InterfacEHS
A Journal on Integrated Management of Occupational Health and the Environment

www.interfacehs.sp.senac.br
http://www.interfacehs.sp.senac.br/en/articles.asp?ed=2&cod_artigo=44

SYSTEMIC APPROACH TO ACCIDENTS AND OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT

Ildeberto Muniz de Almeida[1]

[1]Department of Public Health of the Botucatu Faculty of Medicine – Unesp

ABSTRACT

The principal objectives of this text are: to propagate concepts of systemic approaches to work accidents and to stimulate reflections on their utilization in Occupational Health and Safety Management Systems (OHSMS) in Brazil. The concepts presented suggest new ways to interpret human behaviors that participate in the proximal or remote causes of accidents. Accident analysis must investigate latent or incubated conditions, and research aspects of interactive complexity, control modes and situations, behavioral modeling mechanisms, system migration to accidents or other aspects. Parties responsible for OHSMS are encouraged to know how to recognize the concepts or approaches most useful to organizations in which they act.

Key words: Workplace accidents, Accident theories, Accident analysis, Occupational Health and Safety Management Systems, System migration.

INTRODUCTION

The analyses of work-place accidents traditionally conclude by attributing blame the victims themselves and denying the existence of problems or malfunction in the systems that give rise to these events. Over the last few decades questions have been raised regarding this conclusion and opinions have highlighted the occurrence of accidents as a warning as to the existence of systemic malfunction, signs of the occurrence of latent problems that need to be heeded and appropriately interpreted by the occupational health and safety management systems (OHSMS).

It is not easy to spread the word about the systemic focus of accidents. In Brazil one of the few works dedicated to systemic focus is “Acidentes industriais. O custo do silêncio” [Industrial Accidents. The cost of silence] by Michel Llory (1999a). In the book’s preface, Gerard Mendel discusses the resistance to this approach, pointing out that it has to do “*with [...] the principle from which science can be founded and developed. [...] science is constructed by increasingly breaking down the reality into distinct and separate disciplinary fields, but despite this reality only exists in a global form. [...] the spirit of the scientist is not prepared to move in these inter-disciplinary fields.*”

The aim of this text is to present some of the concepts of this approach that have been used over the last few decades when analyzing accidents and to discuss the implications of incorporating them into OHSMS. The discussion will be accompanied by questions, suggested as topics for reflection. It does not aim to establish “new truths”, but it demands at least an explanation of the reasons that lead each system to make the choices they do. In short, the text points to the existence of OHSMS paths that are little known among us.

JAMES REASON’S ORGANIZATIONAL ACCIDENT MODEL

The expression *organizational accident* was used by Reason (1997) as a contrast to the idea of the *individual accident*. According to Reason, in the latter all happenings relative to the accident, in other words, its causes and consequences, can be considered as limited to the individual who carries out the activity and who suffers the accident and the injury. Organizational accidents are “comparatively rare events, but frequently

catastrophic, that occur within a complex modern technology, such as nuclear power stations, commercial aviation, the petrochemical industry, chemical process plants and railroad and marine transport systems, [...]" (p. 1).

In no time at all, this idea begins to be used in the approach to accidents occurring in other types of systems and situations. Reason himself uses it when studying maintenance accidents, particularly in aviation, and also in accidents that occur in health services.

Figure 1 shows the accident model suggested by Reason; a triangle and a rectangle are used to represent the accident. In the upper part of the Figure the rectangle represents the outcome of the accident. In his scheme the author here reproduces the idea of accident as a phenomenon that always includes the uncontrolled liberation of one (or more) particular type of energy in such a way as to produce losses in the system: material and environmental damage, other forms of loss or human victims.

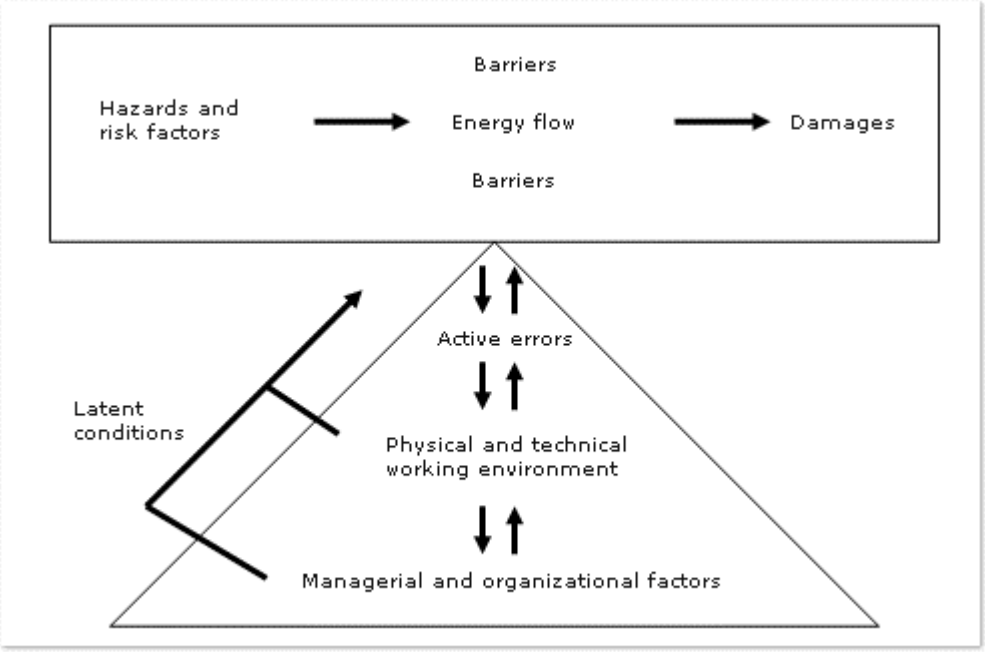

Figure 1: James Reason's (1997) organizational accident model

The energy liberated was present in the system controlled by barriers that are unable to prevent the liberation of its flow at the time of the accident. At the top of the figure the arrow represents this idea of energy flow crossing the barriers.

