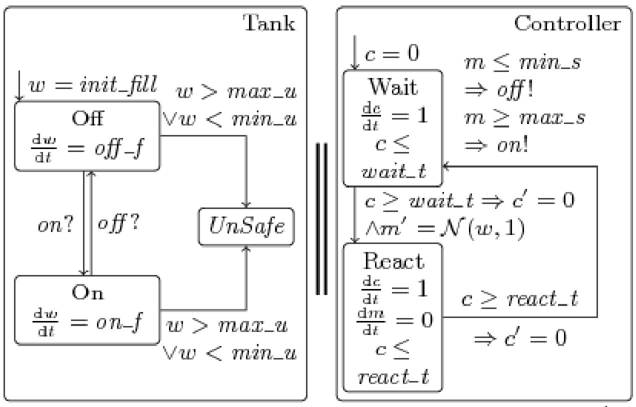
Water Level Control (HSCC 2011)

AVACS H4
Phase 2

July 28, 2011

1 Description of the Model

We consider a model of a water level control system extended from the one of Alur et al. [1] and our previous paper [4]. In particular, we use this case study to demonstrate the influence which different abstractions of the same continuous stochastic command have. The abstraction of a guarded command with a continuous probability distribution into one with a discrete probability distribution is described in a recent publication [2]. A water tank is filled by a constant stream of water and is connected to a pump which is used to avoid overflow of the tank. A control system operates the pump in order to keep the water level within predefined bounds. The controller is connected to a sensor measuring the level of water in the tank. A sketch of the model is given in Figure 1. The state "Tank" models the tank and the pump, and w is the water level. Initially, the



$init\_fill = 6.5\mathrm{l}$, $wait\_t = 1\mathrm{s}$, $react\_t = 0.1\mathrm{s}$, $off\_f = 1\frac{\mathrm{l}}{\mathrm{s}}$, $on\_f = -2\frac{\mathrm{l}}{\mathrm{s}}$, $max\_s = 8\mathrm{l}$, $min\_s = 5\mathrm{l}$, $max\_u = 12\mathrm{l}$, $min\_u = 1\mathrm{l}$

Figure 1: Sketch of the Water Level Control Model

tank contains a given amount of water. Whenever the pump is turned off in state "Off", the tank fills with a constant rate due to the inflow. Conversely, more water is pumped out than flows in when the pump is on.

Time bound	Abstraction A			Abstraction B		
	Prob.	Build (s)	States	Prob.	Build (s)	States
20s	0.1987	3	999	0.0982	3	1306
30s	0.2830	6	2232	0.1433	8	2935
40s	0.3580	16	3951	0.1860	18	5212
50s	0.4250	34	6156	0.2264	42	8137
60s	0.4848	67	8847	0.2647	86	11710

Time bound	Abstraction C			Abstraction D		
	Prob.	Build (s)	States	Prob.	Build (s)	States
20s	0.1359	3	1306	0.0465	5	1920
30s	0.1870	8	2935	0.0693	15	4341
40s	0.2547	18	5212	0.0916	47	7734
50s	0.3024	43	8137	0.1134	108	12099
60s	0.3577	85	11710	0.1347	219	17436

Table 1: Water level control results. We round probabilities to four decimal places. Abstractions used are $A = w + \{[-2, 2], (-\infty, 1.9] \cup [1, 9, \infty)\}$,
$B = w + \{[-2, 2], (-\infty, 1.9], [1.9, \infty)\}$,
$C = w + \{[-2.7, 2.7], (-\infty, 1.2), [1.2, \infty)\}$,
$D = w + \{-1.5, 1.5], [-1.5, -2], [1.5, 2], (-\infty, 1.9), [1.9, \infty)\}$

The controller is modelled by automaton "Controller". In state"Wait", the controller waits for a certain amount of time. Upon the transition to "React", the controller measures the water level. To model the uncertainties in measurement, we set the variable m to a normal distribution with expected value w (the actual water level) and standard deviation 1. According to the measurement obtained, the controller switches the pump off or on.

We are interested in the probability that within a given time bound, the water level leaves the legal interval.

2 Results

In Table 1, we give upper bounds for this probability for different time bounds computed by *ProHVer* [1] as well as the number of states in the abstraction computed by *PHAVer* [3] and the time needed for the analysis. Notice, that the resulting probabilities may be different than the ones in the paper for this model. The reason is that we manually

[1] `http://depend.cs.uni-sb.de/tools/prohver`

inserted the precise values in the *.graph* files generated by the modified version of *PHAVer* which serve as input for *ProHVer*. For the stochastic guarded command simulating the measurement, we consider different abstractions by probabilistic guarded commands of different precision, for which we give the abstraction functions in the table caption. When we refine the abstraction A to a more precise B, the probability bound decreases. If we introduce additional non-determinism as in abstraction C, probabilities increase again. If we refine B again into D, we obtain even lower probability bounds. The price to be paid for increasing precision, however, is in the number of abstract states computed by *PHAVer* as well as a corresponding increase in the time needed to compute the abstraction.

Manual analysis shows that in this case study, the over-approximation of the probabilities only results from the abstraction of the stochastic guarded command into a probabilistic guarded command and is not increased further by the state-space abstraction.

References

[1] Rajeev Alur, Costas Courcoubetis, Nicolas Halbwachs, Thomas A. Henzinger, Pei-Hsin Ho, Xavier Nicollin, Alfredo Olivero, Joseph Sifakis, and Sergio Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138:3–34, 1995.

[2] Martin Fränzle, Ernst Moritz Hahn, Holger Hermanns, Nicolás Wolovick, and Lijun Zhang. Measurability and safety verification for stochastic hybrid systems. In *HSCC*, pages 43–52, New York, NY, USA, 2011. ACM Press.

[3] Goran Frehse. PHAVer: Algorithmic Verification of Hybrid Systems Past HyTech. pages 258–273. Springer, 2005.

[4] Lijun Zhang, Zhikun She, Stefan Ratschan, Holger Hermanns, and Ernst Moritz Hahn. Safety verification for probabilistic hybrid systems. In *CAV*, volume 6174 of *LNCS*, pages 196–211. Springer, 2010.