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

ANDREA BONDAVALLI[1] AND ROBERTO FILIPPINI[2]

[1]*Dipartimento di Sistemi e Informatica, University of Florence, via Lombroso 6/17, I-50134, Italy*
[2]*CERN, CH 1211 Geneva 23, Switzerland*
Email: a.bondavalli@dsi.unifi.it, roberto.filippini@cern.ch

This paper describes a way of managing the modeling and analysis of Scheduled Maintenance Systems (SMSs) 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 applied 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 using an efficient analytical solution method. This methodology is implemented by the DEEM tool specifically developed for modeling and evaluating the dependability of Phased Mission Systems (PMSs). We test our methodology with such a case study to check whether it can master real and complex SMS problems and to compare its efficacy with traditional approaches (fault trees). The paper also investigates the problem of the optimal tuning of a maintenance program, giving a useful decision support tool for evaluating the system performance from the early design stage.

Received 12 July 2003; revised 14 January 2004

1. INTRODUCTION

Maintenance is the main instrument for ensuring quality of service of a system over time, despite aging and wear out of its components. The entire set of 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 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 a proper set of actions and their timed sequence that best satisfy dependability requirements, subject to budget constraints. In most cases this is a very tough 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 (reliability centered maintenance) [1]) 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 component failure rates and modes.

From the modeling point of view, a system under a scheduled maintenance program (SMS) can be seen as a multiple phased system (MPS). Each phase is associated with the configuration of the system during some time interval (the entire system or only the part being actually maintained or operative [2]), while the SMS 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 toward testing our new modeling and evaluation approach [3]. 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 a 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 [3, 4]. This approach is fully integrated in the DEEM tool [5], specifically tailored for dependability modeling and evaluation of MPS.

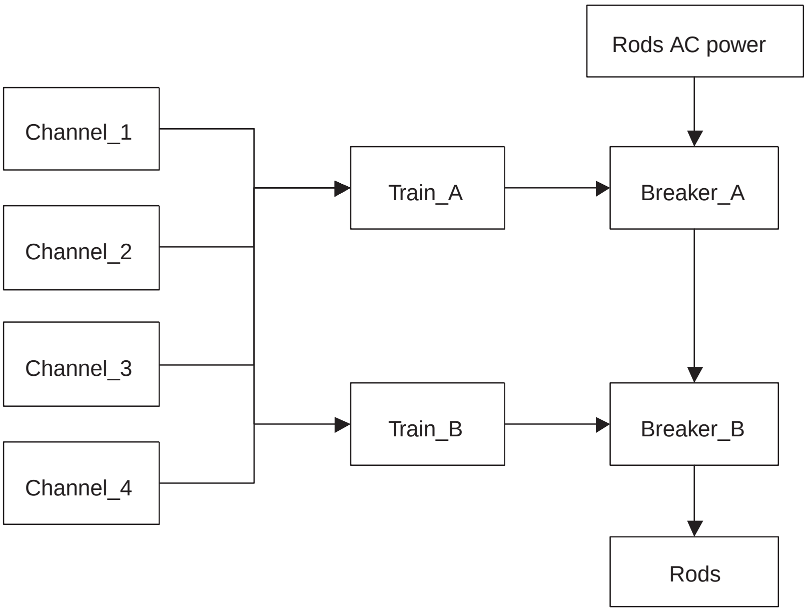


FIGURE 1. RPS architecture.

The SMS problem we consider in this work is the case of a 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 Westinghouse's nuclear plants [6]. The service delivered by this system is assuring a safety function or protective action to a nuclear plant in order to prevent and reduce the risk of potentially catastrophic events [7, 8, 9]. The safety function is associated with executing reaction process shutdown. The most important dependability measure of such a system is its availability to correctly perform the safety function when needed: in other words, safety on demand. Previous studies used a fault tree modeling approach whose top event was the availability of the safety function [8], and others have collected a huge amount of failure data of the system components [6]. We have instead built the DSPN model of such a system.

The purpose of this work is twofold.

- On the one hand we want to exercise our methodology, to check whether it can master real and complex SMS problems and to compare its efficacy with traditional approaches (fault trees).
- On the other hand, we want to investigate the problem of optimal tuning of a maintenance program in order to provide a useful decision support tool to evaluate the system performance from the earliest 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 of 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 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) any time a potentially catastrophic event occurs in the nuclear plant [6]. Catastrophic events are those events that could lead the plant to a state where the risk of damaging things, people and the environment is very high. The safety function performed by RPS corresponds to stopping the nuclear plant reaction and to leading the plant to a safe state. The contribution of RPS to the safety of the plant is represented by the availability of its safety function, whose evaluation (in terms of minimal requirement) is made through risk analysis of the operational data [10, 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 of continuously monitoring and processing a certain number of physical quantities (temperature, pressure and many others) and generating 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 two of four majority voter logic. A redundancy of four channels allows two simultaneous faults to be handled and fault tolerance capabilities to be maintained 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 functional diversity.

The trip signal starts the safety action, which is completed by the breakers with the descent of the rods into the

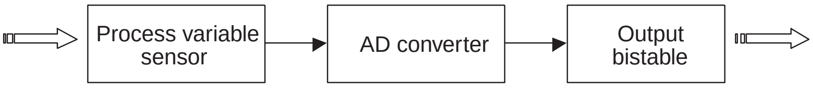


FIGURE 2. Signal processing line.

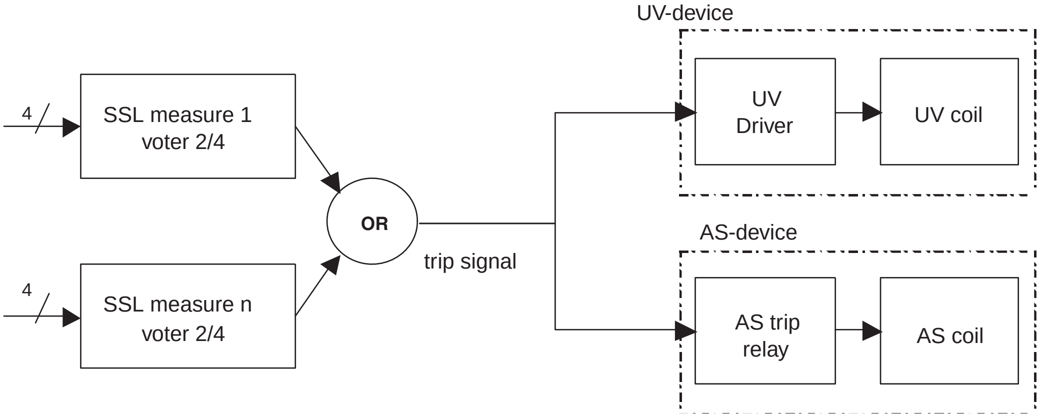


FIGURE 3. Trains architecture.

reactor core and the shutdown of the nuclear reaction. The general fault tolerance design principles adopted here are the tolerance of at least a single fault, modular independence, functional and structural diversity and testability of the components [7]. This last feature consists of the numerous built-in test facilities for periodically checking the system without interrupting the service.

Automatic generation of the trip signal is not the only way of accomplishing 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 generate the trip signal manually, if needed. Anyway, we do not consider the contribution of any human operator to the safety or 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 signals 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 bistable 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.

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 that generates the shutdown command. The SSL takes the four signals from the channels and generates the trip signal according to a two out of four voting logic. Just one of the n SSLs of the train voting for the trip is sufficient to generate the trip signal for the RPS. The trip signal drives two devices, the Under Voltage (UV) and the Auto Shunt trip (AS), 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 for one state change to start the shutdown command.

2.3. Breakers segment

The reactor trip breakers (RTBs) are electromechanical devices that during normal operational conditions keep the rods outside the reaction core. Between the rod control system and the AC power supply there is a double circuitry, the primary and the secondary circuits, joined together as shown in Figure 4. Normally, in the absence of a shutdown command, a closed path (involving primary or secondary circuitry) connects the power supply to the rod control system. Opening the circuit ensures that the rods fall by gravity into the reactor core and stop the reaction. There are about 50/60 rods; however, it is not necessary that all the rods drop into the reactor, even 10 of them are enough to assure completion of the system shutdown.

