Design Research in Cyber-Physical Systems through Weak-Bisimulation

Roy McCANN and Khalid RAHMAN
Dept. of Electrical Engineering, University of Arkansas
Fayetteville, Arkansas 72701, USA

Bisimulation methods for design and verification of complex digital electronics have become well established in engineering practice. Concurrently, there have been dramatic theoretical advances in the theory of hybrid dynamical systems. This paper explores the how these advances can be incorporated into research methods for the emerging area of cyber-physical systems from a cybernetics perspective. The results can be used in determining how design of engineered systems can be safely integrated into physical systems.

***Index Terms*—Bisimulation, cyber-physical systems.**

1. INTRODUCTION

There has been increasing deployment since the 1970's of digital communications and computer control of complex infrastructure systems. Examples include air traffic control, the operation of electric utility grids, ground transportation traffic management, biomedical monitoring systems, weapon systems (remotely operated drones, guided missiles), automated manufacturing and logistics support (supply chain management), banking and financial institutions, as well as in the operation of computer data networks in directing message traffic. The proliferation of safety and mission-critical computer controlled systems has motivated the emergence of cyber-physical (CP) systems as a new area of engineering research [1]. Cyber-physical systems are intrinsically hybrid dynamical in nature in that there is a coupling between the discrete-event and finite-state machine orientation of the cyber elements intermingled with the continuous-state nature of physical dynamics that are conventionally modeled by differential/difference equations. The challenges in designing and verifying the behavior of CP systems has been noted in terms of the intractable nature of attempting to model overall macro-level CP behavior based on explicit micro-level component simulations of detailed cyber and physical dynamics [2]- [4]. Thus, it is both challenging and an urgent priority to investigate design research in CP systems.

2. BISUMULATION OF DIGITAL SYSTEMS

A bisimulation is an abstraction in theoretical computer science. In a strict sense, a bisimulation is a relation between two state-transition systems such that state changes in one system are tracked in the other system, and vice-versa. This theoretical construct has yielded significant advances in verifying complex digital systems by determining a bisimulation between the complex detailed design whose states are grouped into broad categories and a simplified system for which tractable solutions exist regarding safe-states, mode changes, state transitions, etc. Previous work has explored expanding the use of bisimulations to linear time-invariant systems that switch between various specific parameters sets; i.e., switched linear systems [5]. Such cases are encountered for example in electric power systems when the electrical dynamics abruptly change as a consequence of an electrical fault that results in a circuit breaker opening and thereby de-energizing some portion of the network. To determine if such automatic response to fault conditions is achievable, methods as in [6] maybe employed in terms of reachability concepts from control systems theory. Ongoing research seeks further understanding for a wider class of dynamic systems, such as those with stochastic and nonlinear behavior [7]-[9].

3. MOTIVATION FOR DESIGN ENGINEERING

The emerging technology field of cyber physical (CP) systems brings to the forefront the needs for innovation in design engineering. In particular, often the cyber elements include software modules that have been well characterized and are reused in various portions of the system. Consequently, a meta-state can be defined that is the aggregate of a number of individual state transitions. By relaxing the state-to-state identification between the actual cyber system, then a weak-bisimulation is formed. This allows then coupling to the physical system for design research purposes at an abstraction level that preserves the important behavioral characteristics of the overall CP system without introducing the intractability of analysis that results when a full bisimulation is defined for the cyber components.

4. CYBER-PHYSICAL SYSTEMS

Cyber-physical (CP) systems as a distinct science have evolved out of continuing advancements in the area of cybernetics, microelectronics, digital communication systems and sensor networks. This has occurred through the convergence of many technologies over the last few decades that has allowed for mobile electronic devices to be incorporated in previously inaccessible areas. Examples include material handling automation using RFID tags for inventory control, traffic controls based on vehicle-to-vehicle

