Cogn Tech Work (2010) 12:133–142
DOI 10.1007/s10111-010-0146-3

ORIGINAL ARTICLE

Human-error-based design of barriers and analysis of their uses

F. Vanderhaegen

Received: 8 January 2010 / Accepted: 22 February 2010 / Published online: 3 April 2010

Abstract The paper discusses on the concept of human errors when operators use barriers or when barriers have to be designed to decrease risks associated with human behaviours. It gives taxonomies of barriers and of their uses and develops the concept of the human-error-based design of barriers to control human errors. Human error assessment methods are then proposed regarding three dimensions: retrospective analysis methods, prospective analysis methods and on-line analysis methods. A new methodology including these dimensions is proposed to take into account several uses of barriers: normal uses, unintentional erroneous uses, intentional diverted uses and uses of new barriers. In order to achieve the identification of these barrier uses, this approach is based on the comparison between the prescriptive and predictive behaviours for a prospective analysis or between prescriptive and real behaviours for a retrospective analysis to define new barriers or to redesign the existing ones. A management of the learning process of such barrier uses is integrated in order to make this design or redesign processes possible.

Keywords Barrier design · Barrier analysis · Barrier uses · Human-error-based design · Human error · Human error assessment

F. Vanderhaegen (✉)
University of Lille Nord de France, 59000 Lille, France
e-mail: frederic.vanderhaegen@univ-valenciennes.fr

F. Vanderhaegen
UVHC, LAMIH, 59313 Valenciennes, France

F. Vanderhaegen
CNRS, UMR 8530, 59313 Valenciennes, France

1 Introduction

Risk analysis of human-machine systems cannot be done without considering the human factor impact. Moreover, this risk analysis process generally concerns the system designers and is done off-line. On field, the system users have to analyse the risks they are facing to and to control them on-line. Then, they learn from their own errors and behaviours (Amalberti 2001). Generally, these human errors relate to two main aspects of the human behaviour:

- The capacity of human operators not to realize correctly their allocated tasks in given conditions during a period of time or a given time, or
- The capacity of human operators to realize additional tasks that may affect the human-machine system functioning in terms of safety, quality, production, workload, etc.

The identification of such human errors can be done by comparison between:

- The prescribed behaviour (i.e. the behaviour that the human operators are supposed to perform) with the real one (i.e. the real behaviour performed by the human operators), or
- The result expected by the prescribed behaviour with the result obtained by the performed behaviours.

Regarding the prescribed behaviours or their results, erroneous behaviours are unintentional or intentional and may be achieved with or without any intention to damage the system. In order to control such human errors, the designers provide the human-machine system with a set of barriers. Barriers are systems that protect the human-machine system from the occurrence or the consequences of undesirable events that may affect the human-machine

system functioning in terms of criteria such safety, workload, production, quality. Therefore, some of them are designed for controlling human errors.

Hollnagel identifies two ways to improve the design of barriers (Hollnagel 1999):

- The former relates to the accident analysis process to explain the failures of a system and to identify the failures of barriers.
- The latter relates to the system design process to specify barriers capable to protect the system against possible failures.

Human erroneous action modes described in (Hollnagel 1998) is a suitable framework to specify the function of barriers and to identify the conditions to activate them (Hollnagel 1999). Therefore, these barriers aim at protecting the system against human errors.

Nevertheless, barriers can also be the cause of the occurrence of particular human errors such as the removals of barriers or the creations of new barriers that produce added behaviours. Both cases (i.e. barrier creations and barrier removals by human operators on field) are never taken into account in the design process of a human-machine system integrating barrier system.

This paper proposes an answer to this lack of methodology and discusses on the concept of barriers initially inspired by the Hollnagel's research. After presenting the principles of the risk assessment in a human-machine system organization, it introduces the concept of barrier and gives taxonomies of barriers and of their uses. Some human error assessment methods are then proposed to support the design of barriers. A three-dimensional approach is finally presented for the retrospective and prospective analysis of the barriers uses in order to support the design or the redesign of on-line human-error-based barriers.

2 Risks assessment principles

In the domain of risk assessment processes, divergences can be due to the differences between the objectives of each decisional level of an organization from the design of a given machine to its use (Vanderhaegen 2003). For instance, a society that uses this machine can divide the decisional process into several hierarchical levels such as the production directors, the foremen, the team leaders, the teams of works and the human operators or users. Operational risk, i.e. the risks related to the system use, can evolve from a quantitative or objective assessment to a qualitative or subjective one. Other risks such as organizational ones, i.e. the risks related to the work management, can evolve from a strategic or long-term viewpoint to a tactical or short-term one.