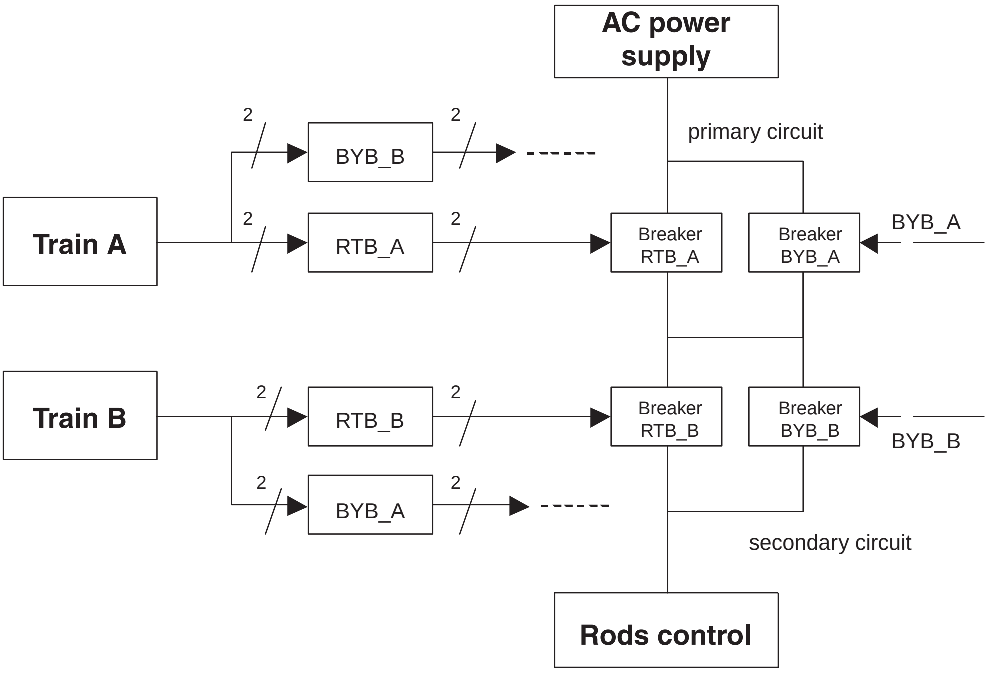


FIGURE 4. Breaker architecture.

The breakers behave like switches, opening the circuit any time the shutdown command is generated. The primary circuitry has two breakers in series (RTB A and B), driven respectively by the trains A and B. The secondary circuitry is identical to the primary and consists of two bypass breakers (BYB A and B). During normal operational conditions, 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 temporarily 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 either breaker disconnects the AC power from the rod control system, which results 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 benefit of such a testing policy is detection of non-self-announcing faults that could have been accumulating in the RPS so as 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 [6] 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.

TABLE 1. T&M programs.

Subject of the T&M	T&M period	Mean length
Channels	3 months	4 h (per trip signal)
Trains–breakers	2 months	2 h

The T&M program is the overlapping of two T&M periodical sequences, respectively of 3 and 2 months' length, so that it needs 6 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.

(i) Full redundancy phase: all components available.
(ii) T&M channel phase: one channel under T&M.
(iii) T&M train–breaker phase: one train–breaker under T&M.
(iv) T&M channels and train–breaker: one channel and one train–breaker under T&M.

Configuration (iv) 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 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 Nuclear Plant Reliability Data System (NPRDS) failure records and it is the result of more than 10 years (1984–1995) of operational failure data collection at the Westinghouse plants [6]. The data collected have been only those events potentially affecting safety as identified by an FMECA (failure mode error criticality analysis) 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 component, or as common, when it involves the failure of more than one component of the same type [8, 11]. The most critical events for the availability of the RPS safety function are common cause failure (CCF) events for the reason that 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 are distinguished from the other dependability measures since they are usually associated with an optimal problem [12, 13]. Costs (not necessarily monetary costs) and benefits are put together in order to weight properly the various alternatives and best tune the design parameters. Efficacy (Did I reach the goal?) and the efficiency (How much did it cost to reach it?) are put together to find their right balance. In the RPS system this can 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. The more frequent and accurate the checks, the 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 not being a major issue for the RPS (availability of the safety function must be maximized), in most SMSs constraints exist on the minimal dependability requirements and the maximum T&M program budget. Therefore we will show how such measures 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 a T&M check. Therefore, it is possible to represent the entire operational life (between two major overhauls) as different periods of deterministic duration called phases. This feature makes the SMS belong to the MPS class.

3.1. MPS, our methodology and the DEEM tool

MPSs 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. [14, 15], or on state space oriented models, such as Markov chains and various classes of Petri nets [16, 17, 18, 19]. Because of their ability to represent complex dependences among system components, state space approaches offer the potential to address the features of the most complex instances of MPSs. Following such a state-based approach, we have proposed a modeling and evaluation methodology [3], based on a specialization of the MRGP theory for the solution of MRSPN (Markov regenerative stochastic Petri Net) models of MPS. The computational complexity of the analytical solution is reduced to the one needed for separate solution of the different phases. The issues introduced by the phased behavior are solved without requiring additional computational costs.

Such methodology is supported by the DEEM tool [5]. DEEM employs the DSPN formalism for modeling MPS. DSPN models extend Generalized Stochastic Petri Nets and Stochastic Reward Nets, allowing the exact modeling of events having deterministic occurrence times. A DEEM model may include immediate transitions, represented by a thin line, transitions with exponentially distributed firing times, represented by empty rectangles, and transitions with deterministic firing times, represented by filled rectangles. DEEM makes available a set of modeling features that significantly improve DSPN expressiveness:

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

This rich set of modeling features, accessible through a graphical user interface, provides DEEM with a general modeling scheme in which two logically separate parts are used to represent MPS models. One is the System Net (SN), which represents the failure/repair behavior of system components, and the other is the Phase Net (PhN), shown in Figure 5, which represents the execution of the various phases.

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

Each net is made dependent on the other by marking-dependent predicates that modify transition rates, enabling

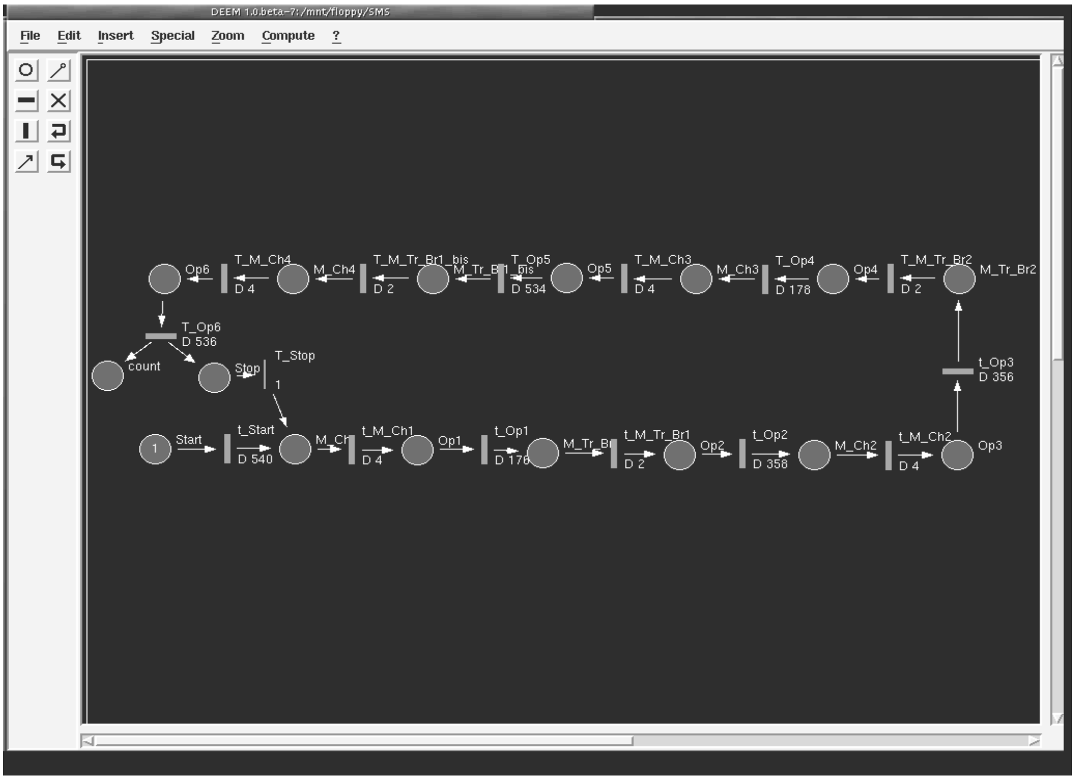


FIGURE 5. Phase Net.

