PERSPECTIVES IN THE USE OF COLOURED PETRI NETS FOR RISK ANALYSIS AND ACCIDENT MODELLING

David Vernez[1*], Didier Buchs[2], Guillaume Pierrehumbert[1]

[1]*Institute of Occupational Health Sciences IST, rue du Bugnon 19, 1005 Lausanne, Switzerland*

[2]*Software Engineering Laboratory, Swiss Institute of Technology, Lausanne, Switzerland*

Numb. of pages : 31
Numb. of words : 6267

---

* Corresponding author. Tel. : ++41 21 314 74 21 ; fax: ++41 21 314 74 20 ; e-mail: David.Vernez@inst.hospvd.ch

Abstract

Current uses and application perspectives of Petri Nets (PNs) in the fields of risk analysis and accident modelling are discussed in this paper. Severe time and combinatory limitations are encountered when trying to model complex events sequences with classical methods. Due to their large calculation capabilities and the development of recent tools, the Petri Nets should be able to overcome these limitations: (1) Previous applications of PNs in the field of safety are reviewed and briefly discussed. Using a direct system description or the results of a Preliminary Hazards Analysis (PHA), authors have used PNs tools in order to get a variety of results such as, accident's critical paths, safety or reliability data. (2) The tool's capabilities are also highlighted through a ″translation″ catalogue, in which common concepts in safety are expressed in the Petri nets formalism. Either qualitative aspects of accident mechanisms or quantitative data, such as time logic or reliability calculations, may be processed in a Petri net.

Despite these promising examples and properties, safety oriented applications in the field of safety are still scarce. The lack of comprehensive tools available and PN inherent complexity may explain this situation. We can hope that the increasing attractiveness of PNs may somehow overcome these difficulties. As a matter of fact, due to the tool continuous development (i.e. recent SRN or Object-Oriented nets development), PNs may play a significant role in risk analysis or accident modelling in the future.

Introduction

Accident models and analysis methods

Intuitively, accidents are perceived as due to a single cause or, at best, to a few determining factors. It is, for instance, quite common amongst both the public and authorities to consider being under the influence of alcohol while driving as a single cause of car accidents. The *domino theory*, formally introduced by Heinrich in 1928, is a typical example of accident models, which reflects this perception. In the domino model, the accident process is considered to be a linear sequence of events. Although of limited consistency with regards to the current safety science standards, such viewpoint is still very common, especially from people involved in the accident process.

More recently, the development of Quantitative Risk Analysis (QRA) methods has originated several other accident models. Thus, the *linear chain of events* has evolved to a *branched events chain* and finally to *a multilinear events* sequence. Beside the development of these events-based models, remarkable accident theories, such as the *catastrophe theory*, have also been proposed.

Despite the variety of the accident theories available at this time, models more complex than the *branched events chain* are seldom used in prospective accident analysis methods. The well-known *Fault-tree analysis (FTA)* or *Event-tree analysis (ETA)* methods, are associated to the *branched chain of events* model, while the *Hazard and Operability study (HAZOP)* method considers accident sequences even less complex. It must be stressed that, due to their elementary theoretical background, these methods encounter some limitations when used to handle complex systems.

Time modelling

The limited use of classical methods becomes evident while simulating dynamic processes with time constraints. The FTA process is, for instance, only able to cope with trivial time logic, as each event entering a logical gate (a causal event) must occur before the outgoing event (a consequence). Time logic, especially concerning events duration, is not fully taken into account into fault or event-trees. Consequently, systems with dynamic constraint, such as concurrency or parallelism, cannot be depicted accurately in such ‘branched chain’ structures.

It must be stressed that time representation is seldom a limiting factor in a retrospective *(a posteriori)* analysis, as the events have occurred in a 'known' order. Time may however become a problem in prospective (*a priori*) analysis, in which all of the relevant events sequences must be explored. Taking time logic into account may become very complex for processes involving 'independent' actors working concurrently. A transportation system is, for instance, a complex parallel system in which several actors (onboard or not) may act concurrently.

Let us consider the case of train fire inside a tunnel. In such a case, there is a serious risk of fumes intoxication for the passengers due to the tunnel confinement. For the same reason, each accident actor (fire, passengers, crew, rescuers,...) has only a few possible courses of action. Despite this and despite the remarkable constancy in the course of actions undertaken by each actor, the consequences of these fires differ significantly from one case to another. As a matter of fact, as shown by an examination of several cases, the accident outcome is strongly dependant of events order and events duration. The simulation of such accident process requires methods able to cope with complex time logic or, in other terms, methods based on ″timed″ accident theoretical models.

Multilinear accident processes

In the *multilinear events sequence (MES)* accident model, introduced by Hendrick and Benner (1986), the accident is depicted as a sequence of parallel events. The events of the accident process are positioned chronologically along ″lines″. Each line being assigned to an actor of the accident.

For a limited number of actors playing an active part in the accident process, the MES model is a powerful tool for accident investigation. The *Sequentially Timed Events Plotting (STEP)* method used for accident reconstruction in the field of transportation is a typical application of the MES model. Despite its successful uses in *a posteriori* investigations, it must be stressed that, the MES model is generally not applied in prospective analysis. As a matter of fact, complex models, such as the MES model or, on a smaller scope , such as the *branched chain of events* models cause combinatory problems. A prospective analysis based, for instance, on an FTA or STEP process may lead to an unmanageable number of possible accident paths. Limitations due to both combinatory and time logic management may somehow explain why events-based accident models have known little developments since Benner's work in 1975.

On the other hand, recently developed computer tools seem able to overcome the limitations previously encountered. Indeed, computer assisted ETA or FTA calculations, Markov chains, or Petri Nets (PNs) have increased dramatically time representation and combinatory capabilities. Surprisingly, the two latest tools are mainly used for quantification purposes rather than for their accident modelling capabilities.

