PERGAMON

Safety Science 41 (2003) 759–789

SAFETY SCIENCE

www.elsevier.com/locate/ssci

Safe design and human activity: construction of a theoretical framework from an analysis of a printing sector☆

Elie Fadier[a,*], Cecilia De La Garza[b], Armelle Didelot[c]

[a]*Institut National de Recherche et Sécurité, Département HT, service EPAP. Avenue de Bourgogne BP 27, 54501 Vandoeuvre cedex 1, France*

[b]*Laboratoire d'Ergonomie Informatique, Université Paris V, 45 rue des Saints-Pères, 75006 Paris, France*

[c]*LIGERON S.A., Les Algorithmes-Bâtiment Euclide, 91194 Saint-Aubin Cedex, France*

Abstract

Analysis of industrial situations on a day-to-day basis shows deviations between that which is foreseen (at the design stage), that which is integrated into and installed on the production site, and that which takes place during operation. These deviations reflected the differences between the task and the activity, which is standard and known in ergonomics, but also between the planned nominal technical operation and the real operation including different situation recovery events, faults and failures (technical, human, organisational, etc.). The result of this real operation then may seriously affect production performance. However, it has been observed that this performance is preserved to a greater or lesser extent by the adaptive and palliative interventions of the operators. In specific cases, these interventions appear as "boundary activities" from the point of view of both the system performance and safety, but are nevertheless tolerated during use. We therefore attempted to understand the origin and characteristics of these activities, as well as their benefits and associated risks in a context marked by different forms of tolerance. Two categories of boundary activities were identified involving actors from different hierarchical levels and decision units, and production operators. Their detailed analysis involves the identification of a set of "boundary conditions tolerated by use". As described by Rasmussen [Safety Science, 27(2–3), (1997) 183], these boundary conditions tolerated by use mark a migration of the system towards less safe levels, reduce the room for manoeuvre of the operators, and engender risks for the socio-technical system. Knowledge of these conditions and their classification in relation to the

☆ This work forms part of a project initiated by the "Prevention Integration through Design Group" of the French National Institute for Research and Safety (I.N.R.S.), and receives the support of the "Production Systems Program" (PROSPER) of the French Centre for Scientific Research (C.N.R.S.).

* Corresponding author.

E-mail addresses: fadier@inrs.fr (E. Fadier), garza@ergo-info.univ-paris5.fr (C. De La Garza), armelle.didelot@lligeron.com (A. Didelot).

0925-7535/03/$ - see front matter
doi:10.1016/S0925-7535(02)00022-X

boundary conditions tolerated by use stemming from the design and the internal boundary conditions tolerated by use of the firm should enable us to let these be taken into account by the designer so that they can be integrated, removed and/or accompanied by specific measures. Thus, consideration of boundary activities and boundary conditions tolerated by use during the design could allow the reference framework of the operational to be brought up to date. In addition, to be efficient, a prevention policy in a given company can benefit from the analysis of these phenomenons.

Keywords: Ergonomic analysis; Boundary activities tolerated during use; Fault tree analysis; Design; Safety; Boundary conditions tolerated by use; Risk management

1. Introduction

From a theoretical point of view, we started out from the global model of risk management proposed by Rasmussen (1997). The starting point for this author was the observation that the analysis of a number of industrial accidents and catastrophes (Bhopal, Flixborough, Zeebrugge, Chernobyl) highlights that the causes should not be sought in a combination of technical failures and human errors, but rather in a deviation of the global behaviour of the organisation under the influence of strong pressure towards efficiency in a highly competitive environment.

This being the case, it is necessary to take into consideration the interaction of the effects of the decisions taken at design level by several actors of the system in a normal work context, and in an organisational context such that: although each actor has a partial and correct view of the system, none has an entire representation of the system at any given time. In this context, and in the case where the entire system (and therefore the actors) is subjected to the pressure of a competitive environment, then according to Rasmussen, a natural migration towards acceptable limit performance is observed during operation, i.e. a deviation of activities towards limit thresholds beyond which it can be considered that performance and/or safety are no longer ensured.

The aim of this work was therefore to make this process of migration operational through the identification, characterisation and definition of all the determining factors of the activity of operating systems, which we shall term "boundary conditions tolerated by use" (Neboit et al., 1998; Fadier et al., 2001).

Compared to the original model, we have added an additional dimension: the life cycle of the installation. Indeed, our hypothesis is that, in terms of performance and safety, the limits are partially defined during design but that they vary and evolve during installation and are again redefined during operation (Fig. 1).

The originality of the GIPC project and this work resides in the fact that it jointly takes into account the boundary conditions tolerated by use tolerated by use and the diachronic dimension of their evolution.

This article is based on the analysis of the design activity undertaken in a manufacturer of web presses and on the analysis of work situations in printing shop that use this type of equipment (Appendix). The paper is also based on the hypothesis

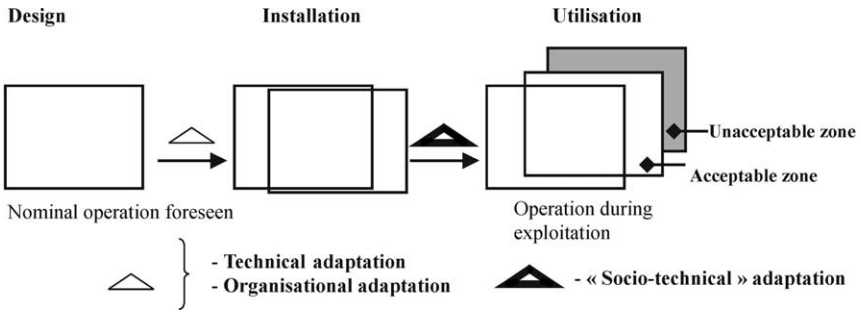


Fig. 1. Evolution of the deviations from nominal with the life of the system.

according to which safety and prevention concern not only the operators of the installation but also involve the process which emerges well upstream (Reason, 1990, 1995; Rasmussen, 1997; Fadier, 1998; Didelot et al., 1999; De la Garza, 1999, 2000). This is why, from a methodological point of view, we took on a systemic perspective and adopted a bottom-up approach. In this respect, we started out from the analysis of different operating situations in order to identify, on the basis of the human–machine interactions, the difficulties and the risks (nature, origin, etc.) encountered in the work as well as how they are managed by the operators. This analysis revealed the existence of the palliative activities adopted by the operators to cope with various situation recovery activities and work requirements. These activities, called boundary activities tolerated during use (Fadier et al., 2001), will be described in this paper, as will their links with the boundary conditions tolerated by use.

From a practical point of view, the identification of these boundary activities should lead to preventive actions by starting from operation and moving up through the different hierarchical levels and decision making centres as far as the design of work equipment, as shown in Fig. 2.

The relations and inter-relations which characterise the different phases of management, design and organisation of a work process are illustrated in this figure. The first choices in terms of safety are beyond the scope of the firm as they fall within

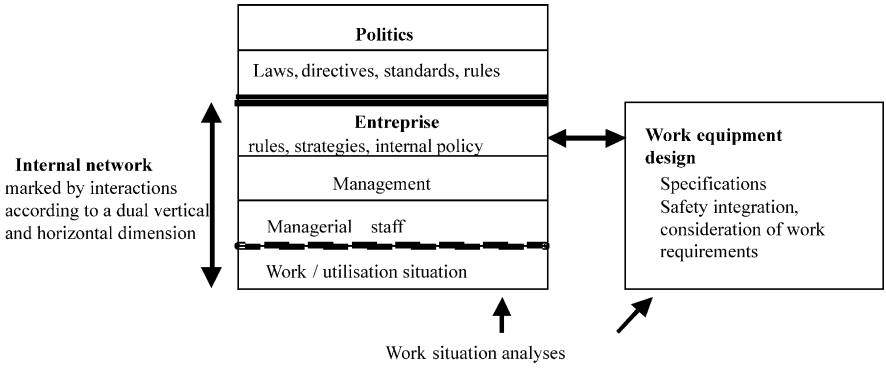


Fig. 2. Diagram of the different actors involved in safety during the phases of a work process.

government policy (laws, decrees, standards, directives). Then, within the firm other choices are made in relation to the design and installation of the work equipment, management of human resources (training, hiring, career progress, etc.), organisation of production, maintenance, quality, safety, etc. In this complex framework, our search seeks to show how the specifications of designers can be improved as regards safety.

The construction of the article follows the diagrammatic form of Fig. 2 starting from the bottom. The boundary activities tolerated during Use are presented first and are illustrated by work situations in the printing sector. These activities then lead us to the analysis of the Boundary conditions tolerated by use tolerated by Use, and to the level of management and design of equipment in the second part. In the third part, we will show the links between boundary activities and boundary conditions tolerated by use, and explore new areas of safety and design.

2. Boundary activities tolerated during use: a necessity given work constraints and requirements

From a methodological point of view, the field study was based on the methodology for analysing reliability and operational ergonomics (MAFERGO, Fadier et al., 1991), the operational objective of which is to improve the reliability and safety of socio-technical systems by seeking to reduce the probability of malfunctions of technical systems and/or the Human/System pair. The principle of this methodology is to study operational reliability in order to propose the adaptations necessary for redesigning the system. A distinctive feature is that it combines ergonomic and reliability analyses at every stage, until now used in an isolated and contradictory way. It is applied by a top-down approach to problems in order to locate and then analyse in an increasingly precise way the malfunctions in systemic terms by combining ergonomic techniques[1] and analyses of reliability.[2] We observed the different operating teams on two sites for some 30 days to identify the real modes of managing work situations and their difficulties, as well as the associated risks.

