A meta model framework for risk analysis, diagnosis and simulation

H Kanj, Jean-Marie Flaus

▶ **To cite this version:**

H Kanj, Jean-Marie Flaus. A meta model framework for risk analysis, diagnosis and simulation. Safety and Reliability Conference ESREL, Sep 2014, Wroclaw, Poland. 10.1201/b17399-280 . hal-01240818

HAL Id: hal-01240818
https://hal.science/hal-01240818

Submitted on 18 Feb 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A Meta Model framework for Risk Analysis, Diagnosis and Simulation

H. Kanj & J.-M. Flaus
Univ.Grenoble Alpes, G-SCOP, F-38000 Grenoble, France
CNRS, G-SCOP, F-38000 Grenoble, France

ABSTRACT

The goal of risk analysis is to identify events that may have one or several undesirable consequences on a system, and to assess the likelihood and severity of these consequences. A lot of methods may be used to conduct risk analysis such as Preliminary Hazard Analysis (PHA), and Failure Mode Effects Analysis (FMEA). In most of these methods, the obtained information may be used to build a risk model.

Very often, the next step after risk analysis is, to study the behavior of the system if the undesirable events occur, in order to evaluate its performance in degraded conditions and its robustness or resilience. An approach allowing integrated risk analysis and simulation would be desirable. Such an approach has been proposed for business process management [Tjoa et al., 2011].

The goal of this paper is to present a meta model, suited to socio-technical systems, that allows describing the system to analyze, the result of the risk analysis and the required aspects of dynamical system behavior in order automatically perform simulation under degraded conditions. The model is an extension of the FIS model presented in [Negrichi et al., 2012]. The meta model may also be used for fault diagnosis as it can be used for generating redundancy relation and performing root cause search [Flaus et al., 2011].

Our meta model consists of three main modules: the structural view, the dysfunctional view and the view of the evolution.:

- The structural view (SysFis): defines the architecture of the analyzed system, breaks it down into subsystems, and describes the characteristics of each subsystem and the material entities used. This is the basic view. that describes the structure of the installation or the analyzed object in a relatively simple manner, by showing the various interactions systems, and specifying, if necessary their functions and the material components (human, technical or informational) that compose them. This part also allows describing links between these elements. The purpose of this view is to provide a frame structure for the dysfunctional or behavioral view.

- The dysfunctional view (DysFis): is built when we realize the risk analysis, It is used for describing the risk analysis or malfunction. This analysis consists in identify, for each element of a system, states in which this element may result in an injury, or be unable to respond to requirements specified with the expected level of performance.

- The view of the evolution (SimFis):

  describes the behavior of the system in normal or degraded mode. It describes the dynamic behavior of the system. It is not necessary to construct this view to perform a simple risk analysis kind, or even to build a fault tree or a bow tie diagram. However, when we have this view, it is possible to simulate the operation of the system, including degraded mode. In addition, some elements of this view can be exploited for diagnostic or prognostic. The dynamical behavior of the system is described using:

  - a BPMN model for representing the sequence of activities,
  - an input/output processor model, with several possible configurations for modeling the flow transformation [Flaus, 2013, Karagiannis et al., 2010].

This model view is related to the structural and dysfunctional model obtained from risk analysis, allowing the generation of the simulation model based on the risk model. We are used this meta model to analyze the risk related to the transportation of dangerous goods by road, and we are detailed the loading function of this materials in a truck.

REFERENCES

[Flaus, 2013] Flaus, J.-M. (2013). *Risk Analysis: Socio-technical and Industrial Systems*.

[Flaus et al., 2011] Flaus, J.-M., Adrot, O., Ngo, Q. D., et al. (2011). A first step toward a model driven diagnosis algorithm design methodology. *Safety and Reliability for Managing Risk ESREL'11*.

[Karagiannis et al., 2010] Karagiannis, G., Piatyszek, E., and Flaus, J. (2010). Industrial emergency planning modeling: A first step towards a robustness analysis. *Journal of Hazardous Materials*, 181:324–334.

[Negrichi et al., 2012] Negrichi, K., Di Mascolo, M., Flaus, J.-M., et al. (2012). Risk analysis in sterilization services: A first step towards a generic model of risk. *Proceedings GISEH'2012*.

