Modeling and Analysis of a Scheduled Maintenance System: a DSPN Approach.

Roberto Filippini and Andrea Bondavalli, *Member, IEEE Computer Society*

Abstract.

This paper describes a way to manage the modeling and analysis of Scheduled Maintenance Systems (SMS) within an analytically tractable context. We chose a significant case study having a variety of interesting features like a heavily redundant architecture and a test and maintenance policy whose execution is made on-line without halting the system. We apply a methodology we previously developed based on the Deterministic Stochastic Petri Net (DSPN) approach where the underlying stochastic process is Markov regenerative (MRGP) solved in our setting with efficient analytical solution method. The model construction and its analysis have been carried out with the help of a tool for the modeling and the dependability evaluation of the Phased Mission Systems (PMS). We exercise our methodology with such case study, to check whether it can master real and complex SMS problems and compare its efficacy with traditional approaches (fault trees). At the same time the paper investigates the problem of the optimal tuning of a maintenance program, giving a useful decision support tool to evaluate the system performance since the early design stage.

Index Terms: Scheduled Maintenance Systems, Deterministic and Stochastic Petri Nets, Analytical modeling and evaluation, Safety, Performability

1 Introduction

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

It is good practice to minimize corrective maintenance by optimally tuning the scheduled maintenance program. Usually this requires finding the proper set of actions and their timed sequence that best satisfy dependability requirements subject to budget constraints. In most cases this is a very though task involving a multi-parametric optimum problem whose solution needs an accurate knowledge of the system behavior, usually represented by some model of the system. Any scheduled maintenance program is periodically subject to a complete review according to a revision procedure (for instance the RCM [11]) in order to discover and correct its weak points. Just to reduce the amount of effort needed in this phase, it is very important to define an accurate model of the system accounting for components failure rates and modes.

From the modeling point of view, a system under scheduled maintenance program (SMS) can be seen as a multiple phased system (MPS). Each phase is associated to the configuration of the system during some time interval (a part of the -or the entire- system being actually maintained or operative [5]), while the scheduled maintenance program drives phase changes. A complex stochastic process that includes failure processes and maintenance actions governs the behavior of the system. Under reasonable assumptions (e.g. constant failure rates and

constant duration of the phases) the stochastic process for the system is a Markov regenerative one, where the maintenance program establishes the renewal sequence while the subordinate processes in each phase are Markov processes.

The work described in this paper is directed towards the experimentation of our new modeling and evaluation approach [12]. This methodology, in the context of SMS, suggests the adoption of the Deterministic and Stochastic Petri Nets (DSPN) as a modeling formalism and relies upon the Markov Regenerative Processes (MRGP) theory for the model solution. Due to their high expressiveness, DSPN models are able to cope with the dynamic structure of MPS and allow defining very complex model in a concise way. These models are solved with a simple and computationally efficient analytical solution technique based on the divisibility of the MRGP underlying the DSPN of the MPS [12, 13]. This approach is fully integrated in the DEEM tool [4], specifically tailored for the dependability modeling and evaluation of MPS.

The SMS problem we are attaching in this work is a case of a very critical system where the maintenance has to be executed on-line without interrupting the service provided. More precisely we model and analyze the Reactor Protection System (RPS) in use at the Westinghouse's nuclear plants [9]. The service delivered from this system is to assure the safety function or protective action to the nuclear plant in order to prevent and reduce the risk of the potentially catastrophic events [7, 8, 10]. The safety function is associated to the execution of the reaction process shutdown. The most important dependability measure of such system is its availability to correctly perform the safety function when needed, in other words, the safety on demand. Previous studies used a fault tree modeling approach whose top event was the availability of the safety function [8] others collected a huge amount failure data of the system components [9]. We have instead built the DSPN model of such system.

The purpose of this work is twofold. On the one side we want to exercise our methodology, to check whether it can master real and complex SMS problems and compare its efficacy with

traditional approaches (fault trees). On the other side, we want to investigate the problem of the optimal tuning of a maintenance program, in order to provide a useful decision support tool to evaluate the system performance since the early design stage.

The rest of this paper is organized as follows. Section 2 describes our case study from a functional point of view. Section 3 contains the model of the system according to the DSPN modeling approach implemented by DEEM. Section 4 contains numerical evaluations of the system availability and performability, and sensitivity analyses to the main parameters. Finally section 5 presents some concluding remarks including comparisons of our approach with previous studies on the same system and data about our models and their solution time.

2 System description

The Westinghouse Reactor Protection System (RPS) is a complex device comprising numerous electronic and electromechanical components. Its task is to generate an automatic shutdown of the mission (i.e., the nuclear reaction) anytime a potentially catastrophic event occurs in the nuclear plant [9]. Catastrophic events are those events that could lead the plant in a state where the risks to damage things, people and the environment are very high. The *safety function* performed by the RPS corresponds to stop the nuclear plant reaction and to lead the plant in a safe state. The RPS contribution to the safety of the plant is represented by the availability of its safety function whose evaluation (in term of minimal requirement) is made with the Risk analysis of the operational data [3, 8].

From a functional point of view, the system, depicted in Figure 1, consists of four segments connected in series: the channels, the trains, the breakers and the rods. The channels have the role to continuously monitor and process a certain number of physical quantities (temperature, pressure and many others) and to generate a signal as soon as a single measure exceeds its set point value. The trains process the signals coming out from the four channels

and generate the so called *trip signal* according to a 2 of 4 majority voter logic. A redundancy of four channels allows to tolerate 2 simultaneous faults and to maintain fault tolerance capabilities in case of reconfigurations due to channel failures or maintenance. The set of monitored variables (of quite different nature) contributes to the same trip signal generation according to the principle of the functional diversity.

The trip signal starts the safety action that is completed by the breakers with the descent of the rods into the reactor core and the shutdown of the nuclear reaction. The general fault tolerance design principles adopted here are the tolerance of at least at a single fault, the modular independence, the functional and structural diversity and the testability of the components [7]. This latest feature consists in the numerous built in test facilities to periodically check the system without interrupting the service.

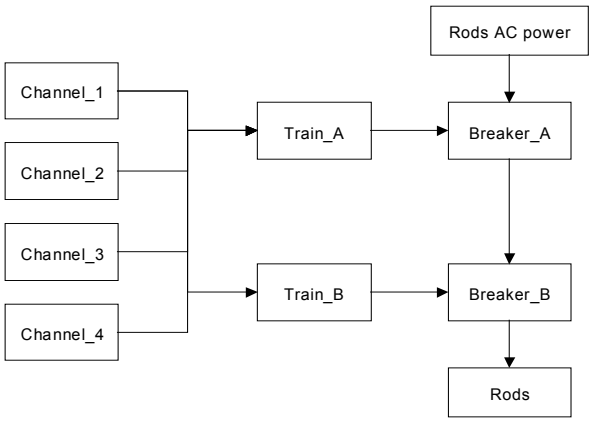

Figure 1. RPS Architecture

The automatic generation of the trip signal is not the only way to accomplish the safety task. Indeed, all the signals arising from the channels segment are available in the control room panel so that it is possible to manually generate the trip signal, if needed. Anyway, we do not consider the contribution of any human operator to the safety as well as the contribution of any support system like generators, power supply, testing circuitry and others not included in the RPS architectural boundaries.

2.1 Channels segment.

The channels segment consists of four identical independent channels (1-4) performing simultaneously the same function. Each channel converts the physical signal from the sensors into digital signals and elaborates them to generate a signal for each measure exceeding the set point value. Usually this happens when the process automatic control device fails to maintain the variable under control. It can happen also when a spurious trip has been generated, an event, however, that does not affect safety.

A channel has *n* processing lines, one for each measure, consisting of one sensor, one signal processor and A/D converter and one bi-stable whose threshold value is the set-point for the monitored variable, shown in Figure 2. Due to the series link between the sub-components, we will consider the processing line as a single component having as failure rate the sum of the failure rates of the sub-components.

Figure 2. Signal processing line

2.2 Trains segment.

The trains segment consists of two identical independent trains (A and B) each receiving the output signals from the channels (four for each variable). Each train, detailed in Figure 3, is composed of *n* SSL (Solid State Logic) modules (one for each variable), connected to a module which generate the shutdown command. The SSL takes the four signals from the channels and generates the trip signal according to a 2-out-of-4 voting logic. Just one of the *n* SSL of the train voting for the trip is sufficient to generate the trip signal for the RPS. The trip signal drives two devices, the UV (Under Voltage) and the AS (Auto Shunt trip) which generate the same shutdown command according to the principle of structural diversity (same function performed by different devices). Normally (absence of trip signal) the UV state is on

(energized) and the AS state is off (de-energized). The signal trip generation inverts the state of the devices so that it is enough one state change to start the shutdown command.

