INTERNATIONAL DESIGN CONFERENCE - DESIGN 2006
Dubrovnik - Croatia, May 15 - 18, 2006.

DESIGN 2006

CONTRIBUTION TO MAINTAINABILITY AND SAFETY ASSESSMENT IN THE MECHANICAL PRODUCT DESIGN

A. Coulibaly, R. Houssin and B. Mutel

Keywords: product behaviour, semantic modeling, reliability, maintainability, safety, CAD systems

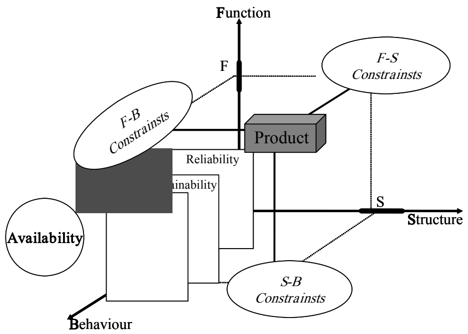
1. Introduction

Evaluating the product performances before manufacturing at early design stage is of great importance to avoid errors costs. Traditionally only functional and structural performances are performed by the designers. Unfortunately, there is a lack of efficient tools for behavioral performance evaluation for domains like availability and its components that are reliability, maintainability and safety which are semantically specified and need formal tools or rules to be assessed. These last years some investigations have been done in this area to take into account other lifecycle constraints at the early stage of the design process. At the MIT, the Design Structure Matrix (DSM) research team has developed a new approach for modeling product data and other constraints all over the lifecycle. A generic FBS (Function, Behavior and Structure) product modeling concept proposed by [Gero 1990] and other derived models like FBS-PPR developed by [Labrousse 2002] are some major contributions for capturing product data and other associated processes in a global and multi-representations model. Such models are not specifically focused on product performance evaluation. On the other hand different industrial tools using virtual reality systems are proposed to verify product functionalities and to analyze its maintainability and reliability. But usually such systems are used very late after the product is completely designed. In addition these approaches are very expansive and difficult to perfom during design. This paper is focused on the prediction of the product Maintainability and Safety at the early stage of design using CAD system. We use a product Behavioral modeling approach based on the FBS concept as outlined in [Coulibaly 2003].

2. Product model for Behavioural assessment

Our behavioural modeling approach (figure 1 a) aims to provide a generic approach for evaluation of product performance at different situations of its lifecycle. Here, we attempt to predict maintainability and safety at design stage using semantic data and criteria associated these aspects.

The product design solution is assumed to consist of multi-components structure built by a set of components which are bind together by different types of assembly links. So that if some of them are made from detachable fasteners, the product can be broken down into sub-systems, or single parts, by removing the links. The product Structure is represented with a CAD model that specifies the geometry and dimensions of the different components and their topological interrelationships. This CAD model is enriched with additional semantic data concerning non graphic characteristics like material properties, functional criticality (K_i), reliability (R_i) or safety (S_i). We represent these data using the Product Semantic Matrix representation as shown is figure 1b. In such representation a n-components product is described by its C_i (with $i=1...n$) components, nb_i is the number of occurencies of component C_i, Link type (C_i, C_j) = L_k is the assembly type between two components C_i and C_j. L_k can take different values depending on how the two components are assembled (Table 2). K_i, R_i and S_i stand respectively for: the functional criticality, reliability and safety associated to component C_i. The functional criticality levels can be estimated by the designer depending on the relative importance of the different components. The components individual reliability can be determined as indicated in the following section.



