Cognition, Technology & Work (2002) 4:171–179

Cognition
Technology &
Work

Theory of Safety-Related Violations of System Barriers

P. Polet[1], F. Vanderhaegen[1] and P. A. Wieringa[2]

[1]Laboratoire d'Automatique et de Mécanique Industrielles et Humaines, Université de Valenciennes et du Hainaut-Cambrésis, Valenciennes, France; [2]Man–Machine Systems, Faculty of Design and Engineering, Delft University of Technology, Delft, The Netherlands

Abstract: This paper focuses on a theory of the safety-related violations that occur in practice during normal operational conditions, but that are not taken into account during risk analysis. The safety-related violations are so-called barrier crossings. A barrier crossing is associated to an operational risk which constitutes a combination of costs: the cost of crossing the barrier, the benefit (negative cost) immediately after crossing the barrier, and a possible deficit (extreme cost) due to the exposure to hazardous conditions that are created after the barrier has been crossed. A utility function is discussed which describes the consequence-driven behaviour and uses an assessment of these costs functions. An industrial case study illustrates the application of the proposed theory.

Keywords: Barrier crossing; Hazardous conditions; Human factors; Risk analysis; Violation

1. INTRODUCTION

Human operators use systems, such as manufacturing systems or transportation systems, to achieve certain dedicated objectives. Nevertheless, operators may also be the cause of incidents or accidents. As a matter of fact, human operators are actors of both improvement and degradation of situations when controlling a dynamic process (Polet et al 1999). If criteria are defined to judge a situation the operator actions may be considered to degrade the situation in accord with a given criterion and may be considered to improve it for another criterion. The operational risks taken by the operators may be the result of a (weighted) compromise between criteria. Nevertheless, operational risks taken by human operators when using a machine are in part considered and predicted by designers. Therefore, human-centred risk analysis should not only consider risks during normal operation, but also in a dynamic and adapted process control context.

This paper explains in terms of a theory what may drive the operators to cross barriers. A method, based on this theory, may be developed to identify barrier crossings and to analyse its associated risks. This analysis can be integrated into existing risk analysis and assessment methods. This paper tries to make a first step towards verification of a qualitative model of barrier crossing. Thus the theory is formalised and put into perspective. All attributes that play a role are mentioned and a theoretical framework is provided.

The proposed theory will involve not only the possible consequences of not respecting (violating) prescribed procedures by the operator, but also the adaptation of these procedures to current operational practices.

Such degraded interaction with a machine is due to human behaviour and operational safety culture. Consequently, different sets of working conditions of system use may be defined:

1. the set of working conditions which are foreseen and defined by the designers;
2. the set of working conditions which are accepted by the users after some time but not explicitly considered by the designer; and
3. the set of working conditions which are accepted by users but explicitly defined as unacceptable by the designers.

Both sets 2 and 3 are so-called 'tolerated use of the machine and tolerated operational practice' by the operators.

These working conditions illustrate different operational modes of the system:

- normal modes, which are guaranteed and anticipated upon by the designer; e.g. working condition (1);

- violation modes, which occur when the designers' instructions are not respected; e.g. working conditions (2) and (3); and
- user-added modes, which do not correspond to any designers' prescription, but which are not violations.

Reason (1990, p. 195) defines violation 'as deliberate – but not necessarily reprehensible – deviations from those practices deemed necessary (by designers, managers and regulatory agencies) to maintain the safe operation of a potentially hazardous system'. Reason assumes that violations are intentional and that for all operational conditions certain (good) practices are described or at least available by either designers, managers or regulatory agencies. This is often not the case because the designer's description of the system's operational conditions is based on a representation of reality. Therefore it may be too brief or even incomplete, leaving the operator free to interpret the situation. Those conditions are 'beyond design' and fall within the set (2) working conditions.

Dougherty (1995) associates violation with unsafe actions! This is not vital; many examples exist where violations are not unsafe actions (e.g. in traffic situations). Dougherty reasons that an unsafe action could be the result of a misunderstanding or conception of the goals (of a system or procedure).

Neither definition has considered operational conditions that are different from the idealised (imagined) designers' conditions; e.g. the much debated valley between theory (design table) and practice.

Work-arounds are deliberate procedural short-cuts and are considered design flaws by Dougherty (1995). However, we will consider them as calculated gambles and thus violations, which are accepted over time.

