Proposal to improve systems performance when there exists a fault

Karen Hernández Rueda[1], María Elena Meda Campaña[2]
[1]Universidad de Guadalajara, Zapopan, México, khernandez@cucea.udg.mx
[2] Universidad de Guadalajara, Zapopan, México, emeda@cucea.udg.mx

INTRODUCTION

A system fails when it does not meet its specification. Depending on the complexity and importance of the system, this failure can be tolerated or may lead to a catastrophe. At present there are many complex system failures that inevitably occur, no matter how safe it is its design, which both control techniques improve, or how good the operators. Therefore, the problem of fault detection and recovery is an existing need, not only by the impact they could be on the systems but also in the same society when you can avoid a catastrophe. A great deal of research effort has been and is being spent on the design and development of automated diagnostic systems. A variety of schemes, differing both in their theoretical framework and in their design and implementation philosophy, have been proposed. From the conceptual viewpoint most existing methods of failure diagnosis can be classified as: 1) fault-tree based methods; 2) quantitative, analytical model-based methods; 3) expert systems; 4) model-based reasoning methods; and 5) discrete-event system (DES)-based methods [Sampath et al, 1998]. Our interest in this work is to study DES but considering fault detection method model-based, on scheme considering, the actual and the expected behavior (from a mathematical model) area compared to identify a fault [Xiaoli1 et al 2009].

There are many factors that can cause a system failure and the main factor is when there are some design errors. However, when a system is already operational and is expensive in time and/or money to redesign it, then there must be alternatives to prevent faults or in other case recover or continue to operate despite the occurrence of the same. So this paper propose one alternative to face up the problem and the work is presented as follows: motivation, conceptualization of the problem, proposal and future work.

MOTIVATION

Safety and reliability are the two main factors that motivate the study of the problem of fault detection and recovery of DES, so as they one related with the avoid the avoid the risky situations that can be catastrophic. Another motivation is to ensure that systems cotinue to work, since some systems, like power plants, should not stop working because they can generate service interruptions that cause severe economic impacts and even danger, as happened with the nuclear reactor in Japan after the tsunami in March 2011.

PROBLEM´S CONCEPTUALIZATION

The goal in designing and building a fault-tolerant system is to ensure the continuous functioning correctly as a whole, even in the presence of faults and degradation of this system**.** The allmost systems have a controller that generates the inputs to the system as the model specification to ensure the smooth operation, but what if controller fails? There are two possibilities: reconfigure the control or modify the specifications. These possibilities are presented in the following diagram shown in Fig. 1:

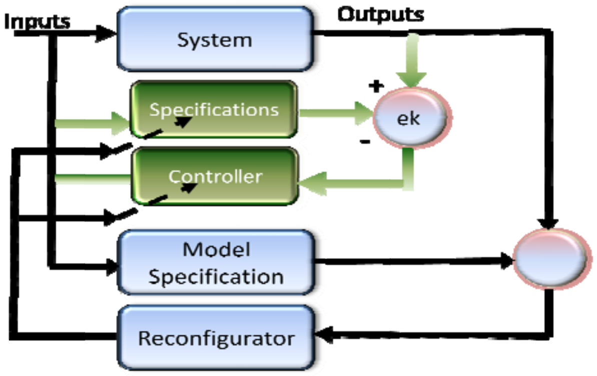

Figure 1: Diagram to configure the controller or change the specifications of a system

As you can see in the Fig. 1, it can detect a failure and decide how to recover it considering the following steps:

- Measure the output on the data.
- Measure the output data assumed by a model specification.
- Computo the output error as the difference between the output of the system and its specification.
  - If the error is zero, implies that the system has a good performance. In other case, implies that the system behaviour is different from its specification.
  - If the error is not zero, Reconfigurator decide whether it´s posible to modify the driver to continue to meet the specifications or whether it also modifies the specifications to lead the system to a safe state.

When the system fails (during its operation), the system-control-specific (shown in Figure 1) should be adapted or reconfigured to continue operating as the system was design. Furthermore, it should indicate that there is a reconfiguration that was repaired because had an error. In systems, however, no there is mechanism for reconfiguration. In fact there is a need to develop a theoretical framework that defines under which circumstances a system can detect an error and recover from it with the least human intervention and with the least degradation of the system as possible.

PROPOSAL

We propose the scheme depicted on Fig 2.

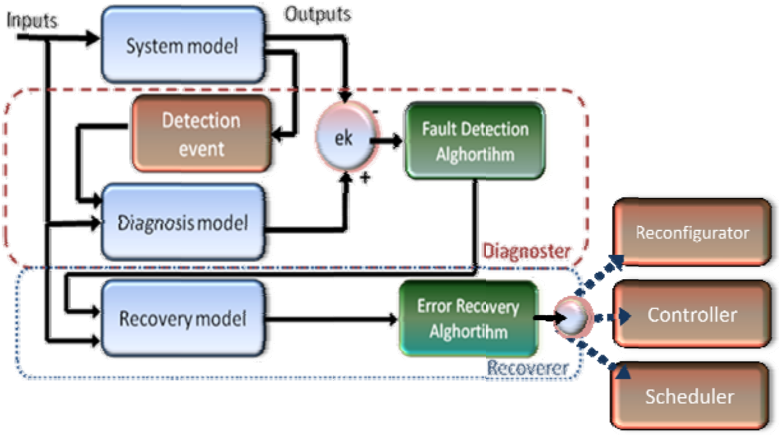

Figure 2: Scheme proposed to diagnoses and recovers faults

It is possible to implement a scheme of fault diagnosis and fault recovery of DES using Petri nets, with minimal degradation in system performance. The diagnosis model must detect and locate line faults in a finite time, even with no diagnosable systems based on the diagnosis model presented in PhD thesis Ruiz [Ruiz, 2007]. The recovery model must modifiy the controller, scheduler or system reconfiguration.

FUTURE WORK

In the future work, some of the following activities that we need to do are:

- Determine when a fault is detectable in the system
- Define and characterize, in IPN terms, the diagnosability and recoverability property based on the system's structure
- Characterize of the redirection of resources and replanning IPN terms
- Implement fault diagnosis and fault recovery algorithms in a computational tool
- Design test methodologies for diagnosis and recovery faults

REFERENCES

Meera Sampath, Stephane Lafortune, Kasim Sinnamohideen, and Demosthenis C. Teneketzis (1998). "Diagnosis of Discrete-Event Systems", *IEEE Transactions on Automatic Control*, Vol. 43, no. 7, pp. 908-929.

Wang Xiaoli1, Chen guangju Xie yue Guo zhaoxin (2009). "Fault Detection and Diagnosis Based on Time Petri Net", *The Eighth International Conference on Electronic Measurement and Instruments*, pp.3-259 - 3-26.

Elvia Ruiz Beltrán (2007). "PhD Thesis: Diagnostic Diagrams Discrete Event Systems". CINVESTAV-unidad Guadalajara. pp. 1- 150.