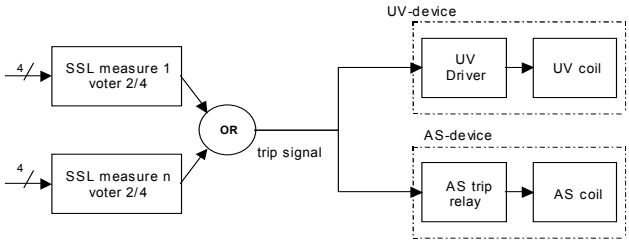

Figure 3. Train Architecture

2.3 Breakers segment.

The reactor trip breakers (RTB) are electromechanical devices that during normal operational condition keep the rods outside the reaction core. Between the rods control system and the AC power supply there is a double circuitry, the primary and the secondary one, joint together as shown in Figure 4. Normally, in absence of shutdown command, a closed path (involving primary or secondary circuitry) connects the power supply to the rods control system. The opening of the circuit assures the rods to fall by gravity into the reactor core and stop the reaction. There are about 50/60 rods, however is not necessary that all the rods drop into the reactor, a number of at least ten of them is enough to assure the completion of the system shutdown.

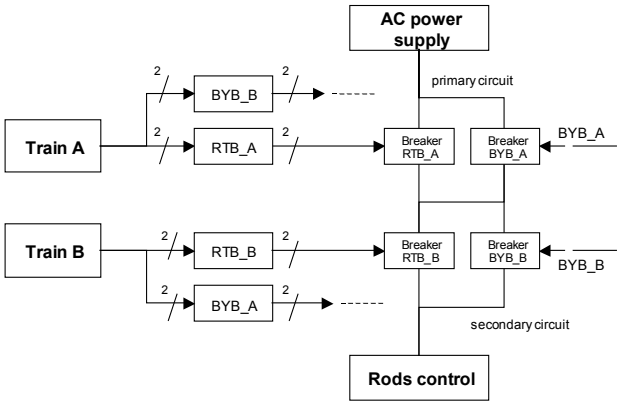

Figure 4. Breakers Architecture

The breakers behave like switches, opening the circuit any time the shut down command has been generated. The primary circuitry has two breakers in series (RTB A and B), driven respectively by the train A and B. The secondary circuitry is identical to the primary and consists of two bypass breakers (BYB A and B). During normal operational condition, the closed path is the primary circuit while the secondary is opened. During the test and maintenance phase, the path is formed by the part of primary circuit involving the breaker still working, and the BYB temporary substituting the RTB under maintenance. In this phase, both the RTB and the BYB are driven by the signal coming from the train still in service. Opening of either breaker disconnects the AC power from the rods control system, which result in the rods dropping into the reactor core.

2.4 Test and maintenance program.

The test and maintenance (T&M hereafter) program ensures the system can be maintained in a state that meets the necessary reliability goal for each single component and the dependability requirement for the service provided. It is composed of a collection of periodical checks performed on-line on the system components without interrupting the service, covering the time between two consecutive major overhauls when the plant is shut down for a long period. The benefits of such a testing policy are to detect non self-announcing faults that could have been accumulated in the RPS so to affect its protective function. The components subjected to T&M are put out of service and the system, left with less redundancy, is less resilient to faults for the time needed for the check.

The original T&M scheduled program [9] consists of two main perfectly staggered scheduled maintenance sequences, one for the channels segment and one for the trains-breakers segment whose duration is shown in Table 1.

The perfectly staggered scheduled maintenance policy has proved to be less compromising to the system availability than the simultaneous T&M policy (i.e. all the channels tested at the

same time, one after the other). The Rods are tested every 18 months, but we do not include them in the system model.

Subject of the T&M	T&M period	Mean length
Channels	3 months	4h (per trip signal)
Train-Breaker	2 months	2h

Table 1. T&M programs

The T&M program is the overlapping of two T&M periodical sequences, respectively of 3 ad 2 months length so that it needs six months (i.e. the period of T&M program) to test and maintain the whole RPS. The maintenance schedule determines four different system configurations depending on the set of components that are operational or under T&M.

1. Full redundancy phase: all components available.
2. T&M channel phase: one channel under T&M.
3. T&M train-breaker phase: one train-breaker under T&M.
4. T&M channels and train-breaker: one channel and one train-breaker under T&M.

Configuration 4 is the less redundant one and is the most critical for availability. It is possible to avoid the system assuming this configuration by anticipating the train breaker T&M. This way, the system does not suffer of the simultaneous loss of channels and trains-breakers redundancy.

2.5 Failure data collection and classification

A failure data collection program has been defined in the LER (Licensee Event Report) and NPRDS (Nuclear Plant reliability data System) failure records and it is the result of more than ten years (1984-1995) of operational failure data collection at the Westinghouse plants [9]. The data collected have been only those events potentially affecting safety as identified by a FMECA previously performed. Due to their non self announcing nature, the way to detect

such failure events has been to test the components during their T&M phase (planned test) or after a shutdown (unplanned test).

A failure event is classified as *random*, when it involves the failure of a single components, or *common*, when it involves the failure of more than one components of the same type [8, 15]. The most critical events for the availability of the RPS safety function are common cause failure (CCF) events for the reason they drastically reduce the redundancy of a part of the system causing in most cases the unavailability of the safety function.

3 System modeling

The most important measure of interest for the system we are studying is the availability of the RPS safety function depending on the T&M scheduled program. The other measure that usually applies to SMS is Performability. Performance related measures distinguish from the other dependability measures since they are usually associated to an optimal problem [14, 16]. Costs (not necessary monetary costs) and benefits are put together in order to properly weight the various alternatives and best tune the design parameters. Efficacy (did I reach the goal?) and the efficiency (how did it cost to reach it?) are put together to find their right balance. In the RPS system this cat take the form of the sum of the T&M cost and the cost due to the unavailability of the safety function. The maintenance costs depend on the frequency of the T&M program checks and on their quality. More frequent and accurate the checks and more expensive will be the maintenance. The unavailability costs are those related to the risk. The risk is directly proportional to the system failure rate, in its turn depending on the maintenance frequency and check quality. Despite performability is not a major issue for the RPS (availability of the safety function must be maximized), in most SMS constrains exist on the minimal dependability requirements and the maximum T&M program budget. Therefore we will show how such measure can be analyzed within our framework.

From the modeling point of view, the T&M program determines a discontinuity in the RPS configuration caused by the temporary unavailability of the components subjected to T&M check. Therefore it is possible to represent the entire operational life (between two major overhauls) split into different periods of deterministic duration called *phases*. This feature makes the SMS belonging to the Multiple phased system (MPS) class for which we have proposed a modeling and evaluation methodology [12], supported by the DEEM tool [4].

Using DEEM, the net is split into two logically distinct sub-nets: the Phase Net (PhN) representing the schedule of the various phases, each one of deterministic duration, and the System Net (SN) representing the behavior of the system. Each net is made dependent on the other by marking-dependent predicates that modify transition rates, enabling conditions, reward rates etc.

Marking dependent attributes are easily defined through the DEEM property window associated to each object (transition, arc, place). Moreover DEEM allows to use parameters in the definition of the models that can be later assigned values or ranges in defining the studies to perform (through the study definition window). It also possesses a 'measures' window, through which it is possible to define the dependability and performability figures of interest for the system modeled. Once the definition of the study and of the measure is completed, the execution of a single study (namely, a collection of experiment one for each parameter setting) is automatically performed and the results are returned in a file and can be easily viewed or plotted. For further details about the tool see [4] while the SW package is currently available at http://bonda.cnuce.cnr.it/DEEM.

The main assumptions we made for modeling the RPS are the following:

(1) The failure rates of each single component are constant.

(2) The T&M time duration is deterministic.

(3) A component entering a T&M phase in good condition may fail during T&M with a probability *e* (i.e. error of the testing action)

(4) A failed component is detected as failed and repaired during a T&M phase with a probability *c* (i.e. coverage of the repair action)

(5) If a failed component, is detected and repaired during a T&M phase, at the end of the T&M phase it is as good as new

(6) We consider just one monitored variable.

