Markov Regenerative Stochastic Petri Nets to Model and Evaluate the Dependability of Phased Missions

Ivan Mura and Andrea Bondavalli, *Member, IEEE Computer Society*

Abstract

This study deals with model based dependability analysis of phased mission systems. From a comprehensive review of the studies in the literature, it appears that several aspects of multi phased systems still pose insurmountable problems for the dependability evaluation methods and tools. To address the weak points of the state-of-the-art we propose a modeling methodology that exploits the power of the class of Markov regenerative stochastic Petri net models. Our approach considerably enlarges the class of phased mission systems that can be analytically studied. It can accommodate in a compact and neat modeling all those peculiar aspects of phased mission systems that could not be dealt with up to now. By taking advantage of the special structure of phased mission systems, we develop an analytical solution technique with a low computational complexity, basically dominated by the cost of the separate analysis of the system inside each phase. Last, the existence of analytical solutions allows us to derive the sensitivity functions of the dependability measures, thus providing the dependability engineer with additional means for the study of phased mission systems.

Index Terms: Phased Mission Systems, Markov Regenerative Stochastic Petri Nets, Analytical modeling and evaluation, Sensitivity analysis

1 Introduction

In this paper we address the analytical dependability modeling of a class of systems that in the literature are known as Phased Mission Systems (PMS, hereafter). PMS perform a series of tasks that must be accomplished in sequence. Their operational life thus consists

of a sequence of non-overlapping periods, called "phases". During a specific phase, a PMS is devoted to the execution of a particular set of tasks, which may be completely different from those performed within other phases. The performance and dependability requirements of a PMS can be utterly different from one phase to another. Moreover, during some phases the system may be subject to particularly stressing environments, thus experiencing dramatic increases in the failure rate of its components. To accomplish its mission, a PMS 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.

Examples of PMS can be found in various application domains. A typical class of PMS frequently found in the literature is represented by the on-board systems for the aided-guide of aircraft, whose mission consists of take-off, ascent, cruise, approach, landing phases. A PMS analysis can be also applied to studying the dependability of a system during its whole life-cycle to establish a proper schedule of maintenance operations. In this context, we talk of the Scheduled Maintenance System (SMS) problem. Another typical example of PMS is provided by the computing systems embarked on long-life spacecraft, which must survive long periods of very low activity, and then are required to achieve the scientific goals of the mission in a short period of intense solicitation.

Besides these classical examples of PMS, there are many other kinds of systems not generally classified as such, that are conveniently reformulated as PMS, and then can be modelled and studied by using the specific methodologies for PMS. More precisely, we are considering systems having a phased mission, for which the phase ordering is dynamically determined by the environment the system is embedded in, or by particular sequences of faults. Real-time systems with "multi-moded" behavior represent good examples of these PMS-like systems.

Because of their deployment in critical applications, the dependability modeling and analysis of PMS is an issue of primary relevance that has been widely investigated. However, due to their dynamic behavior, PMS offer challenges in dependability modeling and

evaluation. The methods proposed in the literature make several restrictive assumptions, which may result in an excessively unrealistic modeling and thus may undermine the confidence that can be put in the analysis result.

In this paper we propose a new methodology for the modeling and evaluation of PMS, based on a Markov Regenerative Stochastic Petri Nets (MRSPN) approach. Our proposal overcomes some of the applicability limits of the previous methods, greatly enlarging the class of PMS that can be analytically studied. In particular, the MRSPN modeling allows relaxing two kinds of assumptions that are typically made by the other approaches for the sake of analytical tractability, and which may result in unreliable estimation of system dependability attributes.

The first concerns the duration of phases, which are usually assumed to last for deterministic periods of time. While this assumption may be realistic for certain PMS scenarios, as for instance space applications where phases are typically pre-planned on ground, it is certainly not appropriate for other classes of PMS, for which the starting and ending of a phase are instead triggered by unpredictable events. On the other hand, considering a constant phase duration enables a comparatively simple solution of the models, whereas dealing with random duration makes the analysis considerably more complicated. The MRSPN methodology we are going to present here accommodates phases of random duration, still providing exact and efficient analytical solutions.

The second kind of approximation is introduced to keep the intraphase model within the boundaries of time-homogeneous Markov chains, thus exploiting the efficient and well experienced solution techniques available for this class of stochastic processes. This requires all the timed activities of the system to be modeled by negatively distributed exponential random variables, no matter which kind of distribution they actually follow; further approximations are thus introduced inside the models. The MRSPN approach relaxes this assumption, allowing for more general intraphase processes.

All those scenarios of PMS previously accommodated by the various studies in the literature are within the applicability limits of our MRSPN approach. Much more, in the

paper we show how well the MRSPN models can deal with those features of PMS that could not be accommodated beforehand. Moreover, thanks to the existence of analytical solutions, we are able to perform the analytical sensitivity study of PMS, a challenging task entirely neglected in the literature.

Another relevant contribution of this paper is found in the specialization of the Markov Regenerative Process (MRGP) theory for the solution of MRSPN models of PMS. We reduce the computational complexity of the analytical solution to the one needed for the separate solution of the PMS inside the different phases, and develop an evaluation procedure that easily lends itself to automation. Hence, the issues introduced by the phased behavior are solved without requiring additional computational costs, the applicability of our approach being only limited by the size of the biggest Petri net model which can be handled by the dependability evaluation tools.

This paper is organized as follows. Section 2 identifies the contribution offered by the MRSPN approach with respect to the current state-of-the-art. In Section 3 we introduce the MRSPN modeling approach, and apply it to an example of PMS that serves as a case study throughout the paper. The general analytical solution of the MRSPN models of PMS is then discussed in Section 4, and several specializations of that solution technique are given in Section 5 for special PMS instances. Section 6 addresses the task of analytical sensitivity analysis of PMS. Section 7 provides guidelines for the practical utilization of the modeling methodology and the theoretical results presented in the paper, and also reports the numerical evaluation of some dependability attributes for the considered example of PMS. Last, conclusions are given in Section 8.

2 Our contribution to PMS dependability analysis

PMS have been widely investigated over the past decades. Many works have been proposed, either based on combinatorial models, such as Fault Trees and Reliability Block Diagrams e.g. [12, 20], or on state space oriented models, such as Markov chains and

various classes of Petri nets [1, 2, 5, 10, 14, 18, 19, 15]. Because of their ability in representing complex dependencies among system components, state space approaches offer the potentialities needed to address the features of the most complex instances of PMS.

However, several aspects of PMS represent a source of formidable problems even for the powerful state space based modeling and analysis techniques. To identify the limits of such methods and to highlight the advantages offered by our new MRSPN approach, we present in the following a series of system scenarios that progressively include more and more features of realistic PMS. For each scenario of PMS, we discuss on which methodologies are able to deal with the particular case.

Scenario 1. Consider first a PMS that has to perform a set of phases of constant duration in a given, fixed order, and for which the intraphase behavior is satisfactorily modeled by a time-homogeneous Markov chain. This scenario of PMS represents in a sense the common ground for the methods in the literature: all of them address this minimal instance of PMS and are able to deal with it. Some of the methods provide more flexibility/reusability, others are more efficient at solution time; a comprehensive review and comparison can be found in [15]. Our MRSPN approach easily accommodates this PMS scenario, as well. More precisely, in this particular case our methodology simplifies to that presented in [15], which is based on Deterministic and Stochastic Petri Nets (DSPN), and which was shown to provide several advantages with respect to the other approaches, concerning both the modeling and the evaluation aspects.

Scenario 2. Consider now a mission for which different goals are defined, some of primary and others of secondary relevance. In this scenario it is natural to endow the PMS with the ability of dynamically adapting the mission profile, by selecting which phase to perform next at the time the preceding phase ends. For instance, phases performed to reach secondary goals may be skipped in favor of the more important primary ones, depending on particular events occurred during PMS life-time. The mission profile is in this case represented by a tree of possible choices, rather than a chain as it is in the case of a predefined sequence of phases. Even if the assumptions of constant phase duration and

Markov intraphase process are kept, this flexibility feature exceeds the modeling and solution capabilities of most of the methods proposed, with the exception of [5]. The MRSPN methodology is able to account for adaptive mission profiles, including those in which phases already initiated can be shortened or even prematurely aborted. These latter features were not taken into account by any of the methods in the literature.

Scenario 3. Consider now a PMS whose phase changes are triggered by unexpected events, such as a fault leading to the removal of a system component, or the arising of an emergency situation of operation. This turns out in phases of random duration, whose initial and ending time instants may be unknown. When phases of random duration are to be considered, an exact analysis becomes much more complicated [3], even if the intraphase process is still a time-homogeneous Markov process. Just to give a clue of the difficulties of the analysis, notice that in this scenario the actual phase completion times, and thus the mission ending time, are unknown. If negative exponential distributions adequately represent the phase duration, then they can be employed to build an overall model of the PMS that still enjoys the Markov property at any point in time, for which the Markov solution techniques apply. However, there are classes of distributions that are not suitably modeled by exponential distributions, e.g. finite support distribution with low variance. Among those studies that addressed the modeling of PMS with random phase duration, some adopted an approximate solution approach (without any bound on the error introduced), such as [1, 19], others resorted to the numerical solution of an associated set of differential equations [18], others ended in a simulative solution [3]. Our MRSPN approach supports the modeling and the exact analytical evaluation of PMS for which the duration of the phases is drawn from the family of distributions that admit an analytical Laplace transform, which encompasses the exponential, deterministic, uniform, Coxian, phase-type distributions.

