DEEM: a Tool for the Dependability Modeling and Evaluation of Multiple Phased Systems

A. Bondavalli[1], I. Mura[2], S.Chiaradonna[3], R. Filippini[3], S.Poli[3], F. Sandrini[3]

[1] DIS, University of Florence, Via Lombroso 6/17 I-50134 Firenze, Italy {a.bondavalli@dsi.unifi.it}
[2] Motorola Technology Center, Via P.C. Boggio 65/A,10139 Torino, Italy
{Ivan_Mura@email.mot.com}
[3] CNUCE Istituto del CNR, Via Vittorio Alfieri 1, 56010 Ghezzano (Pisa) ITALY,

Abstract

Multiple-Phased Systems, whose operational life can be partitioned in a set of disjoint periods, called "phases", include several classes of systems such as Phased Mission Systems and Scheduled Maintenance Systems. Because of their deployment in critical applications, the dependability modeling and analysis of Multiple-Phased Systems is a task of primary relevance. However, the phased behavior makes the analysis of Multiple-Phased Systems extremely complex.. This paper is centered on the description and application of DEEM, a dependability modeling and evaluation tool for Multiple Phased Systems. DEEM supports a powerful and efficient methodology for the analytical dependability modeling and evaluation of Multiple Phased Systems, based on Deterministic and Stochastic Petri Nets and on Markov Regenerative Processes.

1 Introduction

Many systems devoted to the control and management of critical activities have to perform a series of tasks that must be accomplished in sequence. Their operational life consists of a sequence of non-overlapping periods, called *phases*. These systems are often called Multiple-Phased Systems (MPS). They include several classes of systems that have been object of active research during the last decades, such as those known as Phased Mission Systems (PMS) and Scheduled Maintenance Systems (SMS). MPS are very general, since their phases can be distinguished along a wide variety of differentiating features.

(1) During a specific phase, an MPS is devoted to the execution of a particular set of tasks, which may be different from the activities performed within other phases.

(2) The performance and dependability requirements of an MPS can be completely different from one phase to another.

(3) During some phases the system may be subject to a particularly stressing environment, thus experiencing dramatic increases in the failure rate of its components.

(4) In order to accomplish its mission, a MPS may need to change its configuration over time, to adopt the most suitable one with respect to the performance and dependability requirements of the phase being currently executed, or simply to be more resilient to an hazardous external environment.

(5) The successful completion of a phase, as well as the activities performed therein, may bring a different benefit to the MPS with respect to that obtained with other phases.

Many examples of MPS can be found in various application domains. For instance, systems for the aided-guide of aircraft, whose mission-time is divided into several phases such as take-off, cruise, landing, with completely different requirements. A very important sub-class of MPS is represented by the so-called Scheduled Maintenance Systems encountered in almost all the application domains where an artefact is to be used for long time and is periodically subject to maintenance actions. An SMS is easily formulated as a MPS considering that the system is run for a number of operational phases, and then undergoes a maintenance phase.

This paper describes DEEM (DEpendability Evaluation of Multiple-phased systems), the dependability modeling and evaluation tool specifically tailored for MPS, being currently developed by the University of Florence and CNUCE-CNR. DEEM supports the methodology proposed in [10] for the dependability modeling and evaluation of MPS. This methodology relies upon Deterministic and Stochastic Petri Nets (DSPN) as a modeling tool 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 concise models. DEEM models are solved with a very simple and computationally efficient analytical solution technique based on the separation of the MRGP underlying the DSPN of a MPS.

The paper is organized as follows. Section 2 describes the modeling features of DEEM and its Graphical User Interface, giving an overview of our DSPN approach. Section 3 describes the specialized solution algorithm implemented by DEEM, highlighting the advantages over previous general MRGP solutions. Then, Section 4 describes how DEEM works. Finally, our concluding remarks are given in Section 5, where we also discuss some possible extensions of the DSPN modeling methodology and the issues related to their inclusion in the DEEM solution technique.

