**Multi-University Research Initiative on**

**High-Confidence Design for Distributed Embedded Systems**

Frameworks and Tools for High-Confidence Design of

Adaptive, Distributed Embedded Control Systems

**Project Summary**

**Vanderbilt:** J. Sztipanovits (PI) and G. Karsai

**UC Berkeley:** C. Tomlin (Lead and co-PI), Edward Lee and S. Sastry

**CMU:** Bruce Krogh (Lead and co-PI) and Edmund Clarke

**Stanford:** Stephen Boyd

FA9550-06-0312

# Abstract

This project aims at developing a comprehensive approach to the model-based design of high-confidence distributed embedded control systems. We leverage a shared theoretical foundation and technology infrastructure in four focus areas: hybrid and embedded systems theory, model-based software design, composable tool architectures, and experimental testbeds.

The project now in the final stages of producing an end-to-end tool chain prototype for distributed control systems that exhibits primary advantages of model-based design: (1) explicit modeling of system layers and their interactions using semantically sound domain-specific modeling languages, (2) model-based verification of system properties, and (3) model-based code generation. The target platform uses time-triggered model of computation that enables using the open-source tool chain in conjunction with commercially available platforms such as TTA or TT-Ethernet. The tool chain has been validated in generating flight control software for the StarMac and the AscTech Hummingbird quadrotor UAVs.

# Highlights of Accomplishments and New Findings

## Hybrid and Embedded Systems Theory

### Embedded Systems Modeling and Deep Compositionality (Krogh, Tomlin, Sastry)

The task of designing provably correct controllers for safety-critical applications is often subject to hard constraints that the system state remains within a safe operating regime at all times, while achieving desired target configurations within finite time. Furthermore, due to various uncertainties in the modeling phase and operation phase, the controller design must be robust to factors such as modeling error, environment disturbances, and adversarial actions.

Our approach to this problem lies at the boundary of control theory and formal verification, namely we derive controllers with provable behaviors from the results of reachability analysis. More specifically, we use reachability algorithms to first determine the subset of states in the system state space which can satisfy the desired safety and target attainability specifications under admissible control inputs, and then explicitly synthesize a controller, in feedback form, for any initial condition in this feasible set. The resulting controller is guaranteed to be provably correct by design.

In the deterministic setting, this approach is applied to the problem of motion planning in adversarial scenarios [1], involving two teams of mobile agents – one having the objective of defending a protected zone, while the other having the objective of entering the protected zone and then safely returning to base. Hamilton-Jacobi reachability is used to compute the winning regions of the respective teams, under the worst-case behavior of the other team. From the solution of the reachability computation, explicit feedback control laws are derived allowing each team to accomplish the desired objectives within its winning region.

In the stochastic setting, this approach is applied to the study of stochastic hybrid dynamic games [2, 3], where the system dynamics is modeled probabilistically and the objective of the control is to maximize the probability of achieving the safety and target attainability specifications, subject to the worst-case adversary behavior. Under a rigorous stochastic game framework, theoretical results are derived for computing this probability over the entire state space through an appropriate dynamic programming algorithm. From this algorithm, an optimal control policy can be synthesized to achieve the desired probability of success. The numerical implementation of the dynamic programming algorithm was illustrated with two applications involving a quadrotor helicopter tracking a ground vehicle and conflict resolution between two aircraft. Motivated by presence of uncertainty in safe sets, such as unknown environments or probabilistic weather forecasts, we also extended this framework to time-varying and stochastic unsafe sets [4].

Related publications since the last report:

[1] H. Huang, J. Ding, W. Zhang, and C. J. Tomlin, “A Differential Game Approach to Planning in Adversarial Scenarios: A Case Study on Capture-the-Flag,” in IEEE International Conference on Robotics and Automation (ICRA), Shanghai, China, May 2011.

[2] M. Kamgarpour, J. Ding, S. Summers, A. Abate, J. Lygeros, and C. J. Tomlin, “Discrete Time Stochastic Hybrid Reach-Avoid Game: Part I - Formulation and Applications”, 2011. Submitted.

[3] J. Ding, M. Kamgarpour, S. Summers, A. Abate, J. Lygeros, and C. J. Tomlin, “Discrete Time Stochastic Hybrid Reach-Avoid Game: Part II - Theory and Implications”, 2011. Submitted.

[4] S. Summers, M. Kamgarpour, C. J. Tomlin, and J. Lygeros, “A Stochastic Reach-Avoid Problem with Random Obstacles, in Hybrid Systems: Computation and Control”, ser. Lecture Notes in Computer Science, 2011.

