ANNUAL REPORT

FOUNDATIONS OF HYBRID AND EMBEDDED SYSTEMS AND SOFTWARE

NSF/ITR PROJECT – AWARD NUMBER: CCR-0225610

UNIVERSITY OF CALIFORNIA, BERKELEY

June 16, 2009

PERIOD OF PERFORMANCE COVERED: JUNE 1, 2008 – May 31, 2009

Contents

1 Participants

1.1 People

PRINCIPAL INVESTIGATORS:

THOMAS HENZINGER (UC BERKELEY, EECS)
EDWARD A. LEE (UC BERKELEY, EECS)
ALBERTO SANGIOVANNI-VINCENTELLI (UC BERKELEY, EECS)
SHANKAR SASTRY (UC BERKELEY, EECS)
CLAIRE TOMLIN (UC BERKELEY, EECS)

POST DOCTORAL RESEARCHER:

ALVARO C ÁRDENAS (UC BERKELEY)

GRADUATE STUDENTS:

ANIL ASWANI (UC BERKELEY, PROF. TOMLIN)
JAN BIERMEYER (UC BERKELEY, PROF. SASTRY)
YOUNG-HWAN CHANG (SUMMER) (UC BERKELEY, PROF. TOMLIN)
MILOS DREZGIC (UC BERKELEY, PROF. SASTRY)
TODD TEMPLETON (UC BERKELEY, PROF. SASTRY)

STAFF:

NICK BOYD (UC BERKELEY)
JESSICA GAMBLE (UC BERKELEY)
NEAL MASTER (UC BERKELEY)
MARY P STEWART (UC BERKELEY)

BUSINESS ADMINISTRATOR:

TRACEY RICHARDS (UC BERKELEY)

EXECUTIVE DIRECTOR:

CHRISTOPHER BROOKS (UC BERKELEY)

1.2 Partner Organizations:

UNIVERSITY OF CALIFORNIA, BERKELEY

1.3 Collaborators:

ALESSANDRO ABATE, (STANDFORD UNIVERSITY, DELFT UNIVERSITY)
PIETER ABBEEL (UNIVERSITY OF CALIFORNIA, BERKELEY)
SAURABH AMIN (UNIVERSITY OF CALIFORNIA, BERKELEY)
CHRISTIAN BERGER (RWTH AACHEN, GERMANY)
ANNARITA GIANI (UNIVERSITY OF CALIFORNIA, BERKELEY)
ANDREW HINES (UNIVERSITY OF BRITISH COLUMBIA)
CHI-YEN HUANG (NATIONAL CHIAO TUNG UNIVERSITY, TAIWAN)
YU-LUN HUANG (NATIONAL CHIAO TUNG UNIVERSITY, TAIWAN)
ZONG-SYUN LIN (NATIONAL CHIAO TUNG UNIVERSITY, TAIWAN)
CHRISTOS H. PAPADIMITRIOU (UNIVERSITY OF CALIFORNIA, BERKELEY)
ADRIAN PERRIG (CARNEGIE MELLON UNIVERSITY)
ANUPAM PRAKSH (UNIVERSITY OF CALIFORNIA, BERKELEY)
TANYA ROOSTA (UNIVERSITY OF CALIFORNIA, BERKELEY)
MOHAN SAROVAR (UNIVERSITY OF CALIFORNIA, BERKELEY)
BRUNO SINOPOLI (CARNEGIE MELLON UNIVERSITY)
JONATHAN SPRINKLE (UNIVERSITY OF ARIZONA)
HSINYI TSAI (NATIONAL CHIAO TUNG UNIVERSITY)

2 Activities and Findings

2.1 Project Activities

This is the seventh Annual Report for the NSF Large ITR on "Foundations of Hybrid and Embedded Systems and Software." This year was a no-cost extension for certain researchers at the University of California, Berkeley (Center for Hybrid and Embedded Systems and Software (CHESS), http://chess.eecs.berkeley.edu. Research at the other CHESS partners: ISIS at Vanderbilt University (Institute for Software Integrated Systems, http://www.isis.vanderbilt.edu), and the Department of Mathematical Sciences, (http://msci.memphis.edu) at the University of Memphis ended before the period covered by this report.
The web address for the overall ITR project is:
http://chess.eecs.berkeley.edu/projects/ITR/main.htm
This web site has links to the proposal and statement of work for the project.
The CHESS ITR grant has been instrumental in supporting the launch of Tomlin's new Hybrid Systems Laboratory in Cory Hall. Specifically, the grant continues to support several new directions in systems biology, centered on the development of hybrid systems models and analysis tools for the analysis and deeper understanding of several protein regulatory networks. The grant has supported Tomlin, her PhD student Anil Aswani, and a Berkeley undergraduate, Nicholas Boyd. Two additional Berkeley undergraduates, Harendra Guturu and Eugene Li, have worked on the project though have been supported by external fellowships. The research experience obtained by these undergraduates has been instrumental in helping them decide their next steps: Guturu was accepted and is currently starting the PhD program in Electrical Engineering at Stanford, and Li has been accepted into the 5th year Masters program at Berkeley and will continue working on the project this year and next. Boyd will continue working on the project as an undergraduate this year.

2.1.1 ITR Events

Main events for the ITR project in its seventh year were:

- A weekly Chess seminar was held at Berkeley. The speakers and topics are listed in Section 4.4.1, presentations for the seminar are available at http://chess.eecs.berkeley.edu/seminar.htm

We organize this section by thrust areas that we established in the statement of work. As year seven was a no-cost extension, we include only thrust areas funded by the no-cost extension.

2.1.2 Hybrid Systems Theory

2.1.3 Deep Compositionality

2.1.4 Robust Hybrid Systems

2.1.5 Hybrid Systems and Systems Biology

The CHESS ITR has enabled a new collaboration, between Tomlin's group and a group of developmental biologists at Lawrence Berkeley Labs and the Department of Molecular and Cell Biology at Berkeley. This group, led by Dr. Mark Biggin and Professor Mike Eisen, are

studying the early Drosophila development. They have developed state of the art tools for RNA and protein data collection, and have collaborated with computer vision researchers to develop a "virtual embryo", visualizing all data at once on a 3D representation of the Drosophila embryo. We have begun a collaboration with their group to design dynamic models of this system: modeling RNA and protein concentrations to try to uncover the detailed interactions between these gene products that are key in fly development. We are developing continuous and hybrid models to represent the dynamics of this system.

Early patterning in the Drosophila melanogaster embryo occurs through a complicated network of interactions involving proteins and mRNA. One such system is the pattern of hunchback mRNA in the presence of Bicoid and Kruppel protein. This system is well-studied, but there is disagreement amongst biologists between two general models. Our aim is to provide evidence to support one of the two models in contention, and we do this through system identification methods. Our general approach is to do nonlinear regression on a parametric, nonlinear partial differential equation model which incorporates transcription, diffusion, and degradation. We perform the nonlinear regression and analyze the results of the nonlinear regression. We interpret the results in the biological context, and we also compare our results to previous work on this system.

In terms of hybrid model development, we have focused in particular on the relationship between a particular class of hybrid systems, known as piecewise affine (PWA) systems, and monotone systems (which have certain properties making them amenable to stability analysis). Monotone systems are order-preserving systems: given a partial order on any two initial conditions, the trajectories of the monotone system preserve this partial order through time. There is a rich theory of strong results about the dynamics and stability of monotone systems with continuous vector fields. These existing results do not apply to piecewise affine (PWA) systems, which have discontinuous vector fields. Though the previous work on monotone systems has largely been theoretical, there is growing interest in monotone systems due to the realization that many systems in biology are monotone. Our work considers the relationship between monotone and PWA systems, which have found applications in biology. Understanding which conditions are sufficient for a PWA system to be monotone is useful, both for understanding the dynamics as well as for designing controllers. In our work, we characterize monotonicity of PWA systems. Then, we prove analogs of the Kamke-Muller and related graph theoretical theorems, both of which provide sufficient conditions for a system with continuous vector field to be monotone. Our analogs give sufficient conditions for a PWA system to be a monotone system.

More generally, we have been studying the topology of graphs representing biological influence models, and investigating the development of a corresponding "control theory" for these graphs. The traditional control scheme has been to input a signal into a plant, where the signal is derived from either an open-loop or a closed-loop. This control strategy requires that the plant be able to accept inputs or can be modified to do so. However, this situation is not always true in biological genetic networks; in these systems, there is often no input or obvious modification to allow inputs. We believe that they require a new paradigm for control. Biotechnology techniques are such that it is easier to make topological changes to a genetic network than it is to either change the states of the pathway or add more elements to the pathway. Thus, for such genetic networks it is important to develop a theory of control based on making large scale changes (e.g. genetic mutations) to the topology of the network; we provide steps towards such a theory. We highlight some useful results from monotone and hybrid systems theory, and show how these results can be used for such a topological

control scheme. We consider the cancer-related p53 pathway as an example; we analyze this system using control theory and devise a controller.