In Reason's model the triangle that forms the base of the figure represents the system process or conditions from which the liberation of the energy flow originates. The behavior of the workers who were operating the system would be frequently found to be present in the immediate vicinity of the outcome of the accident, or the uncontrolled energy. These actions, or omissions, are represented at the top of the triangle and were called by Reason, *active errors,* including both voluntary and involuntary behaviors (or "errors"). Active errors correspond to the unsafe acts of the traditional approach to accidents.

In the middle of the triangle the physical and technical working environment factors are represented. They are the origin of the active errors, and in turn have their origins in managerial factors and those relating to the organization of work, which are represented at the base of the triangle. These two groups of factors are called latent conditions, which according to the scheme, may give rise to the uncontrolled energy, released in the accident in a direct way, in other words, without active errors being present. The 'latent conditions' arrow, which is parallel to the triangle, shows the possibility of accidents without active "errors" that have their direct origins in these conditions.

According to Reason, active errors are unimportant when it comes to prevention, in particular, because the different possible combinations of latent condition factors constantly create new conditions that facilitate the appearance of active errors. In other words, it is not possible to directly eliminate these errors; they are consequences and not causes. For this very reason, those who are interested in prevention should prioritize the elimination or minimization of latent conditions.

Perhaps the most important contribution to be highlighted in the studies of Reason is the idea that for those who are interested in accident prevention the path to follow is not in the study of "human errors", especially when this expression is taken in the sense of *active errors,* understood as being the result of the failure of the individual or operator who committed them. The characteristics of human behavior in the work-place lead those who study the topic to recognize that "to err is human", in other words, that errors are always going to exist and that for this reason ideal prevention must be based on an approach to those characteristics of the system that increase the chances of the occurrence of these errors.

Reason's contribution has an influence on everyone's approach to accidents. Those interested in finding out about it in more depth may look for it directly under the author's name in search engines and databases. Many examples of the application of these concepts in the study of maintenance-related accidents may be found in a recent book (REASON; HOBBS, 2003).

LLORY'S PSYCHO-ORGANIZATIONAL ACCIDENT

Other authors also use the expression "organizational accident" in a similar sense to that used by Reason. In 1997, a new edition of "Man made disasters" (TURNER; PIDGEON, 1997), was launched, which describes the stages or steps of the accident in the life of the system. In 1999, in France, Llory summarized the proposal of Turner & Pidgeon in three phases. The first, the *pre-accident,* or *incubation period,* in which a slow and progressive deterioration of the system leads to the second, *properly called, accident* phase, generally set off by a specific event. The third is the *post-accident* phase*,* in the course of which the social and institutional consequences of the accident manifest themselves, in the shape of an organizational and social crisis (LLORY, 1999b, p. 114).

"The accident is organizational to the extent that it is, primarily, the product of a socio-technical organization. It is no longer only the result of an 'unfortunate' combination of passive and latent failures with active and direct failures, no longer only the result of a specific combination of human errors and material failures" (p. 113). The accident is *"[...] rooted in the history of the organization: a series of decisions, or the absence of decisions; the evolution of the organizational, institutional and cultural context that interferes in the future of the system; the progressive evolution (deterioration) of conditions or factors that are inside the organization; some particular events that have a notable impact on the life and functioning of the socio-technical system, creating an unfavorable situation: territory into which the accident (or incident) may intrude and develop. [...] the accident incubates. The incubation period may be long [...]."* (p. 113-4).

Considering the above ideas of organizational accident the first questions suggested to those who are interested in OHSMS are:

What concept of accident is used in the system in which you operate?

Do your accident analyses identify latent conditions or aspects of the history of the incubation of these events? Do you adopt any of the concepts mentioned?

How do you consider the statement that the majority of accidents are due to operator error and that the main objective to be adopted for preventing them is the elimination of these errors?

CHARLES PERROW'S NOTION OF NORMAL OR SYSTEMIC ACCIDENT

One of the first works on the systemic focus was published in 1984 by the American sociologist, Charles Perrow: "Normal Accidents. Living with high-risk technologies". In this work he emphasizes the role of the structure of complex systems in the origins of what he called, *normal* or *systemic accidents*.

In his book Perrow (1999a) highlights an idea of risk that is not normally considered as such in traditional technical approaches. This is the risk arising from the possibility of interaction between factors, elements or components of socio-technical systems. This type of risk is described by the author as associated with systemic complexity, in other words, with a property of complex systems.

The author classifies systems into simple and complex as a function of the type of interaction that exists between their elements. In simple systems interactions of the type that are foreseeable, called simple, predominate, such as those present in a set of dominoes. The consequence of one of them falling, i.e. knocking down those that are in front of it, is easily foreseeable. In complex systems there is a greater frequency of interactions coming from the accumulation of aspects or factors that, seen in isolation, are not considered as risk, and even when considered as a whole, do not allow one to foresee the outcomes with which they are associated.

According to Perrow, in complex systems the emergence of complex interactions may give rise to unforeseen systemic behaviors that evolve so quickly that they make it impossible for the operators to re-establish their understanding of what is happening. As a consequence these situations evolve into accidents that are impossible to avoid.

The systems that present the most chances of being involved in accidents of this type are those that include a part, unit or sub-system that performs multiple functions simultaneously. For example, a heater that is used both for heating gases in a tank “A”, as well as for exchanging heat in such a way as to absorb any excess from a chemical reactor Its failure may mean that tank “A” is too cold for recombining the gas molecules and that the chemical reactor is over-heating at the same time, due to the non-absorption of the excess heat.

According to Perrow, systemic accidents tend to present accumulations of consequences of this type of failure, called common-mode failures, which tend to react with unfamiliar feedback to members of the system. Furthermore, the systems most susceptible to this type of accident may possess *interactivity,* characterized by the *physical proximity* between components, *information of an indirect* or *inferential nature, control of many parameters with potential interactions* and *limited understanding of some processes.* Summarizing the notion of *interactive complexity,* MARAIS et al., (2004) state that it “refers to the presence in a system of sequences of unfamiliar, unplanned and unexpected events”; they are also invisible and not immediately understandable.