A typical example of such application is the State Space Method (Brummer et al., 1994), in which Markov chains' properties are used to calculate the reliability, availability or maintainability of the system. Although of great interest for quantitative analysis, the State of Space Method (SSM) is not used as a ″prospective″ analysis. Indeed, as a description of the system states is required in order to process calculation, all possible situations should be known prior to the SSM analysis. Similar problems are also encountered in methods on PNs use for fault-tree modelling (Liu and Chiou., 1997).

It must also be pointed out that, neither Markov chains or Petri Nets methods does refer explicitly to known accident models theories.

Petri Nets

Defined by C.A. Petri in 1962, Petri nets are mathematical tools, which allow dynamic simulation of parallel and concurrent systems with time constraints. Designed originally for the computer-engineering field, Petri nets are now used for dynamic systems specification, description and verification in a wide range of applications. Dynamic systems modelling through Petri nets have encountered a large success and several new developments have been made since Dr. Petri's early work. Some of these developments, such as hierarchical nets, Stochastic Petri Nets (SPN), or Coloured Petri Nets (CPN), are of utmost interest for safety-related applications.

Formalism

Formally, a PN may be described by a set of places, a set of transitions, a valuation function and an initial marking. For analytical computations, Petri nets are defined by means of linear algebra where vectors represents markings and matrices flow relations (Vidal-Naquet and Choquet-Genet, 1992). For convenience, a PN is generally depicted in a graphical structure where a circle represents a place and a thin rectangle represents a transition. Arrows and tokens respectively illustrate valuation functions and marking (see Figure 1).

Figure 1. Functional and graphical description of PNs

Places could be seen as conditions and transitions as events. The marking describes the state of the net. A precondition (specific marking), is required in order to fire the transition. When the transition is fired, the net reaches a new state, i.e., a new marking.

Occurrence graph

An occurrence graph is a structure describing all distinct states (markings) reachable during the net evolution. Distinct markings are illustrated as nodes in the occurrence graph, while labelled arcs are representing transitions (events) that produce the state evolution. Final states of the evolution are called dead nodes. The size of the occurrence graph may be expressed using its number of nodes. These graphs can be finite or infinite and mathematical techniques have been developed to analyse them by means of analytical methods or optimised simulation techniques. Explicit construction of the occurrence graph lead to untracktable complexity problems, quite a lot of techniques have been studied to reduce this combinatorial explosion either by coding set of states or by combining similar behaviours. See Buchs and Buffo (1999) for a thorough survey of the Petri nets analysis techniques.

Extensions of the basic Petri net model

Although the original model of Petri is often sufficient to model real systems, it rapidly appears that various extensions were necessary to take into account the needs for modeling of the average systems. Extensions have been proposed in the direction of expressiveness of repeated similar situations, time information, probability and structuring. We will shortly describe in the following sections the main innovative extensions of Petri nets. Current research is devoted to improve structuring and dynamicity of the basic model and to enrich the set of existing analysis techniques.

Coloured Petri Nets

Contrary to classical Petri nets, tokens may be differentiated in Coloured Petri Nets (CPN). In coloured nets, complex properties may be attributed to the tokens (numeric values, string of characters, etc.) by colors. The flow relation is modified accordingly to take into account the transition firing modes i.e. the color that is used to fire a transition.

Timed Petri Nets

In timed Petri nets (TPNs), time logic is taken into account by the use of firing times or duration. While only a specific marking is required in a basic PN for a transition firing, time constraints are included in TPNs.

Stochastic Petri Nets

There are several possibilities to include delay timed firing conditions in the net. If the delay is a random distribution function, the resulting net class is called Stochastic Petri Net (SPN).

Generalized Stochastic Petri Nets

Generalized Stochastic Petri Nets (GSPN) are like SPN but include also immediate transitions. Once enabled, the immediate transitions are fired in zero time. They are very useful for modelling an activity with negligible delay compared with other exponential transitions.

Stochastic Reward Nets

In order to describe the system dependability, GSPN were extended with new features to create Stochastic Reward Nets (SRN). These nets include enabling functions, timed transition priorities, variable cardinality arcs, halting condition, and reward rates.

Modular or Object-Oriented Nets

The intensive use of Petri nets in large projects naturally leads researchers to propose new concepts to manage the complexity of the Petri nets that are used in these systems. Moreover, openness and dynamic creation/destruction of entities are characteristics of the modern software systems. Hierarchical nets are the first attempt to introduce structure in nets. Unfortunately, dynamic evolutions are not very well supported in these approaches. With the rapid emergence of Object-Orientation (that quite naturally take these aspects into account), various approaches have been proposed to give an object-oriented structuring to Petri nets. See (Guelfi et al., 1997) for a comparative study of the Object-Oriented approach and (Buffo and Buchs, 1997) for a description of the most common approaches in this field. More recently, components have been introduced in these Object Oriented models (Buchs and Guelfi, 2000; Biberstein et al., 2001) that enable us to enrich Petri nets with consideration about the architecture of the system i.e. the way components are organized and how they communicate.

Use of Petri nets in safety

Petri nets, as tools for discrete events simulation, are of utmost interest in safety. Dynamic changes in the Petri nets are induced by transition firing during simulation. Firing of one or several transitions changes the net marking or, in other terms, induces a discrete change of state. Thus, dynamic properties of Petri nets such as parallel firing, successive firing, or firing of concurrent transitions may be used to simulate complex events sequences.

These last years, several authors have investigated the use of Petri Nets for safety-related applications. A brief review of some of these applications is presented in Table 1.

Table 1. Use of PNs tools in the field of safety

Towards Petri nets modelling

Current uses and application perspectives of Petri Nets PNs in the fields of risk analysis and accident modelling are discussed in this paper. As other authors have already studied extensively PNs' calculations perspectives (see Table 1), this work has been focused on qualitative rather than quantitative modelling.

The properties of PNs for modelling functions or elements commonly used in the field of risk analysis have been investigated. A translation ″catalogue″ between the Petri nets formalism and the safety science is proposed. A special emphasis is given on linking the CPNs tool with known concepts and accidents theoretical models.

