Available online at www.sciencedirect.com
ScienceDirect
Reliability Engineering and System Safety 93 (2008) 1720–1729
RELIABILITY ENGINEERING & SYSTEM SAFETY
www.elsevier.com/locate/ress

Modeling demand rate and imperfect proof-test and analysis of their effect on system safety

Manoj Kumar[a,*], A.K. Verma[b], A. Srividya[b]

[a]*Control Instrumentation Division, BARC, Trombay, Mumbai 400085, India*
[b]*Reliability Engineering Group, IIT Bombay, Powai, Mumbai 400076, India*

Received 28 February 2007; received in revised form 27 November 2007; accepted 2 December 2007
Available online 15 December 2007

Abstract

Quantitative safety assessment of a safety system plays an important role in comparing design alternatives at design stage and deciding appropriate design options to apply for safety systems. There are a number of such indices given in the literature. Most of the safety indices consider only system parameters (hazard rate, repair rate, diagnosis, coverage, etc.) along with proof-tests (or inspection). This paper extends the underlying model to incorporate demand rate and imperfect proof-tests. It also introduces a new safety index, average probability of failure on actual demand (PFaD), and an availability index, manifested availability (mAv).

This paper uses Markov regenerative process-based analysis for state probabilities. Based on state-probability values of various states of the underlying Markov chain, solutions are derived for safety index PFaD and availability mAv.

Keywords: Probability of failure on demand; Fail dangerous; Fail safe; Markov model; Markov regenerative process; Continuous-time Markov chain; Proof-test; Availability

1. Introduction

Safety systems are used for automatic shutdown of equipment under control (EUC), whenever the equipment or plant parameters go beyond the acceptable limits for more than acceptable time. These kinds of systems are used in a variety of industries, such as oil refining, nuclear power plants, chemical and pharmaceutical manufacturing, etc. When the safety system is functioning correctly (successfully), it permits the EUC to continue provided its parameters remain within safe limits. If the parameters move outside of an acceptable operating range for a specified time, the safety system automatically shuts down the EUC in a safe manner.

Safety systems generally have some redundancy and can tolerate some failures while continuing to operate successfully. As discussed in Refs. [1–3,11], a system's independent channels can fail leading the system to the following states:

1. *Safe failure* (*SF*) state: where it erroneously commands to shut down a properly operating equipment. Taking a channel offline and shutting down of a channel is also referred to as safe failure.
2. *Fail dangerous detected* (*DD*) state: where a channel(s) has (have) failed in dangerous mode, but is (are) detected by internal diagnostics, and announced.
3. *Fail dangerous undetected* (*DU*) state: where a channel(s) has (have) failed in dangerous mode and is (are) not detected by internal diagnostics, hence not announced.

The safety system can fail in two distinctly different ways [1–3,7,11]:

1. *Safe failure* (F_S): Failure that does not have potential to put the safety system in a hazardous or fail-to-function state [1]. This occurs when more than tolerable numbers

*Corresponding author. Tel.: +91 22 25591822; fax: 91 22 25505151.
E-mail address: kmanoj@iitb.ac.in (M. Kumar).

0951-8320/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2007.12.001

Nomenclature

CTMC	continuous-time Markov chain
CCF	common cause failure
DC	diagnostic coverage
DD	dangerous detected (failure category in IEC-61508)
DU	dangerous undetected (failure category in IEC-61508)
SF	safe failure (failure category in IEC-61508)
DF	dangerous failure (failure category in IEC-61508)
DEUC	damage to EUC (or accident)
EUC	equipment under control or process plant
PFD	average probability of failure on demand
PFaD	average probability of failure on actual demand
MTBD	mean time between demands
MBF	multiple beta factor
T_{proof}	proof-test interval
mAv	manifested availability
F_{DU}	dangerous undetected state of the safety system
F_S	safe failure state of the safety system
λ_{SF}	hazard rate of a channel leading to SF
λ_{DD}	hazard rate of a channel leading to DD
λ_{DU}	hazard rate of a channel leading to DU
μ	repair rate of a channel in F_S
$\mu_P(t)$	time-dependent proof-test rate
λ_{arr}	demand arrival rate (1/MTBD)
Δ	probability redistribution matrix
demand	refers to a condition when the safety system must shut down EUC. The condition arises when EUC parameters move outside of an acceptable operating range for a specified time. The safety system shuts down the EUC by opening its output control switch(s)
IEC	safety standard IEC 61508

of channels are in safe failure. This type of failure is referred to in a variety of ways including fail safe [3,7], false trip and false alarm.

2. *Dangerous failure* (*DF*): Failure that has the potential to put the safety system in a hazardous or fail-to-function state [1]. More than tolerable numbers of channels in DD and/or DU lead to this failure. The system fails in such a way that it is unable to shut down the EUC properly when shutdown is required (or demanded).

Dangerous failures are important from a safety point of view. A survey of recent research work related to safety quantification indicates that there are diverse safety indices, methods and assumptions about safety systems. Safety indices used are PFD (probability of failure on demand) [1,2,4,11–15], $MTTF_D$ (mean time to dangerous failure) [3,7], $MTTF_{sys}$ (mean time to system failure) [5], MTTUF (mean time to unsafe failure) and S_{SS} (steady-state safety) [6], and MTTHE (mean time to hazardous event) [9]. Simplified equations [1,4,11–13], Markov models [2,3,5–7,9,10,14,15] and fault trees [12] are the methods used for safety quantification. Safety indices of [6,9] consider only repair, [3] considers repair as well as periodic inspection to uncover undetected faults, [1,2,4,11–13] consider common cause failure (CCF) and periodic inspection along with repair, and [10] considers demand rate. Ref. [4] discusses the CCF model (beta factor) of [1] and suggests generalization, the multiple beta factor (MBF) model.

Safety index PFD [1] has already been published as a standard. We take this index as a basis for this paper. IEC [1] gives simplified equations for safety evaluation. A review of different techniques by Rouvroye [8] suggests that Markov analysis covers most aspects for quantitative safety evaluation. Bukowski [14] compares various techniques for PFD evaluation and defends Markov models. Zhang [2] provides a Markov model for PFD evaluation without considering demand rate and modeling imperfect proof-tests. Bukowski [10] gives a safety measure based on PFD considering demand rate, but this model does not consider periodic proof-tests. A detailed comparison of these models with the one proposed here is given in Section 2.

The system model taken here for analysis is similar to the model of IEC [1] and uses the Markov model for analysis. This model explicitly considers periodic proof-test (perfect or imperfect), demand rate and safe failures. Incorporation of safe failure enables modeling of all possible system states and estimation of additional measures such as availability (or probability of being in one or more specified states) for a given amount of run time.

The paper is organized as follows. Section 2 gives system description and assumptions about the system to derive a Markov model. Performance-based safety index and availability are derived in Section 3. In Section 4 an example is taken to illustrate computation of safety index and availability. Advantage of modeling safe failures and availability along with safety index is discussed in Section 5. Conclusions are given in Section 6.

2. System model

The systems being discussed here fall into the category of programmable electronic systems (PES) as defined in IEC [1]. These systems are used for control, protection or monitoring based on one or more programmable electronic devices [1]. The elements of the system (sensors, processing devices, actuators, power supplies and wiring, etc.) are grouped into channels that independently perform a function.

To model the system, most of the assumptions taken here are similar to those given in Annex B of part 6 of IEC [1]. Assumptions such as (i) failure rates are constant over