Uncertainty and Reconfigurability in Hilbertean Formal Methods

Marius C. Bujorianu[†], Manuela L. Bujorianu[*‡]
[†] Department of Computer Science and Mathematics, Anglia-Ruskin University, Cambridge, UK
[*]University of Twente/Faculty EWI, Enschede, The Netherlands
[‡]CICADA, University of Manchester, UK

Abstract— Hilbertian Formal Methods is a recently introduced paradigm for embedded systems operating in harsh physical environments. This paradigm has been more developed for the deterministic case. However, it is very rare that a physical environment follows precisely a deterministic rule and then it is more realistic to consider stochastic models. A major problem in dealing with stochastic differential equations, the ubiquitous mathematical for phenomena arising from biology, medicine, meteorology and other domains, is that they can be solved only for very particular classes (linear and quasi linear). The Hilbertian Formal Methods are designed for situations when the solutions are not known (like for non-linear stochastic equations), but enough mathematical information about them can be derived helping in solving problems like stability, controllability, convergence, system design and verification.

In this paper, we present an integrated formal model for embedded systems operating in uncertain and nonlinear environments that can reconfigure their communication structure. This is achieved by introducing the observability logic, which is a formal notation for the observations of environment evolutions. This logic is integrated with a probabilistic version of the Pi-calculus that makes possible the real time communication of the measurements of the continuous evolutions, concurrency and reconfiguration of the embedded system. For example, these characteristics are necessary for mobile robot brigades, storm surge barrier systems, sensor networks or cardiac stimulators.

Keywords: embedded systems, event structures, Markov processes, Pi calculus

I. Introduction

The impressive development in embedded systems have made possible applications of formal methods that would have been considered non-standard a decade ago. In this development, a general tendency is the integration of very different features, like mobility, randomness, continuity and discrete / continuous mixed behaviors. This situation can be easily observed in distributed embedded systems areas like sensor networks, gene regulatory networks, robotics, storm prevention systems, cardiac stimulators and other medical applications. A development paradigm, called multi-dimensional codesign [19], [11], has been recently proposed in order to deal with this situation. In this paper, we approach multidimensional codesign using Hilbertean Formal Methods (HFM), another recently introduced [9] development paradigm for embedded systems, where concurrency is modelled explicitly and it is made available at the design stage. This approach complements the categorical approach presented in [15]. Concretely, we investigate this issue for embedded controllers operating in a continuous, uncertain and change prone environment.

The usual practice in embedded system engineering is to model environment by a stochastic differential equation (abbreviated SDE). Some parameters are measured using (a possible network of) sensors, and the measurements outputs determine a discrete controller to take some actions. Of course, the simple controllers just pick some discrete values from sensors and everything is reduced to standard automata theories. However, in many important applications discrete measurements are not enough to adequately approximate the environment evolutions and then complex mathematical models should be considered. The HFM approach mimics the mathematical practice, where important issues like the existence of solutions, system stability, controllability and convergence are established without knowing the expression of any solution. For this purpose, we introduce a specification language, called stochastic observability logic (SOL for short), in which the solutions of stochastic differential equations and their properties can be specified. We then integrate SOL with a probabilistic PI-calculus, in order to describe the communication structure of the embedded system. Pi-calculus is the basic ingredient for many architecture description languages supporting dynamic reconfiguration and self-management, like ArchWare [31], Pi-SPACE and $\pi-$ADL[1].

A model of our integrated specification language is a multi-agent system, each agent evolving in a continuous uncertain environment. The agents can dynamically exchange information about their environments with each other or with a server. The system can reconfigure its structure, according with the environment changes or because of birth/death of agents.

One major contribution is that we can attach an energy space to each agent. This contribution is two fold. First, it proposes an integration of the formal and analytic methods, necessary in the design of probabilistic systems. This construction is essential for the formal verification. The model checking of systems

[1] http://www-valoria.univ-ubs.fr/publications/Keyword//archlog-en.html

with continuous state components in the presence of probability is enormously difficult. One reason for this is that the most useful properties used in model checking deterministic hybrid automata or the discrete probabilistic automata are lost. Another reason is that the probability is a measure very sensitive to the changes made during system abstraction. This is why model checking for continuous stochastic systems is based on continuous mathematics, with their core given by energy spaces [5], [14], [12], [6].

The paper is structured as follows. In the section 2 we introduce the main mathematical notations and concepts. In the sections 3 and 4 we define the specification notations: for the discrete embedded controllers (a probabilistic Pi-calculus) and for their physical environments (the SOL). We show how these notations can be integrated using an algebraic model of embedded systems. Some tools of stochastic analysis, like the energy integral, are added to the framework in section 5. In the final sections we draw some conclusions and discuss related and future work. In a separate appendix[2] we present the omitted proofs.

II. Mathematical Preliminaries

A. Markov models

Let $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P, P_x)$ be a strong Markov process [16]. We suppose that the state space X is a Hausdorff space. The state space will be equipped with its Borel σ-algebra (i.e., σ-algebra generated by the open sets.) $\mathcal{B}(X)$.

In this paper, we suppose that all the Markov processes M used satisfy the following hypotheses.
1. The paths $t \to x_t(\omega)$ have the cadlag property, i.e. all the paths are right continuous functions on $[0, +\infty)$ and have left-hand limits on $[0, \zeta)$ almost surely.
2. X is a separable metric space homeomorphic to a Borel subset of some compact metric space (X is called Lusin space). Let $\mathcal{B}(X_\Delta)$ be the Borel σ-algebra of X_Δ.
3. The operator semigroup of M maps $\mathbf{B}(\mathbf{X})$ into itself.
4. The excessive functions of M are right continuous on trajectories.
Hypotheses 2., 3., 4. mean that M is a Borel process [26].

We have used the following concepts:
• The set $\mathbf{B}(\mathbf{X})$ is the lattice of bounded real measurable functions defined on X.
• The semigroup of operators is given by

$$P_t f(x) = E_x f(x_t) = \int f(y) p_t(x, dy), t \geq 0 \qquad (1)$$

where E_x is the expectation w.r.t. P_x and $p_t(x, A)$, $x \in X$, $A \in \mathcal{B}$ represent the transition probabilities, i.e. $p_t(x, A) = P_x(x_t \in A)$.

[2] that could be omitted in the final version.

• Using the semigroup of operators, one can define the kernel operator

$$Vf = \int_0^\infty P_t f dt,\ f \in \mathbf{B}(\mathbf{X}) \qquad (2)$$

and then the set of excessive functions, i.e.

$$\mathcal{E}_M = \{Vf | f \in \mathbf{B}(\mathbf{X}); f \geq 0\} \qquad (3)$$

According to the Blumenthal-Getoor-McKean theorem [16], the cone of excessive functions determines the process up to a time change.

B. Event structures

A complete lattice is a partially ordered set in which every subset has a least upper bound and a greatest lower bound. A conditionally complete lattice is a lattice such that every non-void bounded subset has a least upper bound and a greatest lower bound.

We consider a set E and a partial order $\preccurlyeq \subseteq E \times E$ is called causal order.

In the case of deterministic environments we used bundled event structures [25]. For uncertain environments, we move to a more general theory of probabilistic event structures [30].

A labelled event structure $\mathcal{E}$ is given by $\mathbb{E} = (E, \preccurlyeq, \#, Act, l)$ with:
(i) E a set of events; (ii) $\preccurlyeq$ is a causal order
(iii) $\# \subseteq E \times E$, the irreflexive and symmetric conflict relation;
(iv) $l : E \to Act$, the action-labelling function;

A partial cell is a set of events that are pairwise in conflict and have the same enabling sets [30]. A maximal partial cell is called a cell. An event structures is called confusion free if its cells are closed under conflict.

Let G be a set of cells of an event structure and let F be the set of events of all these cells. A partial probabilistic event structure is a confusion free event structure $(\mathbb{E}, G)$ with a cell valuation, which is a function $p : F \to [0, 1]$ such that, for every $c \in G$: $\Sigma_{e \in c} p(e) = 1$. A probabilistic event structure is partial probabilistic event structure with $F = E$.