Embedded Software for National and Homeland Security

Autonomous Ground Vehicles

Ground vehicle research, although more stable than airborne vehicles, presents the subtle problem of providing intelligent behavior which operates in real-time, executes safely, and yet provides a "smooth" reaction to stimuli—i.e., the software behavior is somewhat humanized. Our application is the DARPA Urban Challenge, and we are using the ground vehicle testbed to show the performance of various algorithms and advancements in theory of switched systems, model-predictive control, parameter identification, time-triggered distributed components, and computer vision, as well as how these components work in real-time with one another. Additional concerns which this project addresses are distributed software testing, component-based design, and vehicle/sensor health monitoring. We are proving many of the theories and algorithms which have been developed in the last four years of the ITR.

Real-time Computer Vision

The goal of this task is to detect moving objects using a stereo camera system mounted on a car. This information will be used to detect, and estimate the trajectories of (possibly) mobile obstacles such as other vehicles. Note that, in this scenario, we wish to detect both objects in close proximity to our vehicle (for example, the vehicle in front of us), and also objects that are farther away (for example, oncoming vehicles), so we cannot make assumptions about whether height errors at adjacent pixels appear to be close to planar. Our solution must also be able to run in real time. In this application, we are interested in determining 3D motion in the scene, rather than the more-studied case of 2D motion in the image. In particular, we want to find the motion of objects in the scene relative to each other; if we have vehicle state data available, or if we can assume that the majority of the scene is not moving, we can determine which motion-segmented region corresponds to the background and remove its perceived motion from the perceived motion of the other objects, obtaining the motion of the other objects in a global frame.

Todd Templeton's focus in the past year has primarily been hardware and software infrastructure for the autonomous / assisted-driving vehicle testbed. This effort has culminated in external time synchronization for all car sensors, which is essential for perception algorithms that utilize multiple sensors, as well as a reusable and extensible library of communication and sensing software components that can run on the variety of hardware platforms carried in the car. In addition to a complement of four half-2U mini-ITX Linux PCs, the car carries Coldfire-based NetBurner embedded processor boards for sensors that do not support external triggering and time-synchronization; the cameras are the only sensors on the car that natively support an external trigger. A hardware interrupt on each microprocessor board is wired to the same (square wave) trigger signal as the cameras, through a solid-state relay for voltage conversion. The master external trigger (generated by a network-controllable signal generator in the car) is enabled after all of the microprocessor boards are powered on, and after the camera driver has initialized the cameras. The first falling edge of the trigger signal causes the first frame to be captured by each camera, and also provides a time-zero reference to the microprocessor boards. Subsequent falling edges of the trigger signal cause subsequent frames to be captured by the cameras, and also provide a time reference from which the microprocessor boards calibrate their internal clocks. Once the master trigger is enabled and a microprocessor board has performed the initial calibration of its clock (after

receiving the second falling edge), it begins time-stamping data from the sensor (such as an INS or LADAR) to which it is attached and sending it over the car's Ethernet network using the Spread multicast messaging service. All perception algorithms, which run on the Linux PCs, use the time-stamp on each piece of sensor data, instead of the current system time, in their calculations.

The embedded Coldfire processors in the car present a challenge to software portability. To this end, Templeton has developed an architecture compatibility library that emulates the required subset of the POSIX C standard library on top of the embedded OS, embedded C library, and NetBurner system libraries. This compatibility library also provides standard I/O over a network socket, and functionality that runs before the program's main() to initialize the system clock against the external trigger.

The software collection for this platform, hopefully to be expanded to other robotic platforms within the group and open-sourced to the larger robotics community, is called the Intelligent Robotics Toolkit (IRT). It is primarily based on software used in a previous vision-based helicopter mapping and landing project, expanded to support distributed computing across a diverse hardware and software environment. We currently have a software engineering doctoral student from RWTH Aachen University in Germany helping us to strengthen the software engineering foundations of this toolkit, and to expand its simulation and visualization capabilities.

Recently, we have achieved time synchronization / triggering across all car sensors, and taken the car out on the roads near Richmond Field Station to capture sensor data from which to formulate and tune perception algorithms.

Templeton expects to graduate in December 2009: in his final contributions, he will focus on the problem of moving object segmentation while driving, using camera data collected from the above-mentioned data-gathering trip. Moving object detection and segmentation is important for both autonomous and assisted driving for two primary reasons: to estimate the trajectories and future positions of mobile obstacles, and to remove points on mobile obstacles from the map of the static portion of the scene (without which mobile obstacles become 3D walls as they move across the scene). Hence, the motion planning process becomes similar to that in a static environment (using the static scene map), with the addition of a list of mobile obstacles and their estimated trajectories and current positions.

The proposed motion segmentation algorithm is non-parametric in that it does not assume a particular shape or appearance of mobile obstacles, which allows it to detect moving obstacles such as bicyclists and pedestrians, and to not detect stationary objects that look like cars (such as parked cars)—these static objects will be handled like any other static part of the scene by the motion planner.

Verification of Driver Augmentation Systems

There has been an explosive growth in the use of embedded systems in cars. By some accounts, it is widely expected that by the end of the decade over 50% of the cost of a car will be vehicular electronics (or veitronics). Beyond the fundamental functionality of an automobile, such as driving, stopping, and turning, a modern car provides additional features for more passenger safety, better comfort, and lower environmental impact. Thus, the number of embedded processors used in a vehicle today is in the order of 80 for luxury cars, and is expected to grow further by some accounts. A contemporary car therefore is a networked embedded system, in which subsystems need to process data and communicate over special networks such as CAN, LIN or Flexray, often within hard real-time constraints. While there has been a great deal of attention paid to hybrid and electric cars and the veitronics for their drive trains, it is our contention that Advanced Driving Assistance Systems (denoted as ADAS) present a big opportunity to apply research that can potentially have a big impact on the whole automotive industry. A key issue with the introduction of these safety critical technologies is the need to have them be verified, validated and in

some cases certified. By verification, we mean formal results guaranteeing the performance (properties such as safety, liveness or non-blocking stability) of models of intelligent software systems embedded with the physical hardware on a car; and by validation we mean testing of the theoretical verified proofs of performance on hardware. Certification usually follows formal specifications laid down by regulatory/ insurance authorities and is accompanied by verification/ validation.

Automotive OEMs and tier 1 suppliers are currently suffering from the high cost of verification and validation of the kinds of features that are being demanded by customers. While the software itself to be used in automotive systems has to undergo rigorous processes for design, implementation, audit and test, using standards such as IEEE-610 or SEI CMMI, limited tools exist for verification of automotive ADAS. These systems provide an additional order of complexity, since they are not only semi-autonomous, but also interaction with a human operator for safety critical decisions is necessary.

The state-of-the art to the extend of our knowledge is a statistical approach: High-precision driving robots or automated mini-series cars such as the VW Golf GTi "53 plus 1" are used to rigorously repeat driving situations within sub-centimeter precision. If statistical measures such as MTTF or MTBF suggest safe operation, the system is deemed deployable in road traffic.

However, there are several problems with such an approach: Foremost, repeated execution with varying initialization parameters is only feasible for limited cases, such as a Parking Assistant. Further, the testing has to be rigorous and thus is costly in monetary terms and drastically increases time-to-market.

It is therefore our strong belief, that a formal verification method for ADAS is needed, to increase car functionality, safety and energy efficiency, as well as decrease development costs and time to market. We are thus developing a new theoretical framework and algorithms for the design of mathematically verified and validated cyber-human systems from beginning with ADAS as a specific case. We are exploring the next generation of cyber-human systems, which will employ much "better models of human cognition", and hence, better assist humans in autonomous or semi-autonomous ways. This research is enabled by recent major advances in the sub-areas of computing and communication, such as stochastic hybrid models, learning methods, signal-to-symbol transformation, distributed decision making and dynamic resource allocation in geographically distributed systems without communications infrastructure.

Over the last 40 years, the fields of knowledge representation, perception, robotics, control, and learning have evolved in their separate ways. The grand vision of cyber-human systems, in which these fields combine into complete agents, has all but disappeared. However, with new results and partial reunifications of these individual sub- disciplines, the time has come to propose a reconstruction of the science of cyber-human systems. The focus of the present research is developing integrated agent designs capable of performing simple tasks reliably in unstructured environments and generating purposive activity over an unbounded period. Such a goal requires dealing with perceptual input, noisy, and partially known dynamics, real-time requirements, and complex environments containing many objects and agents.

