Modelling and analysis of a scheduled maintenance system: a DSPN approach.

A.Bondavalli[1], R.Filippini[2]
[1] DSI, University of Florence, Via Lombroso 6/17 I-50134 Firenze, Italy {a.bondavalli.dsi.unifi.it}
[2] CNUCE Istituto del CNR, Via Vittorio Alfieri 1, 56010 Ghezzano (Pisa) Italy.

Maintenance is the main instrument to assure system quality service over time, despite of ageing and wearing of its components. The entire set of the maintenance actions (inspections, replacements, repair, refuelling etc.) carried out on a system during its operational life can be classified into preventive and corrective actions. The former are all those actions performed on the system according to a previously settled time scheduled program and represent the scheduled maintenance program. The latter represent the part of maintenance devoted to the emergency repair and restoration of the system (or just a part of it) each time a failure occurred.

It is good practice to minimize corrective maintenance by optimally tuning the scheduled maintenance program. Usually it means to find the proper set of actions and their timed sequence that best satisfy dependability requirements subject to budget constraints. In most cases this is a very though task involving a multi-parametric optimum problem whose solution needs an accurate knowledge of the system behaviour, usually represented by some model of the system and of its behaviour.

From the modelling point of view, a system under scheduled maintenance program (SMS) can be seen as a multiple phased system (MPS). Each phase is associated to the configuration of the system during some time interval (the part of the system being actually maintained or operational [1]), while the scheduled maintenance program drives phase changes. The behaviour of the system in each time period (phase) is governed by a complex stochastic process accounting for the simultaneous presence of the individual components failure processes and of maintenance actions, which depend on the phase performed. Under reasonable assumptions (constant failure rates and constant duration of the phases) we have a Markov process, in each phase, and a Markov regenerative process for the phase sequence. The state space modelling approach gives us the basis for the analytical solution of such a problem (Markov renewal theorem), nevertheless there remain computational obstacles due to the well know state-explosion problem that limits drastically the size of problem to be solved.

Starting from these considerations our work is directed towards the proposal of a new modelling approach and its experimentation for checking whether it can bring some advantages. This methodology relies upon Deterministic and Stochastic Petri Nets (DSPN) as a modelling formalism and on Markov Regenerative Processes (MRGP) for the model solution. Due to their high expressiveness, DSPN models are able to cope with the dynamic structure of MPS and allow defining very complex model in a concise way. These models are solved with a simple and computationally efficient analytical solution technique based on the divisibility of the MRPS underlying the DSPN of the MPS [2]. This approach is fully integrated in the DEEM tool [3], specifically tailored for the dependability modelling and evaluation of MPS. Using DEEM the model of a MPS is split into two logically distinct sub-nets, the Phase net (PhN) and the System net (SN). The Phase net represents the execution of the various phases, each of deterministic duration, while the System net represents the behaviour of the system components being subject to exponentially distributed failure/repair process. Thanks to a user-friendly graphical interface, the model itself can be easily modified. Moreover, the SN dependency from the marking of the PhN (i.e. the phase performed) permits to deal with almost all the SMS problems scenarios encountered in the literature.

The SMS problem we are attaching in this work is a case of a very critical system where the maintenance has to be executed on-line without interrupting the service provided. More precisely we are modelling and analysing the Reactor Protection System (RPS) in use at the Westinghouse's nuclear plants [4]. The service delivered from this system is to assure the safety function or protective action to the nuclear plant in order to prevent and reduce the risk of the potentially catastrophic events [5,6,7]. The safety function is associated to the execution of the reaction process shutdown thus reaching a safe

state. To accomplish this task, a set of process variables (temperature, pressure, etc…) are continuously monitored and elaborated. The system architecture is heavily redundant in each single part in order to minimize the probability to miss the shutdown request and the occurrence of spurious protective action caused by a wrong detection. Furthermore, the system is subject to a periodical scheduled maintenance program thus splitting its operational life in periods, the phases. To allow continuos delivery of the service, the program prescribes a proper alternation of the components to be inspected.

The most important dependability measure of such system is its availability to correctly perform the safety function when needed, in other words, the safety on demand. Previous studies used a fault tree modelling approach whose top event was the availability of the safety function [6] others collected a huge amount failure data of the system components [4]. We have instead built the DSPN model of the system: the PhN representing the timed sequence of phases and the SN representing the stochastic behaviour of the system in each phase. The most relevant aspects of our models are the following:

- we considered the failure of each component as random failure if involving only the single components and common failure if involving the similar components altogether.
- all the failure processes have been modelled as exponential and
- failures can be detected only under maintenance.
- maintenance is not perfect: there is a probability of not correctly detect and repair failed components.

The purpose of this work is twofold. On the one side we want to exercise our methodology, to check whether it can master real and complex SMS problems and compare its efficacy with traditional approaches (fault trees). On the other side, we want to investigate the problem of the optimal tuning of a maintenance program, giving a useful decision support tool to evaluate the system performance since the early design stage. Regarding to this last objective we are able to evaluate the availability of the safety function at time t, depending on one or more parameters, such as the maintenance frequency or the coverage of the failure detection so to discover the bottlenecks of the system. Moreover, we can analyse any cost function defined for the system, such as a combination of the risk associated to maintenance actions and the unavailability of the safety function.

One very interesting analysis concerns the optimal frequency of maintenance actions. Indeed, we know maintenance actions positively affect availability, in fact without maintenance the system performance degrades to unacceptable values. On the other side, during maintenance the system works in a less redundant configuration thus being less resilient to faults. In addition one may also consider a risk associated to maintenance operation and to reconfigurations contrasting the positive effects of maintenance.

At this point in time we have defined our DSPN models using DEEM and are refining them to account for more and more detailed phenomena. Moreover we have started some of the analyses described earlier with some promising results. We start understanding which are the critical parameters and the way they interplay in determining the system dependability figures. In conclusion, the DSPN approach, the methodology we are adopting and the DEEM tool appear to properly support the analysis of this kind of problems and we intend to check if it can represent an effective alternative to more traditional approaches.

References

[1] A.Bondavalli, I.Mura, K.Trivedi: "Dependability modelling and sensitivity analysis of SMS". EDCC-3 1999 pp.7-23.

[2] A.Bondavalli, I.Mura, X.Zang, K.Trivedi: "Dependability modelling and evaluation of Phased mission systems". *DCCA* 1999 pp.319-337.

[3] A.Bondavalli, I.Mura, S.Chiaradonna, R.Filippini, S.Poli, F.Sandrini: "DEEM: a tool for the dependability modelling and evaluation of MPS". *FTCS* 2000.

[4] "Reliability study: Westinghouse Reactor protection system". Idaho national engineering and environmental laboratory (INEEL), Lockeheed Martin Idaho technologies company. *NUREG/CR-5500* 1999.

[5] "Protection systems and related features in nuclear power plant: a safety guide". *International atomic energy agency* IAEA 1980.

[6] "IEEE guide for general principles of reliability analysis of nuclear power generating station protection systems". *IEEE inc*. 1975.

[7] J.McDermid: "Issues in the development of safety critical systems". Safety-critical systems. Autors F.Redmill, T. Anderson. *Chapman&Hall* 1990 pp.16-41.