Scenario 4. Suppose now that modeling the intraphase behavior of a PMS through an homogeneous Markov chain does not result in a realistic representation of system behavior. For instance, consider a PMS in which failed components are replaced, so that

they are only unavailable for a deterministic amount of time. Fixed-duration activities are a good example of those finite support distributions with a low variance (the variance is null in the particular case) mentioned above, for which an approximation with negatively exponentially distributed random variables may results in significant discrepancies between the behavior of the real system and that of the modeled one. Among the methods that appeared in the literature, only the one reported in [18] is concerned with more general intraphase processes. The authors proposed building a non-homogeneous Markov model of the PMS, in which time varying failure and repair behavior are easily modelled. However, the adopted solution approach requires a computational cost that makes it practically feasible only for very simple PMS. The MRSPN approach allows considering general intraphase stochastic processes, where timed non-exponential activities are exactly modeled. The intraphase time-homogeneous Markov chain just becomes a particular case. The limit of practical applicability of our results is represented by the possibility of computing the transient solution of the intraphase process. Under given assumptions about the type of non-exponential activities included in the intraphase process, we provide an exact analytical solution of the models. In case such assumptions are not satisfied, an approximate solution technique is still applicable, which provides upper and lower bounds on the exact results. The accuracy of the approximation can be improved to reduce the gap between the bounds, accepting an increased computational cost.

To complete the matching between the set of possible PMS scenarios and the methods that apply for their solution, consider the following assumptions:

assumption a) the duration of the phases is deterministic;

assumption b) the mission profile is static;

assumption c) each intraphase process is a time-homogeneous Markov chain.

Denote a PMS scenario with the corresponding letters of the assumptions it satisfies, so that "abc" is the PMS corresponding to the first scenario among those listed above, "ac" to the second one, and "-" is the most general scenario of PMS where assumption a, b, and c have all been relaxed.

	abc	ab	ac	bc	a	b	c	"-"
Meyer et al. 1979 [14]	√							
Arlat et al. 1986 [2]	√							
Alam et al. 1986 [1]	√			√				
Smotherman et al. 1989 [18]	√	√		√		√		
Aupperle et al. 1989 [3]	√							
Dugan 1991 [10]	√							
Somani et al. 1992 [19]	√			√				
Bondavalli et al. 1997 [5]	√		√					
Mura et al. 1999 [15]	√		√					
This approach	√	√	√	√	√	√	√	√

Table 1: Applicability of the methods for PMS analysis

Table 1 shows the applicability limits of the state-space based modeling methodologies appeared in the literature, and points out the generality of our MRSPN approach. Besides greatly enlarging the class of PMS that are analytically tractable, the MRSPN methodology also allows addressing the sensitivity analysis of PMS, a challenging task that has been neglected in the literature. Indeed, thanks to the existence of explicit analytical solutions, we are able to analytically compute the derivatives of the dependability measures with respect to the variations of the parameter of interest.

3 MRSPN modeling of PMS

Modeling the complex dynamic behavior of PMS requires employing highly representative and expressive tools. To attack the problem, we resort to the MRSPN models, and couple their representative power with the a set of modeling features that significantly improve their expressiveness and allow for a compact modeling of the PMS peculiar aspects. MRSPN are defined as follows:

Definition 1 *A Petri net is a MRSPN if its underlying marking process is a Markov regenerative process (MRGP) [8].*

Definition 1 does not give an immediate description of the modeling features allowed for the MRSPN, this will be clarified later in the paper when the exact definition of MRGP is given. For the time being, it is enough to anticipate that Markov processes are special cases of MRGP, and thus the SPN and GSPN classes of Petri nets belong in fact to the MRSPN

class. Also, the set of DSPN for which an analytic solution method exists is included in the MRSPN. Moreover, MRGP encompass the class of semi-Markov processes, too, for which activities having generally distributed duration are allowed. Thus, MRSPN may include exponential, instantaneous, deterministic, as well as general transitions. However, to guarantee that the marking process is indeed a MRGP, some restrictions must be imposed on the concurrent enabling of the non-memoryless transitions. We shall come back to this issue later when dealing with the analytical solution.

The following modeling features have been recently added to the Petri net models to increase the expressive power. The firing rates of timed transitions, as well as the rewards associated to the markings of the Petri net, may depend on the marking of the model, which permits to model very complex behaviors in an extremely compact way. It is worth observing that the possibility of defining marking dependent firing rates allows modeling phases whose duration can be modified after they have already started. Another very interesting possibility to enrich the capabilities of Petri nets is the introduction of logic conditions, also called guards, which control the enabling of transitions. A guard can be any function of the marking of the model, which is added to the specification of the transition without impairing the clearness of the modeling. Input arcs with variable cardinality provide additional simplifications of the modeling. Besides a clearer and more concise modeling, these capabilities avoid the introduction of many vanishing markings that need to be subsequently eliminated from the reachability graph of the models. However, it is worthwhile observing once again that these features do not increase the power and thus the applicability of the models, but represent only convenient shorthand notations that simplify the modeling and generation of the underlying marking process.

We present the guidelines for the MRSPN modeling of PMS through an example of PMS application, which includes most of the typical features of the PMS that pose issues to the modeling and evaluation methodologies.

3.1 A challenging PMS example

We consider a PMS that executes 4 phases whose duration is a random variable having general distribution $F_i(t)$, $i = 1, 2, \ldots, 4$. The PMS is equipped with 4 redundant identical processors, which can be used in various configurations. Within a given phase, the PMS adopts the configuration that best fits the ideal one for the activities executed therein. Unused processors act as cold spares.

The ideal and minimal configuration of the various phases are shown in Table 2, where a denotes the number of active processors. Active processors are subject to faults, whereas spare ones are not. Active processors fail independently from each other, and the time to failure is exponentially distributed. The failure rate is constant within a phase, though the same processor may have different failure rates in different phases, as shown in Table 2. When a processor fails, a spare component is activated to recover the ideal configuration. This activity, performed in a negligible amount of time, succeeds with probability c. In case it fails, the spare processor that does not switch on is declared faulty, and the PMS configuration further degrades. A faulty processor is replaced with a new one. This replace takes a deterministic amount of time τ. Repaired processors become either spares or active processors, depending on the requirements of the current phase.

Phase	Ideal configuration	Minimal requirement	Failure rate	Next phase	Starting criterion
1	$a = 3$	$a = 2$	2λ	2	-
2	$a = 2$	$a = 1$	λ	{3,4}	-
3	$a = 3$	$a = 3$	5λ	4	$f = 0$
4	$a = 3$	$a = 3$	2λ	-	

Table 2: Phase-dependent parameters of the PMS

The goals of the mission are represented by the activities the PMS performs inside phases 3 and phase 4. However, phase 4 is the primary objective that has to be necessarily performed, whereas phase 3 is a secondary optional objective. Since during phase 3 the PMS is subject to a high failure rate, the secondary objective is pursued if and only if it does not jeopardize the reliable execution of the more important phase 4. The decision on whether to perform phase 3 or not is taken at the time phase 2 ends, by evaluating

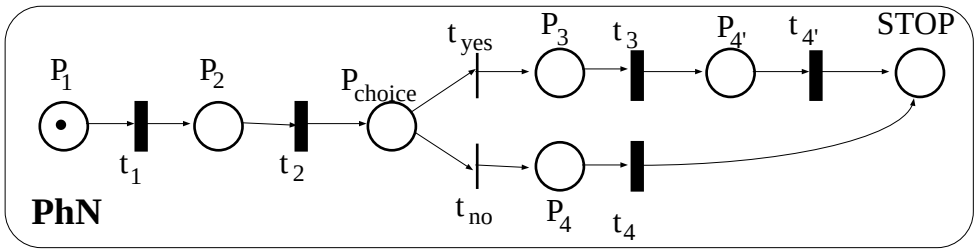

Figure 1: PhN submodel for the example of PMS

the starting criterion given in Table 2, where f denotes the number of faulty processors. Moreover, in case a processor fails after phase 3 has started, the duration of the phase is shortened to reduce the risks of further failures. Precisely, the expected duration τ_3 of phase 3 is defined as a function of the number of faulty processors, $\tau_3 = \tau_3(f)$. Therefore, both the sequence of phases performed by the PMS and the overall duration of the mission itself may dynamically change depending on processors availability.

3.2 MRSPN modeling of the example

At an high abstraction level, we build the model of a PMS as composed of two logically separate MRSPN. One part is called System Net (SN) and represents the system, that is its components, their interactions, their failure/repair behavior. The other part is called Phase Net (PhN), and represents the control part, which describes the phase changes. The adequacy of this scheme for the modeling of PMS is found in the possibility of expressing even complex behaviors through the relations between the PhN and SN submodels.

