A Formal Framework for User-centric Control of Multi-Agent Cyber-physical Systems

Bujorianu, Marius and Bujorianu, Manuela and Barringer, Howard

2009

ISSN 1749-9097

A Formal Framework for User Centric Control of Probabilistic Multi-Agent Cyber-Physical Systems

Marius C. Bujorianu, Manuela L. Bujorianu and Howard Barringer

Centre for Interdisciplinary Computational and Dynamical Analysis,
University of Manchester, UK

email: {*Marius, Manuela*}.*Bujorianu@manchester.ac.uk*,
Howard.Barringer@manchester.ac.uk

Abstract. Cyber physical systems are examples of a new emerging modelling paradigm that can be defined as multi-dimensional system co-engineering (MScE). In MScE, different aspects of complex systems are considered altogether, producing emergent properties, or loosing some useful ones. This holistic approach requires interdisciplinary methods that result from formal mathematical and AI co-engineering. In this paper, we propose a formal framework consisting of a reference model for multi-agent cyber physical systems, and a formal logic for expressing safety properties. The agents we consider are enabled with continuous physical mobility and evolve in an uncertain physical environment. Moreover, the model is user centric, by defining a complex control that considers the output of a runtime verification process, and possible commands of a human controller. The formal logic, called safety analysis logic (SafAL), combines probabilities with epistemic operators. In SafAL, one can specify the reachability properties of one agent, as well as prescriptive commands to the user. We define symmetry reduction semantics and a new concept of bisimulation for agents. A full abstraction theorem is presented, and it is proved that SafAL represents a logical characterization of bisimulation. A foundational study is carried out for model checking SafAL formulae against Markov models. A fundamental result states that the bisimulation preserves the probabilities of the reachable state sets.

Keywords: *multi agent systems, cyber-physical systems, user centric control, stochastic model checking, bisimulation, runtime analysis, symmetries.*

1 Introduction

Cyber physical systems (CPS) are tight integrations of computation with physical processes. Examples can be found in diverse areas as aerospace, automotive, chemical processes, civil infrastructure, energy, manufacturing, transportation and healthcare. A realistic formal model for CPS will consider the randomness of the environments where there are deployed, as well as the fact that in most applications these are interacting agents. The agents are used to model entities enabled with physical mobility (e.g. cars, planes or satellites), which are able to do autonomous or guarded transitions, which are able to communicate and with evolutions continuous in both time and space. In the past all these essential system features were studied separately or shallowly integrated. The new technologies like CPS and ubiquitous computing require deep integration of orthogonal multiple features, raising the issue of modelling of emerging or lost system properties. This problem is approached in this problem by proposing a formal framework called *multi-dimensional system co-engineering* [7, 6] (MScE), a holistic view combining formal, mathematical and control engineering. With this respect, formal methods for the specification and verification have been only recently developed, like *Hilbertean formal methods* [4, 5] or *stochastic model checking* [10] . The most effective verification method has proved to be model checking [17]. This paper is a *foundational* study of model checking for a stochastic model of agents. In this model, each agent is a new computational model called *agent stochastic cyber-physical system (aCPS)*, i.e. each agent can move physically, thus it can be thought of as a hybrid system. Moreover, uncertainty is considered for both environment and for agent's hybrid behavior, and this uncertainty is quantified probabilistically. In the *multi-agent stochastic cyber-physical system (MAPS)* model all agents are embedded in a common physical environment and they communicate using channels. The new model, which is the kernel of MScE, addresses three new issues:

- provide real time information about the changing environment of agent based CPS.
- represent the information collected during runtime system analysis
- model the co-existence of the human control and automated control (making the model *user-centric*)

User enabled control is very important for CPS, where failures or incorrect usage may be catastrophic.

The MScE framework comprises:

- The holistic, mathematical models of aCPS and MAPS, and
- A formal logic, called *safety analysis logic* (SafAL), that offers original specification techniques for the probabilistic properties of single agent reachability. It also contains coloring types and two imperative operators: one of control theoretic nature saying that a discrete transition (a control) will take place, and a recommendation operator that prescribes a discrete transition.
- A verification strategy of safety properties expressed in SafAL against aCPS using system symmetries. We investigate the issues of bisimulation and of model checking.

There are two key concepts in model checking: *reachability analysis* and *bisimulation*. The first concept gives the effective behavior of the system, while bisimulation means the elimination of the computationally irrelevant states (duplicate or the unreachable states). Our approach departs by introducing a new and natural concept of bisimulation. Two continuous stochastic processes are considered bisimilar if their reachable sets have the same hitting probabilities.

A fully abstract semantics is constructed for the SafAL and it is proved that two states are bisimilar iff they are spatially symmetric. This result shows that bisimulation is a concept too strong for practical verification and it justifies the coloring approach. Using colors, more flexible equivalence concepts can be introduced.

Recent advances in probabilistic model checking have been achieved using the state space symmetries [19]. We use space symmetries to define a new semantics for SafAL. One main advantage of this new semantics is that we can refine the bisimulation concept. In practice, the probabilities are approximated and their equality is difficult to check. Most of current approaches consider a metric and ask that the transition probabilities differ very little [11]. In our approach, we ask the equality only for the reach set probabilities associated to some sets selected using the symmetries. One advantage of this definition is that some transition probabilities might be different, but these differences should 'compensate' when we consider global behaviors.

Using state space symmetries, we establish two important results. One of them assures the full abstraction of this new logic. The second one opens the possibility of model checking of SafAL formulas.

The paper is organized as follows. The next section succinctly presents a communicating multi-agent model. In section 3, safety analysis logic is introduced for the specification of safety properties for the multi-agent model. Section 4 is devoted to the development of a formal semantics for the logic, based on symmetries, which makes possible the model checking. In section 5, a new bisimulation concept is introduced, and a full abstraction result is proved. The paper ends with some concluding remarks. An appendix contains background material on stochastic processes.

2 A stochastic model for multi-agent cyber-physical systems

A cyber-physical system (CPS) is a system featuring a tight combination of, and coordination between, the system's computational and physical elements [24]. The US National Science Foundation (NSF) has identified cyber-physical systems as a key area of research. Starting in late 2006, the NSF and other United States federal agencies sponsored several workshops on cyber-physical systems.[1]

[1] "Cyber-physical systems". Grant opportunities. Grants.gov, a United States governmental resource. http://www.grants.gov/search/search.do?

2.1 An informal presentation

An *agent stochastic cyber-physical system (aCPS)* is based on the concept of stochastic hybrid system [8, 23] (SHS). A hybrid automaton consists of a discrete controller that switches between different continuous dynamical systems via some control laws modeled as guards. The evolution of every dynamical system is depicted as an open set in the Euclidean space, called location. The controller is represented as guarded transitions between modes.

The aCPS model considers nondeterminism in mode change and introduces two classes of probabilities:

• the noise in the modes; the evolution of each dynamical system is governed by a stochastic differential equation

• the probabilities of discrete transition, described by *reset maps.* These probabilities (formally *probability kernels*) evaluate the chances to restart a given dynamical system and depend on time and on the current evolution in a mode.

