A Dependable Automated People Mover System Modeled and Verified using Timed Automata: A Case Study

Guilherme Kunz, guilhermekunz@gmail.com
Western Paraná State University, Centro de Engenharias e Ciências Exatas, Foz do Iguaçu, Brazil

Eduardo Perondi, eduardo.perondi@ufrgs.br
Federal University of Rio Grande do Sul, Mechanical Engineering Department, Porto Alegre, Brazil

José Machado, jmachado@dem.uminho.pt
University of Minho, Mechanical Engineering Department, CT2M Research Centre, Guimarães, Portugal

Abstract. *Automated People Movers (APM) are systems for passenger transport with fully automated operation and high frequency service. For this study we have used the system named Aeromovel installed in Porto Alegre, Brazil. Aeromovel is a non-conventional Automatic People Mover whose operation principle is based on pneumatics. This paper proposes the use, in a complementary way, of two analysis techniques, simulation and formal verification, in order to guarantee the desired behavior for an APM propulsion system composed by a centrifugal fan and ten (on-off and proportional) pneumatic valves driven by pneumatic pistons. This approach is based on the use of timed automata and UPPAAL model-checker. The more focused aspect is the modeling of the propulsion system associated at the distributed control system. Some simulation and formal verification results are presented, considering desired behavior properties in order to improve the system's dependability.*

Keywords: *Modelling, Simulation, Automated People Movers.*

1. INTRODUCTION

An *Automated People Mover* (APM) is a fully automated, grade-separated mass transit system. The term is generally used only to describe systems serving relatively small areas such as airports, downtown districts or theme parks, but is sometimes applied to considerably more complex automated systems. Usually they circulate in headways that don't interfere with other traffic ways in order to guarantee safety for passengers and security for the system (IEEE, 2004).

From the existing APMs, one-quarter of them function as urban metros; the remainder are short-range, privately built shuttles and loops that operate as an integral part of the functioning of airports, amusement parks, institutions, and shopping centers across North America, Europe, and Japan. They all have in common a high level of frequent service. Some of these, or earlier generations of them, have been operating since the late 1960s (Neumann and Bondada, 1985; Inouye and Kurokawa, 1993; Sproule *et al.*, 1993; AFCET, 1996; Shen *et al.*, 1996; SDE, 1999).

An APM realizes automatically the control of movement, the execution of the safety instructions and the direction of the trains. The automatic realization of these functions is assured by the *Automated Train Controller* (ATC) system that is composed by the following sub-systems:

- ATP - *Automatic Train Protection*. Protection against collisions, excess of speed, invasion of the train way, among other danger situations;
- ATO - *Automatic Train Operation*. Speed control, programmed stops at the stations and control of the doors, among other operations of the same kind (usually, in a non-automated transportation system, these operations would be associated at the train operator).
- ATS - *Automatic Train Supervision*. Functions of monitoring and adjustment of the individual performance of each train, in order to guarantee the schedule of departures and arrivals of trains from and to existing stations.

An ATC must include, imperatively, the ATP system and, optionally, it can include the ATO and/or ATS systems. In order to guarantee the communication among these systems, the standard *IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements* (IEEE, 2004) must be followed. This standard describes the functional requirements and also the communications performance concerning the described controller systems of the APM (*Communications Based Train Control* - CBTC). The main characteristic of CTBC include:

- Information about the precise positioning of the train, not dependent of the sensors of the way.
- Continuous communication between the train and other processes that are not directly related with it.
- Verification of the train control conditions for the ATP (*Automatic Train Protection*). Functionalities of ATO (*Automatic Train Operation*) and ATS (*Automatic Train Operation*) can be also realized.

Safety aspects related with operation of these systems are crucial, so there are safety requirements that must be accomplished when these systems are operating. These safety requirements are defined by International Standards - as mentioned above - and cover all the aspects of the system controller.

In order to improve the robustness of controllers of automation systems some techniques can be used. In this case two analysis techniques are chosen in order to be used in a complementary way: Simulation (Baresi *et al.*, 1998) and Formal Verification (Moon, 1994).

Simulation allows experimenting automation systems behavior with a reduced and finite number of evolution scenarios. While the results thus obtained are valuable for the tested scenarios only, it becomes possible to quickly detect some errors in the specification of the controller. More important than the generation of numerous evolutions of the system (changing different logical inputs), it is preferable to obtain these evolutions from the evolution of a plant model. Following this methodology, the plant model has a direct influence (Baresi *et al.*, 1998) in the pertinence of the stimuli of the controller model and, clearly, in the pertinence of the results obtained with the simulation technique.