The goal is to demonstrate our work on two examples: Automatic Parking and Highway Cruise Control with linear and lateral track, as well as negative and positive acceleration, authority. We chose the parking example, since several luxury cars already deploy such systems, and our approach can readily be compared with existing solutions. The highway example, however, is on the road map of all major OEMs, yet we argue that existing verifi-

cation approaches will fail here. This is where our major contribution will be.
Automated Driver Automation Systems (ADAS) are required to perform safety-critical tasks with hard-real time guarantees. Simulation and validation based methods alone cannot guarantee that all specifications are met and that undesired behaviors are not executed. Formal methods offer a rigorous framework to prove that a mathematical abstraction of embedded software satisfies the required correctness properties. The mathematical abstraction of ADAS embedded software can be completely behavioral in that it closely describes all possible executions or it could be simply prescriptive in that it only specifies what the system should do. In both cases, the mathematical abstraction should specify evolution of the physical environment of the system such as the effect of forces, actions of the driver, presence of external entities like obstructions, other vehicles etc. In addition, the ADAS models should also include description of maneuvers such as cruise mode, lane changing, parking, and overtaking. The specification of required correctness properties can be generally translated into safety, i.e., the system never performs a bad execution; and liveness, i.e., the system eventually performs a good execution and does not deadlock.
The modeling of ADAS requires hierarchies of different models of computation, some discrete and others continuous. Such system models are referred to as hybrid system models. These models are especially suited to modeling compound behaviors arising from composition and interaction between heterogeneous sub-systems in automotive systems. A prototypical example is the hierarchical layering of finite state machines and nonlinear continuous time differential equations.
However, modeling uncertainty associated with human behavior in verification of ADAS raises new issues and challenges: First, the human-ADAS interface determines the mode and extent of information the user has about the behavior of the system. Secondly, the modes of interaction that are not proven to be correct can raise important safety issues of such systems. In particular, the human-machine interaction can lead to unpredictable behaviors if the assumption of human user does not match with the guarantee that the ADAS can provide. As an example, if the human user gives control of a safety- critical task to the ADAS but assumes a wrong model of the system's behavior, the ADAS may not be able to successfully execute the task. Lastly, such systems also raise an important modeling question: Can human cognitive limits be reasonably modeled and incorporated in ADAS verification framework? We plan to address these research challenges by formalizing probabilistic specifications of human-ADAS interaction. We are inspired by developments in modern cognitive science which holds the viewpoint that human mind is a computational system. Prior research has also demonstrated that significant headway can be made in understanding how a human's cognitive resources can be integrated most effectively into the problem when mental models of the human, and information about the human's cognitive limits, are incorporated into the design of the control architecture in the very early stages of design specification. We will build a framework in which successive refinements of models of human cognitive functions will be checked for correctness against formal models of ADAS. Our research will benefit from the efforts to model interaction between human operators and air- traffic management systems by accounting for the physical constraints that come from applications. Horvitz at Microsoft Research has pioneered the use of Bayesian networks in the design of models of human interaction with automation: NASA operators with varying levels of expertise, interacting with the fuel control systems on board the Space Shuttle. Using these models to indicate the context and timing of the information to display to the operator, the expected utility of the operator's decisions can be greatly enhanced.

In our approach to verification, we use a multi-world semantics hierarchical system. We break up the verification task into individual components, and verify each in its own, and its interface to neighboring components in the hierarchy. An expression at each level is interpreted at the same level. Therefore, checking the truth-claim at that level is performed in its own declarative world. Relating these disconnected worlds together is a nontrivial task; however, we are collaborating with Jonathan Sprinkle from University of Arizona on using metamodels for the interface design between components. This both enables better analyzability as well as potential for using components developed by different research groups. Instead of semantic flattening, where an expression has to be both syntactically translated and semantic interpreted, we are following human reasoning and cognition, and propose the use of high-level expressions, which will be compiled into idealized lower-level expressions and then interpreted. Invariants will be used to show that higher-level truth-claims now become conditional lower level truth- claims. In this setting, higher-level truth-claims become necessary conditions. This is contrary to one-world semantics, in which higher- level claims are sufficient conditions.

Suppose one-world interpretation leads to falsification of higher- level claims that are true in multi-world semantics. This can happen, when lower-level faults are not accounted for in higher-level descriptions. Then, multi-world semantics must be split into multiple- frameworks, each dealing with the identified faults.

Our proposed framework is kept general enough to apply to various systems. From the sensory point-of-view, these levels have increasingly coarse representations of the world as one moves toward higher levels, while from the actuation point-of-view, the tasks become more strategic, supervisory and planning-oriented at the higher levels starting from "reactive" ones at lower levels.

The highest level, the Mission Planner, is the human operator in the automotive context. The output of this level could be in the form of "go to San Francisco". The Route Planner then takes this input and transforms it into an actual plan, in our context it would be an A* implementation detailing which roads to take. Next, the Maneuver Control layer takes these roads and transforms them into driving decisions, considering current sensor readings. From there, the Low- level Control transforms these driving decisions into actual control input for the physical vehicle.

This model also has what we call in analogy to database design a "roll- back mechanism": If a component cannot perform a task given from a higher-level component, it has to communicate the reasons why it failed at execution. The higher level then has to roll-back: to revert to a more feasible strategy or pre-defined back-up plan.

There are several challenges associated with the verification of such hierarchical architecture. One has to establish such a hierarchy in a formal way with different models appropriate at the respective levels: define the semantics of interaction between different levels for operational and emergency goals, define assumptions about the model of interactions between the levels, the levels of service each level can provide, and define the set of services each level must accept in order to provide requisite services.

Within this hierarchy, we are also interested in knowing how uncertainty and fault propagates between different levels and their criticality to the goals.

Our mathematical framework for the hierarchy is currently under constant change. We defined a series of increasingly complex examples of (semi)-autonomous system that we try to capture in our framework, and apply our framework to these. If properties of the system cannot be described with the current definitions, these are altered or amended. Our examples

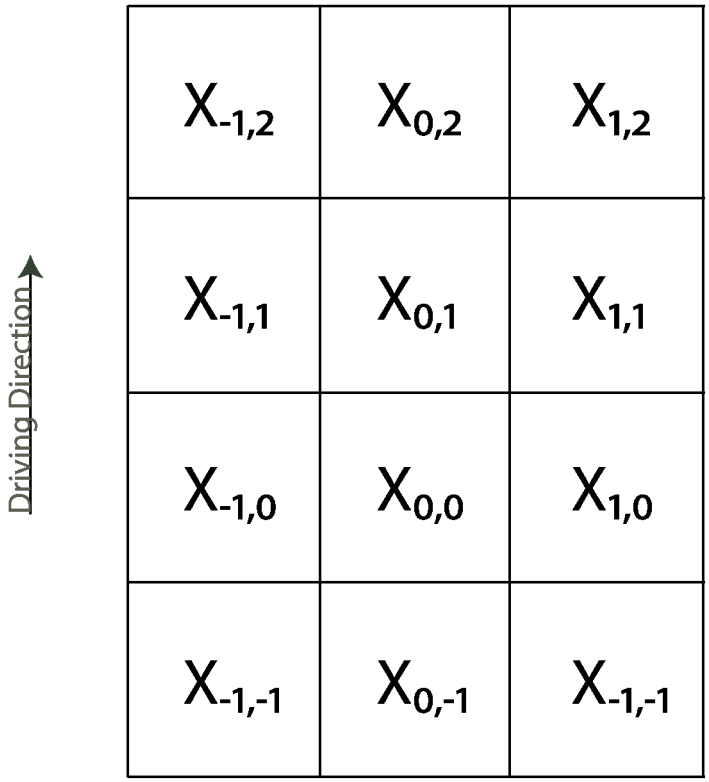

Figure 1: Matrix representation

range from the common water tank problem in hybrid systems theory via agents that have two simultaneous missions or objectives such as to traverse an area and to remain stealthy, to a collection of heterogeneous agents which each have unique sets of capabilities and have to work together towards a goal declared by the Mission Planner.
We are about to finalize this framework and intend to publish a detailed white paper in the upcoming Fall on our findings to invite feedback from the research community.
While the research effort described above is mainly aimed at verifying a (Semi-) autonomous system, an ADAS capable of making autonomous driving decisions also has to incorporate knowledge and assumptions about other traffic participants. We therefore propose the investigation into using an Algorithmic Game Theory (AGT) approach. While game theory itself is only descriptive, AGT however is prescriptive, and therefore could be used in this effort.
Clearly, interaction of cars (normally) cannot be described as an adversial game. However, it is also not really a collaborative effort, since one driver has no incentive to help another driver to achieve his goal. We are thus modeling traffic as an implicit collaboration:
Ideally, human drivers not only care for their own safety and goals, but also attempt to not inconvenience other traffic participants. Recent research conducted by our partners from the University of Aachen in co-operation with Volkswagen suggests that it suffices to use a 3x3 or 3x4 matrix to make informed LTT driving decisions. The car being the center in the matrix (X_{00} in Figure 1), its local neighborhood can be divided into segments to its sides, in front and behind, and on the diagonals. If there is any car detected in a segment, it's estimated speed is entered into the matrix. In the case of a sensor that can see further ahead than up to the next car (such as
Same advanced automotive radar), one column in driving direction extends the matrix. Each cell of the matrix contains the speed and the distance of a car, or Null if there is no car detected.
To model the interaction between cars, we are using coordination games (CG). Coordination

Figure 2: 2008 Ford Escape Hybrid ByWire XGV

games model situations in which all agents can realize mutual gains as long as they make mutually consistent decisions. For such games, there typically exist several pure strategy Nash Equilibria, so that the agents have to chose the same or corresponding strategies. However, often the coordination has to be done without any ability to communicate. Finally, some equilibria may give higher payoffs, be more fair, or, most important to the application at hand, may be safer, thus occasionally leading to interest conflicts.

We argue that this fits the interaction of cars on a highway well. We do not want to force cars to be able to communicate with each other, for two major reasons: security and deployment. Communication between cars would have to be done wirelessly, and thus provides an easy point of attack for malicious parties. Also, for such a system, all traffic participants would have to be equipped with such communication facilities, rendering it unusable for the next decade. Further, just for the interaction of two cars and one possible disturbance, we can foresee several equilibria, and cars should settle for a common equilibrium that maximizes overall welfare.

