8th International IFAC Symposium on
Dynamics and Control of Process Systems
Preprints Vol.1, June 6-8, 2007, Cancún, Mexico

OPTIMIZATION-BASED SAFETY ANALYSIS OF AN INDUSTRIAL-SCALE EVAPORATION SYSTEM WITH HYBRID DYNAMICS

Anna Völker, Christian Sonntag, Sven Lohmann, [1]
Sebastian Engell

Process Control Laboratory (BCI-AST), Department of Biochemical and Chemical Engineering, University of Dortmund, 44221 Dortmund, Germany

Abstract: While current approaches for the safety verification of hybrid systems yield rigorous proofs for system safety, their applicability is restricted to relatively small systems. In this paper, the safety properties of a large-scale industrial processing system with hybrid dynamics are investigated using two optimization-based approaches. While the first approach regards the hybrid system as a black box (i.e. only considers the input-output behavior) and attempts to determine worst-case scenarios by embedded hybrid simulation, the second approach additionally takes the internal structure of the system into account and employs theorem proving techniques to rigorously show certain properties of the system.

Keywords: Hybrid systems, Safety analysis, Validation, Optimization, Simulation, Verification

1. INTRODUCTION

Since discrete controllers are often employed in processing systems to realize sequential procedures or to ensure process safety, and due to the presence of discrete phenomena in the (usually nonlinear) continuous dynamics, such systems are suitably modeled as hybrid systems, i.e. systems with mixed discrete-continuous dynamics. Many aspects of hybrid systems have been studied extensively in academia, one of which is the task to verify that a hybrid system cannot evolve into some unsafe region in the state space. To solve this safety verification task, which is often challenging due to the usually complex behavior of hybrid systems, several approaches have been developed in recent years, most of which are based on abstraction or modularization of the original hybrid model in combination with the exact or approximate computation of reachable sets in the state space, see e.g. Clarke et al. (2003); Stursberg et al. (2004); Tomlin et al. (2003). If the continuous dynamics are modeled by systems of differential-algebraic equations (DAEs), the verification task becomes even more involved (Dang et al., 2004; Prajna and Jadbabaie, 2004).

Most of the existing verification approaches are only applicable to hybrid systems with low-dimensional continuous dynamics which is mainly due to the large computational burden imposed by the determination and representation of reachable sets. Since the nonlinear continuous dynamics of the controlled industrial-scale evaporation process considered in this work can only be modeled accurately using high-dimensional systems of DAEs, existing verification techniques are not applicable. Hence, this paper proposes an alternative approach to analyze safety properties of the evap-

[1] Corresponding author: s.lohmann@bci.uni-dortmund.de.
The authors gratefully acknowledge the financial support by the EU-funded NoE HYCON and the GRADUATE SCHOOL OF PRODUCTION ENGINEERING AND LOGISTICS at the University of Dortmund. Furthermore, we would like to thank Olaf Stursberg, Technical University of Munich, for helpful comments.

oration process which is based on exploration of the state space by simulation of a hybrid process model. In contrast to other simulation- or sampling-based approaches (see e.g. Branicky et al. (2005)), nonlinear optimization techniques are employed to guide the simulations towards worst-case scenarios and, thus, to minimize the computational effort while maximizing the probability of finding unsafe system evolutions.

After the controlled evaporation process has been introduced in Sec. 2, an analysis approach based on black-box optimization is presented in Sec. 3 in which only the input-output behavior of the hybrid model is considered. Although this approach proves effective in determining worst-case scenarios, it does not provide a detailed understanding of the process behavior, and it does not provide rigorous proofs for system safety. Thus, in Sec. 4, another approach is detailed that explicitly considers the internal structure of the hybrid model and employs a combination of theorem proving and nonlinear optimization with embedded simulation. Finally, Sec. 5 concludes the paper.

