Is it time, in the process industry, to question the limits of safety audits ?

Jean-Christophe Le Coze, Michèle Dupre

Is it time, in the process industry, to question the limits of audits?

Jean-christophe Le Coze (INERIS)
Michèle Dupré (CNRS)

Abstract
This paper argues that current safety assessment methodologies and models must be revised in order to reflect what is now known about the complexity of technological disasters. It first introduces the normal accident debate and indicates three types of issues that maintain the quarrel unsettled: the retrospective fallacy, the unanticipated consequences of technological and social actions and the difficulty to establish normative frames. Second, it argues, despite the 'normal accident' background, that there is much room for improvement in the way safety is assessed, if one considers closely, for instance, the lessons from socio-technological disasters. The Macondo well case study in 2010 (Chief Counsel Report, 2011) illustrates the complexity of the problem and the multidimensional nature of disasters. As safety assessments rely for a good part on safety management system audits (although the situation differs according to the high risk industries concerned), it is found relevant to start questioning their limits. This is what is explored in a third section, based on literature, empirical studies, official documents from high-risk companies and theory. The conclusion is that the audit rationale is not adapted to address the complexity of high-risk socio technical system and what we know from major accidents investigations. Fourth, some authors addressing the limits of current safety assessment practices are discussed, and ideas to move forward are introduced.

1. The 'normal accident' debate

Many major accidents in the past ten years in the process industry have been slowly challenging industry, regulators but also public's confidence about our ability to prevent them (e.g. Toulouse, 2001, Billy Berclau, 2003, Ghislenghien, 2004, Texas City, 2005, Buncefield, 2005, Macondo, 2010, Pembroke, 2011). This paper intends therefore first to provide a critical perspective to the question addressed in the conference call '*How do I know that I am not going to have a major accident tomorrow*?' This question has, in the literature, almost a thirty years old history (and probably a much older one, although historical views on technological disasters are scarce, see however, Fressoz, 2012). It was indeed Perrow's contention that 'normal accidents' could occur from time to time, despite all preventive measures, due the levels of complexity and coupling of certain kind of high risk systems (Perrow, 1984).

His approach was very much technological, or structural, leaving not much space in his interpretation to understand the part played by actors, organisations and institutions in the genesis of technological disasters. Thus, a sociologist like Vaughan (1996) has been able to extend Perrow's argument, using Turner's incubation framework (Turner, 1978) in order to show that complex socio technical systems could fruitfully be analysed from a historical, dynamic and systemic point of view. Her study of NASA Challenger's accident has become a landmark in the fields of both social and safety sciences.

For Vaughan, individuals, organisations and their environment have to be analytically linked together in systemic manner to understand better how socio technical systems are, not only technologically, but also socially, complex (Vaughan, 1999, 2005). Complexity is of course not only a technological or structural attribute as asserted by Perrow, it is also very much a social one (Le Coze, 2005). Other authors have then also clearly stressed the limitations of Perrow's early perspective, either for questioning (Bourrier, 1999), rejecting (Hopkins, 2001)

or expending it (Evan and Manion, 2002). For these different authors, Perrow's framework offers indeed a much too restricted analytical tool, although it has contributed to undermine the technological faith of a certain engineering community.

Despite these critics and new approaches to technological disasters, the argument whether accidents can be, or not, predicted in complex socio technical systems has remained unsolved. For example, the 'debate' of the 90's that Sagan (1993) contributed in shaping, between normal accidents and high reliability organisations, has never really settled, as Boin and Schulman (2010) recall in a critical review of the Columbia Accident Investigation Board (CAIB, 2003). It will probably never do. The diversity of high risk systems, the variety of situations and contexts but also the very often unspoken different philosophical assumptions on society, human nature and technology will keep the debate opened for ever between the pros and cons (Le Coze, 2008a). Even for the pros, some accidents seemed, after investigation, reasonably preventable (see Perrow's comments after the financial crisis, Perrow, 2010, or Fukushima, Perrow, 2011). Without pretending to be exhaustive, here are, at least, three corner stone and intertwined issues of this debate.

First, there is the problem of the retrospective fallacy (or hindsight bias). This is the problem of the observer (e.g. investigator) when he/she look back with full a view and understanding of the end of the story whereas actors located at different positions in socio technical systems involved don't. This issue has been well identified and commented for a long time now from many disciplinary angles including cognitive scientists dealing with 'human error' at sharp end (Rasmussen, 1981), to sociologists (Turner, 1978, Wynne, 1988) and management scientists (Starbuck, Milliken, 1988) dealing with failure of foresight at the 'blunt' end, including engineers and executives. To understand accidents, one needs to investigate to a certain level of qualitative depth in order to be sensitised better about what was then the contexts in which actors were immersed. *'This warning is the warning of the retrospective fallacy understanding organisational failure depends on systematic research that avoids the retrospective fallacy by going beyond secondary sources and summaries, relying instead on personal expertise based on original sources that reveal all the complexity, the culture, the culture of the task environment, and the meaning of actions to insiders at the time'.* (Vaughan, 1996).

Second, there is the question of the unanticipated consequences of technological and social actions, when the sheer number, nature and intensity of interactions between human and non human parts of socio technical systems lead to unexpected behaviours. As one is always located somewhere in a vast network of interacting parts, one can't pretend to have a full grasp of the entire system. This distributed nature of knowledge (and bounded rationality) makes it impossible for anyone to foresee every possible situation of interactions, moreover in a highly dynamic system where change is the norm rather than the exception. This distributed situation has been perfectly well captured by Weick regarding its implications for organisation theory '*We know most organizations function quite well even though no one knows quite what's going on*' (Weick, 1979, 109). The downside of this is however, from time to time, an accident.

Third, there is the difficulty of establishing and stabilising normative frames of conduct for every situations and every actors of an entire socio technical system. Innovation, both at managerial, engineering and operational levels consists in breaking rules or established standards, consists in exploring new ways of doing when coping with complexity. It implies flexibility and creativity to adapt organisations to their environments (e.g. markets) for managers but also to produce knowledge and understanding about unruly technologies for engineers and to cope with work situations for operators. This line of thinking is both relevant for operators, engineers and managers as Rasmussen wrote few years back now '*Analogy can*

be drawn between the adaptive mechanisms involved in the skill attainment of individual (...) and the role of management decisions – which may be errors in a safety point of view – in the adaptation to efficiency measures of an organisation. Errors in management and planning are intimately related to organisational attempts to adapt to the requirement of a competitive environment' (Rasmussen, 1987).

