Vigilance: a process contributing to the resilience of organizations

Ambre BRIZON[1] and Jean-Luc WYBO[2]

[1] Ecole des Mines de Paris, Pôle Cindyniques, BP 207 F-06904 Sophia Antipolis, France
ambre.brizon@ensmp.fr
[2] Ecole des Mines de Paris, Pôle Cindyniques, BP 207 F-06904 Sophia Antipolis, France
jean-luc.wybo@ensmp.fr

Abstract. From the analysis of emergency management activities, four main processes can be identified that contribute to the resilience of an organization facing a hazardous situation: Prevention, Protection, Learning and Vigilance. Vigilance is the ability of a system to detect and interpret weak signals and alerts. By doing so, it develops its anticipation capacities. We define two types of vigilance: individual and organizational. First one is required to run safely a system, but is difficult to set up. The second one permits to avoid crisis. After that we expose an organization of vigilance in three times: 1. Instantaneous danger, 2. Non instantaneous but known danger, 3. Unknown danger. But being vigilant requires access to information. We define three barriers that weaken vigilance: A *contextual barrier*, an *interest (*or *routine) barrier* and a *communication barrier*. Finally, we propose rules to promote a vigilant behavior and to organize vigilance in a system.

INTRODUCTION

Resilience, with respect to the behavior, was defined by Cyrulnik [2002]; he explains that resilience is a set of mechanisms established by beaten children for not reiterating their parents' errors. This enjoins us on a reflection on the evolution. Aims of the children are not the same than the ones when they will be adults. This evolution was underlined by Hoc and Amalberti [1994, p.187]. They focus that most problems of our systems come from their dynamic and increasing complexity.

To answer to this problem, Hollnagel [Hollnagel & al., 2006] proposes the concept of resilience engineering. He explains [p.3] that resilience engineering concept is reactive in front of an attack, but also proactive for preventing from threats.

Learning from experience (LEX) provides a better knowledge about threats and about the behavior of people and organizations. From the analysis of emergency management activities, four main processes can be identified that participate in the resilience of an organization facing a hazardous situation:

- Prevention. The organization knows the threat in advance (from analysis or experience) and sets up preventive and protective barriers.
- Protection. When the system is attacked, it reacts to stop or reduce the threat.
- Learning. The system uses its experience to adapt itself (for instance to an unprecedented threat) and develops its evolution capacities (learning loop, cf. [Argyris and Schön, 2002]).
- Vigilance. The system develops capacities of observation, detection and interpretation of weak signals and alerts. By doing so, it develops its anticipation capacities.

According to this processes, enterprises created the function of risk manager in the seventies (for more information on risk manager see [Véret and Mekouar, 2005]), in a more proactive than reactive vision. But the risk manager position exists only in large enterprises, and even in these ones, they cannot work alone. Every one is concerned by the vigilance. A banker has to be vigilant to stock exchanges, a farmer to insects, a chemical operator to his workshop conditions.

In this paper we will not look at economic vigilance (banker with stock exchanges), because it does not raise questions about type of signals one has to observe. A banker knows signals he has to catch. And in this case we do not talk about vigilance but about attention. Attention is related to a specific point; vigilance concerns all the environment, without any preconceived ideas. The second question not raised by the economic vigilance, is the problem of information traffic. In this area, information arrives to the right person (cf. [Lesca, 2001, p.5] and [Lesca and Dourai, 2004, p.113]).

When we talk about vigilance we are tempted to measure it. But we cannot propose a scale, because that scale would depend on perception of risk and would require a deep knowledge of its objective. It is the experts' work ; they are able to set up hypothesis and validate or undermine them. For that purpose, they have knowledge and LEX. Only experts have a sufficient knowledge to elaborate a good scale (in their enterprise), with an exhaustive list of all important parameters. Furthermore, if being vigilant is not easy for a specialist, it is worse for a simple operator, who has to pay attention to all different types of parameters: health, security, quality, hygiene, etc. A risk manager knows that, and has to consider it when he organizes vigilance.

In this paper, vigilance is applied to industrial or state-owned systems. First, we will define two types of vigilance, individual and organizational. After that, we will point out how experts are vigilant in their function, and barriers that may weaken vigilance capacities. Finally, we will propose means to suppress those barriers and to organize vigilance in industrial systems.

