**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

Year 4 Progress Report

Vanderbilt University
Institute for Software Integrated Systems
2015 Terrace Place, Nashville, TN 37203
(615) 322-3455 (office)
(615) 343-7440 (fax)
janos.sztipanovits@vanderbilt.edu

TEAM MEMBERS:

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

1. Objectives

This project aims to develop a comprehensive approach to the model-based design of high-confidence distributed embedded systems. We will take advantage and fully 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 objectives of our research in the focus areas are the following:

1. Develop theory of deep composition of hybrid systems with attributes of computational and communication platforms. We will address compositionality, concurrency, heterogeneity and resource, robustness, approximate verification and adaptive control architectures for uncertainty handling.
2. Develop foundations of model-based software design for high-confidence, networked embedded systems applications. We will investigate new semantic foundations for modeling languages and model transformations, precisely architected software and systems platforms that guarantee system properties via construction, and new methods for static source code verification and testing, as well as for dynamic runtime verification and testing.
3. Develop composable tool architecture that supports high-level reusability of modeling, model-analysis, verification and testing tools in domain-specific tool chains. We create new foundation for tool integration that goes beyond data modeling and data transfer.
4. Demonstrate the overall effort by creating an end-to-end design tool chain prototype for the model-based generation and verification of embedded controller code for experimental platforms.

2. Status of the Effort

We have reached the following major milestones toward the compositional design of high confidence embedded control systems on computational and communication platforms.

1. We have developed a modular code generation mechanism for hierarchical SDF models. As hierarchical SDF models are themselves not compositional, we proposed so-called DSSF profiles, which form a compositional abstraction of composite actors that can be used for modular compilation. Our method guarantees maximal reusability, but it also allows to tradeoff reusability for greater modularity.
2. Including semantic information in models helps to expose modeling errors early in the design process. We have developed a correct, scalable and automated method to infer semantic properties using lattice-based ontologies, given relatively few manual annotations. We have demonstrated the approach on a nontrivial Ptolemy II model of an adaptive cruise control system. The paper presenting this work [2] was the recipient of the MODELS 2009 Distinguished Paper Award. We have released Ptolemy II 8.0.beta on February 26, 2010 including the following new or greatly improved features:

- Model Transformation -a framework for the analysis and transformation of actor models using model transformation techniques
- Ptera (Ptolemy Event Relationship Actor) Domain
- Causality Analysis: Updates to our non-conservative causality analysis for modal models within discrete-event (DE) systems
- Continuous and Modal Domains: a substantial rework of modal models and the underlying finite state machine infrastructure to make them work predictably and consistently across domains.

3. We have enriched a significant subset of hierarchical Ptolemy II DE models with formal verification capabilities using Real-Time Maude as back-end. To this end, we formalized in Real-Time Maude the semantics of a subset of hierarchical Ptolemy II DE models, and used the code generation infrastructure of Ptolemy II to automatically synthesize a Real-Time Maude verification model from a Ptolemy II design model. This enables a model-engineering process that combines the convenience of Ptolemy II DE modeling and simulation with formal verification in Real-Time Maude.

4. We have extended our open toolchain to use the TrueTime tool for the simulation-based analysis of controllers. We generate a plant and controller-specific TrueTime scheduler that mimics the execution semantics of the time-triggered platform, and use the actual functional code and actual schedule that has been generated by the toolchain for closed-loop analysis of the controller's performance.

5. We have started work on a revised version of the time-triggered software platform that ESMoL models are executed upon. The new FRODO virtual machine layer provides much more comprehensive error detection and correction and efforts are ongoing to add a robust event-based execution aspect to the VM for task dispatch and inter-node communications.

6. Over the past year, we have had a strong focus on both development of theory for hybrid systems and some exciting experimental results. We have developed a method for automatic control design for hybrid systems using reachable sets. We have designed a methodology for optimal control of hybrid systems. The former has been demonstrated on the quadrotor vehicles, the latter in simulation. In addition, we have demonstrated our earlier reachable set code in real time quadrotor aerobatics. Our next and final year of the MURI will see a continuation of the theoretical and algorithmic development for hybrid systems, and continued collaboration across the MURI locations on the quadrotor on experimental demonstrations.

7. We have created and implemented an inherently distributed and passive communication architecture, which allows strictly-output passive, dynamical systems to be coupled through any discrete time overlay network in a stability-preserving manner, regardless of time-varying delays and data loss.

8. We have continued development of an architectural approach to managing consistency across heterogeneous models used for design and verification of embedded control systems. A new cyber-physical system (CPS) architectural style has been developed in which components and connectors for physical systems are first-class elements along with the components and connectors used in traditional software architecture description languages (ADLs). The multiple models and modeling formalisms used for embedded control system design are integrated as architectural views of the base CPS architecture

for a system. This architectural approach is currently being applied and evaluated for the STARMAC quadrotor.

3. Accomplishments and New Findings

We continued our work on developing tools, methods and other components of the project along the four objectives.

3.1 Hybrid and Embedded Systems Theory

3.1.1 Hybrid and Embedded Systems Theory (Lee)

Finite State Machines and Modal Models in Ptolemy II Finite-state machines (FSMs) and modal models provide a very expressive way to build up complex model behaviors. As a consequence of this expressiveness, it takes some practice to learn to use them well. Edward Lee has compiled a technical memorandum [1] that describes the usage and semantics of FSMs and modal models in Ptolemy II.

FSMs are actors whose behavior is described using a finite set of states and transitions between the states. The transitions between the states are enabled by guards, which are boolean-valued expressions that can reference inputs to the actor and parameters in scope. The transitions can produce outputs and can update the value of parameters in scope. Modal models extend FSMs by allowing states to have refinements, which are hierarchical Ptolemy II models. The refinements may themselves be FSMs, modal models, or any composite actor containing a director compatible with the domain in which the modal model is being used. On the basis of several examples, the memorandum describes the operational semantics, the practical usage, and the semantics of time in modal models.

Each of the figures in the document corresponds to an executable Ptolemy II model. To execute and experiment with these models the reader can simply click on the corresponding figures in the document. There is no need to pre-install Ptolemy II or any other software.

3.1.2 Constructive Architectures for Digital Controllers of Continuous Time Systems (Kottenstette)

We have recently demonstrated how to interconnect either a linear or non-linear interior-conic continuous time systems (in which passive systems are a special case) to an appropriately constrained conic digital controller in which continuous time stability (Lm2-stability) can be guaranteed in spite of time varying delay. The key to achieving a stronger result and further weaken our initial passivity assumptions of the continuous time system is to explicitly consider the resulting conic-system properties resulting from the feed-back loops created from our use of wave-variables. Initial results demonstrate improved rejection of high-frequency noise which can be effectively filtered with multi-rate passive samplers (PS:MTs) and passive hold devices (PH:M Ts) while achieving better performance over traditional sample-and-hold digital control systems. As a result, we can now control the position of robotic-arm-manipulators using direct position feedback instead of indirect velocity feedback. In addition we have shown that the in-

ner-product-equivalent-sampler and zero-order-hold (IPESH) not only preserves passivity properties of a given system but preserves the more general interior-conic system properties as well. The implication is that like the bilinear-transform which preserves both passivity and stability properties when mapping a continuous linear time invariant (LTI) system to a discrete LTI system, the IPESH in general preserves stability for non-linear interior conic systems such that if the IPESH is applied to a continuous interior conic system which is inside the sector [a,b] then the resulting discrete-time system whose output is scaled by (1/Ts) remains inside the sector [a,b]. These results should extend to those related to control over power-junction-networks.

Some of our past reported work related to control over power-junction-networks will appear in IJSCC's Special Issue on Progress in Networked Control Systems. However new results involving these control networks continue to be discovered. We have demonstrated that a simplified linear-power- junction-network can be used in distributed deployment of point-mass systems whose inertial position control system closely resembles that used to control position for our quadrotor aircraft. Furthermore a resilient-power-junction-network has also been demonstrated to allow a single plant to be reliably controlled by many redundant digital controllers in order to better withstand both denial-of-service (DOS) attacks and even safely handle certain compromises of the redundant controllers. The linear-power-junction-network appears to be a good candidate for networked control of quadrotor aircraft as well as fixed-wing aircraft.

In order to better study formation control of fixed wing aircraft for a potential aerial refueling scenario posed at our 2009 review we had to develop an inertial control system and model of a fixed wing aircraft. Therefore we developed and verified an advanced Simulink-based fixed-wing model of the Cessna A-37 whose velocity flight-path and heading angles were maintained by a resilient backstepping control law. The backstepping control law was derived using a simplifying small-angle assumption involving the angle of attack and bank angle while maintaining the side-slip angle near zero. It achieves performance close to its adaptive counterparts while allowing for system model verification. In addition we demonstrated that if we filter one of the feedback terms typically required to achieve asymptotic stability results for our backstepping controller then we could better withstand discrete time wind gusts. In general we proved our backstepping control law can be applied not only to the control of fixed-wing aircraft but other non-linear systems which posses triangular structures and invertible controller affine terms. Finally, we demonstrated that a classical anti-windup compensator can be applied to the velocity control system when subject to control thrust saturation which can occur during aggressive maneuvers. Using the small angle assumption allowed us to significantly simplify our backstepping control law for our fixed-wing aircraft, however, the quadrotor aircraft control system was still much less complicated. Although both systems share the same kinematic equations of motion, the fixed-wing aircraft dynamics depend heavily on the wind velocity vector. As a result it is not clear how to exploit the passivity like subsystems related to the kinematics in order to simplify the control design as was done for the quadrotor aircraft. However, one technique to simplify controller design which looks promising is Interconnection Damping Assignment Passivity Based Control (IDA-PBC).

IDA-PBC attempts to derive control laws which attempt to exploit the passivity like properties of a system in order to derive a dissipative structure which achieves asymptotic stability. Unlike backstepping control laws, IDA-PBC is not as an aggressive method in attempting to

cancel non-linear terms in the system in order to make it appear as a cascade of integrators. As a result the IDA-PBC control laws are typically less computationally intensive and possess more linear feed-back terms similar to those seen with our quadrotor control system. Therefore, we have studied, implemented and refined an IDA-PBC control algorithm initially presented by Johnsen & Allgower related to the control of a four-tank process. We have developed preliminary tools to automatically generate IDA-PBCs while providing improved integrator anti-windup compensators. Furthermore we determined that the bilinear-transform works quite well in implementing low-sampling rate (possibly non-linear) integrator terms in theses IDA-PBCs. Furthermore IDA-PBC allows us to determine explicit gain and trajectory constraints to apply to our controller implementation in order to further improve system resilience.

