INTERNATIONAL CONFERENCE ON ENGINEERING DESIGN
ICED 03 STOCKHOLM, AUGUST 19-21, 2003

SAFETY ANALYSIS DURING INDUSTRIAL EQUIPMENT REDESIGN: EVALUATION OF A CASE STUDY

François Gauthier

Abstract

Safety integration during the design of industrial equipment has been studied intensively for the past 15 years. Many authors have proposed different methods to improve the effectiveness of this critical task. However, the redesign or modification of industrial equipment during its working life is a quite different situation. This paper shows the results of a case study conducted with the intent to implement a systematic safety analysis procedure in the context of industrial equipment redesign. A team identified a total of 55 different hazards using simple methods such as documentation analysis, task observation and interviews with operators. The study concluded that safety analysis can be efficiently implemented during redesign of operating industrial equipment. Team members and company managers were satisfied and thought that it was a major improvement over their traditional way of doing things when modifying equipment. However, such a project could not be conducted without the help of a safety analysis facilitator who can support the risk analysis team.

Keywords: Industrial case study; Introduction of methods in industry; Safety; Man-machine interaction

1. Introduction

The recent studies that were undertaken to analyze the accidents involving various types of industrial machinery generally reached the same conclusion: many tools, machines and industrial production systems are not well adapted to occupational safety and health considerations (OS&H) [1-3]. There is now growing recognition of the fact that this poor adaptation is the result of an inadequate design with regard to OS&H [4]. Accordingly, safety integration during the design of industrial equipment or machinery has been studied intensively for the past 15 years. Several authors have proposed different methods and procedures to improve the effectiveness of this critical engineering task. Many are specific to particular fields such as the chemical industry and naval construction (see for example [5-6]), but some are relevant to machinery design [7-10]. National and international standards have also been adopted in order to guide designers in this matter [11-15].

However, these methodological developments (which are, in fact, still being continuously enhanced) are generally intended more for the initial design, i.e., before the actual equipment or machinery is installed and operated in an industrial environment. In industry, equipment redesign or modification is often required to improve productivity, quality or to upgrade its production capacity. Considering also that the safety level of many industrial machines is often not adequate due to improper initial design, redesign of industrial equipment during its working life is a very common activity. The conditions under which this redesign is

accomplished are quite different from the well-documented initial design process. While it is easier to identify hazards and evaluate risks with operating equipment, it is a more challenging task to identify risk control measures that can be suitably implemented into the existing design and its environment. Moreover, the people involved are inevitably different: project engineers and operation and maintenance personnel will take the place of the original design engineers. In this context, the risk analysis approach must be adapted.

A recent study was conducted in a heavy industry processing plant. The intention of this study was to establish the feasibility of efficiently implementing a systematic safety analysis procedure in the context of industrial equipment redesign. Another objective was to define the proper adjustments to be made to the usual design-for-safety procedure and to the planning and managing of the risk analysis activities in order to adapt to this context of application. This paper presents the results and key findings of the study.

2. The case study

2.1 Analyzed equipment

The equipment selected for this project was a relatively simple installation involving two operators and four workstations. It involved two cranes carrying heavy containers of hot liquid, a manual pouring station, and a trimming station. The equipment is used to fill molded blocks (which are carried by an elevator and a conveyor) with the hot liquid using a special pouring device. Operators are exposed to various hazards, including burns by the hot liquid they are handling, and various crushing and impact hazards from the mobile parts of the equipment and from movement of the blocks and containers.

This installation was chosen because it represented a good opportunity for an initial simple attempt to apply the risk analysis procedure and because it was in the (unhurried) process of being redesigned/modified to improve its reliability and productivity. It was also the company's safety intervention priority since it had been involved in many major incidents and a few minor accidents in the last seven years.