III. The Stochastic Observability Logic

We consider systems having the major characteristic that they operate in a physical continuous environment, and the interaction with this environment can be complex. Examples include sensor networks opearating on the bottom of the sea or in very remote placed windmills, medical electronic implants operating the most sensitive parts of the human body like heart and brain, etc. These systems exhibit complex behaviors like adaptivity and self-management. Traditionally, this class of applications has been associated with embedded systems. The continuous dynamics of the environment has very peculiar features like nonlinearity, uncertainty, etc. Usually, these have

been abstracted away by drastic discretizations: the environment evolution is measured using a finite set of sensors. The real values of these parameters were the only continuous aspects considered in the design of an embedded controller. In control engineering and hybrid systems, there are cases when the continuous aspects are fully considered in the form of continuous dynamical systems. However, there are subtleties regarding their practical use: these dynamical systems are, in general, designed by humans (engines, cars, planes, trains, etc). These systems are simpler and less uncertain than the physical processes from nature and biological systems. When continuous processes are considered in their full generality there is little or no use at all of formal methods (like in gene regulatory networks, control engineering, bioengineering, etc). In this paper, we address the issue of constructing a semantic framework that bridges the formal methods and the stochastic continuous physical modeling. The intelligent embedded systems need to meet the requirements of modern control (prevision, adaptation, learning, self-management) and critical safety requirements. To achieve that, they consider sophisticated environment representations. The main obstacles in using physical features in formal methods are due to the different nature of the semantics. The difference between the semantics of the discrete controller and the continuous environment is in fact very deep and it acts in multiple dimensions. The most obvious is the density of trajectories of the environment behavior. Moreover, if in the deterministic case these trajectories are uniquely determined by an initial condition, in the probabilistic case this property is lost.

A. Syntax and Markovian semantics

We start with a specification language that offers support for continuous mathematics primitives, like reals, continuous functions, differentiable or integrable functions. A suitable language is Z [21], mainly because it preserves the favorite mathematical notations.

There is a difference between the presentation of a continuous Markov process in a standard textbook and the presentation (actually the specification) that an engineer use. In practice, the continuous Markov processes arise more often from stochastic differential equations.

An SDE has the form

$$\begin{cases} d\mathbf{X} = \mathbf{b}(\mathbf{X}, t)dt + \mathbf{B}(\mathbf{X}, t)d\mathbf{W} \\ \mathbf{X}(0) = \mathbf{X}_0 \end{cases} \quad (4)$$

where $\mathbf{b}(\mathbf{X}, t)dt$ is the deterministic part (usually a differential operator, perhaps with partial derivatives) and $\mathbf{B}(\mathbf{X}, t)d\mathbf{W}$ represents the "noise" (usually a Wiener process). The solution of the SDE is a Markov process with the transition probabilities defined as $P(x, s, A, t) = P\{X_{x,s}(t) \in A\}$, where

$$\mathbf{X}(t) = \mathbf{X}_0 + \int_0^t \mathbf{b}(\mathbf{X}(s), s)ds + \int_0^t \mathbf{B}(\mathbf{X}(s), s)d\mathbf{W} \quad (5)$$

The major problem is that the integral equation (5) has the same complexity as the initial SDE (4). Solutions are known only for particular classes, like linear SDEs. The solution proposed by HFM is to replace the solutions of the SDE (4) with their observations. Naturally, an observation should be a real function with some continuity properties on the paths space. Because the SDE it is not solvable, it is expected that not all observers can be computed. This approach is similar with the one from the deterministic case [10], where the observer role is played by the excessive functions (or potentials) of the deterministic differential operator. In [9] it is shown that the excessive functions of a Markov process form a class of models for the Hilbertian logic. These functions are defined by the formula (3) from section II.A.

A complete observer for the SDE given by formula (4) is a real valued function f such that:

i) it is measurable, non-negative and

ii) considering the semigroup (P_t) of the Markov process from formula 5, given by formula 1, we have $P_t f \leq f$ for all $t \geq 0$ and $P_t f \nearrow f$ as $t \searrow 0$.

The next result states that a complete observer is indeed continuous on system paths.

Theorem 1: A complete observer is continuous on any trajectory of the systems determined by SDE.

Moreover, we can further prove that the complete observers determine completely a system.

Theorem 2: The Markov process solution of the SDE is completely determined by the all complete observers of it.

Consider a generic collection of types, called stochastic types. Each type is specified by a stochastic differential equation.

The terms of a given type T are generated by the following grammar

$$f := \mathbf{1} | \perp | \top | f \odot f | f : f | f \overset{\circ}{-} c | \inf(f, f) | \sup(f, f) | < V > f$$

Let F denotes the set of all words generated by this grammar. The set of all terms is obtained from F by taking the quotients of the following equations:

$f \odot \top = \top$, $f \odot \perp = f$, $f \overset{\circ}{-} \perp = f$, $f \overset{\circ}{-} \top = \perp$

Each term denotes an action with effects that can quantified numerically. The simplest way is to see a term as a numerical function. The constants have the following intuitive meaning:

- $\top$ represents the deadlock,
- $\perp$ represents the null action (i.e. no effect), and
- $\mathbf{1}$ represents the step that generates one unit quantitative measurement.

The meaning of the operators is roughly as follows:

- $\odot$ represents the addition of effects (the pointwise addition in the functional interpretation).
- : has the opposite effect of $\odot$. Its notation is that of the residual in the lattice theory.
- $\overset{\circ}{-} c$ represents a cut of magnitude c units.

- inf, sup represent the usual lattice operations (which implies a semantic domain that is latticeal ordered).
- $< V >$ represents a modality, in this case, associated with the kernel operator V.

To each type T we attach two (super-)types V_T and E_T and the terms of type V_T are of the form $< V > f$ with f ranging the terms of type T. The terms of type E_T are of the form $\sup_{n\in\mathbb{N}} p_n$ with p ranging the terms of type V_T.

The most important operator, the modality, describes, in an abstract way, an evolution of a stochastic system. In a functional interpretation, a term of type V_T represents a potential (see subsection II-A). Then a term of type E_T denotes an excessive function. The construction of the type E_T is based on a famous theorem of Hunt (the "balayage theorem") [16]. It is well known that any Markov process can be characterized using its associated excessive functions. In the discrete case, this result represents an obvious combinatorial property of the transition probabilities. In the continuous case, this theorem represents a basic tool for studying Markov processes. Therefore, the SOL can be thought of as a specification formalism for the analytical properties of systems whose behaviors form a continuous Markov process.

The formulas are defined as equalities or inequalities between terms. The (in)equalities where the left hand side term is of type E_T are called trace formulas.

The seemantics is constructed as follows. We consider the Markov process $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x)$ associated with the SDE, as in subsection II-A, the interpretation of an $f \in F$ is a function $f : X \to \mathbb{R}$ which belongs to $\mathbf{B}(\mathbf{X})$. Then

$\mathbf{1}(x) := 1, \forall x \in X$

$\perp(x) := 0$

$\top(x) := \infty$, where ∞ is a large enough constant

$(f \odot g)(x) := f(x) + g(x)$

$$(f : g)(x) := \begin{cases} f(x) - g(x) & , \text{ if } f(x) \geq g(x) \\ 0 & , \text{ otherwise} \end{cases}$$

$$(f \overset{\circ}{-} c)(x) = \begin{cases} f(x) - c & , \text{ if } f(x) \geq c, \forall x \in X \\ 0 & , \text{ otherwise} \end{cases}$$

$(< V > f)(x) := \int [\int_0^\infty f(x_t(\omega))dt] P_x(d\omega)$

The infimum and supremum are defined pointwise. The action of V on a term f is given by

$$(< V > f)(\cdot) = E.[\int_0^\infty f(x_t)dt] = \int_0^\infty P_t f(\cdot)dt = Vf(\cdot) \tag{6}$$

The elements of $\mathbf{B}(\mathbf{X})$ can be thought of as terms in a stochastic observability logic associated to M. When M is transient, it is known, that from the set $\{Vf | f \in \mathbf{B}(\mathbf{X}), 0 \leq f \leq 1\}$, one can extract a countably (uniformly dense) subset, from which, it is possible to construct a countable set $\mathcal{O}_M$ of complete observers, only using infimum and supremum operations. The set $\mathcal{O}_M$ is dense in order from below in $\mathcal{E}_M$.