3.1.3 **Robust Group Consensus**

For many sensing, surveillance, or tracking applications, it is often desirable to deploy a group of unmanned aerial vehicles (UAVs) for reconnaissance or scouting using consensus algorithms for decentralized control. Using large numbers of UAVs equipped with surveillance and sensing equipment is beneficial because redundancy reduces the likelihood of missing interesting events in the presence of obstructions caused by non-uniform terrain, man-made structures, or man-made interference. Therefore, we aim to develop methods that utilize decentralized control of UAVs to enhance security and redundancy for group coordination problems.

Performing coordinated consensus tasks such as establishing a formation or output synchronization requires local interactions (e.g., via message passing) in a discrete-time framework for multi-agent systems. However network uncertainties such as delays and dropped packets introduce additional challenges to achieving the desired task. In particular, stability of the networked system can be jeopardized by these effects. To circumvent the stability problems caused by the discrete-time implementation of multi-agent networks, a compositional approach has been created using passivity, which ensures l_{m2}-stability of the global system whenever the individual components are passive. Specifically, we have created and implemented an inherently distributed and passive communication architecture, which allows strictly-output passive, dynamical systems to be coupled through any discrete time overlay network in a stability-preserving manner, regardless of time-varying delays and data loss.

The specific problem we consider for our application of the passive communication architecture is the situation where n agents distributed randomly in a two-dimensional environment attempt to create a formation surrounding a target position. Each agent has a neighborhood within which it is able to communicate, and no information is shared globally.

Figure 1 presents an example three node neighborhood communication scheme between nodes i, j, and q. Each node sends position information encoded as a wave variable u(k) to a "delay" state d(k). The delay state passes the delayed information v(k) as an input to the corresponding node. The entire scenario is made of collections of these neighborhoods that have overlapping nodes.
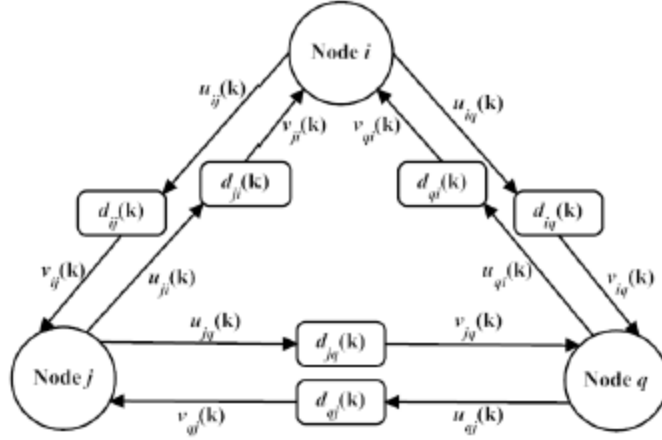
Figure 1. An example3-node communication network, illustrating the delay terminology.

We have developed and tested the decentralized passivity and consensus algorithms for multiple UAV formation control. We verified using simulations that the algorithms perform well in the presence of communication delays and dropouts, and have been shown to work well for systems even in the presence of large communication loss or delays.

One of our experimental scenarios involved a network of eight UAVs distributed in a regular lattice network structure. Each UAV has four neighbors that it can communicate with using our passivity framework over the network, and we modeled a 10% probability of packet loss. The scenario was modeled using Matlab and TrueTime for network communication simulation. Figure 2 presents snapshots of the UAV positions at various times during the simulation. It can be seen that the UAVs end up surrounding the target in the desired formation even with the network interference.
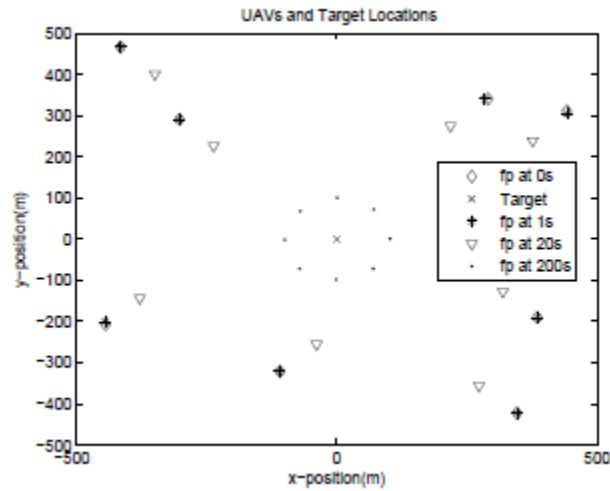
Figure 2. Progression of UAVs to desired locations in presence of 10% packet loss.

3.1.4 **Embedded Convex Optimization (Boyd)**

This work concerns the use of convex optimization in high speed, real-time embedded systems, such as those found for signal processing, automatic control, estimation, resource allocation and decision making. While convex optimization is widely used on time scales of seconds or minutes, typically with a skilled engineer 'in the loop' supervising the optimization solver, it is less commonly seen for real-time applications.

A primary concern in real-time or embedded applications is the solver speed. We have addressed this for a variety of applications, including using hand-coded solvers, including software for high-speed model predictive control (MPC). Taking this work further, we have created an automatic code generator, CVXGEN, which takes a high-level description of a convex optimization problem and automatically generates compilable, library-free C code for a high speed solver.

This enables extensive (automatic) customization for the problem at hand, and makes solution much faster than existing methods. While with a hand-written solver, even small changes in problem specification necessitated painstaking redesign, even a complete change only requires the use of CVXGEN to automatically generate new code. This, combined with extremely fast solvers that carry out convex optimization on millisecond or even microsecond time scales, means that many new applications are possible, particularly for embedded systems.

A parallel branch of work investigates high-speed control algorithms for use in linear stochastic control. Here we evaluate a control-Lyapunov policy at each time step. For small problems the associated QP can be solved explicitly, but for larger problems on-line optimization is required. This means the control-Lyapunov policy is often considered excessively computationally intensive for real-time or embedded systems. We have demonstrated several techniques for accelerating evaluation of control-Lyapunov policies, including the pre-computation of certain quantities, and the use of performance bounds that enable much faster approximate policies to be used instead. The performance bounds are computed offline using linear matrix inequalities and semidefinite programming.

3.1.5 **Statistical Probabilistic Model Checking (Clarke, Donzé)**

Statistical Model Checking is an efficient technique for solving the Probabilistic Model Checking problem that is, finding out whether a system satisfies a specification with at least (or at most) a fixed probability. For example: "does the system fulfill a request within 1ms with probability at least 0.99?"

Our Statistical Model Checking approach encompasses both hypothesis testing and estimation, and it is based on Bayes' theorem and sequential sampling. Bayes' theorem enables us to incorporate prior information about the model being verified, where available. Sequential sampling means that the number of sampled traces is not fixed a priori, but it is instead determined at "run-time", depending on the evidence gathered by the samples seen so far. This often leads to significantly smaller number of sampled traces (simulations). Our estimation method follows directly from our Bayesian approach. In fact, Bayes' theorem enable us to obtain the posterior distribution of the true probability p with which the model satisfies the formula (i.e., the distribution

of *p* according to the data sampled and chosen prior). By integrating the posterior over a suitably chosen interval, we can compute a Bayes interval estimate with any given confidence coefficient. We have continued investigating the applicability of Bayesian Statistical Model Checking to the verification of Probabilistic Bounded Linear Temporal Logic (PBLTL) properties of Simulink/Stateflow (SL/SF) models. The technique combines model checking of system simulation traces and statistical techniques to infer whether a property is true or not. In particular, it uses Bayesian hypothesis testing and estimation. We have proved error bounds for both statistical techniques. We have applied the approach to a SL/SF model implementing a fault-tolerant fuel control system for a gasoline engine, with very good performance results. In particular, our estimation method can be orders of magnitude faster than other estimation-based model checking techniques. This work was presented at the HSCC 2010 conference.

First-year student Anvesh Komuravelli (CMU) has devised and implemented a model checker for BLTL formulas. The algorithm analyzes system traces "on the fly", i.e., element by element, without requiring access to the full trace. This feature is highly desirable for Statistical Model Checking, because we wish to stop system simulation as soon as we can decide whether a BLTL property is true or false on the current trace. Also, the algorithm does not store any information about the trace being analyzed, so its memory requirements are minimal. A technical report is forthcoming.

On 17-19 May 2010, Paolo Zuliani (CMU) visited Vanderbilt, in order to start integrating CMU's statistical model checking techniques with Vanderbilt's tool chain. Work focused in particular on the verification of a Stateflow/Simulink model for the STARMAC Quadrotor controller. Faults were injected into the model as missing sensors' readings. Fault occurrence and duration were modeled by a Poisson process and by an exponential distribution, respectively. We verified PBLTL properties of the Quadrotor, e.g. "with probability at least 0.99, over the next 200 seconds it is never the case that the Quadrotor strays from the target path more than *threshold* for more than 10 seconds", where *threshold* can be chosen to test different levels of design strength. Our initial findings confirm that statistical model checking can be effectively applied for the verification of real-world embedded systems.

3.1.6 **Verification of Hybrid Systems via Differential Invariants (Clarke, Platzer)**

André Platzer has written a book about hybrid systems verification that will appear with Springer as "Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics." This book describes basic and advanced verification techniques for hybrid systems, including applications to air traffic control analysis. It will be a good introduction for graduate students working in the area.

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

The CPS architectural style has been implemented in ACMEStudio with annotations on components and connectors to encode behavioral semantics using finite state processes (FSP) and linear hybrid automata (LHA). Plug-ins generate models for existing verification tools, providing an integrated framework for analysis using heterogeneous models and tools. We are demonstrating through a set of test cases how the CPS architecture becomes a unifying context for

maintaining consistency between models and drawing implications from multiple verification activities through assume-guarantee constructs.

3.1.2 Hierarchies of Robust Hybrid and Embedded Systems (Tomlin, Krogh, Sastry)

We have investigated the use of simulation relations between hybrid automata as a tool for performing assume-guarantee (AG) reasoning, illustrating the two fundamental issues that limit scalability of the AG approach to hierarchical and large-scale applications: finding assumptions that serve as provably correct environments for components, and computing simulation relations algorithmically. We have developed a set of heuristics to address both of these problems and have demonstrated their effectiveness for a set of case studies. We are currently investigating ways to characterize the types of problems for which these heuristics are effective in general and are extending the studies to hierarchical decompositions of embedded control systems.