[Tjoa et al., 2011] Tjoa, S., Jakoubi, S., Goluch, G., Kitzler, G., Goluch, S., and Quirchmayr, G. (2011). A formal approach enabling risk-aware business process modeling and simulation. *Services Computing, IEEE Transactions on*, 4(2):153–166.

A Meta Model framework for Risk Analysis, Diagnosis and Simulation

H. Kanj & J.-M. Flaus
Univ.Grenoble Alpes, G-SCOP, F-38000 Grenoble, France
CNRS, G-SCOP, F-38000 Grenoble, France
hassan.Kanj@g-scop.inpg.fr
Jean-Marie.Flaus@g-scop.inpg.fr

ABSTRACT:
This document represents an overview of the Function Interaction Structure (FIS) modeling, where the goal is to represent a system and the risk analysis that is made, and to obtain a simulation model from the risk analysis. This model is able to show the results of risk analysis. This model is supplemented by information on its behavior, in order to generate the dynamic model in degraded mode. Our proposed meta model is also used to analyze the risk associated with a system such as: evacuation system, transport of dangerous goods, ...

1 INTRODUCTION

The goal of risk analysis is to identify events that may have one or several undesirable consequences on a system, and to assess the likelihood and severity of these consequences. A lot of methods can be used to conduct risk analysis (Flaus, 2013a) such as Preliminary Hazard Analysis (PHA) and Failure Mode Effects Analysis (FMEA)(Papadopoulos et al., 2004). In most of these methods, the obtained information may be used to build a risk model.The next step after risk analysis is to study the behavior of the system, when the undesirable events occur, in order to evaluate its performance in degraded conditions, and its robustness or resilience. An approach to allow integrated risk analysis and simulation has been proposed for business process management (Tjoa et al., 2011).

The aim of this paper is to present a meta model, suitable to socio-technical systems. This model allows describing the system to analyze, the result of the risk analysis, and the required aspects of dynamical system behavior, in order to automatically perform simulation under degraded conditions. The model is an extension of the FIS model presented in (Flaus, 2011, Negrichi et al., 2012). The meta model may also be used for fault diagnosis, as it can be used to generate redundancy relation and to perform root cause search (Flaus et al., 2011).

The remainder of this paper is organized as follows. Section 2 represents the first part of the FIS model, defines the architecture of the analyzed system, and describes the characteristics the system and the material entities used. This is the basic view. Section 3 represents the second part of the FIS model. It is built when we realize the risk analysis (Karagiannis et al., 2010). Section 4 displays the last part of the FIS model. It is assembled when we describe the behavior of the system in normal or degraded mode. An illustration of this method on transporting hazardous material by road is presented and discussed in Section 5. Finally, Section 6 concludes this paper.

2 SYSFIS VIEW

This part describes the structure of the equipment or the analyzed object, in a relatively simple manner by showing the various systems interactions, and specifying, if necessary their functions and the material components (human, technical or informational) that compose them (see Figure 1). This part also allows describing the links between these elements. The purpose of this view is to provide a frame structure for the dysfunctional or for behavioral view (Flaus, 2008).

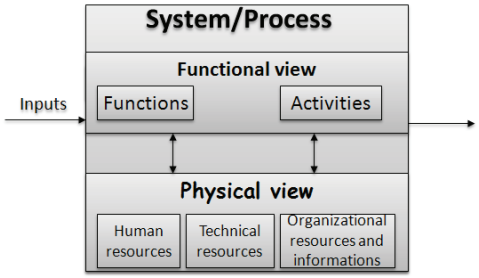

Figure 1: SysFis Model

2.1 *Elements of the model*

The basic element of the representation is the $process$ or $system$, composed of functions, physical resources and input/output ports. A process or system is seen as an organized set of activities that uses resources (personnel, device, equipment and machinery, raw material and information) to transform inputs into output elements. Each process or system is described internally by:

- The $structural\ elements$ (SE), known as $resources$ or $entities$, which consist of hardware (machinery and materials), informational, human and organizational activities to conduct the process activities. We distinguish machines, materials and processed parts, human actors, methods represented by procedures, software, The physical context characterized by variables such as temperature, the concentration of various products, the noise level ...