Naturally, one could ask about the connection between SOL and Hil, the Hilbertean logic which is the heart of Hilbertean Formal methods. The answer is that SOL is the stochastic version of Hil, as stated formally in the next result.

Theorem 3: A non-negative function is a complete observer iff it is excessive.

B. Algebraic semantics

A basic space is defined as being a structure $< \mathbb{S}, \leq, \perp, \top, \odot >$ where:

(S_1) $< \mathbb{S}, \leq, \perp, \top >$ is a lattice for which:

- $\perp$ the minimal element and $\top$ the greatest element;
- the lattice $(\mathbb{S}\backslash\{\top\}, \leq_{|\mathbb{S}\backslash\{\top\}}, \perp)$ is lower complete and upper conditionally complete;
- $\leq$ is called the essential order; we denote by $\vee$ resp. $\wedge$ the supremum resp. infimum wrt $\leq$;
- $\perp$ is called the nil action; $\top$ is called deadlock;

(S_2) $(\mathbb{S}, \odot, \perp)$ is a monoid for which:

- $s = \perp$ if $s \odot s = \perp$ $(\forall s \in \mathbb{S})$;
- $s \odot \top = \top$ $(\forall s \in \mathbb{S})$;

(S_3) and the following compatibility axioms holds:

- $s \odot (a \vee b) = (s \odot a) \vee (s \odot b)$ $(\forall a, b, s \in \mathbb{S})$;
- $a \odot b = (a \wedge b) \odot (a \vee b)$ $(\forall a, b \in \mathbb{S})$.

The residual of a by b, denoted by $a : b$, is the greatest element (if exists) such that $b \odot (a : b) \leq a$.

The semantics of a type T of SOL is a basic space $\mathbb{S}_T$ and the semantics of a term of type T is an element of $\mathbb{S}_T$. The logical operators $\odot, :, \inf, \sup, \perp, \top$ are interpreted by their obvious correspondent in a basic space. The semantics of the logical constant 1 is the neutral of the basic space monoid. The semantics of trace formulae of type T are elements of $\mathbb{S}_T$ satisfying the axioms $\mathbf{P1} - \mathbf{P8}$ from section 4.

Two elements $a, b \in \mathbb{S}$ are called strongly dual, denoted by $a \perp b$, if $a \wedge b = \perp$. We denote the class of orthogonal elements of a, by $a^\perp$, i.e. $a^\perp =: \{s \in \mathbb{S}; a \perp s\}$.

Let $\mathbb{S}$ be a basic space.

The specific order $\leq_\odot$ is defined by $a \leq_\odot b$ iff $(\exists c \in \mathbb{S}) : b = a \odot c$. We denote by $\bigvee_\odot$ resp. $\bigwedge_\odot$ the supremum resp. infimum in this order (if they exist).

Proposition 4: Every basic space has the decomposition property.

Proposition 5: We have $\leq_\odot \subseteq \leq$ (the specific order is coarser than the essential order).

We define the order topology $\tau_\leq$ on $< \mathbb{S}, \leq >$ by putting $(a_i)_{i\in I} \underset{\tau_\leq}{\to} a$ iff ($(a_i)_{i\in I}$ is increasing and dominated and $\bigvee_{i\in I} a_i = a$) or ($(a_i)_{i\in I}$ is decreasing and $\bigwedge_{i\in I} a_i = a$). Analogously can be defined the specific order topology $\tau_{\leq_\odot}$ on $< \mathbb{S}, \leq_\odot >$

Proposition 6: The superposition is continuous in the order topology.

Remark 1: The latticeal operations $\vee$ and $\wedge$ are continuous in the order topology.

The algebraic semantics can be integrated into Z semantics by shallow embedding.

IV. Integrated specification of embedded processes

A. Motivation

Embedded systems work in a real life environment, whose behaviour is highly unpredictable. In many situations, these behaviours are governed by stochastic differential equations that can be changed by discrete events (triggers). These behaviours are difficult to study by classical mathematical tools: solutions of stochastic equations are partial system evolutions, thus we can not derive conclusions on the global evolutions.

The mechanism used to integrate the specification notations is essentially observational. It consists of the recording that an external observer observes the evolutions of the physical environment, as well as the changes in these evolutions determined by the controller actions. This observation process can be interpreted in an abstract computational way (as in the case of event structures, for example) or strictly physical like in biomedical applications. For example, consider the case of a cardiac stimulator: the real observer is the cardiac specialist that effectively records a sequence of heart activity potentials. These potentials can be easily specified in SOL and they compose in sequence. When dangerous potentials appear, the stimulator activates electrical impulses that trigger the firing of excitatory heart potentials. This sequential evolution is modelled using a li relation. The change of potential is done in a smooth continuous way. This continuous change can be modelled either by functional composition (i.e. we consider a globally defined function) or by properties imposed on the *causal* relation. With this respect, the poset approach is very expressive. Continuous changes are modelled by the density property (see bellow). Moreover, one can distinguish different degrees of density. Another example is that of an embedded controller monitoring the patients with brain affections. The brain activity is monitored the sequence of electrical brain potentials (the encephalogram). When dangerous potentials are uncounted, the monitor can alert immediately the medical staff or even can take some emergency actions (like dropping a medicine in a perfusion). Obviously, there are cases when the physical process is simultaneously observed by different devices. This concurrent evolution is modelled by the co relation. In a computationally abstract sense, this order might be use to give semantics to different kinds of concurrent systems specified for example using process algebra or Petri nets. Further advantages for using posets come from their recent use in formal verification.

B. The probabilistic Pi-calculus

We consider the probabilistic extension of Pi-calculus considered in [29]. The language has two equivalent semantics, operational (in terms of Segala automata) and denotational (based on event structures).

The syntax

$P ::= 0 \ / \ !x(\widetilde{y}).P \ / \ (\nu x)P \ / \ P|Q \ / \ x\Phi_{i\in I} in_i(\widetilde{y}_i).P_i$
$/x \oplus_{i\in I} p_i in_i(\widetilde{y}_i).P_i$

As usual, $!x(\widetilde{y}).P$ denotes the replicated input, $(\nu x)P$ is the restriction, $P|Q$ is the parallel composition and $x\Phi_{i\in I} in_i(\widetilde{y}_i).P_i$ denotes the branching input. The process $x \oplus_{i\in I} p_i in_i(\widetilde{y}_i).P_i$ represents the probabilistic version of selecting output. The values $p_i \in [0,1]$ represent the probabilities ($\Sigma_{i\in I} p_i = 1$) associated with the events.

The causal order semantics

We use the semantics introduced in [29], based on probabilistic event structures.

Because the probabilistic $\pi-$calculus terms are identified up to $\alpha-$conversion (thus the identity of bound terms is not relevant) while in typed partial probabilistic event structure the identity of the object name is inportant, we have to consider a semantics parameterized by a set of names. Consider a function ρ that assigns to every bound name a set of fresh distinct names. This set can be a singleton. As usual, the semantics is given by a family of partial functions $[-]^{\rho}$ that takes a judgement of probabilistic $\pi-$calculus and return a partial probabilistic event structure. The semantics is defined inductively on the derivation of the typed judgement and it is briefly described in Fig.1 (borrowed from [29]).

The servers are interpreted as infinite parallel compositions. This interpretation makes also necessary the name parameterization since every bound name of a server corresponds to infinitely many names in the interpretation.

The basic ingredients of this framework are the causality relation, modeled as a partial order relation ($a \preceq b$ means the event a is the cause of b) and an algebraic structure (called here embedded process) that can associated to Markov process in a standard way (see Example 3). Markov processes are studied using tools specific to stochastic analysis, like excessive functions [4] and Dirichlet forms [23]. Two system evolutions a, b that are causal independent (i.e. $a \not\preceq b$ nor $b \not\preceq a$) can take place simultaneously (true concurrency).

C. Stochastic embedded processes

In this section, we present the mathematical model of the true concurrent stochastic processes, called the embedded process. We define first event spaces, the mathematical model of dynamics of the environment recorded by an embedded system. The elements of an event space are then decorated with elements of a basic space, a mathematical frame in which many biological potentials and dynamical systems can be defined.