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

As we have demonstrated throughout the course of this MURI, the control of complex nonlinear systems can be aided by modeling each system as a collection of simplified hybrid modes, each representing a particular operating regime defined by the system dynamics, or by the region of the state space in which the system operates. Guarantees on the safety and performance of such hybrid systems can still be challenging to generate, however. Reachability analysis using a dynamic game formulation provides a useful way to generate these types of guarantees: reachable sets computed using Hamilton-Jacobi methods are flexible enough to analyze a variety of systems. As a result, reachability analysis has been used on a wide range of systems. In our work this past year, we used hybrid dynamic models and reachability tools to design provably safe aerobatic maneuvers. We applied this method to the STARMAC quadrotor helicopter performing a back-flip maneuver with three modes: impulse (initializing rotation), drift (motors off while rotating and free-falling), and recovery (return to controlled hover). Provably safe switching conditions on altitude, attitude, and their rates are generated using the solution of the Hamilton-Jacobi equation in the dynamic game formulation of reachable sets to guarantee that the vehicle will successfully pass through all three modes, to arrive at a specified, safe, final condition.

Figure 3: Reachable sets for the quadrotor backflip, shown in the in-plane angle phi (radians) and phi_dot (radians/s) plane. The quadrotor starts in the region labeled F (impulse mode), attains target set E, rotors switch off (D), drift mode (C), target set (B), recovery mode (A) to final
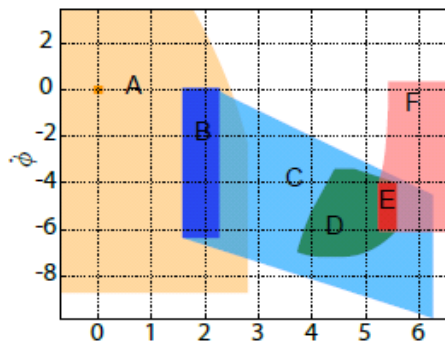
Figure 4: Showing an experimental demonstration of the quadrotor backflip in a mosaic. (a) The quadrotor has finished the climb portion of the backflip and is starting the impulse mode. (b) The quadrotor has finished the impulse stage and is entering into the drift portion. (b)-(f) Display of the drift stage of the backflip. (f) The drift mode is concluding and the recovery has started. (f)-(j) The recovery mode is safely returning the quadrotor to its hovering position.
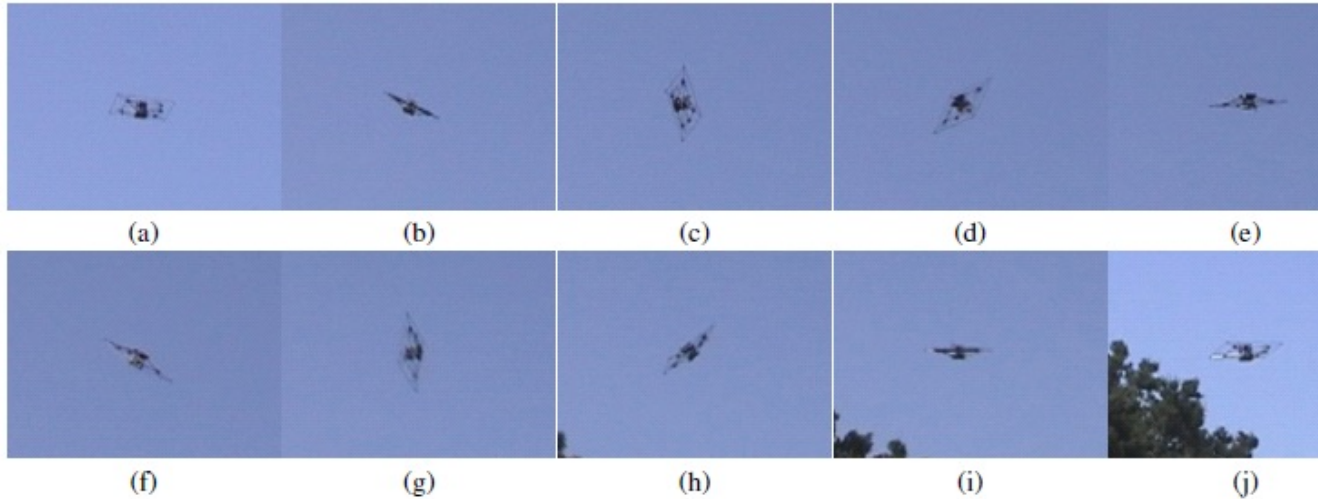

Figure 5: Three experimental validations (solid, dash, and dash-dot lines) of the backflip maneuver overlaid on the composite reach sets. The transitions from the impulse to drift mode are shown as black diamonds which are contained in the region E, and the transitions from the drift to the recovery mode are indicated by the black squares that are confined to region B.
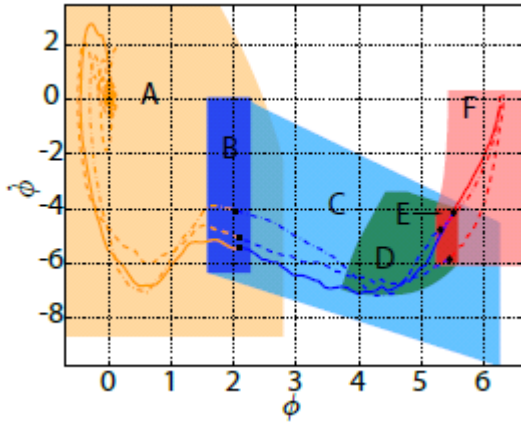
Reachability analysis. We have developed a method for automatically synthesizing controllers that provide hard guarantees of safety and target reachability for sampled and quantized switched systems under bounded continuous disturbances. Techniques from hybrid system verification are used to perform continuous time differential game calculations on each sampling interval, and iterative procedures are given for computing the set of states for which there exists a feasible control sequence that satisfies the properties of safety and reachability over a finite time horizon. From this computation, we show how to obtain explicit state feedback policies in the form of multiple reachable sets, and an algorithm is given for using this feedback law in closed

loop control of the system. We have applied the technique in simulation to an automated aerial refueling example, and in experiment to the quadrotor helicopter attempting to land on moving targets.

While previous methods for hybrid system reachability have found success in open loop verification of properties of hybrid systems, recovering an implementable control law that solves the reachavoid problem is in general nontrivial. In some special cases, it may be possible to find this control law by analytic calculations or by automatic verification tools. However, there are in general no systematic methods for synthesizing explicit feedback policies that can be used in closed loop control of hybrid systems with nonlinear continuous dynamics. This is the question we seek to answer in our recent work, under the restriction that: 1) the system is switched, 2) disturbance cannot affect discrete transitions. The controller synthesis method that we have developed is based upon the game theoretic hybrid controller developed earlier, with the advantage of being able to handle disturbances, nonlinear continuous dynamics, and possibly nonconvex state constraints. We extend previous efforts by formulating an iterative procedure for computing the explicit set-valued feedback law that can be used in closed loop control of sampled and quantized switched systems, in the form of multiple reachable sets. Due to the intimate connection of game theoretic techniques to optimal control, it becomes evident that the feedback policy we synthesize is the robust minimum time to reach controller for the switched system

Figure 6: Showing (top) the automated aerial refueling example; (bottom) the target set and reachavoid set in the relative (x-y) position and relative orientation of the UAV with respect to the tanker.
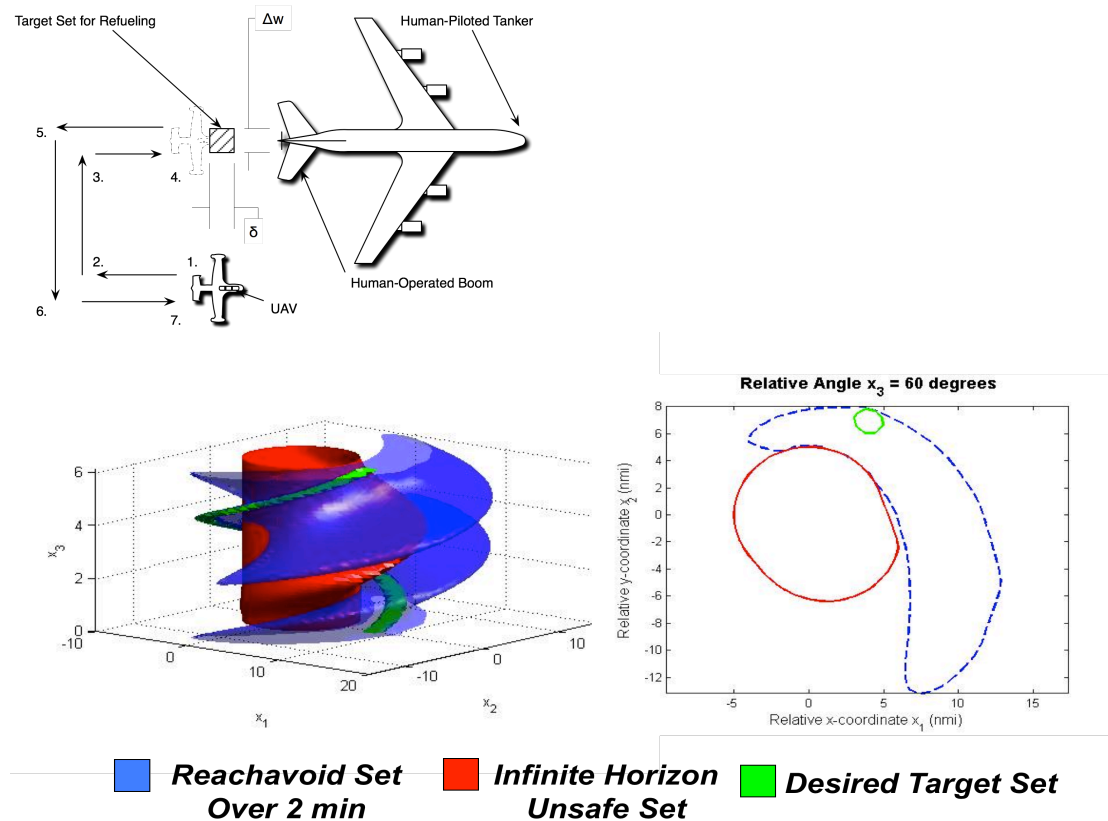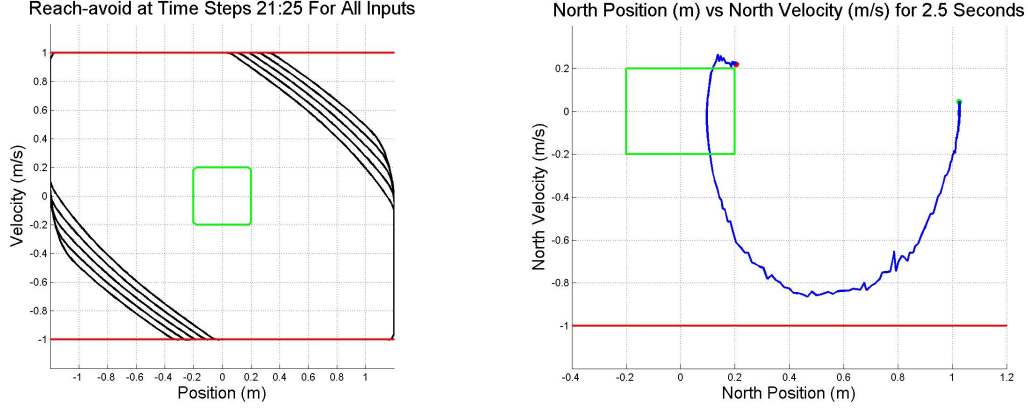
Figure 7: Experimental demonstration of new reachability calculations on STARMAC quad-rotor. (a) Sets computed from which the quadrotor can reach the target set while avoiding ground and limits on velocity. (b) Experimental data shown quadrotor flying this control law.