2.2 Project team

A safety analysis team was created, consisting of the project engineer in charge of the redesign project, an operator, a mechanic, an electrician and the author. The project engineer was responsible for translating the results of the risk analysis into specifications for the redesign project. He was also responsible for presenting the results of the analysis to the managers and for obtaining the budget to implement the team's recommendations in the redesign project. The author's role was to act as a consultant on safety matters, to plan the safety work, and to guide the team during the analysis. The operator, mechanic and electrician all had lengthy experience in the company and were considered as "experts" on the equipment. However, they were selected not only for their technical expertise, but also for their personal attitudes, open-mindedness and on their interest in participating in the analysis.

2.3 Project execution

After one day of team member training provided by the author, the installation was analyzed on a half-day basis every two or three weeks. Team meetings had to be planned far in advance in order to cope with the sometimes inconsistent schedules of the team members (two were on shift work schedules). It took four months to complete the analysis. Each team

meeting was held in a dedicated room, located near the equipment to be analyzed. The room was equipped with a computer and a video-data projector. During the meetings, the progress in the analysis was shown on the screen using an Excel worksheet in which the results were logged. In addition to the team meetings, team members had to work on individual tasks between the meetings. In the initial planning, most of the analysis work was to be done by the team members outside the team meetings.

Following each meeting, the author collected the team members' comments on their perception of the progress and the results of the analysis. At the end of the risk analysis, individual interviews were conducted with the team members to complete the data collection.

2.4 Risk analysis methodology

The risk analysis methodology selected for this application was based on the *Operating and Support Hazard Analysis* method (O&SHA), as described in the *System Safety Handbook* published by the *System Safety Society* [16]. This method (also known as *Operating Hazard Analysis*) was selected because it did not require any special expertise from the team members other than their operational experience and also because it could efficiently uncover most of the operational hazards in order to feed the redesign project with the safety improvements that had to be taken into account. This analysis "*is performed primarily to identify and to evaluate hazards associated with the environment, personnel, procedures and equipment involved throughout the operation of a system. (..) The focus of the O&SHA is on the operations during various modes and the effects of those operational aspects to the system and environment*"[16]. It involved an eight-step procedure going from establishing the scope of the analysis to the reporting of results, including hazard[1] identification, risk assessment, and the identification of hazard control measures.

On many points, the procedure was in accordance with the EN 1050 standard *Principles for Risk Assessment* [11]. However, since the objective of this case study was a practical evaluation of the possibility of efficiently implementing a systematic **redesign-**for-safety procedure, some adjustments were made to the "standard" EN 1050 procedure. Figure 1a shows the risk assessment procedure defined in the EN 1050 standard, while Figure 1b shows the procedure used in this project. As can be seen, the two procedures are comparable with respect to project definition and planning (Determining the limits or Establishing the scope), hazard identification, and risk assessment (Risk estimation and evaluation or Assessing the risk).

However, the procedure used in the project adds one step to the EN 1050 procedure: the identification of existing hazard control measures. In the redesign of operational industrial equipment, this information becomes critical since the risk level cannot be assessed without knowing which control measures are really used and to what extent. This is quite different from a design perspective where the environment and the operational reality are far less present. It is also different since risk analysis during initial design of equipment is often done informally in the early design phases, before hazard control measures have been implemented in the design.

[1] In this paper, the word "hazard" means a source of possible injury or damage to health, and the word "risk" means a combination of the probability and degree of possible injury or damage to health in a hazardous situation. [12]

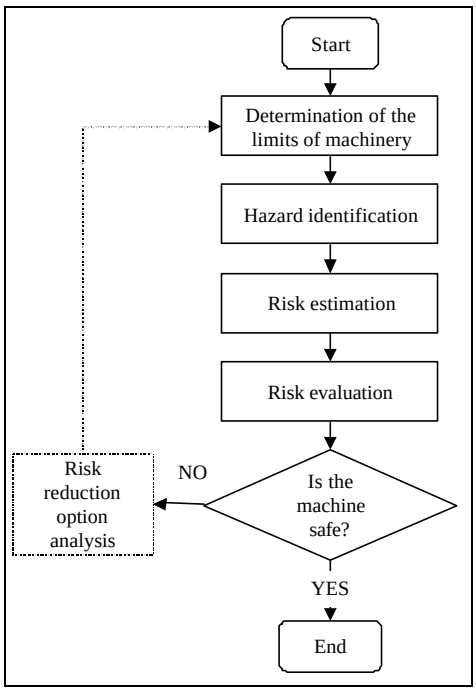

Figure 1a. The risk assessment procedure proposed in EN 1050 [11].