The assessment of these risks concerns different sources and sometimes can diverge (Table 1):

- For the designers, the objective of risk analysis is usually limited to a quantitative assessment of risk on safety. This evaluation is a mono-criterion and an off-line process. Its validation stops evolving when the machine is on field operation and is quite stable because it concerns a common decision. Nevertheless, this process of risk evaluation is external because it is usually made independently of the users and focuses on the factors related safety non-conformity events in order to define tools such as barriers or user manual.
- The society that installs and operates this machine has to demonstrate the on-field safety conformity. It is an off-line and external process focusing only on the safety criterion. Its validation and its integrity are not constant because it can take into account data from feedback of experience that may change initial prescriptions, adding barriers or improving training.
- Regarding the users, the risk analysis rather relates to a multi-criterion and an on-line risk control process. Users have to control risks associated with operational situations evaluating them after their detection and intervening on the piloted process to avoid the occurrence or limited the consequences of a given event. This control is multi-criterion because it takes into account not only the system safety but also economical criteria such as production or quality or social criteria such as motivation or workload. Depending on the variability of the operational situations to be controlled and on the inter-individual and intra-individual differences, the risk control process is dynamic and variable. Moreover, it can concern all factors related to whatever field events and can support the definition of new individual or collective barriers, the increase in the learning on the system behaviour, the improvement of the human competences.

The main and joint output of these risk assessment processes is the design of barriers. The concept of serial defenses or defenses in depth to control system safety is usually guaranteed by barriers. It consists in designing several barriers for controlling the same events. Different barriers can then be specified from the design of a machine to its use in order to control the same unsafe events.

3 The design of barriers

Hollnagel (1999) defines a barrier as an obstacle, an obstruction or a hindrance that may either (1) prevent an action from being carried out or a situation to occur, or (2) prevent or lessen the severity of negative consequences.

Table 1 Risks analysis process of the designers, the employers and the users of a human-machine system

Actors	Designers	Employers	Users
Objective	Risk evaluation	Conformity assessment	Risk control
Criterion	Mono-criterion	Mono-criterion	Multi-criterion
Processing	Off-line	Off-line	On-line
Validation	Static	Dynamic	Dynamic
Integrity	Stable	Variable	Variable
Source	External	External	Cognitive
Content	Factors related to unsafe events	Factors related to unsafe events	Factors related to multi-criteria-based events
Output	Barriers	Barriers	Personal barriers
		Training	Learning process
		Reorganization	Experience

The design of a barrier requires the definition of three characteristics (Hollnagel 2004):

- Its objective, i.e. a barrier is designed for prevention or protection.
- Its function, i.e. the condition of activation of the barrier in order to achieve its goal.
- Its integration into the defence in-depth process taking into account the system organization and its structure.

A barrier is then a technical or human support that protects the human-machine system against the occurrence or the consequences of undesirable events. These events may affect criteria such as safety, workload, production or quality. Facing an undesirable event affecting these criteria, three levels of barriers may be designed: barriers of prevention, barriers of correction and barrier of containment (Fig. 1). Barriers of prevention and correction aim at avoiding the occurrence of an unwanted event such as an accident, and the barriers of containment focus on the limitation or the control of the consequences of this accident or on the avoidance of the over-accident to protect the others. Prevention process relates to supports for anticipating events. Correction process consists in defining supports for recovering, interrupting or stopping events. Containment process aims at protecting the system, evacuating people or material, mitigating or diverting the consequences of the unrecoverable events or at avoiding the occurrence of other undesirable and unrecoverable events such as over-accidents.

The avoidance or the control of accidents involves several actions for facilitating the design of barriers (Hollnagel 2004, 2008): the identification of the types of the accidents that may occur, the identification of the location of these accidents onto the global system, the identification of the causes of their occurrence, the identification of the conditions of their occurrence, the identification of the human contributions to their occurrence. Barriers are mainly used as means to prevent the unwanted events such as accidents from reappearing again (Hollnagel 2008).

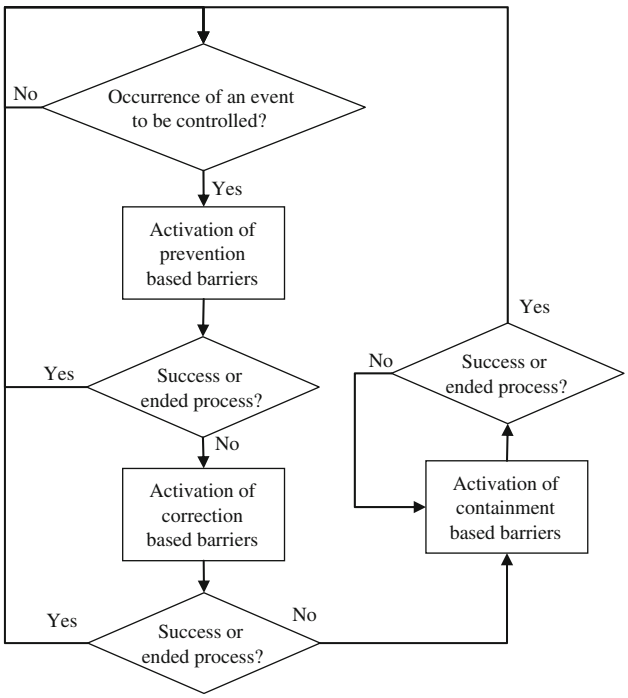

Fig. 1 Barriers of prevention, of correction and of containment

Undesirable events can be human errors. In order to protect a system from potentially unsafe human behaviour, barriers are necessary. Four barrier classes can be distinguished (Hollnagel 1999, 2008):

- Material barriers (such as walls or doors) that physically prevent an action or limit the negative consequences of a given operation,
- Functional barriers (such as keys to open doors) that logically or temporally link actions and operational situations,
- Symbolic barriers (such as signals or panels) that require interpretation to be applied, and
- Immaterial or incorporeal barriers (such as rules or norms) that are not physically present on the work place but that the human operators are supposed to know.