Assumption (3) and (4) allow describe the quality of the T&M checks with respect to the detection coverage and the possibility of human error during the T&M phase. Assumption (5) implies an ideal repair any time a fault has been detected. Assumption (6) allows reducing the complexity of the system in terms of number of components involved, still representing the worst case for the availability of the safety function. In fact, if more variables are processed the probability of detecting catastrophic events increases. The spurious trip probability increases as well, but this does not harm safety.

Moreover we point out that we intentionally consider the effect of the T&M scheduled program on the failure process disregarding any type of corrective maintenance. Although corrective actions are taken anytime a self-announcing fault occurs, we limit to the case where we consider non self-announcing faults only: the sole possibility to detect the faults and repair them is to wait for the nearest scheduled check (no way to anticipate it).

Assumptions (1) and (2) provide sufficient conditions to identify a Markov regenerative process for the system and an underlying Markov process in each phase and thus for assuring the existence of an analytical solution [1, 2, 6, 13].

3.1 Phase net.

The PhN, depicted in Figure 5, represents the execution of the various phases according to the T&M program and it is cyclic for the reason the program is periodical. A token in a place of the PhN (except for the *count* and the *stop* places) represents the phase being executed. *count* is the place where a token is put at the completion of a cycle, whereas, when a token is in *stop*

a decision is taken whether going on, performing one more cycle, or stopping, depending on the *max_count* variable value.

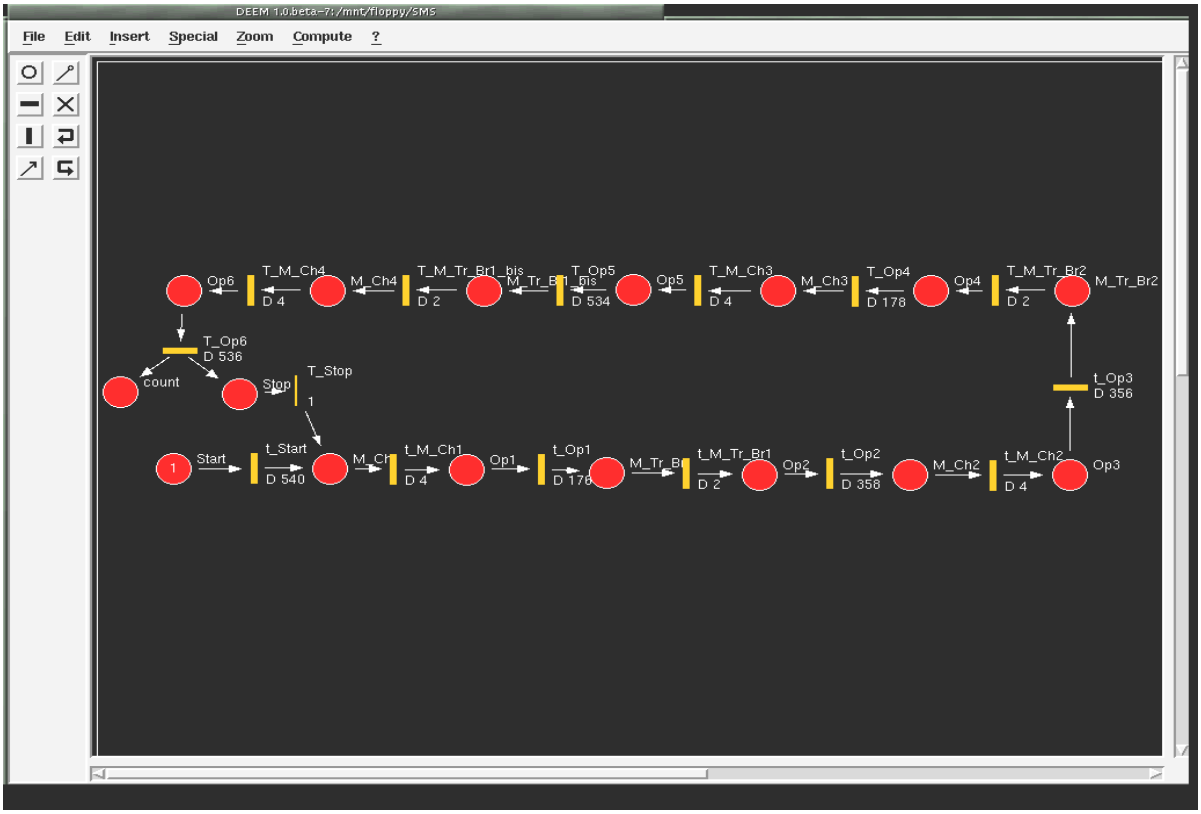

Figure 5. Phase Net

Figure 5 is a snapshot of the DEEM editing window. In the following, just to avoid an excessive waste of space (the models become really very large), we will compact the net pictures without showing their representation with DEEM.

The periodicity of the T&M program determines a periodical behavior of the system. By considering the aging state of the components (waiting for their turn to go under T&M) and the T&M program we can recognize that after nine months from the start (6480 hours) the system is exactly in the same state encountered after three months (2160 hours). Therefore, after an initial transient of three months, the system has a period of six months after which it repeats the same behavior. The description of the PhN transitions is shown in table 2.

Immediate transition	Enabling condition
T_Stop	Mark(Count) < max_count
Timed transition	**Firing time (h)**
t_M_Ch1,2,3,4	4
t_M_Tr-Br1,2 M_Tr-Br1_bis	2
t_Start	540
t_Op1	176
t_Op2	358
t_Op3	356
t_Op4	178
t_Op5	534
t_Op6	536

Table 2. PhN transitions

3.2 System net.

The SN represents the stochastic behavior of the system subject to failures and maintenance checks and repairs. It is divided into three main sub-networks: one for the channels, one for the Trains and the last for the Breakers. The components in the Channels and Trains sub-networks are modeled using four places to represent respectively the working state (Up place), the failed state (Fail place) and the T&M states for the component entering maintenance after having failed (T&M_fail place) or not (T&M_up place). Random and common cause failures are modeled separately by exponential transitions, whose firing rate depends on the phase executed. The maintenance checks and repairs are represented by instantaneous transitions enabled at the start and at the end of each T&M phase. From the Up place we can reach the T&M_up place as well the T&M_fail place depending on the maintenance error probability *e* (assumption 4). From the Fail place we can reach the T&M_fail place. At the end of the T&M phase the tokens in the T&M_up places go back to the Up_place while the tokens in the T&M_fail place can reach the Up place with probability *c* and the Fail place with probability 1-*c* (assumption 3).

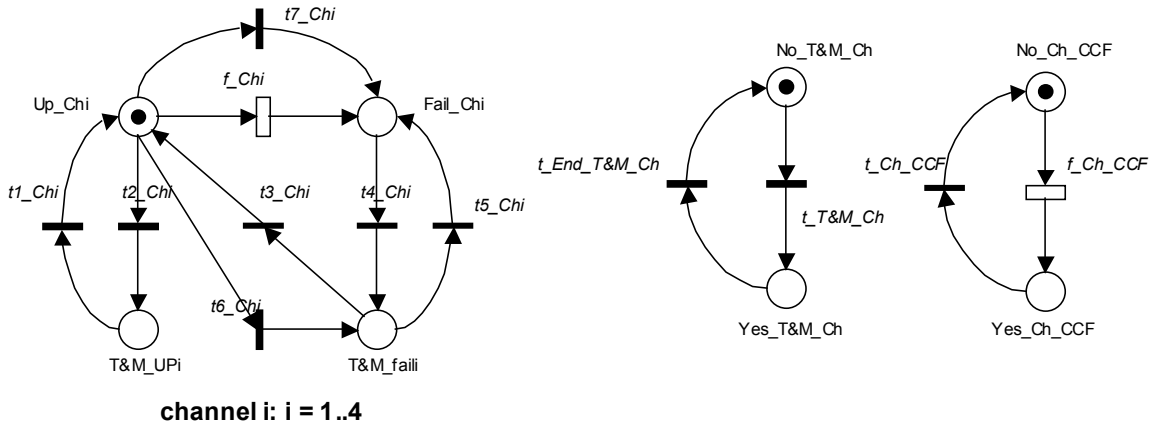

Figure 6. Channels sub-net

The channels sub-net shown in Figure 6 consists of four identical models describing the random failure process and the maintenance check for each channel (just one of them is depicted in the left side of the Figure). The common cause failure is modeled by the immediate transition t7_Ch1 whose enabling condition depends on the marking of the place yes_ch_CCF. The T&M_channel net is used to express the enabling conditions in a more compact way.