As the complexity of the systems being built increases, so does decrease the degree of confidence that can be achieved by simulation. In this context, it is commonly argued that formal mathematical notations should be used to support modeling and reasoning (Jones, 1980). Using them, a model of the intended design can be developed and reasoned about. This process of exploring the model with theorems representing properties to be verified is called formal specification verification (or validation). This is clearly different from formal program verification, the process of formally proving that a given system satisfies a specification, which was the traditional area of verification (Loeckx and Sieber, 1984; Jones, 2003). At this point it should also be clear that formal verification is different from simulation and testing. Formal verification establishes the validity of a property in a given specification in an absolute manner.

In this paper it is intended to use simulation and formal verification by model-checking (Remelhe *et al.*, 2004), in a complementary way (Machado *et al.*, 2011), in order to improve the dependability of the controllers of these systems. For this purpose, a specific case study is used: an APM that uses pneumatic power for displacement, in which the combination of a pneumatic propulsion system control and the control of a set of *on-off* and *proportional* valves is crucial to guarantee the system's dependability.

Several formalisms can be used to model timed systems. Timed automata were adopted as the modeling formalism for system modeling due to two main reasons: first, the study of the proposed system needs to take time into account; and, second, it is the input formalism of the UPPAAL model-checker (Behrmann *et al.*, 2004). Hence, it is well adapted to the formal verification of timed systems. Also the fact that UPPAAL software allows simulation of timed systems, the proposed study is facilitated.

In order to achieve the main goals of this paper the section 2 presents the case study; section 3 deals with the system modeling where the distributed controller system and the plant are modeled; section 4 is devoted to presentation of the simulation and formal verification results and finally, section 5, presents some conclusions about this study.

2. CASE STUDY: *AEROMOVEL*

The main features of the technology are the exclusive *Aeromovel* traffic on the route, the high ratio of useful load/weight carried and external traction. These characteristics are due, respectively, of the fact that car travel above ground in a unique way and have external power system. This makes it relatively lighter than other similar transportation systems, allowing less robustness for the beams where it operates, reducing the costs of construction, installation and maintenance of the system (Britto, 2008).

The *Aeromovel* uses rail technology in the interface between the vehicle and the ground. Thus, there is using less energy being the friction metal/metal below the rubber/concrete. The vehicle has four-wheel independent sets. The independence of the wheels allows the *Aeromovel* make curves with radii smaller than conventional trains, which have fixed wheels on the axes. The flaps are articulated, which allows the vehicle to make turns and moves uphill and downhill without clashing with the duct wall (Britto, 2008).

The power unit, known as power train group or propulsion system, is responsible for generating pressure differential and is basically composed of an asynchronous electric motor that drives the industrial centrifugal fan (Furtado, 1994). Each power train group is connected to the main duct through a pipeline with $1m^2$ of cross-sectional area.

The proposed fluidic power system (Fig. 1) consists of an industrial centrifugal fan (with air flow of up to $10^6 m^3/h$) and a set of two proportional valves (*VP0* and *VP1*) that allow control of pressure and consequently the force imposed on the vehicle and eight on-off valves (*V0-7*) They allow the effect of the fan switch on the main duct through which the vehicle moves, and can perform inflation or exhaust air as seen in Fig. 1.The valves used in the *Aeromovel* system are characterized by causing obstruction of flow from angular movement. Pneumatic pistons are used to rotate the flaps of the valve due to high flow rates involved.

According to (Aeromovel, 1999) the ideal complete system of transport can be segmented into sections between two stations, which are called "Standard-Block". The standard block is formed by two power train groups, one at each station and a vehicle. This configuration allows for three types of operation of the system:

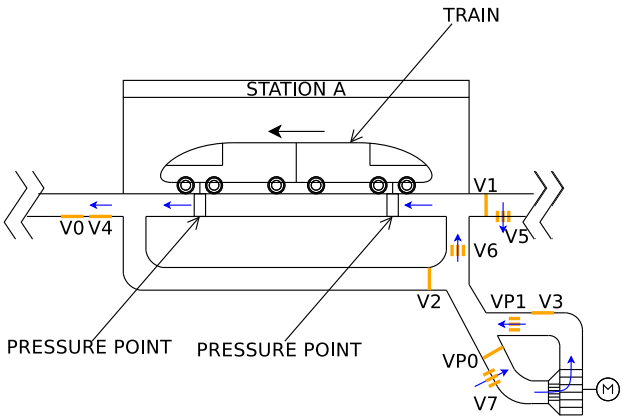

Figure 1. Layout of power train group - Push to Left

- *Push* - the vehicle is pushed by the pressure caused by the operation of the power train group upstream of the vehicle. In the chamber downstream of the vehicle, the atmospheric valve is open, communicating the product to the atmosphere (see Fig. 1 and Fig. 2).
- *Pull* - the vehicle is pulled by the *vacuum* caused by the operation of power train group downstream of the vehicle. In the chamber upstream of the vehicle, the atmospheric valve is open, communicating the product to the atmosphere (see Fig. 3 and Fig. 4).
- *Push-Pull* - both power train groups are connected to the duct and two atmospheric valves are closed. Thus, the vehicle moves in there due to the pressure upstream and downstream *vacuum*. In this form of operation the vehicle may develop higher speeds.

