



Safety and reliability in computer-based traffic management: a probabilistic approach using Petri nets

P. Firpo, S. Savio & G. Sciutto

*Dipartimento di Ingegneria Elettrica, Università di Genova,
Via all'Opera Pia, 11a - 16145 Genova, Italy*

Abstract

Real time computer systems, already employed in several industrial fields, as far as system management concerns, are today applied, thanks to their high flexibility, reliability and compactness, also in the transport area, particularly in life-critical applications, where electromechanical devices are state of the art.

In such applications safety and reliability must be the keywords of the problem: safety to preserve human lives from dangerous events and reliability to keep the system operational as far as possible.

One of the most flexible approaches is the statistical approach based on the high modelling capabilities of Petri nets. In particular, the stochastic extension of Petri nets is today, probably, the best modelling tool to perform safety and reliability analysis of real time computer systems.

In this paper the authors present a safety and reliability analysis, based on a Petri net model, of a life-critical system; a central apparatus for vehicle routing and peripheral management for a railway station traffic control, is modelled and statistical results are presented.

1 Introduction

Modelling plays a fundamental role in performing a safety and reliability analysis, which must provide information about the correctness of the choices made during the design process. In particular, at each design phase, the candidate design has to be analyzed to verify if the user's specifications are fulfilled. Only after the verification process a lower level design phase may start.

Therefore, safety and reliability analysis must be performed at several detail levels; the more detailed will be the design the more refined will be the results. The analysis presented in this paper regards the highest level design phase where the candidate architecture is verified in order to validate the choice preformed by the designer and to provide guidelines for the next design phases. The authors present the application of the Petri nets modelling to an existing system, the ACS (Apparato Centrale Statico), a centralized vehicle routing system for a railway station, utilized in Italian Railways [1], showing how to perform dependability measures using Stochastic Petri nets solution tools.

2 The ACS architecture

In Figure 1 is shown the architecture of the ACS system, which is today under a testing phase in some stations of Italian Railways [1]. The ACS can be splitted into two main parts: the *life-critical subsystem*, composed of the Fail Safe Nucleus (FSN), the Video Switching Unit, the Communication System and the Peripheral Units (PU), and the *non life-critical subsystem*, composed of the Diagnosis and Remote Control Unit (RDC).

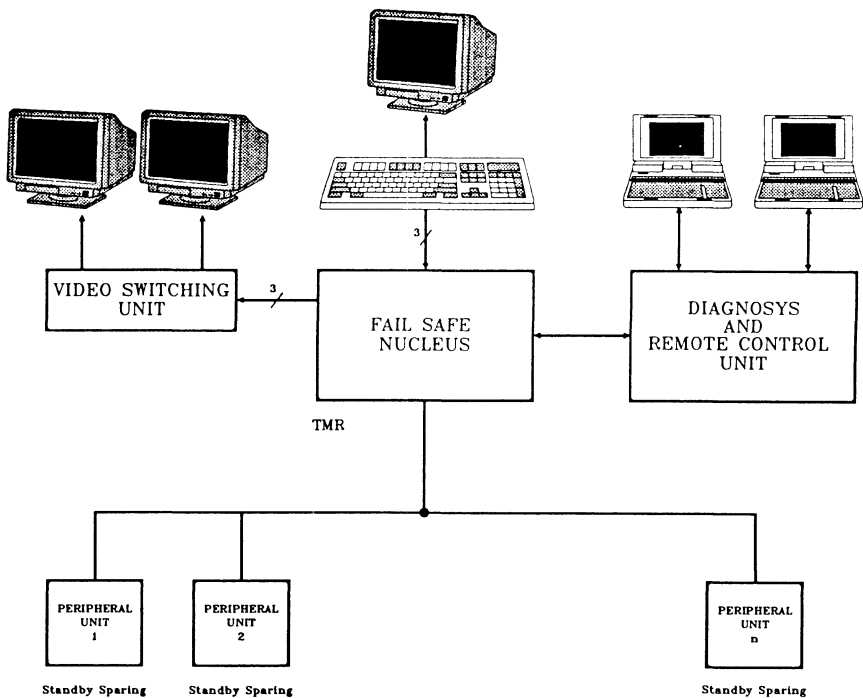


Figure 1: The ACS system architecture.