The agents can have *physical mobility*, i.e. the differential equation in modes may describe the moving equations of some devices (perhaps cars, planes or satellites) in a physical environment. This mobility can be affected by the *environment uncertainty* (captured formally by the SDEs from modes) and the agent decisions (the reset maps) can be also *unpredictable* (captured by the probability kernels).

Moreover, a MAPS has communication labels, and the transitions are classified in *send* transitions and *receive* transitions. A multi-agent model then considers several SHS, each one with an associated agent, and the communications between them is done via a given set of communication channels.

To every channel l there are associated two distinct labels:

• l^s denotes the action of sending a message through the channel l, and

• l^r denotes the action of receiving a message through the channel l.

In the standard models of hybrid systems, the transitions are guarded, with guards interpreted as boundaries of the location's invariant set. In the colored version, the boundary is extended to a colored region (red in this example), where a discrete transition must be triggered.

The first extension of the SHS model which allows to model agents is given by the concept of user triggered transitions. These are unguarded transitions (i.e. mode changes) that offer to an agent more freedom in controlling their evolution. An autonomous transition can be triggered, for example, by the inter-agent communication or by a driver after being warned by the brake assistance system. In the colored model, there is a colored region (yellow in this case) where the user *is required* to perform a discrete transition.

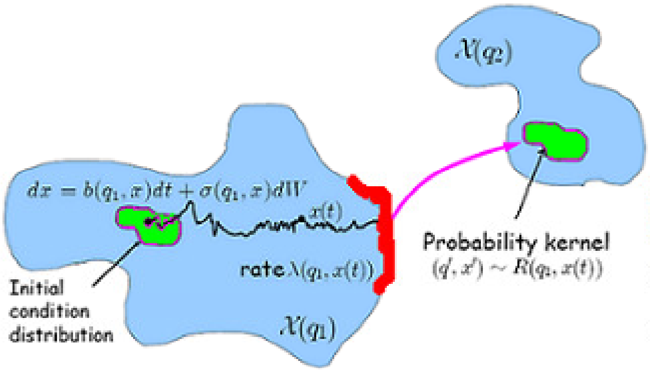
$\mathcal{X}(q_2)$
$dx = b(q_1, x)dt + \sigma(q_1, x)dW$
$x(t)$
Probability kernel
$(q', x') \sim R(q_1, x(t))$
rate $\lambda(q_1, x(t))$
Initial
condition
distribution
$\mathcal{X}(q_1)$

Figure 1

A further development of the model requires that the two types of discrete transitions and colored region coexist. Moreover, the red regions are always included in the yellow regions, which means that a controlled transition takes place only if the user has not triggered any discrete transition. It is also essential that any of the user triggered or the controlled transition produces the same post location (otherwise it means that the user is allowed to make unsafe procedures). These conditions are depicted in Figure 2.

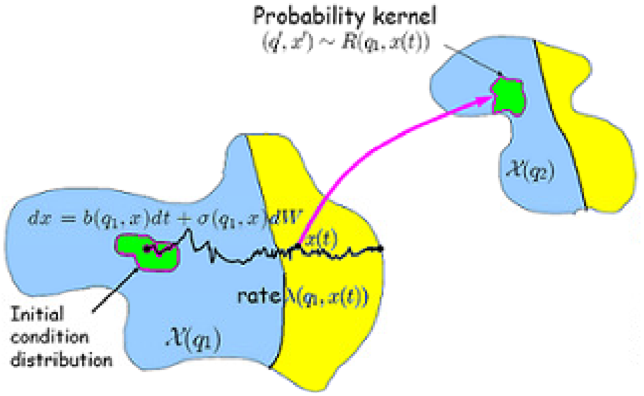
Probability kernel
$(q', x') \sim R(q_1, x(t))$
$\mathcal{X}(q_2)$
$dx = b(q_1, x)dt + \sigma(q_1, x)dW$
$x(t)$
rate $\lambda(q_1, x(t))$
Initial
condition
distribution
$\mathcal{X}(q_1)$

Figure 2

The models illustrated in Figures 1 and 2 can be interpreted as two different viewpoints on a CPS. In Figure 1, it is expressed the viewpoint of observing an autonomous car. The viewpoint from Figure 2 is that of observing the behaviour of a driver. The model in Figure 3 can be thought of as a viewpoint integration, where the automated control and the human control coexist. Moreover, the model is user centric because the two forms of control are hierarchical, user decisions having the higher priority.

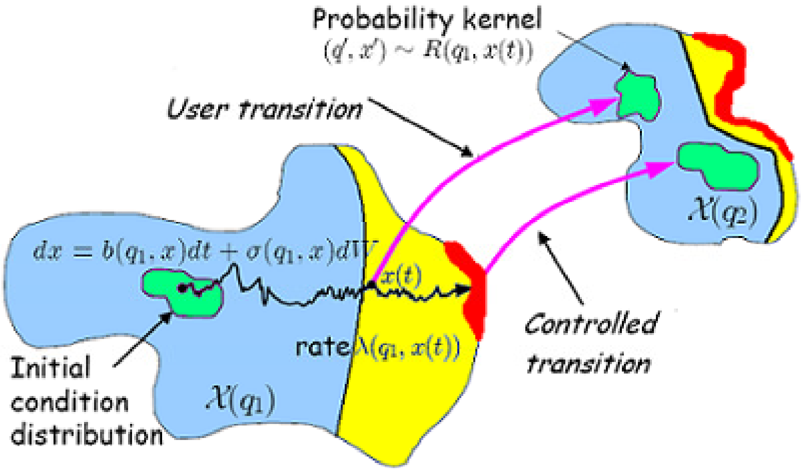

Figure 3

2.2 The formal model

An *agent stochastic cyber-physical system (aCPS) is a collection* $\langle (Q, d, \mathcal{X}), (y,r), ((J, \lambda, R), (m, f, \sigma)), L\rangle$ where:
(i) $(Q, d, \mathcal{X})$ describes the *state space*, which is a countable union of open sets from an euclidean space (the *modes*), each one corresponding to a discrete location. Note that the dimension of embedding euclidean space might be different for different locations.
(ii) (y,r) is the *coloring structure*. At each time, the coloring functions give, for each mode, the dangerous region (the *guard*), colored as red, and, respectively, the potentially dangerous zone (the *safety awareness guard*) colored as yellow.
(iii) $((J, \lambda, R), (m, f, \sigma))$ gives the *transition structure*, comprising the *discrete transition structure* (J, λ, R) and the *continuous (physical) transition structure* (m, f, σ). $J = C \cup U$ is the set of all *discrete transitions (or jumps)*. This is the union of the *controlled transitions* C and the *user triggered transitions* U. The controlled transitions C depend on the transition-choice function R. λ is the *jump rate* (it determines the rate of process discrete transitions). (m, f, σ) characterizes the continuous dynamics within the modes.
(iv) L is the set of *communication channels* (or *labels*).

These entities are formally defined next.

The complex structure of the state space (i) is defined as follows:

- Q is a finite set (of *locations*),
- $d : Q \to \mathbb{N}$ is a map giving for each location the dimension of the continuous state space in that location,
- $\mathcal{X} : Q \to \mathbb{R}^{d(\cdot)}$ is the mode definition function that maps each $q \in Q$ into an open subset $\mathcal{X}(q) = X^q$ of $\mathbb{R}^{d(q)}$ i.e. for each $q \in Q$, X^q is the *mode* (the *invariant* set) associated to the location q.

