Reliability Engineering and System Safety 172 (2018) 159–170

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

A stochastic hybrid systems model of common-cause failures of degrading components

Mengfei Fan[a], Zhiguo Zeng[b,*], Enrico Zio[b,c], Rui Kang[a], Ying Chen[a]

[a] School of Reliability and Systems Engineering, Beihang University, Beijing, China
[b] Chair System Science and the Energy Challenge, Fondation Electricité de France (EDF), CentraleSupélec, Université Paris Saclay, Gif-sur-Yvette, France
[c] Energy Department, Politecnico di Milano, Milan, Italy

ARTICLE INFO

Keywords:
Common-cause failures
Random shocks
Component degradation
Stochastic hybrid systems
Binomial failure rate model
Monte Carlo simulation

ABSTRACT

Common-Cause Failures (CCFs) are an important threat to safety critical systems. Most existing CCF models assume that the component failure behavior does not vary over time. Such an assumption is often challenged in practice due to the influence of various degradation mechanisms, e.g., wear, corrosion, fatigue, etc. In this paper, we develop a new model for CCFs considering components degradation. The model is developed in the mathematical framework of Stochastic Hybrid Systems (SHS). The CCFs are modeled as random shock processes that affect a group of components simultaneously and the components degradation processes are modeled by stochastic differential equations derived from physics-of-failures. The benefit of using the SHS model for CCFs is that the developed model is analytically solvable. The system reliability can, then, also be solved analytically in closed form. The proposed CCF modelling framework is demonstrated by a numerical example of a three-unit redundant system and, then, applied to an Auxiliary Feedwater Pump (AFP) system of a Nuclear Power Plant (NPP). A comparison to the Binomial Failure Rate (BFR) model of literature shows that by considering the components degradation processes, the proposed model can accurately describe the CCF effect on the reliability of a system with degrading components.

1. Introduction

Common-Cause Failures (CCFs) are simultaneous failures of multiple components of a system due to a shared root cause [1]. They are a most important threat to the reliability of safety critical systems in various industries, e.g., nuclear [2], oil and gas [3], aerospace and aviation [4], etc. Due to the shared root cause, redundancies can be defeated. From the modelling point of view, the basic events of components failure are no longer independent, which makes CCFs modelling a challenging task in risk and reliability analysis. In general, models that consider CCFs can be derived by breaking down the event of system failure into a series of conditional independent basic events of different component groups using the law of total probability. Various methods can be used for this, e.g., basic probability model [5], dynamic fault tree [6–11], Bayesian network [12–15], etc.

According to [2], existing CCF models can be broadly classified into two categories: non-shock models (statistical models) and shock models (mechanistic models). Non-shock models do not consider the actual process which leads to the CCFs. Rather, the models are constructed by directly estimating the probability of CCF events using statistical data related to these events [2]. Typical non-shock models include the Beta Factor (BF) model [16], the Alpha Factor (AF) model [17], the Multiple Greek Letter (MGL) model [18], etc. Since statistical data for CCF events, especially for higher order CCF events, are generally rare, parameter estimation becomes a challenging problem in practice [19].

As advocated in Zio et al. [20,21], reliability modelling in general, and CCF modelling in particular, can be greatly advanced by integrating the large body of Knowledge, Information and Data (KID) that is continuously becoming available on the processes of failure and degradation of components and systems. A typical example of such integration is the use of shock models to explicitly model the actual process leading to CCFs: when a CCF shock arrives, simultaneous component failures may occur [2]. Compared to the non-shock models, the shock models attempt to integrate additional knowledge on the CCF failure process, explicitly modelling it as random shocks. A typical example of shock models is the Binomial Failure Rate (BFR) model, used for example in the nuclear industry [22]. First proposed by Vesely [23], the BFR model assumes that when a CCF shock (non-lethal shock) arrives, the components may fail with some failure probability. Then, the failure probability related

* Corresponding author.
E-mail addresses: fanmengfei@buaa.edu.cn (M. Fan), zhiguo.zeng@centralesupelec.fr (Z. Zeng), enrico.zio@ecp.fr (E. Zio), kangrui@buaa.edu.cn (R. Kang), cheny@buaa.edu.cn (Y. Chen).

https://doi.org/10.1016/j.ress.2017.12.003
Received 6 April 2017; Received in revised form 6 December 2017; Accepted 10 December 2017
Available online 12 December 2017
0951-8320/

Acronyms

AFP	Auxiliary feedwater pump
BFR	Binomial failure rate
CCF	Common-cause failure
CCCG	Common cause component group
FT	Fault tree
FOSM	First order second moment
HPP	Homogeneous Poisson process
KID	Knowledge, information and data
MC	Monte Carlo
MLE	Maximum likelihood estimation
NPP	Nuclear power plant
PDF	Probability density function
SHS	Stochastic hybrid systems
SDE	Stochastic differential equation
TTF	Time-to-failure

