Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Markov analysis of redundant standby safety systems under periodic surveillance testing

Mario Hellmich*, Heinz-Peter Berg

Bundesamt für Strahlenschutz (Federal Office for Radiation Protection), Willy-Brandt-Straße 5, 38226 Salzgitter, Germany

ARTICLE INFO

Article history:
Received 18 November 2013
Received in revised form
22 July 2014
Accepted 21 August 2014
Available online 2 September 2014

Keywords:
Periodic surveillance testing
Allowed outage time
Standby safety system
Markov model
Probabilistic safety assessment

ABSTRACT

In modern applications of probabilistic safety assessment (PSA), maintenance planning and changes to technical specifications play an important role, not least due to regulatory requirements. In particular, standby safety systems under periodic surveillance testing are at the center of this issue. Since traditional PSA techniques impose limitations when complex maintenance and repair strategies are to be taken explicitly into account, we introduce continuous time Markov models to discuss various strategies for organizing repair and testing of two-train standby safety systems, which have the potential to replace traditional system models based on fault tree techniques in PSA. Besides a conventional steady state analysis of these Markov models, we provide a general numerical method which allows the calculation of the probability of exceeding allowed outage times of equipment in Markov models of safety systems, and we apply it to the models introduced in the present paper.

1. Introduction

Probabilistic safety assessment (PSA) is an important tool to assess various safety attributes of nuclear power plants and other high risk undertakings, especially in process engineering. Besides the calculation of integral risk measures for the plant operation, like the core damage frequency or large early release frequency in the case of nuclear power plants, the scope of PSA applications has continuously widened in the recent past. Today, qualitative PSA aspects like the assessment of the balancedness of safety concepts or the detection of weaknesses become increasingly important [4]. Moreover, in connection with risk informed decision making, the impact of maintenance planning and changes of technical specifications are now essential fields of PSA application [15].

In this context the question of surveillance testing of standby safety systems, together with the specification of allowed outage times of components or subsystems, has been discussed repeatedly in the literature. The traditional techniques used in PSA, like fault tree analysis, impose constraints when test or repair operations are to be included. Therefore, it is current industry practice to use simple approaches without employing an explicit time-dependent model of the testing and repair operation, like taking the probability for a failure on demand of components under surveillance testing equal to $\frac{1}{2}\lambda T$, where λ is the failure rate and T the test interval. To overcome these limitations, various modeling approaches have been used which go beyond the traditional ones.

In the present paper it is our goal to study periodically tested standby safety systems by using continuous time Markov models that are manageable and incorporate all relevant features. We choose this modeling technique since it is standard, and appropriate software tools are readily available to compute the probability of failure on demand of standby systems. Besides the probability of failure on demand, another less frequently studied reliability index is important for such systems: in the nuclear sector, often regulations require that the plant must be shut down, or other compensatory measures must be implemented when the repair of a failed safety system cannot be finished during the allowed outage time interval of a component. Not only for reasons of plant availability but also from a risk perspective a shutdown needs to be taken into account due its potential to cause transients, which may lead to a non-negligible risk contribution. Therefore, for standby safety systems the probability of exceeding allowed outage times becomes relevant. To address this need we propose a new dedicated numerical method to calculate this reliability index in Markov models.

As a test case we consider a two-train standby safety system in which the two trains can fail with a given constant failure rate during standby, both independently and due to a common cause. To ensure the availability of the system, both trains are subjected to periodic surveillance tests during which potential failures are revealed. In this context we analyze three policies to organize the repair and a possible additional test on the other train once a failure has been detected: in policy 1 no additional test on the other train is performed once a failure is detected and repair is initiated, and the

* Corresponding author.
E-mail addresses: mhellmich@bfs.de (M. Hellmich), hberg@bfs.de (H.-P. Berg).

http://dx.doi.org/10.1016/j.ress.2014.08.007
0951-8320/© 2014 Elsevier Ltd. All rights reserved.

normal testing schedule is resumed after the repair is finished. In policy 2, after the repair of a train which was found to be failed is finished, the other train is subjected to an additional test with a possible repair if a failure is found. In policy 3, an additional test in the other train is carried out immediately once a failure is found, and if the other train is found to be failed as well it is repaired in parallel with the first. We concentrate on the system level; risk considerations at the plant level may be carried out by integrating the results obtained at the system level in an existing PSA.

We develop continuous time Markov models which describe the three test and repair policies. The availability of the safety system and the probability of exceeding allowed outage times are calculated for all three policies at steady state. There are two reasons to consider the models at steady state: first, the steady state unavailability (or more precisely, the availability of two, one, or no train) of a standby safety system, i.e., the probability of failure on demand, is of direct relevance in a PSA. Here the Markov models may be used as a substitute for conventional modeling techniques like fault trees. Second, since sojourn time distributions are always exponential for continuous time Markov processes and the models involve periodic calendar based testing operations, the Markov model in the transient situation is likely to be only a coarse approximation. However, at steady state results only depend on the first moments of the corresponding distributions, thus the approximation is very accurate here.