Dougherty concludes that a violation is the behaviour that results when a person assesses that the formal and expected response is inadequate. The criteria for this conclusion are not discussed but may be personal and social (cultural), operational (workload) or experience related (knows better, trust).

This paper focuses on particular violations, namely the safety-related violations called barrier crossings. First the paper presents the possible constraints of work conditions and then defines a theory for the driving force for barrier crossing. The final part applies this theory to a detailed field observation representing a complex industrial process.

2. CONSTRICTED WORKING CONDITIONS

Human decision making depends on several attributes that characterise a situation (Hollnagel 1993; Swain and Guttmann 1983):

- process state variables are used to observe the dynamic evolution of the process;
- process parameters define the dynamics of the process;
- disturbances affect the process state;
- operator performance shaping factors (PSFs) illustrate the impact on human performance of internal psychological, physiological and cognitive matters and external environmental conditions;
- process objectives of prescribed procedures and set points which direct the operational activity;
- managerial factors that determine the conditions for the working environment and organisation of jobs.

Two viewpoints for the values and working range of these attributes are considered: the operational situation and the situation considered during design (Table 1).

The operational situation considers the real values of each attribute whereas the designed situation anticipates the future operational situation and considers only restricted and prescribed working ranges and values. It is not possible to consider all operational values and ranges of the attributes during the design phase. Therefore the designer has to reduce the degree of freedom of the process and its working range (Polet and Vanderhaegen 2000). Constraints of use are, for example:

- constraints related to the equipment; i.e. constraints related to process state variables, process parameter values and possible disturbances. The system architecture imposes such constraints, for instance: mechanical constraints, electrical constraints, geographical accessibility constraints;
- constraints related to human behaviour; i.e. constraints related to PSFs, objectives for production, product quality and operational safety and the managerial aspects.

The study of future work situations to assess human reliability or human error during these situations requires methods that use predictive models (Humphrey 1988; Kirwan 1997; Reason 1990; Swain 1990). These methods may facilitate the identification of those constraints that

Table 1. Characterisation of a situation

Attributes	Values in an operational situation	Values considered during the design
Process state variables	Limited by physical constraints	Limited range
Process parameters	Pre-selected range and subject to degradation	Fixed range
Disturbances	Depending on the plant context	Limited (range & nature)
Operator PSF	Unrestricted	Neglected or considered optimal
Objectives	Revised	Prescribed
Managerial aspects	Between poorly and well understood	Ignored or optimal

evoke undesired operator behaviour because of unaccepted working conditions or high perceived workload by the operators. Such constraints, when not respected by the operators, may expose the operators to unwanted hazardous conditions. The designer defines such constraints as a means to prevent risky conditions and protect the operators against hazardous working conditions.

3. HUMAN PREVENTION AND PROTECTION AGAINST RISKS

A measure of a risk is usually a combination of the probability that an undesired situation may occur and the consequences of this undesired situation. Consequently, designers can take measures to reduce the risk value of a given situation by decreasing its occurrence probability and/or by decreasing its negative consequences. The negative consequences are assessed, for example, during a careful hazard and operability study. The design and implementation of barriers aim at achieving those objectives: prevention and protection (Kecklund et al 1996).

More precisely, a barrier is defined as an obstacle, an obstruction or a hindrance that may either (Hollnagel 1999):

- prevent an action from being carried out or a situation from occurring;
- prevent or lessen the severity of negative consequences.

Regarding the operations carried out on a given machine, the effectiveness of barriers depends on three main preconditions:

- the existence of adequate training to prevent a wrong use of a machine and application of procedures;
- the existence of adequate human–machine interfaces to make sure that the use of a machine as designed will be possible; and
- the existence of sufficient procedures to direct the operations on a machine.

Four classes of barrier are distinguished (Hollnagel 1999):

- material barriers: barriers that physically prevent an action or limit the negative consequences of a situation;
- functional barriers: barriers that logically or temporally link actions and situations;
- symbolic barriers: barriers that require interpretation;
- immaterial barriers: barriers that are not physically in the work situation.

A barrier can belong to more than one of these classes. Table 2 gives examples of barriers introduced by different safety actors.

