Reliability Engineering and System Safety 124 (2014) 1–12

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

A delay time model with imperfect and failure-inducing inspections

Roger Flage *

University of Stavanger, Norway

ARTICLE INFO

Article history:
Received 28 April 2012
Received in revised form
22 November 2013
Accepted 27 November 2013
Available online 4 December 2013

Keywords:
Delay time model
Passive system
Periodic inspection
Imperfect inspection
Failure-inducing inspection

ABSTRACT

This paper presents an inspection-based maintenance optimisation model where the inspections are imperfect and potentially failure-inducing. The model is based on the basic delay-time model in which a system has three states: perfectly functioning, defective and failed. The system is deteriorating through these states and to reveal defective systems, inspections are performed periodically using a procedure by which the system fails with a fixed state-dependent probability; otherwise, an inspection identifies a functioning system as defective (false positive) with a fixed probability and a defective system as functioning (false negative) with a fixed probability. The system is correctively replaced upon failure or preventively replaced either at the *N*'th inspection time or when an inspection reveals the system as defective, whichever occurs first. Replacement durations are assumed to be negligible and costs are associated with inspections, replacements and failures. The problem is to determine the optimal inspection interval *T* and preventive age replacement limit *N* that jointly minimise the long run expected cost per unit of time. The system may also be thought of as a passive two-state system subject to random demands; the three states of the model are then functioning, undetected failed and detected failed; and to ensure the renewal property of replacement cycles the demand process generating the 'delay time' is then restricted to the Poisson process. The inspiration for the presented model has been passive safety critical valves as used in (offshore) oil and gas production and transportation systems. In light of this the passive system interpretation is highlighted, as well as the possibility that inspection-induced failures are associated with accidents. Two numerical examples are included, and some potential extensions of the model are indicated.

1. Introduction

Inspection (testing) of failure-critical systems is implemented and optimised by the rationale that the benefit and cost of inspection should be balanced against the potential cost of system failure. The effect of an inspection is often purely informational, in the sense that the inspection only provides information about the state of a system and does not affect its time to failure. In some cases, however, inspections could be potentially harmful to a system. The inspection procedure could introduce new (external) failure modes, or otherwise affect the time to system failure. Then the positive informational effect of an inspection is counteracted not only by the (often relatively minor) cost of the inspection, but also by the potential cost of an inspection-induced failure. The positive informational effect of inspection could also be corrupted by imperfect inspection results, in the sense that an inspection may not reveal the true state of a system for certain; it may identify a functioning system as failed (false positive result) and a failed system as functioning (false negative result).

The combination of these two aspects – failure-inducing and imperfect inspections – is relevant and applicable to many inspection maintenance models. In this paper we focus on the basic delay-time model, which is a fundamental and versatile model of inspection maintenance for a system that can be characterised by three states: perfectly functioning, defective and failed. Assuming that system failures are observed immediately, the inclusion of a defective state makes the delay-time model relevant not only in relation to false positives, but also in relation to false negatives. In the former case an inspection reveals the system as being in the defective state when it is actually in the perfectly functioning state, while in the latter case an inspection reveals the system as being in the perfectly functioning state when it is actually in the defective state.

Various early developments of the delay-time model are reviewed in e.g. [5,8,9]. More recent developments and extensions of the basic delay-time model include, for single-component systems, consideration of four system states (instead of the three states of the basic delay-time model) [21], of multiple types of nested inspections at different intervals [23], and of two types of inspections and repairs (revealing and correcting different types of deterioration) [22]; and for multi-component systems the pooling of individual component failure modes (delay-time) modellings to form a system inspection model [25], as well as a study of a block-based inspection policy for a

* Tel.: +47 51 83 19 08; fax: +47 51 83 17 50.
E-mail address: roger.flage@uis.no

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.11.009

multi-component system comprising components with individual delay-time failure models [24].

In the present paper we consider a delay-time type system. To reveal defective systems, inspections are performed periodically using a procedure by which the system fails with a fixed state-dependent probability; otherwise, an inspection identifies a functioning system as defective (false positive) with a fixed probability and a defective system as functioning (false negative) with a fixed probability. The system is correctively replaced upon failure or preventively replaced either at the N'th inspection time or when an inspection reveals the system as defective, whichever occurs first. Replacement durations are assumed to be negligible and costs are associated with inspections, replacements and failures. The problem is to determine the optimal inspection interval T and preventive age replacement limit N that jointly minimise the long run expected cost per unit of time.

The system may also be thought of as a passive system subject to random demands. The system then has two states, functioning and failed, and the three states of the model are functioning, undetected failed and detected failed. In such a passive system interpretation the 'delay time' becomes the time between system failure and the first subsequent demand, i.e. the forward recurrence time of a demand. To ensure the renewal property of replacement cycles the demand process generating the 'delay time' is then restricted to the Poisson process.