- The $functional\ elements$ (FE), called $functions$ or $system\ activities$, are defined as the role played by a set of resources in terms of purpose. It is a kind of dematerialization of a set of entities specifying what the system can do. This represents a specification of the system behavior. A function can be active or not active at a given time. Its behavior is characterized by a set of variables, and eventually by a performance model describing the temporal evolution.

It is possible to define for each system a structural element and a main functional components. A system is decomposed of subsystems, which themselves can be described by structural elements and/or functional components.

The advantages of this model for risk analysis are:

- on the one hand: it allows a description of the installation or the object analyzed, in an organized and hierarchical way. This description may be systemic, functional or structural where the different parts of the model are managed simultaneously.

- and on the other hand, it helps at the identification of risks, based on the category of the different elements of the model. For example, a risk of explosion types can be identified for the element "gas pressure".

Note: When modeling a complex reality, it is necessary to decompose it in several systems, and eventually subsystems.

2.2 *Links between model elements*

Relationships may be defined between the structural and functional elements of the model (Figure 2). To perform a function or activity :

- a number of incoming items may be necessary, they are consumed or brought using information, there are "inputs" for the function. This is the case of a raw material, a part to be assembled or a sensor;

- other elements are generated where there state is modified, resources are then "outputs" for the function. This is the case of a material produced from an assembled or machined object;

- finally, some $structural\ elements$ may be used, they are "supports" for the function. For example, this is the case of a machine or an operator used to perform a function.

When the links are given at the systems level, they represent a broader point of view, because they do not detail the relationships within a system. Links between elements of the model may contain information, such as coefficients or properties.

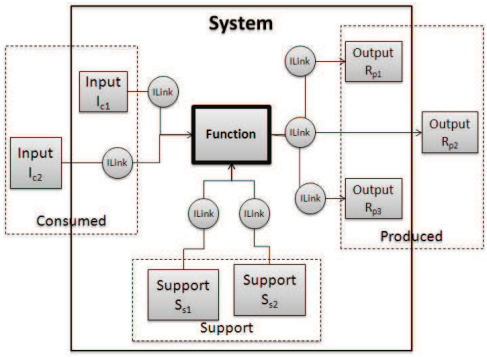

Figure 2: Relations

Remark. *Resources include both items that are processed, items products and components used for processing. The terminology used in the context of flow simulation, is to call entity, produced and consumed resources and resources, used ressources.*

2.3 *Details of model elements*

Before describing in detail the elements of the model, we may define:

- A $variable$, which corresponds to a magnitude that can be represented by an integer, a real, ...
- An $attribute$, that can describe any property given by: $a =< name, value >$, where value is any value representable by a structured string character following the ECMA-404 JSON Data Interchange Standard syntax.

A $variable$ can be used to evaluate system behavior, values are the possible values of a state variable of a hybrid dynamical system. An $attribute$ is of a different nature. Its aim is

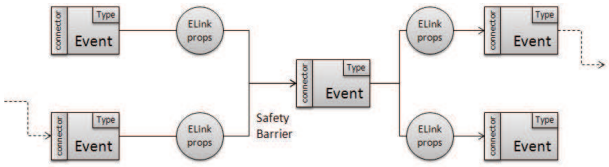

Figure 3: Events Graph

to represent one of the properties of a meta element. Its values can be generally represented by an object, the chosen format is JSON.

Formally, a structural view of a model is defined by $M =< S, L >$ where :

- S is a set of systems, $S = \{s_i | 0 \leq i \leq n\}$ with $s =< F(s), R(s), Sub(s), V(s), A(s) >$ is a system defined by a set of functions F, a set of resources R, a set of subsystems Sub, a set of variables $V(s)$ and a set of attributes $A(s)$.
- L is a set of links defined as follows $L =< me_s, me_t, nature, A(l), nature, direction, M_s \times M_t >$

A model element, me may be a system, a functional element or a structural element. The set of model elements connected to a model element is denoted by $N_s(me)$.