TABLE 2. PhN transitions.

Immediate transition	Enabling condition	Description
T_Stop	Mark(Count) ≥ max_ count	Completion of the system lifetime
Timed transition	Firing time (h)	Description
t_M_Ch1,2,3,4	4	Checks for channels
t_M_Tr-Br1,2 M_Tr-Br1_bis	2	Checks for train–breakers
t_Start	540	First phase
t_Op1	176	Operating phase
t_Op2	358	Operating phase
t_Op3	356	Operating phase
t_Op4	178	Operating phase
t_Op5	534	Operating phase
t_Op6	536	Operating phase

conditions, reward rates, etc. to model the specific MPS features. Marking-dependent attributes of the various objects (arcs, places and transitions) can be defined through the DEEM property window associated with each object. Phase-triggered reconfigurations, which add a significant complexity to the treatment of dependences among phases, are easily handled by DEEM through the implicit mapping that is embedded in the model. Moreover DEEM allows one 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 experiments, 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 [5], while the SW package is currently available at http://bonda.cnuce.cnr.it/DEEM.

3.2. Assumptions

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

(i) The failure rates of each component are constant.
(ii) The T&M time duration is deterministic.

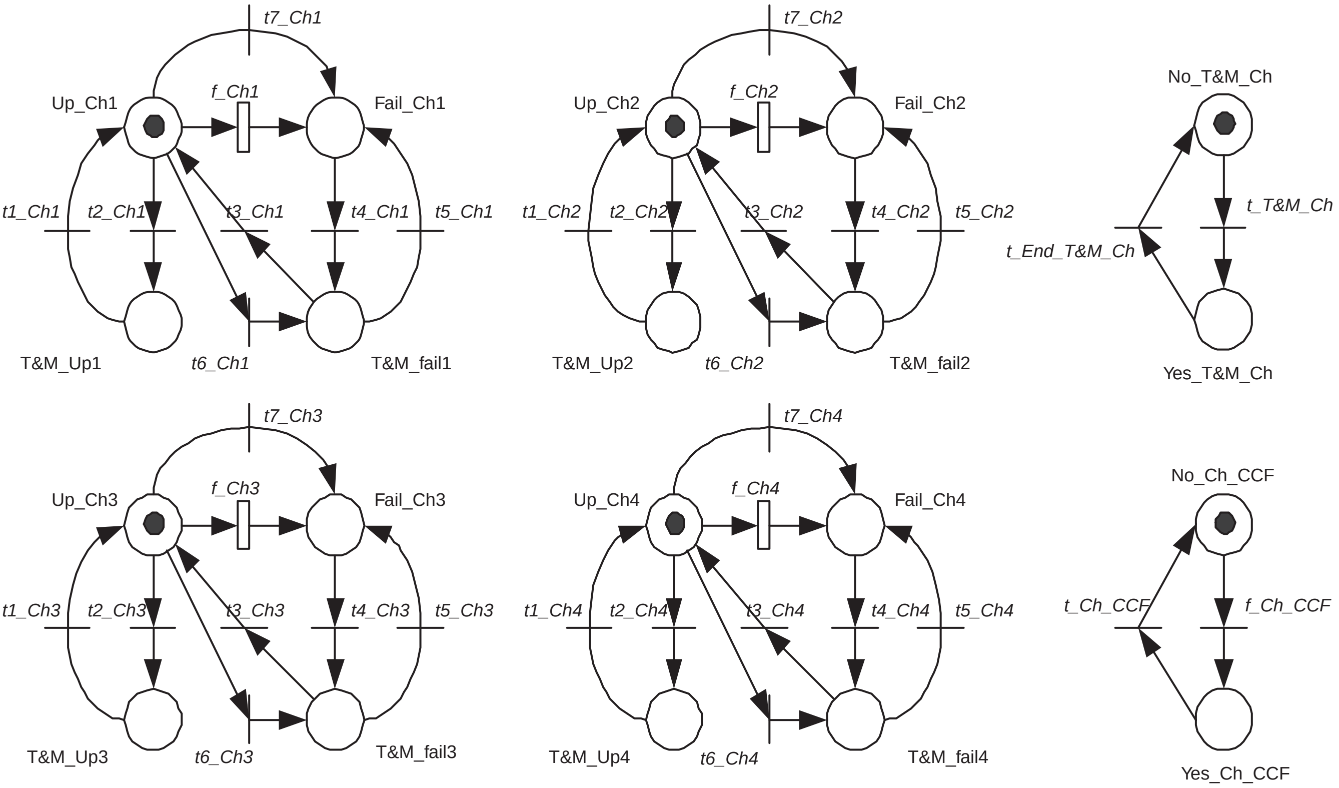


FIGURE 6. Channels sub-net.

(iii) 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).

(iv) 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).

(v) 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.

(vi) We consider just one monitored variable.

Assumptions (iii) and (iv) allow us to 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 (v) implies an ideal repair any time a fault has been detected. Assumption (vi) allows reducing the complexity of the system in terms of the 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 any time a self-announcing fault occurs, we limit ourselves to the case where we consider non-self-announcing faults only: the sole possibility of detecting the faults and repairing them is through waiting for the nearest scheduled check (there is no way to anticipate it). Assumptions (i) and (ii) 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 [20, 21, 22, 4].

3.3. Phase net

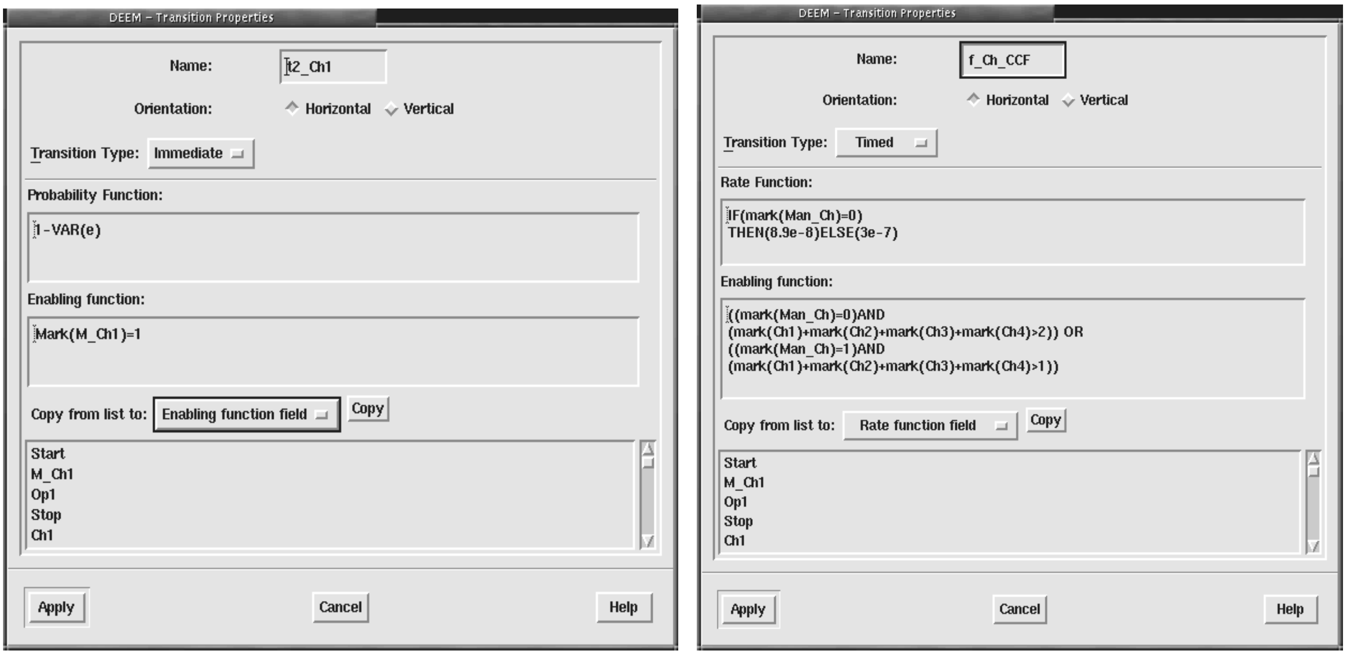
The PhN depicted in Figure 5 represents the execution of the various phases according to the T&M program, and it is cyclic for the reason the program is periodical. A token in a place of the PhN (except for the Count and the Stop places) represents the phase being executed. Count is the place where a token is put at the completion of a cycle, whereas when a token is in Stop a decision is taken about whether it is going on, performing one more cycle or stopping, depending on the max count variable value.