Let us denote by X the whole space, i.e. $X = \cup\{(q, X^q)|q \in Q\}$. Define the boundary set $\partial X^q := \overline{X^q}\backslash X^q$ of X^q and the whole space boundary $\partial X = \cup\{(q, \partial X^q)|q \in Q\}$.

The coloring structure (ii) is given by

- two coloring functions, the yellow function $y : \mathbb{R} \to 2^X$ and the red function $r : \mathbb{R} \to 2^X$, where $\mathbb{R}$ is the set of reals. For any location, every red colored state set must be included in the yellow colored one, i.e. if $r(t) = (q, A)$ and $y(t) = (q, B)$ then $A \subset B$. Moreover, every colored set must be included in a single location, i.e. $A, B \subset \mathbb{R}^{d(q)}$.

The jump structure from (iii) is given as follows:

- Each controlled transition $v \in C$ is a quadruple $v =: (q, l, q', R_b)$ where q is the origin location, l is the label of the jump, q' is the target location, and R_v is the *reset map* of the jump (or the *green coloring* function), i.e. for each $x \in \partial X^q$ with $R(v, q, x) > 0$ (see next item) and for all Borel sets A of $X^{q'}$ the quantity $R_v(x, A)$ is the probability to jump in the set A when the transition v is taken from the guard state x (boundary state).
- U is the set of *user triggered transitions*. Each element $u \in U$ is a pentuple $u =: (q, l, q', R_u, \lambda)$, where q is the origin location, l is the label of the jump, q' is the target location, R_u is the reset map of the jump.
- The function $R : C \times Q \times \partial X \to [0, 1]$ is defined such that for all $q \in Q$, all $x \in \partial X^q$, and all $v \in C$, which are outgoing transitions of q, the quantity $R(v, q, x)$ is the probability of executing a controlled transition v. In rest, R takes the zero value. Moreover, $\sum\limits_{v \in C_{q\to}} R(v, l, x) = 1$ for all l, x, where $C_{q\to}$ is the set of all elements of C that are outgoing transitions of q.

The continuous motion parameters from (iii) are given as follows:

- $f : X \to \mathbb{R}^{d(\cdot)}$ is a vector field
- $m : Q \to \mathbb{N}$ is a function that returns the dimension of the Wiener processes (that governs the evolution in the continuous state space, see the next item)
- $\sigma : X \to \mathbb{R}^{d(\cdot)\times m(\cdot)}$ is a $X^{(\cdot)}$-valued matrix. For all $q \in Q$, the functions $f^q : X^q \to \mathbb{R}^{d(q)}$ and $\sigma^q : X^q \to \mathbb{R}^{d(q)\times m(q)}$ are bounded and Lipschitz continuous and the continuous motions is governed by the following stochastic differential equation (SDE):

$$dx(t) = f^q(x(t))dt + \sigma^q(x(t))dW_t$$

where $(W_t, t \geq 0)$ is an $m(q)$-dimensional standard Wiener process in a complete probability space.
- Moreover, we assume the following *axioms*:
Assumption about the diffusion coefficients: for any $i \in Q$, the existence and uniqueness of the solution of the SDEs $f : Q \times X^{(\cdot)} \to \mathbb{R}^{d(\cdot)}$, $\sigma : Q \times X^{(\cdot)} \to \mathbb{R}^{d(\cdot)\times m(\cdot)}$ are bounded and Lipschitz continuous in z.

Assumption about non-Zeno executions: if we denote $N_t(\omega) = \sum I_{(t \geq T_k)}$ then for every starting point $x \in X$, $\mathbf{E}^x N_t < \infty$, for all $t \in \mathbb{R}_+$.
Assumption about the transition measure and the transition rate function:
(A) $\lambda : X \rightarrow \mathbb{R}_+$ is a measurable function such that $t \rightarrow \lambda(x_t^i(\omega_i))$ is integrable on $[0, \varepsilon(x^i))$, for some $\varepsilon(x^i) > 0$, for each $z^i \in X^i$ and each ω_i starting at z^i.
(B) for all A Borel measurable set**,** $R(\cdot, A)$ is measurable**;** for all $x \in \overline{X}$ the function $R(x, \cdot)$ is a probability measure; $R(x, \{x\}) = 0$ for $x \in X$.

The communication structure from (iv) is given by a structured set *labels*, each label $l \in L$ is a set $l = \{l^s, l^r\}$. There is a function which assigns a label to each jump from J, but we do not use it here.

Theorem 1. *Every aCPS is a strong Markov process.*

We assume that M is *transient* [13]. The transience of M means that any process trajectory which will visit a Borel set of the state space it will leave it after a finite time.

In this model, the environment is represented in two forms: the noise perturbation of system behavior in each location, and the information provided by the coloring functions. One can suppose the following scenario: The multi-sensorial perception of the changes in the environment is input to a safety analysis process. The results of the safety analysis consist of probabilities in reaching dangerous state sets. The safety evaluations of these probabilities are communicated to the human operator in the form of colored state sets. A yellow colored region means that a change (discrete transition) is recommended. A red colored region means that the automatic control must act.

A *multi-agent stochastic cyber-physical system* is a finite set of aPCS which can communicate pairwise using a common set of communication channels.

3 SafAL, the safety analysis logic

In this section, we define a model theoretic logic, the safety analysis logic (SafAL), for specifying probabilistic safety properties of the aCPS model defined in the previous section. This is a qualitative approach that can complement the already existing numerical approaches. The qualitative reasoning provides a global and symbolic expression of the reach set probabilities, which is a good starting point for numerical evaluations. This logic is necessary in the formal specification of the coloring maps, as well as for the specification of normative prescriptions to the human operator.

3.1 Syntax and functional semantics

We depart from a variant of Larsen and Skou's probabilistic modal logic [20], a logic that has also inspired the real valued logic for the (discrete) labeled

Markov Processes from [15]. Our approach differs fundamentally. The formulas of the logic are upper bounds for probabilities of reachable sets. In [15], the meaning of a formula is some measurable function.

The syntax is constructed from a formal description of a Markov process. That means we have a logic language where we can specify concepts like probability space, random variables, transition probabilities.

The main design scheme is based on the following principles. The system is modeled by a general Markov process. The sets of states are coded by their indicator functions. Obviously, these are elements of $\mathbf{B}(X)$. The application of the kernel operator on these functions generates the probabilities of the events that the system trajectories hit the respective sets.

The vocabulary of the logic is given by a family of measurable sets in a Lusin space. Each set is represented by its indicator function. For example, the interval $A = [0, 1/2]$ is represented, in the logic, by the function 1_A, which in each point x takes the value 1 if $0 \leq x \leq 1/2$ and the value 0 otherwise. The union of two disjoint sets A and B will be represented by the function $1_A + 1_B$. The intersection of two sets A and B will be represented by the function $\inf(1_A, 1_B)$. The complementary of the set A is represented by $1 - 1_A$.

