Design for safety: proposition of a model to detect hazards through energy flows analysis

Nicholas de Galvez, Jacques Marsot, Patrick Martin, Ali Siadat, Alain Etienne, Xavier Godot

Design for safety: proposition of a model to detect hazards through energy flows analysis

Nicholas de Galvez[a,*], Jacques Marsot[a], Patrick Martin[b], Ali Siadat[b], Alain Etienne[b], Xavier Godot[b]

[a]*Institut national de recherche et de sécurité (INRS), 1 rue du Morvan, CS 60027, Vandoeuvre Cedex 54519, France*
[b]*Laboratoire de Conception Fabrication Commande, Arts et Métiers ParisTech, 4 rue Augustin Fresnel, Metz Technopole, Metz Cedex 3 57078, France*

* Tel.: +33 3 83 50 20 00; fax: +33 3 83 50 20 97. *E-mail address:* nicholas.degalvez@inrs.fr

Abstract

The European directive 2006/42/CE promulgates the machine safe design principles to prevent professional risks. However, outside machines that have specific safety standards, the designers of special machines and manufacturing systems can only use generic safety standards, limiting as a consequence the results of hazards detection. The aim of this paper is to present an original approach for this detection during the design of working equipment.
We based our study on a hypothesis of the literature that links hazards to the presence of energy flows. Thus, the hazards detection is reduced to the study of the building of energy flows and the detection of potential links between these flows and the operator. Thanks to such data, the designer will be able to select the best risk prevention solutions.
To reach this goal, we decided to use the Functional Energetic Model (FEMo) to model the technical system and its energy flows. This choice was made because this model was developed for the design of technical systems integrating different types of energy. By using this modelling, the designer can easily analyses every potential interactions between the energy flows and the operator, depending on the future working situations in each life cycle phases. Our approach builds on this model all along the design process, allowing the designer to early detect hazards and to apply at the best moment the risk prevention solutions.
We present the application of this approach during the design of a working equipment, since the definition of the raw need. We confirm that its application and the system modelling in the EFM formalism are possible since the conceptual design phase. Data from the next design phases enrich the model, and consequently improve the detection and characterization of hazards.

Keywords: Design; safety; human; machine; damage; predictive; decision making; feedback; analysis

1. Introduction

In 2013, out of the 618,623 work accidents declared in France, about 8% were associated with machines, and thus partially to production equipment [1]. Regarding these accidents in particular, and more generally occupational health and safety, “design” is a path of prevention whose advantages no longer need demonstrating, as it involves “integrated prevention”. This consists in applying safe design principles to an item of equipment as early as possible, a process set out in European directive 2006/42/EC known as “Machines” [2] and in the associated norms . The prevention strategy recommended in these texts focuses on the *a priori* evaluation of risks; it sets as objective for the machine designer the need to obtain the lowest possible level of residual risk in view of the state of the art.

However, apart from certain “standard” items of production equipment for which specific standards exist (known as type “C”) that incorporate this risk assessment, the designers of special production equipment can only rely on transversal standards (types “A” and “B”), especially standard ISO 12100 [3] relating to general design principles. It is also important to recall that “production equipment” design companies are mostly medium, small or very small enterprises. Indeed, according to the 2014 data

of the Chambers of Commerce and Industry in France, more than two thirds of these companies had fewer than 10 employees and 90% had fewer than 50. Therefore since the designers belonging to these SMEs/VSEs (project managers, engineers and technicians of engineering offices) are not specialised in "prevention" and have no formal resources or tools adapted to perform *a priori* risk assessments, they are limited, on the one hand, to the risk families closest to their field of experience (for example, mechanical), and on the other hand, to carrying out this assessment more often at the end of the project, once all the technical solutions have been defined. Furthermore, the data required for risk assessments (seriousness, frequency and/or exposure, probability of occurrence, possibility of avoidance) are not directly linked to the design data, thereby widening the gap between design and safety. Occupational health and safety requirements are thus treated as constraints of adaptation and correction instead of design.

In response to this issue, we propose an approach to assist designers of special production machines to identify hazardous phenomena. As shown in figure 1, this approach, based on the Functional Energetic Model (FEMo) [4] must enable linking the parameters with those used in risk assessment methods (ISO 12100 [3] and ISO 14121 [5]). In particular, these works will be focused on architectural and detailed design phases since it is essentially in these phases that the technical choices that give rise to most hazardous phenomena are made.