This type of accident tends to be set off by common failures, apparently without any great significance as far as safety is concerned. For example, a defect in a coffee machine leading to a fire that ends with an airplane crashing. In the Three Mile Island accident a maintenance warning sign was covering an important luminous warning. In these cases the situations may seem bizarre to those examining them from outside, but they normally have a rational explanation from the operator.

The probability of these accidents is associated both to their *interactive complexity*, mentioned above, as well as by another property of these interactions: the fact that they are *tightly coupled*. This means that the system is highly interdependent in such a way that a change in one part of it may rapidly affect the status of other parts. Unlike loose interactions these prove to be strictly dependent, or associated. According to Perrow, *tightly coupled systems* have the following characteristics:

a) They have a greater number of processes that are time dependent, i.e. they cannot be shut down, for example, awaiting corrective interaction;

b) They have a greater proportion of specific and unvarying sequences, in such a way that the occurrence of A always leads to B happening;

c) In addition to specific sequences that do not vary the global design of the process allows for only one path for obtaining the production goal, for example, a nuclear plant cannot produce electricity from any other fuel, in other words, this is a system with little flexibility;

d) They have little room for maneuver, or slack, i.e. quantities must be accurate, resources cannot be substituted for others, temporary substitutions of equipment are not possible, etc. (PERROW, 1999a, p. 93 –4).

Perrow's view leads to a reading of the situation that is essentially *pessimistic* as far as the possibilities of preventing accidents in this type of system are concerned. It is not possible to foresee and avoid all the chances of complex interactions and some of them, because they are strongly coupled, would end up leading to *normal* or *systemic accidents*. This name was given, not because they are accidents that happen frequently, but because they arise from characteristics that are inherent to the system.

The alternative to these disasters lies in the political decision not to accept the introduction of this type of system in the area. Subsequently, prevention of this type of accident is discussed based on the idea of reducing *systemic complexity* (PERROW, 1999b; SAGAN 1993), including strategies of *structured pessimism* (PERROW, 1999b), i.e., the systematic exploration of worst-case scenarios as support for the preparation of prevention practices.

Although he was criticized for his pessimism Perrow's view has a large influence on those interested in the safety and reliability of systems. The concepts of *complex interaction* and *tightly coupled interaction* start to be considered in the design and operation of systems and the notion of the origins of accidents in the characteristics of the *structure* of systems starts to be used, as opposed to blaming the operators.

Those interested in other examples of the use of Perrow's concepts can find them in search engines and databases. The "Journal of Contingencies and Crisis Management" is compulsory reading for those interested in this topic.

THE SYSTEMIC APPROACH AND ACCIDENT ANALYSIS

The theory of systems has its origins in the 1930s and 1940s. The traditional scientific method adopts the division of the system into parts in such a way as to examine them separately. This process of decomposition, called *analytical reduction*, works with the following assumptions, among others: each component or subsystem operates independently, in other words, these components would not be subject neither to the effects of the results of their actions, nor to those of other system components. In short, this focus considers that the behavior of the components (for example, the pedals of a bicycle) is the same when examined in isolation (with the bicycle dismantled), as when exercising their role within the whole (in the assembled bicycle) (LEVESON, 2002).

The systemic focus is centered on the system taken as a whole, assuming that some of its properties can only be dealt with adequately in their entirety. The foundations of the theory of systems are to be found in two pairs of ideas: 1) emerging properties and hierarchy, and 2) communication and control.

In other words, complex systems may be described as presenting different levels organized hierarchically. Each level is characterized as having *emerging properties*, i.e., that do not exist at lower levels in the system. This can be illustrated with the idea of the components of a bicycle, or a technical system, and the function of this bicycle, or system. In isolation the pieces of the bicycle cannot be used as a means of transport. The work of the operators in assembling the bicycle makes this property, which does not exist in the set of isolated parts, emerge.

The notion of *hierarchy* aims to explain relationships between different levels. The upper hierarchical levels are responsible for controlling those lower down. To obtain this control they must impose behavioral laws, in other words, *constraints* or *limits* on the *degrees of freedom* of the components at the lower *level*. For example, the control of maintenance workers in terms of workplace safety, may be achieved by using constraints that come from the managers of the maintenance, safety and production sub-systems. This control derives from the *emerging properties* of the upper hierarchical levels.

Besides defining the constraints, for example, information that it imposes upon the lower hierarchical level, the upper level also defines forms of ascending communication that provide information about the real functioning of the system, especially how the

effective imposition of those constraints is working - or not, as the case may be - and completing the control loop between the different segments of hierarchy.

Safety is a typical example of a system's emerging property. It is impossible to assess whether a plant is safe by examining a valve in this plant. Statements about the safety of the valve without any information about the context in which it is being used make no sense. One might even talk about the *reliability* of this valve, defining *reliability* as the probability that its behavior will satisfy its specifications over time and under certain conditions. A component that is perfectly "safe" in one system may not be in another.

The concepts of *communication* and *control* of the theory of systems serve as the basis for developing information flow channels within organizations. The upper hierarchical levels take part in the design of constraints destined for the implementation of the system's "*laws of behavior*". These "laws" include the norms, means and practices to be used and that are aimed at ensuring the system's reliability and safety, thereby constituting the instruments or *regulatory* or *control actions* of the system.

In hierarchical organizations like companies, these control processes operate at the interface between the different levels, ranging from those who work on the factory floor to top management. In open systems *information and control loops* are considered fundamental when it comes to the continuity of their operation in dynamic equilibrium in their exchanges with the external environment. Figure 2, taken from Leveson (2004), shows the components of a typical *control loop* in the situation in which a human supervisor controls a particular automatic sub-system.