(a)

Components	C_1	--	C_i	---	C_n	Criticality	Reliability	Safety
C_1	nb_1					K_1	R_1	S_1
¦	¦					¦	¦	¦
C_i	Link type $(C_i, C_1)=L_i$		nb_i			K_i	R_i	S_1
¦	¦					¦		
C_n	Link type $(C_n, C_1)=L_{n,1}$	---	Link type $(C_n,C_i)=L_{n,i}$	---	nb_n	K_n	R_n	S_1
Number of links	d_1		d_i		d_n	K_0	R_0	S_0

(b)

Figure 1. Behavioural modeling approach and the Product Semantic Matrix

3. Reliability estimation

We assume that the product has an acceptable level of reliability. This condition can be ensured by using methods proposed by [Zwingmann 2002] to estimate reliability using virtual samples tests in a CAD system. This approach is based on the Strain-Stress method which is used to estimate the reliability R_i for the different components. Where R_i is defined as the probability that this component performs its function in a given conditions over a its life time. Let T be the product life time, then the reliability is expressed as :

$$R_i(t) = Pr\,(t<T) \tag{1}$$

For a multi-component product reliability is expressed by:

$$R(t) = \prod_{i=1}^{n} R_i(t) \tag{2}$$

R(t) can be determined in the design process using CAD system that contains a finite element method module.
The next following sections present our approach for maintainability and Safety assessment.

4. Maintainability assessment

4.1 Maintainability criteria

The maintainability is commonly defined as the characteristics of equipment design and installation that provides the ability for this equipment to be repaired easily and efficiently. From the user point of view, maintainability refers to the aspects of a product that increase its serviceability and reparability, increase the cost-effectiveness of maintenance, and ensure that the product meets the requirements for its intended use, [Dhillon 1999]. For high integrated products consisting of mechanical parts, electronic devices and software the maintainability assessment must take into account all these different aspects. Here, we consider the case of basic mechanical products with no electronic

equipments and no software. In this case the maintainability depends on the complexity of the structure: i.e. the geometry of parts and how components are assembled.
Depending on what activities are considered, maintainability can be affected by actions beginning from the Failure detection and those concerning Diagnostic, Reparation and Control. Maintainability depends on all criteria that may affect the main maintenance steps with different actions to be carried out to bring the product back to its functional status. Table 1 presents the different types of criteria that affect maintainability.

Table 1. Maintainability criteria classification

Intrinsic Criteria	Reparability, Accessibility, Dismountability, Assemblability, Disassemblability, Standardisation, Interchangeability. Survivability, Redondance.
Contextual Criteria	Competencies, tools, logistics
Mixed Criteria	Surveillability, Detectability, Testability, Manœuvrability, auto diagnostic.

Intrinsic criteria are those depending on the product structure configuration. Contextual criteria depend on the maintenance context including human and equipments resources
Here we focus on intrinsic criteria that are the most important for alternative solutions comparison.
To assess the maintainability we consider the time required to detect components or subsystems failures and to bring the product back to its operation conditions. Let, T_{Maint} be this overall time, it can be defined as:

$$T_{Maint} = T_{FD} + T_{Diag} + T_R + T_C \qquad (3)$$

Where: T_{FD} is the Failure Detection time, T_{Diag} is the Diagnostic time, T_R is the Reparation time and T_C is the Control time.
To increase product serviceability all these different times must be as shorter as possible. In practice, to evaluate the maintainability, the 1010/CCT specification defines the MTTR (Mean Time To Repair) as a most significant criterion. Usually this measure is obtained from statistical data collected over a certain period of product utilization. This can be suitable for existing products. But at design stage, in the case of new products for what no statistical data exists, the MTTR may be estimated by using simulation methods or any other techniques. Several investigations mentioned in [Dhillon 1999], present contributions on the integration of maintainability criteria in the product design process. These works try to give some rules to apply for the design for Maintainability.
The MTTR is defined as the total time required for making diagnostic, reparation or replacement and control.

$$MTTR = T_{Diag} + T_R + T_C \qquad (4)$$

The diagnostic time, T_{Diag}, depends on the type of failure. It can be instantly in the case of break of main components. But it can also take from a few minutes to much longer period if the failure occurred progressively as in the case of parts wear. Thus the T_{Diag} is practically difficult to be estimated at the design stage. In the other hand the control time, T_C, requires to verify that the product works properly is generally. This time can very short or can imply a long period of settings. Here, this time is not taken into account. The time devoted to reparation or replacement tasks, T_R, is usually the most important characteristic that determines product maintainability. T_R depends on many criteria like: Disassembly/Assembly operations to be performed, components Accessibility, components or sub-assemblies Manoeuvrability, Reparability and Maintenance resources. In this study we consider the criteria of Disassembly/Assembly operations. In the following sections, we present an approach to predict the maintainability using a module that can be implemented in conventional CAD systems environment.