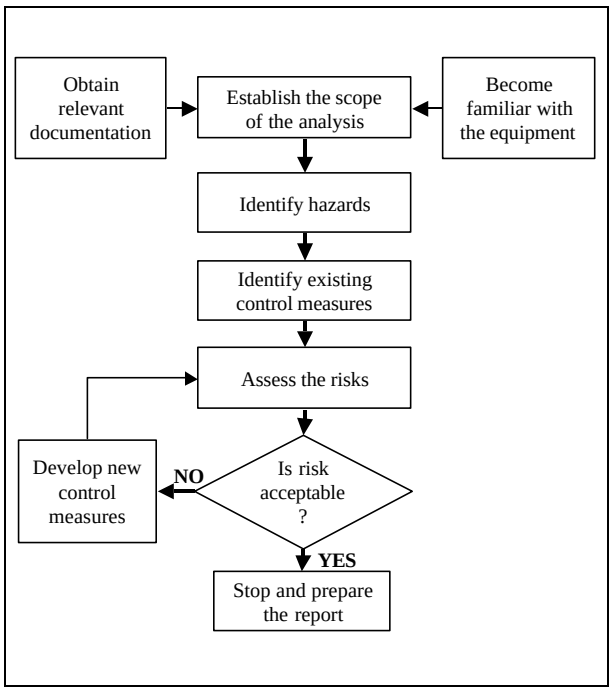

Figure 1b. The risk analysis procedure used in the project.

Another difference between the two procedures is: the steps relating to the development of solutions to control hazards are not connected up to the same level. In the EN 1050 procedure, once the risk reduction options have been defined, they are processed through the entire risk analysis procedure. In the procedure used in this project, once new control measures have been defined, only the risk level is reevaluated. This is another particularity of risk analysis during redesign of operational industrial equipment. Since the new hazard control measures are in fact supplemental measures or layers of protection, they usually don't have important impacts on the system. This procedure was considered as a compromise between completeness of the analysis and the time available to the analysts.

3. Risk analysis results

Eight team meetings were required to complete the analysis. The first two meetings were spent specifying the scope of the analysis and establishing a common terminology and knowledge of the system by all team members. This was accomplished through observations of work activities in the plant and with photos and videos. Documents such as the task description, plant layout and process flow diagrams were also consulted for this task. The team members were then asked to work individually on hazard identification using the critical incident technique (see [16]), mainly on the basis of their experience and through documentation analysis (incident and accident reports, equipment failure data, work procedures). During the next two meetings, hazards identified from the individual analysis were collected and more hazards were pinpointed through documentation analysis, task analysis, interviews with more operators and team discussions. The team identified a total of 55 different hazards using these simple hazard identification methods.

Following hazard identification, existing hazard control measures were listed for each hazard and evaluated for their effectiveness. A checklist of generic hazard control measures was

used to facilitate this task. A qualitative risk assessment was then done, based on the matrix defined in MIL-STD-882D [17]. Figure 2 shows the risk assessment matrix used. Severity was ascertained on the worst credible case defined by the team members, and the probability of mishap was established qualitatively on the probability of the worst credible case using past experience in this and other plants of the company. This task, including the analysis of existing hazard control measures, took two more team meetings. It concluded that 36 of the 55 identified hazards led to acceptable risks, while 16 led to marginal risks for which supplemental control measures were required. None of the 55 identified hazards resulted in unacceptable risks.