To be the most efficient, this approach has to verify the four following characteristics:

- **generic:** in front of the different types of risks, the different design approaches followed and the sectors of activity of the enterprises concerned;
- **inductive:** based on the design parameters (causes) to ascertain hazardous phenomena (effects);
- **dynamic and traceable:** certainty of taking into account the evolution of the characteristics and the configuration of the system's components during the different design phases,
- **integrated and/or compatible with current design tools and methods:** this ensures interoperability. It must also be monitored and instrumented with indicators of potential risks in order to quantify and use the data.

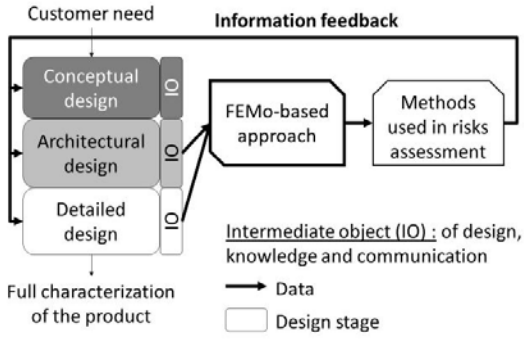

Fig. 1. Positioning of the risk identification approach proposed.

2. Literature review

Initially, a literature study is performed in two areas: that of design in view to defining the impact of different approaches to the generation of design parameters, and that of integrating prevention in design to identify the parameters used to estimate risks.

2.1. Definitions

For the sake of clarity, and on the basis of the literature, we propose a definition and a classification of some terms linked to design. Thus we consider that a *design approach* is a set of *design phases* (first stage design, detailed design, etc.), as they structure the *design activities* (structure of the control architecture, definition of system functions, etc.). The latter are composed of five *design tasks*, sources of design data (parameters, intermediate objects) (cf. fig. 2). The intermediate objects (IO) construct with a professional viewpoint the data flows between activities [6-8].

2.2. Design approaches

A large number of works on design approaches are identified in the literature to solve all kind of problems [9-15]. They can mainly be distinguished by their way of organising the design phases and activities. However, the tasks [16] and intermediate objects (deliverables) [10] are generic. In his thesis on "project-data" interaction « during the design of a multi-technology product, Godot [16] established that a design activity could be summarised by the five following tasks: creation, dimensioning, representation, optimisation /evaluation and validation.

Our approach therefore will use these elementary tasks and the parameters generated from them, since they are independent from design approaches and their formalisation (cf. fig. 1). This point is essential as the enterprises targeted are mostly VSEs/SME which seldom take a formal approach to design.

2.3. Risk prevention in design

Research works on integrating occupational risks in production system design mainly focuses on two areas: the design process and risk evaluation. In both cases, these works present limits regarding our problem.

Those who focus on the design process mostly propose methods that call on collaborative project reviews [17]. The reduction of risk in general, and the identification of hazardous phenomena in particular, are based on cooperation between the different actors during these project reviews. Therefore this type of approach does not guide the designer in decision-making when they work independently in front of their workstation [18]. Furthermore, when these project reviews are performed using numerical mock-ups or physical prototypes, this type of approach must be sufficiently advanced in the design process to analyse the risks [19].

Regarding works on risk assessment, i.e. the determination of an index used to classify potential risks, they are generally specific to a single type, for example

mechanical risk [20]. Moreover, the methods proposed are essentially focused on the approach taken to combine the different parameters involved in assessing risks. These parameters are quite similar from one method to another. As recommended by standard ISO 12100 [3], these parameters include seriousness damage, frequency /duration of exposure, probability of occurrence of a hazardous event and the possibility of avoidance. The main difference between the methods proposed concerns the number of levels used to evaluate these parameters and how they are combined: matrix, graph, numerical equation, abacus, and chart. Consequently, these works do not provide a response to our problem, which is to identify hazardous phenomena.