1. INDIVIDUAL VIGILANCE AND ORGANISATIONAL VIGILANCE

As said before, we propose to define two types of vigilance: individual and organizational. They need different mechanisms, but they both have their place in a system. Individual vigilance is difficult to set up, but an organizational vigilance can not be sustainable without it.

Bourrier [2001, p.30] shows the importance of vigilance for regulating conflicts (vigilance but also communication and interaction between actors; this refers to the notion of trust). For someone to be vigilant, Chateauraynaud [1996, pp.81-82] says that the person should not be worried or preoccupied. For that, he should only be attentive to something, or he should be attentive to nothing.

But individual vigilance is limited. Amalberti [2001, pp.68-70] observes that attention capacities of operators are flimsy. They are split in two groups: general attention capacities (we will call them vigilance capacities, because the attention is paid to the whole environment), and specialized attention capacities (we will call them attention capacities, because here the attention is on precise points). In order to cope with this difficulty, vigilance should be organized as a process, involving several people in the organization.

Bourrier [2001, p.30] says that vigilance contributes to the organizational stability, and especially in the vision of High Reliability Organizations (HRO). But vigilance contributes also to avoid crisis or accidents. For example Vaughan [2003] shows that Challenger and Columbia accidents could have been avoided if the organization had been vigilant to several fault signals. This problem came from the lack of vigilance of decision-makers and the lack of trust of operators in their knowledge.

In order to set up an organizational vigilance process, all members of the organization should be involved, from the workshop to the top management (cf. [Chateauraynaud, 2003], [Wybo, 2004], [Axelsson, 2006]). Moreover, for being vigilant, people need to trust each other [Slovic, 1993] and to communicate [Wybo, 2004]. Without this climate of trust and exchange, vigilance would only be strategic (bottom-up transmission) but not tactic (embedded in action) and effective.

If vigilance can already exist for each person in the system, organizational vigilance has to be set up by the risk manager. He has to organize his own vigilance, the system's one, and improve the individual's one.

2. HOW ARE WE VIGILANT?

With the collaboration of an expert of chemical processes, we analyzed the vigilant behavior he set up when he works in his factory. We validated this *model of a vigilant behavior* with four other safety chemical experts, and present it in Table 1. In this model, different types of vigilance are ordered by priority.

Table 1. Model of vigilant behavior.

1. Imminent danger, the vigilance goes first to the vital points of the system. (death danger, explosion danger, etc.)
2. Not imminent but known danger, the vigilance goes on the general environment: are there any abnormalities in the system's environment? Does it works correctly?
3. Unknown danger, reflection is on the potential danger, need to check barriers than already exist.

For example, in the industry, a safety manager will be vigilant to:

1. Imminent danger: vigilance concerns human safety.
2. Not imminent but known danger: vigilance concerns the environment:
    a. Does it work as it should at this moment ?
    b. Have people integrated learnt lessons (LEX) ?
3. Unknown danger: reflection is on the potential danger, one needs to check the working state of safety barriers (technical, organizational or human).

Other examples of vigilance can be found in social insurance:

1. Setting up of medical committee for a patient with many pathologies. Crisis could come from a rapid deterioration of the health state of the patient, caused by an accumulation of aggravating factors in different medical specialties (first

aspect of vigilance behavior).

2. In France, medical staff has to collect incidents and weak signals (see http://www.anaes.fr). This corresponds to the third aspect of vigilance behavior.

3. Still in France, the number of categories of professional diseases raised from 10.000 to 40.000 in ten years (1995–2005). We do not know what will be the future professional diseases, but the French health insurance system has launched an information campaign for industrials to take care of their long term employees' health and not only during their activity period.

This vigilance model is only valid if the system owns the required information: vigilance process consists in capacities of vigilance associated to sources of information. This information may come from the system itself or from outside. The job of the risk manager is to be vigilant to all kinds of information. But all signals or data are not important, and he has to pick up relevant ones. For that, we divide information into external information (see fig. 1) and internal information (see fig. 2).

