How to prevent a normal accident in a high reliable organisation ? The art of resilience, a case study in the chemical industry

Jean-Christophe Le Coze, Michèle Dupre

How to prevent a Normal Accident in a High Reliable Organisation? The art of resilience, a case study in the chemical industry.

Jean christophe Le Coze[1] & Michèle Dupré[2]

[1] INERIS Institut National de l'environnement Industriel et des Risques
Parc Alata - F - 60550 Verneuil en Halatte
Jean-christophe.lecoze@ineris.fr

[1] GLYSI-SAFA – ISH – 14 avenue Berthelot- F - 69363 LYON cedex 07
michele.dupre@ish-lyon.cnrs.fr

Abstract: The trend in France in the chemical industry following the Toulouse accident in 2001 has created a situation where some of the installations have got closer to the definition of high reliable or resilient systems. This papers based on an empirical case study elaborates on the question: can we see better with the help of an articulation of safety engineering, safety management and social concepts (extracted from the safety and accident field) some dimensions, for example the level of resilience (or reliability), that are not captured today with traditional tools? Our approach articulates two investigative modes to capture an organisational safety dynamic: a normal study approach (what's happening when nothing is happening?) with an incidental-accidental one (looking at past incidents or accidents and their organisational genesis) in order to generate assumptions regarding the presence of organisational patterns influencing safety.

1. INTRODUCTION

The trend in France in the chemical industry following the Toulouse accident in 2001 has created a situation where some of the installations have got closer to the definition of high reliable or resilient organisations[1]. They are indeed under pressure from the society for being very safe while also being under pressure from the market for producing in the most efficient ways, for maximising profits. Economic pressure is one of the strong trait of our capitalistic societies and a resulting effect of a global world market. Companies must be managed under strong financial and competitive pressures. Constraints also come now from the expectations and sensitivity from society regarding safety. These expectations push companies to communicate more on safety. They for example as a result sometimes open their doors for the public in order for it to visit the plants, with a goal of transparency and societal trust. The societal needs following the Toulouse disaster also led authorities, as a political measure, to increase the number of inspections by recruiting more inspectors and the relevance of the inspections, by training inspectors specifically to major hazard prevention.

Some of these chemical plants have high safety performances, with only minor incidents over a 20-30 years period. Some could have therefore been considered

[1] By choosing "organisation", we target the actors employed by the company and working in the plant. The "socio-technical system" expression can be used to open the organisation to other actors such as the regulators, the sub-contractors, the corporate, the public. When we use "organisation" in this paper, we mean the organisation within its socio-technical system. In an approach acknowledging the complexity of safety and accidents dynamic, such a perspective is unavoidable.

as equivalent to high reliable organisations even before the Toulouse accident. As a result in terms of prevention, one of the difficulty becomes therefore in these type of systems to capture the potential drifts and deviancies, as shown by accidents investigations and works from scholars, in particular when they have implemented all safety management best practices existing in the industry.

The field of resilience addresses this issue, and a fruitful way of turning it is also to follow Snook (2000) with saying that the insidious accidents threatening these organisations are Normal Accident in High Reliable Organisations, so that one of the purpose of these organisations is to maintain a sense of vulnerability and an ability to be introspective enough to anticipate the "slippery slopes" (Vaughan, 2005), to be able to "dance" with the Brownian movement (Rasmussen, 1997) and to prevent a Resonance phenomena (Hollnagel, 2004) within their installations. This perspective implies therefore not to focus solely on the technological complexity but as Snook indicated in regards with his work on what we call the organisational safety and accident dynamic: *"While Perrow's emphasis was on complex technologies and demonstrating the inevitability of such accidents , mine is on uncovering their underlying behavioral and organisational dynamics (...)"*.

One of the question can thus be: how to provide useful auditing tools linking safety engineering, safety management practices and social concepts of organisations (Le-Coze, 2005) to help identifying these potential slippery slopes? It raises the question that everyone is asking following an accident, why couldn't we see before what seems quite clear after, with hindsight? How to design the tools to see what is obvious only after, when we know that the accidents dynamics lies in the complexities of the interactions between the technical, human and organisational dimensions?

Our current research project has three purposes and questions in that respect:

1. Can we see better with the help of an articulation of safety engineering, safety management and social concepts (extracted from the safety and accident field) some dimensions that are not captured today with traditional tools, the level of resilience (or reliability) of a chemical site?

2. Is what we see helpful for practitioners so that they can use it as a support for creating or sustaining safety in a better way that they did before, without us?