$\mathbb{E} = (E, \preccurlyeq, \#, Act, l)$

An event space is a structure

$$< \mathbb{M}, \preccurlyeq, \#, Act, l, p >$$

$$[\![0 \triangleright x_i : (\tau_i)^?, y_j :\updownarrow]\!]^\rho = \emptyset$$

$$[\![(\nu\, x)P \triangleright \Gamma]\!]^\rho = [\![P \triangleright \Gamma, x : \tau]\!]^\rho \setminus x$$

$$[\![P_1 \| P_2 \triangleright \Gamma_1 \odot \Gamma_2]\!]^{\rho_1 \cup \rho_2} = ([\![P_1 \triangleright \Gamma_1]\!]^{\rho_1} \| [\![P_2 \triangleright \Gamma_2]\!]^{\rho_2}) \setminus S$$

$$[\![\overline{x} \bigoplus_{i\in I} \mathbf{in}_i(\tilde{y}_i).P_i \triangleright \Gamma, x : \bigoplus_{i\in I}(\tilde{\tau}_i)^\uparrow]\!]^{\rho,(\tilde{y}_i \to \tilde{z}_i)_{i\in I}} = \sum_{i\in I} \overline{x}\mathbf{in}_i\langle\tilde{z}_i\rangle.[\![P_i[\tilde{z}_i/\tilde{y}_i] \triangleright \Gamma, \tilde{z}_i : \tau_i]\!]^\rho$$

$$[\![x\, \Phi_{i\in I}\, p_i \mathbf{in}_i(\tilde{y}_i).P_i \triangleright \Gamma, x : \Phi_{i\in I}(\tilde{\tau}_i)^\downarrow]\!]^{\rho,(\tilde{y}_i \to \tilde{z}_i)_{i\in I}} = \sum_{i\in I} p_i x\mathbf{in}_i\langle\tilde{z}_i\rangle.[\![P_i[\tilde{z}_i/\tilde{y}_i] \triangleright \Gamma, \tilde{z}_i : \tau_i]\!]^\rho$$

$$[\![!x(\tilde{y}).P \triangleright \Gamma, x : (\tilde{\tau})^!]\!]^{\rho[K],\tilde{y} \to \{\tilde{y}_k\}_{k\in K}} = \prod_{k\in K} x\langle\tilde{y}^k\rangle.[\![P \triangleright \Gamma]\!]^\rho[\tilde{y}^k/\tilde{y}][Y^k/Y]$$

$$[\![\overline{x}(\tilde{y}).P \triangleright \Gamma, x : (\tilde{\tau})^?]\!]^{\rho,\tilde{y} \to \tilde{w}} = \overline{x}\langle\tilde{w}\rangle.[\![P \triangleright \Gamma, x : (\tilde{\tau})^?[\tilde{w}/\tilde{y}]]\!]^\rho$$

Fig. 1.

such that

(M_0) $\mathcal{E} = (\mathbb{M}, \preccurlyeq, \#, Act, l)$ is a probabilistic event structure.

(M_1) $< \mathbb{M}, \preccurlyeq >$ is a lower complete semi-lattice. The order $\preceq$ is called the causal order. We note by $\curlywedge$ (resp. $\curlyvee$) the infimum (resp. supremum if exists) of this semi-lattice and

(M_2) if $(\alpha_i)_{i\in I}$ is increasing and dominated in $\mathbb{M}$ by α, $\alpha \in \mathbb{M}$, then there exists $\underset{i\in I}{\curlyvee} \alpha_i$.

The elements of Act denote the agent communications.

Let $\mathbb{D} \subseteq \mathbb{M}$. We call $\mathbb{D}$

• dense in order from below (in $\mathbb{M}$) if for any $\alpha \in \mathbb{M}$ we have

$$\alpha = \curlyvee\{\gamma \in \mathbb{D}; \gamma \preccurlyeq \alpha\}; \tag{7}$$

• increasingly dense if the set $\{\gamma \in \mathbb{D}; \gamma \preccurlyeq \alpha\}$ is increasing to α for any $\alpha \in \mathbb{M}$.

A stochastic embedded process is a three-tuple

$$< \mathcal{E}, \mathcal{S}, \ell >,$$

where

$$\mathcal{E} =< \mathbb{M}, \preccurlyeq, \#, Act, l >$$

is a probabilistic event space,

$$\mathcal{S} =< \mathbb{S}, \leq, \perp, \top, \odot >$$

is a basic space and

$$\ell : \mathbb{M} \to \mathbb{S}$$

is an injective isotone labelling function such that, if $\mathbb{B} = \ell(\mathbb{M})$ then:

(P_1) $\ell(\alpha \curlyvee \beta) \geq_\odot \ell(\alpha) \vee \ell(\beta)$ if $\alpha \curlyvee \beta$ exists

(P_2) if $\ell(\alpha \curlyvee \beta) = \intercal$ and $\gamma \succ \alpha \curlyvee \beta$ then $\ell(\gamma) = \top$

(P_3) $\perp \in \mathbb{B}$

(P_4) $< \mathbb{B}, \leq_{|\mathbb{B}}, \wedge >$ is a lower complete semi-lattice of $< \mathbb{S}, \leq >$

(P_5) $\mathbb{B}$ is linearisable;

(P_6) $(\mathbb{B}, \odot, \perp)$ is a monoid;

(P_7) The superposition is continuous in the order topology on $\mathbb{B}$;

(P_8) $\mathbb{B}$ has the decomposition property.

The elements of an embedded process are called basic occurrences and will be denoted by Greek letters: α, β, etc. Their labels $\ell(\alpha), \ell(\beta)$ are called atomic processes. In the following we consider these concepts the same.

A typical example of embedded process is the encephalogram. The brain potentials are functions of the form $< V > f$ and their succession is captured by the relation $\preccurlyeq$.

The concept of complete observer might be too strong. Now we introduce a weakest version of the concept.

A continuous observer is a function $cob : \mathbb{B} \to \overline{\mathbb{R}}_+$ with the following properties:

(CO_1) $\alpha \preceq \beta \Rightarrow cob(\alpha) \leq cob(\beta)$, $(\forall \alpha, \beta \in \mathbb{B})$;

(CO_2) $cob(\beta) = \sup_{i\in I}(cob(\beta_i))$ if $(\beta_i)_{i\in I} \uparrow \beta$;

(CO_3) $(\forall \beta \in \mathbb{B})$ $(\exists (\beta_i)_{i\in I} \uparrow \beta) : cob(\beta_i) < \infty$.

A continuous observer cob is called nondeterministic iff

$$cob(\alpha \odot \beta) = \max(cob(\alpha), cob(\beta)) \tag{8}$$

An embedded process is called continuous observable if admits a continuous observer.

The image of a process under the all continuous observations will play an important role in the next section.

The process image is

$$Im\mathbb{B} = \{cob : \mathbb{B} \to \overline{\mathbb{R}}_+; cob \text{ is an additive continuous observer}\} \tag{9}$$

Remark 2: $Im\mathbb{B}$ can be ordered with the usual pointwise order

$cob_1 \leq cob_2 \Leftrightarrow cob_1(\beta) \leq cob_2(\beta)$ $(\forall \beta \in \mathbb{B})$.

In this order $Im\mathbb{B}$ is a lattice and

$$(cob_1 \vee cob_2)_{(\beta)} = \sup_{\beta_1 \odot \beta_2 \leq \beta} \{cob_1(\beta_1) + cob_2(\beta_2)\}$$

$$(cob_1 \bigwedge cob_2)_{(\beta)} = \inf_{\beta_1 \odot \beta_2 = \beta} \{cob_1(\beta_1) + cob_2(\beta_2)\}$$

Example 1: The Oosterscheldekering storm surge barrier[3] from the South Zeeland (on the Rhine-Meuse Delta) and the Maeslant Storm Surge Barrier[4] (near Rotterdam) in the South Holland, both provinces of the Netherlands. These barriers are software operated, based on information about weather collected from different source. The control software must take the decision of closing the barrier based on estimations of

[3] http://en.wikipedia.org/wiki/Delta_Works

[4] http://www.keringhuis.nl/engels/home_flash.html

the Ocean water level. If this level is overestimated and the barrier is closed, that could affect the local business, that could means loss of millions. If the water level is underestimated and barrier is kept open, it means that rapid and dangerous floods are possible. The role of water level estimation is crucial in the operations of these megastructures. The estimation is realized by processing information from many sources, based on the water, in the air or on the ground. The measurement functions are often placed on mobile devices, like ships, cars or satellites.. Pi-calculus proves to be a suitable formal language to describe these kind of communications. However, the essential ingredient remains how to measure and predict the meteorological events. These events are typical examples of nonlinear and uncertain continuous processes. Moreover, these processes are observed in their succession order, and they are difficult (if not impossible) to influence or to describe in enough rigorous detail to model them, for example, like a hybrid automaton.