Petri nets formalism vs. Safety

Petri nets have been known since the early sixties, but they are still used at a limited extent in the field of safety. Due to their hermetic formalism and the lack of ″comprehensive″ tools available, PNs are often considered by the *safety science community* as made for and used exclusively by computer scientists. The idea of describing discrete events

through places and transitions is quite easy to grasp. Still, it doesn't help to understand how to apply it in the field of safety.

In order to give some insight of the PNs potential for safety-oriented applications, the problem can be considered from the safety science viewpoint. Despite ″bending″ existing PNs structures for safety purposes, let's consider first concepts and functions commonly used in risk analysis or accident modelling.

As shown in Table 2, a translation into the PN formalism exists for a number of these functions. It must be emphasised that, due to the versatile nature of PNs tools, other translations than those presented in Table 2 may exist.

Table 2. ″Translations″ of safety concepts into PN structures

Discussion

Using PNs in safety related applications

Although far from exhaustive, the translation catalogue presented in Table 2 highlights the tremendous possibilities of PNs. First, as PNs' tools are generic, a large number of concepts and functions may be modelled through their formalism. Indeed, many concepts currently used in risk analysis methods based on event-sequences accident theories may be implemented in PNs structures. Secondly, PNs do suffer fewer limitations regarding combinatory management and function/concepts combination than classical methods. Given the appropriate PN tool, it is therefore possible to expand significantly the boundaries of a risk analysis.

It is for instance possible, using a timed CPN, to model altogether time constraint, parallelism and cause to consequences relationships (including divergent consequences). While unmanageable with many classical tools, such combination of functions may be simulated in a PN structure containing up to several hundred thousand states (the number of occurrence graph nodes). Considering the element being modelled, four possible uses of PNs in the field of safety may be distinguished:

Objects and modes modelling

Petri nets have been designed in order to model the behaviour of dynamic systems. Thus the most straightforward way to use them is to model a physical system such as manufacturing processes (Rudas and Horvath, 1997; Wang and Wu, 1998). As all the reachable states of the net are explored during the simulation process, system instabilities and blocking situations are revealed. To produce safety or reliability information about the system being modelled is a general propriety of PNs . When a physical or logical system is modelled without emphasis on safety, this property comes as a spin off of the simulation process. Numerous examples of applications without special emphasis on safety are reported in literature and have therefore not been presented in Table 1.

Despite the PNs intrinsic properties regarding safety, safety-oriented uses are still scarce. Amongst other causes, the computer tools' development required may explain the lack of applications reported in this field. Indeed, both net structure and simulation analysis tools must be specifically designed or adapted to get safety and reliability data.

Still, a safety-oriented use of PN is of utmost interest. It allows inductive processing while taking account of complex cause to consequence relationships between events. Compared to classical method, such PN analysis may be assimilated to an expanded FMEA or HAZOP procedure in which parallelism and concurrency are taken into account. While in classical methods, consequences of a single deviation are propagated through the system, all the objects' functioning modes in PNs are considered simultaneously.

Accident modelling

From a functional viewpoint, a desired event cannot be distinguished from an undesired one, except that their probabilities of occurrence may differ considerably. Thus, rather than modelling a physical or functional system, it is possible to model the accident events' sequence itself in order to get safety data.

In such accident modelling, possible combinations of events are explored in a systematic way. By analogy with known methods, it may be compared to build a prospective STEP analysis. Combining Benner's multilinear sequence model with cause to consequences branching (OR causal gates or divergent consequences branching) may produce elaborated accident scenarios. Although of utmost interest, this method does suffer limitations in its applications. As a matter of facts, all the significant events of the accident process must be known in order to build the PN structure, which may require previous accident analysis or risk analysis processes.

State of space modelling

In the state of space method, stochastic nets are used in order to get quantitative data about the system reliability, availability and maintainability. The dynamic modelling capability of SPN does indeed allow calculations of complex systems.

It must be stressed, however, that the state space method is a calculation process rather than a risk analysis. As a matter of fact, all the significant states of the system must be known prior to modelling. Thus, the state of space method may be applied to well-known systems or to quantify the results of a previous risk analysis.

Fault and event-tree modelling

Several authors (Liu and Chiou, 1997; Yang and Liu, 1998) have pointed out the possible analogies between fault-trees and the PNs structures. Translating a fault or event-tree in a net structure does not constitute a risk analysis process as a previous analysis is, here also, required.

Despite these limitations, this method opens perspectives for future applications. Indeed, combining a physical or functional description of the system with a fault or event-tree *generator* may be of great interest.

CPN Applications

Modelling accident processes in a transportation system

Context. In order to predict possible accident scenarios in the Swissmetro, a high-speed underground train planned for interurban linking in Switzerland, PNs modelling capabilities have been investigated. Roughly speaking, the future Swissmetro system may be compared to a subway or a train in tunnels. This comparison is somewhat oversimplified as the Swissmetro presents a unique combination of hazards, usually encountered in either ground or air transportation. Thus, even if the experience acquired through previous accident cases may be of interest, the use of a prospective analysis method is required.

Approach. A STEP analysis has been conduced on several accident cases, which had occurred in similar systems (railway tunnel accidents). Surprisingly, it has appeared that: (1) the number of actors and events which may affect significantly the accident process is quite limited, (2) the time of occurrence or the duration of events is a key factor in such accident processes.

Relevant actors, events and causal relationships, identified during the retrospective STEP process, have been *translated* into the Petri net formalism. During simulation, one of the possible events succession is processed. Rather than investigating each *accident scenario* separately, the overall simulation results are examined through the occurrence graph, which recapitulate the reachable states allowed by the net structure. Interesting states may be investigated systematically, using the software built-in functions for occurrence graph nodes analysis. The approach used, which is briefly presented in Figure 2, may be perceived as a ″prospective″ STEP analysis. The calculation of the occurrence graph generates all possible sequence of events (or transitions), achievable in a multilinear accident process.

