DISTA
Università del Piemonte Orientale ”A. Avogadro”
Corso Borsalino 54, 15100 Alessandria

TECHNICAL REPORT - TR-INF-2002-02-02-UNIPMN

From FPN to NuSMV: The temperature control system of the ICARO cogenerative plant

Authors: Andras Horváth, Marco Gribaudo and Andrea Bobbio

February 2002

TECHNICAL REPORT - TR-INF-2002-02-02-UNIPMN
February 2002

From FPN to NuSMV: The temperature control system of the ICARO cogenerative plant

Authors: Andras Horváth, Marco Gribaudo and Andrea Bobbio

Contents

From FPN to NuSMV: The temperature control system of the ICARO cogenerative plant

TR-INF-2002-02-02-UNIPMN

András Horváth[1], Marco Gribaudo[2] and Andrea Bobbio[3]

[1] Department of Telecommunications, University of Technology and Economics, Budapest, Hungary
[2]Dipartimento di Informatica, Università di Torino, 10149 Torino, Italy
[3]DISTA, Università del Piemonte Orientale, 15100 Alessandria, Italy.

Abstract

The modeling and analysis of hybrid systems is a recent and challenging research area which is actually dominated by two main lines: a functional analysis based on the description of the system in terms of discrete state (hybrid) automata (whose goal is to ascertain for conformity and reachability properties), and a stochastic analysis (whose aim is to provide performance and dependability measures). The present technical report investigates a unifying view between formal methods and stochastic methods by proposing an analysis methodology of hybrid systems based on Fluid Petri Nets (FPN). It is shown that the same FPN model can be fed to a functional analyser for model checking as well as to a stochastic analyser for performance evaluation. We illustrate our approach and show its usefulness by applying it to a "real world" hybrid system: the temperature control system of a co-generative plant. The technical report describes the systems in terms of FPN, then shows how the FPN can be converted into a hybrid automata (following the specifications of the tool HyTech) and into a discrete model based on finite state machine according to the specifications of the tool NuSMV. The complete NuSMV specifications are finally provided, and some results derived using the tool NuSMV.

1 Introduction

This paper investigates an approach to model checking starting from a fluid Petri net (FPN) model, for formally verifying the functional and safety properties of hybrid systems. This paper shows that FPN [1, 2, 3] can constitute a suitable formalism for modeling hybrid systems, like the system under study, where a discrete state controller operates according to the variation of suitable continuous quantities (temperature, heat consumption). The parameters of the models are usually affected by uncertainty. A common and simple way to account for parameter uncertainty is to assign to them a range of variation (between a minimum and a maximum value), without any specification on the actual value assumed by the parameter in a specific realization (non-determinism). Hybrid automata [4] and discretized model checking tools [5] operates along this line. If a weight can be assigned to the parameter uncertainty through a probability distribution, we resolve the non-determinism by defining a stochastic model: the FPN formalism [2, 6] has been proposed to include stochastic specifications. However, the paper intends to show that a FPN model for an hybrid system can be utilized as an input model both for functional analysis as well as for stochastic analysis. In particular, the paper shows that the FPN model can be translated in terms of a hybrid automaton [7, 8] or a discrete model checker [9].

FPN's are an extension of Petri nets able to model systems with the coexistence of discrete and continuous variables [1, 2, 3]. The main characteristics of FPN is that the primitives (places, transitions and arcs) are partitioned in two groups: discrete primitives that handle discrete tokens (as in standard Petri nets) and continuous (or fluid) primitives that handle continuous quantities (referred to as fluid). Hence, in the single formalism, both discrete and continuous variables can be accommodated and their mutual interaction represented.

Even if Petri nets and model checking rely on very different conceptual and methodological bases (one coming from the world of performance analysis and the other form the world of formal methods), nevertheless the paper attempts to gain cross fertilizations from the two areas. The main goal of the research work presented in this paper is to investigate on the possibility of defining a methodology which allows to refer to a common FPN model to be used both for formal specification and verification with model checking tools and for performance analysis.

We describe our approach and show its usefulness by using a meaningful "real world" application. Namely, we assume as a case study the control system of the temperature of the primary and secondary circuit of the heat exchange section of the ICARO cogenerative plant [10] in operation at centre of ENEA CR Casaccia. The plant, under study, is composed by two sections: the gas turbine section for producing electrical power and the heat exchange section for extracting heat from the turbine exhaust gases.

The paper is organized as follow. Section 2 describes our case study. Section 3 introduces the main elements of the FPN formalism, provides the FPN model of the case study, and its conversion into an hybrid automaton. Section 4 shows how the same FPN model can be translated into a discrete models checker (NuSMV [11]) and provides some of our experimental results. Section 5 gives the conclusions.

2 Temperature control system

The ICARO co-generative plant is composed by two sections: the electrical power generation and the heat extraction from the turbine exhaust gases. The exhaust gases can be conveyed to a re-heating chamber to heat the water of a primary circuit and then, through a heat exchanger, to heat the water of a secondary circuit that, actually, is the heating circuit of the ENEA Research Center.

If the thermal energy required by the end user is higher than the thermal energy of the exhaust gases, fresh methane gas can be fired in the re-heating chamber where the combustion occurs. The flow of the fresh methane gas is regulated by the control system through the position of a valve.

The block diagram of the temperature control of the primary and secondary circuits is depicted in Figure 1. The control of the thermal energy used to heat the primary circuit is performed by regulating both the flow rate of the exhaust gases through the diverter D and the flow rate of the fresh methane gas through the valve V. T_1 is the temperature of the primary circuit, T_2 is the temperature of the secondary circuit, and u is the thermal request by the end user.

