Proceedings of ICAD2009
The Fifth International Conference on Axiomatic Design
Campus de Caparica – March 25-27, 2009
ICAD-2009-01

SYSTEMATIC HUMAN-SAFETY ANALYSIS APPROACH BASED ON AXIOMATIC DESIGN PRINCIPLES

Rima Ghemraoui
rima.ghemraoui@cemagref.fr
Research Institute for Agricultural Engineering, Cemagref
Parc de Tourvoie, BP 44
92163 Antony Cedex, France

Luc Mathieu
luc.mathieu@lurpa.ens-cachan.fr
Laboratoire Universitaire de Recherche en Production Automatisée - LURPA,
ENS Cachan – Paris XI
61 Avenue du Président Wilson, 94230 Cachan, France

Nicolas Tricot
nicolas.tricot@cemagref.fr
Research Institute for Agricultural Engineering, Cemagref
Parc de Tourvoie, BP 44
92163 Antony Cedex, France

ABSTRACT

Current means of safety integration, which consist in safety barriers implementation for risk reduction, have reached their limits. In fact, risk reduction analysis and safety barriers are implemented in the end of the design process, in the detailed design phase, and are rapidly increasing in variety, size, complexity and sophistication. This paper firstly, describes the problematic of integrating safety indicators as soon as possible in the design process. Secondly, a brief state of the art of the Axiomatic Design is introduced. Then, the conceptual risk reduction model and the risk analysis approach in all design stages are detailed. Finally, the preliminary results of the application to the Tractor-Implements Hitch (TIH) design are developed.

Keywords: Axiomatic design, systematic design, human-factors, risk analysis, tractor-implements hitch

1 INTRODUCTION

Nowadays, the discipline of product design can no longer be separated from the concept of human safety integration. Safety is defined as the absence of unwanted events. Risk is defined as something unwanted can happen. According to a common definition [Hollnagel, 2008 a; Fadier, 2008], *Safety can be brought by eliminating risks, by preventing initiating event, and/or by protecting against outcomes*. The risk reduction process is, for instance, based on three phases: (1) understanding if there is a problem and what the problem is; (2) understanding the mechanisms or the ways in which the adverse outcomes can arise; (3) finding the means which can be used to reduce or eliminate risk, or to protect against the consequences. If one or more of these phases fail, the risk may not be noticed until something happens, when it is usually too late to do anything about it.

Current means of safety integration, which consist in safety barriers implementation for risk reduction, have reached their limits. In fact, safety barriers are implemented in the end of the design process (add-on safety solutions), and contributes to the complication of the product. In the literature, several classifications of safety barriers are distinguished [Sklet, 2006]. A commonly used classification is to distinguish between physical and non-physical barriers. Physical barriers are barriers that physically prevent an event from taking place. Non-physical barriers correspond to instructions and procedures that may be given to operator. Hollnagel has proposed a classification based on barrier's nature describing four groups: physical or material, functional, symbolic and incorporeal or immaterial barriers [Hollnagel, 2008 a]. Other barriers description differentiates inherent versus add-on barriers [Sklet, 2006]. An inherent barrier consists in changing a design parameter. Add-on barriers are systems or components that are added to the detailed solution because of safety consideration. Fadier & De la Garza consider that adding safety barriers contribute to accentuate the antagonism between productivity and safety [Fadier & De la Garza, 2006].

An often used solution for risk reduction constitute in principle's substitution, what usually conducts to automation. Human performance is thus replaced by automated devices. However, automation has several limitations; it may contribute to increase the mental load to the human operator due to the difficulty of control, the maintenance becomes more difficult, it necessitates trainings…

Hollnagel relates risks to the increase of new system's complexity and thus, to the increase of system's coupling [Hollnagel, 2008 b]. This type of design lets more difficult to understand the problem in order to pinpoint the significant risk which constitutes the basis of traditional "risk analysis" methods as the tree fault method. In this regard, many authors [Fadier & De la Garza, 2006; Hollnagel, 2008 b; Suh, 2001] have pinpointed the fact that more complex the system is more complex the control will be and then the implementation of efficient safety solutions become more complex. The surveillance and control role of the operator is therefore increased.

From product design point of view, the current support tools available to assist designers in safety integration task are very limited [Shupp, 2006].

- The existing techniques for risk assessment and design review generally intervene quite late in the design process, often only on the stage of detailed design, when significant decisions about product principles and structures have been taken. Existing methods that are used early in the design process generally set constraints and are used for verify and validate, rather than being design methods making safety part of the design objective.
- Current safety solutions can lead to various delays and cost increases when safety problems are considered too late in the product design.