2 The DEEM approach to model MPS

DEEM employs the DSPN formalism [1] for the modeling of MPS. DSPN models extend Generalized Stochastic Petri Nets and Stochastic Reward Nets, allowing for the exact modeling of events having deterministic occurrence times. A DEEM model may include immediate transitions, represented by a thin line, transitions with exponentially distributed firing times, represented by empty rectangles, and transitions with deterministic firing times, represented by filled rectangles.

Besides the introduction of deterministic transitions, DEEM makes available a set of modeling features that significantly improve DSPN expressiveness:

- firing rates of timed transitions may specified through arbitrary functions of the marking;
- arbitrary functions of the marking may be employed to include additional enabling conditions, named guards, to the specification of the transitions;
- rewards can be defined as arbitrary functions of the model marking;
- arc cardinalities may be expressed through marking-dependent functions.

This rich set of modeling features, accessible through a Graphical User Interface, provides DEEM with a general modeling scheme in which two logically separate parts are used to represent MPS models. One is the System Net (SN), which represents the failure/repair behavior of system components, and the other is the Phase Net (PhN), which represents the execution of the various phases, as described in Figure 1.

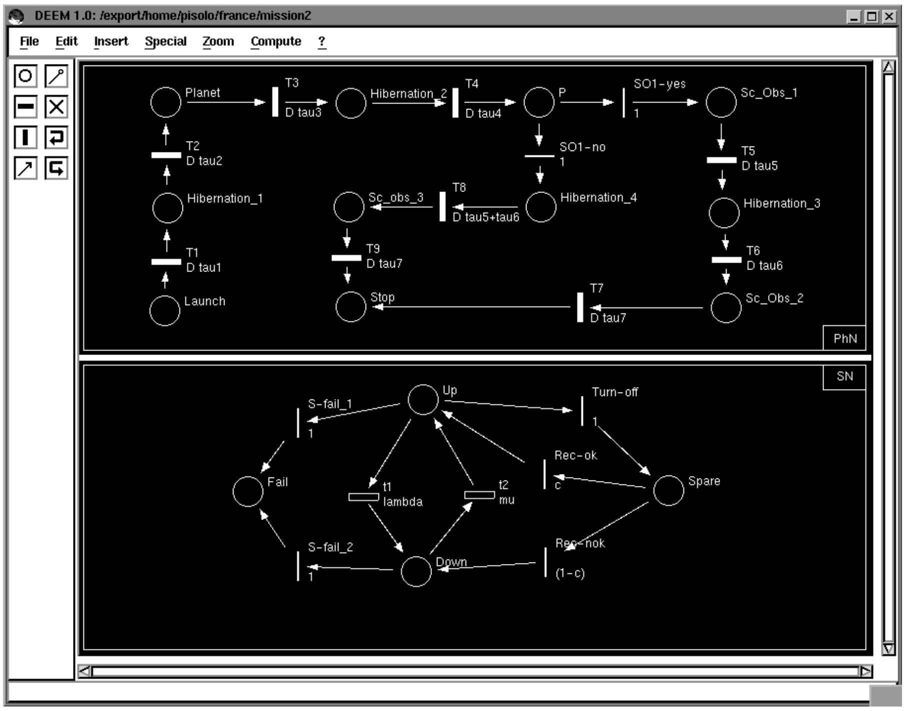
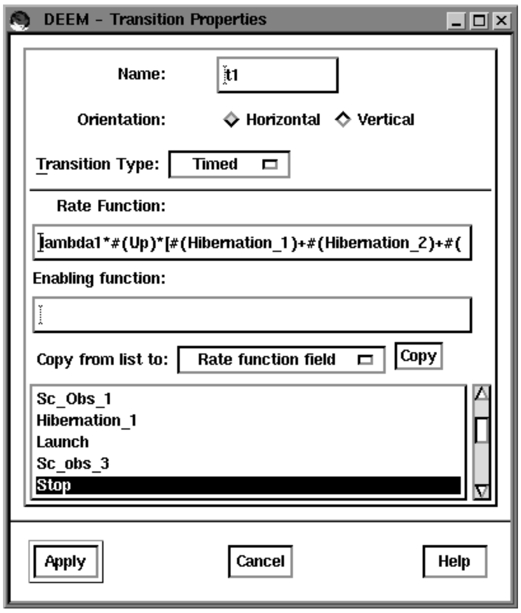


