Discrete and Hybrid Systems Dependability Analysis with ESA PetriNet

Romaric Guillerm, Nabil Sadou, Hamid Demmou

Discrete and Hybrid Systems Dependability Analysis with ESA PetriNet

Romaric Guillerm[#1], Nabil Sadou[*2], Hamid Demmou[#3]

[#]*LAAS-CNRS, Université de Toulouse*
7, avenue du Colonel Roche, 31077 Toulouse Cedex 04, France
[1]guillerm@laas.fr
[3]demmou@laas.fr

[*]*SUPELEC / IETR*
Avenue de la Boulais, BP 8112, 35511 Cesson-Sevigne, France
[2]nabil.sadou@supelec.fr

***Abstract*—Based on Petri net modelling and linear logic as formal framework, ESA PetriNet allows to carry out dependability analysis of discrete (based on temporal Petri nets modelling) or hybrid systems (differential predicate-transition Petri nets modelling). ESA PetriNet implements the approach for critical scenarios deriving. The approach is based on a qualitative analysis of Petri net model. It consists in determining a sequence of events represented by transition firings in the Petri net model that leads the system from normal working to critical situation. ESA PetriNet allows deriving only pertinent scenarios. Minimality of these scenarios (composed by the necessary events) is introduced to facilite the analysis step.**

***Keywords*—Petri net, dependability analysis, embedded system, feared scenario, minimality.**

I. Introduction

To address reliability of dynamic systems [1], some approaches are based on the deriving of feared scenarios. These approaches consist on determining the sequences of events that lead a system to a critical situation.

Our approach is focused on the search for feared scenarios. In order to propose a way to avoid the problem of state space explosion, the basic idea is to use a Petri net model and directly extract the feared scenario without building the accessibility graph [2].

Based on Petri net model [3], a qualitative analysis allows determining a partial order of transition firings and extracting feared scenarios. The analysis is focalized on the parts of the model that are interesting for reliability analysis [4], avoiding the exploration of the global system.

The identification of feared scenarios can be helpful for the designer. It allows understanding the system failure reasons in order to establish the redundancy mechanisms and the reconfigurations.

ESA PetriNet (Extraction Scenarios Analysis) is a software tool which implements our algorithm to extract critical scenarios. This paper gives, shortly, the principles of the algorithm implemented in ESA PetriNet and overviews of tool capabilities, and applications.

This paper is organized as follows: section 2 presents the discrete deriving feared scenarios algorithm and the continuous scenarios extraction algorithm. Section 3 describes ESA PetriNet tool. Section 4 gives a short example of application and section 5 draws conclusions and future works.

II. Scenario Extraction Algorithm

A feared scenario is a set of events (transition firings for a Petri net model) verifying a partial order and leading from one partial state corresponding to normal behaviour (partial marking) to another one that represents a dangerous situation of the system. This situation can represent a degraded operating mode or a failure of the system.

A. Discrete Scenario Deriving Algorithm

The algorithm is based on a qualitative analysis stemming from the Petri net model. The objective is to extract and clearly identify the feared scenarios starting from a model that contains the necessary knowledge to make the analysis. In this model, normal and abnormal states are defined.

The initial partial knowledge of the feared state is progressively enriched while analyzing the components necessary to its occurrence. This algorithm is made up of two steps: a backward and a forward reasoning process. The backward reasoning starts from the partial feared state in order to derive the events that are necessary to reach it, and gives the last nominal (normal) states preceding the critical behaviour. The forward reasoning starts from these nominal states, and determines the components at the origin of the feared scenario. To determine the complete context in which the feared scenario occurs, the concept of context enrichment is introduced. The context enrichment is carried out by adding tokens to some places (empty input places of potentially enabled transitions) that can have an impact on the feared scenario that is being explored.

B. Continuous Scenario Deriving Algorithm

The continuous algorithm is developed for hybrid systems analysis [5]. It combines the initial algorithm (discrete scenario deriving algorithm) and a differential equation solver to handle the continuous part. The Petri net model used is differential predicate-transition Petri net proposed in [6]. The Petri net model describes the operation modes, the failures and the reconfiguration mechanisms. The differential equations

represent the evolution of continuous variables of the energetic part of the system.