Remark. *The function $O(x)$ defines the owner(s) of x. This function is denied for variables $O(v)$, $attributesO(a)$, functions, structural element $O(r)$, ...*

3 DYSFIS VIEW

3.1 *Elements of the model*

The dysfunctional view (Figure 3) is used to describe the risk analysis or malfunction. This analysis consists in identifying, for each element of a system, states in which this element may cause a damage, or might be unable to answer correctly with the expected level of performance. The principle of this analysis with the view DysFis is as follows:

- each fact that may occur is represented by an event;
- the nature of the fact is described by the type of events: there are such events characterizing hazards, failure modes or deviations of variables;

- each event is associated with the element of the model view SysFIS to which is related. For example, a failure mode can be associated with a given resource;

- the causal links between events can describe the sequence of malfunctions. It is possible to associate properties to these links and barriers that affect the propagation.

The list of event types proposed by the model is the following: events representing the degraded dangerous phenomena (dp), events representing the failure modes (fm), events representing the deviations of variables ($vdev$), events representing degradation events (dam), intermediate events (gen), events characterizing the hazardous situations (hs), central unwanted events characterizing the loss of control (uce).

Each event is associated with a Boolean value. For a model element, the OK mode is defined as true if no event model dysfunction is true.

3.2 *Links between model elements*

Events are related to each other by links representing causal relationships: the causes of an event are connected to the input of the resulting event. Different types of connectors exist, such as AND and OR connectors. Links between events may occur with a certain probability, in particular an influence coefficient. Each link may relate to the input or the output of an event a barrier characterized by a reduction coefficient of the likelihood or severity.

The events are connected depending on the causal links. The model allows then to generate the fault tree relating to an event. Furthermore, the links between events can be weighted and it is possible to associate them with security gates.

3.3 *Details of model elements*

Figure 4 illustrates the relationship between the views SysFis and DysFis: events are associated with different elements. Links between the elements of SysFis model can guide the analysis of the propagation of dysfunctions for causal links between events.

Formally, the dysfunctional view is defined by a set of events $E = \{e_i\}$, and a graph G. The events are defined as $e =< N, P(e), S(e), O(e), g, \mu, \nu, A(e), V(e) >$ where

- N is the set of the nature of events. Most often, $N \subset \{dp, fm, vdev, hs, uce, dam, gen\}$;

- $P(e)$ and $S(e)$ are sets of predecessors and successors of the event;

- $O(e)$ is the owner of event;

- $g_i(e)$ is the input gate;

- μ is a function that defines the likelihood of the event, and v is the severity of the event.

The event graph G is defined with the sets $P(e)$ and $S(e)$ for each event; $\rho(e_i, e_j)$ is a partially defined function which describes a weight related to the edge between two events; $M(e_i, e_j)$ a partially defined function which associates modifiers to the relation between e_i and e_j. An example of modifier is a safety barrier. The failure mode of a model element is denoted by $fmode_i$ (failuremode). The normal of a model element is defined as :

$$ok = \bigwedge_i \neg dfmode_i$$

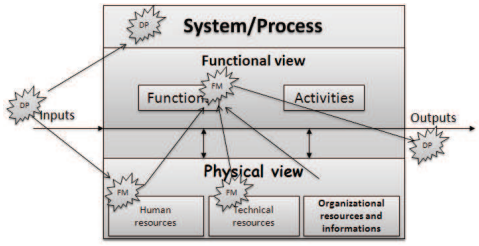

Figure 4: Links between system element , function, resources and events

4 SIMFIS VIEW

The SimFis view describes the dynamic behavior of the system. It is not necessary to construct this view to perform a simple risk analysis or even to build a fault tree or node bow tie diagram. However, when we have this view, it is possible to simulate the operation

of the system, including degraded mode. In addition, some elements of this view can be exploited for diagnostic or prognostic (Flaus, 2013b, Giap et al., 2009).