Figure 2. Principle of accident modelling

The model has been implemented on Design CPN (version 3.04, for Unix) software. Events, actors and cause-to-consequence relationships pointed out during the previous STEP analysis have been used to built the basic Petri net structure. Each actor of the accident process is depicted by a place in the net structure. Each token is coloured with a couple of values: A qualitative argument (the actor's action or situation) and a quantitative argument (the time of occurrence of the event). Only a limited number of possible events have been taken into account (about 20).

The PN structure describing one of the accidents actors (the passengers) is presented in Figure 3. It must be stressed that this example is somehow trivial, as the transitions are not depicted in a detailed way (time logic, input and output conditions). Each actor is depicted by a single place and a set of possible transitions. Each transition is dedicated to one of the possible events which may affect the actor. The passengers may, for instance, initiate a fire fighting action, assuming that there is an ignition and that a fire extinguisher is available. Thus, the fire *fighting* event is linked to two other actors: the fire and to the vehicle. Even if the right conditions are fulfilled, the fire fighting action may not be undertaken by the passengers. Two concurrent events may occurs in such a situation: (1) the passengers fight the fire until extinction or until it growth out of hands (2) for some reason no fire fighting is undertaken and the passengers are available for another action.

Figure 3. Modelling an actor of the accident process through Design CPN

Results. Despite the limited size of the net used, the simulation of the net structure leads to a large number of distinct scenarios. Modifying parameters, such as initial marking (initial accident conditions), time logic or cause to consequences relationships, while keeping the same number of events, leads to occurrence graph size ranging from 10^1 to $5 \cdot 10^4$ nodes.

Both net structure and simulation conditions must be chosen carefully in order to avoid occurrence graph outgrowing. As an example, Table 3 shows the occurrence graph's size resulting of a Petri net simulation according to two modes of time logic.

Table 3. Occurrence graphs size for several accident modelling

Accident scenarios have been interpreted in a more elaborate way, using Design CPN built-in functions to examine occurrence graph nodes. The results obtained are coherent regarding both previous tunnel accidents and tunnel safety principles (Vernez, 1999b).

Modelling health risks induced by man-technical workplace interactions (MORM project)

Context. The modelling of industrial processes through Petri nets to address OH&s concern in a systematic way is currently investigated. This project, which has started the year 2000, has the following goals. (1) to develop a model to describe a technical workplace dynamics ; (2) to establish, using known models in human cognitive behaviour, a man-at-work description ; (3) to develop a prototype tool for modelling and analysing occupational hazard due to the man-workplace interactions; and (4) to develop and to validate a user interface designed for occupational and safety specialists. The PN structures are built using the COOPN software tool (Biberstein, 2001)

Approach. As shown in Figure 4, the workplaces have been separated in three parts: a flow of material, one or several machines, and the human operator. The flow of material, which links the machines of the same process, is used to depict the operating sequence. The machines are perceived as entities which may induce changes to the flow properties (temperature, shape, weight,…).

The human actor is modeled in a rather implicit way. Indeed, each machine is linked to a set of possible actions, which can be undertaken by the human operator. Correct actions can easily be deduced from the machine's properties, while the CREAM cognitive model (Hollnagel 1998) is used to establish the set of possible errors. The human operator is modelled as a set of possible transitions, which may change the machine states, rather than as a Petri net in itself. CREAM is only used in a qualitative sense at the present time, but a quantitative analysis is intended in the MORM project.

Two types of man-machine interactions are considered. (1) The chronic and acute risks associated with the machines' states, which may affect the worker. (2) By remote control or direct (manual) operation, the worker may induce a

change of state in the machine. This action may be either an action intended in the normal operating procedure, a corrective action or an error. An overview of the model is presented in the Figure 4.

Figure 4. Principle of OH&S risks modelling through PNs

The machine was modelled using a physical state description. Every state (normal and degraded) was identified and related by transitions (e.g. *advance to blocking*).

Possible acute and chronic occupational risks (e.g. *electrocution*, *electrosmog*, *cutting*, *chemical*, etc.) are associated with the machines' states. Acute effects are modelled with new transitions that are attached to machine state (e.g. *electrocution* at breakdown). Chronic effects are modelled as new places that are filled up when some transitions are fired (e.g. *electrosmog* dose received at normal state), until a threshold is reached.

Results. At the present time, data on industrial machine are collected in order to build the corresponding PNs structures. Simulations have not been performed yet, but an example of the PNs developed to depict an industrial wire making process may give some insight of the project outcomes.

The aim of this industrial process is to produce metal wires from large metal billets. Metal billets are passed through a conveyor and distributed between three parallel stock slides. In the next step, the billets are heated in induction furnaces. When the correct temperature is reached, a hydraulic piston pushes the billet out of the furnace. The same piston brings the next billet from the corresponding stock slide. Another conveyor brings the red-hot billets to a hydraulic press. The billets are then pressed, at 200 atm, into metal wires.

Figure 5. A schematic representation of the wire making process

The metal wire making process is partly automated. The operator starts the sequence and then controls the operations through an indicator panel with electric commands. However, the operator or its co-workers still perform several tasks manually such as: (1) extracting hot billets from the furnace when the temperature is reached (based on the temperature value given on the panel); (2) starting the pressing sequence; and (3) separating the metallic residues adhering on the joint after pressing.

A schematic view of the PN state space obtained for an induction furnace is presented in Figure 6. For practical reasons, the possible human errors are not depicted here. Changes (PN transitions) in the possible machine states are linked to two external actors: the incoming material flows and the furnace operator. The furnace-degraded states (breakdown, overheating) may be linked to external situations, in which chronic occupational risks are of concern.

Figure 6. Modeling an induction furnace through COOPN

Although structured as a machine state-space, the PN model intended in the MORM project does both man-machine and man-flux interactions. As a matter of fact, a ″machine″ description does include the machine state-space itself, but is also directly linked to external events. Such events may be for instance; (1) normal actions, corrective actions or possible errors from the operator; (2) changes due to the incoming material flow and (3) occurrence of situations due to a machine degraded state (e.g. an EMF emission due to a furnace overheating).