We consider a linear space of bounded measurable functions, ranged over by the variable f. We define the terms by the following rules:

- the atomic terms are given by $\mathbf{1}$ or $\mho.f$, where $\mho$ is an '*action operator*'
- any other term is obtained from the atomic terms using:

$$g := g + g' | g - g' | \inf(g, g') | \sup_{n \in \mathbb{N}} g_n$$

The set of terms is denoted by $\mathcal{T}$.

A *reach type* formula is a statement of the form $g \leq v$, where g is a term and v is a real in $[0, 1]$. Other reach type formulae are obtained using the usual Boolean operators.

A *color* consists of a sub-interval $[a, b]$ of $[0, 1]$ and a subset C of the vocabulary such that $\mho.f$ takes values in $[a, b]$, for all $f \in C$.

A *safety formula* is obtained using the predefined predicate $\Game$ and the logical operator ∇ (which can not be nested).

The meaning of $\Game$ is that a discrete transition is triggered. A formula of the form ∇P means that it is "obligatory" [2] that the predicate P will be fulfilled. In particular, $\nabla\Game$ means that a jump is requested. The formula $\neg\nabla\neg P$ means that the predicate P is "permitted", $\nabla\neg P$ means that the predicate P is "forbidden".

The semantic domain consists of a Markov process $M = (x_t, P_x)$ satisfying the hypotheses of Section 2 and a countable set of Boolean variables *Prop*.

We consider only those bounded measurable functions that are indicator functions of measurable sets of states. For simplicity, consider a term, which contains only a bounded measurable function f. Intuitively, a term denotes a function that, when applied to a state x, provides the probability of all trajectories, starting from x, reaching a set 'indicated' by f. The reachability property is formulated relatively to several sets of states, then the term is formed with their indicator functions.

The interpretation of a term $f \in \mathcal{T}$ is a function $f : X \rightarrow \mathbb{R}$, which is a measurable bounded function. The interpretation $\Im$ of the atomic terms is given by:

$\Im(\mathbf{1}) = \mathbf{1}$, $\Im(\mho.f) = \mho.f$

where, for all $x \in X : \mathbf{1}(x) = 1$, $(\mho.f)(x) = \int [\int_0^\infty f(x_t(\omega))dt] P_x(d\omega)$

The infimum and supremum are defined pointwise.

The following characterization of the action of $\mho$ to a term g is insightful

$$(\mho.f)(\cdot) = E_{\cdot}[\int_0^\infty f(x_t)dt] = \int_0^\infty P_t f(\cdot)dt = Vf(\cdot). \qquad (1)$$

The terms are statistical statements about sets in the state space. An atomic term is the expectation of the random variable provided by the "visits" of a target set.

The formal semantics of the ∇ operator is defined considering a family of Markov processes $\mathcal{P}$ and a "normative" relation $\circlearrowleft \subseteq \mathcal{P} \times \mathcal{P}$ and a valuation function V :$Prop \times \mathcal{P} \rightarrow \{0,1\}$. The $P \circlearrowleft Q$ denotes that P is an alternative norm to Q. The function V assign a truth value to any variable in a MAPS $\mathcal{P}$ and we write $M \;\; P \models A$ whenever $V(A,P) = 1$.

$M \;\; P \models A$ iff $V(A,P) = 1$.

$M \;\; P \models \neg A$ iff not $M \;\; P \models A$.

$M \;\; P \models \nabla A$ iff $.\forall Q \in \mathcal{P}$ (if $P \circlearrowleft Q$ then $M \;\; Q \models A$).

Example 1. Consider the case of an aircraft for which we want to check that the probability to reach the sphere $S(u,2)$ starting from an initial point x is less than 0.01. We can consider a Markov process in the Euclidean space modelling the aircraft dynamics. The probability is given by the following SafAL formula $\mho.(1_{S(u,2)})(x) \leq 0.01$ which in the above semantics means $E_x[\int_0^\infty 1_{S(u,2)}(x_t)dt] \leq 0.01$. This formula appears frequently in the mathematical models used in air traffic control.

Example 2. The SafAL formula $\mho.1_A \geq 0.25 \supset \nabla \Game$ describes a yellow colored state set, where the dangerous area is described by the term A and the danger level for a reach probability is 0.25.

Example 3. The graphs from Fig. 4 depict SafAL terms (i.e. functions) that can be used for defining colors. Each graph depict the values of the probability of a discrete transition relative to the time of the first discrete transition. In the case (a) it is depicted the probability of a required discrete transition. In the case (b) it is shown the user ability to trigger a controlled transition, in the form of a probability. The case (c) illustrates the probability distribution for a supervisory controller to react, and it depends on the previous probabilities.

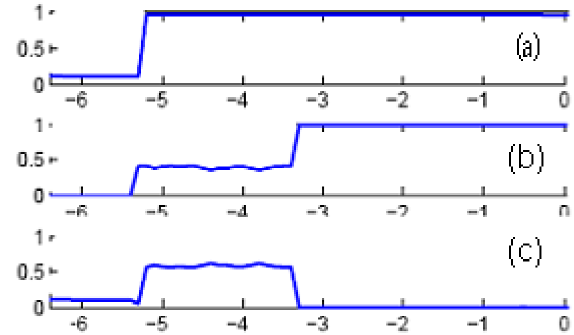

Figure 4

3.2 A formal semantics based on symmetries

Symmetry reduction is an efficient method for exploiting the occurrence of replication in discrete probabilistic model checking [19]. The verification of a model can be then performed for a bisimilar quotient model, which is up to factorial smaller. This is why, in this section, we explore the possibility of an alternative semantics of SafAL based on symmetries.

Let $\mathcal{S}(X)$ be the group of all homeomorphisms $\varphi : X \to X$, i.e. all bijective maps φ such that φ, φ^{-1} are $\mathcal{B}(X)$-measurable. When X is finite, $\mathcal{S}(X)$ is the set of (finite) permutations of X.

Any permutation[2] of X induces a permutation of the group of measurable functions (in particular of the terms) as follows. Let $* : \mathcal{S}(X) \to Perm[\mathbf{B}(X)]$ be the *action* $\mathcal{S}(X)$ to $\mathbf{B}(X)$ defined by $*(\varphi) = \varphi^* : \mathbf{B}(X) \to \mathbf{B}(X)$ where φ^* is the linear operator on $\mathbf{B}(X)$ given by

$$\varphi^* f = f \circ \varphi. \tag{2a}$$

The range of $*$ is included in $Perm[\mathbf{B}(X)]$ (the permutation group of $\mathbf{B}(X)$). This fact is justified by the invertibility of φ^*. The invertibility of φ^* can be derived from the bijectivity of $\varphi \in \mathcal{S}(X)$ because it is clear that $(\varphi^*)^{-1} = (\varphi^{-1})^*$. Then φ^* can be thought of as a symmetry of $\mathbf{B}(X)$ for each φ given in the appropriate set (see also the appendix).