Optimization of hybrid systems. Switched dynamical systems have shown great utility in modeling a variety of systems. Unfortunately, the determination of a numerical solution for the optimal control of such systems has proven difficult, since it demands optimal mode scheduling. Recently, we constructed an optimization algorithm to calculate a numerical solution to the problem subject to a running and final cost. For such systems, the control parameter has both a discrete component, the sequence of modes, and two continuous components, the duration of each mode and the continuous input. We developed a bi-level hierarchical algorithm that divides the problem into two subproblems. At the lower level, we keep the modal sequence fixed and construct the optimal mode duration and optimal continuous input. At the higher level, we employ a single mode insertion technique to construct a new reduced cost sequence. We proved the convergence of this algorithm, and have illustrated its utility on several simulation examples, including flight planning for the STARMAC quadrotor. Recently, we modified our original approach in three ways to make our algorithm's application more tenable. First, we transformed our algorithm to allow it to begin at an infeasible point and still converge to a lower cost feasible point. Second, we incorporated multiple waypoints into our cost function, which makes the development of an optimal control in the presence of multiple objectives viable. Finally, we extended our approach to penalize the number of hybrid jumps.

3.2.2 Autocoding Embedded Software for Safety Critical Systems (Lee)

Modular Code Generation for SDF. Modeling languages with built-in concepts of concurrency, time, I/O interaction, and so on, are particularly suitable in the domain of embedded systems. Languages such as Simulink, UML or SystemC, and corresponding tools, are particularly popular in this domain, for various applications. The tools provide modeling and simulation, but often also code generation and static analysis or verification capabilities, which are increasingly im-

portant in an industrial setting. A widespread model of computation in this domain is Synchronous Data Flow (SDF).

To manage complexity, as with other models, SDF models are built in the Ptolemy framework in a modular, hierarchical manner. But hierarchical SDF models are not compositional: a composite SDF actor cannot be represented as an atomic SDF actor without loss of information that can lead to deadlocks. Motivated by the need for incremental and modular code generation from hierarchical SDF models, we have studied the problem of developing a compositional SDF representation.

For this purpose, we propose DSSF profiles. DSSF (Deterministic SDF with Shared FIFOs) forms a compositional abstraction of composite actors that can be used for modular compilation.

1. We have developed algorithms for automatic synthesis of non-monolithic DSSF profiles of composite actors given DSSF profiles of their sub-actors.
2. We show how different tradeoffs can be explored when synthesizing such profiles, in terms of modularity (keeping the size of the generated DSSF profile small) versus reusability (preserving information necessary to avoid deadlocks) as well as algorithmic complexity.
3. We show that our method guarantees maximal reusability and report on a prototype implementation.

Ptolemy Hierarchical Orthogonal Multi-Attribute Solver. The Ptolemy Hierarchical Orthogonal Multi-Attribute Solver (PtHOMAS) project (in conjunction with Bosch Research Center, Palo Alto) is focused on enhancing model-based design techniques with the ability to include semantic information about data (what the data means) within models, to check consistency in the usage of data across models, and to optimize models based on inferences made about the meaning of the data.

Including semantic information in models helps to expose modeling errors early in the design process, engage a designer in a deeper understanding of the model, and standardize concepts and terminology across a development team. It is impractical, however, for model builders to manually annotate every modeling element with semantic properties. We have developed a correct, scalable and automated method to infer semantic properties using lattice-based ontologies, given relatively few manual annotations. Semantic concepts and their relationships are formalized as a lattice, and relationships within and between components are expressed as a set of constraints and acceptance criteria relative to the lattice. Our inference engine automatically infers properties wherever they are not explicitly specified. Our implementation leverages the infrastructure in the Ptolemy II type system to get efficient and scalable inference and consistency checking. We demonstrate the approach on a non-trivial Ptolemy II model of an adaptive cruise control system.

The paper "Scalable semantic annotation using lattice-based ontologies" [2] presenting this work was accepted at the MODELS conference, which had an acceptance rate of 15%. It was the recipient of the MODELS 2009 Distinguished Paper Award.

In a joint effort with Bosch, we started refactoring our ontologies implementation. We are taking what we learned about ontologies, doing a ground-up redesign and building a system that will be easier to use, extend and test.

Verifying Hierarchical Ptolemy II Discrete-Event Models using Real-Time Maude. Model-based design principles put the construction of models at the center of embedded system design processes. Useful models are executable, providing simulations of system functionality, performance, power consumption, or other properties. Ptolemy II is a well-established modeling and simulation tool, developed at UC Berkeley, that provides a powerful and intuitive graphical modeling language to allow a user to build hierarchical models that combine different models of computations including discrete-event (DE) models, which are explicit about timing behavior of systems. Discrete-event modeling is a time honored and widely used approach for system simulation.

Kyungmin Bae (University of Illinois at Urbana-Champaign), Peter Csaba Olveczky (University of Oslo), Thomas Huining Feng and Stavros Tripakis have enriched a significant subset of hierarchical Ptolemy II DE models with formal verification capabilities using Real-Time Maude as back-end. Real-Time Maude is a high-performance tool that extends the rewriting-logic-based Maude system to support the formal specification and analysis of object-based real-time systems. We formalized in Real-Time Maude the semantics of a subset of hierarchical Ptolemy II DE models, and used the code generation infrastructure of Ptolemy II to automatically synthesize a Real-Time Maude verification model from a Ptolemy II design model. This enables a model-engineering process that combines the convenience of Ptolemy II DE modeling and simulation with formal verification in Real-Time Maude. In particular, Ptolemy users can specify temporal logic properties to be verified without understanding how Ptolemy models are represented in Real-Time Maude. Real-Time Maude allows to verify live-ness properties, that cannot be checked using Ptolemy simulations. Furthermore, the synthesized verification model can be formally analyzed with respect to other properties (e.g., determinism, etc.).

3.3 Composable Tool Architectures

3.3.1 Advanced Open Tool Integration Framework (Karsai, Sztipanovits)

Formal specification of behavioral semantics. We have continued our efforts on the formal specification of behavioral semantics for domain specific modeling languages. In the last year we have started integrating with Sifakis' Behavior-Interaction-Priority (BIP) model as an abstraction layer in the design flow. Currently, we are working on two parallel tasks related to BIP. First, BIP uses Petri nets as an internal model of computation; therefore we are extending the FRODO virtual machine runtime layer to support non-time-triggered task execution and communication. Second, we are developing a BIP-to-ESMoL importer that will allow the toolchain to incorporate BIP defined software components into larger system designs. Once these two steps are complete, we plan on developing in the other direction, an ESMoL-to-BIP conversion. By converting ESMoL system definition, both hardware platform and software components, into a BIP model we can utilize the deadlock analysis tools within the BIP toolchain to ensure that the system execution will be deadlock free.

3.3.2 **Prototype Tool Chain (Karsai, Sztipanovits)**

Prototype toolchain. We continued our work on the prototype tool chain, based on the modeling language ESMoL. The toolchain has been extended with a TrueTime interface for timing analysis, and the functional and non-functional code generators have been significantly improved. The TrueTime interface makes the high-fidelity simulation based analysis of controller designs feasible. The actual functional code and the actual schedule (generated by other toolchain elements) are used in the analysis; hence the platform effects are directly observable. The TrueTime interface is now based on actual TrueTime 'kernel' that simulates the run-time platform's scheduler.

For the STARMAC quadrotor helicopter control system we can generate platform-specific code from models, and run a time-triggered distributed controller in a hardware-in-the-loop configuration to detect design and software generation errors. We have a prototype integration of the CMU statistical model checking tools with our STARMAC model to analyze the robustness of our design to fault conditions. We also have a preliminary analysis of the delay effects of different data links with respect to the passivity assumptions in a simplified version of the quadrotor design.

As mentioned above, we are currently extending the FRODO virtual machine to support event-based task execution or communication. The online scheduler within FRODO now handles the dispatch of both time-triggered and event-based tasks. The time-triggered tasks maintain a higher priority than the event-based ones in order to not invalidate the TTA invariants.

We have experimented with model-based constructive control design approaches, including a custom modeling language for building and simulating simple passive digital controllers, and a prototype symbolic controller generation tool for nonlinear port-Hamiltonian control designs.

We have revised the integration of the TrueTime simulation and verification toolbox with the tool chain. This integration now allows the high-fidelity simulation of the control system together with the plant, such that all platform effects (such as delays caused by message transfers and scheduling jitter) are faithfully included. Once the controller models are componentized, and the component deployment is modeled, the offline scheduling tool produces a feasible schedule. This schedule is then used to configure the TrueTime simulation, such that platform effects in the closed loop control could be studied. Observations on this simulation provide valuable feedback for the designer on how well the actual controller implementation will work in the real environment. Once the design is found satisfactory, the code can be generated and deployed on the real platform (robo+gstix) and its performance studied using a Hardware-in-the-Loop simulation (utilizing the XPC platform from Mathworks).