Notation

q	The discrete state of the system
x	The continuous state of the system
λ	The intensity of the Poisson process
ϕ	The reset map
ψ	The test function
H	The threshold of the component degradation process
w_t	The standard Wiener process
Y	The Boolean state variable
l	The number of degrading components in the system
n	The number of the discrete states of the SHS
$O(\cdot)$	The "big Oh" notation used to describe the complexity of algorithms

to the CCF event can be calculated from a binomial distribution. Atwood et al. [22] generalized the model to consider both lethal shocks and non-lethal shocks, where lethal shocks cause the simultaneous failure of all the components in a Common Cause Component Group (CCCG). Hauptmanns [24] developed a Multi-Class Binomial Failure Rate (MCBFR) model as an extension to the original BFR model, where the CCFs are divided into different technical classes with different coupling factors. Kvam [25] extended the BFR model to consider multiple shock sources, assuming that the probability of random shocks follow a beta distribution. Nonparametric maximum likelihood estimation of the BFR model parameters were discussed in Kvam [26]. Berg et al. [27] developed a Process-Oriented Simulation (POS) model as a simulation-based extension to the original BFR model. Differently from the BFR model, the POS model distinguishes immediate failures and delayed failures of the components affected by a common cause event, and assigns probabilities to different degrees of effects of a common cause event on the components. Atwood and Kelly [28] developed a Bayesian inference method for the BFR model.

Apart from the BFR model, other widely applied CCF shock models include the Stochastic Reliability Analysis (SRA) model [29], the General Multiple Failure Rate (GMFR) model [30] and the Common Load Model (CLM) [19]. The SRA model was developed by Dorre [29] to consider the uncertainty in the probability of the CCF events, given the arrival of the shock. A similar model was developed in Hughes [31] where the distribution of the CCF probabilities is modeled as a weighted average of the corresponding conditional probability under different environment conditions. The GMFR model was developed in [30] for CCF events that result from random shock processes with independent rates. Vaurio et al. applied the GMFR model to investigate the unavailability of redundant standby systems [32] and m-out-of-n: G systems [33] under different test strategies, respectively. In the CLM [34], the common load shared by a group of components is regarded as the "root cause" of the CCFs and the reliability is estimated using the stress-strength interference model [19]. Based on the CLM, Mankamo and Kosonen [35] proposed an Extended Common Load Model (ECLM) for CCF modelling of highly redundant systems. Xie [19] developed a Knowledge-Based Multi-dimension Discrete (KBMD) CCF model and related parameter estimation method. Failure data from similar CLMs are used in [36] for the CCF probability assessment based on a data mapping approach.

In the existing CCF shock models reviewed above, the effect of the shock on the CCF event is assumed to be independent of time. In practice, however, degradation mechanisms might affect the components behavior to failure, e.g., wear, fatigue, corrosion, etc. [37]. The components degradation processes are not fully considered in the existing CCF shock models. To this regard, we develop a new model to consider both components degradation and CCFs, which further extends the knowledge base of the CCF models by integrating physics-of-failure degradation models. The model is developed based on a mathematical framework, called Stochastic Hybrid Systems (SHS), which is used for modelling and analyzing dynamic stochastic systems involving both discrete and continuous states [38]. By solving a set of differential equations generated by Dynkin's formula [39], the probability distribution of the discrete states, as well as the conditional moments of the continuous states under each discrete state can be derived [40]. Typical applications of SHS include modelling of networked control systems [41], Markov reward models [39], dynamic power systems [42], dependent failure processes [43], etc. However, to the best of our knowledge, the present work represents the first attempt to use SHS for modelling CCFs.

The developed model contributes to the existing scientific literature in two aspects:

- a new SHS-based model for CCFs is developed, which allows considering components degradation;
- a closed-form expression for system reliability is derived based on the SHS model.

The remainder of this paper is organized as follows. Section 2 presents the developed SHS model for CCFs of degrading components. The SHS model is demonstrated using a numerical example (Section 3), and then, applied on an Auxiliary Feedwater Pump (AFP) system of a Nuclear Power Plant (NPP) (Section 4). Section 5 concludes this paper.

2. The SHS model of CCFs of degrading components

In this section, we present the SHS model of CCFs, considering components degradation. First, SHS modelling is briefly introduced in Section 2.1. In Section 2.2, we describe the SHS model of CCFs of degrading components. Conditional moments of the state variables are derived in Section 2.3. System reliability is, then, estimated based on the conditional moments in Section 2.4. In Section 2.5, estimation of the SHS model parameters is discussed.

2.1. SHS modelling

The state space of an SHS is a combination of discrete and continuous states. Let us denote the discrete states by $q(t)$, $q(t) \in Q$, where Q is a finite set containing all the possible discrete modes of the system. The continuous states are denoted by $x(t), x(t) \in \mathbb{R}^l$. An SHS is defined based on the following assumptions [38,40,44]:

(1) The evolution of the continuous states is governed by a set of Stochastic Differential Equations (SDEs):

$$dx(t) = f(q(t), x(t))dt + g(q(t), x(t))dw_t, \tag{1}$$

where $w_t : \mathbb{R}^+ \to \mathbb{R}^k$ is a k-dimensional Wiener process; $f : Q \times \mathbb{R}^l \to \mathbb{R}^l$ defines the evolution of the continuous state and $g : Q \times \mathbb{R}^l \to \mathbb{R}^{l\times k}$ determines the coefficients of the Wiener process.

(2) At any time t, if the system is in state $(q(t), x(t))$, it undergoes a transition with a rate $\lambda_{ij}(q(t), x(t)) : Q \times \mathbb{R}^l \to \mathbb{R}^+$, $i, j \in Q$. That is,