Safety Science 50 (2012) 1438–1444

Contents lists available at ScienceDirect

Safety Science

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

Availability organisational analysis: Is it a hazard for safety?

Marc Voirin [a,*], Sandrine Pierlot [a], Michel Llory [b]

[a] EDF/R&D/MRI, 1, Avenue du Général de Gaulle, 92141 Clamart, France
[b] Institut de l'Analyse Organisationnelle (IAO), Mas Saint Sauveur – Route de Torreilles, 66430 Bompas, France

ARTICLE INFO

Article history:
Available online 1 February 2011

Keywords:
Availability
Safety
Organisational analysis

ABSTRACT

This main issue of this article analyses the possible way to use for availability improvement, the organisational analysis methodology initially developed for accident safety investigations. As the last decade examples in the industrial world prove that some organisational weaknesses could either impact safety or availability, we have for purpose to make some important clarifications, with the help of the organisational paradigm, and grounded on our knowledge of safety accidents or local inquiries in hazardous technical complex systems.

We will first give our definition of an availability event, by comparison with a safety event and recall what is for us an organisational analysis. Then we will consider the safety organisational paradigm pathogenic factors in wondering if these factors could also be seen as pathogenic factors for availability; or if specific availability pathogenic factors can be inferred from these safety pathogenic factors.

In the end we will try to assess the common points and the differences between an availability oriented organisational analysis and a safety oriented one, with a particular attention to possible negative follows-up on safety issues and to the methodology issue.

1. Introduction

The safety of the high-risk industries is based on practices established since many years. These practices could be summed up in three items:

- current safety issues analysis,
- forecast safety analysis as Probabilistic Safety Assessments developed for nuclear power plants,
- safety event feedback analysis.

However, although these practices are grounded and generally implemented in the industries with a lot of important means, many managers and experts point out that the number of significant incidents and accidents does not decrease durably (Dien, 2006); as if these practices and the associated methods had allowed to reach an unbridgeable asymptote; as if these methods, focused on the correction of technical failures and the integration of the human factor in the design and the daily operation had reached such a maturity level that they would have exhausted their ratio of beneficial contribution and they would have been no more sufficient to go further more.

According to us, the safety level's asymptote is not a fatality. Other tracks for the safety improvement are full of promise, such as the integration of the role the organisations play in the occurrence of the incidents, accidents, or crisis.

Since 1999, EDF R&D, with the support of Michel Llory, has been developed a method for a safety organisational analysis derived from, on one hand, a systematic and detailed analysis of more than 20 industrial accidents, and, on the other hand, the knowledge of several dozens of incidents and accidents, including complex occupational accidents (Dien and Llory, 2007; Pierlot et al., 2007). The first objective of this method is to highlight the pathogenic organisational factors having precipitated or facilitated the occurrence of accidents or incidents resulting from a degradation of the plant safety level; the second one is to realize safety level diagnoses for high-risk plant at any time in the life of the concerned plant (thus beyond a post-accidental investigation).

However, whatever is the domain of activity, the economic competition becomes a main stake of the industries. Among all the indicators, the availability and its opposite – that is the unavailability of the plant, the period during which it cannot produce any more – is a parameter put under surveillance in numerous high-risk industries.

Then, these industries express the need of having deepened analyses to understand the root causes of the occurrence of events leading to consequent availability losses of their plants.

Knowing this, with the help of our theoretical and field knowledge on the safety issues, we consider that availability organisational analyses could be helpful in the search for a better availability level for hazardous plants. Nevertheless, dealing with the question of availability organisational analysis sends back to

* Corresponding author. Tel.: +33 1 47 65 46 75; fax: +33 1 47 65 51 73.
E-mail address: marc.voirin@edf.fr (M. Voirin).

0925-7535/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ssci.2010.12.013

the difficult issue of the connections between safety and availability. We can wonder, and we have to wonder if the availability improvement is always compatible with the preservation of a good safety level.

It is then necessary to put in balance the arguments of those claiming that safety and availability naturally keep pace, and the thoughts of those who are sceptical and consider that the search for a better availability can worsen the safety of hazardous plant.

