A Randomized Model for Communicating Embedded Systems

Marius C. Bujorianu and Manuela L. Bujorianu

Abstract—Nowadays, there is an intense research activity in designing systems that operate in real life, physical environments. This research is spanned by various areas in computer science and engineering: embedded systems, reactive systems, wireless communications, hybrid systems, stochastic processes, etc. A severe limitation in the development of these systems is due to the mathematical foundation and complexity of the physical environment. Often, the physical environment is continuous and uncertain, and modelled in terms of continuous stochastic processes. These mathematics are quite different from the underlying mathematics of discrete controllers based on logic and algebra. In this paper, we make further developments of Hilbertian formal methods, an integrated specification framework based with a rich algebraic semantics. This framework axiomatises and abstracts away advanced structures from functional and stochastic analysis. We integrate a probabilistic version of Pi-calculus to provide a rigorous framework for embedded systems with mobile and adaptive communication structure. The integration mechanism is based on partial ordered sets. The resulting framework has the modelling power of connectionist models like neural networks. Moreover, we construct an energy integral to every specification. The power of formal specification and stochastic analysis are combined in a rigorous mathematical framework for the software development of embedded systems. In this way, we achieve a new foundation for the multidimensional codesign.

Keywords: embedded systems, Markov processes, Pi-calculus, adaptive systems

I. INTRODUCTION

In this paper we present some development of two recently modelling paradigms, called *multi-dimensional codesign* [8] and *Hilbertian formal methods* (abbreviated HFM) [5], [6]. In multi-dimensional codesign, several system dimensions (or aspects) are considered simultaneously. This is the case in distributed embedded systems areas like sensor networks, gene regulatory networks, robotics, storm prevention systems, cardiac stimulators and medical applications. We approach this issue using HFM. In our case, the continuity of the environment is considered simultaneously with the discrete operation coupled with mobile, reconfiguring communication for the embedded controller.

We further investigate these issues for embedded controllers operating in a continuous and uncertain environment. Concretely, in this paper, we present three major contributions:

- A stochastic interpretation of Hil [6], the logic at the core of HFM,

- An integration of Hil with probabilistic Pi-calculus [13]. The integrated language can be used to describe the operations of the discrete controller in its continuous environment. Pi-calculus is the basic ingredient for many architecture description languages supporting dynamic reconfiguration and self-management, like ArchWare [14], Pi-SPACE and π -ADL.

- A mathematical construction that associates to each integrated specification an energy integral [10], an important tool of stochastic analysis.

The last contribution is a very difficult enterprise. It bridges formal methods and stochastic analysis in a new manner for building a robust foundation for software development of distributed embedded controllers with stochastic features.

A model of our integrated specification language is a multi-agent system, each agent evolving in a continuous, uncertain and change prone 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.

The paper is structured as follows. In the next section we present a practical motivation for our fundamental approach. In the section III we introduce the main mathematical notations and concepts. In section IV we define the modelling languages: a probabilistic Pi-calculus (for the discrete embedded controllers) and the Hil logic (for their physical environments). In the following section we show how these languages 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 VI. In the final section we draw some conclusions and discuss related and future work.

II. MOTIVATION

The explosive growth in microelectronics, biomedical implants, and ubiquitous computing raises challenges to formal methods that would have been hard to consider seriously a decade ago. Microprocessor, sensor networks and various controllers function now in the most unexpected physical environments. In medicine, there are electronic implants in the most sensitive parts of the human body like heart and brain. The bottom of the sea and the very remote windmills are monitored by sensor networks exhibiting complex behaviors like adaptivity, self-management, etc. If we considered wireless communications, robotics and the classical applications of hybrid systems (chemical industry, automotive systems, power and nuclear plants), this list would be even longer. A major characteristic of these systems is that they operate

This work was supported by the NWO project AiSHA
Marius C. Bujorianu is with CICADA, University of Manchester, UK.
This work was carried out before he joined CICADA.