As a result of these three issues, one central problem met by anyone involved in a direct or indirect manner in safety management of high risk systems is fairly well coined by Pidgeon (1998) '*One puzzle for prediction, raised in several of the contributions, is that any of the background pre-conditions found in man-made disasters would apply to any modern organisation, successful or not. Barry Turner liked to quote the following observation from a close colleague, David Weir, who has suggested (personal communication) that 'most organisations operate in a degraded mode most of the time*'!'. One absolutely can't predict the future (1), one can't pretend to have the big picture (2) and one must always, in real life situations, innovate beyond the established normative frames of conduct to cope with an uncertain - ill structured - world (3). One understands, how, brought together, these three issues create the background for the sustained assumption that accidents will keep on happening from time to time.

Interpreting an accident for judging whether or not it was 'normal', i.e. inevitable, is as a consequence, always a matter of judgment, considering these three examples of issues. Such a judgement is based on a mix of professional and more theoretical backgrounds, including a lot of hidden philosophical preconceptions and understanding of socio technical systems (see for example the work of Reiman, Rollenhagen, 2011 on they chose to call 'biases'). This can be a disturbing and confusing experience for an investigator when he/she oscillates between managerial, neutral or more critical viewpoints (e.g. Habermas, 1973). In any case, it seems extremely difficult to ensure that a high risk socio technical system will never suffer a major accident. So, to the question '*How do I know that I am not going to have a major accident tomorrow*?' in the light of the 'normal accident' debate, one is very challenged to come up with an affirmative answer. However, this certainly does not mean that there is no room for improvement in the way safety is managed. Knowing about these features of any socio technical situation implies thinking and acting accordingly. Are current methods, tools and approaches up to the challenge of these three issues? This is an interesting part of current safety developments. In particular, one would like to see how much of what we know now about accidents is really translated into safety management practices. This brings us to the second section of the paper.

2. Findings of modern accident investigations

In the past twenty years, a wealth of well documented reports on major accidents has been produced in different industrial domains. What do they teach us? Let's illustrate this with the recently investigated Macondo well disaster (Chief Counsel Report, 2010). If one wants to approach this accident in a systemic manner, it is possible to distinguish five areas which will be briefly introduced here with the help of several illustrations extracted from the report (figure 1):

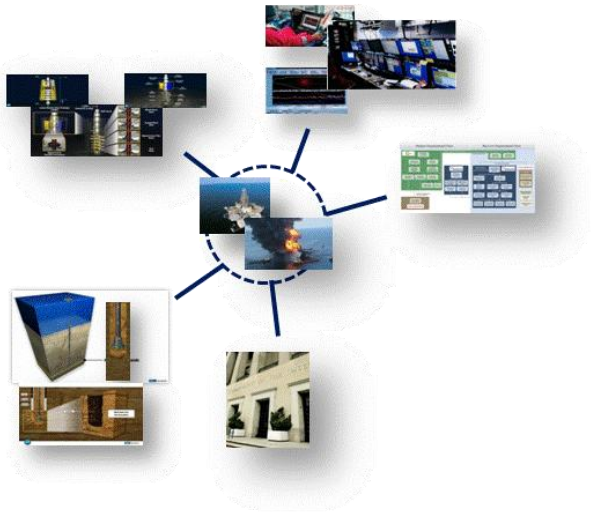
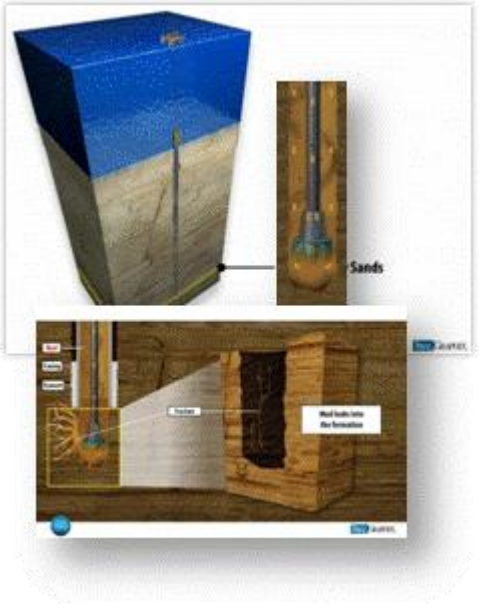


Figure 1. Macondo well disaster, five areas to consider, for simplification

- first, the technological hazardous situation (figure 2),
- second the technologically based defence in depth principles (figure 3),
- third, the work situations of operators (including very often human machine interfaces) (figure 4),
- fourth, the organisational dimensions including also very often several organisations interacting, and (figure 5),
- fifth the regulatory aspect of high risk industries (figure 6).

These five items are now briefly commented each in turn.



Deep water exploration entails drilling operations with safety issues including (among others) loss of containment of gas from the well. One scenario is a 'kick' followed by the release of gas on the platform, creating a flammable cloud at the surface. The uncertainties involved in drilling and the likelihood of a 'kick', are conditioned by interactions between the tools and the characteristics of geological formations (e.g. temperatures, pressures, nature of sediments).

The Macondo well accident is due to a loss of containment of gas.

Figure 2. Technology and hazardous situation

For preventing identified scenarios, barriers or defence in depth are designed. A BOP (blow out preventer) is one of the key elements of this defence in depth strategy, along with the casing, shoe track cement, cement plugs.

The accident is due to the failure of the defences in depth, including the BOP (its functioning, maintenance and design).

