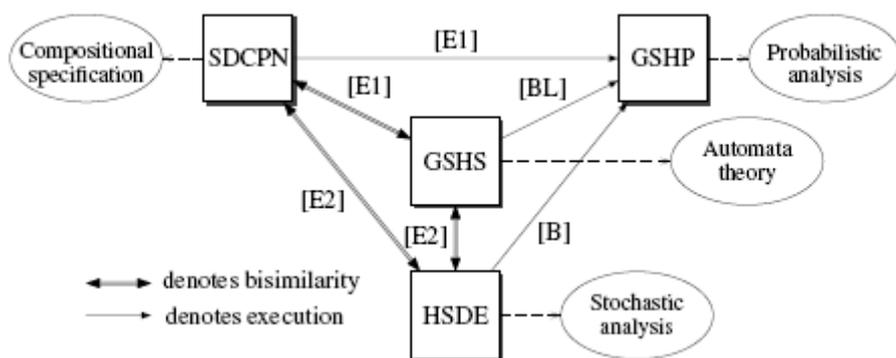


## Executive summary

# BISIMULATION RELATIONS BETWEEN AUTOMATA, STOCHASTIC DIFFERENTIAL EQUATIONS AND PETRI NETS



**Report no.**  
NLR-TP-2010-325

**Author(s)**  
M.H.C. Everdij  
H.A.P. Blom

**Report classification**  
UNCLASSIFIED

**Date**  
April 2010

**Knowledge area(s)**  
Vliegveiligheid (safety & security)

**Descriptor(s)**  
Petri nets  
Hybrid automata  
Bisimulation  
Compositional modelling  
Air transport safety

### Objective

The aim of this paper is to explain bisimilarity relations between SDCPN (stochastically and dynamically coloured Petri net), GSHS (general stochastic hybrid system) and HSDE (hybrid stochastic differential equation), which means that the strengths of one stochastic model formalism can be used by both of the other stochastic model formalisms. More specifically, these bisimilarity relations make it possible to combine the formal verification power of automata with the analysis power of stochastic differential equations and the compositional specification power of Petri nets.

### Description of work

We start by defining SDCPN and the resulting SDCPN stochastic

process, which is referred to as a GSHP (general stochastic hybrid process). Next, we present a simple but illustrative SDCPN example model. Subsequently, we use this example model to study GSHP as an execution of a GSHS and to show that SDCPN and GSHS are bisimilar. Next, we study GSHP as a stochastic process solution of HSDE and show with the illustrative example that SDCPN and HSDE are bisimilar.

### Results and conclusions

The bisimilarities between SDCPN, GSHS and HSDE models for the example considered mean that the resulting example model inherits the strengths of all three formal stochastic modelling formalisms. Examples of GSHP properties are

This report is based on a paper published in Volume 20 of Electronic Proceedings in Theoretical Computer Science (EPTCS), 2010, pp. 1-15, M. Bujorianu and M. Fisher (editors), doi: 10.4204/EPTCS.20.1.

convergence in discretisation, existence of limits, existence of event probabilities, strong Markov properties, reachability analysis. Examples of GSHS features are their connection to formal methods in automata theory and optimal control theory. Examples of HSDE features are stochastic analysis tools for semi-martingales. Examples of SDCPN features are natural expression of causal dependencies, concurrency and synchronisation mechanism, hierarchical and modular construction, and graphical representation. These complementary advantages of SDCPN, GSHS, HSDE and GSHP perspectives tend to increase with the complexity of the system considered.

#### **Applicability**

An illustrative large scale application of bisimilarity relations between SDCPN, HSDE and stochastic hybrid automata has been developed in air traffic management. Currently, pilots depend of air traffic controllers in solving potential conflicts between their flight trajectories. This places a huge requirement on the tasks of an air traffic controller. The number of aircraft that one air traffic controller can handle ranges between 10 and 20, depending of the complexity of the traffic pattern. It had been suggested by RTCA (1995) that this limitation of the air traffic

controller can be solved by moving the responsibility of conflict resolution from the air traffic controller to the pilots. Since then this airborne self separation idea has received a lot of research attention. Nevertheless, it still is unknown how much more air traffic can safely be accommodated under a well designed airborne self separation way of working. In order to add to the solution of this debate, a series of large European studies towards solving this question have been started under the name HYBRIDGE and iFly, respectively. The way of working is to first develop a well defined SDCPN model of the airborne self separation concept of operation to be analysed. Subsequently this SDCPN model is further analysed by using a bisimilar HSDE and hybrid automation formal model representation, in which powerful stochastic analysis theory is exploited for the speeding up of Monte Carlo simulations. Using this approach, Blom, Klein Obbink and Bakker (2009) have shown that the first generation of airborne self separation concept designs falls short in safely accommodating higher air traffic demand than conventional ATM can. The feedback of this finding to advanced air traffic concept designers triggered the development of more advanced airborne self separation concept of operation.

NLR-TP-2010-325

## BISIMULATION RELATIONS BETWEEN AUTOMATA, STOCHASTIC DIFFERENTIAL EQUATIONS AND PETRI NETS

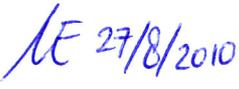
M.H.C. Everdij  
H.A.P. Blom

*This report is based on a paper published in Volume 20 of Electronic Proceedings in Theoretical Computer Science (EPTCS), 2010, pp. 1-15, M. Bujorianu and M. Fisher (editors), doi: 10.4204/EPTCS.20.1.*

*The contents of this report may be cited on condition that full credit is given to NLR and the authors.*

**Customer** National Aerospace Laboratory NLR  
**Division** Air Transport  
**Owner** NLR  
**Distribution** Unlimited  
**Classification of title** Unclassified  
April 2010

Approved by:

Author  27/8/2010	Reviewer Anonymous peer reviewers	Managing department  2/9/10
---	--------------------------------------	--

# CONTENTS

1	INTRODUCTION	5
2	SDCPN	7
2.1	SDCPN elements	7
2.2	SDCPN execution	8
2.3	SDCPN stochastic process	9
3	AIR TRAFFIC EXAMPLE AND ITS SDCPN MODEL	10
4	FROM SDCPN TO GSHS	11
4.1	GSHS definition	12
4.2	A bisimilar GSHS for the example SDCPN	13
5	FROM SDCPN TO HSDE	14
5.1	HSDE definition	14
5.2	A bisimilar HSDE for the example SDCPN	16
6	CONCLUSIONS	17
7	REFERENCES	18

# Bisimulation Relations Between Automata, Stochastic Differential Equations and Petri Nets

Mariken H.C. Everdij

Henk A.P. Blom

National Aerospace Laboratory NLR  
Amsterdam, Netherlands

everdij@nlr.nl

blom@nlr.nl

Two formal stochastic models are said to be bisimilar if their solutions as a stochastic process are probabilistically equivalent. Bisimilarity between two stochastic model formalisms means that the strengths of one stochastic model formalism can be used by the other stochastic model formalism. The aim of this paper is to explain bisimilarity relations between stochastic hybrid automata, stochastic differential equations on hybrid space and stochastic hybrid Petri nets. These bisimilarity relations make it possible to combine the formal verification power of automata with the analysis power of stochastic differential equations and the compositional specification power of Petri nets. The relations and their combined strengths are illustrated for an air traffic example.

## 1 Introduction

Two formal stochastic models are said to be *bisimilar* if their solutions as a stochastic process (i.e. their *executions*) are probabilistically equivalent [8, 23]. Bisimilarity relations between formal stochastic models are very useful to study since they allow one stochastic model to take advantage of the strengths of the other stochastic model. The aim of this paper is to show bisimulation relations between three different stochastic modelling formalisms: stochastic hybrid automata, stochastic differential equations on hybrid space, and stochastic hybrid Petri nets. These bisimulation relations make it possible to combine the formal verification power of automata with the analysis power of stochastic differential equations and the compositional specification power of Petri nets.

For the stochastic automata formalism, we take the *general stochastic hybrid system* (GSHS) theoretical setting developed by [7]. A GSHS is a hybrid automaton defined on a hybrid state space. This hybrid state space consists of a countable set of discrete modes, and per discrete mode a Euclidean subset. Per discrete mode, a stochastic differential equation (SDE) is defined. Two additional GSHS elements are a jump rate function and a GSHS transition measure. The execution of these elements provides a stochastic process that follows the solution of the SDE connected to the initial discrete mode. After a time period, defined by the jump rate function, the process state may spontaneously jump to another mode, defined by the GSHS transition measure. A jump may also be forced if the process state hits the boundary of the Euclidean subset. The GSHS execution is referred to as *general stochastic hybrid process* (GSHP). One of the main strengths of the automata formalism is the availability of formal verification tools.