In parallel to our verification efforts, we also created the Berkeley DRIVR Lab, in close collaboration with CHESS, with the intend to showcase successfully verified algorithms. After participating in the DARPA Urban Challenge, we published a paper in AAET 2008, outlining our ideas on how to apply lessons learned from autonomous driving towards ADAS. Discussions about our paper with other researchers in the field and OEMs led to our insight on the necessity of formal ADAS verification techniques. However, other lessons learned were on the need for a robust and scalable hardware platform, as well as test bed, and a lightweight software toolkit.

We have outfitted a fully automated 2008 Ford Escape Hybrid ByWire XGV as testbed for (semi-) autonomous driving (Figure 2). Actuation is done transparently via a commercial toolkit (Torc Technologies) that directly communicates with the car's ECU. A cluster of customized quad- core mini-ITX computers is used to process data and make driving decisions, communicating among each other and with the car via Gigabit Ethernet. Various built-in screens and a KVM switch, as well as the possibility to connect notebook computers enables in-car debugging, while wireless network access enabled remote debugging, data streaming and offline analysis. All sensors, such as visual light cameras, thermal infrared cameras, laser scanners, radar, inertial measurement units and GPS are connected to time-synchronized embedded processors which trigger synchronized data-acquisition and timestamp data before relaying it to the computation cluster via Gigabit Ethernet for pre-processing, fusion and influencing driving decision making.

Since there is no robotics software framework available that satisfies all our demands for robustness, ease of use, reliability, platform independence, lightweight communication and interfaces to existing standards such as JAUS among others, we opted for implementation of our own.
Our software and computational approach is based on the following principles:

- Sensor drivers and communication methods must be abstracted as much as possible, to enable maximum flexibility in choosing different sensors and communication methods in the future.

- Transparent timestamping and synchronization facilities must be available at the sensor input level. To enable this, sensor drivers must be lightweight enough to run on an embedded processor; in particular, this means minimal or no threading.

- Transparent multicast, logging, and replaying facilities must be available at all levels (including the sensor-input level), in order to encourage the modularization of software, and to enable the independent development and verification of individual modules.

- Software modules must be able to be written in a variety of languages and run on a variety of platforms, with minimal invasiveness on the part of the infrastructure.

- Software modules should make optimal use of the computing hardware, from embedded processors via multi-core CPUs to manycore GPUS by utilizing frameworks such as Intel Thread Building Blocks, OpenMP and OpenCL or CUDA.

- Although the infrastructure is written in C/C++ due to its efficiency and ease of use, it is written with multi-platform compatibility in mind, and its interface is simple and can be easily wrapped for other programming languages, such as MATLAB.

- Where available, existing software components will be used, such as scientific and numerical libraries (BLAS, LAPACK), or vision libraries such OpenCV or the NASA Vision Workbench.

The software toolkit is currently undergoing final evaluation and testing, both internally as well as in collaboration with other research groups. We intend to release it with a free BSD license in Fall 2009. Given its ease of use, portability and free license, we are content for a broad acceptance among both academic research groups as well as commercial R&D facilities.

Control of Communication Networks

In a series of papers Abate and co-authors have continued to explore using stochastic hybrid systems congestion control schemes for both wired and wireless networks. These methods have tremendous applicability to other classes of network embedded systems as well (see).

Cybersecurity of Embedded Systems

2.2 ProjectFindings

Abstracts for key publications representing project findings during this reporting period, are provided here. A complete list of publications that appeared in print during this reporting period is given in Section 4 below, including publications representing findings that were reported in the previous annual report.

- [1]Anil Aswani, Peter Bickel, Claire Tomlin. "Statistics for Sparse, High-Dimensional, and Nonparametric System Identification," IEEE ICRA 2009, 2133-2138, 15, May, 2009.

  Local linearization techniques are an important class of nonparametric system identification. Identifying local linearizations in practice involves solving a linear regression problem that is ill-posed. The problem can be ill-posed either if the dynamics of the system lie on a manifold of lower dimension than the ambient space or if there are not enough measurements of all the modes of the dynamics of the system. We describe a set of linear regression estimators that can handle data lying on a lower-dimension manifold. These estimators differ from previous estimators, because these estimators are able to improve estimator performance by exploiting the sparsity of the system - the existence of direct interconnections between only some of the states - and can work in the "large p, small n"' setting in which the number of states is comparable to the number of data points. We describe our system identification procedure, which consists of a presmoothing step and a regression step, and then we apply this procedure to data taken from a quadrotor helicopter. We use this data set to compare our procedure with existing procedures.

- [2]Alvaro Cárdenas, Tanya Roosta, S. Shankar Sastry. Ad Hoc Networks, "Rethinking Security Properties, Threat Models and the Design Space in Sensor Networks : A case study in SCADA systems," pp. in publication, May 2009.

  In recent years we have witnessed the emergence and establishment of research in sensor network security. The majority of the literature has focused on discovering numerous vulnerabilities and attacks against sensor networks, along with suggestions for corresponding countermeasures. However, there has been little guidance for understanding the holistic nature of sensor network security for practical deployments. In this paper, we discuss these concerns and propose a taxonomy composed of the security properties of the sensor network, the threat model, and the security design space. In particular, we try to understand the application-layer goals of a sensor network, and provide a guide to research challenges that need to be addressed in order to prioritize our defenses against threats to application-layer goals.

- [3]Saurabh Amin, Alvaro Cárdenas, S. Shankar Sastry. "Safe and Secure Networked Control Systems Under Denial-of-Service Attacks.," Hybrid Systems: Computation and Control, Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 31-45, 30, April, 2009.

  We consider the problem of security constrained optimal control for discrete-time, linear dynamical systems in which control and measurement packets are transmitted over a communication network. The packets may be jammed or compromised by a malicious adversary. For a class of denial-of-service (DoS) attack models, the goal is to find an (optimal) causal feedback controller that minimizes a given objective function

subject to safety and power constraints. We present a semi-definite programming based solution for solving this problem. Our analysis also presents insights on the effect of attack models on solution of the optimal control problem.

- [4]Alvaro Cárdenas, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, S. Shankar Sastry. "Challenges for Securing Cyber Physical Systems," First Workshop on Cyber-physical Systems Security, DHS, submitted, 2009.

  We discuss three key challenges for securing cyberphysical systems: (1) understanding the threats, and possible consequences of attacks, (2) identifying the unique properties of cyber-physical systems and their differences from traditional IT security, and (3) discussing security mechanisms applicable to cyber-physical systems. In particular, we analyze security mechanisms for: prevention, detection and recovery, resilience and deterrence of attacks.

- [5]Zong-Syun Lin, Alvaro Cárdenas, Saurabh Amin, Yu-Lun Huang, Chi-Yen Huang, S. Shankar Sastry. "Model-Based Detection of Attacks for Process Control Systems," 16th ACM Computer and Communications Security Conference, ACM, submitted, 2009.

  We present security analysis of process control systems (PCS) when an attacker can compromise sensor measurements that are critical for maintaining the operational goals. We present the general sensor attack model that can represent a wide variety of DoS and deception attacks. By taking example of a well studied process control system, we discuss the consequences of sensor attacks on the performance of the system and important implications for designing defense actions. We develop model-based detection methods that can be tuned to limit the false-alarm rates while detecting a large class of sensor attacks. From the attacker's viewpoint, we show that when the detection mechanisms and control system operations are understood by the attacker, it can carry stealth attacks that maximize the chance of missed detection. From the defender's viewpoint, we show that when an attack is detected, the use of model-based outputs maintains safety under compromised sensor measurements.

- [6]Anil Aswani, Harendra Guturu, Claire Tomlin. "System identification of hunchback protein patterning in early Drosophila embryogensis," CDC 2009, 2009; Submitted.

  Early patterning in the Drosophila melanogaster embryo occurs through a complicated network of interactions involving transcription factor proteins and the mRNA of their target genes. One such system is the pattern of hunchback mRNA and its regulation by Bicoid and Krüppel proteins. This system is well-studied, but there is disagreement amongst biologists on how exactly hunchback expression is regulated. We attempt here to provide evidence to distinguish between two models in contention, through system identification. Our general approach is to do nonlinear regression on a parametric, nonlinear partial differential equation model which incorporates transcription, diffusion, and degradation. We perform the regression, analyze the results and then interpret the results in the biological context. We also compare our results to previous work on this system.

- [7]YuLun Huang, Alvaro Cárdenas, Saurabh Amin, Song-Zyun Lin , Hsin-Yi Tsai, S. Shankar Sastry. International Journal of Critical Infrastructure Protection, "Under-

standing the Physical and Economic Consequences of Attacks Against Control Systems.," pp. in publication, 2009.

This paper describes an approach for developing threat models for attacks on control systems. These models are useful for analyzing the actions taken by an attacker who gains access to control system assets and for evaluating the effects of the attacker's actions on the physical process being controlled. The paper proposes models for integrity attacks and denial-of-service (DoS) attacks, and evaluates the physical and economic consequences of the attacks on a chemical reactor system. The analysis reveals two important points. First, a DoS attack does not have a significant effect when the reactor is in the steady state; however, combining the DoS attaack with a relatively innocuous integrity attack rapidly causes the reactor to move to an unsafe state. Second, an attack that seeks to increase the operational cost of the chemical reactor involves a radically different strategy than an attack on plant safety (i.e., one that seeks to shut down the reactor or cause an explosion).