Manuela L. Bujorianu is with Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, 7500 AE Enschede, The Netherlands L.M.Bujorianu@cs.utwente.nl

in a physical continuous environment, and the interaction with this environment can be complex. Traditionally, this class of applications has been associated with embedded systems. The research in embedded systems has focused mainly on real time constraints and resource limitations. 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 models. 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 will consider sophisticated environment representations. The main obstacles in using physical features in formal methods are due to the very 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.

III. MATHEMATICAL PRELIMINARIES

A. Markov models

Let $M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P, P_x)$ be a strong Markov process [9]. We suppose that the state space X is a Hausdorff space. The state space will be equipped with its Borel σ -algebra $\mathcal{B}(X)$.

In this paper, we suppose that all the Markov processes M used satisfy the following hypotheses.

1. The paths $t \rightarrow x_t(\omega)$ have the cadlag property,
2. X is a Lusin space.
3. The operator semigroup of M maps $\mathbf{B}(X)$ into itself.

The hHypotheses 2., 3. mean that M is a Borel process [9].

We use the following concepts:

- The set $\mathbf{B}(X)$ is the lattice of bounded real measurable functions defined on X .
- The semigroup of operators is given by $P_t f(x) = E_x f(x_t) = \int f(y) p_t(x, dy), t \geq 0$ 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. $p_t(x, A) = P_x(x_t \in A)$.

• Using the semigroup of operators, one can define the *kernel operator* $Vf = \int_0^\infty P_t f dt$, $f \in \mathbf{B}(X)$ and then the set of *excessive functions*, i.e. $\mathcal{E}_M = \{Vf | f \in \mathbf{B}(X); f \geq 0\}$

B. Lattices and event structures

A *conditionally complete lattice* is a lattice such that every non-void bounded subset has a least upper bound and a greatest lower bound.

If $(B, \prec)$ is a lattice, then a set $M \subset B$ is an *ideal* if it is *solid*, i.e. $a \in M$ and $b \prec a$, then $b \in M$.

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

A *labelled event structure* $\mathcal{E}$ is given by $\mathbb{E} = (E, \preceq, \#, Act, l)$ with:

- (i) E a set of events; (ii) $\preceq$ is a causal order
- (iii) $\# \subseteq E \times E$, the irreflexive and symmetric conflict relation;
- (iv) $l : E \rightarrow Act$, the action-labelling function;

A partial cell is a set of events that are pairwise in conflict and have the same enabling sets [13]. 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 $p : F \rightarrow [0, 1]$ such that, for every $c \in G : \sum_{e \in c} p(e) = 1$. A *probabilistic event structure* is partial probabilistic event structure with $F = E$.

IV. THE SPECIFICATION LOGIC FOR THE ENVIRONMENT

We start with a specification language that offers support for continuous mathematics primitives, like reals, continuous functions, differentiable or integrable functions.

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

$$f := \mathbf{1} \mid \perp \mid \top \mid f \odot f \mid f : f \mid f \wedge f \mid f \vee f \mid V.f \mid \sup_{n \in \mathbb{N}} V.f_n$$

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 $\odot$.

- $\wedge, \vee$ represent the usual lattice operations.
- V represents a modality, in this case, associated with the kernel operator V .

The formulas are defined as equalities or inequalities between terms. The formulas involving terms of the form $\sup_{n \in \mathbb{N}} V.f_n$ are called trace formulas.

The stochastic interpretation is constructed as follows.

We consider the Markov process

$$M = (\Omega, \mathcal{F}, \mathcal{F}_t, x_t, P_x),$$

as in subsection III-A, the interpretation of an $f \in F$ is a function $f : X \rightarrow \mathbb{R}$ which belongs to $\mathbf{B}(X)$. Then

$$\begin{aligned} 1(x) &:= 1, \perp(x) := 0, \forall x \in X \\ \top(x) &:= \infty, \text{ where } \infty \text{ is a large enough constant} \\ (f \odot g)(x) &:= f(x) + g(x) \\ (f : g)(x) &:= \begin{cases} f(x) - g(x) & , \text{ if } f(x) \geq g(x) \\ 0 & , \text{ otherwise} \end{cases} \\ (V.f)(x) &:= \int [\int_0^\infty f(x_t(\omega)) dt] P_x(d\omega) \end{aligned}$$

The elements of $\mathbf{B}(X)$ can be thought of as *terms*.