2.1. Analysis of usual operation and identification of palliative activities

The analysis of the usual, i.e. day-to-day, operation of a modern industrial system (offset printing line) with a high degree of automation showed that the role of the human activities established by the actors to ensure and maintain expected performance remains considerable. This result confirms the observation which have been established for several years concerning the paradox of automation. Automated systems are required to be more reliable and without human intervention, however

[1] Analysis of work activity, semi-directed interviews with different members of staff: production operators, supervisors, maintenance, safety and production managers, designers; analysis of documents: accident reports, production data sheets, maintenance data sheets, daily production files.

[2] Structuro-functional analysis, event tree analysis, analysis of failure modes and their effects and criticality, fault tree analysis.

they are still controlled by human operators. To a certain extent these systems can turn out to be less reliable when the automation makes them less accessible and introduces new risks (Bainbridge, 1982; Neboit, 1989; Vandaele; 1993; Fadier, 2001). Hence, to deal with work requirements, the operators develop working procedures through the construction of knowledge about the operation of equipment, task appropriation, adaptation of tools and procedures to the work situation, while taking in to account work requirements and constraints. It can be considered that this entails operational responses to:

- deviations that emerge between the design of a standard technical system and its adaptation accompanied by the designer for a given user;
- deviations reinforced by others adaptations coming from the installation of the system on site then during its operation;
- technical, functional and/or safety solutions which are inappropriate to and/or hinder the daily use of the system;
- production, quality or time constraints; and
- technical incident or failure situations requiring recovery activities.

However, in specific conditions, these operating modes appear as palliative activities to maintain the performance of the system, sometimes to the detriment of the health and safety of the operators as their primary objective is the optimisation of the system. In addition, they are the result of a compromise faced with managing various system constraints and "operating deviations" in the process characterising a migration towards tolerance limit thresholds from the performance and safety points of view. They are constructed and adapted by the organisation using the system (evolution of the Human-Task system) and evolve with the environment and with time. They therefore have a dynamic character that, depending on the situation, can tend towards a reduction in uncertainty by increasing the room for manoeuvre of the operators or, they may lead to increase in uncertainty by reducing the room for manoeuvre of the operators. By uncertainty here we mean the possibility of controlling the situation (anticipation, diagnosis, actions, dynamic aspect of the situation) or of losing control of it. Uncertainty evolves in any given situation and is partly linked to the room for manoeuvre of the operators. Indeed, the latter refers to the span of initiative and the span of tolerance that operators actually have to regulate the operation of the Human–Machine system (Weill-Fassina and Valot, 1997). Room for manoeuvre depends on the rules, the instructions and means given to the operators, their skills, and the effective characteristics of the situation. Analysis of the regulation of the process of social action shows the difference between two possibilities of room for manoeuvre: autonomy and discretion (De la Garza et al., 1999b).

Autonomy concerns "the degree of freedom of decision that individual or collective actors seek to construct or assert" in a system regulated from the exterior; "this means the capacity to produce their own rules and to manage their own processes of action" (Maggi, 1996). In the process of work, it indicates a capacity of influence on the organisation of production and the assertion of a certain *independence* as regards

the hierarchy. It results from employing skills that are not necessarily recognised by the management, but the practices are implicitly accepted as long as the desired results are achieved (de Terssac, 1992). We shall see in the remainder of this article that this implicit acceptance is far from innocuous and promotes the tolerance of the use of these palliative activities, which is not necessarily without risk for the system. In contrast, *discretion* "indicates room for action in a regulated process where the operator carrying out the task is obliged to decide and choose within a framework of *dependence*" (Maggi, 1996). In the work process, it is *bestowed* on the operator, it is a delegation by the management to deal with either an incompleteness of or a difficulty in defining the procedures. Exercising discretion can have either advantages or drawbacks for the operator depending on the framework of the *possibilities* and the *means* left by the organisational choices to fulfil this discretion. The process of autonomy and discretion marks the palliative activities observed in the printing company insofar as, on the one hand, they refer to specific skills and to individual and collective modes of managing the situation at hand (Didelot et al., 1999; De la Garza, 2000). On the other hand, cases exist where the operators are obliged to take a decision and initiatives to deal with a situation unforeseen either from the design point of view or from the internal organisation point of view. In both cases, account taken of the fact that this involves boundary activities with respect to the safety of the system, the choices made by those involved in the work situation may lead to an incident or accident. Indeed, these activities are at the limit as they refer to means of partial compensation engendering risks for the performance and safety of the human–machine system. This is the specific character that distinguishes them from other work activities and from other notions as human error, violation or normal deviance (De la Garza and Fadier, 2002; Vaughan, 1996).

From the risk prevention point of view, these activities are therefore interesting insofar as they allow identification of the difficulties and the dysfunctions in the situations studied in relation to the human–machine interactions in the real use of the equipment. They translate the characteristic accident or incident producing circumstances of the system studied.

These activities are observable during the analysis of a situation as they are translated by the concrete actions of those involved in the work. We shall see that it was possible to observe these types of activities stemming directly from the basic operators as we closely monitored day-to-day operation. However, for the boundary activities involving actors of other hierarchical levels and decision centres, what we observed in the field were the choices made upstream and their consequences on the work conditions of the operators downstream.

2.2. Boundary activities as the result of partial means of compensation

Schematically, these palliative and boundary activities result, according to the circumstances:

- from an acceptance of the fact that the initiating conditions are such that the operator has no alternative;

- from a compromise between the production/safety pair;
- from a slow migration of daily deviations which have been applied to satisfy the real constraints of the situation (operational); and
- from the necessity of immediate management of an exceptional situation.

The framework of the construction and application of these boundary activities is generally situated outside that laid down, and can not only overcome the inherent shortcomings of the rules, but also breach the safety barriers (Hollnagel, 1999; Polet et al., 2000) established by the designer and/or the organisation. They are characterised by the search for a trade-off between production, safety and quality. At first sight, "conscious risk taking" on the part of the operator can be assumed (in other words in the knowledge that it is dangerous). However, it involves boundary activities countered by a positive construction of a space/time of safety within which the operator considers that he is protected. Indeed, the operators construct recovery skills and strategies allowing them to establish partial means of compensation. To a certain degree this means the reconstruction of rules which consists, depending on the case, in adjustments, adaptations, transformations or non-application of the rules. These rules are linked to work requirements or to the perturbations that can appear during the activity (De la Garza et al., 1999a). On the one hand, we can distinguish, depending on the rules laid down and the situation, impromptu reconstruction carried out in an improvised way in the field, and without preparation to cope with an incident or an unexpected constraint. Ordinary reconstruction, on the other, is routinely employed according to the work rules and constructed with the experience gained in similar situations encountered more or less frequently. The first have an *exceptional* character and generally the operators involved are less at ease than in the case of the second. However, if the incident in question occurs from time to time, this impromptu reconstruction tends to become ordinary. Thus, in ordinary reconstruction, that which is *usual* can be distinguished from that which occurs *sometimes*. For example, every day at a given time, the rollers are cleaned with a "ball" of cloth when the equipment is still in operation to ensure print quality while avoiding any waste of paper, loss of time and machine stoppage. In contrast, from time to time, the production team changes a belt which breaks inside the folding machine whereas this should normally be carried out by maintenance staff.

From the point of view of the regulation of the process of action, this reconstruction corresponds to applying rules laid down by a specific actor or by a group of actors which are different from those coming from the upper hierarchical levels or other decision centres, particularly the design office. This reconstruction can be prior to the action or intrinsic during the action itself. In every case, it bears witness to the operator taking autonomy. Depending on the rules and instructions laid down it manifests in the operator exercising discretion or in the infringement of an imposition. This reconstruction of the rules can be situated at different hierarchical levels and therefore involve both the operators of the installation and management personnel.

From a cognitive point of view, this reconstruction involves diagnoses of situations and targeted decisional processes, either towards modulation of the prescribed

rules integrated into the activity or towards the elaboration of an opportunist strategy which requires adaptation to each new situation.

From the point of view of the reliability of the human–machine system, the efficiency or the failure of this reconstruction depends on the interactions between the different modes of compensation, the choices concerning the reconstruction of the rules, and the circumstances in which the activity is being carried out (De la Garza et al., 1999a).

However, the reconstruction of the rules, analysed here as palliative activities, are limit from the point of view of system performance and the safety of the personnel as they result from the compromise established by the different actors, who seek to integrate production requirements, quality, safety, technical and human resources, condition of the equipment, etc. These compromises are therefore the result of qualitative weighting on the part of the operators in relation to the room for manoeuvre that they have (Weill-Fassina and Valot, 1997) and, although they seek to "manage the risk", they nevertheless weaken the socio-technical system. As a result, these operating modes, analysed as boundary activities, can get out of hand and engender risks related to the reliability of the system and/or the health and safety of the operators.

