Developing a Decision Support Tool for Dam Management with SPIN

María-del-Mar Gallardo[1], Pedro Merino[1], Laura Panizo[1] and Antonio Linares[2]
[1]Dept. Lenguajes y Ciencias de la Computación. University of Málaga.
{gallardo, pedro, laurapanizo}@lcc.uma.es
[2] BEFESA AGUA, SAU
Antonio.linares@befesa.abengoa.com

1. Motivation

- ❑ Traditionally, critical systems have been analysed with numerical simulations. However, most of them present a hybrid behavior with unexpected events that are not taken into account with numerical analysis.
- ❑ We propose the use of formal methods and verification techniques, such as model checking, to analyze critical hybrid systems. In recent years, different hybrid formalisms have appeared to analyse these systems.
- ❑ We apply our proposal to the development of a Decision Support Tool (DST) for dam management. We use the PROMELA formal language to model the dam, and SPIN to perform an analysis that returns information about the possible consequences of dam operator actions, which can help us to ensure both safety and efficient use of the water.

2. Modeling hybrid systems with PROMELA

- ❑ We have developed a hybrid model that includes:
  - Dam outflow elements, with hybrid behavior characterized by:
    - Continuous variables with time dependency: water level, water released, etc.
    - Discrete variables: opening degree of the outflow elements.
  - Environmental inflows.
  - User operation.
  - Requirements and constraints.
- ❑ Goals of modeling hybrid systems with PROMELA:
  - Development of a time/synchronization model to include time dependency of continuous behavior (Fig. 3).
  - Description of the continuous behavior -> PROMELA C code extension.
  - Integration of the discrete behavior model, implemented in PROMELA, and the continuous behavior model.

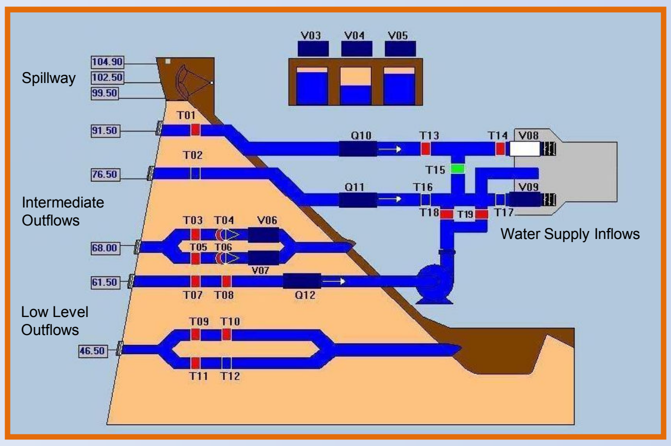

Fig. 1 Section of a real Dam

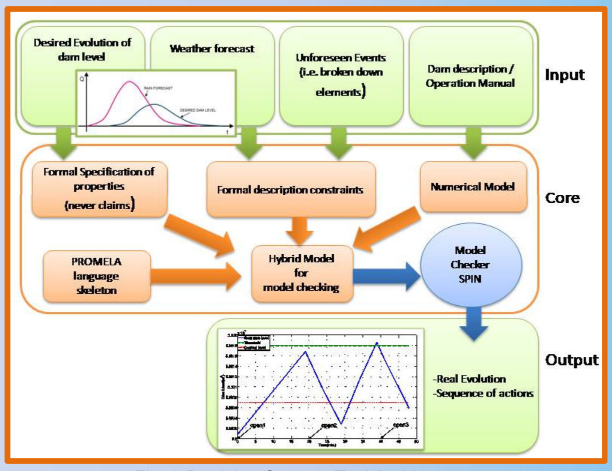
Desired Evolution of dam level
Weather forecast
Unforeseen Events (i.e. broken down elements)
Dam description / Operation Manual
Input
RAIN FORECAST
DESIRED DAM LEVEL
Q
t
Formal Specification of properties (never claims)
Formal description constraints
Numerical Model
Core
PROMELA language skeleton
Hybrid Model for model checking
Model Checker SPIN
Output
open1
open2
open3
-Real Evolution
-Sequence of actions