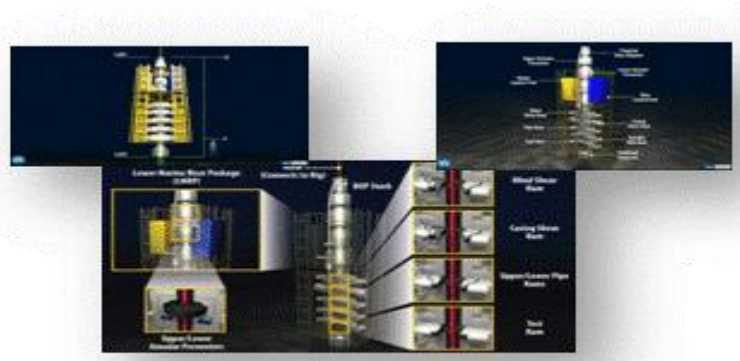


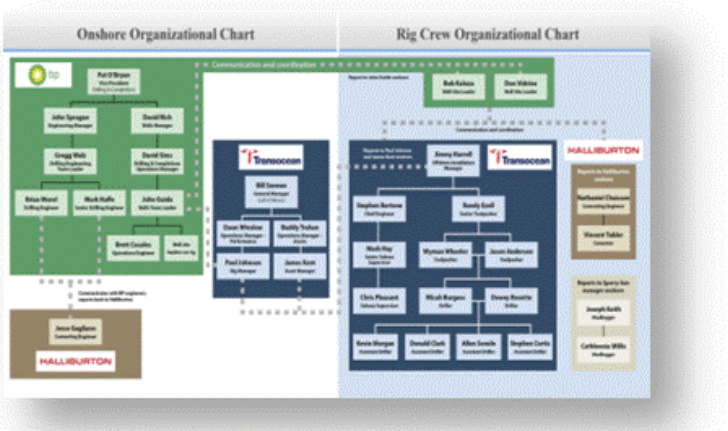
Figure 3. Barriers or defence in depth.

For conducting drilling, an important task consists in supervising operations from a distance, with the support of computerised technology. Along with this, more visual manual tasks are also involved on the deck of the platform (e.g. mudlogging). **Retrospectively, in the light of the events, it appears that the design of human machine interfaces included issues regarding the handling of displayed information and the management of alarms.**

Figure 4. Work situations and human-machine interfaces

Drilling activities involve the interaction of many expertises belonging to different organisations, including BP, Transocean, Halliburton, etc. They require design choices before as well engineering adaptations in the course of operations. This requires a tight coordination between various scientific, engineering and operating backgrounds.

This accident involves many issues including communication,



hierarchy, expertise, time and cost pressure, power and organisation structure.

Figure 5. Intra or/and inter organisational interactions

Deepwater explorations are under the supervision of control authorities who requires from operators that they demonstrate their ability to operate safely.

In retrospect, issues of regulatory oversight have been indicated such as conflict of interest between safety and industry development but also technical engineering competences in face of evolving technologies.

Figure 6. Regulatory issues

An accident is always to be explained as the result of an interaction of different types of dimensions including the ones presented above (on different investigation rationales, see Le Coze, 2008b). It requires several disciplinary backgrounds to be brought together, including engineering, ergonomics, social sciences, management and political sciences. This requirement for safety modelling was translated in Rasmussen's influential research program throughout the 90's (e.g. Rasmussen, 1997). His socio technical model is a very well known representation of this program. While other authors have also provided similar frameworks to illustrate this systemic view (Moray, 1994, Evan, Manion, 2002), it is Rasmussen's model which associates very explicitly each level with several scientific disciplines (for a more detailed review of Rasmussen's legacy, see Le Coze, 2012a).

Applied to the Macondo well case study, one sees very well the relevance of Rasmussen's conceptual formulation. To investigate and understand technical issues related to the gas 'kick' scenario or to the BOP failure, one needs an engineering background relevant in this domain. Without it, one would be faced with the difficulty of generating hypothesis about what happened. However, once everything is clarified, a fairly clear story can be written for anyone without any engineering background. Understanding that gases sprung at the surface because of the pressure from the geological formation and that the BOP failed to prevent it is quite straightforward. This retrospective understanding of technology in interaction with its environment made available to anyone also contributes to the 'hindsight bias' effect.

Once hypotheses have been generated and that a specific accidental scenario is selected from a technological point of view, a second layer of investigations including decisions and actions of humans can start, including other disciplinary backgrounds. In reality, actions and decisions of humans close to the events have already been included in order to produce hypotheses for the technical side of the accident. What people heard, saw or did before,

during and after main events leading to the accident are always information needed to formulate most likely hypotheses.

Exploiting human contribution from different point of views, using for example ergonomics, management and sociology comes in a second step, and with different models than engineering ones. To describe the coupling between computers, machines and humans, but also to better grasp the phenomena of interacting humans within teams and (inter/intra)organisations, one needs complementary observations and interviews than the one applied at the engineering phase of the investigation. The same applies when one wants to include aspects related to regulatory oversight. When this is performed, a very rich perspective is available, combing issues related to power plays, cultural and cognitive dimensions. One can see decision making processes where conflicts, uncertainties, hierarchy and communications aspects interact all together within time, but also budget and expertise constrains. It is only when these different dimensions are brought together that a systemic interpretation of the accident is produced (Le Coze, 2010). Another 'hindsight bias' is then possible, this time for those without cognitive, psychological and social sciences backgrounds.

3. What do we find in audits?

Now, one question that comes to mind immediately after this example of investigation (among others) is how much of what we know in retrospect can be found in organisations beforehand? In other words, do organisations produce a level of information for their own decision making processes that matches the quality of data that one finds afterwards in reports? Such a question was expressed, few years back, in 2004, by French control authorities after an investigation commissioned by the ministry to INERIS (this investigation and its results have been described, later on, in Le Coze, 2010). This question was expressed as follows '*Why don't we perform this kind of investigation before, rather than after?*'. This was an interesting question indeed.

A first answer had been framed at the time with the help of the field of complexity but also in relation to the limits of audits (Le Coze, 2005). The argument was that organisations were complex systems that couldn't be thought through a deterministic and reductionist view; a certain level of methodological and theoretical plurality was advocated. It was also argued that safety management system (sms) audits[1] relied on structural views of organisations and as a result were clearly unable to sensitise the complexity of socio-technico-organisational life. This is a problem because audits are one of the main safety tools for companies (of course, there exist differences between industrial sectors and from on company to another in the same sector). This statement was based on theoretical and professional experience. Let's carry on in this paper with the limits of audits and extend this line of argument. There are many ways to approach this issue.