Figure 5 is a snapshot of the DEEM editing window. In the following, just to avoid 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 the 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 9 months from the start (6480 h) the system is exactly in the same state encountered after 3 months (2160 h). Therefore, after an initial transient of 3 months, the system has a period of 6 months, after which it repeats the same behavior. The description of the PhN transitions is shown in Table 2.

TABLE 3. Channel *i* transitions.

Immediate transition	Enabling condition	Probability	Description
t1_Chi	#(M_Chi) = 0		End T&M for channel *i* not failed
t4_Chi	#(M_Chi) = 1		Start T&M when channel *i* is failed
t3_Chi	#(M_Chi) = 0	c	Channel *i* failed and repaired
t5_Chi	#(M_Chi) = 0	$1 - c$	Channel *i* failed and not repaired
t2_Ch	#(M_Chi) = 1	$1 - e$	Start T&M when channel *i* is not failed
t6_Chi	#(M_Chi) = 1	e	T&M error on a functioning channel
t7_Chi	#(Yes_Ch_CCF) = 1		Common mode failure
t_T&M_Ch	#(M_Chi) = 1		One channel under T&M
t_End_T&M_Ch	#(M_Chi) = 0		No channels under T&M
t_Ch_CCF	#(Up_Chi) = 0		Not enough channels up for common mode failure
Exp. transition	Firing rate	Enabling condition	Description
f_Chi	λ_{CH}		Channel random failure rate
f_Ch_CCF	$\lambda_{CCF3/4}$	#(No_T&M_Ch) = 1	Common mode failure rate
	$\lambda_{CCF2/3}$	#(No_T&M_Ch) = 1	Common mode failure rate



(a)

Name: t2_Ch1

Orientation: Horizontal

Transition Type: Immediate

Probability Function:

```
1-VAR(e)
```

Enabling function:

```
Mark(M_Ch1)=1
```

Copy from list to: Enabling function field

```
Start
M_Ch1
Op1
Stop
Ch1
```

(b)

Name: f_Ch_CCF

Orientation: Horizontal

Transition Type: Timed

Rate Function:

```
IF(mark(Man_Ch)=0)
THEN(8.9e-8)ELSE(3e-7)
```

Enabling function:

```
((mark(Man_Ch)=0)AND
(mark(Ch1)+mark(Ch2)+mark(Ch3)+mark(Ch4)>2)) OR
((mark(Man_Ch)=1)AND
(mark(Ch1)+mark(Ch2)+mark(Ch3)+mark(Ch4)>1))
```

Copy from list to: Rate function field

```
Start
M_Ch1
Op1
Stop
Ch1
```

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

3.4. 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 failures and CCFs are modeled separately by exponential transitions, whose firing rate depends on the phase executed. The CCF model is a beta factor model. 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 as the T&M_fail place, depending on the maintenance error probability, *e* (Assumption iv). 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 iii).

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. The beta factor for the channel CCF is implicitly modeled by the immediate transition t7_Ch1, whose enabling condition depends on

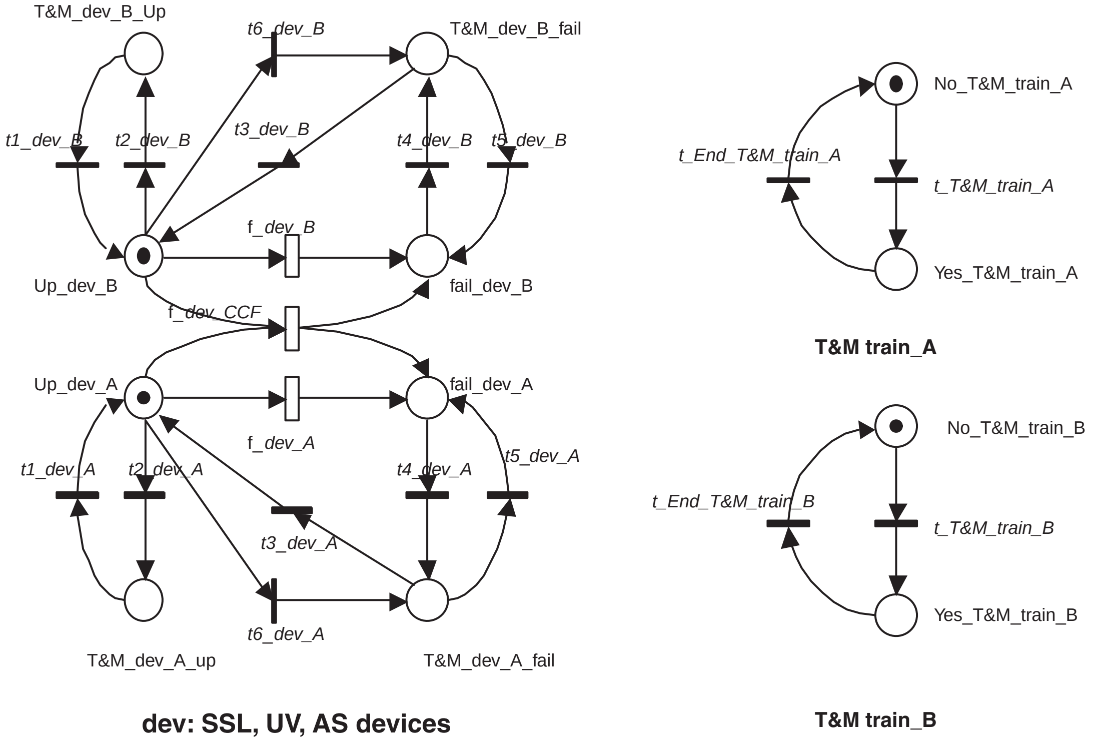


FIGURE 8. Trains sub-net.

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.

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 (just one of them is depicted in the left-hand 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. The beta factor is suitably implemented by this mechanism.

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 of missing the insertion of the spare or of finding it failed for any reason. Moreover, we assume perfect failure detection and no possibility of failure of 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.

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 sub-models.

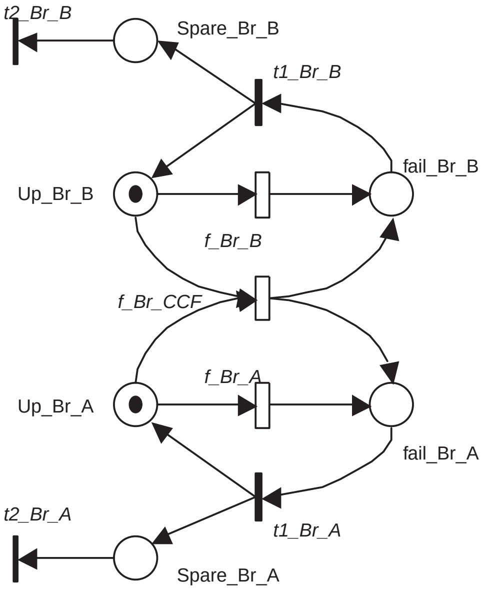


FIGURE 9. Breakers sub-net.

4. MODEL EVALUATION AND SYSTEM ANALYSIS

This section describes first which dependability measures are studied and how they are defined in the DEEM model.

TABLE 4. Exponential transitions firing rate of the trains and the breakers sub-models.