The MRSPN model of the PhN is shown in Figure 1. A token in place P_i, $i = 1, 2, \ldots, 4, 4'$, models the execution of the corresponding phase of the PMS. The sequence of phases ends with a token in STOP place, which represents the end of the mission. Notice that place $P_{4'}$ is introduced because phase 4 can be executed along two possible different paths of the mission. The general transition t_i, $i = 1, 2, \ldots, 4, 4'$, models the duration of the corresponding phases. To depict transitions, we adopted the usual convention: instantaneous transitions are depicted as thin bars, exponential ones as empty rectangles, and non-memoryless transitions as black-filled rectangles.

PhN element	SN marking
t_{yes} enabled if	$m(Down) = 0$
t_{no} enabled if	$m(Down) > 0$
firing rate of t_3	$\tau_3(m(Down))$

Table 3: Parameters of the PhN dependent of the SN marking

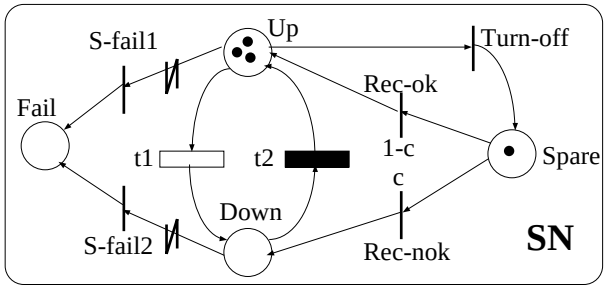

Figure 2: SN submodel for the example of PMS

The dynamic features of the PMS mission profile are easily modeled by making the evolution of the PhN dependent on the marking of the SN. For instance, place P_{choice} plus the two instantaneous transitions t_{yes} and t_{no} model the dynamic selection of the next phase to be performed, which takes place at the end of phase 2. The two instantaneous transitions are guarded by enabling conditions that relate to the marking of the SN submodel. Similarly, transition t_3 has a firing rate that is a function of the SN sub model marking. This particular dependency has been named *marking-dependency by a scaling factor* [9], because the distribution of the firing time is affected by the marking changes only in its expected value, and not in its general law. All the dependencies of the PhN parameters on the SN markings are given in Table 3. The initial marking of the PhN assigns 1 token to the place P_1, modeling the start of the first phase.

The SN submodel is shown in Figure 2. The state of the processors is modeled by the three places Up, $Down$, and $Spare$. The marking of these places represents the number of actively working, failed and cold spare processors, respectively. The exponential transition t_1, and the deterministic one t_2 model the failure and repair process of the processors, respectively, moving tokens back and forth between place Up and place $Down$. The mission goes on unless a token reaches place $Fail$, which models the mission failure.

The SN evolution is conditioned to the marking of the PhN by proper marking de-

SN element	PhN marking			
	$m(P_1)$=1	$m(P_2)$=1	$m(P_3)$=1	$m(P_4) + m(P_{4'})$=1
firing rate of t_1	$2\lambda m(Up)$	$\lambda m(Up)$	$5\lambda m(Up)$	$2\lambda m(Up)$
Turn-off enabled if	$m(Up)$ >3	$m(Up)$ >2	$m(Up)$ >3	$m(Up)$ >3
Rec-ok enabled if	$m(Up)$ <3	$m(Up)$ <2	$m(Up)$ <3	$m(Up)$ <3
Rec-nok enabled if	$m(Up)$ <3	$m(Up)$ <2	$m(Up)$ <3	$m(Up)$ <3
S-fail1 enabled if	$m(Down)$=3	$m(Down)$=4	$m(Down)$=2	$m(Down)$=2
S-fail2 enabled if	$m(Down)$=3	$m(Down)$=4	$m(Down)$=2	$m(Down)$=2

Table 4: Parameters of the PhN dependent of the SN marking

pendent predicates, which modify transition rates and enabling conditions. The phase-dependent parameters of the SN are shown in Table 4. The rate of transition t_1 is made dependent from the marking of the PhN, to model the different failure intensities of the processors inside the various phases. The instantaneous transition $Turn-off$ models the switching off of a processor that, according to the requirements of the phase being currently executed, is not longer needed to be active. Similarly, the two instantaneous transitions $Rec-ok$ and $Rec-nok$ model the spare reactivation, and the possible successful or failed result of this operation. The three instantaneous transitions $Turn-off$, $Rec-ok$, and $Rec-nok$, are controlled by enabling conditions depending on the marking of the PhN subnet, as shown in Table 4. Finally, the instantaneous transitions $S-fail1$ and $S-fail2$ are introduced to model the failure criteria of the different phases. They are controlled by the guards shown in Table 4, and once enabled, flush all the tokens of the corresponding input places to the $Fail$ place. Notice that the input arcs of these two transitions are variable cardinality arcs. The initial marking of the SN is shown in Figure 2, with 3 tokens in the Up place and 1 in $Spare$.

The resulting model of the PMS is extremely concise. The two submodels shown in Figure 1 and 2 completely represent our example of PMS. Notice the close resemblance of the conditions that relate the behavior of the two submodels as they are presented in Table 3 and 4, and the form these same conditions are given in Table 2. Our high level MRSPN modeling allows to define models of PMS in a way that is very similar to that of a system specification language, easily understandable, unambiguous and easily modifiable.

4 Analytical solution

In this section we present an analytical solution method to obtain the time-dependent marking occupation probabilities of the MRSPN models of PMS. This method is based on the general solution method for MRGP [7], which applies for the solution of any MRSPN model. By taking into account the special structure of the PMS models, we derive a solution strategy much more efficient than the general one in terms of computational complexity. However, before moving our attention towards the solution technique, we have to be sure that the models built according to the methodology explained above are indeed MRSPN models, or, in other words, we have to show that a Markov renewal sequence is definitely found, embedded in the underlying marking process.

4.1 MRGP structure of the marking process

Because of their generality, it is not easy to check whether a given timed Petri net model is a MRSPN or not. In general, the marking process must be inspected to verify the existence of a Markov regenerative sequence, but this can be a very costly check for complex models. A possible way to build Petri nets that are MRSPN is to prescribe constraints on the net structure, in such a way that a Markov renewal sequence is definitely found in the underlying marking processes. To this aim, a sufficient constraint to be imposed on the net structure, is the following one:

Constraint 1 *At most 1 general transition is enabled in each marking of the Petri net.*

In this case, the Markov property holds (at least) each time a general transition fires or it is disabled. This constraint is the one usually adopted [8], for it provides an easy-to-check condition to test for the existence of the MRGP structure in the underlying marking process. However, the Petri net model we built in the previous section does not comply with this constraint. Indeed, two general transitions, namely the one representing the phase in the PhN, and that modeling the repair in the SN, are allowed to be simultaneously enabled. Notice that the condition expressed by Constraint 1 would be obviously

fulfilled by the PMS model sketched above if the sole general transitions of the model were those included in the PhN subnet. This would mean to keep the SN as a simple GSPN model, or, equivalently, to maintain the intraphase process within the boundaries of time-homogeneous Markov chains. In fact, in the special case of the models of PMS, a much less restrictive constraint is sufficient to ensure that the Petri net model is a MRSPN:

Constraint 2 *Whenever a timed transition fires in the PhN, each non-memoryless enabled transition resamples a new firing time, which can only depend on the net marking.*

Owing to the structure of the PhN submodel, this constraint ensures that the firing times of the timed transitions in the PhN (the phase completion times) are regeneration points of the MRSPN model. Thus, a specific Markov renewal sequence is identified embedded in the marking process, and the underlying marking process is therefore a MRGP. It is worthwhile observing that this condition is much less restrictive than the one prescribed by Constraint 1. Between two phase completion instants, the marking process of the model can be a completely general stochastic process. This allows including general transitions in the SN submodel, which can be concurrently enabled with the general transitions of the PhN, as long as no transition fires in the PhN.

Still, the Petri net model we defined in the previous section does not respect this weaker constraint, neither. Indeed, suppose transition t_2, which models the repair activities in the SN, is enabled at the time a phase completes. Resampling a new firing time for t_2 implies that the memory of the work already done has to be lost. We can model the loss of memory either with a premature completion of the repair at the phase ending time, or with its restart at the beginning of the next phase. In both cases an approximation is introduced in the model, in that such a behavior is not in the semantic of the repair.

Anyway, even if for some special cases of PMS it might be possible to further weaken the constraint on the net structure and still obtain a MRSPN model, we will assume Constraint 2 as the condition to be met for the analytical tractability of the models.

Also, the loss of memory at phase boundaries does not imply any approximation for some classes of PMS, when maintenance activities are performed between consecutive phases. In this case, keeping track of the repair work already performed but not yet completed have no use at all. This scenario is common in the context of SMS [6], which has been modeled through the PMS methodologies. In other cases the loss of memory does result in an approximate modeling, still it is possible to decide in a sensible way, for each transition, whether the resampling is modeled as a restart or a premature completion, so that upper and lover bound models can be obtained. Consider our example of PMS, and suppose that, at the phase ending times, we force the premature completion of the repairs that are currently being executed. It is easy to realize that such a model provides an optimistic estimation of the dependability measures of the original PMS. Conversely, we can obtain a pessimistic estimation of the dependability measures if the repairs that are not completed when a phase ends simply start again from the beginning as the next phase starts. These two alternatives provide an upper and lower bounds on the exact dependability measures, thus allowing for the estimation of the error introduced with the loss of memory. If one desires to improve the tightness of the bounds, some modifications can be made to the upper and lower bound models, to improve their accuracy, and consequently limit the gap between the pair of results they provide. Each non-memoryless transition of the SN for which the loss of memory results in an approximate behavior can be split in a sequence of shorter activities, for which the influence of the approximation will be less relevant. For instance, in our example of PMS we could model transition t_2, whose duration is τ, with two consecutive deterministic transitions, each one having constant delay $\tau/2$. In this way, the restart or the premature completion of a repair activity will affect only one out of the two stages, resulting in a better approximation of the original PMS.