3.4 **Testing and Experimental Validation (Tomlin, Sastry, Lee, Karsai)**

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

platform. A prototype software test generation framework has been developed, which is being applied to a multi-core implementation of the Cessna fixed-wing backstepping controller (in progress). This prototype was run as a class research project, with students working to implement the controller on the Cell processor architecture executing a local time-triggered scheduler.

We continue to refine the real-time simulation environment for the Stanford STARMAC quadrotor aircraft control software. The interface between the plant simulator and the controller is 'hard real-time', and the xPC box simulates the real-time behavior of the plant with high-fidelity (e.g., inner loop control can be easily run at 100Hz). The control software is generated and con-figured with the tool chain. We have started investigating the use of small quadrotor devices from Ascension Technologies. We have worked on the communication interface, but the deployment of actual controller code on the platform is future work.

4. Personnel Supported

Vanderbilt:

1. Professor Janos Sztipanovits (PI)
2. Professor Gabor Karsai
3. Nicholas Kottenstette (Research Scientist, funded by this contract)
4. Joe Porter (Graduate Student, funded by this contract)
5. Graham Hemingway (Graduate Student, funded by this contract)

Associated but not supported:

1. Harmon Nine (Senior Engineer, funded elsewhere)

Berkeley:

1. Professor Claire Tomlin
2. Professor Edward A. Lee (Faculty, funded elsewhere)
3. Professor Shankar Sastry (funded elsewhere)
4. Man-Kit (Jackie) Leung (Research staff, funded by this contract)
5. Christopher Brooks (Software engineer, partially funded)
6. Jan Reineke (Postdoctoral scholar, partially funded)
7. Jerry Ding (Graduate student, funded by this contract)
8. Humberto Gonzales (Graduate student, funded by this contract)
9. Maryam Kamgarpour (Graduate student, funded by this contract)
10. Eugene Li (Graduate student, funded by this contract)

Associated but not supported:

1. Haomiao Huang (Graduate student, funded elsewhere)
2. Jeremy Gillula (Graduate student, funded elsewhere)
3. Michael Vitus (Graduate student, funded elsewhere)
4. Ben Lickly (Graduate student, funded elsewhere)
5. Thomas Huining Feng (Graduate student, funded elsewhere)

6. Stavros Tripakis (Research scientist, funded elsewhere)
7. Bert Rodiers (Graduate student, funded elsewhere)
8. Dai Bui (Graduate student, funded elsewhere)

CMU
1. Professor Edmund M. Clarke
2. Professor Bruce Krogh
3. Professor André Platzer (Faculty, funded elsewhere)
4. Alexandre Donzé (Postdoctoral scholar, funded by this contract)

Associated but not supported:

5. Anvesh Komuravelli (Graduate student, funded elsewhere)
6. Axel Legay (Postdoctoral scholar, funded elsewhere)
7. Azadeh Farzan (Postdoctoral scholar, funded elsewhere)
8. Himanshu Jain (Graduate student, funded elsewhere)
9. Paolo Zuliani (Postdoctoral scholar, funded elsewhere)
10. Matthias Althoff (Postdoctoral scholar, funded elsewhere)

Stanford:

1. Professor Stephen Boyd
2. Jacob Mattingley (Graduate student, funded by this contract)
3. Yang Wang (Graduate student, funded by this contract)

5. Publications

1. H. Gonzales, R. Vasudevan, M. Kamgarpour, S. S. Sastry, R. Bajcsy, and C. J. Tomlin, "A Numerical Method for the Optimal Control of Switched Systems", Submitted to the IEEE CDC, 2010.
2. H. Gonzalez, R. Vasudevan, M. Kamgarpour, S. Sastry, R. Bajcsy, and C. Tomlin, Computable optimal control of switched systems with constraints, Proceedings of the 13th International Conference on Hybrid Systems: Computation and Control, 2010.
3. J. Gillula, G. Hoffmann, H. Huang, M. Vitus, and C. J. Tomlin. "Applications of Hybrid Reachability Analysis to Robotic Aerial Vehicles", Submitted to IJRR, February 2010.
4. S. Shankaran, D. M. Stipanovic, and C. J. Tomlin, "Collision Avoidance Strategies for a Three Player Game", Accepted to appear in the Annals of the International Society of Dynamic Games, 2010.
5. J. Gillula, H. Huang, M. Vitus, and C. J. Tomlin, "Design of Guaranteed Safe Maneuvers using Reachable Sets Autonomous Quadrotor Aerobatics in Theory and Practice", In the Proceedings of the 2010 IEEE International Conference on Robotics and Automation, May 2010.
6. J. Ding and C. J. Tomlin, "Trajectory Optimization in Convex Underapproximations of Safe Regions", In the Proceedings of the 48th IEEE Conference on Decision and Control, December 2009.

7. J. Gillula, H. Huang, M. Vitus, and C. J. Tomlin, "Design of Guaranteed Safe Maneuvers using Reachable Sets: Autonomous Quadrotor Aerobatics in Theory and Practice", In the Proceedings of the 2010 IEEE International Conference on Robotics and Automation, May 2010.

8. J. Ding and C. J. Tomlin, "Trajectory Optimization in Convex Underapproximations of Safe Regions", In the Proceedings of the 48th IEEE Conference on Decision and Control, December 2009.

9. J. Ding and C. J. Tomlin, "Safety and reachability in switched nonlinear systems under sampling and quantization", Submitted to the IEEE CDC, 2010.

10. M. Kamgarpour and C. J. Tomlin, "Optimal Control of Non-Autonomous Switched Systems Under a Fixed Switching Sequence'", Submitted to the SIAM Journal on Control and Optimization, 2010.

11. J. Gillula, H. Huang, M. Vitus, and C. J. Tomlin, "Reachable Sets for Maneuver Scheduling and Design: Applications to Autonomous Quadrotor Aerobatics", In the Proceedings of the International Symposium on Robotics Research, September 2009.

12. J. Ding and C. J. Tomlin, "Aircraft conflict detection: a dynamic programming approach", In the Proceedings of the AIAA Guidance, Navigation, and Control Conference, August 2009.

13. E. A. Lee, "Finite state machines and modal models in ptolemy ii," EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-151, Nov 2009.

14. J. M.-K. Leung, T. Mandl, E. A. Lee, E. Latronico, C. Shelton, S. Tripakis, and B. Lickly, "Scalable semantic annotation using lattice-based ontologies," in 12th International Conference on Model Driven Engineering Languages and Systems. ACM/IEEE, October 2009, pp. 393–407, (recipient of the MODELS 2009 Distinguished Paper Award).

15. S. Tripakis, D. N. Bui, M. Geilen, B. Rodiers, and E. A. Lee, "Compositionality in synchronous data flow: Modular code generation from hierarchical SDF graphs," UC Berkeley, Tech. Rep. UCB/EECS-2010-52, May 2010.

16. S. Tripakis, D. N. Bui, B. Rodiers, and E. A. Lee, "Compositionality in synchronous data flow: Modular code generation from hierarchical SDF graphs (poster abstract)," in ACM/IEEE First International Conference on Cyber-Physical Systems, R. Rajkumar, Ed., April 2010.

17. K. Bae, P. C. Olveczky, T. H. Feng, and S. Tripakis, "Verifying Ptolemy II discrete-event models using Real-Time Maude," in ICFEM '09: Proceedings of the 11th International Conference on Formal Engineering Methods, December 2009, pp. 717–736.

18. K. Bae, P. Olveczky, T. H. Feng, E. A. Lee, and S. Tripakis, "Verifying hierarchical Ptolemy II discrete-event models using Real-Time Maude," UC Berkeley, Tech. Rep. UCB/EECS-2010-50, May 2010.

19. P. Zuliani, A. Platzer, Edmund M. Clarke: Bayesian Statistical Model Checking with Application to Stateflow/Simulink Verification. HSCC 2010: 243-252.

20. H. Jain, E. M. Clarke: Efficient SAT solving for non-clausal formulas using DPLL, graphs, and watched cuts. DAC 2009: 563-568.

21. E. M. Clarke, E. A. Emerson, and J. Sifakis: Model checking: algorithmic verification and debugging. Commun. ACM 52(11): 74-84 (2009).

22. H. Jain, E. M. Clarke, O. Grumberg: Efficient Craig interpolation for linear Diophantine (dis)equations and linear modular equations. Formal Methods in System Design 35(1): 6-39 (2009).

23. J. Mattingley, Y. Wang and S. Boyd, "Code Generation for Receding Horizon Control", manuscript, May 2010.
24. J. Mattingley and S. Boyd , "Real-Time Convex Optimization in Signal Processing", IEEE Signal Processing Magazine, 27(3):50-61, May 2010.
25. Y. Wang and S. Boyd, "Approximate Dynamic Programming via Iterated Bellman Inequalities", manuscript, April 2010.
26. Y. Wang and S. Boyd, "Fast Model Predictive Control Using Online Optimization", IEEE Transactions on Control Systems Technology, 18(2):267-278, March 2010.
27. J. Mattingley and S. Boyd,"Automatic Code Generation for Real-Time Convex Optimization", chapter in Convex Optimization in Signal Processing and Communications, Y. Eldar and D. Palomar, Eds., Cambridge University Press, 2009.
28. Y. Wang and S. Boyd, "Fast Evaluation of Quadratic Control-Lyapunov Policy", manuscript, July 2009.
29. Y. Wang and S. Boyd, "Performance Bounds and Suboptimal Policies for Linear Stochastic Control via LMIs", manuscript, May 2009.
30. Y. Wang and S. Boyd,"Performance Bounds for Linear Stochastic Control", Systems and Control Letters, 58(3):178-182, March 2009.
31. N. Kottenstette, J. Hall, X. Koutsoukos, P. Antsaklis and J. Sztipanovits, "Digital control of multiple discrete passive plants over networks", International Journal of Systems, Control and Communications (IJSCC), (Special Issue on Progress in Networked Control Systems (To Appear)).
32. Kottenstette, N. and Antsaklis, P.J. "Relationships between positive real, passive dissipative, & positive systems", in American Control Conference – ACC2010, 1–8., Baltimore, Maryland, USA.
33. Kottenstette, N., "Constructive non-linear control design with applications to quad-rotor and fixed-wing aircraft", Technical Report, Nashville, TN, Institute for Software Integrated Systems, Vanderbilt University, Jan. 2010.
34. Kottenstette, N., Porter, J., "Backstepping Control Design with Applications to Fixed-Wing Aircraft", (under review CDC 2010).
35. Kottenstette, N., G. Karsai, and J. Sztipanovits, "A Passivity-Based Framework for Resilient Cyber Physical Systems", ISRCS 2009 2nd International Symposium on Resilient Control Systems, Idaho Falls, ID, IEEE, 08/2009.
36. Kottenstette, N., Porter, J., Karsai, G. and Sztipanovits, J., "Discrete-Time IDA-Passivity Based Control of Coupled Tank Processes Subject To Actuator Saturation", 3rd International Symposium on Resilient Control Systems (ISRCS 2010), Under Review.
37. LeBlanc, H., Eyisi, E., Kottenstette, N., Koutsoukos, X., and Sztipanovits, J., "A passivity-based approach to deployment in multi-agent networks." In Proceedings of the 7th International Conference on Informatics in Control, Automation and Robotics (ICINCO 2010). SciTePress, Funchal, Madeira - Portugal.
38. Kottenstette, N., H. LeBlanc, E. Eyisi, and X. Koutsoukos, "Multi Rate Networked Control of Conic Systems", Technical Report, Nashville, TN, Institute for Software Integrated Systems, Vanderbilt University, 09/2009 (revised and under review CDC 2010).
39. J. Porter, G. Hemingway, C. vanBusKirk, N. Kottenstette, G. Karsai, J. Sztipanovits. "Online Dynamic Stability Verification Using Sector Search". Submitted to the ACM International Conference on Embedded Software (EMSoft) 2010.

