Towards Co-Engineering Communicating Autonomous Cyber-physical Systems

Marius C. Bujorianu and Manuela L. Bujorianu[*]
[Marius,Manuela].Bujorianu@manchester.ac.uk
School of Mathematics, University of Manchester, UK

Abstract

In this paper, we sketch a framework for interdisciplinary modeling of space systems, by proposing a holistic view. We consider different system dimensions and their interaction. Specifically, we study the interactions between computation, physics, communication, uncertainty and autonomy. The most comprehensive computational paradigm that supports a holistic perspective on autonomous space systems is given by cyber-physical systems. For these, the state of art consists of collaborating multi-engineering efforts that prompt for an adequate formal foundation. To achieve this, we propose a leveraging of the traditional content of formal modeling by a co-engineering process.

Keywords: *cyber-physical systems, uncertainty, degrees of autonomy, communication, formal modeling, structured operational semantics, system co-engineering.*

1 The need for holistic modeling

Many systems from aerospace engineering can be characterized as been *cyber-physical*, i.e. their dynamics is based on the interaction between *physics* and *computation* and they are networked. Satellites, aircraft, planetary rovers are instants of cyber-physical systems (CPS). In the process of formal modeling of these systems, a developer should consider actually consider the interactions between *communication*, physics and computation. We sketch a reference framework, where the subtleties of these interactions can be captured. Moreover, we add a further dimension to these complex interactions by adding *uncertainty*. However, the special conditions in which the space systems are deployed require also a high degree of *autonomy*, adding an extra-dimension to system modeling. We approach the issue of mastering the interactions of many system dimensions for complex space systems by integrating formal modeling into a larger system development process called *system co-engineering*. Instances of this process are the *Hilbertean formal methods* [2] and the *multidimensional system co-engineering* (MScE) framework [1].

Autonomous systems can be modeled from two perspectives: *black box* and *white box*. The black box view is specific to the approaches based on *hybrid dynamical systems*. In these approaches, the system behavior is described as seen by an *external observer*. This observer records a sequence of continuous behaviors, each one triggered by a discrete transition (event). In our model, there are two types of discrete transitions: *controlled*, which are the transitions of a discrete automaton, and *spontaneous* (or *autonomous*), which are transitions that can not be explained using only the elements of the model. The systems with spontaneous transitions are called *uncertain*, and they are usually modeled as random processes. Using *structured operational semantics* (SOS), some spontaneous transitions can be defined as a special class of controlled transitions that are triggered by communication. In this way, communication reduces the randomness of the model. In the white box view, some of the internal system structure is revealed. In our framework, we explain the interaction between communication, autonomy and control using the concept of *nested feedback*. The feedback is the fundamental structure of the controlled systems, constructed by connecting some input and output channels. A nested feedback results from adding a feedback loop to a system that has already another feedback in its structure. When applying this concept to CPS, one can easily distinguish a subclass known as *hierarchical hybrid systems* [6]. We define and use nested feedbacks to explain the autonomy and its interaction with communication. Specifically, as more nested feedbacks are added, the system autonomy increases. A system with four nested feedbacks

E. Denney, D. Giannakopoulou, C.S. Păsăreanu (eds.); The First NASA Formal Methods Symposium, pp. 176-180

[*]This work was funded by the CICADA project under the EPSRC grant EP/E050441/1.

can be considered as fully autonomous because it has enough *information structure* to partially control itself. Systems with five nested feedbacks or more have additional features like *concurrency* and *self-* properties* (self-reconfiguration, self-healing, etc). In a hierarchy of nested feedbacks, communication is defined as the top loop. In this way, the whole behavior of the cyber-physical system is controlled via communication. A rigorous study of autonomy and communication in a cyber-physical context goes beyond the traditional content of formal methods, in a form of an interdisciplinary paradigm that we call *system co-engineering* (see [1] and the references therein). Co-engineering is a creative process combining concepts and techniques from two different scientific disciplines. In our approach, the system co-engineering is *multi-dimensional*, integrating *formal engineering*, *control engineering*, and *mathematical engineering*. The integration process departs from a mathematical model of complex systems called *stochastic hybrid processes* (SHS) [3].