A barrier can belong to more than one of these classes. A barrier is characterized by its source, i.e. who is the designer of the barrier, and its target, i.e. who will use this barrier. Three levels of barrier design process can be defined (Table 2). The designers of a given machine equip it with barriers with respect to the norms or risk analysis results. The employer who installs and operates this machine on an industrial site defines other barriers on field with respect to the implantation environment. Finally, the human operators who use this machine may modify some existing barriers or create new ones. The choice of the barriers of the first level (i.e. the designers of a machine) is the result of a risk analysis process. At the second level (i.e. the society that instals and operates the machine), additional barriers are linked to the operational conformity to be followed. However, the possible behaviours of human operators on field who face technical barriers or who are considered as barriers or who are designing their own barriers are not formally assessed.

Among functional barriers, there are supports based on the technical redundancy principle and on the human-machine cooperation one (Vanderhaegen 2003). The redundancy principle involves redundant and non-interactive systems: when a system failed, a task is allocated to another reliable system. The human-machine cooperation principle involves redundant and interactive system: tasks can be then shared dynamically among different cooperative decision-makers.

Three levels of cooperation can be implemented for solving problems facing undesirable events to be controlled (Jouglet et al. 2003; Millot and Vanderhaegen 2008):

- Pre-action-based supports provide human operators who act alone on the process with advices.
- Post-action-based supports aim at recovering possible human errors after human actions.
- Regulation-based supports concern barriers operating during action. This requires an organization in which the assistant support system and the human operator are on the same decisional level. Control and supervisory tasks can then be distributed between human and machine in order to relieve human operator of underloaded or overloaded situations. This aims at both reducing the risk of human error and regulating workload.

In fact, two groups of barriers might then be considered (Polet et al., 2002):

- Barrier affecting the system integrity if they are removed. There are physical barriers: if they are removed or not respected, the system is physically modified.
- Barrier unrelated to the system integrity if they are removed. There are symbolic or immaterial barriers: if they are removed or not respected, the system is not modified physically.

Vanderhaegen and Petersen (2007) defined barrier removals as a gap between the so-called intentional barriers and apparent barriers:

- Intentional barriers are barriers that are designed for pre-defined objectives.
- Apparent barriers are barriers that are really perceived and used by the human operators on field.

The design of intentional barriers requires an analysis of their uses integrating:

- The assessment of the possible perception of these barriers by human operators on field, identifying the risks associated with a degraded perception of the interest of intentional barriers.
- The assessment of the system integrity with and without barrier removals, identifying the compromises between different evaluation criteria.

Several reasons can facilitate the removing of barriers. An error of design of the barriers implemented on field can lead to the misuses of the system (Foot and Doniol-Shaw 2008).

Table 2 Examples of barriers defined by the designers, the employers and the users of a human-machine system

	Material	Functional	Symbolic	Immaterial
Designer	Electrical box	Detection sensors, interlocking system, remote control system, redundancy	Signalling support	Users manual
	Isolation		Visual and sound support	Training program
			Labelling on working tools	
Employer	Emergency exits	Fire detection and control system	Safety rule panels	Internal training
	Individual protection means	Support tools	Ground signalling or indicators	Internal procedures and rules
		Functional access area limitation		
Team	Physical access limitation	Task and responsibility allocation	Gestural, sound or verbal communication	Report
		Cooperation		Advices during relief
			Collective notice board	
Individual	Physical organization of the workplace	Personal access area definition	Personal notice boards	Personal notes and rules

Regarding the constraints of a given organization, a lack of degree of liberty when applying procedures can encourage the users to modify these procedures in order to make them more flexible and applicable (Grote et al. 2009). Other reasons can lead to the removing of barriers (Vanderhaegen and Petersen 2007):

- Barriers are removed because they failed.
- Barriers are removed because they are temporarily or permanently unsuitable.
- Barriers are misused because of insufficient experience of human operators.
- Barriers are removed because some operations such as maintenance operations require their removal.

Intentional deviation from the prescribed behaviour required by the system specifications is called a violation (Reason 1990). A so-called barrier removal was initially defined as the voluntary barrier inhibition with the intention to optimize the possible compromises between criteria such as safety, workload, production, quality (Polet et al. 2003). Thus, a barrier removal, or an intentional misuse or non-respect of a barrier under appropriate conditions, is an optimizing or exceptional violation made without any intention to damage the human-machine system. Barriers can then be removed in different ways such as:

- The barriers are deactivated temporarily or permanently.
- The structure or the function of barriers is modified temporarily or permanently, totally or partially.
- The barriers are removed by one human operator or by a group of human operators.
- The barriers are removed intentionally or unintentionally.
- The barriers are removed with or without coordination between human operators or between groups of human operators (e.g. people on maintenance and people on operation).