2.3. Tolerance during use of boundary activities or lack of knowledge of their existence?

We started out from the principle that the existence over time of these boundary activities is tolerated during use. The following section attempts to highlight the reality of a framework of tolerance. Based on the results of our field analyses, three axes around the concept of "tolerance" appeared relevant to analyse. A main axis marked by a collective dimension, as tolerance involves different work actors. Two other axes which link up with the first, and which appear as conditions necessary for this collective tolerance: individual tolerance and the robustness of the system

2.3.1. A "collective" tolerance

From the point of view of this "collective" tolerance, it can be considered that boundary activities are tolerated during use as they are in keeping with production. Indeed, the ultimate objective, even implicit, of these activities is to maintain an acceptable level of performance allowing optimisation of operation. This optimisation manifests itself in the longer or shorter term by, for example:

- maintenance of the availability of production (limitation of production losses) and, in parallel, a reduction in the time of unavailability;
- limitation of consumables and, in parallel, of preventative maintenance intervention time;
- time saved in the execution of a task; and
- a reduction in costs relative to training, maintenance and the brief reduction in the size of teams.

Tolerance is used in this case as an acceptance of these practices in the firm. As a result, it implies knowledge of the existence of these practices by the actors who allow them. Our analyses revealed different examples of this.

- There is a tolerance within the teams of production practising these boundary activities. This in no way means the direct involvement of all the operators. In addition, it emerged that team leaders or their deputies [the chief or second operator (i.e. foreman and second foreman] carried out most of these activities observed. As explained earlier, these boundary activities require the construction of knowledge, techniques and know-how that demonstrate the skills of the operator. This tolerance stems from the fact that the operators consider that they have no alternative, which may be true in certain cases. However, in others, this tolerance stems from the fact that these boundary activities are more efficient than the procedures laid down and are generally accompanied by benefits such as the considerable amount of time saved.
- From the point of view of the management, certain of these boundary activities are not always known. In this case, one cannot speak of tolerance. In contrast, other activities are not only known but also tolerated. This tolerance is then tacit and can be considered ''passive'' (the management do not formally recognise them). The management ''turns a blind eye'' either because it avoids another solution being found while still expecting the system to produce or because these activities respond to what has been described in the documentation as implicit obligations, in other words tasks implicitly laid down but not written or said in an explicit way but nevertheless ''expected'' (Chabaud, 1990). This corresponds to production obligations (e.g. to finish a print run on time, particularly when it involves an important customer and regardless of the conditions). This tolerance is therefore not an individual process and can involve actors of different decision centres and hierarchical levels.
- This tolerance also directly commits managers when the boundary activities come from hierarchical levels or decision centres upstream of the work activity. In this case, the management lays down ''new procedures''. The tolerance stemming from this instruction is then explicit (termed active). In this respect, the management provides certain resources to the operators to accomplish specific activities. Put another way, the ''producer'' actors of boundary activities are also actors of the production, maintenance, managerial staff or management. The same type of phenomenon has been demonstrated and described in relation to, for example, latent failures (Reason, 1990) or the highlighting of a functional network within a firm where the ''producers of errors'' can be located at different hierarchical levels and decision centres (De la Garza, 1999). Indeed, safety can concern not only basic operators.

2.3.2. Two conditions necessary for tolerance: individual tolerance and tolerance of the technical system

Although our analysis is primarily centred on global and collective tolerance, two other axes relative to individual and technical tolerance should be considered.

Firstly, individual tolerance refers to the possibilities of adaptation of operators according to their knowledge of the system, their skills, know-how and functional state (tiredness, age, health) in interaction with the characteristics of the situation and the effective means at their disposal (rules, procedures, state of the equipment, organisation of the teams, training). This capacity to adapt manifests through the modes of compensation and/or the recovery procedures employed, by changes in the management and comprehension of situations, as well as by transformations of the environment. This tolerance has an impact on the modes of anticipation, diagnosis and effective control of the situation and depends greatly on the possible room for manoeuvre of the operators in the situation at hand and in its evolution. Put another way, this tolerance is closely related to their autonomy and the possibilities of exercising their discretion in work conditions that are acceptable to a greater or lesser extent. Besides, this individual tolerance can engender short-term benefits for the system (situation recovery, attainment of the production target, etc.), and shorter or longer-term risks for those involved in the work (occupational diseases, stress, fatigue, accident).

Secondly, tolerance of the technical system is probably that most often studied, and is defined in relation to the robustness of the technical system (Hollnagel, 1991). In this specific case, the robustness of the system is its capacity to carry out a particular function in environmental conditions for which it was not designed or which it cannot withstand: i.e. beyond the boundary conditions tolerated by use of use''. Thus, this robustness may be put to the test when the operators act in accordance with limit modes of operation beyond that laid down. However, it can also be put to the test when certain conditions of use do not respect the criteria established by the designer, for example, the raw material used (quality of paper or ink) or when the maintenance cycles decided by the company exceed the recommended date. This tolerance presents short-term benefits (no stoppage of the machine, avoidance of losses, reduction in economic costs). Nevertheless, this technical tolerance also involves the associated risks, in particular as regards the reliability of the installation. Indeed, the tolerance of the technical system is dynamic (reduces with the time of limit operation) and hence, in the longer or shorter term, these different practices can promote a migration of the equipment towards limit thresholds from the point of view of reliability, and even an incident (failure, dysfunction, breakage of a component).

These three axes of tolerance occur in daily work and guarantee, in relation to the boundary activities tolerated during use, an acceptable operational reliability of the socio-technical system.

In conclusion, most of these boundary activities are merely ''tolerated'', but cannot be integrated as written rules or procedures or accepted explicitly in the company. Indeed, they are the result of the constructions of the actors of work, appearing as partial means of compensation engendering both immediate benefits and associated risks for the health or safety of the operators in relation to the different compromises established. Hence the term adopted in the remainder of this article: Boundary Activities Tolerated during Use (BATU). The immediate benefits can be of a different nature depending on the actors involved in the boundary

activities of the work situation at hand, as can the risks. And besides, although this tolerance gives a certain flexibility to the system (benefit: upkeep of acceptable performance), daily boundary activities can promote migration of the system towards limit boundaries, thus underlining their paradoxes. In this respect, both to better understand BATU and to better target prevention and design actions, we have distinguished two types of BATU which are presented in what follows.

3. Two types of BATU according to the level of analysis of the work process

Categorisation of BATU turns out to be necessary according to the different phases of a work process, the actors involved and, as a result, according to the field of action, in particular in terms of feedback towards the design of work equipment. Indeed, the set of boundary activities appears in relation to the constraints and the deviations of the work situation, creating fragile environments from the point of view of safety and system performance.

However, these constraints can be located in or be characteristic of different phases and/or hierarchical levels or again primarily concern certain decision centres more than others (Fig. 2). The actors involved can also be both production operators and members of the management team. Thus, two types of BATU were differentiated, namely operational BATU and managerial BATU, the consequences of which may not have the same impact on safety and the performance of the "human–machine" system. In what follows we give the characteristics and specific features of each of these categories as well as a few illustrations, and we shall see that the fields of action in terms of prevention are not the same.

3.1. Operational BATU

This type of BATU refers to practices primarily oriented towards an improvement in productivity and the achievement of production targets in relation to production constraints, quality and safety. They result from the interaction between the work environment and the characteristics of the operators (Fig. 3). Operational BATU primarily concern those involved in work production and they can require the intervention of several operators and, consequently, the establishment of processes of cooperation, prior or contextual coordination, collaboration or mutual assistance between the members of the team (De la Garza and Weill-Fassina, 2000). These forms of collective interactions are constructed with experience and appear as strategies to deal with different work requirements, even with the ambiguities or incompatibility coming, for example, from the choice of technical design or the choices made when drafting the user's manual (De la Garza, 2000). These forms of interaction also bear witness to autonomy taking on the part of those involved in the work and are the guarantors of the success of the BATU. Within the teams, these BATU, like the work activity, require the construction and sharing of a common operating reference system (de Terssac and Chabaud, 1990), and the construction of the know-how of prudence (Cru, 1995), which allow a

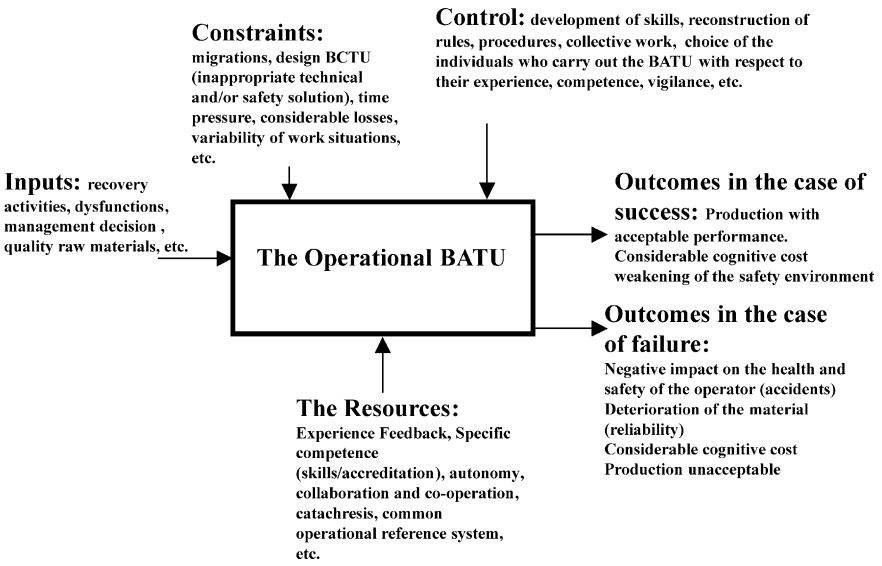


Fig. 3. Actigram, according to the SADT formalism, representing the operational BATU.

more or less efficient reaction to day-to-day work situations and situation recovery activities.