The function of the RDC Unit is to inform operators on the status of the system, to signal the occurrence of faults and consequently to request a repair operation, to record the sequence of commands sent, by the operator to the life-critical subsystem and to allow the user to poll the system for informations on its operation. Two video terminals are available for the user and a spare unit is present to substitute the active unit in case of failure.

The FSN is the most important and critical block of the ACS system and is triple redundant. The FSN performs the following functions: it checks the correctness of the command sequences sent by the operator, it prepares commands for the PUs in order to accomplish the operator's requests, it acquires the actual status of the PUs and sends them command signals and finally it manages the Communication System for a fail safe data exchange between the FSN itself and PUs.

The user interface is composed by a Functional Keyboard, with triplicated contacts for each key, to send commands to the FSN, a display to echo the pressed keys, two Graphic Monitors on which a graphic representation of the actual status of the station is displayed: both the monitors display the same picture and are driven by one of the three units of the FSN. The Video Switching Unit chooses the unit which has to drive the monitors.

Each PU has to control a peripheral device, such as a signal or a point, and is double redundant. The data exchange between FSN and PUs is performed on fiber optics redundant lines using a fail safe protocol.

The FSN is the target of the safety and reliability analysis which is going to be performed. In the following paragraph the FSN architecture is described and the safety and reliability Petri net models are built.

3 The Fail Safe Nucleus architecture

The solution adopted for the FSN is a Triple Modular Redundancy [2] reconfigurable architecture. Each of the three FSN units is organized into two subunits: the User Interface and Logic (UI&L) Unit and the Peripheral Management (PM) Unit.

Each FSN unit dialogues with the other units to implement a 2 of 3 voting. Some assumptions about the fault detection techniques utilized have now to be made: a first reasonable assumption is that each of the UI&L units and of the PM units performs diagnostic tests to detect hardware failures; a second reasonable assumption is that each UI&L unit compares its outputs with the outputs of the other UI&L units producing a voted output for the PM units and allowing the detection of errors due to undetected faults [2]. Similar operations are assumed to be performed by the PM units. The resulting FSN architecture, characterized by a two level voting with triplicated voters, is shown in Figure 2.

A logical circuit named Exclusion Logic (EL) is able to perform a system reconfiguration in case of detection of a fault in one of the three FSN units. The fault detection can be performed either by the self diagnostic utilities embedded in each subunit or by the comparison implemented in the voting operation. When a fault is detected the EL disables the unit in which the fault has occurred

258 Railway Operations

and the system continues to operate as a Duplication With Comparison (DWC) redundant system [2].

In this case the EL will perform a safe shut down of the system if a new fault is detected in the DWC configuration. It has been assumed that the system can be reconfigured, during DWC operation, to the TMR configuration after a repair operation is performed on the faulty unit.

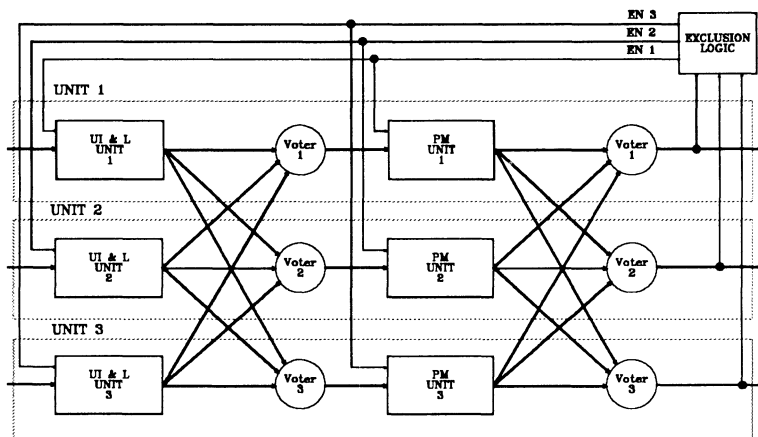


Figure 2: The Fail Safe Nucleus architecture.