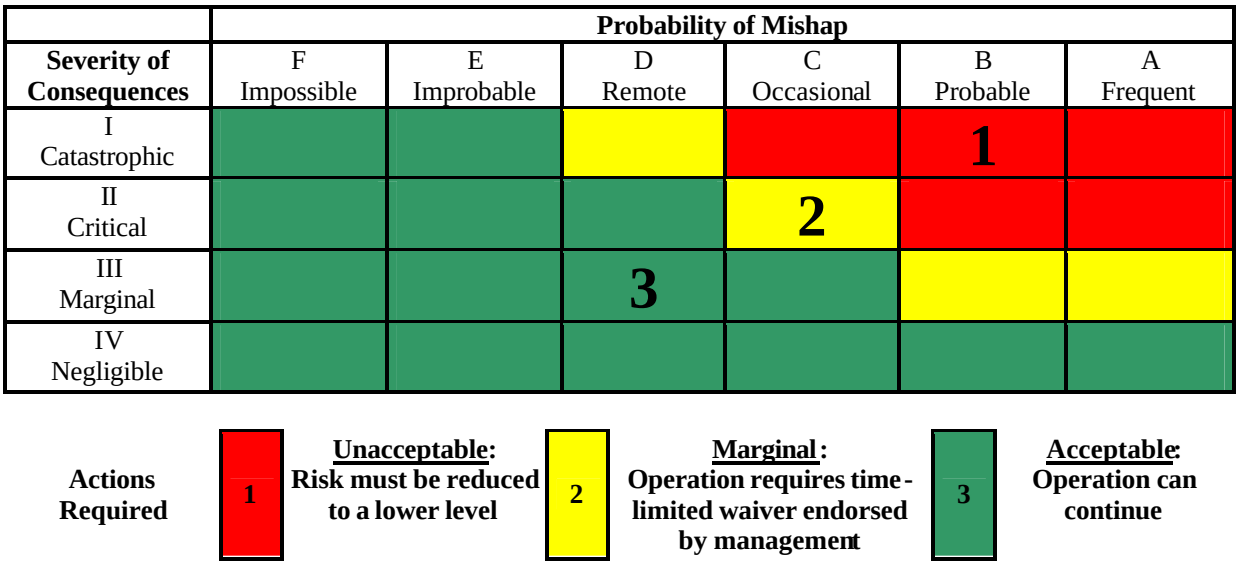

Figure 2. The risk assessment matrix adapted from MIL-STD-882D [17].

For the 16 marginal risks, new hazard control measures were recommended and translated into specifications to be applied to the redesign project. The majority of these new hazard control measures or layers of protection were of a technical nature involving mechanical and control system modifications. Some were of an organizational nature involving a need for new work procedures, safety training and information for workers. Risks were then reassessed to make sure that they were all going to drop to the "acceptable" level after implementation of the new control measures. Table 1 presents the risk analysis worksheet that was used and some examples of results from the analysis. Various columns from the original risk analysis worksheet such as "section of equipment", "category of control measure" and "comments" are not shown in Table 1.

In all cases, the new specifications did not require reversing the redesign process, since the analysis was done at the beginning of the process. However, after discussion with the redesign team of technicians and engineers, two of the recommended control measures had to be reevaluated since they presented high-level technical problems. Moreover, some of these specifications had to be discussed with the company manager in order to adjust the financing of the redesign project. The risk analysis team, supported by design engineers, made some adjustments to a few of its recommendations in order to be consistent with the technical and financial limits of the redesign project. Six months after the risk analysis project was completed, most of the recommended hazard control measures were accepted and integrated into the redesign project planning. The actual equipment modification work has not yet been initiated.

Table 1. Risk Analysis worksheet and examples of results.

