Safety Verification and Failure Analysis of Goal-Based Hybrid Control Systems

Thesis by

Julia M. B. Braman

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

2009

(Submitted May 27, 2009)

Acknowledgements

I would like to thank my advisor, Professor Richard Murray, for his support and encouragement. Richard is a great teacher and is extremely hard-working, accommodating, and enthusiastic about what he does, and all those qualities help make him a wonderful advisor.

I would like to thank Professors Jim Beck, Joel Burdick, and Mani Chandy for serving on my thesis committee. Having taken courses from all, I truly respect the enthusiasm each shows for his field.

There are several people that I must thank from the Jet Propulsion Laboratory. First, Mitch Ingham, Dave Wagner, and Kenny Meyer have been great resources, Mitch for all the technical discussions and brainstorming sessions, Dave for the tremendous amount of help in setting up and becoming proficient with MDS, and Kenny for keeping me connected with the MDS group at JPL. Bob Rasmussen and Dan Dvorak deserve special mention for their invaluable instruction on the intricacies of State Analysis and MDS. Many others on the MDS team have given feedback on the many presentations I have given, and I am grateful for their time and insight. Finally, some other JPL folks were kind enough to discuss ideas with me, most notably Alberto Elfes for the Titan aerobot discussions, and Gerard Holzmann and Rajeev Joshi for the Spin model checker discussions.

Last but not least, I would like to thank my family. My parents, Mark and Mary Ann Badger, fought for me when I could not fight for myself. My husband Kevin has been amazing during this journey and I am eternally grateful for his love and support. Thanks also goes to Cooper for sleeping through the night from a very young age.

Abstract

The success of complex autonomous robotic systems depends on the quality and correctness of their fault tolerant control systems. A goal-based approach to fault tolerant control, which is modeled after a control architecture developed at the Jet Propulsion Laboratory, uses networks of goals to control autonomous systems. The complex conditional branching of the control program makes safety verification necessary. Three novel verification methods are presented. In the first, goal networks are converted to linear hybrid automata via a bisimulation. The converted automata can then be verified against an unsafe set of conditions using an existing symbolic model checker such as PHAVer. Due to the complexity issues that result from this method, a design for verification software tool, the SBT Checker, was developed to create goal networks that have state-based transitions. Goal networks that have state-based transitions can be converted to hybrid automata whose locations' invariants contain all information necessary to determine the transitions between the locations. An original verification software called InVeriant can then be used to find unsafe locations of linear hybrid systems based on the locations' invariants and rate conditions, which are compared to the unsafe set of conditions. The reachability of the unsafe locations depends only on the reachability of the states of the state variables constrained in the locations' invariants from those state variables' initial conditions. In cases where this reachability condition is not trivially true, the software efficiently searches for a path to the unsafe locations using properties of the system. The third verification method is the calculation of the failure probability of the verified hybrid control system due to state estimation uncertainty, which is extremely important in autonomous systems that rely heavily on the state estimates made from sensor measurements. Finally, two significant example goal network control programs, one for a complex rover and another for a proposed aerobot mission to Titan, a moon of Saturn, are verified using the three techniques presented.

Table of Contents

Nomenclature

β	Contribution set
χ	Uncertain state variable
Γ	Passive state space
$\mathcal{D}$	Set of passive state variables
$\mathcal{G}$	Set of goals in a goal network
$\mathcal{L}_{r,k}$	Set of executable branches of goals in $\mathcal{S}_{r,k}$
$\mathcal{S}_{r,k}$	Set of descendants of root goal $g_r^{0,0}$ in group $\mathcal{G}_k$
$\mathcal{U}$	Set of uncertain state variables
ν	Nominal path
Ω_k	Set of unsafe complete system states in group V_k
ϕ	Flow of an executable set of goals
Π	Set of failure paths
ψ_i	Flow equations for location v_i
ρ	Transition between executable sets of goals
Σ	Set of transition conditions in a hybrid system
τ	Transition condition in a hybrid system
Θ_k	Set of executable sets of goals in group $\mathcal{G}_k$
Υ'_k	Set of all consistent executable branch combinations

Ξ_k	Set of nominal complete system states in group V_k
ζ	Unsafe condition; set of unsafe constraints
A	Set of resets in a hybrid system
a_k	Initial failure probability of group V_k
B_k	Set of all contribution values in group V_k
c_k	Completion time for group V_k
E	Set of edges in a hybrid system
F_k	Set of Safing complete system states in group V_k
$g_n^{i_n,j_n}$	Goal
Q_k	Nominal transition probability matrix for group V_k
R_k	Set of root goals in group $\mathcal{G}_k$
S	Set of complete system states
T	Time point
t	Execution time
V	Set of locations in a hybrid system
W_k	Vector of initial nominal probabilities for group V_k
W_s	Failure probability
$W_{u,k}$	Failure transition probability vector for group V_k
X	Set of controlled state variables
Z	Unsafe set
k	Group number
n	Goal index

i_n Parent goal index

j_n Tactic number