The four classes of barriers can be gathered into two groups related by their physical presence or absence (Table 3). The two groups of barriers are:

- *Group I*. The barriers of this group are mounted onto the machine and form one integrated system with the machine. Crossing this kind of barrier cannot be done without modifying the physical integrity of the machine, i.e. taking away the safety integrity. Material and functional barriers belong to this group.
- *Group II*. The barriers in this group can be violated or crossed without affecting the physical integrity of the machine. These barriers are not a part of the machine itself but only of the operation of the machine. Crossing does not require a physical modification of the machine. Symbolic and immaterial barriers belong to this group.

A barrier from Group I is a rigid barrier because there is no crossing possible without losing the system's integrity,

Table 2. Barriers and safety actors (adapted from Hollnagel 1999)

	Reduce impact	Prevent erroneous action		
	Material barriers	Functional barriers	Symbolic barriers	Immaterial barriers
Designer	Grid of protection, airbags, safety belts . . .	Sensors, inter-lock, key . . .	Monitoring, panel, labelling, signal . . .	Training, documentation, procedures
Organisation	Outfit of workplace and workshop, fire exits . . .	Keys, access limitation, passwords . . .	Labelling, pictures, sign on the floor . . .	Internal training, rules
Users	Protective equipment or cloths.	Lock out	Tag out, communication (verbal, gesture)	Report, individual limit

Table 3. Relation between Group I and II barriers and the four classes of barriers defined by Hollnagel

Reduce impact	Prevent erroneous action		
Group I		Group II	
Material barriers	Functional barriers	Symbolic barriers	Immaterial barriers

whereas a barrier from Group II is a flexible barrier because it is possible to cross it. Both sets are means to limit or restrict the geographical and temporal space of use of a machine and to maintain operational safety when using it.

4. THE CONCEPT OF BARRIER CROSSING

An intentional deviated behaviour from that required by the prescription without causing any deliberate damage on system performance is called a violation (Reason 1990; Carpignano and Piccini 1999). The particular safety-related violations affect barriers. A *safety-related violation is an intentional misuse or disobeying of a barrier provided that adequate conditions are present*.

The crossing of a barrier is considered a violation only when it could have been avoided. The causes of a barrier crossing may be:

- a desire to improve performance by means of improving working conditions; or
- a desire to realise a triumph over the automation (based on operational experience).

Both causes are driven by behaviour based on judgement of the costs, benefit and deficits associated with the barrier crossing. Hence, assessment of the situation is a crucial element of these driving forces. Therefore, indirectly the causes for barrier crossing may be:

- a poor or incomplete assessment of the situation which results in complacency; i.e. a wrong assessment of cost, benefit and potential deficit;
- human error such as a reasoning error, commission error or perception error; e.g. a wrong situation awareness because the human operator overlooks the situation.

Negative consequences of a barrier crossing may be:

- an alteration of defence in depth; by crossing a barrier, the human operator removes a protection and exposes himself to hazardous conditions;
- a critical top event due to the physical disintegration of the machine.

The paper focuses on a theory of the crossing of barriers. The operational risk of a barrier crossing is a combination of a cost of the crossing, of an immediate benefit after a crossing and a possible deficit due to the crossing:

- The immediate cost of crossing: in order to cross a barrier the human operator sometimes has to modify the material structure (essentially for material and functional barrier, barriers of Group I), and/or the operational mode of use (essentially for symbolic and immaterial barriers, barriers of Group II). It usually leads to an increase in workload, but can have negative consequences on productivity or quality.
- A barrier crossing is goal driven. Crossing a barrier is immediately beneficial. The benefits outweigh the costs.
- A barrier that is crossed introduces a potentially dangerous situation. Thus, the crossing of a barrier has also a possible deficit.

Usually barriers of Group I are designed such that they pose a high cost of crossing; i.e. the operator weakens the physical integrity of the machine when crossing the barrier. Meanwhile, the barriers of Group I hamper operation of the machine. Therefore, the immediate benefit for the operator is high. Designers use these kinds of barriers because a potential danger would exist if the barrier were absent. Removing the barrier exposes the operator to this danger and thus the possible deficit for the crossing of this barrier is important.

Barriers of Group II have a low or almost zero cost of crossing. The crossing can lead to improved operational efficiency and comfort from the operator's point of view. Field observations have shown that generally barriers of Group II are crossed more frequently than barriers of Group I because the cost of crossing is low.