The main objective remains linked to productivity. In this respect, Didelot and Fadier (2001) constructed a Fault Tree having as its peak: the stoppage of production due to a technical incident on a web press. On the one hand, this analysis allowed evaluation of the fragility of the system (a minimum of 327 cut sets, 76% of which were of order 1) and, on the other, justification of the role and place of operational BATU as "barriers" blocking certain cut sets thereby reducing the frequency of stoppage of production due to incidents. Given that the system does not appear to stop as often in relation to the diversity and the number of recovery activities which make up the tree, certain BATUs therefore function as barriers to these incidents on the system in operation. However, when stoppage cannot be avoided, other BATU reduce this stoppage time. We have qualified these events operational BATU, linked to operation.

The following extract (Fig. 4) of the fault tree indeed shows the location of these barriers.

Although the main objective is linked to productivity, safety nevertheless remains a concern insofar as the operator gradually establishes and controls "second degree" safety procedures. However, as pointed out earlier, these practices can engender risks for the human–machine system if they exceed the limits of tolerance of the system.

In this respect, a logic tree analysis based on the analyses of the activities of a particular work situation (particular BATU) highlighted the different conditions of failure and their combinations (exceeding the threshold of limits accepted by the system) and then the different consequences of these failures (Didelot, 2001).

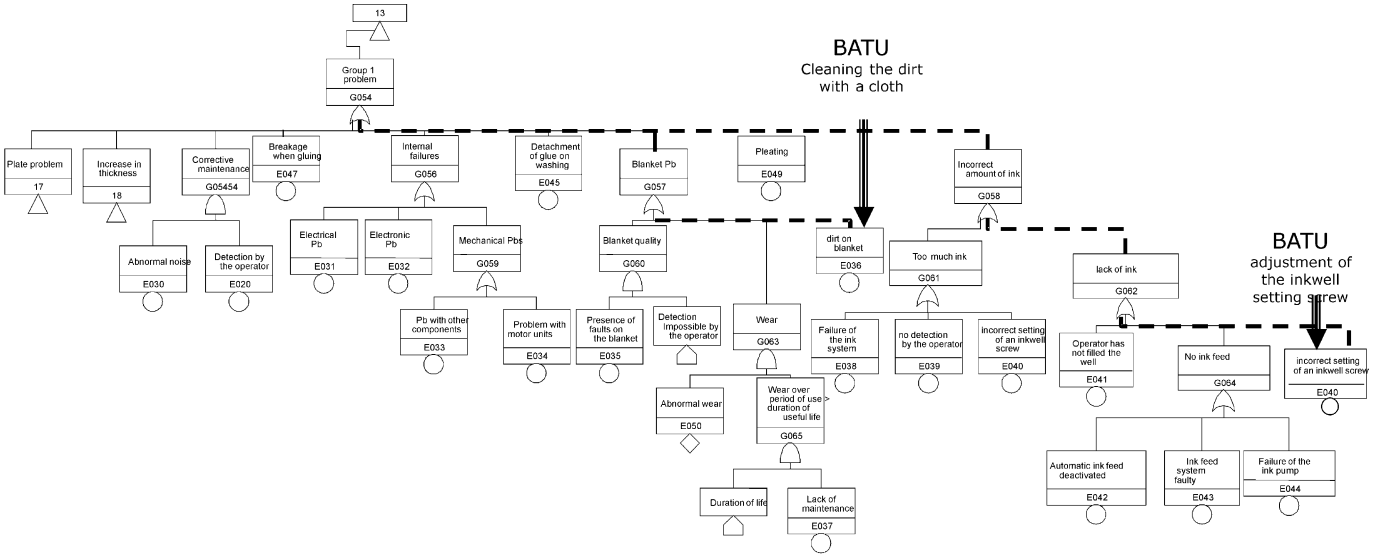


Fig. 4. Extract of the fault tree showing the contribution of operational BATU to the improvement of the availability of an industrial web press (according to Didelot and Fadier, 2001).

Several characteristics were identified that allow these types of activities to be explained and understood. These attributes can be considered in isolation or in combination.

BATU carried out with or without defeating a safety device: the execution of these activities is in relation to the safety devices installed by the designer. When an opposition exists between the work requirements and the application by the manufacturer of standards relative to machine safety (EN 292; EN 614; EN 1010), the operators often tend to defeat these devices to be able to work. In contrast, in other cases, the operators have room for manoeuvre which allows them to act with precaution on the system while it is in operation without defeating the safety device.

BATU carried out by obligation or in the interests of comfort: it is an obligation when the operators find it impossible to carry out the manipulation while respecting the instructions. In contrast, it is in the interests of comfort when the manipulation can be carried out while respecting questions relative to protection

BATU carried out during operation of the system or when it is stopped: this activity is carried out during operation of the system with the aim of continuing production without stopping the machines. In contrast, the reduction in system unavailability time remains the objective of the BATU carried out during failure of the system.

However, the particularity of these situations lies in the fact that they are initiated exclusively by the operators who find themselves facing an operational situation, either known or not, in which they must react as quickly as possible.

For example, during a "paper break" or "jam" type incident, the foreman and his assistant rush (common) to stop the machine as quickly as possible; in the configuration observed, i.e. a two-stage line, there were numerous and narrow stairways with steep and irregular steps. The benefit of this type of BATU is to limit losses, but it does engender various risks: risk of same-level falls (which is a source of accident known in the printing sector) and a risk of increased fatigue. Furthermore, this line only functions with young teams (between 27 and 38 years old) with the exception of one 52-year-old operator. The operators themselves say: "you have to be young to keep up with the rate of this line". Here, a probable migration can be anticipated in relation to individual tolerance as, with ageing of the population, these operating modes become more difficult to apply.

A second example concerns cleaning the blankets[3] although the line is still in operation. This cleaning is carried out when the chief or second operator observes repeated print faults on the booklets at the output of the machine. This fault generally comes from dirt building up on a blanket of one of the units. Once the blanket causing this fault has been identified, the operators intervene directly on it (not

[3] A blanket is a cylinder composed of a rubber sheet allowing transfer of the pattern/prints of the metal printing plate to the paper (intermediate support).

however being sure of the solution: a process of trial and error), without stopping production, by manually wiping it with a cloth to remove the dirt.

This intervention is carried out with a know-how of prudence regarding the way the cloth is held (in a tight ball, fingers retracted), thus ensuring that the fingers are protected and that the cloth is not swallowed up by the rollers; if this does occur it is in principle the cloth that goes first, triggering stoppage of the machines and reducing the consequences for the hand of the operator. Nevertheless, the recommended procedure in this type of situation is to trigger automatic washing during operation. This operation leads to a loss of paper and productivity. In addition, if the fault persists, the line must be stopped to carry out this operation in total safety, as the risk of crushing exists. This also leads to a loss of productivity.

It can indeed be seen that the BATU induce consequences that are primarily characterised by the limitation of production losses, but also by a possible loss of safety/health. This vision appears to us plausible in the short term. In contrast, the analysis of its projection to the medium and long-term seems to limit the expected effects, and even introduce reverse/harmful effects (risk of ''losses''):

- Although the BATU induce a sentiment of reduction in uncertainty through the establishment of the means of compensation, this sentiment may in reality turn out to be inappropriate, even erroneous in terms of the safety level of the different work situations. This phenomenon is explained to a great extent by the fact that it involves partial means of compensation, which do not necessarily cover all the risks and which could be difficult to update given the evolution and dynamic nature of the work situation.
- On account of a continuous migration towards thresholds of tolerance limits with respect to the performance and safety of the system, a deterioration of the reliability of the tool may be observed over time.

3.2. Managerial BATU

Managerial BATU come from a management decision, and are therefore independent of the operating dynamic of the system (in contrast to operators who take decisions directly linked to this dynamic), but which have a direct impact on it.

These BATU are essentially oriented towards a reduction in costs in relation to economic and management constraints.

They concern management staff at different hierarchical levels and decision centres. In this respect, they refer to the concept of ''latent failure'' defined by Reason (1990) or to ''organisational error'' (Reason, 1995; Baram, 1995).

As regards the characteristics of BATU, we considered that the decisions taken primarily concern two broad and highly interactive dimensions, namely human and technical, and are expressed through:

- Management of human resources; for example, in terms of team organisation we observed (1) the partial means of compensation faced with a lack of

personnel within a team, as nothing had been foreseen to overcome the absence of an operator and (2) on-the-job training practices faced with the absence of training of certain operators.

- Maintenance management; for example, the non-respect of preventative maintenance cycles, and minimum or even no preventative maintenance were observed, which can be translated by an increase in corrective maintenance and, in the longer term, an increase in stoppage time of the machines.
- Management of the safety of work equipment; for example, defeating of a safety device intended to protect the operators but which turns out to be incompatible with production requirements (paradoxical safety situation) was observed.

The immediate benefits of these BATU are primarily linked to a reduction in economic costs. However, the indirect fallout of these BATU concerns the activity of the operators as they imply, in certain cases, a redistribution of assignments within the team in the case of a reduction in manpower. In other cases, they involve a permanent adjustment/resetting of components to overcome the lack and/or absence of preventative maintenance.

