Reliability Engineering and System Safety 138 (2015) 154–162

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

A recursive framework for time-dependent characteristics of tested and maintained standby units with arbitrary distributions for failures and repairs

Jussi K. Vaurio *

Prometh Solutions, Hiihtäjänkuja 3K, 06100 Porvoo, Finland

ARTICLE INFO

Article history:
Received 18 September 2014
Received in revised form
27 January 2015
Accepted 30 January 2015
Available online 11 February 2015

Keywords:
Maintenance
Periodic testing
Renewal
Safety system
Standby
Unavailability

ABSTRACT

The time-dependent unavailability and the failure and repair intensities of periodically tested aging standby system components are solved with recursive equations under three categories of testing and repair policies. In these policies, tests or repairs or both can be minimal or perfect renewals. Arbitrary distributions are allowed to times to failure as well as to repair and renewal durations. Major preventive maintenance is done periodically or at random times, e.g. when a true demand occurs. In the third option process renewal is done if a true demand occurs or when a certain mission time has expired since the previous maintenance, whichever occurs first. A practical feature is that even if a repair can renew the unit, it does not generally renew the alternating process. The formalism updates and extends earlier results by using a special backward-renewal equation method, by allowing scheduled tests not limited to equal intervals and accepting arbitrary distributions and multiple failure types and causes, including failures caused by tests, human errors and true demands. Explicit solutions are produced to integral equations associated with an age-renewal maintenance policy.

1. Introduction

Standby safety systems generally consist of parallel units or trains that are all normally on standby but are activated (i.e., tested) periodically to verify their ability to work if needed. Although many maintenance policies have been developed and reviewed for normally operating systems [1], models and theories are not quite as complete for standby safety systems. Certainly reliability and cost characteristics of standby units and systems under several testing and maintenance policies have been studied in the literature since 1960s. An extensive review of earlier works and categorization was included in [2] which analysed unavailability and cost characteristics under typical preventive-maintenance (PM) policies for three types of testing and repair categories, [T_{new},F_{new}], [T_{old},F_{new}] and [T_{old},F_{old}]. In this notation, T_{old} indicates that a test does not change the hazard rate of a unit, while T_{new} indicates that a test makes the unit as good as new. Similarly F_{old} and F_{new} indicate similar effects for repairs (and replacements).

Several unavailability models for category [T_{new},F_{new}] have been developed in [3–10], each considering different assumptions, failure modes, human errors and distributions. These were synthesised in a general recursive model in [11].

Category [T_{new},F_{old}] has not been specifically studied in the literature. It seems to be difficult to justify renewing an unfailed unit but not renewing a failed unit.

Category [T_{old},F_{old}] was among other categories included in the unavailability models of FRANTIC II computer code [12]. This category was further analysed with periodic preventive maintenance and cost functions for optimising test and maintenance intervals, first in case of instantaneous tests and repairs in [2], then extended to finite repair and maintenance times in [13,14].

Models for category [T_{old},F_{new}] have been developed in [2,13–17], Refs. [15-17] focusing on the unavailability function and Refs. [2,13,14] more on maintenance, cost functions and optimisation.

This paper is an extension of earlier works, especially Refs. [5,11,18,2,13,14], to obtain time-dependent unavailability functions, failure counts and repair counts under rather general conditions, maintenance options, failure modes and distributions. Arbitrary testing times (intervals) and arbitrary distributions are allowed to times to failure and repair durations. In addition to usual internal failures, the model includes failures caused by test-demands as well as human errors and failures due to true demands, usually called initiating events. The first part is focussed on the characteristic of a single standby unit (train) such that tests do not renew or age a unit but repairs and replacements do, i.e., category [T_{old},F_{new}]. Corresponding results are presented in Appendices B and C for categories [T_{old},F_{old}] and [T_{new},F_{new}] as well. A specific feature of the model is that even if a repair renews

* Tel.: +358 404139949.
E-mail address: Jussi.vaurio@pp1.inet.fi

http://dx.doi.org/10.1016/j.ress.2015.01.027
0951-8320/

a component (unit), the unavailability process does not start as from the beginning because next test is not moved forward by the repair time but takes place according to the original testing scheme and schedule. This is the realistic way tests and repairs in redundant systems are normally carried out. This feature makes the current work different from most others that have made different assumptions to be able to use the traditional renewal theory. The present work actually identifies "backward" renewal equations as explicit solutions to "forward" integral equations. Cost aspects are discussed to some extent but optimisation methods are not described in details. Much of such principles and methods are basically covered in [18,19,2,13,14].

Concerning earlier works on the unavailability of a unit in category $[T_{old},F_{new}]$, Ole Platz [15] analysed this process with a general time-to-failure distribution and periodic tests while assuming instantaneous tests and repairs (i.e., zero durations), and no periodic renewals. Hilsmeier et al. [17] developed explicit results and numerous examples under the same conditions as Platz. Dialynas and Michos [16] analysed the unavailability of a unit in $[T_{old},F_{new}]$ – category with strictly periodic testing using quite different recursive equations and assuming instantaneous tests and fixed (non-random) repair and maintenance durations.