The controller has two distinct regimes (two discrete states) represented by the position 1 or 2 of the switch W in Figure 1. Position 1 is the normal operational condition, position 2 is the safety condition. In position 1, the control is based on a proportional-integrative measure (performed by block PI_1) of the error of temperature T_2 with respect to a (constant) set point temperature T_s. Conversely, in position 2, the control is based on a proportional-integrative measure (performed by block PI_2) of the error of temperature T_1 with respect to a (constant) set point temperature T_s. Normally, the switch W is in position 1 and the control is performed on T_2 to maintain constant the temperature

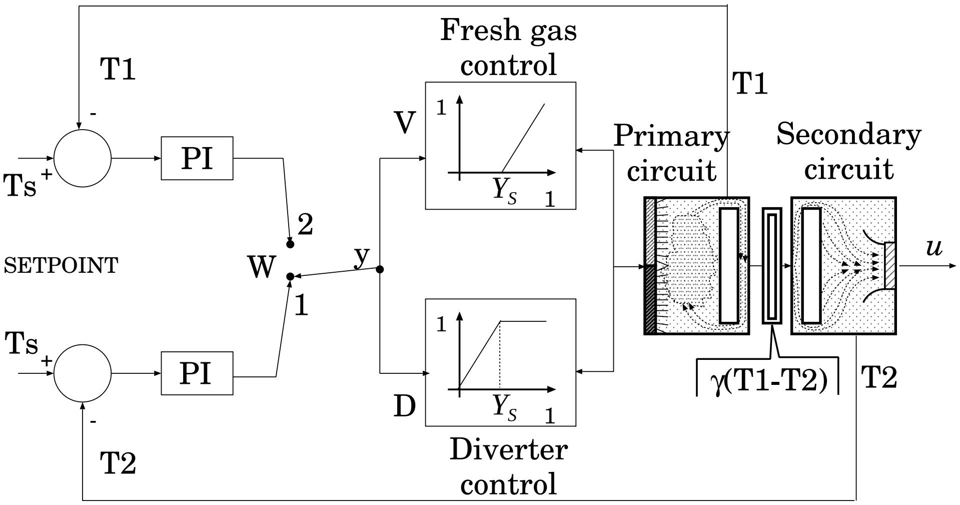

Figure 1: Temperature control of the primary and secondary circuits of the ICARO plant.

to the end user. Switching from position 1 to position 2 occurs for safety reasons, when the value of T_2 is higher than a critical value defined as the set point T_s augmented by an hysteresis value T_h and the control is locked to the temperature of the primary circuit T_1, until T_1 becomes lower than the set point T_s.

The exit of the proportional-integrative block (either PI_1 or PI_2, depending on the position of the switch W) is the variable y which represents the request of thermal energy. When y is lower than a split point value Ys the control just acts on the diverter D (flow of the exhaust gases), when the diverter is completely open, and the request for thermal energy y is grater than Ys, the control also acts on the flow rate of the fresh methane gas by acting on the valve V.

The heating request is computed by the function $f(y)$ represented in Figure 2. Since the temperature T_2 is checked out when W is in position 1, and the temperature T_1 is checked out in state 2, the function $f(y)$ depends on y_2 when $\mathsf{W} = 1$ and on y_1 when $\mathsf{W} = 2$. The function $f(y)$ is defined as the sum of two non-deterministic components $g_1(y)$ which represents the state of the valve V, and $g_2(y)$ which represents the state of the diverter D. The non-determinism is introduced by the parameters $\alpha_{min}, \alpha_{max}$ that give the minimal and maximal heat induced by the fresh methane gas, and β_{min}, β_{max} that define the minimal and maximal heat induced by the exhaust gases.

Finally, the heat exchange between the primary and the secondary circuit is is approximated by the linear function $\gamma(T_1 - T_2)$, proportional (through a constant γ) to the

$$\frac{g_1(y)}{\alpha_{max}} + \frac{g_2(y)}{\beta_{max}} \leq f(y) \leq \frac{g_1(y)}{\alpha_{min}} + \frac{g_2(y)}{\beta_{min}}$$

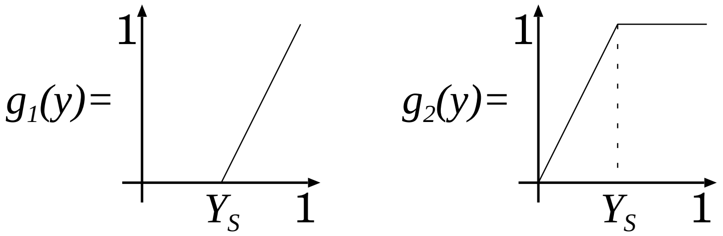

Figure 2: The heating request function $f(x)$

temperature difference.

3 Fluid Petri Nets

Fluid Petri Nets (FPN) are an extension of standard Petri Nets [12], where, beyond the normal places that contain a discrete number of tokens, new places are added that contain a continuous quantity (fluid). Hence, this extension is suitable to be considered for modeling and analyzing hybrid systems. Two main formalisms have been developed in the area of FPN: the Continuous or Hybrid Petri net (HPN) formalism [1], and the Fluid Stochastic Petri net (FSPN) formalism [2, 3]. A complete presentation of FPN is beyond the scope of the present paper and an extensive discussion of FPN in performance analysis can be found in [6].

Discrete places are drawn according to the standard notation and contain a discrete amount of tokens that are moved along discrete arcs. Fluid places are drawn by two concentric circles and contain a real variable (the fluid level). The fluid flows along fluid arcs (drawn by a double line to suggest a pipe) according to an instantaneous flow rate. The discrete part of the FPN regulates the flow of the fluid through the continuous part, and the enabling conditions of a transition depend only on the discrete part.