- The information relative to experience feedbacks often arrives to designers in a relatively haphazard and narrative way, and is usually related to specific accidents in a specific context. There is no support that contributes to abstract this information to integrate them more naturally in the preliminary design phase.
- …

In our research, we proposed a design method to integrate inherent barriers early in the design process. We consider inherent barriers as those implemented during the design process and taking part of the design functionality. The objective of this paper is to develop the proposed systematic risk analysis approach. This approach takes part of a conceptual model for risk reduction. Thus, before developing the concepts of the proposed approach, we will firstly introduce the proposed risk reduction model. Secondly, the fundamentals of the axiomatic design are introduced. Then, a brief state of the art of the use of the axiomatic design to ergonomic design is reviewed. Finally, the preliminary results to our case study are presented.

2 CONCEPTUAL RISK REDUCTION MODEL IN THE DESIGN PROCESS

The proposed conceptual risk reduction model for human-safety (Figure 1) is developed in the framework of the systematic design approach [Pahl & Beitz, 1988] that divides the design process into several main stages: conceptual design, embodiment design and detailed design. Our model consists on a general suggestion for systematic safety integration in the early design throughout the product development process. The starting point of the model is the use of the experience feedbacks to control the design from the safety point of view. Risks are thus, defined from the one hand, by the information arisen on ground and from the other hand, by the analysis of design choices at each phase. So, the risk analysis needs a formal description of the design process.
The traditional way to integrate safety into the design consists on exploring the consequences of risks related to the experience feedbacks arisen on ground and then to implement corrective actions by modifying the detailed solution.

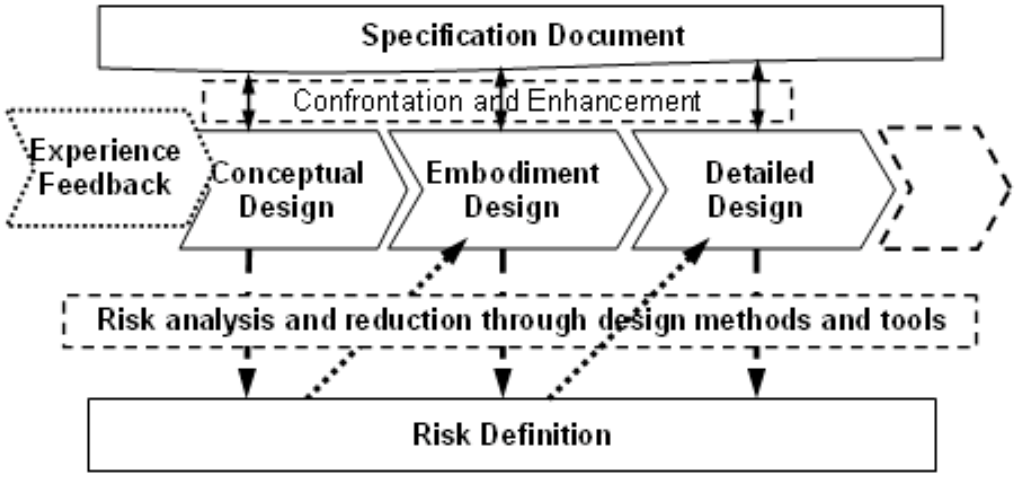

Figure 1. Conceptual risk reduction model

In our approach, we consider that to integrate safety efficiently during the design, we have to work on the elements that may cause risks "which risk is associated to a used resource?" rather than considering the consequences "what happened to cause the risk?" and this is throughout the product development process. Risks result from the interaction of the human with the design resources as functions, energy, space, time, performances… So, these interactions are analyzed and potential risks are listed. The experience feedbacks are used to investigate the nature of risks related to the studied context and then to the surroundings (environment, machines…) and those related to the technology used in design (through standardizations).
Indeed, the risk reduction process is divided into three main levels; 1) risk identification and problems definition, 2) risk reduction by problems solving 3) product validation from technical and safety viewpoints (by the confrontation to the specification document and defined safety indicators). We propose to use the current design methods and tools for a formal analysis and reduction process. Then, it keeps to know which methods and tools are the most placed to fit our objective.
The proposed approach for systematic risk analysis constitutes the first level of the process; the risk identification and problems definition (the part of the model shown in Figure 2). We have based this level on the axiomatic design principles.

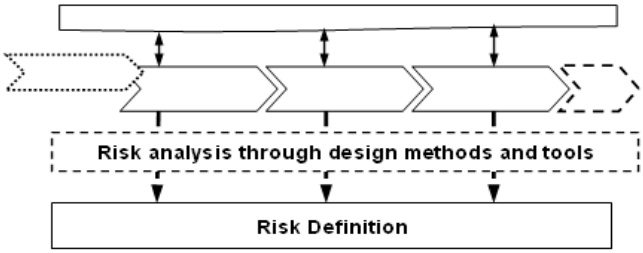

Figure 2. Risk analysis process

3 THE AXIOMATIC DESIGN THEORY

3.1 FUNDAMENTALS OF AXIOMATIC DESIGN

There are four fundamental concepts in the AD: (1) design as a mapping process; (2) design abstraction in the form of a top-down, hierarchical structure; (3) design laws in the form of axioms; (4) design matrix as a notation for representing functional dependencies [Lo & Helander, 2007; Suh, 2001]. A basic introduction of these concepts is provided below.