Now we succinctly present an abstract, algebraic semantics.

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

(S₁) $\langle \mathbb{S}, \leq, \perp, \top \rangle$ is a lattice for which:

- $\perp$ the minimal element and $\top$ the greatest element;
- the lattice $(\mathbb{S} \setminus \{\top\}, \leq_{\mathbb{S} \setminus \{\top\}}, \perp)$ is lower complete and upper conditionally complete;

(S₂) $(\mathbb{S}, \odot, \perp)$ is a monoid for which:

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

(S₃) the following compatibility axioms hold:

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

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 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 **P1** – **P8** from subsection V.B.

V. INTEGRATED SPECIFICATION OF EMBEDDED PROCESSES

A. The probabilistic Pi-calculus

We consider the probabilistic extension of Pi-calculus considered in [13]. The language has two equivalent semantics, operational (in terms of Segala automata) and denotational (based on event structures).

The syntax

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

As usual, $!x(\tilde{y}).P$ denotes the replicated input, $(\nu x)P$ is the restriction, $P|Q$ is the parallel composition and $x\Phi_{i \in I} \text{in}_i(\tilde{y}_i).P_i$ denotes the branching input. The process

$$\begin{aligned} \llbracket 0 \triangleright x_i : (\tau_i)^?, y_j : \tau_j \rrbracket^\rho &= \emptyset \\ \llbracket (\nu x)P \triangleright \Gamma \rrbracket^\rho &= \llbracket P \triangleright \Gamma, x : \tau \rrbracket^\rho \setminus x \\ \llbracket P_1 \parallel P_2 \triangleright \Gamma_1 \odot \Gamma_2 \rrbracket^{\rho_1 \cup \rho_2} &= \\ &= (\llbracket P_1 \triangleright \Gamma_1 \rrbracket^{\rho_1} \parallel \llbracket P_2 \triangleright \Gamma_2 \rrbracket^{\rho_2}) \setminus S \\ \llbracket x \oplus_{i \in I} \text{in}_i(\tilde{y}_i).P_i \triangleright \Gamma, x : \oplus_{i \in I} (\tau_i)^! \rrbracket^{\rho, (\tilde{y}_i \rightarrow \tilde{z}_i)_{i \in I}} &= \\ &= \sum_{i \in I} \overline{x} \text{in}_i(\tilde{z}_i). \llbracket P_i[\tilde{z}_i/\tilde{y}_i] \triangleright \Gamma, \tilde{z}_i : \tau_i \rrbracket^\rho \\ \llbracket x \Phi_{i \in I} p_i \text{in}_i(\tilde{y}_i).P_i \triangleright \Gamma, x : \Phi_{i \in I} (\tau_i)^! \rrbracket^{\rho, (\tilde{y}_i \rightarrow \tilde{z}_i)_{i \in I}} &= \\ &= \sum_{i \in I} p_i \overline{x} \text{in}_i(\tilde{z}_i). \llbracket P_i[\tilde{z}_i/\tilde{y}_i] \triangleright \Gamma, \tilde{z}_i : \tau_i \rrbracket^\rho \\ \llbracket !x(\tilde{y}).P \triangleright \Gamma, x : (\tilde{\tau})^! \rrbracket^{\rho[K], \tilde{y} \rightarrow \{\tilde{y}_k\}_{k \in K}} &= \\ &= \prod_{k \in K} \overline{x}(\tilde{y}^k). \llbracket P \triangleright \Gamma \rrbracket^{\rho[\tilde{y}^k/\tilde{y}]}[Y^k/Y] \\ \llbracket \overline{x}(\tilde{y}).P \triangleright \Gamma, x : (\tilde{\tau})^? \rrbracket^{\rho, \tilde{y} \rightarrow \tilde{z}} &= \\ &= \overline{x}(\tilde{z}). \llbracket P \triangleright \Gamma, x : (\tilde{\tau})^?[\tilde{z}/\tilde{y}] \rrbracket^\rho \end{aligned}$$

Fig. 1.

