

# Dependability Evaluation of Fault Tolerant Distributed Industrial Control Systems<sup>1</sup>

J.C. Campelo, P. Yuste, F. Rodríguez, P.J. Gil, J.J. Serrano

Department of Computer Engineering  
Technical University of Valencia – Spain  
{jcampelo, pyuste, prodrig, pgil, juanjo}@disca.upv.es

**Abstract.** Modern distributed industrial control systems need improvements in their dependability. In this paper we study the dependability of a fault tolerant distributed industrial control system designed in our university. This system is based on fault tolerant nodes interconnected by two communication networks. This paper begins showing the architecture of a single node in the distributed system. Reliability and safety results for this node are presented using a theoretical model based on Stochastic Activity Networks (SAN). Based on this architecture, the theoretical model of the distributed system is then presented; in order to evaluate the reliability and safety of the whole system models based on stochastic activity networks are used, and the results obtained using UltraSAN are presented.

## 1 Introduction

Distributed industrial control systems are becoming one of the most important research areas in embedded control applications. In this sense, control and supervision of those systems is accomplished through the co-operation of different nodes that are interconnected through industrial local area networks.

The fault tolerant systems group of the Technical University of Valencia, has developed a fault tolerant distributed industrial control system. In this sense, the fault tolerant architecture for the node of a distributed industrial control system is shown in this paper and a theoretical model of this architecture based on stochastic activity networks is used to obtain its reliability and safety. In order to study the distributed system, a hierarchical modeling approach is used, also with stochastic activity networks, based on the fault tolerant node model and joining several nodes to obtain a complex system.

This paper is organized as follows. After the introduction, an overview of the node of the distributed system is given. The structure and the model of the fault tolerant node are presented. In sections three and four the modelling approach of the distributed system and the results are presented. This paper ends with the conclusions obtained.

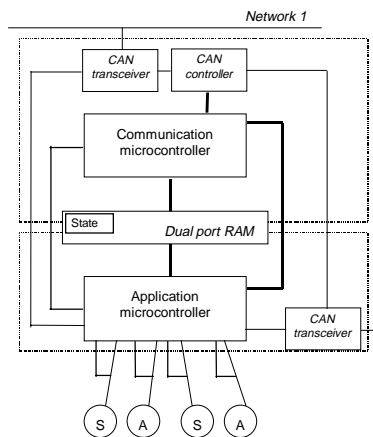
---

<sup>1</sup> This work is supported by the Spanish *CICYT* under project CICYT-TAP96-1090-C04-01

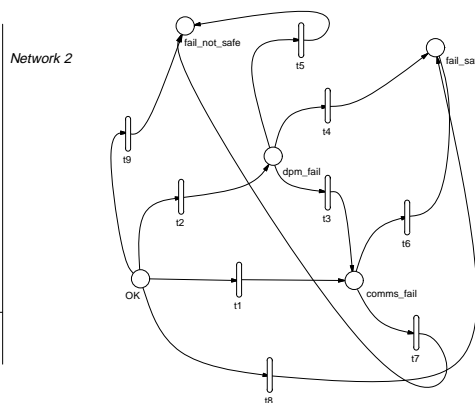
## 2 Node Architecture

The node architecture of the distributed industrial control system developed has as its main objective reliability and safety improvements with a low cost. This node (figure 1) consists of two communication networks, two microcontrollers, one for communication tasks and other for the execution of the control algorithms, and a dual-port RAM.

Commonly in industrial applications different nodes could accomplish similar functions. This is due to the fact that they can be connected to the same set of sensors and actuators. So, an important aspect is to store the state of each node in the dual-port RAM and to update it periodically. Thus, in case of failure in the application microcontroller, the communication microcontroller can send the state to other node that could continue its function. To do this, an important aspect is to reach a high coverage factor, mainly for the application microcontroller (the most complex component). In order to obtain a high coverage factor, the communication microcontroller also fulfils functions of watchdog processor. In this way, the communication microcontroller can detect errors in the other processor and inhibit possible outputs to the actuators and possible error messages to the network (this is known as fail-silent behaviour).