Section 2 of the current paper develops an explicit unavailability function for a unit in $[T_{old},F_{new}]$ category by extending the recursive approach of Platz-formalism [15]. As extensions to earlier approaches the current method allows arbitrary testing times (intervals), arbitrary distributions to failure times and repair durations as well as additional failure modes caused by tests, human errors and true demands. Beyond earlier works explicit equations are obtained also for time-dependent expected accumulated numbers of failures and repairs.

In Section 3 several preventive maintenance (PM) policies are introduced. These include a strictly periodic PM, random demand-initiated PM and a combined process-age and demand-initiated PM. It is assumed that the plant and the process are shut down for the period of PM, and the whole alternating process then starts from the beginning. It is common practice that a plant like a nuclear power station is regularly shut down for maintenance (and refuelling) and shut down also when a true demand event occurs. It should be noticed that even if repairs may renew a component, they do not begin a new process cycle. A new approach to obtain unavailability and failure intensity functions for a unit with PM is to develop probabilistically explicit "backward-renewal equations". No Volterra-type renewal integral equation needs to be solved in this approach. An important feature is that the obtained "backward-equations" can be used as such also for the unavailabilities of any category other than $[T_{old},F_{new}]$. Therefore unavailability and failure count equations are solved also for categories $[T_{old},F_{old}]$ and $[T_{new},F_{new}]$ in Appendices B and C, respectively. In all models PM is assumed to be perfect, i.e., it renews the unit. Several models of imperfect PM (reducing the hazard rate but not making the unit as new) have been suggested and reviewed in Chapter 7 of Ref. [1] but have not yet been adopted within the scope of current models for standby units.

Section 4 gives conclusions and directions for future work.

2. Failure and repair characteristics

A unit can be a single component or several components in series so that they can be tested simultaneously and modelled as a unit (with one failure and repair distribution). Typically, such safety trains consist of valves and a pump with associated power sources and instrumentation, for example.

2.1. Model assumptions and justifications

1. The unit is either good or bad (unavailable); its state is reliably discovered at tests (including inspections) and only at tests. Thus, all hidden failures are detected at tests.
2. The process starts at time $t_0=0$ and tests are initiated at times $t_1, t_2,\ldots,t_{M-1}$. The process ends at time t_M, the mission time. The end is typically a plant shutdown initiating a major maintenance during which the unit is not needed. After revision the plant is started with the unit in the same condition as at t_0.
3. Test intervals $t_k–t_{k-1}$ are arbitrary, but often $t_1–t_0$ and $t_M–t_{M-1}$ are different from the rest of the intervals that are mutually equal.
   The reason is that standby safety systems usually consist of several similar parallel units that are tested periodically but in a staggered scheme. Then the first and the last intervals cannot be the same for all units, and therefore they can differ from the normal test interval.
4. Test durations are negligibly short compared to the test intervals, and tests do not cause unavailability.
   This assumption can often be justified because a test takes less than an hour or two compared to a test interval that can be weeks. Also, if a true demand occurs during a test, there is usually enough time to terminate the test and realign the unit to perform the safety function.
5. Repair (or replacement) of the unit is carried out after a test in which a failed state was discovered. The unit is unavailable during repair. Repair time τ has a probability density $g_R(\tau)$, maximum value τ_{max}, mean value τ_{av} and cumulative distribution function $G_R(\tau)$. Repair is always successful. (Typically there is a test at the end of repair to confirm the unit condition.)
6. τ_{max} is shorter than any test interval. This assumption is realistic because test intervals are typically weeks and repair times are hours or days at most. In addition, plants usually have a rule to shut down the plant if repair cannot be completed within a certain time, and this limit is normally shorter than a test interval. After shutdown and repair the process can start at the point at which it was stopped.
7. After a successful test the unit is "as good as old", i.e., a test does not cause renewal or ageing or other changes in the hazard rate. The case "as good as new" is analysed in Appendix C.
8. After successful repair the unit is "as good as new", except when specified "as good as old" (in Appendix B).
9. Repair includes a test to verify that the unit is operational after a repair.
10. The unit has time-to-failure density $f(x)$ and cumulative distribution $F(x)$, where x is the time counted from t_0 or from the latest preceding renewal (repair or maintenance completion), whichever is later. The causes of these failures are internal to the unit or continuously present (i.e., not caused by phenomena associated with tests or true demands).
11. $\overline{G}=1-G$ for any probability or fraction G.

2.2. Point unavailabilities

Let us define the unavailability $u(t)$, probability of a unit to be down at time t, for each test interval k, i.e. $(t_k,t_{k+1}]$ in terms of the local time x as

$$u_k(x)=u(t_k+x), \quad 0<x\le t_{k+1}–t_k, \quad k=0,\ 1,\ldots,\ t_M-1. \tag{1}$$

Explicit recursive equations can be written for these based on the fact that to be down at time t the unit (1) must have experienced the first failure in (t_k,t) or (2) it must be down at t_k and repair not