Exponential transition	Firing rates	Description
f_SSL_A	$\lambda_{SSL} + \lambda_{SSL\_CCF}$#(Yes_T&M_train_B)	Random plus CCF failure rate for the SSL_A (only when train B is under T&M)
f_SSL_B	$\lambda_{SSL} + \lambda_{SSL\_CCF}$#(Yes_T&M_train_A)	Random plus CCF failure rate for the SSL_B (only when train A is under T&M)
f_SSL_CCF	λ_{SSL_CCF}	CCF failure rate for the SSL A and B
f_UV_A	$\lambda_{UV} + \lambda_{UV\_CCF}$#(Yes_T&M_train_B)	Random plus CCF failure rate for the UV_A (only when train B is under T&M)
f_UV_B	$\lambda_{UV} + \lambda_{UV\_CCF}$#(Yes_T&M_train_A)	Random plus CCF failure rate for the SSL_B (only when train A is under T&M)
f_UV_CCF	λ_{UV_CCF}	CCF failure rate for the UV A and B
f_AS_A	$\lambda_{AS} + \lambda_{AS\_CCF}$#(Yes_T&M_train_B)	Random plus CCF failure rate for the AS_A (only when train B is under T&M)
f_AS_B	$\lambda_{AS} + \lambda_{AS\_CCF}$#(Yes_T&M_train_A)	Random plus CCF failure rate for the AS_B (only when train A is under T&M)
f_AS_CCF	λ_{AS_CCF}	CCF failure rate for the AS A and B
f_Br_A,B	λ_{BR}	Random failure rate for the BR_A and BR_B
f_Br_CCF	λ_{BR_CCF}	CCF failure rate for the BR_A and BR_B

TABLE 5. Enabling conditions and probabilities related to immediate transitions of the trains and the breakers sub-models.

Immediate transition	Enabling conditions	Probabilities	Description
t1_dev_A(B)	#(Yes_T&M_Train_A(B)) = 0		End T&M when device A (B) is not failed
t4_dev_A(B)	#(Yes_T&M_Train_A(B)) = 1		Start T&M when device A (B) is failed
t3_dev_A(B)	#(Yes_T&M_Train_A(B)) = 0	Prob = c	Device A (B) failed and repaired
t5_dev_A(B)	#(Yes_T&M_Train_A(B)) = 0	Prob = $1 - c$	Device A (B) failed and not repaired
t2_dev_A(B)	#(Yes_T&M_Train_A(B)) = 1	Prob = $1 - e$	Start T&M when device A (B) is not failed
t6_dev_A(B)	#(Yes_T&M_Train_A(B)) = 1	Prob = e	T&M error on device A (B)
t1_Br_A	#(Yes_T&M_Train_A) = 1 AND #(Spare_Br_A) = 0		Start T&M breaker A and spare A insertion
	#(Yes_T&M_Train_A) = 0 AND #(Spare_Br_A) = 1		End T&M breaker A and spare A disinsertion
t1_Br_B	#(Yes_T&M_Train_B) = 1 AND #(Spare_Br_B) = 0		Start T&M breaker B and spare B insertion
	#(Yes_T&M_Train_B) = 0 AND #(Spare_Br_B) = 1		End T&M breaker B and spare B disinsertion
t2_Br_A	#(Yes_T&M_Train_A) = 0		Flag of spare A disinsertion
t2_Br_B	#(Yes_T&M_Train_B) = 0		Flag of spare B disinsertion
t_T&M_train_A	T&M_tr_A = ((#(count)%2 = 0) AND(#(M_Tr-Br1) + #(M_Tr-Br1_bis) = 1)) OR ((#(count)%2 = 1)and (#(M_Tr-Br2) = 1))		Start T&M train A
t_T&M_train_B	T&M_tr_B = ((#(count)%2 = 1) AND(#(M_Tr-Br1) + #(M_Tr-Br1_bis) = 1)) OR ((#(count)%2 = 0)AND (#(M_Tr-Br2) = 1))		Start T&M train B
t_End_T&M_train_A	NOT(T&M_tr_A)		End T&M train A
t_End_T&M_train_B	NOT(T&M_tr_B)		End T&M train B

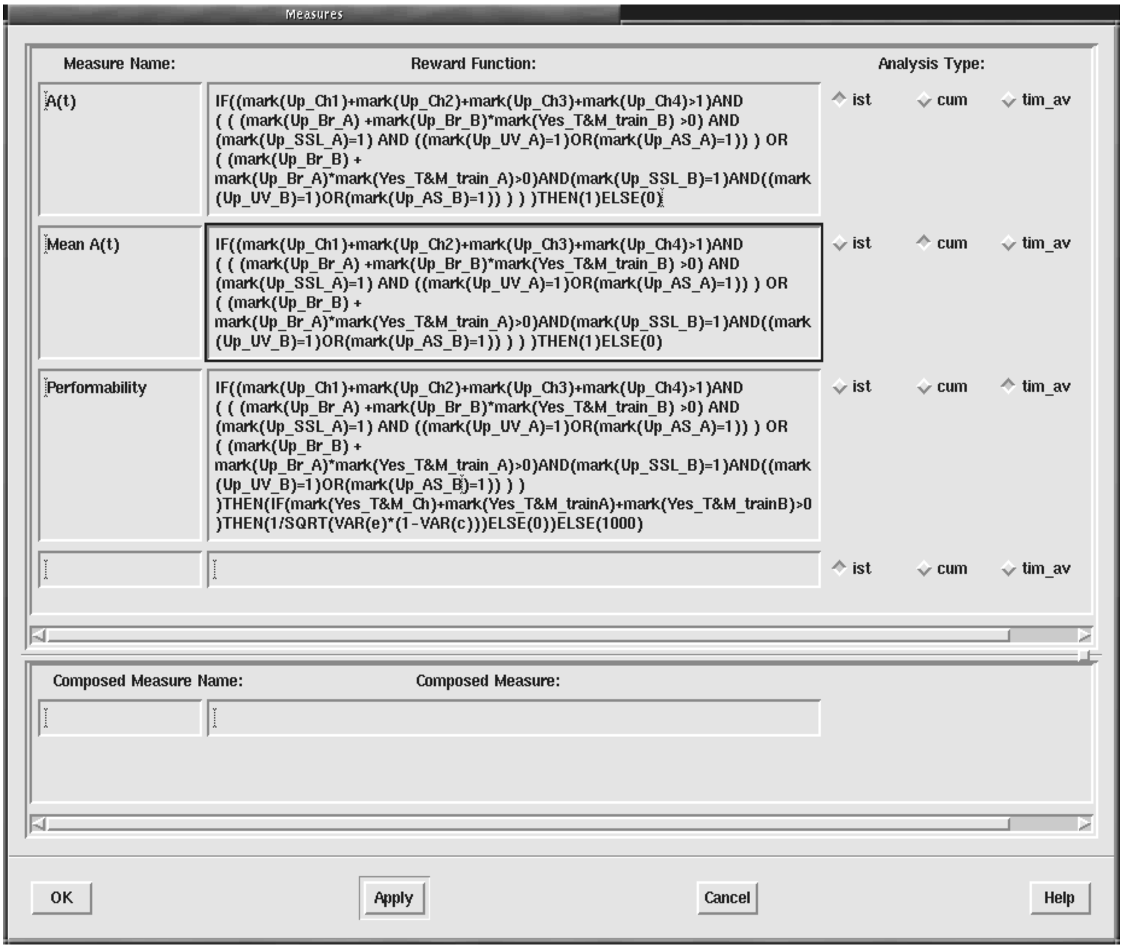
The default values assigned to the model parameters are then shown, and the relevant parameters to vary while performing sensitivity analyses are identified. Finally, several results obtained by evaluating the model are presented and discussed.