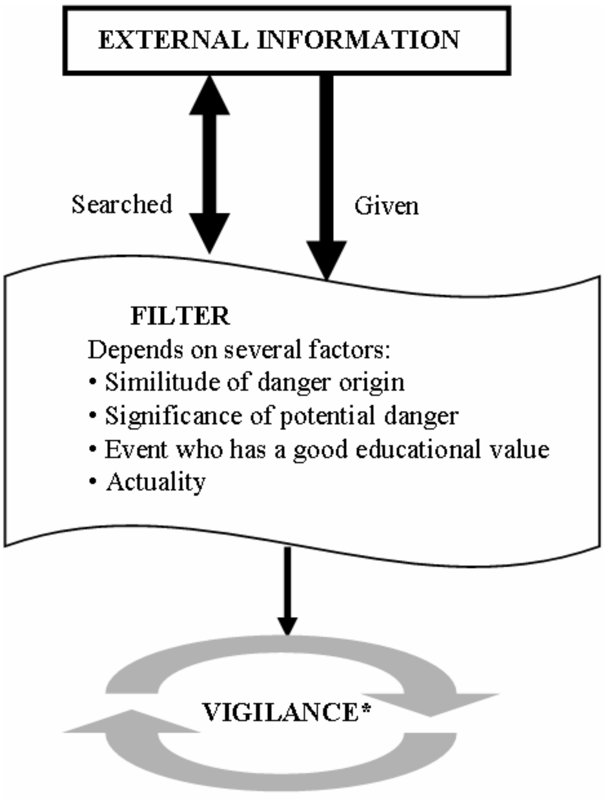

Fig.1. Management of external information.

*Here, vigilance is seen as a life cycle, than needs to be fed.

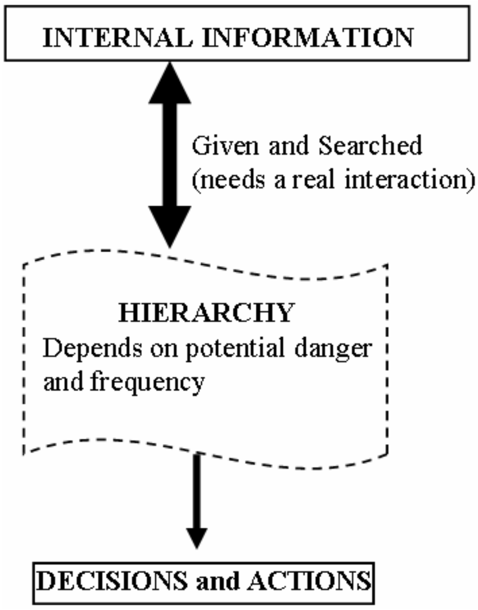

Fig.2. Management of internal information.

We see with these two figures that external information needs a filter. The risk manager cannot take all of them. Unlike internal information, that is processed but in a hierarchical order. More of that, external information feeds the vigilance, as the internal one always drives decisions and actions. But information does not appear spontaneously; the incoming information may face several difficulties before it can be processed.

3. VIGILANCE'S BARRIERS

Setting up an organizational vigilance process needs to solve three types of difficulties that we represent as barriers:

3.1 Contextual barrier

What is to be detected? This refers to the notion of normality/abnormality in a given environment ("is the situation normal?"). Experts are more efficient for detecting abnormal signals in their working environment.

The problem of contextual barrier is the most related to vigilance. Among the three kinds of barriers, this one points out a lack of professionalism of the person, who should not be only attentive to a set of given signals and data, but to the whole workshop environment. At this stage of the vigilance process, we are not trying to conceptualize a potential danger but only at the phase of detecting precursor signals. One way to reduce this barrier is to exercise the actor's eye. A solution could be to set up regular exercises, for making people more sensitive to their environment and able to detect abnormalities.

3.2 Routine barrier

The "human sensor" should have a sense of danger for being vigilant to precursors. What makes the relevance of a given signal or data for him: its relation with a given risky situation. We can bridge that to the notion of *routine barrier*. When the risk perception is reduced, precursor signals are present but one does not consider them as he does not perceive a potential risk in the current situation.

The routine barrier corresponds to the lack of perception of potential danger. Signals are perceived, but no one pays attention to them. Perception of potential danger is not always innate. It needs to be learnt and periodically reminded to maintain vigilance capacities. This could be achieved by training and exercises, but also by regular interaction with the risk manager.

