Journal of Loss Prevention in the Process Industries xxx (2016) 1–6

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp

Limitations of current risk assessment methods to foresee emerging risks: Towards a new methodology?

Jean Escande [a], Christophe Proust [a, b, *], Jean Christophe Le Coze [b]

[a] Sorbonne University, Technological University of Compiègne, TIMR Lab., 60200 Compiègne, France
[b] INERIS, Parc Technologique ALATA, BP2, 60550 Verneuil-en-Halatte, France

A R T I C L E I N F O

Article history:
Received 11 March 2016
Received in revised form
31 May 2016
Accepted 20 June 2016
Available online xxx

Keywords:
Decision engineering
Hazards identification
Management and planning
Safety

A B S T R A C T

The objective of this work-in-progress is to investigate the potentialities but also the limitations of traditional risks analysis tools especially in the context of emerging technologies and develop a method facilitating the early detection of scenarios of accidents. This is certainly a challenge particularly for new industrial fields since, in this case, very little or no lesson from past accidents is available. It is believed that such situations cannot be conveniently treated using traditional risk assessment methods (HAZOP, FMEA, …) and typical examples are given. The reason is that those methods rely heavily on past accidents and are therefore "trapped" in them so that they are largely "inductive". In terms of foreseeing the future, the shortcomings of inductive methods are recalled. The possibility to imagine the future with very little clues is then discussed on the ground of theoretical consideration and a way to do so is proposed (abduction, serendipity). Then on the basis of the observation of how the experts work and how discoveries are made, a potential new methodology is outlined.

1. Introduction

To identify, rank and control industrial risks a significant number of tools is nowadays available which seems to satisfy the users. Among these tools, ready to use packaged methods such that FMEA, HAZOP, Bow Tie diagrams, … are largely taught in universities and may even be available in laptop softwares (Vinnem, 2014).

Being largely used, those methods and their results have also been, for long, criticized (Mannan, 2012). In particular, they might be ill adapted to emerging technologies because primarily of the lack of feedback from accidents/incidents and secondly because, as they stand (or are currently used) today (in standards, in computer programs, spreadsheet, …) they would lack flexibility to accommodate for totally new situations.

The difficulty is certainly very real since, despite an extensive use of such methods, the Challenger accident of NASA in 1986 or the Fukushima disaster in 2011 did happen. If in very well resourced industrial domains, such as the space and the nuclear industry, where a high level of expertise is available, extreme events of this kind occur, there is certainly still much more to explore about the limits of risk assessment exercises.

So what can go wrong with the risk analysis methods?

Investigating the limitations of engineering knowledge and the practice of risk analysis is not particularly new because the question of "the unexpected occurrence" is a central issue (Weick and Sutcliffe, 2007; Le Coze, 2016). Early examples exists (Turner, 1978; Perrow, 1984) but more recent ones too (Tierney, 2010; Downer, 2011), suggesting this concern has been lasting for long. The subjective part of the risk assessment is particularly stressed out which is far away from the rational aspects of the relevant methods which are traditionally taught in universities. But risk or safety can also be understood as social constructions (Aven, 2012; Le Coze, 2012).

Note first that HAZOP or FMEA, two major risk analysis methods, were developed in the sixties to help the "safe" development of emerging technologies of that period of time ! New chemical plants, nuclear power plants, nuclear weapons, aviation, space industry… within sometimes (especially nuclear developments) a context of very limited feedback from experience … Second, despite some severe pitfalls, the related systems (nuclear plant, planes, rockets, …) have over time achieved an acceptable level of safety, suggesting that a number of potential problems were identified and cured through the use of these risk analysis methods.

So, before thinking about developing alternative risk analysis

* Corresponding author. INERIS, Parc Technologique ALATA, BP2, 60550 Verneuil-en-Halatte, France.
E-mail address: christophe.proust@ineris.fr (C. Proust).

http://dx.doi.org/10.1016/j.jlp.2016.06.008
0950-4230/

methods, it is necessary to look how the "traditional methods" were initially developed and how they are currently being used. The idea is to better understand what works in order to understand why might not especially when facing new contexts.