Finally, the risk assessment process done at the design level of a system aims at solving unacceptable scenarios involving human errors for instance and transform them into acceptable ones by integrating new barriers to control unsafe events generated by human operators. Several methods can be used to facilitate the design of such human error tolerant barriers.

4 Human-error-based design of barriers

4.1 Synthesis of human error analysis to design barriers

Several methods are useful to support the design of human errors centred barrier. They are based on on-line analysis to activate or deactivate real-time barriers, on prospective analysis to design barriers and on retrospective analysis to redesign barriers or verify their efficiency regarding safety or performance indicators (Table 3).

4.2 On-line analysis

Some authors defended the hypothesis related to the fact that an high level or a low level of workload increases the risk of human error occurrence, and decreases the system performance (Weiner et al. 1984; Chignell and Hancock 1985; De Waard 1996). Indeed, low human workload generates a decrease in the human vigilance and increases the risk of human error (Popieul et al. 2002) and high workload provokes an increase in the risk of erroneous perception and action (Vanderhaegen et al. 1994). Therefore, the use of workload assessment methods is useful for activating or deactivating barriers such as decision support systems regarding the dynamic context of work (Vanderhaegen 1999a). They are methods such as:

- Subjective workload assessment methods such as TLX, Task Load Index (Hart and Stavelang 1988) or SWAT, Subjective Workload Assessment Technique (Reid and Nygren 1988).
- Objective workload assessment methods such as those implemented into the SPECTRA project (French acronym for Experimental Platform to Share Tasks between Human and Machine in Air Traffic Control). For instance, there are methods based on a functional task demand estimator to assess the complexity of a global situation (Vanderhaegen et al. 1994) or methods based on a temporal task demand estimator to assess the possible saturation of the human processor (Vanderhaegen 1999b).

Subjective assessment of workload is sometimes affected by erroneous perception of the tasks allocated to human operators, and the correlations between both subjective and objective assessment methods may then be wrong. Nevertheless, indicators on human workload or task demand are useful to manage the activation or the deactivation of barriers in order to optimize the performance and the safety of the human-machine system. These barriers based on human workload or task demands aim at preventing or at recovering human errors that may degrade the system performance or safety.

Prospective methods are other ways to support the design of barriers. They are based on human error prediction.

4.3 Prospective analysis

The classical Fault Tree method can be helpful to identify the contribution of human error to the occurrence of an incident or an accident or to identify the events that may

Table 3 Analysis for human-error-based barriers

Example	Principle	Objective
On-line analysis for barrier activation or deactivation		
TLX, SWAT	Subjective assessment	Workload analysis
SPECTRA	Objective assessment	Task demand and allocation analysis
Prospective analysis for barrier design regarding system performance objective		
Fault Tree	Scenario occurrence probability	Undesirable event analysis
THERP, SLIM	Error occurrence probability	Quantitative error analysis
GEMS, CREAM	Cognitive model	Cognitive error analysis
DYLAM, HITLINE	Human behaviour simulation	Safety behavioural analysis
ACIH-APRECIH	Benefit/Cost/Deficit model	Consequences analysis
Retrospective analysis for barrier design regarding system performance assessment		
Injury, breakdown	Counters	Statistical analysis
Human error rates	Ratios	Comparative analysis
HERMES, HERA	Functional model	Accident and incident analysis
ACIH-APOSCIH	Benefit/Cost/Deficit model	Consequences analysis

provoke the human error occurrence and to access its probability. The design of barriers is done to reduce the probability of this human error occurrence. Some approaches to predict human errors are quantitative methods such as THERP, Technique for Human Error Rate Prediction (Swain and Guttmann 1983; Zio et al. 2009) or SLIM, Success Likelihood Index Method (Embrey et al. 1984; Khan et al. 2006; Park and Lee 2008). They are based on mathematical model to assess the probability of success or failure of a given behaviour combined with the impact of factors that may affect the performance of this behaviour. Nevertheless, the results of such methods are not homogeneous. Studies have shown that a given method used by several groups or different methods used by a same group do not produce reliable results (Kirwan 1997; Reer 2008). This can be due to different reasons (Cépin 2008; Johnson 1999; Vanderhaegen 2001):

- The analysis of the tasks does not integrate all the dependencies between tasks (e.g. temporal dependencies, causal dependencies, functional dependencies).
- The feedback to assess the human error probability is sometimes insufficient.
- Even if probabilities on human error are available, they usually cannot be compared because they do not have homogeneous units of assessment.
- The probability assessments are rarely verified on field regarding retrospective analyses.

Qualitative or cognitive approaches facilitate the prediction of human error. They propose human erroneous actions taxonomies or models such as:

- The Reason's taxonomy (Reason 1990). Unsafe or unoptimal human actions relate to intentional or unintentional behaviour: slips are non-intentional and relate to skills and attention-based failure; lapses are non-intentional and relate to skills and memory-based failures; faults are intentional and relate to rules or knowledge-based failures; violations are intentional and can relate to intentional behaviour such barrier removal with or without the intention to damage the human-machine system.
- The Hollnagel's taxonomy (Hollnagel 1998). This describes erroneous actions by different parameters called phenotypes that are causes by genotypes, i.e. individual, systemic or environmental causes. These parameters concern the erroneous actions characteristics such as goal, sequence, duration.