2. THE CONTROLLED EVAPORATION SYSTEM

2.1 Process Description

Evaporation processes are widely used in the processing industries to concentrate liquids in the form of solutions, suspensions, or emulsions. Fig. 1 shows a simplified flowsheet of such a process that represents a subpart of a multi-stage evaporation system operated at a large chemical company. Its main components are an evaporating vessel (A) and a heat exchanger (B). A liquid cold feed consisting of a nonvolatile product and the volatile solvents water and alcohol enters the evaporation vessel through the valve assembly V_{S3} and is heated by supplying hot steam to the heat exchanger through the valve assembly V_{VS2}. The heat transfer leads to an evaporation of the volatile components water and alcohol, and the vapor is drained through the pipe P_V. The liquid is drained through the valve assembly V_{S4} if the product concentration in the liquid phase w_A meets given purity requirements.

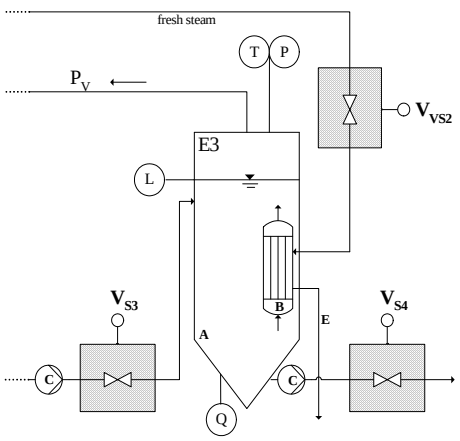

Fig. 1. Simplified flowsheet of the evaporation system.

2.2 The Logic Controller

The valve assemblies can only be switched discretely between two states (open/closed) by a logic controller that was designed to keep the critical process variables (i.e. the liquid level [2] L, the temperature T, and the pressure P within the evaporation vessel) within safe bounds in the face of equipment malfunctions. The controller receives discrete events from the plant if (1) the level, temperature, or pressure cross the upper warning thresholds $L_{w,u} := 90\ \%$, $T_w := 430\ K$, and $P_w := 4.6\ bar$ from below, (2) if the level crosses the lower warning threshold $L_{w,l} := 20\ \%$ from above, and (3) if all measurements have reentered a subset of the state space designated as the nominal operating region ($L \in [30\ \%, 80\ \%]$, $T < 425\ K$, $P < 4.4\ bar$). The response of the discrete controller to the plant events is given in Tab. 1.

Table 1. Strategy of the logic controller.

Controller state	$\mathbf{V_{S3}}$	$\mathbf{V_{S4}}$	$\mathbf{V_{VS2}}$
Nominal operating region	open	open	open
$L \leq L_{w,l}$	open	close	close
$L \geq L_{w,u}$	close	open	open
$T \geq T_w \wedge P \geq P_w$	open	open	close
$T \geq T_w \wedge P \geq P_w \wedge L \geq L_{w,u}$	close	open	close

2.3 The Task of Safety Analysis

Initially, the evaporation system is close to steady-state operation, and all process variables lie within a subset of the nominal operating region, henceforth called the initial set. Now it is assumed that within the time interval [10, 300] seconds after the simulation has started, two errors of the following types occur: the valve assemblies are blocked (i.e. the controller cannot influence the valve setting), or the pipe P_V (and, thus, the vapor outflow) is obstructed. Tab. 2 gives an overview over all errors that can occur. It is assumed that the error is removed after at most 130s when the valve assembly has switched to a redundant line and the pipe is cleared again.

The safety analysis task is to verify that the logic controller always keeps the system within safe bounds for at least 1000 seconds [3], where the safe region is defined by critical thresholds on the process measurements. The upper critical thresholds are given by $L_{c,u} := 100\ \%$, $T_c := 440\ K$, and $P_c := 5\ bar$, and a lower critical threshold for the liquid level is defined as $L_{c,l} := 0\ \%$.

2.4 The Hybrid Process Model

In previous work, the controlled evaporation system described above was implemented as a set of communicating automata [4]. In this framework, the plant is

[2] The liquid level is here defined in %, where 0 % is the minimum, and 100% is the maximum allowed value.

[3] This value was derived under the assumption that the process is at steady-state again after at most 1000 seconds

[4] For a more detailed description of the model, see Sonntag and Stursberg (2005).

Table 2. List of possible errors.