2 Cyber-physical systems: autonomy and communication

Designing safe autonomous space systems requires accurate and holistic models, where all interactions between orthogonal system features can be understood. In a formal approach, the first step will be to define formal models for which these interactions can be mathematically studied. Such systems would involve digital control of some devices with continuous dynamics and embedded in a physical environment. They are also uncertain in the sense that they are subject to some random perturbations from the physical environment. Moreover, we adopt a holistic view by studying each device in its deployment context and by proposing a concurrent model. For example, in the case of an outerspace aircraft there can be communications with the ground control or/and with the ISS. Another example is that of two extra-terrestrial rovers that co-ordinate their activities by communicating complex data (position, etc.).

2.1 A formal model for cyber-physical systems

First, we need to model the physical environment. For simplicity, we consider the system state space to be a subset X of the Euclidean space of dimension n (the number of relevant parameters). A system will evolve within a set Q of regions (that we call formally *modes* or *locations*) defined as a sort of topological sets (that could be open/closed/compact sets, and so on). Each mode $q \in Q$ is characterized by a predicate β_q. The random perturbations are modeled as a "white" noise, i.e. in each region there is defined a Wiener process $(W_t, t \geq 0)$. Note that, in different regions, the system can be subject to different types of perturbation.

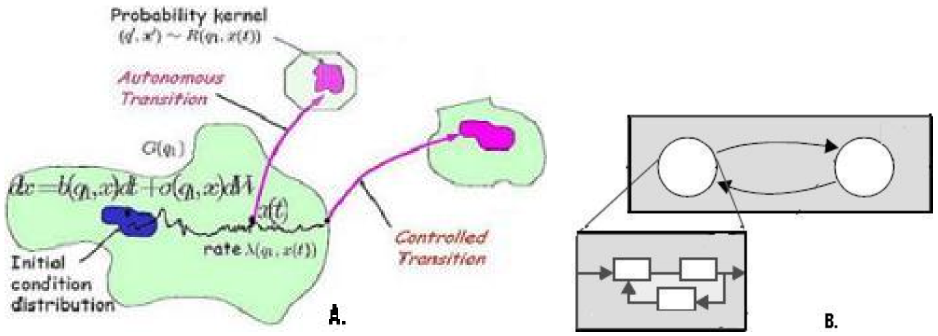
Probability kernel
$(q', x') \sim R(q_1, x(t))$
Autonomous Transition
$G(q_1)$
$dx = b(q_1, x)dt + \sigma(q_1, x)dW$
$x(t)$
rate $\lambda(q_1, x(t))$
Initial condition distribution
Controlled Transition
A.
B.

Figure 1: Simple and hierarchical cyber-physical systems

In each location, the system dynamics is described by a system of deterministic differential equations (usually a first order moving equations), called the designed behavior. In practice, because the system behavior is affected, in each location, by a white noise, the resulted dynamics is described by a stochastic differential equation (SDE): $dx(t) = f^q(x(t))dt + \sigma^q(x(t))dW_t$ and we call that the *physical dynamics*.

The controller transitions are discrete transitions between locations that are triggered by Boolean guards B. We call these *controlled transitions*. However, there is also a class of discrete transitions that take place because of the system autonomy and that are called *spontaneous (or autonomous) transitions*.

Some controlled transitions have communication labels l, usually denoting a communication channel. These are called *communication triggered transitions*. The data types that can be transmitted throughout communication channels are specific to a mode. We denote by γ_q the predicate that state the correctness of communicated data.

In order to predict, evaluate and control the physical dynamics on long time, we need to associate probabilities to all discrete transitions. We call these *jump probabilities* and we denote their rates by λ. Using the jump probabilities, a discrete transition can be formalised by means of a stochastic kernel $R : \overline{X} \times \mathscr{B}(X) \to [0,1]$, where $\mathscr{B}(X)$ represents a class of universal measurable subsets of X. This is a special function, which is measurable in the first argument and a probability measure in the second.

The full formal model is described in [1]. The jump probabilities can be defined using the stochastic kernel and various parameters of the physical dynamics. This is the key to define many sorts of stochastic dependencies between the physical behaviors (*physics*) and discrete transitions (the *computation*).