4 Faults and Errors Detection in FSN

Figure 3 and Figure 4 report two Stochastic Petri Nets (SPN) which model the behaviour of the system when a fault occurs in one of the six subunits which compose the FSN. A fault free EL is assumed.

The SPN shown in Figure 3, represents the reconfiguration process when a fault occurs in one subunit when the system is in the TMR configuration.

The diagnostic fault coverage is assumed equal to C both for the UI&L and for the PM units. The failure rate of one single UI&L unit is assumed equal to $\lambda_{UI\&L}$ while λ_{PM} is the failure rate of one PM unit. The comparison

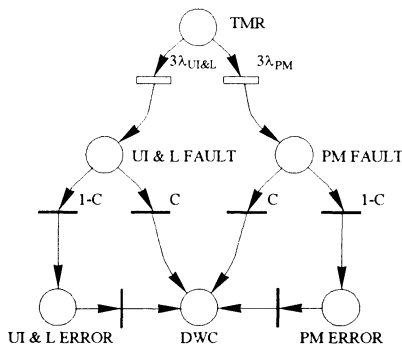


Figure 3: TMR to DWC reconfiguration.

coverage is assumed to be perfect: in this way if a fault goes undetected by the self diagnostics, the resulting error will be surely detected by the comparison process.

The SPN shown in Figure 4, represents the safe shut down process resulting from the occurrence of a fault when the system is in the DWC configuration. The SPN structure is the same of the net shown in Figure 3 and similar considerations can be

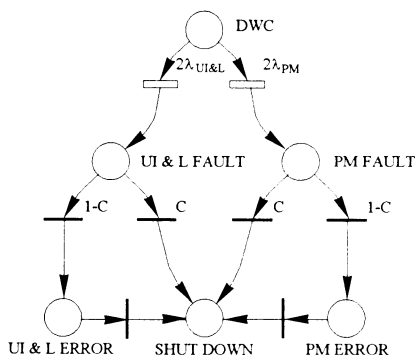


Figure 4: FSN safe shut down.

made. The only difference between the two SPNs is related to the coefficient which multiplies the failure rate of the single units: in the first case this coefficient is equal to 3 because three units are operating in TMR configuration, while in the second case the coefficient is equal to 2.

Because of the perfect fault coverage due to the perfect comparison coverage assumed, it is possible to simplify the structure of the SPNs as shown in the following paragraph.

5 Safety Model and Reliability Model of FSN

The complete SPN model of the FSN has to take into account both the possibility of performing maintenance operations on the FSN faulty unit and the eventuality of faults occurring in the EL circuits.

It is assumed that in case of an undetected fault in the EL, this unit doesn't modify its output, so only the occurrence of a further fault in a FSN unit could result in an unsafe failure.

It is also assumed that a maintenance operation requires a mean time to repair (MTTR) equal to $1/\mu$ hours, being μ the repair rate of the system.

Safety and reliability models are lightly different: the difference consists on the definition of the SPN absorbing markings, since in the reliability model the absorbing marking will be that one in which the system fails, without regard to nature of the failure, while in the safety model the absorbing marking will be that one in which the system fails unsafely. For this reason in the safety model a repair operation is assumed to be performed in the safe shut down status in order to bring the system in the TMR configuration, while in the reliability model both the safe and the unsafe failures collapse in one unique status.

Figure 5 and Figure 6 show the reliability and the safety models of the FSN unit respectively.

260 Railway Operations

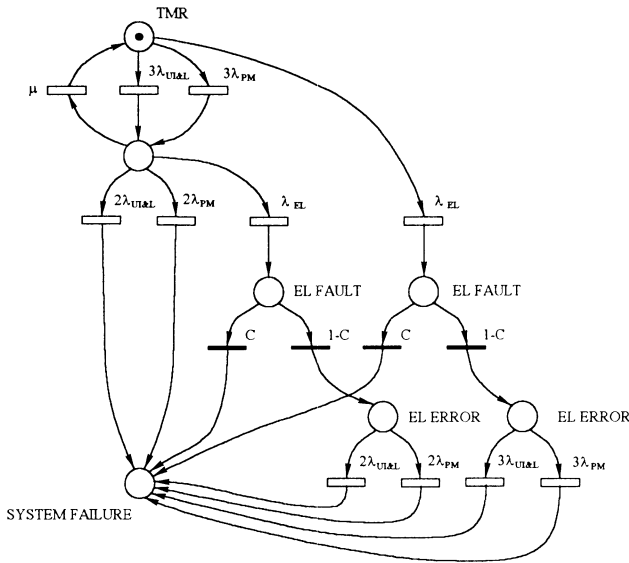


Figure 5: FSN reliability model.