$x \oplus_{i \in I} p_i \text{in}_i(\tilde{y}_i).P_i$ represents the probabilistic version of selecting output. The values $p_i \in [0, 1]$ represent the probabilities ($\sum_{i \in I} p_i = 1$) associated with the events.

The causal order semantics

We use the semantics introduced in [13], based on probabilistic event structures.

Because the probabilistic π -calculus terms are identified up to α -conversion (thus the identity of bound terms is not relevant) while in typed partial probabilistic event structure the identity of the object name is important, 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 π -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 [13]).

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 ($a \leq b$ 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. Markov processes are studied using tools specific to stochastic analysis, like excessive functions

[2] and Dirichlet forms [10]. Two system evolutions a, b that are causal independent (i.e. $a \not\prec b$ nor $b \not\prec a$) can take place simultaneously (*true concurrency*).

B. Stochastic embedded processes

In this subsection, 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.

An *event space* is a structure $\langle \mathbb{M}, \preceq, \#, Act, l, p \rangle$ such that

- (M₀) $\mathcal{E} = (\mathbb{M}, \preceq, \#, Act, l)$ is a probabilistic event structure.
- (M₁) $\langle \mathbb{M}, \preceq \rangle$ is a lower complete semi-lattice. The order $\preceq$ is called the *causal order*. We note by $\wedge$ (resp. $\vee$) the *infimum* (resp. *supremum* if exists) of this semi-lattice and
- (M₂) if $(\alpha_i)_{i \in I}$ is increasing and dominated in $\mathbb{M}$ by α , $\alpha \in \mathbb{M}$, then there exists $\bigvee_{i \in I} \alpha_i$.

The elements of Act denote the agent communications.

A *stochastic embedded process* is a three-tuple $\langle \mathcal{E}, \mathcal{S}, \ell \rangle$, where $\mathcal{E} = \langle \mathbb{M}, \preceq, \#, Act, l \rangle$ is a probabilistic event space, $\mathcal{S} = \langle \mathbb{S}, \leq, \perp, \top, \odot \rangle$ is a basic space and $\ell : \mathbb{M} \rightarrow \mathbb{S}$ is an injective isotone labelling function such that, if $\mathbb{B} = \ell(\mathbb{M})$ then:

- (P₁) $\ell(\alpha \vee \beta) \geq \ell(\alpha) \vee \ell(\beta)$ if $\alpha \vee \beta$ exists
- (P₂) if $\ell(\alpha \vee \beta) = \top$ and $\gamma \succ \alpha \vee \beta$ then $\ell(\gamma) = \top$
- (P₃) $\perp \in \mathbb{B}$
- (P₄) $\langle \mathbb{B}, \leq_{\mathbb{B}}, \wedge \rangle$ is a lower complete semi-lattice of $\langle \mathbb{S}, \leq \rangle$
- (P₅) $\mathbb{B}$ is linearisable;
- (P₆) $(\mathbb{B}, \odot, \perp)$ is a monoid;
- (P₇) The superposition is continuous in the order topology on $\mathbb{B}$;
- (P₈) $\mathbb{B}$ 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.

In the following we describe informally three examples of embedded processes.

Example 1: 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 $\preceq$.

Example 2: An important class of examples constitute the *storm surge barriers*, like the Oosterscheldekering storm surge barrier¹ on the Rhine-Meuse Delta and the Maeslant storm surge barrier² (near Rotterdam). The both systems are placed in the south 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 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 3: Another suitable example of stochastic embedded process can be obtained by randomization of the *bucket brigade* example from [11]. 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.

VI. 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 [10]. These are the key concepts in the formal verification of stochastic hybrid systems [4], [7].