40. G. Hemingway, J. Porter, N. Kottenstette, H. Nine, C. vanBuskirk, G. Karsai, and J. Sztipanovits. "Automated Synthesis of Time-Triggered Architecture-based TrueTime Models for Platform Effects Simulation and Analysis". To appear Rapid Systems Prototyping (RSP), 2010.

41. J. Porter, G. Hemingway, H. Nine, N. Kottenstette, C. vanBusKirk, G. Karsai and J. Sztipanovits. "On Semantically Consistent Tool Integration in Model-Based Cyber-Physical Systems Design." ACM Trans. in Embedded Comp. Sys. - Special Issue on the Synthesis of Cyber-Physical Systems (SCPS), submitted (Feb), 2010.

42. E. Eyisi, J. Porter, J. Hall, N. Kottenstette, X. Koutsoukos, and J. Sztipanovits, "PaNeCS: A Modeling Language for Passivity-based Design of Networked Control Systems" In 2nd Workshop on the Architecting and Constructing of Embedded Systems - Model-Based (ACES-MB). Denver, Colorado. Oct. 2009.

43. J. Porter, P. Volgyesi, N. Kottenstette, H. Nine, G. Karsai, and J. Sztipanovits, "An Experimental Model-Based Rapid Prototyping Environment for High-Confidence Embedded Software", 20th IEEE/IFIP International Symposium on Rapid System Prototyping (RSP'09), Paris, France, 06/2009.

44. A. Rajhans, S-W Cheng, B. Schmerl, D. Garlan, B. H. Krogh, C. Agbi, A. Bhave, An architectural approach to the design and analysis of cyber-physical systems, Proceedings of the 3rd International Workshop on Multi-Paradigm Modeling (MPM 2009), Denver, CO, Oct 2009.

45. Ajinkya Bhave, David Garlan, Bruce H. Krogh, Akshay Rajhans, and Bradley Schmerl, Architectural Modeling and Analysis of Cyber-Physical Systems, Embedded Real-Time Software and Systems, Toulouse, May 2010.

Publications from Previous Years

46. J. Porter, G. Karsai, J. Sztipanovits: Towards a Time-Triggered Schedule Calculation Tool to Support Model-Based Embedded Software Design In Proc. of ACM Intl. Conf. on Embedded Soft. (EMSOFT '09), Grenoble, France, Oct 2009.

47. J. Porter, Z. Lattmann, G. Hemingway, N. Mahadevan, S. Neema, H. Nine, N. Kottenstette, P. Volgyesi, G. Karsai, and J. Sztipanovits: The ESMoL Modeling Language and Tools for Synthesizing and Simulating Real-Time Embedded Systems, 15th IEEE Real-Time and Embedded Technology and Applications Symposium, San Francisco, CA, April, 2009.

48. J. Porter, P. Volgyesi, N. Kottenstette, H. Nine, G. Karsai, and J. Sztipanovits: An Experimental Model-Based Rapid Prototyping Environment for High-Confidence Embedded Software, 20th IEEE/IFIP International Symposium on Rapid System Prototyping (RSP'09), Paris, France, June, 2009.

49. J. Skaf and S. Boyd: "Analysis and synthesis of state-feedback controllers with timing jitter," IEEE Transactions on Automatic Control, 54(3):652-657, March 2009

50. A. Zymnis, S. Boyd, and D. Gorinevsky: "Relaxed maximum a posteriori fault identification," Signal Processing, 89(6):989-999, June 2009

51. Y. Xu, K.-L. Hsiung, X. Li, I. Nausieda, L. Pileggi, and S. Boyd: "Regular Analog/RF Integrated Circuits Design Using Optimization with Recourse Including Ellipsoidal Uncertainty," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 28(5):623-637, May 2009

52. J. Skaf and S. Boyd: "Nonlinear Q-design for convex stochastic control," To appear in IEEE Transactions on Automatic Control, 2009

53. M. Zavlanos, A. Julius, S. Boyd, and G. Pappas: "Identification of stable genetic networks using convex programming," Proc. American Control Conf., pages 2755-2760, June 2009

54. S. -J. Kim, K. Koh, S. Boyd, and D. Gorinevsky: "l_1 Trend Filtering," SIAM Review, problems and techniques, May 2009

55. A. Mutapcic, and S. Boyd: "Cutting-set methods for robust convex optimization with pessimizing oracles," Optimization Methods and Software, June 2009

56. H. Huang, G. M. Hoffmann, S. L. Waslander, and C. J. Tomlin, Aerodynamics and Control of Autonomous Quadrotor Helicopters in Aggressive Maneuvering, Proceedings of the IEEE Int. Conf. on Robotics and Automation (ICRA), Kobe, Japan, May 2009.

57. Flavio Lerda, James Kapinski, Hitashyam Maka, Edmund M. Clarke, and Bruce H. Krogh, Model checking in-the-loop, 2008 American Control Conference, Seattle, June 2008.

58. Ajinkya Y. Bhave and Bruce H. Krogh, Performance Bounds on State-Feedback Controllers with Network Delay, IEEE Conference on Decision and Control, Dec. 2008

59. James Kapinski,, Alexandre Donze, Flavio Lerda, Hitashyam Maka, Silke Wagner, and Bruce H. Krogh, Control Software Model Checking Using Bisimulation Functions for Nonlinear Systems, IEEE Conference on Decision and Control, Dec. 2008

60. Alexandre Donzé, Bruce Krogh, Akshay Rajhans, Parameter Synthesis for Hybrid Systems with an Application to Simulink Models, Hybrid Systems: Computation and Control, San Francisco, April 2009.

61. Hitashyam Maka, Goran Frehse, Bruce H. Krogh, Polyhedral Domains and Widening for Verification of Numerical Programs, Workshop on Verification of Numerical Software, San Francisco, April 2009.

62. André Platzer, Edmund M. Clarke: Computing Differential Invariants of Hybrid Systems as Fixedpoints. CAV 2008: 176-189.

63. Edmund M. Clarke, Alexandre Donzé, Axel Legay: Statistical Model Checking of Mixed-Analog Circuits with an Application to a Third Order Delta-Sigma Modulator. Formal Methods in System Design, *to appear*

64. Yu-Fang Chen, Azadeh Farzan, Edmund M. Clarke, Yih-Kuen Tsay, Bow-Yaw Wang: Learning Minimal Separating DFA's for Compositional Verification. TACAS 2009: 31-45

65. André Platzer, Edmund M. Clarke: Computing Differential Invariants of Hybrid Systems as Fixedpoints. Formal Methods in System Design, 35(1): 98-120 (2009).

66. Himanshu Jain, Daniel Kroening, Natasha Sharygina, Edmund M. Clarke: Word-Level Predicate-Abstraction and Refinement Techniques for Verifying RTL Verilog. IEEE Trans. on CAD of Integrated Circuits and Systems 27(2): 366-379 (2008)

67. Xenofon Koutsoukos, Nicholas Kottenstette, Joe Hall, Panos Antsaklis, Janos Sztipanovits , Passivity-Based Control Design of Cyber-Physical Systems", *Proceedings of the Workshop on Cyber-Physical Systems - Challenges and Applications (CPS-CA'08)* held in conjunction with In conjunction with the 4th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS'08)

68. Kottenstette, N., X. Koutsoukos, J. Hall, P. J. Antsaklis, and J. Sztipanovits, "Passivity-Based Design of Wireless Networked Control Systems for Robustness To Time-Varying Delays", 29th IEEE Real-Time Systems Symposium (RTSS 2008), Barcelona, Spain, IEEE, pp. 15-24, 12/2008.

69. Kottenstette, N., and J. Porter, "Digital Passive Attitude and Altitude Control Schemes for Quadrotor Aircraft", Technical Report, Nashville, TN, Institute for Software Integrated Systems, Vanderbilt University, pp. 1-12, 11/2008.

70. Kottenstette, N., X. Koutsoukos, J. Hall, J. Sztipanovits, and P. J. Antsaklis, "Passivity-Based Design of Wireless Networked Control Systems Subject To Time-Varying Delays", Technical Report, Nashville, TN, Institute for Software Integrated Systems, Vanderbilt University, pp. 1-17, 08/2008.

71. N. Kottenstette and P. J. Antsaklis, "Wireless control of passive systems subject to actuator constraints", 47th IEEE Conference on Decision and Control (CDC 2008), Cancun, Mexico, IEEE, pp. 2979-2984, 12/2008.

72. N. Kottenstette and P. J. Antsaklis, "Wireless Digital Control of Continuous Passive Plants Over Token Ring Networks", International Journal of Robust and Nonlinear Control: Special Issue on Control with Limited Information, 11/2008.

73. J. Porter, Z. Lattmann, G. Hemingway, N. Mahadevan, S. Neema, H. Nine, N. Kottenstette, P. Volgyesi, G. Karsai, and J. Sztipanovits, "The ESMoL Modeling Language and Tools for Synthesizing and Simulating Real-Time Embedded Systems", 15th IEEE Real-Time and Embedded Technology and Applications Symposium, San Francisco, CA, 04/2009.