radio communications as well as roadside sensors, and implantable medical devices for the treatment and monitoring of hypertension and diabetes. Of particular interest for cybernetics related is the role of feedback between the cyber and physical subsystems. In general, the difficulty presented in the design engineering of CP systems is the complexity of understanding the possible number of interactions that may occur once a particular event transpires. As an example, the state of an electric utility grid is comprised of the voltages and currents flowing between generators and loads at a particular instant. Various circuit breakers and disconnects are positioned in such a manner that each of the transmission lines and transformers within the system are overloaded. Due to adverse weather conditions resulting in thunderstorms and high winds, a fault might be induced where a transmission line is broken and results in a short circuit to ground. This results in an abrupt electrical transient whose characteristics are dictated by the physics of the electrical circuit. Immediately after the fault condition, the electrical current then rapidly increases in the vicinity of the faulted transmission line. This fault condition is sensed by the protection circuitry, and automatically responds in a manner to isolate the fault condition by opening circuit breakers. Once the related circuit breakers activate, there is an ongoing re-closure sequence where the protection control circuits seek to reenergize the system to restore electrical service in the vicinity of the damaged transmission line. Each of these control functions related to switching the electrical system in response to the fault condition results in a physics-based electrical transient. However, the decision regarding what automatic protection function to initiate is cybernetic in nature. Each cyber-related interaction (e.g., opening a circuit breaker) involves the selection among many possible choices – that is, it is not known *a priori* which circuit breaker operation will achieve an optimal result in terms of both isolating the fault while also minimizing the service area that suffers from an interruption of electric power. In fact, for most of the electric power systems in operation throughout the world today there is such a large number of possible protection sequences that could be taken that it is a practical necessity that only the most rudimentary protection actions be implemented. Through a similar line of reasoning, the same type of dilemma is encountered in many other types of CP systems, such as air-traffic control, logistics planning, transportation networks, manufacturing operations, etc.

For CP systems, the complicating element of analysis involves the abrupt transition from one mode of operation to another ([5]-[9]). This can be formalized as shown in Fig. 2 where the state *i* is modeled by a set of differential equations $F_i(x)$ [6], [7]. From the example involving the electric power system, this would be the conditions corresponding to the fault condition of the transmission line short-to-ground, but prior to any circuit breaker protection functions. Once the current increases to a maximum allowed level, a boundary or "edge" condition is reached corresponding to one of the electrical currents in the state space of $F_i(x)$. Once the current reaches the edge, then the associated "guard" function is triggered (a circuit breaker is opened) which results in a "jump transformation" in the electrical system to a new set of state equations $F_j(x)$ and state

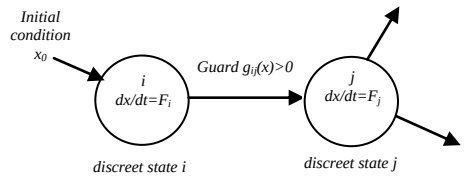

Fig. 1: State transition diagram [6].

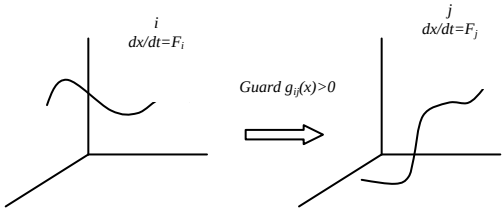

Fig. 2: Switched trajectories during transition jump.

condition *j* [6] for the new power system configuration. In Fig. 1 the concept of each state node is identified with a set of differential and algebraic equations for the set of conditions that the system is operating at that instant. In general, there are many possible guard conditions that might be defined, and a multiplicity of defined edges to account for the various conditions that would necessitate a transition to a new operating node. Each node point in the state-transition diagram of Fig. 1 itself has some set of dynamics in the time behavior of the system. This is shown in Fig. 2 to indicate how the states (three-dimensional state-space in this example) might evolve during the transition from one node to the next corresponding to Fig. 1.

In order to formulate a design engineering structure that addresses the challenges in dealing with CP systems, we begin by noting the available computer aids that are currently available for modeling jump-transition systems. Fig. 3 shows a block diagram of a jump-transition system that could be adapted to Matlab-Simulink [14] using the StateFlow package as in [13]. This gives the design engineer a modeling tool for simulation of complex systems – however it is noted that this does not provide complete guidance in the synthesis aspects of CP systems.

For developing a CP synthesis method we consider another approach – that is, rather than beginning with the details of physics-based models (differential equations), one instead begin with the cyber description of transitions ([6], [11]), as a automata employing the design verification techniques that have been developed for complex digital systems such as microprocessors and VLSI microelectronic circuits [4], [7]. The techniques for verifying large scale digital electronic circuits are based on first verifying individual gate-level logic functions. Once these gate-level

functions have been verified, then they are re-used as part of more complex circuits.

At the highest system level, the verification process only concerns itself with approximations of the system behavior. That is, it is not necessary to verify every possible gate-level transition, but rather to partition the automata into groups of states, and to examine only the transitions across the portioned states.