2. The current practice of traditional risk analysis methods

The "traditional methods" like FMEA, HAZOP, Bow Tie diagrams have been abundantly documented in the scientific and technical literature (Mannan, 2012). In some cases the historical context of the development of the method is invoked, but they mainly describe the procedural aspects. In the examples given, idealized situations are used smearing out many practical difficulties as illustrated hereafter. The bias of this "pedagogical" (communication ?) method is that a superficial know-how is transmitted together with a preformatted method. Following, resulting safety studies might be highly standardized containing only little new information.

Nevertheless, many long experienced experts know that important and fully relevant scenarios may emerge first from a deep analysis of data (including simulating work situations in order to approach closer to the real operating conditions), second from a detailed investigation of the physical phenomena associated to the process and third from keeping the eyes opened on the general context. Illustrations of some of these issues are given in the follow up, partly coming from the experience of the authors.

2.1. Gathering data: the importance of real life situations

This example is about the safe manipulation of a missile to be attached below the wing of a jet (Fig. 1). In this particular context, the kind of risk is known (unwanted ignition due to a shock for instance), the relevant information was available, at least on the paper. And all looked fine: for instance the missile had to be approached on a trailer and the wheels of the latter were mechanically blocked as soon as the operator removed his hands from the trailer (when for instance manipulating other parts of the missile). During a demonstration, because of the limited space below the wing, the operator had, without any other option, to bypass the mechanical safety brake so as to be able to position correctly the trailer. The conditions for an unwanted hazardous situation were met.

This is not due to insufficient knowledge but to incomplete information of real life working constraints. The description of the technical lock was given on paper but another piece of information, without words or figures, but accessible only through the observation of the real task performed by the operator, was given out only by the real life simulation.

Fig. 1. Plane and missile example.

2.2. Expertise of physical (or chemical) phenomena

This aspect pertains to the interpretation of the information and is linked to the level-breath of expertise the risk analysis team incorporates.

To illustrate that point, the example of BP Texas City refinery big explosion is first given. In this accident, the overflooding of a distillation column was not detected and resulted in a massive flammable mixture leading to a large scale explosion. One of the key reasons why the team did not succeed in preventing the overfilling of the distillation column was that they did not know that the level indicator would tell that all is OK when the highest measurable level would be significantly surpassed. Note that many maintenance, integrity, management issues were associated with this disaster as root causes (Hopkins, 2012), but this example is given to show that a risk analysis team working on the distillation column would have failed in identifying this accident scenario if not aware of the functional details of the level detectors.

This is certainly not an isolated example. The following tells more about the kind of spectrum of physical knowledge which should sometimes be engaged. In this LNG harbor (Fig. 2), the LNG filling line is provide with several automatic isolation valves placed in series in particular to prevent a massive leakage. To investigate further the reliability of the device, an FMEA was performed. Immediately it came out that if the energy supply went down, all valves closed jointly because they were chosen « failed closed ». A priori, no more massive leakage: safe! would claim the process control engineer, but … the physicist would comment further that because the lines are never perfectly insulated, the LNG contained between the valves will vaporize and the internal pressure would theoretically rise by tens of atmosphere, breaking the equipments potentially leading to the undesired event, which might, in the present case, even be the worst with the largest consequences.

In those examples, the expertise does exist somewhere but may easily not be implemented if not made available. Turner (1978) commented that earlier, talking about disasters which he described as information problems.

2.3. General context: humans, organizations & societies

A striking example of ignoring part of the general context in which humans and societies evolve is now given.

Planes are equipped with safety doors separating the pilot cockpit from the passenger cabin. The motivation is to avoid

Fig. 2. LNG lines in a harbor.