3. Can we transfer these tools to "non experts" for internal auditing purposes performed for example by safety people and safety auditors?

This paper elaborates on the first question. It is based on an empirical case study for which we attempted to connect safety engineering with safety management and social concepts. This paper is meant to be part of a reflexive step in our research process rather than a definitive conclusion to the question. The content of the paper is also very restricted, it is a rather general view that is presented here, without the details.

In a first part, we introduce the plant where we carried out the research. In a second part we discuss the strategy we followed to try to describe and interpret what we call the *organisational safety dynamic* and we conclude.

2. THE PLANT

The plant described here is an entity of a chemical company located in the USA and owner of 100 subsidiaries all over the world. The company is organised under a matrix principle. It means that certain activities are centralised either in the headquarters or in companies having specific resources for dealing with specific questions (such as salary payment), a particular production and consequently working for other plants. Through different restructurations of the production lines in the world, the plant has a leader role in its production segment, but a margin position when we consider the global production set of the whole company. It has around 350 employees, develops its production volume and have therefore to hire people while the other companies in the neighbourhood have been firing employees regularly during the last decade. The "safety culture" as they formulate it, is a great challenge for the company which tries to enhance the safety performance of the whole company through different actions and is used to communicate broadly on this topic. It has to be added that the safety manager in this French plant is responsible for safety not only in France, but in Europe, and belongs to the network of safety managers aiming to maintain the plants on a high safety level.

As mentioned, the plant can be described as a HRO (Roberts, 1990): it has namely a very safe production history with no accident registered in the last 22 years, the safety perception of the employees is reinforced over different tools and systems, last but not least it has very good relations to the regulators because it fits with the objectives given to the industry. The social organisation is also designed for having good work conditions, for example six shifts of five people have been introduced after the working time reduction for targeting a full team work all over the year. Nevertheless the production pressure has increased in the last years.

3. DESCRIBING AND INTERPRETING AN ORGANISATIONAL SAFETY DYNAMIC

Our research strategy is based on two strong principles:

1. Articulating the organisational safety dynamic on the safety barriers (technical and human) of the installations. This has now a long history, from Haddon (1973) through Johnson (1973) to more recent works like, Hollnagel (2004) or Hale et al. (2005), Hale et al. (2006). The approach retained here is to be anchored enough in the preventive design of the system against major hazard scenarios at a micro level (technical and individual and collective) in order to link this design with higher features of the system, like meso level (organisation) and macro level (environment of the organisation). The idea is to try to *put the organisation in*

motion. Organisations are indeed characterised by constant evolutions and stability seems rather to be the exception in these systems, than the norm.

2. Articulating two investigative modes to reveal an organisational safety dynamic: a normal study approach (what's happening when nothing is happening?) with an accidental one (looking at past incidents or accident and the organisational sides of the genesis of accident) in order to generate assumptions regarding the relevant patterns influencing safety.

3.1 Connecting with the barriers

The initial step consisted in applying the first principle introduced above and therefore in understanding the hazards and related technical and human barriers designed and implemented for controlling risks. Through this step, we identified several scenarios and finally focused on two main activities of the plant. The choice was to limit the areas to be investigated as the time available for the project would have not allowed us to look at all the activities of the plant. However by choosing a highly automated and core process of the plant with one of the most hazardous scenario, we thought that we could get quite in depth in the way the organisational safety dynamic influenced these activities.

The safety barriers are a combination of technical (hardware and software) and human tasks to be performed in order for the installation to stay within the safety limits as defined during design and risk analysis. Due to the interactions between technology and humans, some of the safety barriers are a mix of tasks to be performed as a co-ordination between technology and people (as for example an operator reacting on an alarm and consequently manually closing a valve). In this case it is possible to discriminate them by indicating the specific role that they play by decomposing each of the tasks required for the safety functions to be met[2]. These tasks can be described in terms of sequences consisting in identification-diagnosis-action to be performed for reaching some defined goals. Both human and software can be described through such sequences. However some technical devices are passive hardware so that they do not integrate software, or even external source of energy, as for example a rupture disk or a dyke. Sometimes, some human tasks do not include the use of safety devices at all (such as an operator checking a quantity of product to be put in a vessel, before putting it, or an operator escaping during an emergency).

[2] There is probably not a single and best way of distinguishing barriers, but this simple decomposition proved heuristically valid and simple enough to be used for the purpose of our research and developments.