- [8]Alessandro DInnocenzo, Alessandro Abate, Maria D. Di Benedetto, S. Shankar Sastry. "Approximate Abstractions of Discrete-Time Controlled Stochastic Hybrid Systems," Decision and Control, 2008. CDC 2008. 47th IEEE Conference on, 221-226, 9, December, 2008.

  This work presents a procedure to construct a finite abstraction of a controlled discrete-time stochastic hybrid system. The state space and the control space of the original system are partitioned by finite lattices, according to some refinement parameters. The errors introduced by the abstraction procedure can be explicitly computed, over time, given some continuity assumptions on the original model. We show that the errors can be arbitrarily tuned by selecting the partition accuracy. The obtained abstraction can be interpreted as a controlled Markov set-Chain, and can be used both for verification and control design purposes. We test the proposed technique to analyze a model from systems biology.

- [9]Anil Aswani, Peter Bickel, Claire Tomlin. Annals of Statistics, "Exterior Derivative Estimation on Manifolds," 2009; Submitted.

  Collinearity and near-collinearity of predictors cause difficulties when doing nonparametric regression on manifolds. In such scenar ios, variable selection becomes untenable because of mathematical difficulties concerning the existence and numerical stability of the regression coefficients. In addition, once computed, the regression coefficients are difficult to interpret, because a gradient does not exist for functions on manifolds. Fortunately, there is an extension of the gradient to functions on manifolds; this extension is known as the exterior derivative of a function. It is the natural quantity to estimate, because it is a mathematically well-defined quantity with a geometrical interpretation. We propose a set of novel estimators using a regularization scheme for the regression problem which considers the geometrical intuition of the exterior derivative. The advantage of this regularization scheme is that it allows us to add lasso-type regularization to the regression problem, which enables lasso-type regressions in the presence of collinearities. Finally, we consider the "large p, small n" problem in our context and show the consistency and variable selection abilities of our estimators.

- [10]Anil Aswani, Claire Tomlin. "Topology Based Control of Biological Genetic Networks," Decision and Control, 2008. CDC 2008. 47th IEEE Conference on, 781-786,

9, December, 2008.

The traditional controller scheme has been to input a signal into a plant, where the signal is derived from either an open-loop or a closed-loop. This control strategy requires that our plant is able to accept inputs or can be modified to do so. However, this situation is not always true in biological genetic networks; in these systems, there is often no input or obvious modification to allow inputs. Many genetic networks are different, and we believe that they require a new paradigm for control. Biotechnology techniques are such that it is easier to make topological changes to a genetic network than it is to either change the states of the pathway or add more elements to the pathway (i.e. changing the "circuit"). Thus, for such genetic networks it is important to develop a theory of control based on making large-scale changes (e.g. genetic mutations) to the topology of the network. We highlight some useful results from monotone and hybrid systems theory, and show how these results can be used for such a topological controller scheme. We consider the cancer-related, p53 pathway as an example. We analyze the system using control theory and devise a controller.

- [11]Jerry Ding, Jonathan Sprinkle, S. Shankar Sastry, Claire Tomlin. "Reachability Calculations for Automated Aerial Refueling," IEEE Conference on Decision and Control, IEEE, 3706-3712, December, 2008.

  This paper describes reachability calculations for a hybrid system formalism governing UAVs interacting with another vehicle in a safety-critical situation. We examine this problem to lay the foundations toward the goal of certifying certain protocols for flight critical systems. In order to pursue these goals, we describe here what mathematical foundations are necessary to inform protocol certification, as well as describe how such formalisms can be used to automatically synthesize simulations to test against certain danger areas in the protocol. This can provide a mathematical basis for the UAV to perhaps reject a command based on the known unsafe behavior of the vehicle. We describe how creating this formalism can help to refine or design protocols for multi-UAV and/or manned vehicle interaction to avoid such scenarios, or to define appropriate behaviors in those cases.

- [12]Alessandro Abate, Maria Prandini, John Lygeros, S. Shankar Sastry. Automatica, "Probabilistic Reachability and Safety for Controlled Discrete Time Stochastic Hybrid Systems," 44(11):2724-2734, November 2008.

  In this work, probabilistic reachability over a finite horizon is investigated for a class of discrete time stochastic hybrid systems with control inputs. A suitable embedding of the reachability problem in a stochastic control framework reveals that it is amenable to two complementary interpretations, leading to dual algorithms for reachability computations. In particular, the set of initial conditions providing a certain probabilistic guarantee that the system will keep evolving within a desired 'safe' region of the state space is characterized in terms of a value function, and 'maximally safe' Markov policies are determined via dynamic programming. These results are of interest not only for safety analysis and design, but also for solving those regulation and stabilization problems that can be reinterpreted as safety problems. The temperature regulation problem presented in the paper as case study is one such case.

- [13]Jonathan Sprinkle, J. Mikael Eklund, Humberto Gonzalez, Esten Ingar Grøtli, Pannag R Sanketi, Michael Moser, S. Shankar Sastry. Technical report, "Recovering

Models of a Four-Wheel Vehicle Using Vehicular System Data," University of California, Berkeley, August, 2008.

This paper discusses efforts to parameterize the actuation models of a four-wheel automobile for the purposes of closed-loop control. As a novelty, the authors used the equipment already available or in use by the vehicle, rather than expensive equipment used solely for the purpose of system identification. After rudimentary measurements were taken of wheelbase, axle width, etc., the vehicle was driven and data were captured using a controller area network (CAN) interface. Based on this captured data, we were able to estimate the feasibility of certain closed-loop controllers, and the models they assumed (i.e., linear, or nonlinear) for control. Examples were acceleration and steering. This work served to inform the separation of differences in simulation and vehicle behavior during vehicle testing.

- [14]Alvaro Cárdenas, Saurabh Amin, S. Shankar Sastry. "Research Challenges for the Security of Control Systems.," Proceedings of the 3rd USENIX Workshop on Hot topics in security, USENIX, Article 6, 25, July, 2008.

  In this paper we attempt to answer two questions: (1) Why should we be interested in the security of control systems? And (2) What are the new and fundamentally different requirements and problems for the security of control systems? We also propose a new mathematical framework to analyze attacks against control systems. Within this framework we formulate specific research problems to (1) detect attacks, and (2) survive attacks.

- [15]Alvaro Cárdenas, Saurabh Amin, S. Shankar Sastry. "Secure Control: Towards Survivable Cyber-Physical Systems," First International Workshop on Cyber-Physical Systems, 495-500, 17, June, 2008.

  In this position paper we investigate the security of cyber-physical systems. We (1) identify and define the problem of secure control, (2) investigate the defenses that information security and control theory can provide, and (3) propose a set of challenges that need to be addressed to improve the survivability of cyber-physical systems.

- [16]Alvaro Crdenas, Saurabh Amin, S. Shankar Sastry. "Secure Control: Towards Survivable Cyber-Physical Systems.," First International Workshop on Cyber-Physical Systems (WCPS2008)., June, 2008.

  In this position paper we investigate the security of cyberphysical systems. We (1) identify and define the problem of secure control, (2) investigate the defenses that information security and control theory can provide, and (3) propose a set of challenges that need to be addressed to improve the survivability of cyber-physical systems.

- [17]Alvaro Cárdenas, Tanya Roosta, Gelareh Taban, S. Shankar Sastry. Giorgio Franceschetti and Marina Grossi (eds.), "Cyber Security: Basic Defenses and Attack Trends," 4, 73-101, First, Artech House, 2008.

  (No abstract.)

- [18]Alessandro Abate, Alessandro D'Innocenzo, Maria D Di Benedetto, S. Shankar Sastry. M. Egerstedt and B. Misra (eds.), "Markov Set-Chains as Abstractions of Stochastic Hybrid Systems," 1, Springer Verlag, 2008.

The objective of this study is to introduce an abstraction procedure that applies to a general class of dynamical systems, that is to discrete-time stochastic hybrid systems (dt-SHS). The procedure abstracts the original dt-SHS into a Markov set-chain (MSC) in two steps. First, a Markov chain (MC) is obtained by partitioning the hybrid state space, according to a controllable parameter, into non-overlapping domains and computing transition probabilities for these domains according to the dynamics of the dt-SHS. Second, explicit error bounds for the abstraction that depend on the above parameter are derived, and are associated to the computed transition probabilities of the MC, thus obtaining a MSC. We show that one can arbitrarily increase the accuracy of the abstraction by tuning the controllable parameter, albeit at an increase of the cardinality of the MSC. Resorting to a number of results from the MSC literature allows the analysis of the dynamics of the original dt-SHS. In the present work, the asymptotic behavior of the dt-SHS dynamics is assessed within the abstracted framework.

- [19]Alessandro Abate, Maria Prandini, John Lygeros, S. Shankar Sastry. "Neuro-Dynamic Programming for Probabilistic Reachability of Stochastic Hybrid Systems," Submitted, 2008.

  (No abstract.)

- [20]Anil Aswani, Claire Tomlin. IEEE TAC, "Monotone Piecewise Affine Systems," 2008; Submitted.

  (No abstract.)

- [21]Alessandro Abate, Maria Prandini, John Lygeros, S. Shankar Sastry. M. Egerstedt and B. Misra (eds.), "Approximation of General Stochastic Hybrid Systems by Switching Diffusions with Random Hybrid Jumps," 598 - 601, Springer Verlag, 2008; Chapter in "Hybrid Systems: Computation and Control," 2008 .

