Modeling common-cause failures using stochastic hybrid systems

Mengfei Fan & Rui Kang & Ying Chen
School of Reliability and Systems Engineering, Beihang University, Beijing, China

Center for Resilience and Safety of Critical Infrastructures, Beihang University, Beijing, China

Zhiguo Zeng
Chair System Science and Energy Challenge, Fondation Electricite de France (EDF), CentraleSupelec, Universite Paris-Saclay, Chatenay-Malabry, France

Enrico Zio
Chair System Science and Energy Challenge, Fondation Electricite de France (EDF), CentraleSupelec, Universite Paris-Saclay, Chatenay-Malabry, France

Energy Department, Politecnico di Milano, Milano, Italy

ABSTRACT

In this paper, we develop a novel Common-Cause Failure (CCF) model for reliability assessment, based on component degradation information. A Stochastic Hybrid Systems (SHS) model is developed to describe the components and system degradation process by state dynamics, under CCFs. A component failure is either caused by cumulative degradation of the component or by destructive external events (shared root causes of CCFs). A case study is considered regarding the Auxiliary Feedwater Pumps (AFPs) of a Nuclear Power Plant (NPP) suffering internal flooding. AFPs may fail due to internal flooding from three main water sources, i.e. service water (SW), circulating water (CW) and fire protection water (FPW). A flood barrier is built to protect the AFP from internal flooding. System's fault tree is presented in Figure 1. Two CCFs are considered in this paper, as illustrated in Table 1.

The developed SHS model is graphically illustrated in Figure 2. In the developed model, degradations of the components are characterized by stochastic differential equations:

$$dx_i(t) = \alpha_i dt + \beta_i \cdot dw_t, i = \mathrm{A,B,C,D}, \quad (1)$$

where A, B, C and D correspond to SW piping, CW piping, FPW piping and flood barrier, respectively. Component failures occur when the degradation reaches the corresponding failure thresholds. The degradation processes might be influenced by non-fatal shocks: when such shocks arrive, the continuous degradation process will be reset by: $\mathbf{x}(t) = \mathbf{x}(t) + \mathbf{d}$, where $\mathbf{d} = (d_{\mathrm{A}}, d_{\mathrm{B}}, d_{\mathrm{C}}, d_{\mathrm{D}}) \in \mathbb{R}^4$ is a vector of shock damages.

Three discrete states, $q(t) \in \{1,2,3\}$, are introduced to model the CCFs, where $1,2,3$ represent "normal", "CCF1", "CCF2", respectively. The system start operation from state 1 where the four components degrade according to (1); when a tornado arrives, the system transfers to "CCF1" state, i.e. $q = 2$, where components A,B,C fail simultaneously with $x_{\mathrm{A}}(t), x_{\mathrm{B}}(t), x_{\mathrm{C}}(t)$ reset to their respective thresholds, while component D degrades as it does in the "normal" state; when an earthquake occurs, the system transfers to "CCF2" state, i.e. $q = 3$, where all components fail with their degradation levels reset to the thresholds. The system reliability is estimated by the First Order Second Moment method (FOSM) (Zhao and Ono, 2001), using the conditional moments of the component degradation level obtained from the SHS model.

Table 1. Common cause failures effecting the AFP

Item	Root Cause	Common Cause Group
CCF1	Tornado	{A,B,C}
CCF2	Earthquake	{A,B,C,D}

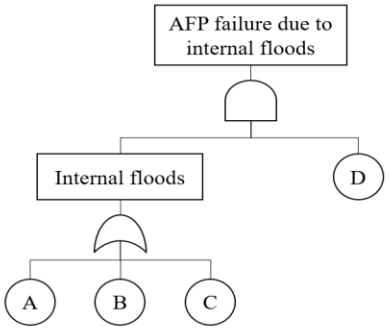

Figure 1. Fault tree for "AFP failure due to internal floods" (A: "SW piping rupture", B: "CW piping rupture", C: "FPW piping rupture", D: "flood barrier break")

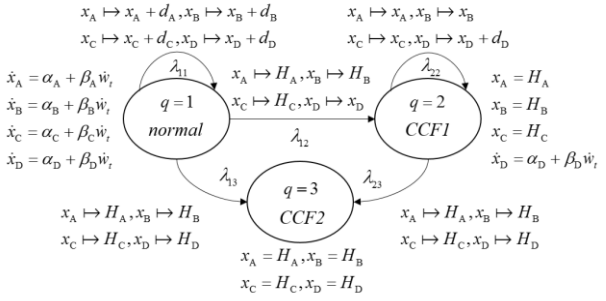

Figure 2. State-transition diagram for the SHS

REFERENCES

ZHAO, Y. G. and ONO, T. 2001. Moment methods for structural reliability. Structural Safety, 23, 47-75.