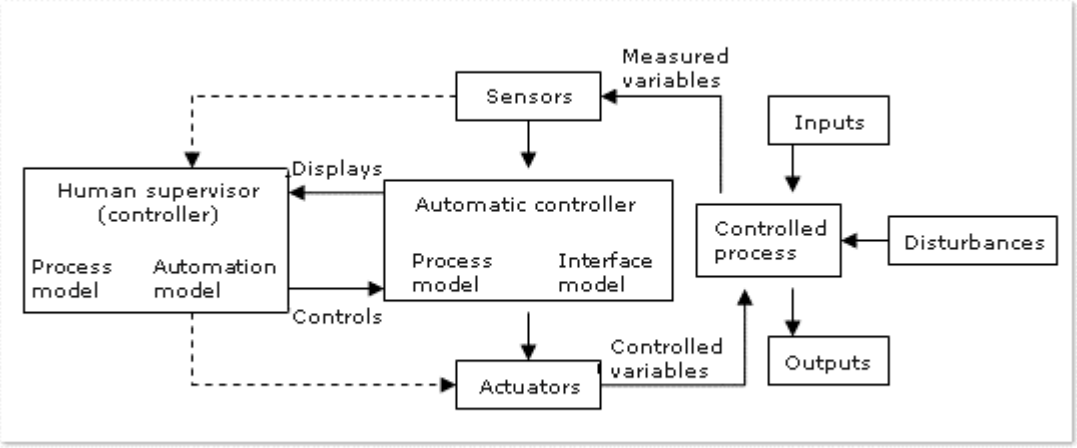

Figure 2: Standard control loop and its components (Leveson 2004)

The controller always has *mental models of the process* and *of automation* as they stand. For example, operating an automatic machine the worker constructs his own mental picture of what he is producing with the machine and on the very functioning of the machine. If he actions a command to close a valve and if in normal operation the response to this is the lighting up of a green light on the command panel, he may tend to interpret the light being on as a sign that the vale is closed. In turn, the machine incorporates the model of its creators regarding the same process and the necessary interfaces with the operators. In discussing accidents in complex systems the necessary *mental models* for managing the whole of the system must be analyzed. When the controller's or manager's model does not correspond to the real situation, for example, it does not include information about the repercussions that his decisions might have outside the system, decisions relating to the management of the safety and reliability of the system may be insufficient for maintaining it.

This notion of control loop is used by Leveson (2002, 2004) to criticize the breadth of the definition adopted by some academics for the expression "human error". Taken in a broad sense, difficulties arising in the *man-machine interaction* are interpreted as human failings. For Leveson, this way of defining *human error* fails to consider the characteristics of the design of the system, in particular those that come into the control loops between man and technical devices and that contribute to weakening the reliability and safety of the system. For example, a failure in the operation of the device that did not supply adequate

feedback regarding the state of the system after a previous action, tends to be attributed to the operator, thereby ignoring the design failure in this device.

IMPLICATIONS FOR SAFETY

These concepts reinforce the role of the various hierarchical levels in organizations when it comes to implementing effective control mechanisms, suggesting questions such as the following for those interested in OHSMS:

1. Do the accident analyses or the design of your organization's OHSMS, reconstruct the design and functioning of the *information and control loops* used between the various levels in the system, with an emphasis on those that refer to the actors involved in the accident?

2. Do the analyses clearly identify the constraints defined in the system in such a way as to check if the efforts made by the actors in the upper hierarchical levels force or encourage the system sufficiently, in the sense of constructing and consolidating the *reliability and safety* of the system?

3. Do the analyses include checking how top management monitors the operation and the performance of this system, including whether it receives information of the true state of the system?

4. Does the accompaniment highlight or emphasize the monitoring of the constant *local adaptations* that occur in the basic design of the systems as a response to the pressures and *variability* of system components in all types of activity?

Commenting on this last aspect, Leveson (2002) emphasizes the idea that every accident model that includes the notion of social and human systems must consider the existence of adaptations. According to her, in this type of system "the only constant is that nothing remains constant the whole time".

In similar fashion to what one sees in studies of the Ergonomics of an Activity, this way of understanding work reflects directly on the way of understanding human behavior in the work-place when the intended objectives are not achieved, in other words, the so-

called “human errors”. Seen from this conceptual framework the supposed human error can no longer be explained as the product of the personal characteristics of the operator, as the traditional approach to accidents invariably does.

The systemic focus starts to define “error” as deviation from rational and normally used procedure as an effective way of facing up to the variability aspects of work, and no longer as a deviation from a procedure or norm theoretically defined as the right way of doing the work. This raises new questions for those interested in OHSMS:

1. What definition of error is used in your system?

2. How does the OHSMS in your organization explain and propose approaching the origins of these events?

Those interested in examples of the use of Leveson’s model will find a large number of examples available in full on the webpage mentioned. The accident with the VLS-1 VO3 satellite launch vehicle, which happened at the Alcântara Base in Brazil, was analyzed using this model and Rasmussen’s vertical model (JOHNSON; ALMEIDA, no prelo).

ASPECTS OF THE EXPLORATION OF THE NOTION OF HUMAN ERROR IN ACCIDENT ANALYSES

Currently there seems to be agreement regarding the idea that work situations are starting to demand more in terms of cognitive reasoning skills than of sensory motor skills. Therefore, studies about the role of the social (human) component of these systems are beginning to grow in importance. Studies seek to explore the cognitive aspects associated with human behaviors with an emphasis on work-related situations.

The above distinction was also used by Rasmussen (1982) to explain the idea that workers use different types of psychic management of their actions because of the types of situation they face. He shows that there are actions that are controlled predominantly in an almost automatic way in routine situations. They may be developed without the need to think about their components. These behaviors are described by Rasmussen as skill-based. At the other extreme are actions controlled predominantly by the use of awareness

and reasoning. They are called knowledge-based and are more typical of new situations, or those that are infrequent. At the intermediary level are actions whose execution is rule-based, used in situations in which it is possible to foresee the majority of situations and train operators in developing them.