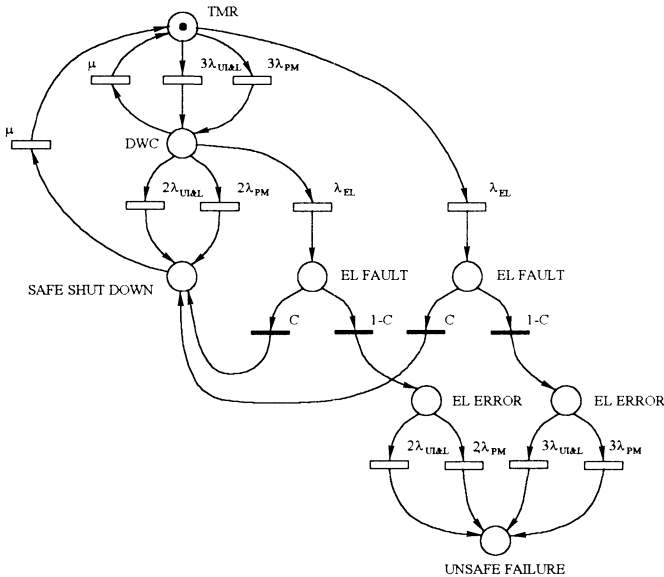


Figure 6: FSN safety model.

In the proposed representation, hollow boxes indicate timed transitions, with an exponential distributed firing time, and firing rate defined by the associated label, while thick bars represent immediate transitions with firing

probability defined by the associated label. Places and transitions are indeed represented with the usual Petri Nets notation.

6 Dependability measures

Dependability measures are computed by means of *Spnp Version 4.0*, a Stochastic Reward Nets solution tool. A Stochastic Reward Net [6] is a SPN in which at each of the valid markings, is associated an index named *reward rate*. For a generic valid marking i , a reward rate r_i is defined and, assuming $P_i(t)$ to be the probability that the marking i is verified at time t , it is possible to define a stochastic process $X(t)$ which denotes the system reward rate at time t . The following measures are then possible [4]:

$$E[X(t)] = \sum r_i P_i(t) \quad (1)$$

where $E[X(t)]$ is the expected reward rate at time t ;

$$E[X(\infty)] = \sum r_i \pi_i \quad (2)$$

where $E[X(\infty)]$ is the expected reward rate at steady state, being π_i the steady state probability of being in marking i ; and

$$E[Y(t)] = \sum r_i \int_0^t P_i(t) dt \quad (3)$$

where $E[Y(t)]$ is the expected accumulated reward rate up to time t .

The reward model of a system is useful for both performability and dependability measures. The analytical solver *Spnp* is able to provide the above mentioned measures by solving the underlying Markov Reward Process of the Stochastic Reward Net model of the system under analysis, allowing the user to perform both transient and steady state analysis.

Dependability is a term which groups reliability, availability and safety concepts; reliability $R(t)$, defined as the conditional probability that the system is correctly operating at time t given that it was operational at time 0 , and safety $S(t)$, defined as the probability that there is no unsafe failure until time t , are the measures performed in this paper on the FSN unit of the ACS system.

Steady state measures have been also performed, in particular Mean Time to Failure (*MTTF*), defined as

$$MTTF = \int_0^{\infty} R(t) \cdot dt \quad (4)$$

and Mean Time Between Hazardous Events (*MTBHE*) [3], defined as

$$MTBHE = \int_0^{\infty} S(t) \cdot dt \quad (5)$$

have been performed by using the *Spnp* utility which allows to compute Mean Time to Absorption (*MTTA*) when a steady state analysis is required.