Table 3 shows the transitions (with enabling conditions, probabilities and rates) of the channels sub-net. Figure 7a shows the DEEM property window of the immediate transition t2_Ch1 while Figure 7b shows the DEEM property window of the exponential transition f_Ch_CCF, respectively.

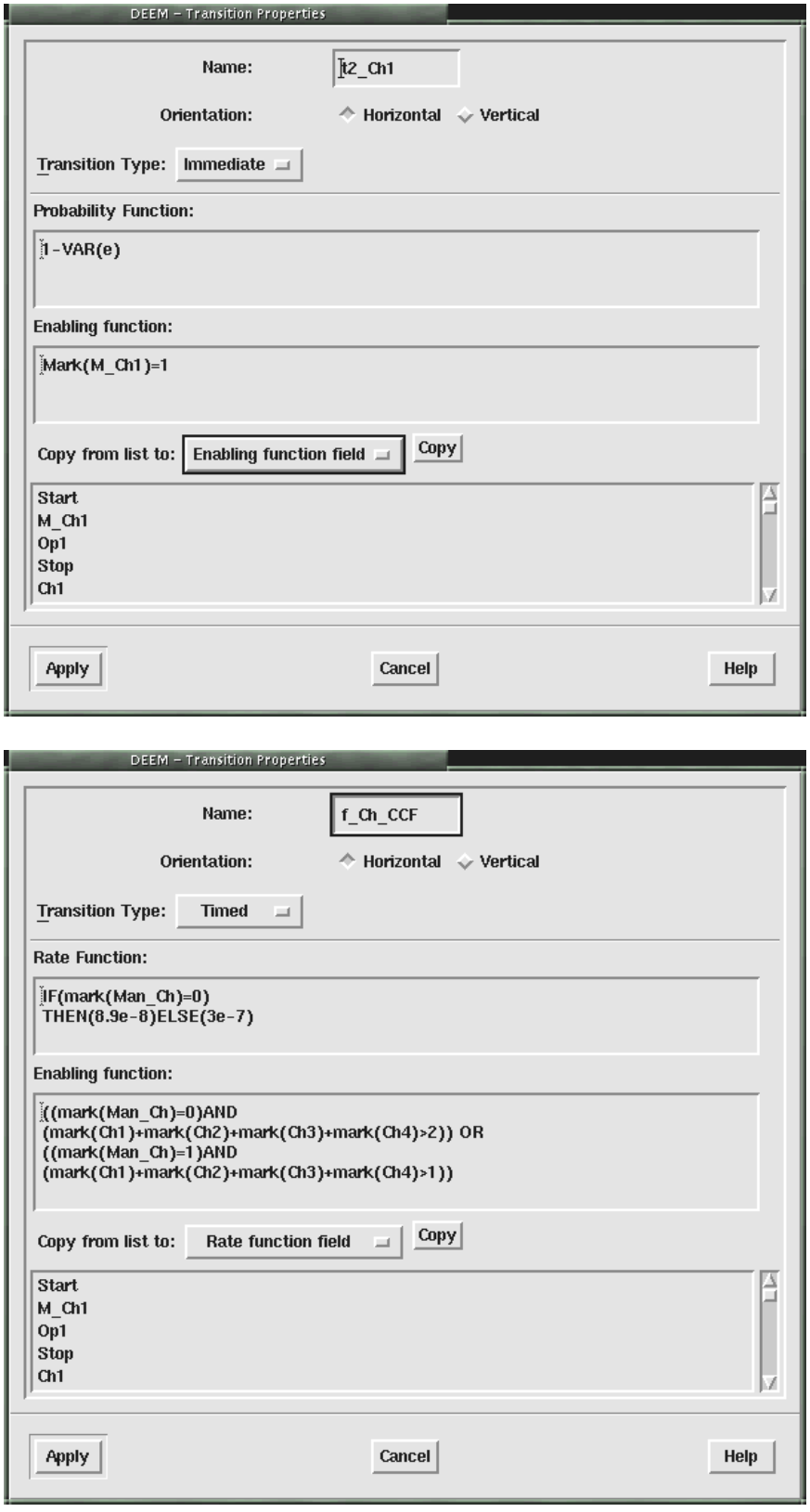

Figure 7. Deem property window of the immediate transition t2_Ch1 (a) and of the exponential transition f_Ch_CCF (b)

Immediate transition	**Enabling condition**	**probability**
t1_Ch(i)	#(M_Ch(i)) = 0, i = 1..4	
t4_Ch(i)	#(M_Ch(i)) = 1, i = 1..4	
t3_Ch(i)	#(M_Ch(i)) = 0 i=1..4	Probability = c
t5_Ch(i)	#(M_Ch(i))=0 i=1..4	Probability = 1 - c
t2,_Ch(i)	#(M_Ch(i))=1 i=1..4	Probability = 1 - e
t6,_Ch(i)	#(M_Ch(i))=1 i=1..4	Probability = e
t7_Ch(i)	#(Yes_Ch_CCF) = 1, i = 1..4	
t_T&M_Ch	∑#(M_Ch(i)) = 1	
t_End_T&M_Ch	∑#(M_Ch(i)) = 0	
t_Ch_CCF	∑#(Up_Ch(i)) = 0	
Exp transition	**Firing rate**	**Enabling condition**
f_Ch1,2,3,4	λ_{Ch}	#(Up_Ch(i)) = 1
f_Ch_CCF	$\lambda_{Ch\_CCF3/4}$	#(No_T&M_Ch) = 1
	$\lambda_{Ch\_CCF2/3}$	#(No_T&M_Ch) = 0

Table 3. Channels transitions

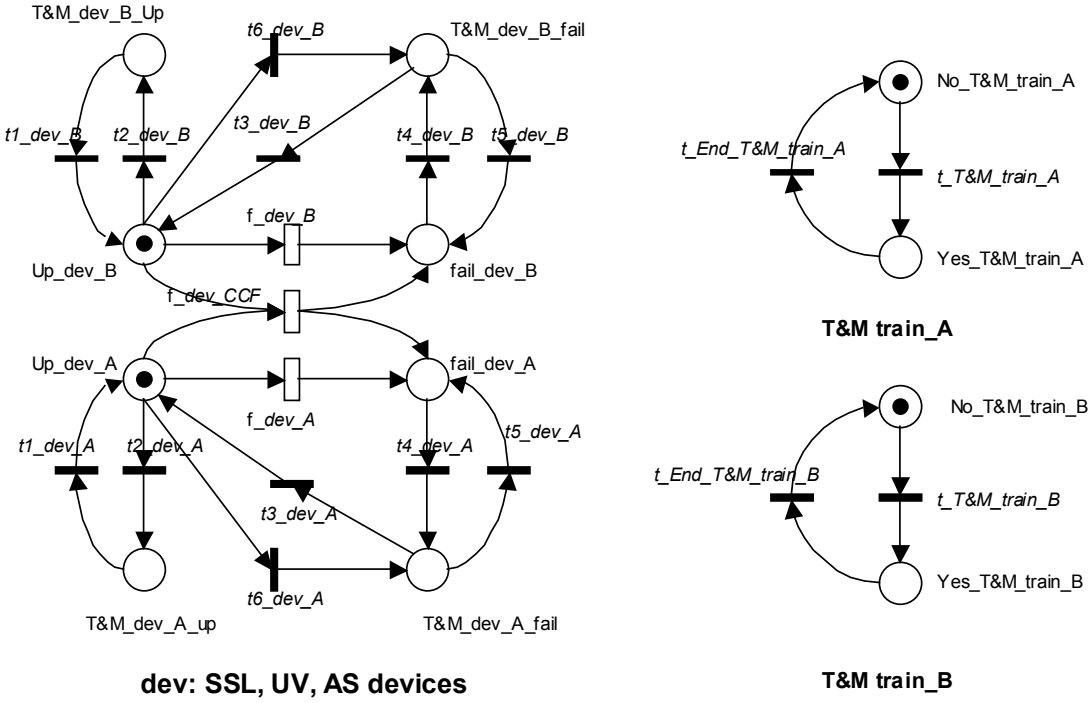

Figure 8. Trains subnet

The train model shown in Figure 8 consists of three identical sub-models, for the SSL device, for the UV device and for the AS device respectively (just one of them is depicted in the left side of the Figure). Each sub-model has the same structure of the channel model for random failures and the T&M activities. Only the CCF event is represented here with an exponential transition enabled to fire as long as the A and B devices (for instance SSL A and B) are in their Up places.