4.2 The transient marking occupation probabilities

We present now a specialization of the general solution method for MRGP to the analytical study of the MRSPN models of PMS. Denote with S the set of markings of the

MRSPN reachability graph. Consider the time-dependent marking occupation probability of marking m' at time t, conditioned to the initial marking m, and denote it $v_{m,m'}(t)$, $m, m' \in S$, $t \geq 0$. Moreover, denote with $V(t) = \|v_{m,m'}(t)\|$ the transient probability matrix that collects these conditional probabilities. According to the MRGP theory [7], matrix $V(t)$ is the solution to the following generalized Markov renewal equation:

$$V(t) = E(t) + K * V(t) \tag{1}$$

where matrix $K(t) = \|k_{m,m'}(t)\|$ and $E(t) = \|e_{m,m'}(t)\|$ are the global and the local kernel of the MRGP, and $K * V(t)$ is the matrix whose generic element is obtained with the row by column convolution of $K(t)$ and $V(t)$.

Let $1, 2, \ldots, n$ be the set of phases performed through the mission, and denote with $s(i)$ the set of phases which can be performed after phase i, $i = 1, 2, \ldots, n$. For the sake of simplicity, we assume that the ordering of phases is such that $j > i$, for each $j \in s(i)$. Note that such an ordering can always be found because of the acyclic structure of the PhN. Let t_i be the transition of the PhN that models the time the PMS spends in phase i, $i = 1, 2, \ldots, n$, respectively. The firing time of transition t_i is a general random variable with probability density function $f_i(t)$, and cumulative distribution function $F_i(t) = \int_0^t f_i(u)du$, $i = 1, 2, \ldots, n$. In the case general transition t_i has a marking dependent firing rate, we can easily reduce it to a marking-independent one [9]. Suppose the expected firing rate of transition t_i is a function $g(m)$ of the current marking m. A marking-independent definition of the firing time of transition t_i is provided by the normalized firing time distribution, defined as $\hat{F}_i(t) = F_i(t/g(m))$, which has average 1 and is not marking-dependent. This normalization is extended to the intraphase stochastic process representing the evolution of the PMS within phase i, by multiplying the rate of the outgoing transitions of marking m by the expected firing delay $g(m)$ of t_i. An intuitive interpretation of this scaling of the intraphase process lies in modifying the relative speed, of the transitions of the SN that are concurrently enabled with t_i, rather than changing the speed of transition t_i itself.

Denote with $\{m(t), t \geq 0\}$ the stochastic process representing the evolution of the marking of the MRSPN. Define $T_0 = 0$, and let T_i be the time instant at which transition t_i completes, $i = 1, 2, \ldots, n$. By construction, the phase ending times T_i represent regeneration points for the marking process $\{m(t), t \geq 0\}$. Indeed, Constraint 2 guarantees that the memoryless Markov property holds of the marking process of the MRSPN at the phase completion times. Thus, the sequence of bivariate random variables $\{(Y_i, T_i)\}$, where Y_i denotes the marking of the MRSPN model at the time immediately after T_i, is a Markov renewal sequence, and consequently the marking process $\{m(t), t \geq 0\}$ is a MRGP. To obtain the transient probability matrix $V(t)$ we proceed by studying the marking process $\{m(t), t \geq 0\}$ over the different phases.

Consider the stochastic process $\{m(t), t \geq 0\}$ during the time interval $[T_{i-1}, T_i]$, when transition t_i is enabled, and denote with $\Pi_i(t)$ its transient probability matrix, and with S_i its state space, $i = 1, 2, \ldots, n$. The set $S_{n+1} = S \setminus \bigcup_{i=1}^{n} S_i$ contains those absorbing markings reached by the model at the end of the mission, when a token is in place STOP. Because of the structure of the MRSPN model of a PMS, the sets S_i, $i = 1, 2, \ldots, n+1$, form a partition of S . Let C_i be the cardinality of set S_i, $i = 1, 2, \ldots, n+1$. The global kernel $K(t)$ and the local kernel $E(t)$ can be reordered according to the partition defined by sets S_i, $i = 1, 2, \ldots, n+1$, and thus partitioned in blocks $K_{i,j}(t)$ and $E_{i,j}(t)$ having dimensions $C_i \times C_j$, respectively. Due to the PMS structure, $K(t)$ is such that the block matrices $K_{i,j}(t)$ take non-zero values if and only if $j > i+1$, whereas $E_{i,j}(t)$ is non-zero if and only if $j = i$. Let $\Delta_{i,j}$, $i, j = 1, 2, \ldots, n+1$ be the $C_i \times C_j$ branching-probability matrix defined as follows:

$$\Delta_{i,j} = \|\delta^{i,j}_{m,m'}\| = Prob[Y_i = m' | m(T_i-) = m], m \in S_i, m' \in S_j$$

where T_i- denotes the time instant immediately before T_i. The elements of $K(t)$ are as follows:

$$k_{m,m'}(t) = Prob[Y_i = m', T_i \leq t | Y_0 = m] = \int_0^t Prob[Y_i = m', T_i = u | Y_0 = m] du =$$

$$= \int_0^t Prob[Y_i = m' | T_i = u, Y_0 = m] f_i(u) du, \quad m, m' \in S, \quad t \geq 0 \tag{2}$$

According to Equation (2), the non-zero blocks matrix $K(t)$ can be obtained as follows:

$$K_{i,j}(t) = \int_0^t \Pi_i(u)\Delta_{i,j}f_i(u)du, \;\; i = 1, 2, \ldots, n, \;\; j \in s(i) \;\; t \geq 0$$

Similarly, the entries $e_{m,m'}(t)$ of the local kernel matrix are given by:

$$e_{m,m'}(t) = Prob[m(t) = m', T_i > t | Y_0 = m] =$$

$$= Prob[m(t) = m' | T_i > t, Y_0 = m] Prob[T_i > t], \;\; m, m' \in S, \;\; t \geq 0$$

and consequently, the non-zero blocks $E_{i,j}(t)$ of the local kernel matrix $E(t)$ are as follows:

$$E_{i,i}(t) = \Pi_i(t)\left(1 - F_i(t)\right), \;\; i = 1, 2, \ldots, n+1, \;\; t \geq 0$$

Consider the block partition of matrix $V(t)$ induced by the sets S_i, $i = 1, 2, \ldots, n+1$. Owing to block structure of matrices $K(t)$ and $E(t)$, all the blocks $V_{i,j}(t)$ are null if $i > j$, that is matrix $V(t)$ exhibits an upper triangular block form. The generalized Markov renewal Equation (1) can be rewritten according to the block partitioning of the matrices:

$$V_{i,j}(t) = E_{i,j}(t) + \int_0^t \sum_{h \in s(i)} dK_{i,h}(u) V_{h,j}(t-u), \;\; i, j = 1, 2, \ldots, n+1, \;\; t \geq 0 \qquad (3)$$

and a backward substitution procedure can be applied to obtain all the non-zero blocks of $V(t)$ in the j-th column, starting from the diagonal block $V_{j,j}(t) = E_{j,j}(t)$.

From the transient marking occupation probability matrix $V(t)$ we can compute the dependability measures of interest. For instance, we obtain the probability R of successfully completing the mission. If m_0 is the initial probability vector over the markings of the reduced reachability graph of the PMS model, then $m_0 V_{1,n+1}(t)$ is the time-dependent marking occupation probability vector at time t, $t \geq 0$, over the markings of S_{n+1}, which represent the state of the PMS at the end of the mission. Since these markings are all absorbing, we can compute R as the product $m_0 V_{1,n+1}(\infty)\Theta$, where Θ is the vector that selects those markings that represent successful states of the system, according to the success criterion defined for the mission of the PMS. The computation of R is thus formulated as the problem of evaluating the limiting probability distribution of the transient

MRGP process. Once the block matrix $V_{1,n+1}(t)$ has been computed, the following limit needs to be obtained:

$$R = \lim_{t\to\infty} m_0 V_{1,n+1}(t)\Theta \tag{4}$$

Directly attacking the solution of the system of integrals in Equation (3) to compute blocks $V_{i,j}(t)$ can be a computationally expensive procedure. Indeed, each of the substitution steps requires the solution of the convolution integral in (3) for the associated submatrices, which is costly and may introduce numerical approximations. Alternatively, we can resort to the analysis in the Laplace-Stieltjes transform (LST) domain. If we take the LST of both sides of Equation (3) we obtain:

$$V^{\circ}_{i,j}(s) = E^{\circ}_{i,j}(s) + \sum_{h\in s(i)} K^{\circ}_{i,h}(s)V^{\circ}_{h,j}(s), \quad i,j = 1,2,\ldots,n+1 \tag{5}$$

where $V^{\circ}_{i,j}(s)$, $E^{\circ}_{i,j}(s)$, and $K^{\circ}_{i,h}(s)$ are the LST of $V_{i,j}(t)$, $E_{i,j}(t)$, and $K_{i,h}(t)$, respectively. The backward substitution can be completed by exploiting the PhN acyclic structure.