Analysis of the literature nonetheless made it possible to identify three approaches that *a priori* provide a response to our problem and to the criteria expected (generic, inductive, dynamic and integrated): the works of Coulibaly et al. [21], the "PAG" multi-agent system [22], the "IRAD" method [23] and the work situation model "MOSTRA" [24]. Respectively, they propose a Factor of Risk (FRis) indicating whether a risk is present or not, additional indicators for numerical mannequins, a method for simultaneously developing technical and safety functions and, lastly, a model that facilitates the inclusion of multi-viewpoint data through the notion of risk,

Although the goals of these works are related to our problem, they sometimes require the generation of parameters that do not appear directly in design [21], or which intervene too late in the design process [22]. Also, they do not always explain how hazardous phenomena are identified [23]. Lastly, they do not systematically define the direct link between design parameters and hazardous phenomena [24].

In spite of the above, several of these works agree on the fact that hazardous phenomena are linked to the notion of energy [23, 25, 26]. Hazardous phenomena of mechanical, electric and thermal origin, and those linked to physical nuisances (noises, vibrations, electromagnetic radiation) can be linked directly to energy parameters (potential energy, kinetic energy, electric currents, thermal energy, electric/magnetic fields, acoustic power, etc.).

On the basis of this hypothesis, our problem is to identify energy flows. Thus we extended our literature analysis in this direction. Energy flows can be represented using different types of Bond-Graph model [27] and the functional energy model (FEMo). Initially developed to analyse existing complex systems, this model based on the notion of energy flow circulation has been completed to guide designers when designing a product [4]. As shown in figure 2 below, this model is based on four elements or representations:

- **frontiers** that delimits a production system, a subsystem or a component in relation to its external environment;
- **functional surfaces** that designate the interfaces via which a production system, a subsystem or a component has links with its environment. They are crossed by one or more energy flows and are characterized by extensive magnitudes (quantity of material, movement, energy, etc.);
- **links** that associate two functional surfaces that do not belong to the same component. They therefore characterise the interfaces that can be classed into three types: conductive (C), semi-conductive (SC) or insulating (I);
- **internal links** that associate two functional surfaces belonging to the same component. They can also be conductive, semi conductive or insulating.

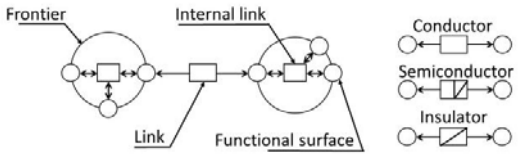

Fig. 2. Illustration of the elements of the functional energy model [4].

Since this model also allows representing the operator(s) of the system with the same elements, we decided to build our approach on this basis in order to study the circulation of energy flows in a system, localise the links with the operators and thus identify the potentially hazardous phenomena. The fact that this model had already been the object of computerisation also partially responded to one of the criteria regarding the operational and integrated nature of the approach considered. An improvement of the integration is currently in progress.

3. Approach

3.1. General principles

The FEMo provides a global and uniform view of the different energy flows within a man/machine system. The identification of hazardous phenomena linked to these energy flows becomes systematic by identifying all the possible interactions between the operators and the functional surfaces of the system. It is through the latter that the energy flows of the system are transmitted.

The designer can therefore be made aware of these potential links. Then, they can define solutions on each of them to control the energy flows from the system to the operator and vice-versa (cf. fig. 3). Indeed, the operator can exert a "mechanical" energy which is a source of accidents (e.g. sudden movement against a sharp edge).

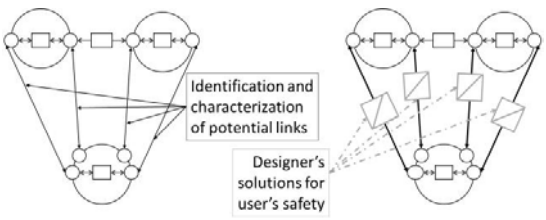

Fig. 3. Identification and prevention of transfers of energy to the operator.

Depending on the type of energy (and thus hazardous phenomena) and their level, the links must either prohibit the passage of energy flows (e.g. contact with mobile transmission components), or control them (e.g. reduction of efforts to be provided by the operator). From this point,

these mechanisms become means of protection. This modelling of flows for future machine tools and working equipment can be reiterated to study the different phases of the life of the product to be designed (utilisation, maintenance, setting, etc.) to ensure a maximum level of safety throughout the life-cycle of the item of equipment. Thus the FEMo becomes an intermediate object capable of alerting designers and communicating on hazardous phenomena [6].