The principle of the continuous deriving of feared scenario algorithm consists on coupling two simulators. The first one simulates the Petri net (deriving scenario algorithm) and the second simulates the differential equations systems (integrator). The two simulators evolve alternatively and are synchronized by the events.

The discrete algorithm determines, according to the discrete state of the system, the equations to be integrated and the thresholds to be supervised. The continuous simulator is called and integrates the equations until all the thresholds of the enabled transitions are reached. Then, the simulator transmits the dates to the algorithm, which runs according to the transmitted firing dates. The algorithm uses these dates to determine the evolution of the discrete state and updates the new system of equations to be integrated.

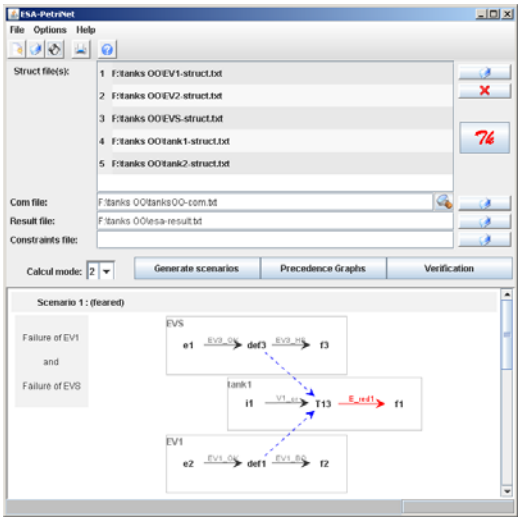

Fig. 1 ESA PetriNet screen snapshot

III. Tool Presentation

In this part, we present the new tool (Fig. 1) which allows the extraction of critical scenarios from a Petri nets model.

A. Input Files

The input files of the tool correspond to a textual description of the temporal Petri net model of the system. The tool TINA (TIme Petri Net Analyzer) [7] is used for Petri net model description and its structural analysis. This structural analysis is necessary because it gives the marking invariants which allow or not the marking enrichments [4].

In the case of the hybrid version of ESA PetriNet, a second type of file must be specified. It contains differential equation associated with each place and so describes the continuous dynamic of the system.

B. Minimality Analysis

The final objective is to determine all minimal scenarios (to guarantee minimality and completeness). Indeed, one scenario can lead to a feared state and contain events (that are the consequence of another events of the scenario), which are not strictly necessary to reach the final feared state. So to restrict the derived scenarios to minimal ones, based on the definition of minimal scenario [8], ESA PetriNet generates only minimal scenarios which are of major interest to the designer.

C. Precedence Graphs: the Feared Scenarios

Once all the input files are specified, the tool provides the feared scenarios in the form of precedence graphs after the research of critical scenarios and the minimality analysis. This representation is very appropriate because it shows clearly the sequences of events and the parallelism.

IV. Case Study

In this part, a short case study presents an application of a feared scenarios research with the tool ESA PetriNet.

A. Presentation

The chosen example to illustrate the approach is based on a volume regulation system of two tanks (Fig. 2). It consists of a controller, two pumps, three electrovalves, two volume sensors, the two regulated tanks and a third tank for draining.

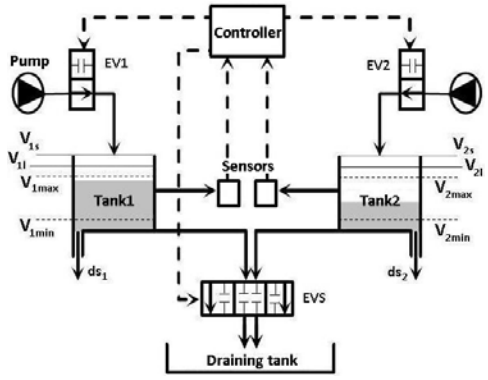

Fig. 2 Case study

The volume of each tank must be kept inside the interval [V_{imin}, V_{imax}]. The volume is regulated by the controller, which decides, according to the values given by the volume sensors, to fill (or not) the concerned tank by opening (or not) the electrovalve. In the case of the volume reaches V_{il}, due to a failure of the electrovalve i, the controller tries to open the relief electrovalve for draining the concerned tank until the volume becomes lower than V_{imin}. If the volume reaches Vis, the tank overflows: which corresponds exactly to the studied critical situation.

To simplify the problem, we consider that only the electrovalves can have failures. And in this paper, we focus only on the discrete approach.