3.1.1 DESIGN AS A MAPPING PROCESS

The AD design process is an interaction between four domains: the customer, the functional, the physical and the process domain (Figure 3).

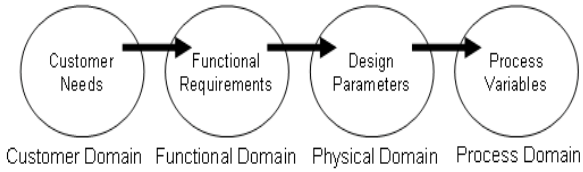

Figure 3. AD design process [Suh, 2001]

Design is conceived as a mapping process between these domains. This mapping describes the transition from one domain to another. The input of a domain represents "what we want to achieve?" and the output of the domain represents "how we propose to achieve it?".

3.1.2 DESIGN TOP-DOWN HIERARCHICAL STRUCTURE

Design usually consists in decomposition with multiple abstraction levels. The higher levels are more abstract, the lower levels are more detailed. The design process has to begin at the system level and to continue through levels of more detail until a point that is enough to clearly represent the design object. This process is called hierarchical decomposition and its outcome is depicted by a tree-model in each one of the four domains.

3.1.3 DESIGN AXIOMS

Suh has formulated the principles (or axioms) of a good product design:

1. The independence axiom (First axiom): Maintain the independence of the Functional Requirements (FR);
   In an acceptable design, mapping between the FRs and the Design Parameters (DP) is such that each FR can be satisfied without affecting the other FRs.
2. The information axiom (Second axiom): Minimize the information content of the design.
   If a set of a design that satisfy the same FRs and conform to the independence axiom, the best one is the one with the minimum information content. The Information Axiom provides a quantitative measure of the merits of a given design.

3.1.4 DESIGN MATRIX

The relation between functional requirements and design parameters is represented in a matrix, which allows evaluating the structure of the product. At a given abstraction level, the relation between the FRs and the DPs can be written as:

$$[FR] = [B]\,[DP] \quad (1)$$

Where [B] is the design matrix.

Designs that satisfy the independence axiom have either a diagonal or triangular design matrix and they are known as, respectively, uncoupled and decoupled designs.

Designs that have neither a diagonal nor a triangular design matrix are known as coupled design [Suh 2001].

3.2 AD FOR ERGONOMIC ANALYSIS

In the literature of the Axiomatic Design, several authors have determined the assets of the theory to analyze products from ergonomic point of view.

Basing on the axiomatic design matrix, a Design Equations for Systems Analysis (DESA) methodology has been developed to study the human-machine systems [Helander & Lo, 2007; Helander, 2007]. Thus, the methodology consists of four domains; User Goals, Functional Requirements, Design Parameters and User Actions; modeling the human-machine system functionally and structurally (Figure 4).

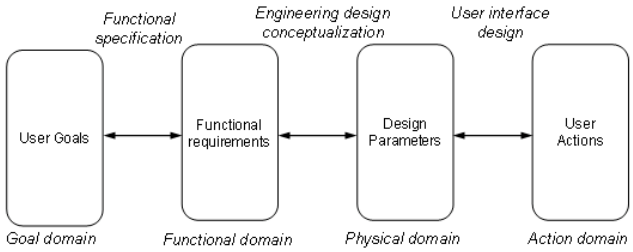

Figure 4. DESA methodology [Lo & Helander, 2007]

The advantages of this approach are:

1. It is an analytical approach to ergonomic evaluation for those with little formal education in ergonomics;
2. It is a formal way to predict the usability of a design;
3. It highlights the relation between poor engineering designs versus poor user interface design.

However, this methodology describes the rules of usability design and then takes into account only the user action to meet a specific user goal. Thus, it consists in analyzing globally the artefacts from design and usability point of view.

Nevertheless, Karwowski describes the rules of a good ergonomic design that consists in the human-artefact compatibility [Karwowski, 2005]. The two axioms of the Axiomatic Design are adapted for ergonomics design purposes. The axiom 1 stipulates the independence of the functional compatibility requirements and the axiom 2 stipulates the need to minimize the incompatibility content of the design. Ergonomics design is defined as mapping from the system-human compatibility needs to relevant compatibility requirements. The system-human compatibility is expressed in terms of human capabilities and limitations at the beginning of the design process. The aspects of preventing from hazards are not taken into account.

Other authors [Heo&al., 2007] used the Axiomatic design principles to develop the fault tree to analyse the reliability

of the design parameters used to meet the functional requirements (Figure 5).