2. First, some definitions

The issue of this paper is focused on the availability of a hazardous and complex socio-technical system. What are we really talking about? What is availability? What is a hazardous complex system?

Llory stated that the systems we are looking at are high level performers where modern technology and complex design aims to insure good daily operating results, a sufficient safety level with the help of numerous redundancies and control instrumentation (Llory and Montmayeul, 2006). And as these technical systems are managed, controlled, fixed by a human organisation (that can be itself complex), they have an indisputable socio-organisational dimension. Chemical factories, nuclear power plants, commercial planes or ships ... are hazardous complex socio-technical systems.

Therefore, dealing with complex socio-technical system means looking at a three dimensions system (technical, human and organisational ones) characterized by a multidimensional aspect and an intrinsic complexity, where many interactions may occur (Duval et al., 2007).

The original Reliability Theory definitions usually point out four fundamental functions that must be met by a given system: reliability, availability, maintainability and safety.

According to the CEI 60050-191 standard, the system *availability* is the capacity of a system to feed its expected mission, within given operating conditions at a given time.

Reliability has the same definition, excepted that the time dimension is not at a given time, but during a time interval.

The *system maintainability* represents the capacity of a given system to be fixed, to recover its original operating performances.

The last function, *safety*, can be described as the system capacity to avoid catastrophic failures, potentially hazardous for workers, for the environment or for the public. Such catastrophic failures are very seldom because high-risk systems are designed in order to avoid or mitigate them (Llory and Dien, 2006).

What can be the expected availability missions of a given system? These missions can be related to time, delays (a commercial plane has to take-off on time and to land on time); to performance (a power plant has to be able to run at requested power); to product qualities (passengers of a commercial plane must travel with a good comfort level)... All of these three missions can be seen of the main goals of a system; each specific systems having its own main goals.

Availability must not be confused with *competitiveness*: competitiveness is the capacity to increase one of the availability missions of a given system. For example, the air-plane industry, in the search of the best competitiveness will try to obtain planes as full with passengers as possible.

The safety missions of a given system are dramatically different from the availability ones. The occurrence probability of catastrophic events must be as low as possible; but as there is always a residual risk, effect of any catastrophic event must be mitigated, must be as less harmful as possible. So, minimisation of event effects is also part of safety missions of a given system.

Due to the importance of the safety issues (serious or deadly injuries, public health issues, environmental impact, social impact, etc.), many tools, methodologies, dispositions have been used or taken since several decades in the chemical industry, the oil industry, the nuclear industry or the air-plane industry, etc.

In many industries (nuclear, aviation, etc.), safety issues take into account the "human factor" since many years, and more recently, "the organisational factors".

Is it possible, recommended or hazardous to use such tools or methodologies in order to assess and then to improve the system availability dimension?

3. The complex interactions between safety and availability

Attention must be paid to the fact that availability and safety of a system are not two totally independent missions.

As example, if we have a look on a nuclear power plant, and if we try to classify simply its technical systems according to their contribution to safety and availability, we could identify three categories for clarification, as shown in Fig. 1.

Area 1 is made of systems dealing only with the plant *availability*, such as the generator group which allows to produce electricity thanks to the steam coming from the Steam Generators.

Area 3 is made of systems dealing only with *safety*. These systems are not required to produce electricity and are not operating: their purpose is only to fulfil a safety action if needed. For example, the Safety Injection System in a nuclear power plant has for mission to ensure the water quantity within the primary circuit, so that decay heat could be still evacuated, even in case of a water pipe break.

Area 2 is made of systems dealing *both with safety and availability*. For example, the Steam Generators fulfil a safety mission because they are part of the second barrier against radioactive material leakage, and also because their cooling capacities are necessary to deal with some accidental events; but Steam Generators have also an availability mission, because they produce the sufficient steam to make the generator group working.

But all of these systems could have both an impact on safety and availability. It is clear for area 2 systems, but, in case of failures, some of area 1 systems could have clearly an impact on safety, as some of area 3 systems could have clearly an impact on availability.