Consider now a Markov process M, as in the Section 2 and the excessive function cone $\mathcal{E}_M$ (clearly a semigroup included in $\mathbf{B}(X)$). We can not define the action of $\mathcal{S}(X)$ to $\mathcal{E}_M$ using formula (2a) because the result of composition in (2a) is not always an excessive function.
Therefore it is necessary to consider some subgroups of permutations of the state space such that we can define the action of these subgroups on the semigroup of the excessive functions $\mathcal{E}_M$.
We consider the *maximal subgroup of permutations* of the state space X, denoted by $\mathcal{H}$, such that we can define the *action of* $\mathcal{H}$ to $\mathcal{E}_M$ $* : \mathcal{H} \to Perm[\mathcal{E}_M]$ defined as the appropriate restriction of (2a). The elements of $\mathcal{H}$ 'preserve' through '$*$'

[2] Here, permutation is used with the sense of one-to-one correspondence or bijection.

the excessive functions, or, in other words, the stochastic specifications of the system.

In the spirit of [19], the elements of $\mathcal{H}$ are called *automorphisms*. Note that in [19], the automorphisms are permutations of the state space, which preserve the transition system relation. For the Markov chains, the automorphisms defined in [19] preserve the probability transition function. For the case of continuous-time continuous space Markov processes, a transition system structure is no longer available (the concept of next state is available only for Markov chains). Therefore, it should be the case that the definition of the concept of automorphism to be different: An automorphism must preserve the probabilistic dynamics of the system. To express formally this idea, we need to use global parameterizations of Markov processes different from transition probabilities, which are local and depend on time. This is the reason why we have defined these automorphisms as maps which preserve the excessive functions.

Using $\mathcal{H}$, an equivalence relation $\mathcal{O} \subset X \times X$, called *orbit relation*, can be defined on the state space X as follows.

Definition 1. *Two states x, y are in the same orbit, written $x\mathcal{O}y$, if and only if there exists an automorphism $\varphi \in \mathcal{H}$ such that $\varphi(x) = y$.*

Let us denote by $[x]$ the equivalence class containing the point x in X. The equivalent classes of $\mathcal{O}$ are called *orbits*. It is clear that an orbit $[x]$ can be described as $[x] = \{\varphi(x) | \varphi \in \mathcal{H}\}$. Let $X/_{\mathcal{O}}$ denote the set of orbits, and let $\Pi_{\mathcal{O}}$ the canonical projection

$$\Pi_{\mathcal{O}} : X \to X/_{\mathcal{O}},\, \Pi_{\mathcal{O}}(x) = [x]. \tag{3}$$

The space $X/_{\mathcal{O}}$ will be equipped with the quotient topology by declaring a set $A \subset X/_{\mathcal{O}}$ to be open if and only if $\Pi_{\mathcal{O}}^{-1}(A)$ is open in X. It is clear now that $\Pi_{\mathcal{O}}$ is a continuous map with respect to the initial topology of X and the quotient topology of $X/_{\mathcal{O}}$.

Example 4. In Figure 5 there are illustrated some basic situations for using symmetries and permutations. In the (a), the agent trajectories on the side are symmetric in respect with the middle agent trajectory. In the case (b), the symmetric agents from case (a) are permuted. In the case (c), the agent trajectories denoted by 3, 4 and 5 can be obtained by symmetry from the configuration formed with the agents 1 and 2: agent 3 is the symmetric of agent 1 with respect with agent 2; then, considering agent 1 trajectory as reference, agent 4 is the symmetric of agent 2 and agent 5 is the symmetric of agent 3.

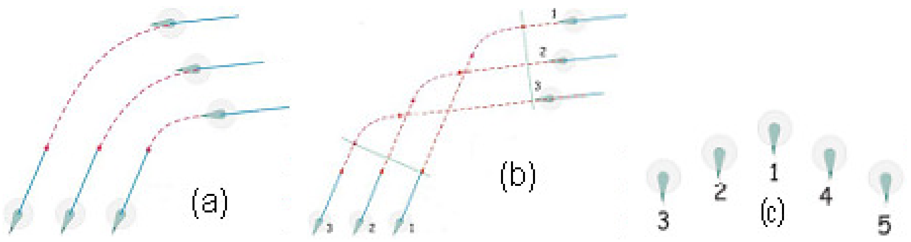

Figure 5

Example 5. Consider that in Figure 5.(a) there are depicted three cars on a motorway. The symmetry approach allows one to consider only two cars placed in lanes next to each other.

Consider an automorphism $\varphi \in \mathcal{H}$.

Definition 2. *A term g is called* φ-symmetric in $x, y \in X$ *if*

$$\varphi(x) = y \Rightarrow g(x) = g(y). \tag{4}$$

The φ-symmetry property of a term gives rise to a new concept of *satisfaction* for a formula.

Definition 3. *A formula $g \leq v$ is* equally satisfied *in $x, y \in X$ if there exists an automorphism $\varphi \in \mathcal{H}$ such that g is* φ-symmetric *in $x, y \in X$.*

4 Model checking safety properties

In this section, we investigate the issue of model checking the SafAL formulae. Because SafAL is a qualitative approach to probabilistic risk analysis, the model checking should be defined in an abstract way, rather than computationally. We establish mathematical properties relative to bisimulation and reachability analysis. In the first step, it is natural to consider model checking relative to any target set regardless their coloring.

4.1 Safety equivalence

The computational equivalence of processes (or bisimulation) is the traditional tool for reducing the complexity of the system state space. In the following, we define this bisimulation for a class of strong Markov processes in an analytical setting. Safety properties can be much more easily checked using a bisimilar system abstraction as illustrated in [11]. In our approach, computational equivalence means equal risk, and two states (safety) are bisimilar if they carry equal risk. We develop a series of mathematical results that constitute the key for the risk assessment. Roughly speaking, these results allow to interpret the risk in terms of the mathematical potentials associated to a Markov process.

For a continuous time continuous space Markov process M with the state space X, an equivalence relation $\mathcal{R}$ on X is a *(strong) bisimulation* if for $x\mathcal{R}y$ we have

$$p_t(x, A) = p_t(y, A), \forall t > 0, \forall A \in \mathcal{B}(X/_R) \tag{5}$$

where $p_t(x, A)$, $x \in X$ are the transition probabilities of M and $\mathcal{B}(X/_R)$ represents the σ-algebra of measurable sets closed with respect to $\mathcal{R}$. This variant of strong bisimulation considers two states to be equivalent if their 'cumulative' probability to 'jump' to any set of equivalent classes that this relation induces is the same. The relation (5) is hard to be checked in practice since the time t runs continuously. Therefore, to construct a robust bisimulation relation on M

it is necessary to use other characterizing parameters of M, such that formula (5) becomes a particular case of this new bisimulation.

In the following we briefly present the concept of bisimulation defined in [11]. This concept is more robust because it can be characterized by an interesting pseudometric [11].
Let $E \in \mathcal{B}(X_{\Delta})$ be a measurable set. Let us consider $T_E = \inf\{t > 0 | x_t \in E)$, the first time at which a given process "hits" a given subset E of the state space. It is possible to define a linear operator on $\mathbf{B}(X)$ (set of measurable bounded functions), denoted P_E by

$$P_E f(x) = P_x[f(x_{T_E}) | T_E < \infty]. \tag{6}$$

If f is excessive, then so is $P_E f$. In particular, $P_E 1(x) = P_x[T_E < \infty]$ is excessive for any $E \in \mathcal{B}(X_{\Delta})$. It can be shown that this function represents the probability measure of the set of process trajectories which hit the target set E, in infinite horizon time [11].