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

$$(EN_1) \mathcal{E}[a \odot b, s] = \mathcal{E}[a, s] + \mathcal{E}[b, s]$$

$$(EN_2) \mathcal{E}[a, b] = \mathcal{E}[b, a]$$

$$(EN_3) \mathcal{E}[s] > 0 \text{ if } s \neq \perp,$$

$$(EN_4) \mathcal{E}[a, b]^2 \leq \mathcal{E}[a, a] \cdot \mathcal{E}[b, b]$$

We define the energy metric $d : [\mathbb{S}] \times [\mathbb{S}] \rightarrow \mathbb{R}_+$ by

$$d(f, g) = \begin{cases} \mathcal{E}^{\frac{1}{2}}[f : g], & \text{if } f, g \in \mathbb{S} \\ \mathcal{E}^{\frac{1}{2}}[(u \odot v') : (v \odot u')], & \end{cases}$$

if $f, g \in [\mathbb{S}]$, $f = (u, v)$, $g = (u', v')$. We define the energy topology τ_d on $[\mathbb{S}]$ as $(f_n)_{n \in \mathbb{N}} \xrightarrow{\tau_d} f$ iff $(d(f_n, g))_{n \in \mathbb{N}} \xrightarrow{\mathbb{R}} 0$.

Proposition 1: The energy topology is a Hausdorff topology.

We denote by $\overline{[\mathbb{S}]}$ the completion of $[\mathbb{S}]$ in the energy topology.

¹http://en.wikipedia.org/wiki/Delta_Works

²http://www.keringhuis.nl/engels/home_flash.html

The energy $\mathcal{E}$ can be extended to $\overline{[\mathbb{S}]}$ by $\mathcal{E}[f, g] = \lim_{n \rightarrow \infty} \mathcal{E}[f_n, g_n]$, $(f, g \in \overline{[\mathbb{S}]})$, where $(f_n) \rightarrow f$, $(g_n) \rightarrow g$, $(f_n) \subset [\mathbb{S}]$, $(g_n) \subset [\mathbb{S}]$.

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.

An energy space is a structure $\langle [\mathbb{S}], \mathcal{E} \rangle$ such that $[\mathbb{S}]$ is an extended space, $\mathcal{E} : \mathbb{S} \times \mathbb{S} \rightarrow \mathbb{R}$ is an energy and $[\mathbb{S}] = \overline{[\mathbb{S}]}$.

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 $\mathcal{E}[a, b] =: \int_a^b a' b' dt$.

Example 5: Let $D \subset \mathbb{R}^n$ be Greenian set (with the Green function G) and let $\overline{[\mathbb{S}]}$ be the class of all Borel measures on D . The mutual energy $\mathcal{E}[f, g]$ of two measures $f' = \mu, g' = \nu$, $f', g' \in \overline{[\mathbb{S}]}$ is defined by $\mathcal{E}'[f', g'] =: \int \int G(x, y) d\mu(x) d\nu(y)$;

Denote $f(x) =: \int G(x, y) d\mu(y)$, $g(x) =: \int G(x, y) d\nu(y)$. There exists resolvents $\mathcal{V}, \mathcal{W}$ which are in duality (with respect to a finite measure μ), such that $f \in \xi_{\mathcal{V}}, g \in \xi_{\mathcal{W}}$ and $\mathcal{E}[f, g] = \mathcal{E}'[f', g']$.

Theorem 2: The structure $\langle [\mathbb{S}], \mathcal{E} \rangle$ is an energy space iff $[\mathbb{S}]$ is closed in the energy topology and the energy $\mathcal{E}$ is a latticeal valuation [3].

Proposition 3: The energy metric is translation invariant.

Proposition 4: The superposition is continuous in the energy topology.

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

(CO₁) $\alpha \prec \beta \Rightarrow cob(\alpha) \leq cob(\beta)$, $(\forall \alpha, \beta \in \mathbb{B})$;

(CO₂) $cob(\beta) = \sup_{i \in I} (cob(\beta_i))$ if $(\beta_i)_{i \in I} \uparrow \beta$;

(CO₃) $(\forall \beta \in \mathbb{B}) (\exists (\beta_i)_{i \in I} \uparrow \beta) : cob(\beta_i) < \infty$.

The *process image* is $Im\mathbb{B} = \{cob : \mathbb{B} \rightarrow \overline{\mathbb{R}}_+; cob \text{ is an additive continuous observer}\}$.