For example, if there is a turbine trip while the plant is operating at full power, the normal way to evacuate the energy produced by the nuclear fuel is no longer available without the help of other systems, and that may endanger safety even if the turbine is only dedicated to availability.

Safety and availability have then complex relationships: this is not because short term or medium term availability is ensured that neither long term availability or safety are also ensured: one shall never forget that, before the explosion, Tchernobyl, as Texas City BP refinery have records of very good availability levels.

One shall never forget that the Bhopal explosion or the Pic de Bure accident in France occurred with safety devices out of order since many months or years, but with a good availability and performance results (Dien and Llory, 1999).

Systems failure could occur on systems belonging to areas 1, 2 or 3, but the organisational pathogenic factor "Production

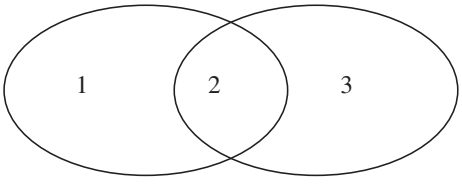

Fig. 1. An availability/safety system design classification.

pressures" (Pierlot et al., 2006) will have an impact mainly on systems belonging to area 3, on systems dedicated only to safety.

The Davis Besse case is a clear illustration of this fact: the self analysis performed by the plant owner (FENOC) underlines that, among the many causes of the crisis, a dramatic change of the management style of the plant, occurring several years prior to the event, made that safety was sacrificed to production goals (Dien and Llory, 2002b).

It means that, in that case, the search for the best short-term availability level was made in detriment of safety issues, resulting in the end, many years after, in a very bad availability record, when FENOC had to stop its plant during a very long period of time.

This makes clear that, ensuring availability does not mean ensuring safety; but also that ensuring availability could, in some cases, endanger safety. Confusion between availability and safety have produced misunderstandings of the situation and have led to catastrophic events: for instance, the loss of *Columbia* space shuttle is partly the result of the belief that the current separation of a piece of insulating foam at each mission was a maintaining issue and not a safety issue (CAIB, 2003).

But, as many safety devices are in stand-by when the plant is operating, any failures of these devices, any decreases of their performances to fulfil their missions, any impacts for the pathogenic organisational factors would not necessarily act immediately or are not readable on the safety level: the consequences could be delayed and be revealed many years after the original cause occurrence.

On the other hand, ensuring safety does not mean insuring availability: if there is a spurious reactor building aspersion (this aspersion is a safety device), the plant would have to be stopped during several days to be cleaned-up before being able to start again. However, the reactor building aspersion is only dedicated to safety and its spurious activation does not endanger safety in a short term.

This relationship between Availability and Safety and the associated hazards have been underlined by Wiroth, in its report dedicated to the EDF safety status: "*One must always insure that safety and availability are two different goals that help each-other to meet greater achievements... Production culture must never become more important than safety culture*"[1] (Wiroth, 2006).

This statement underlines the complexity of the relationship between safety and availability: it is then necessary to analyse availability on one side and safety on the other side, at least at the beginning.

When both the availability and safety organisational paradigms will be consolidated, we would maybe be able to analyse these two issues jointly; but before being able to reach that goal, it is necessary, with the help of real inquiries, to deepen our knowledge of safety and availability from the organisational point of view.

4. Is the methodology of the organisational safety analysis transposable into the study of the availability?

First, let us precise what we mean by a safety organisational analysis. The accident model underlying our approach may be defined as follows: any event is caused by direct, immediate technical and/or human causes but its occurrence and/or development is triggered, promoted and precipitated by underlying organisational causes and conditions (Dien, 2006). This model leads us to extend our analysis beyond the immediate causes. Every industrial system is coping with factors that impact safety, both positively and adversely. We consider that pathogenic organisational factors (POF) could be sources of dysfunctions. They are elements within the organisation which encourage the occurrence of an incident or an accident. According to our study, a typology of Pathogenic Organisational Factors could be established. We consider too that resiliencies could be favourable sources of resistance to the occurrence of accidents, sources of recovery if a minor incident occurs. Life of an high-risk system is a continuous tension between resilient organisational factors (ROF) and pathogenic organisational factors (POF). An accident occurs when POFs overtake ROFs. Fig. 2 (from ESREDA Working Group on Accident Investigation (2009)) below portrays how events can be seen (with the medical metaphor) as symptoms of prevailing conditions.