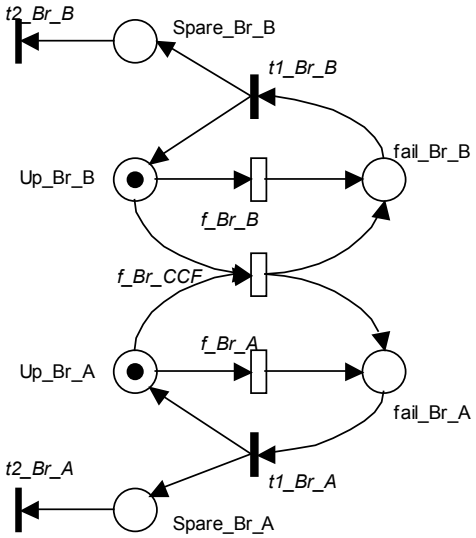

Figure 9. Breakers subnet

The breaker model differs from the previous ones and it is shown in Figure 9. During the breaker T&M phase a spare breaker (BYB) replaces the original breaker so that we have always two breakers on service in every phase. We did not consider the possibility to miss the insertion of the spare, or to find it failed for any reason. Moreover, we assume perfect failure detection and no possibility to fail the breaker under T&M. This choice is due to the higher intrinsic reliability and robustness of the breakers with respect to the other components.

Exponential transition.	**Firing rate**
f_SSL_A	$\lambda_{SSL}+\lambda_{SSL\ CCF}$ #(Yes_T&M_train_B)
f_SSL_B	$\lambda_{SSL}+\lambda_{SSL\ CCF}$ #(Yes_T&M_train_A)
f_SSL_CCF	$\lambda_{SSL\ CCF}$
f_UV_A	$\lambda_{UV}+\lambda_{UV\ CCF}$ #(Yes_T&M_train_B)
f_UV_B	$\lambda_{UV}+\lambda_{UV\ CCF}$ #(Yes_T&M_train_A)
f_UV_CCF	$\lambda_{UV\ CCF}$
f_AS_A	$\lambda_{AS}+\lambda_{AS\ CCF}$ #(Yes_T&M_train_B)
f_AS_B	$\lambda_{AS}+\lambda_{AS\ CCF}$ #(Yes_T&M_train_A)
f_AS_CCF	$\lambda_{AS\ CCF}$
f_Br_A,B	λ_{BR}
f_Br_CCF	$\lambda_{BR\ CCF}$

Table 4. Exponential transitions firing rate of the trains and the breakers submodels.

Table 4 shows the exponential transitions firing rate while Table 5 shows the enabling conditions and probabilities related to immediate transitions of the trains and the breakers submodels.

Immediate transitions	**Enabling conditions**	**Probability**
t1_dev_A,B	#(Yes_T&M_Train_A,B) = 0	
t4_dev_A,B	#(Yes_T&M_Train_A,B) = 1	
t3_dev_A,B	#(Yes_T&M_Train_A,B) = 0	Probability = c
t5_dev_A,B	#(Yes_T&M_Train_A,B) = 0	Probability = 1 - c
t2_dev_A,B	#(Yes_T&M_Train_A,B) = 1	Probability = 1 - e
t6_dev_A,B	#(Yes_T&M_Train_A,B) = 1	Probability = e
t1_Br_A	#(Yes_T&M_Train_A) = 1 AND #(Spare_Br_A) = 0	
	#(Yes_T&M_Train_A) = 0 AND #(Spare_Br_A) = 1	
t1_Br_B	#(Yes_T&M_Train_B) = 1 AND #(Spare_Br_B) = 0	
	#(Yes_T&M_Train_B) = 0 AND #(Spare_Br_B) = 1	
t2_Br_A	#(Yes_T&M_Train_A) = 0	
t2_Br_B	#(Yes_T&M_Train_B) = 0	
t_T&M_train_A	((#(count)%2 = 0) AND (#(M_Tr-Br1) + #(M_Tr-Br1_bis) =1)) OR ((#(count)%2 = 1) and (#(M_Tr-Br2) = 1))	
t_T&M_train_B	((#(count)%2 = 1) AND (#(M_Tr-Br1) + #(M_Tr-Br1_bis) =1)) OR ((#(count)%2 = 0) AND (#(M_Tr-Br2) = 1))	

Table 5. Enabling conditions and probabilities related to immediate transitions of the trains and the breakers submodels.

4 Model evaluation and system analysis

This Section describes first which are the dependability measures studied and how they are defined in the DEEM model. The default values assigned to the model parameters are then shown and the relevant parameters to vary while performing sensitivity analysis are identified. Finally several results obtained by evaluating the model are presented and discussed.

4.1 Dependability measures and parameter settings

The 'measures' window provided by DEEM permits to define any reward measure as a Boolean expression, function of the net marking. The tool permits to specify the measure as instantaneous, cumulative or mean value.

The safety function availability, A *(t)* (i.e. the RPS availability) corresponds to the following expression on the markings of our model:

RPS is available IF

{(#(Channels Up) ≥ 2) AND *((Train-breaker A is available)* OR *(Train-breaker B is available))}*

Train-breaker is available IF

{(SSL is Up) AND *((UV is Up)* OR *(AS is Up))* AND *(Breaker is Up)}*

The above expression has been properly translated into a DEEM reward measure. We will study its instantaneous and mean value.

As already mentioned performability is not a major issue for the RPS. Still we show how it can be analyzed since it is very important for a wide class of SMS. The cost (performability) function we define (just for the sake of an example, without any pretension of truthfulness) is the following:

$C(t) = C_{Risk}[1-A(t)]+C_{Man}P_{Man}$

C_{Risk} =1000

C_{Man} =1

P_{Man} = IF *(Phase executed ≡ T&M)* THEN 1 ELSE 0

C(t) has been translated into a DEEM reward expression on the markings of our model as well, its cumulated value will be analyzed.

Figure 10 shows the DEEM measures window with the reward expressions corresponding to the availability and cost (performability).

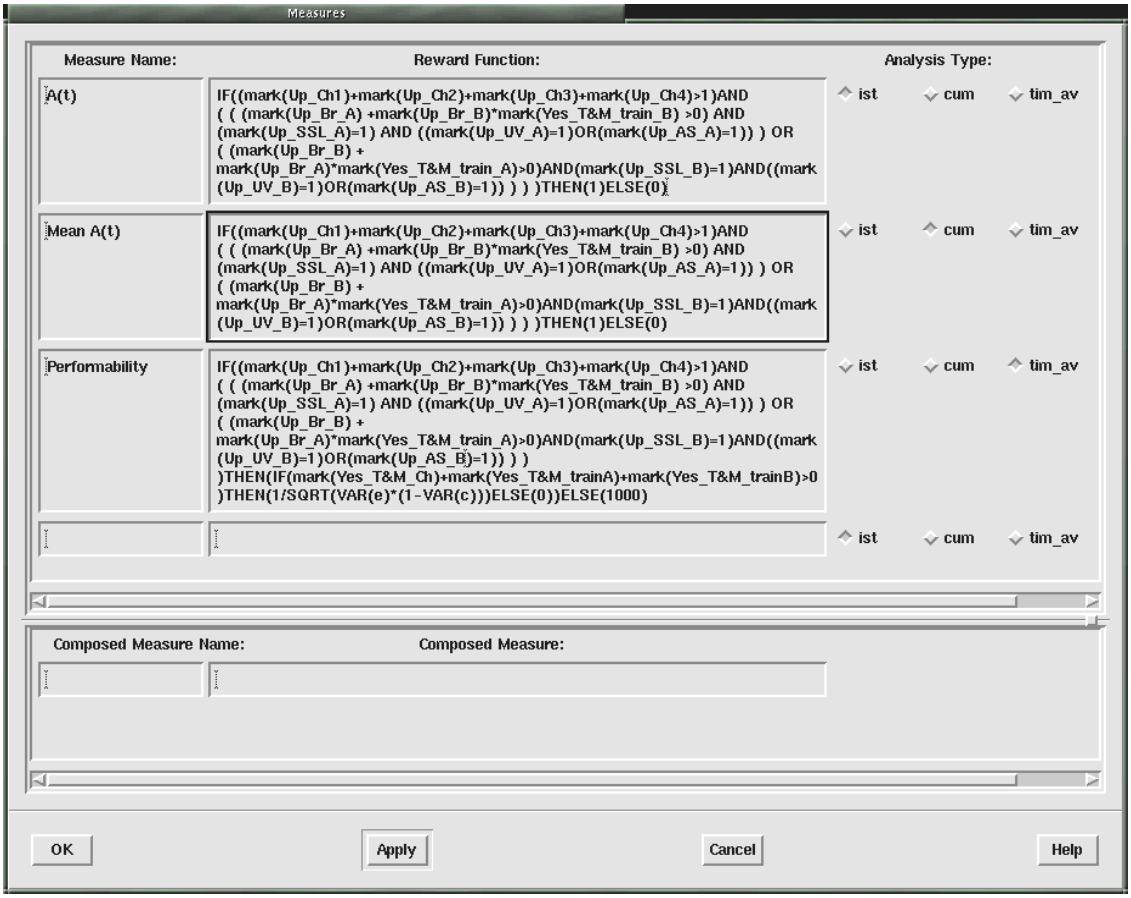

Figure 10. Deem measures setting window

As already mentioned DEEM permits to define several studies. In each study values are assigned to the model parameters, note that two parameters are allowed to vary within some interval or set of values. The result of any study, is a collection of data that can be easily plotted.

