DE GRUYTER OPEN

DOI: 10.1515/aucts-2015-0020

ACTA UNIVERSITATIS CIBINIENSIS – TECHNICAL SERIES
Vol. LXVI 2015

INTEGRATING RISK ANALYSIS WITH SAFETY DYAGNOSTIC IN COMPLEX INDUSTRIAL SYSTEMS: MODELING HAZARD

CIOCA Lucian Ionel
Faculty of Engineering/Department of Industrial Engineering and Management, "Lucian Blaga" University of Sibiu, Sibiu, Romania, lucian.cioca@ulbsibiu.ro

MORARU Roland Iosif
Faculty of Mines/Department of Mining, Surveying and Civil Engineering, University of Petroşani, Petroşani, Romania, roland_moraru@yahoo.com

BĂBUŢ Gabriel Bujor
Faculty of Mines/Department of Mining, Surveying and Civil Engineering, University of Petroşani, Petroşani, Romania, gabriel_babut@yahoo.com

UNGUREANU Nicolae Stelian
Faculty of Engineering - North University Centre of Baia Mare/Department of Engineering and Technology Management, Technical University of Cluj-Napoca, Baia Mare, Romania, Nicolae.Ungureanu@ubm.ro

Abstract: *Admitting as known the instruments that lends itself to highlighting the causes - consequences relationships in an industrial plant, the purpose of this research is, on the one hand, to integrate these relationships in the safety diagnostic procedures and, on the other hand, to use these "consequences" to forecast future failures likely to occur within the technical system. In this context, the paper aims to study systemic hazard models to develop structural, functional and behavioural models, describing a complex industrial system*

Key words: risk analysis, safety diagnosis, industrial system, integration

1. Systemic modelling of hazards

We can define a system as a determined set of discrete elements (or components) *interconnected* or *interacting* [7]. Structural modelling of a system is the simplest and most natural modelling there can exist: it comes to "cut - off" the envisaged system in different entities, trying to follow a certain *"granulometry"*, even if there are introduced some intermediate clippings, in the form of subsystems.

The complexity characterize an organized, orderly system, generating "unknown", system which is able to innovate in order to adapt him to his own development and its environment change. The complexity of a system will allow him to adjust with any situations of confusion (or dysfunction) and even to generate order starting from disorder. This is another premise derived from the systems' theory that underlies the process of risk analysis [5].

Industrial systems are basically, from this point of view, interferences between *complicated* systems and *complex* systems. Controlling and - even - dominating their associated risks requires entering in the field of complexity. Systemic analysis suggests that:

- modelling through systems allows to simplify the complex, allowing better understanding and domination, being aware that *"simple"* is an arbitrary time out of complexity;
- the principle of complexity has two characteristics: *entirety* (the object should be regarded as an active and permeated part in its environment) and *accuracy* (an object is defined in terms of explicit and implicit intentions of that who models it).

A complex system can not be analyzed principally only by splitting it into parts. The working system is composed of elements that have meaning only in the privacy of the system; his evolution is not predictable more than for a period of time called *time horizon*; the system can undergo rapid change, however important, without apparent external cause and show different aspects depending on the scale of analysis [6].

Complex systems differ fundamentally of complicated systems by the fact that the prediction difficulty lies not only in failure of the observer to take into account all the variables that could influence its dynamics, but also in the system's sensitivity to initial conditions (slightly different initial conditions lead to very different developments), plus the effect of a process of self-organization, process driven itself by the interactions between subsystems and components which results in spontaneous occurrences - fundamentally unpredictable - of the order relations. A complex system has which not necessarily results from an evolution of analysis of his response to a given stimulus (dynamic analysis); i.e., dynamics and evolution of a complex system are two different issues that require specific approaches.

Moving forward, modelisation of a system may underlie on the systemic approach, which is a "methodology of representation, of modelling active finite objects (in turn defined as combinations of active entities interacting dynamically), physical or immaterial, found themselves in interaction with the surrounding environment through energy, information or materials flows, on which the system exerts an action: flows that the system changes and processes" [4].

Structural modelling

From the structural point of view, any system comprises four components:

- ***Entities,*** that are constituent parts, whose number and nature can be evaluated, even if sometimes only approximately; these components are the most homogeneous ones.
- ***Boundaries*** (or limits), which separates all entities in relation to the system environment; these limits are always more or less porous and represents an interface with the external environment.
- ***Links*** (relations) ***network***: entities are physically interconnected. The main types of relationships are transport and communications; basically these two can be reduced to one, since communicating means to information transport, and transportation serves to communicate (to circulate) materials, energy or information.
- ***Stocks*** (or inventories, reservoirs, tanks), where materials, energy or information are stored to be transmitted or received.