It involves an interest in the root causes of an organisational nature, in particular the pathogenic organisational factors, which require use of a method to highlight them (Dien, 2006). The organisational analysis approach is separated from the search for the main causes in order to better explore the *history* of the organisation, understand the *organisational network* involved in the accident at the level of both the industrial site's hierarchy and the entities with which this organisation has contacts (interactions between sub-contractors, safety authorities, subsidiaries, etc.) (Dien and Llory, 2007).

4.1. The historical dimension

Consideration of the historical dimension involves turning back the clock to understand and analyse the dynamics and development trends that have occurred to produce the accidental situation studied.

4.2. The vertical dimension

Study of the organisation's vertical dimension involves the hierarchical operation of the company, in particular the communications that are formally and informally established, both top-down and bottom-up. Its purpose is to highlight and understand the interactions between the decisional domain – at the high and intermediate level – the experts, and the field staff. It is specifically interested in the methods of relation, communication, circulation of information and decision-making, as well as methods of cooperation between front-line workers, experts and decision-makers.

4.3. The cross-functional dimension

The organisation's cross-functional dimension involves all entities with a close or distant involvement in the accident. Its scope is specific to the investigation conducted and may vary from one investigation to the other depending on the parties involved in the occurrence of the accident. This dimension allows the *organisational network* of the accident to be established as distinct from the organisation chart of the various parties. It reveals the complexity of the functional relations between entities, and in some cases highlights the absence or deterioration of relations between parts of the organisation that are supposed to work in close collaboration.

4.4. The comprehensive approach

The *comprehensive approach* is an essential contribution for the analyst wishing to conduct an organisational analysis. It is based on an approach involving inter-subjective analysis (between investigators and staff from the organisation targeted by the investigation) and a search for meaning, and in which not only the causes are sought, but also the reasons, intentions, motivations and reasoning of the people involved. In that respect it is distinctly different from the analysis methods based essentially on anonymous questionnaires.

Today, organisational analyses were already realized or are in progress within EDF on events connected to a loss of availability

[1] Authors translation.

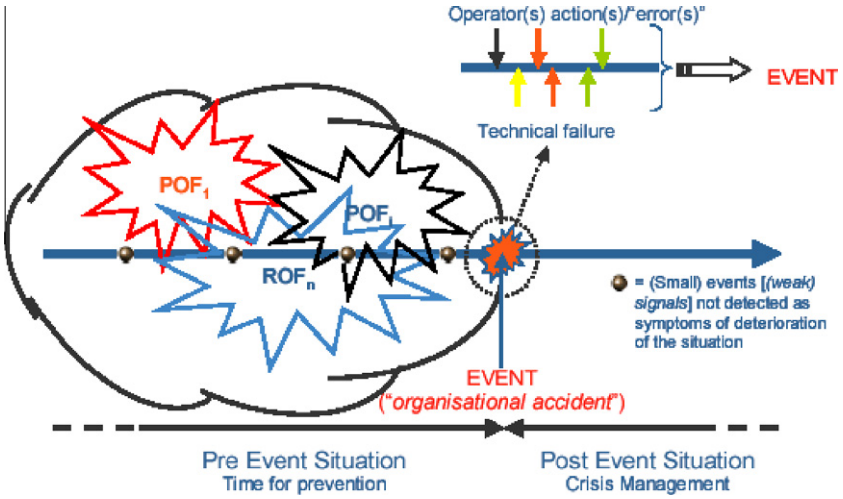

Fig. 2. Event development model (from Working Group on Accident Investigation (2009)).

of the plants. These organisational analyses bring for each case studied a supplement of understanding on availability issues which are commonly seen only as either purely technical dysfunctions, either connected only to human failures, or, in the best cases, as a combination of these two types of explanation.