4.2 Maintainability performance indicator

This is the general case where the disassembly sequences are determined for all of the different components. Let S_N^k, then the optimal disassembly sequence to access to the component k, where N is the number of components to remove to reach the target component k. $\mathrm{Re}\,move(S_{N-i+1}^k, i)$ is the time required to remove the component i in the remaining sequence after the (i-1) first components have already been removed. This time depends on the type of assembly technique used between the different components. In table 2 we give a relative level of difficulty for different assembly techniques.

Table 2. Assembly types required time valuation

Link type	No link	Contact	Housing	Welding	Screwin g	Glueing	….
Required time	0	1	7	10	3	8	….

Then the time required to reach a target component, k, is defined by(5) and then we express the general maintainability indicator for the whole product by (6).

$$R_{time}^k = \sum_{i=1}^{N} \mathrm{Re}\,move(S_{N-i+1}^k, i) \tag{5}$$

$$I_M = \sum_{k=1}^{n} R_{time}^k \tag{6}$$

Where n is the total number of components or sub-assemblies that the product consists of. For better maintainability, I_M must be as smaller as possible.

This general maintainability indicator gives a global idea of the product complexity but it is not significant information for choosing between different design solutions. In fact, it does not take into account components criticality. In the case of criticality-based maintainability, the indicator is evaluated by taking into account only critical components identified in the product. Then we define a criticality-based maintainability indicator, I_M^*. This assumes that the product may consist of N components but only a few of them are considered to be critical. The criticality is defined here as the ability of the system to operate with a certain failure tolerance depending on the components technical functions.

So, for each component a criticality level can be defined on a scale ranging from 1 to 0. The criticality will be set to 1 for the components that cause the system to stop working when they fail. The level 0 is affected to components with no influence on the system operation. And, while modeling a product the designer may attribute criticality level to the different parts. Then, it becomes possible to assess a maintainability performance for a given level of criticality, χ, by:

$$I_M^* = \sum_{k=1}^{N^*} R_{time}^k * w_k \tag{7}$$

Where $N^* = |\Omega|$, is a number of critical components, $\Omega = \{component \in product/criticality \geq \chi\}$ and w_k is the criticality level of the component k,$w_k \in [0,1]$. This indicator can be used to compare different alternative design solutions.

5. Safety assessment

Why and how to integrate the users safety of complex systems into CAD systems? The answer of the first question is the subject of several publications quoted in [Hasan 2003]. To answer the second one,

it is necessary to distinguish the necessary methods and tools. As regards methods we find those proposed by the standards and applied in companies. Where designer treats safety problem once he finishes the product functional design. Safety integration in the last phases of design causes several problems [Hasan 2006].
This late integration is, on one hand, the fruit of consciousness lack of the importance of the integration of safety as soon as possible in design. On the other hand, because of the lack of tools and methods to assistant designer. What leads us to the second part which concerns tools. As it is quoted above CAD is a basic tool for the designers. In [Hasan 2006] a method has been proposed to integrate as soon as possible the safety in design process.
We propose to integrate the model proposed by Hasan [Hasan 2006] in the bevioural model to evaluate at design stage users safety throughout product lifecycle. This is done through risks analysis to determine an Indicator of Safety *(I_S)*. This indicator allows to appreciate the level of the users safety. It is given by the following equation:

$$I_S = FRis * IRis \quad (8)$$

Where, *FRis* is the factor of Risk which concern the existence of a risk and *IRis* is the Index of Risk which concern its qualification and quantification. For better safety, I_S must be as smaller as possible.