Equation (5) is remarkable for its generality. It allows to derive the LST of the time dependent marking occupation probabilities for the MRSPN model of a PMS with general duration of the phases, and general intraphase marking process. Of course, a numerical antitransformation is needed to obtain the final result in the time domain. However, we only need to antitransform a single block $V^{\circ}_{i,j}(s)$, rather than performing a sequence of numerical solutions of integral equation systems, as required by the analysis in the time-domain with Equation (3). Furthermore, it is also possible to take advantage of the LST theory to directly compute the limit in Equation (4) without obtaining the time-domain expression of $V_{1,n+1}(t)$, but rather dealing with its transform. Precisely, because of the time-invariance of m_0 and Θ, and from the *final-value* theorem of Laplace transforms, the reliability R is obtained as:

$$R = \lim_{t\to\infty} m_0 V_{1,n+1}(t)\Theta = m_0 \left(\lim_{t\to\infty} V_{1,n+1}(t)\right)\Theta = m_0 \left(\lim_{s\to 0^+} V^{\circ}_{1,n+1}(s)\right)\Theta \tag{6}$$

To avoid a cumbersome notation, let us consider the case when the PhN submodel is a chain rather than a tree, that is phases $1,2,\ldots,n$ are performed in a fixed order. In this

case, the transform $V^{\circ}_{1,n+1}(s)$ takes the following form:

$$V^{\circ}_{1,n+1}(s) = \prod_{i=1}^{n} K^{\circ}_{i,i+1}(s) E^{\circ}_{n+1,n+1}(s) = \prod_{i=1}^{n} K^{\circ}_{i,i+1}(s)$$

where the last equivalence comes from the fact that all the markings of S_{n+1} are absorbing markings, and thus $E^{\circ}_{n+1,n+1}(s)$ is the identity matrix. Let $K^{*}_{i,i+1}$ denote the limit for $s \to 0^{+}$ of matrix $K^{\circ}_{i,i+1}(s)$, which surely exists for the properties of the transient probability matrices. Then, we can rewrite Equation (6) as follows:

$$R = m_0 \lim_{s \to 0^{+}} \prod_{i=1}^{n} K^{\circ}_{i,i+1}(s)\Theta = m_0 \prod_{i=1}^{n} K^{*}_{i,i+1}\Theta \tag{7}$$

Thus, an explicit formula can be obtained for probability R, without any need to evaluate the transient state probability matrix of the MRGP underlying the PMS model. It is worthwhile observing that the approach followed to compute the reliability of the PMS at the time the mission ends can be also applied to obtain the reliability at the system at each phase completion instant. Indeed, each phase of the system can be seen as being the last one the system has to perform, and thus the probability distribution at the end of phase i, $i = 1, 2, \ldots, n$, is computed as an absorption probability through the limit of the global kernel submatrices transforms.

Other dependability attributes of interest, such as the pointwise reliability and availability, can be evaluated once the transient marking occupation probability matrix $V(t)$ has been obtained. Cumulative measures are computed from $V(t)$ by integration. For instance, by superimposing a reward structure over the markings of the MRSPN, it is possible to compute the performability of the PMS as the total reward cumulated during the mission.

5 Specializations for particular classes of PMS

In this section we present a specialization of the general results provided by Equations (3) and (5) for the transient marking occupation probabilities, and by Equation (4) for the reliability at mission completion time. We consider three particular scenarios. First, we

consider the case when phases have a deterministic duration, denoted by "a" in Section 2, for which we derive a simpler form for $V(t)$. Then, we explore the case when the subordinate process is a homogeneous continuous-time Markov chain, that is scenario "c" of Section 2. For this scenario we can derive very compact formulae for the reliability of the system at phase completion times. Last, we discuss the applicability limits of our approach, dealing with the most general scenario, denoted as "-".

5.1 Constant phase duration

Let τ_i be the deterministic firing time of transition t_i, $i = 1, 2, \ldots, n$. In this special case, the probability density function $f_i(t)$ of the phase duration is the Dirac impulse function at τ_i, and the cumulative distribution function is the delayed unit step function $F_i(t) = u(t - \tau_i)$. The blocks of the global kernel matrix $K(t)$ take the following form:

$$K_{i,j}(t) = \int_0^t \Pi_i(u)\Delta_{i,j} f_i(u)du = \Pi_i(\tau_i)\Delta_{i,j} F_i(t), \quad i = 1, 2, \ldots, n, \quad j \in S_i, \quad t \geq 0$$

and thus the transient matrix blocks $V_{i,j}(t)$ can be rewritten as follows:

$$V_{i,j}(t) = E_{i,j}(t) + \int_0^t \sum_{h \in s(i)} d\Pi_i(\tau_i)\Delta_{i,h} F_i(u) V_{h,j}(t - u) =$$

$$= E_{i,j}(t) + \sum_{h \in s(i)} \Pi_i(\tau_i)\Delta_{i,h} \int_0^t f_i(u) V_{h,j}(t - u)du = E_{i,j}(t) + \sum_{h \in s(i)} \Pi_i(\tau_i)\Delta_{i,h} V_{h,j}(t - \tau_i)$$

Notice that the integral are solved due to the fact that the Dirac impulse function allows reducing the convolution integral to just a time shift. We can complete the analysis in the time domain without resorting to the LST, completing the backward substitution in Equation (3). For instance, in the case of a linear mission profile, we obtain the following expression for the transient probability matrix blocks $V_{i,j}(t)$:

$$V_{i,j}(t) = \prod_{h=i}^{j-1} \Pi_h(\tau_h)\Delta_h E_{j,j}(t - \sum_{h=1}^{j-1} \tau_h), \quad i = 1, 2, \ldots, n, \quad j \geq i, \quad t \geq 0 \tag{8}$$

where the product over an empty set is to be intended the identity matrix. It is worthwhile remarking that Equation (8) is applicable to whichever MRSPN model of a PMS with constant phase duration that satisfies Constraint 2, regardless of the structure of the SN.

5.2 Markov chain subordinate processes

In this case, the transient probability matrix $\Pi_i(t)$ of the subordinate process can be expressed via the matrix exponential $e^{Q_i t}$, where Q_i is the infinitesimal generator of the subordinate Markov process, $i = 1, 2, \ldots, n$. The expressions given for the global and local kernel matrix blocks can be rewritten as follows:

$$K_{i,j}(t) = \int_0^t e^{Q_i u} \Delta_{i,j} f_i(u) du, \quad E_{i,i}(t) = e^{Q_i t}(1 - F_i(t)), \;\; i = 1, 2, \ldots, n, \;\; t \geq 0$$

The LST of the preceding expressions can be computed as follows:

$$K^{\circ}_{i,j}(s) = L[e^{Q_i t} f_i(t)]\Delta_{i,j}, \quad E^{\circ}_{i,i}(s) = sL[e^{Q_i t}(1 - F_i(t))], \;\; i = 1, 2, \ldots, n \tag{9}$$

where $L[\cdot]$ denotes the Laplace transform operator. Quite interestingly, these expressions can be completely worked out and the integration solved in many interesting special cases. For instance, consider the case of a finite support distribution, namely the distribution obtained by truncating at time $\tau > 0$ the negative exponential distribution of parameter λ, and then normalizing with respect to the probability $e^{-\lambda\tau}$. The LST of the kernel blocks are obtained from Equation 9 as follows:

$$K^{\circ}_{i,j}(s) = \int_0^{\tau} e^{-st} e^{Q_i t} \frac{\lambda e^{-\lambda t}}{1 - e^{-\lambda\tau}} dt \Delta_{i,j} = \frac{\lambda((s+\lambda)I - Q_i)^{-1}}{1 - e^{-\lambda\tau}} \left(I - e^{((s+\lambda)I - Q_i)\tau}\right) \Delta_{i,j}$$

Similarly, we compute the blocks of the local kernel, obtaining the following expression:

$$E^{\circ}_{i,j}(s) = \frac{s}{1 - e^{-\lambda\tau}} \left[((s+\lambda)I - Q_i)^{-1} \left(I - e^{((s+\lambda)I - Q_i)\tau}\right) - e^{-\lambda\tau} (sI - Q_i)^{-1} \left(I - e^{(sI - Q_i)\tau}\right)\right]$$

Owing to the fact that the explicit expressions for the LST of the global kernel matrix blocks are available, we can compute the reliability R by applying Equation (4). For instance, consider a periodic PMS alternating the execution of a phase whose duration is a random variable exponentially distributed with parameter λ, and a constant duration phase that lasts for τ units of time. The PMS cyclically executes the two phases over time. The reliability R_{2n} at the time the $2n$-th phase ends is obtained as follows:

$$R_{2n} = m_0 \lim_{s \to 0^+} \prod_{i=1}^{n} \left(\lambda((s+\lambda)I - Q_i)^{-1} \Delta_1 e^{-(sI - Q_2)\tau} \Delta_2\right) \Theta = m_0 \left(\lambda(\lambda I - Q_i)^{-1} \Delta_1 e^{Q_2)\tau} \Delta_2\right)^n \Theta$$

Notice that deterministic and random phase duration can be freely mixed and the reliability of the PMS is still easily obtained according to Equation (7).

