Analysis and Risk Assessment of the Real Time Volcanic Monitoring System

Luis Enrique Colmenares Guillén[1], Omar Ariosto Niño Prieto[1, 2]

[1] Benemerita Universidad Autonoma de Puebla,
Facultad de Ciencias de la Computación,
BUAP – FCC, Ciudad Universitaria,
Apartado Postal J-32,
Puebla, Pue. México.
lecolme, omar.ariosto@gmail.com

[2] Université Claude Bernard Lyon 1
Bâtiment Nautibus
43, Boulevard du 11 novembre 1918
69622 Villeurbanne Cedex France
OMAR.NINO-PRIETO@bvra.etu.univ-lyon1.fr, omar.ariosto@yahoo.fr

Abstract. In this work, first present the methodology used in the Real Time Volcanic Monitoring System such as SA-RT (Structured Analysis for Real Time) used for the design of the system, and the system itself created for the prevention of the consequences during a catastrophic volcanic event. During the second phase, the Analysis and Risk Assessment of the system is presented. The main contribution of this paper is the complete Risk Assessment Analysis done after finished the design of the system. In order to make a complete Risk Assessment Analysis for complex systems and critical systems done by the engineers, some methodologies are used like the Fault Tree Analysis (FTA), The Markov Analysis and the Petri Nets. In this paper all of them are presented and used since the beginning. First, the Petri Nets are used by the SA-RT methodology in the design of the system. Then the Fault Tree Analysis is used to perform the reliability and safety analysis and to prevent the consequences of an eventually catastrophic volcanic event. The Markov Analysis is used to model all the system because it has high dependencies between its components. Finally the parallel software design is done by the LACATRE methodology.

Keywords: Risk Assessment, Qualitative Risk Assessment, Quantitative Risk Assessment, Markov Analysis, Fault Tree Analysis.

1 Introduction

The active volcanoes are a risk for the society that live near, so it is necessary to study them in order to predict a major event and prevent its consequences like the lost of lots of human lives, the environmental damage and in general the society is very

Received 30/04/10
Final version 19/05/10
Accepted 14/05/10

affected because of this. The Software and Hardware systems help the specialists to predict and to understand this activity better than before, but still doesn't exist 100% of true prediction about a catastrophic volcano event. The Risk Assessment Engineering of certain complex systems[13, 14] like the critical systems of a nuclear plant helps to prevent catastrophic events[11, 14, 15] but in the case of natural disasters exist event a more random probability to occur because is not in function of human activity.

The volcanic monitoring is a hard work that requires a lot of time and effort to have success. So it is necessary to use an automatic system to do this job but also it is necessary to make the Risk Assessment Analysis in order to maintain it always working. The Real Time Monitoring System is a developer tool that helps to monitoring the Popocatepetl activity, additionally of the existing monitoring systems like CENAPRED systems UNAM system and the related work done by many countries in order to prevent this catastrophic event [1, 2].

2 Real Time Monitoring Systems

2.1 Architecture Requirements

Two magnetometers are located strategically in the cone of the Popocatepetl volcano to monitor the magnetic activity and they would transmit that activity trough a GSM Web that will transmit the data by Internet [1]. A computer system located in the research center of CUPREDER will receive that information and the specialists will be able to make an interpretation of the actual activity, but some Critical Parameters shall be taken into consideration in order to register an abnormal activity and try to predict the comportment of the volcano[1,2] (Fig. 1).

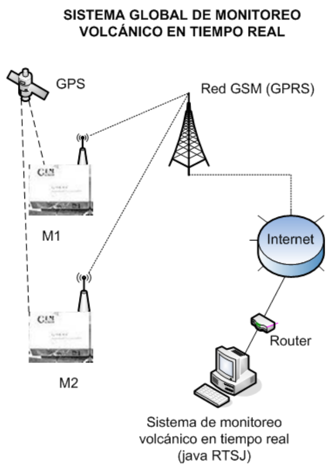

Fig. 1. Global System

2.2 Real Time Monitoring System Methodology

The methodology used to design the Real Time Monitoring System was SA-RT (Structured Analysis for Real Time) that shows a coherent and structured vision of the design of Real Time Systems. The objective of the magnetometers is to transmit the magnetic signal by wireless information to the GSM system that will send that wireless signal to the RTSJ System. While the system is working, the information will be shown in the screen and if there should be an abnormal activity registered by the critical parameters an alarm will be activated. All the data will be saved in a Database that will be accessed by another analysis subsystem [1, 2, 3, 4, 6 and 8]. This is shown by the context diagram (Fig. 2).