### Advances in Reachability Analysis

Reachability computations are foundational to the verification of continuous and hybrid dynamic systems. We have developed new methods for computing tight overapproximations of reachable sets for linear dynamic systems with uncertain, time-varying parameters and bounded input signals. This makes it possible to compute much tighter approximations to reachable sets for nonlinear systems using on-the-fly local linearizations. Using zonotopes as the fundamental representation of sets, reachable sets can be computed for systems with dozens of continuous state variables. Improvements of two to three orders of magnitudes in computation times have been achieved.

Related publications since the last report:

J. Kapinski, B. H. Krogh, On incrementally bounded systems, American Control Conference (ACC), Baltimore, MD, July 2010, pp. 6348 - 6350.

M. Althoff, C. Le Guernic, B. H. Krogh, Reachable set computation for uncertain time-varying linear systems, Conference on Hybrid Systems: Computation and Control (HSCC), Chicago, IL, Apr 2011

### Network Control Framework for Aircraft

Our overall research goal this past year has been to create constructive networked control architecture for formation control of both quadrotor and fixed-wing aircraft which allows for collision avoidance while maintaining stability. In order to obtain this goal we: 1) developed a constructive non-linear control framework which allows non-linear affine systems such as fixed-wing aircraft to be rendered strictly-output passive; 2) established a networked control architecture to interconnect multiple-agents in order to achieve a formation; and 3) modified a classic collision avoidance algorithm in order to achieve separation of aircraft.

Our first result applies to networked control of non-linear affine systems, including fixed wing aircraft, quadrotor aircraft, robotic, thermal, semiconductor manufacturing, alternative energy generation, and active suspension systems. These nonlinear affine systems can be expressed through what we term "m-Triangular Systems". The m-Triangular System renders possible a well-posed, distributed, continuous-time, control law which can be applied to nonlinear affine systems. This control law creates a strictly-output passive system which can then be integrated into a multi-rate discrete time networked control architecture. This robust architecture permits a discrete time strictly passive lag compensator to determine the desired output of the strictly-output passive system. Thus, we can integrate unmanned jet fighter aircraft into the NextGen system in which the lag compensator is located at the ground-control station. We can now safely control the inertial position of these aircraft despite communication time varying delays and data loss [NK-1a,b,c].

Our second result builds on our advanced digital networked control architecture in which passivity is preserved in spite time varying delays and data loss [NK-2]. The key to this architecture is our networking abstraction known as the power-junction and some minor analysis showing that it can be distributed over arbitrary overlay network topologies [NK-3a,b]. The overall architecture then allows for steady-state analysis in order to derive final formations of quadrotor aircraft. These predicted results have been verified using our advanced Simulink based models of quadrotor aircraft in which time varying delays and data loss were simulated using TrueTime.

Related publications since the last report:

[NK-1a] N. Kottenstette, H. LeBlanc, E. Eyisi, J. Porter, A Backstepping Control Framework for m-Triangular Systems, ISIS Technical Report, ISIS-11-104, Vanderbilt University - pp. 2-17 April 28, 2011 (Under review in IEEE Transactions on Control Systems Technology: A Backstepping Control Framework for Networked Control of m-Triangular Systems).

[NK-1b] N. Kottenstette, J. Hall III, X. Koutsoukos, J. Sztipanovits, P. Antsaklis, Passivity-Based Design of Wireless Networked Control Systems Subject to Time-Varying Delays, ISIS Technical Report, ISIS-08-904, Vanderbilt University - pp. 2-17, February 5, 2011 (Provisionally Accepted IEEE Transactions on Control Systems Technology).

[NK-1c] N. Kottenstette, H. LeBlanc, E. Eyisi, X. Koutsoukos, Multi-Rate Networked Control of Conic Systems, ISIS Technical Report, ISIS-09-108, Vanderbilt University - pp. 2-12 March 2011 (Abridged version will appear in 2011 American Control Conference - ACC 2011, San Francisco, CA, USA; in addition this will shortly be submitted to the International Journal of Robust and Nonlinear Control).

[NK-2] N. Kottenstette, J. Hall III, X. Koutsoukos, P. Antsaklis, J. Sztipanovits, Digital Control of Multiple Discrete Passive Plants Over Networks, International Journal of Systems, Control and Communications - Vol. 3, No. 2, pp. 194 - 228 April 2011.