5.1 Factor of Risk (*FRis)*

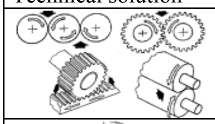
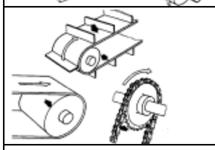
This indicator gives a potential risk which appears in case of incident or accident. There are a damage to users once this indicator has a value different from zero. It is the product of the following criteria:

$$FRis = Ph * Zo * InH \quad (9)$$

Where

- *Ph* is the dangerous phenomenon resulting form technical solution identification. This criterion takes one of two values 1 (there is) or 0 (there is not) a dangerous phenomenon. In CAD, choosing or drawing a solution allows to define the value of this criterion. In table 3 we presented some examples of technical solutions, associated dangerous phenomena and some of it parameters. These values are stored in a database. Nevertheless, for each technical solution already stored designer find the dangerous phenomena generated by this solution.
- *Zo* is a dangerous zone generated by a dangerous phenomenon. Designer should size the zone in which there is a danger. This criterion could take values 0 or 1. It takes the value 0 if the zone is not penetrable by man or by one of his organs. For example the zone between two miniscule gears in a watch does not penetrable so *Zo=0*. If not, it takes the value 1.
- *InH* is human intervention in a dangerous zone. This criterion takes one of two values: 1 if there is a human intervention in the identified zone and 0 if not.

Table 3. Technical solutions and associated dangerous phenomena

Technical solution	Dangerous Phénomène	Parameters
	Destruction Training Burn	- couple, - dimensions, - material, - shape, …
	Destruction Training Severing Shock	- couple, - tension, - dimensions, - force, - speed,…
…..	….	….

It is possible to modify one of the previous parameters to cancel the value of this indicator. If it is not possible, in that case it is necessary to determine *IRis to* quantify the risk.

5.2 Index of Risk (*IRis*)

It allows to calculate a value of risk to estimate its acceptability or not. The acceptability of risk is defined by the compagne with regard to its activities. So we proposed to calculate *IRis* as following:

$$IRis = Gr * Ex * Pr * Ev \tag{10}$$

Where:

- *Gr* is the gravity of risk which depend on the nature (cut, burn), level (a finger wound, or a hand cut) of dangerous phenomena and on the number of persons touched by this dangerous phenomena (one or many operators).
- *Ex* is the exposure duration and frequency. It concerns the socio-technical realization of a tasks identified in the dangerous zone.
- *Pr* is the probability of dangerous event happening. It is obtained by studying system human reliability [Fadier 1998].
- *Ev* is the possibility of avoiding. It depend on the happening nature of incidents or the accident (degradation or not). Il allows to estimate the possibility that the operator discovers the accident or the incident before that this last one to take place. This requires among others to study and to analyze the modes of possible technical and human failings.

Once I_S is determinate, designer compare its value with a reference value. He can also compare two value for to solutions. While in our case, system does not yet exist, it is more difficult to determine this indicator a priori.
The integration of these criteria in a system CAD requires the availability of the semantic data concerning the safety. A list of the dangerous phenomena engendered by technical solutions drawn in CAD must existed in a database (table 3). For a new solution it is necessary to enter the dangerous phenomena which does not exist in the database. Then, designer must determine and define dangerous zone from the geometrical data and verify if user go in this zone [Hasan 2006]. If the answer is yes, the indicator *FRis* is equal to zero and it is necessary to determine *IRis* to estimate the risk. A not acceptable value of *IRis* requires a modification which can concern one of four criteria (decrease the exposure duration or frequency). These data have to enrich the available geometrical and topological data in CAD. Some data are to extract form standards or they result from designers experiences.

6. Application

Figure 2 shows an example with a partial representation of a gearbox. To satisfy the specified function designer has several alternative technical solutions.