Figure 1: DEEM Interface and the DSPN model of the MPS in [10]

SN contains only exponentially distributed and immediate transitions, whereas the PhN contains all the deterministic transitions of the overall DSPN model and may as well contain immediate transitions. A token in a place of the PhN model represents a phase being executed, and the firing of a deterministic transition models a phase change.



Name: t1

Orientation: ◇ Horizontal ◇ Vertical

Transition Type: Timed

Rate Function:

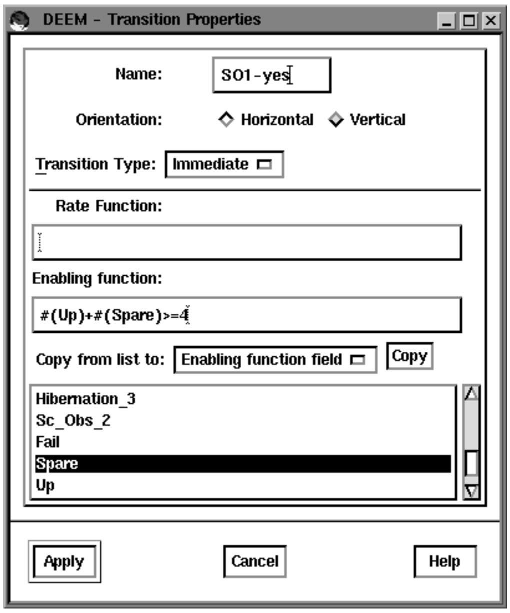
lambda1*#(Up)*[#(Hibernation_1)+#(Hibernation_2)+#(

Enabling function:

Copy from list to: Rate function field

Sc_Obs_1
Hibernation_1
Launch
Sc_obs_3
Stop

Figure 2: Property windows associated to Transition t1



Name: SO1-yes

Orientation: ◇ Horizontal ◇ Vertical

Transition Type: Immediate

Rate Function:

Enabling function:

#(Up)+#(Spare)>=4

Copy from list to: Enabling function field

Hibernation_3
Sc_Obs_2
Fail
Spare
Up

Figure 3: Property windows associated to TransitionSO1-yes

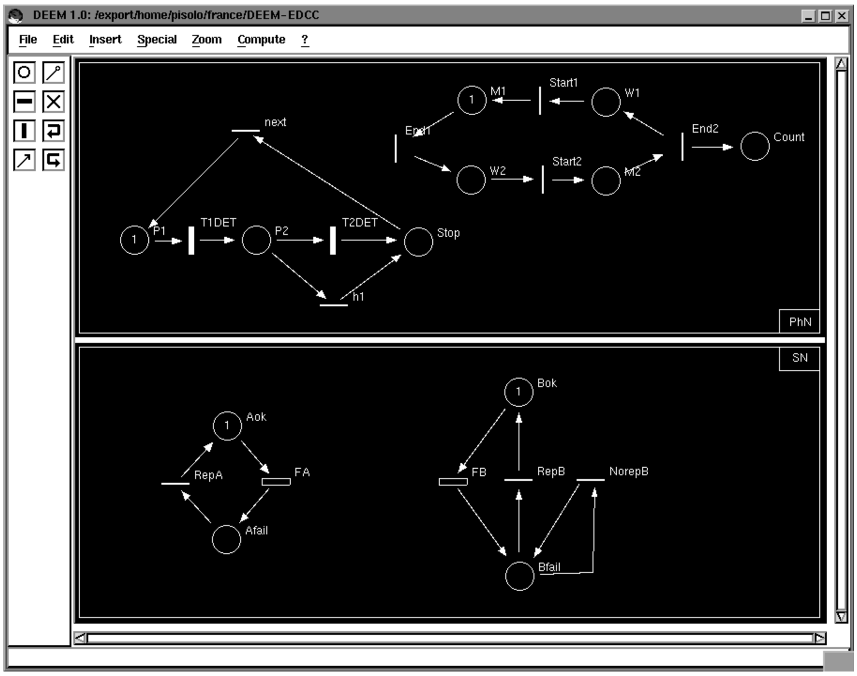


Figure 4: DEEM Interface and the DSPN model of the MPS in [5]

