Available online at www.sciencedirect.com

SCIENCE DIRECT®

Reliability Engineering and System Safety 90 (2005) 186–195

RELIABILITY ENGINEERING & SYSTEM SAFETY

www.elsevier.com/locate/ress

Uncertainties and quantification of common cause failure rates and probabilities for system analyses

Jussi K. Vaurio*

Fortum Power and Heat Oy, P.O. Box 23, 07901 Loviisa, Finland

Accepted 30 October 2004
Available online 15 December 2004

Abstract

Simultaneous failures of multiple components due to common causes at random times are modelled by constant multiple-failure rates. A procedure is described for quantification of common cause failure (CCF) basic event probabilities for system models using plant-specific and multiple-plant failure-event data. Methodology is presented for estimating CCF-rates from event data contaminated with assessment uncertainties. Generalised impact vectors determine the moments for the rates of individual systems or plants. These moments determine the effective numbers of events and observation times to be input to a Bayesian formalism to obtain plant-specific posterior CCF-rates. The rates are used to determine plant-specific common cause event probabilities for the basic events of explicit fault tree models depending on test intervals, test schedules and repair policies. Three methods are presented to determine these probabilities such that the correct time-average system unavailability can be obtained with single fault tree quantification. Recommended numerical values are given and examples illustrate different aspects of the methodology.

Keywords: Common cause failures; Data analysis; Empirical Bayes; Failure rate; Impact vector; Mapping; Standby system; Unavailability; Uncertainty

1. Introduction

Common cause events are defined as events that cause simultaneous failed states of multiple components due to a common cause. Such failures often dominate the unavailability of a standby safety system designed to react to a threatening incident. Failures occur at random times. General multiple-failure rates λ_i, λ_{ij}, $\lambda_{ijk\ldots}$, etc. are defined so that $\lambda_{ij\ldots}\,\mathrm{d}t$ is the probability of an event failing specific components $i,j,\ldots$ in a small time interval $\mathrm{d}t$. Such shocks have been used in early models with various assumptions [1–5]. In standby safety systems these failures remain latent until discovered by a scheduled test and then repaired. Safety components are usually tested periodically. Because single failures as well as CCF can occur at any time, the system unavailability can be a complicated function of time, depending on the event rates, test intervals, test scheduling and repair policies. When a system fault tree is made and the system unavailability is computed step by step as a time-dependent function, typical time-dependent probabilities of CCF-events $Z_{ij\ldots}$ are

> $P[Z_{ij\ldots}(t)] = u_{ij\ldots}(t) = \lambda_{ij\ldots}(t - T_t)$ = probability of failed states of components $i,j,\ldots$ at time t due to a common cause failing exactly these components simultaneously with rate $\lambda_{ij\ldots}$, when the last possible discovery and repair of such failure occurred at T_t.

The time factors are assumed such that these probabilities are clearly smaller than unity.

In fault tree models such basic events are input through OR-gates to components $i,j,k,\ldots$, as illustrated in Figs. 1 and 2. Fig. 3 illustrates the time-dependent unavailabilities of a simple standby system with two trains and staggered (alternating) testing. In this example every test reveals and repairs also double failures, not only the single unit scheduled for testing. This is why $u_{12}(t)$ starts from zero after every test. An alternative is that a double failure would reduce to a single failure at the first test after a CCF occurs.

* Address: Lappeenranta University of Technology, Lappeenranta, Finland. Tel.: +358 10 4554700; fax: +358 10 4554435.
E-mail address: jussi.vaurio@fortum.com.

0951-8320/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2004.10.014

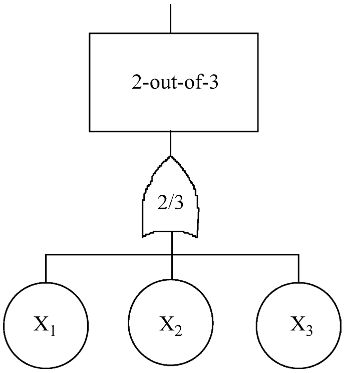

Fig. 1. Component-level fault tree (example, $n=3$).

Modern computer codes for fault tree quantification should allow such models and input data for realistic calculation or monitoring the system unavailability or plant risk.

