Controlled Hybrid System Safety Verification: Advanced Life Support System Testbed

Sonja Glavaški , Antonis Papachristodoulou, Kartik Ariyur

***Abstract*— In this paper we demonstrate the use of Barrier Certificates as a method to verify safe performance of a hybrid Variable Configuration CO_2 Removal (VCCR) system. We designed a simple nonlinear feedback controller that tracks a desired CO_2 profile, while ensuring that the CO_2 and O_2 concentrations stay within acceptable limits. Though the controller and its switching rules are simple, we do not have a closed form expression for the equilibrium sets of the closed loop hybrid system, and hence Lyapunov stability analysis and computation of region of attraction are impossible. We used Sum-Of-Squares programming approach to construct and verify that our control law provides safe functionality of VCCR system.**

I. Introduction

Our objective was to automatically synthesize verifiable controllers for hybrid systems. Several methods have been developed to handle systems with large scale discrete dynamics and simple continuous dynamics (such as integrators). More recently, control synthesis tools have been developed for hybrid systems whose continuous dynamics are linear and time invariant. However, these approaches break down in the face of nonlinear continuous dynamics combined with complex decision rules. Moreover, there are seldom any guarantees of performance of the controlled system. We have endeavored in this effort to build practical control synthesis and verification tools for a large class of control systems. The specific application domain for this work was a simulated advanced life support system test-bed.

II. Brief System Description

A more detailed description of the system specifics can be found in [6]. It consists of the main crew cabin and two adsorb/desorb beds, whose purpose is to keep the levels of CO_2 and O_2 inside the two beds at acceptable levels, while tracking a desired reference concentration of O_2 and CO_2. To achieve this, each bed goes into a 3 phase cycle in the following sequence:

- An *adsorb* phase, in which CO_2 is removed from the cabin and gets adsorbed on the bed surface. The adsorbing bed returns CO_2 lean air back in the cabin.
- An *airsave* phase in which the desorbing bed recycles CO_2-lean air back to the cabin from its gas phase. It is assumed that the solid phase CO_2 is frozen in this process, so that no gas escapes from the bed.
- The *desorb* phase, in which the adsorbed CO_2 is removed from the adsorbent, which is accumulated in the CO_2 buffer.

The adsorber beds have a saturation capacity of solid-phase CO_2 they can adsorb. The system is configured in such a way so that when one of the beds is connected to the crew cabin adsorbing CO_2, the other one is undergoing airsave/desorption. After every half-cycle, the beds change their roles and the adsorbing bed goes through airsave/desorption and the desorbing bed goes through adsorption. It is assumed that all desorb/adsorb processes occur at a constant rate.

A. Control Design

The equations that describe the state evolution are different for the airsave, adsorb and desorb processes. They are however simple mass balance equations,that due to limited space are not going to be described in detail. We designed a simple switching PI feedback controller that tracks a desired CO_2 profile, while ensuring that the CO_2 and O_2 concentrations stay within acceptable limits. To do this, we first model controlled VCCR system as a finite automaton using the framework presented in [1].

We initialize the system in Mode 1, at a configuration in which the initial concentration of CO_2 in the cabin and bed 1 is about atmospheric and in bed 2 is below atmospheric. Bed 1 is in adsorber mode and bed 2 is in airsave mode. In the next mode, airsave ends and bed 2 starts desorbing. Switching from Mode 1 to Mode 2 should then happen when the level of CO_2 in bed 2 has reduced significantly. For the switching from Mode 2 to Mode 3 the deciding factor is the level of CO_2 that has been adsorbed in bed 1, i.e. whether it has saturated, and whether the level of CO_2 is almost zero in bed 2, which is desorbing. Switching from Mode 3 to Mode 4 and from Mode 4 to Mode 1 can be done in a symmetric manner. As the adsorption happens at a much slower rate than desorption, the bed that is desorbing will reach saturation before the bed that is adsorbing. This necessitates the introduction of two intermediate modes. The final switching rules are as per Figure 1.

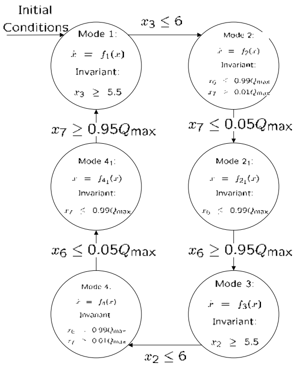

Fig. 1. VCCR finite automaton model.

We should stress that the control laws are functions of the concentration of CO_2 in the cabin and the two beds: the flow rate of the two streams connecting the cabin with the two beds depends on the discrepancy between the desired and actual level of CO_2 in the cabin. Moreover, the switching strategy is also a function of the CO_2 concentration in the beds. The feedback on the O_2 concentration is a "follower" of this strategy, and it is the only link between O_2 and CO_2 dynamics.

III. Barrier certificates for the Advanced Life Support System Safety Verification

Our task is to verify the safety of the system, in particular to ascertain that the levels of CO_2 and O_2 do not vary outside the required levels. To handle the verification problem, we consider the setup presented in [4]. We present here only information relevant to this particular problem.

A. Background

A hybrid system is a tuple $H = (\mathcal{X}, L, X_0, I, F, T)$ with the following components.

- $\mathcal{X} \subset \mathbb{R}^n$ is the continuous state-space.

S.Glavaški (sonja.glavaski@honeywell.com), and K.Ariyur are with Honeywell Labs, 3660 Technology Dr, Minneapolis, MN 55418.
A. Papachristodoulou is with the Department of Control and Dynamical Systems, California Institute of Technology, Pasadena, CA 91125.