A high probability of crossing a barrier may occur when the benefit outweighs the costs and the perception of the possible deficit (Table 4). The qualitative probability ratings in Table 4 are subjective and given by the authors. In Table 4, Case 1 represents a situation with a high benefit, low cost and low perceived negative consequence of disobeying the barrier. Thus it is very likely that such barriers will always be crossed. On the contrary, Case 8 represents a situation with low benefit, high cost and high possible deficit. It is very likely, therefore, that this case will never be crossed. The other cases are ordered according to their probability of crossing (judgement by the authors).

As the probability of crossing a given barrier is a benefit-driven human behaviour, the designer should identify for each barrier which case applies and should take measures to reduce this probability of crossing. The design objective is then threefold: (1) to minimise the benefit of a barrier

Table 4. Probability of barrier crossing. In case the outcome is undetermined (?) the worst case is considered (High)

Case	Benefit after crossing	Costs of crossing	Possible deficit due to the crossing: calculated risk	Probability of crossing
1	High	Low	Low	High
2	High	Low	High	? (High)
3	High	High	Low	? (High)
4	High	High	High	? (High)
5	Low	Low	Low	Low
6	Low	Low	High	Low
7	Low	High	Low	Low
8	Low	High	High	Low

crossing; (2) to maximise its cost of crossing; and (3) to maximise the perception of the possible deficit.

5. THEORY OF BARRIER CROSSING

Human operators control their own activity. Figure 1 illustrates the human behaviour involved in controlling dynamic situations. The time of the occurrence of a situation is denoted by t and the objective to be achieved by j. This j may relate to a procedure.

The human operator is able to determine those local objectives that are needed to achieve global system objectives. These local objectives use an expected situation represented by $\hat{S}_{n+1}(t_n, j)$ that the human operator tends to obtain. The human behaviour can be considered as a control strategy applied to the production system. Disturbances act on this production system. Some of the disturbances come from human errors, such as errors of commission. The result of a human action on the production system is the real situation represented by $S_{n+1}(t_{n+1}, j)$. The human operator perceives this result affected by an observation noise. The perceived situation is represented by $\overline{\overline{S}}_{n+1}(t_{n+1}, j)$. A comparison of the new perceived situation and the expected situation at the previous step of reasoning will direct future local objectives and the next expected situation.

Human operators have a large degree of freedom to operate upon the machine. The degree of freedom is situation dependent. Barrier crossing is intentional and results from human decision making. This decision making is guided by preferences on several criteria. The result of the decision making may be a deviated but tolerated procedure.

For a given procedure, several barriers may be active. The human operators select the more relevant procedure, taking into account one or several barrier crossings. The barrier crossing is consequence driven and may depend on personal preferences. The possible consequences are multiple: the cost, benefit and possible deficit (Fig. 2).

The following functions will be used as a framework for

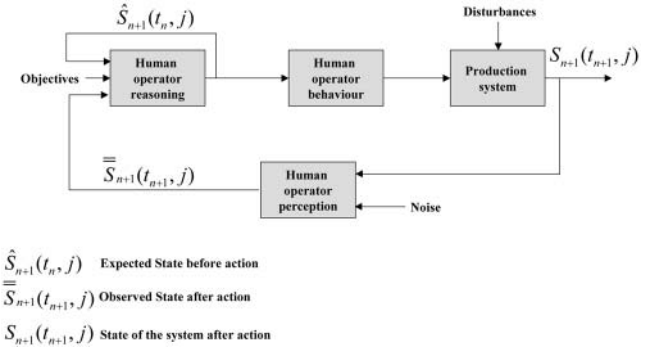

Fig. 1. Human behaviour to control dynamic situations.

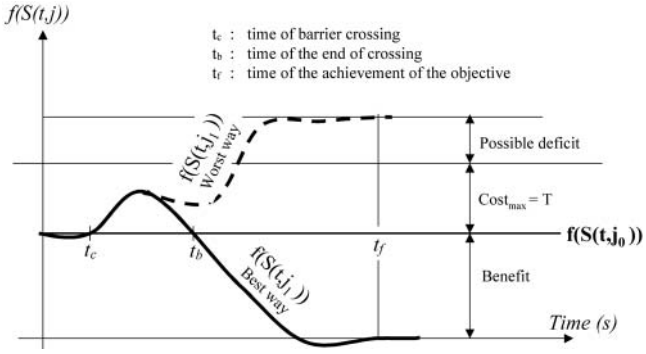

Fig. 2. Example of deficit, cost and benefit of barrier crossing. The best way indicates the evolution when no deficit occurs, whereas the worst way is the case that an accident occurs and the deficit becomes apparent.

the analysis and discussion of the theory. Let $f(S(t, j))$ be the function assessing the severity for a situation when a procedure j is followed.