Functional/behavioural modelling

From a functional perspective, a system can be decomposed as:

- ***Material, energy or information flows***, undergoing transit network of relationships and stocks. Flows are working through input/output to/from the environment.
- ***Decision - making centres***, who organize the network of relations, through coordination and management of inventory/stock flows.
- ***Feed-back loops,*** which serve to inform the input stream about the situation at the output, so as to allow the centre of the decision to know as soon as the general state of the system.

Next, we summarize three models representing the concepts of hazard and hazard scenario:

- MADS Model of Systems Dysfunction Analysis;
- MoDyF Model of Formal Dysfunctions;
- Scenarisk Model, based on prior MoDyF model.

2. MADS Model of Systems Dysfunction Analysis

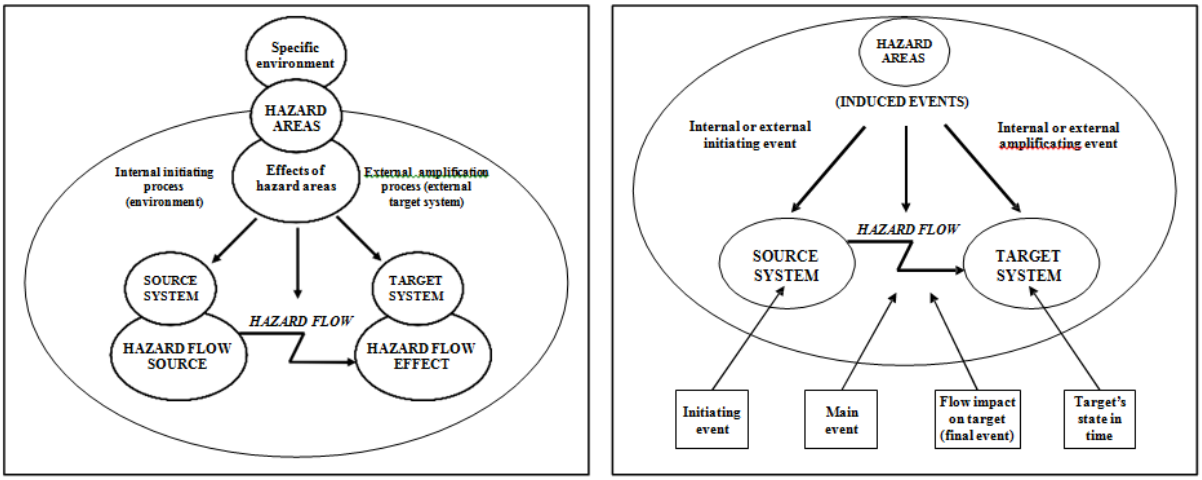
Figure 1 illustrates the hazard model as a set of processes for the purposes of systems theory [4]. Undesirable event occurs at an encounter between the main process and the target system. ***The hazard*** is all the processes that lead to the main process that can be generated from a hazard source system. ***Hazard flow*** is produced by a source which starts from a hazard source system consisting of matter, energy, information. If this flow can reach ***a target*** system (human, environmental, property on which the effects are occurring, then one can speak of risk. The assembly of process is set in a specific environment (the environment in which it relates) that generates zones exerting effects on the process. ***The source*** of hazard flow is given by an initiating process of internal or external origin. On the opposite side, there may be a process to increase the flow on the target, a process that may be of internal or external origin (which comes also from the specific environment).

This model of hazard and risk is a general model that allows organizing knowledge and general methodology modelling for risk analysis. If the processes are defined as events, the model may be represented in the diagram of Figure 1 (right side), wherein:

- the initial event is the source of hazard flow;

- the flow is the main event;
- the final event is the flow impact on the target;
- the target states are the states that the target system will take during time;
- the induced events (or consequences generated) are the effects of the hazard zone together with initiating event induced by the initiator process, and the amplifier (enhancer event).

Figure 1: MADS modelling of hazard: events modelling Source: (Le Moigne, J-L., 1991)



The hazard being modelled as a process, the flow will be composed of matter, energy and information. Characterization of information depends on receptors. Flows are located in specific areas some of which being hazard zones. The environment contains a variety of different natures processes, generating hazard zones while there are subordinated to them (to these processes). The interaction of these processes is the source of events involved in the occurrence of an undesirable event.