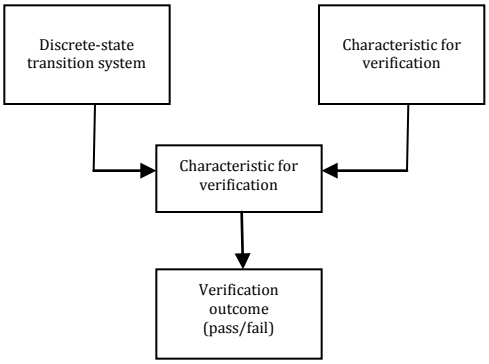

Fig. 3: Computer aided simulation model of CP system.

For designing a CP system, there is a set of criteria defined for proper operation of the system. These requirements can be listed and prioritized into a set of properties P_i that correspond to the defined set of requirements [5]-[7]. For the example of the electric power system, properties might include power flows being below that maximum rated value of a transmission line, and the operating voltage at service connections to customers. The difficulty in CP synthesis (verification) is that direct verification of the system by examining each possible transition as in Fig. 1 is prohibitive in terms of computational intensity, as well as not necessarily giving a definitive result even if one attempted to exhaustively consider ever possible transition [2].

If an adequate approximation model M' of the original physical system M can be developed that captures the boundaries and guard conditions, then this simplified model M' can be verified in a process that yields a design approach for the system [12]. The simplified system M' is designed in terms of the characteristics P' which encompasses the response of the system in terms of its significant outcomes rather than a detailed (and hence burdensome) description in the state-space. The model correspondence that is used in relating M to M' is then used in defining the synthesis attributes P to P' for then relating back to the design specifications of the original system [13]. This relationship between the physics-based model M and synthesis attributes P to the design model M' and synthesis properties P' is shown in Fig. 4.

For the process of developing CP systems, the structure of design synthesis is often tabulated as a set of properties to be achieved. Each property of the design then needs to be synthesized to ensure compliance.

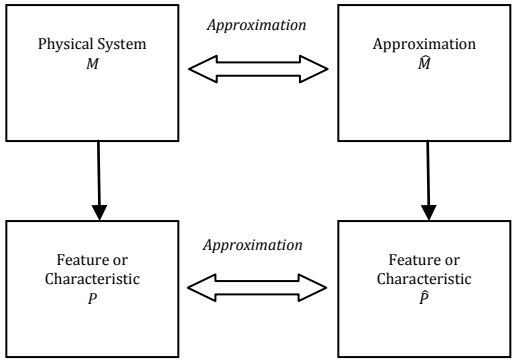

Fig. 4: CP system model approximation.

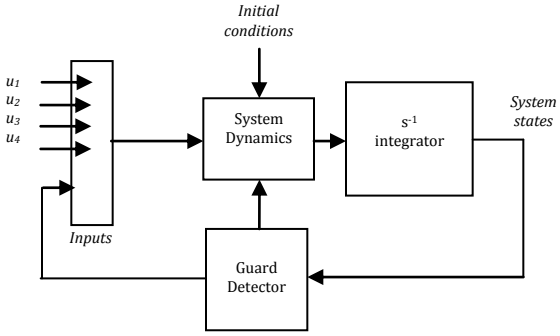

Fig. 5: CP system design and synthesis.

This is done on the model through a model checking program that propagates the set of states of M' instead of individual trajectories as in Fig. 1. The result of the model checking program is either a confirmation of the characteristic, or a counter example showing that the characteristic (design feature) fails. This structure of synthesis through defined characteristics P' to function verification is shown in Fig. 6. With this then the structure for CP system design within the context of Computer Aided Control System Design (CACSD) is shown in Fig. 6 [13].

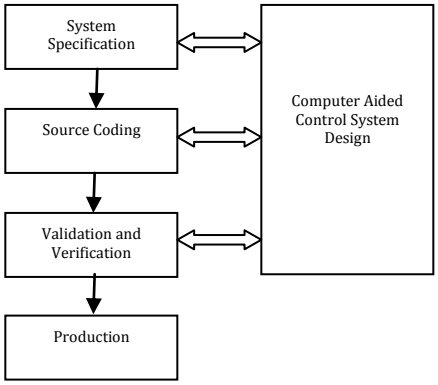

Fig. 6: Computer aided cyber system design.