When j_0 is the prescribed procedure and j_1 is an alternative procedure resulting from a particular barrier crossing, we define $\Delta(S(t, j_1)) = f(S(t, j_1)) - f(S(t, j_0))$. Both procedures are compared at time t.

The values of the function $\Delta(S(t, j_1))$ can be classified as follows (see Table 5):

- The cost of crossing: $\Delta(S(t, j_1)) = c(S(t, j_1))$. The cost of crossing shows the increase in severity that the operator experiences when a barrier is being crossed. Part of this function can be a physical load or a mental load. A negative value is not considered as a cost because it means an immediate benefit when crossing the barrier (see below). An excess of workload above a certain threshold T is interpreted as deficit.
- The benefit of crossing: $\Delta(S(t, j_1)) = -b(S(t, j_1))$. The anticipated benefit (by definition positive) equals the reduction of the severity function below the value $S(t, j_1))$ taken into account during the design.
- The possible deficit: $\Delta(S(t, j_1)) = d(S(t, j_1))$. This value is the increase in severity because the removal of the barrier causes negative effects on workload or safety. In fact the possible deficit reflects an unacceptable cost.

Figure 2 shows our theory for a standard barrier crossing (thick line) and for a worst case when the barrier crossing

Table 5. Definition of cost, benefit and deficit related to a barrier crossing

The cost of crossing	$c(S(t, j_1)) =$	$\begin{cases} 0, & \text{if } \Delta(S(t, j_1)) \leqslant 0 \\ & \text{or } \Delta(S(t, j_1)) > T \\ \Delta(S(t, j_1)), & \text{else} \end{cases}$	
The benefit of crossing	$b(S(t, j_1)) =$	$\begin{cases} 0, & \text{if } \Delta(S(t, j_1)) \geqslant 0 \\ -\Delta(S(t, j_1)), & \text{else} \end{cases}$	
The possible deficit	$d(S(t, j_1)) =$	$\begin{cases} 0, & \text{if } \Delta(S(t, j_1)) \leqslant T \\ \Delta(S(t, j_1)), & \text{else} \end{cases}$	

results in negative side affects. The standard barrier crossing shows an increase in severity (e.g. workload) followed by a reduction. In fact, this reduction is what motivates the operator to cross the barrier. The possible negative effects (deficit) are not always present but only occur when a worst case evolves. The possible deficit is what the operator withholds from crossing the barrier.

5.1. Human Operator Decision Driving Force

It is assumed that a global utility function drives the human operator decision making. The utility function is based on consequence evaluation. This function is a combination of the benefit, cost and deficit:

$$U(t_c,\ j_1) = f\Big(\int_{t_c}^{t_b} c(S_i(t_i, j_1)), \int_{t_b}^{t_f} b(S_i(t_i, j_1)),$$

$$\int_{t_b}^{t_f} d(S_i(t_i, j_1))\Big)$$

This utility function may be used to compare the expected utility noted $\hat{U}(t_c, j_1)$, and the observed utility noted $\bar{\bar{U}}(t_c, j_1)$:

$$\hat{U}(t_c,\ j_1) = f\Big(\int_{t_c}^{t_b} c(\hat{S}_i(t_{i-1}, j_1)), \int_{t_b}^{t_f} b(\hat{S}_i(t_{i-1}, j_1)),$$

$$\int_{t_b}^{t_f} d(\hat{S}_i(t_{i-1}, j_1))\Big)$$

$$U(t_c,\ j_1) = f\Big(\int_{t_c}^{t_b} c(S_i(t_i, j_1)), \int_{t_b}^{t_f} b(S_i(t_i, j_1)),$$

$$\int_{t_b}^{t_f} d(S_i(t_i, j_1))\Big)$$

Moreover, the utility function may be used as a framework to compare advantages in terms of benefit, cost and deficit so that different alternative procedures facing a given situation can be examined. The selected alternative among k possibilities regarding the prescribed one, j_0, may depend on human preferences. For example, the evaluation of the relevant alternative procedures may be aimed at the minimisation of the cost of the barrier crossing, the maximisation of the benefit after crossing and the minimisation of the possible deficit. The following illustration gives an example for which the preference focuses on the maximisation of the benefit.