Exempligratia: A pressurized gas leakage is composed of matter and energy (pressure wave) which is distributed in space. Leakage will be limited in time. In the context of this leakage, wind speed will be an effect of the danger zone that will interfere with the dispersion (and will determine it) and hence on its effects on targets. A radiation consists of energy (wave) and matter (particles associated) which will be scattered into space. They are limited in time, because if one neutralizes the emission source the emission source will disappear. Reflection, refraction or absorption of these radiations in the context of emission, are the elements of the hazard zone that will interfere with the characteristics and their effects on targets. A chemical or radioactive contamination consists of radioactive material associated with energy (radiation). It will be chronic because it is impossible to completely decontaminate a polluted area.

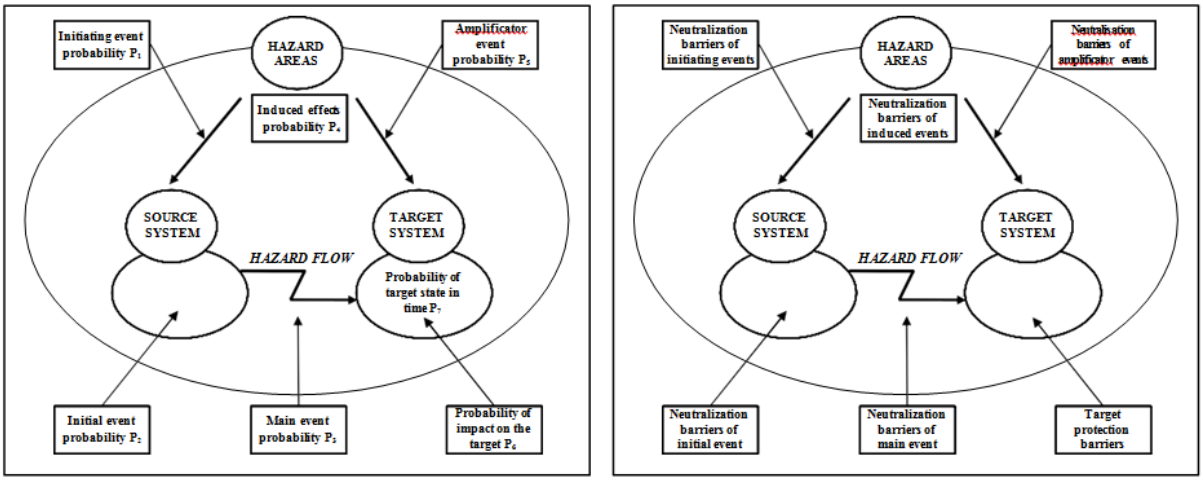
The MADS model summarizes the chain of events which, starting from the initial event, is leading to different states of the target. The probability of chaining of the events (scenario development), which is a composite probability, is shown in Figure 2 (left). This model shows the difficulty in assessing the probability of an undesirable event that requires knowledge of the probability of each event. Representation and probabilistic assessment tools are of dysfunction flowchart schemes based on the use of Boolean algebra, of network type (Petri nets) or Markov series that appeal to matrix calculus.

The effects of undesired events on targets are materialized through an immediate impact or sometimes by a delayed impact. The different types of impact and consequences are determining the different states of the target. Determination of risk acceptability is negotiated with all participants in the events. In some cases, the acceptability level may be imposed by legislation or specific rules.

Establishing means of neutralization of causal chaining leading to unwanted events (undesirable event scenarios occurrence), represents the very essence of risk prevention and basically consist in identifying preventative barriers at the source system level, at the main event and induced effects level and in finding protective barriers at target system's level (Figure 2, right). The model is operational and enables the identification of the events which, starting from the initiating some cases lead to undesired events. The principle of this methodology can be illustrated by taking as an example a liquid propane storage facility. The storage container generates hazards (hazard

source) that are related to pressure. There may be a crack in its wall, due to internal initiating event (e.g. corrosion) or external (lightning from a storm). The main event for liquefied propane tank is a matter emission (leakage). To determine which will be achieved should be evaluated Main Event features and known distance between source and target.
To determine which targets will be achieved should be *evaluated* the main event features and should be *known* the distance between source and target.