These taxonomies are useful to define the objectives of the barriers to be implemented. However, the associated human behavioural model they used is sometimes difficult to apply and their interpretation can be ambiguous (Johnson 1999; De Keyser 2001).

Other methods such as DYLAM (Cacciabue 1998) or HITLINE (Macwan and Mosleh 1994) complete the quantitative and qualitative methods by simulating the whole human-machine system behaviour facing predefined undesirable events. They require sufficient realistic models of human behaviour, process behaviour and the interface behaviour. The more complex a human-machine system is, the more difficult the simulation and the definition of barriers are.

All these prospective analysis methods focus mainly on the analysis of non-intentional errors without taking into account intentional errors such as violations or additional behaviours. The ACIH method (French acronym for Analysis of Consequences of Human Unreliability) assesses the

consequences of human errors such as violations or barrier removals (Vanderhaegen 2003). The APRECIH (French acronym for Prospective Analysis of the Consequences of Human Unreliability) is the module of ACIH that compares the prescribed behaviours with the anticipated possible ones (Vanderhaegen 1999c). Extension of the ACIH method aims at using the multi-criteria-based framework of the so-called Benefits/Costs/Deficit model (BCD model) in order to assess the consequences in terms of benefits and costs in case of the success of the erroneous behaviour and of potential deficits or dangers in case of its failures (Vanderhaegen 2003, 2004). Different criteria such as safety, quality, production or workload can be used for assessing such consequences.

These prospective analyses to design barriers might be completed by using retrospective ones in order to verify the efficiency of the barriers.

4.4 Retrospective analysis

Among the approaches to assess retrospectively, the human error and the efficiency of the associated barriers, several ratios or counters are useful (Vanderhaegen et al. 2004). They are indicators such as:

- The number of injuries or system breakdown after an incident or accident.
- The number of human errors upon the opportunity for errors. Criteria of opportunity have then to be defined.
- If the criterion of opportunity relates to the solicitation of a given task, this ratio is the number of incorrect tasks upon the total number of solicitations of the task. This assesses the number of erroneous tasks per solicitation.
- This probability can also be the number of human errors upon an interval of time. This aims at assessing a number of human errors per time unit.

Other methods such as HERA, Human Error in European Air Traffic Management (Isaac et al. 2002) or HERMES, Human Error Risk Management for Engineering System (Cacciabue 2005) are framework for the analysis the impact of human errors on the occurrence of organizational dysfunctions and for the design of database on incidents and accidents. The retrospective approach of the ACIH method is called the APOSCIH, a French acronym for Retrospective Analysis of the Consequences of Human Unreliability (Vanderhaegen 2001). It compares the prescribed behaviours with the observed ones and interprets differences in terms of consequences.

The application of these retrospective analysis methods to design barriers or to verify their efficiency requires the recording and the analysis of an important number of data that are not always available or observable and that are not entirely identified. Moreover, the results of these analyses focus mainly on the negative contributions of the human operators without taking into account the possible positive ones, i.e. without considering the possibility for the human operators to become a barrier for the system safety or performance by avoiding or recovering an incident or an accident. The design of barriers requires the integration of the management of this degree of liberty of human actions in order to make this avoidance or recovering process possible at any time, or to support this process by specific barriers.

Finally, the process of human error analysis is much more limited to a retrospective one than a prospective one. Instead of focusing on the incident or accident prevention, the investigation effort related to human errors is done after the occurrence of a danger, an incident or an accident due to human factors, i.e. when the barriers and/or the human operators failed.

These methods do not take into account all the possible behavioural alternatives the human operators have when they are facing barriers. The following section is an extension of the ACIH approach that aims at taking into account several uses of barriers retrospectively or prospectively and to manage the knowledge on the consequences of theses uses or misuses of existing barriers or on the consequences of possible new barriers created by users on field.

5 Toward an analysis method of possible uses, misuses or creations of barriers

The new ACIH methodology for the design of barriers aims at supporting the management of the negative and positive consequences of human behaviours such as human errors or violations. It is a three-dimensional view of the human-error-based design of barriers (Fig. 2):

- A prospective step to compare prescribed behaviours with the possible ones via a prediction model of behaviour.
- A retrospective step to compare the prescribed behaviour with the observed ones.
- A redesign step to validate the current barrier system, to modify it or to specify new barriers.

Regarding the system objective, the constraints and the initial list of barriers, the analysis related to the system structure and functions is done, and then the analysis of the human tasks involved in the achievement of the system functions aims at identifying the operational contexts and the required procedures. The contextual and procedural analysis identified the tasks the human operators are supposed to achieve. Within these human tasks, possible human errors are identified, and their consequences are assessed. Several categories of barrier use are taken into