5. The organisational safety analysis as a guide for availability issues

In the organisational safety analysis as we define it, the investigation guide is based mainly on pragmatic findings. It is drawn largely from the results of the analyses of a large number of accidents, incidents and crises, which make up a database. This knowledge base has been split into several generic organisational factors and associated markers that constitute useful background knowledge at the start of any analysis. Following the analysis of over twenty case studies and the analyses of accident reports, we came up with seven pathogenic organisational factors for the safety: production pressures, difficulty in implementing feedback experience, weakness of control bodies, shortcomings in the organisational culture of safety, failure in daily safety management, poor handling of organisational complexity, no re-examining of the design hypotheses (Pierlot et al., 2006). One has to note that these pathogenic factors are not fully independent and interact between each others (Dien and Llory, 2002a). The pathogenic organisational factors offered represent the formalisation of repetitive, recurrent or exemplary phenomena detected in the occurrence of multiple events. The list is not exhaustive, but can be used as a guide in investigations or inquiries.

Availability events are not as well documented and we did not have the opportunity to perform a large number of organisational analysis of availability events. As a result, we do not have yet the means to identify pathogenic organisational factors as we did for safety ones.

This is why at first, we suggest using the wide knowledge acquired within the framework of the organisational safety analysis to perform organisational availability factors.

We consider that it is reasonable to transpose to availability some of the safety organisational factors in the following way:

5.1. Difficulty of implementing feedback experience

The feedback experience comprises four steps: events detection, collection and analysis; corrective actions definition and implementation; evaluation of the efficiency of these actions; treatment memorization. As a result, the difficulty in implementing feedback experience concerns in the same time (Pierlot et al., 2006):

- the weaknesses of the feedback experience where the feedback process might be fully respected, but too few resources to work on it, or where, although still full respected, the feedback analysis results stay unknown for the organisation,
- the insufficiency of the feedback experience where only part of the feedback process is performed,
- the impossibility to solve the problems due to superficial corrective actions resulting from light analysis.

It is easily conceivable that *difficulty in implementing feedback experience* could be safety or availability related. The case study of a French nuclear power plant is very interesting from this point of view. We saw that one of the root causes of the event was that the feedback experience failed: not only this nuclear power plant had a near miss a few years before the event but also another plant already suffered the exact same event 1 year before the event (Dien and Hofseth, 2005). We conclude in first step that *difficulty in implementing feedback experience* is also a pathogenic organisational factor for availability, as for safety. And this is reinforced by the fact that the availability events collection and memorization is less developed and far more recent than for events related to safety.

5.2. Production pressures

Production pressures signal a situation in which production-related issues are predominant in the high-risk activity, to the detriment of safety-related activities (Pierlot et al., 2007). The production pressures are then seen as a rupture of the subtle equilibrium between safety and competitiveness, to the detriment of safety, because production-related issues are mostly feed by competitiveness concerns.

Even if it could be curious at first sight, it is our belief that *Production Pressures* could also apply for availability, and that, as the same manner that there is an equilibrium between safety and competitiveness, there is also an equilibrium between availability and competitiveness; between short-term availability and long term availability. Indeed, the failures of the 1999 NASA Mars missions (Mars Polar Lander and Marc Climate Orbiter) are mainly due to the implementation of the Faster, Better, Cheaper (FBC) program

(Montmayeul and Llory, 1999). The FBC program had for objectives to build smallest spaceships, to increase the flight numbers, to decrease the cycle time, to use new technologies so that the flight costs could be decreased, to accept minor risks if they are associated to an important gain expectancy, to implement well-known and secure management and engineering processes.

But in the end, this program resulted not only in a decrease in the safety, because of the minimizing of teams dedicated to safety (Dien and Llory, 2003), minimizing mainly obtained with the departure of experimented professionals (Montmayeul and Llory, 1999) but also in a general crisis among the teams: un-motivated teams, communication failures, risks being hide by sub-contractors ... (Montmayeul and Llory, 1999).

The way the FBC program was implemented at NASA resulted then in Production Pressures, to the detriment of safety (*Columbia* space shuttle accident in 2003), but also to the detriment of availability (six Mars mission failures upon 16).

We believe then that production pressures are a Pathogenic Organisational Factor for availability as for safety. The only difference is that, for safety, *Production Pressures* result in a rupture of the equilibrium between safety and competitiveness; while, for availability, *Production Pressures* result in a rupture of the equilibrium between availability and competitiveness.