Each net is made dependent on the other one by marking-dependent predicates which modify transition rates, enabling conditions, reward rates, etc., to model the specific MPS features. Marking dependent attributes of the various objects (arcs, places and transitions) can be defined through the DEEM property window associated to each object. Figure 2 shows the window associated to transition T1 of the SN of Figure 1, while Figure 3 shows that associated to transition SO1-yes of the PhN.

Phase-triggered reconfigurations, which add a significant complexity to the treatment of dependencies among phases, are easily handled by DEEM through the implicit mapping which is embedded in the model (as in [2; 4; 7; 12]). Any structure of the SN sub-model can be considered, whereas the DSPN of the PhN must possess distinct markings corresponding to different phases. This limitation is introduced because the DEEM solution algorithm focuses on the time-dependent evolution of the MPS, and thus requires to distinguish the sequence of phases performed during the MPS history. DEEM is able to automatically recognize MPS models that are amenable to analytical solution from those that violate the required assumptions. The transient solution allows to evaluate the dependability related measures at specific time instants, thus providing a means to estimate the probability of successful mission completion, the relative impact of each single phase on the overall dependability figures, etc.

Notice that the constraint on the PhN still allows for quite general structures of the sub-model. In particular, the PhN is not limited to have a linear structure, but it may take a tree structure with a dynamic choice of the next phase to perform (using enabling guards) to model a dynamic profile of the mission. It may have a cyclic structure as well, provided that the marking includes enough information to distinguish phases performed within a cycle from those executed within another one, as exemplified in Figure 4.

3 The DEEM specialized analytical solution

DEEM provides a specific and efficient analytical solution for MPS models. We briefly recall the background mathematics and then describe the solution algorithm.

3.1 The analytical technique

The specialized solution finds its ground by observing that the only deterministic transitions in a DSPN model of a MPS are the phase duration, and that these transitions are enabled one at the time. Thus, the marking process $\{M(t), t \geq 0\}$ of the DSPN is a Markov Regenerative Process (MRGP) [6] for which the firing times of the deterministic transitions are indeed regeneration points. Moreover, the following property holds of the DSPN model of a MPS:

Property 1: in every non-absorbing marking of the DSPN there is always one deterministic transition enabled, which corresponds to the phase being currently executed.

The general solution method for MRGP processes considers computing matrix $V(t)$, whose entry $\vec{m}, \vec{m}'$ is the occupation probability of marking $\vec{m}'$ at time $t \geq 0$ given the initial marking $\vec{m}$. Matrix $V(t)$ is the solution to the generalized Markov renewal equation $V(t) = E(t) + K(t) * V(t)$, where $K(t)$ and $E(t)$ are the global and local kernel matrices [6] and '*' is the convolution operator. Instead of directly attacking the solution of the generalized Markov renewal equation by numerical algorithms or Laplace-Stiltjes transform, DEEM computes matrix $V(t)$ according to the following analytical method, proposed in [10].

Let S denote the state space of the MRGP process, let $1, 2, \ldots, n$ be the set of phases the MPS can perform, and finally let τ_i denote the duration of phase i, $i = 1, 2, \ldots, n$. Consider the following subsets of S:

$$S_i = \{\vec{m} \in S \mid \textit{phase } i \textit{ is being performed, } i = 1, 2, \ldots, n\}$$

$$S_{n+1} = \{\vec{m} \in S \mid \textit{no phase is being performed}\}$$

Owing to **Property 1**, and because different phases correspond to distinct markings of the DSPN model, sets S_i, $i = 1, 2, \ldots, n+1$, are a partition of the marking space S. The stochastic process $\{M_i(t), t \geq 0\}$, defined as the restriction of the MRGP within the execution of phase i, is a continuous-time Markov chain with state space S_i, $i = 1, 2, \ldots, n$. Denote with Q_i the transition rate matrix of $\{M_i(t), t \geq 0\}$, $i = 1, 2, \ldots, n$. The transient analysis of the MRGP is carried out by separately considering the evolution of the processes $\{M_i(t), t \geq 0\}$.