			Severity				Probability						Risk			
Activity	**Hazards**	**Existing Hazard Control Measures**	Catastrophic	Critical	Marginal	Negligible	Impossible	Improbable	Remote	Occasional	Probable	Frequent	Acceptable	Marginal	Unacceptable	**New Hazard Control Measures**
Unjamming of block	Crushing of arms by block-elevator when unjamming block	Removable safeguard Use of a scaling bar Operator experience		x						x				x		Modify conveyor's rollers to avoid jamming of blocks. Interlock block-elevator with safeguard.
Moving liquid container	Burns to passerby due to splashing of hot liquid	Overhead crane collision detection Safety perimeter Personal protective equipment		x						x				x		Relocate the catwalk. Install safety signs about walking in the sector.
Moving liquid container	Crushing of foot by descending container	Safety boots Operator experience			x				x				x			Remote control of overhead crane.
Skimming	Burns to operator while skimming container	Personal protective equipment			x					x			x			None: Risk acceptable as is.
Manual pouring	Crushing of leg by container due to an unexpected movement of the overhead crane	None		x						x				x		Reinforce operator's cabin Install safety frame.
Trimming	Minor injuries when the operator's foot slides between two conveyor rollers	Safety boots Operator experience			x				x				x			Install step-plates between rollers in the dangerous portion of the conveyor.

4. Discussion

4.1 Project assessment and difficulties

Some problems were ascertained during the development of this project. These problems were observed at specific and general levels. At the specific level, Table 2 summarizes the main difficulties encountered during each step of the risk analysis procedure.

At a more general level, the guidance provided by the author as a facilitator required more than just attending the meetings: planning and preparation work was found to be critical to the success of the project. Also, the relatively slow pace at which the analysis was conducted was considered by most team members to be a major drawback in this project. It was due to some logistical and scheduling problems (availability of team members and key operators, availability of the room and equipment, etc.) and led to demotivation of some team members at the end of the analysis, despite an ongoing strong commitment from the company managers. Intervention by the author to resume the process was sometimes necessary.

However, the team members, and especially the operations and maintenance personnel, were surprised with the unexpected number of marginal risks with which they were coping in their everyday activities. It appeared that an initial impact of the risk analysis activities was an awareness of the sometimes unsuspected hazards that were inherent in this equipment. Team members and company managers were in general very satisfied with the results of the analysis and thought that it was a major improvement over their traditional way of doing things when redesigning or modifying equipment. In addition, the engineer responsible for the redesign project considered that this risk analysis, carried out early in the redesign process, would in fact save the company money, reducing the need to incorporate modifications into the new design at the end of the redesign process.

Table 2. Difficulties encountered during in the application of the risk analysis procedure.

Risk analysis step	**Difficulties encountered**
Establish the scope	Limiting the extent of the analysis: defining where the equipment starts and where it ends.
Obtain relevant documentation	No particular difficulties obtaining the documentation. However, team members were unenthusiastic about reviewing the documents individually, thus limiting the effectiveness of the analysis.
Become familiar with the equipment	Team members had different knowledge about the equipment but generally assumed that they knew it well enough. They were not very keen on becoming familiar with one another's perspective.
Identify hazards	Difficulties of team members in dealing with hypothetical events. Individual work that was required outside meeting times was not done. This limited the effectiveness of the analysis and unduly lengthened the team's work. Also, due to the limited expertise of team members in risk analysis, the hazard identification methods that were used were rather basic and could have affected the completeness of the analysis.
Identify existing hazard control measures	Limited knowledge of team members about technical details of the equipment regarding safety. Difficulty obtaining consensus among team members about the reality of application of some measures.
Assess the risks	Ambiguous definition of severity and probability of mishap levels leading to tedious and time-consuming discussions.
Develop new control measures	Lack of technical (safety) expertise of team members leading to sometimes unclear or unrealistic solutions.

4.2 Risk analysis in the context of a redesign project

Following the investigation of this case study, three key factors can be identified that could explain the most significant problems encountered during the project:

- Time availability and motivation of team members to work on the project outside the meetings.
- Planning and scheduling problems that unduly lengthen the project, producing demotivation among team members.
- Limited knowledge of team members about risk analysis and control.