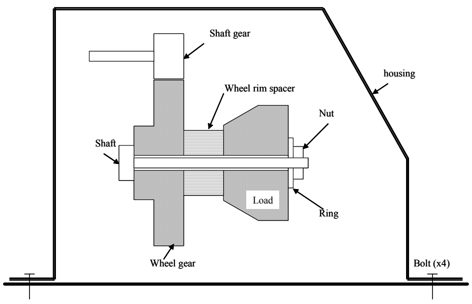


Figure 2. Gearbox (partial view)

For a given set of solutions, we have to study for each solution its performance with respect to maintainability and safety. We have to determine (I_M) and (I_S). We consider solution S1, consisting of the gearbox without a housing. Here the shaft gear and the wheel gear are considered to be the most critical components from the maintainability and safety points of view. We ensure that the reliability is better than 95% for these two components by using virtual samples tests method .

For safety assessment, I_S is estimated for S1: according to (Eq.8) it is necessary to calculate $FRis_1$ and $IRis_1$. According to (Eq.9) we could notice that the solution for transferring the movement between the two axis, uses two gears turn in opposite senses. Then there is a dangerous phenomena which is the danger of destruction between gears so *Ph*=1. If designer handles a new solution which not stored before, then he must stores the solution with all its characteristics.
Zo is calculable from the solution geometrical data existing in all CAD systems. For our example we find that the danger zone has a penetrable size by a human organ so *Zo* has the value 1. As regards *InH*, there is a human intervention so designer give *InH* the value 1. This value is determinate by the designer, in analyzing that operator does some task in this zone.
$FRis_1$ =1 means that a risk of destruction exists. It is necessary, in this case, to calculate the index of risk (*IRis*). By using (Eq. 10) every enterprise according to its domain determine scales for each of *Gr, Ex, Pr* and *Ev*. To evaluate the value of *Gr* we define a scale from 1 to 10. For the treated example the gravity is estimated at 5 (destruction of one finger between both gears). *Ex* has its values on a scale form 1 to 2 so for a strong frequency and enough weak duration *Ex* =1,5.
The criterion *Pr* (on a scale form 0,5 to 1,5) can have the value 1,5 because the dangerous zone is accessible by user so a dangerous event is very probable. *Ev* = 1 for a not foreseen event. It take its values on a scale from 0,5 to 1. This allows to have a value of I_{S1} = 1,5 for the solution S1. For this solution operators safety is clearly not assured. So we consider an alternative solution, S2, where the operators safety is ensured by the putting of a housing component. In solution S2 the risk is suppressed by using the housing (*Ph*=1, *Zo*=0 for not penetrable zone, *InH* = 1) so $FRis_2$ = 0. So we don't need to evaluate $IRis_2$ and $I_{S2} = 0$. This integration has been implemented in a demonstration software (Figur 3).

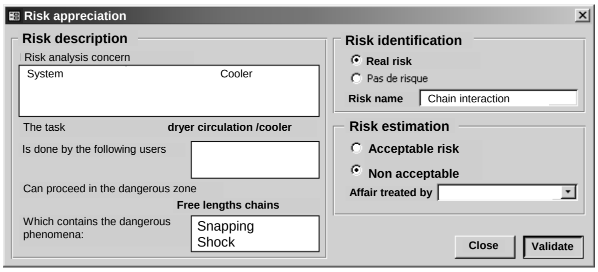


Figure 3. A window form devolpped demonstrator

To assess the maintainability, we assume that a maximum criticality level is associated to these same components (shaft gear and the wheel gear). L et K_i=1 for of both. Then we determine the I_{M1}, I_{M2} for solutions S1 and S2. The housing influences the maintainability because it adds a new component which increases the necessary time for disassembly operations. So solution S2 is less maintainable than S1. The different indicators determined using the above methods are summarised in Table 4.