3.1 A FPN description of the system

The FPN modeling the case study of Figure 1 is represented in Figure 3. The FPN contains two discrete places: $P1$ which is marked when the switch W is in state 1, and $P2$ which is marked when the switch W is in state 2. Fluid place *Primary* (whose marking is denoted by T_1, and has a lower bound at T_s) represents the temperature of

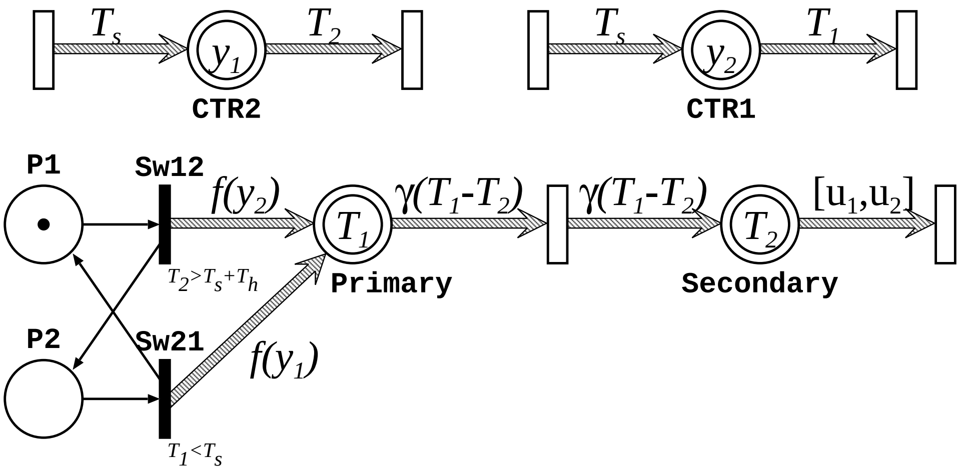

Figure 3: FPN model of the temperature Controller

the primary circuit, and fluid place *Secondary* (whose marking is denoted by T_2 and has an upper bound at $T_s + T_h$) represents the temperature of the secondary. The fluid arcs labeled with $\gamma(T_1 - T_2)$ represent the heat exchange between the primary and the secondary circuit. The system jumps from state 1 to state 2 due to the firing of immediate transition $Sw12$. This transition has associated a guard $T_2 > T_s + T_h$ that makes the transition fire (inducing a change of state) as soon as the temperature T_2 exceeds the *setpoint* T_s augmented by an histeresys value T_h. The change from state 2 to state 1 is modeled by the immediate transition $Sw21$, whose firing is controlled by the guard $T_1 < T_s$ that makes the transition fire when the temperature T_1 goes below the *setpoint* T_s. In order to simplify the figure, we have connected the fluid arcs directly to the immediate transitions. The meaning of this unusual feature is that fluid flows across the arcs as long as the immediate transitions are enabled regardless of the value of the guards.

The fluid arc in output from place *secondary*, represents the end user demand. The label on this arc is $[u_1, u_2]$, indicating the possible range of variation of the user demand. Fluid place $CTR2$, whose marking is denoted by y_1, models the exit of the proportional-integrator PI_1. This is achieved by connecting to place $CTR1$ an input fluid arc, characterized by a variable flow rate equal to T_2, and by an output fluid arc with a constant fluid rate equal to the *setpoint* T_s. In a similar way, the exit of the proportional-integrator PI_2 is modeled by fluid place $CTR2$ (whose marking is denoted by y_2). The fluid arcs that connect transition $Sw12$ and $Sw21$ to fluid place *primary*

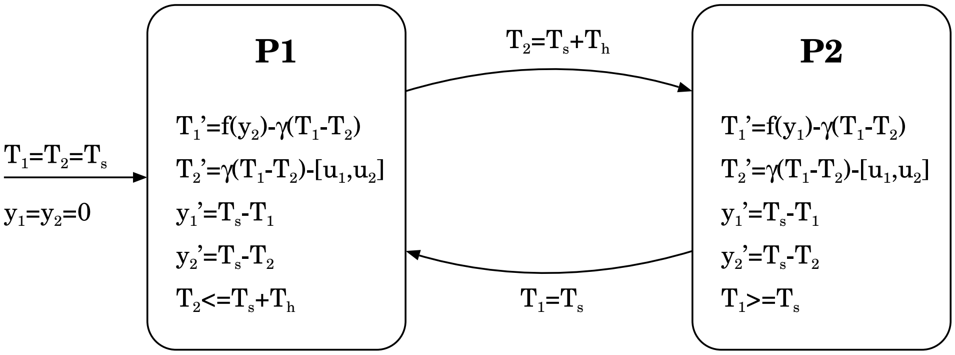

Figure 4: Hybrid Automata obtained from the FPN of Figure 3

represent the heating up of the primary circuit.

3.2 From FPN to Hybrid Automata

Using the technique proposed in [8], and some of the ideas presented in [7], the FPN of Figure 3 can be translated in the hybrid automaton [4] of Figure 4. An automatic conversion algorithm could be easily envisaged.

The hybrid automaton has the following set of real variables T_1, T_2, y_1 and y_2 (corresponding to the fluid variables of the FPN) and two control modes $P1$ and $P2$ (corresponding to the two discrete markings of the FPN). Each continuous variable has a derivative equal to the flow rate of the corresponding fluid place in that state. Transitions from control mode $P1$ to $P2$ and from $P2$ to $P1$ are labeled with the guards of the immediate transitions that cause the state change. State $P1$ has also associated the invariant condition $T_2 \leq T_s + T_h$ and $P2$ the invariant condition $T_1 \geq T_s$ to reflect the bounds posed on those fluid places. The model of Figure 4 could be analyzed by means of appropriate tools for hybrid automata [13].