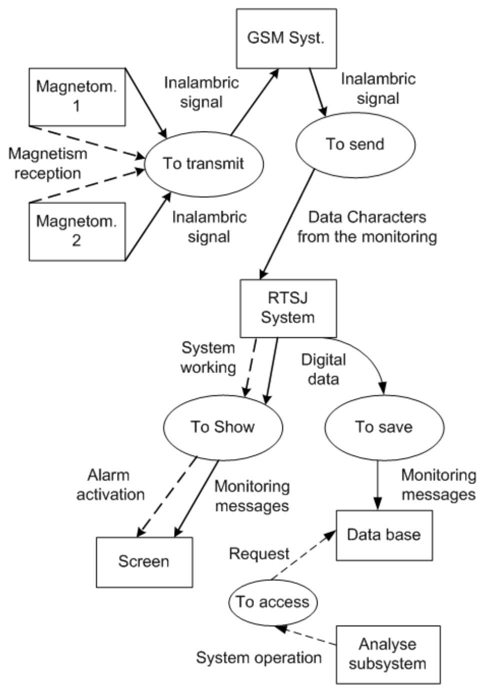

Fig. 2. Context diagram

The Data Flow Diagram (DFD) is shown below (Fig. 3) with all the system processes and the events that enter and go out from the control bar. Also the data flow interact with the whole system and can be compared with the Critical Parameters in order to compare and better understand an abnormal volcanic activity if produced. The State Transition Diagram is derived from the DFD (Fig. 4) and shows each state of the system while functioning.

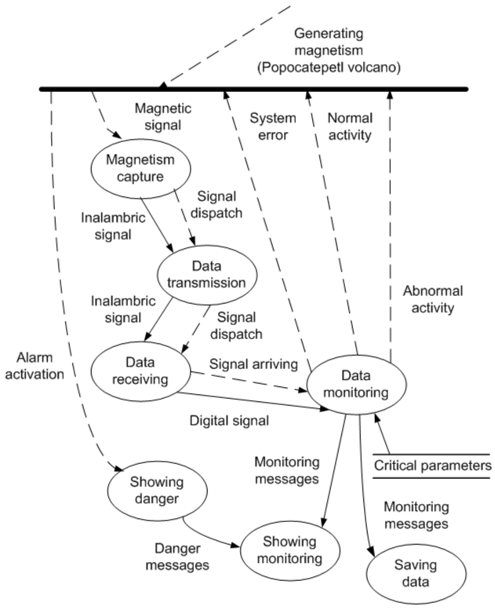

Fig. 3. Data Flow Diagram (DFD**)**

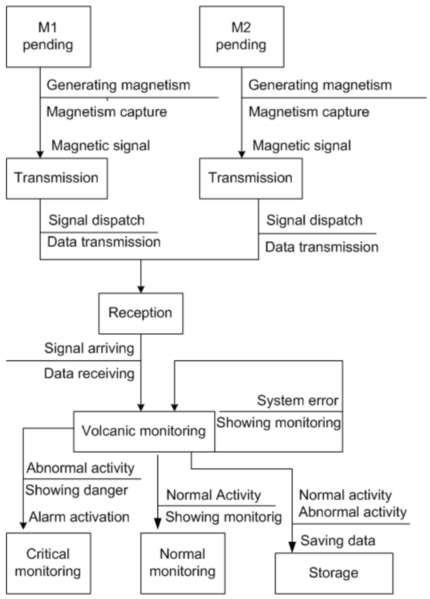

Fig. 4. State Transition Diagram

3 An approach of Analysis and Risk Assessment of the system

The Risk Assessment is a discipline that search the probability of catastrophic events that have catastrophic consequences such as the lost of human lives or irreversible economical and environmental damage [7]. For maintaining the components of a system in a good state in order to prevent those consequences, the Analysis of Risk Assessment of a system is made by the Qualitative Analysis and the Quantitative analysis [10]. *The Qualitative risk assessment* requires calculations of two components of risk: R, the magnitude of the potential loss L, and the probability p, that the loss will occur. The *Quantitative risk assessment* determines the probability of the occurrence of a catastrophic event, and the weakness of a system [10, 11].

The availability is the probability of the good operation of a component. The reliability is the capacity of success of a component during a period of time. The reliability study is made to ensure the success of critical systems that works in cold or warm redundancy [10, 11, and 20].