5.3. Shortcomings in the organisational culture of availability

Shortcomings in the organisational culture of safety is a pathogenic organisational factor that refers to the definition of the safety culture by AIEA INSAG-4 (1991). Regarding the availability culture, there is no standardised definition. Nevertheless, as for safety, risk analysis for availability could be deficient, knowing that we are speaking of probabilistic or deterministic analysis. As for safety, the risks analysis (for availability) could be grounded on the past success and not on the current situation. As for safety, a good reliability level could be seen as a good availability level, even if the cut between reliability and availability is not may be as clear as the difference between reliability and safety. As for safety, there could be no comparison between the field practices and the written procedures. As for safety, there could be a blame culture instead of a root causes search culture. As for safety, there could be no attention paid to the whistler blowers ...

The Diane Vaughan's study about the Challenger space shuttle explosion (Vaughan, 1996) brings us a lot of information about the development of the accident during all the incubation period, according to the definition of Barry Turner (Turner and Pidgeon, 1997).

From an availability point of view, when NASA closes its eyes and considers that the effects of the failure of one O-ring could be downsized with the help of another-one, even though the design needed two complementary O-rings, it is a form of lack of availability culture. Why? Because, engineers and decision-makers consider each time, for each new launch, that it could work once more again.

Even if the organisational culture of safety has nothing to do with availability, it appears clearly that some of the field proofs of a deficiency of this organisational culture of safety could be considered for availability concerns. Culture of availability is clearly related to culture of production, with attention in housekeeping, maintenance, continuity of production, attention to weak signals of potential loosing of performance.

We believe then that, as far as there are potential shortcomings in the organisational culture of safety, they could be also potential shortcomings in the organisational culture of availability. But still, we believe that any availability organisational analysis should take a look at the "field proofs" mentioned above.

5.4. Poor handling of the organisational complexity

From the safety point of view, the organisational complexity deals with organisations operating rules which results in a complication of the daily work and of the decisions making processes on one hand, and, on the other hand, of communications routes dedicated to risks, hazards, threats and safety.

This poor handling could either generate a deficiency in organisational communication, where new elements important for work are not transmitted to the concerned persons; or generate a lack of coordination between the different services, departments of the organisation ...

A good example of the role of the organisational complexity is the Columbia shuttle accident (CAIB, 2003). In a very bureaucratic structure as NASA was, the informal structure itself called Debris Assessment Team and constituted by engineers from NASA and contractors had a lot of difficulties to be considered by the established structure. Whatever the issue to manage is, an availability one or a safety one, the organisational complexity and its resulting bureaucratic operating way prevent the organisation to be efficient out of the usual operating routes.

As such a poor handling could exist all over the organisation, it could have negative effects on availability.

5.5. No re-examining of design hypothesis

The design hypothesis of a socio-technical system give a vision of the future system operation. But, with time going on, these hypothesis could become inadequate to the real system operation or could be proved as false.

If the organisation is unable to treat such evolutions for the design hypothesis, it is a threat for safety (Pierlot et al., 2006). The fire in the Mont Blanc road tunnel (March 1999) could be a good illustration of some consequences of a no re-examining of design hypothesis on availability. Between 1965 and 1999, car traffic doubled and heavy truck traffic increased by a factor of 17. Nevertheless, the tunnel's surveillance and emergency equipment had not been updated. More, the signals asking drivers to respect the distance between vehicles had been reduced to such an extent that the tunnel had turned into a corridor of trucks which moved along bumper to bumper. Finally, after this dramatic fire, the tunnel was closed for about 2 years (Pierlot et al., 2006).

It is clear that the target to maintain a high level of performance implies the periodic re-examination of design hypothesis, in particular when the level of performances are increased.

5.6. Failure in daily availability management

The goal of the daily safety management is to obtain a good adequacy between the work to be performed and the knowledge of the people in charge of this work, to give an adapted training to people in charge, and to be sure that safety knowledge is transmitted to all the concerned persons all along their professional life, even for sub-contractors.