Table 4. Performance indicators for design solutions

	Maintainability	*Safety*
Solution S1	I_{M1}=7	I_{S1}=1,5
Solution S2	I_{M2}=11	I_{S2}=0

These results may be used to allow the designer to decide for the acceptability for evaluated solutions depending on the requirements constraints. Then the final choice of the best solution will be the solution with defining a compromise between maintainability and safety aspects. As regards other indicators, this study allows to analyze the question early enough in the design process. What allows to take into account in a systematic way maintainability and safety.
This relative evaluation give an idea about the product behaviour at any step in the design progression. We can note that, the choice decision is a multi-criteria optimisation problem. In the other hand there are two levels of contradiction to solve. First one, between this three indicators. Improving one of

them could degraded one or both the other. For instance, the use of the housing improves the safety but causes the lost of maintainability. The second one is between the solutions. If S1 have a very good I_M and bad I_S and S2 have a very good I_M and bad I_S which solution designer well choose. The balanced indicators allows to have a compromise which could be a bad solution. These points are the subject of our actual study.

7. Conclusions and future works

In this paper, an approach is presented for maintainability and safety assessment in the design process using CAD model enriched with behavioural semantic data. This is a very helpful tool to assist designers for taking into account semantic behaviors that are traditionally evaluated after the design is finished by using physical tests and/or other virtual reality devices. The application outline has shown the feasibility of our approach.

The present results are limited to provide specific performance indicators of the product but do not show how to improve availability. For choosing between different alternative design solution multi-criteria approaches may be used to lead to better compromise. In addition, we have not considered the influence of the context related to maintenance tools, logistics or the role of human operators when we determine the indicators. All these aspects may be treated in future works with the challenge aiming to determine performance indicators for the different lifecycle points of view.

References

Gero, J.S., "Design Prototypes: A Knowledge Representation Schema for Design", Artificial Intelligence Magazine, Vol. 11, No 4, 1990, pp. 26-36.

Coulibaly A., X. Zwingmann, D. Ait-Kadi, B. Mutel "Formalisation des contraintes de maintenabilité des produits mécaniques à partir de Modèles de CAO". Int. Journal of Design and Innovation, Research, Vol. 3, N°1&2, 2003, pp. 67-80.

Dhillon B.S. "Engineering Maintainability, How to design for reliability and easy maintenance?" Ph. D, University of Ottawa, ISBN 0-88415-257-X, Gulf Publishing Company, 1999.

Fadier, E. "l'intégration des facteurs humains à la conception,travaux actuel et perspectives de recherches" la revue de la sûrete de fonctionement – numéro spécial, 1998, pp. 59-78.

Hasan R., A. Bernard, J. Ciccotelli et P. Martin. "Integrating safety into the design process: elements and concepts relative to the working situation" Safety Sciences J. Safety by design. Vol. 41/2-3, 2003 pp. 155-179.

Hasan R., A. Bernard, P. Martin, G. Ris, and F. Cherrier, "Information system based on the working situation model for an original concurrent engineering design approach" Journal of Engineering Design, 17 No 1, 2006.

Labrousse, M., A. Bernard "Lodèle FBS enrichi pour la modélisation des processus d'entreprise" roceeding of CPI Conference 2003,Marocco.

Lambert A. J. D. "Disassembly sequencing: a survey", International Journal of Production Research, vol. 41, no. 16, 2003, pp. 3721-3759.

Schuëller,G.I. "Recent Software Developments for Structural Reliability Assessment" In PSAM 5 Probabilistic Safety Assessment and Management n°2, Universal Academy Press, Tokyo, Japan, 2000, pp. 1229-1234.

Zwingmann X., Aït-Kadi D., Coulibaly A., & Mutel B. "Product reliability assessment using virtual samples". IEEE International Conference on Systems, Man and Cybernetics, n°3, 2002, pp. 629-634.Hammamet.

Amadou Coulibaly, Associate Professor
LGECO, INSA de Strasbourg
24 Bd de la Victoire, 67084 Strasbourg, France
Tel.: (+33) 3 88 14 47 00
Fax.: (+33) 3 88 14 47 99
Email: amadou.coulibaly@insa-strasbourg.fr
URL: http://www.insa-strasbourg.fr