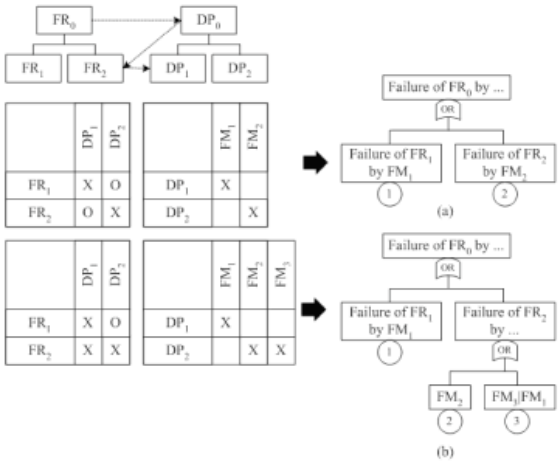

Figure 5. Conversion of a FR-DP hierarchical tree into a Fault Tree [Heo & al., 2007]

Each of the approaches reviewed above has focused in a specific aspect of human-safety (artefact controllability, artefact compatibility with human limitation and physical parameters failure modes). None of them have integrated the aspect of risk of accident and thus none of them can be considered as a complete and systematic approach to analyze human safety and to integrate inherent barriers at the early design phase.

4 USE OF AD FOR SYSTEMATIC RISK ANALYSIS

The proposed approach is based, from the one hand on the systematic design that divides the design process into three main stages: conceptual, embodiment and detailed design; and from the other hand on the AD principles. As explained before, the AD defines four domains to describe the design process: the customer, the functional, the physical and the process domains.

As in the AD, the systematic safety design is conducted by the axiom of independency that insures a good design. In addition, this type of design allows studying more easily the human-machine interface in the detailed design phase. Thus, in our approach the design is divided into functional and physical domains. The relation between the functional and physical domain and the systemic design has been described by Ge & al. [Ge & al., 2002] and called the extended axiomatic design. This approach decomposes each stage of the systematic design into two domains, functional and physical and the design process is divided into six phases (Figure 6).

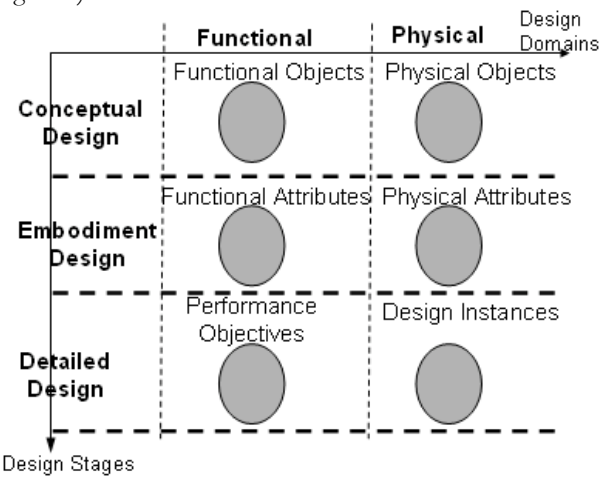

Figure 6. The EAD phases

The asset of the Extended Axiomatic Design (EAD) is to cover the lack of the systematic design process integrated to our model. In fact, the systematic design constitutes a description of the multiple tasks (What to achieve?) that have to be implemented to develop a product. In any case this process describes the way to fulfill these tasks (How to achieve it?). This lack shows the need to complete the systematic design by an approach that allows the transition from the "what" to the "how" in a formalized way in each phase of the development process. We have to notice in [Gonçalves-Coelho, 2003], *the AD's functional trees are not similar to the function structures resulting from Pahl & Beitz's "systematic approach"*.

To analyse the risks systematically, we have considered that to each phase of the EAD corresponds risk knowledge and then the transition from the design phases to the risk knowledge constitutes a mapping process. This risk knowledge allows the risks definition.

The mapping process describes the interaction between the human characteristics and the design (Figure 7). The Risk Analysis Process (RAP) describes the risks induced by this interaction.

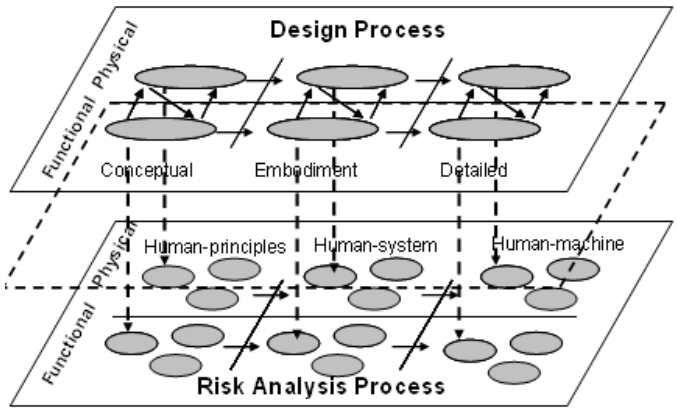

Figure 7. An overview of the mapping process between the design phases and the risk analysis contexts

As for the design process, the RAP is divided into three stages according to the abstraction levels of the solution. Thus, we noticed the Human-Principles Interaction (HPI), Human-System Interaction (HSI) and the Human-Machine Interaction (HMI). The HPI corresponds to the interaction between the human and the design solution in the conceptual design phase. The HSI corresponds to the interaction between the human and the design solution in the embodiment design phase. Finally, the HMI corresponds to the interaction between the human and the design solution in the detailed design stage. To each phase of the design corresponds one or many contexts in the RAP. At the conceptual design stage, all the risks that may be induced by the available resources are considered.

