A Formal Framework of Cyber-Physical Systems

Jing Liu', Guobin Wang", Xiaohong Chen", Zuohua Ding[2]

'Shanghai Key Laboratory of Trustworthy Computing
East China Normal University, Shanghai, China
jliu©sei.ecnu.edu.cn
[2]Center of Math Computing and Software Engineering
Zhejiang Sci-Tech University Hangzhou, China
zuohuading@hotmail.com

Abstract. Cyber-Physical Systems (CPS) involve communication, computation, sensing and actuating through heterogeneous and widely distributed physical devices and computational components. The close interaction between physical world and cyber world place integrated CPS framework as the bases of system modeling and analysis. In this paper, a generic formed framework of CPS is presented. In this framework, a cyber-physical system is uniformly represented by State *Space, Controlling Vectors, Invariants, Evolution* and *Event.* Additionally, a relating guarded transition system is defined to specify the computation logic. The framework can be used both in a discrete system modeling and a continuous system modeling. Furthermore, for a cyber-physical system the computability as well as the existence and uniqueness of the solution can be guaranteed by the healthy condition. The proposed framework is the first step towards CPS modeling and analysis.

Keywords: CPS; formal model of CPS; mathematical model; guarded transition system.

1 Introduction

From different aspects, different point of views could be obtained on what CPS is[3][8].Many mathematical models have been proposed in order to reveal the inner operating principles of CPS [2] [7], however, most of them focus on either low-level mathematical model or high-level automata abstraction, few has been done in perspective of linking them together through a rigorous mathematical transformation that computing paradigm of CPS could be derived[4]. Besides, taking the view of computation process could provide us another way of designing and analyzing software architecture, which is especially important in both real-time and embedded applications, not to mention CPS. Thus, in this paper, efforts has been paid in this direction.

Four original mathematical models refined step by step describing CPS are developed first, following that, a formal model specifying both the inner evolution and outward interaction with environment of CPS is proposed, and at last, an equivalent guarded transition system is derived such that computing mechanism of corresponding software architecture would be revealed.

2 Related Work

The concept of CPS framework has been investigated in several contexts. For instance, an aspect-oriented specification framework for CPS has been proposed in [1], in that paper, CPS is viewed as a system consisted of dynamical and control parts, communication parts and computation parts.

Another CPS model originating from multi-agent systems is proposed in [2] [5], in that model, CPS has been viewed as an organized multi-agent group interacting with the physical environment full of uncertainties which is modeled as a stochastic differential equation, and related formal method on analyzing safety property has also been proposed.

And in [7], a networked CPS model is considered, in this paper, distributed declarative Control mechanism is the main topic. Work in this direction also includes [6] .

In most of the solutions mentioned above, there is an implicit assumption that rigorous qualitative analysis relies heavily on concrete equation models, insisting on different aspects could different types of equation models be formed. However, the inclusion mechanism forming the basis of computing paradigm of softwares has not been elaborated enough yet. One promising direction of extending the CPS model disscussed here is to integrate dynamic equations with state machine. It is particularly relevant for cyber systems that control and interact with physical process. We derive a CPS framework from dynamic equations of the system. And healthy conditions are defined for guarantee the existence and uniqueness of solution to a cyber-physical system.

3 CPS Framework

CPS could be viewed in different aspects thus distinguished models can be formed. In this part, a formal CPS framework is proposed, which consists of a formal five-tuple, a guarded transition system transformed from the aforesaid tuple. That framework is generated from the inclusion of differential-algebraic equations.

3.1 Dynamic Equations of CPS

Process in CPS could be classified as being discrete and continuous in general. Therefore, every CPS could be attributed to the following differential-difference equations.

{*X E Ccontinuous x E*   *F(x)*
D discrete   *x*+ E *G(x)*   *(Equation 1)*

Where the differential equation x^{i} E *F(x)* represents the continuous evolution of CPS as the differential inclusion *x E* *Ccontinuous* called flow set represents the valid set of the corresponding continuous evolution; Comparatively, difference equation $x+$ E $G(x)$ corresponds to the discrete process of the system while x E Ddiscrete called jump set regulates its the feasible region. The variable of x illustrates the state of the running process of concerning system, the set of which is defined as state space.