5.3 General instances of PMS

The general results stated by Equations (3), (5), and (4) are valid under any scenario of PMS among those considered in this paper. Random phase duration, flexible mission profile, and general intraphase stochastic process are all accommodated in our modeling and solution scheme. The limit of practical applicability of the theoretic results derived in this paper for the MRSPN models of PMS is represented by the possibility of evaluating the time-dependent marking occupation probabilities of the subordinate process i during the enabling period of transition t_i, $i = 1, 2, \ldots, n$. This information is absolutely necessary to complete the analytical derivation of the expressions for the time-dependent marking occupation probabilities and the reliability of the models.

Besides the particular case of homogeneous Markov chains we dealt with above, there are other types of subordinate process that are amenable to analytical solution in terms of their time-dependent marking occupation probabilities. For instance, exact methods exist for the transient analysis of non-homogeneous Markov chain [17]. Another interesting case is when the subordinate process is a semi-Markov process [11], as in the case when some general transitions are included in the SN submodel and they restart their firing each time a marking change occurs. Last, the subordinate process could be a MRGP itself. In this case the SN is allowed to contain general transitions, which must however fulfil Constraint 1, that is a single general transition can be enabled in each marking of the nested MRGP. The transient marking occupation probabilities of the subordinate process can be computed according to Equation (1).

6 Sensitivity analysis

Suppose now that we are interested in studying the effects that the variations in the value of some parameters have on the dependability measures of the PMS, either because such parameters are only known with uncertainty, or because different scenarios of the system are to be analyzed. Obviously, whenever the dependence of the measure of interest

from the parameters only involves simple functions that can be computed at a limited computational cost, the sensitivity analysis can be conveniently conducted through multiple evaluations, to plot the dependability measures for the whole range of parameter values. Conversely, when the dependability measure object of the evaluation is a complex function, or when more parameters can be varied simultaneously, performing multiple evaluations becomes an expensive task.

In our MRSPN scenario, an effective alternative to this multiple evaluation scheme is offered by the possibility of conducting an analytical time-dependent sensitivity analysis, The existence of an analytic expression for the marking dependent occupation probabilities allows to evaluate the derivatives of the dependability measures of interest with respect to the variations of some parameters. These derivatives, also called sensitivity functions [13], complement the means available for the study of PMS, providing guidelines for the system optimization [4], and in some cases avoid or limit the need of performing long batches of evaluations for a number of different values of the parameters. These functions can be conveniently employed to perform an analytical study of the effects that the parameter variations have on the dependability. The absolute value of the derivative indicates the magnitude of the variations of the measure for a small perturbations of the parameter, and its sign reveals whether an increase of the parameter value would cause an increase or instead a decrease of the measure. When more parameters may simultaneously vary, by comparing the partial derivatives with respect to various parameters it is possible to identify those to which the dependability measures are sensitive the most.

In the following, we analytically derive the sensitivity functions that represent the effects that parameter variations may have on the transient marking occupation probability matrix $V(t)$, and on the probability R of successfully completing the mission.

6.1 Sensitivity analysis of $V(t)$

To carry on the sensitivity analysis of the transient marking occupation probability matrix, we consider the matrix $V(t)$ as being a function of some independent parameter θ, that

is $V(t) = V(\theta; t)$. We denote with $S(\theta; t)$ the derivative of $V(\theta; t)$ with respect to θ.

Matrix $S(\theta; t)$ can be partitioned into its blocks $S_{i,j}(\theta; t)$ according to the same partition as that defined for $V(\theta; t)$. Since the expression for the transient marking occupation probabilities is given in terms of the LST of the kernel matrices in Equation (6), we obtain the sensitivity function matrix in the transform domain. Let us denote with $V^{\circ}_{i,j}(\theta; s)$ and $S^{\circ}_{i,j}(\theta; s)$ the Laplace Stieltjes transform of block matrix $V_{i,j}(\theta; t)$ and $S_{i,j}(\theta; t)$, respectively. The sensitivity function transform is obtained as follows:

$$S^{\circ}_{i,j}(\theta; s) = \int_0^{\infty} e^{-st} d\frac{\partial}{\partial\theta} V_{i,j}(\theta; t) = \frac{\partial}{\partial\theta} \int_0^{\infty} e^{-st} dV_{i,j}(\theta; t) = \frac{\partial V^{\circ}_{i,j}(\theta; s)}{\partial\theta}$$

where the second equality comes from the fact that θ is independent from both s and t. The differentiation of $V^{\circ}_{i,j}(\theta; s)$ according to Equation (5) gives the following expressions:

$$S^{\circ}_{i,j}(\theta; s) = \frac{\partial}{\partial\theta} V^{\circ}_{i,j}(\theta; s) = \frac{\partial}{\partial\theta} E^{\circ}_{i,j}(\theta; s) +$$

$$+ \sum_{h \in s(i)} \left(\frac{\partial}{\partial\theta} K^{\circ}_{i,h}(\theta; s) \right) V^{\circ}_{h,j}(\theta; s) + K^{\circ}_{i,h}(\theta; s) \left(\frac{\partial}{\partial\theta} V^{\circ}_{h,j}(\theta; s) \right), \quad i, j = 1, 2, \ldots, n+1 \quad (10)$$

Thus, the evaluation of the sensitivity function $S(\theta; t)$ is reduced to the computation of the derivatives with respect to θ of the LST of the blocks of the kernel matrices. When more specific assumption on the structure of the MRSPN model of the PMS are made, the general Equation (10) can be further simplified. For instance, in the case the subordinate processes are homogeneous Markov chains, the derivatives of the LST of the kernel matrix blocks can be obtained as follows:

$$\frac{\partial K^{\circ}_{i,h}(\theta; s)}{\partial\theta} = \frac{\partial}{\partial\theta} L\left[e^{Q_i t} \Delta_{i,j} f_i(t) \right] = L\left[\frac{\partial e^{Q_i t}}{\partial\theta} \Delta_{i,j} f_i(t) \right] + L\left[e^{Q_i t} \frac{\partial \Delta_{i,j}}{\partial\theta} f_i(t) \right] + L\left[e^{Q_i t} \Delta_{i,j} \frac{\partial f_i(t)}{\partial\theta} \right]$$

$$\frac{\partial E^{\circ}_{i,h}(\theta; s)}{\partial\theta} = \frac{\partial}{\partial\theta} sL\left[e^{Q_i t}(1 - F_i(t)) \right] = sL\left[\frac{\partial e^{Q_i t}}{\partial\theta}(1 - F_i(t)) \right] - sL\left[e^{Q_i t} \frac{\partial(1 - F_i(t))}{\partial\theta} \right]$$

6.2 Sensitivity analysis of R

Consider now the probability R of successfully completing the mission as being a function of some independent parameter θ, that is $R = R(\theta)$. Let $r(\theta)$ denote the derivative of $R(\theta)$ with respect to parameter θ. From Equation (4), we evaluate $r(\theta)$ as follows:

$$r(\theta) = \frac{\partial R(\theta)}{\partial\theta} = \frac{\partial}{\partial\theta} \left(m_0 \lim_{s \to 0^+} V^{\circ}_{1,n+1}(\theta; s) \Theta \right) = m_0 \lim_{s \to 0^+} \left(\frac{\partial}{\partial\theta} V^{\circ}_{1,n+1}(\theta; s) \right) \Theta$$

If we consider a particular distribution of the phase duration and a specific type of subordinate process, the general expression given above for function $r(\theta)$ can be further specialized. For instance, consider a MRSPN model for a PMS that sequentially performs n phases having an exponential duration, and whose subordinate process that in each phase is a homogeneous Markov chain. In this case, we obtain the following expression:

$$r(\theta) = m_0 \sum_{j=1}^{n} \prod_{h=1}^{j-1} (I - Q_h/\lambda_h)^{-1} \Delta_h \left(\frac{\partial}{\partial \theta} (I - Q_j/\lambda_j)^{-1} \Delta_j \right) \prod_{h=j+1}^{n} (I - Q_h/\lambda_h)^{-1} \Delta_h \Theta$$

7 Putting the MRSPN approach at work

The MRSPN approach offers several contributions with respect to the previous methodologies that appeared in the literature, concerning both the modeling and the solution aspects. In this section we first discuss the practical relevance of the methodology we have devised in the preceding sections, presenting the main guidelines for its effective exploitation. Then, we present the results of a numerical evaluation of the dependability attributes of the example of PMS we considered throughout this paper, to show the deep understanding that can be gained on the system behavior with adopting our approach.

7.1 Guidelines for the practitioner

First of all, let us focus on the modeling alone. The MRSPN approach represents a relevant improvement of the current PMS modeling practice. From the review presented in [15], it appears that several limits of the state-of-the-art are due to the low-level modeling tools employed, typically Markov chain models. Moving from a direct state-based representation to a more abstract and concise one allows the dependability engineer, on one side to maintain a more comprehensible view of the correspondence between the real system and the modeled one, and on the other side to easily represent PMS features that could not be accommodated beforehand.