4.1. Dependability measures and parameter settings

The 'measures' window provided by DEEM permits us to define any reward measure as a Boolean expression as a function of the net marking. The tool permits us 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))



Measure Name:	Reward Function:	Analysis Type:
A(t)	IF((mark(Up_Ch1)+mark(Up_Ch2)+mark(Up_Ch3)+mark(Up_Ch4)>1)AND (((mark(Up_Br_A) +mark(Up_Br_B)*mark(Yes_T&M_train_B) >0) AND (mark(Up_SSL_A)=1) AND ((mark(Up_UV_A)=1)OR(mark(Up_AS_A)=1))) OR ((mark(Up_Br_B) + mark(Up_Br_A)*mark(Yes_T&M_train_A)>0)AND(mark(Up_SSL_B)=1)AND((mark (Up_UV_B)=1)OR(mark(Up_AS_B)=1)))))THEN(1)ELSE(0)	◆ ist ◇ cum ◇ tim_av
Mean A(t)	IF((mark(Up_Ch1)+mark(Up_Ch2)+mark(Up_Ch3)+mark(Up_Ch4)>1)AND (((mark(Up_Br_A) +mark(Up_Br_B)*mark(Yes_T&M_train_B) >0) AND (mark(Up_SSL_A)=1) AND ((mark(Up_UV_A)=1)OR(mark(Up_AS_A)=1))) OR ((mark(Up_Br_B) + mark(Up_Br_A)*mark(Yes_T&M_train_A)>0)AND(mark(Up_SSL_B)=1)AND((mark (Up_UV_B)=1)OR(mark(Up_AS_B)=1)))))THEN(1)ELSE(0)	◇ ist ◆ cum ◇ tim_av
Performability	IF((mark(Up_Ch1)+mark(Up_Ch2)+mark(Up_Ch3)+mark(Up_Ch4)>1)AND (((mark(Up_Br_A) +mark(Up_Br_B)*mark(Yes_T&M_train_B) >0) AND (mark(Up_SSL_A)=1) AND ((mark(Up_UV_A)=1)OR(mark(Up_AS_A)=1))) OR ((mark(Up_Br_B) + mark(Up_Br_A)*mark(Yes_T&M_train_A)>0)AND(mark(Up_SSL_B)=1)AND((mark (Up_UV_B)=1)OR(mark(Up_AS_B)=1)))))THEN(IF(mark(Yes_T&M_Ch)+mark(Yes_T&M_trainA)+mark(Yes_T&M_trainB)>0)THEN(1/SQRT(VAR(e)*(1-VAR(c)))ELSE(0))ELSE(1000)	◇ ist ◇ cum ◆ tim_av
		◆ ist ◇ cum ◇ tim_av

Composed Measure Name:	Composed Measure:

FIGURE 10. DEEM measures setting window.

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

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 SMSs. The cost (performability) function we define (just for the sake of an example, without any pretension of truthfulness) is the following:

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

$$C_{\text{Risk}} = 1000$$

$$C_{\text{Man}} = 1$$

$$P_{\text{Man}} = \text{IF(Phase executed} \equiv \text{T\&M) THEN 1 ELSE 0}$$

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

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

As already mentioned, DEEM permits us to define several studies. In each study value is 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. Failure rates.

	Rates (failure / h)
Random event	
Breaker electrical–mechanical 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	
$\frac{3}{4}$ Channels	8.9E − 8
$\frac{2}{3}$ Channels	3.0E − 7
Train A and B	1.5 E − 8
$\frac{2}{2}$ UV device A and B	1.4 E − 7
$\frac{2}{2}$ AS device A and B	1.6 E − 7
$\frac{2}{2}$ Breakers mechanical A and B	1.2 E − 7

Table 6 shows the default values used for the rates of the exponential transitions of the net. These values have been derived from the Idaho National Engineering and Environmental Laboratory (INEEL) reports [6]. In [6] values

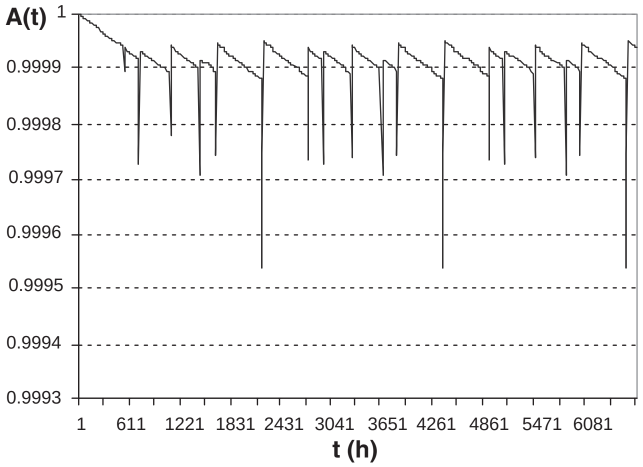


FIGURE 11. Instantaneous availability.

are given as failures on demands, in other words, the number of failures divided by the number of tests, and have been translated into failures per hours.

The numerical solution of our model provides answers to many interesting questions including the variations of the relevant measures of 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 (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 lasts 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.

When a part of the system goes under maintenance there is a loss of redundancy and consequently the availability suffers from 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 shows the mean availability curves of the RPS, the channels and the trains–breakers for the same settings. As can be seen, the T&M program has the positive effect of stabilizing 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 for by the scale factor, *s*, and on their quality [11, 21, 23], accounted for 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 functions of e ($c = 0.9$, $s = 1$).

The availability, as expected, increases with 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 through the higher redundancy of the channels segment, which makes it less sensitive to increasing maintenance errors.

Performing maintenance may bring availability gains or losses. For example, with the setting chosen for Figure 12, we observe a positive effect of T&M on the instantaneous availability. The availability gain depends on the parameters *e* and *c*, and 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 by $p(t)$ 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:

$$p(t+\Delta t) = p(t)(1-e) + [1 - p(t) + p(t)e]c \geq p(t)$$
$$\Longrightarrow e \leq c[1-p(t)]/[p(t)(1-c)].$$

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

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 toleration of even an excessively high maintenance error.

To explain this it is sufficient to consider that a smaller value of $p(t)$ (and a smaller availability of the whole channels segment) is observed in correspondence to a bigger maintenance error. In the case of a big maintenance error, a significant contribution 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 contribution may be absorbed by the fault detection and correction, depending on its probability of success.

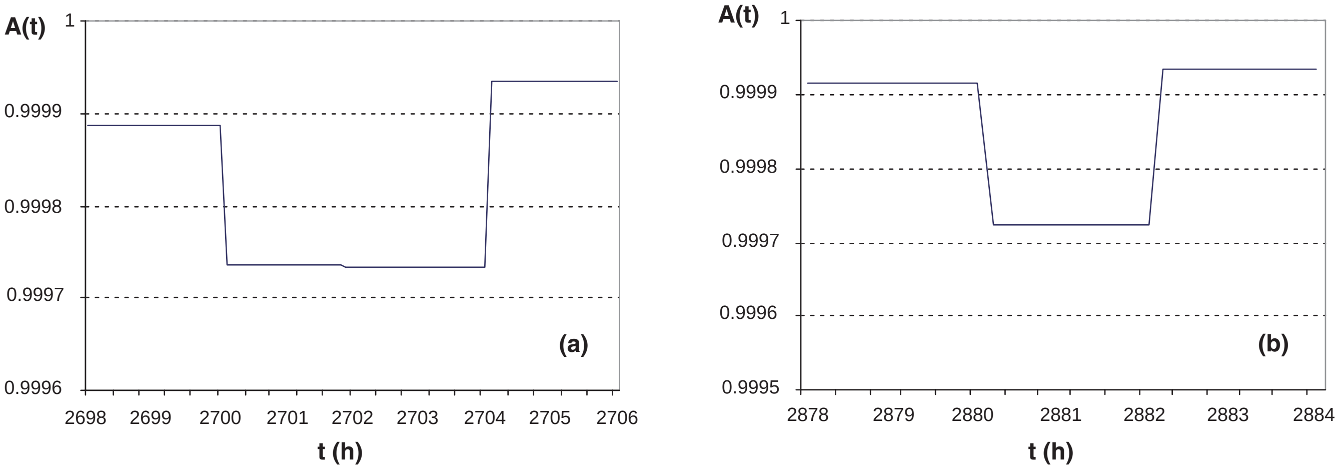


FIGURE 12. T&M phases.

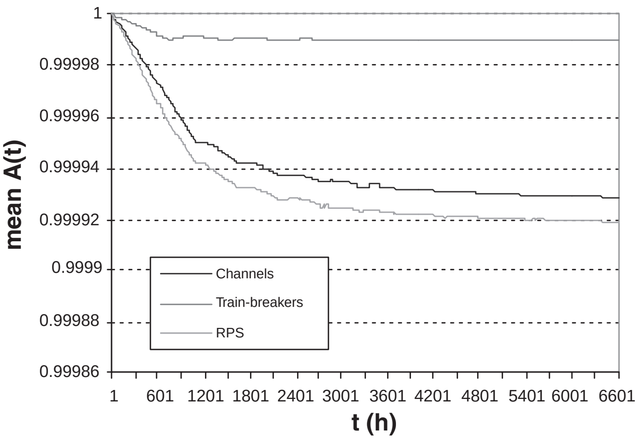


FIGURE 13. Mean availability.