Suppose we have given a Markov process M on the state space X, with respect to a probability space $(\Omega, \mathcal{F}, \mathbf{P})$. Assume that $\mathcal{R} \subset X \times X$ is an equivalence relation such that the quotient process $M|_{\mathcal{R}}$ is still a Markov process with the state space $X/_{\mathcal{R}}$, with respect to a probability space $(\Omega, \mathcal{F}, \mathbf{Q})$. That means that the projection map associated to $\mathcal{R}$ is a Markov function.

Definition 4. *A relation $\mathcal{R}$ is called a behavioral bisimulation on X if for any $A \in \mathcal{B}(X/_{\mathcal{R}})$ we have that*

$$\mathbf{P}[T_E < \infty] = \mathbf{Q}[T_A < \infty]$$

where $E = \Pi_{\mathcal{R}}^{-1}(A)$ (i.e. the reach set probabilities of the process M and $M|_{\mathcal{R}}$ are equal).

Our first major assumption is that $X/_{\mathcal{O}}$ is a Lusin space. Often, this assumption can be checked, but there are some cases when $X/_{\mathcal{O}}$ fails to be Hausdorff (i.e. it is possible that two different orbits to share the same vicinity system). In these cases some minor modifications of X (changing, for example, the original topology) lead to a Hausdorff quotient space.

The main result of this section is that the orbit relation $\mathcal{O}$ is indeed a bisimulation relation defined on the state space X.

Theorem 2. *The orbit relation $\mathcal{O}$ is a behavioral bisimulation (as in the Definition 4).*

To prove this theorem we need some auxiliary results, which will be developed in the following.

Lemma 1. *If $f \in \mathcal{E}_M$ and $\varphi \in \mathcal{H}$ then*

$$P_E f = \varphi^*[P_F(\vartheta)] \tag{7}$$

where $F = \varphi(E)$; $\vartheta = \varphi^{-1*} f$ the action of '$*$' is given by (2a) and P_F is the hitting operator associated to F.

Proof of Lemma 1. It is known (Hunt's balayage theorem [3]) that

$$\begin{aligned} P_E f(x) &= \inf\{h(x) | h \in \mathcal{E}_M, h \geq f \text{ on } E\} \overset{(\text{if } \varphi \in \mathcal{H})}{=} \\ &= \inf\{h \circ \varphi^{-1}(\varphi(x)) | h \in \mathcal{E}_M, h \circ \varphi^{-1} \geq f \circ \varphi^{-1} \text{ on } \varphi(E)\} \\ &= \inf\{k(\varphi(x)) | k \in \mathcal{E}_M, k \geq f \circ \varphi^{-1} \text{ on } \varphi(E)\} \\ &= P_{\varphi(E)}(f \circ \varphi^{-1})(\varphi(x)) \\ &= P_{\varphi(x)}[(f \circ \varphi^{-1})(x_{T_{\varphi(E)}}) | T_{\varphi(E)} < \infty]. \end{aligned}$$

Remark 1. The equality (7) remains true for functions of the form $f_1 - f_2$ where f_1 and f_2 are excessive functions, and from there to arbitrary Borel measurable functions.

Proposition 1. *Let $g : X/_{\mathcal{O}} \to \mathbb{R}$ be a $\mathcal{B}(X/_{\mathcal{O}})$-measurable and let $E = \mathit{\Pi}_{\mathcal{O}}^{-1}(A)$ for some $A \in \mathcal{B}(X/_{\mathcal{O}})$. Then*

$$P_E f = \varphi^*[P_A f], \forall \phi \in \mathcal{H} \tag{8}$$

where $f : X \to \mathbb{R}$, $f = g \circ \mathit{\Pi}_{\mathcal{O}}$.

Proof of Prop. 1. If in Lemma 1, we let $f = g \circ \mathit{\Pi}_{\mathcal{O}}$, then $\vartheta = \varphi^{*-1} f = f \circ \varphi^{-1} = g \circ \mathit{\Pi}_{\mathcal{O}} \circ \varphi^{-1} = f$. More, $\varphi(\mathit{\Pi}_{\mathcal{O}}^{-1}(A)) = \mathit{\Pi}_{\mathcal{O}}^{-1}(A)$, so the proposition follows from the above lemma.

Formula (8) shows that the function $P_E f$ (where $f = g \circ \mathit{\Pi}_{\mathcal{O}}$) is constant on the equivalent classes with respect to $\mathcal{O}$. Then it makes sense to define a collection of operators (Q_A) on $(X/_{\mathcal{O}}, \mathcal{B}(X/_{\mathcal{O}}))$ by setting $Q_A g([x]) = P_E(g \circ \mathit{\Pi}_{\mathcal{O}})(x)$ where $E = \mathit{\Pi}_{\mathcal{O}}^{-1}(A)$. Proposition 1 allows to use any representative x of $[x]$ in the right side. It easy to check that $Q_A Q_B = Q_B$ if A and B are open sets of $X/_{\mathcal{O}}$ with $B \subset A$. Under some supplementary hypotheses one can construct a Markov process $M/_{\mathcal{O}} = (\mathit{\Omega}, \mathcal{F}, \mathcal{F}_t, [x]_t, Q_{[x]})$ with these hitting operators [13].

Now, we have all the auxiliary results needed to prove the Theorem 2.

*Proof of the Th.*2. If $E = \mathit{\Pi}_{\mathcal{O}}^{-1}(A)$ for some $A \in \mathcal{B}(X/_{\mathcal{O}})$ and we let $g \equiv 1$ then, for all $x \in X$

$$P_x[T_E < \infty] = Q_{[x]}[T_A < \infty]. \tag{9}$$

Formula (9) illustrates the equality of the reach set probabilities, i.e. $\mathcal{O}$ is a bisimulation relation.

4.2 Logical characterization of safety bisimulation

Theorem 3 (Full Abstraction Theorem). *Any two states $x, y \in X$ are bisimilar (through $\mathcal{O}$) if and only if, for any SafAL formula is equally satisfied by x and y.*

Proof of the Th. 3.
Necessity:

$x\mathcal{O}y$ implies that there exists $\overline{\varphi} \in \mathcal{H}$ such that $\overline{\varphi}(x) = y$. Since $\overline{\varphi} \in \mathcal{H}$, for all $g \in \mathbf{B}(X)$ we have from Lemma 1 (taking $E = \{\Delta\}$ and $\overline{\varphi}\{\Delta) = \Delta$) that $Vg(x) = V(g \circ \overline{\varphi}^{-1})(\overline{\varphi}(x))$. Or, taking $\varphi = \overline{\varphi}^{-1}$

$$Vg(x) = (Vg \circ \varphi)(x) \tag{10}$$

and using the fact any excessive function f is the limit of an increasing sequence of potentials (by Hunt theorem [3]) we can make the following reasoning. For a stochastic specification $f \in \mathcal{E}_M$ there exists a sequence $(g_n) \subset \mathbf{B}(X)$ such that Vg_n is increasingly converging to f. Then, from (10), we obtain that $(f \circ \varphi)(x) =\uparrow \lim Vg_n(\varphi(x)) =\uparrow \lim Vg_n(x), \forall x \in X$, i.e., we get that $f(x) = (f \circ \varphi)(x)$, $\forall f \in \mathcal{E}_M$. Therefore, the evaluations of each stochastic specification f in x and y are equal when $x\mathcal{O}y$. Then the result is true also for $f \in \mathcal{T}$, since any measurable function can be represented as the difference of two excessive function.