No.	Symbol	Explanation
1	$P_{V,c}$	P_V is obstructed
2	$V_{S3,o}$	V_{S3} is blocked in open position
3	$V_{S3,c}$	V_{S3} is blocked in closed position
4	$V_{S4,o}$	V_{S4} is blocked in open position
5	$V_{S4,c}$	V_{S4} is blocked in closed position
6	$V_{VS2,o}$	V_{VS2} is blocked in open position
7	$V_{VS2,c}$	V_{VS2} is blocked in closed position

implemented as a hybrid automaton [5], the controller, the valve assemblies, and the pipe are modeled as finite-state automata, and a set of timed automata represents the occurrence and the correction of errors. The continuous dynamics of the plant are modeled using two discrete locations with distinct systems of DAEs (each with 4 differential and 13 algebraic states) that are chosen depending on the state of the liquid in the evaporation vessel (*non-evaporating* or *evaporating*).

3. SAFETY ANALYSIS USING BLACK-BOX OPTIMIZATION

In this section, a black-box approach to the safety analysis of the evaporation system is presented that employs continuous nonlinear optimization with embedded simulation of the hybrid process model. The optimizer only considers the input-output behavior of the system to drive it towards worst-case scenarios. The continuous decision variables of the optimization problem are assembled in a vector according to

$$x = [w_{A,0}, w_{B,0}, L_0, T_0, t_{e1}, t_{e2}]^T. \quad (1)$$

Here, $w_{A,0}$ ($\frac{kg}{kg}$), $w_{B,0}$ ($\frac{kg}{kg}$), L_0 (%), and T_0 (K) represent the concentrations of product and water in the liquid phase, the liquid level, and the temperature in the evaporation vessel that are used as initial values for the embedded hybrid simulation [6] (see Sec. 2.3), and t_{e1} and t_{e2} are the time instances in seconds at which the errors e_1 and e_2 occur in the system.

The optimization task is complicated by the presence of discrete decision variables (the types of the errors e_1 and e_2, see Tab. 2) that actually lead to a mixed-integer optimization problem. However, under the reasonable assumption that a valve assembly or the pipe can only malfunction once within the simulation duration of 1000 seconds, only 18 combinations of two errors (e_1, e_2) can occur. Thus, the discrete decision variables can be removed from the problem by performing separate continuous optimizations for every possible error combination according to:

$$\min_x \Omega(x), \quad (2)$$

subject to the dynamics of the controlled evaporation system and the linear inequality constraints

$$x \leq [0.84, 0.2, 85, 420, 300, 300]^T, \quad (3)$$

$$x \geq [0.8, 0.16, 75, 410, 10, 10]^T, \quad (4)$$

$$[1, 1, 0, 0, 0, 0] \cdot x \leq 1, \quad (5)$$

where x is defined according to Eq. 1. Here, the constraints in Eqs. 3 and 4 restrict the initial values of the state variables to the initial region described in Sec. 2.3 and the time instances at which errors may occur to the range $[10, 300]$. The concentrations of the components in the liquid phase are defined in a relative fashion, and the relation $w_A + w_B + w_C = 1$ must always hold. The constraint in Eq. 5 reflects this relation.

The cost function Ω is chosen such that the simulated trajectories for temperature, pressure, and level tend to a critical state. Since it was not possible to determine a single objective function Ω that represents the goal of maximizing/minimizing L, T, and P at the same time (due to the strong and highly complex relations between L, T, and P), the problem is simplified by performing several optimizations of the problem defined in Eq. 2 for each critical threshold separately. For the case of maximizing the temperature $\Omega(x) = -max_S T$, where the operator $max_S T$ represents the maximum value of T over a simulated trajectory (see Fig. 2). This approach leads to 4 optimization problems which have to be solved, each for 18 possible error combinations, leading to $4 \cdot 18 = 72$ optimization problems.

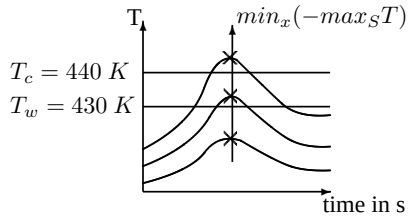

Fig. 2. Concept of the objective function for T.

The main results of the safety analysis using the black-box approach can be summarized as follows [7]:

(1) The critical threshold for the pressure is reached when P_V is obstructed and V_{VS2} is blocked in the open position.
Fig. 3 depicts the trajectory of the pressure that was obtained for this error scenario with $t_{e1} = t_{e2} = 10\ s$. e_1 causes the system to reach P_w, and e_2 blocks the controller action, thus leading to a critical situation.