3.1 The mathematical models

There are some mathematical models used in the Analysis and Risk Assessment of the systems. One of the most used is the Fault Trees, The Markov Analysis, and the Petri Nets [10, 11, 12 and 20] which are used in the design of the whole system.

Fig. 5. Mathematical models

3.2 Analysis with a Fault Tree

This method construct a logic connected diagram by AND and OR gates It has the objective to find the combinations of failures of the components and the *minimal cut set* that describe the combinations of component failures that cause the TOP catastrophic event to occur. This method is deductive and it has the top event, intermediate event and the base event which is the beginning of the failure of the system [10, 11, 12 and 20]. For the Analysis and Risk Assessment of the Real Time Volcanic System, the following Fault tree is proposed:

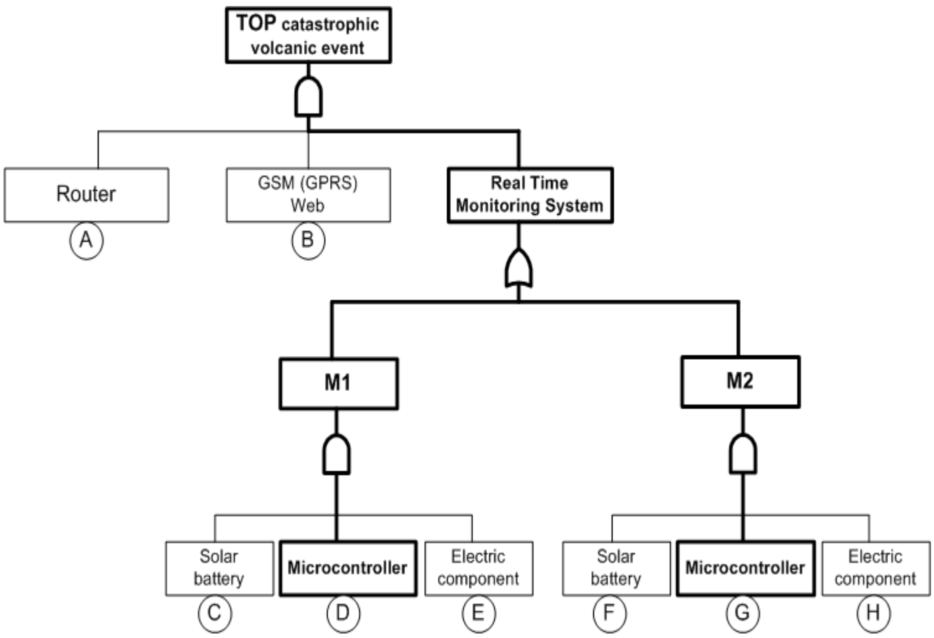

Fig. 6. Real Time Monitoring System Fault Tree

In order to understand the fault tree, first the base failures like the failure of the micro-controller or the battery or any electric component of the design of the system [1] are introduced. After those failures, one of the magnetometers would send corrupted data if the micro-controller fails or simply the magnetometers (M1, M2) stop working. The design of the system allows working in warm redundancy. If one of the magnetometers fails, the system could still be working but with less data to provide to the specialists during the volcanic event. The system fails if the Real Time System fails, because the two magnetometers don't have any sense without an interpretation of the data received by them. Nevertheless, if the Real Time System fails, the data from the magnetometers could be taken manually during normal conditions where there is not an important volcanic event. This doesn't work if exist a catastrophic volcanic event. The minimal cut set is bold in the Real Time Monitoring System Fault Tree, and the mathematical Boolean expression of this tree in order to express the TOP event is represented like follows [10, 11, 12, and 20]:

$$TOP = A * B * ((C * D * E) + (F * G * H))$$

Each base event (A, B, C, D, E, F, G, and H) has a probability p (x) to be produced.

3.3 Markov Analysis

The Markov Analysis permits to visualize the states of the systems and the transitions between them. This method visualizes diagrams of state and space of the systems behavior. This method makes a detailed analysis of the systems that could have another intermediary state different from failure or success. It also permits to study the degraded systems and a probability is associated for each state changing [10, 11, and 20].

The Markov modeling is not random because the states are dependent from the last immediate state but independent from the others [10]. This can model systems without memory and the probability of changing of state is constant. The comportment of the system depends on the present state that is continuous in the time and discrete in space [10, 11, and 20].