Example 2: Another suitable example of stochastic embedded process can be obtained by randomization of the bucket brigade example from [27]. A bucket brigade consists of five robots arranged in a straight line. The first two robots pick up a part from a part feeder, execute a specific goal, move right, pass the part to the second robot and returns left for another part. The second robot picks stochastically a part from the first two, moves right with the part, passes it probabilistically to one of the forth or fifth robot, and returns left for another exchange. The last two robots move right and drops the part in the output bin, then return to meet the second robot.

V. Integrating formal and analytical methods

The advanced analytical investigation of partial differential operator and Markov processes made necessary the generalization of Hilbert product and norm to, respectively, energy form and the energy integral [23]. It is an area of Markov process theory that uses the energy of functionals to study a Markov process from a quantitative point of view. Recently Coste [20] used energy forms to analyze Markov chains with finite state spaces, by making energy comparisons. In this way, information about a simple chain is parlayed into information about another, more complicated chain. The book by Aldous and Fill [1] uses energy forms for similar purposes. Energy forms can be used to study Markov processes taking values in spaces of fractional dimension, i.e., fractals (see Fukushima [22]). The energy form techniques can be applied to study Markov processes taking values in infinite dimensional spaces [23]. Such processes are used to describe complex natural phenomena, such as the diffusion of gas molecules or the genetic evolution of a population. Each such system is made up of an effectively infinite number of individuals whose evolution in time is governed by a combination of chance and interactions with the other individuals in the system.

In the following, we define the energy of two elements (thought as generalised processes), present some (the simplest) examples from differential equations and Markov processes, and investigate the energy towards the main result, the theorem, that shows that, for a class of embedded processes called dissipative, one can associate an energy in canonical fashion.

The mutual energy $\mathcal{E}[a,b]$ of two elements a,b is a map $\mathcal{E}:\mathbb{S}\times\mathbb{S}\to\mathbb{R}$ with the following properties:

($\mathrm{EN}_{\mathbf{1}}$) the superposition principle: $\mathcal{E}[a\odot b,s]=\mathcal{E}[a,s]+\mathcal{E}[b,s]$

($\mathrm{EN}_{\mathbf{2}}$) the symmetry condition: $\mathcal{E}[a,b]=\mathcal{E}[b,a]$

($\mathrm{EN}_{\mathbf{3}}$) $\mathcal{E}$ is positive definite i.e. $\mathcal{E}[s]>0$ if $s\neq\perp$, where $\mathcal{E}[s]=\mathcal{E}[s,s]$ is called the energy of the element s

($\mathrm{EN}_{\mathbf{4}}$) the weak sector condition: $|\mathcal{E}[a,b]|^2\leq\mathcal{E}[a,a]\cdot\mathcal{E}[b,b]$

We consider a very important class of processes, that have correspondent in physics the dissipative systems (i.e. systems that evolve in time by increasing the energy).

Definition 1: An embedded process is called dissipative if $\leq_{|\mathbb{B}}=\preceq$.

In this section every process is supposed to be dissipative and all continuous observers to be additives.

In the following, we show that an embedded dissipative process can be embedded into an ordered group.

Let $\mathbb{A}\subset\mathbb{S}$ be a set such that $<\mathbb{A},\leq_{\mathbb{A}}>$ satisfies the axioms $(P_3)\div(P_7)$. Define $[\mathbb{A}]$, the group generated by $\mathbb{A}$, as follows.

1. We introduce on $\mathbb{A}\times\mathbb{A}$ the following equivalence relation

$$(a,b)\approx(a^{'},b^{'})\Leftrightarrow a\odot b^{'}=a^{'}\odot b.$$

2. We shall denote by $[\mathbb{A}]$ the quotient space of $\mathbb{A}\times\mathbb{A}$. For any $a,b\in\mathbb{A}$ we denote by $\widehat{(a,b)}$ the element of $[\mathbb{A}]$ generated by (a,b).

On $[\mathbb{A}]$ the following relations and operations can be defined:

- $\widehat{\perp}^{'}=:\widehat{(a,a)}$;
- $\widehat{(a,b)}\ \odot^{'}\ \widehat{(a^{'},b^{'})}=:\ \widehat{(a\odot a^{'},b\odot b^{'})}$; $\widehat{(a,b)}\ :^{'}\ \widehat{(a^{'},b^{'})}=:\widehat{(a,b)}\odot^{'}\widehat{(b^{'},a^{'})}$;
- $\widehat{(a,b)}\leq^{'}\widehat{(a^{'},b^{'})}$ if $a\odot b^{'}\leq a^{'}\odot b$;
- $\widehat{((a,b))}^{*}=:\widehat{(b,a)}$;
- $\widehat{(a,b)}\preceq^{'}\widehat{(a^{'},t^{'})}$ iff $\widehat{((a,b))}^{*}\preceq\widehat{((a^{'},b^{'}))^{*}}$;

Proposition 7: The map $a\to\widehat{a}=\widehat{(a,0)}$ is a one-to-one and ordered-preserving map of $\mathbb{A}$ into $[\mathbb{A}]_{\uparrow}=:\{\widehat{a}\in[\mathbb{A}];\widehat{a}\geq\perp\}$.

We can extend the energy to $[\mathbb{S}]\times[\mathbb{S}]$ by

$$\mathcal{E}[a:b,c:d]=\mathcal{E}[a,c]+\mathcal{E}[b,d]-\mathcal{E}[a,d]-\mathcal{E}[b,c].$$

The elements $a,b\in\mathbb{S}$ are called dual in energy (noted $a\in b^{\perp}_{\mathcal{E}}$) if $\mathcal{E}[a,b]=0$

Lemma 8: For any $a,b\in[\mathbb{S}]$

i) $\mathcal{E}[\perp]=0$; ii) $\mathcal{E}[a,\perp]=0$; iii) $\mathcal{E}[a]>0$ if $a\neq\perp$; iv) $\mathcal{E}[a^*]=\mathcal{E}[a]$;

v) $\mathcal{E}^{\frac{1}{2}}[a\odot b]\leq\mathcal{E}^{\frac{1}{2}}[a]+\mathcal{E}^{\frac{1}{2}}[b]$; vi) $\mathcal{E}[a\odot b]+\mathcal{E}[a:b]=2(\mathcal{E}[a]+\mathcal{E}[b])$;

An energy space is a structure $<[\mathbb{S}],\mathcal{E}>$ such that $[\mathbb{S}]$ is an extended space, $\mathcal{E}:\mathbb{S}\times\mathbb{S}\to\mathbb{R}$ is an energy and

(ES$_1$) $[\mathbb{S}]=\overline{[\mathbb{S}]}$;

(ES$_2$) $a\in b^{\perp}\Rightarrow a\in b^{\perp}_{\mathcal{E}}$, $(\forall a,b\in[\mathbb{S}])$.

The terms energy and energy space have been inspired by their use in the mathematical modelling world.

Example 3: Let $\overline{[\mathbb{S}]}$ be the class of all the spaces of excessive functions $\xi_{\mathcal{V}}$ of all sub-Markovian resolvents $\mathcal{V}$ which are in duality (with respect to a finite measure μ) and for which the initial kernels are proper. For any $\xi_{\mathcal{V}}$, $\xi_{\mathcal{W}}\subseteq\overline{[\mathbb{S}]}$ and $a\in\xi_{\mathcal{V}}$, $b\in\xi_{\mathcal{W}}$ define the mutual energy $\mathcal{E}[a,b]$ of a and b by

$$\mathcal{E}[a,b]=:\sup\{\int f\,W g\,d\mu\,;\,a,b\in\mathfrak{F},\,Vf\leq s,\;Wg\leq t\}\tag{10}$$

where V is the initial kernel for $\mathcal{V}$, W is the initial kernel for $\mathcal{W}$ and $\mathfrak{F}$ denotes the set of all $\mathfrak{B}$-measurable positive numerical functions on X, $(X,\mathfrak{B},\mu)$ being the measurable space.