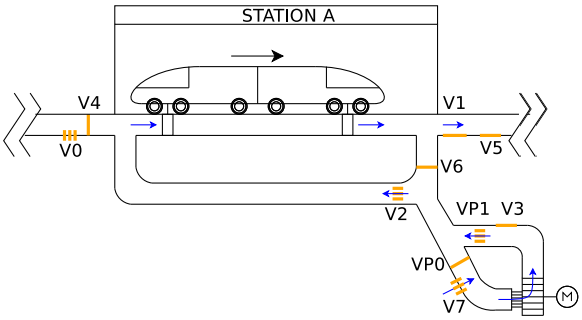

Figure 2. Layout of power train group - Push to Right

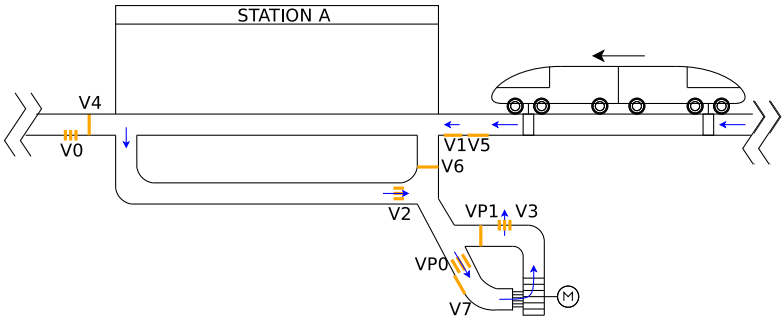

Figure 3. Layout of power train group - Pull from Right

One of the difficulties of working with this power train group is that the change of states (from push to pull for example) - because the valves can briefly set up a power train group in addition to the three states mentioned above - may cause safety problems for people and security problems for the equipment. To avoid making changes of states of the valves in sequence (which implies a longer time to change) is proposed, in this paper, the inclusion of a condition called *OFFLINE* where the power train group does not influence the movement of the vehicle, independently of the state of motor since the segments valves remain closed (*V1* and *V4*) while the atmospheric segment valves remain open (*V0* and *V5*). Thus,

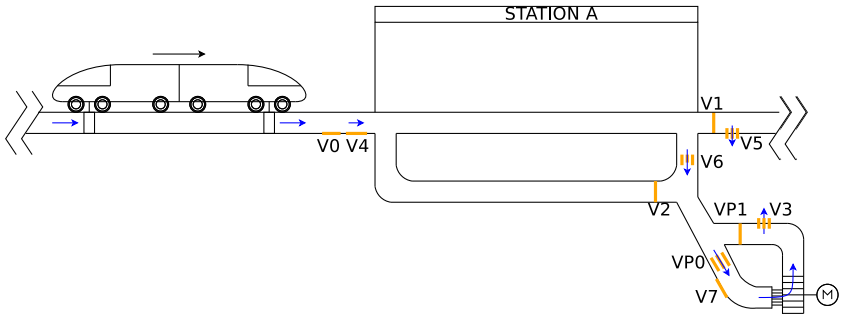

Figure 4. Layout of power train group - Pull from Left

the states independently of the other valves there is no interference in the movement of the vehicle, while the propulsion system remains in *OFFLINE* state. This state is used during the exchange process between the states *PUSH* and *PULL* or when the vehicle remains stationary at the station.

3. MODEL OF THE SYSTEM

In order to detail the explanation of the realized study, this paper presents only the study of one propulsion system with a single vehicle. Aiming the simplicity of the model of the complete system (vehicles and drivers), this work discusses the propulsion system or power train group (motor and set of pneumatic valves) in order to verify the possible states and prove that the proposed controller for the propulsion system is result in only three different states: *OFFLINE*, *PUSH* and *PULL*.