The Real Time Volcanic Monitoring System has different components like the magnetometers (A, B) which has the comportment of repairable systems, the Real Time RTSJ (C) that has the comportment of degradable system and they are represented by the Chains of Markov in Alta Rica Data Flow Programming [16, 17, 18, 19, 21 and 22]. Those models were created before in order to understand, simulate and predict the comportment of the critical systems [17, 18, 19, 21 and 22], and adapted for the Real Time Volcanic Monitoring System components. Those models could be more complex, but the basic representation for the correct operation is represented below.

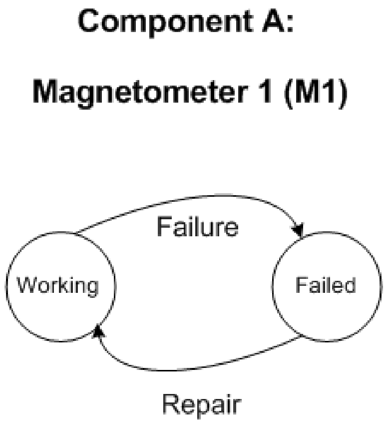

Fig. 7. Repairable model A

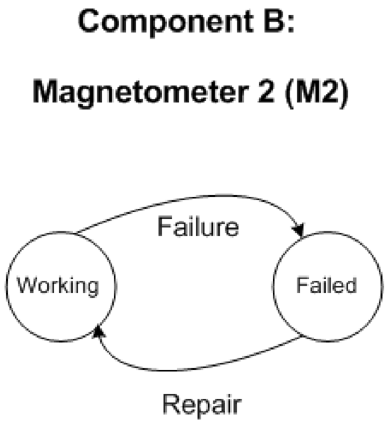

Fig. 8. Repairable model B

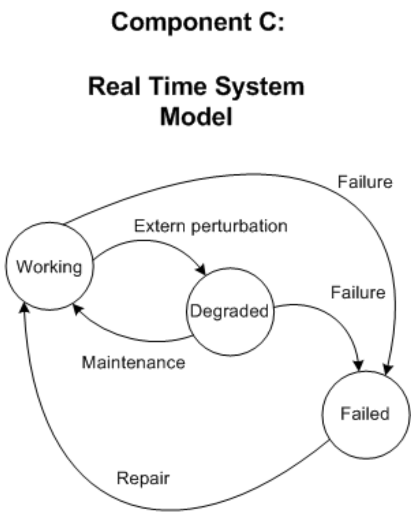

Fig. 9. Degraded System model C

Each component has a comportment Markov model, but the interaction of the system is done by the composition [16, 17, 18, 19, 21 and 22] of the models of the basic components. First twelve different combinations of the states of the components could be found, but in order to find the correct model of the system, the semantic of The Real Time Volcanic Monitoring System is respected. The concrete model of the Real Time Volcanic Monitoring System is proposed below.