Example 4: Let $\overline{[\mathbb{S}]}$ be the class of all absolute continuous functions f on (x,y) with $f^{'}\in L^2(x,y)$ and $f(x)=f(y)=0$. Define the mutual energy $\mathcal{E}[a,b]$ of a and b by $\mathcal{E}[a,b]=:\int_x^y a^{'}b^{'}dt$.

Definition 2: For any $a\in[\mathbb{S}]$ we shall call the regular form of a the element $\overline{a}\in\mathbb{B}$ defined by

$$\overline{a}=\bigwedge\{\beta\in\mathbb{B};a\leq^{'}(\beta,\perp)\}\tag{11}$$

Lemma 9: For any $a,b\in\mathbb{S}$

i)$\overline{a}\leq\overline{b}$ if $a\leq b$; ii) $\overline{a\odot b}\leq\overline{a}\odot\overline{b}$; iii) $\overline{(\overline{a})}=\overline{a}$;

iv) $(\overline{s_i})_{i\in I}\uparrow(\overline{s})$ if $(s_i)_{i\in I}\uparrow s$; v) $(\overline{s_i})_{i\in I}\downarrow(\overline{s})$ if $(s_i)_{i\in I}\downarrow s$.

Theorem 10: The space of basic occurrences $\mathbb{B}$ is a lower complete lattice in the specific order.

Proposition 11: If $\mathbb{A}\subset\mathbb{B}$ is an substructure which is dense in order from below and specifically solid then $\mathbb{A}$ is increasingly dense.

Proposition 12: If the subsets $\mathbb{A},\mathbb{A}^{'}\subset\mathbb{B}$ are solid and increasingly dense then $\mathbb{A}\cap\mathbb{A}^{'}$ is solid and increasingly dense.

Theorem 13: The structure $<[\mathbb{S}],\mathcal{E}>$ is an energy space iff $[\mathbb{S}]$ is closed in the energy topology and the energy $\mathcal{E}$ is a latticeal valuation.

An embedded process $\mathbb{B}$ is called a generalized process if there exists a map $\urcorner:\mathbb{B}\to\mathrm{Im}\,\mathbb{B}$ such that :

(W$_1$) $\urcorner[\alpha\odot\beta]=\urcorner[\alpha]+\urcorner[\beta]$, and

$\alpha\leq\beta\Leftrightarrow\urcorner[\alpha]\leq\urcorner[\beta]$, $(\forall\alpha,\beta\in\mathbb{B})$;

(W$_2$) $\urcorner[\mathbb{B}]$ is solid and increasingly dense in $Im\mathbb{B}$;

(W$_3$) $\urcorner[R(\alpha)]=\tilde{R}(\urcorner[\alpha])$, $(\forall\alpha\in\mathbb{B})$;

(W$_4$) for any two sweepings S and T on $\mathbb{B}$ such that $S\vee T=id_{\mathbb{B}}$ we have $S\circ T=T\circ S$.

The basic intuition behind a generalized process is that its atomic processes could be interpreted as the weak solutions (i.e. solutions in the sense distributions theory) of a very general classes of stochastic differential operators. The weak solutions always exist, despite the fact that, in the classical (computational) sense, the solutions may not exist or may not be computable.

Let $\mathcal{C}:\mathbb{B}\times\mathbb{B}\to\overline{\mathbb{R}}_+$ defined by $\mathcal{C}[\alpha,\beta]=\urcorner[\beta](\alpha)$. For any generalized process $\mathbb{B}$ define

$$\mathbb{B}^f=:\{\beta\in\mathbb{B};\mathcal{C}[\beta,\beta]<\infty\}$$

Lemma 14: The couple of observers $\mathcal{C}$ has the followings properties. For any $\alpha,\beta\in\mathbb{B}$, $(\alpha_i)_{i\in I}\uparrow\alpha$ and $cob\in\mathrm{Im}\,\mathbb{B}$; (i)$\alpha\leq\beta\Rightarrow\mathcal{C}[\sigma,\alpha]\leq\mathcal{C}[\sigma,\beta]$; (ii) $\bigvee_{i\in I}\mathcal{C}[\sigma,\alpha_i]=\mathcal{C}[\sigma,\alpha]$; (iii) For any there exists $\beta\in\mathbb{B}$: $cob(\alpha)=\mathcal{C}[\beta,\alpha]$

Corollary 15: The axioms W$_1$) W$_2$) are logical equivalent with the properties (i), (ii), (iii). The axiom W$_3$) is logical equivalent with the following property for any sweeping S on $\mathbb{B}$:

$$\mathcal{C}[S\alpha,\beta]=\mathcal{C}[\alpha,S\beta]$$

For any $\beta\in\mathbb{B}$ define $\mathbb{B}_\beta=:\{\alpha\in\mathbb{B}^f;\exists m,n\in\mathbb{N},\alpha^{(m)}\leq\beta^{(n)}\}$. Then $\mathbb{B}^f=\bigcup_{\beta\in\mathbb{B}^f}\mathbb{B}_\beta$.

Proposition 16: $\mathbb{B}^f$ is solid and increasingly dense in $\mathbb{B}$.

Lemma 17: $\mathbb{B}^f$ is a basic space if, for any $\beta^f\in[\mathbb{B}^f_\alpha]$ and $\alpha\in\mathbb{B}^f:\mathcal{C}[\beta^f,\beta^f]\geq 0$

Corollary 18: For any $\alpha,\beta\in\mathbb{B}$

$$\mathcal{C}[\alpha,\beta]+\mathcal{C}[\beta,\alpha]\leq\mathcal{C}[\alpha,\alpha]+\mathcal{C}[\beta,\beta]$$

and $\mathcal{C}[\alpha,\alpha]=0\Rightarrow\alpha=\perp$.

Let $\beta\in[\mathbb{B}^{'}]$, $\mathbb{B}^{'}\subseteq\mathbb{B}$ be solid in $\mathbb{B}$ with respect to the specific order and such that $\mathcal{C}[\beta]<\infty$, $\beta=\alpha:\alpha^{'}$, $\alpha:\alpha^{'}\in\mathbb{B}$ and $(\beta_n)_{n\in N}$ be the sequence defined by $\beta_1=\beta$, $\beta_{n+1}=\overline{\beta}_n:\beta_n$.

Lemma 19: We have $\mathcal{C}[\beta]=\sum_{n=1}^{\infty}\mathcal{C}[\overline{\beta}_n]$.

Lemma 20: Let $\mathbb{A}\subset\mathbb{B}$ a inferior semilattice, solid with respect the specific order and $\mathcal{C}[\alpha]<+\infty$, $(\forall\alpha\in\mathbb{A})$. If the couple of observers $\mathcal{C}$ is regular, then $\mathcal{C}[S_\alpha\sigma,\sigma^{'}]=\mathcal{C}[\sigma,S_\alpha\sigma^{'}]$, $(\forall\alpha\in[\mathbb{A}]_\uparrow,\,\forall\sigma,\sigma^{'}\in\mathbb{A})$.

Now we can formulate one the most important results of this work.

Theorem 21: Let $\mathbb{B}$ be a generalized process. Then $<[\mathbb{B}^f_\alpha],\mathcal{E}_{\mathcal{C}}>$ is an energy space, $(\forall\alpha\in[\mathbb{B}])$.

Proof.

We prove now condition (ES). We prove first

(SW) $S_\beta(\beta)=\beta$, for any $\beta\in[\mathbb{B}^f_\alpha]$.

Let S and T be two sweepings on $\mathbb{B}$ such that $S\vee T=id_{\mathbb{B}}$. Take $T=S^{'}$.We have then $S\circ S^{'}=S^{'}\circ S$ and therefore $S_\beta\circ S^{'}_\beta=S^{'}_\beta\circ S_\beta$, $(\forall\beta\in[\mathbb{B}^f_\alpha])$. We have $S_\beta(id_{\mathbb{B}}:S^{'}_\beta)=id_{\mathbb{B}}:S^{'}_\beta$.