A first one is through the literature. What is available in the literature regarding audits, and more importantly for the topic of this paper, about their limits? Has a lot been written about it? A second is the interviews and observations from empirical fieldworks. For the past few years, we have been investigating, in normal operations or in the context of incidents or accidents, many different work situations and high risk organisations, including observations and interviews with several types of actors (e.g. operator, engineers and managers). What do people from the industry say during our interviews about the limits of audits? What do we see through our observations about the way audits guide collection and interpretation of data?A third one is the data that company produce publicly about themselves, either during

[1] In the rest of the paper, 'audits' means 'safety management system audits'.

conferences or by other means (i.e. journals, internet). What can we infer from publicly available companies discourses regarding the exercise of auditing? A last one is theory. From a theoretical point of view, is it possible to pinpoint limits of audits that would be intrinsic to their underlying rationale? These four threads are now in turn developed.

3.1. Literature.

It is difficult to find either empirical or theoretical works dedicated to auditing, but two interesting ones are worth introducing here. In a study raising the question of the impact of audits, Chaplin and Hale (1997) analysed the implementation of ISRS (International Safety Rating System) in a company of the petrochemical industry. Although the paper had a rather positive tone about the value of audits, the conclusion was tempered with the following issues. T*he ISRS system is quite clearly designed for organisations which are used to working with the paperwork systems typical of bureaucracies.(...) it would be less likely to work in organisations where there needs to be constant improvisation, or where the organisation is small enough not to need to commit everything to paper'* (Chaplin, Hale, 1998, 183). Thus, for these organisations in high risk contexts which need to rely on improvisation and adaptation to unforeseen events, these conclusions undermined somehow the value of the auditing approach.

But, around the same time, outside the field of industrial safety, a much more critical orientation was found in Power's book (1997), a theme that he further explored 10 years later (Power, 2007). For this author, '*standardized elements, such as the auditable management system (…) represent the rationalizing tendencies of audit to reproduce ever more formal auditable structure, regardless of demonstrable effectiveness*' or '*Images of control over pollution and derivatives (…) get manufactured by an audit process which necessarily insulates itself from organizational complexity in order to make things auditable and to produce certificate of comfort'*. (Power, 1997, 123, 140). Applied to financial, medical and environmental activities, the picture depicted by Power is then much darker and radical than the one suggested by Chaplin and Hale.

While they identify the problem of improvisation but also of bureaucracy, Power does not hesitate to criticize further the result of framing everything under auditing principles, among which the drawback of 'paperwork'. '*What audits really procure, other than working papers, is more opaque than is commonly admitted*' (Power, 1997, 39). Although not grounded in the traditional high risk industries, many of Power's insights do echo with, for instance, what major accident investigations have revealed since many times. In these investigations, many organisational problems were without any doubt in the background of the disaster but never described in a systematic and systemic manner beforehand, whether publicly or within the corporation itself where actions could have been taken.

These accidents do reveal again and again that '*individuals are infinitely more complex and adaptable than normalizing attempts to measure and control them; a substantive, messy rationality always reasserts itself over formal, technical rationality*' (Power, 1997, 120). Although, without any doubt, major contributors of improvement in safety over the years, as asserted by Chaplin and Hale, auditing practices can also then be criticised, as Power does, for clearly oversimplifying organisational complexities and misleading organisations in the appreciation of their own limits (Starbuck and al, 2005). Although one can see the added value of auditing as asserted by Hale and Chaplin (apart from the issue of improvisation), Power's interpretation also echoes fairly well with our own fieldwork experience.

3.2. Elements from empirical fieldworks

In our empirical studies, mainly in the chemical industry, one question that we always ask to safety technicians, engineers or managers is what they think about audits. Everyone is not necessarily critical in the same ways. Nevertheless, what comes out first is that auditing has become a formal exercise, a routine. Everybody seems to know what auditors are after. After some years of experience, people know what to answer to satisfy auditors. The rationale of auditing is indeed very often based on paperwork. According to auditing principles, paperwork can demonstrate in a tangible manner that systems are in place. Auditors look for documents showing that the system is implemented. These documents are recordings of different types of activities, like the results of an inspection of a vessel in a chemical plant, or a signature on a document proving that someone with a specific expertise has been consulted. They can also be procedures describing specific steps of a task, transformed in checklists to fill.

Second aspect that comes out is, from a process safety point of view, that auditing is not directed to the right kind of problems. In many cases, auditors seem to be more interested in secondary issues rather than primary ones. Secondary issues for individuals with process safety functions are for example checking if people use pedestrians crossing in the factory or if the pedestrian crossings are visible. Although they do recognise the importance of these types of concerns for occupational safety, they regret that they come first at the expense of more technically oriented relevant enquiries (e.g. checking a barrier, e.g. a sensor, on the process), which matter directly for process safety. As one engineer put it, auditing is as good as the auditor (and this auditor can be, in consulting companies, a young and inexperienced one, which helps bringing down the costs).

If an auditor is knowledgeable in the area he/she is auditing, then the audit can have a positive outcome. If not, the audit can become a waste of time. For this reason, many prefer, when possible, cross auditing. Cross auditing consists in being audited by someone with a similar position and experience in the company. Such a person goes straight to the key issues, and can prioritise much better in the discussion between primary and secondary areas. It becomes an exchange between two experts, or professionals, rather than a formal exercise guided by procedures that are not understood with a background about real life, concrete, work contexts. They can discuss on the basis of a shared understanding of real life situations (and engineering expertise) rather than on a basis of an abstract management system view of safety.

During a research in an international group where we interviewed individuals both from sites and corporate levels, audits were found to be the principal source of data for decision making regarding safety matters (along with incident investigations and technical risk analysis). Relying on these audits was a very strong input to the group safety strategy at a corporate level, on the basis of which they elaborated indicators and tables ‘ranking’ sites. The difference of views between people on site and corporate individuals about the relevance of audits was therefore striking. While corporate safety managers saw audits as an effective tool for monitoring sites, safety engineers or managers on sites were challenging, along the line explained above, the quality of the approach. Thinking that corporate levels rely on these audits without considering their limits described by site people was, as a consequence, an important theme for our feedback session to the company. It triggers concern regarding the ability of audits to inform top managers and executives about real work conditions and as a consequence the ability to trigger appropriate responses by companies.