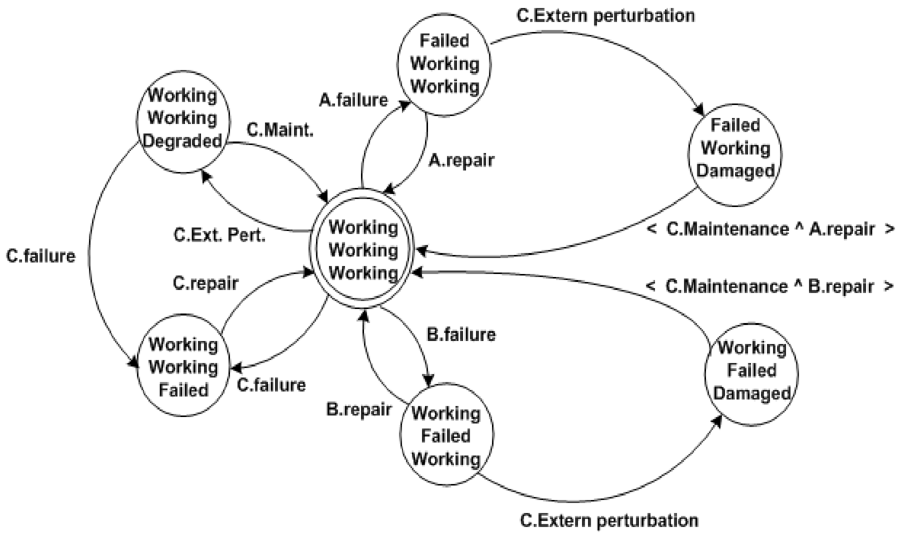

Fig. 10. The Real Time Volcanic Monitoring System Model

The correct operation of the Real Time Volcanic Monitoring System doesn't allow that the three components fail at the same time, because if exist a volcanic event, the system wouldn't be able to report a volcanic abnormal event nor predict it [2]. So there are some states that don't have any sense to stay. Also the system should be in warm redundancy [15] because there are two Magnetometers working at the same time and providing important data while they are transmitting the magnetism [1]. In the beginning, the whole system is working; if exist a failure from the magnetometer one or two the state will be changed, but the system will continue working. After this state, the computer system could be damaged or have any external perturbation so there is a new changing of state. At this time, the system is still working but it has to return to the initial state to continue working without any problem, so there are transitions that are mixed up with the synchronization [16, 17, 18, 19, 21 and 22] in order to return as soon as possible to the initial state. The computer system could be damaged and eventually fail while the two magnetometers are working this has a new state and this is also modeled. Finally, the prevention is the main idea of the model of the system, knowing that the TOP event consequence (human, economical) is the lack of prevention and incertitude of a major volcanic event.

4 The software design of the system

The software design [1] is represented by the LACATRE [5, 9] real time systems methodology (Fig. 11). The main program is divided in several modules. The main () function will work with the following threads:

P2: Magnetometer 1, with priority 1.
P3: Magnetometer 2, with priority 2.
P4: Monitoring, with priority 3.
P5: Alarm, with priority 4.
P6: Prediction, with priority 5.

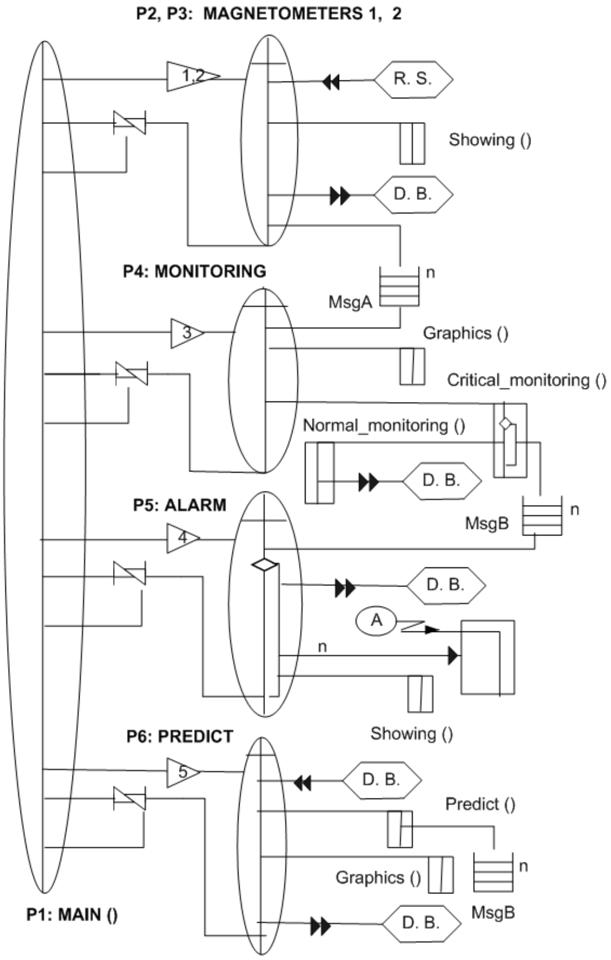

Fig. 11. LACATRE Diagram

The threads are synchronized by semaphores to ensure that all the processes have the correct data. The signal from the magnetometers are obtained with a communication data protocol and transmitted by the data resource (R.S.) to the threads P1 and P2 that shows the magnetic activity with the function *Showing( )* that has all the procedures to show the numerical data in the screen. Then all the data are saved in a Data Base and the messages from each magnetometer are sent independently to one FIFO data structure, and the thread P4 receive them to process the information received by the functions *Graphics(), Critical_Monitoring()* and *Normal_Monitoring ().*

If an abnormal activity exists, the function *Critical_Monitoring ( )* send a message to another FIFO to register the abnormality and those messages are transmitted to the thread P5 which write the abnormal data in the data base and activate an alarm. At the same time the function *Showing ( )* is showing all the abnormal activity in the screen. The system has another thread P6 which has the function *Prediction ( ),* and this function makes a prediction of the magnetic activity using neural networks algorithms [2].