Since $\beta\in Ker_{S^{'}_\beta}$ it follows $S_\beta(\beta)=\beta$, for any $\beta\in[\mathbb{B}^f_\alpha]$.

Let now $\alpha, \beta \in [\mathbb{B}^f_\alpha]$ be such that $\alpha \in \beta^\perp$. We have $\mathcal{E}_\mathcal{C}[\alpha, \beta] = \mathcal{E}_\mathcal{C}[S_\alpha\alpha, \beta] = \mathcal{E}_\mathcal{C}[S_\alpha\alpha, S_\alpha\beta] = \mathcal{E}_\mathcal{C}[S_\alpha\alpha, \perp] = 0$
so $\alpha \in \beta^\perp_{\mathcal{E}_\mathcal{C}}$.□

The map $\mathcal{E}_\mathcal{C} : [\mathbb{S}] \times [\mathbb{S}] \to R$ defined by

$$\mathcal{E}_\mathcal{C}[\alpha, \beta] =: \frac{\mathcal{C}[\alpha, \beta] + \mathcal{C}[\beta, \alpha]}{2}$$

is an energy which will be called the energy associated to the generalized process $\mathbb{B}$.

Therefore, to an integrated specification of an embedded system (semantically, a generalized process) we can associate an energy space, i.e. the main stochastic analysis tool [23].

VI. Related Work

The most relevant mathematical model to our approach constitutes the stochastic hybrid automata [7], [8]. Our model it is not a hybrid automaton, which consists of a set of continuous dynamical system and a discrete controller that commutes between them. The idea behind the stochastic embedded system model is that the environment plays the dominant role, and that, very often its evolutions can not be changed but only be observed. In the storm surge barrier example, the information collected about the environment is used to control a remote device and not the environment itself. In our model, the concept of location from hybrid automata is missing. The environment and the embedded controller actions are labels on the same set of events of an event structure.

A different model of Markov processes with multiform time is presented and developed in long series of papers, see for example [2] and the references therein. Computer networks inspire the model and therefore it is developed based on different guiding principles. The time in the definition of a Markov net is a poset, and the concurrent transitions are stochastic independent. This approach can be viewed as the classical dual of HFM: every line of a Markov net is a trajectory in the classical sense of Markov processes theory. Perhaps a true concurrent extension of stochastic hybrid systems is a more appropriate characterization of Markov nets.

An integration (called Phi-calculus) of the hybrid automata model with Pi-calculus is presented in [27]. The main difference relies on the system/environment emphasis. The classes of reactive systems we consider have behavior driven by the environment and therefore axiomatic modelling of real life environments plays a dominant role. In the Phi-calculus, the controller can change the environment by adding new (possibly continuous) constraints. Moreover, the models of the Phi-calculus are deterministic and operational.

A model of probabilistic systems with continuous state components is presented in [17]. In this model, although the state space can be continuous, the transitions are discrete.

VII. Conclusions

We have introduced a stochastic, multi-agent model for embedded systems. Every mobile agent observe a continuous phenomena from its physical environment and executes a communication for each observation. A mobile agent is defined formally as an embedded stochastic process, which is essentially a probabilistic event structure, decorated with continuous observations and a (variable) set of communication channel names. Each continuous observation is model of a formal specification in a newly introduced language, called the stochastic observability logic.

The stochastic observability logic is an attempt of specifying solutions of such models inspired by the mathematical practice. The key idea is to consider the largest class of functions having the known properties of the solutions (for example, functions that are Lebesgue squared integrable, right continuous, etc). The solutions are then characterized in this class of elements by axiomatic means or by advanced functional analysis methods like norm, Hilbert product, energy form, etc. The energy space we have introduced in the paper algebraically axiomatizes the energy methods originating from Hilbert and developed over a half of century in mathematical physics [22]. We have shown that for a class of systems called dissipative, every model of the stochastic observability logic specification of such systems has canonically associated an energy space (thus a Hilbertian functional analytic method).

The model introduced in this paper has the basic ingredients of a connectionist model, like neural networks [28]. In future work, we intend to explore issues like learning, adaptive behavior and self-management, with possible applications to robotics. It would be also interesting to explore this model in a categorical setting, like the stochastic relations [18], starting from our work [6], [13], [15].

More background material and examples can be found in the extended version of this paper, available on www[5].

Acknowledgments

This work was partly funded by the NWO Project AiSHA[6]. The first author would like to gratefully thank Prof. Feruccio Tiplea, for kind support and continuous encouragements offered in the early days of Hilbertean Formal Methods. The second author thanks Prof. Holger Hermanns and Dr. Rom Langerak, co-investigators at the AiSHA project.

References

[1] D. Aldous, J. Fill Reversible Markov Chains and Random Walks on Graphs. 1999. Available at www.stat.Berkeley.EDU/users/aldous.

[2] A. Benveniste, E. Fabre, S. Haar. Markov Nets: Probabilistic Models for distributed and concurrent systems. IEEE Transactions on Automatic Control 48(11):1936-1950, November 2003.

[5] http://wwwhome.cs.utwente.nl/~manuela/aisha/SOL.pdf

[6] http://wwwhome.cs.utwente.nl/~manuela/aisha/index.html

[3] E. Best, C. Fernandez "Non-Sequential Processes" EATCS Monograph in Theoretical Computer Science, Springer-Verlag, 1990.
[4] N. Boboc, G. Bucur, A. Cornea "Order and Convexity in Potential Theory. H-Cones" Lecture Notes in Math, vol 853, Springer Verlag, Berlin, 1981.
[5] M.L. Bujorianu, M.C.Bujorianu 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 4054, 2006.
[6] Bujorianu, M.L., Lygeros, J., Bujorianu, M.C.: Bisimulation for General Stochastic Hybrid Systems. In M. Morari and L. Thiele (Eds.), Proc. Hybrid Systems: Computation and Control, 8th International Workshop, Springer LNCS 3414, pp. 198-216, 2005.
[7] M.L Bujorianu. Extended Stochastic Hybrid Systems and their Reachability Problem. In R. Alur, G. Pappas Eds., Hybrid Systems: Computation and Control 7th International Workshop, HSCC'04, pp. 234-249, Springer LNCS vol. 2993, 2004.
[8] M.L. Bujorianu, M.C. Bujorianu: Distributed Stochastic Hybrid Systems. In Horacek P., Simandl M., Zitek P. (Eds.), "Proceedings of the 16th IFAC World Congres" 2005.
[9] M.C. Bujorianu, M.L. Bujorianu Towards Hilbertian Formal Methods Proc. of the 7th International Conference on Application of Concurrency to System Design ACSD, IEEE Press, 2007.
[10] M.C. Bujorianu, M.L. Bujorianu An integrated specification framework for embedded systems, Proc. of SEFM, IEEE Press, 2007.
[11] M.L. Bujorianu, M.C. Bujorianu: Multi-dimensional codesign: towards an integration paradigm Research Report, Department of Engineering, University of Cambridge, 2005.
[12] M.L. Bujorianu, J. Lygeros, R. Langerak Stochastic Reachability Analysis by Optimal Control HSCC 2008, in press.
[13] M.C. Bujorianu, M.L. Bujorianu, R. Langerak An Interpretation of Concurrent Hybrid Time Systems over Multiclock Systems Proc. of the 17th IFAC World Congress 2008, Elsevier, in press.
[14] M.L. Bujorianu, M.C. Bujorianu, H. Blom Approximate Abstractions of Stochastic Hybrid Systems Proc. of the 17th IFAC World Congress 2008, Elsevier, in press.
[15] M.C. Bujorianu, M.L. Bujorianu Towards a Formal Framework for Multi-Dimensional Codesign, submitted.
[16] Blumenthal, R.M., Getoor, R.K.: "Markov Processes and Potential Theory", Academic Press, 1968.
[17] S. Cattani, R. Segala, M. Kwiatkowska, G. Norman: Stochastic Transition Systems for Continuous State Spaces and Non-determinism. In Proc. of Fossacs, Springer LNCS 3441, (2005): 125–139.
[18] E.-E. Doberkat: "Stochastic Relations. Foundations for Markov Transition Systems." Chapman & Hall, New York, 2007.
[19] Design, Implementation and Adaptation of Sensor Networks through Multi-dimensional Co-design EPSRC Project EP/C014782/1 available as www.dcs.gla.ac.uk/dias/Files/CfS-Full-final.pdf
[20] L. Salo -Coste Lectures on finite Markov chains. Lectures on Probability Theory and Statistics. Ecole d' et e de probabilit es de Saint-Flour XXVI, Springer-Verlag Lecture Notes in Math. no. 1665, 1996.
[21] C. J. Fidge, I. J. Hayes, and B. P. Mahony. Defining differentiation and integration in Z. Second IEEE International Conference on Formal Engineering Methods (ICFEM'98), IEEE Computer Society Press, pp. 64-73, 1998.
[22] M. Fukushima Dirichlet forms, diffusion processes and spectral dimensions for nested fractals. In : "Ideas and methods in mathematical analysis, stochastics, and applications" Cambridge University Press, pp. 151-161, 1992.
[23] M. Fukushima "Dirichlet Forms and Markov Processes" North Holland, 1980.
[24] Hespanha, J.P., Tiwari, A. (Eds.): "Proc. Hybrid Systems: Computation and Control", 9th International Workshop, HSCC 2006, LNCS 3927 Springer 2006.
[25] J-P. Katoen Qualitative and Quantitative Extensions of Event Structures. Ph.D thesis, University of Twente, 1996.
[26] Meyer, P.-A.: "Probability and Potential". Blaisdell, Waltham Mass, (1966).
[27] Rounds W.C., Song H.: The Phi-Calculus: A Language for Distributed Control of Reconfigurable Embedded Systems. Proc of HSCC 2003, Springer LNCS 2623, (2003) 435-449.
[28] J. L. Shapiro. A solvable model of hard learning. In "Neural Networks, From Models to Applications." IDSET, 1988.
[29] D. Varacca, N. Yoshida Probabilistic pi-calculus and Event Structures Proc. of QAPL, 2007
[30] D. Varacca, H. Völzer, G. Winskel Probabilistic Event Structures and Domains Theoretical Computer Science 358(2-3), 2006
[31] BC Warboys e.a. Using a Reflective Pi-Calculus Based ADL to Create an Active Software Engineering Environment. , 2nd European Workshop on Software Architectures. 2005.