An embedded process $\mathbb{B}$ is called *observable* if there exists a map $\top : \mathbb{B} \rightarrow Im\mathbb{B}$ such that :

(W₁) $\top[\alpha \odot \beta] = \top[\alpha] + \top[\beta]$, and

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

(W₂) $\top[\mathbb{B}]$ is solid [3] and increasingly dense [3] in $Im\mathbb{B}$;

(W₃) $\top[R(\alpha)] = \bar{R}(\top[\alpha])$, $(\forall \alpha \in \mathbb{B})$;

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 $\mathcal{C} : \mathbb{B} \times \mathbb{B} \rightarrow \overline{\mathbb{R}}_+$ defined by $\mathcal{C}[\alpha, \beta] = \top[\beta](\alpha)$. For any generalized process $\mathbb{B}$ define $\mathbb{B}^f =: \{\beta \in \mathbb{B}; \mathcal{C}[\beta, \beta] <$

$\infty\}$. 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 $\mathbb{B}^f = \bigcup_{\beta \in \mathbb{B}^f} \mathbb{B}_\beta$.

Theorem 5: Let $\mathbb{B}$ be a generalized process. Then $\langle [\mathbb{B}_\alpha^f], \mathcal{E}_\mathcal{C} \rangle$ is an energy space, $(\forall \alpha \in [\mathbb{B}])$.

The map $\mathcal{E}_\mathcal{C} : [\mathbb{S}] \times [\mathbb{S}] \rightarrow \mathbb{R}$ defined by $\mathcal{E}_\mathcal{C}[\alpha, \beta] =: \frac{1}{2}(\mathcal{C}[\alpha, \beta] + \mathcal{C}[\beta, \alpha])$ 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 [10].

In the following we define the concepts of *system* and its associated embedded process.

Definition 2: A system is a map $\Gamma : \overline{[\mathbb{S}]} \rightarrow \overline{[\mathbb{S}]}$ such that

(S₁) $\Gamma[a \odot b] = \Gamma[a] \odot \Gamma[b]$;

(S₂) Γ is continuous in τ_d ;

(S₃) there exists $m = m_\Gamma \in \mathbb{R}_+$ such that

$$\frac{1}{m} \cdot \mathcal{E}[a] \leq \mathcal{E}[\Gamma a] \leq m \cdot \mathcal{E}[a], \quad (\forall a \in \overline{[\mathbb{S}]})$$

(S₄) $\Gamma[\mathbb{B}]$ is dense in $\overline{[\mathbb{S}]}$;

(S₅) $\mathcal{E}[a, b] = \frac{\mathcal{E}[\Gamma a, b] + \mathcal{E}[a, \Gamma b]}{2}$.

Definition 3: For any system Γ we can associate its Γ -energy $\mathcal{E}_\Gamma$ defined by

$$\mathcal{E}_\Gamma[a, b] = \mathcal{E}[\Gamma a, b].$$

Definition 4: For any system Γ define the space

$$[\mathbb{B}_\Gamma] =: \{\alpha \in \overline{[\mathbb{S}]}; \mathcal{E}_\Gamma[\alpha, s] \geq 0, \forall s \in \overline{[\mathbb{S}]}_\top\}$$

named the *embedded process* associated to the system Γ (or the Γ -embedded process).

In the following we investigate the energetic properties of systems.

Theorem 6: The lattice operations $\vee$ and $\wedge$ are continuous in the Γ -energy topology.

For any $s \in [\mathbb{S}]$ define the energy reduction $\underline{s} \in [\mathbb{B}_\Gamma]$ as the unique element which satisfy $\mathcal{E}_\Gamma[s : \underline{s}, \underline{s}] = 0$. The next two results establish algebraic properties of the energy reduction.

Proposition 7: The following property $\mathcal{E}_\Gamma[\underline{s}] \leq \mathcal{E}_\Gamma[s \odot t]$ holds $(\forall t \in \overline{[\mathbb{S}]}_\top)$;

Proposition 8: $\underline{s} = \bar{s}$ for any $s \in \overline{[\mathbb{S}]}$.

The following results give sufficient conditions for the convergence in the energy topology.

Proposition 9: Any increasing and dominated net is τ_d convergent.

Proposition 10: Any decreasing net is τ_d convergent.