(2) The warning threshold $T_w = 430\ K$ is not reached.

(3) The warning thresholds $P_w = 4.6\ bar$, $L_{w,u} = 90\ \%$, and $L_{w,l} = 20\ \%$ are only reached when

[5] A formal definition of the modeling framework can be found in Sonntag et al. (2006).

[6] Given initial values for these four state variables, unique initial values of the remaining state variables of the plant model can be computed.

[7] All nonlinear optimization problems considered in this paper were solved on an AMD Opteron 2.39 GHz using the algorithms *ego*, *rbfSolve*, *glcDirect*, and *multiMin* that are part of the MATLAB-based optimization framework TOMLAB (Holmström et al., 2006).

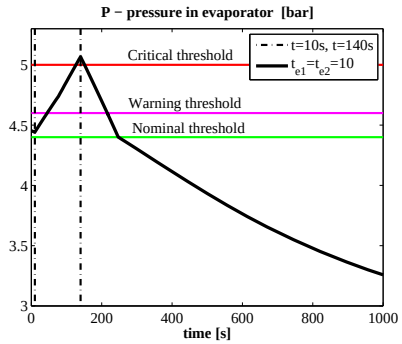

Fig. 3. Crossing of the critical threshold P_c.

the pipe P_V is obstructed.

The corresponding simulation result for the level is depicted in the upper figure of Fig. 4. It shows that $L_{w,l}$ is reached at $t = 820\ s$ after $L_{w,u}$ was reached at $t = 110\ s$. The monotonous decrease of L indicates that the system is not stabilized by the controller after reaching the nominal region. This is due to the fact that, by definition, the system is at nominal operation if **all** process measurements L, T, and P are within the nominal region. However, the lower figure, which depicts the evolution of the temperature, shows that the nominal operation region is not reached in the time range t=[170, 850]. Hence, the controller does not switch back to nominal operation. This behaviour is not safety critical but unnecessary large movements are undesired.

(4) The warning thresholds are only exceeded when the nominal controller response (Tab. 1) is prevented by an error.

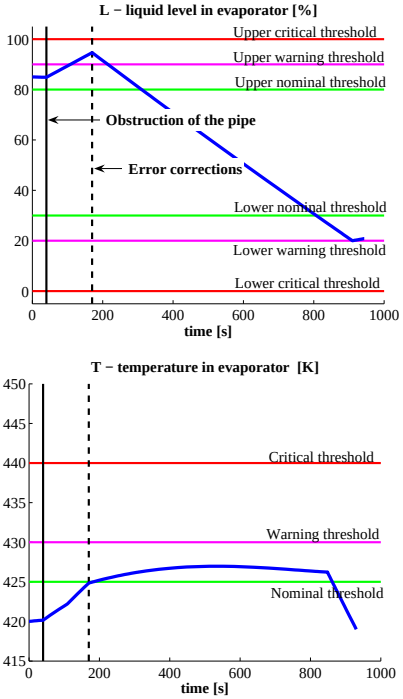

Fig. 4. Simulation result for an obstruction of P_V and the reaching of $L_{w,l}$.

4. OPTIMIZATION-BASED SAFETY ANALYSIS BASED ON PROCESS INSIGHT

Although the black-box approach described in the previous section could effectively determine worst-case scenarios, it does not provide a detailed understanding of the process dynamics. Furthermore, it does not allow for rigorous proofs of safety properties as is for example possible by theorem proving the equations describing the continuous dynamics. To gain deeper information based upon insight into the evaporation system, this section introduces a white-box approach to safety analysis that combines theorem-proving with optimization-based techniques. The term *white-box* here refers to a strategy in which knowledge of the internal structure (e.g. the dynamics) of a process is used to generate a series of investigations where the result of the previous investigation determines the current investigation. Since the continuous dynamics of the evaporation system differ depending on the state of the liquid in the vessel (*non-evaporating* or *evaporating*), different analysis schemes are applied for these two cases, but the general procedure is similar for both as depicted in Fig. 5 and Fig. 6. The main idea is to rule out error scenarios based on process insight which will definitely not drive the system into a critical state. The safety analysis is carried out either by theorem proving, or, if this is not possible, using an optimization technique with embedded simulation of the evaporation system [8].