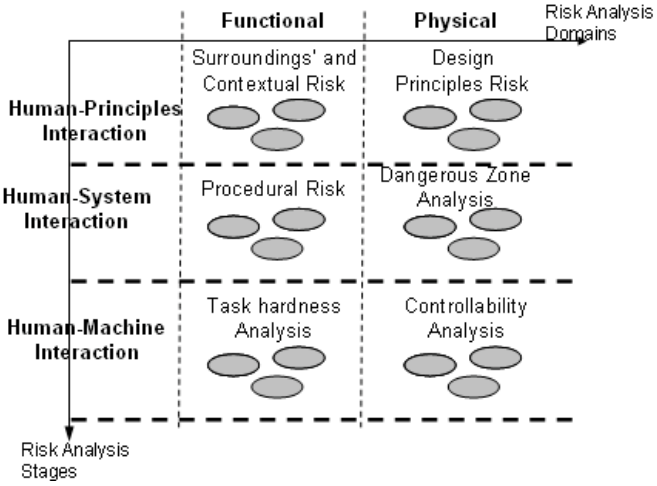

Figure 8. Risk analysis contexts

Every stage of the RAP is divided into Functional and Physical Interaction (FI and PI respectively). According to the nature of the interaction phase/context at each domain and each stage, the FI provides the solution analysis from ergonomics and human factor points of view; procedural, contextual and task analysis. However, the PI contributes to analyse the risk of accident and incident related to the design choices, and has as attributes the dangerous zone (nature, volume and localisation), the energy used and the controllability analysis (Figure 8).

4.1 MAPPING TO RISK ANALYSIS PROCESS

The risk analysis is considered as a characterization of the injuries that may touch the user over the use phase. The risk can be related to the interaction of the human with the functional or physical domain.

Due to the different characteristics between the design phases and the risk analysis contexts (concepts versus knowledge) the transition is not straightforward. The mapping process can be one-to-one, many-to-one or one-to-many. We consider that inherent barriers can be implemented in the solution functional requirements as they can be implemented in physical choices. For example, the impact of injuries is variable according to the required performance objectives. The same is true depending on the physical choices.

In the sequel of the paper, the collected knowledge and then the risk contexts at each stage is developed.

4.2 THE RISK DEFINITION PROCESS

Each context of the risk analysis process formalizes an aspect of the risk definition. These contexts are detailed as following:

Context 1: surrounding's and contextual risk (Figure 9)

1. Describe risks related to the product's surroundings (machines, ground, atmosphere, operators…); Define their nature and severity;
2. Point out the functions that necessitate the operator intervention and formulate the safety functional requirements;
3. Characterize the operator typologies (body's measurements, physical and mental limitations…);
4. Analyse the experience feedbacks and set safety indicators constraints (not developed in this paper).

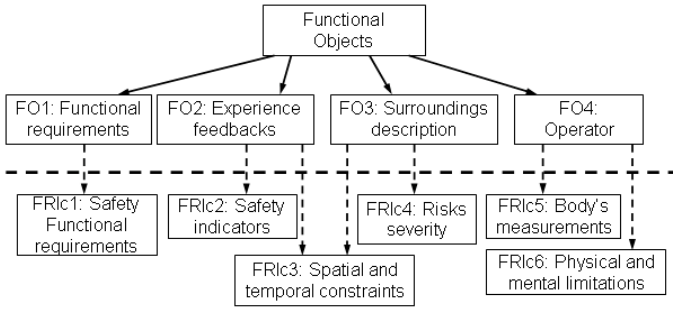

Figure 9. Mapping Phase 1/ Context 1

Context 2: design principles risk (Figure 10)

1. Analyze the severity of the available resources;
2. Determine the volume of the potential Dangerous Zone (D-Z) according to the power and the propagation way of the energy used.

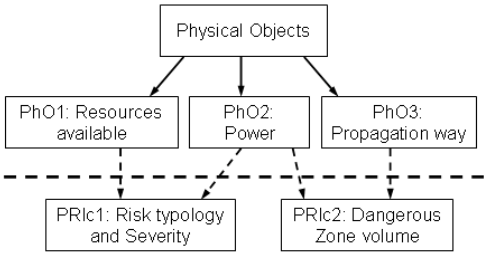

Figure 10. Mapping Phase 2/ Context 2

Context 3: procedural risk (Figure 11)

1. From the functional structure of the product and regarding the sub-functions that necessitates operator's intervention (determined in context 1), identify the possible localizations of the operator;
2. Predict the occurrence of the intervention and the required time to accomplish the function.