262 Railway Operations

The computation of $R(t)$ and $S(t)$ has been possible by defining a reward rate equal to 1 only for the unique absorbing marking, respectively in the reliability and the safety SPN model, and 0 otherwise, obtaining in this way the values of $I-R(t)$ and $I-S(t)$.

7 Results

Figure 7 and Figure 8 show respectively the results of the reliability and of the safety analysis.

In Figures from 7a through 7c the results of the reliability transient analysis are shown; in all the tests the EL failure rate λ_{EL} is assumed to be constant and equal to $5 \cdot 10^{-7}$ faults/hour.

The diagram in Figure 7a represents the reliability $R(t)$ versus time t for values of $\lambda_{UI\&L} = \lambda_{PM}$ varying from 10^{-4} through 10^{-3} faults/hour. No repair operation ($\mu=0$) is considered in the DWC configuration.

In Figure 7b, is shown the same $R(t)$ versus t diagram considering a repair operation from the DWC configuration to the TMR configuration, with a repair rate μ equal to 10^{-1} repairs/hour.

A third $R(t)$ versus t diagram is shown in Figure 7c, in which is assumed a constant value for $\lambda_{UI\&L} = \lambda_{PM}$, equal to $5 \cdot 10^{-4}$ faults/hour, while the represented curves are computed for values of μ varying from $5 \cdot 10^{-2}$ through $5 \cdot 10^{-1}$ repairs/hour.

The diagram in Figure 7d represents the results of the steady state reliability analysis; the picture show the $MTTF$ versus the UI&L and PM failure rate $\lambda_{UI\&L} = \lambda_{PM}$ diagram for different values of the repair rate μ varying between $5 \cdot 10^{-2}$ and 10^{-1} repairs/hour.

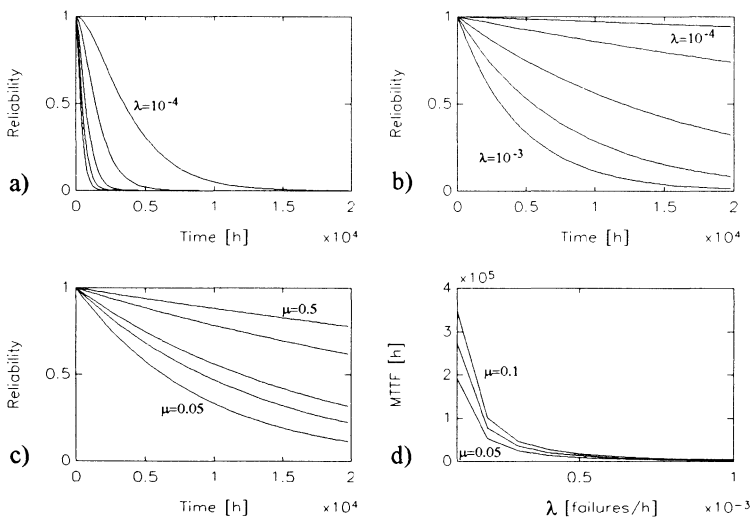


Figure 7: Reliability analysis results.

Figures 8a and 8b represent the safety transient analysis results; constant values for the UI&L and PM failure rate $\lambda_{UI\&L} = \lambda_{PM}$ and for the repair rate μ are assumed to be equal respectively to 10^{-3} faults/hour and to 10^{-1} repairs/hour.

Figure 8a shows the $S(t)$ versus t diagram for values of the EL failure rate λ_{EL} varying from 10^{-7} through 10^{-6} faults/hour and for a diagnostic fault coverage C equal to 0, while Figure 8b represents the same diagram but assuming a constant value for λ_{EL} equal to $5 \cdot 10^{-7}$ faults/hour and a diagnostic fault coverage C varying between 0.1 and 0.9.

Finally, in Figure 8c the steady state safety analysis results are shown. The $MTBHE$ versus λ_{EL} diagram is represented for different values of the diagnostic fault coverage C varying between 0 and 0.8.