Human apprenticeship is described as a process in which, initially, conscious actions become automatic the more they are repeated. With *familiarization,* the operator's skill in their execution increases and they move to a level of cognitive regulation that demands less of the operator. When someone is learning to drive an automobile the learning process relating to taking the foot off the clutch pedal illustrates this situation. At the beginning the driver pays full attention to the speed with which he removes his foot and the action is consciously controlled. When the driver learns to drive the action is performed "automatically". The same reasoning applies to all learning situations. It is worth pointing out that when the work involves the occurrence of constantly new, or uncertain situations, conscious regulation will be more present. In fact, it is precisely the operator's skill in detecting and interpreting signs of change in the evolution of the activity that leads him to change the psychic management way he is using.

This knowledge raises questions for those who are interested in OHSMS:

1. In exploring human behaviors involved with work-related accidents does your OHSMS analysis team analyze the types of situation and the type of psychic management used by the operators?

2. In the accident analyses conducted by your OHSMS are the main parameters used and the characteristics of the ways with which they manifest themselves identified and are they perceived by the operators in managing the system? Are possible intervening factors explored?

3. In cases involving omissions is the possibility of there being cognitive traps in the system explored?

Those interested in examples of the use of these concepts in accident analyses can consult Reason; Hobbs (2003), Almeida; Binder (2004), Rasmussen; Svedung (2000), and others.

Broadening the accident analysis perimeter with the notion of migration from the system to the accident

Over the last decade Rasmussen (1997), Rasmussen; Svedung (2000), Svedung; Rasmussen (2002) have described what they consider to be the important challenge of today: risk management in a dynamic society.

The challenge has its origins in the rapid transformations through which society is currently passing, including:

The accelerated rhythm of technological change at the operative levels in society;

The increase in the scale of industrial installations with an increase in the potential for accidents of major proportions;

The rapid development of information technology and communication, leading to systems with a high degree of tightly coupled interactions; and

Environments that are highly aggressive and competitive that increase the number of potential conflicts to be experienced by the decision-makers, leading them to focus on short term financial gains and the survival criteria of systems in detriment to their safety.

The speed of change in the technical and organizational bases of the processes used in transport, industrial, health service provider and other systems that incorporate a large amount of new technology, is faster than that in management processes and very much faster than that found in extra-company systems, used for developing policies and legislation for controlling the risks of these processes This time lag, which prejudices the risk control mechanisms developed in socio-technical systems, becomes more evident in the face of the aggressive environment and exacerbated competitiveness in which these companies normally find themselves.

Under these conditions pressures in the system arise which, frequently, influence managements, leading them to adopt decisions of an immediatist nature that push the system close to the boundaries of its safety.

This dynamic process, par excellence, shows that these systems live in constant need of adaptation and changes in the environment in which they are inserted and also in

their own components. Under these conditions the traditional way of managing safety, based on prescriptive and normative approaches, becomes outdated.

In these systems accidents start involving aspects up until then non-existent, or that occur less frequently. Operators do not have to hand a rule or operational procedure that is capable of indicating how they should act when faced with such a disturbance.

In the systems he studied Rasmussen also shows that management decisions taken outside the walls of the company-system properly called, play their part in the origins of accidents. This type of situation is called distributed decision making and was exemplified by analysis of the capsize of the ferry in Zeebrugge in March, 1987. The authors show that this accident involved aspects relating to the design of the boat and the port, characteristics of cargo and passenger management, traffic timetables and the operation of the boat. The managers from each of the areas mentioned have to live with their own particular difficulties and pressures and cannot see the wood for the trees. Their decisions tend to ignore possible collateral effects in other sub-systems. The accumulation of the collateral effects of the decisions taken in each of the sub-systems only emerges in the system seen as a whole; it does not exist as a property of the components in isolation.

In this type of situation once a set of decisions has been adopted the system becomes vulnerable, or in other words, it becomes intolerant to a great number of changes, whether they be behavioral or from another of its components. In other words, if the accident had not been caused by specific factor x1, it could have been caused by x2, or any other.

This explains the criticism of Rasmussen (1997) of the idea of the "*basic cause*" or "*root cause*" of accidents, so widely divulged in the area of work-place safety. In traditional thinking, if the *basic cause* is eliminated this type of accident no longer occurs. Rasmussen has been showing that in dynamic systems accidents with similar aspects may occur without the presence of that particular cause thought of in isolation, because in the real work situation, the 'accidentogenic' scenario that is formed is the product of the interaction or accumulation of the collateral effects of decisions taken by different actors in scenarios where it is difficult to foresee the possibility, either of the accumulation, or of the effects. Furthermore, each decision in isolation is not capable of producing the effect revealed by the accident.

This scenario of vulnerability, of a reduction in the tolerance to change, or in the resilience of the system, is described by Rasmussen as a process of *system migration* to the accident or to the acceptable boundaries of its safety.

Once the migration has occurred the accident may be set off by many types of small changes, whose elimination, in accordance with the causal rationale of the traditional model of safety management, reveals itself to be powerless to bring about an effective improvement in the reliability and safety of the system.

Figure 3 shows the model suggested by Rasmussen (1997) to represent the migration of the system in the direction of its safety boundaries.

In every working system, human behavior is modeled by objectives and constraints that must be respected by the actors with a view to their achieving success in their interventions. Therefore, it is the system that imposes limits or boundaries, which if exceeded may threaten its survival or relative stability. There are frontiers of an economic nature, especially relating to cost, and there are also boundaries imposed by the work load to which the operators are submitted.

The working space in which the actors freely move is also limited by administrative, functional and safety constraints. They set the boundaries of *acceptable and perceived* performance. However, during their activities operators always have certain *degrees of freedom* that will be “closed” by the use of *local adaptations,* guided by criteria relative to the process in question, such as work-load, the cost benefit relationship, the risk of failure, the pleasure of exploring, etc.

This model calls our attention to the dynamic nature of the activity. “The normal changes found in local working conditions induce frequent strategy modifications and the activity shows great variability” (RASMUSSEN 1997, p. 189). Such local variations, induced by the situation, are compared by Rasmussen to the “Brownian motion” of gas molecules. During these attempts at *adaptation, effort and cost gradients* are established, the result of which tends to be a *systematic migration* towards the boundaries of functionally acceptable performance, which if crossed, result in error or accident. Because of this the author states that analysis must focus on the *mechanisms that generate the behaviors within the true and dynamic contexts of work,* and not human errors or violations.