After spending several days applying an ethno-sociological type of investigation on a site of this group, our own point of view regarding these auditing practices by corporate levels was

on the side of sites safety engineers and managers. Although audits were performed by a team of two to three trained people over two or three days (sometimes more), their way of questioning the organisation made them unaware of issues involving real life working conditions including organisational changes concretely affecting safety practices. The presence of a new director with a different experience and decision making practices that the previous one, the replacement of the experimented safety manager by a younger one with expertise in process engineering, the change of policy for sub contracting, training and recruiting, the problem of having to adapt procedures in some production pressures circumstances, were key issues over the past months and years transforming the profile of the site. However, none of these aspects were included in the audits. Audits expressed instead their own rationales, based on checking completion of paperwork, and approaching organisations through safety management system items, disconnected from each other (that we called the 'drawer effect'). More about the audit rationale is explored next.

3.3. Publicly made available data on high-risk organisations

In 2009, the petro-chemical group Total suffered a series of four deadly accidents in different sites, including:

1. two explosions in two different sites (3 deaths and 11 employees injured),
2. one exposition to dangerous substances (1 death) and,
3. one accident involving a truck (1 death) [2].

The company decided as a consequence to assess widely the situation. Rather than considering this as bad luck, the corporation considered that a deeper problem might be found in the background of this dark series ('*série noire*' in French). The company commissioned internally what they described as a 'general safety inspection'[3]. This inspection covered 13 sites of the company in France. After five months of inspection (from September 2009 to January 2010), a document was then made available in February 2010, summarising the findings of this inspection[4]. This report is very interesting as it shows in a rather direct way how the company conceptualises the problems related to these accidents. We will argue that it reveals quite clearly some aspects of the rationale of audits.

One can imagine that the document does not provide all the findings, and the most critical aspects might not be revealed in this public version, but it is not so much what interests us here. Instead, it is the implicit models that the document contains about the interaction between technology, humans, systems and organisations in relation to safety that is relevant. It helps to surface some of the assumptions one finds in probably many high risk companies when it comes to interpreting socio technical issues with regard to safety. It is therefore important here to recall that this section of the paper is not critical of Total for its initiative but, on the contrary, stresses positively this strategy of transparency. This section however takes the chance to analyse the content of the report to explore some of what seems to be underlying assumptions about safety, or at least, the ones the company is openly communicating about.

In the inspection reports, many safety management system areas are addressed. These are areas where improvements are expected in the future. These are organised in 7 sections including 1. Risk analysis methods, 2. Operations, 3. Maintenance and inspection, 4. Sub contractors, 5. Management of competence, 6.Monitoring efficiency, 7. Organisation. For each section, a summary is written, followed by recommendations. The essence of the audit

[2] http://www.usinenouvelle.com/article/total-l-inspection-generale-de-securite-est-bouclee.N128067
[3] http://www.total.com/fr/groupe/actualites/actualites-820005.html&idActu=2312
[4] http://www.total.com/MEDIAS/MEDIAS_INFOS/3186/FR/IGS_synthese.pdf

rationale is perfectly contained in the following quote from the introductory section of the 16 pages report '*The general safety inspection was able to observe that the operations of inspected sites rely on a robust basis, , and particularly on teams professionalism, it is however crucial to always ensure the solidity of this basis. This basis, ensuring operational mastery, is a referential comprising technical standards, organisational procedures and operating procedures that one must not depart from for fear of opening a path to failure*'

In this quote, there is the very idea that standards or procedures, once written down, define a global framework to comply with for ensuring safety. Moving away from this framework creates opportunity for accidents. What is interesting here is the absence of any indication about the part played by humans, apart from the mention of 'professionalism'. The picture, or metaphor, conveyed is a mechanistic one, a rigid one: there is a structure based on thorough risk analysis that once designed and if implemented, is in a position to contain the risks. In many places in the report, one can see the influence of this view. For instance '*These rules and procedures are constraining, they result from operating experience and risk analysis, complying with them is a discipline of every moment*'.

One wonders why so little space is dedicated to introducing other fundamental dimensions of safety such as the ability of individuals, at many different positions within companies (e.g. operators and line managers, production and safety engineers, managers, etc), to adapt when facing novelty or unruly technology, when working conditions expected to be found to implement rules are not met or when decisions must be taken under uncertainties. One could expect to see the three types of issues described in the 'normal accident' section of this paper to be acknowledged as challenges for high risk industries. With this report, we are very far from the kind of description one finds in accident investigation reports such as the one chosen for the argument of this paper (section 2).

Of course, this is not an accident investigation report, but there are no indications about the complex interactions between humans, technology, organisations including issues of power, hierarchies, cultures but also conflicts or decision making processes over technology or strategy orientations. Companies deal with them everyday, find solutions to cope with them in order to be successful, so why not mentioning them? These phenomena are the daily life encountered by anyone in these organisations. Where are they in the report? Nowhere. Instead, it is argued that the image promoted by the report relies on a safety management system audit rationale. It is almost as if humans were excluded of the picture. Human are expected to comply with a normative framework. This reflects quite well our own empirical data (section 3.2) but also echoes Power critics ''*individuals are infinitely more complex and adaptable than normalizing attempts to measure and control them; a substantive, messy rationality always reasserts itself over formal, technical rationality*' (Power, 1997, 120). This can also be illustrated quite clearly from a theoretical point of view.

3.4. **Theory**

If one wants indeed to look into the audit rationale from a theoretical angle, another strategy consists in differentiating it from other kinds of approaches. This is what the following figure does (figure 7). It contains similar dimensions than other figures mentioned in section 2 (i.e. Ramussen, 1997, Moray, 2000, Evan, Manion, 2002) but with slightly different graphic principles e.g. all domains are interacting, not separated from each other by socio-technical 'levels' or 'layers'.