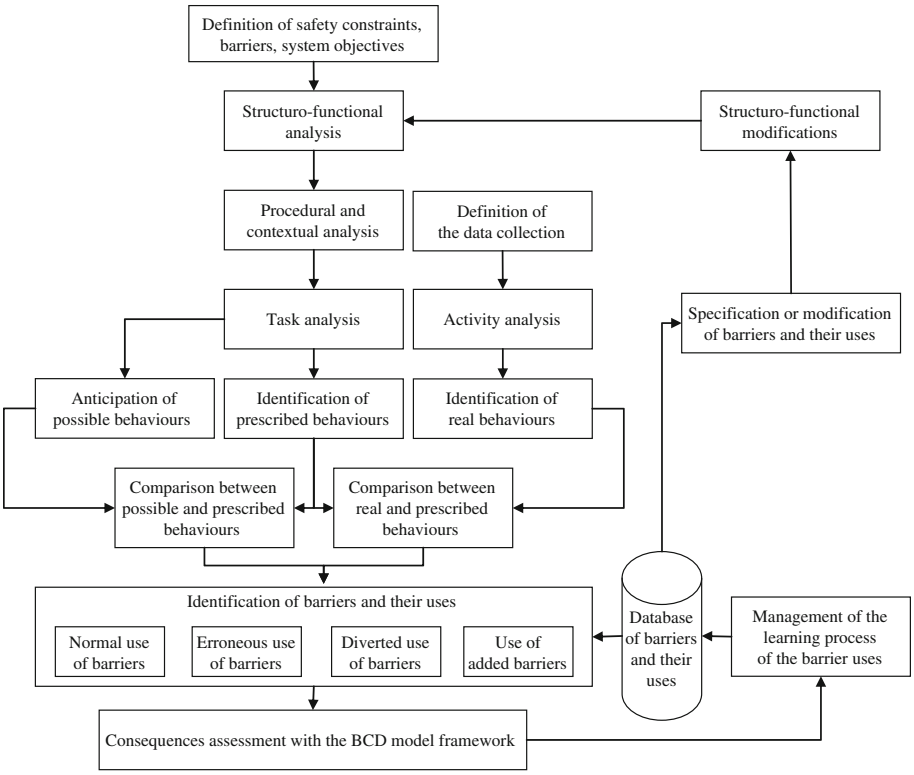

Fig. 2 The three-dimensional ACIH methodology

account: the normal uses of barriers, the unintentional erroneous uses of barriers, the intentional diverted uses of barriers and the uses of new barriers created by human operators.

The possible motivation for a human operator to divert intentionally from a given prescription can relate to the improvement of the human-machine system behaviour or consequences. This improvement can be assessed quantitatively or qualitatively regarding several criteria. As mentioned earlier, the BCD model is based on indicators that assess the positive and the negative consequences of human behaviours on several criteria related to technical or human performance or state. Positive ones are benefits, whereas negative ones are acceptable costs when the undesirable events are under control or are unacceptable deficits when they are over control. In other words, a cost is an acceptable negative consequence when the human behaviour is successful and a deficit is an unacceptable consequence when this behaviour fails and damages the human-machine system regarding the safety or other criteria. Therefore, whatever the barrier use states due to human behaviours (i.e. normal, erroneous, diverted or added use of barriers), the corresponding human action occurrence is supposed to be valuable by three distinct consequences on several evaluation criteria (Polet et al. 2002, 2009; Vanderhaegen 2004):

- The expected benefits (i.e. the B values of the BCD model) due to the success of the performed action.
- The acceptable costs (i.e. the C values of the BCD model) due to the success of the performed action. It can relate to a cognitive cost to control the potential deficit or danger or to a physical one to modify the operational constraints of the use of a given system such a barrier.
- The unacceptable possible deficits or dangers (i.e. the D values of the BCD model) related to the potential occurrence of a hazardous situation, in case of an unsuccessful action.

A human behaviour can be then explained in terms of benefits and costs when it is a success or in terms of deficits or dangers when it fails. For an on-line intentional human behaviour under control, the benefits and costs are considered as quasi-immediate, whereas the deficits are potential. Indicators are then required to compare dependent or independent situations (Vanderhaegen 2004). Two situations are dependent when the state of a situation occurring at a given time is modified and leads to another short or long-term situation. This modification can be due to the dynamic evolution of the process or to a strategic or tactical action. Two situations are independent when they can occur at the same time but concern two different paths to achieve same goals. Independent situations can then relate to the

possible action plans of different decisional levels of a given organization to solve a current situation. Different actions plans or procedures, i.e. different series of successive dependent situations due to human actions, can then be compared. Whatever the hierarchical level, the BCD model is able to take into account qualitative and subjective data or quantitative and objective ones using several functions.

The third dimension of this new ACIH methodology consists in developing databases and systems capable to learn from barrier uses interpreted in terms of the BCD model framework. A database is then required to record all the formatted data related to the barriers and their uses and to design or redesign the current barrier system. A redesign of the existing barriers or the specification of new barriers requires the modifications of the initial function allocation or the structure of the human-machine system.

Several studies have been done for the prospective and retrospective analyses of particular diverted uses of barriers, i.e. the intentional removal of barriers. There are studies such as:

- The retrospective analysis of barrier removals during the use of production system such as industrial rotary press (Polet et al. 2002, 2003).
- The retrospective analysis of barrier removal during the control of a simulated railway system (Polet et al. 2009).
- The use of such retrospective analysis to build a database on railway barriers and their uses and to predict railway barrier removals for prospective analysis (Zhang et al. 2004; Vanderhaegen et al. 2008).
- The prospective analysis of possible railway procedure removals (Chaali-Djelassi et al. 2007).