5. BISIMULATION METHODS

The theory of simulation of timed-automata has been developed by a number of researchers [5]-[9]. To summarize, T_2 is a simulation of the timed-automata T_1 for the following definition [9], [10]:

T_2 *simulates* T_1 if there exists $\preccurlyeq \in Q_1 \times Q_2$ a binary relation such that:

- Is total and onto (involving all Q_1 and Q_2).
- $Q_{10} \preccurlyeq Q_{20}$
- $q_1 \rightarrow q_1'$ *and* $q_1 \preccurlyeq q_2$
  $\Rightarrow$ *there exists* q_2' *such that* $q_1' \preccurlyeq q_2'$

A graphical representation showing the mapping of state-trajectories T_1 and T_2 between state Q_1 and Q_2 [10] is shown in Fig. 7. It is emphasized that the simulation relationship is directional in that it is reflexive for T_2 with respect to T_1.

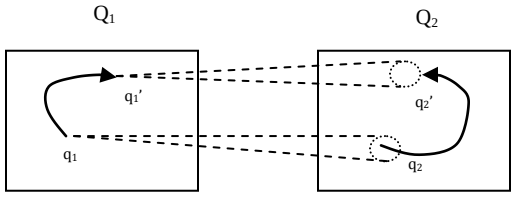

Fig. 7: Simulation relationship.

Bisimulation has been formalized as a design tool for large scale digital systems. Bisimulation is defined in terms of a symmetric relationship [5], [6], [10]:

Given $T_1 = (Q_1, \rightarrow Q_{1,} Q_{10}), T_2 = (Q_2, \rightarrow Q_{2,} Q_{20})$,
$a\ relation \equiv \in Q_1 \times Q_2\ is\ a\ bisimulation\ if$
$\equiv\ is\ a\ simulation\ relation\ for\ T_1\ to\ T_2$
$\equiv^{-1}\ is\ a\ simulation\ relation\ for\ T_2\ to\ T_1$

The symmetric relationship for bisimulation is shown in Fig. 8. This allows for conclusions to be drawn regarding the original physics-based system state Q_1 based upon state-transitions T_1 and T_2 observed in the simulation state Q_2. Bisimulation is shown graphically in Fig. 9.

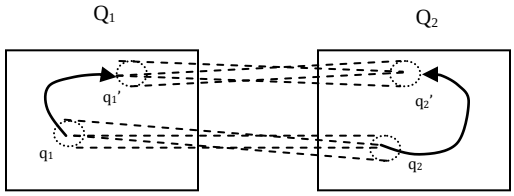

Fig. 8: Bisimulation relationship.

The bisimulation can then be integrated into the overall synthesis structure by modifying Fig. 6 to include the simulation system in place of the physics-based detail model. Once a bisimulation has been established for a CP system, then the original system can be portioned in order to establish the design synthesis properties. Formally, this is accomplished by creating a quotient transition system [9], [11].

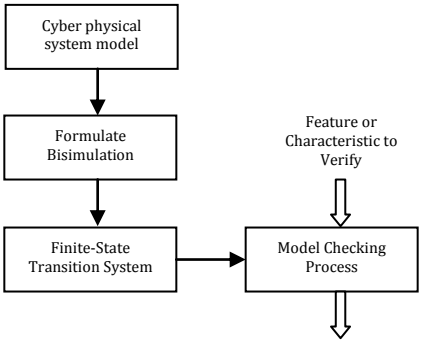

Fig. 9: CP system synthesis with bisimulation.

A quotient transition system is conceptually a portioning of the state space of the physics-based model into regions which would correspond to the edges for which a guard would initiate some specified jump transition in the CP-system [15]. The advantage of using a quotient transition system is that this provides a means for the designer to specify the desired behavior of the CP system (synthesis), rather than simply analyzing the behavior of a given system (analysis). Formally, a quotient transition system is defined by [8], [10]:

Given a transition system T:

$$T/P = (P, \rightarrow p, Q_0/P)$$

Is a quotient transition system where

- P is a partition of Q
- $P_1 \rightarrow p\ P_2\ for\ P_1, P_2\ \in P$
- *If* $q_1 \rightarrow q_2\ for\ some$
  $q_1 \in P_1\ and\ q_2 \in P_2$

Graphically [10], a conceptual use of a quotient transition system (readers are referred to sources such as [15] to synthesize the CP-system) is shown in Fig. 10 where the partitioning of the state trajectories T is shown in terms of the partitions of the quotient transition system T/P.