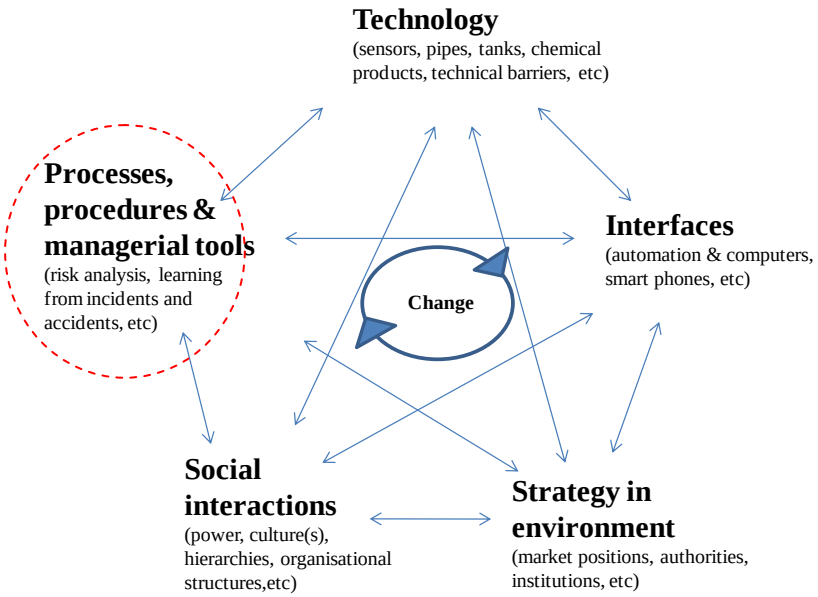


Figure 7. Several approaches to safety.

The red circle indicates what audits target. Audits focus on processes, procedures and recordings. When doing so, they leave aside technology, interfaces, social interactions and company's relation to its environment. From a theoretical point of view, it is therefore not a surprise if audits only catch a limited aspect of socio technical complexity. Let's comment each of these points in a clockwise direction. Audits often don't establish a link with technology (1). As described in 3.2, fieldwork observations and interviews indicate that audits are somehow disconnected from technology, especially when it comes to process safety. This idea is now well established with accident investigations showing that occupational safety indicators are not reliable indicators of process safety (Baker Panel, 2007). If auditors focus on occupational safety for major hazard prevention, they miss the point. A relevant audit from a process point of view can only be performed if the technological dimension of the problem is included in the picture (e.g. a description of defence in depth principles) based on sound engineering knowledge of installations and risks.

Audits are not designed to consider human machine interfaces, and more generally work situations (2). Although human computers interactions are now a central issue in any high risk industry, audits don't investigate them. This would require observations, interviews of a different kind that audits. It is the field of cognitive engineering or cognitive ergonomics, which emerged in the eighties with the increase of automation and was developed to introduce an array of complex issues related to display of information. The need for a mix of engineering and psychological/cognitive background is necessary for assessing human machine interfaces situations. It is doubtful that audits are in a position to provide this kind of expertise when solely relying on processes, procedures and recordings.

Audits do not consider explicitly the environment of a company (or a site within a group) to understand its resources and constraints (3). One dimension of the environment is company's (or site's) top management strategy regarding interactions with regulators, adaptation to market (or group) opportunities or subcontracting options. This view of the organisation is to be balanced with the institutional (or societal) forces shaping company's opportunities, such as professions or demography, social changes or professional associations. Last, audits are not designed to include sociological understanding of organisations (4). This would rely on understanding of combined effects of organisational structure, conflicts, power plays and cultural dimensions. The kind of investigation and knowledge needed to include (3) and (4)

depart from audit methodology consisting in following processes, procedures and recordings. Instead of relying on closed questions, an analysis of social interactions and organisation's environment necessitates opened questions and long period of time for obtaining a minimum of 'intimacy' with real life situations. Instead of considering organisations through processes and procedures, one considers organisations as a result social interactions between actors.

3.5. Summary section 3

This section started with some critical views from the literature. Power provided interesting, although certainly radical, comments about audits (Power, 1997). In his view, management system audits frame reality in a simplistic manner, relying on an excess of paperwork to demonstrate compliance with standards. While doing so, '*the abstract system tends to become the primary external auditable object, rather than the output of the organisation itself, and this adds to the obscurity of the audit as a process which provides assurance about systems element and little else* (Power, 1997, 85). Although radical, this statement can be observed in reality as we have commented with our own observations.

First audits can miss the point when not designed to establish links with certain specific problems (e.g. occupational versus process safety). Second, standards are inadequate to support auditors judgment of real work situations if they are not supported by relevant expertise in the area audited (hence the appeal by operational people for cross auditing). Third, safety management systems audits can miss, as we observed, key dimensions related to everyday life of companies, such as (organisational) changes ('drawer effect', i.e. studying safety management system items separately).

A similar analysis could be made of the general inspection report produced by Total in 2009. This report contains many expressions that reveal quite clearly a mechanistic or structural image or metaphor of safety management. Finally, these comments based on empirical investigations or available documents could be supported by a theoretical approach. Safety management system rationale is shaped by a process and procedural view of companies that tends to produce structural, mechanistic or rigid expectations. This frame, like any frame, influences what is selected, filtered, collected and interpreted. As such, it can be compared with other safety approaches including engineering, sociology and ergonomics. When doing so, it is clear that audits only look into organisation from one specific angle, a kind of 'tayloristic' one, denying the innovative and most needed manual, cognitive and relational adaptations of different categories of employees, from operators to line managers including process and production engineers.

4. How to move forward? Some existing guidance

If one accepts the idea that audits are limited, a next step is what could extend, complement or replace them? In fact, this paper is not the first one to challenge the limits of current safety approaches and to express the need to move beyond them (e.g. Dalzell, Hopkins, 2006, Berman, Ackroyd, 2006, Reiman, Oedewald, 2009). Although these authors do not always explicitly criticise audits as a starting point, they do stress the need for new perspectives or models for assessing safety, and offer some guidance. Dalzell and Hopkins (2006) want thus to connect much more explicitly technological risk assessments with the operational and managerial activities of different actors of high risk systems. For this purpose, they combine Rasmussen's socio technical levels (individual, facility, managerial and corporate) with what they define as nine attributes of hazards and risk management (e.g. line responsibility, risk hazard and understanding, corporate unease, identification of critical elements and the existence of minimum standards, the definition and application of clear operating limits, etc).