For the hybrid stochastic differential equations formalism we take the *hybrid stochastic differential equations* (HSDE) theoretical setting developed in a series of complementary studies [1, 2, 20, 21]. A HSDE consists of a sequence of SDEs on a hybrid state space, driven by a Poisson random measure. When the Poisson random measure generates a multivariate point, a spontaneous jump occurs. A jump may also be forced if the process state hits the boundary of a Euclidean subset. The HSDE solution process is referred to as *general stochastic hybrid process* (GSHP). In [16] it is shown that whereas the GSHS formalism is at some points more general than HSDE (for GSHS the dimension of the Euclidean

subset may depend on the discrete mode; for HSDE this dimension is fixed), HSDE has the advantage of an established semi-martingale property and includes the coverage of jump-linear systems.

For the stochastic hybrid Petri nets formalism, we take *stochastically and dynamically coloured Petri nets* (SDCPN) developed in a series of studies by [13, 14, 15]. A Petri net has *places* (circles), which model possible discrete states or conditions, and which may contain one or more *tokens* (dots), modelling which of these states are current. The places are connected by *transitions* (squares), which model state switches by removing input tokens and producing output tokens along *arcs* (arrows). In SDCPN, the tokens have Euclidean-valued colours that follow SDEs. Some of the transitions remove and produce tokens spontaneously, other transitions are forced and occur when the colours of their input tokens reach the boundary of a Euclidean subset. The collection of token colours in all places forms a *general stochastic hybrid process* (GSHP). The specific strength of SDCPN is their compositional specification power, which makes available a hierarchical modelling approach that separates local modelling issues from global modelling issues. This is illustrated for a large distributed example in air traffic management [17], which covers many distributed agents each of which interacts in a dynamic way with the others. Other typical Petri net features are concurrency and synchronisation mechanism, hierarchical and modular construction, and natural expression of causal dependencies, in combination with graphical and equational representation.

The aim of this paper is to illustrate the relations between SDCPN, GSHP, HSDE and GSHS which show that SDCPN, GSHS and HSDE are bisimilar. This means that if we take the elements of any one of these formalisms, we can construct the elements of another formalism in such a way that their associated GSHPs are probabilistically equivalent. Fig. 1 shows the relations between the formalisms, and the key tools available for each of them.

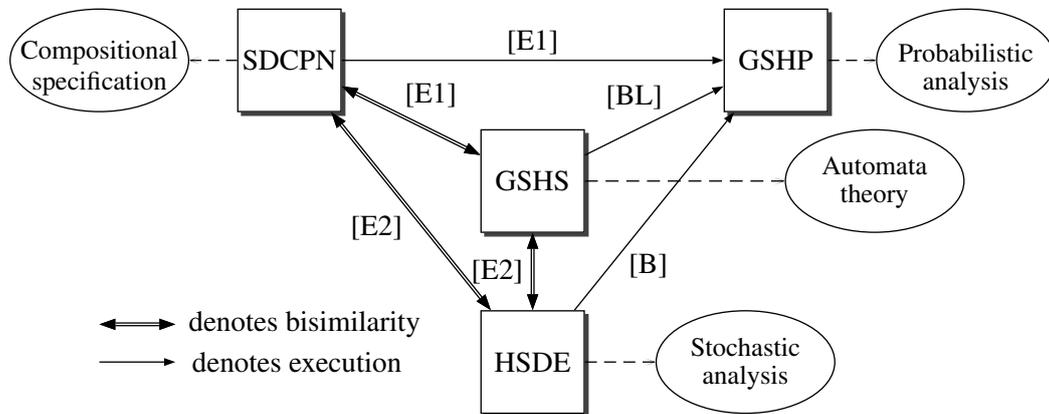


Figure 1: Relationship between SDCPN, GSHS, GSHP and HSDE, and their key properties and advantages. The [B] arrow is established in [1]. The [BL] arrow is established in [7]. The [E1] arrows are established in [15]. The [E2] arrows are established in [16].

With these relations, the properties and advantages of the various approaches come within reach of each other. The compositional specification power of SDCPN makes it relatively easy to develop a model for a complex system with multiple interactions. Subsequently, in the analysis stage three alternative approaches can be taken. The first is direct execution of SDCPN and evaluation through e.g.

Monte Carlo simulation. The second is mapping the SDCPN into a GSHS and evaluating its execution, with the advantages of connection to formal methods in automata theory and to optimal control theory [6]. The third is mapping the SDCPN into HSDE and evaluating its solution, with the advantages of stochastic analysis for semi-martingales [10, 11]. With the GSHP resulting from any of these three means, properties become available such as convergence of discretisation, existence of limits, existence of event probabilities, strong Markov properties, and reachability analysis [7, 9, 12].

The organisation of this paper is as follows. Section 2 defines SDCPN and the related SDCPN process. Section 3 presents an example SDCPN model for a simple but illustrative air traffic situation. Section 4 defines GSHS and illustrates how the example SDCPN can be mapped to a bisimilar GSHS. Section 5 defines HSDE and illustrates how the example SDCPN can be mapped to a bisimilar HSDE. Section 6 gives conclusions.

## 2 SDCPN

This section outlines *stochastically and dynamically coloured Petri net* (SDCPN). For a more formal definition, we refer to [16].

**Definition 2.1** (Stochastically and dynamically coloured Petri net.) *An SDCPN is a collection of elements  $(\mathcal{P}, \mathcal{T}, \mathcal{A}, \mathcal{N}, \mathcal{S}, \mathcal{C}, \mathcal{I}, \mathcal{V}, \mathcal{W}, \mathcal{G}, \mathcal{D}, \mathcal{F})$ , together with an SDCPN execution prescription which makes use of a sequence  $\{U_i; i = 0, 1, \dots\}$  of independent uniform  $U[0, 1]$  random variables, of independent sequences of mutually independent standard Brownian motions  $\{B_t^{i,P}; i = 1, 2, \dots\}$  of appropriate dimensions, one sequence for each place  $P$ , and of five rules R0–R4 that solve enabling conflicts.*

### 2.1 SDCPN elements

The SDCPN elements  $(\mathcal{P}, \mathcal{T}, \mathcal{A}, \mathcal{N}, \mathcal{S}, \mathcal{C}, \mathcal{I}, \mathcal{V}, \mathcal{W}, \mathcal{G}, \mathcal{D}, \mathcal{F})$  are defined as follows:

- $\mathcal{P}$  is a finite set of places.
- $\mathcal{T}$  is a finite set of transitions which consists of 1) a set  $\mathcal{T}_G$  of guard transitions, 2) a set  $\mathcal{T}_D$  of delay transitions and 3) a set  $\mathcal{T}_I$  of immediate transitions.
- $\mathcal{A}$  is a finite set of arcs which consists of 1) a set  $\mathcal{A}_O$  of ordinary arcs, 2) a set  $\mathcal{A}_E$  of enabling arcs and 3) a set  $\mathcal{A}_I$  of inhibitor arcs.
- $\mathcal{N} : \mathcal{A} \rightarrow \mathcal{P} \times \mathcal{T} \cup \mathcal{T} \times \mathcal{P}$  is a node function which maps each arc  $A \in \mathcal{A}$  to a pair of ordered nodes  $\mathcal{N}(A)$ , where a node is a place or a transition.
- $\mathcal{S} \subset \{\mathbb{R}^0, \mathbb{R}^1, \mathbb{R}^2, \dots\}$  is a finite set of colour types, with  $\mathbb{R}^0 \triangleq \emptyset$ .
- $\mathcal{C} : \mathcal{P} \rightarrow \mathcal{S}$  is a colour type function which maps each place  $P \in \mathcal{P}$  to a specific colour type. Each token in  $P$  is to have a colour in  $\mathcal{C}(P)$ . If  $\mathcal{C}(P) = \mathbb{R}^0$  then a token in  $P$  has no colour.
- $\mathcal{I}$  is a probability measure, which defines the initial marking of the net: for each place it defines a number  $\geq 0$  of tokens initially in it and it defines their initial colours.
- $\mathcal{V} = \{\mathcal{V}_P; P \in \mathcal{P}, \mathcal{C}(P) \neq \mathbb{R}^0\}$  is a set of token colour functions. For each place  $P \in \mathcal{P}$  for which  $\mathcal{C}(P) \neq \mathbb{R}^0$ , it contains a function  $\mathcal{V}_P : \mathcal{C}(P) \rightarrow \mathcal{C}(P)$  that defines the drift coefficient of a differential equation for the colour of a token in place  $P$ .