B. Modelling

In order to find the feared scenarios with ESA PetriNet, we must model the system. We propose 3 object classes for the modelling: one tank class and two electrovalve classes. Using the formalism of temporal Petri net, we defined two objects (*tank1* and *tank2*) instances of tank class (Fig. 3), two objects (*EV1* and *EV2*) instances of the first electrovalve class (Fig. 4) and one object (*EVS*) instance of the third class (Fig. 5). In

this paper, we will not explain in details the modelling. Only some important points will be given.

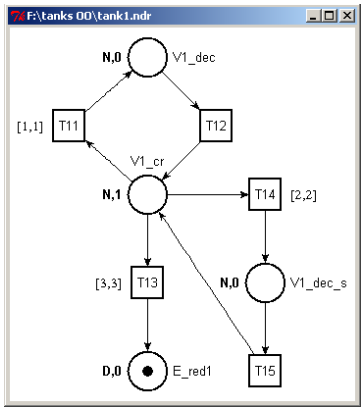

Fig. 3 Model of the tank 1

In the tank model, the three transitions *T11*, *T14* and *T13* will respectively allow the use of *EV1*, allow the use of *EVS* in the case of *EV1* failure, and represent the overflow of the tank. The thresholds *[1,1]*, *[2,2]* and *[3,3]* define like a priority between these three transitions.

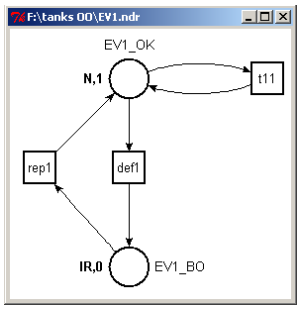

Fig. 4 Model of the electrovalve 1 (EV1)

The electrovalve *EV1* is used when the transition *t11* is called. It can fail when *def1* is fired, in this case the electrovalve is out of service and *t11* cannot be called.

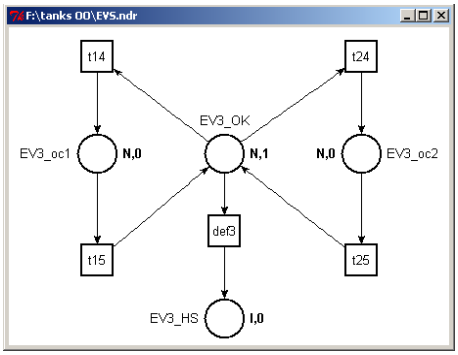

Fig. 5 Model of the relief electrovalve (EVS)

Concerning the relief electrovalve, it can be free for use (place *EV3_OK* marked) or can be used by only one of the two tanks at the same time (place *EV3_oc1* for *tank1* and place *EV3_oc2* for *tank2*), the other tank haven't access to *EVS* until it become free another time.

Thus, five objects are defined and modelled. In order to build a consistency model of the system, we mustn't forget to specify the communication between these objects. This is done throw the communication file given in the Fig. 6. Just to give one example, the first information of this file shows that the transition *T11* of *tank1* called the transition *t11* of *EV1*.

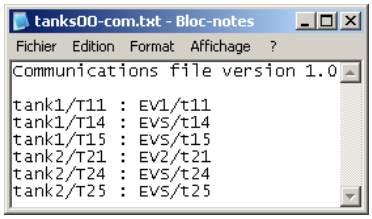

Fig. 6 Communication file

C. Use of ESA PetriNet: the Feared Scenarios

The model of the system is ready, with all the normal states specified (through the label '*N*') and a partial critical state defined (place *E_red1* marked, representing the overflow of the tank 1). Thus, ESA PetriNet can be used for extracting the feared scenarios. The Fig. 1 gives a screen snapshot of the tool just after the generation of the feared scenarios. Two scenarios are identified.

The first one, in Fig. 7, is composed by the events: failure of the electrovalve *EV1*, failure of the relief electrovalve *EVS*, followed by the overflow of *tank 1*.

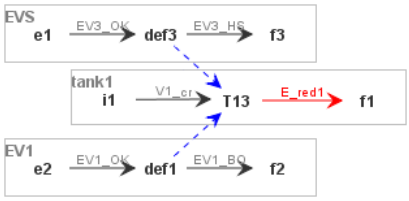

Fig. 7 Feared scenario 1

The second scenario, in Fig. 8, is composed by the events: failure of the electrovalve *EV1*, failure of *EV2*, use of *EVS* to drain the *tank 2*, followed by the overflow of *tank 1* which doesn't have access to the relief electrovalve *EVS*.