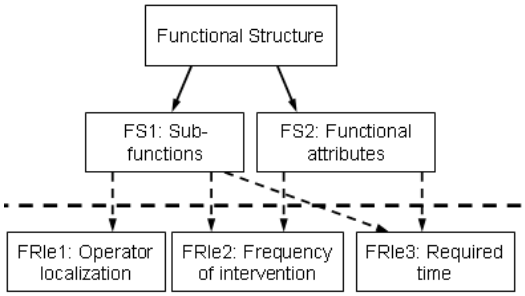

Figure 11. Mapping Phase 3/ Context 3

Context 4: dangerous zones (Figure 12)

1. Localize the dangerous zone related to the physical structure of the product,
2. Confront the potential operator localization and body's measurements with the dangerous zone location and identify the members that may be affected;
3. Classify the dangerous zone from the severity point of view taking into account the severity of the energy, the member affected, the time passed in the zone and the frequency of intervention.

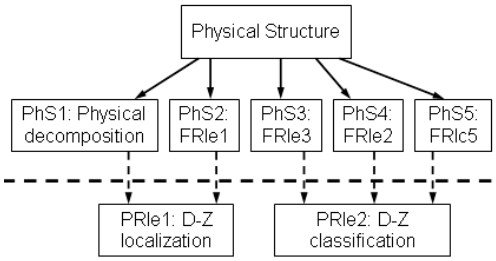

Figure 12. Mapping Phase 4/ Context 4

Context 5: tasks hardness (Figure 13)

1. Evaluate the hardness of tasks according to the human physical limitations when required performances are met;
2. Evaluate the hardness of tasks according to the human physical limitations when required performances are not met.

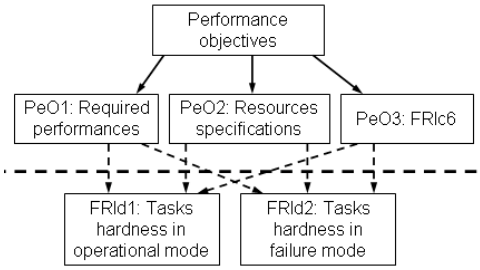

Figure 13. Mapping Phase 5/ Context 5

Context 6: controllability (Figure 14)

1. Evaluate the product controllability according to Axiomatic Design independence axiom;
2. Analyze the consequences when the controller fails.

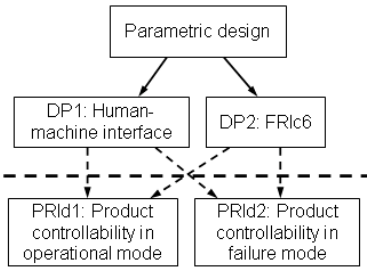

Figure 14. Mapping Phase 6/ Context 6

As can be seen, the context 6 that corresponds to the detailed design phase doesn't integrate the traditional risk analysis method for barriers implementation. We consider that safety in integrated throughout the design process through the inherent barriers.

5 PRACTICAL APPLICATION

Nowadays, the agricultural sector constitutes a serious problem in the domain of safety and health. The French Research Institute for Agricultural Engineering in collaboration with the Agricultural Social Insurance has defined a research framework to solve this problem. In fact, the agricultural hitches that let to link an agricultural implement to a tractor constitute the main source of accidents. Recent French statistics demonstrate that the only hitching/unhitching phase generated 3764 accidents from 2000 to 2004. Several factors have led to this situation. One of them resides in the fact that the existing system (called the three points hitch) is the result of 80 years of evolution. Concretely, this evolution is restricted to local modifications and adaptations of the system to his environment. Our purpose is to re-conceive the hitching system (Figure 15) by taking human-safety and the experience feedbacks into account. In the sequel, the application of the proposed approach (Figure 2) to the tractor-implement hitch, called the three-point hitch, is developed.

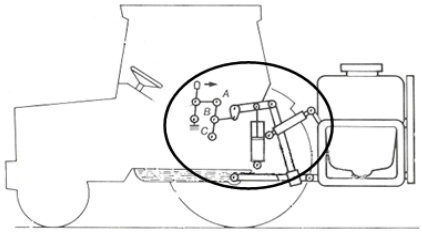

Figure 15. The design boundary

5.1 CASE STUDY: THE THREE-POINT HITCH SYSTEM

The three-point hitch is a system dedicated to link a mounted-implement to a tractor. This typology of implements has the particularity to be entirely lifted by the tractor. Figure 16 shows the typical three points hitch system, which is composed by three arms: a pair of lower hitch arms (1 and 2) and a third upper hitch arm (3). The lower arms are pivotally connected to the tractor through a ball joint connection and are retained by link arms (4 and 5) that are pivotally connected to each lower hitch arm. The upper ends of the link arms (4 and 5) are connected by ball joints to the link arm mounts (6 and 7) respectively. The lower arms can be raised and lowered by the movement of the arm-mounts, which are actuated by hydraulic pistons.