Consider the block structure that is induced on matrix $V(t)$ as a result of the marking space partitioning. Each block $V_{i,j}(t)$ is separately computed as follows. Consider the unique path $p(i, j)$ that links phase i to phase j according to the structure of the PhN. This path is a set of phases $p(i, j) = \{p_1, p_2, \ldots, p_r\}$, with $p_1 = i$, and $p_r = j$. Block $V_{i,j}(t)$ is given by:

$$V_{i,j}(t) = \left(\prod_{h=1}^{r-1} e^{Q_{p_h} \tau_{p_h}} \Delta_{p_h, p_{h+1}} \right) e^{Q_j \delta} \qquad (1)$$

where $\delta = t - \sum_{h=1}^{r-1} \tau_{p_h}$, and $\Delta_{p_h, p_{h+1}}$, $h = 1, 2, \ldots, r-1$ is the branching probability matrix, whose entry $\Delta_{\vec{m}, \vec{m}'}^{p_h, p_{h+1}}$ is defined as the probability that $\vec{m}'$ is the initial marking of phase p_{h+1}, given that $\vec{m}$ is the marking at the end of phase p_h.

3.2 The solution algorithm

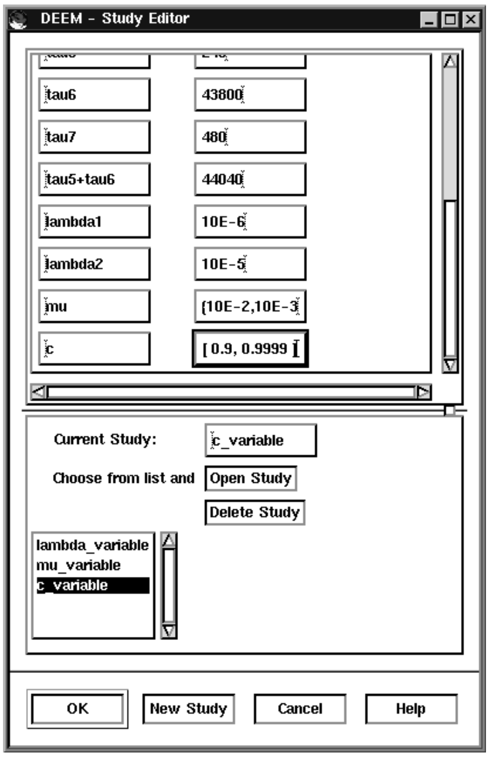
Equation (1) allows to evaluate $V(t)$ through the separate analysis of the various alternative paths which compose the mission, and only requires the derivation of matrix exponentials $e^{Q_i t}$, and branching probability matrices $\Delta_{i,j}$, $i,j = 1,2,\ldots,n$, which can be automatically obtained when the reachability graph is generated. The solution of the DSPN model is thus reduced to the cheaper problem of solving a set of homogeneous, time-continuous smaller Markov chains.

To compute a block $V_{i,j}(t)$ and then the dependability figures of the system, the solution engine of DEEM takes as input the DSPN model and its initial probability vector, and performs the following steps:

1) Builds RGP, the reachability graph of the PhN sub-model. This graph has exactly one stable marking $\dot{m}_i$ for each phase i the MPS may perform.
2) For each stable marking $\dot{m}_i$ in RGP, builds the reachability graph RGS($\dot{m}_i$) of the whole DSPN model when marking $\dot{m}_i$ is the only one permitted for the PhN. From RGS($\dot{m}_i$) obtains the transition rate matrix Q_i of the continuous-time Markov chain describing the evolution of the DSPN during the execution of phase i.
3) For each pair of stable marking $\dot{m}_i$ and $\dot{m}_j$ in RGP, such that marking $\dot{m}_j$ is reachable from $\dot{m}_i$ through the single firing of some deterministic transition $t_{i,j}^{Det}$, builds the reachability graph RGS($\dot{m}_i, \dot{m}_j$) of the whole DSPN model, when the initial marking of the PhN is $\dot{m}_i$, and transition $t_{i,j}^{Det}$ is the only one allowed to fire. From RGS($\dot{m}_i, \dot{m}_j$) obtains the branching probability matrix $\Delta_{i,j}$ for the transition from phase i to phase j.
4) Multiplies the matrix exponentials and the branching probability matrices, according to the order given by Equation (1), to obtain matrix $V_{i,j}(t)$.
5) Evaluates the specific dependability measure of interest for the MPS from the initial probability vector and $V_{i,j}(t)$, according to the standard computation algorithms.

4 DEEM at work

As already described in Section 2, DEEM possesses a GUI inspired by [3] and realized using an X11 installation with Motif runtime Libraries which the user employs to define his model of a MPS. We remark that while building the models, the attributes of the model objects, like rates or probabilities, can be expressed through parameters rather than numerical values directly. Therefore, prior to proceed to the model evaluation (‘Transient Analysis’ in the ‘Compute’ Menu), the user has to assign values to the parameters. DEEM automatically builds a parameter table collecting all the symbols defined in the model. This table is made accessible through the command ‘Parameters’ in the ‘Compute’ Menu, as described in Figure 5.



tau6	43800
tau7	480
tau5+tau6	44040
lambda1	10E-6
lambda2	10E-5
mu	{10E-2,10E-3
c	[0.9, 0.9999

Current Study: c_variable

Choose from list and

lambda_variable
mu_variable
c_variable

Figure 5: Parameters window with one study for the example in Figure 1.

Many studies can be defined, each represented by a column in the table. In each study one parameter is allowed to take a range of values and another parameter to take a set, this way a family of curves can be obtained by the evaluation of a single study. The specific dependability measure of interest for the MPS evaluation is defined through the general mechanism of marking-dependent reward functions (‘Set Reward Function’ in the ‘Compute Menu’).

Then the evaluation can be launched (on the selected study) and the algorithm described in Section 3 is executed. Values are returned in a file which can be further elaborated for producing plots or tables of the dependability measures.

The main computational cost of the DEEM solution algorithm is that required for the transient solutions and the multiplications in step 4) of the algorithm sketched in the previous section. Notice that the DEEM approach to generate the required matrices ever requires to handle the entire state space of the MRGP process. Thus, DEEM is able to deal with all the scenarios of MPS that have been analytically treated in the literature, at a cost which is comparable with that of the cheapest ones [9; 11; 13], completely solving the issues posed by the phased-behavior of MPS.

It is worthwhile remarking the advantages DEEM offers for the modeling and evaluation of MPS when compared to general-purpose DSPN tools (such as DSPNexpress 2.000 [8]). On the modeling side, the tool GUI allows defining the PhN and SN sub-models to neatly model the phase-dependent behaviors of MPS. On the evaluation side, the specialized separate algorithm implemented by DEEM results in a relevant reduction of the MPS model solution time.

5 Concluding remarks

This paper focused on the description of DEEM, the dependability modeling and evaluation tool specifically tailored for Multiple Phased Systems, being currently developed by the University of Florence and CNUCE-CNR. DEEM supports the methodology proposed in [10] for the dependability modeling and evaluation of MPS. Modeling is based on Deterministic and Stochastic Petri Nets, able to cope with the dynamic structure of MPS, and on a set of modeling features that significantly improve the expressiveness allowing for the definintion of very concise models. DEEM models are then solved with a very simple and computationally efficient analytical solution technique based on the separation of the MRGP underlying the DSPN of a MPS. DEEM deals with all the scenarios of MPS that have been analytically treated in the literature, at a cost that is comparable with the cheapest ones, completely solving the issues posed by the phased-behavior of MPS.

