A study on some system safety models

L. Cui, X. Zhao & J. Li

School of Management & Economics, Beijing Institute of Technology, Beijing, P. R. China

ABSTRACT: In this paper two system safety models are built based on some practical situations. The system state can be distinguished into three states: working, fail-safe and fail-dangerous. The probabilities that the system are in working state, fail-safe state and fail-dangerous state, respectively, are derived. Also the mean times for the system working, fail-safe and fail-dangerous, are given. Finally some numerical examples are presented to illustrate the results obtained in this paper.

1 INTRODUCTION

In real situation there are lots of systems with multi-failure-state, different failure-state has different effects for systems. In general, people classify the failure-state into two kinds of categories: fail-safe states and fail-dangerous states, specially for some important reliability and safety systems such as nuclear power plant, chemical processing plant, power transmission, bank payment system, commercial surgical robot system, etc.. This kind system usually has a control subsystem, which monitors the operating system to prevent it from occurrence of dangers events. In the literature, there are some researches on this problem. Bukowsiki & Goble (2001), Bukowsiki (2001) discussed this kind problem by using Markov Chain Method, the important measure MTTF in a particular failure state was separated from MTTF into $MTTF_D$ (fail dangerous) and $MTTF_S$ (fail safe), and their formulas were derived. Cowing et al.(2004), Inagaki, Ikebe (1989) & Zhou (1987) also discussed safety critical systems, and among others. If the Markov method was employed, then the transition rates are constants, i.e., the exponential distributions are used, which model the real situation narrowly. In this paper, we assume that the distributions to be used are general forms, which extends the past results in the literature. The purpose of this paper is to present some indexes formulae for evaluating the system safety performance such as probabilities of fail-safe, fail-dangerous, mean time to fail-safe, mean time to fail-dangerous in terms of two models, which will be built based on some real practical problems. In the system to be considered, there are three states as shown in figure 1. Because we just consider a simple case, the working state, denoted as W, can only transfer to two failure states: fail-safe, denoted as FS, and fail-dangerous, denoted as FD.

Figure 1. The transition diagram of the system.

Two safety models are introduced first in Section 2. In Section 3 some indexes for system reliability and safety aspects are proposed, also their closed-form solutions for the computation of the aforementioned indexes are derived. Some numerical examples are presented to illustrate the application of the solutions to a particular case.

2 MODELS & ASSUMPTIONS

There are two models to be built for safety systems in this paper. The models can used to describe lot of situation in reliability field such as chemical production, nuclear-power station and alarm systems.

The assumptions for model 1 are as follows,

1. The system is working if component $X$ or $Y$ works;
2. If component $X$ is down first, then component $Y$ is down second, then the system is in the fail-safe state;
3. If component $Y$ is down first, then component $X$ is down second, then the system is in the fail-dangerous state.
The assumptions for model 2 are as follows:
The system works if component $X$ works;
The other assumptions are the same as assumptions (2) & (3) listed above for model 1. Also the assumptions of independence and nonnegative lifetime among components for discussion are needed for both models. Components $X$ and $Y$ have distributions $F(x)$ and $G(y)$, respectively.

Some concrete backgrounds for the above models can be seen the following statements. Model 1, component $X$ is a device without alarm or protector; component $Y$ is the standby device with alarm or protector, and the alarm or protector can fail together with the device of $Y$, also the function of the alarm or protector is useful for both devices of $X$ and $Y$. Model 2, Component $X$ is a device, component $Y$ is an alarm or protector. Throughout the paper, we use the symbols $X$ and $Y$ to represent both components and their lifetimes.

3 INDEXES FOR SYSTEM SAFETY

The important reliability and safety indexes such as fail-safe probability, fail-dangerous probability, mean time to fail-safe, mean time to fail-dangerous for both models need to be studied, which have practical and theoretical meanings for safety systems, also they can be used in evaluating and measuring the performance of the systems. They also can provide some significant help in design and maintenance work.

The closed-form formulas for these important indexes are derived as follows for the two models in terms of the definitions of these indexes. All results are new ones.

For Model 1:
(1) fail-safe probability:

$$F_1^{(1)}(t) = P(X < Y < t)$$

$$= \int_0^t [G(t) - G(x)] dF(x);$$

(2) fail-dangerous probability:

$$F_1^{(2)}(t) = P(Y < X < t)$$

$$= \int_0^t [F(t) - F(y)] dG(y);$$

(3) mean time to fail-safe:

$$MTTF_1^{(1)} = E[Y \mid X < Y]$$

$$= \frac{1}{P(X < Y)} \int_{x,Y} y dG(y)$$

$$= \frac{\int_0^\infty yF(y) dG(y)}{\int_0^\infty F(y) dG(y)};$$

(4) mean time to fail-dangerous:

$$MTTF_1^{(2)} = E[X \mid Y < X]$$

$$= \frac{\int_0^\infty xG(x) dF(x)}{\int_0^\infty G(x) dF(x)};$$

The both mean time formulae are can be used in calculating the characteristics of safety systems, which are often used in practice. On the other hand, we can know from the above four formulae that the symmetric property between distributions $F(x)$ and $G(y)$ holds, which results from the fact that safe state and dangerous state are symmetry in mathematical meaning.