4 Bisimulation Relations Between Automata, Stochastic Differential Equations and Petri Nets

- $\mathcal{W} = \{\mathcal{W}_P; P \in \mathcal{P}, \mathcal{C}(P) \neq \mathbb{R}^0\}$  is a set of token colour matrix functions. For each place  $P \in \mathcal{P}$  for which  $\mathcal{C}(P) \neq \mathbb{R}^0$ , it contains a measurable mapping  $\mathcal{W}_P : \mathcal{C}(P) \rightarrow \mathbb{R}^{n(P) \times h(P)}$  that defines the diffusion coefficient of a stochastic differential equation for the colour of a token in place  $P$ , where  $h : \mathcal{P} \rightarrow \mathbb{N}$  and  $n : \mathcal{P} \rightarrow \mathbb{N}$  is such that  $\mathcal{C}(P) = \mathbb{R}^{n(P)}$ . It is assumed that  $\mathcal{W}_P$  and  $\mathcal{V}_P$  satisfy conditions that ensure a probabilistically unique solution of each stochastic differential equation.
- $\mathcal{G} = \{\mathcal{G}_T; T \in \mathcal{T}_G\}$  is a set of transition guards. For each  $T \in \mathcal{T}_G$ , it contains a transition guard  $\mathcal{G}_T$ , which is an open Euclidean subset with boundary  $\partial\mathcal{G}_T$ .
- $\mathcal{D} = \{\mathcal{D}_T; T \in \mathcal{T}_D\}$  is a set of transition delay rates. For each  $T \in \mathcal{T}_D$ , it contains a locally integrable transition delay rate  $\mathcal{D}_T$ .
- $\mathcal{F} = \{\mathcal{F}_T; T \in \mathcal{T}\}$  is a set of firing measures. For each  $T \in \mathcal{T}$ , it contains a firing measure  $\mathcal{F}_T$ , which generates the number and colours of the tokens produced when transition  $T$  fires, given the value of the vector that collects all input tokens: For each output arc, zero or one token is produced. For each fixed  $H$ ,  $\mathcal{F}_T(H; \cdot)$  is measurable. For any  $c$ ,  $\mathcal{F}_T(\cdot; c)$  is a probability measure.

For the places, transitions and arcs, the graphical notation is as in Figure 2.

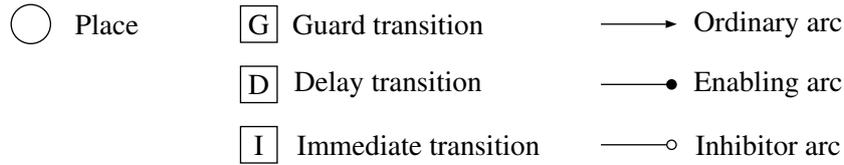


Figure 2: Graphical notation for places, transitions and arcs in an SDCPN

## 2.2 SDCPN execution

The execution of an SDCPN provides a series of increasing stopping times,  $\{\tau_i; i = 0, 1, \dots\}$ ,  $\tau_0 = 0$ , with for  $t \in (\tau_k, \tau_{k+1})$  a fixed number of tokens per place and per token a colour which is the solution of a stochastic differential equation.

**Initiation.** The probability measure  $\mathcal{I}$  characterises an initial marking at  $\tau_0$ , i.e. it gives each place  $P \in \mathcal{P}$  zero or more tokens and gives each token in  $P$  a colour in  $\mathcal{C}(P)$ , i.e. a Euclidean-valued vector.

**Token colour evolution.** For each token in each place  $P$  for which  $\mathcal{C}(P) \neq \mathbb{R}^0$ : if the colour of this token is equal to  $C_0^P$  at time  $t = \tau_0$ , and if this token is still in this place at time  $t > \tau_0$ , then the colour  $C_t^P$  of this token equals the probabilistically unique solution of the stochastic differential equation  $dC_t^P = \mathcal{V}_P(C_t^P)dt + \mathcal{W}_P(C_t^P)dB_t^{i,P}$  with initial condition  $C_{\tau_0}^P = C_0^P$ , and with  $\{B_t^{i,P}\}$  an  $h(P)$ -dimensional standard Brownian motion. Each token in a place for which  $\mathcal{C}(P) = \mathbb{R}^0$  remains without colour.

**Transition enabling.** A transition  $T$  is *pre-enabled* if it has at least one token per incoming ordinary and enabling arc in each of its input places and has no token in places to which it is connected by an inhibitor arc. For each transition  $T$  that is pre-enabled at  $\tau_0$ , consider one token per ordinary and enabling

arc in its input places and write  $C_t^T$ ,  $t \geq \tau_0$ , as the column vector containing the colours of these tokens;  $C_t^T$  evolves through time according to its corresponding token colour functions. If this vector is not unique (i.e., if one input place contains several tokens per arc), all possible such vectors are executed in parallel. A transition  $T$  is *enabled* if it is pre-enabled and a second requirement holds true. For  $T \in \mathcal{T}_I$ , the second requirement automatically holds true at the time of pre-enabling. For  $T \in \mathcal{T}_G$ , the second requirement holds true when  $C_t^T \in \partial \mathcal{G}_T$ . For  $T \in \mathcal{T}_D$ , the second requirement holds true at  $t = \tau_0 + \sigma_1^T$ , where  $\sigma_1^T$  is generated from a probability distribution function  $D_T(t - \tau_0) = 1 - \exp(-\int_{\tau_0}^t \mathcal{D}_T(C_s^T) ds)$ . A Uniform random variable  $U_i$  is used to determine this  $\sigma_1^T$ . In the case of competing enablings, the following rules apply:

- R0 The firing of an immediate transition has priority over the firing of a guard or a delay transition.
- R1 If one transition becomes enabled by two or more sets of input tokens at exactly the same time, and the firing of any one set will not disable one or more other sets, then it will fire these sets of tokens independently, at the same time.
- R2 If one transition becomes enabled by two or more sets of input tokens at exactly the same time, and the firing of any one set disables one or more other sets, then the set that is fired is selected randomly, with the same probability for each set.
- R3 If two or more transitions become enabled at exactly the same time and the firing of any one transition will not disable the other transitions, then they will fire at the same time.
- R4 If two or more transitions become enabled at exactly the same time and the firing of any one transition disables some other transitions, then each combination of transitions that can fire independently without leaving enabled transitions gets the same probability of firing.

**Transition firing.** If  $T$  is enabled, suppose this occurs at time  $\tau_1$  and in a particular vector of token colours  $C_{\tau_1}^T$ , it removes one token per ordinary input arc corresponding with  $C_{\tau_1}^T$  from each of its input places (i.e. tokens are not removed along enabling arcs). Next,  $T$  produces zero or one token along each output arc: If  $(e_{\tau_1}^T, a_{\tau_1}^T)$  is a random hybrid vector generated from probability measure  $\mathcal{F}_T(\cdot; C_{\tau_1}^T)$  (by making use of a Uniform random variable  $U_i$ ), then vector  $e_{\tau_1}^T$  is a vector of zeros and ones, where the  $i$ th vector element corresponds with the  $i$ th outgoing arc of transition  $T$ . An output place gets a token iff it is connected to an arc that corresponds with a vector element 1. Moreover,  $a_{\tau_1}^T$  specifies the colours of the produced tokens.

**Execution from first transition firing onwards.** At  $t = \tau_1$ , zero or more transitions are pre-enabled (if this number is zero, no transitions will fire anymore). If these include immediate transitions, then these are fired without delay, but with use of rules R0–R4. If after this, still immediate transitions are enabled, then these are also fired, and so forth, until no more immediate transitions are enabled. Next, the SDCPN is executed in the same way as described above for the situation from  $\tau_0$  onwards.

### 2.3 SDCPN stochastic process

The marking of the SDCPN is given by the numbers of tokens in the places and the associated colour values of these tokens and can be mapped to a probabilistically unique SDCPN stochastic process  $\{M_t, C_t\}$  as follows: For any  $t \geq \tau_0$ , let a token distribution be characterised by the vector  $M_t' = (M_{1,t}', \dots, M_{|\mathcal{P}|,t}')$ , where  $M_{i,t}' \in \mathbb{N}$  denotes the number of tokens in place  $P_i$  at time  $t$  and  $1, \dots, |\mathcal{P}|$  refers to a unique ordering of places adopted for SDCPN. At times  $t \in (\tau_{k-1}, \tau_k)$  when no transition fires, the token distribution

is unique and we define  $M_t = M'_t$ . The associated colours of these tokens are gathered in a column vector  $C_t$  which first contains all colours of tokens in place  $P_1$ , next (i.e. below it) all colours of tokens in place  $P_2$ , etc, until place  $P_{|\mathcal{P}|}$ . If at time  $t = \tau_k$  one or more transitions fire, then the SDCPN discrete process state at time  $\tau_k$  is defined by  $M_{\tau_k}$  = the token distribution that occurs after all transitions that fire at time  $\tau_k$  have been fired. The associated colours of these tokens are gathered in a column vector  $C_{\tau_k}$  in the same way as described above. This construction ensures that the process  $\{M_t, C_t\}$  has limits from the left and is continuous from the right, i.e., it satisfies the càdlàg property.

### 3 Air traffic example and its SDCPN model

To illustrate the advantages of SDCPN when modelling a complex system, consider a simplified model of the evolution of an aircraft in one sector of airspace. The deviation of this aircraft from its intended path is affected by its engine system and its navigation system. Each of these aircraft systems can be in either *Working* (functioning properly) or *Not working* (operating in some failure mode). Both systems switch between these modes independently and with exponentially distributed sojourn times, with finite rates  $\delta_3$  (engine repaired),  $\delta_4$  (engine fails),  $\delta_5$  (navigation repaired) and  $\delta_6$  (navigation fails), respectively. If both systems are *Working*, the aircraft evolves in *Nominal* mode and the position  $Y_t$  and velocity  $S_t$  of the aircraft are determined by  $dX_t = \mathcal{V}_1(X_t)dt + \mathcal{W}_1dW_t$ , where  $X_t = (Y_t, S_t)'$ . If either one, or both, of the systems is *Not working*, the aircraft evolves in *Non-nominal* mode and the position and velocity of the aircraft are determined by  $dX_t = \mathcal{V}_2(X_t)dt + \mathcal{W}_2dW_t$ . The factors  $\mathcal{W}_1$  and  $\mathcal{W}_2$  are determined by wind fluctuations. Initially, the aircraft has position  $Y_0$  and velocity  $S_0$ , while both its systems are *Working*. The evaluation of this process may be stopped when the aircraft has *Landed*, i.e. its vertical position and velocity are equal to zero.