Indeed, this type of BATU appears upstream of the work activity and therefore partly determines the work conditions of the basic operators. We shall see in the following section that these BATU act as internal boundary conditions tolerated by use of the firm and promote the appearance of operational BATU during production.

As for operational BATU, managerial BATU are partial means of compensation. They are also compromises on the part of certain actors. In the medium and long term, the final fallout of these BATU can translate, for example, by a deterioration in skills, premature ageing of the system and a loss of the system and reference model. Indeed, in the long term and alongside the deterioration in skills and maintenance policy, the system transforms into a system comprising a set of procedural and material deviations. In this perspective, the notion of managerial BATU can come closer of the notion of normal deviance defined by Vaughan (1996). However, this author puts the accent on the organisational dysfunction and do not integrate cognitive process analysis in relation with recovery actions. The results stemming from this migration of the system should be evaluated not only in terms of benefits but also in terms of deficit with respect to the reference system (Didelot et al., 1999). This latter point should furthermore allow us to orient plausible and desirable areas of action from the point of view of design.

Table 1 summarises a few properties of the two classes of BATU as well as their dependence. This table provides a comparison of the two classes of BATU that takes into consideration the initiator, the expected effects and their possible consequences in terms of benefits and/or risks.

In conclusion, these two types of boundary activities tolerated during use are even more interesting as they highlight the existence of a functional network involved in the reliability of the socio-functional system (De la Garza, 1999). This observation will lead to showing that aspects of safety and risk prevention concern not only the operators of the installation and, in parallel, that everything cannot be resolved

Table 1
Summary of the main characteristics of the two types of BATU

Type: BATU	Initiators	Expected effects benefits/risks	Possible consequences benefits/risks	Characteristics
Operational	Operators	Reduction in unavailability time Maintenance of the availability of system assignment Weakening of safety level	Limitation of losses Risk of incident and/or accident	In operation/when stopped Individual/collective Comfort/Obligation With/without defeating of a safety device
Managerial	Management	Reduction in costs: At a human level, this concerns manpower and training At a technical level, this can concern the defeating of equipment, changing the preventative maintenance cycle and sometimes the total absence of this type of maintenance	Operational BATU: Restructuring of teams and activities On-the-job training leading to a deterioration of skills Hindrances to work and risk taking by those on site Deterioration of equipment in the medium and long term	Outside the operational dynamic With and/or without dialogue with the designer With and/or without dialogue with the personnel Implicit/explicit

exclusively by way of design as the equipment and the operators form part of an organisation. We shall see in the following section how the analysis of boundary conditions tolerated by use tolerated by use is a means of accessing the sources of BATU, and therefore of acting.

4. The boundary conditions tolerated by use: "witnesses" of the migration of the socio-technical system

The analysis and comprehension of BATU led us, in our "bottom-up" approach to identifying and analysing the source phenomena and elements of these BATU, which we have termed the Boundary Conditions Tolerated by Use (BCTU). In what follows, we shall define these BCTU and identify a typology from them which allows specific areas of prevention activity to be envisaged.

4.1. Definition

The word "conditions" has not been chosen haphazardly in that it refers to "a situation", "a state", "external circumstances to which people or entities are subjected, and/or circumstances to which the accomplishment of an action may be subordinate", to take the definition of the Petit Larousse (1998). It should be borne in mind that we started out from the model of Rasmussen (1997) which highlights the existence of multiple constraints that can cause a migration of certain parameters towards borderline limit areas from the point of view of the performance and safety of the system.

In this perspective, the Boundary Conditions Tolerated by Use (BCTU) are a set of factors and elements (environmental, material, human, production) of the work situation which, by their very existence and their interactions lead to or create particular circumstances. These circumstances are caused by the operational dynamic. They promote the migration of the system towards zones that are unsafe to varying degrees and increase the uncertainty in the work system by reducing the room for manoeuvre of the operators. Consequently, these boundary conditions tolerated by use, which partly determine the real work conditions, are likely to engender risks for the work system (H–M).

System migration could not be observed over the short study periods in the different locations, but the existence of BCTU bears witness to a possible migration towards the limit thresholds.

In contrast to BATU, BCTU cannot be observed directly in the field; they can (however) be inferred by the actions of the operators and the choices of the various actors of the work. The ultimate aim of BCTU, even implicit, can at the end of the day be translated by the optimisation of financial investment. BCTU are accepted, then suffered in a manner of speaking by the user organisation, and promote the appearance and tolerance of boundary activities such as those described previously. The analysis of BCTU requires going up the different hierarchical levels even as far as the design to clearly identify the origins (Fig. 5). Put another way, it involves

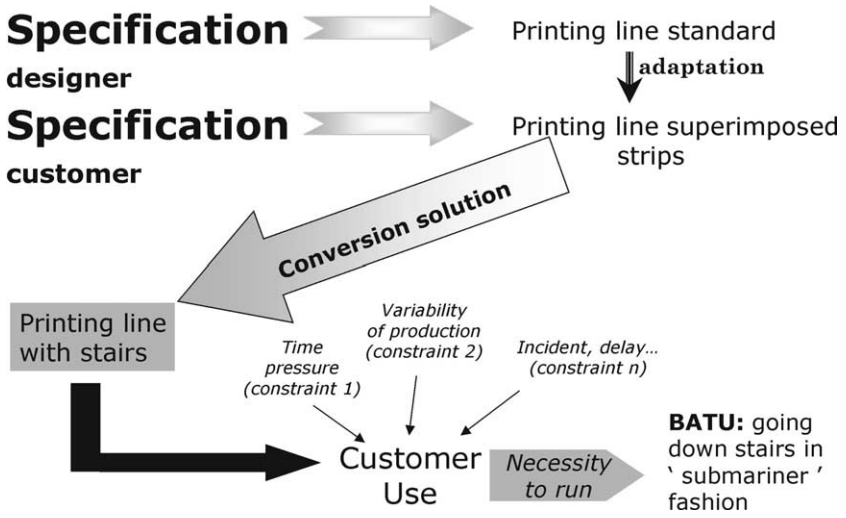


Fig. 5. Example showing the system reaction in the form of BATU faced with various constraints and deviations in a printing line.

"reconstructing" the history of certain choices and certain decisions (BCTU). Hence, we distinguished two types of BCTU, according to the design phases of a global work process.

4.2. Typology of BCTU according to the design phases of a work process

Two classes of BCTU were therefore distinguished in relation to the methodological aspects described earlier:

- internal BCTU which emerge from different hierarchical levels and decision centres;
- external BCTU whose origin lies in the design.

Their emergence does not have the same origins and, as a result, the action mechanisms are not of the same nature and do not concern the same actors. In certain cases, causal links can be highlighted between these two families of BCTU. From the safety point of view, it is then important to analyse these links and to couple the typology of the deviations with these two families.

From the point of view of internal BCTU, it would appear that they refer to the global conception of work situations in relation to the policy of the company. This does not fall with the scope of equipment design but nevertheless requires to be considered within a broader prevention policy.

Compared to external BCTU, the analyses relative to deviations revealed four types highlighting four possible action in terms of design:

1. Deviations between safety solution and safety function: conflict between the protective device installed and its objective which leads its being defeated.
2. Deviations between technical solutions and work requirements: initial technical solutions incompatible with the requirements of the activity.
3. Deviations between model designed and model installed. Final technical solution not optimal or degraded compared to the initial solution.
4. Deviations between the nominal conditions foreseen and the real operational conditions.

In relation to this analysis we can show that the migration process can commence at the design phases but may also begin only during the production phase. Indeed, design choices exist which becomes BCTU in interaction with the work requirements, as is the case in earlier points 1 and 2. Points 3 and 4 illustrate cases where the migration begins on account of changes during the design process (installation) or a lack of consideration being given to the real operating modes (production) of equipment during design.

The links between BATU and BCTU express a dynamic phenomenon according to the phases of the design process and work process as shown in Fig. 6. The possible sources of migration are therefore multiple. For example, the analysis of the activity of design highlighted the existence of BCTU regarding the integration or non-integration of safety (De la Garza, 2000). Thus, the design of a folding machine, in particular with respect to paper lead, obliged the operators to adopt acrobatic positions and to take risks by climbing onto a guardrail to be able to access these points at a specific position on the folder machine. The design choices did not take into account all the operations to be carried out.

Although the work analysis focussed on the activity of management personnel within the company, BATU stemming from various decision centres will also evolve as BCTU for those working downstream and promote the appearance of BATU to cope with the work requirements. Hence, if the management makes a choice relative to training policy in which a reduction in costs is favoured to the detriment of a complete training programme for all the operators (only a few operators are trained), this choice constitutes a BATU which may promote, for example, a

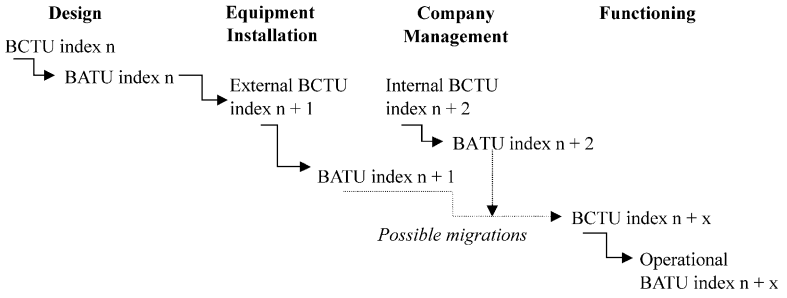


Fig. 6. Evolutionary character and links between BCTU and BATU according to the phases of the design process and work process.

migration towards limit thresholds in terms of skills due to their deterioration. BCTU will appear and in the production situation the establishment of on-the-job training can be observed as a palliative yet insufficient practice.