When the barriers are identified, they can be assessed in terms of their adequacies for preventing the events that they are supposed to prevent. Features such as the response time, the independence, the redundancy, the capacity to fulfil the function, the level of confidence, are to be considered. Of course technical and human tasks can't be assessed the same way (human cognition and human interactions models are for example not as accurate as those in use for man-made software and hardware), but this issue is not developed in this paper. One of the outcome of this first step can be for example a graphic representation showing in a simple way the safety barriers designed for preventing the hazardous scenario. In the case retained for this paper, the scenario identified concerns the loss of containment of toxic chemical products following an increase of pressure and leading to a rupture of the vessel (figure 1).

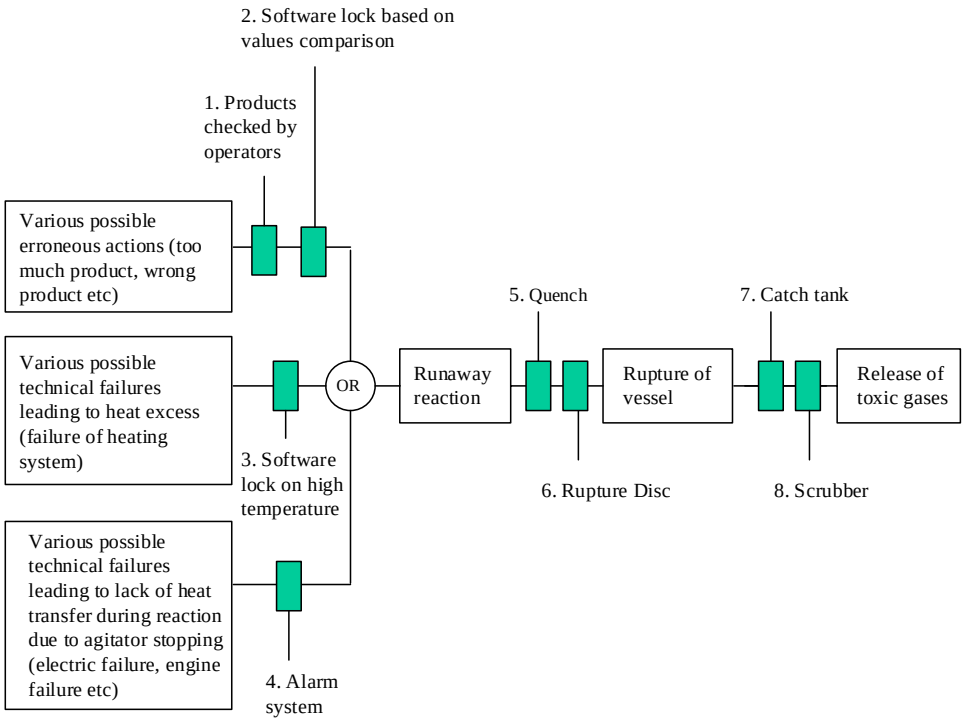

figure 1: Barriers for loss of containment of toxic substances

A set of 8 barriers have been identified. The possibility of an operator loading too much or loading incompatible product to the reaction is one first event. This is prevented by operators checking what they are supposed to put (this is carried out by two people from two different teams) but also by a software function based on value comparison of masses and expected pumping time. The heat excess and loss of agitator is backed up by first a software action linked with heat excess and an alarm in case of electric loss or agitator failure. The next barrier is the presence of a quench in case of a runaway reaction. This hardware is meant to pour water in the reaction for stopping a runaway reaction, and can be manually activated but is also programmed to be activated on high pressure threshold. The sixth one is a rupture disk designed to relieve pressure in case of runway reaction. This prevents

the vessel from reaching a rupture threshold and blowing. The seventh one is a catch tank collecting what is released through the relief system. The last one is a vent scrubber designed for treating atmospheric emissions in case of high pressure in the catch tank requiring release of product outside.

This simplified description is meant, when we move away from the scenarios themselves to the human and social world, to guide, to focus interviews and observations, with in mind what is there to be prevented by the organisation.

3.2 A normal, non incidental-accidental study perspective

The next step consisted in putting the organisation in motion in a non incidental-accidental perspective. To get into this normal perspective, we implemented two techniques:

1. Describing and assessing the safety management system in place, and compare it to existing good practices in the field, in a more traditional auditing approach. This consists in checking the presence and articulation of safety related activities, from risk analysis to learning from experience through training or maintenance. The specificity was to anchor questions in relation with the barriers identified.