An SDCPN graph for this example is developed in two stages. In the first stage, the agents of the operation are modelled separately, by one local SDCPN each, see Fig. 3a. In the next stage, the interactions between the agents are modelled, thus connecting the local SDCPN, Fig. 3b.

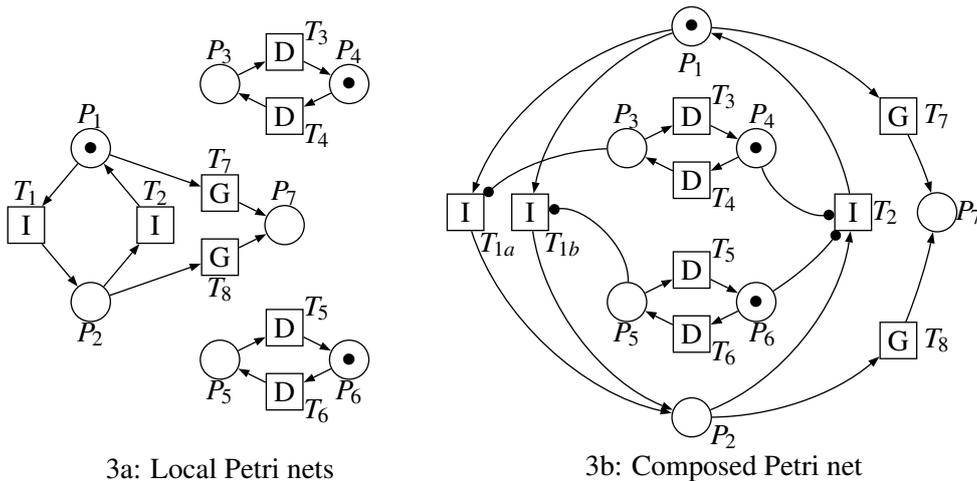


Figure 3: SDCPN graph for the aircraft evolution example

Fig. 3b shows the SDCPN graph for this example, where,

- $P_1$  denotes aircraft evolution *Nominal*, i.e. evolution is according to  $\mathcal{V}_1$  and  $\mathcal{W}_1$ .
- $P_2$  denotes aircraft evolution *Non-nominal*, i.e. evolution is according to  $\mathcal{V}_2$  and  $\mathcal{W}_2$ .
- $P_3$  and  $P_4$  denote engine system *Not working* and *Working*, respectively.
- $P_5$  and  $P_6$  denote navigation system *Not working* and *Working*, respectively.
- $P_7$  denotes the aircraft has landed.
- $T_{1a}$  and  $T_{1b}$  denote a transition of aircraft evolution from *Nominal* to *Non-nominal*, due to engine system or navigation system *Not working*, respectively.
- $T_2$  denotes a transition of aircraft evolution from *Non-nominal* to *Nominal*, due to engine system and navigation system both *Working* again.
- $T_3$  through  $T_6$  denote transitions between *Working* and *Not working* of the engine and navigation systems.
- $T_7$  and  $T_8$  denote transitions of the aircraft landing.

The graph in Fig. 3b completely defines SDCPN elements  $\mathcal{P}$ ,  $\mathcal{T}$ ,  $\mathcal{A}$  and  $\mathcal{N}$ , where  $\mathcal{T}_G = \{T_7, T_8\}$ ,  $\mathcal{T}_D = \{T_3, T_4, T_5, T_6\}$  and  $\mathcal{T}_I = \{T_{1a}, T_{1b}, T_2\}$ . The other SDCPN elements are specified below:

$\mathcal{S}$ : Two colour types are defined;  $\mathcal{S} = \{\mathbb{R}^0, \mathbb{R}^6\}$ .

$\mathcal{C}$ :  $\mathcal{C}(P_1) = \mathcal{C}(P_2) = \mathcal{C}(P_7) = \mathbb{R}^6$ , i.e. tokens in  $P_1$ ,  $P_2$  and  $P_7$  have colours in  $\mathbb{R}^6$ ; the colour components model the 3-dimensional position and 3-dimensional velocity of the aircraft.  $\mathcal{C}(P_3) = \mathcal{C}(P_4) = \mathcal{C}(P_5) = \mathcal{C}(P_6) = \mathbb{R}^0 \triangleq \emptyset$ .

$\mathcal{I}$ : Place  $P_1$  initially has a token with colour  $X_0 = (Y_0, S_0)'$ , with  $Y_0 \in \mathbb{R}^2 \times (0, \infty)$  and  $S_0 \in \mathbb{R}^3 \setminus \text{Col}\{0, 0, 0\}$ . Places  $P_4$  and  $P_6$  initially each have a token without colour.

$\mathcal{V}$ ,  $\mathcal{W}$ : The token colour functions for places  $P_1$ ,  $P_2$  and  $P_7$  are determined by  $(\mathcal{V}_1, \mathcal{W}_1)$ ,  $(\mathcal{V}_2, \mathcal{W}_2)$ , and  $(\mathcal{V}_7, \mathcal{W}_7)$ , respectively, where  $(\mathcal{V}_7, \mathcal{W}_7) = (0, 0)$ . For places  $P_3 - P_6$  there is no token colour function.

$\mathcal{G}$ : Transitions  $T_7$  and  $T_8$  have a guard defined by  $\mathcal{G}_{T_7} = \mathcal{G}_{T_8} = \mathbb{R}^2 \times (0, \infty) \times \mathbb{R}^2 \times (0, \infty)$ .

$\mathcal{D}$ : The jump rates for transitions  $T_3$ ,  $T_4$ ,  $T_5$  and  $T_6$  are  $\mathcal{D}_{T_3}(\cdot) = \delta_3$ ,  $\mathcal{D}_{T_4}(\cdot) = \delta_4$ ,  $\mathcal{D}_{T_5}(\cdot) = \delta_5$  and  $\mathcal{D}_{T_6}(\cdot) = \delta_6$ .

$\mathcal{F}$ : Each transition has a unique output place, to which it fires a token with a colour (if applicable) equal to the colour of the token removed.

## 4 From SDCPN to GSHS

Following [7], this section first presents a definition of *general stochastic hybrid system* (GSHS) and its execution. In [15] it has been proven that under a few conditions, SDCPN and GSHS are bisimilar. In Subsection 4.2 this is illustrated by showing how the SDCPN example of the previous section can be mapped to a bisimilar GSHS.

#### 4.1 GSHS definition

**Definition 4.1** (General stochastic hybrid system) A GSHS is an automaton  $(\mathbf{K}, d, \mathcal{X}, f, g, \text{Init}, \lambda, Q)$ , where

- $\mathbf{K}$  is a countable set.
- $d : \mathbf{K} \rightarrow \mathbb{N}$  maps each  $\theta \in \mathbf{K}$  to a natural number.
- $\mathcal{X} : \mathbf{K} \rightarrow \{E_\theta; \theta \in \mathbf{K}\}$  maps each  $\theta \in \mathbf{K}$  to an open subset  $E_\theta$  of  $\mathbb{R}^{d(\theta)}$ . With this, the hybrid state space is given by  $E \triangleq \{\{\theta\} \times E_\theta; \theta \in \mathbf{K}\}$ .
- $f : E \rightarrow \{\mathbb{R}^{d(\theta)}; \theta \in \mathbf{K}\}$  is a vector field.
- $g : E \rightarrow \{\mathbb{R}^{d(\theta) \times h}; \theta \in \mathbf{K}\}$  is a matrix field, with  $h \in \mathbb{N}$ .
- $\text{Init} : \mathcal{B}(E) \rightarrow [0, 1]$  is an initial probability measure, with  $\mathcal{B}(E)$  the Borel  $\sigma$ -algebra on  $E$ .
- $\lambda : E \rightarrow \mathbb{R}^+$  is a jump rate function.
- $Q : \mathcal{B}(E) \times (E \cup \partial E) \rightarrow [0, 1]$  is a GSHS transition measure, where  $\partial E \triangleq \{\{\theta\} \times \partial E_\theta; \theta \in \mathbf{K}\}$  is the boundary of  $E$ , in which  $\partial E_\theta$  is the boundary of  $E_\theta$ .