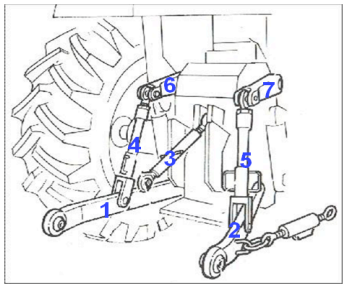

Figure 16. The typical three points hitching system

This system is mostly characterized by his adaptability to any kind of implements (plough, seeder, sprayer…), whatever its size and the localization of its hitching points.
To link the implement to the tractor, operator firstly, sets up the lower arms, vertically, by actuating the arm-mounts. The

arm-mounts can be actuated from the inside or the outside of the tractor. The free ends of the lower arms are assembled to the lower implement hitching points. Then, the third upper arm is manually adjusted and fixed. So, the operator is involved in most of the system's adjustments. These adjustments require from the operator to get into the dangerous zone.

The functional analysis (FA) provided by the Figure 17, illustrates the interdependence between the operator and the system's parts. The super-systems elements are shown by white boxes and subsystems by grey boxes. The effective functions are illustrated by continuous relations. The useful unsafe functions are shown by discontinuous relations.

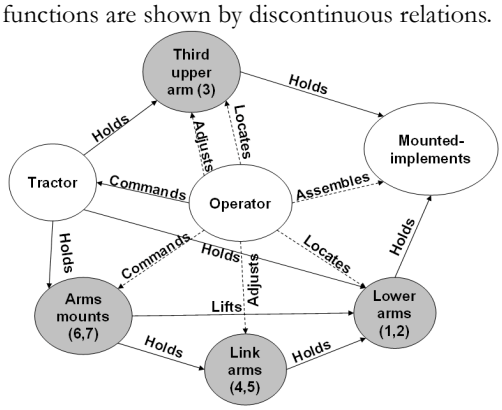

Figure 17. FA overview of the typical three-point hitch

5.2 THE EXPERIENCE FEEDBACK

The hitching operation highlights some difficulties for the operator. The following information is provided from the ground's feedbacks in normal use situation. This list has no exhaustive character:

1. it requires the presence of the operator sometimes inside and sometimes outside the tractor;
2. the mounted-implement is unsteady during the hitching operation;
3. the operator is led to interfere in the dangerous zone (the zone between the tractor and the implement);
4. the assembling of the lower arms to the implement is usually difficult because of the non-horizontality of the ground;
5. the third arm is usually high placed and hard to reach;
6. most of the arms are adjustable independently which increases the difficulty of the operation;
7. …

5.3 THE FUNCTIONAL REQUIREMENTS

FO1: Link rigidly a mounted implement

- → FS 1: Positioning the hitch points
- → FS 2: Setting up the implement in the Z direction
- → FS 3: Rotate the implement around the X axis
- → FS 4: Rotate the implement around the Y axis

To explain the multiple required mobility, we have associated the (X, Y, Z) reference to the rear of the tractor as shown in Figure 17.

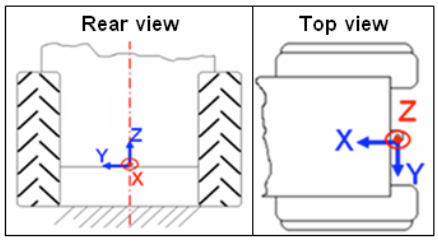

Figure 18. The R reference

5.4 THE SURROUNDING ELEMENTS

The surrounding elements related to the tractor-implements hitch context are stated in Table.1 with their own attributes.

Table 1. Surroundings elements related to the TIH

Human: characteristics
Morphological measurements
Physical and mental limitations
Experience
Environment: characteristics
Climate
Obstacle
Grounds topology and typology
Implements: characteristics
Dimensions
Weight
Required Powers
Tractor: characteristics
Type
Power
Dimensions

5.5 THE RISK DEFINITION

The mapping from the design to the risk definition by the application to the TIH is developed in Table 2. This process allows formulating and localizing safety problems through the product development process. Risk is defined from its root to its consequences by the related function, energy, operator, performance, surroundings and components.