[NK-3a] H. LeBlanc, E. Eyisi, N. Kottenstette, X. Koutsoukos, A Passivity-Based Approach To Deployment In Multi-Agent Networks, Seventh International Conference on Informatics in Control, Automation and Robotics (ICINCO 2010), Funchal, Madeira - Portugal, SciTePress, pp. 53-62 June 2010 (best student paper).

[NK-3b] ---, A Passivity-Based Approach To Deployment In Multi-Agent Networks, Informatics in Control, Automation and Robotics, ser. Lecture Notes in Electrical Engineering, J. A. Cetto, J.-L. Ferrier, and J. Filipe, Eds. Springer Berlin Heidelberg, 2011, vol. 89, pp. 135–149. url: <http://dx.doi.org/10.1007/978-3-642-19539-6_9> .

## Foundations for model-based software design

### Precision Timed (PRET) Machines (Lee)

Guaranteeing the correct behavior of embedded systems is extremely difficult, especially with respect to timing constraints and their relationship to the safety of the physical systems. The traditional verification process is facing two major challenges regarding timing constraints:

1. The execution time of a program depends on the hardware on which it is running. Every new hardware realization requires the development of new timing analysis tools. 2. The development process of such analysis tools is becoming increasingly error-prone and time-consuming for modern, complex hardware realizations.

PRET tackles both of these challenges. By introducing a timed semantics for the instruction set architecture, timing becomes a property of programs rather than a property of programs running on particular hardware realizations. As a consequence, programs can be ported from one realization to the next without having to recertify and develop new timing analysis tools. Furthermore, due to the simplicity of the timing model associated with the ISA, precise and efficient timing analysis becomes possible. We anticipate this work to entail a paradigm shift in the development of hardware realizations for embedded systems: instead of focusing on improving performance, new hardware realizations will be developed that optimize aspects such as energy and power consumption, implementation cost, and reliability.

In the past year, we have taken the following steps towards the PRET vision:

* We have introduced four so-called "deadline" instructions, which introduce control over timing at the ISA level. These instructions allow enforcing upper and lower bounds on the execution time of blocks of code and they provide the ability to act upon deadline misses. As higher-level models of computation (MoC) often have a timed semantics, the deadline instructions can be used to implement such MoCs at the binary level, thereby filling a void in the model-based development of high-confidence systems from high-level models to low-level realizations. This work [DAC‚2011] has been presented at DAC 2011.
* We have continued the development of a prototypical PRET processor called PTARM, which shall implement the four deadline instructions and provide predictable timing behavior [Asilomar‚2010]. In particular, we have developed a new DRAM controller which provides predictable and composable memory access times to the four hardware threads of the PTARM core. This work [CODES‚2011] is currently under review at CODES+ISSS 2011.

Related publications since the last report:

[CODES‚2011] Jan Reineke, Isaac Liu, Hiren Patel, Sungjun Kim, Edward A. Lee. PRET DRAM Controller: On the Virtue of Privatization. (submitted to CODES+ISSS 2011)

[DAC‚2011] Dai Bui, Edward A. Lee, Isaac Liu, Hiren D. Patel, Jan Reineke. Temporal Isolation on Multiprocessing Architectures. In DAC, June 2011.

[Asilomar‚2010] Isaac Liu, Jan Reineke, Edward A. Lee. A PRET Architecture Supporting Concurrent Programs with Composable Timing Properties. In 44th Asilomar 2010.

### Architectural Modeling (Krogh)

We have continued the development of an architectural approach to multi-modeling for the development of complex embedded control systems. Models in heterogeneous formalisms are related by associating each model with an architectural view of a base architecture. Structural consistency is evaluated through the analysis of graph morphisms, with algorithmic methods for identifying inconsistencies in connectivity and encapsulations. These methods have been applied to the analysis of multiple heterogeneous models of the STARMAC quadrotor system. We have also performed an architectural analysis and restructuring of the lower-level control system for the quadrotor in our laboratory. We also developed a new approach to specifying and analyzing semantic consistency between models through the evaluation of logical conditions on the constraints on model parameters. Plug-ins for both structural and semantic consistency are being developed during the last months of the project.

Related publications since the last report:

A. Bhave, B. H. Krogh, D. Garlan, B. Schmerl, Multi-domain modeling of cyber-physical sytems using architectural views, Analytic Virtual Integration of Cyber-Physical Systems Workshop, San Diego, CA, Nov 2010.

A. Bhave, B. H. Krogh, D. Garlan, B. Schmerl, View consistency in architectures for cyber-physical systems, International Conf. on Cyber-Physical Systems (ICCPS), Chicago, IL, Apr 2011.