There exist many papers treating imperfect inspections. In [17] models of imperfect maintenance are reviewed, including imperfect inspections. In [14] a delay-time model with imperfect inspections (called 'failed-safe' and 'failed-dangerous', corresponding to false positives and false negatives in the present paper, respectively) is developed. The model in the present paper also shares some features with the model described in [10], which also considers a system with three states (good, faulty and failed) subject to imperfect (false positives or false negatives) periodic inspections and replacement (overhaul) after a fixed number of inspections. However, unlike the present paper, the model in [10] includes only non-invasive inspections, and focus is on determining the optimal number of inspections only before preventive replacement. Furthermore, unlike the model described in the present paper, the model in [10] includes the possibility of imperfect repair of faulty systems and uses a Markovian structure in the computation of average costs. The model described in [26] is also concerned with optimal scheduling of periodic inspections and preventive age replacement; however, the model is of a two-state system (non-failed, failed). In [7] a study is performed on the quality of inspections in a maintenance optimisation model of a standby system where inspections may result in false positives or false negatives. This model is further developed in [6] by considering the two alternative scenarios that a false positive does or does not lead to a renewal of the system; as well as the possibility that replaced systems are drawn from a heterogenous population where new systems may be 'strong' or 'weak'. Failure-inducing inspections are studied in e.g. [12].

The inspiration for the model described in the present paper has been safety critical valves as installed in (offshore) oil and gas production and transportation systems. In this setting, safety critical valves would typically be taken to include emergency shut-down valves (ESDVs), blow down valves (BDVs), pressure safety valves (PSVs), subsea isolation valves (SSIVs) and down-hole safety valves (DHSVs) [13]. The purpose of all the previously mentioned types of safety critical valves is to sectionalise oil and gas production and transportation systems during hazardous situations, to avoid feeding leakages or fires. The functionality of these types of valves can be tested in several ways, with different levels of completeness. A full scale function test involves a complete valve closure, which would typically require the production to be shut-down (or rerouted if possible). Production shut-downs lead to considerable losses in revenue, and the shut-down and restart procedure could also pose an accident risk. As a result, production shut-downs are highly undesirable. Planned maintenance requiring an entire plant or system to be shut-down is usually only performed during so-called 'revision stops', during which as much planned maintenance as possible is performed. The alternative to a full scale test is an incomplete (partial) test in which not all possible failure modes are tested or, more generally, where the test result is unreliable (imperfect) in the sense that a test does not always reveal the true state of the tested system. An example of a partial test in the context of safety-critical valves is the so-called 'partial stroke' procedure, in which the actuator of a valve is only minimally activated. The valve is then only partially closed, and it is not known whether a complete closure would have occurred in the case that a complete test had been performed instead.

In a guideline [16] to the Norwegian petroleum legislation, the Petroleum Safety Authority Norway (PSAN) specifies annual testing of safety critical valves that are not covered by safety integrity level (SIL) standards:

> … the following should be used in the area of health, working environment and safety: […] the emergency shut-down system is verified in accordance with the safety integrity levels set on the basis of the IEC 61508 standard [11] and OLF's Guideline 070 [15]. For plants that are not covered by this standard and this guideline, the operability should be verified through a full-scale function test at least once each year. The test should cover all parts of the safety function, including closing of valves. The test should also include measurement of interior leakage through closed valves. Recording of the plant's or equipment's functionality in situations where the function is triggered or put to use, may replace testing of the plant or the equipment

Interior leakage refers to the phenomenon that during testing of valves in oil and gas production and transportation systems there could be some flow of hydrocarbons through a valve in the closed position. For subsea valves the Norwegian oil and gas industry today typically uses acceptance criteria defined by API recommended practices [1,2] to determine the maximum acceptable flow rate through a closed valve. A consequence-based methodology has also been developed to determine an acceptable internal leakage rate [19], based on the idea that only leaks through a closed valve that do not have significant consequential effects on a release to the atmosphere in terms of fire and/or explosion scenarios should be accepted.

Safety-critical valves in (offshore) oil and gas production and transportation systems also provide an example of how inspections could introduce (external) hazards to the system under inspection. Testing of such valves could lead to a gas leak which, if ignited, leads to an explosion or a fire in which the valve could be damaged. Such an accident scenario could also have consequences beyond damage to the valve (which, in a maintenance modelling setting, translate into a valve replacement cost). In particular, an explosion or a fire could lead to injuries or fatalities among the personnel carrying out the test if the test procedure necessitates physical proximity between the personnel performing the test and the valve being tested. Testing could also have negative environmental effects, e.g. if it becomes necessary to flare gas to the atmosphere during the testing. Considering loss of life as a potential consequence of an accident, the expected 'safety costs' would typically be determined as

$$c_A = r_A E[L|A] VPF,$$

where r_A is the probability of an accident A given a system failure, $E[L|A]$ the expected number of fatalities given an accident, and VPF the so-called 'Value of a Prevented Fatality' [20]. The first two quantities would typically be determined in a quantitative risk