**Definition 4.2** (GSHS execution) A stochastic process  $\{\theta_t, X_t\}$  is called a GSHS execution if there exists a sequence of stopping times  $0 = \tau_0 < \tau_1 < \tau_2 \dots$  such that for each  $k \in \mathbb{N}$ :

- $(\theta_0, X_0)$  is an  $E$ -valued random variable extracted according to probability measure  $\text{Init}$ .
- For  $t \in [\tau_k, \tau_{k+1})$ ,  $\theta_t = \theta_{\tau_k}$  and  $X_t = X_t^k$ , where for  $t \geq \tau_k$ ,  $X_t^k$  is a solution of the stochastic differential equation  $dX_t^k = f(\theta_{\tau_k}, X_t^k)dt + g(\theta_{\tau_k}, X_t^k)dB_t^{\theta_{\tau_k}}$  with initial condition  $X_{\tau_k}^k = X_{\tau_k}$ , and where  $\{B_t^\theta\}$  is  $h$ -dimensional standard Brownian motion for each  $\theta \in \mathbf{K}$ .
- $\tau_{k+1} = \tau_k + \sigma_k$ , where  $\sigma_k$  is chosen according to a survivor function given by  $F(t) = \mathbf{1}_{(t < \tau^*)} \exp(-\int_0^t \lambda(\theta, X_s^k)ds)$ . Here,  $\tau^* = \inf\{t > \tau_k \mid X_t^k \in \partial E_{\theta_{\tau_k}}\}$  and  $\mathbf{1}$  is indicator function.
- The probability distribution of  $(\theta_{\tau_{k+1}}, X_{\tau_{k+1}})$ , i.e. the hybrid state right after the jump, is governed by the law  $Q(\cdot; (\theta_{\tau_k}, X_{\tau_{k+1}-}))$ .

[7] show that under assumptions G1-G4 below, a GSHS execution is a strong Markov Process and has the càdlàg property (right continuous with left hand limits).

- G1  $f(\theta, \cdot)$  and  $g(\theta, \cdot)$  are Lipschitz continuous and bounded. This yields that for each initial state  $(\theta, x)$  at initial time  $\tau$  there exists a pathwise unique solution  $X_t$  to  $dX_t = f(\theta, X_t)dt + g(\theta, X_t)dB_t$ , where  $\{B_t\}$  is  $h$ -dimensional standard Brownian motion.
- G2  $\lambda : E \rightarrow \mathbb{R}^+$  is a measurable function such that for all  $\xi \in E$ , there is  $\varepsilon(\xi) > 0$  such that  $t \rightarrow \lambda(\theta_t, X_t)$  is integrable on  $[0, \varepsilon(\xi))$ .
- G3 For each fixed  $A \in \mathcal{B}(E)$ , the map  $\xi \rightarrow Q(A; \xi)$  is measurable and for any  $(\theta, x) \in E \cup \partial E$ ,  $Q(\cdot; \theta, x)$  is a probability measure.
- G4 If  $N_t = \sum_k \mathbf{1}_{(t \geq \tau_k)}$ , then it is assumed that for every starting point  $(\theta, x)$  and for all  $t \in \mathbb{R}^+$ ,  $\mathbb{E}N_t < \infty$ . This means, there will be a finite number of jumps in finite time.

## 4.2 A bisimilar GSHS for the example SDCPN

Next we transform the SDCPN example model of Section 3 into a bisimilar GSHS. The first step is to construct the state space  $\mathbf{K}$  for the GSHS discrete process  $\{\theta_t\}$ . This is done by identifying the SDCPN *reachability graph*. Nodes in the reachability graph provide the number of tokens in each of the SDCPN places. Arrows connect these nodes as they represent transitions firing. The SDCPN of Fig. 3b has seven places hence the reachability graph for this example has elements that are vectors of length 7. These nodes, excluding the nodes that enable immediate transitions, form the GSHS discrete state space.

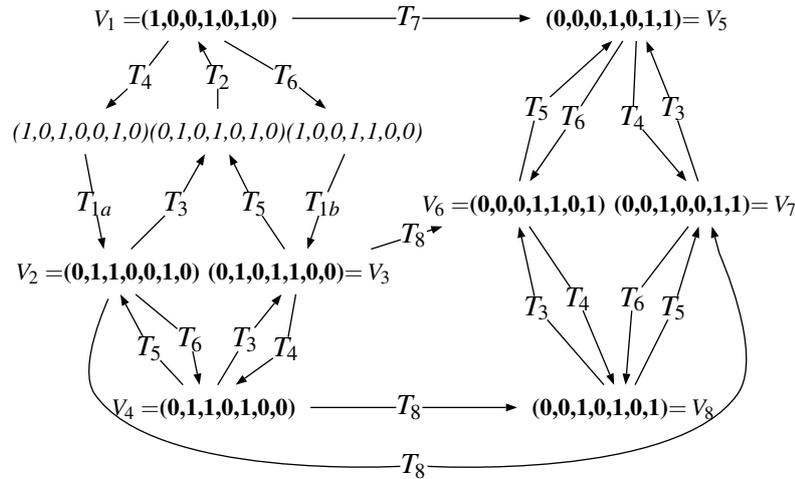


Figure 4: Reachability graph for the SDCPN of Fig. 3b. The nodes in bold type face correspond with the elements of the GSHS discrete state space  $\mathbf{K}$ .

The reachability graph is shown in Fig. 4, with nodes that form the GSHS discrete state space in Bold typeface, i.e.  $\mathbf{K} = \{V_1, \dots, V_8\}$ , with  $V_1 = (1, 0, 0, 1, 0, 1, 0)$ ,  $V_2 = (0, 1, 1, 0, 0, 1, 0)$ ,  $V_3 = (0, 1, 1, 0, 1, 0, 0)$ ,  $V_4 = (0, 1, 0, 1, 1, 0, 0)$ ,  $V_5 = (0, 0, 0, 1, 0, 1, 1)$ ,  $V_6 = (0, 0, 1, 0, 0, 1, 1)$ ,  $V_7 = (0, 0, 1, 0, 1, 0, 1)$ ,  $V_8 = (0, 0, 0, 1, 1, 0, 1)$ . Since initially there is a token in places  $P_1$ ,  $P_4$  and  $P_6$ , the GSHS initial mode equals  $\theta_0 = V_1 = (1, 0, 0, 1, 0, 1, 0)$ . The GSHS initial continuous state value equals the vector containing the initial colours of all initial tokens. Since the initial colour of the token in Place  $P_1$  equals  $X_0$ , and the tokens in places  $P_4$  and  $P_6$  have no colour, the GSHS initial continuous state value equals  $\text{Col}\{X_0, \emptyset, \emptyset\} = X_0$ . The GSHS drift coefficient  $f$  is given by  $f(\theta, \cdot) = \mathcal{V}_1(\cdot)$  for  $\theta = V_1$ ,  $f(\theta, \cdot) = \mathcal{V}_2(\cdot)$  for  $\theta \in \{V_2, V_3, V_4\}$ , and  $f(\theta, \cdot) = 0$  otherwise. For the diffusion coefficient,  $g(\theta, \cdot) = \mathcal{W}_1$  for  $\theta = V_1$ ,  $g(\theta, \cdot) = \mathcal{W}_2$  for  $\theta \in \{V_2, V_3, V_4\}$ , and  $g(\theta, \cdot) = 0$  otherwise. The hybrid state space is given by  $E = \{\{\theta\} \times E_\theta; \theta \in \mathbb{M}\}$ , where for  $\theta \in \{V_1, V_2, V_3, V_4\}$ :  $E_\theta = \mathbb{R}^2 \times (0, \infty) \times \mathbb{R}^2 \times (0, \infty)$  and for  $\theta \in \{V_5, V_6, V_7, V_8\}$ :  $E_\theta = \mathbb{R}^6$ . Always two delay transitions are pre-enabled: either  $T_3$  or  $T_4$  and either  $T_5$  or  $T_6$ . This yields  $\lambda(V_1, \cdot) = \lambda(V_5, \cdot) = \delta_4 + \delta_6$ ,  $\lambda(V_2, \cdot) = \lambda(V_6, \cdot) = \delta_3 + \delta_6$ ,  $\lambda(V_3, \cdot) = \lambda(V_7, \cdot) = \delta_3 + \delta_5$ ,  $\lambda(V_4, \cdot) = \lambda(V_8, \cdot) = \delta_4 + \delta_5$ . For the determination of GSHS transition measure  $Q$ , we make use of the reachability graph, the sets  $\mathcal{D}$ ,  $\mathcal{G}$  and  $\mathcal{F}$  and the rules R0–R4. In Table 1,  $Q(\theta', x'; \theta, x) = p$  denotes that if  $(\theta, x)$  is the value of the GSHS state before the hybrid jump, then, with probability  $p$ ,  $(\theta', x')$  is the value of the GSHS state immediately after the jump.