Table 6 shows the default values used for the rates of the exponential transitions of the net. These values have been derived from the INEEL (Idaho national Engineering and Environmental Laboratory) reports [9]. In [9] values are given as failures on demands, in other words, the number of failures divided the number of tests, and have been translated into failures per hours.

RANDOM EVENT	**RATE (failure/h)**
Breaker electr-mech. failure	2.5 E-7
AS device failure	4.7 E-6
SSL failure	2.6 E-7
UV device failure	4.1 E-6
Single channel failure	7.0 E-6
CCF EVENT	**RATE (failure/h)**
¾ Channels	8.9 E-8
⅔ Channels	3.0 E-7
Train A e B	1.5 E-8
½ UV device A e B	1.4 E-7
½ AS device A e B	1.6 E-7
½ Breakers mech. A e B	1.2 E-7

Table 6. Failure rates

The numerical solution of our model provides answers to many interesting questions including the variations of the relevant measures to some design parameters. The parameters used in this study for performing sensitivity analysis have been the coverage *c*, the maintenance error *e* and the maintenance frequency.

A parameter *s* (scale factor) has been defined, corresponding to the inverse of the T&M frequency, as a variable multiplying the duration of each operative phase in the PhN net (for instance, VAR(s)*540 will be the length of the first phase). This way the T&M frequency can be changed at will, keeping the same T&M duration.

4.2 Availability of the RPS

The instantaneous availability using the default values of 1, 0 and 1 for *c, e and s* respectively (i.e. ideal coverage, no maintenance error and the original T&M scheduled program) is shown

in Figure 11. The curve shows a periodical trend as expected. The transient period last 3 months and after that the curve has a period of 3 months instead of the 6 months after which the system is back in the same state (Section 3.1) because the two train-breakers A and B are indistinguishable from a statistical point of view. The discontinuities occur at the beginning and the end of a T&M phase.

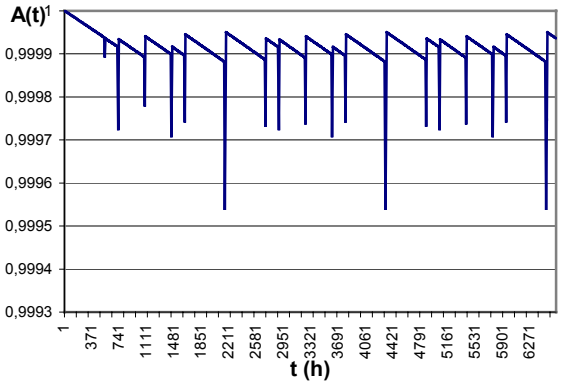

Figure 11. Instantaneous Availability

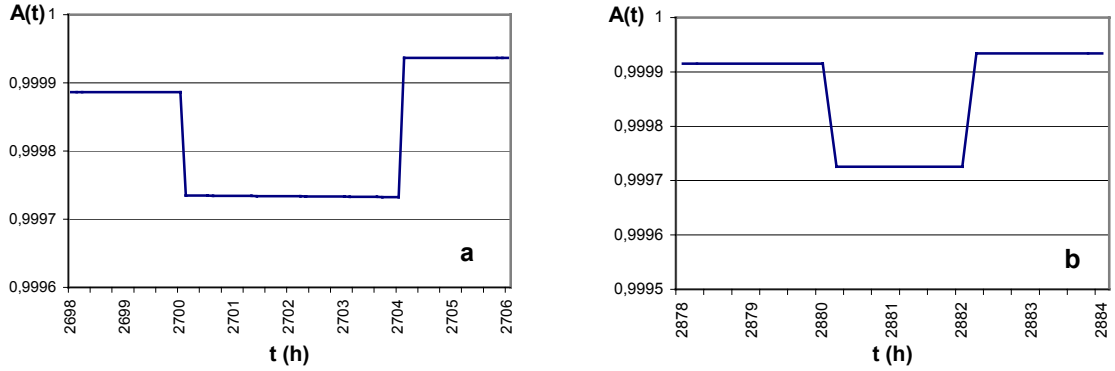

Figure 12. T&M phases

When a part of the system goes under maintenance there is a loss of redundancy and consequently the availability suffers of it, while the restoration of the components determines an availability increase. More detailed plots of the availability through T&M phases are shown in Figure 12a for the channels and Figure 12b for the trains.

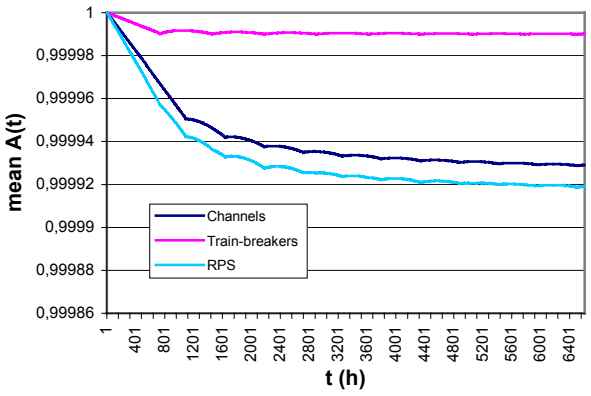

Figure 13. Mean Availability

Figure 13 shows the mean availability curves of the RPS, the channels and the trains breakers for the same settings. As it can be seen the T&M program has the positive effect to stabilize the RPS mean availability to an asymptotic constant value (for this setting 0.99991) that is just the mean value computed in a single period. The Figure shows also how the channel segment is the bottleneck for the RPS availability.

4.3 Sensitivity analysis of the RPS Availability

The efficacy of a T&M program depends on the number of checks executed (T&M frequency), accounted by the scale factor *s*, and on their quality [2, 15, 17] accounted by the coverage parameter *c* and the maintenance error *e*.

Figure 14a shows the mean availability curves for the channels, the trains breakers and the RPS respectively computed at 9 months as a function of *c* (*e* = 0, *s* =1). Figure 14b shows the same measures as function of *e* (*c* = 0.9, *s* =1).

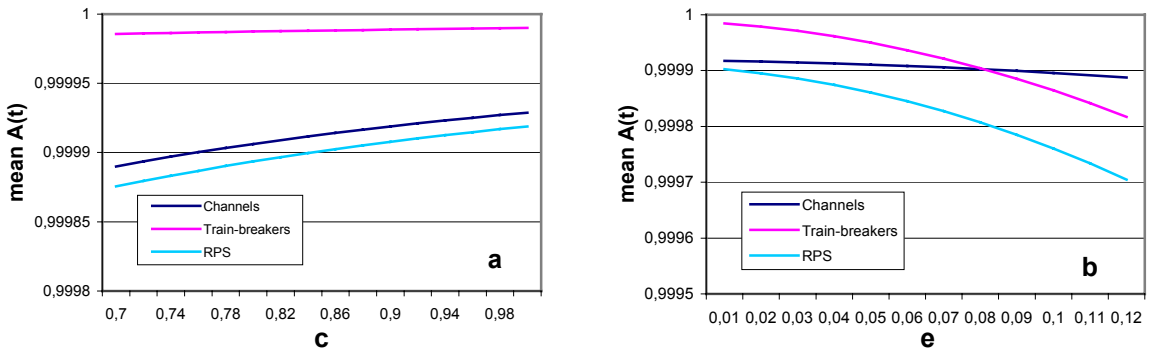

Figure 14. Sensitivity analysis of the mean availability

The availability, as expected, improves at increasing values of *c* (rather smoothly), with the availability of the train-breakers being almost constant. On the contrary, the system appears to be more sensitive to variations of *e*, with the availability worsening for increasing values. Moreover the train-breakers are more sensitive than the channels. In fact, there exists a value where the curves intersect and the train-breaker segment becomes the new bottleneck of the systems. We explain this behavior due to the higher redundancy of the channels segment that makes it less sensitive to increasing maintenance errors.