The train control system is usually centralized, but in aiming a solution based on the IEC 61850 standard (Hewings, 2008) the models were developed based on distributed controllers so in the models consider real time dedicated to each individual device. The units are connected to a communication bus that provides information exchange with other processing unit responsible for interfacing with the user, thus reducing the processing request individually. In general, the decision to use a distributed control system is motivated by cost reduction and increased system flexibility and control in this particular case the distance between the elements of the system.

Models of plant system devices and controllers were developed using a timed automata formalism and analyzed using the UPPAAL for both simulation and formal verification. The model was divided into the following templates:

- *Valvs_Control*. The on-off valves controller has a controller for each of the eight valves (see Fig. 5).
- *Valvs*. The on-off valves of propulsion system have four states considered (*closed*, *closing*, *open*, *opening*) modeled by the four locations of each corresponding automaton. The time for changing of state is fixed. The system is initialized with all the valves in known states. This template is repeated for each of the eight on-off valves (see Fig. 6).
- *Valvs_Prop_Control*. The proportional valves controller has a controller for each one of the two proportional valves (see Fig. 7).
- *Valvs_Prop*. Model of pneumatic proportional valves with two states (*moving* or *stationary*). The time of change is proportional to the displacement required. This template is repeated for each of the two proportional pneumatic valves (see Fig. 8).
- *GMP_Control*. The controller of propulsion system template is unique for the standard block (see Fig. 9) and it is responsible for receiving messages from other controllers in the system and send them to the other components of propulsion system. This model is essential to simplify since verifying the total of states that allowed this model to the propulsion system is the only one that remains in the analysis of the complete system (including vehicles and other ATC systems) modeling the time required between changes of the states *PUSH*, *PULL* and *OFFLINE* obtained in this work.
- *Motor*. The motor physical system model with 3 states (see Fig. 10). The time for changing of state is fixed. The fan works in steady state. This template is unique for the standard block.
- *Random*. The random model generator request for power train group. The requests include all the input message of propulsion system and are executed at predetermined fixed time, with no known sequence (see Fig. 11).

The models of the physical system (*Motor*, *Valv* and *Valv_Prop*) were modeled in order to allow free behavior, without restrictions, for these plant parts. The models of the controllers (*GMP_Control*, *Valv_Control* and *Valv_Prop_Control*) are