3.2. Extension of the FEMo to all hazardous phenomena

Initially, the FEMo was developed by modelling the main energy flows used in systems (mechanical, electric, electromagnetic) in view to analysing these systems. However, it is necessary to widen the notion of energy in order to deal with all the hazardous phenomena defined by standard ISO 12100. First, the notion of energy needed to be extended to allow the approach to work on hazard phenomena linked to noise, chemical products and the disrespect of ergonomic principles.

By reusing the concept of generalized variables [4], the generalised effort and generalised current of every type of energy can be defined to link them to the common notion of power.

4. Proposal of a table of generalized variables and its use in hazard characterization

The mechanical domain was first described as comprising three types of energy: kinetic energy (part in movement), potential energy (the mass of objects) and elastic/static energy (pressurised gas, springs, etc.). This is expressed in the first three lines of table 1.

By analogy, and by using standards ISO 12100 (mechanical), NF C15-100 and NF C13-200 (electric), NF X35-112 (thermal), NF EN 62471 (light radiation), NF EN 60825 (laser), NF EN ISO 14253 (vibration), ISO 11688 (acoustic), directive 98/24/EC (chemical/biological), NF EN 1005 (biomechanical) coupled with standard ISO 14121, these generalised effort and current have defined the domains of chemistry, acoustics, and biomechanics.

These generalised variables or their combination (generalised power) will define the energy flows crossing the functional surfaces of the FEMo. It is therefore these that will give rise to “alerts” to the designer regarding the potential presence of hazardous phenomena. For example, the specification of a velocity of a part to the ground is a primary parameter for detecting kinetic energy. Indeed, the object driven by this velocity is a hazardous phenomenon of mechanical type due to its kinetic energy.

However, generalised variables are not enough to define a hazardous phenomenon with precision. Let us take the case of the generalised current (velocity) of a part in movement. The nature of the material (rigid or flexible) the state of the surface of the part in movement (ex. : smooth, rough), its shape (sharp or blunt edge), its position in relation to other fixed or mobile parts, etc. will have an impact as decisive on the level of risk as the initial energy parameters.

Table 1. “Generalized” efforts and currents.

Type of energy	Generalised effort	Generalised current
Mechanical (translation) *Kinetic energy, potential energy*	Force (N)	Velocity (m/s)
Mechanical (rotation) *Kinetic energy*	Torque (Nm)	Angular velocity (rad/s)
Mechanical (pneumatic / hydraulic) *Elastic/static energy*	Pressure (P)	Flowrate (m^3/s)
Electric	Voltage (V)	Intensity (A)
Thermal	Temperature (K)	Heat flow (J/s=W)
Radiation (electromagnetism)	Magnetic fields (Tesla)	Magnetic flux (Weber)
Radiation (light)	Wavelength (m)	Spectral density (W/m)
Radiation (laser)	Wavelength (m)	Photon flux (s^{-1})
Vibration	Acceleration ($m.s^{-2}$)	Exposure time (s)
Acoustic	Sound intensity (dB)	Exposure time (s)
Chemical / biological	Chemical/biological potential (J/mol)	Molar flux (mol/s)
Biomechanical	Force (N)	Velocity (m/s) and/or frequency

Likewise, regarding the domain of biomechanics, the efforts linked to the weight of a part to be handled and the frequency of this action are not enough to qualify the presence of a hazardous phenomenon linked to conformity or nonconformity with ergonomic principles. The shape of the part, the presence or absence of handles, the dimensions of the work station, etc. will determine the type of handling and posture, and thus have a decisive impact on the level of biomechanical stress.

Thus it can be seen that it is necessary to draw a “map” of the design parameters linked to each generalised variable to define the indicators that identify and characterise hazardous phenomena. These works are in progress and the map below the first elements involving mechanical risk (cf. fig. 4).

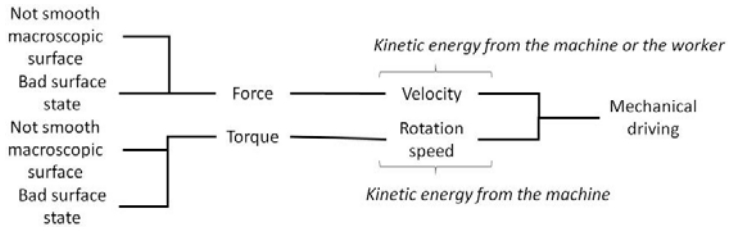

Fig. 4. Extract of the causal diagram of design parameters for driving/trapping mechanical risk.