4 Analysis of the FPN model via NuSMV

In order to show the generality of our approach and to enlarge the class of models that can be automatically derived from the FPN description, we sketch, in brief, how the FPN can be converted into a discrete model based on a finite state machine and whose specifications are defined using a Computational Tree Logic (CTL). For this purpose, we have chosen the language NuSMV, for which an analysis tool is available [11]. The NuSMV language allows the user to include uncertainty ranges for the parameter with non-deterministic logic. The complete specification of the present case study in the NuSMV language is in [14].

As the first step of the automatic translation, all the continuous variables (fluid levels of the FPN) and their range of variation must be discretized. Let x be the fluid variable in FPN whose fluid place is lower bounded by B_l and upper bounded by B_u. We define a discretization step δ such that the continuous range of variation of x is discretized in n steps. With this assumption, the possible discretized values of the level x are defined in NuSMV as:

```
x: 0..n;
```

where $n = \lceil (B_u - B_l)/\delta \rceil$ ($\lceil \cdot \rceil$ denotes the closest larger integer of its argument). Then, the assignment $x = i$ in NuSMV means that the actual fluid level of this place is $B_l + i\delta$.

In the FPN of Figure 3, four fluid variables are defined: y_1, y_2 and T_1, T_2. The fluid levels y_1 and y_2, of fluid places $CTR1$ and $CTR2$, respectively, are normalized in the range $[0, 1]$; the normalization constant for y_1 and y_2 is denoted by dy and represents how fast the system reacts to the temperature difference with respect to the setpoint temperature (output from block PI). In NuSMV, the variables describing the level of $CTR1$ and $CTR2$ are denoted by $y1$ and $y2$, respectively, and are discretized with a step interval 1/30. The assignment $y1 = i$ $(0 \leq i \leq 30)$ implies that the actual level of $CTR1$ is $i/30$.

The fluid levels T_1 and T_2 of fluid places *Primary* and *Secondary*, respectively, are bounded between $T_\ell = 138$ and $T_u = 145$ (with a range of variation $T_u - T_\ell = 7$) and the discretization step chosen for these variables is 0.1. In NuSMV, the variable describing the level of *Primary* (*Secondary*) is denoted by $T1$ ($T2$); $T1 = i,\ 0 \leq i \leq 70$ implies that the actual value of the primary temperature is $138 + i * 0.1$. Furthermore, we introduce a discrete variable *marking*, whose value can be either 1 or 2, to reflect the two possible positions of the switch. All the above definitions, are grouped in NuSMV under the keyword `VAR` (see the NuSMV description below).

The second step in the translation requires that the FPN constants that are used in the fluid rate functions or in the enabling conditions of the transitions are rescaled according to the chosen discretization steps and the bounds of the fluid levels. As a simple example, let us assume that a fluid level has B_l as lower bound, B_u as upper bound and δ as discretization step. An additive or comparative constant K in a rate of a transition connected to this place, in the discretized version becomes: $\mathsf{round}((K - B_l)/\delta)$ where the functions $\mathsf{round}(\cdot)$ denotes the closest integer to its argument. Note that proper rescaling of a constant is not always easy and has to be done with care, however, can be done automatically in a wide range of cases. These constants are listed under the keyword `DEFINE` (see the NuSMV description below). In the present case, the constants are the following:

- *alphamin, alphamax,*: non-deterministic range of the heat induced by the fresh methane gas (see Figure 2): rescaled values *alphamin=15*, *alphamax=30.*
- *betamin, betamax*: non-deterministic range of the heat induced by the exhaust gas (see Figure 2): rescaled values *betamin=6*, *betamax=9.*
- *sp* gives the constant setpoint temperature value $T_s = 141\ ^oC$ that is used as the setpoint for the proportional integrator and that controls the firing of transition $Sw21$; the rescaled value of this setpoint temperature is 30.
- *hys* gives the hysteresis temperature value $T_h = 2$ such that $T_s + T_h = 143\ ^oC$ controls the firing of transition $Sw12$; the rescaled value of the hysteresis temperature is 20.
- *ys* gives the value for the split point Y_s; since the fluid levels $y1$ and $y2$ are scaled between [0..30], the rescaled value for the split point is assumed equal to 15.
- *dy* is a normalization constant for the variables $y1$ and $y2$, and defines how fast the system reacts when the temperatures are not equals with the value of the setpoint; its rescaled value is 10.
- In order to define easily the possible changes of the fluid levels, the constants $y1max, y2max, T1max, T2max$, that give the maximal possible value for the variables that describe fluid levels, are defined as well. As already discussed, the rescaled value are: $y1max = y2max = 30$, $T1max = T2max = 70$.
- *gamma* describes the degree of heat exchange between the primary and secondary circuit; indeed, the heat exchange is proportional, through *gamma* to the temperature difference $T_1 - T_2$; its rescaled value is 2.

- further non-determinism is introduced by the heat consumption which is determined by a minimal and a maximal value, $u1 = 1$ and $u2 = 3$.

The second part under the keyword `DEFINE` gives the possible fluid changes in the different states of the model. Both minimal and maximal fluid changes have to be calculated, this is done by summing ingoing and outgoing fluid rates and considering minimal and maximal values of the appearing variables. These are the following:

- $m1\_y1$ gives the (deterministic) fluid rate of place $CTR1$ in state 1;
- $m1\_y2$ gives the (deterministic) fluid rate of place $CTR2$ in state 1;
- $m1\_T1\_min$ and $m1\_T1\_max$ give the minimal and maximal flow rate of fluid place $Primary$ in state 1;
- $m1\_T2\_min$ and $m1\_T2\_max$ give the minimal and maximal flow rate of fluid place $Secondary$ in state 1;
- $m2\_y1$, $m2\_y2$, $m2\_T1\_min$, $m2\_T1\_max$, $m2\_T2\_min$ and $m2\_T2\_max$ give the above quantities in state 2.