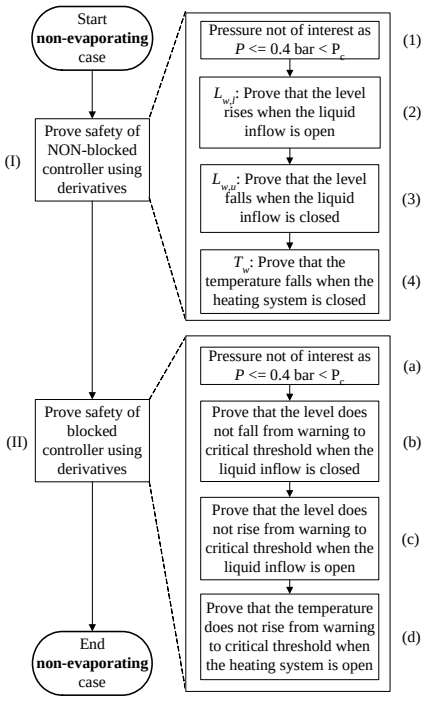

Fig. 5. Analysis scheme for the non-evaporating case.

For the non-evaporating case, the analysis scheme consists of two steps (see Fig. 5): In the first step (I),

[8] Due to space limitations, only a brief description of the analysis schemes can be given here. Furthermore, all analytically computed time derivatives of the system dynamics are omitted.

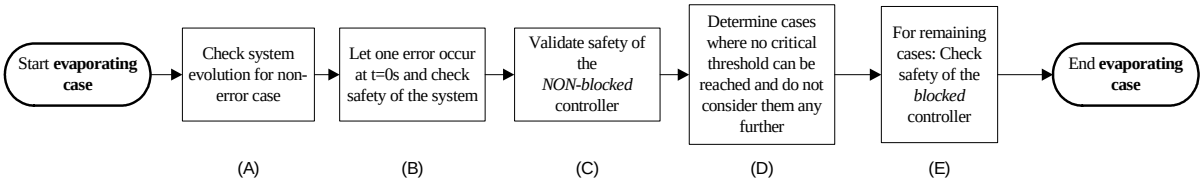

Fig. 6. Analysis scheme for the evaporating case.

the goal is to verify that the system always remains safe if the controller actions are not blocked by an error, and in the the second step (II), it is determined if the systems remains safe even if the controller actions are blocked by an error. The control strategy (Tab. 1) leads to four properties (see Tab. 3, Fig. 5.(1)-(4)) which ensure safety for the non-blocked case in step I if they are fulfilled for all possible evolutions of the system dynamics and all possible configurations of the valves. These properties are checked by theorem proving considering the time derivatives $\dot{T}$ and $\dot{L}$ which are computed analytically. This leads to the following results:

Table 3. Effects of the inputs to prove.

No.	Description
(1)	P always decreases when the heating system (V_{VS2}) is switched off.
(2)	L always rises if the liquid inflow (V_{S3}) is open, the liquid outflow (V_{S4}) is closed, and the heating system (V_{VS2}) is switched off.
(3)	L always decreases when the liquid inflow (V_{S3}) is closed and the liquid outflow (V_{S4}) is open.
(4)	T always decreases when the heat exchanger (V_{VS2}) is switched off.

(1) The pressure P is by definition always less than P_w in the non-evaporating case.
(2) $L = L_{w,l} \mapsto \dot{L} \geq 0$ for V_{S3}: The inflow is greater than the outflow, hence L is always increasing.
(3) $L = L_{w,u} \mapsto \dot{L} \leq 0$ for $\neg V_{S3}$: The inflow stops and the outflow continues, hence L is always decreasing.
(4) $T = T_w \mapsto \dot{T} \leq 0$ for $\neg V_{VS2}$: The temperature T is always decreasing.

