Hybrid System Modeling of Tandem Dynamically-Positioned Vessels

James P. Millan
Institute for Marine Dynamics
National Research Council
St.John's, Newfoundland
Canada A1B 3T5
jim.millan@nrc.ca

Siu D. O'Young
Faculty of Engineering and Applied Science
Memorial University of Newfoundland
St.John's, Newfoundland
Canada A1B 3X5
oyoung@engr.mun.ca

Abstract

A Hybrid System model is used to aid the design and verification of a coordinated control system for two Dynamically Positioned marine vessels. A simple supervisory controller for the Emergency Shutdown and Disconnect operation is developed and verified using the automatic validation software HyTech.

1 Introduction

In recent years, efforts to develop offshore oil and gas resources have lead to the utilization of large Floating Production Storage and Offloading vessels (FPSO), typically displacing 200,000 tonnes, which are moored in various ways to the seafloor. The FPSO is often assisted by a closed-loop control system known as a Dynamic Positioning system (DP) which actively uses the vessel's thrusters to help maintain position and heading of the vessel in response to environmental loading from wind, waves, and current. The FPSO must be serviced by another large vessel, a shuttle tanker, which services the FPSO by offloading the crude oil and transporting it to shore for refining. During the offloading activity, it is required that the FPSO and the shuttle tanker come into close proximity and connect an oil transfer hose. There is no load-bearing connection between the two vessels and the DP systems are used to keep both vessels on station and at the specified heading angle. Failure to maintain position or heading by either vessel may lead to a collision, so an Emergency Shutdown and Disconnect (ESD) system is in place to stop pumping, drain the oil in the line, and disconnect the hose without breaking it.

In general, there has been an increased level of automation in order to reduce manning requirements on these vessels and to improve the efficiency. In spite of these measures, many vessels are not yet automated to this extent and vessel operators still experience incidents involving vessel drive-off, drift-off, and unstable behavior. Many of these undesirable incidents have generally been attributed to operator error[1], and to poor system integration. Existing analysis tools, Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA), both of which belong entirely in the discrete domain, are currently the tool of choice of the system designer. Hybrid systems theory appears to provide a alternative framework for modeling the tandem DP vessel system more effectively. We choose a supervisory controller structure to manage both vessels' DP systems as well as the ESD system.

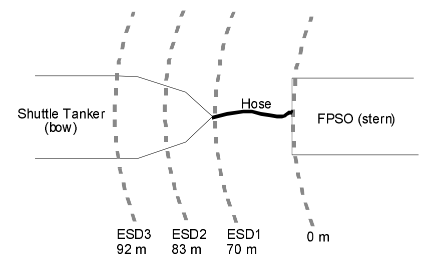

Figure 1: Emergency Shutdown and Disconnect scenario showing the various levels of ESD alarms.

2 Hybrid Model of DP Vessels

We need to obtain a usable hybrid automaton model based on the continuous linear vessel dynamics. Reachability analysis in hybrid systems has been shown to be decidable only for certain restrictive classes of hybrid automata, primarily the so-called *linear-hybrid automata*.[2] Under this definition, the vessel dynamics, normally described by derivatives of the continuous variables, are restricted to being constant functions of time. This is not an unreasonable simplification, since the dynamics of the vessel can subsumed by the apparent linearization provided by the underlying DP system.

The ESD system alarms are illustrated in figure 1. In the event of a power or thruster failure, the tanker will drift back (to the left) with the net environmental load, since the vessels are aligned to minimize loading by pointing the bows into the prevailing conditions. The drift occurs assuming that a large enough failure has reduced the vessel's capability to the point that it is unable to keep station. As the shuttle drifts slowly back, the supervisory controller can take immediate action to correct the increasing distance between both vessels by commanding the FPSO to move back as well. The FPSO will have a limited capability to move back, due to the constraints of the mooring, and its own limited power budget, bringing it to a stop at the maximum extent allowed by the mooring. In the meantime, the supervisor can attempt to restart the failed generator(s) on board the tanker . If this is not feasible, the supervisor can initiate ESD events to the ESD system, to allow for an orderly disconnect process that does not cause system damage. All communications with the supervisory controller were modeled with an uncertain latency of 1 to 2 seconds, as if the controller were operating from a remote location which was subject to communication delays.

A system of hybrid automata were developed to model this scenario; for more detail, see [3]. The software package HyTech, an automated verification tool designed specifically to handle linear hybrid automata, was used to verify safe operation of the ESD supervisory controller. Alternatively, various conditions for safe disconnection of the offloading hose were also parameterized. The tanker and FPSO automata represent the velocity as constants, over a range of possible values. For example, the drifting of the tanker is represented by the rate expression $\frac{dx}{dt} \in [75, 100]$, indicating the velocity of the vessel occupies a possible range of speeds of anywhere from 75 to 100 cm/s.

In conclusion, the result of this simple example was to produce a problem that is not trivially solvable, since we have combined a number of automata. The resulting parameterization of the hose disconnect time model yielded a value which is conservative due to the conservative modeling of the drift velocity.

3 Contributions and Future Work

Our contributions are threefold: firstly, this is one of the first applications of hybrid systems theory to the control of surface marine vessels, in particular those with closed loop DP control systems. Secondly, we have presented a formal verification of a supervisory controller for the Emergency Shutdown and Disconnect of a tandem offloading operation. Lastly, this work has presented enough details to serve as a benchmark for other researchers in the area of marine control systems who may wish to apply hybrid systems theory to their particular problems.

The continuous dynamics of our hybrid model have been abstracted as integrators with uncertain rates. The next step is to enhance the fidelity of the modeling of the continuous dynamics through the use of "nonlinear" automata to capture the more general linear time-invariant (LTI) dynamics, e.g. state-space systems. Even though the verification of the behaviour of a general nonlinear automaton is not tractable, there are special cases where one can quantize both time and the signal space, and build a finite-state approximation of an LTI system using a truncated history of the discrete-time quantized-input/output sequences[4]. It is also desirable to be able to model nondeterministic transitions to reflect unmodeled dynamics of the environment, e.g. one could have "black-out" or "brown-out" of the power system at any instant of time and from almost any location within the hybrid automation. In terms of design, it is desirable to be able to perform formal controller synthesis instead of just the verification of the controlled behaviour for a given and fixed controller, i.e. for a given specification, synthesize a least restrictive controller such that the controlled process behaves within the specification. Formal control synthesis can often be posed as a fixed-point problem where unsafe plant dynamics are trimmed by repeated formal verification runs until no more unsafe dynamics can be found. Finally, it would also be useful to have a simulation of the hybrid system such that a trajectory of the events which leads to an unsafe location can be demonstrated. This is useful in the design stage to identify deficiencies in the plant dynamics and instrumentation, and in the operation stage as an operator-aid to warn the operator of imminent dangers due to unsafe procedures.

References

[1] D. Phillips, “Dynamic positioning of ships:the problems solved?,” in *UKACC International Conference on Control*, pp. 1214–1219, IEE, September 1996.

[2] T. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya, “What's decidable about hybrid automata?,” *Journal of Computer and System Sciences*, 1998.

[3] J. Millan and S. O'Young, “Tandem dynamically positioned vessels: A hybrid system model,” Tech. Rep. LM-2000-16, Institute for Marine Dynamics, September, 2000.

[4] J. Raisch and S. O'Young, “Discrete approximation and supervisory control of continuous systems,” *IEEE Transactions on Automatic Control*, vol. 43, pp. 569–573, April 1998.

[5] D. Bray, *Dynamic Positioning*, vol. 9 of *Oilfield Seamanship*. Oilfield Publications Inc., 1998.