For any set $A \subset [\mathbb{S}]$ we define its polar A° by $A^\circ =: \{s \in A^\circ; \mathcal{E}_\Gamma[a, s] \leq 0, \forall a \in A\}$.

Proposition 11: The energy $\mathcal{E}_\Gamma$ is isotone on $[\mathbb{B}_\Gamma]$.

The following result show that the embedded processes can be completely investigated using the energy.

Theorem 12: Any Γ -embedded process is uniquely determined by its energy.

Proposition 13: The following property holds $\overline{[\mathbb{B}_\Gamma]} = \overline{[\mathbb{S}]}$.

For $\hat{s} \in \overline{[\mathbb{S}]}$ let us define $\hat{s}_\top = \hat{s} \vee_{\overline{[\mathbb{S}]}} 0$, $\hat{s}_\downarrow = (\perp : \hat{s}) \vee_{\overline{[\mathbb{S}]}} 0$, $\hat{s}_\top = \hat{s}_\top \odot \hat{s}_\downarrow$.

Proposition 14: For any system Γ the space $\mathbb{B}_\Gamma =: [\mathbb{B}_\Gamma]_\uparrow$ is an embedded process.

Proposition 15: We have $\alpha : \overline{(\alpha : \beta)} \in \mathbb{B}_\Gamma$, $(\forall \alpha, \beta \in \mathbb{B}_\Gamma)$.

Define $[\mathbb{S}]^\sigma =: \text{Ker} \sigma$, $\sigma^S =: \text{Ker} \sigma \cap \mathbb{S}$ and $\Gamma_\sigma =: \Gamma_{[\mathbb{S}]^\sigma}$. The structure $\langle [\mathbb{S}]^\sigma, \mathcal{E}_\Gamma \rangle$ is the energetic space associated to the system Γ_σ .

Proposition 16: The following properties are valid

i) $\mathbb{B}^\sigma$ is solid in the Γ_σ – embedded process $\mathbb{B}_{\Gamma_\sigma}$;

ii) for any $\beta \in \mathbb{B}_{\Gamma_\sigma}$ there exists a sequence $(\beta_n)_{n \in \mathbb{N}} \subset \mathbb{B}^\sigma$

such that $\beta = \bigodot_{n=1}^\infty \beta_n$;

iii) for any $\alpha \in [\mathbb{S}]^\sigma$ such that $\beta \in \mathbb{B}^\sigma \Rightarrow \alpha \wedge \beta \in \mathbb{B}^\sigma$ we have $\alpha \in \mathbb{B}_{\Gamma_\sigma}$;

iv) for any $\beta \in \mathbb{B}$ and any $\alpha \in \mathbb{B}_{\Gamma_\sigma}$ we have $\alpha \wedge \beta \in \mathbb{B}_{\Gamma_\sigma}$.

Example 6: The Laplacian Δ is defined on all of $L^2(V; dx)$ in the sense of Schwartz distributions. Then $\Gamma =: \frac{1}{2}\Delta$ with domain $\{u \in H_0^{1,2}(V) \mid \Delta u \in L^2(V; dx)\}$ is the system corresponding to $\langle \mathcal{E}, [\mathbb{B}] = H_0^{1,2}(V) \rangle$ on $[\mathbb{S}] = L^2(V; dx)$.

Example 7: Let $m = dx$ and let “.” resp. “.” denote Fourier transform, i.e. $f(x) = (2\pi)^{-n/2} \int \exp[i \langle x, y \rangle] f(y) dy$, resp. its inverse. Define for $0 < u \leq 1$: $(-\Delta)^u f := (|x|^{2u} \hat{u})$ ($\in L^2(\mathbb{R}^n; dx)$); $f \in C_0^\infty(\mathbb{R}^n)$. Then $(-\Delta)^u$ is a system on $[\mathbb{S}] =: L^2(\mathbb{R}^n; dx)$ with dense basic space $[\mathbb{B}] =: C_0^\infty(\mathbb{R}^n)$. Define the energy $\mathcal{E}_{(-\Delta)^u}^{(u)}$

$$\mathcal{E}_{(-\Delta)^u}^{(u)}[f, g] =: \frac{1}{2} \int \hat{u} \bar{\hat{v}} |x|^{2u} dx ; (f, g \in C_0^\infty(\mathbb{R}^n))$$

where “.” means complex conjugation. Its closure $\langle \mathcal{E}_{(-\Delta)^u}^{(u)}, [\mathbb{B}] =: H^{u,2}(\mathbb{R}^n) \rangle$ is hence a symmetric closed form on $[\mathbb{S}] =: L^2(\mathbb{R}^n; dx)$.