The first topic of this paper deals with estimation of the rates $\lambda_{ijk\ldots}$ under uncertainties associated with incomplete records or ambiguities of event observations and interpretations. Moments of the rates are obtained with a method that extends earlier results [6–9] to more complex observations [14]. A special impact vector weighting procedure is suggested to account for multiple events in a single observation.

The second task is to point out how the moments of CCF-rates so obtained for many individual plants can be combined in the empirical Bayesian estimation (EBE) framework to obtain improved posterior estimates for a target plant or for all plants. This methodology is based on *equivalent observations*, first introduced in 2001 [10] and later to a wider audience with additional applications [11]. Several variants of one-stage or two-stage EBE could be used in this context.

The third problem to be addressed here is: How to define the input probabilities for a fault tree model so that correct time-average risk (or system unavailability) can be obtained with a single fault tree computation, avoiding time-dependent step-by-step calculations? This topic has been addressed in three different ways for standby systems with n redundant trains, $n=1$, 2, 3 and 4, considering (1) analytical expressions of the system unavailabilities [12], (2) expected residence times of each CCF [13], and (3) mathematically exact transformation equations [17]. The last two methods have produced probabilities also for non-identical components and non-symmetric rates (e.g. $\lambda_{12}\neq\lambda_{13}$). In the latest method [17] the probabilities depend on the number of redundant components n (common cause component group size) but not on the system success criterion, and the probabilities include both linear and nonlinear terms of the test interval T. The alternatives are compared, advantages and disadvantages of the results are discussed, and practical numerical recommendations are provided. Three testing and repair policies are considered: consecutive testing, staggered testing with extra tests, and staggered testing without extra tests.

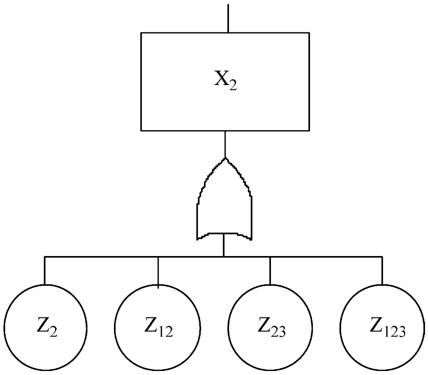

Fig. 2. Component event X_2 modelled by cause events Z_{ij}.

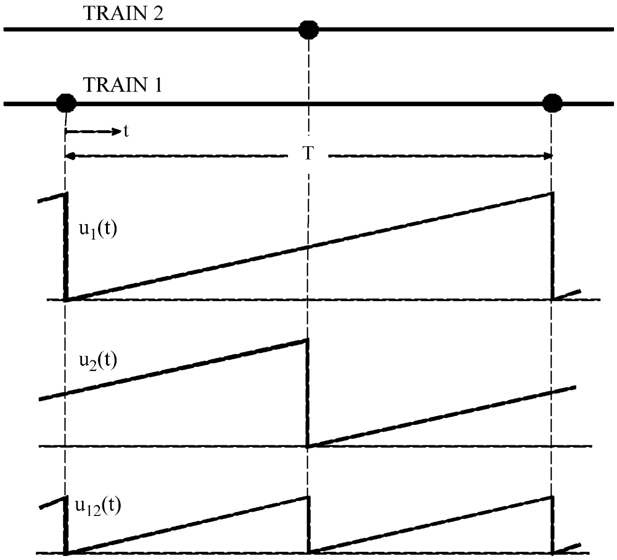

Fig. 3. Staggered testing scheme for $n=2$ trains. Single failure unavailabilities $u_1(t)$ and $u_2(t)$, CCF unavailability $u_{12}(t)$.

These developments are synthesised into a procedure that leads from raw event data collection to plant-specific input parameters for system reliability and risk assessment.

1.1. Notation and acronyms

CCCG	common cause component group; n components subject to common cause events
CCF	common cause failure(s)
ETRR	Extra Testing and Repair Rule: whenever a component is found failed in a test, the other $n-1$ trains are also tested or inspected, and any failed components are repaired
ITRP	Individual Testing and Repair Policy: components are tested and repaired individually with regular intervals T; no other component is tested immediately even if one is found to be failed
$\lambda_{k/n}$	rate of CCF events failing specific k trains or channels (and no others) in a system with n