  In this work we propose an approximation scheme to transform a general stochastic hybrid system (SHS) into a SHS without forced transitions due to spatial guards. Such switching mechanisms are replaced by spontaneous transitions with state-dependent transition intensities (jump rates). The resulting switching diffusion process with random hybrid jumps is shown to converge in distribution to the original stochastic hybrid system execution. The obtained approximation can be useful for various purposes such as, on the computational side, simulation and reachability analysis, as well as for the theoretical investigation of the model. More generally, it is suggested that SHS which are endowed exclusively with random jumping events are simpler than those that present spatial forcing transitions. In the opening of this work, the general SHS model is presented, a few of its basic properties are discussed, and the concept of generator is introduced. The second part of the paper describes the approximation procedure, introduces the new SHS model, and proves, under some assumptions, its weak convergence to the original system.

3 Outreach

3.1 Project Training and Development

3.2 Outreach Activities

Continuing in our mission to build a modern systems science (MSS) with profound implications on the nature and scope of computer science and engineering research, the structure of computer science and electrical engineering curricula, and future industrial practice. This new systems science must pervade engineering education throughout the undergraduate and graduate levels. Embedded software and systems represent a major departure from the current, separated structure of computer science (CS), computer engineering (CE), and electrical engineering (EE). In fact, the new, emerging systems science reintegrates information and physical sciences. The impact of this change on teaching is profound, and cannot be confined to graduate level.
This year we have continued our work to lay the foundation for a new philosophy of undergraduate teaching at the participating institutions.

3.2.1 Curriculum Development for Modern Systems Science (MSS)

Our agenda is to restructure computer science and electrical engineering curricula to adapt to a tighter integration of computational and physical systems. Embedded software and systems represent a major departure from the current, separated structure of computer science (CS), computer engineering (CE), and electrical engineering (EE). In fact, the new, emerging systems science reintegrates information and physical sciences. The impact of this change on teaching is profound, and cannot be confined to graduate level. Based on the ongoing, groundbreaking effort at UCB, we are engaged in retooling undergraduate teaching at the participating institutions, and making the results widely available to encourage critical discussion and facilitate adoption.
We are engaged in an effort at UCB to restructure the undergraduate systems curriculum (which includes courses in signals and systems, communications, signal processing, control systems, image processing, and random processes). The traditional curriculum in these areas is mature and established, so making changes is challenging. We are at the stage of attempting to build faculty consensus for an approach that shortens the pre-requisite chain and allows for introduction of new courses in hybrid systems and embedded software systems.

3.2.2 Undergrad Course Insertion and Transfer

At many institutions, introductory courses are quite large. This makes conducting such a course a substantial undertaking. In particular, the newness of the subject means that there are relatively few available homework and lab exercises and exam questions. To facilitate use of this approach by other instructors, we have engaged technical staff to build web infrastructure supporting such courses. We have built an instructor forum that enables submission and selection of problems from the text and from a library of submitted problems and exercises. A server-side infrastructure generates PDF files for problem sets and solution sets.
The tight integration of computational and physical topics offers opportunities for leveraging technology to illustrate fundamental concepts. We have developed a suite of web pages

with applets that use sound, images, and graphs interactively. Our staff has extended and upgraded these applets and created a suite of PowerPoint slides for use by instructors.
We have begun to define an upper division course in embedded software (aimed at juniors and seniors). This new course will replace the control course at the upper division level at San Jose State. We also continued to teach at UC Berkeley the integrated course designed by Prof. Lee, which employs techniques discovered in the hybrid and embedded systems research to interpret traditional signals.

Course: Introduction to Embedded Systems (UCB EECS 124)
http://chess.eecs.berkeley.edu/eecs124

Instructors:
Prof. Edward A. Lee
Prof. Sanjit A. Seshia
Prof. Claire J. Tomlin

Professor Tomlin assisted in development of the undergraduate Introduction to Embedded Systems course, EECS 124. The new material was taught in the Spring Semester of 2009 by Professor Sanjit A. Seshia.

The abstract for the class is below:

EECS 149 is a new undergraduate course, first offered on a pilot basis in Spring 2008 with course number EECS 124. This class is intended to introduce students to the design and analysis of computational systems that interact with physical processes. Applications of such systems include medical devices and systems, consumer electronics, toys and games, assisted living, traffic control and safety, automotive systems, process control, energy management and conservation, environmental control, aircraft control systems, communications systems, instrumentation, critical infrastructure control (electric power, water resources, and communications systems for example), robotics and distributed robotics (telepresence, telemedicine), defense systems, manufacturing, and smart structures.

A major theme of this course will be on the interplay of practical design with formal models of systems, including both software components and physical dynamics. A major emphasis will be on building high confidence systems with real-time and concurrent behaviors.

This is the second offering of the course, and we are still actively engaged in developing the course content and labs. This offering is therefore advised for advanced and adventurous undergraduates.

Course: Introduction to Control Design Techniques (UCB EECS 128)
http://inst.eecs.berkeley.edu/ ee128/fa08/

Instructor:
Prof. Claire J. Tomlin

Professor Tomlin has redesigned the undergraduate control theory and engineering course, EECS 128, adding new labs and course material. The new material was taught in the Fall Semester of 2008.

The abstract for the class is below:

Root-locus and frequency response techniques for control system synthesis. State-space techniques for modeling, full-state feedback regulator design, pole placement, and observer design. Combined observer and regulator design. Lab experiments on computers connected to mechanical systems.

- Transfer function and state space models for control system analysis and syn-

thesis. Pole locations and relationship to time response. Root locus methods. Stability.

- Feedback. Review of single-input single output (SISO) analysis and control methods in the frequency domain (Bode, Nyquist).
- SISO analysis and control using state space models. The matrix exponential and its relationship to time response. Controllability and observability. Combining state feedback with observers.
- Multi-input multi-output analysis and control using state space models.
- The linear quadratic regulator.

3.2.3 Graduate Courses

As part of the no-cost extension, a course in embedded systems was taught in the area of embedded and hybrid systems, as well as systems modeling. This course is a reflection of the teaching and curriculum goals of the ITR and its affiliated faculty.

Course: Linear System Theory(UCB EE221A)
http://inst.eecs.berkeley.edu/ ee221A/fa08/

Instructor: Claire J. Tomlin

Professor Tomlin is modernizing the graduate course in linear system theory, EECS 221A, adding units in linear programming and more general optimization. The new material was taught in the Fall Semester of 2008.

The abstract for the class is below:

This course provides a comprehensive introduction to the modeling, analysis, and control of linear dynamical systems. Topics include: A review of linear algebra and matrix theory. The solutions of linear equations. Least-squares approximation and linear programming. Linear ordinary differential equations: existence and uniqueness of solutions, the state-transition matrix and matrix exponential. Input-output and internal stability; the method of Lyapunov. Controllability and observability; basic realization theory. Control and observer design: pole placement, state estimation. Linear quadratic optimal control: Riccati equation and properties of the LQ regulator. Advanced topics such as robust control and hybrid system theory will be presented based on allowable time and interest from the class.

This course provides a solid foundation for students doing research that requires the design and use of dynamic models. Students in control, circuits, signal processing, communications and networking are encouraged to take this course.

- Linear Algebra: Fields, vector spaces, subspaces, bases, dimension, range and Null spaces, linear operators, norms, inner products, adjoints.
- Matrix Theory: Eigenspaces, Jordan form, Hermitian forms, positive definiteness, singular value decomposition, functions of matrices, spectral mapping theorem, computational aspects.
- Optimization: Linear equations, least-squares approximation, linear programming.

- Differential Equations: existence and uniqueness of solutions, Lipschitz continuity, linear ordinary differential equations, the notion of state, the state-transition matrix.
- Stability: Internal stability, input-output stability, the method of Lyapunov.
- Linear Systems - open-loop aspects: controllability and observability, duality, canonical forms, the Kalman decomposition, realization theory, minimal realizations.
- Linear systems - feedback aspects: pole placement, stabilizability and detectability, observers, state estimation, the separation principle.
- Linear quadratic optimal control: least-squares control and estimation, Riccati equations, properties of the LQ regulator.
- Advanced topics: robust control, hybrid systems.

4 Publications and Products

In this section, we list published papers only. Submitted papers and in press papers are described in Section 2.2.

4.1 Technical reports

- [13]Jonathan Sprinkle, J. Mikael Eklund, Humberto Gonzalez, Esten Ingar Grtli, Pannag R Sanketi, Michael Moser, S. Shankar Sastry. Technical report, "Recovering Models of a Four-Wheel Vehicle Using Vehicular System Data," University of California, Berkeley, August, 2008.

4.2 Conference papers

- [16]Alvaro Crdenas, Saurabh Amin, S. Shankar Sastry. "Secure Control: Towards Survivable Cyber-Physical Systems.," First International Workshop on Cyber-Physical Systems (WCPS2008)., June, 2008.

- [10]Anil Aswani, Claire Tomlin. "Topology Based Control of Biological Genetic Networks," Decision and Control, 2008. CDC 2008. 47th IEEE Conference on, 781-786, 9, December, 2008.

- [19]Alessandro Abate, Maria Prandini, John Lygeros, S. Shankar Sastry. "Neuro-Dynamic Programming for Probabilistic Reachability of Stochastic Hybrid Systems," Submitted, 2008.