The links between the left trees and the right one represent the contribution of a parameters to the hazardous phenomenon of being drive or trap by a part animated by a velocity. This hazard exist since there is a velocity coupled with a torque or a force and a not smooth macroscopic surface or a bad surface state.

The completion of this map is currently in progress by using the previous references and particularly the different formulas used to assess risks. The main one linked the risk to the calculus of the severity of a damage and its likelihood of exposure. However, some risks are unavoidable and their assessment are linked to the dose of the hazard phenomenon received instead of the likelihood of exposure (ex.: heat, vibration, noise). Finally, risks linked to the disrespect of ergonomic principles are assessed by the analysis of the exertion required, the posture of the user and the frequency of this action.

Once completed, this map will be the base for the FEMo. Through the insertion of design parameters in the FEMo and combining them the way the map shows it, it is possible to study the construction of a hazard phenomenon and eventually inform the designer of its evolution. Thus, he might be able to act before the complete construction of the hazard.

5. Discussion

Modelling an item of production equipment with FEMo can therefore be performed from the architectural design phase and more particularly when a flowchart or kinematic diagram of the system structuring elements is available. Plus, this model was used by different group of student and none had any problem to use it, nor have results about the identification of hazard phenomena. This model makes it possible to represent on the same diagram all the energy flows within the limits of the system during a chosen phase of life or work situation.

In order to make an exhaustive survey of the hazardous phenomena linked to the system, this model must be applied to all the phases of life and work situations having different energy configurations. The energies present and the potential interactions with the operators are not necessarily the same in the assembly, production or maintenance phases.

The map of links between the design parameters and those used for the risk analysis should then permit characterising the functional surfaces of the FEMo to provide increasingly more detailed information on potential hazardous phenomena to the designer.

Figure 5 shows the sequence of the different steps of the approach proposed: from the identification of energies present in the system to the characterisation of hazardous phenomena.

To finalise our approach, and in addition to the “map” of design parameters mentioned previously, our works are continuing in two directions:

- The first focuses on the dynamic treatment of the parameters and the traceability of the process to allow the designer to modify decisions taken earlier.
- The second focuses on the approach to the conceptual design phase, and more specifically from the creation of the functional architecture. The difficulty lies in the fact that this stage comprises few or non-defined energy flows. The main energy information that can nonetheless be used is that linked to the stakeholders: the type and characteristics of the materials and consumables used (the cutting capacity of a tool or metal strip, the toxicity of a solvent, glue application temperature, etc.).

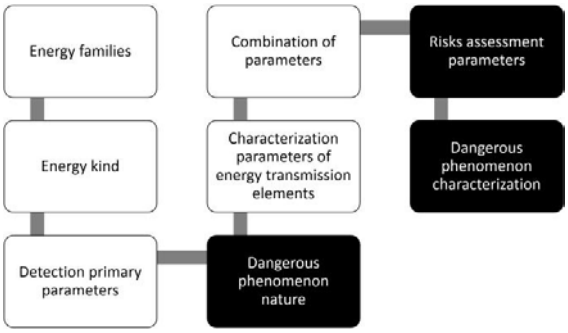

Fig. 5. Proposal of design parameter analysis (white) – and parameters used in the risk analysis (black).

By obtaining this information about the hazardous phenomena of his work throughout the design phase, the designer can therefore define the means for prevention which will evolve at the same time as the technical solutions, facilitating their structural, energetic and logical integration.

This study is currently being performed in the framework of a PhD thesis in the joint INRS-ENSAM laboratory. The different points raised are therefore in the process of development in order to obtain a fully functional approach.

6. References

[1] Ministère du Travail, de l'Emploi, de la Formation professionnelle et du Dialogue social - Direction générale du travail. Conditions de travail - Bilan 2013 - Conseils d'orientation sur les conditions de travail. 2013.

[2] European Comission Enterprise and Industry. Directive 2006/42/EC of the european parliament and of the council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast); 2006.

[3] Standard. ISO 12100:2010 - Safety of machinery - General principles for design - Risk assessment and risk reduction. AFNOR; 2010.