Each execution path is a Markov string [3]. As result, the global dynamics can be formalised as a Markov process (more specific, a stochastic hybrid process).

2.2 Degrees of autonomy

Considering the very harsh and highly unpredictable environments, in which space systems are deployed, a large autonomy and high reliability are desirable. In this subsection we follow the white box view by defining an original structural classification of autonomous system and indicate how communication can be added by a top feedback to CPS.

The *autonomy degree* of a system is

• (*no feedback*) of level zero (i.e. the system is non-autonomous) if the system is without any feedback connection between or within its components.

• (*nested feedback*) of level n if is obtained by a feedback connection between a system of $(n-1)$ degree with a system with a degree inferior to $(n-1)$ (see *Fig. 2 A.*).

Let us denote the class of n degree systems by $DS(n)$. A *balanced feedback* coupling is a feedback connection for which $n-k \leq 2$. The control of an un-balanced autonomous system is more difficult.

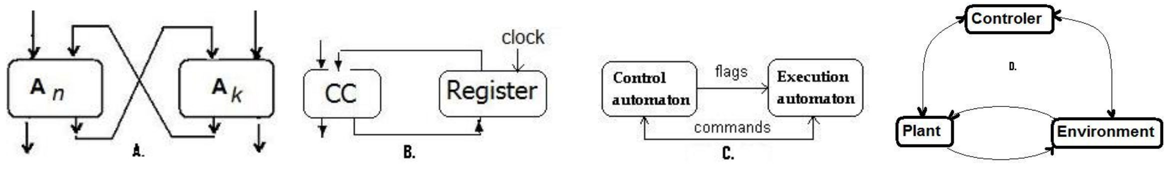

Figure 2: Nested feedbacks: latch, automaton, processor, cyber-physical system

Let us consider in the DS(0) class all *combinational circuits and systems*. Then the DS(1) class contains the *elementary memory* functions (consider NOR gates for the components from Fig. 2 A.). The DS(2) class contains execution (i.e. combinatorial) elements coupled with a memory, i.e. the automata

(Fig. 2. B). The processors are in the DS(3) class (Fig. 2. C), and in the DS(4) class the computer (the von Neumann architecture) can be defined (as a un-blanced couple between a processor and a memory). We can make a correspondence between this hierarchy and the formal languages hierarchy: DS(2) class -> *regular languages*; DS(3) class -> *context-free languages*; DS(4) class -> *context-sensitive languages*.

When considering for level zero a continuous dynamical system we get a hierarchical hybrid system [6] (Fig. 1. B). A CPS contains at least three nested feedbacks (Fig. 2. D), its autonomy degree being thus higher then five (the controller is supposed to be a DS(2) automaton).

In [5], a feedback is modeled as a generalised relation (a span $\swarrow\searrow$ as in category theory) between succesive instances of the plant, modeled as objects in a suitable category. The message passing communication in a CCS style is defined as relations (i.e. spans, i.e. feedback) between systems. This construction can be straight forward applied to the category of SHS defined in [4]. Because we have shown in the previous section that the behaviors of CPS is a SHS, the construction can be also applied to CPS. A network of communicating autonomous CPS has an autonomy degree higher then six.

2.3 Communicating cyber-physical systems

The study of communication in computer science produced a large number of formal models. Not surprisingly, there is wealth of formal models for hybrid systems, and even more for probabilistic systems. However, for more complex systems like SHS communication is less studied [7, 8]. A reason might be the lack of interdisciplinarity, i.e. the communication is not studied in relationship with control and stochastic modeling. This observation is the departing point of our approach in defining communicating CPS in black box style.

The message passing is defined as an one-way communication that takes place only when the sender executes a communication triggered transition.

We denote by $q \overset{l,B,R,a}{\mapsto} q'$, $q \overset{l,B,R,a}{\rightarrow} q'$ and $q \overset{l,R,\lambda}{\rhd} q'$ respectively the communication triggered, controlled, and autonomous transitions from q to q' with label l, guard B, reset map R and communicated data stored in the variable a. The appearance of B, a and λ is optional.