Another interesting problem is to understand whether 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 check frequency increases the periods of 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 16a shows the curves of the channels instantaneous availability with four and three channels' (T&M phase). The first curve lies always above the second one, and their difference increases with time. So, the longer we wait for the maintenance, the more we pay in terms of loss of availability. Moreover, for a continuous checking policy ($s \to 0$, 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 with 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 longer the case that more frequent maintenance makes the system more available. A value for s (different from 0) exists that allows us 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 that maximizes availability. It moves from smaller to bigger values at increasing values of 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 with increasing e.

4.4. Performability

We now study 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 as to compare the result with the original T&M program.

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 the scale factor, s, 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 train–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 us to spend more money on human resources and

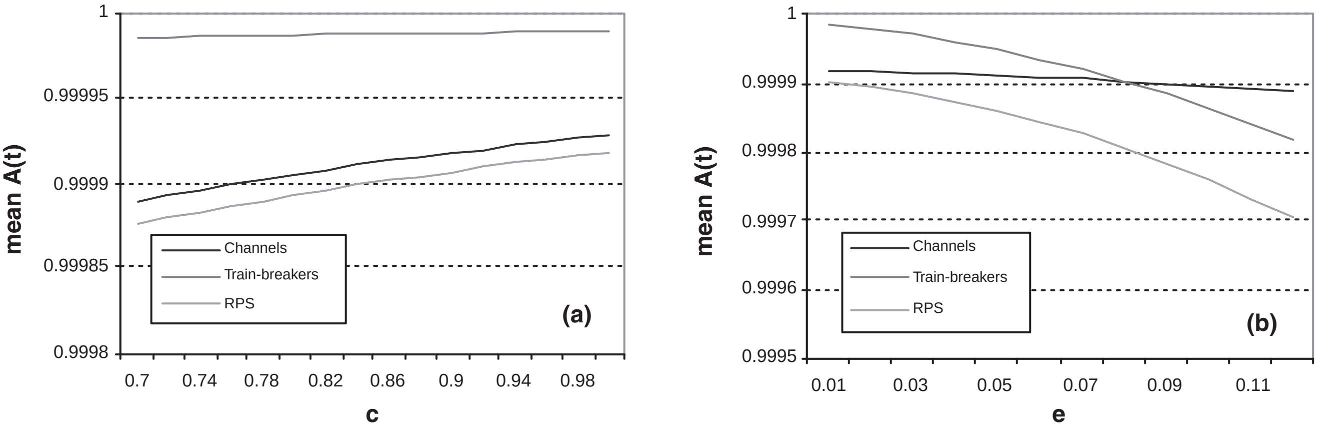


FIGURE 14. Sensitivity analysis of the mean availability.

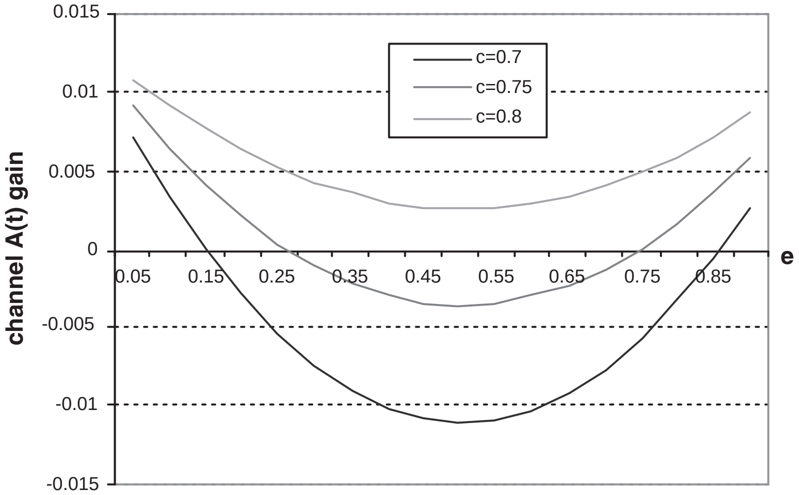


FIGURE 15. Availability gain due to the single channel T&M check.

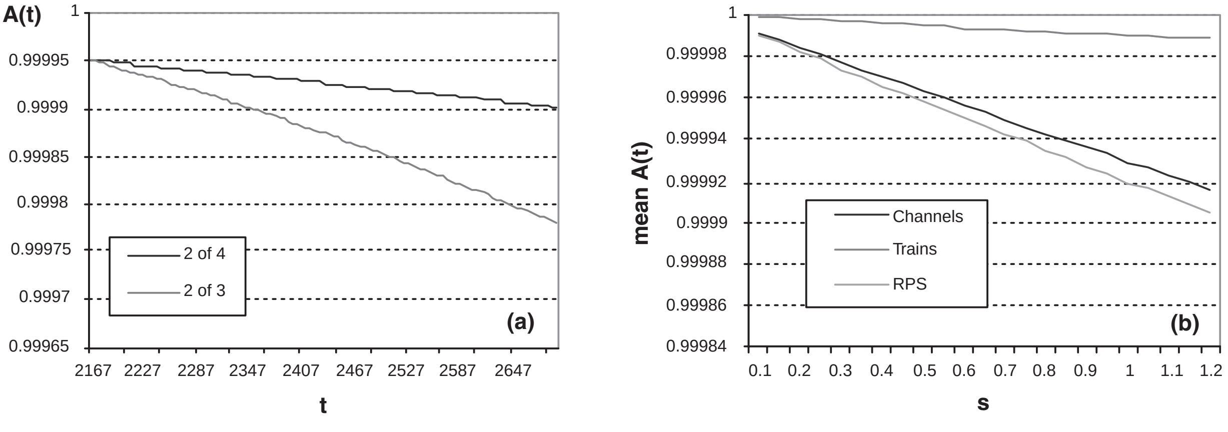


FIGURE 16. Availability trend as a function of T&M frequency.

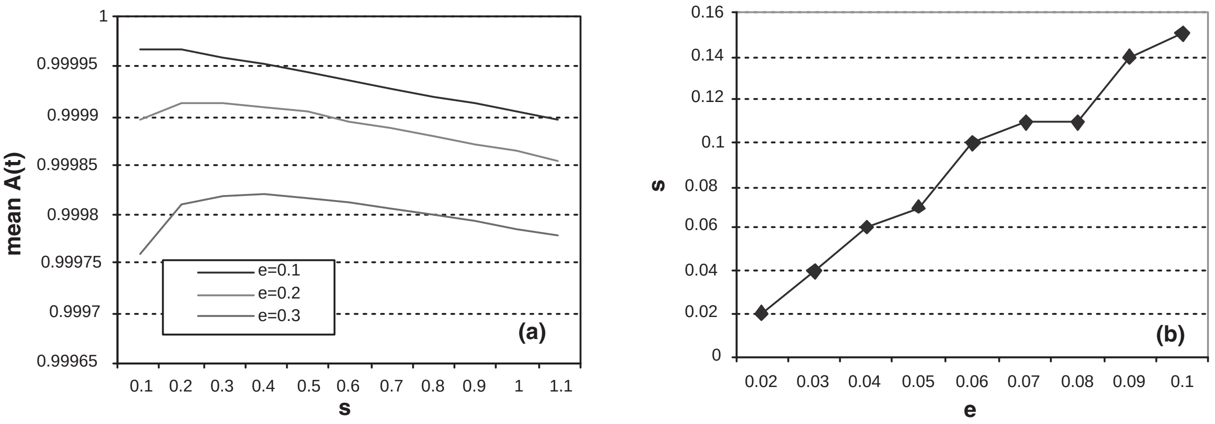


FIGURE 17. Availability as a function of *s* for different values of *e* (a). Scale factor maximizing Availability as a function of *e* (b).

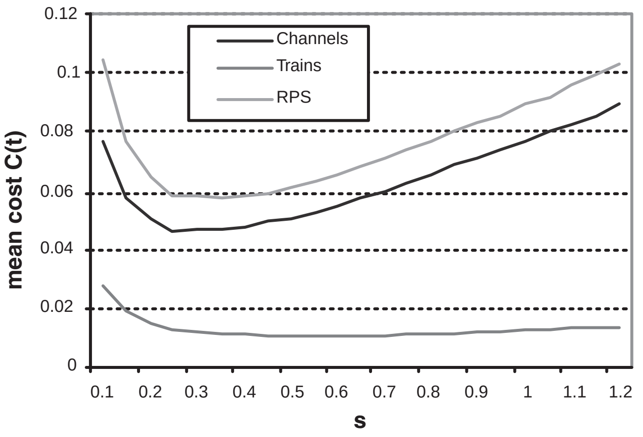


FIGURE 18. Cost (performability) of the RPS as a function of *s*.