6. ILLUSTRATION

The reference example is taken from observations of the use of an industrial rotary press. Deviations between the designed operational use and the actual operational use are presented. These deviations affect the safety, quality or production objectives of the machine. The rotary press poses many hazardous conditions for the human operator, such as burns, electrocution, cuts or falls, heat radiation, excessive noise and intoxication. Moreover, production losses rapidly increase when the rotary press is not running or when it is not operating well. Different incidents can disturb the production: breaking of the printing plate, overtightening of the screw that provides ink, breaking of the printed paper strip and problems in adjusting the folding machine. When solving these problems that occur during production, human operators are aware of the compromise between lost production time and repair quality. The longer the time to repair, the more important the production losses.

For each maintenance or repair action upon the rotary press, human operators have to respect the safety procedures prescribed by the designer. Sometimes those procedures are adjusted or abandoned because of other operational constraints. Field observations of the maintenance and repair scenarios show a compromise between four criteria. The criteria are related to either human objectives or machine objectives and have different natures. The change in human workload is the difference between the prescribed operations and executed procedure on the rotary press, whereas human safety concerns the reduction or increase of the number of hazardous conditions against which the user's body is not protected. System production relates to the gain or loss of production time, whereas system quality is the degradation or improvement of the number of printed products.

Several barrier crossings were observed (Polet et al 2000; Vanderhaegen and Polet 2000). One example of safety-related violation is developed below. This example is a violation of a procedure when washing a roll. Constraints of use are as follows:

- *Quality constraint*. Whatever the production to begin, the entire roll has to be clean.
- *Accessibility constraint*. A reduced part of the roll is accessible and visible by users. This necessitates several sequential rotation steps of the roll to clean a part of the roll's surface at a time.
- *Safety constraint*. A rotating roll poses a threat when users are interacting with it, e.g. when applying solvent to the surface to clean the rolls.

Table 6 describes the procedure prescribed by the designer (P0) and possible deviated procedures (P1, P2 and P3). The procedure describes the operation to clean the rolls of a

Table 6. Example of safety-related violation

Prescribed procedure (P0)	Deviated procedure 1 (P1)	Deviated procedure 2 (P2)	Deviated procedure 3 (P3)
1. To wear rubber gloves	1. To push on the PRINTING button	1. To wear rubber gloves	1. To push on the PRINTING button
2. To push on the PRINTING button	2. To push the EMERGENCY STOP button	2. To push on the PRINTING button	2. To push the rotation manually activate button until desired speed
3. To push the EMERGENCY STOP button	3. To clean the visible surface with a sponge	3. To push the rotation manually activate button until desired speed	3. To clean the visible surface with a sponge
4. To clean the visible surface with a sponge	4. To dry the surface exposed with a rag	4. To clean the visible surface with a sponge	4. To dry the surface exposed with a rag
5. To dry the surface exposed with a rag	5. To release the EMERGENCY STOP button	5. To dry the surface exposed with a rag	5. To push the STOP button
6. To release the EMERGENCY STOP button	6. To keep the ROTATION MANUALLY ACTIVATE button pressed	6. To push the STOP button	
7. To keep the ROTATION MANUALLY ACTIVATE button pressed	7. To repeat steps 2–6 as necessary		
8. To repeat steps 3–7 as necessary			

rotary press. Several barriers have been identified for this task:

- rubber gloves: because operators use solvent to clean, they have to wear rubber gloves to protect themselves against aggressive chemicals;
- unauthorised intervention with the rotating rolls to prevent injuries (cuts, crushes) on fingers and hands;
- the emergency stop button: this button is used to activate a physical barrier and can be used to limit the consequences in case an accident occurs. Not activating the button gives the operator more operational freedom but exposes dangerous conditions.

Three deviations from the prescribed procedures are given in Table 5:

- the deviated procedure P1 is a barrier crossing for which the rule to wear rubber gloves is ignored;
- the deviated procedure P2 is a barrier crossing for which the rule to not intervene in the machine running is ignored;
- the deviated procedure P3 is a combination of the two precedent barrier crossings in P1 and P2.