For (3), with $F_{in} = 0$, follows

$$\dot{L} = \frac{(F_{in} - F_{out})\rho_{liq} - F_{in}(\rho_{liq,in} - \rho_{liq})m_{liq}}{\rho_{liq}^2 v_{L,3}} = \frac{-F_{out}}{\rho_{liq} v_{L,3}} \leq 0 \quad (6)$$

with F_{in}, F_{out} inflow, outflow rate of vapor into, from the heat exchanger ($\frac{kg}{s}$), ρ_{liq} ($\rho_{liq,in}$) density of (inflowing) liquid in the evaporator ($\frac{kg}{m^3}$), m_{liq} total mass of liquid phase in the evaporator (kg), $v_{L,3}$ relation between level and volume in the evaporator ($\frac{m^3}{\%}$).

Considering the case in which the controller response is blocked by an error (step (II) in Fig. 5), it must be shown based on the system of equations that the critical threshold is never reached within 130 seconds after the warning level was reached since, by that time, both errors have been corrected and no critical situation can be reached as shown in (1)-(4) above. The results of step II are:

(a) The pressure is by definition always less than P_w in the non-evaporating case.
(b) $130s \cdot \dot{L}_{min} \geq L_{c,l} - L_{w,l}$, with the fixed valve setting $\neg V_{S3}$, shown by theorem proving.
(c) $130s \cdot \dot{L}_{max} \leq L_{c,u} - L_{w,u}$, with the fixed valve setting V_{S3}, shown by optimization.
(d) $130s \cdot \dot{T}_{max} \leq T_c - T_w$, with the fixed valve setting V_{VS2}, shown by optimization.

Here, $\dot{L}_{min}$, $\dot{L}_{max}$, and $\dot{T}_{max}$ are the minimal and maximal changes of the corresponding variables with time. These were determined by analytic solution or, in the case of the properties (c) and (d), by numerical optimization of the time derivatives of the system equations. For (b), it follows that Eq. 6 becomes minimal if ρ_{liq} becomes minimal ($\dot{L}_{min} \approx -0.039\frac{\%}{s}$), leading to $-130 \cdot 0.039\% = -5.07\% > 0\% - 20\%$.

In summary, it was shown for the non-evaporating case that the unsafe region is never reached for all types of errors.

The analysis for the evaporating case is much more involved since the dynamic equations are too complex for a direct analytic investigation, e.g. for $\dot{T}$ no closed form could be derived. Therefore, conclusions on the safety of the system were drawn based on the results from optimization by embedded simulation or numerical computation of the derivatives of the process states. For the initial set described above, the process is always in the evaporating mode. In a first step, it is determined that no warning thresholds can be reached without the occurrence of an error (A). Next, it is checked whether a warning threshold is reached from the initial set with only one error occurrence (B). For the steps (A) and (B), the initial set was gridded, and brute-force simulation was applied (one reachable set is shown in Fig. 7). The results were validated by optimization. For (B), those errors can be ruled out which do not introduce a change to the system, e.g. blocking a valve in open position when all valves are initially open. Furthermore, it can be concluded that only the distance between t_{e1} and t_{e2} is significant if the initial set is enlarged such that it covers all states that are reachable without error (A), so $t_{e1} = 0\ s$ can be assumed.

If it can then be shown that the system remains within the safe region if the controller is not blocked (C),

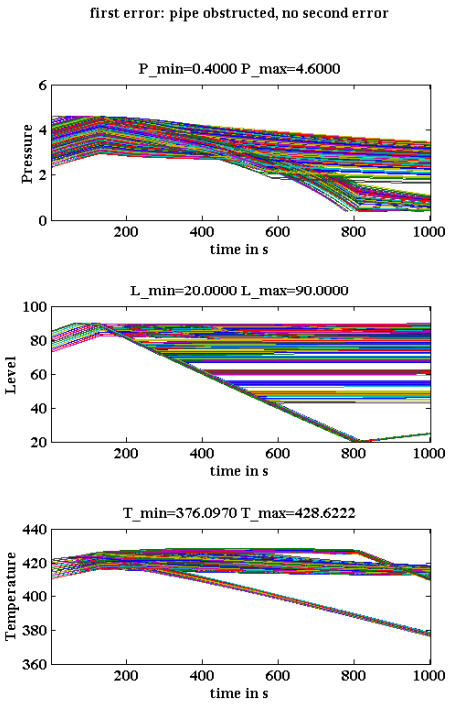

Fig. 7. Simulation result for enlarged initial set and pipe P_V obstructed (P, L, T).