Conclusions

The perspectives of PN applications to the field of risk analysis and accident modelling have been discussed in this paper. The possible "translations" of key concepts or functions used in safety sciences into the Petri Net formalism suggest tremendous possibilities. Indeed, either qualitative aspects of accident mechanisms or quantitative data, such as time logic or reliability calculations, may be processed in a Petri Net. This huge potential is also suggested by the wide range of previous applications made in the field of safety. Using a direct system description or the results of a Preliminary Hazards Analysis (PHA), authors have used PNs tools in order to get a variety of results such as, accident’s critical paths, safety or reliability data.

Despite this, it must be stressed that safety-oriented applications are still scarce. The lack of comprehensive tools available and PN inherent complexity may explain this situation. We can hope that, the increasing attractiveness of PNs may somehow overcome these difficulties. As a matter of fact, due to the tool continuous development (i.e.,

recent SRN or Object-oriented nets developments), PNs may play a significant role in risk analysis or accident modelling in the future.

References

Balakrishnan, M., Trivedi, K.S., 1996. Stochastic Petri nets for the reliability analysis of communication network applications with alternate-routing. Reliability Engineering and System Safety 52, 243-259.

Biberstein, O., Buchs, D., Guelfi, N., 2001. Object-oriented nets with algebraic specifications: The CO-OPN/2 formalism. In: Agha, G., De Cindio, F., Rozenberg, G. (Eds.). Concurrent Object-Oriented Programming and Petri Nets, Springer, Berlin, pp. 70-127. (Lecture Notes in Computer Science, Vol. 2001).

Brummer, J., Kersken, M., Märtz, J., 1994. Tools for software analysis. Reliability Engineering and System Safety 46, 123-138.

Buchs, D., Guelfi, N., 2000. A Formal Specification Framework for Object-Oriented Distributed Systems. IEEE TSE 26, 635-652.

Buchs, D., Buffo, M., 1999. Rapid prototyping of formally modelled distributed systems. In: Titsworth, F.M. (Ed.). Proc. of the Tenth International Workshop on Rapid System Prototyping RSP'99, IEEE, june 1999.

Buffo, M., Buchs, D., 1997. Coordination model for distributed object systems. In: Garlan, D., Le Metayer, D., (Eds.). Coordination Languages and Models, Springer, Berlin, pp. 410–413. (Lecture Notes in Computer Science, Vol. 1282).

Cordier, C., Fayot, M., Leroy, A., Petit, A., 1997. Integration of process simulations in availability studies. Reliability Engineering and System Safety 55, 105-116.

Dutuit, Y., Châtelet, E., Signoret, J.-P., Thomas, P., 1997. Dependability modelling and evaluation by using stochastic Petri nets : application to two test cases. Reliability Engineering and System Safety 55, 117-124.

El Koursi, M., 1992. Analyse de sécurité par réseau de Petri. Recherche Transports Sécurité 36, 11-21.

Ereau, J.-F., Saleman, M., Valette, R., Demmou, H., 1997. Petri nets for the evaluation of redundant systems.

Reliability Engineering and System Safety 55, 95-104.

Guelfi, N., Biberstein, O., Buchs, D., Canver, E., Gaudel, M.-C., von Henke, F., Schwier, D., 1997. Comparison of object-oriented formal methods. Technical Report 1997, Technical Report of the Esprit Long Term Research Project 20072, Design For Validation. University of Newcastle Upon Tyne, Department of Computer Science, Newcastle.

Hendrick, K., Benner, L., 1986. Investigating accidents with STEP. Dekker, New York.

Hollnagel, E., 1998. Cognitive reliability and error analysis method. Elsevier, Oxford.

Katsumata, M., Kurihara, M., Ohuchi, A., Sugasawa, Y., 1996. Serial failure diagnosis of a distributed processing system by Petri nets. Computers & Mathematics with Applications 31, 57-62.

Kontogiannis, T., Leopoulos, V., Marmaras, N., 2000. A comparison of accident analysis techniques for safety-critical man-machine systems. International Journal of Industrial Ergonomics 25, 327-347.

Liu, T.S., Chiou, S.B., 1997. The application of Petri nets to failure analysis. Reliability Engineering and System Safety 57, 129-142.

Malhotra, M., Trivedi, S., 1995. Dependability modelling using Petri-nets. IEEE Transactions on Reliability 44, 428-440.

Marier, S., El Mhamedi, A., Binder, Z., 1997. Analysis of a computer-aided teleoperation process by means of generalized stochastic Petri nets. Control Engineering Practice 5, 931-942.

Rochdi, Z., Driss, B., Mohamed, T., 1999. Industrial systems maintenance modelling using Petri nets. Reliability Engineering and System Safety 65, 119-124.

Rudas, I.R., Horvath, L., 1997. Modeling of manufacturing processes using a Petri net representation. Engineering Applications of Artificial Intelligence 10, 243-255.

Sczücs, A., Gerzson, M., Hangos, K.M., 1996. An intelligent diagnostic system based on Petri nets. Computers & Chemical Engineering 20, S635-S640.

Srinavasan, R., Venkatasubramanian, V., 1998a. Automating HAZOP analysis of batch chemical plants. Part I, The knowledge representation framework. Computers & Chemical Engineering 22, 1345-1355.

Srinavasan, R., Venkatasubramanian, V. 1998b. Automating HAZOP analysis of batch chemical plants. Part II, Algorithms and application. Computers & Chemical Engineering 22, 1357-1370.

Vernez, D., 1999a. Analyse de risque lors de la conception de projets novateurs : application au Swissmetro. Swiss Institute of Technology, Lausanne.

Vernez, D., 1999b. Using Petri nets for improving intrinsic safe design in a new transportation system. In: Goossens, L.H.J. (Ed.). Proceedings : 9th Annual Conference Risk Analysis, Facing the new millenium, Rotterdam, The Netherlands, October 10-13 1999, Delft university press, Delft, pp. 64-67.