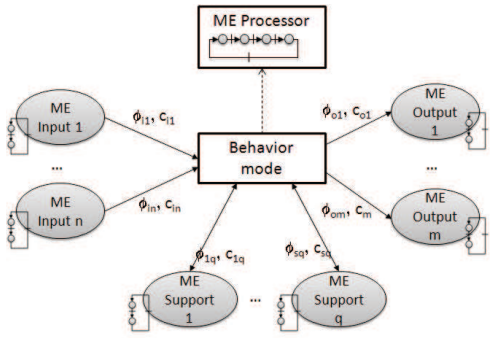

Figure 5: Process

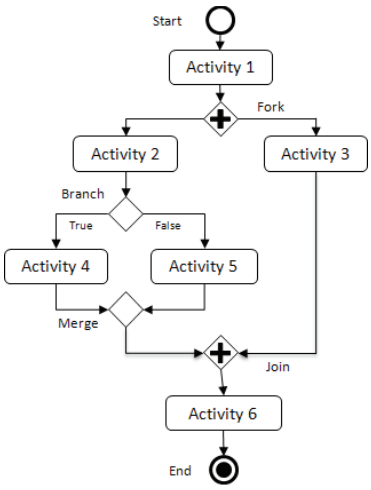

Figure 6: Activity diagram

The behavior is described by several complementary aspects. Each model element ($System$, $Functional\ element$ or $Structural\ element$), which is desired to describe the evolution, has one or more behavior modes. Usually, at least one mode of behavior is defined for the *OK* mode of , and a mode of behavior is associated with each failure mode that could be interesting to simulate. A model element may be active or inactive, which means that it is not used in a given configuration.

At each mode of behavior is associated with one or more activities, which can be of the following types:

- a simple modification activity of the informational state, described by a mathematical relationship and an execution duration (may be null);
- an activity of transformation element, which can be seen as an entity processor (Figure 5) and used to represent the flow diagrams of processing: a $System$, a $Functional\ element$ or a $Structural\ element$ can be seen as a processor which transforms into output, member elements, or that performs actions on elements. A processor can be active or not;
- a macro-type activity described by a diagram of subset of BPMN Type (Figure 6).

When an element becomes active for a given mode, the corresponding activities to this mode become active and can describe the behavior of this element. When it changes its operation mode, i.e from a normal mode OK to a dysfunctional mode DM1, the current activity is interrupted and the dynamic behavior changes. More precisely, a simple activity is defined by $a =< name, x \leftarrow f_a(x), \delta >$ where x is a vector of variables defined in the model element or the set of model elements via a structural link $N_s(me)$, and δ is a positive integer representing the time $t = \delta.T_s$.

A transformation activity is defined by:

- a transformation relation defined as follow:

$$\sum n_i me_i|\phi_i .. \rightarrow \overset{n_s me_s|\phi_s}{\longrightarrow} \sum n_o me_o|\phi_o\{m_i\}$$

  where me_i is an input model element, required in number n_i and which must satisfy the condition ϕ, which a logical relation expressed with respect to the variables, the attributes and the events available in the scope. me_o is an output and me_s is a model element representing a support;
- a positive integer duration δ representing the time $t = \delta.T_s$, and/or a set of final conditions;
- a priority p;
- a set of input actions defined as mathematical relation on variables in the scope $\{me\} \cup N_s(me)$.

$$x_c(k) \leftarrow f_{input}(x_c(k)) \cup \{m_i\};$$

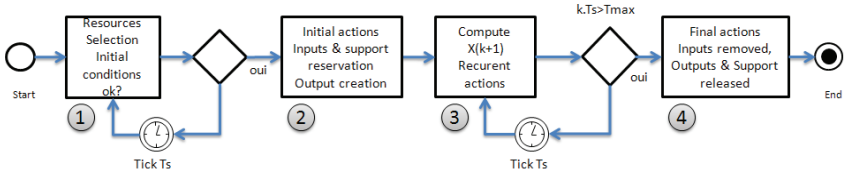

Figure 7: Activity diagram

- a set of output actions defined in a similar way

$$x_c(k) \leftarrow f_{ourtput}(x_c(k)) \cup \{m_i\};$$

- a set of evolution equations, computed at each sampling time

$$x_c(k+1) = f(x_c(k)) \cup \{m_i\}.$$

This set of elements allows to model the system behavior as follows:

1. A model element, when it is active, evolves according to the diagram in Figure 7:
   (a) block 1 is activated : this step consists of searching input elements satisfying the conditions in adequate numbers. If all items are not available, the block 1 is still active;
   (b) else, block 2 becomes active. The input actions are performed;
   (c) block 3 becomes active and evolution calculation is performed, if the equations are defined;
   (d) while the execution time mode is less then max time and the final condition is false, the block will be executed;
   (e) the final actions are executed, the inputs are destroyed and the support and outputs are released.