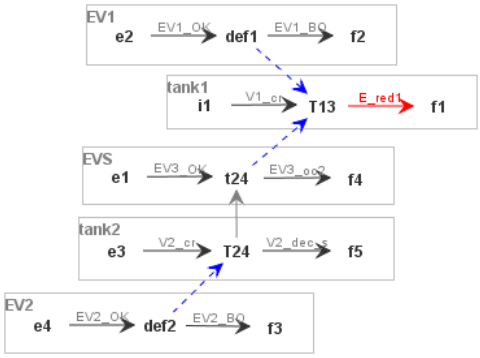

Fig. 8 Feared scenario 2

D. Exploitation of the Results

The approach makes it possible to highlight the interactions between the different components that are implicated in the

feared scenarios. It shows the sharing of the relief electrovalve between the two tanks and the competition between the release of this resource by one of the two tanks and the overflow of the other one.

The designer is informed that there are only these two scenarios which lead to the overflow of the tank 1, considering the failures of the three electrovalves. Thus, he can note that only one failure of one electrovalve doesn't lead the system in the critical situation. The only possibilities which lead to the overflow of the tank 1 are with a minimum of two defective electrovalves. So, the designer can evaluate the dependability of the system and his reconfiguration mechanism with one relief electrovalve. He can be satisfied with the results or, if he doesn't, can propose new system architecture in order to improve the dependability of the system.

V. CONCLUSIONS

The tool (ESA PetriNet) presented in this paper is based on the modelling of embedded systems by temporal or hybrid Petri net. Oriented object concepts are introduced to facilitate system modelling and scenario analysis. Indeed, by exploiting the object independence principle, a global analysis problem is decomposed into a set of local object analysis.

ESA PetriNet allows deriving, from this Petri net model, scenarios leading to feared states. It allows, starting from a feared state, to go back through the chain of causality and to point out all the possible scenarios leading to a feared state. Each scenario is given by a partial order between the events necessary to the occurrence of the feared event.

The tool allows generating only pertinent scenarios. It takes into account the notion of minimal scenario which is the relevant information for designers.

Future work concerns the quantitative analysis. Monte Carlo simulation is a technique that will be used to achieve quantitative analysis and will be implemented in ESA PetriNet.

REFERENCES

[1] Dufour. F, Y. Dutuit, "Dynamic Reliability: A new model", 13-ESREL2002 European Conference, Lyon - France - 18 au 21 Mars 2002.

[2] N.Sadou, H.Demmou, J.C.Pascal, R.Valette, "Continuous dynamic abstraction for reliability and safety analysis of hybrid systems," *6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Beijing, 2006.

[3] Ramchandani. C, *Analysis of asynchronous concurrent systems by Petri nets*, Massachusetts Inst. Technol. Cambridge, Project MAC,TR-120, 1974.

[4] N.Sadou, H.Demmou, J.C.Pascal, R.Valette, "Object oriented approach for deriving feared scenarios in hybrid system," *2005 European Simulation and Modeling Conference*, Portugal, 24-26 Octobre 2005, pp.572-578.

[5] R. Alur, T. Henzinger, G. Lafferriere, and G.Pappas. Discrete abstractions of hybrid systems. In Proceedings of IEEE, volume 88, pages 971-984, 2000.

[6] Champagnat, R, P. Esteban, H. Pingaud, R. Valette (1998) "Modelling and simulation of a hybrid system through Pr/Tr PN DAE model", ADPM'98 3rd International Conference on Automation of Mixed Processes, 19-20 March, Reims, France p. 131-137.

[7] B. Berthomieu, F. Vernadat, "Time Petri Nets Analysis with TINA, tool paper," *In Proceedings of 3rd Int. Conf. on The Quantitative Evaluation of Systems (QEST 2006)*, IEEE Computer Society, 2006.

[8] N. Sadou, H. Demmou, "Minimality of critical scenarios in Petri net model," *2006 IEEE International Conference on Systems Man and Cybernetics (SMC'06)*, Taipei (Taiwan), 8-11 October 2006, 8p.