Sufficiency:

In this case, we have to show that if for each $f \in \mathcal{T}$ there exists $\varphi \in \mathcal{H}$ such that (4) is true, then $x\mathcal{O}y$. This statement is straightforward.

The Full Abstraction Theorem establishes that our model is correct and complete for the safety analysis logic. It provides new insights to the bisimulation relation $\mathcal{O}$, as follows.

Two states are equivalent when, for all system trajectories passing them some relevant probabilistic properties are evaluated to be the same. This computational copy of a state is given by the permutation φ from (4).

Corollary 1 The action of $\mathcal{H}$ to $\mathcal{E}_M$ can be restricted as the action of $\mathcal{H}$ to $\mathcal{P}_M$, i.e. $* : \mathcal{H} \times \mathcal{P}_M \to \mathcal{P}_M$ given by (2a).

This corollary is a direct consequence of the fact that $\mathcal{P}_M$ generates the cone $\mathcal{E}_M$. Then in the definition of $\mathcal{O}$, we can work not with excessive functions, but with potentials. This means that we can give the following characterization of the orbit relation.

Proposition 2. *$x\mathcal{O}y$ if and only if they have the 'same potential', i.e. there exists $\varphi \in \mathcal{H}$ such that $Vf(x) = Vf(y)$, $y = \varphi(x)$ for all $f \in \mathbf{B}(X)$*

Corollary 1 If $x\mathcal{O}y$ then there exists $\varphi \in \mathcal{H}$ such that $\varphi(x) = y$ and $p_t(x, \varphi^{-1}(A)) = p_t(y, A), \forall t \geq 0, \forall A \in \mathcal{B}$.

Summarizing, the model checking problem provides a very good motivation for the colored model. Without using colors, the only safety bisimilar states exist only for the systems that exhibit symmetries. Intuitively, two states are bisimilar only if they are spatially symmetric. Using colors, the bisimulation concept is coarser because the risk is considered only for colored sets. For example, two states can be colorly bisimilar even they are not spatially symmetric. For the car example, a state situated in the vicinity of a colored set, but characterized by a small velocity can be safety equivalent with a state situated far from the colored set but characterized by high velocity. Moreover, because the coloring functions depend on time, the safety equivalence for the colored model varies over the time. In other words, two safety bisimilar states can not be bisimilar anymore a few seconds later.

5 Final Remarks

Conclusions

In this paper, we have proposed the multi-dimensional system co-engineering framework, consisting of a stochastic multi-agent model, a formal logic for expressing safety properties and a foundational study of the basic formal verification concepts of bisimulation and model checking. An agent is modeled as an evolution of a cyber-physical system, which, in turn is an extension of a stochastic hybrid system. Agent models have been developed for discrete probabilistic systems [16] and hybrid systems [1]. Moreover, model checking methodologies have been developed for these systems. However, these methods can not be extended for agent models of systems which are simultaneously hybrid and stochastic. In this case, essential systems properties are lost and new properties emerge, as described within Hilbertean formal methods [4, 5].

Examples of lost properties include:

- The uniqueness of a continuous trajectories that start from a given point;
- The availability of the "next state" concept
- The representation of the transition probabilities in the compact form of a matrix. Instead, this situation leads to the use of linear operators. Consequently, their specification logics should be based on a different semantics.

The following situations can be considered as emergent properties:

- In the description of the system behavior, one is constrained to use only measurable sets of states and measurable sets of trajectories. Therefore, a specification logic based on such principles needs to be introduced.
- The reachability properties can not be expressed, as in the discrete case, using only the transition probabilities. Instead, we have to consider measurable sets of trajectories that visit a target set of states. This situation conducts to possibly unpleasant consequences: the model checking techniques developed for deterministic hybrid systems or for discrete probabilistic systems are not usable anymore.

To the authors knowledge the problems presented in this paper and the proposed solutions are new.

The existence of a fully abstract model, but still very general and constructive, forms the basis for future automated reasoning systems.

Related work

A model of agents as deterministic hybrid systems that communicate via shared variables is implemented in the Charon system (see [1] and the references therein). For discrete time and probabilistic agents, there exist well developed models [17]. However it is very difficult to model the agents as stochastic hybrid systems, especially because of the emergent properties presented before.

Symmetries have been used by Frazzoli and coauthors (see [18] and the references therein) in the optimal control of single agent, deterministic hybrid systems.

Bisimulation has got a large palette of definitions for discrete systems, and, similarly, there exist different definitions in the continuous and hybrid case. A categorical definition is proposed in [12], and non-categorical variants are introduced and investigated in [7], [11]. Other approaches to formal verification of probabilistic systems, like labelled Markov processes [14], consider automata models which are not agent oriented. The full abstraction theorem from section 6 extend a similar result established for discrete probabilistic automata.

Note that, in contrast with the action operator defined in the probabilistic modal logic for labeled Markov processes [14], the SafAL operator is defined using the time.

The SafAL can be fruitfully applied to performance analysis. In [10], it is shown that the expressions (1), i.e. the semantics of some SafAL formulas, represent performance measures for the fluid models of communication networks. Moreover, in the cited paper, it is developed a model checking strategy for a set of formulae that belong to SafAL against strong Markov processes, which enrich the formal verification toolset of MScE.

Future work

In a following paper we will extended SafAL to include inter-agent communication and develop an operational semantics for it. Considering the efficient model checking methods based on symmetry reduction [19], it is natural to further investigate developing similar numerical methods for SafAL. Application domains where MScE can be used include aerospace engineering[3], air traffic control and automotive industry.

More background material on stochastic processes and stochastic hybrid systems can be found in an early version [9] of this paper which is available on-line[4].

Acknowledgments

This work was partly funded by the EPSRC project EP/E050441/1. We thank the anonymous reviewers for useful comments.

References

1. Alur R., Grosu R. e.a.: *Modular Specification of Hybrid Systems in CHARON* Proc. of HSCC (2000): 6-19.
2. Barringer, H.: *The Future of Imperative Logic*, British Colloquium for Theoretical Computer Science 1990.
3. Boboc, N., Bucur, G., Cornea, A.: "*Order and Convexity in Potential Theory. H-Cones*"**.** Lecture Notes in Math, Vol. **853**, Springer Verlag (1992).
4. M.C. Bujorianu, M.L. Bujorianu: *Towards Hilbertian Formal Methods* Proc. of Conf. on Application of Concurrency to System Design, IEEE Press, (2007).
5. M.C. Bujorianu, M.L. Bujorianu: *An Integrated Specification Framework for Embedded Systems,* Proc. of SEFM, IEEE Press, (2007).