As mentioned earlier, in the original planning of the project, most of the analysis work was supposed to be done individually, while meeting times were for sharing ideas and achieving consensus on the results. In reality, not much work was accomplished by team members outside the meetings. This was explained by a simple but important fact: it is easier for production and maintenance personnel (generally not used to office or analysis work) to find time out from their usual jobs to attend analysis team meetings than to do the individual work that needs to be done between meetings. This fact also influenced the completeness of the analysis. Thus, the first factor, i.e., work done outside the team meetings, is important to consider when working on a redesign project where the people involved are not necessarily the engineers and technicians who are responsible for the actual redesign work. Even though all risk analysis team members are theoretically part of the redesign team, they feel more like "consultants" in the redesign project. Planning of risk analysis activities should put less emphasis on team members working outside the meetings in order to keep the project schedule on a more realistic basis. However, one team member should be responsible for

getting some work done between the meetings in order to make the most of the meeting time. It was the team members' and author's opinion that such a project could not be conducted without the support of a safety analysis facilitator who can give directions, periodically set goals, and do some work between the team meetings in order to get the most out of the meeting time. In this project, the author carried out this role but the objective of the company is to eventually have a few people who can carry out this role in the near future. Other redesign projects are planned and will serve as training sessions for internal safety analysis facilitators.

This first factor also had an influence on the 2nd factor, i.e., the length of the project. While the initial goals could not be accomplished at each meeting, planning and scheduling problems occurred and it became increasingly difficult to plan the continuation of the activities. This lengthened the project and eventually led to loss of interest of some team members, despite the initial good attitude of all those involved. Such a risk analysis project would be better accomplished in a blitz fashion, where team members are released from their usual jobs for a two- to three-day period. In fact, other projects led by the author seem to confirm this assumption. However, this is more difficult to achieve in a redesign project that is far from the main assignment of the operations and maintenance personnel.

The team members' limited knowledge about risk analysis and control had impacts on many steps of the risk analysis procedure. During hazard identification, operations and maintenance personnel had difficulty picturing hypothetical events and situations in order to identify new hazards. They were more comfortable with a retrospective approach to hazard identification by relying on their past experience than working prospectively to unveil potentially dangerous unsuspected hazards. Also, considering the limited expertise of team members with risk analysis methodologies, hazard identification had to rely solely on basic and intuitive methods. The author's opinion is that the use of these less systematic and less thorough methods has slightly diminished the results, but it is difficult to evaluate to what extent. Methods such as *Failure Mode and Effect Analysis* or *Fault Tree Analysis* could have identified more unsuspected hazards but their application would have been prohibitive in this redesign context. Nevertheless, the overall result seems to be a suitable compromise between time availability, the skills of the personnel, and the completeness of the analysis.

When assessing the risks, the team members' experience in risk analysis could be overcome by prolonging the discussions, mainly on the probability of mishap levels. The author's and team members' opinion is that the classification of risks obtained is acceptable. However, there is no way of knowing whether the assessment of each risk established by the team members is accurate. There is a high level of subjectivity in this task and no study has yet been conducted to evaluate the accuracy and the robustness of risk assessment tools such as the one proposed in MIL-STD-882D [17]. Research in this field is certainly needed.

Identifying and defining hazard control measures requires specific knowledge about safety's technical aspects. In this case, only the author had sufficient expertise in this field to propose realistic hazard control measures that could be implemented in an existing design. Here again, the help of a safety consultant guiding the team during the analysis is an important factor for the success of such a project. However, the team members did not master all the technical aspects of the equipment, which had a negative impact on the solution finding process. At this point, the involvement of technicians and engineers in the redesign team who are more knowledgeable about the technical aspects of the analyzed equipment would have been helpful. The active involvement of technicians and engineers in the risk analysis should come as early as possible, in order to avoid struggling and delays in the completion of the analysis.

5. Conclusions

The general conclusion of this case study is that safety analysis can be efficiently implemented during the redesign of operating industrial equipment. In this project, a small team composed of a project engineer and operations and maintenance personnel (all minimally trained) were able to satisfactorily carry out a risk analysis in the context of a redesign process. Nevertheless, the study also showed that such a project could not be conducted without the support of a facilitator who is knowledgeable about risk analysis and control and who can advise the team on safety matters, plan the risk analysis activities, and do some work between the team meetings. Particular attention also has to be paid to the careful and realistic planning of the risk analysis activities.