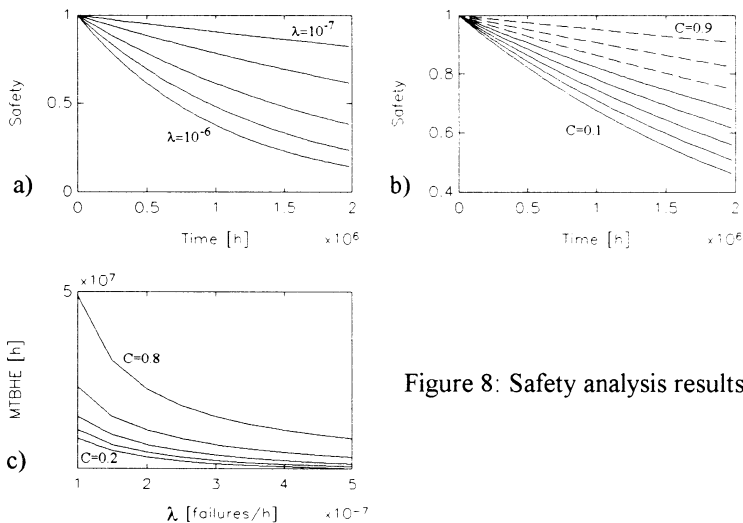


Figure 8: Safety analysis results.

Conclusions

The obtained results are related to parameters, such as failure rates and fault coverages, which are not the real values of the existing ACS system, but only reasonable values for such kind of devices.

In fact, during high level phases of the design process, an accurate knowledge of such parameters is impossible, because the detail of the design is still too low. For this reason analytic models of reliability and safety are considered only a means for investigate on what the designer has to do to better fit design specification, as far as dependability concerns.

The results presented in this paper suit these consideration showing how dependability measures are affected by chnges made on the key parametes, such as failure rates, fault coverages and repair rates. In particular, the results show



as a considerable improvement in safety could be obtained with a high fault coverage for the Exclusion Logic circuits, which failure rate is nevertheless higher than that of the other FSN subsystems. Similar considerations can be made on the reliability measure, which can be kept high if a repair is performed, in a rather short time, in the DWC configuration.

Furthermore, because of the particular structure of the system, and therefore of its SPN model, it must be noted that safety and reliability could be adjusted independently by tuning respectively the EL and the FSN computing subunits (UI&L and PM units) failure rates.

Such considerations could constitute useful guidelines for the lower level phases of the design process, indicating on which parameters the designer has to act and how to do this.

References

1. Milizia, E. L'ACEI elettronico, *La Tecnica Professionale*, 1992, Vol. 11, pp 6-16.
2. Johnson, B.W. Design and Analysis of Fault Tolerant Digital Systems, Chapter 3, *Design Techniques to Achieve Fault Tolerance*, pp 47-167, Addison-Wesley Publishing Company, 1989.
3. Bozzolo, D., Giras, T.C. & Profeta III, J.A. Comparative safety analysis of simplex, duplex and triplex hardware designs using Petri Nets, in *Convegno Sviluppo e Prospettive dei Trasporti Elettrificati: Ricerca ed Innovazione*, Vol. II, pp 359-368, *Proceedings*, Genova, Italy, 1992.
4. Tomek, L., Mainkar, V., Geist, R.M., Trivedi, K.S. Reliability modeling of life-critical, real-time systems, *Proceedings of the IEEE*, Vol. 1, 1994, 108-121.
5. Peterson, J.L. *Petri Net Theory and the Modeling of Systems*, Prentice Hall, Inc., Englewood Cliffs, 1981.
6. Muppala, J.K. Woollet, S.P. & Trivedi, K.S. Real time systems performance in the presence of failures, *Computer*, No. 5, 1991, pp 37-47.
7. Molloy, M.K. Performance analysis using Stochastic Petri Nets, *IEEE Transactions on Computers*, Vol. C-31, No. 9, 1982, pp 913-917.
8. Johnson, B.W. & Aylor, J.H. Reliability and safety analysis of a fault-tolerant controller, *IEEE Transactions on Reliability*, Vol. R-35, No. 4, 1986, pp 355-362.