A communication label has two forms: $l = !a$, meaning the value of a is send throughout the channel l or $?b$, meaning the value received the channel l is stored in the variable b. If the label l has the form $!a$ then the label $\bar{l}$ is like $?b$ and viceversa.

The parallel composition of two CPS (with components indexed as 1 and 2) has the parameters:

- $Q = Q_1 \times Q_2$;
- its state space is embedded in the product of the Euclidean spaces corresponding to the two CPS;
- the perturbation is modeled by the product of the two Wiener processes that describe the perturbations corresponding to the two CPS;
- its modes (locations) are obtained by means of tensor products of the component locations;
- $f^{(q_1,q_2)} = \begin{pmatrix} f^{q_1} \\ f^{q_2} \end{pmatrix}$ and $\sigma^{(q_1,q_2)} = \begin{pmatrix} \sigma^{q_1} \\ \sigma^{q_2} \end{pmatrix}$;

The concurrent composition adds the following transition rules to a parallel composition

$$\frac{q_1 \overset{l,B_1,R_1,a}{\mapsto} q_1', q_2 \overset{\bar{l},B_2,R_2,b}{\rightarrow} q_2'}{(q_1,q_2) \overset{l,B,R,c}{\rightarrow} (q_1',q_2')} \quad , \quad \frac{q_1 \overset{l,B_1,R_1,a}{\mapsto} q_1', q_2 \overset{l,R_2,\lambda,b}{\rightsquigarrow} q_2'}{(q_1,q_2) \overset{l,B',R,c}{\rightarrow} (q_1',q_2')} \; l = !a,\, B = B_1 \times B_2,\, B' = B_1 \times \beta_{q_2'}, R = R_1 \times R_2$$

$$\frac{q_1 \overset{l,B_1,R_1,a_1}{\mapsto} q_1', q_2 \overset{\bar{l},B_2,R_2,a_2}{\rightarrow} q_2'}{(q_1,q_2) \overset{l,B,R,a_1}{\rightarrow} (q_1',q_2')} \quad , \quad \frac{q_1 \overset{l,B_1,R_1,a_1}{\mapsto} q_1', q_2 \overset{l,R_2,\lambda,a_2}{\rightsquigarrow} q_2'}{(q_1,q_2) \overset{l,B',R,a_1}{\rightarrow} (q_1',q_2')} \text{ where } B = B_1 \wedge B_2 \wedge \beta_{q'}$$

$$\frac{q_1 \overset{l,R_1}{\mapsto} q_1', q_2 \overset{l}{\not\rightarrow}}{(q_1,q_2) \overset{l,R}{\mapsto} (q_1',q_2)} \quad , \quad \frac{q_1 \overset{l,R_1}{\mapsto} q_1', q_2 \overset{l}{\not\rhd}}{(q_1,q_2) \overset{l,R}{\mapsto} (q_1',q_2)} \quad , \quad \frac{q_1 \overset{l,B_1,R_1,a1}{\mapsto} q_1'}{(q_1,q_2) \overset{l,B_1,R_1,a1}{\mapsto} (q_1',q_2)}$$

$$\frac{q_1 \overset{l,R_1,\lambda_1}{\triangleright} q_1', q_2 \overset{l}{\nrightarrow}}{(q_1,q_2) \overset{l,R,\lambda}{\triangleright} (q_1',q_2)}, \quad \frac{q_1 \overset{l}{\nrightarrow}, q_2 \overset{l,R_2,\lambda_2}{\triangleright} q_2'}{(q_1,q_2) \overset{l,R,\lambda}{\triangleright} (q_1,q_2')} \quad , \frac{q_1 \overset{l,R_1}{\rightarrow} q_1', q_2 \overset{l,R_2}{\rightarrow} q_2'}{(q_1,q_2) \overset{l,R}{\rightarrow} (q_1',q_2')} \quad , \quad \frac{q_1 \overset{l,B_1,R_1}{\longrightarrow} q_1', q_2 \overset{l,B_2,R_2}{\longrightarrow} q_2'}{(q_1,q_2) \overset{l,R}{\rightarrow} (q_1',q_2')}$$