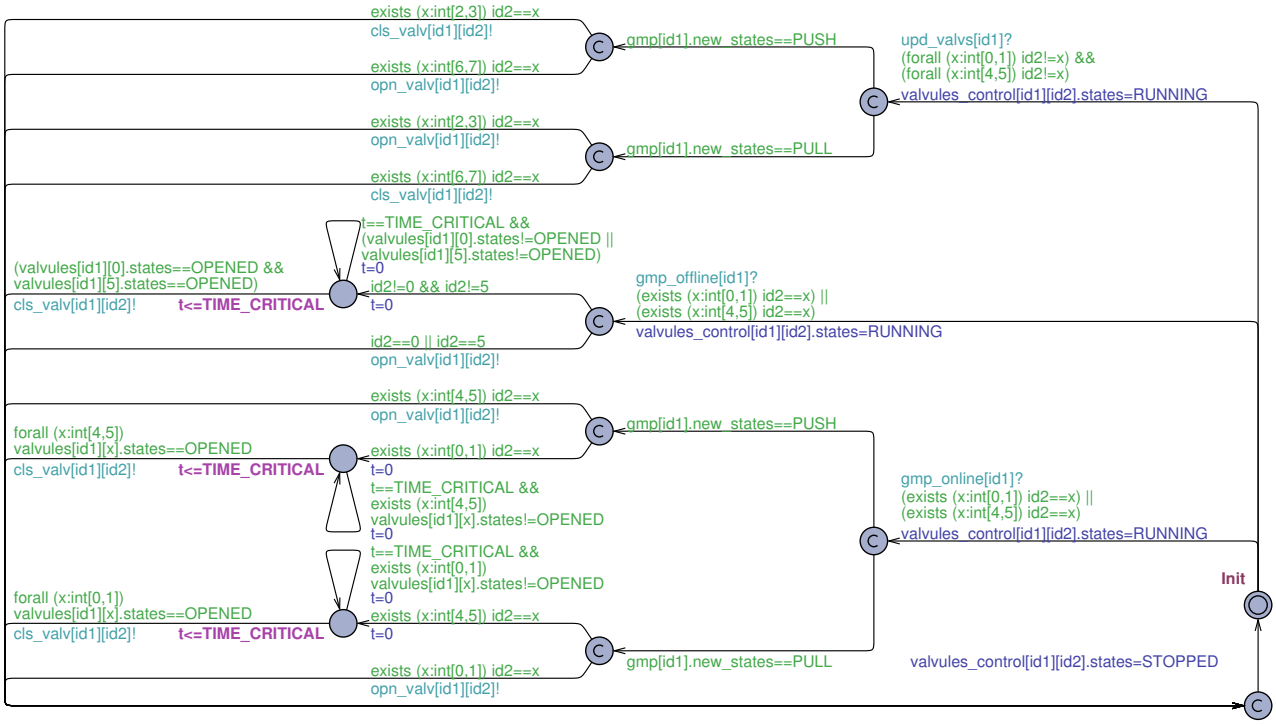

Figure 5. Controller Model of On-Off Valves

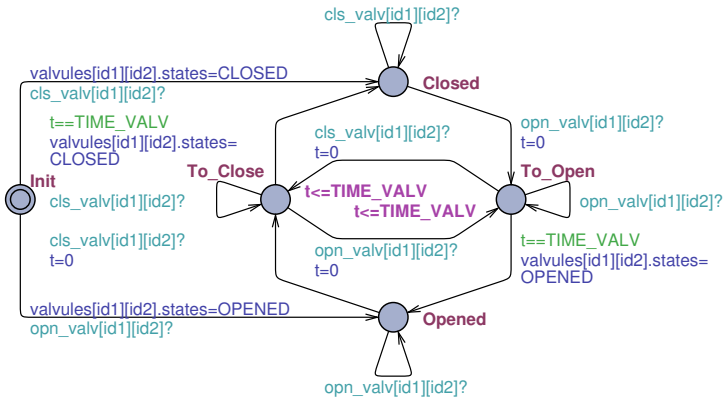

Figure 6. Model of On-Off Valves

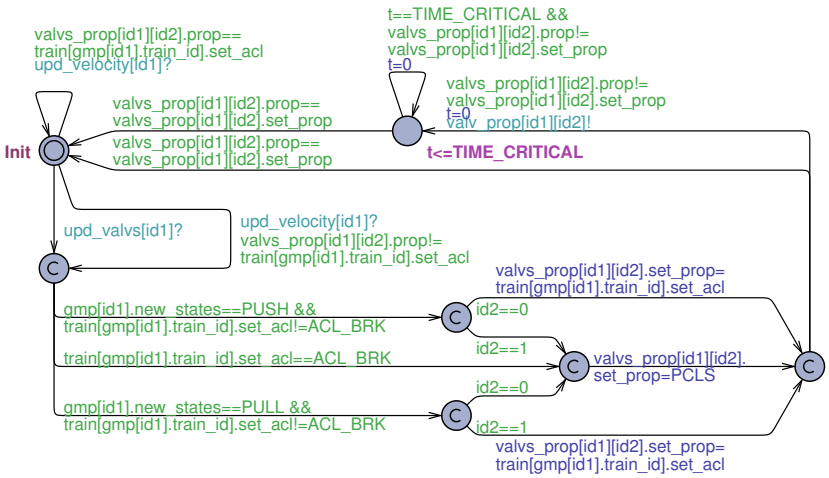

Figure 7. Controller Model of Proportional Valves

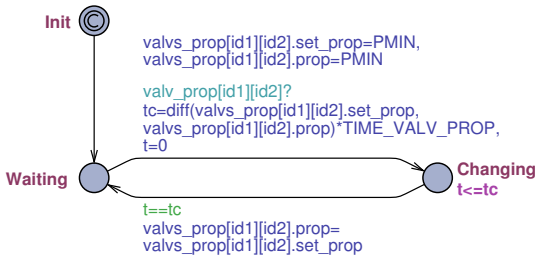

Figure 8. Model of Proportional Valves

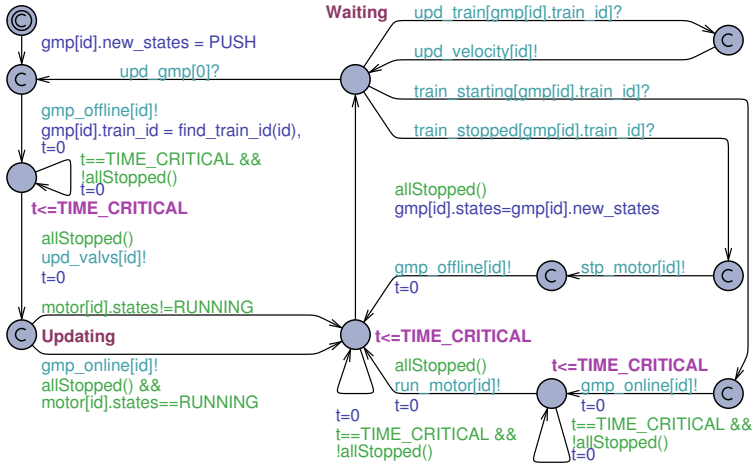

Figure 9. Propulsion System Controller Model

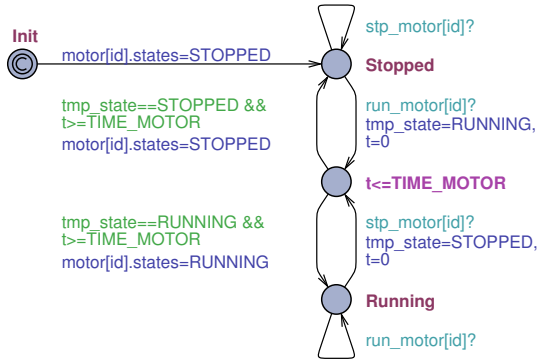

Figure 10. Motor Model

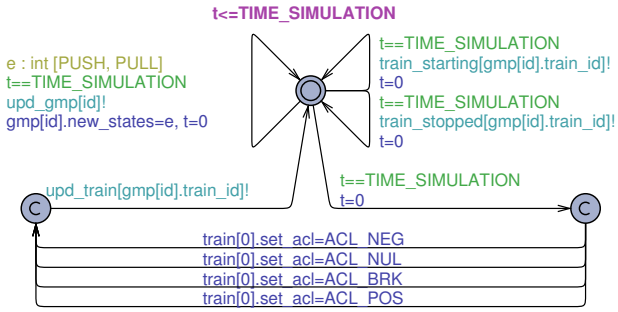

Figure 11. Random Generator Model

responsible for restricting movement of models of plant in order to prevent undesired behavior. Because of the duplicity of equipments is checked a total of 23 models.

4. SIMULATION AND FORMAL VERIFICATION RESULTS

For all the models, the range of all variables has been limited in order to decrease the necessary computational capacity to obtain results, when executing formal verification tasks. For all the locations of the entire automata model - with exception of the "committed" locations - it is necessary a time interval to allow evolutions, in all automaton models, from a location to another location.

4.1 Simulation Results

Concerning simulation results, the data of the file *XTR* (simulation registry) have been used to obtain the diagram of Fig. 12 by using its own software being developed for the purpose and ploted using a spreadsheet. This diagram illustrates the behavior of all the valves when the system changes for the states: *OFF*, *PUSH* or *PULL*.

VP0 and *VP1* are proportional pneumatic valves, but in this chart - and for simplifying the analysis - they appear only totally open or totally closed. *V0*, *V1*, *V2*, *V3*, *V4*, *V5*, *V6* and *V7* are on-off valves. *OFF*, *PUSH* and *PULL* represent the