all error combinations for which the first error does not drive the system into a warning threshold can be ruled out ((C) and (D)). For the remaining cases, the first error is chosen such that it causes the system to reach a warning threshold, and the second error is chosen to block the resulting controller action. By this approach, the number of error combinations that have to be investigated can be reduced to six. These cases are analyzed by optimization which includes t_{e2} as a decision variable (E):

1 $P_{V,c} \wedge V_{VS2,o}$ may lead to P_c,
2 $P_{V,c} \wedge V_{VS2,o}$ may lead to T_c,
3-4 $P_{V,c} \wedge V_{S3,o}$ and $P_{V,c} \wedge V_{S4,c}$ may lead to $L_{c,u}$,
5-6 $P_{V,c} \wedge V_{S3,c}$ and $P_{V,c} \wedge V_{S4,o}$ may lead to $L_{c,l}$,

Using the white-box approach, the results of the black-box approach could be fully confirmed. 164 optimization problems were evaluated. Since for the former approach, the internal structure of the plant was considered, several additional insights were gained , e.g. it might be possible that the pressure rises while the temperature falls depending on the concentration of the liquid in the evaporator.

5. CONCLUSIONS AND FUTURE WORK

In this paper, two approaches for the safety analysis of an industrial-scale evaporation system with hybrid dynamics were presented. While the first approach is based upon the input-output behavior of the system and employs a black-box optimization scheme with embedded hybrid simulation to determine worst-case scenarios, the second approach additionally employs knowledge about the system dynamics and uses theorem proving in combination with optimization-based methods. It was found that, although the formulation of the optimization problem for the first approach is relatively simple, the resulting problems are computationally expensive, and this approach does not provide a detailed understanding of the process dynamics. The application of the second approach is more involved, but it gives a deeper insight into the process dynamics and can be used to reveal and remedy shortcomings of the control scheme. For both approaches, global solvers have to be used where none of the applied solvers can guarantee optimality. Due to the large number of optimization problems, the parameters of the solvers were used with default settings. Hence, the optimization performance could be improved by individual parameter tuning experiments. Although the application of optimization-based approaches for the safety analysis of processing systems does not guarantee safety in a strict sense, it considerably reduces the computational effort and increases the confidence in the obtained results in comparison to purely simulation-based approaches.

REFERENCES

M. S. Branicky, M. M. Curtiss, J. Levine, and S. Morgan. Sampling-based planning, control, and verification of hybrid systems. In *16th IFAC World Congress*, 2005. Code: We-M12-TO/5.

E. Clarke, A. Fehnker, Z. Han, B.H. Krogh, O. Stursberg, and M. Theobald. Verification of hybrid systems based on counterexample-guided abstraction refinement. In *Tools and Algorithms for the Construction and Analysis of Systems*, volume 2619 of *LNCS*, pages 192–207. 2003.

T. Dang, A. Donze, and O. Maler. Verification of analog and mixed-signal circuits using hybrid systems techniques. In *Formal Methods for Computer Aided Design (FMCAD)*, volume 3312 of *LNCS*, pages 21–36. 2004.

K. Holmström, A. O. Göran, and M. M. Edvall. *User's Guide for TOMLAB*, 2006.

S. Prajna and A. Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *Hybrid Systems: Computation and Control*, volume 2993 of *LNCS*, pages 477–492. 2004.

C. Sonntag and O. Stursberg. Safety verification of a discretely controlled evaporation system. Technical report for the European Network of Excellence HyCon, Universität Dortmund, September 2005.

C. Sonntag, O. Stursberg, and S. Engell. Dynamic optimization of an industrial evaporator using graph search with embedded nonlinear programming. In *Proc. 2nd IFAC Conf. ADHS*, pages 211–216, 2006.

O. Stursberg, A. Fehnker, Z. Han, and B. H. Krogh. Verification of a cruise control system using counterexample-guided search. *Control Engineering Practice*, 12(10):1269–1278, 2004.

C. J. Tomlin, I. Mitchell, A. M. Bayen, and M. Oishi. Computational techniques for the verification of hybrid systems. *Proceedings of the IEEE*, 91(7): 986–1001, 2003.