74. N. Kottenstette and N. Chopra, "Lm2-stable digital-control networks for multiple continuous passive plants", Technical Report, Nashville, TN, Institute for Software Integrated Systems, Vanderbilt University, pp. 1-14, 04/2009.

75. Gabor Karsai, Sandeep Neema, David Sharp, Model-driven architecture for embedded software: A synopsis and an example, Science of Computer Programming, Volume 73, Issue 1, 2008, Pages 26-38.

76. Anantha Narayanan, Gabor Karsai, Towards Verifying Model Transformations, Electronic Notes in Theoretical Computer Science, Volume 211, 2008, Pages 191-2008.

77. Narayanan A., Karsai G., "Verifying Model Transformations by Structural Correspondence", Electronic Communications of the EASST, vol. 10, 2008.

78. Karsai, G. and Narayanan, A. 2008. Towards Verification of Model Transformations Via Goal-Directed Certification. In Model-Driven Development of Reliable Automotive Services: Second Automotive Software Workshop, ASWSD 2006, San Diego, Ca, Usa, March 15-17, 2006, Revised Selected Papers, M. Broy, I. H. Krüger, and M. Meisinger, Eds. Lecture Notes In Computer Science, vol. 4922. Springer-Verlag, Berlin, Heidelberg, 67-83.

79. Karsai, G. and Sztipanovits, J. 2008. Model-Integrated Development of Cyber-Physical Systems. In Proceedings of the 6th IFIP WG 10.2 international Workshop on Software Technologies For Embedded and Ubiquitous Systems (Anacapri, Capri Island, Italy, October 01 - 03, 2008). U. Brinkschulte, T. Givargis, and S. Russo, Eds. Lecture Notes In Computer Science, vol. 5287. Springer-Verlag, Berlin, Heidelberg, 46-54.

80. Gray, J., Fisher, K., Consel, C., Karsai, G., Mernik, M., and Tolvanen, J. 2008. DSLs: the good, the bad, and the ugly. In Companion To the 23rd ACM SIGPLAN Conference on Object Oriented Programming Systems Languages and Applications (Nashville, TN, USA, October 19 - 23, 2008). OOPSLA Companion '08. ACM, New York, NY, 791-794.

81. G. Karsai and G. Taentzer. 2008. Third international workshop on graph and model transformations. In Companion of the 30th international Conference on Software Engineering (Leipzig, Germany, May 10 - 18, 2008). ICSE Companion '08. ACM, New York, NY, 1055-1056.

82. S. Joshi and S. Boyd: "Sensor selection via convex optimization," IEEE Transactions on Signal Processing, 57(2):451-462, February 2009

83. A. Magnani and S. Boyd: "Convex piecewise-linear fitting," Optimization and Engineering, 10(1):1-17, March 2009

84. Y. Wang and S. Boyd: "Performance bounds for linear stochastic control," Systems and Control Letters, 58(3):178-182, March 2009

85. J. Mattingley and S. Boyd : "Automatic code generation for real-time convex optimization," To appear as chapter in Convex Optimization in Signal Processing and Communications, Y. Eldar and D. Palomar, Eds., Cambridge University Press, 2009

86. D. Gorinevsky, S.-J. Kim, S. Beard, S. Boyd, and G. Gordon: "Optimal estimation of deterioration from diagnostic image sequence," IEEE Transactions on Signal Processing, 57(3):1030-1043, March 2009

87. S. Joshi and S. Boyd: "An Efficient Method for Large-Scale Gate Sizing'" IEEE Transactions on Circuits and Systems I, 55(9):2760-2773, November 2008

88. R. Panicker, J. Kahn, and S. Boyd: Compensation of multimode fiber dispersion using adaptive optics via convex optimization," IEEE Journal of Lightwave Technology, May 2008

89. Z. Wang, S. Zheng, Y. Ye and S. Boyd: "Further relaxations of the semidefinite programming approach to sensor network localization," Siam Journal on Optimization, July 2008

90. D. O'Neill, A. Goldsmith, and S. Boyd: "Optimizing adaptive modulation in wireless networks via utility maximization'" Proc. IEEE International Conf. on Comm., pages 3372-3377, May 2008

91. S.-J. Kim, A. Zymnis, A. Magnani: "Learning the kernel via convex optimization," Proc. IEEE Internaltional Conf. on Acoustics, Speech, and Signal Processing, pages 1997-2000, April 2008

92. J. Skaf and S. Boyd: "Design of affine controllers via convex optimization," Submitted to IEEE Transactions on Automatic Control, April 2008

93. K.-L. Hsiung, S.-J. Kim, and S. Boyd: "Tractable approximate robust geometric programming," Optimization and Engineering, June 2008

94. Y. Wang and S. Boyd: "Fast model predictive control using online optimization," To appear IEEE Transactions on Control Systems Technology

95. A. Mutapcic, S. Boyd, A. Farjadpour, S. Johnson, and Y. Avniel: "Robust design of slow-light tapers in periodic waveguides," Engineering Optimization, April 2009

96. J. Ding, J. Sprinkle, S. S. Sastry and C. J. Tomlin: "Reachability analysis for an Automatic Refueling Protocol," IEEE Conference on Decision and Control, December 2008.

97. S. Forbes. Real-time C Code Generation in Ptolemy II for the Giotto Model of Computation, M.Sc. thesis, EECS Department, University of California, Berkeley, 2009.

98. Ben Lickly, Isaac Liu, Sungjun Kim, Hiren D. Patel, Stephen A. Edwards and Edward A. Lee, "Predictable Programming on a Precision Timed Architecture," in Proceedings of International Conference on Compilers, Architecture, and Synthesis for Embedded Systems (CASES), October, 2008.

99. Shanna-Shaye Forbes, Hugo A. Andrade, Hiren Patel, Edward A. Lee, "An Automated Mapping of Timed Functional Specification to A Precision Timed Architecture", in Proceedings of the 12th IEEE International Symposium on Distributed Simulation and Real Time Applications, October, 2008

100. Hiren D. Patel, Ben Lickly, Bas Burgers and Edward A. Lee, "A Timing Requirements-Aware Scratchpad Memory Allocation Scheme for a Precision Timed Architecture," EECS Department, University of California, Berkeley, Technical Report No. UCB/EECS-2008-115, September 12, 2008.

101. Gang Zhou, "Partial Evaluation for Optimized Compilation of Actor-Oriented Models," Ph.D. Dissertation, EECS Department, University of California, Berkeley, Technical Report No. UCB/EECS-2008-53, May 16, 2008.

102. J. Sprinkle, J. M. Eklund, H. Gonzalez, E. I. Grøtli, B. Upcroft, A. Makarenko, W. Uther, M. Moser, R. Fitch, H. Durrant-Whyte and S. S. Sastry. *Model-based design: a report from the trenches of the DARPA Urban Challenge.* Software and Systems Modeling, 2009.

103. H. Gonzalez, E. I. Grøtli, T. R. Templeton, J. O. Biermeyer, J. Sprinkle, and S. Shankar Sastry. *Transitioning Control and Sensing Technologies from Fully-autonomous Driving to Driver Assistance Systems.* Presented at AAET'08.

104. G. M. Hoffmann and C. J. Tomlin, Mobile Sensor Network Control using Mutual Information Methods and Particle Filters, Accepted to appear in the IEEE Transactions on Automatic Control, 2009.

105. G. M. Hoffmann and C. J. Tomlin, Decentralized Cooperative Collision Avoidance for Acceleration Constrained Vehicles, In the Proceedings of the 47th IEEE Conference on Decision and Control, Cancun, Mexico, December 2008.

106. M. P. Vitus, S. L. Waslander, and C. J. Tomlin, Locally optimal decomposition for autonomous obstacle avoidance with the Tunnel-MILP algorithm, In the Proceedings of the 47th IEEE Conference on Decision and Control, Cancun, Mexico, December 2008.

107. G. M. Hoffmann, S. L. Waslander, and C. J. Tomlin, Quadrotor Helicopter Trajectory Tracking Control, Proceedings of the AIAA Guidance, Navigation, and Control Conference, August 2008.

108. M. P. Vitus, V. Pradeep, G. M. Hoffmann, S. L. Waslander and C. J. Tomlin, Tunnel-MILP: Path Planning with Sequential Convex Polytopes, Proceedings of the AIAA Guidance, Navigation, and Control Conference, August 2008.

109. M. P. Vitus and C. J. Tomlin, Hierarchical, Hybrid Framework for Collision Avoidance Algorithms in the National Airspace, Proceedings of the AIAA Guidance, Navigation, and Control Conference, August 2008.

6. Interactions/Transitions

6.1 Participation/presentations at meetings, conferences, seminars

1. MURI team attended the bi-weekly MURI telecons.
2. HCDDES Review Meeting, December 2009, Berkeley.
   Edward Lee presented "Principled Design of Embedded Software"

Claire Tomlin and Shanka Sastry presented " Demonstration of the Starmac Experimental Platform and Overview of Hybrid Control Design Challenges"

Gabor Karsai presented "Model-Based Tool Chain for High Confidence Design"

Janos Sztipanovits presented "Project Overview"

Stephen Boyd presented "Robust Control Design"

Bruce Krogh presented "Model-based Testing and Verification of Embedded System Implementations"

Nicholas Kottenstette presented "Constructive Non-linear Control Design with Applications to Quad-Rotor and Fixed-Wing Aircraft".

Andre Platzer and Edmund Clarke presented: "Saturation-based Scaling Techniques for Symbolic Verification of Hybrid Systems"

3. Ben Lickly presented "Scalable Semantic Annotation using Lattice-based Ontologies" at the 12th International Conference on Model Driven Engineering Languages and Systems (MoDELS) in Denver, Colorado, October 2009

4. Dai Bui presented a poster about "Compositionality in synchronous data flow: Modular code generation from hierarchical SDF graphs" at the International Conference on Cyber-Physical Systems (ICCPS) in Stockholm, Sweden, April 2010

5. Jacob Mattingley: Talk on "Embedded Convex Optimization" at UC Berkeley, March 2, 2010.

6. Stephen Boyd: Many talks, including Plenary on "Real-Time Embedded Convex Optimization" at the International Symposium on Mathematical Programming, Chicago, August 23-28, 2009. More than 1000 people present.