Their purpose is '*moving to the next level, distilling the knowledge from the safety cases and risk assessments to optimise what we do (...) it is moving from managing the basics into these areas which are less quantifiable but can deliver significant risk reductions*' (Dalzell and Hopkins, 2006, 896). After describing for different actors what would be expected from them with regards to the nine attributes, they then question one by one the current practices of the industry (more specifically, it seems, the chemical and petro-chemical industry), based on their experience. The strategy is thus first to define a normative framework, second, to compare this one with reality. Here is an illustration. The authors provide a normative statement coupling a chosen level and an attribute, e.g. the definition and application of clear operating limits at facility level. '*Boundaries should be defined within the performance standards discussed above.* (...) *At the facility level, the performance limits of the plant are easy to define in terms of throughput but less precise when considering the minimum manning, the maximum level of activity or occupancy and the point at which the combined deficiency of apparently unrelated critical systems, including people, becomes intolerable*.' (Dalzell and Hopkins, 2006, 889) They then turn into an evaluative mode corresponding to the items normatively described earlier and come with a statement.

For our example, their view is the following one '*At the middle levels, there appears to be a much more general tendency to ask – 'what do we need to do to keep going...or can we get by without ...?' At the managerial levels there seems to be a reluctance or inability to set precise limits and to say no. Instead, the opposite is appearing – the setting of stretch targets for production and return, and the encouragement always to say 'yes*''(Dalzell and Hopkins, 2006, 893). They repeat the same process throughout their paper for each item. The conclusion contains then a critical tone '*the attributes for effective hazard and risk management listed above have not been widely observed*' (Dalzell and Hopkins, 2006, 896). They advise as a consequence to reduce the complexity of some of the developments in risk reduction of the past years (e.g. human factors, hazard analysis techniques, technology, hardware) and to '*hand risk management back to the line managers*' (Dalzell and Hopkins, 2006, 900).

For Berman and Ackroyd (2006), there is a need to devise new models and methods to be in a position to better capture 'organisational drift'. Looking back into several accidents from medical, nuclear power and space sectors (e.g. David Besse, Toïkamura, Columbia), they identify a common pattern of organisational drift across their case studies. They remark that for the David Besse case, where '*the nuclear power plant, near Toledo, Ohio, came within 3/8'' of a loss of coolant accident that would have earned it a place Chernobyl*', it '*had been rated 'INPO 1' which meant that an independent review process undertaken by industry peers had judged it to be a high-performing organisation*' (Berman, Ackroyd, 2006). This story has puzzled other authors involved in the nuclear industry (e.g. Perin, 2005, 15). Several assumptions could be made about this story. Some are briefly introduced here.

One is that external peers missed that particular scenario although they could have in principle. They didn't because of lack of time or 'lack' of identification of this area as safety critical at the time of the assessment[5]. Another one is that the individuals commissioned for the assessment were not qualified enough to perform it adequately. They didn't have the expertise to challenge practices of operators, engineers and managers regarding the specific issues revealed by the incident. A last mentioned here is that the background model to assess

[5] This is Perrow's view, with a strong critical, dark, flavor '*Objecting workers were disciplined and the reactor was allowed to continue functioning under very dangerous conditions. One objecting worker went directly to the Nuclear Regulatory Agency, forcing the embarrassed agency to act upon information they already had but chose to ignore. The worker was fired. When he sued the company for unlawful dismissal, the NRC sued him in turn'* (Perrow, 2010, 313).

safety was inadequate to identify flaws or problems that increased the likelihood of an accident.

This last hypothesis seems to be, implicitly, what Berman and Ackroyd have chosen. They have indeed classified several approaches met in the nuclear industry into 1. Peer review, 2. Safety culture assessments, 3. External audits, 4. Learning and feedback systems, 5. Performance indicators, 6. Internal oversight departments and 7. Formal reviews. Regarding audits, they assert that '*this is frequently to general in scope*'. They conclude that '*organisational drift*' is invisible to all of these approaches, hence the good external assessment of David Besse nuclear power plant, just before the very serious near-miss. In front of the limits of all these approaches, their answer consists in offering a model of organisational drift combining 'major or incremental changes' with 'degradation' combined with 'oversight failure'. Designing new models for capturing organisational drifts is advocated as a solution to overcome some of the limits of current approaches.

It is a similar line of argument, but more developed and elaborated, that can be found in Reiman and Oedewald (2009). They, also, establish a list of approaches that one can find in the nuclear industry; very close to Berman and Ackroy's list (e.g. safety management system audits, safety culture evaluation, peer review, etc). One difference is that Reiman and Oedewald separate several historical periods regarding the way safety has been theorised. They consider that this list corresponds to a third era of safety, to conclude that '*a challenging issue is the evaluation of the organisation as dynamic complexity and not merely an aggregate of the above mentioned factors*' (Reiman, Oedewald, 2009, 18). Their conclusion is also to move beyond current perspectives, to enter a fourth era through new models because '*in these evaluations, more emphasis is still placed on the assessment of technical systems, structures and documents*' (Reiman, Oedewald, 2009, 33). Their model suggests a combination of different insights on organisations, through psychological properties and conception of the personnel, organisational structure and processes, social processes and organisational core task and the basic technology.

All these authors share the same line of reasoning. First, they identify a problem, i.e. the way safety is assessed is not appropriate; second, new models are advocated to address this problem. Some of these models have a more normative orientation (Dalzell and Hopkins, 2006) and some other have a more descriptive one (Berman, Ackroyd, 2006, Reiman, Oedewald, 2007, 2009). Some target situated actors at several levels of socio technical systems in order to specify what is expected from them according to different attributes (Dalzell and Hopkins, 2006) while some target observers; whether external or internal, in a position to perform assessments of high risk organisations as a whole, by providing adequate models (Berman, Ackroyd, 2006, Reiman, Oedewald, 2009). More specifically, what the latter share is a sense of dynamic and systemic views to be applied to safety assessment of high risk organisations. Although, as indicated, these authors do not target audits directly, their ideas are relevant as an answer to the limits of audit.