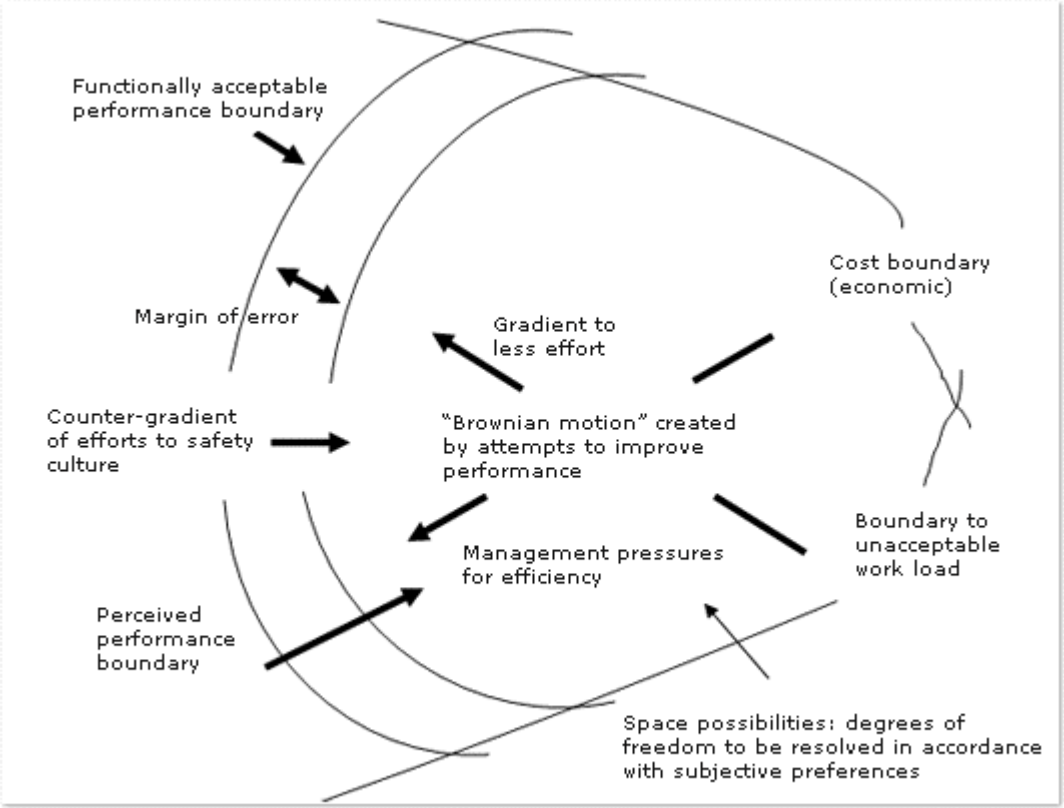

Figure 3: System migration to the boundaries of safe performance. (Rasmussen 1997)

According to Rasmussen, the majority of major accidents analyzed over the last few years show, in their origins, exactly this type of systematic migration to the safety boundaries of the system and not a “coincidence of independent failures and human errors”. Because of this, safety management in these types of system should be pro-active, centering on the study of the *normal activities* of the actors who prepared this scenario.

Well conceived systems have countless *barriers*, controls or *lines of precautions* to avoid accidents, so that the eventual violation of one of them does not lead immediately to an *adverse event*. The safety of a sub-system, or system in particular, also depends on the collateral effects of the actions of actors situated in other sub-systems, or systems. In systems in which the pressures for cost effectiveness dominate, the systematic degeneration of these protections is installed over time. The German sociologist, Ulrich Beck, called this process “produced uncertainty and organized irresponsibility” and “strategic uncertainty and structural vulnerability”, considering it to be the key problem for current research into risk management (apud SVEDUNG; RASMUSSEN, 2002, p. 399).

The example below was taken from a recent text. It illustrates the close relationship between notions of emerging property and system migration:

"During the company's night shift with two wood chippers, one of the chipper operators is absent and the older machine and the one with fewer operational resources remains switched off for lack of staff. Soon after, the log handling machine breaks down and is not repaired and its operator is left temporarily with time on his hands. Soon after, a new truck arrives in the yard loaded with lumber and is not unloaded due to the breakage of the log handling machine. Knowing that the truck is paid by the time it remains in the yard and aware of the pressures from management for fast unloading the head of the shift allocates the operator of the log handling machine to operate the stopped chipper and asks for the truck to be unloaded directly onto the conveyor belts of this machine.

Do the decisions taken create safety or risk?" (ALMEIDA, 2006, p. 37)

The concepts presented raise new questions for those interested in OHSMS. Other questions are presented after the text on vertical accident analysis models.

1. How does formal safety approach situations like the one in the example above?

2. Considering that the decision of the head of the shift corresponds to what is expected in the majority of systems, how do you classify the analysis conclusions of this type of accident, which explains them as the result of non-compliance with safety norms on the part of the operator?

3. How do your organization's OHSMS (formal safety) approach the emergence of situations of work disturbance and variability that demand responses from the workers that are equivalent to the notion of local adaptations, as mentioned above?

VERTICAL ACCIDENT ANALYSIS MODELS

These ideas are the basis of the risk management and accident analysis proposal developed by Rasmussen (1997) and also of the *Systems-Theoretic Accident Models and Processes* (STAMP) method, developed by Leveson (2004). Socio-technical systems

involved in risk management begin to be considered in their entirety, with all their hierarchical levels, going from “non-shop floor” operators to the legislators and government agencies responsible for the formulation and implementation of control policies.

Figure 4 shows the system described by Rasmussen. This vertical orientation model was suggested to “capture the causal process of losses as a boundary condition of working under pressure and [...] to identify sensitive parameters for controlling the behavior of organizations and individuals” (SVEDUNG; RASMUSSEN, 2002, p. 401).