0-7803-9098-9/05/$25.00 ©2005 AACC

- L is a finite set of locations. The overall state-space of the system is $X = L \times \mathcal{X}$, and a state of the system is denoted by $(l, x) \in L \times \mathcal{X}$.
- $X_0 \subset X$ is a set of initial states.
- $I : L \rightarrow 2^{\mathcal{X}}$ is the invariant, i.e. the set of all possible continuous states while at location l.
- $F : X \rightarrow 2^{\mathbb{R}^n}$ is a set of vector fields, one for each location.
- $T \subset X \times X$ is a relation describing discrete transitions between two locations, when the state in the particular mode finds itself in the guard set G.

As the system evolves from the initial conditions in the set X_0, and after a sequence of continuous flows and discrete transitions that are described by the map T, the safety verification problem aims in deciding whether the system can reach a set of unsafe states $X_u \subset X$. Construction of barrier certificates is generally not easy, and even proving that a given barrier certificate satisfies the required conditions is hard. However, for systems whose vector fields are polynomial and whose set descriptions are semialgebraic (i.e. described by polynomial equalities and inequalities) then we can use the Sum of Squares decomposition [2] and semidefinite programming to construct polynomial barriers. This procedure is described in detail in [4].

Proposition 1: Let the hybrid system $H = (\mathcal{X}, L, X_0, I, F, T)$, the unsafe set X_u and some nonnegative constants $\sigma_{l,l'}$ be given. Suppose there exists a barrier certificate, i.e. a collection $\{B_l(x)\}$ of functions $B_l(x)$ for all $l \in L$, each of which is differentiable with respect to its argument and satisfies

$$B_l(x) > 0 \qquad \forall\ x \in \text{Unsafe}(l) \tag{1}$$

$$B_l(x) \leq 0 \qquad \forall\ x \in \text{Init}(l) \tag{2}$$

$$\frac{\partial B_l(x)}{\partial x} f_l(x) \leq 0 \qquad \forall\ x \in I(l) \tag{3}$$

$$B_l(x) - \sigma_{l,l'} B_{l'}(x) \leq 0 \qquad \text{for some } l' \in L \text{ and } x \in \text{Guard}(l', l). \tag{4}$$

Then the safety of the hybrid system H is guaranteed.

B. Computational considerations and Verification Result

Though the controller and its switching rules are simple, we do not have a closed form expression for the equilibrium sets of the closed loop hybrid system, and hence Lyapunov stability analysis and computation of region of attraction are impossible. We use Sum-Of-Squares programming approach to construct and verify that our control law provides safe functionality of VCCR system. In order to proceed, one has to obtain descriptions of the unsafe, initial invariant and guard sets as semi-algebraic sets, i.e. they are captured by a vector of polynomial inequalities $g_{\text{Unsafe}(l)} \leq 0$, $g_{\text{Init}(l)}(x) \leq 0$, $g_{I(l)}(x) \leq 0$, and $g_{\text{Guard}(l,l')}(x) \leq 0$. The search for a barrier certificate can then be formulated as a Sum of Squares optimization problem. Due to limited space we will not be able to describe them in detail.

The VCCR system consists of 6 modes with vector fields in each mode of dimension 10 . The vector fields are polynomial in their variables, which facilitates the use of the Sum of Squares decomposition for the analysis, and are of highest order 2. What is required therefore is to construct 6 functions B_l as required by Proposition 1 and have 4 SOS conditions for each one of them. All conditions but condition 3 are of order 2 if B is of order 2. Condition 3 will be higher order than the rest. In fact with 10 state variables the size of the LMI that is produced by this setup is on the boundary of what can be solved using any current SDP solver [5]. Another problem that appears in such computations is inherent stiffness in the systems, i.e. having fast and slow dynamics, or even states that take values in different orders of magnitude. To alleviate this problem, we rescale all states so that they are of the same order of magnitude.

Given the initial, unsafe, invariant and guard sets, a quadratic set of Barrier functions was constructed that proves the safety of the system. The control law provides safe functionality which is verified by constructing a Barrier certificate. The software used is SOSTOOLS [3].

IV. Conclusion and Future work

In this paper we demonstrated the use of Barrier Certificates as a method to verify safe performance of the simple switching controller. Construction of a barrier certificate for the controlled hybrid system proves that it will not escape into unsafe operating regions. Though we were able to provide a barrier certificate for our controlled VCCR system, we were on the limits of what could be achieved with current computing capabilities on a desktop.

V. Acknowledgements

This material is based upon work supported by NASA Ames Research Center under Contract No. NAS2-01067.

References

[1] R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X. Nicolin, A. Oliviero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138:3–34, 1995.

[2] Pablo A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization.* PhD thesis, California Institute of Technology, Pasadena, CA, 2000. Available at http://www.control.ethz.ch/ parrilo/pubs/index.html.

[3] S. Prajna, A. Papachristodoulou, and P. A. Parrilo. SOSTOOLS – Sum of Squares Optimization Toolbox, User's Guide. Available at http://www.cds.caltech.edu/sostools and http://www.aut.ee.ethz.ch/ parrilo/sostools, 2002.

[4] Stephen Prajna and Ali Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *Hybrid Systems: Computation and Control, LNCS 2293*, pages 477–492. Springer–Verlag, 2004.

[5] J. F. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization Methods and Software*, 11–12:625–653, 1999. Available at http://fewcal.kub.nl/sturm/software/sedumi.html,.

[6] D. Subramanian, K. Ariyur, N. Lamba, R. Deshpande, and S. Glavaski. Control design for a hybrid dynamical system: A nasa life support system. In *Hybrid Systems: Computation and Control, LNCS 2293*, pages 570–584. Springer–Verlag, 2004.