With this, the SDCPN of the aircraft evolution example is uniquely mapped to an GSHS. It can be shown that the SDCPN execution and the execution of the resulting GSHS are probabilistically equiva-

Table 1: Example GSHS transition measure for size of jump

For $x \notin \partial E_{V_1}$ :	$Q(V_2, x; V_1, x) = \frac{\delta_4}{\delta_4 + \delta_6}$ ,	$Q(V_4, x; V_1, x) = \frac{\delta_6}{\delta_4 + \delta_6}$
For $x \in \partial E_{V_1}$ :	$Q(V_5, x; V_1, x) = 1$	
For $x \notin \partial E_{V_2}$ :	$Q(V_3, x; V_2, x) = \frac{\delta_6}{\delta_3 + \delta_6}$ ,	$Q(V_1, x; V_2, x) = \frac{\delta_3}{\delta_3 + \delta_6}$
For $x \in \partial E_{V_2}$ :	$Q(V_6, x; V_2, x) = 1$	
For $x \notin \partial E_{V_3}$ :	$Q(V_4, x; V_3, x) = \frac{\delta_5}{\delta_3 + \delta_5}$ ,	$Q(V_2, x; V_3, x) = \frac{\delta_3}{\delta_3 + \delta_5}$
For $x \in \partial E_{V_3}$ :	$Q(V_7, x; V_3, x) = 1$	
For $x \notin \partial E_{V_4}$ :	$Q(V_3, x; V_4, x) = \frac{\delta_4}{\delta_4 + \delta_5}$ ,	$Q(V_1, x; V_4, x) = \frac{\delta_5}{\delta_4 + \delta_5}$
For $x \in \partial E_{V_4}$ :	$Q(V_8, x; V_4, x) = 1$	
For all $x$ :	$Q(V_6, x; V_5, x) = \frac{\delta_4}{\delta_4 + \delta_6}$ ,	$Q(V_8, x; V_5, x) = \frac{\delta_6}{\delta_4 + \delta_6}$
For all $x$ :	$Q(V_7, x; V_6, x) = \frac{\delta_6}{\delta_3 + \delta_6}$ ,	$Q(V_5, x; V_6, x) = \frac{\delta_3}{\delta_3 + \delta_6}$
For all $x$ :	$Q(V_8, x; V_7, x) = \frac{\delta_5}{\delta_3 + \delta_5}$ ,	$Q(V_6, x; V_7, x) = \frac{\delta_3}{\delta_3 + \delta_5}$
For all $x$ :	$Q(V_7, x; V_8, x) = \frac{\delta_4}{\delta_4 + \delta_5}$ ,	$Q(V_5, x; V_8, x) = \frac{\delta_5}{\delta_4 + \delta_5}$

lent, i.e. the SDCPN and the GSHS are bisimilar. Thanks to this bisimilarity we can now use the automata framework to analyse the GSHP that is defined by the SDCPN model for the example.

## 5 From SDCPN to HSDE

Following [1] and [2], this section first presents a definition of *hybrid stochastic differential equation* (HSDE) and gives conditions under which the HSDE has a pathwise unique solution. This pathwise unique solution is referred to as *HSDE solution process* or GSHP. The basic advantage of using HSDE in defining a GSHP over using GSHS is that with the HSDE approach the spontaneous jump mechanism is explicitly built on an underlying stochastic basis, whereas in GSHS the execution itself imposes an underlying stochastic basis. In [16] it has been proven that under a few conditions, SDCPN and HSDE are bisimilar. In Subsection 5.2 this is illustrated by showing how the SDCPN example of the previous section can be mapped to a bisimilar HSDE.

### 5.1 HSDE definition

For the HSDE setting we start with a complete stochastic basis  $(\Omega, \mathfrak{S}, \mathbb{F}, \mathbb{P}, \mathbb{T})$ , in which a complete probability space  $(\Omega, \mathfrak{S}, \mathbb{P})$  is equipped with a right-continuous filtration  $\mathbb{F} = \{\mathfrak{S}_t\}$  on the positive time line  $\mathbb{T} = \mathbb{R}^+$ . This stochastic basis is endowed with a probability measure  $\mu_{\theta_0, X_0}$  for the initial state, an independent  $h$ -dimensional standard Wiener process  $\{W_t\}$  and an independent homogeneous Poisson random measure  $p_P(dt, dz)$  on  $\mathbb{T} \times \mathbb{R}^{d+1}$ .

**Definition 5.1** (Hybrid stochastic differential equation) *An HSDE on stochastic basis  $(\Omega, \mathfrak{S}, \mathbb{F}, \mathbb{P}, \mathbb{T})$ , is defined as a set of equations (1)-(8) in which a collection of elements  $(\mathbb{M}, E, f, g, \mu_{\theta_0, X_0}, \Lambda, \psi, \rho, \mu, p_P, \{W_t\})$  appear.*

The elements  $(\mathbb{M}, E, f, g, \mu_{\theta_0, X_0}, \Lambda, \psi, \rho, \mu, p_P, \{W_t\})$  are defined as follows:

- $\mathbb{M} = \{\vartheta_1, \dots, \vartheta_N\}$  is a finite set,  $N \in \mathbb{N}$ ,  $1 \leq N < \infty$ .

- $E = \{\{\theta\} \times E_\theta; \theta \in \mathbb{M}\}$  is the hybrid state space, where for each  $\theta \in \mathbb{M}$ ,  $E_\theta$  is an open subset of  $\mathbb{R}^n$  with boundary  $\partial E_\theta$ . The boundary of  $E$  is  $\partial E = \{\{\theta\} \times \partial E_\theta; \theta \in \mathbb{M}\}$ .
- $f : \mathbb{M} \times \mathbb{R}^n \rightarrow \mathbb{R}^n$  is a measurable mapping.
- $g : \mathbb{M} \times \mathbb{R}^n \rightarrow \mathbb{R}^{n \times h}$  is a measurable mapping.
- $\mu_{\theta_0, X_0} : \Omega \times \mathcal{B}(E) \rightarrow [0, 1]$  is a probability measure for the initial random variables  $\theta_0, X_0$ , which are defined on the stochastic basis;  $\mu_{\theta_0, X_0}$  is assumed to be invertible.
- $\Lambda : \mathbb{M} \times \mathbb{R}^n \rightarrow [0, \infty)$  is a measurable mapping.
- $\psi : \mathbb{M} \times \mathbb{M} \times \mathbb{R}^n \times \mathbb{R}^d \rightarrow \mathbb{R}^n$  is a measurable mapping such that  $x + \psi(\vartheta, \theta, x, \underline{z}) \in E_\vartheta$  for all  $x \in E_\theta$ ,  $\underline{z} \in \mathbb{R}^d$ , and  $\vartheta, \theta \in \mathbb{M}$ .
- $\rho : \mathbb{M} \times \mathbb{M} \times \mathbb{R}^n \rightarrow [0, \infty)$  is a measurable mapping such that  $\sum_{i=1}^N \rho(\vartheta_i, \theta, x) = 1$  for all  $\theta \in \mathbb{M}, x \in \mathbb{R}^n$ .
- $\mu : \Omega \times \mathbb{R}^d \rightarrow [0, 1]$  is a probability measure which is assumed to be invertible.
- $p_P : \Omega \times \mathbb{T} \times \mathbb{R}^{d+1} \rightarrow \{0, 1\}$  is a homogeneous Poisson random measure on the stochastic basis, independent of  $(\theta_0, X_0)$ . The intensity measure of  $p_P(dt, d\underline{z})$  equals  $dt \cdot \mu_L(dz_1) \cdot \mu(d\underline{z})$ , where  $z = \text{Col}\{z_1, \underline{z}\}$  and  $\mu_L$  is the Lebesgue measure.
- $W : \Omega \times \mathbb{T} \rightarrow \mathbb{R}^h$  such that  $\{W_t\}$  is an  $h$ -dimensional standard Wiener process on the stochastic basis, and independent of  $(\theta_0, X_0)$  and  $p_P$ .

Using these elements, the HSDE process  $\{\theta_t^*, X_t^*\}$  is defined as follows:

$$\theta_t^* = \theta_t^k \text{ for all } t \in [\tau_k^b, \tau_{k+1}^b), k = 0, 1, 2, \dots \quad (1)$$

$$X_t^* = X_t^k \text{ for all } t \in [\tau_k^b, \tau_{k+1}^b), k = 0, 1, 2, \dots \quad (2)$$

Hence  $\{\theta_t^*, X_t^*\}$  consists of a concatenation of processes  $\{\theta_t^k, X_t^k\}$  which are defined by (3)-(8) below. If the system (1)-(8) has a solution in probabilistic sense, then the process  $\{\theta_t^*, X_t^*\}$  is referred to as *HSDE solution process* or *GSHP*.

$$d\theta_t^k = \sum_{i=1}^N (\vartheta_i - \theta_{t-}^k) p_P(dt, (\Sigma_{i-1}(\theta_{t-}^k, X_{t-}^k), \Sigma_i(\theta_{t-}^k, X_{t-}^k)) \times \mathbb{R}^d) \quad (3)$$

$$dX_t^k = f(\theta_t^k, X_t^k)dt + g(\theta_t^k, X_t^k)dW_t + \int_{\mathbb{R}^d} \psi(\theta_t^k, \theta_{t-}^k, X_t^k, \underline{z}) p_P(dt, (0, \Lambda(\theta_{t-}^k, X_{t-}^k)) \times d\underline{z}) \quad (4)$$

with  $\theta_0^0 = \theta_0, X_0^0 = X_0$  and with  $\Sigma_0$  through  $\Sigma_N$  measurable mappings satisfying, for  $\theta \in \mathbb{M}, \vartheta_j \in \mathbb{M}, x \in \mathbb{R}^n$ :

$$\Sigma_i(\theta, x) = \begin{cases} \Lambda(\theta, x) \sum_{j=1}^i \rho(\vartheta_j, \theta, x) & \text{if } i > 0 \\ 0 & \text{if } i = 0 \end{cases} \quad (5)$$