We intend to extend DEEM capabilities for analyzing a wider class of Systems. The first step will consist in moving from DSPN to Markov Regenerative Stochastic Petri Net (MRSPN). MRSPN models, characterized by having a Markov Regenerative Process as their underlying stochastic marking process, allow the tractability of MPS having random (instead of constant) phase duration. The modeling of non-exponential intra-phase activities will be the next step. To deal efficiently with intra-phase models other than time-homogeneous Markov chains, we are developing a specialization of the Markov Regenerative Process (MRGP) theory driven by the peculiar characteristics of MPS.

DEEM will be made available soon to the academic world, for information see http://bonda.cnuce.cnr.it.

References

[1] M. Ajmone Marsan and G. Chiola, “On Petri nets with deterministic and exponentially distributed firing times,” in “Lecture Notes in Computer Science 266”, Ed., Springer-Verlag, 1987, pp. 132-145.

[2] M. Alam and U. M. Al-Saggaf, “Quantitative Reliability Evaluation of Reparaible Phased-Mission Systems Using Markov Approach,” IEEE Transactions on Reliability, Vol. R-35, pp. 498-503, 1986.

[3] S. Allmaier and S. Dalibor, “PANDA - Petri net analysis and design assistant,” in Proc. Performance TOOLS’97, Saint Malo, France, 1997.

[4] B.E. Aupperle, J.F. Meyer and L. Wei, “Evaluation of fault-tolerant systems with non-homogeneous workloads,” in Proc. IEEE FTCS-19 Fault Tolerant Computing Symposium, 1989, pp. 159-166.

[5] A. Bondavalli, I. Mura and K. S. Trivedi, “Dependability Modelling and Sensitivity Analysis of Scheduled Maintenance Systems,” in Proc. EDCC-3 European Dependable Computing Conference, September 15-17,Prague, Czech Republic, 1999, pp. 7 – 23 (also Lecture Notes in Computer Science N. 1667)

[6] H. Choi, V.G. Kulkarni and K.S. Trivedi, “Transient analysis of deterministic and stochastic Petri nets.,” in Proc. 14th International Conference on Application and Theory of Petri Nets, Chicago Illinois, USA, 1993, pp. 166-185.

[7] J. B. Dugan, “Automated Analysis of Phased-Mission Reliability,” IEEE Transaction on Reliability, Vol. 40, pp. 45-52, 1991.

[8] C. Lindemann, A. Reuys and A. Thummler, “DSPNexpress 2.000 Performance and Dependability Modeling Environment,” in Proc. IEEE FTCS-29 Fault-Tolerant Computing Symposium, June 15-18, Madison, Wisconsin, USA, 1999, pp. 228-231.

[9] J.F. Meyer, D.G. Furchgott and L.T. Wu, “Performability Evaluation of the SIFT Computer,” in Proc. IEEE FTCS’79 Fault-Tolerant Computing Symposium, June 20-22, Madison, Wisconsin, USA, 1979, pp. 43-50.

[10] I. Mura, A. Bondavalli, X. Zang and K. S. Trivedi, “Dependability Modeling and Evaluation of Phased Mission Systems: a DSPN Approach,” in Proc. DCCA-7 Dependable Computing for Critical Applications, San Jose CA, 1999, pp. 319—337.

[11] I. Mura and A. Bondavalli, “Hierarchical Modelling and Evaluation of Phased-Mission Systems,” to appear in IEEE Transactions on Reliability, Vol. 48, December 1999.

[12] M. Smotherman and K. Zemoudeh, “A Non-Homogeneous Markov Model for Phased-Mission Reliability Analysis,” IEEE Transactions on Reliability, Vol. 38, pp. 585-590, 1989.

[13] A. K. Somani, J. A. Ritcey and S. H. L. Au, “Computationally-Efficent Phased-Mission Reliability Analysis for Systems with Variable Configurations,” IEEE Transactions on Reliability, Vol. 41, pp. 504-511, 1992