3.3 Communication barrier

Will the "transmitter" be willing to transmit the signal ? Will he be listened to and understood by his peers and managers ? The easier the dialog is with others, the lower the barrier is.

Finally the communication barrier shows us the problem of getting information. If the two first barriers are more individual, this one is more organizational. The risk manager has not only to set up training and exercises for his staff; he also has to search for information in the workshop and develop a good atmosphere among people to promote dialog and trust. He has to pay attention to stories and anecdotes told by his staff. But staff has to volunteer to give information. Vigilance is the work of all members of the system: everyone has to listen and talk about what happens and about what they feel or perceive.

CONCLUSION

Vigilance is one of the key processes that participate to the resilience of industrial systems. Vigilance is achieved by individuals but it needs to be organized. Three barriers have been identified as the main obstacles that weaken the vigilance process by limiting collection and sharing of information. We propose three simple rules to promote a vigilant behavior and to be able to organize vigilance in an industrial system:

Rule 1: *inform people about potential risks; danger is not obvious for every one*. This information can be given by training, LEX or exercises.

Rule 2: *search information from all the system's members*, they are observers of precursor signals.

Rule 3: *process causes before consequences*. Even if it needs more time, energy, and money, solutions will be stronger. Because it is difficult to forecast the system behavior and evolution in the future.

AKNOWLEDGEMENT

We would like to thank M. Jacques Expert (Sanofi Aventis safety group) for his help in safety management. And Ms. Aïnhoa Paré (PhD student) for her approach of vigilance.

REFERENCES

Argyris C., Schön D.A. (2002). *Apprentissage organisationnel*. Ed. De Boeck Université. original edition, Organizational Learning II. Theory, Method, and Practice, 1996.

Axelsson L. (2006) *Chapter 10, Structure for Management of Weak and Diffuse Signals*. in: Hollnagel E., Woods D.D., Leveson N.G. (2006). *Resilience Engineering, concepts and precepts.* Ed. Ashgate Pub Co, pp151-154.

Bourrier M. (2001). *Organiser la fiabilité*. Edition Risques Collectifs et Situations de Crise, L'Harmattan.

Chateauraynaud F. (1996). *Modèles de responsabilité, formes de preuves et dynamique des alertes.* Intervention in the seminar of Programme Risques Collectifs et Situations de Crise, in Paris, the february 15th, 1996.

Chateauraynaud F. (2003). *Pour un observatoire informatisé des alertes et des crises environnementales - Une application des concepts développés lors des recherches sur les lanceurs d'alerte.* Rapport Final. CEMAGREF, GSPR-EHESS.

Cyrulnik B. (2002). *Un merveilleux malheur*. Edition Odile Jacob, January 31.

Hoc J.M. et Amalberti R. (1994). *Diagnostic et prise de Décision dans les Situations Dynamiques*. Psychologie Française, n°39-2, p. 177-192.

Hollnagel E., Woods D.D., Leveson. N.G. (2006). *Resilience Engineering, concepts and precepts.* Edition Ashgate Pub Co, pp9-18.

Lesca H. (2001). *Veille stratégique : passage de la notion de signal faible à la notion de signe d'alerte précoce.* In Colloque VSST (Veille Stratégique, Scientifique et Technologique), Barcelone, 7p.

Lesca H. and Dourai R. (2004). *Traque et remontée des informations de veille stratégique anticipative : une approche par la notion d'épanouissement de soi.* FACEF PESQUISA Vol 7, N°2, pp.110- 126.

Slovic P. (1993). *Perceived Risk, Trust, and Democracy.* Risk Analysis, Vol. 13, No. 6.

Vaughan D. (2003). *Chapter 8, History As Cause : Columbia and Challenger. in : Columbia, accident investigation board.* Report vol.1, pp195-204, august.

Véret C. and Mekouar R. (2005). *Fonction: Risk Manager*. Ed. Dunod, p.354.

Wybo, J.L. (2004). *Mastering risks of damage and risks of crisis: the role of organisational learning.* International Journal of Emergency Management Vol. 2, N°1&2, p.22-34.