6.1. Comparison of the Different Procedures

Two main criteria have to be considered: the first is the impact of the activity on productivity; the second concerns the safety of the operator. Regarding quality, the four procedures lead to a similar acceptable result. In fact, the human operator has a quality conserving task.

Figure 3 shows the result of the time duration comparison. Between the prescribed procedure and deviated one, P3, there is a gain of 90 seconds. Regarding productivity the deviated procedure P3 leads to a 57% reduction of execution time.

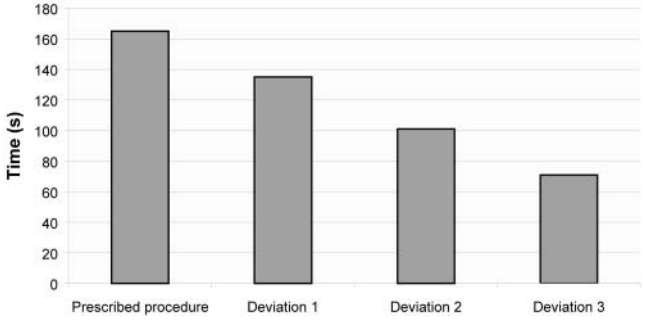

Fig. 3. Processing time for each procedure.

Barrier crossing reduces the defences in depth of the system. Human operators experience a loss of protection and prevention. Moreover, deviated procedures lead to new dangerous exposures:

- in the case of P1, the human operator is exposed to toxic and aggressive chemicals;
- in the case of P2, the human operator is exposed to spraying of toxic solvent and to pinching of fingers or crushing a hand;
- in the case of P3, the human operator is exposed to toxic and aggressive chemicals, of spraying of toxic solvent and to injuries to fingers and hands.

This exposure to danger occurs at specific steps during each procedure (see Fig. 4).

Finally, the possible deficit can be evaluated by the product of the number of hazardous occasions and the duration of the exposure to those threats. Regarding this criterion the procedure P3 is the most hazardous (see Fig. 5).

This example highlights the compromise between productivity and the safety.

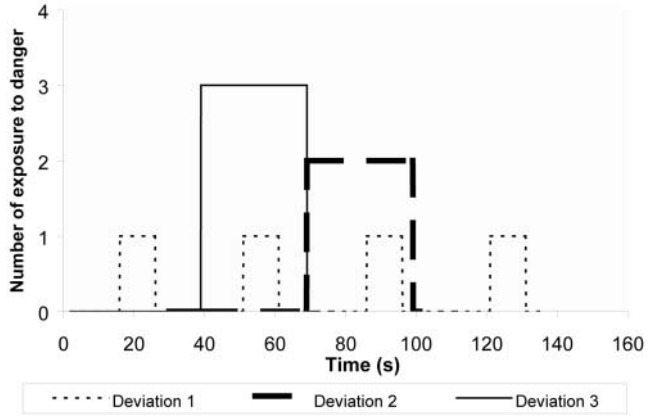

Fig. 4. Comparison of the evolution of exposure to dangerous situations.

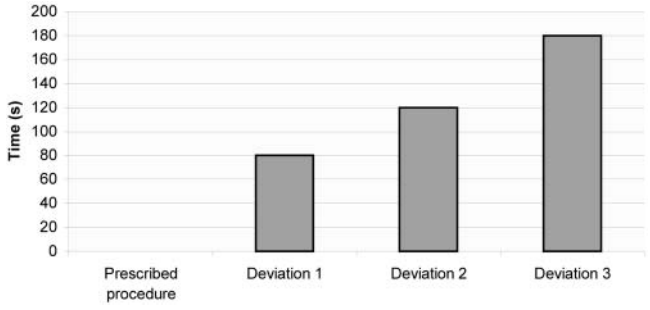

Fig. 5. Exposure to dangerous situations for each procedure.