BCTU therefore bear witness to a migration that may originate far upstream. They also bear witness to a complex reliability network linking equipment design and the overall conception of work situations.

Fig. 7 shows a migration similar to the model of Rasmussen (1997) going from a nominal zone towards a zone of usual practices and leaving room for manoeuvre for the different work actors. Finally, there is a zone or a gap between this envelope of efficient usual practices oscillating between exceeding the safety barriers and the operational layer of safety, and the limit marking the passage towards the unacceptable.

The model that we propose (Fig. 7) is constructed around three main zones:

1. The first is called the nominal operation zone lying between the first safety barrier and the higher acceptable level of performance.
2. The second is called the unacceptable operation zone, from the point of view of safety and production. It covers the external part of this model. In other words, beyond the last safety barrier and lower acceptable lever of performances.
3. Between these two zones is a third zone called the boundary operation zone tolerated by use which is located beyond the first safety barrier while still remaining in the acceptable level of performance. At the outset (at the design stage), this limit zone represents both the regulation/standard layer of safety and the acceptable layer of performance.

Like in the model of Rasmussen (1997), here we describe in diagram form a migration towards a zone of usual practices. However, according to our field studies, this zone corresponds to a zone constructed by the different work actors in which they seek to increase their room for manoeuvre by, among other things, taking autonomy in relation to their skills and in interaction with the requirements and constraints of the work situation. In addition, although in the model of Rasmussen this gap is characterised by a margin of error, our studies show that is:

- in certain cases, rather a discrepancy unique to the appearance and the evolution of palliative activities which can stretch towards a limit zone and even force the threshold of tolerance (permissiveness) of the system; and
- in other cases, a migration in the opposite direction, i.e. towards an area of safer practices. This is illustrated by incident recovery situations.

Thus, this model underlines the dynamic "reaction" of the production system faced with various constraints (recoveries, migrations, malfunctions, etc.) which deteriorate the performance of the system by taking it into the unacceptable operation (left-hand side of the model). This reaction promotes a migration towards the organisational choices and operating modes whereas the boundary activities tolerated by use take the performance towards the acceptable layer of performance by breaching the first safety barrier foreseen at the design stage and then weakening the overall safety of the socio-

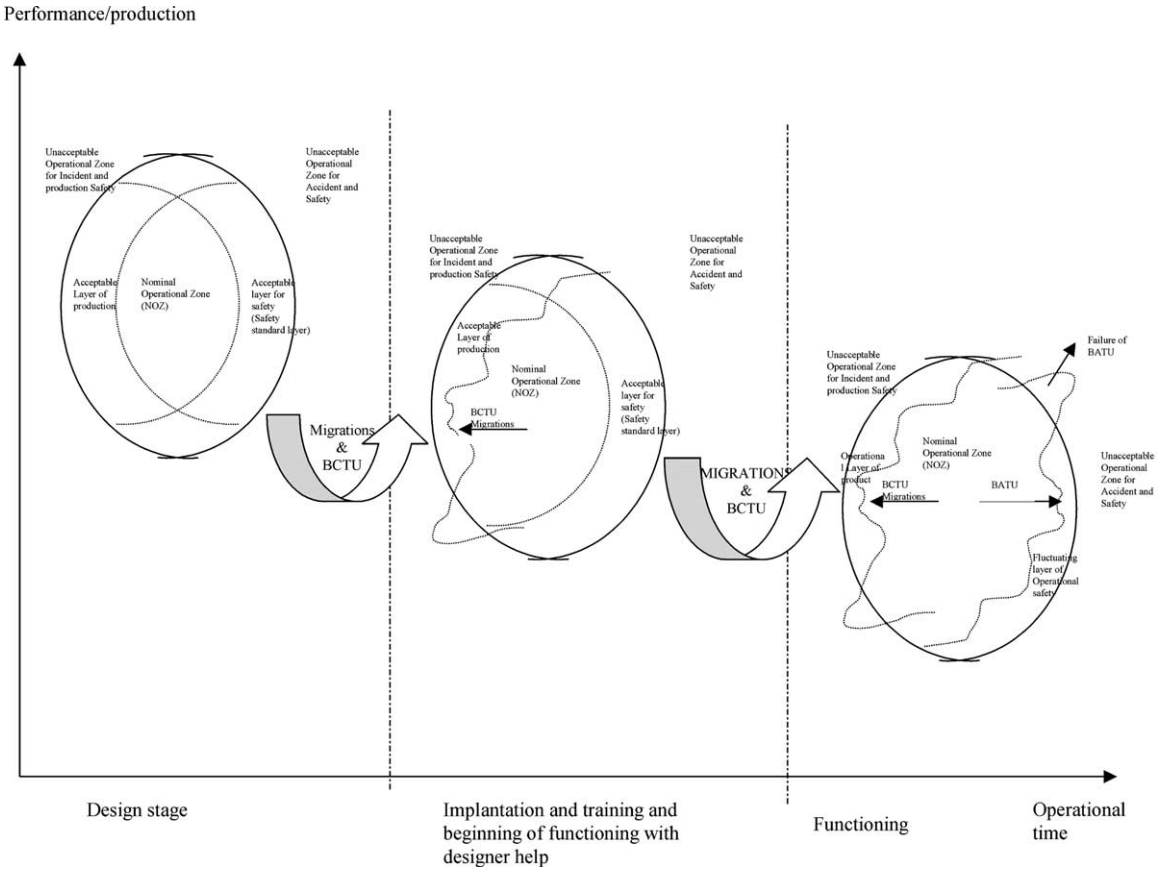


Fig. 7. Model of the migration towards limit zones from the point of view of performance and safety in relation to safety barriers and operational layers of safety and productivity.

technical system. However, this breach is compensated by the construction and establishment of second order safety procedures, thereby constituting a operational layer of safety, and in so doing reducing the regulation or standard layer of safety (R/S LS). This operational layer is fluctuating. It oscillates within the R/S LS but can exceed it in the case of failure, thereby provoking the incident or accident.

5. Towards a safer design

Differentiating and highlighting the dynamic links between the palliative activities employed to deal with various perturbations (recoveries, malfunctions) and the BCTU made it possible to analyse the events and circumstances liable to lead to accidents. Knowledge of these events and their characteristics will allow us to reintroduce them at the design stage so that they can be integrated. In addition, taking BATU into account during the design could update the reference framework of the operational system and the activity generated to ensure and maintain its performance.

5.1. The links between BATU and BCTU requiring identification for risk prevention

We have shown that BATU play an important role in taking the operation of automated systems and the safety of operators to the limit. However, their variability is such that it is impossible to take them into account directly and thoroughly during design. This does not mean lapsing into the known shortcomings of design: the impossibility of predicting everything. In contrast, knowledge of their links with the ''initiating causes'' (migrations and boundary conditions tolerated by use of design) will allow us to help the designer consider the existence of different work situations as well as the different types of interventions on the equipment in order either to eliminate or contain these BATU and migrations. However, this assistance incorporates knowledge of certain characteristics of the BCTU and BATU. Indeed, as Fig. 6 shows, BATU and BCTU always go in pairs and refer to multiple dysfunctions within the work process and the design process. It would appear to us important to consider at least four characteristics that should be studied either alone or in combination in these two processes.

Origin/initiator. Knowledge of the origin of the BCTU firstly allows an understanding of the reason for its existence and therefore orientation towards unbiased ways forward.

If it is the designer who is at the origin, this means that there was no means to anticipate the consequences of his or her technical choice (accuracy of the specifications and normative requirements, reuse of known and economically viable solution as not in possession of specific solutions, ambiguous specifications, insufficient experience feedback).

If the BCTU comes from a consensus between the designer and the customer, this means that the standard solution proposed to the customer does not suit the characteristics of the production site and/or it is too expensive.

Finally, if the origin of the BCTU is an implicit consensus between management and operators, this can stem either from a management policy and system specific to the user company or from the incapacity of the system to manage all the work situations.

Anticipation. This is the possibility and the capacity of prediction at the design stage. At standard equipment design level, the specifications are more centred on technical performance which integrates little or no safety and ergonomics. Experience feedback in relation to BATU and BCTU could allow a broader vision of the characteristics of the use of equipment and thus anticipation of possible migrations that weaken the reliability of the socio-technical system. However, design does not stop at the design office and requires the integration of the on-site installation and operation phases, which are the phases promoting the appearance of deviations in relation to that foreseen upstream. This phase also commits the user company and refers to adaptations to deal with the constraints of each specific situation (particular architecture, particular line composition, etc.). Based on experience feedback, this phase requires knowledge of the specific work situations and location, and anticipation of the consequences of the choices made regarding the work conditions and the reliability of the socio-technical system. The last phase that must be considered in this anticipation is production. This probably the most difficult as the adaptations and migrations of the socio-technical system are induced by the work situation itself and by specific work conditions. Here, equipment design is one element among others: the choices in terms of personnel, training, maintenance, production, etc. will also determine possible migrations towards limit thresholds.

"Frequency of appearance". The frequency of appearance of a BATU can facilitate how it is taken into account, integrated and anticipated within the design. Indeed, faced with an exceptional BATU which occurs from time to time, it is more difficult to react firstly to identify then to analyse and lastly to contain it within the design. In contrast, faced with a frequent even routine BATU functioning as the reference for the operators, experience feedback to the design is both easier and richer.