The initial state of the model is described under the keyword `INIT`. The temperatures T_1 and T_2 are set to 140 ^oC; this specification is translated into the rescaled variables ($T1 = 20$ & $T2 = 20$). The initial variables controlling the heating are set to $y1 = 0$ and $y2 = 0$.

In order to analyze the behavior of the control system versus time, we assume a time step (in arbitrary unit) and describe the dynamic evolution of the system at the integer multiples of the time step. Non-determinism is expressed by using properly the minimal and maximal flow rates. The evolution of the model is stated under the keyword `TRANS` and must be described marking by marking. Since in the present model we have two markings (states), the evolution description is restricted to four expressions:

- possible changes of the variables inside state 1;
- possible changes of the variables inside state 2;
- jump from state 1 to state 2 (when the secondary temperature reaches 143 ^oC);
- jump from state 2 to state 1 (when the primary temperature reaches 140 ^oC).

4.1 The complete NuSMV specifications

In the following we show an example of translation of the FPN into NuSMV.

```
MODULE main


VAR
     y1: 0..30;
     y2: 0..30;
     T1: 0..70;
     T2: 0..70;
     marking: 1..2;
```

Variables to describe possible levels of fluid places and discrete marking of the model.

```
DEFINE
     alphamin=15;
     alphamax=30;
     betamin=6;
     betamax=9;
     sp:=30;
     hys:=20;
     ys:=15;
     dy:=10;
     y1max:=30;
     y2max:=30;
     T1max:=70;
     T2max:=70;
     gamma:=2;
     u1:=1;
     u2:=3;
```

Rescaled constants of fluid rate functions and enabling conditions.

```
  -- rate of fluid flows in marking_1

     m1_y1:=(sp - T2)/dy;
     m1_y2:=(sp - T1)/dy;
```

Deterministic fluid rate of place $CTR1$ and $CTR2$ in state 1.

```
     m1_T1_min:= case
       y1<=ys : 2*y1/alphamax - (T1 - T2)/gamma;
       1 : y1max/alphamax+2*(y1 - ys)/betamax -
           (T1 - T2)/gamma;
     esac;
     m1_T1_max:= case
       y1<=ys : 2*y1/alphamin - (T1 - T2)/gamma;
       1 : y1max/alphamin+2*(y1 - ys)/betamin -
           (T1 - T2)/gamma;
     esac;
```

Minimal and maximal fluid rate of place *Primary* in state 1.

```
      m1_T2_min:=(T1 - T2)/gamma - u1;
      m1_T2_max:=(T1 - T2)/gamma - u2;
```

Minimal and maximal fluid rate of place *Secondary* in state 1.

```
   -- rate of fluid flows in marking_2

      m2_y1:=(sp - T2)/dy;
      m2_y2:=(sp - T1)/dy;
```

Deterministic fluid rate of place $CTR1$ and $CTR2$ in state 2.

```
      m2_T1_min:= case
        y2<=ys : 2*y2/alphamax - (T1 - T2)/gamma;
        1 : y2max/alphamax+2*(y2 - ys)/betamax -
            (T1 - T2)/gamma;
      esac;
      m2_T1_max:= case
        y2<=ys : 2*y2/alphamin - (T1 - T2)/gamma;
        1 : y2max/alphamin+2*(y2 - ys)/betamin -
            (T1 - T2)/gamma;
      esac;
```

Minimal and maximal fluid rate of place *Primary* in state 2.

```
      m2_T2_min:=(T1 - T2)/gamma - u2;
      m2_T2_max:=(T1 - T2)/gamma - u1;
```

Minimal and maximal fluid rate of place *Secondary* in state 2.

```
INIT

      marking=1 & y1=0 & y2=0 & T1=20 & T2=20
```

Initial situation

```
TRANS
```

```
(
marking=1 & T2<sp+hys &
next(marking)=1 &
( (y1+m1_y1<0 & next(y1)=0) |
  (y1+m1_y1>y1max & next(y1)=y1max) |
  (y1+m1_y1>=0 & y1+m1_y1<=y1max &
   next(y1)=y1+m1_y1) ) &
( (y2+m1_y2<0 & next(y2)=0) |
  (y2+m1_y2>y2max & next(y2)=y2max) |
  (y2+m1_y2>=0 & y2+m1_y2<=y2max &
   next(y2)=y2+m1_y2) ) &
( (T1+m1_T1_max<0 & next(T1)=0) |
  (T1+m1_T1_min>T1max & next(T1)=T1max) |
  (T1+m1_T1_max>=0 & T1+m1_T1_min<=T1max &
   next(T1)>=T1+m1_T1_min &
   next(T1)<=T1+m1_T1_max) ) &
( (T2+m1_T2_max<0 & next(T2)=0) |
  (T2+m1_T2_min>T2max & next(T2)=T2max) |
  (T2+m1_T2_max>=0 & T2+m1_T2_min<=T2max &
   next(T2)>=T2+m1_T2_min &
   next(T2)<=T2+m1_T2_max) )
) |
```