These ameliorated modeling capabilities are coupled with a very efficient solution technique. Notice that, in principle, to solve the MRSPN model of a PMS one could

employ a general purpose transient solver for MRGP processes. The algorithms that implement the general solution Equation (1) for the time-dependent marking occupation probabilities are nowadays being included in the automated tools for the dependability evaluation. Of course, in this case no advantage is obtained from the particular structure of the MRSPN models of PMS. Rather, to exploit the results we have obtained in this paper, specific algorithms can be developed and implemented, to take advantage of the separability of the analytical solution over the various phases. For instance, suppose we are interested in computing the probability that the mission has successfully completed at time t, for any $t > 0$, for a given initial probability vector m_0. This requires to evaluate the expression $m_0 V_{1,n+1}(t)\Theta$. To compute the matrix block $V_{1,n+1}(t)$ according to the results we derived above, a solution algorithm would perform the following steps:

1. build the i-th subordinate intraphase process, from the analysis of the reachability graph of the model during the enabling period of transition t_i, $i = 1, 2, \ldots, n$;
2. build the branching probability matrix $\Delta_{i,j}$, from phase i to phase j, $j \in s(i)$, $i = 1, 2, \ldots, n$;
3. obtain the transient state occupation probability matrix $\Pi_i(t)$ of the subordinate intraphase process i, $i = 1, 2, \ldots, n$;
4. if phases have deterministic duration, then complete the analysis in the time domain according to Equation (3), or else compute the LST of the kernel matrix blocks, apply Equation (5), and then antitransform to get the final result in the time domain.

All of the steps described above only require well-known algorithms; in fact they have been implemented in many of the tools for the automated evaluation of dependability. Therefore, implementing the algorithm steps is not a challenging task. Notice that the actual computational cost of the algorithm is dependent on the properties of the subordinate processes and of the phase duration distributions. However, the state space of the MRGP process ever needs to be generated and handled as a whole, but rather the various subordinate intraphase processes are separately generated and solved. Therefore, the solution scheme classifies as a computationally efficient one. Just to give a more precise

	abc	ac	bc	c
Complexity	$O(\sum_{i=1}^{n} C_i^2 q_i \tau_i)$	$O(\sum_{i=1}^{n} C_i^2 q_i \tau_i)$	$O(\sum_{i=1}^{n} C_i^3)$	$O(\sum_{i=1}^{n} C_i^3)$

Table 5: Computational costs for evaluating R under various PMS scenarios

idea about the computational cost, suppose we are interested in evaluating the reliability at mission completion time, for a MRSPN model of a PMS whose intraphase process is a Markov chain. More precisely, suppose phase i has an underlying Markov chain whose state space has C_i states, $i = 1, 2, \ldots, n$. Table 5 shows the computational cost required to execute the steps of the algorithm in the various possible scenarios:

where q_i is the maximum module entry of the Markov chain generator matrix of phase i, and τ_i the deterministic duration of phase i. In those scenarios where constant phase duration is assumed, the computational complexity is basically dominated by the cost needed for the evaluation of the time-dependent state occupation probability distribution at phase ending times (Equation 9), whereas when a random phase duration is assumed, the dominating cost is that to compute the limiting absorption probability distribution through the inverse of the fundamental matrix (Equation 7). Observe that the computational complexity always grows linearly with the number of phases. When restricted to the particular PMS scenario 'abc', the MRSPN approach turns out to perform as efficiently as the best solution approaches listed in [15]. Notice that all the computational cost reported here are to be intended as upper-bounds. In fact, the matrices obtained are quite often sparse, thus allowing cheaper solution techniques [16]. Last, notice that, with respect to the evaluation of the PMS time-dependent marking occupation probabilities, the evaluation of the sensitivity functions only requires an additional small computation effort. Indeed, mostly the same matrices are required in both the two tasks, and solely the way they are arranged by the analytical expressions is different.

7.2 Numerical evaluation

We present now the result of a numerical evaluation we conducted on the example of PMS considered throughout the paper. The unreliability of the system at mission completion

Phase	Distribution	Average duration
1	Deterministic with delay δ	$\delta = 100h$
2	Negative exponential with rate λ_2	$\lambda_2^{-1} = 200h$
3	2-stage Erlang with rate λ_3	$2\lambda_3^{-1} = 40h$ if $f = 0$, $2\lambda_3^{-1} = 4h$ if $f > 0$
4	Uniform within the time window [a,b]	$(b + a)/2 = 7.5h$, $(a = 5h, b = 10h)$

Table 6: Stochastic characterization of phase duration

Parameter	Meaning	Value
λ	Active processor failure rate	$\lambda = 10^{-3}/h$
τ	Faulty processor repair delay	$\tau = 1h$
c	Probability of successful spare insertion	$c = 0.95$

Table 7: Values for SN parameters

time has been selected as the measure of interest for the evaluation. As the loss of memory imposed to transition t_2 changes the semantics of the repair activities, the result we obtain are approximate. However, we exploit the approach explained in Section 4.1 (page 16), to obtain upper bounds and lower bounds on the measures of interest, thus providing accurate estimates of the error introduced.

The duration of the 4 phases of the mission are characterized by the random variables listed in Table 6. Notice that the unit all the time measure are expressed is the hour (h). Both distributions with finite and infinite support are considered. The expected duration of phase 3, which is dependent of the state of the PMS, is reduced to a tenth of the original one in case the system enters a vulnerable state.

The values of the parameters necessary to fully define the SN submodel are given in Table 7. Those values are given without any pretension of realism, just to experience the analyses that can be carried out within the modeling framework presented here. A few evaluations will be performed by considering a number of possible system scenarios, which are obtained by varying the parameter values in a range around their nominal values given by Table 7.

To compute the block matrices required for the evaluation, we have implemented the algorithmic steps described above, by using the general purpose tool *Mathematica*.

We conduct a first evaluation session to estimate the effect that a more or less accurate modeling of the repair activity may have on the final dependability results. More precisely,

we plot in Figure 3 a) the unreliability of the PMS at mission completion time, as obtained from three different models. The first model is the one we developed in this paper, in which the repair is modeled by a deterministic transition, and for which a pair of bounds on the exact unreliability result are provided by our analytical solution method. The second model approximates the deterministic transition with an exponential transition of expected firing time $\tau = 1$. Since the subordinate processes are in this case simple Markov chains, we are able to compute the exact unreliability of such model. The last model approximates the repair with a transition having a firing time drawn from the Erlang(4,4) distribution, whose expected values is again $\tau = 1$. By splitting the Erlang repair into the 4 exponential stages it is composed of, we can analytically obtain the exact unreliability for this model as well.

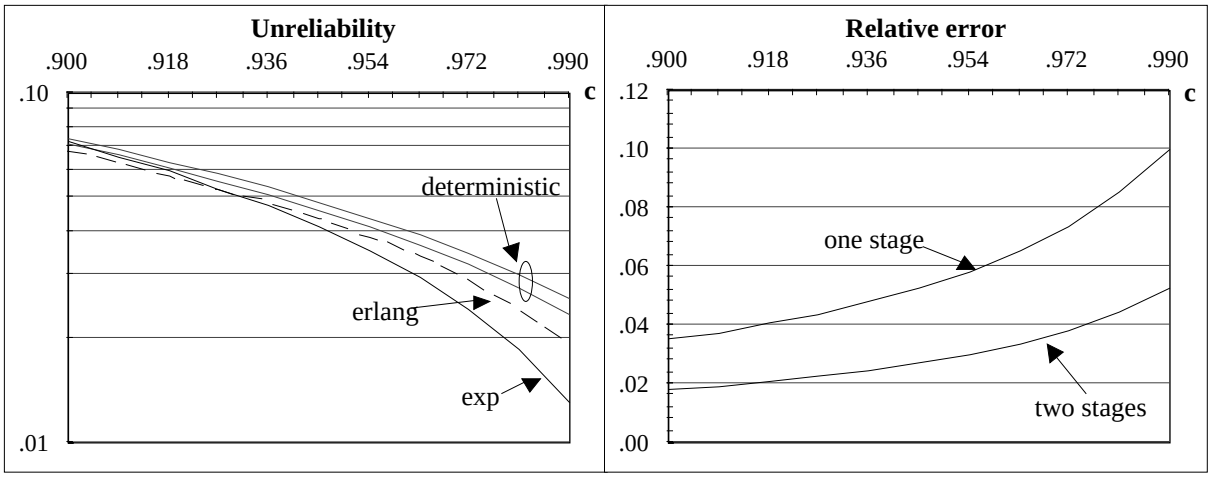

Figure 3: Estimation of the reliability of the PMS

Parameters other than the successful spare insertion c are fixed to their respective nominal value, whereas c ranges within $[0.9, 0.99]$. From Figure 3.a we appreciate the accuracy achieved with the modeling of the deterministic repair. The results obtained with the exponential repair would lead indeed to a excessively optimistic assessment of system dependability for high values of c. The Erlang distribution better approximates the deterministic repair than the exponential one, due to its lower coefficient of variation. However, modeling the 4 exponential stages of the Erlang distribution significantly increases the computation time required for the solution. Notice the tightness of the pair

of bounds our method returns for the deterministic repair, which permits to achieve a very good quality of the approximation of the exact unreliability results. Moreover, by splitting the deterministic repair transition into two shorter deterministic transition, each of length $\tau/2$, we are able to further reduce the gap between the two bounds. Figure 3.b shows the relative error incurred by our bounded solution in case 1 single stage or 2 stages are used to model the repair activity. Subsequent decompositions of the repair process lead to further improvements of the bound tightness. Obviously, this also results in an increase of the state space of the intraphase processes, and requires devising adequate trade-offs between the computational cost and the accuracy of the estimation.