Other studies are required for a complete application of this three-dimensional ACIH methodology in order to extend the analysis of barriers and their uses and to take into account other uses such as:

- The unintentional erroneous uses of barriers.
- The intentional diverted uses of barriers such as the uses of failed barriers or the misuses of unadapted barriers.
- The uses of new barriers.
- The normal uses of barriers in order to identify the optimal ones.

6 Conclusion

This paper introduces a new methodology for the human-error-based design of barrier systems. Several uses of barriers are analysed prospectively or retrospectively. The results of these analyses aim at managing a database of barriers and their uses in order to redesign the barriers or to design new ones. The BCD model is applied as a framework for formatting the positive and negative consequences of human behaviours facing barriers. Different uses are identified and analysed: the normal uses of barriers, the unintentional erroneous uses of barriers, the intentional diverted uses of barriers and the uses of new barriers. As the human error assessment methods presented on this paper do not take into account the dynamic evolution of the human-machine system, e.g. the learning effect and the evolution of human knowledge and behaviours, this new approach includes a management module of the learning process from the barrier uses.

Future studies will apply such a concept in order to implement into intelligent barriers the capacity to learn from their uses and to control possible additional risks due to erroneous or diverted uses of current barriers. Due to limited capacity of this new possible generation of barriers, dynamic task allocation between barriers and human operators to control situations might be developed. One of the possible solutions consists in providing human operator with barriers capable to cooperate with them and to learn from human-machine interactions between barriers and human operators (Zieba et al. 2009). The use of human operators as barriers for the system safety or performance will also be studied in order to adapt the proposed human-error-based design approach into a human-centred design one.

Other future studies will aim at comparing cooperation and competition activities and at designing barriers to support these activities (Vanderhaegen et al. 2006). The BCD model will be then a good support for analysing the sources and the target of a given action, i.e. the actors of a given action and the possible allocations of the consequences of this action to the same actors or other actors. Organizational barriers involving several decision-makers or several groups of decision-makers will be then studied and criteria such as safety and security will be applied.

Acknowledgments The present research work has been supported by the International Campus on Safety and Intermodality in Transportation the European Community, the Délégation Régionale à la Recherche et à la Technologie, the Ministère de l'Enseignement Supérieur et de la Recherche, the Région Nord Pas de Calais and the Centre National de la Recherche Scientifique, the Scientific Research Group on Supervisory, Safety and Security of Complex Systems, the European Research Group on Human-Machine Systems in Transportation: the authors gratefully acknowledge the support of these institutions.

References

Amalberti R (2001) The paradoxes of almost totally safe transportation systems. Saf Sci 37(2–3):109–126