VII. FINAL REMARKS

We have introduced a stochastic, multi-agent model for embedded systems, in the context of multi-dimensional codesign [8]. Every mobile agent observes 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.

The contribution of this paper makes possible to study adaptive systems and reconfiguration capabilities in *Hilbertian formal methods* [5], [6], a modeling paradigm for embedded systems, introduced by the authors.

The most relevant mathematical model for our approach constitutes the stochastic hybrid automata (see [4] and the references therein). Our model 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 discrete location (mode) from hybrid automata is missing. The environment and the embedded controller actions are labels on the same set of events of an event structure.

An integration (called Phi-calculus) of the hybrid automata model with Pi-calculus is presented in [11]. 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.

The model introduced in this paper has the basic ingredients of a connectionist model, like neural networks [12]. In future work, we intend to explore issues like learning, adaptive behavior and self-management, with possible applications to robotics.

More examples and the omitted proofs can be found in an extended version [3] of this paper.

REFERENCES

- [1] E. Best and C. Fernandez, *Non-Sequential Processes* Springer Verlag, 1990.
- [2] N. Boboc, G. Bucur and A. Cornea, *Order and Convexity in Potential Theory. H-Cones* Lecture Notes in Math, vol 853, Springer, 1981.
- [3] M.L. Bujorianu and M.C. Bujorianu, “A Randomized Model for Communicating Embedded Systems” Technical Report TR-CTIT-08-22 Centre for Telematics and Information Technology, University of Twente, 2008.
- [4] M.L. Bujorianu, “Extended Stochastic Hybrid Systems and their Reachability Problem” In R. Alur, G. Pappas Eds., *Hybrid Systems: Computation and Control HSCC’04*, pp. 234-249, Springer LNCS vol. 2993, 2004.
- [5] M.C. Bujorianu and M.L. Bujorianu, “Towards Hilbertian Formal Methods” *Proc. of ACSQ, Conf. on Application of Concurrency to System Design*, IEEE Press, 2007.
- [6] M.C. Bujorianu and M.L. Bujorianu, “An integrated specification framework for embedded systems” *Proc. of SEFM*, IEEE Press, 2007.
- [7] M.L. Bujorianu, H.A.P. Blom, H. Hermanns, “Functional Abstractions of Stochastic Hybrid System” In *Proc. of IFAC Conference Analysis and Design of Hybrid Systems ADHS’06*, pp. 160-165, 2006.
- [8] M.L. Bujorianu and M.C. Bujorianu, “Towards a Formal Framework for Multidimensional Codesign” Technical Report TR-CTIT-08-21 Centre for Telematics and Information Technology, University of Twente, 2008.
- [9] R.M. Blumenthal and R.K. Getoor, *Markov Processes and Potential Theory*, Academic Press, 1968.
- [10] M. Fukushima, *Dirichlet Forms and Markov Processes* North Holland, 1980.
- [11] W.C. Rounds and H. Song, “The Phi-Calculus: A Language for Distributed Control of Reconfigurable Embedded Systems” *Proc of HSCC*, Springer LNCS 2623, pp. 435-449, 2003.
- [12] J. L. Shapiro, “A solvable model of hard learning” In *Neural Networks, From Models to Applications*. IDSET, 1988.
- [13] D. Varacca and N. Yoshida, “Probabilistic pi-calculus and Event Structures” *Proc. of QAPL*, 2007.
- [14] B.C. Warboys e.a., “Using a Reflective Pi-Calculus Based ADL to Create an Active Software Engineering Environment” 2nd European Workshop on Software Architectures, 2005.