Possible change of the variables in one step inside marking 1 described using the rates defined above.

```
(
marking=2 & T1>sp &
next(marking)=2 &
( (y1+m2_y1<0 & next(y1)=0) |
  (y1+m2_y1>y1max & next(y1)=y1max) |
  (y1+m2_y1>=0 & y1+m2_y1<=y1max &
   next(y1)=y1+m2_y1) ) &
( (y2+m2_y2<0 & next(y2)=0) |
  (y2+m2_y2>y2max & next(y2)=y2max) |
  (y2+m2_y2>=0 & y2+m2_y2<=y2max &
   next(y2)=y2+m2_y2) ) &
( (T1+m2_T1_max<0 & next(T1)=0) |
  (T1+m2_T1_min>T1max & next(T1)=T1max) |
  (T1+m2_T1_max>=0 & T1+m2_T1_min<=T1max &
   next(T1)>=T1+m2_T1_min &
   next(T1)<=T1+m2_T1_max) ) &
( (T2+m2_T2_max<0 & next(T2)=0) |
  (T2+m2_T2_min>T2max & next(T2)=T2max) |
  (T2+m2_T2_max>=0 & T2+m2_T2_min<=T2max &
   next(T2)>=T2+m2_T2_min &
   next(T2)<=T2+m2_T2_max) )
) |
```

Possible change of the variables in one step inside marking 2 described using the rates defined above.

```
(
marking=1 & T2>=sp+hys &
next(marking)=2 &
( (y1+m1_y1<0 & next(y1)=0) |
  (y1+m1_y1>y1max & next(y1)=y1max) |
  (y1+m1_y1>=0 & y1+m1_y1<=y1max &
   next(y1)=y1+m1_y1) ) &
( (y2+m1_y2<0 & next(y2)=0) |
  (y2+m1_y2>y2max & next(y2)=y2max) |
  (y2+m1_y2>=0 & y2+m1_y2<=y2max &
   next(y2)=y2+m1_y2) ) &
( (T1+m1_T1_max<0 & next(T1)=0) |
  (T1+m1_T1_min>T1max & next(T1)=T1max) |
  (T1+m1_T1_max>=0 & T1+m1_T1_min<=T1max &
   next(T1)>=T1+m1_T1_min &
   next(T1)<=T1+m1_T1_max) ) &
( (T2+m1_T2_max<0 & next(T2)=0) |
  (T2+m1_T2_min>T2max & next(T2)=T2max) |
  (T2+m1_T2_max>=0 & T2+m1_T2_min<=T2max &
   next(T2)>=T2+m1_T2_min &
   next(T2)<=T2+m1_T2_max) )
) |
```

Possible change of the variables in one step jumping from state 1 to state 2 described using the rates defined above.

```
(
-- statechanges from marking_2 to marking_1
marking=2 & T1<=sp &
next(marking)=1 &
( (y1+m2_y1<0 & next(y1)=0) |
  (y1+m2_y1>y1max & next(y1)=y1max) |
  (y1+m2_y1>=0 & y1+m2_y1<=y1max &
   next(y1)=y1+m2_y1) ) &
( (y2+m2_y2<0 & next(y2)=0) |
  (y2+m2_y2>y2max & next(y2)=y2max) |
  (y2+m2_y2>=0 & y2+m2_y2<=y2max &
   next(y2)=y2+m2_y2) ) &
( (T1+m2_T1_max<0 & next(T1)=0) |
  (T1+m2_T1_min>T1max & next(T1)=T1max) |
  (T1+m2_T1_max>=0 & T1+m2_T1_min<=T1max &
   next(T1)>=T1+m2_T1_min &
   next(T1)<=T1+m2_T1_max) ) &
( (T2+m2_T2_max<0 & next(T2)=0) |
  (T2+m2_T2_min>T2max & next(T2)=T2max) |
  (T2+m2_T2_max>=0 & T2+m2_T2_min<=T2max &
   next(T2)>=T2+m2_T2_min &
   next(T2)<=T2+m2_T2_max) )
)
```

Possible change of the variables in one step jumping from state 2 to state 1 described using the rates defined above.

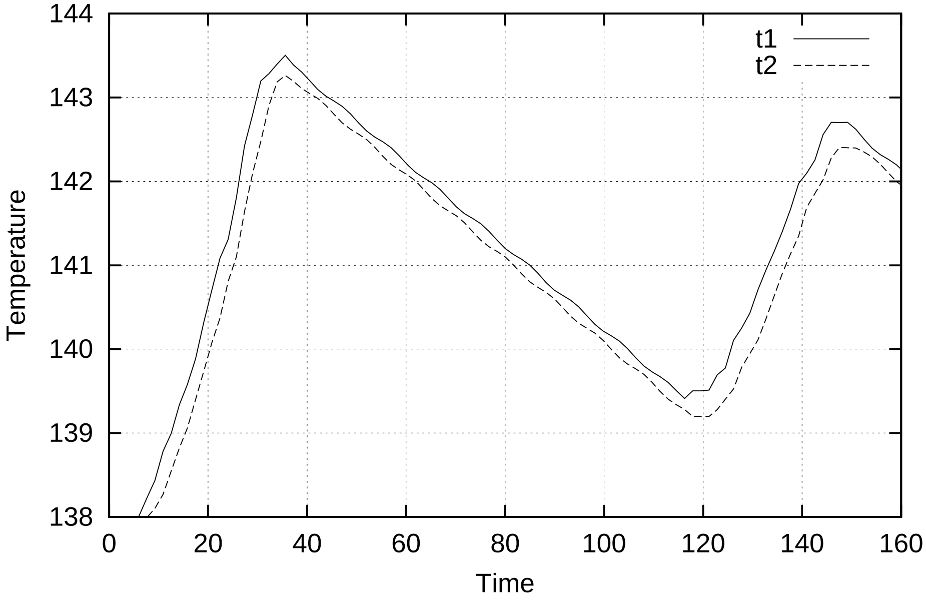

Figure 5: Change of temperature given by a simulation trace

4.2 NuSMV results

NuSMV is a model checking tool and, in order to explore the dynamics of the system, it contains also a simulation engine which gives the possibility of creating traces in random, interactive or even constrained manner. Figure 5 depicts the evolution of the temperatures of the system for a given simulation trace.