7. CONCLUSION

A situation was defined as a causal relational network between the constraints of system use, the possible actions of human operators and the states of the controlled process. Barriers are then constraints that reduce the degree of liberty of humans by either preventing them or protecting them. The motivation of a barrier crossing was considered as a combination of an immediate benefit, immediate cost and possible deficit. Thus, this paper has proposed the principles of a safety consequence-driven violation for which the research of the maximum of benefit is balanced with a cost and a possible deficit when crossing a barrier. The theory includes functions of utility to assess and compare a given alternative situation, including a barrier crossing, with the prescribed one in order to achieve a similar or identical objective. Those utility functions are also used to balance the consequences of expected controlled situations related to barrier crossing with those of the observed ones. A practical example was developed for a procedure to clean rolls of an industrial rotary press: the prescribed procedure was compared with three possible alternatives in terms of benefit and possible deficit.

For the human operator the benefit, cost and deficit are perceived and may be determined by objective and subjective factors. The designer has to identify these factors that facilitate a barrier crossing and may try to reduce the motivation for this crossing. Therefore, the theory of safety-related violation may be used to improve risk assessment associated with barrier crossings and may be added to classical risk assessment methods. One way to improve the effectiveness of barriers is by increasing the perception of the utility of barrier crossing; i.e. decrease the perception of the benefit and increase the perception of the costs and possible deficit.

Acknowledgements

This work was done as a part of two complementary projects: (1) a project planned by the 'Prevention Integration through Design Group' of the French National Institute for Research and Safety (INRS), and supported by the 'Production Systems Program' (PROSPER) of the National Centre for Scientific Research (CNRS); (2) a programme supported by the French and Dutch governments, called the Van Gogh programme, which is aimed at scientific and technical bilateral cooperation. This project involves the Man–Machine Systems group of the Delft University of Technology, The Netherlands, and the Laboratory of Automated Systems and Mechanics on Industrial and Human aspects of the University of Valenciennes, France.

References

Carpignano A, Piccini M (1999). Cognitive theories and engineering approaches for safety assessment and design of automated systems: a case study of a power plant. Cognition, Technology & Work 1:47–61.

Dougherty A (1995). 'Violation' – does HRA need the concept? Technical Note. Reliability Engineering and System Safety 47:131–136.

Humphrey P (1988). Human reliability assessors guide. In Sayers BA (ed). Human factors and decision making: their influence on safety and reliability. Elsevier Applied Science, Oxford, pp 71–86.

Hollnagel E (1993). Human reliability analysis context and control. Academic Press, London.

Hollnagel E (1999). Accident and barriers. In 7th European conference on cognitive science approaches to process control, Villeneuve d'Ascq, France, pp 175–180.

Kecklund LJ, Edland A, Wedin P, Svenson O (1996). Safety barrier function analysis in a process industry: a nuclear power application. Industrial Ergonomics 17:275–284.

Kirwan B (1997). Validation of human reliability assessment techniques: Part 1 – Validation issues. Safety Science 27:25–41.

Polet P, Vanderhaegen F (2000). Analysis of deviated modes for risk assessment. In Proceedings of ESREL2000: European annual conference on safety and reliability, 15–17 May 2000, Edinburgh, UK, pp 133–140.

Polet P, Vanderhaegen F, Millot P (1999). Toward a risk-taking model of the human supervisor. In European annual conference on human decision making and manual control, 25–27 October 1999, Loughborough, UK, pp 135–144.

Polet P, Vanderhaegen F, Wieringa P (2000). Theory of barrier crossing. In

Cacciabue PC (ed). Proceedings of the 19th European annual conference on human decision making and manual control, Ispra, Italy, June 2000, pp 73–80.

Reason J (1990). Human error. Cambridge University Press, Cambridge.

Swain AD (1990). Human reliability analysis: need, status, trends and limitations. Reliability Engineering and System Safety 29:301–311.

Swain AD, Guttmann HE (1983). Handbook of reliability analysis with emphasis on nuclear plant applications. Technical report NUREG/CR-1278, August 1983. NUclear REGulatory Commission, Washington, DC.

Vanderhaegen F, Polet P (2000). Human risk assessment method to control dynamic situations. In 4th IFAC symposium on fault detection, supervision and safety for technical processes (SAFEPROCESS 2000), 14–16 June 2000, Budapest, Hungary, pp 774–779.

Correspondence and offprint requests to: P. Polet, LAMIH, UMR 8530 Université de Valenciennes et du Hanaut-Cambresis, Le Mont Houy, 59313 Valenciennes Cedex 9, France. Email: Philippe.Polet@univ-valenciennes.fr