2. Interviewing people (operators, managers, executives) in an open perspective, without being guided by an underlying safety management system model, but instead having opened discussions about subjects related to safety, but also to subjects that would be relevant but not always directly related to safety (such as working conditions, team relationships, evolutions, trends in management, technologies, market etc), in a more sociological approach. The underlying and guiding models are those from the human and social sciences in general, and the ones specifically developed in the safety field. In regards with what we know from accidents (drift, deviancies and their underlying favourable conditions), it was for example, found relevant to describe the evolutions of the organisation, and interview people about the impacts of these on their work in regards with safety, about the impacts on their interaction with their working colleagues.

The two techniques are complementary. It seems especially relevant when the company has a good approach of safety management and a long tradition of implementing safety management principles[3]. The second approach in that case helps in identifying interesting factors.

Thus, we identified important trends such as the new market and competition of China but also the changes in technology with more and more automation towards an harmonisation throughout the plant and processes. We also found useful to notice other changes located at corporate levels affecting the organisation, so that managers don't have much power anymore but only manage money and do not have strong strategic autonomy. The plant has become a profit center.

Production pressure got also more and more intense and they for example as a consequence look for alternative way of producing during holidays. This would

[3] This comment is quite compatible with idea of the need for different safety-accident models according to the type of system investigated, from safe to ultra safe systems.

help limiting the duration of plant stops. This has consequences for maintenance planning, as maintenance teams have always had so far a traditional break throughout the summer for taking the time to perform their activities. Some internal organisational changes have also recently affected the safety meetings so that people from different units do not meet in the same way that they used to anymore.

In fact, it can be revealed a situation of the plant under similar constraints of a policy of Better / Cheaper /Faster, coping with at least three sometimes antagonistic goals: safety & environment, production, quality. Some plays around the safety rules (such as “necessary violations”, Reason, 1993 or adaptations such as the ETTO concept, Hollnagel, 2004) thanks to tacit agreements from the hierarchy do happen. Without them, the organisation would probably not run smoothly under such constraints (we have heard it, and we have seen it). Of course this picture of an organisation which gives signs of playing with its limits (Starbuck et al, 2005) can't be applied strictly to this plant as downsizing, budget restrictions or loss of expertise with departure of experienced and skilled workers is not the case at all here. It must be on the contrary balanced with good signs of resilience or reliability. For example, the expertise on safety issues by the safety department is high and time is taken for performing risk analysis, management of change but also training and learning from experience. The management of the plant has a strong experience of the chemical industry and a background of chemical engineering helping him to better conceptualise the technical safety issues. The expertise available in safety engineering throughout the group is also very high and helpful when used.

The next part introduces the incidental-accidental approach, that we used for discussing the findings of the non incidental-accidental, normal, perspective as described above. In theory, this technique is easier because it consists in describing and interpreting events by unfolding the context of these ones.

3.3 Incidental & accidental study perspective

The other strong advantages is that it shows the organisation as it really is because the incidental-accidental study reveals the true side – or the "dark side" (Sagan, 1993, Vaughan, 1999) – of the organisation. The interest in looking at the incidental-accidental perspective is to have the opportunity to describe the impact of a specific organisational design on safety. It is indeed very difficult to describe the impact of the regular evolutions and transformations of the organisational design without the help of concrete safety related events. The absence of events is also indeed in principle a strong indication that the level of safety is good, but it might also be interpreted that relevant information are not captured and analysed.

In our case study, two incidents were easily identified, and couldn't have gone unnoticed. Two runaway reactions, in the processes that we chose to study for the research, ended up in the catch tank few months ago. These two incidents were very similar, revealing a weakness in the installation design but also therefore in the way the organisation was able to identify and assess risks. However, a positive side of the event was that it also made clear that the back up design of the

installations was well dimensioned for the scenario, because toxic gases were contained and only a small quantity of gas treated through the scrubber was released to the atmosphere. The incident didn't trigger any concern from the nearby towns and inhabitants.

After studying the analysis performed by the company on these events, the approach that we followed consisted in interviewing the operators involved during the incidents, in order to hear directly the chronology but also how they perceived the events, and the way it was treated internally. We then interviewed the people who participated to the analysis, so that we could understand better how it impacted their representation regarding the level of safety of the plants but also how the organisation did learn from it.

The main technical cause is linked with the agitator stopping in both cases (one for a power cut and the other for a failure of a software component) and then creating a direct path to an uncontrollable runaway reaction leading to the rupture disk to blow and then to release the content of the vessel in the catch tank. This accident sequence is quite clear when using figure 1. It is interesting to notice that the quench that was supposed to stop the runaway reaction couldn't serve this purpose when the agitator was stopped, so that in this specific scenario, it is in general inadequate.