The curves in figure 12 show (in the chosen setting) a positive effect of T&M on the instantaneous availability. The availability gain depends on the parameter *e* and *c* so we want to analyze for which values of *e* and *c* performing maintenance is convenient or results in a negative gain of availability. Denoting $p(t)$ and $p(t+\Delta t)$ the availability before and after a T&M check (of Δt duration) of a single component we get the following:

$$P(t+\Delta t) = p(t)(1-e)+[1-p(t)+p(t)e]c \geq p(t)$$

$$\Downarrow$$

$$e \leq c[1-p(t)]/[p(t)(1-c)]$$

Figure 15 plots the availability gain as a function of *e* for different values of *c*.

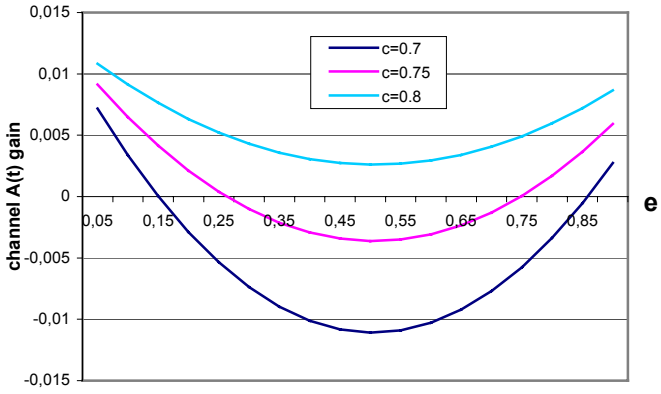

Figure 15. Availability gain due to the single channel T&M check

The availability gain depends on both *e* and *c* but in an apparently strange way. There are two values of *e* corresponding to a zero availability gain. This happens for $c = 0.7$ and $c = 0.75$ while for $c = 0.8$ the curve lies always over zero. Performing T&M on channels is always convenient if the coverage *c* is sufficiently high. Indeed, a high coverage allows tolerate even an excessively high maintenance error.

To explain this is sufficient to consider that a smaller value of $p(t)$ (and a smaller availability of the whole channels segment) is observed in correspondence of a bigger maintenance error. In the case of a big maintenance error, a significant contribute to the unavailability is given by the maintenance itself, (the limit $e = 1$ yields $p(t + \Delta t) = c$ otherwise $p(t + \Delta t) > c$). Actually, this undesired contribute may be absorbed by the fault detection and correction depending on its probability of success.

Another interesting problem is to understand whether it is always true that more frequent maintenance makes the system more available. Actually the execution of each T&M check may bring some risk (or cost). Indeed during each T&M phase, one can observe a loss of availability, as shown in Figure 12. Increasing the T&M checks frequency increase the periods in which the RPS redundancy, and therefore availability, is lower.

However, if one considers the ideal case with $c = 1$ and $e = 0$, it is the case that more frequent maintenance makes the system more available. To show this, take for instance, the channels segment (but this holds for the train-breakers as well).

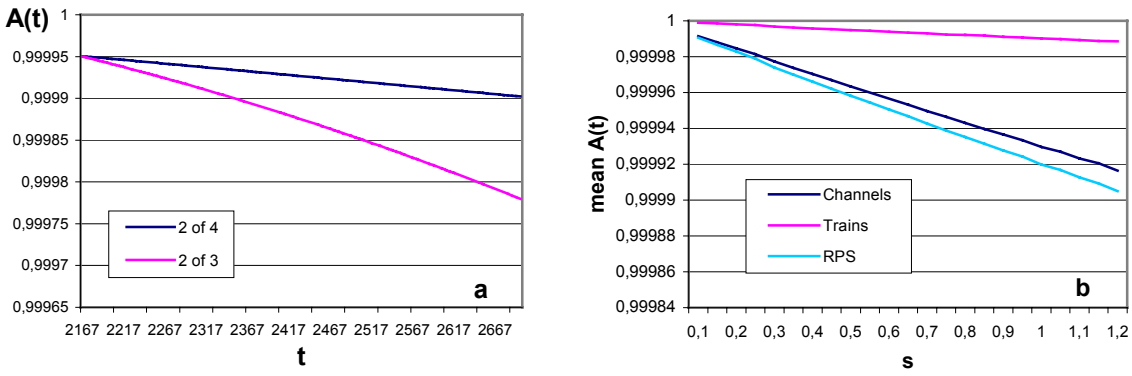

Figure 16. Availability trend in function of T&M frequency

Figure 16a shows the curves of the channels instantaneous availability with four and three channels (T&M phase). The first curve lies always upon the second one and their difference increases with time. So, the longer we wait for the maintenance, the more we pay in term of loss of availability. Moreover, for a continuous checking policy ($s \rightarrow 0$, i.e. the system is continuously performing T&M phases), it becomes negligible. Figure 16b shows the trend of the mean availability for the RPS and the single segments as a function of s.

In a more realistic scenario, where $c < 1$ and $e > 0$, the risk associated to performing each T&M phase is a function of e, and it accumulates depending on the check frequency and the coverage. In this scenario, it is no more the case that more frequent maintenance makes the system more available. A value for s (different from 0) exist which allows to maximize availability.

Figure 17a shows the mean availability of the channels segment as a function of s for different values of e ($c = 0.9$). The curves demonstrate that a value for s exists which maximizes availability. It moves from smaller to bigger values at increasing values for e.

Figure 17b plots the values of *s* for which the highest availability is obtained as a function of *e* (*c* fixed to 0.9). These values increase at increasing *e*.

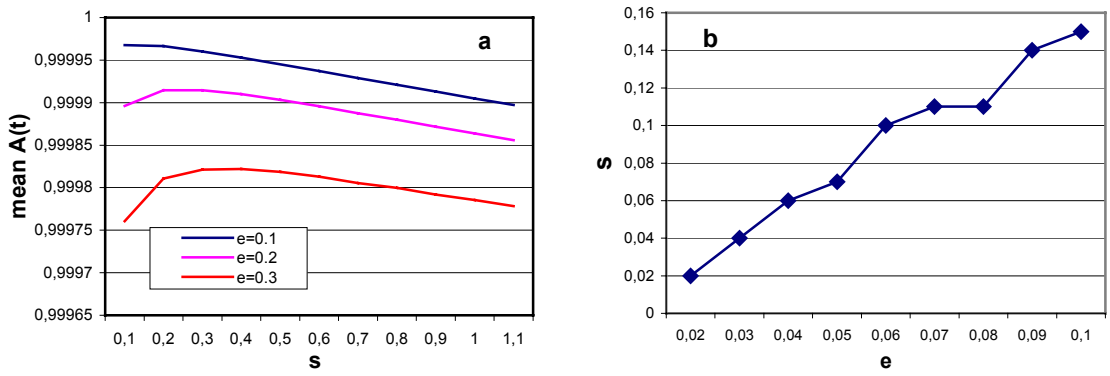

Figure 17. Availability as a function of *s* for different values of *e* *(a)* Scale factor maximizing Availability as a function of *e* (b).

4.4 Performability

We study now the performability aiming at finding an optimal tuning of the T&M frequency using the cost function defined in Section 4.1. Figure 18 shows the plots of C(t) (performability) for the T&M program as a function of *s*, both for the RPS system as a whole and separately for the channels and the train-breakers. The default values for *c* and *e* are used so to compare the result with the original T&M program.

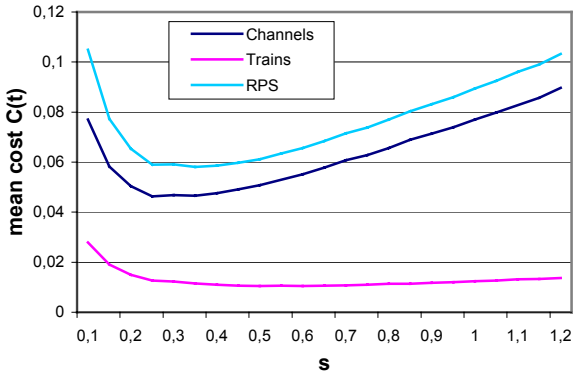

Figure 18. Cost (Performability) of the RPS as a function of s

In all cases a value for *s* yielding the minimum C(t) exists. For the RPS with this setting and this cost function, the value 0.35 for *s*, the scale factor of yields the minimum cost, resulting

in a mean availability of 0.999966 instead of the original 0.99991. If channels and train-breakers are considered separately, two values of *s* can be found: 0.25 for the channels and 0.5 for the trains-breakers. This separate setting of the T&M frequency improves the mean availability to 0.999976, and slightly reduces the cost (5,68e-02 against 5,81e-02). This means that we can best tune our T&M program choosing the T&M frequency separately for each segment.