Vidal-Naquet, G., Choquet-Genet, A., 1992. Réseaux de Petri et systèmes parallèles. Armand Colin, Paris.

Wang, L.-C., Wu, S.-Y., 1998. Modeling with colored timed object-oriented Petri nets for automated manufacturing systems. Computers & Industrial Engineering 34, 463-480.

Yang, S.K., Liu, T.S., 1998. Petri net approach to early failure detection and isolation for preventive maintenance. Quality & Reliability Engineering International 14, 319-330.

Yoshikawa, H., Nagakawa, T., Furuta, T., Hasegawa, A., 1997. Development of an analysis support system for man-machine system design information. Control Engineering Practice 5, 417-425.

Figure 1. Functional and graphical description of PNs

$P \in \{P_1 ... P_m\}$ = *set of places*

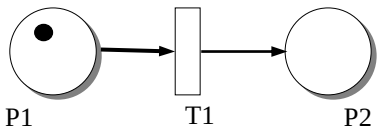
$T \in \{T_1 ... T_n\}$ = *set of transitions*

W = *valuation function* $P \cup T$ ($\times T \cup P$ *dans* N)

M_0 = *initial marking*

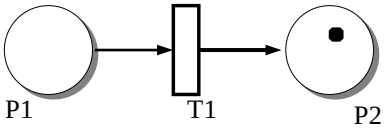
$W(P_i,T_j)$ = *precondition of a transition (number of token necessary in place i to fire the transition j)*

$W(T_j,P_i)$ = *post condition of a transition (number of token given to place i after firing the transition j)*



Initial marking (1;0)

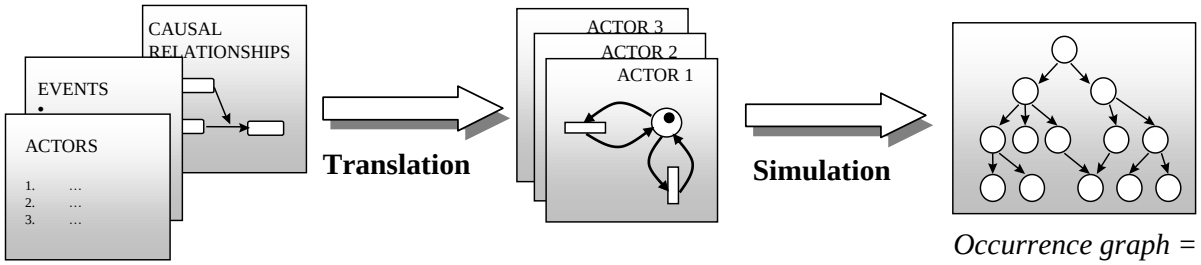
(a). transition before firing



final marking (0;1)