The elimination capacity or reversibility. The eliminable–reversible character must be considered within a context integrating both existing equipment and future equipment, in interaction with the work requirements and the constraints unique to the production situation. Thus, depending on the case, it may be decided to eliminate a BATU rather than to contain it as the risk engendered is too great and the means are available to achieve the same aim differently. It may also be decided for existing equipment to contain them (Amalberti, 2001), but to eliminate them in the future by providing the means of anticipation in the specification.

5.2. Conclusion: a philosophy of prevention in design integrating the characteristics of the socio-technical system

As regards safety, the design of automated systems has revealed a number of paradoxes which many authors have already pointed out and which our work

confirms. However, our results emphasise one paradox in particular in relation to the increasing complexity of automated systems. Indeed, the more complex the system the greater the attempt made to compensate this complexity by the abundant and increasing existence of procedures, instructions, and safety and control systems (''adding'' safety solutions). In this context, there is a risk of the system becoming more and more opaque for the user. In parallel, it remains difficult to anticipate everything, and the surveillance and control role of the operators is therefore increased, the work sometimes being transformed into an assignment rather than a set of well-defined tasks (de Terssac, 1992) which leaves a number of choices at the discretion of the operators.

From the design point of view, the performances of these systems are founded on the reliability of this complexity (components, interactions, completeness, etc.), with ''priority'' given to safety in the case of ''safety-productivity'' conflict. This vision of the designer, both normative and ''optimistic'', is based on the fact that during design, a level of reliability and availability is guaranteed such that there will be no conflict and in the worst situation this conflict will remain minimum. However, our field analyses show that this vision is not viable. Dealing with work requirements and constraints necessitates considerable autonomy and responsibility taking by the operators in order to take decisions during delicate situations. Indeed, contrary to that stated, the following are observed:

- frequent dysfunctions and recovery situations;
- considerable variability of work situations, the majority of which are not covered by the existing solutions and procedures; and
- the existence of a large number of situations where the ''productivity–safety'' conflict goes in the direction of stopping production whereas in fact priority is given to production to the detriment even of safety.

As a result, and to ensure production objectives, the system tends to tolerate practices like BATU which can extend to changing procedures by constructing others, and even defeating safety devices in order to be able to work. The efficiency of the technical system, which should have been be ensured by its reliability, becomes based more or less completely on these practices. Outside the regulatory framework laid down, these practices, induced by the design and by the deviations and migrations undergone by the socio-technical system, accentuated by operational constraints and reinforced by managerial decisions (internal BCTU), often go in the direction of production to the detriment of a weakening of the safety level.

It would therefore appear important to bring in a change from the point of view of design philosophy.

5.2.1. Going beyond technical knowledge

Experience has shown that as regards the design of automated systems, the decision is made on the basis of the presupposed efficiency of the choice of technical solutions. However, if this technological certainty (high reliability, process stability,

etc.) is compared to the operating reality of an industrial system, it becomes clear that:

- Whereas a "unique situation" is presupposed (as broad as its definition may be) a variability of situations and multiple work contexts actually exists (Fadier, 1998; De la Garza, 2000).
- The existence of human variability (intra and inter) underlines a diversity of representations of reality and of the meaning accorded by the operators to their actions.
- The dynamic aspect of work situations must be taken into account, which means that one element of the system cannot be modified without upsetting the entire structure.
- There is a necessity to intervene on a system in degraded operation on a daily basis faced with a process highly likely to produce events.
- As the ergonomic analysis has highlighted, work is achieved by adaptations and regulations, the optimal operating conditions very rarely being met. This divergence (and sometimes contradiction) between the expected operation (in principle) and the real operation (integrating situation recovery management) is considered as one of the most important sources of "risk taking" as it involves the operator/user betting with a situation not foreseen at the design stage.

Thus, techno-centred analyses and design provide only a partial response to taking into account real work needs. On the other hand, within the context of a systemic approach, they can advantageously be completed and added to by the contribution of ergonomic analyses of the real work. The MAFERGO methodology, for example, allows this enriching as it combines technical analyses of reliability with ergonomic analyses of the work to better understand the different work situations and to compare them with the technical solutions proposed during design.

5.2.2. Broaden the scope of design

To integrate prevention requirements (those directly dependent on human activities) into the design efficiently, a shift in viewpoint is necessary, which consists of:

Taking into account the different phases of design, installation and operation: in this respect, design must not be considered as achieved at the end of the design phase. Hence, work carried out by INRS (Neboit et al., 1998) demonstrated that the installation phase constitutes the phase of applying the designed system. It is considered as being an instantiation of the design (comparison of the functional model to the reality and characteristics of the context). This phase can furthermore be considered as presenting certain characteristics of the design and even as forming part of it. Moreover, other authors (Perrin, 1991; Daniellou, 1992; Fadier, 1998; Rasmussen, 2001) have insisted on the fact that design terminates by end use. Consequently, taking the activity into account requires integration of the

imperfections of the system by means of experience feedback and eventual reversibility of the technical system. Broadly speaking, this involves considering the data stemming from operational analyses within an iterative process using tools capable of taking these data into account (Didelot and Fadier, 2000; Fadier et al. 2001).

Better distribution of the "Human–Machine" functions through an efficient and participative ergonomic policy: as regards design, technical knowledge has saturated the area of intellectual knowledge to the detriment of the knowledge and know-how accumulated in the domain of human and social science. In addition, it has been shown that when carrying out a design functional analysis, attention is primarily focussed on technical functions. The operator is only summarily taken into account (ergonomics of the handle, colour of the interface, etc.) and more often than not "inherits" the functions that the technical system cannot fulfil. This analysis therefore does not allow either the activities of future users (production activities, maintenance activities, etc.) or the potential contexts of use (in particular degraded operating conditions) to be taken into consideration. Unfortunately, not taking future work activities into account is a shortcoming and one of the reasons behind certain occupational health and safety problems. Current knowledge in ergonomics allows, in certain cases, contribution of the elements that have been missing until now to answer certain questions: what balance in the distribution of technical and human functions? According to which criteria and constraints? The definition of probable future activities (content, internal coherence, collective activity, physical and mental load, organisation, etc.), the definition of operating interfaces (procedures, operating modes, alarm displays, diagnostic aids, hazard detection and anticipation aids, planning and management aids, etc.). This set of data is not totally stabilised at the present time and therefore cannot be generalised to every situation.

Safety culture versus design culture: design logic pushes industrial concerns, in situations of conflict, to favour productivity (seen as the profitability of investments) rather than safety (seen as a cost and a constraint). A shift in viewpoint is required and can be achieved by considering these types of requirements (occupational health and safety) from the design stage onwards not as constraints (in any case as difficult to integrate into functional logic) but as integral parts of the system (Rasmussen, 1997). In this respect, the new approach (EN 09–000), which is based on the principle of obligation of results, allows the safety function to be considered as an integral part of the technical system and therefore as an "industrial investment" to be made profitable. Table 2 summarises the characteristics and interest of this new approach compared to the more traditional approach.

This means getting away from a restrictive and "fixed" safety philosophy towards proactive and "user-friendly" safety. This change of philosophy means gradually giving safety a status in equipment specifications in the same way as performance

Table 2
Comparison of the two safety integration policies

"Obligation of means" policy (traditional approach)	"Obligation of results" policy (New approach)
Defensive	Offensive
Passive	Active
Static	Dynamic
Determinist	Probabilistic
Partial	Global
Guilt based	Responsibility based
Safety considered as a cost, a constraint	Safety considered as an investment

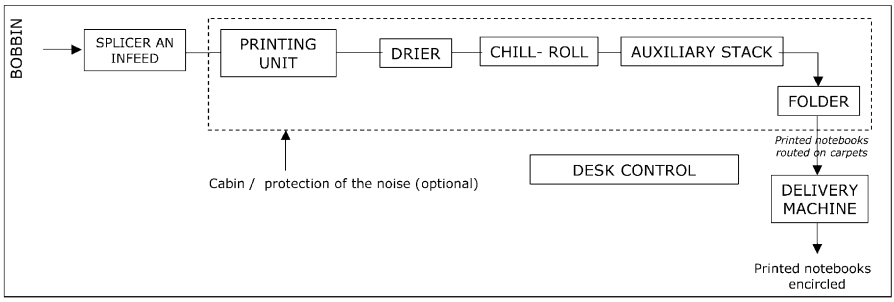
and technical choices, planning and anticipating the safety parameters during the design process systematically.

In addition, our studies have highlighted the necessity of establishing a specific experience feedback structure for aspects relative to the overall reliability of the socio-technical system. Indeed, with the exception of certain very specific sectors (e.g. aeronautical), experience feedback in the domain of safety functions in a more empirical than systematic way. Feedback regarding design often therefore leads to "one by one" transformations rather than to consideration being given to all the factors which really orient the design of equipment.

Taking work organisation into account. As Fig. 6 summarises, two main axes should concern prevention, namely the internal organisation of the company and the design of equipment. To the technical system and a personal view of the role of man in safety, this additional dimension must be considered in relation to organisational aspects in the approach to safety. Indeed, the analysis of important accidents shows that these aspects play a role in the construction of the combined factors having led to these accidents (Reason, 1995; Rasmussen, 1997; Neboit et al., 1998; De la Garza, 1999; Perrow, 1984), and that these aspects represent a priority way forward to improve safety in complex systems. Thus, to be efficient, a global safety policy such as that advocated for several years (Cox and Cox, 1996; Hale and Baram, 1998; Pidgeaon and O'Leary, 2000) could be enhanced by establishing feedback analysis structured around the study of BCTU and BATU.