Cacciabue PC (1998) Modelling and simulation of human behaviour in system control. Springer, London
Cacciabue PC (2005) Human error risk management methodology for safety audit of a large railway organisation. Appl Ergon 36:709–718
Cépin M (2008) DEPEND-HRA a method for consideration of dependency in human reliability analysis. Reliab Eng Syst Saf 93:1452–1460
Chaali-Djelassi A, Vanderhaegen F, Cacciabue PC, Cassani M (2007) Barrier removal prediction based on a new approach—application to a degraded train speed procedure. Proceedings of the 26th European annual conference on human decision making and manual control, 20–22 June 2007, Copenhagen, Denmark
Chignell M, Hancock P (1985) Knowledge-based load levelling and task allocation in human-machine systems. Proc Annu Conf Man Control 21:9.1–9.11
De Keyser V (2001) Incident report system. In: Amalberti R, Fuchs C, Gilbert C (eds) Around risk assessment: a pluridisciplinary question. Publications de la MSH-ALPES, Grenoble, pp 41–71
De Waard D (1996) The measurement of drivers' mental workload. Ph.D. thesis. University of Groningen, Traffic Research Centre, Haren
Embrey DE, Humphreys PC, Rosa EA, Kirwan B, Rea K (1984) SLIM-MAUD: an approach to assessing human error probabilities using structured expert judgment. Report NUREG/CR-3518, BNL-NUREG-51716. Department of Nuclear Energy, Brookhaven National Lab, Upton, NY
Foot R, Doniol-Shaw G (2008) Questions raised on the design of the "dead-man" device installed on trams. Cogn Technol Work 10:41–51
Grote G, Weichbrodt JC, Günter H, Zala-Mezö E, Künzle B (2009) Coordination on high-risk organizations: the need for flexible routines. Cogn Technol Work 11:17–27
Hart SG, Stavelang LE (1988) Development of NASA-TLX (Task Load Index): results of empirical and theoretical research. Adv Psychol 52:139–183
Hollnagel E (1998) Cognitive reliability and error analysis method CREAM. Amsterdam, Elsevier
Hollnagel E (1999) Accident and barriers. 7th European conference on cognitive science approaches to process control. Villeneuve d'Ascq, France, pp 175–180
Hollnagel E (2004) Barriers and accident prevention. Ashgate Publishung Limited, Hampshare
Hollnagel E (2008) Safety + Barriers = Safety? Saf Sci 46:221–229
Isaac A, Shorrock ST, Kirwan B (2002) Human error in European air traffic management: the HERA project. Reliab Eng Saf Syst 75:257–272
Johnson C (1999) Why human error modelling has failed to help system development. Interact Comput 11:517–524
Jouglet D, Piechowiak S, Vanderhaegen F (2003) A shared workspace to support man-machine reasoning: application to cooperative distant diagnosis. Cogn Technol Work 5:127–139
Khan FI, Amyotte PR, DiMattia DG (2006) HEPI: a new tool for human error probability calculation for offshore operation. Saf Sci 44:313–334
Kirwan B (1997) Validation of human reliability assessment techniques: part2—validation results. Saf Sci 27:43–75
Macwan A, Mosleh A (1994) A methodology for modelling operators errors of commission in probabilistic risk assessment. Reliab Eng Syst Saf 45:139–157
Millot P, Vanderhaegen F (2008) Toward cooperative and human error-tolerant systems. Proceedings of the 17th IFAC World Congress, 6-11 June 2008, Seoul, Korea
Park KS, Lee J (2008) A new method for estimating human error probabilities: AHP-SLIM. Reliab Eng Syst Saf 93:578–587
Polet P, Vanderhaegen F, Wieringa PA (2002) Theory of safety-related violations of system barriers. Cogn Technol Work 4:171–179
Polet P, Vanderhaegen F, Amalberti R (2003) Modelling border-line tolerated conditions of use (BTCUs) and associated risks. Saf Sci 41:111–136
Polet P, Vanderhaegen F, Millot P (2009) Human behaviour analysis of barrier deviation using the benefit-cost-deficit model. Advances in human-computer interaction. Available on http://downloads.indawi.com/journals/ahci/2009/642929.pdf
Popieul JC, Simon P, Loslever P (2002) Using failure detection and diagnosis methods to detect dangerous evolution of the driver behaviour. Control Eng Pract 10:577–583
Reason J (1990) Human error. Cambridge University Press, Cambridge
Reer B (2008) Review of advanced in human reliability analysis of errors of commission—part 2: EOC quantification. Reliab Eng Syst Saf 93:1105–1122
Reid GB, Nygren TE (1988) The subjective workload assessment technique: a scaling procedure for measuring metal workload. Adv Psychol 52:185–218
Swain AD, Guttmann HE (1983) Handbook of reliability analysis with emphasis on nuclear plant applications. Nuclear regulatory commission, NUREG/CR-1278, Washington DC
Vanderhaegen F (1999a) Toward a model of unreliability to study error prevention supports. Interact Comput 11:575–595
Vanderhaegen F (1999b) Multilevel allocation modes—allocator control policies to share tasks between human and computer. Syst Anal Modell Simul 35:191–213
Vanderhaegen F (1999c) APRECIH: a human unreliability analysis method—application to railway system. Control Eng Pract 7:1395–1403
Vanderhaegen F (2001) A non-probabilistic prospective and retrospective human reliability analysis method–application to railway system. Reliab Eng Syst Saf 71:1–13
Vanderhaegen F (2003) Analyse et contrôle de l'erreur humaine (Analysis and control of human error). Lavoisier—Hermès Science Publications, Paris
Vanderhaegen F (2004) The benefit-cost-deficit (BCD) model for human analysis and control. Proceedings of the 9th IFAC/IFORS/IEA symposium on analysis, design, and evaluation of human-machine systems, Atlanta, GA, USA, 7–9 Sept 2004
Vanderhaegen F, Petersen J (2007) Barriers at work. Proceedings of the 10th IFAC/IFIP/IFORSD/IEA symposium on analysis, design, and evaluation of human-machine systems
Vanderhaegen F, Crévits I, Debernard S, Millot P (1994) Human-machine cooperation: toward an activity regulation assistance for different air traffic control levels. Int J Hum Comput Interact 6(1):65–104
Vanderhaegen F, Jouglet D, Piechowiak S (2004) Human-reliability analysis of diagnosis support cooperative redundancy. IEEE Trans Reliab 53(4):458–464
Vanderhaegen F, Chalmé S, Anceaux F, Millot P (2006) Principles of cooperation and competition—application to car driver behavior analysis. Cogn Technol Work 8(3):183–192
Vanderhaegen F, Ziéba S, Polet P (2008) A reinforced iterative formalism to learn from human errors and uncertainty. Eng Appl Artif Intell 22:654–659
Weiner EL, Curry RE, Faustina ML (1984) Vigilance and task load: in search of the inverted U. Hum Factors 26(2):215–222
Zhang Z, Polet P, Vanderhaegen F, Millo P (2004) Artificial neural network for violation analysis. Reliab Eng Syst Saf 84(1):3–18
Zieba S, Polet P, Vanderhaegen F, Debernard S (2009) Resilience of a human-robot system using adjustable autonomy and human-robot collaborative control. Int J Adapt Innov Syst 1(1):13–29
Zio E, Baraldi P, Librizzi M, Podofillini L, Dang VN (2009) A fuzzy set-based approach for modelling dependence among human errors. Fuzzy Sets Syst 160:1947–1964