Even though our models and methods are more general, the present study is motivated by a concrete application: the emergency power supply system of a nuclear power plant. In many nuclear power plants in the world it consists of two independent diesel generators, each with its own ancillary equipment such as starters, cooling systems, switchgear, instrumentation and control equipment. The emergency power supply system has a 1-out-of-2 character, i.e., it is considered to be available if there is at least one operable redundancy. For the quantification of the Markov models we use reliability data corresponding to this case. We remark that in some nuclear power plants the emergency diesel generator system is not a two train system, but is more complex (e.g., newer German pressurized water reactor plants employ two independent 2-out-of-4 systems, with altogether eight diesels, where the second system plays a special role in dealing with external events). The Markov models can be readily generalized to the 2-out-of-4 case with staggered surveillance testing, but at the expense of a much larger state space. In order to keep the models transparent for the purpose of this study, we have chosen a 1-out-of-2 layout here. Nevertheless, the larger models in the 2-out-of-4 case would not challenge modern computing equipment as far as steady state availability and allowed outage times are concerned.

The literature on applications of Markov models to reliability and safety engineering, and in particular to maintenance problems, is abundant. Markov and semi-Markov models for systems with various types of periodic surveillance testing are introduced and discussed from a general point of view in [6,28,33,32,21], and in [1,9,10] with an emphasis on applications to nuclear engineering. Hybrid approaches which combine Markov modeling with other techniques are discussed in [31,34]. Beyond the nuclear sector, the interest in periodic testing recently revived considerably due to the IEC 61508 international standard on functional safety [11,16,17]. As already remarked, the problem of assessing standby safety systems under periodic surveillance testing has been considered using various techniques: in [23,7,8,27,24] the problem is addressed mainly by exploiting existing PSAs and with the objective of test optimization or allowed outage time and surveillance test interval extensions. The three test and repair policies introduced above have been discussed in [22] from a qualitative point of view. In [20] they are analyzed in detail by employing a state space model with a Markov type time evolution together with redistribution of occupation probabilities to account for periodic testing. The time evolution equation is solved numerically, and both system level and plant level results are obtained by incorporating outcomes from existing plant PSAs. The redistribution technique of [6] has also been used in [34], together with reliability block diagrams. Even though it can more accurately describe the transient behavior of the system, that approach assumes negligible test durations, whereas our approach addresses the possibility of a failure during a test.

The present paper is organized as follows. In Section 2 we start by recalling some basic facts concerning continuous time Markov processes, present methods to obtain an upper bound for the necessary time for the approach to the steady state up to some specified error, and provide a result which allows, in conjunction with a numerical procedure described in Appendix A, the calculation of the probability of exceeding allowed outage times. In Section 3 we introduce and discuss the three surveillance test and repair policies together with the corresponding Markov models, and Section 4 presents the numerical results. Besides upper bounds for the time to approach the steady state we calculate the system unavailability and the probability for exceeding allowed outage times, and investigate the dependence of these quantities on the most important model parameters, such as the surveillance test interval. The paper closes with some concluding remarks in Section 5.

2. Mathematical preliminaries

2.1. Markov jump processes

To fix notation we recall the definition of a continuous time discrete state space Markov process (or Markov jump process) and record some results for later use. Refer to [26,29] for the general theory of Markov jump processes, and to [30] for some foundations concerning the applications to reliability modeling.

Let $E=\{1,\dots,d\}$ be the set of states which are incorporated in the mathematical model of the system under consideration. We assume that the system's time evolution is represented by a continuous time homogeneous Markov process $Z=\{Z(t)\}_{t\ge 0}$ with values in E. Thus the memoryless property

$$\begin{aligned}\mathbb{P}\{Z(t_{n+1})=i_{n+1}|Z(t_n)=i_n,\dots,Z(t_1)=i_1\}\\ =\mathbb{P}\{Z(t_{n+1})=i_{n+1}|Z(t_n)=i_n\}\\ =p_{i_n,i_{n+1}}(t_{n+1}-t_n),\end{aligned} \tag{1}$$

is satisfied for all $n\in\mathbb{N}$, all $0\le t_1\le\dots\le t_{n+1}$ and all $i_1,\dots,i_{n+1}\in E$. The $d\times d$-matrix function $P(t)=[p_{ij}(t)]$ is called the transition probability matrix of Z. From (1) the semigroup property $P(s+t)=P(s)P(t)$ for $s,t\ge 0$, and $P(0)=\mathbb{1}$, can be established. For any such semigroup there exists a matrix $Q=[q_{ij}]$, called its generator, such that $P(t)=\exp(tQ)$. It follows that the Kolmogorov forward and backward equations

$$\frac{d}{dt}P(t)=P(t)Q=QP(t)\quad\text{for any } t\ge 0, \tag{2}$$

hold, which govern the time evolution of $P(t)$. It can be shown that

$$q_{ij}=\lim_{t\downarrow 0}\frac{1}{t}p_{ij}(t)\quad\text{if } i\ne j,\quad q_i:=-q_{ii}=\lim_{t\downarrow 0}\frac{1}{t}(1-p_{ii}(t)).$$

Thus q_{ij}, $i\ne j$, is the transition rate of Z from state i to j, and q_i is the rate for leaving state i. Moreover, the sojourn time in state i is exponentially distributed with parameter q_i, and the mean sojourn time is $1/q_i$.

Let $\nu=(\nu_1,\dots,\nu_d)$ be a probability distribution on E (i.e., $\nu_i\ge 0$ for all $i=1,\dots,n$ and $\nu_1+\dots+\nu_d=1$). Given that the distribution of Z at time s is equal to ν then, using matrix notation, $\nu P(t)=\nu\exp(Qt)$