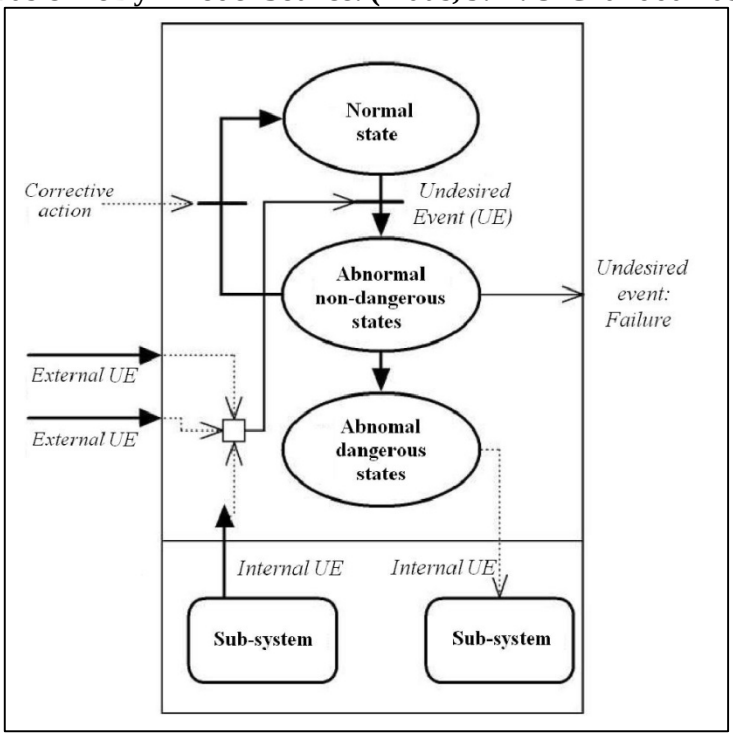
Figure 2: MADS methodology: Probability of events enchainment and barrier location Source: (Moraru, R.I. & Băbuţ, G.B., 2010)



3. MoDyF model

A more recent model [2] is MoDyF, model (Formal Model of Dysfunction) which is in fact a complement of MADS model, being dedicated to the description of a network of entities under possible dysfunction (Figure 3).

Figure 3: Basic MoDyF model Source: (Flaus, J.M. & Granddamas, O., 2002)



Under this model:

- the states of each entity are described by a set of variables which characterize the situation in which entity finds itself. Each set of values corresponding to physical condition is associated with an operating state that can have the following values (normal state, abnormal but not dangerous state, dangerous abnormal state);
- dysfunctions propagates through cause - effect relationships between entities.

This model is based on a discrete representation, the dysfunction relations being of event occurrence type. The system described is placed in an environment with which it interacts. Effects of dysfunction can occur both internally or externally. Similarly, conditions that can cause a dysfunction may be related to internal events or interactions with the external environment.
In developing the model of dysfunctions in a systematic manner, Flaus propose a structural and functional model version, resumed and completed later on called FISE [1], entailing four descriptive aspects, namely:

- ***Functions:*** relating to the functions required to describe the list of functions that can be provided be the entity;
- ***Interactions:*** interactions which, as in the MADS model, are describing as flows of matter, energy and information, the relations between entities and environment;
- ***Structure:*** information on the structure is defining the physical structure of the entity and is specifying the physical boundary delimiting the system under consideration. They also allow specifying whether the entity is a *contained* object or a c*ontaining* one;
- ***Internal state:*** which is a set of quantities aimed to characterize the situation of the entity.

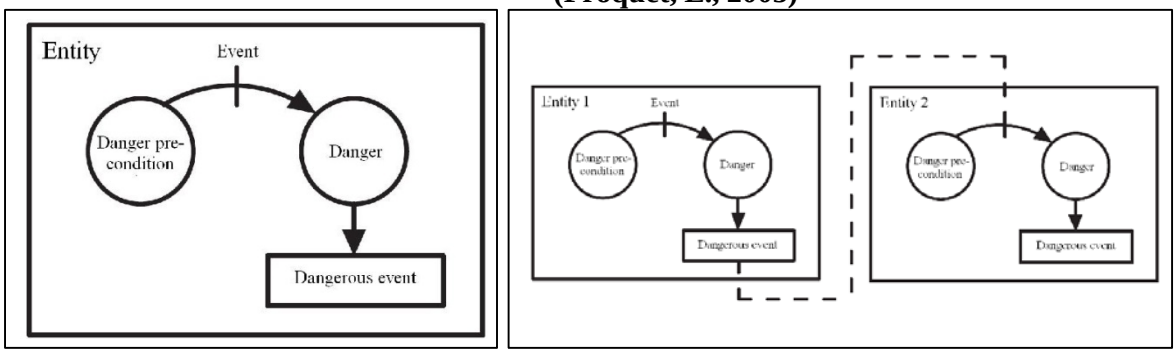
All these issues are both described in a correct functioning or malfunctioning state. Then, under certain assumptions, causal dysfunctions chart is built on the physical model of the system, considering that any failure propagates through the intermediate of an abnormal physical interaction. This modelling is extended to each entity within the system.