As there is a daily safety management, we believe that there should be also a daily availability management, which is related to the above mentioned points, but also to the spare part management linked to recovery issues, to the organisation management during critical phases for availability, to the overall knowledge management.

The former paragraphs show that an availability organisational analysis must focus not only of the occurrence of an availability event, but also on the recovery capacity of a given organisation after an availability event occurrence. Are there any other pathogenic factors for availability? There could be. Only real cases studies could confirm our thoughts.

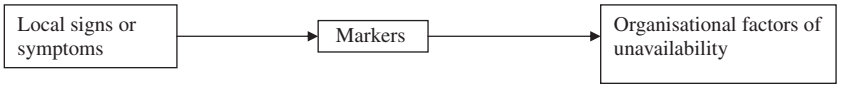

Fig. 3. From local signs to organisational factors.

The fact is that the pathogenic factors for availability seems to be very closed from the pathogenic factors for safety. Is it then possible to perform an availability organisational analysis without looking at safety issues? If it is possible, would not it be a threat for safety? These questions underline the difficult issue of the complex relationship between safety, availability and also reliability.

6. Conclusion

It appears clearly that the methods and the concepts developed within the framework of the safety organisational approach can be used for an availability and productive performances organisational approach. Transpositions are necessary, but they do not appear to present major difficulties.

One of the bases of the investigations concerning the organisational availability is made of a "system of indicators", built according what was done for safety as shown on Fig. 3.

With such a three levels system, the analyst can ground its field investigations and its analyses on knowledge resulting from the feedback experiment, either after a more or less serious incident of availability, or either for a diagnosis, related to availability, of the health of the concerned socio-technical system. These three levels correspond to different degrees of general information within the socio-technical system. In the *thick description*[2], required for the understanding of an incident or the health assessment of the socio-technical system, the three levels represent increasingly synthetic reference marks (when one passes from local signs to global factors of dysfunction).

However, the current status of investigation means as regards availability is less favourable than as regards safety. For availability and productive performances organisational studies, the background, the ground knowledge that we have for safety are not yet developed with the same details level for availability. A consequent effort should be made in particular:

- to build a detailed library of case studies of incidents being able to be used as reference,
- to develop a more systematic analysis of the availability,
- to develop methods or tools allowing to assess the severity of the availability incidents (as does the Probabilistic Safety Assessment for safety).

In parallel, some applied research must be undertaken to sustain the background knowledge related to local signs, markers and organisational factors, in order to increase the capacity for field analyses, and more generally, to increase our knowledge on the specific problems related to availability.

The use of the principles of the organisational analysis methods, however, was already carried out in a given number of cases: studies of availability incidents (Dien and Hofseth, 2005) and deep analyses of complex problems dealing with availability issues (studies on EDF nuclear power plants are currently in progress).

The results obtained prove the feasibility of such analyses and their interest: these analyses bring a better understanding, an improved explanation capacity of the complex phenomena that led to the events and, of course, as a result, larger fields of intervention (corrective actions). The organisational analysis increases then the knowledge on the availability issues (and of course also on safety issues) which are impacting complex systems.

In addition, the availability organisational analyses cannot be carried out without taking into account:

- the safety level reached and its evolution trends (factors of degradation of safety),
- the potential impacts of availability policy on safety.

The study of many cases of serious incidents and accidents shows that productive pressures, the noticeable production constraints increase, can have a catastrophic impact on the systems, generally in the medium or the long term. Obtaining (temporary) very good records of production level does not mean that the medium term performances (availability and safety) will be still ensured. This is of course true a fortiori in the long run.

The availability analysis must thus be particularly attentive to the equilibrium of the balance safety/availability which is always delicate to reach and sometimes fragile. Availability analyses cannot be based on passed successes, with the risk of disastrous disappointments. To some extent, effectiveness thresholds, production and work rate levels, high level performances, cannot be improved without caution: they could hide side effects which can deteriorate medium term availability and often simultaneously safety: equipment ageing, fatigue of employees or teams, organisational stress, tendency to by-pass controls, downsizing which prove to be prejudicial in the long term for availability and without any doubt for safety.