[3] *Engineering Autonomous Space Software* Project, EPSRC EP/F037201/1, http://gow.epsrc.ac.uk/ViewGrant.ASPx?Grant=EP/F037201/1

[4] http://eprints.eemcs.utwente.nl/12112/

6. Bujorianu, M.C., Bujorianu, M.L.: *Towards a Formal Framework for Multidimensional Codesign.* Technical Report TR-CTIT-08-21 Centre for Telematics and Information Technology, University of Twente, 2008, http://eprints.eemcs.utwente.nl/12108/
7. Bujorianu, L.M., Bujorianu, M.C.: *Bisimulation, Logic and Mobility for Markovian Systems.* In: Proc of Eighteenth International symposium on Mathematical Theory of Networks and Systems (2008)
8. Bujorianu, M.L.: *Extended Stochastic Hybrid Systems and their Reachability Problem.* In R. Alur, G. Pappas Eds., *Hybrid Systems: Computation and Control* HSCC04, Springer LNCS 2993, (2004): 234-249.
9. Bujorianu, L.M., Bujorianu, M.C., *Bisimulation, Logic and Reachability Analysis for Markovian Systems.* Technical Report TR-CTIT-08-23 Centre for Telematics and Information Technology, University of Twente (2008)
10. Bujorianu, M.L., Bujorianu, M.C.: *A Model Checking Strategy for a Class of Performance Properties of Fluid Stochastic Models.* In M. Telek e.a. eds., Proceedings of 3rd European Performance Engineering Workshop, Springer LNCS, (2006)
11. Bujorianu, M.L., Lygeros, J., Bujorianu, M.C.: *Abstractions of Stochastic Hybrid System.* Proc. 44th Conference in Decision and Control. IEEE Press (2005).
12. Bujorianu, M.L., Lygeros, J., Bujorianu, M.C.: *Bisimulation for General Stochastic Hybrid Systems.* In [21]: 198-216.
13. Blumenthal, R.M., Getoor, R.K.: "*Markov Processes and Potential Theory*", Academic Press, (1968).
14. Desharnais, J., Edalat, A., Panangaden, P.: *A Logical Characterization of Bisimulation for Labeled Markov Processes.* LICS (1998): 478-487.
15. Desharnais, J., Gupta, V., Jagadeesan, R., Panangaden, P.: *Metrics for Labelled Markov Systems.* In Proc. of CONCUR99, Springer-Verlag, (1999): 258-273.
16. Fisher, M., Bordini, R. H., Hirsch, B., and Torroni, P. *Computational Logics and Agents: A Roadmap of Current Technologies and Future Trends.* Computational Intelligence 23(1):61-91. Blackwell Publishing, February 2007.
17. Fisher, M., Ballarini, P., Wooldridge, M. *Uncertain Agent Verification through Probabilistic Model-Checking.* In Proceedings of 3rd International Workshop on Safety and Security in Multiagent Systems (SASEMAS '06).
18. Frazzoli, E., Bullo., F.: *On Quantization and Optimal Control of Dynamical Systems with Symmetries.* In Proc. IEEE Conf. on Decision and Control, volume 1, (2002): 817-823.
19. Kwiatkowska, M., Norman, G., Parker, D.: *Symmetry Reduction for Probabilistic Model Checking.* In Proc. 18th International Conference on Computer Aided Verification, Springer LNCS **4144**, (2006): 234-248.
20. Larsen, K.G., Skou, A.: *Bisimulation through Probabilistic Testing.* Information and Computation, **94** (1991): 1-28.
21. Morari, M., Thiele, L. (Eds.): "*Proc. Hybrid Systems: Computation and Control*" 8th International Workshop, Springer LNCS 3414 (2005)
22. McCall, J.C.; Trivedi, M.M.: *Driver Behavior and Situation Aware Brake Assistance for Intelligent Vehicles* Proceedings of the IEEE Volume 95, Issue 2, (2007): 374 - 387
23. Pola, G., Bujorianu, M.L., Lygeros, J., Di Benedetto, M. D.: *Stochastic Hybrid Models: An Overview with applications to Air Traffic Management*. In "Procceedings Analysis and Design of Hybrid Systems" IFAC ADHS03, Elsevier IFAC Publications (2003): 45-50.
24. Wikipedia *Cyber-physical system* http://en.wikipedia.org/wiki/Cyber-physical systems

6 Appendix: Background on stochastic processes

Let us consider $M = (x_t, P_x)$ a strong Markov process with the state space X. Let $\mathcal{F}$ and $\mathcal{F}_t$ be the appropriate completion of σ-algebras $\mathcal{F}^0 = \sigma\{x_t | t \geq 0\}$ and $\mathcal{F}_t^0 = \sigma\{x_s | s \leq t\}$. $\mathcal{F}_t$ describes the history of the process up to the time t. Technically, with any state $x \in X$ we can associate a natural probability space $(\Omega, \mathcal{F}, P_x)$ where P_x is such that its initial probability distribution is $P_x(x_0 = x) = 1$. The *strong Markov* property means that the Markov property is still true with respect to the stopping times of the process M. In particular, any Markov chain is a strong Markov process.
We adjoin an extra point Δ (the cemetery) to X as an isolated point, $X_\Delta = X \cup \{\Delta\}$. The existence of Δ is assumed in order to have a probabilistic interpretation of $P_x(x_t \in X) < 1$, i.e. at some 'termination time' $\zeta(\omega)$ when the process M escapes to and is trapped at Δ. As usual, $\mathbf{B}(X)$ denotes the set of bounded real functions on X.

Suppose that the following hypotheses are fulfilled.
1. M paths are right-continuous with left limits (the cadlag property).
2. X is equipped with Borel σ-algebra $\mathcal{B}(X)$ or shortly $\mathcal{B}$. Let $\mathcal{B}(X_\Delta)$ be the Borel σ-algebra of X_Δ.
3. The operator semigroup of M maps $\mathbf{B}(X)$ into itself.

- The set $\mathbf{B}(X)$ is the Banach space of bounded real measurable functions defined on X, with the sup-norm $||\varphi|| = \sup_{x \in X} |\varphi(x)|$, $\varphi \in \mathbf{B}(X)$.
- The semigroup of operators (P_t) is given by

$$P_t f(x) = E_x f(x_t) = \int f(y) p_t(x, dy), t \geq 0 \tag{11}$$

where E_x is the expectation with respect to P_x and $p_t(x, A)$, $x \in X$, $A \in \mathcal{B}$ represent the transition probabilities, i.e. $p_t(x, A) = P_x(x_t \in A)$.The semigroup property of (P_t) can be derived from the Chapman-Kolmogorov equations satisfied by the transition probabilities.

- A function f is *excessive* with respect to the semigroup (P_t) if it is measurable, non-negative and $P_t f \leq f$ for all $t \geq 0$ and $P_t f \nearrow f$ as $t \searrow 0$.

To the operator semigroup, one can associate the *kernel operator* as

$$Vf = \int_0^\infty P_t f dt, \; f \in \mathbf{B}(X) \tag{12}$$

The kernel operator is the inverse of the opposite of the infinitesimal operator associate to M.

Remark 2. The state space X can be chosen to be an analytic space (as the most general case), but we restrict ourself to the case of a Lusin space since our work is motivated by a multi-agent model where every agent is a realization of a stochastic hybrid systems who have, in most of the cases, Lusin state spaces.