When interaction mechanism are considered, an equivalent mathematical model refined from the previous one is introduced in the form of differential-algebraic equations.

$$\begin{array}{lll} x = Ax + Bu & x\ E\ \mathit{Ccontinuous} & \\ x^{+} = Rx + Tu & x\ E\ \mathit{Ddiscrete} & \mathit{(Equation\ 2)} \\ y = Cx + Du & x\ E\ X = \mathit{Ccontinuous\ U\ Ddiscrete} & \end{array}$$

where x = *(Xi,j)nxn, u* = (tti,l)nx17 y — (Yi,l)nx1

In that model, the evolution mechanism is described by the differential equation $x' = Ax+Bu$, in which A is an n x n matrix illustrating CPS, while the n x / matrix B models the interacting effects on CPS by external control command u, and x is the same state variable as in *Equation 1*. Here, $x = Ax + Bu$ is a concrete form refined from the corresponding differential equation in Equation 1. Similarly, $x+ = Rx +Tu$ describes the discrete jump or event-triggered process, where R is an n x n matrix T is an n x k matrix. Meanwhile, output represented by an m x 1 matrix y could be produced by $y = Cx + Du$, where C illustrates how the internal states would transform into a reachable states, and D explains the effects of u on y. Generally, this refined model integrates continuous and discrete processes into an interleaved integrity.

Inclusion of distinguished equations each of which being represented by differential-algebraic *Equation 2* is given:

{{ $x1$:$_{DC}$1 $\quad$ x$_i$ E *F1(x)*
xi E *Gi(x)*

{x_s E C_s

x_s E D_s

x; = A$_1$x$_1$ + B1u1 xi
{ = R$_1$x$_1$ + Tin' yi =
C$_1$x$_1$ + D1u1 xi E X1
u1 E U1

•

x'_s E $F_3(x)$ *(Equation* 3)
$_s F$ E G_S *(x)*

x_s E
E

where X$_1$,• • • *,X,* are state spaces of each subsystems, meanwhile, each of U$_1$,- • • ,U. is a corresponding controlling vectorial set that following *Healthy Conditions* promising the existence and uniqueness of solutions to state and controlling vector of CPS model should be met:

Axiom 3.1 Vx3X_i3e > 0 *(x, e) c Xi,* i E *N;*

Axiom 3.2 Vi *j* x_i n x_j = 0, 1 < i,i < *s* A *i,j* E *N;*

Axiom 3.3 Vx E $U7_{—1,iEN}$ *11 ' ,j,Uk*

xi = Aix,' + BjUi

{A x = R$_3$x$_3$ ± T3u3 *Xk+= Akxk + Bkuk* *X$_k$ = RkXk ± TkUk*

j = k, j, k E N);

yi = *Cixi* + *DjuiMe* = *CkXk* + *DkUkt* -- --

3

By above **Axiom 3.1, 3.2,** partition relationship between Xi and *X is* promised, while controllability of CPS is promised by **Axiom** 3.3.

Following previous axioms, definitions on Equation 3 concerning formal CPS system are given out:

Definition 3.1 *(State Space of CPS) The state space X is X =* M ...,*i*= ',JEN Xi *where X is a union set called the* state *space of CPS as the union of domains defining differential and difference equations.*

Definition 3.2 *(Controlling Vectors of CPS) The controlling vectors U is U =U*=1 • 2,2EN *Ui where U is a union set called controlling vectors of CPS as the union of sets consisting of controlling vectors U_i.*

Definition 3.3 *(Invariants) The invariants Invariant is Invariant = {X_1, • • • , X_s} where Invariant is a set called Invariant of CPS consisting of all sets X_i.*

Definition 3.4 *(Evolution) The evolution Evolution is Evolution = {x_i = A_1x_1 + Blur, • • • , x^i_s = A_sx_s + B_su_s} where Evolution is a set called Evolution of CPS consisting of all differential equations.*

Definition 3.5 *(Event) The event Event is Event = {xiE = R_1x_1 +Tiui, • • • , x $_8$+ = R_sx_s +T_su_s} where Evolution is a set called Event of CPS consisting of all difference equations.*

Therefore, the equations representing CPS including its interaction with environment could be transformed equivalently into the following standard form:

controlling vectors uLLiEN ^{Il}i

State *Space* *U i^s =1 ,ieN xi*

Invariants *f X_i*

1 X_s

(Equation 4)

x^i_i = A_1x_1 + B1u1

Evolution

x^i = A_sx, + B,

Event *{x^F = R_1x_1 + To O].*

x-,,F = R_sx_s + Tsus

3.2 CPS Formal Framework

Based on previous dynamic

equations of CPS, a formal model specifying both the inward coordination represented by corresponding differential equations and outward interaction mechanism represented as difference equations is proposed regulating modeled software computing paradigm. Based on previous definition 31 - 35, formal framework of CPS is given as follows:

Definition 3.6 *CPS Framework* A *cyber-physical system is a five-tuple (U, X, Invariant, Evolution, Event) where:*