- [15]Alvaro Cárdenas, Saurabh Amin, S. Shankar Sastry. "Secure Control: Towards Survivable Cyber-Physical Systems," First International Workshop on Cyber-Physical Systems, 495-500, 17, June, 2008.

- [8]Alessandro DInnocenzo, Alessandro Abate, Maria D. Di Benedetto, S. Shankar Sastry. "Approximate Abstractions of Discrete-Time Controlled Stochastic Hybrid Systems," Decision and Control, 2008. CDC 2008. 47th IEEE Conference on, 221-226, 9, December, 2008.

- [5]Zong-Syun Lin, Alvaro Cárdenas, Saurabh Amin, Yu-Lun Huang, Chi-Yen Huang, S. Shankar Sastry. "Model-Based Detection of Attacks for Process Control Systems," 16th ACM Computer and Communications Security Conference, ACM, submitted, 2009.

- [14]Alvaro Cárdenas, Saurabh Amin, S. Shankar Sastry. "Research Challenges for the Security of Control Systems.," Proceedings of the 3rd USENIX Workshop on Hot topics in security, USENIX, Article 6, 25, July, 2008.

- [11]Jerry Ding, Jonathan Sprinkle, S. Shankar Sastry, Claire Tomlin. "Reachability Calculations for Automated Aerial Refueling," IEEE Conference on Decision and Control, IEEE, 3706-3712, December, 2008.

- [3]Saurabh Amin, Alvaro Cárdenas, S. Shankar Sastry. "Safe and Secure Networked Control Systems Under Denial-of-Service Attacks.," Hybrid Systems: Computation

and Control, Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 31-45, 30, April, 2009.

- [4]Alvaro Cárdenas, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, S. Shankar Sastry. "Challenges for Securing Cyber Physical Systems," First Workshop on Cyber-physical Systems Security, DHS, submitted, 2009.

4.3 Book chapters or sections

- [17]Alvaro Cárdenas, Tanya Roosta, Gelareh Taban, S. Shankar Sastry. Giorgio Franceschetti and Marina Grossi (eds.), "Cyber Security: Basic Defenses and Attack Trends," 4, 73-101, First, Artech House, 2008.

- [21]Alessandro Abate, Maria Prandini, John Lygeros, S. Shankar Sastry. M. Egerstedt and B. Misra (eds.), "Approximation of General Stochastic Hybrid Systems by Switching Diffusions with Random Hybrid Jumps," 598 - 601, Springer Verlag, 2008; Chapter in "Hybrid Systems: Computation and Control," 2008 .

- [18]Alessandro Abate, Alessandro D'Innocenzo, Maria D Di Benedetto, S. Shankar Sastry. M. Egerstedt and B. Misra (eds.), "Markov Set-Chains as Abstractions of Stochastic Hybrid Systems," 1, Springer Verlag, 2008.

4.4 Journal articles

- [20]Anil Aswani, Claire Tomlin. IEEE TAC, "Monotone Piecewise Affine Systems," 2008; Submitted.

- [7]YuLun Huang, Alvaro Cárdenas, Saurabh Amin, Song-Zyun Lin , Hsin-Yi Tsai, S. Shankar Sastry. International Journal of Critical Infrastructure Protection, "Understanding the Physical and Economic Consequences of Attacks Against Control Systems.," pp. in publication, 2009.

- [2]Alvaro Cárdenas, Tanya Roosta, S. Shankar Sastry. Ad Hoc Networks, "Rethinking Security Properties, Threat Models and the Design Space in Sensor Networks : A case study in SCADA systems," pp. in publication, May 2009.

- [12]Alessandro Abate, Maria Prandini, John Lygeros, S. Shankar Sastry. Automatica, "Probabilistic Reachability and Safety for Controlled Discrete Time Stochastic Hybrid Systems," 44(11):2724-2734, November 2008.

Although this is a long term project focused on foundations, we are actively working to set up effective technology transfer mechanisms for dissemination of the research results. A major part of this is expected to occur through the open dissemination of software tools.

4.4.1 The 2008-2009 Chess seminar series

The Chess seminar series provides a weekly forum for the problems and solutions found and solved by Chess members, as well as ongoing research updates. This forum works best when the audience is diverse in background, because the goal is to aid researchers in seeing how

the other sub-disciplines are approaching similar problems, or to encourage them to work on problems they had not yet considered.
A full listing of this project-year's speakers is below. Most talks can be downloaded from the seminar website, at http://chess.eecs.berkeley.edu/seminar.htm

- "Model Transformation with Hierarchical Discrete-Event Control"
  Thomas Huining Feng, University of California, Berkeley, May 6, 2009.

- "Interval-based Abstraction Refinement and Applications"
  Pritam Roy, University of California, Santa Cruz, May 5, 2009.

- "Underpinning Empirical Architecture in a Concurrent Cyber-Physical World"
  Graham Hellestrand, Embedded Systems Technology Inc., San Carlos, California, April 28, 2009.

- "Modeling, Simulation and Analysis of Integrated Building Energy and Control Systems"
  Michael Wetter, Simulation Research Group, Lawrence Berkeley National Laboratory, Berkeley, April 21, 2009.

- "On the synthesis of correct-by-design embedded control software"
  Paulo Tabuada, University of California, Los Angeles, April 17, 2009.

- "Embedded system design with the Polychronous paradigm"
  Albert Benveniste, INRIA/IRISA, Rennes, France, April 14, 2009.

- "Mobile Millennium: using smartphones to monitor traffic in privacy aware environments"
  Alexandre Bayen, University of California, Berkeley, April 7, 2009.

- "1: Design as You See FIT: System-Level Soft Error Analysis of Sequential Circuits & 2: Optimizations of an Application-Level Protocol for Enhanced Dependability in FlexRay"
  Daniel Holcomb and Wenchao Li, UC Berkeley, March 31, 2009.

- "Integrative Modeling and Heterogeneous System Simulation"
  Dr. Jonathan Sprinkle, University of Arizona, March 17, 2009.

- "Manycore Vector-Thread Architectures"
  Christopher Batten, University of California, Berkeley, March 10, 2009.

- "Uses of Synchronized Clocks in Test and Measurement Systems"
  Jeff Burch and John Eidson, Agilent Labs, March 3, 2009.

- "Implementing Synchronous Models on Distributed Execution Platforms"
  Stavros Tripakis, University of California, Berkeley, February 24, 2009.

- "The APES-LESS project: Access Point Event Simulation of Legacy Embedded Software Systems"
  Stefan Resmerita, University of Salzburg, February 17, 2009.

- "Model-Based Development of Fault-Tolerant Real-Time Systems"
  Christian Buckl, TU Munchen, February 10, 2009.

- "Modular Code Generation from Synchronous Block Diagrams: Modularity vs. Reusability vs. Code Size"
  Stavros Tripakis, University of California, Berkeley, February 3, 2009.

- "Time Portable Programming the JAviator in Tiptoe OS"
  Christoph Kirsch, University of Salzburg, January 13, 2009.

- "Synchronous Reactive Communication: Generalization, Implementation, and Optimization"
  Guoqiang (Gerald) Wang, University of California, Berkeley, December 9, 2008.

- "Service Component Architecture (SCA)"
  Luciano Resende, IBM Silicon Valley, San Jose, California, December 2, 2008.

- "Process Network in Silicon: A High-Productivity, Scalable Platform for High-Performance Embedded Computing"
  Mike Butts, Ambric, Inc., Beaverton, Oregon, November 25, 2008.

- "The Design of a Platform-Based Design Environment for Synthetic Biology"
  Douglas Densmore, UC Berkeley, Berkeley, California, November 18, 2008.

- "The Nimrod/K director for the Kepler workflow environment"
  Colin Enticott, Monash University, Australia, November 12, 2008.

- "Toward the Predictable Integration of Real-Time COTS Based Systems"
  Marco Caccamo, University of Illinois, Urbana Champaign, October 28, 2008.

- "Model Engineering"
  Edward A. Lee and the Ptolemy Pteam, University of California, Berkeley, Berkeley, October 21, 2008.

- "Verification-Guided Error Resilience"
  Prof. Sanjit Seshia, University of California, Berkeley, Berkeley, October 7, 2008.

- "Game-Theoretic Timing Analysis"
  Sanjit Seshia, UC Berkeley, Berkeley, California, September 23, 2008.

- "Integrating Timing with Data and Space Availability as Firing Rules for Actors in a Graphical Dataflow Language"
  Tim Hayles, National Instruments, Austin, Texas, September 9, 2008.

- "On Computer Science in Systems Biology"
  Oded Maler, CNRS-VERIMAG, Grenoble, France, August 22, 2008.

- "From Control Loops to Software"
  Oded Maler, CNRS-VERIMAG, Grenoble, France, August 21, 2008.

- "Timed Automata: Modeling and Analysis"
  Oded Maler, CNRS-VERIMAG, Grenoble, France, August 20, 2008.