4. Scenario - based modelling: ScenaRisk method

ScenaRisk method [3] is designed to generate scenarios from a library of elements of existing scenarios and using a representation of the system specifications. The hazard model on which it is based is represented as an automated block of states and is grounded on the MoDyF model described above.
The principle, as for any type of hazard, is to represent the mode of occurrence and evolution of the system that could lead to an undesirable event. The resulting hazard model is based on two principles (Figure 4):

- the first principle resulting from relating the concepts of *ante-threatening* condition and *hazard state* of an entity; hazard state is materialized as a consequence of a ante - threatening state on the condition of achieving an event;
- the second principle stems from admitting the assumption that each entity which is in a state of hazard is likely to generate a hazardous event.

Figure 4: Schematic layout of ScenaRisk model, with/without enchainment Source: (Froquet, L., 2005)



Thus, it is possible to clearly highlight the possible causal connections, and therefore the generation mode of scenarios, because each state of hazard that generates a hazardous event may be at the origin of one or more transitions from a state of ante - threatening of the entity to a state of hazard.

5. Conclusions

Through the intermediate of various modelling tools described in this paper, a certain amount of information and their specific concepts will be integrated into models for risk analysis and safety diagnosis of industrial systems. Some of these concepts and principles are derived from systemic analysis, and another part is extracted from MADS, MoDyF and Scenarisk hazard models.
Concepts resulting from the models presented and which are relevant in terms of integration into a unified methodology for risk analysis and safety are the diagnosis following:

- the systemic approach, together with FISE modelling may be useful as a basis for structural and functional modelling formalization that we want to develop;
- the concept of flow, which will allow the consideration of the cause - effect relationships between components and their integration of these relations into the safety diagnostic analysis.

Here we have the foundation required to formalize a structural and functional model of a risk analysis that integrates appearance of the cause-effect relationship between system components (aspect not considered in traditional methods derived from reliability theory, where the causes are sought only modes failure and no failures itself).

Behavioural patterns associated to the assumptions regarding the operation of systems' components are the strong link that will allow to relate the results of risk analysis with the methods of diagnosis: on the one hand the state assumptions (correct or incorrect) for diagnosis, and on the other hand risk analysis that put in causes - consequences relationships, expressed in terms of faults and dysfunctions.

Given that the usual methods of risk analysis do not allow simple integration of them with diagnostic analysis, it is necessary to develop a formalism and content adapted to allow integration, based on a structural, functional and behavioural common formalism of the risk analysis and safety diagnosis of industrial systems.

References

- Flaus, J.M., Adrot, O. & Désinde, M., A mixed structural/functional graph based model for fault diagnosis and systemic risk analysis, In: *Safety and Reliability for Managing Risk* - C. Guedes Soares & E. Zio (eds), Vol. 1, pp. 221-229, Taylor & Francis Group, London, UK, (2006).
- Flaus, J.M., Granddamas, O., Towards a formalisation of MADS, system failure analysis model, *ESREL' 2002*, Lyon, France, (2002).
- Froquet, L., *Contribution à l'analyse des risques: Proposition d'une méthode par scénarios et capitalisation de connaissance*, PhD thesis, Institut National Polytechnique de Grenoble (INPG), Grenoble, France, (2005).
- Le Moigne, J-L., *La modélisation des systèmes complexes*, Éditions Dunod, Paris, France, (2002).
- Moraru, R.I, Băbuţ, G.B., *Participatory risk assessment and management: a practical guide* (in Romanian), Focus Publishing House, Petroşani, Romania, (2010).
- Moraru, R.I., Băbuţ, G.B., Cioca, L.I., Rationale and criteria development for risk assessment tool selection in work environments, *Environmental Engineering and Management Journal*, Vol. 13, No. 6, pp. 1371-1376, (2014).
- Vesely, W.E., Supplemental viewpoints on the use of importance measures in risk-informed regulatory applications, *Reliability Engineering & System Safety*, Vol. 60, No. 3, pp. 257-259, (1998).