Fig. 2 Decision Support Tool Architecture

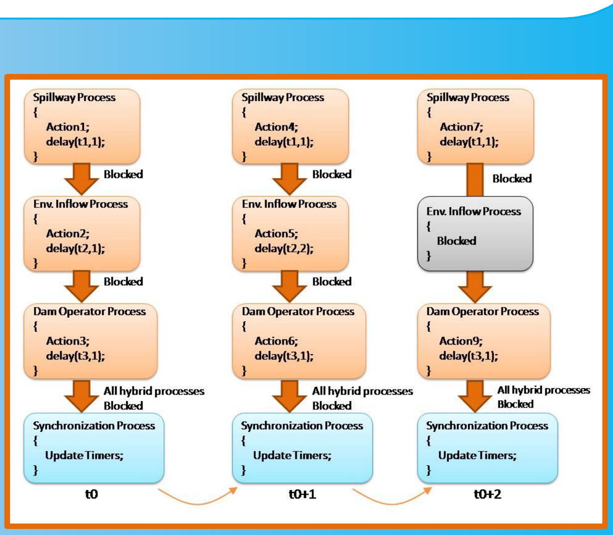

Fig. 3 Time Model

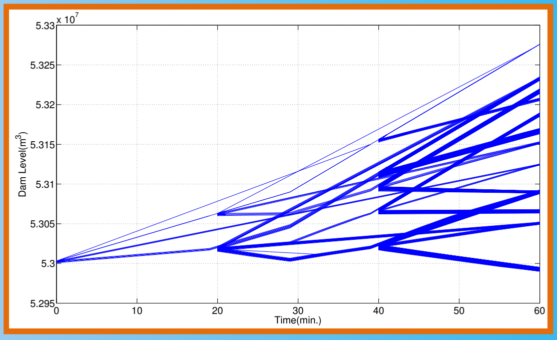

Fig. 4 Possible Execution traces

3. DST with SPIN

- ❑ DST functionality is based on the verification of the hybrid model with the SPIN model checker (Fig. 2).
- ❑ Constraints and user requirements are used to define properties. The resulting *never claim* automaton is included in the hybrid model.
- ❑ The analysis looks for a counter example that does not satisfy the property. However, the returned counterexample satisfies the requirements and the constraints.
- ❑ We have defined two types of timed properties:
  - During a period of time a condition is satisfied.
    - Property A: From time 40 to 60, the dam level in in the range (min, max). (Fig. 5)
  - The time elapsed between two conditions is in a range of values.
    - Property B: If the dam level goes up to threshold level, it decreases to the desired level in less than 10 time units. (Fig. 6)
- ❑ Different tests have been carried out, Table 1 shows the statistics:
  - Basic SPIN distribution (1 core).
  - SPIN multi-core extension (2 core).

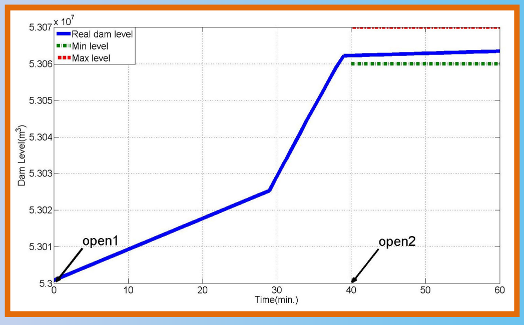

Fig. 5 Counterexample Property A

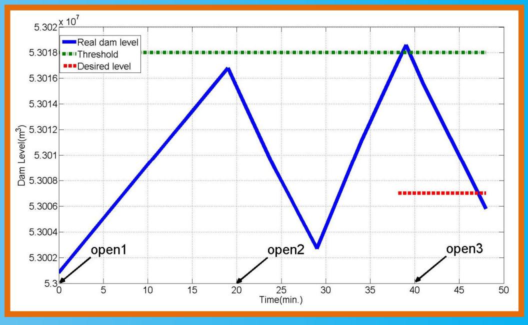

Fig. 6 Counterexample Property B

	Property A		Property B	
Number of Cores	1 Core	2 Core	1Core	2 Core
State Vector	148	148	156	156
Depth reached	2.837	2.299	2.839	1.139
States(stored)	1.117.263	524.113	8.968.761	112.986
States(matched)	1.025.582	592.117	9.686.355	136.935
Transitions	2.143.205	1.116.230	18.655.116	249.921
Atomic Steps	1.231.807	678.326	11.435.409	186.293
Total Memory MB	132,583	192,558	1174,497	145,512
Elapsed Time sec	4,89	3,75	53,4	1,06

Table 1 SPIN statistics

4. Conclusions

- ❑ The use of hybrid formal methods in dam management is producing very promising results.
- ❑ The adaptation of PROMELA to model and analyze hybrid systems is still a open issue, some aspects have to be improved such as time evolution.
- ❑ SPIN Multi-core modifies the analysis algorithm, this can lead to reductions in the time and the memory consumption to find the first counterexample. These improvements depend on the load balance.
- ❑ Future work will focus on a more complex dam model and the definition of new scenarios and timed property.

Partially supported by Befesa Agua and by grants
P07-TIC3131 (Andalusia) and TIN2008-05932 (Spain)

Acknowledgments:
Authors would like to thank Agustín Merchán, Spanish expert in dams, for his help.