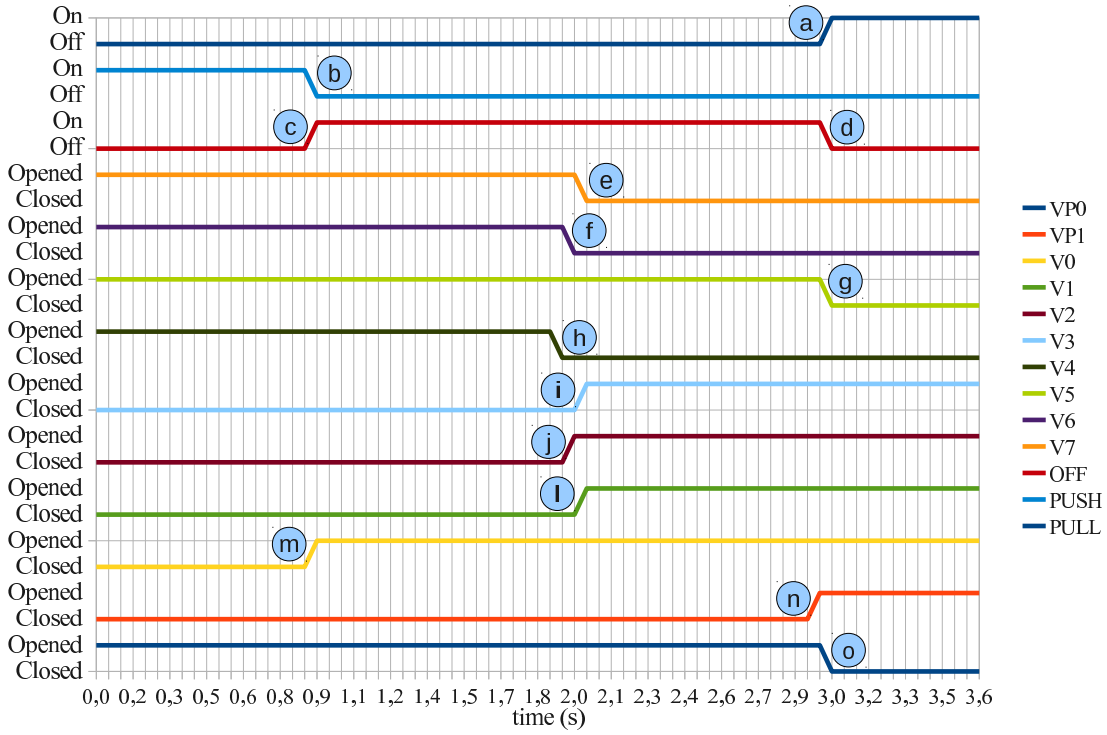

Figure 12. Simulation Results

states *OFFLINE*, *PUSH* and *PULL*, respectively, of the valves set and motor of the pneumatic propulsion system. The motor of this system is not presented in the chart of Fig. 12 because it is always running, during the presented analysis.

By the analysis of the mentioned chart of Fig. 12 it can be observed that the system starts by the *PULL* state. When occurs the changing of state of the valve *V0* (from *closed* to *opened* illustrated by the changing "m", in the chart) the valve *V4* starts changing o respective state (from *opened* to *closed* illustrated by the changing "h", in the chart). In parallel with the changing of valve *V4* begins the changing of the configuration for the state *PUSH*, defined by changing of state of the valves *V1*, *V2*, *V3*, *V6* and *V7* (illustrated by the changing "l", "j", "i", "f" and "e" in the chart). The proportional pneumatic valves change their state too. The *VP0* proportional valve changes from *opened* state to *closed* state (illustrated by the changing "o" in the chart) and *VP1* proportional valve changes from *closed* state to *opened* state (illustrated by the changing "n" in the chart). Once the system is reconfigured the valve *V5* changes from *opened* state to *closed* state (illustrated by the changing "g" in the chart) and the Propulsion System is now in the *PUSH* state (illustrated by the changing "a" in the chart).

The simulated behavior is the expected one for this system. However, the step considered - after this one - was to consider also formal verification in order to be sure about the behavior of the propulsion system.

4.2 Formal Verification Results

Concerning formal verification tasks have been identified some behaviors intended for the APM propulsion system. These behaviors are described using natural language and formalized using the input language of UPPAAL model-checker (see Table 1). For the deduction of properties was used a tool described in (Campos and Machado, 2009).

All the properties have been verified using Difference Bound Matrices (DBM) state space representation in a PC Intel(R) Core(TM)2 Duo CPU 2.10GHz (4Gb RAM) on less than 250 minutes.

5. CONCLUSIONS

The use, in a complementary way, of simulation and formal verification techniques was helpful for obtaining good results when analyzing a part of the distributed controller for the APM system. Until now, the propulsion system behavior has been verified and the achieved states are the predicted states for this system's behavior.

With this study, it is shown, in this paper, that a distributed controller - corresponding to a part of a complex system - has been verified and it is concluded that this part of the controller accomplishes the main behavior desired for the system. With the partial verification of the distributed controller, it was possible to obtain results in reasonable intervals of time and with not very high computational memory consuming during formal verification tasks.

As future work, other partial controllers will be verified - concerning the same system - and, finally, an abstraction of

Table 1. Behavior properties of the propulsion system

Informal Description	Formal Description
The GMP system must attend always the states *PUSH* or *PULL*	`E<>((forall (x:int[0,3]) Valvs(0,x).Closed && (forall (x:int[4,7]) Valvs(0,x).Opened && valvs_prop[0][1].set_prop == PCLS) ||((forall (x:int[0,3]) Valvs(0,x).Opened) && (forall (x:int[4,7]) Valvs(0,x).Closed) && valvs_prop[0][0].set_prop == PCLS)`
If the motor of the propulsion system is running and if the Propulsuion System Controller is not processing information and it is not in the *OFFLINE* state then the Propulsuion System is necessarily in the *PUSH* state or in the *PULL* state	`A[] (Motor(0).Running and GMP_Control(0).Waiting and !Valvs(0,0).Opened and !Valvs(0,5).Opened) imply (((forall (x:int[0,3]) Valvs(0,x).Closed && (forall (x:int[4,7]) Valvs(0,x).Opened && valvs_prop[0][1].set_prop == PCLS) ||((forall (x:int[0,3]) Valvs(0,x).Opened) && (forall (x:int[4,7]) Valvs(0,x).Closed) && valvs_prop[0][0].set_prop == PCLS))`
The valves *V1* and *V5* must never be closed simultaneously	`A[] not (Valvs(0,1).Closed and Valvs(0,5).Closed)`
The valves *V0* and *V4* must never be closed simultaneously	`A[] not (Valvs(0,0).Closed and Valvs(0,4).Closed)`
If the motor of the propulsion system is running and if the Propulsion System Controller is processing information then the Propulsuion System is necessarily in the *OFFLINE* state	`A[] (Motor(0).Running and GMP_Control(0).Updating) imply (Valvs(0,0).Opened and Valvs(0,5).Opened and (Valvs(0,4).Closed ||Valvs(0,4).To_Close) and (Valvs(0,1).Closed ||Valvs(0,1).To_Close))`
The system never attend the *deadlock* state	`A[] not deadlock`