The increase of availability pressures, paradoxically, should lead to an increase in resources, at the same time to reinforce the availability itself – to satisfy the new requirements for availability – but also to guarantee balance with safety. It is simply possible that, in their quest for a better availability level, socio-technical complex systems reach quickly their own limits, which cannot be pushed further without avoiding a high level catastrophic event occurrence risk.

[2] Concerning "*thick description*" concept see (Geertz, 1998).

References

CAIB, 2003. Columbia Accident Investigation Board Report, vol. 1.
Dien, Y., 2006. The organizational factors of industrial accidents. In: Industrials Risks, Complexity, Uncertainties and Decision: an crossed approach. Tec & doc Editions, Lavoisier, France, pp. 133–173 (in French).
Dien, Y., Hofseth, C., 2005. Rise in temperature of the exciter of the alternator of a French NPP – an event embedded in the organization. EDF-R&D Internal Report. Clamart, France (in French).
Dien, Y., Llory, M., 2005. The accident of the cable car of the pic de Bure (France) of July 1, 1999. Analyze and First Synthesis, EDF/R&D Internal Report. Clamart, France (in French).
Dien, Y., Llory, M., 2002. Synthesis of results issued from the "event sentinel system". EDF/R&D Internal Report. Clamart, France (in French).
Dien, Y., Llory, M., 2002. The incident of the nuclear power plant of Davis-Besse. Analyze and first synthesis, EDF/R&D Internal Report. Clamart, France (in French).
Dien, Y., Llory, M., 2003. An organisational accident: the columbia shuttle. EDF-R&D Internal Report. Clamart, France (February 1).
Dien, Y., Llory, M., 2007. Practical method of the organizational analysis and diagnosis for the safety, EDF-R&D Internal Report. Clamart, France (in French).
Duval, C., Leger, A., Weber, P., Levrat, A., Lung, B., Farret, R., 2007. Choice of a risk analysis method for complex socio-technical system. In: Aven, T., Vinmen, J.E. (Eds.), Risk, Reliability and Societal Safety, vol. 1. University of Stavanger, Norway, pp. 17–25.
ESREDA Working Group on Accident Investigation, 2009. Guidelines for safety investigations of accidents. June.
Geertz, C., 1998. The thick description, The Description, vol. 1, Enquête, pp. 73–105 (in French).

INSAG-4, 1991. Safety series. The Safety Culture, 75-INSAG-4, AIEA, Vienne.
Llory, M, Dien, Y., 2007. The at-risk socio-technical systems: a needed distinction between availability and safety, Performances, vol. 30. France (in French, vol. 31, 2006, vol. 32, 2007).
Llory, M., Montmayeul, R., 2006. The organisations in question. In: Proceedings, First Seminar of Saint-André. France (in French).
Montmayeul, R., Llory, M., 1999. The failure of projects of NASA in 1999: ''Mars polar lander'' and ''Mars climate orbiter''. EDF-R&D Internal Report. Clamart, France (in French).
Pierlot, S., Llory, M., Dien, Y., 2006. Risk management between safety requirements and production pressures. In: Guedes Soares, C., Zio, E., (Eds.), Safety and Reliability for Managing Risk, vol. 2. pp. 1219–1226.
Pierlot, S., Dien, Y., Bourrier, M., 2006. Definition of the pathogenic organisational factors of the safety. EDF-R&D Internal Report. Clamart, France (in French).
Pierlot, S., Llory, M., Dien, Y., 2007. From organisational factors to an organizational diagnosis of the safety. In: Aven, T., Vinmen, J.E. (Eds.), Risk, Reliability and Societal Safety, vol. 2. University of Stavanger, Norway, pp. 1329–1335.
Turner, B.A., Pidgeon, N.F., 1997. Man-Made Disasters, Second ed. Butterworth Heinemann, Oxford, UK.
Vaughan, D., 1996. The Challenger Launch Decision. Risky Technology, Culture, and Deviance at NASA. The Chicago University Press, Chicago, USA.
Wiroth, P., 2006. Report of the General inspector for Nuclear Safety and Protection against radiation. EDF report. France (in French).