Appendix A. General presentation of a printing line

An offset printing line is established by the following elements: a splicer, an infeed, four printing units, a drier, a chill-roll, an auxiliary stack, a slitters, a folder machine, a delivery machine and the control console.



The following table summarises the principal functions of these elements:

Element	Function
Splicer	Splice and stop the bobbin.
Infeed	Adjust the paper tension and give the paper.
Printing units	Lay down printing ink film, water film and additives in the paper Control of the speed strip paper
Drier	Dry strip paper with hot air
Chill-roll	Cools the paper by making get through the strip cylinders containing some water in 20 °C. Could adjust the paper tension
Auxiliary stack	Guide paper strip Stabilise the printing ink by laying down silicone The camera of location reads the adaptation of marks on the edge of the books
Coupes	Cut paper
Folder machine	Cut and folder the books
Delivery machine	Stack books Hoop the piles of books

References

Amalberti, R., 2001. The paradoxes of almost totally safe transportation systems. Safety Science 37, 109–126.

Baram, M., 1995. Safety management: organizational learning disabilities in using incident analysis. Presented at Network Meeting, Bad Homburg, Germany.

Bainbridge, L., 1982. Ironies of automations. In: Duncan, K., Leplat, J. (Eds.), New Technology and Human Error. Wiley & Sons, Chichester, pp. 271–286.

Chaband, C., 1990. Tâche attendue et obligations implicites. In Dadoy, M., Henry, C., Hillau, B., de Terssac, G., Troussier, J.F., Weill-Fassina, A. (Eds.), Les analyses du travail enjeux et formes. CEREQ 54, 174–182.

Cru, D., 1995. Règles de métier, langue de métier: dimension symbolique au travail et démarche participative de prévention. Le cas du bâtiment et des travaux publics. Mémoire du Diplôme de l'EPHE, LEPC, Paris.

Cox, S., Cox, T., 1996. Safety Systems and People. Butterworth-Heinemann, Oxford.

Daniellou, F., 1992. Le statut de la pratique et des connaissances dans l'intervention ergonomique de conception. Document de synthèse présenté à l'Université de Toulouse le Mirail en vue d'obtenir l'Habilitation à diriger des Recherches.

De la Garza, C., 2000. Modalités d'intégration de la sécurité dans une activité de conception: l'exemple d'une rotative. Rapport d'avancement, Projet PROSPER, Convention INRS-LEI, décembre.

De la Garza, C., 1999. Fiabilité individuelle et organisationnelle dans l'émergence de processus incidentels au cours d'opérations de maintenance. Le Travail Humain, 62 (1) 63–91.

De la Garza, C., Fadier, E., 2002. Contribution of the Unsafe Acts Analysis to Safe Design and Application to the Printing Sector PSAM6, San Juan, Puerto Rico, 23–28 June.

De la Garza, C., Weill-Fassina, A., 2000. Régulations horizontales et verticales du risque. In: Benchekroun, T.H., Weill-Fassina, A., (coordinateurs), Le travail collectif. Perspectives actuelles en ergonomie. Octarès éditions, Toulouse, pp. 217–234.

De la Garza, C., Weill-Fassina, A., Maggi, B., 1999a. Modalités de réélaboration des règles : des moyens de compensation des perturbations dans la maintenance d'infrastructures ferroviaires. Actes du 34ème Congrès de la SELF, Caen, pp, 335–343.

De la Garza, C., Maggi, B., Weill-Fassina, A., 1999b. Tempo autonomia e discrezionalita nella manutenzione di infrastrutture ferroviarie/Time, autonomy and discretion in railway maintenance. Ergonomia 12, 36–43.

de Terssac, G., 1992. Autonomie dans le Travail. Sociologie d'Aujourd'hui. PUF, Paris.

de Terssac, G., Chabaud, C., 1990. Référentiel opératif commun et fiabilité. In: Leplat, J., de Terssac, G. (Eds.), Les Facteurs Humains de la Fiabilité dans les Systèmes Complexes. Octarès editions, Marseille, pp. 111–139.

Didelot, A., 2001. Contribution à l'identification et au contrôle des risques dans le processus de conception. Thèse de doctorat, INRS, LRGSI, Nancy, octobre 2001.

Didelot, A., Fadier, E. 2001. Caractérisation des situations à risques à partir d'une analyse opérationnelle pour l'optimisation de la conception. In: 4ème congrès international pluridisciplinaire Qualité et Sûreté de fonctionnement, 22–23 mars, Annecy–France.

Didelot, A., Fadier, E., 2000. L'apport de l'analyse opérationnelle à la conception: cas d'un processus d'imprimerie. Actes du 12ème Congrès National de Sûreté de fonctionnement, Montpellier, pp. 231–240.

Didelot, A., Fadier, E., De la Garza, C., Ottensen, C., 1999. Analyse d'une situation de travail dans l'imprimerie et application de MAFERGO: le cas de la rotative M3000. Rapport d'avancement INRS-LEI-LRGSI, octobre.

EN 292. Sécurité des machines—notions fondamentales, Principes généraux de conception, décembre 1991.

EN 614. Sécurité des machines—principes ergonomiques de conception, avril 1995.

EN 1010. Sécurité des machines—prescription de sécurité pour la conception et la construction des machines d'impression et de transformation du papier, juillet 1997.

Fadier, E., 1998. L'intégration des facteurs humains à la conception, travaux actuels et perspectives. Phoebus: La Revue de la sûreté de fonctionnement. Numéro spécial consacré aux facteurs humains, pp. 59–66.

Fadier, E., 2001. The safety of automated systems in terms of human factors: overview and outlook. In: Second International Conference "Safety of Industrial Automated Systems". Bonn, Germany, 13–15 November.

Fadier, E., Poyet, C., Neboit, M., 1991. Advantage of an integrated approach of reliability and ergonomical analysis- Application to a hybrid system of sequential production. In: Queinnec, Y., Daniellou, F. (Eds.), Designing for Everyone. Taylor & Francis, London, pp. 477–479.

Fadier, E., Didelot, A., De la Garza, C., Neboit, M., 2001. Caractérisation, typologie et définition des conditions limites tolérées par l'usage et des activités limites tolérées à l'usage. 3e Conférence Francophone de Modélisation et SIMulation 'Conception, Analyse et Gestion des Systèmes Industriels', MOSIM'01, 25–27.

Hale, A., Baram, M. (Eds.), 1998. Safety Management. The Challenge of Change. Pergamon, Elsevier Science, Oxford.

Hollnagel, E., 1999. Accident and barriers. In: Seventh European Conference on Cognitive Science Approaches to Process Control, 21–24 Septembre, Villeneuve d'Ascq, France, pp. 75–180.
Le Petite Larousse illustré, 1998. Edition nouvelle. Larousse, Paris.
Maggi, B., 1996. La régulation du processus d'action de travail. In: Cazamian, P., Hubault, F., Noulin, M. (Eds.), Traité d'Ergonomie (nvlle. édition actualisée). Octarès Éditions, Toulouse, pp. 637–662.
Neboit, M., 1989. Impact de l'automatisation/information des processus sur l'activité des équipes de conduite (conséquences pour l'ergonomie et la formation). Colloque AISS, Paris.
Neboit, M., Fadier, E., Ciccotelli, J., 1998. Intégration des conditions limites d'utilisation des équipements de travail, pour la prévention des risques associés, dès la conception des systèmes de production. Rapport d'avancement INRS, novembre.
Perrin, J., 1991. Construire une science des techniques, L'interdisciplinaire, Limonest, Paris.
Perrow, C., 1984. Normal Accidents. Living with High Risk Technologies. Basic Books, New York.
Pidgeaon, N., O'Leary, M., 2000. Man-made disasters: why technology and organizations (sometimes) fail. Safety Science 34, 15–30.
Polet, P.H., Vanderhaegen, F., Wieringa, P., 2000. Theory of barrier crossing. In Nineteenth European Annual Conference on Human Decision Making and Manual Control, Ispra, Italy, 26–28 June.
Rasmussen, J., 1997. Risk Management in a dynamic society: a modelling problem. Safety Science 27 (2–3), 183–213.
Rasmussen, J., 2000. Accident causation and risk management: basic re'search problems in dynamic, tightly coupled society. In Fourth Multidisciplinary Seminar on "Risk, Errors and Accidents, and their Control", Risk Control and Risk Management, 14–15 mai, CNRS, Gif-sur-Yvette.
Reason, J., 1990. Human Error. Cambridge University Press, Cambridge.
Reason, J., 1995. A systems approach to organizational error. Ergonomics 38 (8), 1708–1721.
Vandaele, A., 1993. Complexité des systèmes et erreur humaine. Revue Préventique 6, 25–32.
Vaughan, D., 1996. The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA. University of Chicago Press, Chicago.
Weill-Fassina, A., Valot, Cl., 1997. Le métier ça va, mais le problème, c'est ce qu'y a autour. In: Recherche, Pratique et Formation en Ergonomie, Actes du XXXIIème Congrès de la SELF, septembre, Lyon, pp. 183–196.