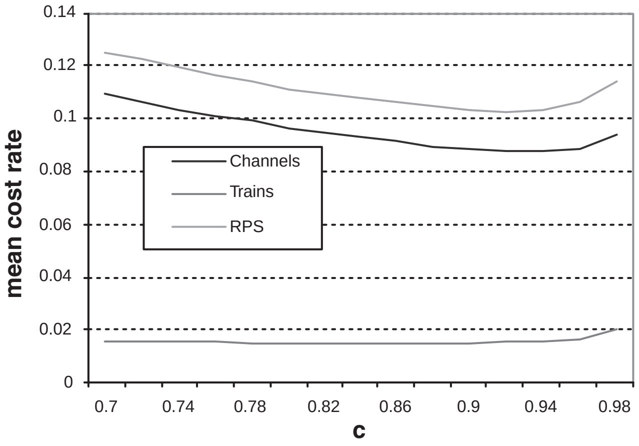


FIGURE 19. Availability trend as a function of T&M frequency.

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:

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

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

It is possible to consider just the same type of checks (with just one pair 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 of *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 train–breakers. A similar analysis performed with varying *e* gives the same kind of results, i.e. there exist values of *e* yielding the minimum $C(t)$.

5. CONCLUDING REMARKS

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

Unlike previous available studies on this system that used fault trees, we have tested our recently proposed methodology [3, 4]. It is based on the DSPN as a modeling formalism and on a simple and computationally efficient analytical solution technique based on the divisibility of the underlying MRGP.

By doing this we have been able to perform a wide set of analyses much more sophisticated than using fault trees and to gain a much deeper understanding of the system, its components and their interplay. The various analyses carried out have permitted us to investigate many different facets of the problem, like understanding how critical parameters inter-play in determining the system dependability figures and understanding under which condition an optimal check frequency for the T&M program exists. All this has been done with a reasonable effort, thanks to (i) the high expressiveness of DSPN, which allows us to define a complex model in a concise way, and (ii) the support provided by DEEM. DEEM allows defining and automatically solving SMS problems and performing several analyses by just modifying a 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 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 a few tens of minutes on a Pentium III 500 MHz, 128 Mb RAM PC.

We accounted for the former work commissioned to INEEL where the mean availability of the RPS has been evaluated according to a fault tree approach [6], 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% of difference). Nevertheless, we have to remark that the complexity of the fault tree approach, resulting in a huge model spread over many sheets and quite prone to errors, compared with 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 SMSs in general, allowing us 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 being suitable for most of the SMS problems normally encountered, further refinements of the methodology [3] cover a wider class of problems where the failure rates are no more constant and the phases length is not deterministic. These extensions, which have still to be included in DEEM, permit us to manage T&M problems with components working in the wear out bath-tub curve. For instance, it appears possible to model all these based on knowledge of the aging or wearing state of the components like the Aging Replacement Policies and the 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. Special thanks also to the DEEM Team. This work was partially supported by the by the Italian Ministry for Education, University and Research (MIUR) within the project 'Strumenti, Ambienti e Applicazioni Innovative per la Societá dell'Informazione', SOTTOPROGETTO 4, and Legge 449/97 Progetto 'SP1 Reti Internet: efficienza, integrazione e sicurezza'.

REFERENCES

[1] Moubray, J. (1991) *Reliability Centered Maintenance*. Butterworth-Heinemann, Oxford, UK.

[2] Bondavalli, A., Mura, I. and Trivedi, K. S. (1999) Dependability modelling and sensitivity analysis of scheduled maintenance systems. In *EDCC-3 European Dependable Computing Conf.*, Prague, Czech Republic, September 15–17, LNCS. **1667**, pp. 7–23. Springer-Verlag.

[3] Mura, I. and Bondavalli, A. (2001) Markov regenerative stochastic petri nets to model and evaluate the dependability of phased missions. *IEEE Trans. Comput.*, **50**(12), 1337–1351.

[4] Mura, I., Bondavalli, A., Zang, X. and Trivedi, K. S. (1999) Dependability modelling and evaluation of phased mission systems: a DSPN approach. In *DCCA-7—7th IFIP Int. Conf. on Dependable Computing for Critical Applications*, San Jose, CA, pp. 319–337. IEEE Computer Society Press.

[5] Bondavalli, A., Chiaradonna, S., Di Giandomenico, F. and Mura, I. (2004) Dependability modeling and evaluation of multiple phased systems using DEEM. *IEEE Trans. Reliab.*, to appear.

[6] INEEL/EXT-97-00740 NUREG/CR-5500. (1999) *Reliability study: combustion engineering reactor protection system, 1984–1998*. Vol. 10, Idaho National Engineering and Environmental Laboratory (INEEL).

[7] International Atomic Energy Agency (1980) Protection System and Related Features in Nuclear Power Plants: A Safety Guide. Technical Report STI/PUB/551, IAEA.

[8] IEEE (1985) IEEE guide for general principles of reliability analysis of nuclear power generating station safety systems. IEEE 352, Nuclear Power Engineering Committee of the IEEE Power Engineering Society.

[9] McDermid, J. A. (1991) Issues in developing software for safety critical systems. *Rel. Engng Syst. Saf.*, **32**, 1–24.

[10] Bell, R. and Reinert, D. (1990) Risk and system integrity concepts for safety related control systems. In Redmill, F. and Anderson, T. (eds), *Safety-Critical Systems*, pp. 275–295. Chapman & Hall, London.

[11] Powell, D. (1995) Failure mode assumptions and assumption coverage. In Randell, B., Laprie, J.-C., Kopetz, H. and Littlewood, B. (eds), *Predictably Dependable Computing Systems*, Esprit Basic Research Series, pp. 133–140. Springer-Verlag.

[12] Murry, R. and Mitchell, B. (1994) Cost savings from a practical predictive-maintenance program. In *IEEE Reliability and Maintainability Symp.*, Annaheim, CA, 24–27 January, pp. 206–209.

[13] Reineke, D., Murdock, W.P., Jr, Pohl, E. and Rehmert, I. (1999) Improving availability and cost performance for complex systems with preventive maintenance. In *IEEE*

Reliability and Maintainability Symposium, Washington DC, 18–21 January, pp. 383–388.

[14] Esary, J. and Ziehms, H. (1975) *Reliability Analysis of Phased Missions*, pp. 213–236. SIAM, Philadelphia.

[15] Somani, A. K. and Trivedi, K. S. (1994) Phased-mission systems using boolean algebraic methods. ACM SIGMETRICS Conference on Measurement and Modeling of Computer Systems, Nashville, TN, 16–20 May. *Perform. Eval. Rev.*, **22**, 98–107.

[16] Alam, M. and Al-Saggaf, U. M. (1986) Quantitative reliability evaluation of repairable phased-mission systems using Markov approach. *IEEE Trans. Reliab.*, **35**, 498–503.

[17] Dugan, J. B. (1991) Automated analysis of phased-mission reliability. *IEEE Trans. Reliab.*, **40**, 45–52.

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

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

[20] Ajmone Marsan, M., Balbo, G. and Conte, G. (1984) A class of generalized stochastic petri nets for the performance analysis of multiprocessor systems. *ACM TOCS*, **2**(2), 93–122.

[21] Arsenault, J. E. and Roberts, J. A. (1980) *Reliability and Maintainability of Electronic Systems*. Pitman, London.

[22] Choi, H., Kulkarni, V. and Trivedi, K. (1993) Transient analysis of deterministic and stochastic petri nets. In Marsan, M. A. (ed.), *Application and Theory of Petri Nets, 14th Int. Conf. on Application and Theory of Petri Nets*, Chicago, IL, 21–25 June, pp. 166–185. *Lecture Notes in Computer Science*, **691**, Springer.

[23] Siewiorek, D. P. and Swarz, R. S. (1998) *Reliable Computer Systems: Design and Evaluation* (3rd edn) AK Peters Ltd, Natick, MA.