Remark.
- *An operating mode can be defined for each phase of life in OK mode, phases of life taking values in the set* $OM : NormalOperatingMode, DW : Shutdown, MA : Maintenance, UP : Startup, DW : Shutdown;$
- *model elements have a variable defining the number of modes of behavior that use and an attribute defining the max number (generally 1);*
- *the dynamic model is only valid for a given mode. In this mode, the connection variables are carried out during the activation step, and they are disconnected during the desactivation phase.*

Remark. *Changing the functional mode for an transforming activity type. When a change mode occurs, if the transformation relationship is not valid for this mode, this one is interrupted and the elements being processed (inputs and outputs) are destroyed. if we desire specifying a simple abnormal transformation of inputs, it is sufficient to define the activity as being valid for this mode, and to specify in the dysfunctional model, that the defects of the support element or the defects associated with the function behavior pattern, lead to a output default. For example, a default in a machine may product a defective part, while maintaining the same behavior in terms of machining.*

4.1 *Use for the simulation and diagnosis*

The proposed meta model may be used to structure the risk analysis, and to allow the exploitation of the obtained information for system simulation and diagnosis(Chittaro and Ranon, 2004). For space reasons, we can not give details here. A simulation approach which uses the transformation of the FIS meta model into High level Petri net may be found in (Negrichi et al., 2012).

5 EXAMPLE OF APPLICATION

In this section, we will illustrate the behavior of the system for transporting hazardous materials by road. This system consists of five functions: $Loading$ of hazardous materials in a truck; $Moving$ of the truck along a given route; $Waiting$ for the truck at various points: parking, waiting for unloading at customer or waiting for loading at supplier; truck

$Unloading$ at customer; $Storage$ at customer or supplier. We will detail the *Loading* function. We will construct the structural, the dysfunctional and the evolution views. This function presents the $Loading$ of hazardous materials (which is simulated in the form of blocks) in a truck. To achieve such a load, many entry attributes are required such as a deposit, a machine, a worker and a truck, and it needs as attributes outputs: a deposit, truck and materials. The deposit and materials are seen as modified resources. $Loading$ will decrease the amount of materials contained in the deposit and will change the positions of contents. Deposit, truck, workman are seen as supports for the *Loading* function, they are reserved prior to loading and released at the end. Figure 8 shows relations of $Loading$ describing before.

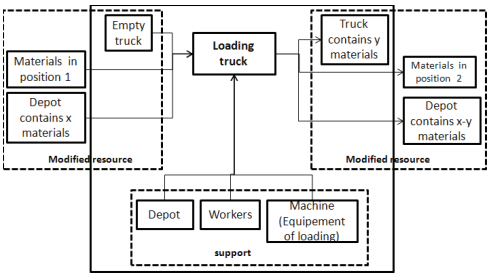

Figure 8: Relations for Loading

To have a good load, we should take note about time loading and the quality of loaded products, and eliminate any incompatibilities of products in the same expedition. A *Load* failure may come from four cases (Flaus and Granddamas, 2002)(Wirth et al., 1996) :

- delay of loading (unavailability of a deposit, truck, worker or machine);
- delay during loading (in case of unavailability of the machine, materials can be loaded manually but it may take much time);
- a collision during loading which can affect the quality of contents;
- and finally a bad loading represented by an expedition of incompatible two products in the same truck.

Figure 9 shows the various failure modes of loading describing a Fault tree (Karagiannis et al., 2010) .

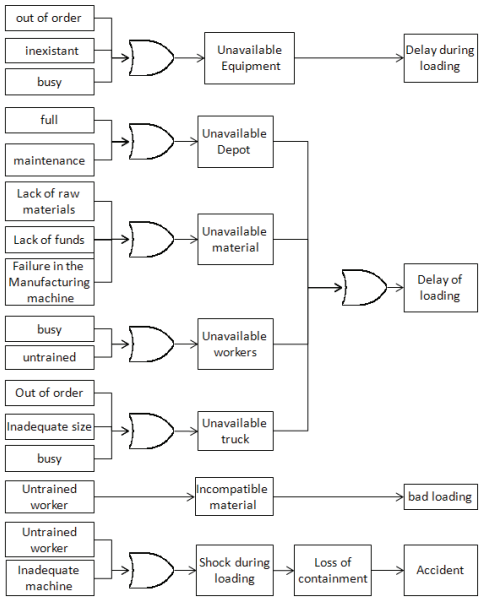

Figure 9: Fault tree for loading

Table 1 illustrates the evolution mode of each situations. Our simulation allows the system to evolve the basic events (basic events Fault tree), and it describes the failure mode of the function. This failure mode helps to obtain the behavior mode related to each failure (Table 1), where each Fault tree (Delay during loading, delay of loading, bad loading and Accident) is carried by a behavior mode evaluating the level of risk related to each situation.