5 Conclusions and Ongoing Research

The main contribution of this work is to have an approach of the risk assessment of the Real Time Volcanic Monitoring System. The catastrophic event is not dependent from human activity like other types of critical systems but always exist a probability of occurrence. Nevertheless if we use the same methodology and the catastrophic event is produced, we will be able to reduce the consequences and the people will be more prepared to face and solve the problems derived from this event like human lives and economical damage. The human factor is always important because sometimes the natural catastrophic events take some time to be produced but it is very important to be prepared.

At this time for the project, many subjects are being studied; one of them the possibility to implement all the system but it is necessary to work as a team with many specialists in electronics, computing science, geologists and volcanologist, all of them from Puebla working as a team at the University of Puebla BUAP, and CUPREDER [1, 2]. This project will help to prevent the natural disasters very frequent in Mexico. We are not able to avoid them, but reduce the negative consequences if happened.

References

1. O. Niño, E. Colmenares, M. Martin, Sistema de Monitoreo Volcánico en Tiempo Real Congreso de IEEE, ANDESCON2008 (Ciudad del Cusco, Peru) Octubre de 2008. ISBN: 978-603-45345-0-6.
2. O. Niño, E. Colmenares, M. Martin, Propuesta para predecir eventos en el Sistema de Monitoreo Volcánico en Tiempo Real basado en la informática bio-inspirada y algoritmos de Redes Neuronales. Congreso SENIE Aguascalientes

2008 Universidad Autónoma de México. (UAM) Oct. de 2008. ISBN : 978-970-31-0944-9

3. BABAU Jean-Philippe, cours 4IF “Conception et Integration d'Applications Industrielles, SA-RT Structured Analysis for Real-Time 4IFCIAI“ (Annee 2007-2008), INSA de Lyon, Couse notes.
4. BABAU Jean-Philippe, cours 4IF “Systemes d'Exploitation avances 4IFSEA, conception Multitâches Lacatre/VxWorks”, (2007-2008), INSA de Lyon, Couse notes.
5. Piotr Szwed, Lacatre Reference Guide, programming tool, http://pszwed.ia.agh.edu.pl/RT/La4_rm/La4_rm.html (2008).
6. Prih Hastono and Sorin A. Huss, Automatic Generation of ExecutableModels from Structured Approach Real-Time Specifications http://www.vlsi.informatik.tu-darmstadt.de/staff/hastono/rtss04-sart.pdf 2008.
7. J.A. McCall, Factors in Software Quality, General Electric no. 77C1502, jun 1977.
8. Babau, Jean-Philipe, SA-RT “Structured Analysis for Real-Time” http://www.if.insa-lyon.fr/chercheurs/jpbabau/cours/sart.pdf (2008).
9. J. J. SCHWARZ, J. J. SKUBICH, Graphical programming for Real-Time Systems, Control Engineering. Practice, Vol. 1, No. 1, pp. 43–49, 1993.
10. Marvin Rausand ; System Reliability Theory, Models and Statistical Methods; John Wiley & Sons,Inc. 1994.
11. J.D Andrews and T.R. Moss; Reliability and Risk Assessment ; Longman Scientific & Technical; 1993.
12. http://faulttreesoftware.info/(2009)
13. http://www.ixxi.fr/Les_SC.php (2009)
14. Ingénierie système, notes de cours M2, ingénierie des systèmes complexes; Thales Université-Ecole Polytechnique, France ; 2007-2008.
15. Storey Neil, Safety-Critical Computer Systems; Addison Wesley; Longman; 1996.
16. Rauzy Antoine, Griffault Alain, Point Gérlald, Arnold André ; The Alta Rica Formalism for Describing Concurrent Systems ; Université Bourdeaux I, CNRS; 2000.
17. Pont Gérald ; Thèse: Alta Rica Contribution à l’unification des méthodes formelles et de la sûreté de fonctionnement ; Université Bordeaux I ; 2000.
18. Roux Olivier, Pagetti Claire, Cassez Frank ; A Timed Extension for Alta Rica; CNRS Nantes ; 2002.
19. Rauzy Antoine, Alta Rica a Formal Language for Oriented Modeling ; IML/CNRS & ARBoost Thechnologies, Marseille, France ; notes de cours.
20. Gondran M. Pagès A. Fiabilité des Systèmes ; Direction des Etudes et Recherches d’Electricité de France ; 1980.
21. http://www.pdfgeni.com/book/AltaRica-pdf.html (2010).
22. Pagetti Claire, Une extension temporisée d’AltaRica Application à la modélisation d’un système embarqué ; IRCCyN 1 rue de la Noë BP 92101, 44321 Nantes Cedex 3 France.