Figure 6 displays the value of y_1 and y_2 as the function of time for the same trace. Figure 7 depicts the state of the model for the same run. The initial state of the trace was $y1 = 0, y2 = 0, T1 = 0, T2 = 0$, i.e. we have started the system with both temperatures equal to lower bound of the possible range ($= 138\,^oC$).

The real specification for the temperatures of the system (given as an invariant condition) are: ($139 \leq T_1 \leq 144$ and $139 \leq T_2 \leq 141$) that translated in the rescaled NuSMV variables becomes:

```
T1>=10 & T1<=60 & T2>=10 & T2<=30.
```

If the invariant does not hold, i.e. the temperatures can be out of the required intervals, NuSMV produces a counterexamples. This is the case when $gamma = 2$, $dy = 10$ and $sp = 20$ ($T_s = 140$) and starting from $y1 = 0, y2 = 0, T1 = 30, T2 = 30$ ($T_1 = T_2 = 141$); the counterexample is shown in Table 1. The table reflects the real value of the quantities instead of the value with which they are encoded in NuSMV. Both temperatures start

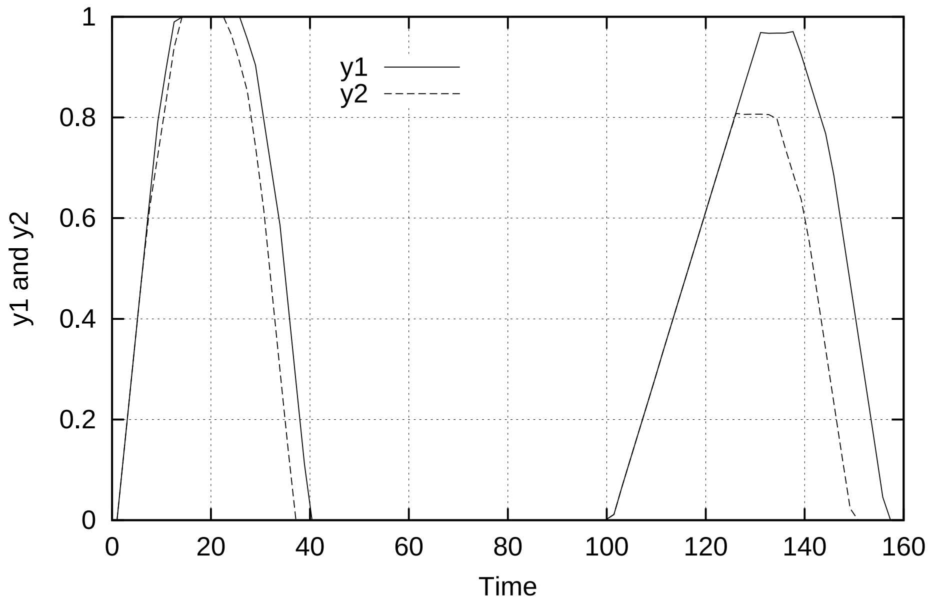

Figure 6: Change of y_1 and y_2 given by a simulation trace

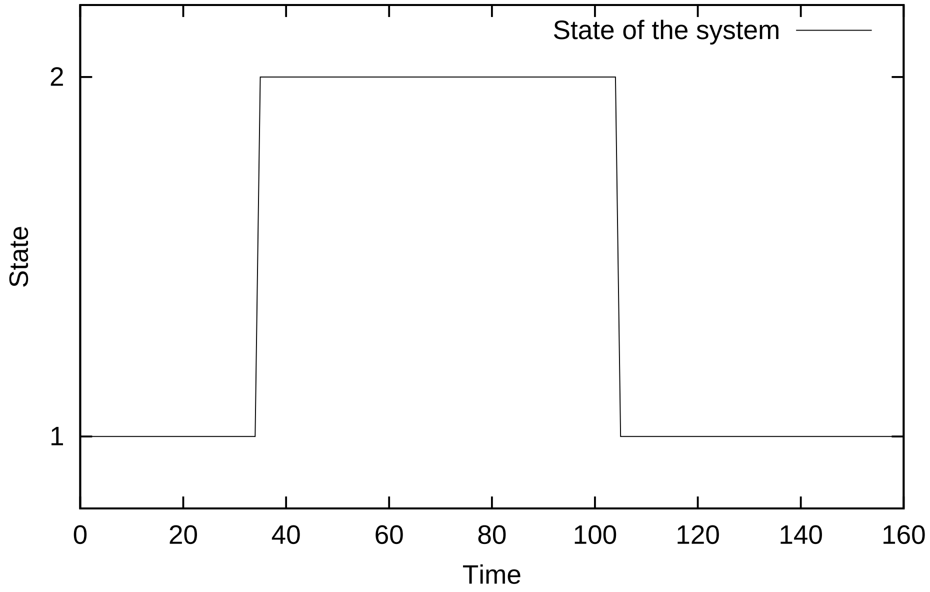

Figure 7: Change of state given by a simulation trace

Step	1	2	3	4	5	6	7	8	9	10	11	12	13	14
State	1	1	1	1	1	1	1	1	1	1	1	1	1	1
T1	141	141	140.9	140.7	140.6	140.4	140.3	140.1	140	139.8	139.7	139.5	139.4	139.2
T2	141	140.7	140.5	140.4	140.2	140.1	139.9	139.8	139.6	139.5	139.3	139.2	139	138.9
y1	0	0	0	0	0	0	0	1/30	2/30	3/30	4/30	5/30	6/30	8/30
y2	0	0	0	0	0	0	0	0	0	1/30	2/30	3/30	4/30	5/30

Table 1: Counterexample

initially from 141 and decrease because of the heat consumption of the user. As T_2 (T_1) reaches T_s, y_1 (y_2) starts to increase. However, the reaction is not fast enough to avoid the undesirable condition on the secondary temperature.