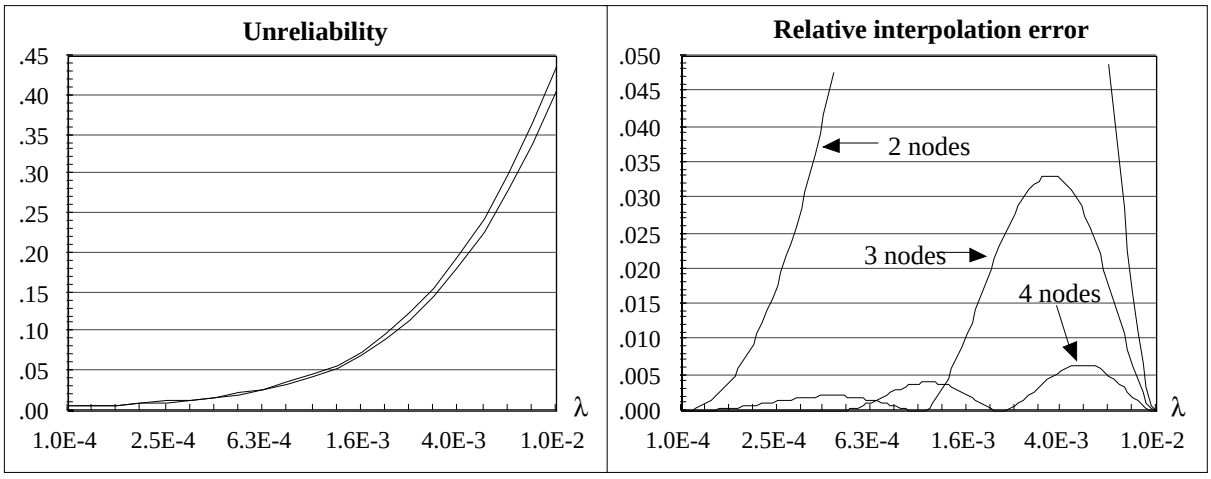

Figure 4: Interpolation error by exploiting the sensitivity functions

We consider now the unreliability of the PMS for values of the failure rate λ ranging within the interval $[10^{-4}/h, 10^{-2}/h]$, while the other parameters are fixed to their nominal values. The plot in Figure 4.a shows how the unreliability increases with λ and remain quite close to each other. The two bounding functions were evaluated at 100 points within the range $[10^{-4}/h, 10^{-2}/h]$. Figure 4.b shows the approximations obtained by exploiting the sensitivity functions. More precisely, we have computed three different approximate curves for the unreliability lower bound, by interpolating the function and its derivative in 2, 3, and 4 interpolation points (the so-called interpolation nodes), respectively. Figure 4.b shows the relative error introduced by the various interpolations over the whole interval of values considered for λ. As it can be observed, increasing the number of interpolating

nodes allows obtaining more and more accurate results, and 4 interpolation nodes appear sufficient to obtain a very tight approximation of the original unreliability figures.

8 Conclusions

In this paper we addressed the analytical dependability modeling of PMS by proposing a new methodology for their modeling and evaluation based on a MRSPN approach. Our proposal allows several extensions wrt. methods proposed in the literature and greatly enlarges the class of PMS that can be analytically studied. In particular, besides being able to deal with all the scenarios proposed by previous studies, the MRSPN modeling allows:

1) accommodating phases of random duration still providing exact analytical solution;
2) intraphase model other than time-homogeneous Markov chains.

A very general example of PMS has been used throughout the paper, to exercise our MRSPN approach in modeling and evaluation of PMS. It includes most of the typical features of PMS, and has been intentionally defined to include those aspects previous methods do not deal with.

Our solution for PMS models is based on the specialization of the Markov Regenerative Process (MRGP) theory for the solution of MRSPN models of PMS. The computational complexity of the analytical solution is reduced to the one needed for the separate solution of the different phases. The issues introduced by the phased behavior are solved without requiring additional computational costs. The applicability of our approach is only limited by the size of the biggest Petri net model which can be handled by the dependability evaluation tools and by the possibility of evaluating the time-dependent matrix of marking occupation probabilities of the subordinate processes, should not be homogeneous Markov chains. Moreover, thanks to the existence of an analytical solution procedure, by computing the partial derivatives with respect to the varying parameters

we have shown how to perform an analytical time-dependent sensitivity analysis of PMS, a task that has been entirely neglected in the literature.

Acknowledgements The authors wish to thank Prof. Kishor S. Trivedi from the Dept. of Electrical and Computer Engineering of the Duke University for the fruitful discussions held during the preliminary stages of this work.

References

[1] M. Alam and U. M. Al-Saggaf. Quantitative reliability evaluation of reparaible phased-mission systems using Markov approach. *IEEE Trans. on Reliability*, R-35:498–503, 1986.

[2] J. Arlat, T. Eliasson, K. Kanoun, D. Noyes, D. Powell, and J. Torin. Evaluation of fault -tolerant data handling systems for spacecraft: Measures, techniques and example applications. Technical Report 86.321, LAAS-CNRS, 1986.

[3] B. E. Aupperle, J. F. Meyer, and L. Wei. Evaluation of fault-tolerant systems with nonhomogeneous workloads. In *FTCS'89 - IEEE Fault-Tolerant Computing Symposiumg*, pages 159–166, Washington, D.C., USA, June 1989. IEEE Computer Society Press.

[4] J.T. Blake, A.L. Reibman, and K.S. Trivedi. Sensitivity analysis of reliability and performability measures for multiprocessor systemss. In *ACM SIGMETRICS Int. Conference on Measurement and Modeling of Computer Systems*, Santa Fe, New Mexico, USA, 1988.

[5] A. Bondavalli, I. Mura, and M. Nelli. Analytical modelling and evaluation of phased-mission systems for space applications. In *HASE'97 - IEEE High Assurance System Engineering Workshop*, pages 85–91, Bethesda, Maryland, USA, 1997. IEEE Computer Society Press.

[6] A. Bondavalli, I. Mura, and K. S. Trivedi. Dependability modelling and sensitivity analysis of scheduled maintenance systems. In *EDCC-3 European Dependable Computing Conference*, Prague, Czech Republic, 1999. Springer Verlag.

[7] E. Çinlar. *Introduction to Stochastic Processes*. Prentice-Hall, 1975.

[8] H. Choi, V. G. Kulkarni, and K. S. Trivedi. Markov Regenerative Stochastic Petri Nets. *Performance Evaluation*, 20:337–356, 1994.

[9] G. Ciardo, R. German, and C. Lindemann. A characterisation of the stochastic process underlying a stochastic petri net. *IEEE Trans. on Soft. Eng.*, 20:506–515, 1994.

[10] J. B. Dugan. Automated analysis of phased-mission reliability. *IEEE Trans. on Reliability*, R-40:45–52, 1991.

[11] J.B. Dugan, K.S. Trivedi, R.M. Geist, and V.F. Nicola. Extended Stochastic Petri Nets: applications and analysis. In *PERFORMANCE'84*, Paris, France, 1984.

[12] J.D. Esary and H. Ziehms. *Reliability analysis of phased missions*, pages 213–236. SIAM Philadelphia, 1975.

[13] P. M. Frank. *Introduction to System Sensitivity Theory*. Academic Press, 1978.

[14] J.F. Meyer, D.G. Furchgott, and L.T. Wu. Performability evaluation of the SIFT computer. In *FTCS'79 - IEEE Fault-Tolerant Computing Symposium*, pages 43–50, Madison, Wisconsin, USA, 1979. IEEE Computer Society Press.

[15] I. Mura, A. Bondavalli, X. Zang, and K. S. Trivedi. Dependability modelling and evaluation of phased mission systems: a DSPN approach. In *DCCA-7 - IFIP Int. Conference on Dependable Computing for Critical Applications*, pages 299–318, San Jose, CA, USA, 1999. IEEE Computer Society Press.

[16] A. Reibman and K.S. Trivedi. Numerical transient analysis of Markov models. *Computers and Operation Research*, 15:19–36, 1988.

[17] A. Rindos, S. Woolet, and I. Viniotis. Exact methods for the transient analysis of non-homogeneous continuous-time Markov chains. In *2-nd International Workshop on the Numerical Solution of Markov Chains*, Raleigh, NC, USA, 1995.

[18] M. Smotherman and K. Zemoudeh. A non-homogeneous Markov model for phased-mission reliability analysis. *IEEE Trans. on Reliability*, R-38:585–590, 1989.

[19] A. K. Somani, J. A. Ritcey, and S. H. L. Au. Computationally-efficent phased-mission reliability analysis for systems with variable configurations. *IEEE Trans. on Reliability*, R-41:504–511, 1992.

[20] A. K. Somani and K. S. Trivedi. Phased-mission systems using boolean algebraic methods. *Performance Evaluation Review*, pages 98–107, 1994.