VIII. Appendix: Proofs

Proof of Proposition 4

Define $t_1 =: s \wedge s_1$ and $t_2 =: s : t_1$. It follows $t_1 \leq s_1$ and $t_2 = (s : s_1) \vee \perp$ so $t_2 \leq s_2$.□

Proof of Proposition 5

$a \leq_{\odot} b \Leftrightarrow \exists c \in \mathbb{S}$: $b = a \odot c \geq a \vee c \Rightarrow a \leq b$.□

Proof of Proposition 4

By Bergmann theorem it is enough to show that $a \wedge s = b \wedge s$ and $a \vee s = b \vee s$ imply $a = b$. But $a \odot s = (a \wedge s) \odot (a \vee s) = (b \wedge s) \odot (b \vee s) = b \odot s \Leftrightarrow a = b$. □

Proof of Proposition 6

We prove that the followings relations holds in any basic space:

($\mathbf{ID_1}$) for any increasing and dominated net $(s_i)_{i \in I} \subset \mathbb{S}$ and any $s \in \mathbb{S}$ we have

$$\bigvee_{i \in I} (s \odot s_i) = s \odot (\bigvee_{i \in I} s_i) \tag{12}$$

($\mathbf{ID_2}$) for any net $(s_i)_{i \in I} \subset \mathbb{S}$ and any $s \in \mathbb{S}$ we have

$$\bigwedge_{i \in I} (s \odot s_i) = s \odot (\bigwedge_{i \in I} s_i) \tag{13}$$

We prove first ($\mathbf{ID_2}$). We set $a =: \bigwedge_{i \in I} s_i$ and $b =: \bigwedge_{i \in I} (s \odot s_i)$. Observe that $s \odot a \leq b$. From $b \leq s \odot s_i$ we obtain $b : s \leq s_i$ $(\forall i \in I)$. Therefore

$b : s \leq a \Leftrightarrow b \leq s \odot a \Leftrightarrow \bigwedge_{i \in I} (s \odot s_i) = s \odot (\bigwedge_{i \in I} s_i)$. We prove now ($\mathbf{ID_1}$). We set $a =: \bigvee_{i \in I} s_i$ and $b =: \bigvee_{i \in I} (s \odot s_i)$. Observe that $s \odot a \geq b$. From $b \geq s \odot s_i$ we obtain $b : s \geq s_i$ $(\forall i \in I)$. Therefore

$b : s \geq a \Leftrightarrow b \geq s \odot a \Leftrightarrow \bigvee_{i \in I} (s \odot s_i) = s \odot (\bigvee_{i \in I} s_i)$.□

Proof of Lemma 9

i)Let $\mathbb{A} = \{\beta \in \mathbb{B} \ / \ a \leq^{'} (\beta, \perp)\}$ and $\mathbb{D} = \{\beta \in \mathbb{B} \ / \ b \leq^{'} (\beta, \perp)\}$. Then

$a \leq b \Rightarrow \mathbb{A} \supset \mathbb{D} \Leftrightarrow \bigwedge \mathbb{A} \leq \bigwedge \mathbb{D} \Leftrightarrow \overline{a} \leq \overline{b}$.

ii)Let $\mathbb{A} \odot \mathbb{D} = \{\beta \in \mathbb{B} \ / \ a \odot b \leq^{'} (\beta, \perp)\}$. Then

$\wedge(\mathbb{A} \odot \mathbb{D}) \leq (\wedge \mathbb{A}) \odot (\wedge \mathbb{D}) \Leftrightarrow \overline{a \odot b} \leq \overline{a} \odot \overline{b}$.

iii)-v) Results by direct calculations.□

Proof of Lemma 14

(i) Results from $\mathcal{C}[\sigma,\alpha] = \urcorner[\alpha](\sigma)$, $\mathcal{C}[s,\beta] = \urcorner[\beta](\sigma)$ and $\alpha \leq \beta \Leftrightarrow \urcorner[\alpha] \leq \urcorner[\beta]$. (ii) Results from $\bigvee_{i\in I} \mathcal{C}[\sigma,\alpha_i] = \urcorner[\bigvee_{i\in I} \alpha_i](\sigma)$, $\mathcal{C}[\bigvee_{i\in I} \alpha_i,\sigma] = \bigvee_{i\in I} \urcorner[\alpha_i](\sigma)$, and if $(cob_i)_{i\in I} \subset \mathrm{Im}\,\mathbb{B}$, $(cob_i)_{i\in I} \uparrow cob \in \mathrm{Im}\,\mathbb{B}$ then $cob[\sigma] = \bigvee_{i\in I} cob_i[\sigma]$. (iii) Follows from the fact that $\urcorner$ is a bijection.□

Proof of Proposition 11

Let $a, \beta \in \mathbb{A}$. Obviously $a \vee \beta \in \mathbb{A}$. Thus $\mathbb{A}$ satisfies the axioms of a basic space which is increasingly dense in $\mathbb{S}$.□

Proof of Proposition 12

Let $\alpha \in \mathbb{B}$ and denote $Y = \{x \in \mathbb{A} \cap \mathbb{A}^{'} / x \leq \alpha\}$ and for $y \in \mathbb{A}$ with $y \leq \alpha$ denote $Y_y = \{x^{'} \in \mathbb{A}^{'} / x^{'} \leq y\}$. Then $Y_y \subset Y$ and $\alpha \geq \bigvee Y \geq \bigvee_{y\in X,\, y\leq a} \bigvee Y_y = \alpha$. For any $y_1, y_2 \in Y$ there exists $x \in X$ such that $y_1 \leq x \leq a$ and $y_2 \leq x$. Since $\mathbb{A}^{'}$ is increasingly dense there exists $x^{'} \in X^{'}$ with $y_1 \leq x^{'} \leq x$ and $y_2 \leq x^{'}$. Obviously $x^{'} \in \mathbb{A}$ and therefore $x^{'} \in Y$.□