7. 7th IEEE International Conference on Control and Automation, December, 2009, Christchurch, New Zealand. Nicholas Kottenstette presented "Digital Passive Attitude and Altitude Control Schemes for Quad-rotor Aircraft" while chairing the session on Aircraft Control and Aerodynamical Systems.

8. 1st IFAC Workshop on Estimation and Control of Networked Systems (NecSys 2009), Venice, Italy. Nicholas Kottenstette presented "Lm2-Stable Digital-Control Networks for Multiple Continuous Passive Plants".

9. J. Porter (ISIS). ARTIST Design Summer School in Europe 2009. Grenoble, France. Sep. 2009.

10. S. Neema (ISIS). Demonstration of Hardware-in-the-loop flight control test architecture at Formal Methods 2009 Tool Exhibition. Eindhoven, Netherlands. Nov. 2009.

11. J. Reineke (UCB), "Caches in WCET Analysis". January 26, 2010. MURI Webex.

12. P. Zuliani (CMU), "Bayesian Statistical Model Checking". March 11, 2010. MURI Webex.

13. IEEE International Symposium on Rapid System Prototyping in Fairfax, VA, June 2010. G. Hemingway will present "Automated Synthesis of Time-Triggered Architecture-based TrueTime Models for Platform Effects Simulation and Analysis".

14. Collaboration meeting at ISIS with Paolo Zuliani (CMU). May 17-19, 2010.

15. 2nd International Symposium on Resilient Control Systems (ISRCS 2009), Idaho Falls, ID. Nicholas Kottenstette presented "A Passivity-Based Framework for Resilient Cyber Physical Systems".

16. SIAM Conference on Control and its Applications (CT09), Denver, CO. Nicholas Kottenstette Chaired the Session on Constructive Methods for High Confidence Networked Control Systems.

17. Dynamics & Control Program Review (July 2009) Washington, D.C. Nicholas Kottenstette presented on "Frameworks and Tools for High-Confidence Design of Adaptive, Distributed Embedded Control Systems" with contributions from Bruce Krogh & Gabor Karsai.
18. AFOSR Dynamics and Control Program Review, Arlington, VA, August 6, 2009. Janos Sztipanovits: Frameworks and Tools for High-Confidence Design of Adaptive, Distributed Embedded Control Systems: Project Overview
19. International Conference on Hybrid Systems Computation and Control 2009, April 14-16, 2009, San Francisco. Alexandre Donze, Bruce H. Krogh:.Parameter Synthesis for Hybrid Systems with an Application to Simulink Models
20. 2008 American Control Conference, Seattle, June 2008. James Kapinski, Bruce H. Krogh, Model checking in-the-loop
21. Workshop on Verification of Numerical Software, San Francisco, April 2009. Bruce H. Krogh: Polyhedral Domains and Widening for Verification of Numerical Programs.
22. 47th IEEE Conference on Decision and Control, December 9-11, Cancun Mexico. Nicholas Kottenstette presented "Wireless control of passive systems subject to actuator constraints"
23. 29th IEEE Real-Time Systems Symposium (RTSS 2008), Barcelona, Spain. Nicholas Kottenstette presented "Passivity-Based Design of Wireless Networked Control Systems for Robustness To Time-Varying Delays
12. Graham Hemingway, Nicholas Kottenstette, Sandeep Neema, Harmon Nine, Joe Porter, Janos Sztipanovits, and Gabor Karsai: Model-Integrated Toolchain for High Confidence Design, talk given by G. Karsai and demonstration given by J. Porter at the Safe & Secure Systems & Software Symposium, Dayton, OH, June 2009.

In addition to the meetings above, we have presented our research results at the following conferences: AIAA GNC 2009, IEEE CDC 2009, ISRR 2009, ICRA 2010, HSCC 2010.
We have also presented our results to Boeing, Lockheed Martin, and Renault.

6.2 Consultative and advisory functions to other laboratories and agencies, especially Air Force and other DoD laboratories. Provide factual information about the subject matter, institutions, locations, dates, and names(s) of principal individuals involved

1. Janos Sztipanovits:
   a. Study member of the AF SAB FY10 Study on Operating the Next-Generation Unmanned
      Aerial Systems for Irregular Warfare
   b. Member of the NASA Advisory Council - Exploration Subcomittee on Avionics, SW and Cybersecurity. 2009-2012

2. Edward A. Lee:
   a. Air Force Research Laboratory, AFRL/RIEA, Rome, NY
      Brian Romano USAF AFMC /AFRL/RIEF
      Brian.Romano@rl.af.mil 315-330-4218

The objective of the Extensible Modeling and Analysis Framework (EMAF) effort is to build on top of Ptolemy II and adapt Ptolemy II for the rapid construction and configuration of modeling and analysis systems that incorporate disparate technologies. The purpose of this gap-filling project is to develop technologies for future incorporation into large-scale modeling and analysis systems, with specific focuses on scalable algorithm description, composition of heterogeneous components, and synthesis of efficient deployable decision-support systems that exploit multicore and distributed computing platforms. In particular, we have applied the code generation infrastructure developed under this MURI to a very large problem consisting of roughly 13000 actors. We were able to reduce the run time from roughly 10 minutes to 3 seconds.

b. Lockheed Martin Advanced Technology Laboratory Trip Denton ldenton@atl.lmco.com 3 Executive Campus, 6th Floor; Cherry Hill, NJ, 08002, USA Work: 856 792-9071 fax:856 792-9925

NAOMI Project (http://chess.eecs.berkeley.edu/naomi) (Also participating are Vanderbilt and UIUC) The purpose of the NAOMI project is to allow disparate modeling tools to be used to ether by tracking model changes within each system where a particular tool owns attributes of the overall design and provides attribute changes to other tools. The NAOMI project may result in useful technology that will allow easier collaboration on this MURI project. This project is using pedestrian/automobile traffic lights as a design driver. We have integrated Ptolemy II to the Naomi frame-work, which allows different tools to own attributes and update other tools when changes occur to those attributes. We have transferred models that use graph transformation and event relationship graphs.

c. The US Army Research Laboratory Jeff DeHart, jdehart@arl.army.mil Scalable Composition of Systems (SCOS) http://chess.eecs.berkeley.edu/scos

The objective of the SCOS research project is to provide scalable techniques for the composition of subsystems in a system-of-systems (SoS) framework for large, complex applications such as FCS. SCOS has synergy with this MURI project in that it deals with large systems. In particular:

- we are using the EmbeddedCActor to wrap legacy C code
- we are collaborating on work on the Kepler Project
- we are using Graph Transformations on models

3. Bruce Krogh
   a. National Science Foundation.
      Helen Gill hgill@nsf.gov
      Contributed to the development of the NSF Soliciation for Cyber-Physical Systems.

b. Lockheed Martin Advance Development Projects (ADP)
   Peter Stanfill peter.o.stanfill@lmco.com
   Consultant to the LM team in the AFRL MCAR program.

6.3 Technology Assists, Transitions, and Transfers.

1. Ptolemy II 8.0.beta was released on February 26, 2010 including

   - Model Transformation -a framework for the analysis and transformation of actor models using model transformation techniques
   - Ptera (Ptolemy Event Relationship Actor) Domain
   - Causality Analysis: Updates to our non-conservative causality analysis for modal models within discrete-event (DE) systems
   - Continuous and Modal Domains: a substantial rework of modal models and the underlying finite state machine infrastructure to make them work predictably and consistently across domains.

2. Key components of Vanderbilt's MIC tool suite (GME, GReAT, UDM) had one major release in 2010. The released tools are available through the ESCHER and ISIS download sites
3. Vanderbilt continued working with GM, Raytheon, Lockheed Martin, Boeing and BAE Systems research groups on transitioning model-based design technologies into programs.
4. Vanderbilt continued working with Boeing's FCS program on applying the MIC tools for precise architecture modeling and systems integration

6.4 New discoveries, inventions, or patent disclosures.

None.

6.5 Honors and Awards

1. Edmund M. Clarke
   a. 2010 LICS Test-of-time Award - Edmund M. Clarke. July 2010, Edinburgh, UK.
   b. Best Paper Award - André Platzer and Edmund M. Clarke: Formal Verification of Curved Flight Collision Avoidance Maneuvers: A Case Study. FM 2009, 547-562.
   c. Strachey Lecture – Edmund M. Clarke. My 27-year Quest to Overcome the State Explosion Problem. Oxford University Computing Laboratory, May 12, 2009, Oxford, UK
   d. Technion CS Distinguished Lectures – Edmund M. Clarke. Technion - Israel Institute of Technology, May 17-26, 2009, Haifa, Israel.
   e. Keynote Speaker – Edmund M. Clarke\

  i. U.S. Department of Defense Workshop on Satisfiability, March 3-5, 2009, Baltimore, MD

2. Claire Tomlin:
 a. Chancellor's Professorship of EECS, UC Berkeley (2007-2010)
 b. Tage Erlander Guest Professorship, Swedish Research Council, 2009.

3. Shankar Sastry:
 a. Appointed Dean of Engineering, UC Berkeley, July 2007 -
4. Janos Sztipanovits:
 a. Elected as foreign member of the Hungarian Academy of Sciences, 2010
 b. Sztipanovits, J.: "Convergence: Model-based Software, Systems and Control Engineering," Harry T. Nquist Distinguished Lecture, Yale University, October 22, 2009
 c. Keynotes:
  i. Sztipanovits, J.: "Compositionality and High-Confidence Design," MPSOC, Savannah, GA, August 7, 2009
  ii. Sztipanovits, J.: The System Integration Challenge: Is Rapid System Prototyping Relevant to the Solution? IEEE International Symposium on Rapid System Prototyping, June 10, 2010
 d. Georgia Tech ECE Distinguished Lectures: "Three Problems of Model-based Design," Atlanta, GA, November, 2008
 e. Appointment: NASA Advisory Council - Exploration Subcomitee on Avionics, SW and Cybersecurity. 2009-2012
5. Edward Lee
 a. MODELS Distinguished Paper Award for "Scalable Semantic Annotation using Lattice-based Ontologies" [2]
  i. Keynotes:
   1. "Model-Based Design for Signal Processing Systems", IEEE Workshop on Signal Processing Systems (SiPS), October 7-9, 2009, Tampere, Finland.
   2. "Beyond Embedded Systems: Integrating Computation, Networking, and Physical Dynamics", ACM SIGPLAN/SIGBED 2009 Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES), June 19-20, 2009, Dublin, Ireland.