**Fig. 1.** Node Architecture



**Fig. 2.** SAN model

The SAN [1,2,3] model that represents a single node is shown in figure 2. In this model each place represents a state of the system and is the direct conversion of the Markov model [4].

### 3 Distributed System Model

Now, that the reliability and safety can be obtained solving the previous model, new questions arise about the reliability and safety of the whole distributed system. In order to study these aspects a distributed system model is presented.

We are assuming a distributed industrial control system composed by six fault tolerant nodes. In this system, due to the characteristics of the industrial process to control, nodes 3 and 4 and nodes 5 and 6, are connected to the same set of sensors and actuators. So, a failure in node 3 can be recovered by node 4 and vice-versa (when node 3 is in a fail-safe state it can send its state to node 4 and this one can continue both jobs). The same behaviour for nodes 5 and 6 also applies.

In order to model the distributed system, we are doing a composed model. As it can be seen in figure 3, the 6 single “node” and “connection” subnets compose this model. The connection subnet will be in charge of deciding which of the failures of the single nodes can be recovered by another node (node 3 can be recovered by node 4 and vice-versa and the same for nodes 5 and 6). In this model, node subnets are slightly different from the previous model. As the failure of a single node does not necessarily take the system to a failure state, there are no faulty states embedded in the subnet. Instead, the “fail safe” and “fail not safe” states are in the connection subnet (due to some UltraSAN limitations – instantaneous activities between common places - a more hierarchical model can not be done [5]). So, the node subnet only has the operational states representing the behaviour of the node. In figure 4 the node model can be seen. The places in this subnet will be common with the same places in the connection subnet. The connection subnet is shown in figure 5. In this subnet there are different kinds of places: first, places representing the inner state of each of the six nodes. These are common places that are both in the connection subnet and in the node subnets. There are the failure places, as in the previous model, two new places, “rg1” and “rg2” and the network places “networks\_down”, “OK\_net1” and “OK\_net2”.

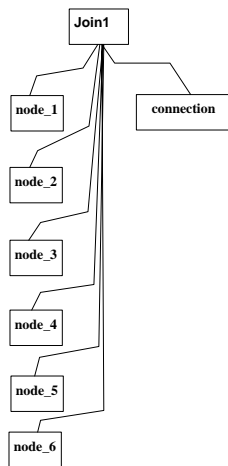


Fig. 3. Composed model

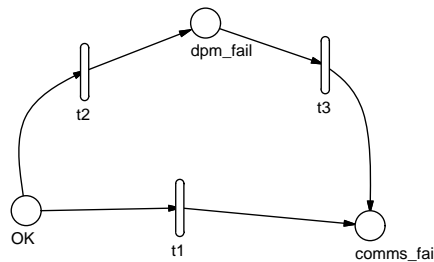
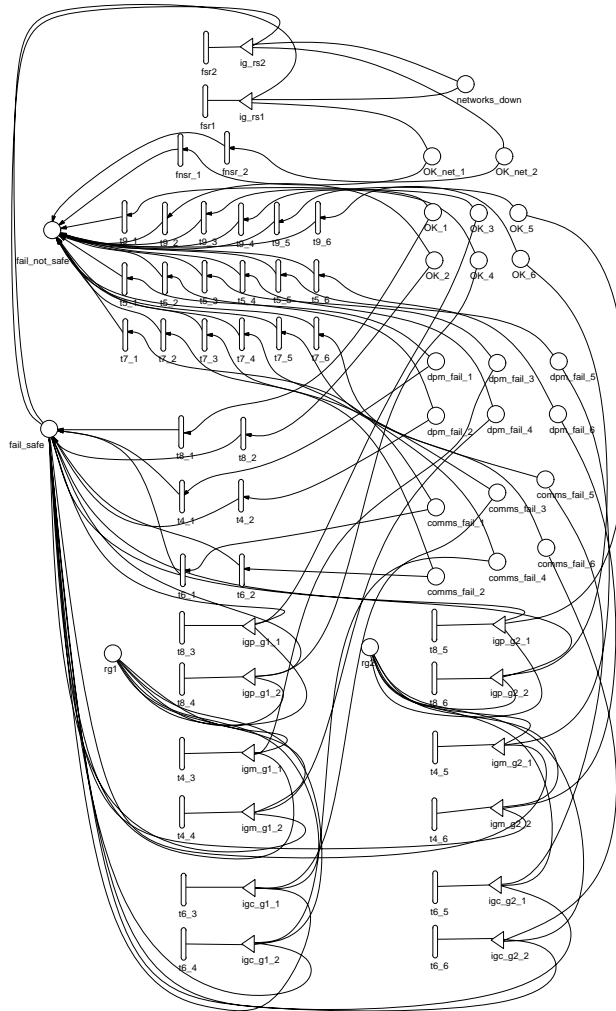