For model 2:
(1) fail-safe probability:

$$F_2^{(1)}(t) = P(X < t, X < Y)$$

$$= \int_0^t [P(X < \min(t,y))] dG(y)$$

$$= \int_0^t F(\min(t,y)) dG(y);$$

(2) fail-dangerous probability:

$$F_2^{(2)}(t) = P(X < t, Y < X)$$

$$= \int_0^t [F(t) - F(y)] dG(y);$$

(3) mean time to fail-safe:

$$MTTF_2^{(1)} = E[X \mid X < Y]$$

$$= \frac{\int_0^\infty x[1 - G(x)] dF(x)}{\int_0^\infty [1 - G(x)] dF(x)};$$

Compared the same index for both models, we can know that $MTTF_2^{(1)} \geq MTTF_2^{(2)}$, which is more intuitive.
mean time to fail-dangerous:

\[ MTTF_D^{(2)} = E[X | X > Y] \]
\[ = \int_0^\infty xG(x)dF(x) \]
\[ = \frac{\int_0^\infty G(x)dF(x)}{\int_0^\infty dF(x)}. \]

It is clear that the relations \( F_S^{(i)}(t) + F_D^{(i)}(t) \leq 1 \) and \( \lim_{t \to \infty} [F_S^{(i)}(t) + F_D^{(i)}(t)] = 1 \) hold for \( i = 1, 2 \), which also can be shown in numerical calculations in next Section. For the above formulae we know that \( MTTF_D^{(1)} = MTTF_D^{(2)} \), it tells us that the mean times to fail-dangerous for both models are the same, which coincides with our intuition. Because the protector or alarms fails first, then the failure of safety device will result in dangerous situation in the same mean time.

In summary, we compare the indexes derived between two models, there are the following results,

1. \( F_S^{(1)}(t) \leq F_S^{(2)}(t) \);
2. \( F_D^{(1)}(t) = F_D^{(2)}(t) \);
3. \( MTTF_S^{(1)} \geq MTTF_S^{(2)} \);
4. \( MTTF_D^{(1)} = MTTF_D^{(2)} \).

**4 NUMERICAL EXAMPLES**

It is assumed that components \( X \) and \( Y \) have distributions \( F(x) = 1 - \exp(-x^2) \) and

\[ G(y) = 1 - (1 + y + \frac{y^2}{2}) \exp(-y). \]

For model 1, using the Maple software, we get the following curves for \( F_S^{(1)}(t) \) and \( F_D^{(1)}(t) \).

Also we get \( MTTF_S^{(1)} = 3.1793 \), \( MTTF_D^{(1)} = 1.3512 \).

Similarly, for model 2, we get the curves for \( F_S^{(2)}(t) \) and \( F_D^{(2)}(t) \).

Also we get \( MTTF_S^{(1)} = 3.1793 \), \( MTTF_D^{(1)} = 1.3512 \).

Similarly, for model 2, we get the curves for \( F_S^{(2)}(t) \) and \( F_D^{(2)}(t) \).

Also we get \( MTTF_S^{(2)} = 0.8460 \) and \( MTTF_D^{(2)} = 1.3512 \).

![Figure 3. The curve for \( F_D^{(1)}(t) \).](image)

![Figure 4. The curve for \( F_D^{(2)}(t) \).](image)
5 CONCLUSION

Two models are built in the paper for safety systems in terms of some practical backgrounds, the important reliability indexes are discussed, and their formulas are derived, which have significant meaning for evaluating the system safety performance and can be used to improve the safety design of the system. All results are new and the corresponding results in the literature are the special cases of our results, and the new results can be used regardless of the forms of component distributions. The relationship between indexes for two models are also presented, which is useful for comparison. The work considers general distribution which is different from the past work, the extension can be done by considering the repair effects.

ACKNOWLEDGMENT

This research is supported by the National Science Foundation Committee of China (No. 70371048), BIT grant and Program for New Century Excellent Talents in University, China (NCET). The Authors thank the anonymous referees for their helpful suggestions which improved the presentation of this paper.

REFERENCES