This idea that new models should be applied to appreciate better safety from a more complex and multidimensional perspective, but still in a position to be practically implemented, is an important research theme that should bring together industry and safety scientists. The fact that many researchers have found important to develop new models is also a sign that the available ones are not satisfactory. One interpretation of the current situation is that the successful models of the past ten or twenty years in the field of safety might have started to become inadequate in relation to the findings of modern investigations and safety research. Thus, Reason (1990, 1997) or Rasmussen (1997) created their hugely influential models on case studies of accident of the eighties and the nineties (e.g. Chernobyl, Challenger, Piper Alpha). They also relied on their psychological and cognitive engineering backgrounds to

conceptualise these events and translate them into simple and useful models (Le Coze, 2012b). Social sciences should now also provide the inspiration for new models and approaches of industrial safety (for an extended discussion on this topic that can't be develop here, see Le Coze, 2012a, 2012c).

Conclusion

The aim of this paper was to demonstrate the relevance of questioning the limits of audits. There are several good reasons to do so, among which, recurrent technological disasters. It was argued that these practices rely on too simplistic method and models. Individuals (whether operators, engineers or managers) are not simply following procedures. Cognitive processes involved in their daily operations are highly complex and adaptive, and involves, for operators, interactions with technology, automation, computer displays and colleagues. Organisations are not mechanical machines behaving according to defined structures. They are socio-politico-cultural realities where power, conflicts, ideologies, change and hierarchies play a very important part in shaping their trajectories. Where are all these complexities in current auditing practices? Nowhere, in fact; or not explicitly. The literature, our empirical case studies, available documents and theory together reveal that these topics, although behind any accidents, are not acknowledged by companies. This might sound as a harsh judgment. But the normalisation of accidents in all industries over the past thirty years (Virilio, 2005, Fressoz, 2011), demonstrate that something is wrong. We believe, with other (e.g. Power, 1997, 2007), that the way audits are conducted (including methods and models) is a part of this problem. The paper introduced elements to support this claim and some ideas to move forward, based on recent developments in the field of safety science.

References

Berman, J., Ackroyd, P. 2006. Organisational drift – a challenge for enduring safety performance. IChemE Symposium series n°. 151.

Boin, R.A. and Paul Schulman (2010). "Assessing NASA's Safety Culture: The limits and possibilities of High Reliability Theory", *Public Administration Review*, Volume 68, Number 6, pp. 1050-1062.

Bourrier, M. 1999. Le nucléaire à l'épreuve de l'organisation. Presses Universitaires de France. [Nuclear industry from an organisational point of view]

Chief Counsel Report. 2011. Macondo. The gulf oil disaster. National commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling.

Dalzell, G., Hopkins, A. 2006. Is hazard management working? IChemE Symposium. Series n°. 151.

Evan, M, W., Manion, M. 2002. Minding the machines. Preventing techonological disasters. Prentice hall

Fressoz, JB. 2012. L'Apocalypse joyeuse. Une histoire du risque technologique. Seuil.
Fressoz, JB. 2011. The lessons of disasters. A historical critic of postmodern optimism. Available at http://www.booksandideas.net/The-Lessons-of-Disasters.html

Hopkins, A., 2001. Was Three Miles Island a normal accident? Journal of contingencies and crisis management. Volume 9. Number 2.Turner, B. 1978. Man-made disasters. The failure of foresight.

Le Coze, JC. 2012a. Reflecting on Jens Rasmussen legacy. Working On Safety. 6th International Conference. 11-14 September 2012. Sopot. Poland.

Le Coze, JC. 2012b. Quels nouveaux modèles FOH pour l'évaluation de la sécurité industrielle ? Conférence-débat. ICSI-ESCP Paris. [How could new human and organisational models for industrial safety assessment look like?] 28th of march 2012.

Le Coze, JC. 2012c. Outline of a sensitising model for industrial safety assessment. Safety Science. Forthcoming.

Le Coze, JC., 2010. Accident in a French dynamite factory: an example of organisational investigation. Safety Science 48 (2010) 80–90.

Le Coze, JC., 2008a. BP Texas city accident: weak signal or sheer power ? In Hollnagel, E., Rigaud, E. (ed.) Proceedings of the third symposium on resilience engineering. Juan les Pins.

Le Coze, JC., 2008b. Organisations and disasters: from lessons learnt to theorising. Safety science (46) 132-149.

Le Coze, JC., 2005. Are organisations too complex to be introduced in technical risk assessment and current safety auditing? Safety science (43) 613-638.

Moray N. 2000. Culture, politics and ergonomics. Ergonomics. vol.43. n°7. 858-868.

Perrow, C. 2011. Fukushima, risk, and probability: expect the unexpected. Bulletin of the atomic scientists.

Perrow, C. 2010. The Meltdown was not an accident. In Markets on trial: sociology of the US financial crisis: Part one. Research in the sociology of organizations, volume 30A, 309-330.

Perrow, C. 1984. Normal Accidents, first ed. Princeton University Press, Princeton.

Perin, C. 2005. Shouldering Risks*:* The Culture of Control in the Nuclear Power Industry. Princeton University Press.

Power, M. 1997. The audit society. Rituals of verification. Oxford University Press.

Power, M. 2007. Organized uncertainty. Designing a world of risk management. Oxford University Press.

Reimann, T., Pia, O. 2009. Evaluating safety-critical organizations – emphasis on the nuclear industry. Available at www.stralsakerhetsmyndigheten.se

Rasmussen, I. 1980. What can Be Learned from Human Error Reports. In Changes in Working Life, ed. K. Duncan, M. Gruneberg and D. Wallis. John Wiley and Sons. New York.

Rasmussen, J. 1997. Risk management in a dynamic society: a modelling problem. Safety Science 27 (2/3), 183–213.

Reason, J. 1997. Managing the risk of organisational accidents. Ashgate.

Starbuck, W,H., Milliken, F, J. 1988. Challenger: Changing the odds until something breaks ", Journal of Management Studies, 25: 319-340.

Turner, B, A. 1978. Man-made disasters. The failure of foresight. Butterworth Heinmann.

Vaughan, D. 1996. The Challenger launch decision: risky technology, culture and deviance at NASA, University of Chicago press, Chicago.

Virilio, P. 2005. L'accident original. Galilée.

Wynne, B. 1988. Unruly technology: Practical Rules, Impractical Discourses and Public Understanding. Social studies of science. vol. 18 no. 1 147-167.