6 CONCLUSION

In this paper, we have presented a method for risk analysis including a specification of the general process and her functions. For each function, we have precised the inputs, the outputs, the required resources, a dysfunctional model, and a model of evolution. The main interest of this meta model is that it allows the representation of risk analysis and dynamical behavior in a coherent manner, which can be used to perform various related tasks: risk evaluation, diagnosis, simulation under degraded conditions, prognostics ...This was illustrated through an example of loading hazardous materials in a truck. One of our future goals is to to simulate several times a complex phenomenon of transportation of dangerous goods, by using multi-agent based simulation and to generate randomly risks via the Monte Carlo simulation.

Table 1: Evolution mode of Load function

Model element	Behavior mode	Related Fault tree event	Equations
Loading	Normal		$T = f(q,d) = \frac{q}{d}$ where T is the loading time, q is the quantity to be loaded, and d is the loading flow;
Loading	Abnormal1	Delay of loading	$T = f(q,d) = \frac{q}{d} + T_1$ where $T1$ time of unavailability of machine, workers, depot, material or truck;
Loading	Abnormal2	Delay during loading	$T = f(q_1,d_1) = \frac{q_1}{d_1 \times n}$ where q_1 is the quantity to be loaded, d_1 is the loading flow for one workers, and n is the number of workers;
Loading	Abnormal3	Bad loading	$\frac{\Delta T}{\Delta t} = F(T, c_a, c_b)$ where c_a is the concentration of product A, c_b is the concentration of product B, and T is the environmental temperature;
Loading	Abnormal4	Accident	$D = f(M,t)$ where M is the material to be loaded, and t is the temperature.

REFERENCES

Chittaro, L. and Ranon, R. (2004). Hierarchical model-based diagnosis based on structural abstraction. *Artificial Intelligence*, 1-2:147–182.

Flaus, J. and Granddamas, O. (2002). Towards a formalisation of mads, system failure analysis model, in lambda-mu 13. ESREL.

Flaus, J. M. (2008). A model-based approach for systematic risk analysis. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 222(1):79–83.

Flaus, J.-M. (2011). A modelling framework for model based risk analysis. *Safety and Reliability for Managing Risk ESREL'11*.

Flaus, J.-M. (2013a). *Risk Analysis: Socio-technical and Industrial Systems*. John Wiley & Sons.

Flaus, J.-M. (2013b). *Risk Analysis: Socio-technical and Industrial Systems*.

Flaus, J.-M., Adrot, O., Ngo, Q. D., et al. (2011). A first step toward a model driven diagnosis algorithm design methodology. *Safety and Reliability for Managing Risk ESREL'11*.

Giap, Q. H., Ploix, S., and Flaus, J.-M. (2009). Managing diagnosis processes with interative decompositions. 296:407–415.

Karagiannis, G., Piatyszek, E., and Flaus, J. (2010). Industrial emergency planning modeling: A first step towards a robustness analysis. *Journal of Hazardous Materials*, 181:324–334.

Negrichi, K., Di Mascolo, M., Flaus, J.-M., et al. (2012). Risk analysis in sterilization services: A first step towards a generic model of risk. *Proceedings GISEH'2012*.

Papadopoulos, Y., Parker, D., and Grante, C. (2004). A method and tool support for model-based semi-automated failure modes and effects analysis (fmea) of engineering designs. *Research and Practice in Information Technology, ACM, ISSN 1445-1336*, 47:89–95.

Tjoa, S., Jakoubi, S., Goluch, G., Kitzler, G., Goluch, S., and Quirchmayr, G. (2011). A formal approach enabling risk-aware business process modeling and simulation. *Services Computing, IEEE Transactions on*, 4(2):153–166.

Wirth, R., Berthold, B., Krämer, A., and Peter, G. (1996). Knowledge-based support of system analysis for the analysis of failure modes and effects. *Engineering Applications of Artificial Intelligence*, 9(3):219–229.