Fig. 4. Node subnet



**Fig. 5.** SAN model: connection

The meaning of these new places is the following: the system has six nodes, two of them are independent and four are grouped in two clusters. Inside each cluster any node can recover any other node's failure and reconfigure itself to execute both tasks. In places "rg1" and "rg2" there is a number of marks equivalent to the number of failed nodes in cluster 1 and 2 respectively. Places "OK\_net1" and "OK\_net2" represent the correct operation of the two networks respectively and "networks\_down" represents when it has more than one mark that both networks are out of service. As it can be seen in the connection subnet, USAN input gates are used to allow the relationships between the different node groups, to model the networks behaviour and the transitions to faulty states.

## 4 Results

Reliability and safety results solving the previous models have been obtained. In table 1 the results can be seen. These results were obtained with a failure rate of the application microcontroller equal to  $1e-05$  (faults/hour), varying coverage for transient faults from 0.75 to 0.999 and time equal to 10000 hours.

<i>Transient faults coverage</i>	<i>Node reliability</i>	<i>Node safety</i>	<i>System reliability</i>	<i>System safety</i>
0.75	0.9588465	0.97822869	0.8395765	0.8748919
0.80	0.96268653	0.98210725	0.8598195	0.8959124
0.85	0.96654194	0.9860013	0.8805511	0.91743846
0.90	0.97041281	0.98991089	0.90178286	0.9394824
0.95	0.97429918	0.99383611	0.92352702	0.96205666
0.99	0.97741949	0.99698756	0.94129954	0.98050646
0.999	0.97812293	0.99769802	0.9453453	0.98470625

**Table 1.** Reliability and safety results

## 5 Conclusions

In this paper a modelling approach to study the reliability and safety of a distributed system has been presented. This model is based on the model of the fault tolerant nodes in the system. With the distributed system model we can study the influence of different fault tolerant nodes analysing the influence of the node reliability and safety in the system results. In this sense we are going to try with other fault tolerant architectures [4] for those nodes that can not be recovered by another one.

## References

1. Sanders, W.H., Obal, W.D.: Dependability evaluation using UltraSAN. 23th International Symposium on Fault Tolerant Computing. Toulouse, France (1993)
2. Sanders, W.H., Obal, W.D., Qureshi, M.A., Widjarnako, F.A.: UltraSAN version 3: architecture, features, and implementation. Technical report 95S02, Center for reliable and high-performance computing. University of Illinois at Urbana-Champaign (1995)
3. UltraSAN users manual. Center for Reliable and High Performance Computing, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign
4. Campelo, J.C., Rodríguez, F., Gil, P.J., Serrano, J.J.: Dependability evaluation of fault tolerant architectures in distributed industrial control system. WFCS'97, 2<sup>nd</sup> IEEE International Workshop on Factory Communication Systems, Barcelona, Spain (1997)
5. Nelli, M., Bondavalli, A., Simonici, L.: Dependability modelling and analysis of complex control systems: an application to railway interlocking. EDDC-2, 2<sup>nd</sup> European Dependable Computing Conference. Taormina, Italy (1996)