In addition, for  $k = 0, 1, 2, \dots$ , with  $\tau_0^b = 0$ :

$$\tau_{k+1}^b \triangleq \inf\{t > \tau_k^b \mid (\theta_t^k, X_t^k) \in \partial E\} \quad (6)$$

$$\mathbb{P}\{\theta_{\tau_{k+1}^b}^{k+1} = \vartheta, X_{\tau_{k+1}^b}^{k+1} \in A \mid \theta_{\tau_{k+1}^b}^k = \theta, X_{\tau_{k+1}^b}^k = x\} = Q(\{\vartheta\} \times A; \theta, x) \quad (7)$$

for  $A \in \mathcal{B}(\mathbb{R}^n)$ , where  $Q$  is given by

$$Q(\{\vartheta\} \times A; \theta, x) = \rho(\vartheta, \theta, x) \int_{\mathbb{R}^d} \mathbf{1}_A(x + \psi(\vartheta, \theta, x, \underline{z})) \mu(d\underline{z}) \quad (8)$$

Next, the following proposition can be shown to hold true [16]:

**Proposition 5.1** *Let conditions H1-H8 below hold true. Let  $(\theta_0^*(\omega), X_0^*(\omega)) = (\theta_0, X_0) \in E$  for all  $\omega$ . Then for every initial condition  $(\theta_0, X_0)$ , (1)-(8) has a pathwise unique solution  $\{\theta_t^*, X_t^*\}$  which is càdlàg and adapted and is a semi-martingale assuming values in the hybrid state space  $E$ .*

**H1** For all  $\theta \in \mathbb{M}$  there exists a constant  $K(\theta)$  such that for all  $x \in \mathbb{R}^n$ ,  $|f(\theta, x)|^2 + \|g(\theta, x)\|^2 \leq K(\theta)(1 + |x|^2)$ , where  $|a|^2 = \sum_i (a_i)^2$  and  $\|b\|^2 = \sum_{i,j} (b_{ij})^2$ .

**H2** For all  $r \in \mathbb{N}$  and for all  $\theta \in \mathbb{M}$  there exists a constant  $L_r(\theta)$  such that for all  $x$  and  $y$  in the ball  $B_r = \{z \in \mathbb{R}^n \mid |z| \leq r + 1\}$ ,  $|f(\theta, x) - f(\theta, y)|^2 + \|g(\theta, x) - g(\theta, y)\|^2 \leq L_r(\theta)|x - y|^2$ .

**H3** For each  $\theta \in \mathbb{M}$ , the mapping  $\Lambda(\theta, \cdot) : \mathbb{R}^n \rightarrow [0, \infty)$  is continuous and bounded, with upper bound a constant  $C_\Lambda$ .

**H4** For all  $(\theta, \vartheta) \in \mathbb{M}^2$ , the mapping  $\rho(\vartheta, \theta, \cdot) : \mathbb{R}^n \rightarrow [0, \infty)$  is continuous.

**H5** For all  $r \in \mathbb{N}$  there exists a constant  $M_r(\theta)$  such that

$$\sup_{|x| \leq r} \int_{\mathbb{R}^d} |\psi(\vartheta, \theta, x, \underline{z})| \mu(d\underline{z}) \leq M_r(\theta), \text{ for all } \vartheta, \theta \in \mathbb{M}$$

**H6**  $|\psi(\theta, \theta, x, \underline{z})| = 0$  or  $> 1$  for all  $\theta \in \mathbb{M}$ ,  $x \in \mathbb{R}^n$ ,  $\underline{z} \in \mathbb{R}^d$

**H7**  $\{(\theta_t^*, X_t^*)\}$  hits the boundary  $\partial E$  a finite number of times on any finite time interval

**H8**  $|\vartheta_i - \vartheta_j| > 1$  for  $i \neq j$ , with  $|\cdot|$  a suitable metric well defined on  $\mathbb{M}$ .

## 5.2 A bisimilar HSDE for the example SDCPN

Next we transform the SDCPN example model of Section 3 into a bisimilar HSDE. This mapping follows much the same procedure as for SDCPN to GSHS, except that the discrete state space is now referred to as  $\mathbb{M}$  (rather than  $\mathbf{K}$ ) and the Markov jump rate is now referred to as  $\Lambda$  (rather than  $\lambda$ ). The main additional difference is that the HSDE elements do not include a transition measure  $Q$  to define the size of jump, but include functions  $\psi$ ,  $\rho$  and  $\mu$  instead. The mapping of SDCPN to HSDE uses the construction of transition measure  $Q$  as an intermediate step, however. For the particular example SDCPN in this paper, these functions can be determined from  $Q$  as follows: Since the continuous valued process jumps to the same value with probability 1, we find that  $\psi(V^i, V^j, x, \underline{z}) = 0$  for all  $V^i, V^j, x, \underline{z}$ . Moreover,  $\rho(V^i, V^j, x) = P_Q(V^i, x, V^j, x)$  and  $\mu$  may be any given invertible probability measure.

With this, the SDCPN of the aircraft evolution example is uniquely mapped to an HSDE. If in addition, we want to make use of the HSDE properties of Proposition 5.1, i.e. the resulting HSDE solution process being adapted and a semi-martingale, we need to make sure that HSDE conditions H1-H8 are satisfied. It is shown below that they are, under the following sufficient condition D1 for the example SDCPN.

**D1** For  $P \in \{P_1, P_2\}$ , there exist  $K_P^v, L_P^v, K_P^w$  and  $L_P^w$  such that for all  $c, a \in \mathcal{C}(P)$ ,  
 $|\mathcal{V}_P(c)|^2 \leq K_P^v(1 + |c|^2)$  and  $|\mathcal{V}_P(c) - \mathcal{V}_P(a)|^2 \leq L_P^v|c - a|^2$  and  
 $\|\mathcal{W}_P(c)\|^2 \leq K_P^w(1 + |c|^2)$  and  $\|\mathcal{W}_P(c) - \mathcal{W}_P(a)\|^2 \leq L_P^w|c - a|^2$ .

We verify that under condition D1, HSDE conditions H1-H8 hold true in this example.

**H1:** From the construction of  $f$  and  $g$  above we have for  $\theta = V_1$ :  $|f(\theta, x)|^2 + \|g(\theta, x)\|^2 = |\mathcal{V}_1(x)|^2 + \|\mathcal{W}_1(x)\|^2 \leq K_{P_1}^v(1 + |x|^2) + K_{P_1}^w(1 + |x|^2) = K(\theta)(1 + |x|^2)$ , with  $K(\theta) = (K_{P_1}^v + K_{P_1}^w)$ . For  $\theta = V_2, V_3, V_4$  the verification is with replacing  $\mathcal{V}_1, \mathcal{W}_1$  by  $\mathcal{V}_2, \mathcal{W}_2$ .

- H2:** From the construction of  $f$  and  $g$  above we have for  $\theta = V_1$ :  $|f(\theta, x) - f(\theta, y)|^2 + \|g(\theta, x) - g(\theta, y)\|^2 = |\mathcal{V}_1(x) - \mathcal{V}_1(y)|^2 + \|\mathcal{W}_1(x) - \mathcal{W}_1(y)\|^2 \leq L_{P_1}^v |x - y|^2 + L_{P_1}^w \|x - y\|^2 = L_r(\theta) |x - y|^2$  with  $L_r(\theta) = L_{P_1}^v + L_{P_1}^w$ . For  $\theta = V_2, V_3, V_4$  replace  $\mathcal{V}_1, \mathcal{W}_1$  by  $\mathcal{V}_2, \mathcal{W}_2$ .
- H3:** Since  $\delta_3 - \delta_6$  are constant, for all  $\theta$ ,  $\Lambda(\theta, \cdot)$  is bounded and continuous, with upper bound  $C_\Lambda = \max\{\delta_4 + \delta_6, \delta_3 + \delta_6, \delta_3 + \delta_5, \delta_4 + \delta_5\}$ .
- H4:** Since for all  $\theta, \vartheta$ ,  $P_Q(\vartheta, \cdot; \theta, x)$  is constant, we find  $\rho(\vartheta, \theta, x) = P_Q(\vartheta, x, \theta, x)$  is continuous.
- H5 and H6:** These are satisfied due to  $\psi(V^i, V^j, x, \underline{z}) = 0$  for all  $V^i, V^j, x, \underline{z}$ .
- H7:** This condition holds due to  $\delta_3 - \delta_6$  being finite and the fact that in this SDCPN example, there is no firing sequence of more than one guard transition.
- H8:** This condition holds for all  $V_1, \dots, V_8$ , with metric  $|a|^2 = \sum_i (a_i)^2$ .