(b). transition after firing

Figure 2. Principle of accident modelling



Accident relevant elements

Petri net

Occurrence graph = accident scenarios

Figure 3. Modelling an actor of the accident process through Design CPN

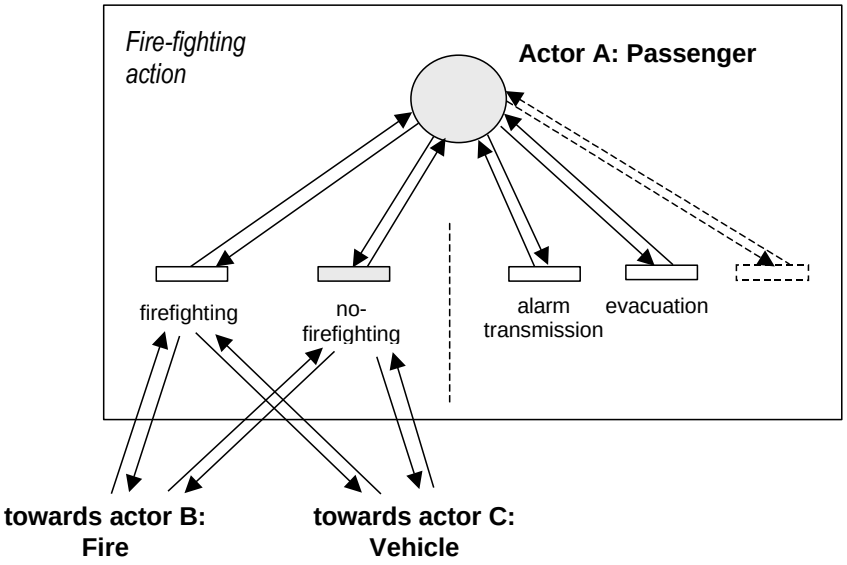


Figure 4. Principle of OH&S risks modelling through PNs

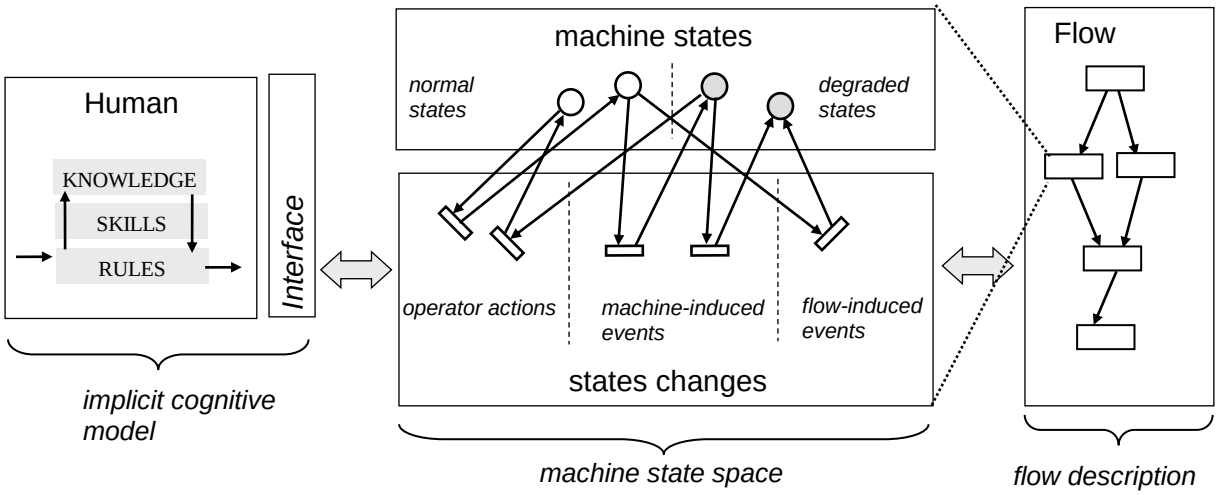


Figure 5. A schematic representation of the wire making process

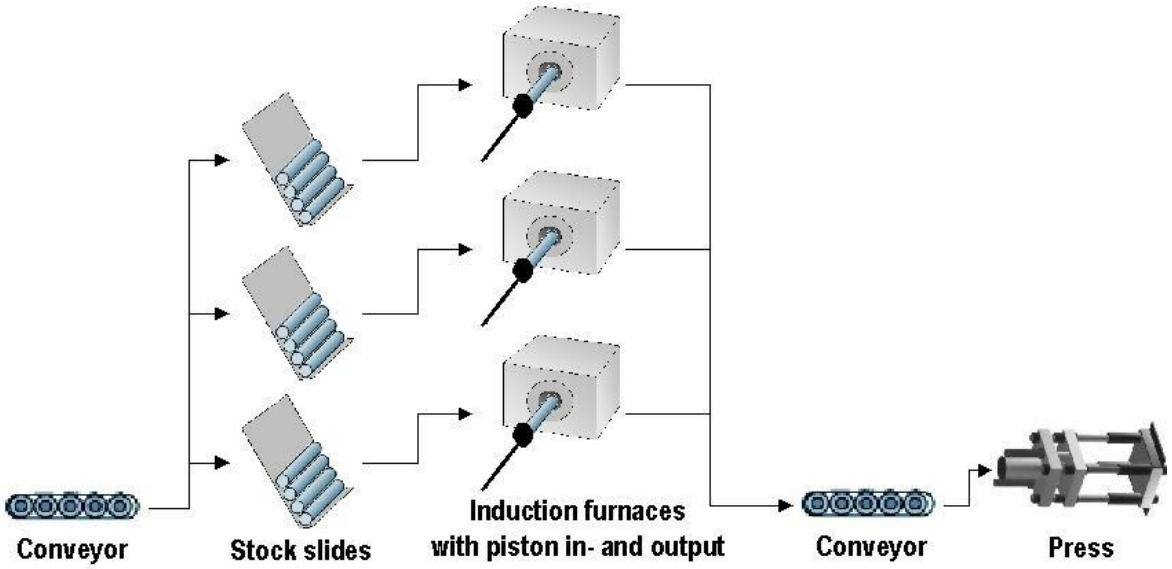


Figure 6. Modeling an induction furnace through COOPN

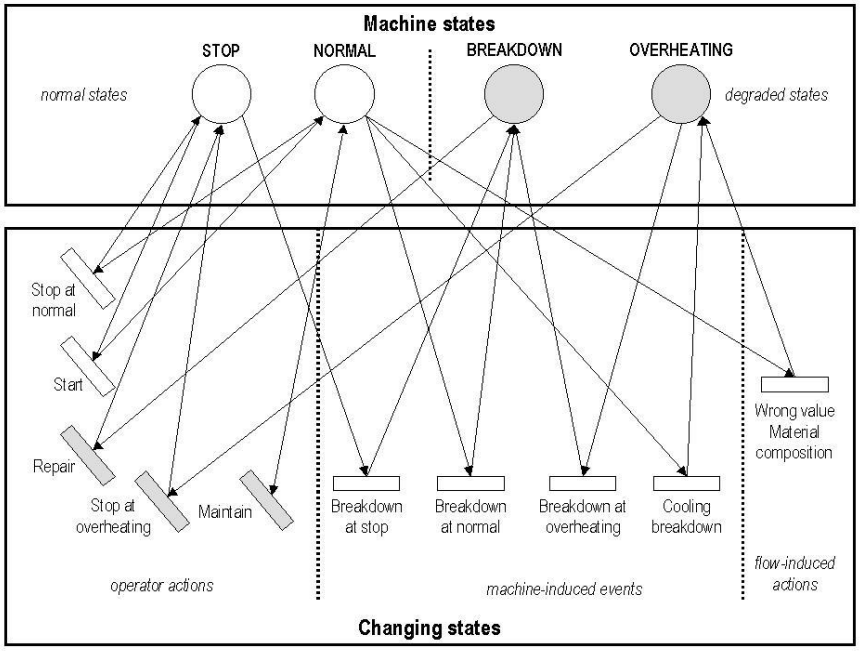
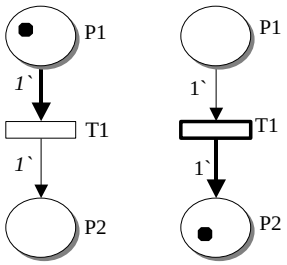
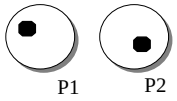
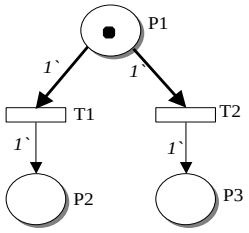
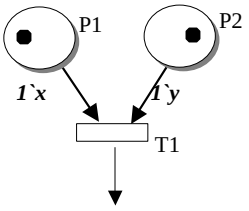
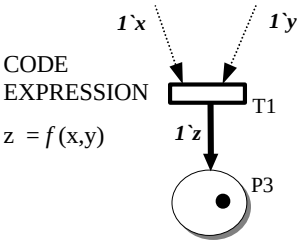
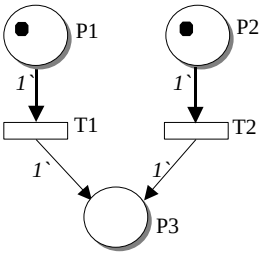
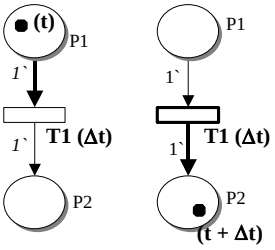