## Composable Tool Architectures

### Prototype Tool Chain (Karsai, Sztipanovits)

Since last April we have completed TrueTime and xPC Target simulations of the Starmac quadrotor and distributed controllers. We have been working since then on ESMoL integration with statistical model checking, and on testing our controller approach using the Ascending Technologies Hummingbird Quadrotor. Paolo Zuliani from CMU visited in May and helped us get set up with an initial example and preliminary version of their statistical model checking tools. During October 2010 we presented a technique for online stability checking of software controllers at EMSoft (in Scottsdale, AZ). We have presented our software modeling, platform simulation, and code generation work at the AFRL-Sponsored Safe & Secure Systems & Software Symposium (S5) in June 2010 and we are presenting a preliminary design for software fault modeling at S5 in June 2011. We also developed an incremental technique for cycle analysis in hierarchical models which will be presented at the Software Composition conference in Zurich in June 2011. Joe Porter completed his dissertation titled 'Compositional and Incremental Modeling and Analysis for High-Confidence Distributed Embedded Control Systems', defended in March 2011. It covers the work on ESMoL modeling, analysis, and hardware-in-the-loop simulation, cycle checking, and a new approach for incremental scheduling.

Related publications since the last report:

Porter, J., G. Hemingway, H. Nine, C. vanBuskirk, N. Kottenstette, G. Karsai, and J. Sztipanovits, The ESMoL Language and Tools for High-Confidence Distributed Control Systems Design. Part 1: Language, Framework, and Analysis, Tech Report ISIS-10-109, Nashville, TN, Vanderbilt University, 09/2010.

Porter, J., G. Hemingway, N. Kottenstette, H. Nine, C. vanBuskirk, G. Karsai, and J. Sztipanovits, "New Developments in Model-Integrated Development of High-Confidence Software", (Presentation) Safe and Secure Systems & Software Symposium, Beavercreek, OH, 06/2010.

Porter, J., G. Hemingway, N. Kottenstette, G. Karsai, and J. Sztipanovits, "Online Stability Validation Using Sector Analysis", International Conf. on Embedded Software (EMSoft), Scottsdale, AZ, ACM, pp. 29-38, 10/2010.

Hemingway, G., J. Porter, N. Kottenstette, C. vanBuskirk, G. Karsai, and J. Sztipanovits, "Automated synthesis of time-triggered architecture-based TrueTime models for platform effects simulation and analysis", Rapid System Prototyping, Fairfax, VA, IEEE, pp. 1-7, 10/2010.

Porter, J., D. Balasubramanian, G. Hemingway, and J. Sztipanovits, "Towards Incremental Cycle Analysis in ESMoL Distributed Control System Models", Software Composition (SC 2011) (Work-in-progress paper), vol. LNCS 6708, Zurich, Springer, pp. 133-140, 2011.

Porter, J., D. Balasubramanian, G. Hemingway, and J. Sztipanovits, Towards Incremental Cycle Analysis in ESMoL Distributed Control System Models, , no. ISIS-11-106, Nashville, TN, ISIS, Vanderbilt University, 04/2011

Zhang, Z., J. Porter, N. Kottenstette, X. Koutsoukos, and J. Sztipanovits, "High Confidence Embedded Software Design: A Quadrotor Helicopter Case Study", International Conference on Cyber-Physical Systems (ICCPS 2011) (Work-in-Progress Session), Chicago, IL, IEEE Computer Society Press, 04/2011

Porter, J., G. Hemingway, G. Simko, N. Kottenstette, H. Nine, C. vanBuskirk, G. Karsai, and J. Sztipanovits, "Modeling, Automatic Fault Simulation, and Statistical Verification in ESMoL (pieces of a work in progress)", Invited Talk, Safe and Secure Systems & Software Symposium, Beavercreek, OH, 06/2011.

## Testing and Experimental Validation (Tomlin, Sastry, Krogh, Lee, Karsai)

We continued testing the baseline controller design of the UAV platforms on the emerging model-based design tool suite. Experimental demonstrations were shown on our quadrotors (at all universities) above, and we continue to collaborate across MURI sites on the control development for the quadrotor platform.

We gave started using a new quadrotor platform from Ascension Technologies (Germany) that allows us to us higher-performance microcontrollers. We have adapted our model-based toolchain for the new platform, modeled controllers, and generated code from the models for the platform. Some simple maneuvers have been successfully executed on the platform.

# Acknowledgment/Disclaimer

This work was sponsored (in part) by the Air Force Office of Scientific Research, USAF, under grant/contract number FA9550-06-0312. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Air Force Office of Scientific Research or the U.S. Government.