— *U represents the controlling vectors of CPS. Each of its elements is an vector whose dimension may not be same to each other according to each evolution equation it follows.*

— X *represents the state space of CPS. Generally,* X *takes only variables that can determine the future behavior of the system when the present state and the corresponding triggering commands are known.*

— *Invariant consists of all domains of each continuous differential equations and discrete difference equations specifying the computability of the modeled physical process.*

— *Evolution consists of all continuous operators represented by continuous differential equations.*

— *Event consists of all discrete operators represented by discrete difference equations reflecting resetting the behavioral mode of the system.*

After the structural specification of CPS formal model, a dynamical transi-tion system is defined as follows:

Definition 3.7 *Guarded Transition System The corresponding guarded transition system specifying the computing sequential logic is a four-tuple (S_o, States, guard, -+) where:*

— S_o *C States represents the initial states.*

— *States represents the state space of CPS. Only could the combination of subsets of elements of* X *and differential operator defined on it be designated as states, whose formal representation is as follows:*

$$States = z=i,iEN(X- E\ X,\ x^{i}. = Aixi + B_iu_i)$$

— *Guard is a set consisted of subsets of elements of* X *specifying the constraints on transition between computing mode, whose formal definition is as follows:*

$$Guard = \{ Z C X_i l V i E N A 1 < i < I X 1 \ : \ X_i E X \}$$

which promises the computing feasibility of chosen equations.

is a ternary relation over States specifying the the transitions between states, whose formal definition is as follows:

=z=1jEN 3{((XiE = +Bu)x(XiEXx,t
=

$$R_jx_j + T_ju_j)\ x\ (X_k\ E\ X,\ X^{i}{}_k = Akxk\ Bkuk))\}$$

where

$$(\ liM\ Xi = liM\ Xk = Xi)\ e\ Xi\ V\ (\ liM\ Xi = liM\ Xk = X\ j)\ E\ X\ j$$

which promises the linking between two continuous processes by a discrete jump.

4 Conclusion and Future Work

In this paper, we have developed a CPS formal model and its relating guarded transition system from a group of rigorous dynamic equations. By that, computational logic of CPS software could be specified clearly that computing paradigm is derived through the transformation and refinement of mathematical models. Additionally, we derive a CPS framework from dynamic equations of the system, as well as healthy conditions for guarantee the existence and uniqueness of solution to a cyber-physical system. The future work includes developing formal semantics of liveness, safety, validity and fairness based on this model and applying them into checking Automatic Train Protection (ATP) system of high-speed railway transportation.

Acknowledgment

We would like to thank the reviewers of this paper for their valuable comments. This work is partially supported by the projects funded by the 973 program 2009CB320702, NSFC 61170084, and the Open Fund of State Key Lab No.HCST201101. Zuohua Ding is supported by the NSF of China under Grant No.61170015, Zhejiang NSF under Grant No.Z1090357. The Lab is supported by NSFC Creative Team 61021004 and 863 Project 2011AA010101.

References

1. Lichen Zhang and Jifeng He, *A Formal Framework for Aspect-Oriented Specification of Cyber Physical Systems.* ICHIT 2011, CCIS 206, pp. 391C398, 2011.
2. Marius C. Bujorianu, Manuela L. Bujorianu, and Howard Barringer, *A Formal Framework for User Centric Control of Probabilistic Multi-agent Cyber-Physical Systems.* CLIMA IX, LNAI 5405, pp. 97C116, 2009.
3. Sha, L., Gopalakrishnan, S., Liu, X., Wang, Q., *Cyber-Physical Systems: A New Frontier.* Springer, Heidelberg (2009); ISBN 978-0-387-88734-0
4. Janos Sztipanovits, *Model Integration and Cyber Physical Systems: A Semantics Perspective.* FM 2011, LNCS 6664, p. 1, 2011
5. Bujorianu, M.L., *Extended Stochastic Hybrid Systems and their Reachability Problem.* In: Alur, R., Pappas, G.J. (eds.) HSCC 2004. LNCS, vol. 2993, pp. 234C249.Springer, Heidelberg (2004)
6. Edmund M. Clarke and Paolo Zuliani, *Statistical Model Checking for Cyber-Physical Systems* . ATVA 2011, LNCS 6996, pp. 1C12, 2011
7. Mark-Oliver Stehr, Minyoung Kim, and Carolyn Talcott, *Toward Distributed Declarative Control of Networked Cyber-Physical Systems.* UIC 2010, LNCS 6406, pp. 397C413, 2010.
8. *Report: Cyber-Physical Systems Summit.* http://ostp.gov/pdf/nitrd_review.pdf, p. 31.