Another experience from this case study is that a compromise has to be made between the depth of the risk analysis and the time to be allocated to complete the analysis. Even if more systematic hazard analysis methods might have produced more thorough results, a less exhaustive approach based on experience is perceived as a better compromise between completeness and the use of time for risk analysis during redesign. Finally, this study highlighted the importance of the team members' technical and safety competency level in the difficult task of identifying risk control measures that can be suitably implemented into an existing design.

References

[1] Mattila, M., Tallberg, T., Vannas, V. and Kivisto-Rahnasto, J., "Fatalities at Advanced Machines and Hazardous Incidents at FMS Implementations", International Journal of Human Factors in Manufacturing, 1995, pp.237-250.

[2] Pratt, S.G., Kisner, S.M. and Moore, P.H., "Machinery-Related Fatalities in the Construction Industry", American Journal of Industrial Medicine, Vol. 32, 1997, No. 1, pp.42-50.

[3] Gardner, D., Cross, J.A, Fonteyn, P.N., Carlopio, J. and Shikdar, A., "Mechanical Equipment Injuries in Small Manufacturing Businesses", From Experience to Innovation – IEA '97. Proceedings of the 13th Triennial Congress of the International Ergonomics Association, Tampere, Finland, June 29-July 4, Ed. by P. Seppala, T. Luopajarvi, C.H. Nygard and M. Mattila, Finnish Institute of Occupational Health, Helsinki, 1997, Vol. 7, pp.109-111.

[4] Gauthier, F., and Charron, F.,"A Structured Procedure of Risk Analysis and Control for Safety Integration in Machinery Design", Journal of Engineering Design, Vol. 13, 2002, No. 2, pp. 77-99.

[5] Wang, J. and Ruxton, T. "A Design-for-safety Methodology for Large Engineering Systems", Journal of Engineering Design, Vol. 9, 1998, No. 2, pp.159-171.

[6] Birmingham, R., Sen, P., Cain, C. and Cripps, R.M., "Development and Implementation of a Design for Safety Procedure for Search and Rescue Craft", Journal of Engineering Design, Vol. 11, 2000, No. 1, pp. 55-78.

[7] Schoone-Harmsen, M. "Design Method for Product Safety", Ergonomics, Vol. 33, 1990, No. 4, pp. 431-437.

[8] Intitut National de Recherche et de Sécurité (INRS) «Enseigner la prévention des risques professionnels - Concevoir une machine sûre », Paris, INRS, 1994, 59 p.

[9] Stoop J.A., "Towards a Safety Integrated Design Method", International Conference on Engineering Design, The Hague, Netherlands, 1993, pp.1165-1173.

[10] Reunanen, M., "Systematic Safety Analysis Methods in Product Design", International Conference on Engineering Design, The Hague, Netherlands, 1993, pp.1174-1181.

[11] EN 1050 "Safety of Machinery – Principles for Risk Assessment", European Committee for Standardization, 1996.

[12] EN 292-1 "Safety of Machinery – Basic Concepts, General Principles for Design – Part 1: Basic Terminology, Methodology", European Committee for Standardisation, 1991.

[13] EN 292-2 "Safety of Machinery – Basic Concepts, General Principles for Design – Part 2: Technical Principles and Specifications", European Committee for Standardization, 1991.

[14] CAN/CSA Z432-94 « Sécurité des machines - Santé et sécurité au travail », Association canadienne de normalisation, Etobicoke Ont., 1994, 63 p.

[15] BSI "British Standard Code of Practice for Safety of Machinery", British Standard Institution, 1988, 156 p.

[16] Stephans, R.A., Talso, W.W. eds. "System Safety Analysis Handbook", 2nd edition, System Safety Society, 1997, 650 p,.

[17] MIL-STD-882D "Military Standard: System Safety Program Requirements", Department of Defence, 2000, United States of America.

For more information please contact:

François Gauthier
Industrial Engineering Department
School of Engineering
Université du Québec à Trois-Rivières
C.P. 500 Trois-Rivières (Québec)
CANADA
Tel : 819-376-5011 ext. 3959, Fax : 819-376-5152
e-mail: francois_gauthier@uqtr.ca