[4] Roucoules L and Eynard B. Background and specifications for a computer Co-operative Design Environment for Concurrent Engineering, in 8th ISPE International Conference on Concurrent Engineering : Research and Applications - CE'2001. 2001: Anaheim (Californy), 28 July- 1st August.

[5] Standard. ISO 14121:2007 - Safety of machinery -- Risk assessment. AFNOR; 2007.

[6] Jeantet A. Les objets intermédiaires dans la conception - Eléments pour une sociologie des processus de conception. Sociologie du Travail. 1998. n°3/98 291-316.

[7] Pahl G and Beitz W. Engineering design: A systematic approach. Springer Science & Business Media; 2013.
[8] Suh NP , The Principles of Design. New York: Oxford University Press; 1990.
[9] Garro O, Salau I, and Martin P. Distributed Design Theory and Methodology in the Context of Concurrent Engineering. Concurrent Engineering: Research and Application. 1995. 3(1): p. 323-311.
[10] Scaravetti D, Nadeau JP, Pailhès J and Sebastian P. Structuring of embodiment design problem based on the product lifecycle. International Journal of Product Development. 2005. 2(1): p. 47-70.
[11] Tichkiewitch S and Veron M. Methodology and product model for integrated design using multiview system. Annals of the CIRP. 1997. 46(1): p.81-84.
[12] Tomiyama T, Gu P, Jin Y, Lutters D, Kind C and Kimura F, Design methodologies: Industrial and educational applications. CIRP Annals - Manufacturing Technology. 2009. 58(2): p. 543-565.
[13] Lutters E, van Houten FJAM, Bernard A, Mermoz E and Schutte CS. Tools and techniques for product design. CIRP Annals - Manufacturing Technology. 2014. 63(2): p. 607-630.
[14] Roy R, Hinduja S, and Teti R. Recent advances in engineering design optimisation: Challenges and future trends. CIRP Annals - Manufacturing Technology. 2008. 57(2): p. 697-715.
[15] Koren Y, Hu SJ, Peihua and Shpitalni M. Open-architecture products. CIRP Annals - Manufacturing Technology. 2013. 62(2): p. 719-729.
[16] Godot X, Etienne A, Siadat A and Martin P. Methodology to develop a geometric modeling process according to collaborative constraints. International Journal on Interactive Design and Manufacturing. 2014. p. 1-17.
[17] Lu SCY , ElMaraghy W, Schuh G and Wilhelm R. A scientific foundation of collaborative engineering. CIRP Annals - Manufacturing Technology. 2007. 56(2): p. 605-634.
[18] Hale A, Kirwan B, and Kjellén U. Safe by design: where are we now? Safety Science. 2007. 45(1–2): p. 305-327.
[19] Kjellén U. Safety in the design of offshore platforms: Integrated safety versus safety as an add-on characteristic. Safety Science. 2007. 45(1–2): p. 107-127.
[20] Hu J, Zhang L, and W Liang. An adaptive online safety assessment method for mechanical system with pre-warning function. Safety Science. 2012. 50(3): p. 385-399.
[21] Coulibaly A, Houssin R, and Mutel B. Maintainability and safety indicators at design stage for mechanical products. Computers in Industry. 2008. 59(5): p. 438-449.
[22] Shahrokhi M and Bernard A. A framework to develop an analysis agent for evaluating human performance in manufacturing systems. CIRP Journal of Manufacturing Science and Technology. 2009. 2(1): p. 55-60.
[23] Ghemraoui R, Mathieu L, and Tricot N. Design method for systematic safety integration. CIRP Annals - Manufacturing Technology. 2009. 58(1): p. 161-164.
[24] Hasan R, Bernard A, Ciccotelli and Martin P. Integrating safety into the design process: elements and concepts relative to the working situation. Safety Science. 2003. 41(2–3): p. 155-179.
[25] Haddon W. Energy damage and the 10 countermeasures strategies. J Trauma. 1973. 13(4): p. 321-331.
[26] Kjellén U. Prevention of accidents through experience feedback. Taylor and Francis; 2000.
[27] Núñez-Hernández I, Breedveld PC, Weustink PBT and Gonzalez-Avalos G. Analysis of Electrical Networks Using Phasors: A Bond Graph Approach. in International Conference on Electric Machines and Drive Systems. 2014. 8(7): p. 931-937.