The model describes the interactions between decision-makers situated at all levels in society in their roles as risk managers. The analysis takes up again the notion of *control loop* discussed previously, by exploring the possibilities of failure:

a) in the design of the constraints necessary for forcing the implementation of control actions;

b) in carrying out these actions;

c) in the feedback provided after carrying out the actions.

The model proposed by Leveson is similar to that of Rasmussen, but it begins by mapping out the actors involved in the accident, without reference to the physical process and the activities mentioned, in Rasmussen’s basic scheme.

The analyses include maps that show the control loops and information prescribed or proposed between the different hierarchical levels of the system and the same maps showing the local adaptations that over the time the system existed were being carried out in the components, whose purpose was to impose regulatory actions or inform management of the results of the actions carried out. Rasmussen and Svedung’s (2000) book includes an appendix with analysis registers of six accidents that use the technique proposed by the authors.

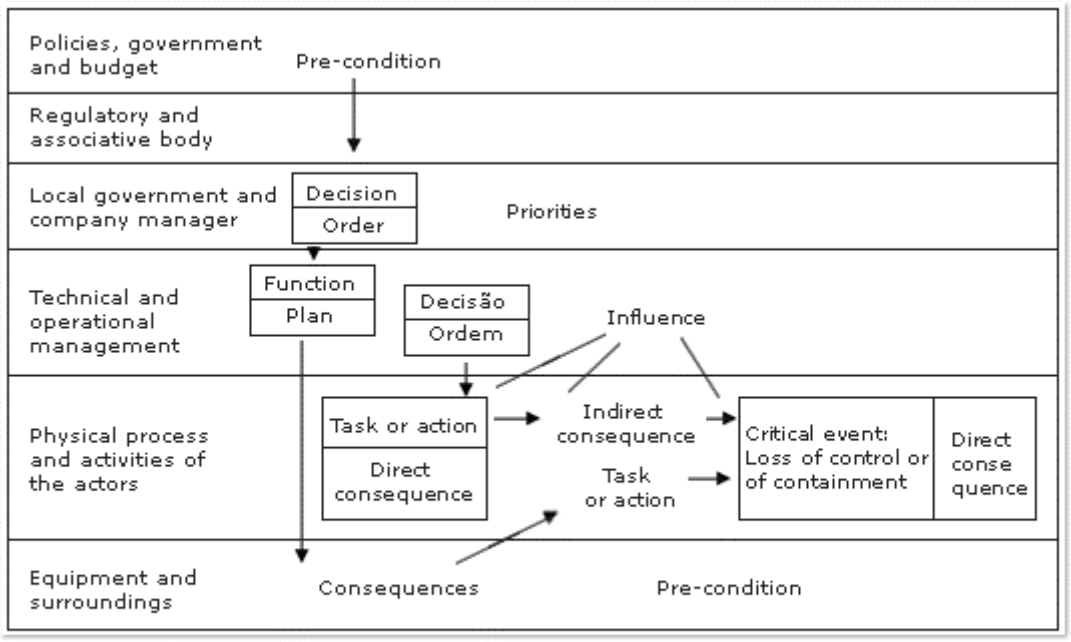

Figure 4: Structure of an accident map (AcciMap)
Adapted from Rasmussen & Svedung 2000

Leveson's (2004) model associates Table 1, which shows the taxonomy of possible failures in the design, execution or feedback of the various loops analyzed.

Using these models demands abandoning the *traditional approach* adopted in safety management, which is based on the structural decomposition of the system, with analyses of tasks focused on action sequence and occasional deviations, treated as human errors. In its place the *behavior-modeling mechanisms model* in terms of working situation constraints, acceptable performance boundaries and subjective criteria guiding the adaptations to the changes should be adopted (RASMUSSEN, 1997).

As the variability and the adaptations they demand are continuous, "human error" begins to be seen as an attempt at adaptation that did not achieve the desired success, but whose result is immediately assumed as "input", or a sign necessary for the diagnosis of the current state of the system and the decisions that will culminate in a new attempt at adaptation. In the words of Amalberti (1996) the error is part of the "*negotiation or cognitive commitment*" developed during the management of the activities.

1) Inadequate nature of the enforcement of constraints for implementing control actions:
1.1) Unidentified hazards.
1.2) Loss, ineffectiveness or inadequacy of the control actions for the hazards identified.
1.2.1) Design of the control algorithm (process) does not enforce constraints. Failures in the creation process. Process change without the corresponding change in the control algorithm (asynchrony of evolutions). Modification or incorrect adaptation.
1.2.2) Model of inconsistent, incomplete or incorrect process ("lack of linkup"). Failures in the creation process.
Failures in up-dating process (asynchronous evolution). Time lags or measurement inaccuracies not accounted for.
1.2.3) Inadequate coordination between controllers and decision-makers (boundary areas between activities and co-activities).

2) Inadequate execution of control actions:
2.1) Communication break-down
2.2) Inadequate "actuator" operation (technical device or person responsible for action conformity after auctioning the specific commands)
2.3) Time lags

3) Loss of or inadequate feedback:
3.1) Not included in the system design
3.2) Communication break-down
3.3) Time lags
3.4) Inadequate sensor operation (incorrect or no information supplied).

Table 1 - Classification of control action failures, according to Leveson.

An aspect to be highlighted in this *behavior-modeling mechanisms approach* is its similarity to the situated behavior focus, adopted in Activity Ergonomics. The reasons associated to the origins the lack of success of certain attempts at adaptation must be looked for in the constraints – or lack of them – that model the behaviors of individuals and organizations, considering the existence of pressures that demand local adaptations on the part of operators. In addition, Table 1 is a guide to the systematization of aspects of the analysis.

Vertical models suggest new questions to those interested in OHSMS:

a) How are managers and intermediate heads responsible for strategic and daily decisions and who contribute, directly or indirectly to the origins of accidents, approached, if indeed they are, in the analysis processes of these accidents?

b) How is the eventual contribution of actors outside the walls of the system-company approached in the analysis of accidents in your organization?