Thanks to this bisimilarity mapping we can now use HSDE tools to analyse the GSHP that is defined by the execution of the SDCPN model for the example.

## 6 Conclusions

The aim of this paper was to explain bisimilarity relations between SDCPN (stochastically and dynamically coloured Petri net), GSHS (general stochastic hybrid system) and HSDE (hybrid stochastic differential equation), which means that the strengths of one stochastic model formalism can be used by both of the other stochastic model formalisms. More specifically, these bisimilarity relations make it possible to combine the formal verification power of automata with the analysis power of stochastic differential equations and the compositional specification power of Petri nets.

We started in Section 2 by defining SDCPN and the resulting SDCPN stochastic process, which is referred to as a GSHP (general stochastic hybrid process). In Section 3 we presented a simple but illustrative SDCPN example model. In Section 4 we studied GSHP as an execution of a GSHS and illustrated by using the example of Section 3 that SDCPN and GSHS are bisimilar. Next, in Section 5 we studied GSHP as a stochastic process solution of HSDE and showed with an illustrative example that SDCPN and HSDE are bisimilar.

The bisimilarities between SDCPN, GSHS and HSDE models for the example considered mean that the resulting example model inherits the strengths of all three formal stochastic modelling formalisms. This has been depicted in Fig. 1 in the introduction. Examples of GSHP properties are convergence in discretisation, existence of limits, existence of event probabilities, strong Markov properties, reachability analysis. Examples of GSHS features are their connection to formal methods in automata theory and optimal control theory. Examples of HSDE features are stochastic analysis tools for semi-martingales. Examples of SDCPN features are natural expression of causal dependencies, concurrency and synchronisation mechanism, hierarchical and modular construction, and graphical representation. These complementary advantages of SDCPN, GSHS, HSDE and GSHP perspectives tend to increase with the complexity of the system considered.

An illustrative large scale application of bisimilarity relations between SDCPN, HSDE and stochastic hybrid automata has been developed in air traffic management. Currently pilots depend of air traffic controllers in solving potential conflicts between their flight trajectories. This places a huge requirement on the tasks of an air traffic controller. Imagine a similar kind of approach for road traffic; then each car driver would be blind and depends of instructions that some road traffic controller is communicating with the car drivers. How many cars do you think can be managed by one road traffic controller? The number

of aircraft that one air traffic controller can handle ranges between 10 and 20, depending of the complexity of the traffic pattern. Over a decade ago, it had been suggested by [22] that this limitation of the air traffic controller can be solved by moving the responsibility of conflict resolution from the air traffic controller to the pilots. Since then this airborne self separation idea has received a lot of research attention. Nevertheless, it still is unknown how much more air traffic can safely be accommodated under a well designed airborne self separation way of working. In order to add to the solution of this debate, a series of large European studies towards solving this question have been started under the name HYBRIDGE [18] and iFly [19] respectively. The way of working is to first develop a well defined SDCPN model of the airborne self separation concept of operation to be analysed, e.g. [17]. Subsequently this SDCPN model is further analysed using a bisimilar HSDE and hybrid automation formal model representation [5, 3], in which powerful stochastic analysis theory is exploited for the speeding up of Monte Carlo simulations. Using this approach, [4] have shown that the first generation of airborne self separation concept designs falls short in safely accommodating higher air traffic demand than conventional ATM can. The feedback of this finding to advanced air traffic concept designers triggered the development of more advanced airborne self separation concept of operation, e.g. see [19].

## References

- [1] H.A.P. Blom (2003): *Stochastic hybrid processes with hybrid jumps*. In: *Proceedings IFAC conference on analysis and design of hybrid system (ADHS), Saint-Malo, Brittany, France*. pp. 361–365.
- [2] H.A.P. Blom, G.J. Bakker, M.H.C. Everdij & M.N.J. Van der Park (2003): *Stochastic analysis background of accident risk assessment for air traffic management*. HYBRIDGE Report, D2.2. <http://hosted.nlr.nl/public/hosted-sites/hybridge/>.
- [3] H.A.P. Blom, G.J. Bakker & J. Krystul (2009): *Rare event estimation for a large scale stochastic hybrid system with air traffic application*. In: G. Rubino & B. Tuffin, editors: *Rare event simulation using Monte Carlo methods*, forthcoming. J.Wiley.
- [4] H.A.P. Blom, B. Klein Obbink & G.J. Bakker (2009): *Simulated collision risk of an uncoordinated airborne self separation concept of operation*. *ATC Quarterly* 17, pp. 63–93.
- [5] H.A.P. Blom, J. Krystul, G.J. Bakker, M.B. Klompstra & B. Klein Obbink (2007): *Free flight collision risk estimation by sequential Monte Carlo simulation*. In: C.G. Cassandras & J. Lygeros, editors: *Stochastic hybrid systems: recent developments and research trends, Control engineering* 24, chapter 10. Taylor & Francis Group / CRC Press, pp. 247–281.
- [6] M.L. Bujorianu & J. Lygeros (2004): *General stochastic hybrid systems: modelling and optimal control*. In: *Proceedings 43rd conference on decision and control (CDC), Nassau, Bahamas*.
- [7] M.L. Bujorianu & J. Lygeros (2006): *Toward a general theory of stochastic hybrid systems*. In: H.A.P. Blom & J. Lygeros, editors: *Stochastic hybrid systems: theory and safety critical applications, Lectures notes in control and information sciences (LNCIS)* 337. Springer, pp. 3–30.
- [8] M.L. Bujorianu, J. Lygeros & M.C. Bujorianu (2005): *Different approaches on bisimulation for stochastic hybrid systems*. In: M. Morari & L. Thiele, editors: *Proceedings 8th international workshop on hybrid systems: computation and control (HSCC), Zürich, Switzerland, Lecture notes in computer science (LNCS)* 3414. pp. 198–214.
- [9] M.H.A. Davis (1993): *Markov models and optimization, Monographs on statistics and applied probability* 49. Chapman and Hall, London.
- [10] R.J. Elliott (1982): *Stochastic calculus and applications, Applications of mathematics: Stochastic modelling and applied probability* 18. Springer-Verlag.

- [11] R.J. Elliott, L. Aggoun & J.B. Moore (1995): *Hidden Markov models: estimation and control*, Applications of mathematics: stochastic modelling and applied probability 29. Springer-Verlag.
- [12] S.N. Ethier & T.G. Kurtz (1986): *Markov processes, characterization and convergence*. Wiley series in probability and mathematical statistics. John Wiley & Sons, New York.
- [13] M.H.C. Everdij & H.A.P. Blom (2003): *Petri nets and hybrid state Markov processes in a power-hierarchy of dependability models*. In: *Proceedings IFAC conference on analysis and design of hybrid system (ADHS)*, Saint-Malo, Brittany, France. pp. 355–360.
- [14] M.H.C. Everdij & H.A.P. Blom (2005): *Piecewise deterministic Markov processes represented by dynamically coloured Petri nets*. In: S. Jacka, editor: *Stochastics: an international journal of probability and stochastic processes*, 77, number 1. Taylor & Francis, pp. 1–29.
- [15] M.H.C. Everdij & H.A.P. Blom (2006): *Hybrid Petri nets with diffusion that have into-mappings with generalised stochastic hybrid processes*. In: H.A.P. Blom & J. Lygeros, editors: *Stochastic hybrid systems: theory and safety critical applications*, Lectures notes in control and information sciences (LNCIS) 337. Springer, pp. 31–63.
- [16] M.H.C. Everdij & H.A.P. Blom (2010): *Hybrid state Petri nets which have the analysis power of stochastic hybrid systems and the formal verification power of automata*. In: P. Pawlewski, editor: *Petri nets: Applications*, chapter 12. InTech, pp. 227–252.
- [17] M.H.C. Everdij, M.B. Klompstra, H.A.P. Blom & B. Klein Obbink (2006): *Compositional specification of a multi-agent system by stochastically and dynamically coloured Petri nets*. In: H.A.P. Blom & J. Lygeros, editors: *Stochastic hybrid systems: theory and safety critical applications*, Lectures notes in control and information sciences (LNCIS) 337. Springer, pp. 325–350.
- [18] HYBRIDGE (2002). *EC project description*. <http://hosted.nlr.nl/public/hosted-sites/hybridge>.
- [19] iFly (2007). *EC project description*. <http://iFly.nlr.nl>.
- [20] J. Krystul (2006): *Modelling of stochastic hybrid systems with applications to accident risk assessment*. Ph.D. thesis, University of Twente, The Netherlands.
- [21] J. Krystul, H.A.P. Blom & A. Bagchi (2007): *Stochastic hybrid systems*, chapter 2: Stochastic differential equations on hybrid state spaces, pp. 15–45. Number 24 in Control engineering series. Taylor and Francis / CRC Press.
- [22] RTCA (1995): *Final report of RTCA Task Force 3; Free Flight implementation*. Final, RTCA Inc., Washington DC.
- [23] A.J. Van der Schaft (2004): *Equivalence of dynamical systems by bisimulation*. *IEEE transactions on automatic control* 49(12), pp. 2160–2172.