$$\frac{q_1 \overset{l,B_1,R_1}{\longrightarrow} q_1', q_2 \overset{l}{\nrightarrow}}{(q_1,q_2) \overset{l,B,R}{\longrightarrow} (q_1',q_2)} \text{ where } B = B_1 \times \gamma_{q_2} \text{ and } R = (R_1 \times 1)\left((x_1,x_2),\cdot\right) = R_1(x_1,\cdot) \otimes 1_{x_2},$$

$$\frac{q_1 \overset{l}{\nrightarrow}, q_2 \overset{l,B_2,R_2}{\longrightarrow} q_2'}{(q_1,q_2) \overset{l,B,R}{\longrightarrow} (q_1',q_2)} \quad \text{where } B = \gamma_{q_1} \times B_2 \text{ and } R = 1 \times R_2$$

$$\frac{q_1 \overset{l,R_1}{\rightarrow} q_1', q_2 \overset{l}{\nrightarrow}}{(q_1,q_2) \overset{l,R}{\rightarrow} (q_1',q_2)}, \frac{q_1 \overset{l}{\nrightarrow}, q_2 \overset{l,R_2}{\rightarrow} q_2'}{(q_1,q_2) \overset{l,R}{\rightarrow} (q_1,q_2')} \text{ where } R\left((x_1,x_2),\cdot\right) = R_1(x_1,\cdot) \otimes R_2(x_2,\cdot)\ x_1 \in \partial X^{q_1}, x_2 \in X^{q_1'}$$

The transition map λ is given by $\lambda(x_1,x_2) = \lambda_1(x_1)$ for all $x_1 \in X^{q_1}$ and $x_2 \in X^{q_1'}$;

If one CPS agent is able to execute a send event and the other CPS agent does not have a matching receive event, then the first agent executes the transition while the second agent stays in the same location. If contrary, the first agent can execute a controlled transition and the second agent has a matching communication triggered transition, then both agents execute respectively the send and communication triggered transitions at the same time. If the first agent has a communication triggered transition with label l and the second agent has no communication triggered transition with label l, then the composed system has a communication triggered transition with label l outgoing from the joint location, which gives the possibility to interact with other CPS agent, in an other composition context. If both agents have a communication triggered transition with the same label, then the composed system also has a communication triggered transition with this label. The implication of this fact is that both agents can execute the communication triggered transitions at the same time in another composition context where a third CPS agent executes a communication transition with the same label.

The main advantage of the reference model described in this paper is that it allows combinations of verification techniques from different disciplines. For example reachability analysis can be carried out using computational methods from statistics and optimal control.

References

[1] Marius C. Bujorianu., Manuela L. Bujorianu, and Howard Barringer: *A Formal Framework for User Centric Control of Probabilistic Multi-Agent Cyber-Physical Systems.* Proc. of the 9th CLIMA workshop, Springer LNCS, (2008), in press.

[2] Marius C. Bujorianu and Manuela L. Bujorianu: *Towards Hilbertian Formal Methods* Proc. of Conf. on Application of Concurrency to System Design ACSD, IEEE Press (2007): 240-241.

[3] Manuela L. Bujorianu and John Lygeros: *Towards Modelling of General Stochastic Hybrid Systems*. In "*Stochastic Hybrid Systems: Theory and Safety Critical Applications"* LNCIS **337** (2006).: 3-30.

[4] Manuela L. Bujorianu, John Lygeros and Marius C. Bujorianu: *Bisimulation for General Stochastic Hybrid Systems*. In Proc. of HSCC, Springer LNCS 3414 (2005):198-216.

[5] Marius C. Bujorianu: *Integration of Specification Languages Using Viewpoints*. In Proc. of Integrated Formal Methods, Springer LNCS 2999, (2004): 421-440.

[6] John Lygeros: *Hierarchical, Hybrid Control of Large Scale Systems*, Ph.D. Thesis, University of California, Berkeley (1996).

[7] Jose Meseguer and R. Sharykin: *Specification and Analysis of Distributed Object-Based Stochastic Hybrid Systems.* Springer LNCS 3927 (2006): 460-475.

[8] Stefan S. Strubbe, Agung Julius and Arjan van der Schaft: *Communicating Piecewise Deterministic Markov Processes*. Conf. on Analysis and Design of Hybrid Systems (2003): 349-354.