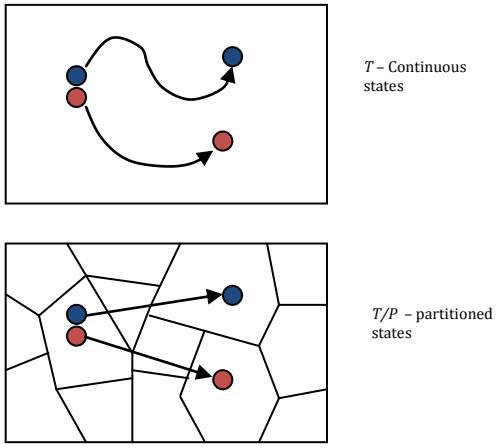

Fig. 10: Quotient transition system partitioning.

6. CONCLUSION

A design-research technique for synthesizing cyber-physical systems is considered. This provides an alternative method that to work directly in terms of physics-based models with supplemental functionality added on by the cyber elements. The method uses the numerous theoretical results from cyber and hybrid systems related researchers to link to the physics-based models. Using these analysis-synthesis tools given by bisimulation of complex digital systems, a framework for design engineering of CP systems can be developed where a quotient transition system would be used to simplify the design process by partitioning the CP system based on the overall system design objectives.

REFERENCES

[1] National Science Foundation, Program Solicitation 08-611, Directorate for Computer and Information Science and Engineering. http://www.nsf.gov/pubs/2008/nsf08611/nsf08611.htm

[2] E. Lee, "Cyber Physical Systems: Design Challenges," Proceedings of the 2008 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC), pp.363-369, 5-7 May 2008.

[3] P. Antsaklis, "On control and cyber-physical systems: Challenges and opportunities for discrete event and hybrid systems," 9th International Workshop on Discrete Event Systems, WODES 2008, pp.1-9, May 28-30, 2008.

[4] M. Bujorianu and H. Barringer, "An Integrated Specification Logic for Cyber-Physical Systems," 2009 14th IEEE International Conference on Engineering of Complex Computer Systems, pp.291-300, 2-4 June 2009.

[5] G. Pola, A. van der Schaft, M. Di Benedetto, "Bisimulation theory for switching linear systems," 43rd IEEE Conference on Decision and Control, vol.2, no., pp. 1406- 1411 Vol.2, 14-17 Dec. 2004.

[6] G. Lafferriere, G. Pappas and S. Sastry, "Reachability analysis of hybrid systems using bisimulations," *Proceedings of the 37th IEEE Conference on Decision and Control*, vol.2, no., pp.1623-1628 vol.2, 16-18 Dec 1998.

[7] P. Tabuada and G. Pappas, "Finite bisimulations of controllable linear systems," Proceedings of 42nd IEEE Conference on Decision and Control, 2003, pp. 634- 639 vol.1, Dec. 9-12, 2003.

[8] A. Julius, A. Girard, and G. Pappas, "Approximate bisimulation for a class of stochastic hybrid systems," American Control Conference, vol., no., pp.6 pp., 14-16 June 2006

[9] A. Girard and G. Pappas, "Approximate bisimulations for nonlinear dynamical systems," CDC-ECC '05, Proceedings of the 44th IEEE Conference on Decision and Control, vol., no., pp. 684- 689, 12-15 Dec. 2005.

[10] A. Chutinan, "Hybrid system verification using discrete model approximations," thesis defense, users.ece.cmu.edu/~krogh/checkmate, Dept. of Elect. and Computer Engineering, Carnegie Mellon University, May 1999.

[11] P. Tabuada, "Symbolic control of linear systems based on symbolic subsystems," IEEE Transactions on Automatic Control, vol. 51, no. 6, June 2006, pp. 1003-1013.

[12] A. Rajhans, S.-W. Cheng, B. Schmerl, D. Garlan, B. H. Krogh, C. Agbi and A. Bhave, "An Architectural Approach to the Design and Analysis of Cyber-Physical Systems," in *Third International Workshop on Multi-Paradigm Modeling*, Oct 2009.

[13] A. Donzé, B. H. Krogh and A. Rajhans, "Parameter Synthesis for Hybrid Systems with an Application to Simulink Models," in *Proceedings of the 12th International Conference on Hybrid Systems: Computation and Control*, 2009.

[14] Matlab-Simulink Users Manual, *The Mathworks*, Natick MA.

[15] Chutinan, A., B. Krogh, "Verification of infinite-state dynamic systems using approximate quotient transition systems," IEEE Transactions on Automatic Control, vol. 46, no. 9, Sept. 2001, pp. 1401-1410.