Table 1. Use of PNs tools in the field of safety

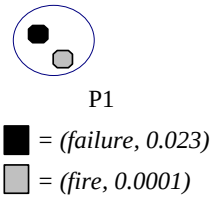
Reference	Required	Modelled	Petri Net	Results
El Koursi, 1992	Physical description	State of space	PN	Safety data
Brummer et al., 1994	System states	State of space	PN	Safety data
Malhotra and Trivedi, 1995	Cause-to-consequences relationships	Events and logical gates	GSPN - SRN	Failure data
Balakrishnan and Trivedi, 1996	System states	State of space	SRN	Reliability data and critical paths
Katsumata et al., 1996	System states	State of space	PN	Failure diagnosis
Szücs et al., 1996	Physical description	Objects, modes, and failure modes	CPN	Critical pathways
Cordier et al., 1997	System states	State of space	SPN	Reliability data
Dutuit et al., 1997	System states	State of space with stochastic transitions	SPN	Reliability data
Ereau et al., 1997	System states	State of space with stochastic transitions	Timed PN	Reliability data
Liu and Chiou, 1997	Cause-to-consequences relationships	Events and logical gates	PN	Failure data
Marier et al., 1997	System states	State of space with stochastic transitions	GSPN	Reliability data
Rochdi et al., 1999	Cause-to-consequences relationships	Events and logical gates	PN	Failure data
Rudas and Horvath, 1997	Physical description	Objects and modes	PN	Dynamic behaviour data
Yoshikawa et al., 1997	System states	State of space	CPN	Safety data
Srinavasan and Venkatasubramanian, 1998a and 1998b	System states	State of space	PN	Safety data
Wang and Wu, 1998	Physical description	Objects and modes	CPN	Dynamic behaviour data
Yang and Liu, 1998	Cause-to-consequences relationships	Events and logical gates	PN	Failure data
Vernez, 1999a and 1999b	Cause-to-consequences relationships	Accident events sequences	CPN	Safety data, critical paths
Kontogiannis et al., 2000	System states	State of space	PN	Reliability data and critical paths

Table 2. ″Translations″ of safety concepts into PN structures

Function/ concept	Comment	*PN structure*	Description
(a) Qualitative aspects			
Discrete event	Discrete event are used in event-based methods to describe the occurrence of a sudden event, which my change the system state.	*Transition firing* 	Firing a transition consumes token(s) from incoming place(s) and produce token(s) to outgoing places. The change of marking does change the state of the net.
Qualitative state/mode	A qualitative description of a component or a subsystem state is commonly used in inductive methods (such as a failure mode in FMEA)	*Place name*  *P1 = failure* *P2 = fire*	Naming a PN place adds a qualitative argument to the system state
		Token's colour  *= (failure, 0.023)* *= (fire, 0.0001)*	In a coloured net, tokens are differentiated through labelling. The argument used for labelling may contain either qualitative or quantitative data. From a functional viewpoint, a coloured net is a synthetic way to express a classical net with labelled places.
Divergent consequences	In an event-tree (or a decision tree), an event with several possible outcomes is expressed, using a divergent branching in the event sequence.	*Conflicting transitions* 	Transitions requiring common resources to be fired are conflicting. Only one of the conflicting transitions will be fired while processing the PN structure. The resulting occurrence graph will display a branching in the sequence of accessible states.

Causal relationship	The prime logical function used in either deductive or inductive RA methods is the cause to consequence relationship. Consequence events may happen only when causal events have occurred.	*Transition conditions*  GUARD EXPRESSION **X=…** andalso **Y=…**	Several ways may be used in PN structures to set conditions to a transition firing: a) incoming arcs may be used to define prerequisite conditions (markings) to a firing b) some PN tools allow the use of transitions with code expressions. Complex firing conditions may be introduced in code expressions (for instance with the use of Boolean logic)
Logical gates	Logical gates are used to describe causes to consequences relationships in a Boolean way. A logical gate is required when the occurrence of an event depends on a combination of previous conditions or events. AND or OR logical gates are commonly used in deductive RA methods, such as FTA.	*Code expression*  	In CPNs, the colour of the token(s) produced by a transition firing may be defined in a code expression. Boolean logic or algebraic calculations may be used in a code expression.
Parallel events sequences	Events without direct cause to consequences relationships may occur in a simultaneously, leading to parallel events sequences. Modelling parallel sequences in a detailed way is of utmost interest in system with time constraints.	*Concurrent transitions*  	Concurrent transitions, which are not conflicting, are fired simultaneously while processing PN structures.
		Timed PNs  	In timed PNs, time constraints may be simulated, while attaching duration to transitions firing.

(b) Quantitative aspects

Failure ratio	Either event frequency or probability is used in quantitative RA methods, such as FTA, in order to calculate a top event occurrence.	*Token's colour*  	In a coloured net, tokens are differentiated through labelling. The argument used for labelling may contain either qualitative or quantitative data. From a functional viewpoint, a coloured net is a synthetic way to express a classical net with labelled places.
		Stochastic nets	In stochastic nets, an occurrence probability is attributed to transitions.

(c) Analysing / processing

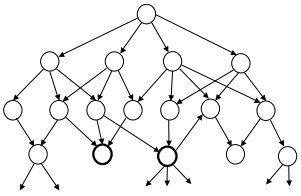
Possible accident paths	The goal of many event-based RA methods is to establish all possible accident paths in a qualitative and/or quantitative way.	*Occurrence graph* 	Processing a PN structure does generate an occurrence graph, which describes all reachable *states* (markings) of the net.

Table 3. Occurrence graphs size for several accident modelling

Simulation conditions	**Numb. of nodes**	**Numb. of death nodes**
all events, fuzzy time	48’975	6533
all events, fixed time	1’857	361