Table 2. TIH risk definition

Phase	Design	Description	Context	Risk analysis	Description
Phase1: Functional Objects	FO 1	Link rigidly	**Context 1: surroundings and contextual**	FRIc 1	Safety requirement: Minimize human involvement
	FO 2	Experience Feedbacks		FRIc 2	Safety indicators: to be determined
	FO 3.1	Tractor		FRIc 4.1	Risk: Limited visibility
	FO 3.2	Implement		FRIc 4.2	Risk: Instability
	FO 3.3	Ground's nature		FRIc 4.3	Risk: Sliding
	FO 3.4	Atmosphere		FRIc 4.4	Risk: Dust, Frost, Heat, Rain…
	FO 4	Operators		FRIc 5	Limitations: Human body's measurement
				FRIc 6.1	Limitations: Mental limitation
				FRIc 6.2	Limitations: Physical limitation
Phase2: Physical Objects	PhO1.1/ PhO2.1	Hydraulic energy/ 200bars	**Context 2: design principles**	PRIc 1.1	Risk severity of hydraulic energy: serious
	PhO1.2/ PhO2.2	Mechanical energy 540/1000rpm		PRIc 1.2	Risk severity of mechanical energy: serious
	PhO1.3/ PhO2.3	Electrical energy 12/24V		PRIc 1.3	Risk severity of electrical energy: safe
Phase3: Functional structure	FS 1.1	Positioning the hitching points	**Context 3: procedural**	FRIe 1.1	Localization for FS 1.1: outside the tractor
	FS 1.2	Setting up in the Z direction		FRIe 1.2	Localization for FS 1.2: inside the tractor
	FS 1.3	Rotate around the X axis		FRIe 1.3	Localization for FS 1.3: outside the tractor
	FS 1.4	Rotate around the Y axis		FRIe 1.4	Localization for FS 1.4: outside the tractor
Phase4: Physical structure	PhS1.1/ FRIe1/FRIc5	Link arms mounts positioning	**Context 4: Dangerous Zone**	PRIe 1	D-Z localization: zone limited by the lower arms, the back of the tractor and the implement
	PhS1.2/ FRIe1/FRIc5	Control the link arms length			
	PhS1.3/ FRIe1/FRIc5	Control the third arm length		PRIe 2	D-Z classification: Implement run over the operator, sliding … → serious risk
	PhS 1.4	Human operator			
Phase5: Performance objectives	PeO 1	Z displacement +1000m	**Context 5: task hardness**	FRId 1	In operational mode: Difficulty to reach the third arm → ergonomic problem
	PeO 2	Y regulation ±100 mm		FRId 2	In failure mode: operator is lead to lift the implement (~10T) → ergonomic problem
	PeO 3	X regulation ±100 mm			
Phase6: Design Parameters	DP 1	Three hitching arms	**Context 6: controllability**	PRId 1	In operational mode: the design matrix is coupled → difficult to control

6 CONCLUSION AND PERSPECTIVES

This paper presented a systematic risk analysis approach based on the axiomatic design principles. The asset of the axiomatic design resides in its formal description of the design process. Then as for the design process the risk analysis process is divided into two domains; functional and physical domains. According to the partition of the product development process into three abstraction levels, the proposed approach is composed by six contexts. Each context gives a new point of view of the potential risks incurred by the users. The AD gives a formal tool for the engineer to study systematically in the early design process the risk reduction aspects. The applicability of the approach to a practical case study has been demonstrated. Our approach allows defining the typology of the risks and the way to measure them. In future studies, the objective is to complete the proposed conceptual risk reduction model by determining from the one hand, the tools that allow resolving safety problems generated by the proposed risk analysis approach and from the other hand, the safety indicators based on the experience feedbacks to evaluate safety at each design phase.

7 REFERENCES

Fadier E. (2008) "Editorial of the special issue on design process and human factors integration", Springer-Verlag, Cogn Tech Work, pp.1-5

Fadier E., De la Garza C. (2006) "Safety Design: Towards a new philosophy", Safety Science, vol. 44, No.1, pp. 55-73

Ge P., Lu S. C.-Y., Suh N. (2002) "An axiomatic approach for target cascading of parametric design of engineering systems", Annals of the CIRP, vol. 51, No.1, pp. 111-114

Gonçalves-Coelho A.M., Mourão A., Pamies-Teixeira J.J. (2003) "Axiomatic design as a background for concurrent engineering education and practice", 10th International Conference on Concurrent Engineering: Research and Applications, pp. 419-427

Helander M.G. (2007) "Using design equations to identify sources of complexity in human-machine interaction", Theoretical Issues in Ergonomics Science, vol. 8, No.2, pp. 123-146

Heo G., Lee T., Do S.H. (2007) Interactive system design using the complementarity of axiomatic design and fault tree analysis, Nuclear engineering and technology, vol. 39, No.1

Hollnagel E. (2008 a) "Risk + barriers = safety?", Safety Science, vol. 46, pp. 221-229

Hollnagel E. (2008 b) "The changing nature of risks", published online: http://erik.hollnagel.googlepages.com/Changingnatureofrisks.pdf

Karwowski W. (2005) "Ergonomics and human factors: the paradigms for science, engineering, design, technology and management of human-compatible systems", Ergonomics, vol. 48, No.5, pp. 436-463

Lo S., Helander M.G. (2007) "Use of axiomatic design principles for analysing the complexity of human-machine systems", Theoretical Issues in Ergonomics Science, vol. 8, No.2, pp. 147-169

Pahl G. (1988) Beitz W., "Engineering design: A systematic approach", Springer Verlag, New York

Sklet S. (2006) "Safety barriers: Definition, classification and performance", Journal of loss prevention in the process industries, vol. 19, pp. 494-506

Suh N. (2001) "Axiomatic Design: Advances and Applications", Oxford University Press

Shupp B., Hale A., Pasman H., Lemkovitz S., Goossens L. (2006), "Design support for systematic integration of risk reduction into early chemical process design", Safety Science, vol. 44, pp. 37-54

