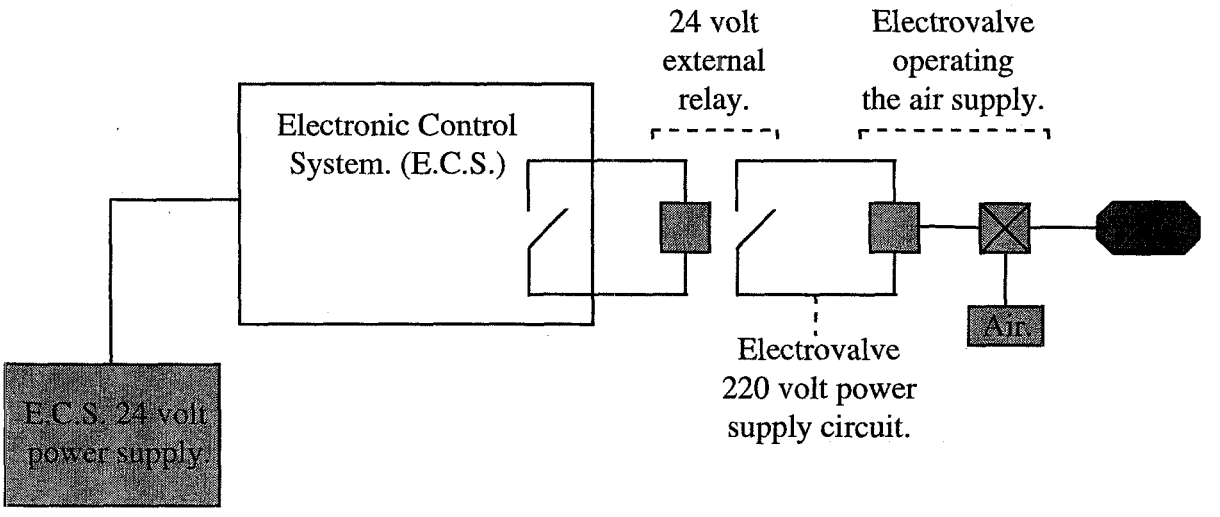

Figure 3: Diagram of the control chain of the « double-effect » valves.

In the case of a decreasing voltage, the tests carried out on the electronic control system and the equipment associated made it possible to retain the following sequence :

the electronic control system stops, prohibiting any operation.

↓

the 24 volt relay falls in preferential position
(rest = open).

↓

the electrovalve is actuated because relay falls and at the release voltage, it remains manoeuvrable.

↓

the « double-effect » valves open.

The decreasing voltage to the entry of the various equipment caused a stop of the former in an anforeseen state, not allowing to keep the « double-effect » valves in the initial state.

In this case also, the characteristics of the electrical alimentation was not taken into account in the design specifications for the electronic control system and the automatic system of the valves.

3.3 LESSONS

The principal lessons of this accident within the framework of this article are :

- the devices or equipment of safety having recourse to automatism are obviously not free from potential failures (for example, emergency power unit) ;
- the definition of the operating range of the important equipment for safety should be defined. This operating range should be, as far as possible, the subject of a qualification performed in particular by tests ;
- in this respect, concerning the tests and qualification of equipment, this accident underlines the interactions between several equipment. Consequently, possible tests should check the whole of a safety loop.

4. CONCLUSION ABOUT REQUIREMENTS FOR SAFETY DEVICES.

The two accidents described above underline failures of safety systems, which are mechanical or associated with automatic devices. These failures emphasise the need of the operating range definition of these systems and their qualification.

In this field, the draft standard IEC 61508 (/4/), relating to the safety of the electric, electronic systems and programmable systems, and its adaptation to the industrial processes through draft standard IEC 61511 (/5/), make it possible to fix a framework of evaluation. For details, the method associated with this last draft standard is declined in four parts :

- Analysis and ranking of the risks of an installation ;
- Definition of the technical requirements applicable to the safety devices, this definition being carried out through classes of requirements ;
- Definition of the qualitative and quantitative requirements ;
- Validation of the technical requirements (analyses or tests).

Beyond a theoretical analysis, the interest to use tests comes out from these accidents, as suggested by Kletz (/6/) for others accidents. In this respect, the draft standard IEC 1511 (//) indicates that the validation of the technical requirements can be treated through tests : functional tests of safety ; tests of behaviour on defect ; tests related on the specifications and the environmental parameters.
Such tests must take into account the whole of the « safety loop », including, for example a sensor, an electronic control system and equipment such as valves. Moreover, the mechanical behaviour of the equipment should also be tested. The accidents reported above point it out.
Beyond these considerations, it appears important that this qualification of the safety devices lies within a more general scope of evaluation of defence lines or defence barriers (/7/), with respect to the dangers within an industrial facility. Such an approach is to be undertaken at the design stage of a plant or before safety devices modifications.
An evaluation scheme must also integrate the ultimate barrier made up by the intervention of equipped personnel.

5. REFERENCES

1. SEVESO directive
   Directives N° 82/501/CEE 24/06/1982 and N° 96/82/CEE 09/12/1996.
2. Lechaudel J-F. and Bauchet S.
   INERIS report, EMA-JLc/CDx-26FA52, (1995).
3. Lechaudel J-F., Davrou C., Halama S. and Masson F.
   INERIS report, EMA-JLc/Cse-1996-26FC47, (1996).
4. IEC 61508, Functional safety of electrical , electronic, programmable electronic safety related systems.
5. IEC 61511, Functional safety : Safety instrumented systems for the process industry.
6. Kletz T.
   Learning from accidents in industry.
   Butterworth & Co., ISBN 0-408-02696-0, (1988).
7. Maddison T.E., Kirk P.G. and Martin M.
   Application of pilot risk study methods to the safety inspection of industrial plant; Loss Prevention Bulletin n°125, pp11-16 (1996).