It can be verified that the same requirements could be fulfilled by setting $gamma = 2$, $dy = 1/10$ and $sp = 18$ (i.e. speeding up the reaction of the system, and changing the setpoint to $T_s = 139.8$).

Using not only invariant conditions but RTCTL (Real-Time Computational Tree Logic [15]) expression one can check the trajectory on which the system proceeds. For example, starting from the lowest possible temperatures ($T_1 = 138$ and $T_2 = 138$) the formula

```
AF (AG (T1>=10 & T1<=60 & T2>=10 & T2<=30))
```

is true if the system gets back to stable state for sure and remains there forever. Setting $gamma = 2$, $dy = 1/10$ and $sp = 18$ the formula evaluates to true. The same formula, with the same settings evaluates to true as well, if the system is started from the upper bound of the temperatures.

Knowing the timing behavior of the system, one can use NuSMV to compute the minimal or maximal time needed to get to a given set of states from an initial situation. For example, the command

```
COMPUTE MIN[y1=0 & y2=0 & T1=70 & T2=70, AG (T1>=10 & T1<=60 &
T2>=10 & T2<=30)]

COMPUTE MAX[y1=0 & y2=0 & T1=70 & T2=70, AG (T1>=10 & T1<=60 &
T2>=10 & T2<=30)]
```

gives the length of the minimal and maximal paths that lead from high temperatures (out of the required range) to temperatures inside the required range in such a way that the system does not leave this range in the future. The above command with parameters $gamma = 2$, $dy = 1/10$ and $sp = 18$ results in $min - path = 21$ and $Max - path = 64$.

5 Conclusion

Using a real world hybrid system as a case study we presented an approach to integrate FPNs and model checking via hybrid automata and NuSMV.

Such integration turns out to be conceptually useful and effective in practice. In fact it allowed us to comfortably model and verify the temperature control system in the co-generative plant ICARO at ENEA (CR).

Acknowledgments - M. Gribaudo and A. Bobbio were partially supported by the Italian Ministry of Education under Grant MIUR-COFIN2001-ISIDE.

References

[1] H. Alla and R. David. Continuous and hybrid Petri nets. *Journal of Systems Circuits and Computers*, 8(1):159–188, Feb 1998.

[2] G. Horton, V. Kulkarni, D. Nicol, and K. Trivedi. Fluid stochastic Petri nets: Theory, application and solution techniques. *European Journal of Operational Research*, 105(1):184–201, 1998.

[3] M. Gribaudo, M. Sereno, A. Horváth, and A. Bobbio. Fluid stochastic Petri nets augmented with flush-out arcs: Modelling and analysis. *Discrete Event Dynamic Systems*, 11 (1/2):97–117, January 2001.

[4] R. Alur, T.A. Henzinger, and P.H. Ho. Automatic symbolic verification of embedded systems. *IEEE Transaction Software Engineering*, 22:181–201, 1996.

[5] E. M. Clarke, E. A. Emerson, and A. P. Sistla. Automatic verification of finite state concurrent systems using temporal logic specifications: A practical approach. *ACM Transactions on Programming Languages and Systems*, 8(2):244–263, 1986.

[6] M. Gribaudo. Hybrid formalism for performance evaluation: Theory and applications. Technical report, Phd Thesis, Dipartimento di Informatica, Università di Torino, 2001.

[7] M. Allam. Sur l'analyse quantitative des réseaux de Petri hybrides: une approche baseée sur lea automates hybrides. Technical report, Phd Thesis, Institut National Polytechnique de Grenoble (in French), 1998.

[8] B. Tuffin, D.S. Chen, and K. Trivedi. Comparison of hybrid systems and fluid stochastic Petri nets. *Discrete Event Dynamic Systems*, 11 (1/2):77–95, January 2001.

[9] A. Bobbio and A. Horváth. Petri nets with discrete phase timing: A bridge between stochastic and functional analysis. In *Second International Workshop on Models for Time-Critical Systems (MTCS 2001)*, pages 22–38, 2001.

[10] A. Bobbio, S. Bologna, E. Ciancamerla, P. Incalcaterra, C. Kropp, M. Minichino, and E. Tronci. Advanced techniques for safety analysis applied to the gas turbine control system of ICARO co-generative plant. In *X Convegno Tecnologie e Sistemi Energetici Complessi*, pages 339–350, 2001.

[11] *NuSMV*. `http://nusmv.irst.itc.it/index.html`.

[12] T. Murata. Petri nets: properties, analysis and applications. *Proceedings of the IEEE*, 77:541–580, 1989.

[13] T.A. Henzinger, P.H. Ho, and H. Wong-Toi. A user guide to HyTech. In *Proceedings 1st Workshop Tools and Algorithms for the Construction and Analysis of Systems - TACAS*, pages 41–71. Springer Verlag, LNCS Vol 1019 - http:// www.eecs.berkeley.edu/ tah/HyTech, 1995.

[14] A. Horváth, M. Gribaudo, and A. Bobbio. From FPN to NuSMV: The temperature control system of the ICARO cogenerative plant. Technical report, Università del Piemonte Orientale, Feb 2002.

[15] E.A. Emerson, A.K. Mok, A.P. Sistla, and J. Srinivasan. Quantitative Temporal Reasoning. *Journal of Real Time Systems*, 4:331–352, 1992.