each part of the controller will be verified in order to guarantee the desired behavior for the system, considering all the distributed controller system.

In adiction, as it is a safety critical application, the controllers communications and occurrence of failure modes will be considered as for example done in failure injection.

6. ACKNOWLEDGEMENTS

Guilherme Kunz is supported by the PTI C&T program (*Fundação Parque Tecnológico Itaipu* - FPTI-BR). The authors would like to thank to PTI C&T/FPTI-BR for financial support and to CESUP-UFRGS for access to the clusters.

7. REFERENCES

Aeromovel, 1999. "Aeromovel system technical specification". Technical report, Aeromovel Brasil S.A.

AFCET, 1996. "Apms toward the 21st century". *5th Int. Conf. on Automated People Movers*.

Baresi, L., Carmeli, S., Monti, A. and Pezzè, M., 1998. "Plc programming languages: A formal approach". *Automation 98*. ANIPLA.

Behrmann, G., David, A. and Larsen, K.G., 2004. "A tutorial on uppaal". *4th International School on Formal Methods for the Design of Computer, Communication, and Software Systems (SFM-RT'04)*. LNCS 3185.

Britto, J.F.F.H., 2008. *Modelo Computacional do Sistema Aeromóvel de Transportes*. Master's thesis, UFRGS.

Campos, J.C. and Machado, J., 2009. "Pattern-based analysis of automated production systems". *13th IFAC Symposium on Information Control Problems in Manufacturing*.

Furtado, S.M.d.L., 1994. *Análise Comparativa entre o Aeromóvel e outros sistemas de transporte urbanos guiados automáticos em vias exclusivas elevadas*. Master's thesis, Universidade de Brasília.

Hewings, D., 2008. "Introduction of integrated protection and control to railway electrification systems". In *Proc. IET 9th International Conference on Developments in Power System Protection DPSP 2008*. pp. 68–73. ISSN 0537-9989.

IEEE, 2004. "Ieee standard for communications-based train control (cbtc) performance and functional requirements".

Inouye, T. and Kurokawa, T., 1993. "Automated people movers iii". *ASCE*. New York.

Jones, C.B., 1980. "Software development: a rigorous approach". *Prentice Hall PTR*.

Jones, C., 2003. "The early search for tractable ways of reasoning about programs". *Annals of the History of Computing, IEEE*, Vol. 25, No. 2, pp. 26–49.

Loeckx, J. and Sieber, K., 1984. "The foundations of program verification". *Wiley*. Chichester, England.

Machado, J., Seabra, E., Campos, J.C., Soares, F. and Leão, C.P., 2011. "Safe controllers design for industrial automation systems". *Computers & Industrial Engineering*.

Moon, I., 1994. "Modeling programmable logic controllers for logic verification". *IEEE Control Systems*, Vol. 14, No. 2, pp. 53–59.

Neumann, E.S. and Bondada, M.V.A., 1985. "Automated people movers: Engineering and management in major activity centers". *ASCE*. New York.

Remelhe, M.P., Lohmann, S., Stursberg, O., Engell, S. and Bauer, N., 2004. "Algorithmic verification of logic controllers given as sequential function charts". *IEEE International Symposium on Computer Aided Control Systems Design*, pp. 53–58.

SDE, 1999. "Society of danish engineers". *7th Int. Conf. on Automated People Movers*.

Shen, L.D., Huang, J. and Zhao, F., 1996. "Apm applications: A worldwide review". *Annu. Meeting of Transportation Research Board*. Washington, D.C.

Sproule, W.J., Bondada, M.V.A. and Neumann, E.S., 1993. "Automated people movers iv". *ASCE*. New York.

8. Responsibility notice

The authors are the only responsible for the printed material included in this paper