Without going too much in the detail of this case and its analysis, it is interesting here to notice that a scenario found its way throughout to create an uncontrolled runaway reaction[4]. Without questioning the outcomes of these events which definitely also proved twice the safe design of the installations, it is however an opportunity for the organisation to learn about the inability of a network of people to anticipate and to prevent the incident. Looking the events this way, some clear organisational dynamic dimensions appeared. They demonstrate how an organisation can sometimes generate its *own blind spots*, but also how the ability to stay updated in regards with available methods and safety technology, although available internally within the group, was not generated to identify and assess the scenario, and investing for example in a new design. Availability of time but also of resources in safety can be pointed at, all these factors diminishing the possibility of a requisite imagination (Adamski, Westrum, 2003). Without the expected behaviour of the barriers as designed (a proportionate design of the relief system, maintenance of catch tank), the events could have ended up in a more important incidents.

4. CONCLUSIONS

The aim of this paper was to introduce current findings and some discussions around the assessment of the resilience or reliability of an organisation by a team of outsiders in the chemical industry based in a case study. The paper stressed the importance for such an assessment of connecting a normal study approach (whats happening when nothing is happening?) with an accidental one (looking at past

[4] We get close here to the Perrow's (1984) normal accident idea, of unplanned and hidden interactions within the installations.

accident and the organisational sides of the genesis of accident). This helps in contrasting interpretations and also articulating them.

Regarding the question "what's happening when nothing is happening?", it is clear to us that, in a capitalistic society, a company looks for technological and organisational transformations that help creating more profits, while maintaining a reasonable perceived level of safety. There is nothing to be surprised of. Changes will affect the system probably until it is proved that the system becomes not safe anymore. The conditions of this dynamical process depends on the interaction of cognitive, psychological, social, cultural, economical and political dimensions, making of prevention a complex phenomena.

The first results of our case study indicate that the company, despite an excellent approach of safety, got surprised by a preventable scenario, demonstrating that even in organisation dedicating resources to reach the features of high reliable systems, the possibility for blind spots to develop is far from being unlikely. The trend affecting the current transformation of the organisation should be considered very carefully in regards with these recent events. Availability of time for key safety people to step back and look at the installations in light of the new available safety technologies, of the new available risk analysis methods and of the incidents from similar installations, should be ensured.

REFERENCES

Adamski, A.J. & Westrum, R. (2003). Requisite imagination: the fine art of anticipating what might go wrong. In E. Hollnagel (Ed.), *Handbook of Cognitive Task Design* (pp. 193-220). Mhawah, NJ: Lawrence Erlbaum Associates.

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

Haddon, Jr. W. (1973). Energy Damage and the Ten Counter-Measure Strategies. *Human Factors Journal*, August.

Hale, A.R., Guldenmund F.W., Goossens L.H.J., Karczewski J., Duijm N-J. , Hourtoulou D., LeCoze J-C., Plot E., Prats F., Kontic B., Kontic D. & Gerbec M. (2005). Management influences on major hazard prevention: the ARAMIS audit. ESREL.

Hale H., Guldenmund F. & Goossens l. (2006). Auditing resilience in risk control and safety management systems, in Hollnagel E., Woods D. & Leveson N. *Resilience Engineering: concepts and precepts*. Ashgate.

Hollnagel, E. (2004). *Barriers and accident prevention.* Ashgate.

Johnson, W.G. (1973). The management oversight and risk tree – MORT including systems developed by the Idaho operations office and aerojet nuclear company. Downloadable on www.nri.eu.com, the website of the Noordwisk Risk Initiative.

Perrow, C. (1984). *Normal accident theory, living with high risk technology*. Second edition. New York: Basic Books.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem, in *Safety Science* vol 27 n°2/3, p 183-213.

Reason J. (1993). *L'erreur humaine.* Le travail humain. Paris: presses universitaires de France.

Roberts K.H. (1990) Some characteristics of one type of high reliability in organisation. *Organisation Science*, 1(2), 160-176.

Sagan, S.D. (1993). *The limits of safety*. Princeton University Press. Princeton.

Snook, S.A. (2000). *Friendly fire, the accidental shootdown of US black hawks over northern Irak*. Princeton university press.

Vaughan, D. (1999). The Dark Side of Organizations: Mistake, Misconduct, and Disaster. *Annual Review of Sociology*, 25, 271-305.

Vaughan, D. (2005). *System effects: on slippery slopes, repeating negative patterns, and learning from mistake?* In Organization at the limit. Lessons from the Columbia disaster. Blackwell Publishing.