FINAL CONSIDERATIONS

In the United Kingdom, recent reports of the analyses of accidents involving slipping and falls, work-related maintenance accidents, traffic accidents, accidents with workers in the health sector and others, carried out by teams of technicians from the Health and Safety Executive (HSE), a body equivalent to Brazil's Ministry of Labor and Employment, show that the use of concepts like those presented in this text are not restricted to university researchers and the safety teams of major companies operating in the most dynamic and powerful sectors of the economy.

Accident analyses are beginning to be recognized as professional practices that qualify those that conduct them as valid spokespersons of all the other actors in the system. They begin to reveal paths along which aspects of the organization and functioning of the system become potentially accidentogenic.

This text tries to show that these aspects can no longer be confused with examples of strange practices, developed by a few researchers who dedicate themselves to studying accidents as "laboratory phenomena". On the contrary, it shows that the incorporation of concepts such as those presented here is growing in the practices of companies and public institutions. This movement is associated to the perception that those interested in the prevention of work-related accidents have a lot to learn from the experience developed in systems that have achieved safety performances recognized as good, "highly reliable" or "ultra-safe", in the light of current knowledge. In other words, those interested in the prevention of adverse events in hospitals, for example, need to learn from the experience of commercial aviation from various countries in the world - and so on and so forth.

However, the perception of this change will not let us ignore that this does not seem to be the path followed in the majority of systems. The traditional approach is still resisting. The idea that the majority of accidents arise from human failings persists and the current response of the traditional approach to this old issue assumes the form of "behavioral safety" proposals (HOPKINS, 2006).

The harsh criticisms presented by authors here mentioned of the idea that work-related accidents arise from human errors should not be understood as a negation of the

recognition of the existence of a human or subjective dimension in these events. Very much to the contrary, as the text itself shows, for those interested in the study of the human behaviors in the working situation these authors suggest approaches that are as yet little divulged in Brazil. They also reveal that the mere identification of human actions or omissions that go contrary to the precepts of current norms or rules are no more than effects, consequences, apparent phenomena, whose essence, especially in terms of origins, needs to be researched; in no way whatsoever, must they be reduced to the idea of the product of the conscience of the operator who behaved in that way.

The aims of this text are ambitious; in the first place, to reveal part of the history of this different, alternative way of conceiving work-related accidents and theory analysis; secondly, to encourage those interested in the theme of occupational health and safety management to reflect upon to what extent the paths here indicated may be useful to the organizations in which they operate.

BIBLIOGRAPHIC REFERENCES

ALMEIDA, I. M. Análise de acidentes do trabalho como ferramenta de prevenção. *Revista Cipa*, ano XXVII, n.320, p.22-49, 2006.

ALMEIDA, I. M.; BINDER, M. C. P. Armadilhas cognitivas: o caso das omissões na gênese dos acidentes de trabalho. *Cadernos Saúde Pública*, v.20, n.5, p.1373-8, 2004.

AMALBERTI, R. *La conduite des sistèmes à risques*. Paris: Presses Universitaires de France, 1996. (Collection Le Travail Humain)

HOPKINS, A. What are we to make of safe behaviour programs? *Safety Science*, 2006 (in press). Disponível em www.sciencedirect.com/science/journal. Acesso em: 10 jul. 2006.

JOHNSON, C. W.; ALMEIDA, I. M. An investigation into the loss of the Brazilian Space Programme's Launch Vehicle VLS-1 V03. No prelo (Aceito para publicação em *Safety Science*).

LEVESON, N. G. A new approach to System Safety Engineering. 2002. Disponível em sunnyday.mit.edu. Acesso em: 25 jan. 2005.

LEVESON, N. G. A new accident model for Engineering Safer Systems. *Safety Science*, v.42, p.237-70, 2004. Disponível em sunnyday.mit.edu. Acesso em: 25 jan. 2005.

LLORY, M. *Acidentes industriais*: o custo do silêncio. Rio de Janeiro: Multimais, 1999a.

LLORY, M. *L'accident de la centrale nucléaire de Three Mile Island*. Paris: L'Harmattan, 1999b.

MARAIS, K.; DULAC, N.; LEVESON, N. Beyond normal accidents and high reliability organizations: the need for an alternative approach to safety in complex systems. MIT ESD Symposium, March 2004. Disponível em sunnyday.mit.edu. Acesso em: 20 abr. 2006.

PERROW, C. *Normal accidents. Living with high-risk technologies*. 2.ed. New Jersey: Princeton University Press, 1999a.

PERROW, C. Organizing to reduce the vulnerabilities of complexity. *Journal of Contingencies and Crisis Management*, v.7, n.3, p.150-5, 1999b.

RASMUSSEN, J. Human errors: a taxonomy for describing human malfunctions in industrial installations. *Journal of Occupational Accidents*, v.4, p.311-35, 1982.

RASMUSSEN, J. Risk management in a dynamic society: a modelling problem. *Safety Science*, v.27, n.2/3, p.183-213, 1997.

RASMUSSEN, J.; SVEDUNG, J. *Proactive risk management in a dynamic society*. Karlstad: Räddningsverket/Swedish Rescue Services Agency, 2000.

REASON, J. *Managing the risks of organizational accidents*. Aldershot: Ashgate, 1997.

REASON, J.; HOBBS, A. *Managing maintenance error*. A practical guide. Hampshire: Ashgate, 2003.

SAGAN, S. D. *The limits of safety*. Organizations, accidents, and nuclear weapons. New Jersey: Princeton University Press, 1993. p.250-79.

SVEDUNG, J.; RASMUSSEN, J. Graphic representation of accident scenarios: mapping system structure and the causation of accidents. *Safety Science*, v.40, p.397-417, 2002.

TURNER, B. A.; PIDGEON, N. F. *Man-made disasters*. Oxford: Butterworth Heinemann, 1997.

Article received on 24.08.2006. Approved on 02.10.2006.