- "Verification for Dummies: A Gentle Introduction to Formal Verification and Hybrid Systems"
  Oded Maler, CNRS-VERIMAG, Grenoble, France, August 19, 2008.
- "Modular Timed Graph Transformation"
  Hans Vangheluwe, McGill University, Quebec, Canada, August 6, 2008.
- "Stability Analysis of Switched Systems using Variational Principles"
  Michael Margaliot, Tel Aviv University, Israel, August 5, 2008.
- "Buffer Capacity Computation for Throughput Constrained Streaming Applications with Data-Dependent Inter-Task Communication"
  Maarten Wiggers, University of Twente, The Netherlands, July 31, 2008.
- "A Type System for the Automatic Distribution of Higher-order Synchronous Dataflow Programs"
  Alain Girault, INRIA, June 10, 2008
- "Heterogeneous System Design with Functional DIF"
  William Plishker, University of Maryland, June 5, 2008.
- "Advanced topics in model-based software development"
  Bernhard Rumpe, Braunschweig University of Technology, June 3rd, 2008

4.4.2 Workshops and Invited Talks

In addition to the below invited and workshop organizational activities, Chess faculty have delivered numerous plenary talks, invited talks, as well as informal dissemination of Chess goals and research.

-

4.4.3 General Dissemination

The Chess website, http://chess.eecs.berkeley.edu, includes publications and software distributions. In addition, as part of the outreach effort, the UC Berkeley introductory signals systems course, which introduces hybrid systems, is available.

4.5 Other Specific Products

The following software packages have been made available during this review period on the Chess website, http://chess.eecs.berkeley.edu:

- Upcoming software release in Fall, 2009, working title "Berkeley Intelligent Robotics Toolkit", to appear on http://robotics.eecs.berkeley.edu/drive/.

5 Contributions

This section summarizes the major contributions during this reporting period.

5.1 Within Discipline

5.1.1 Hybrid Systems Theory

5.1.2 Model-Based Design

5.1.3 Advanced Tool Architectures

5.2 Other Disciplines

5.3 Human Resource Development

Several panels in important conferences and workshops pertinent to embedded systems (e.g., DAC, ICCAD, HSCC, EMSOFT, CASES, and RTSS) have pointed out the necessity of upgrading the talents of the engineering community to cope with the challenges posed by the next generation embedded system technology. Our research program has touched many graduate students in our institutions and several visiting researchers from industry and other Universities so that they now have a deep understanding of embedded system software issues and techniques to address them.

Specifically, our directors played a major role in the development of workshops and briefings to executives and researchers in the avionics industry to motivate increased research spending due to an anticipated drop in research funds available to train graduates in embedded software and embedded systems. One particular intersection with our efforts is the Software Producibility Initiative out of the Office of the Secretary of Defense.

The industrial affiliates to our research program are increasing and we hope to be able to export in their environments a modern view of system design. Preliminary feedback from our partners has underlined the importance of this process to develop the professional talent pool.

5.4 Integration of Research and Education

In this report, we have touched multiple times on research and education especially in the outreach section. In addition, there has been a strong activity in the continued update of the undergraduate course taught at Berkeley on the foundations of embedded system design. The graduate program at Berkeley and at Vanderbilt has greatly benefited from the research work in the ITR. EE249 at Berkeley has incorporated the most important results thus far obtained in the research program. EE 290 A and C, advanced courses for PhD students, have featured hybrid system and the interface theories developed under this project. EE219C, a course on formal verification, has used results from the hybrid theory verification work in the program. Finally, many final projects in these graduate courses have resulted in papers and reports listed in this document. The course EE291E on Hybrid Systems: Computation and Control is jointly taught at Berkeley and Vanderbilt and is benefiting a great deal from comments of students as far as the development of new text book material.

In addition to the influence on graduate students, we have endeavored to show hybrid and embedded systems as emerging research opportunities to undergraduates. We have also demonstrated that for advanced undergraduates these topics are not out of place as senior design courses, or advanced topics courses, which may in the future lead to the integration of these as disciplines in engineering across a broader reach of universities.

5.5 Beyond Science and Engineering

Embedded systems are part of our everyday life and will be much more so in the future. In particular, wireless sensor networks will provide a framework for much better environmental monitoring, energy conservation programs, defense and health care. Already in the application chapter, we can see the impact of our work on these themes. In the domain of transportation systems, our research is improving safety in cars, and foundationally improving control of energy conserving aspects such as hydrocarbon emissions. Future applications of hybrid system technology will involve biological systems to a much larger extent showing that our approach can be exported to other field of knowledge ranging from economics to biology and medicine. At Berkeley, the Center for Information Technology Research in the Interest of Society is demonstrating the potential of our research in fields that touch all aspects of our life. Some key societal grand challenge problems where our ITR research is making a difference includes health care delivery, high confidence medical devices and systems, avionics, cybersecurity, and transportation.

References

[1] Anil Aswani, Peter Bickel, and Claire Tomlin. Statistics for sparse, high-dimensional, and nonparametric system identification. In IEEE ICRA 2009, pages 2133–2138, May 2009.

[2] Alvaro Cardenas, Tanya Roosta, and S. Shankar Sastry. Rethinking security properties, threat models and the design space in sensor networks : A case study in scada systems. Ad Hoc Networks, page in publication, May 2009.

[3] Saurabh Amin, Alvaro Cardenas, and S. Shankar Sastry. Safe and secure networked control systems under denial-of-service attacks. In Hybrid Systems: Computation and Control, pages 31–45. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, April 2009.

[4] Alvaro Cardenas, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, and S. Shankar Sastry. Challenges for securing cyber physical systems. In First Workshop on Cyber-physical Systems Security, page submitted. DHS, 2009.

[5] Zong-Syun Lin, Alvaro Cardenas, Saurabh Amin, Yu-Lun Huang, Chi-Yen Huang, and S. Shankar Sastry. Model-based detection of attacks for process control systems. In 16th ACM Computer and Communications Security Conference, page submitted. ACM, 2009.

[6] Anil Aswani, Harendra Guturu, and Claire Tomlin. System identification of hunchback protein patterning in early drosophila embryogensis. In CDC 2009, 2009. Submitted.

[7] YuLun Huang, Alvaro Cardenas, Saurabh Amin, Song-Zyun Lin, Hsin-Yi Tsai, and S. Shankar Sastry. Understanding the physical and economic consequences of attacks against control systems. International Journal of Critical Infrastructure Protection, page in publication, 2009.

[8] Alessandro D'Innocenzo, Alessandro Abate, Maria D. Di Benedetto, and S. Shankar Sastry. Approximate abstractions of discrete-time controlled stochastic hybrid systems. In Decision and Control, 2008. CDC 2008. 47th IEEE Conference on, pages 221–226, December 2008.

[9] Anil Aswani, Peter Bickel, and Claire Tomlin. Exterior derivative estimation on manifolds. Annals of Statistics, 2009. Submitted.

[10] Anil Aswani and Claire Tomlin. Topology based control of biological genetic networks. In Decision and Control, 2008. CDC 2008. 47th IEEE Conference on, pages 781–786, December 2008.

[11] Jerry Ding, Jonathan Sprinkle, S. Shankar Sastry, and Claire Tomlin. Reachability calculations for automated aerial refueling. In IEEE Conference on Decision and Control, pages 3706–3712. IEEE, December 2008.

[12] Alessandro Abate, Maria Prandini, John Lygeros, and S. Shankar Sastry. Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems. Automatica, 44(11):2724–2734, November 2008.

[13] Jonathan Sprinkle, J. Mikael Eklund, Humberto Gonzalez, Esten Ingar Grtli, Pannag R Sanketi, Michael Moser, and S. Shankar Sastry. Recovering models of a four-wheel vehicle using vehicular system data. Technical report, University of California, Berkeley, August 2008.

[14] Alvaro Cardenas, Saurabh Amin, and S. Shankar Sastry. Research challenges for the security of control systems. In Proceedings of the 3rd USENIX Workshop on Hot topics in security, page Article 6. USENIX, July 2008.

[15] Alvaro Cardenas, Saurabh Amin, and S. Shankar Sastry. Secure control: Towards survivable cyber-physical systems. In First International Workshop on Cyber-Physical Systems, pages 495–500, June 2008.

[16] Alvaro Crdenas, Saurabh Amin, and S. Shankar Sastry. Secure control: Towards survivable cyber-physical systems. In First International Workshop on Cyber-Physical Systems (WCPS2008)., June 2008.

[17] Alvaro Cardenas, Tanya Roosta, Gelareh Taban, and S. Shankar Sastry. Cyber Security: Basic Defenses and Attack Trends, chapter 4, pages 73–101. Artech House, first edition, 2008.

[18] Alessandro Abate, Alessandro D'Innocenzo, Maria D Di Benedetto, and S. Shankar Sastry. Markov Set-Chains as Abstractions of Stochastic Hybrid Systems, volume 1, pages 1–15. Springer Verlag, 2008.

[19] Alessandro Abate, Maria Prandini, John Lygeros, and S. Shankar Sastry. Neurodynamic programming for probabilistic reachability of stochastic hybrid systems. In Submitted, 2008.

[20] Anil Aswani and Claire Tomlin. Monotone piecewise affine systems. IEEE TAC, 2008. Submitted.

[21] Alessandro Abate, Maria Prandini, John Lygeros, and S. Shankar Sastry. Approximation of General Stochastic Hybrid Systems by Switching Diffusions with Random Hybrid Jumps, pages 598 – 601. Springer Verlag, 2008. Chapter in "Hybrid Systems: Computation and Control," 2008.