In a more realistic scenario the cost of the T&M checks depends on *c* and *e*. A higher quality of the checks requires to spend more money in human resources and means (support logistic). Thus it is reasonable to assign a higher cost to a more accurate T&M check. As an example the cost (performability) function can be refined as follows:

$$C(t) = C_{Risk}[1-A(t)]+P_{Man}/2[e(1-c)]^{1/2}$$

where the same C_{Risk} and P_{Man} are maintained as before.

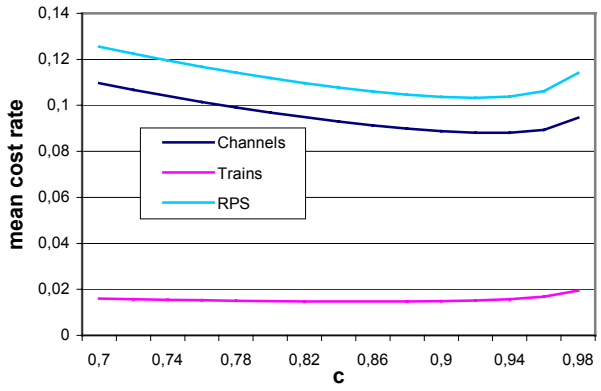

Figure 19. T&M failure detection optimal tuning

It is possible to consider just the same type of checks (with just one couple of parameters *c* and *e*) for all the T&M activities, or to further distinguish between channels T&M checks and train-breakers T&M checks (in this case two couples of parameters are needed). The analysis, considering the same type of checks, has been carried out separately for *c* and *e*, setting to their default values the parameters not involved. Figure 19 reports C(t) as a function of *c* both for the RPS system as a whole and separately for the channels and the train-breakers. It shows

that a value for *c* yielding the minimum C(t) exists. For the RPS *c* = 0.92 yields the minimum cost of 0.103. If channels and train-breakers are considered separately, two values of *c* can be found: 0.94 for the channels and 0.85 for the trains-breakers. A similar analysis performed at varying *e* has given the same kind of results; i.e., there exist values for *e* yielding the minimum C(t).

5 Concluding remarks

This work addressed the dependability modeling and analysis of a significant case study of Scheduled Maintenance Systems. The SMS example we dealt with is a very critical system where the maintenance has to be executed on-line without interrupting the provided service: the Reactor Protection System (RPS) and its maintenance policy in use at the Westinghouse's nuclear plants.

Differently from previous available studies on this system that used fault trees, we have exercised our recently proposed methodology [12, 13]. It is based on of the Deterministic and Stochastic Petri Nets (DSPN) as a modeling formalism and on a simple and computationally efficient analytical solution technique based on the divisibility of the underlying Markov Regenerative Processes (MRGP).

The various analysis carried out have permitted to investigate many different facets of the problem, like understanding how critical parameters interplay in determining the system dependability figures as well as understanding under which condition an optimal check frequency for the T&M program exists. All this things have been made with a reasonable effort, thanks to i) the high expressiveness of DSPN which allow to define complex model in a concise way, ii) the support provided by DEEM. DEEM allowed defining and automatically solve SMS problems and performing several analyses by just modifying few parameters of our model.

The computing time needed to carry out the analysis using our methodology depends on the size (i.e. number of states) of the underlying Markov models (one for each phase), on the complexity of the marking dependent expression and on the number of experiments dealing with a single study. For the RPS studied, the model is of the order of one million of states, but thanks to the separation of the solution of the various phases the biggest model solved was of 4096 states (full redundancy phase). In spite of a massive use of variables and complex marking dependent expressions the time needed to perform a single study did not exceed in media the order of few tens of minutes on a Pentium III 500 MHz, 128Mb Ram PC.

We accounted for the former work commissioned to the INEEL where the mean availability of the RPS has been evaluated according to a Fault Tree approach [9], first to get the system specification and second to validate our results. Considering some minor differences in the assumptions made, we found a reasonable accord with their results (0.06 percent of difference). Nevertheless, we have to remark the complexity of the fault tree approach resulting in a huge model spread over many sheets and quite prone to errors compared to the more compact DSPN one. Moreover our methodology has allowed us to extend quite significantly the analyses performed, with respect to just the mean availability computed with the fault trees. In fact we have been able to perform a transient analysis and a sensitivity analysis with respect to many relevant parameters. Furthermore we have analyzed the performability (or cost) of the SMS program of the RPS system showing how well our methodology addresses SMS in general, allowing to compare different scheduling of maintenance actions and to identify the best frequency for a given SMS program.

Finally we want to remark that despite the assumptions we made are suitable for most of the SMS problems normally encountered, further refinements of the methodology [12] cover a wider class of problems where the failure rate are no more constant and the phases length is not deterministic. These extensions, which have still to be included in DEEM, permit to manage T&M problems with components working in the wear out bath-tube curve. For

instance, it appears possible to model all those policies based on the knowledge of the aging or wearing state of the components like the ARP (Aging Replacement Policies) and the WRP (Wearing Replacement Policies).

Acknowledgements The authors wish to thank Prof. Pierre-Jacques Courtois from the Université Catholique de Louvain, Belgium for the fruitful discussions held in the preliminary stages of this work.

References

[1] M. Ajmone Marsan, G. Balbo and G. Conte, "A Class of Generalized Stochastic Petri Nets for the Performance Analysis of Multiprocessor Systems," ACM TOCS, Vol. 2, pp. 93-122, 1984.

[2] J. E. Arsenault and J. A. Roberts, "Reliability and Maintainability of Electronic Systems," London, Pitman, 1980.

[3] R. Bell and D. Reinert, "Risk and system integrity concepts for safety related control systems," in "Safety-critical systems", F. Redmill and T. Anderson Ed., Chapman&Hall, 1990, pp. 275-295.

[4] A. Bondavalli, I. Mura, S. Chiaradonna, R. Filippini, S. Poli and F. Sandrini, "DEEM: a Tool for the Dependability Modeling and Evaluation of Multiple Phased Systems," in Proc. DSN2000 Int. Conference on Dependable Systems and Networks (FTCS-30 and DCCA-8), New York, USA, 2000, pp. 231 - 236.

[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, Prague, Czech Republic - September 15-17, 1999, 1999, pp. 7 - 23.

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

[8] IEEE, "IEEE guide for general principles of reliability analysis of nuclear power generating station protection systems," 1975.

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

[10] J. A. McDermid, "Issues in developing software for safety critical systems," Reliability Engineering and System Safety, Vol. pp. 1990.

[11] J. Moubray, "Reliability Centered Maintenance," Butterworth-Heinemann, 1991.

[12] I. Mura and A. Bondavalli, "Markov Regenerative Stochastic Petri Nets to Model and Evaluate the Dependability of Phased Missions," IEEE Transactions on Computers, Vol. 50, 2001 (to appear).

[13] I. Mura, A. Bondavalli, X. Zang and K. S. Trivedi, "Dependability Modelling and Evaluation of Phased Mission Systems: a DSPN Approach," in Proc. DCCA-7 - 7th IFIP Int. Conference on Dependable Computing for Critical Applications, San Jose, CA, USA, 1999, pp. 319-337.

[14] R.J. Murry and B.F. Mitchell, "Cost savings from a practical predictive-maintenance program," in Proc. IEEE Reliability and Maintainability Symposium, 1994, pp. 206 -209.

[15] David Powell, "Failure Mode Assumptions and Assumption Coverage," in "Predictably Dependable Computing Systems", B. Randell, J. -C. Laprie, H. Kopetz and B. Littlewood Ed., Springer-Verlag, 1995, pp. 133-140.

[16] D.M. Reineke, W.P. Murdock, Jr., E.A. Pohl and I. Rehmert, "Improving availability and cost performance for complex systems with preventive maintenance," in Proc. IEEE Reliability and Maintainability Symposium, 1999, pp. 383 -388.

[17] D. P. Siewiorek and R. S. Swarz, "Reliable Computer System - Design and Evaluation," Digital Press, 1992.