AN ADVANCED RELIABILITY MODEL FOR AUTOMATED "SAFETY SYSTEM-PROTECTED OBJECT" COMPLEX WITH TIME REDUNDANCY

A. I. Pereguda, D. A. Timashov

●

Obninsk Institute for Nuclear Power Engineering, Obninsk, Russia

e-mail: pereguda@iate.obninsk.ru

ABSTRACT

The paper presents a new reliability model for an automated "safety system-protected object" complex with time redundancy. It is supposed that the time redundancy is caused by a protected object inertia. Scheduled periodic inspections of the safety system are also taken into account. Two-sided estimates of the mean time to accident are proposed.

1 INTRODUCTION

Redundancy is a widely used and widely referenced concept. Time redundancy means that some excess time is available after the system fault. It is possible to prevent an accident during this period. Such kind of redundancy may arise by design or as a natural byproduct of design. There are some methods available for the estimation of reliability indices of systems with time redundancy (Gnedenko & Ushakov 1995). But there is a lack of reliability models for automated "safety system-protected object" complex with the time redundancy caused by a protected object inertia. Systems of such kind are quite common in the nuclear power engineering due to an inertia of physical processes in the reactor core. This natural redundancy is seldom acknowledged and exploited. In the present study we set out to analyze the reliability of such system. We follow Pereguda (Pereguda 2001) in assuming that the operation of the complex can be described using a superposition of alternating renewal processes. Our objective is to provide an asymptotic estimation for the mean time to accident.

2 MODEL DESCRIPTION

Let us consider an automated complex of a safety system and a protected object. The safety system and the protected object are repairable. They are restored to an as-good-as-new state. It is assumed that safety system failures can be detected only during periodic inspections of the safety system. All failures are supposed to be independent. Safety system consists of two subsystems: the temperature subsystem and the power subsystem. If the power subsystem fails then the temperature subsystem is still able to prevent an accident. By χ_i, $i = 1,2,\ldots$ denote the time to the i-th protected object failure due to the increased power level. Let χ_i, $i = 1,2,\ldots$ be independent and identically distributed (i.i.d) random variables with CDF $F_\chi(t)$. By γ_i, $i = 1,2,\ldots$ denote the time to the protected object repair after it's i-th failure due to the increased power level. Let γ_i, $i = 1,2,\ldots$ be i.i.d. random variables with CDF $F_\gamma(t)$. Suppose that moments of the protected object repair after it's failure due to the increased power level are renewal points of the operation process of the complex. By δ_i denote the time between i-th protected object failure due to the increased power level and the subsequent failure due to the increased temperature. Let δ_i, $i = 1,2,\ldots$ be i.i.d. random variables with CDF $F_\delta(t)$. Thus the power safety subsystem may prevent an accident during the $[\chi_i, \chi_i + \delta_i)$ interval. Alternatively the temperature safety subsystem may prevent an accident at $\chi_i + \delta_i$. By α_i, $i = 1,2,\ldots$

denote the time to the protected object repair after such an event. Let α_i, $i = 1,2,\ldots$ be i.i.d. random variables with CDF $F_\alpha(t)$. Suppose that moments of the protected object repair after it's failure due to the increased power level and subsequent increased temperature are renewal points of the operation process of the complex. By φ_i, $i = 1,2,\ldots$ denote the time to the i-th protected object failure due to the increased temperature. Let φ_i, $i = 1,2,\ldots$ be independent and identically distributed (i.i.d) random variables with CDF $F_\varphi(t)$. By ψ_i, $i = 1,2,\ldots$ denote the time to the protected object repair after it's i-th failure due to the increased power level. Let ψ_i, $i = 1,2,\ldots$ be i.i.d. random variables with CDF $F_\psi(t)$. Suppose that moments of the protected object repair after it's failure due to the increased temperature are renewal points of the operation process of the complex. By ξ_i^p, $i = 1,2,\ldots$ denote the time to the i-th failure of the power safety subsystem. Let ξ_i^p, $i = 1,2,\ldots$ be i.i.d. random variables with CDF $F_{\xi^p}(t)$. By η_i^p, $i = 1,2,\ldots$ denote the time to the power safety subsystem repair after it's i-th failure. Let η_i^p, $i = 1,2,\ldots$ be i.i.d. random variables with CDF $F_{\eta^p}(t)$. Suppose that moments of the power safety subsystem repair after it's failure are renewal points of the operation process of the power safety subsystem. By T^p denote the period of scheduled inspections of the power safety subsystem. By θ^p denote the duration of scheduled inspections of the power safety subsystem. By ξ_i^t, $i = 1,2,\ldots$ denote the time to the i-th failure of the temperature safety subsystem. Let ξ_i^t, $i = 1,2,\ldots$ be i.i.d. random variables with CDF $F_{\xi^t}(t)$. By η_i^t, $i = 1,2,\ldots$ denote the time to the temperature safety subsystem repair after it's i-th failure. Let η_i^t, $i = 1,2,\ldots$ be i.i.d. random variables with CDF $F_{\eta^t}(t)$. Suppose that moments of the temperature safety subsystem repair after it's failure are renewal points of the operation process of the temperature safety subsystem. By T^t denote the period of scheduled inspections of the power safety subsystem. By θ^t denote the duration of scheduled inspections of the power safety subsystem. The safety system is inactive during the inspection. By ω denote the time to accident. Our aim is to estimate the mean time to accident $E[\omega]$.

2 MAIN RESULTS

Since the operation process of the complex is a superposition of alternating renewal processes, it follows that

$$\omega = \sum_{i=1}^{\nu-1} \sigma_i + \sigma'_\nu$$

where

$$\sigma_i = \min(\chi_i, \varphi_i) + \left(\left(\beta_i + \gamma_i\right)J_{B_i} + \left(\delta_i + \alpha_i\right)J_{\overline{B}_i}\right)J_{\chi_i \le \varphi_i} + \psi_i J_{\varphi_i < \chi_i}$$

and

$$\sigma'_i = \min(\chi_i, \varphi_i) + \delta_i J_{\chi_i \le \varphi_i}\,.$$

By β_i we denote the interval between the protected object failure due to the increased power level and the activation of the power safety subsystem. Note that $0 \le \beta_i < \delta_i$. By B_i we denote the event that the power safety subsystem was activated in the $[\chi_i, \chi_i + \delta_i)$ interval. By $\overline{B}_i$ we denote the event that the power safety subsystem was not activated in the $[\chi_i, \chi_i + \delta_i)$ interval. J_B is an indicator function of the event B.

We obviously have

$$F_\omega(t) = \Pr(\omega \le t) = \Pr\left(\sum_{i=1}^{\nu-1} \sigma_i + \sigma'_\nu \le t \right).$$

Applying the Laplace-Stieltjes transform to $F_\omega(t)$, we obtain

$$\widetilde{F}_\omega(s) = E\left[e^{-s\omega}\right] = \sum_{n=1}^{\infty} E\left[e^{-s\omega} \mid \nu = n\right] \Pr(\nu = n)$$

where $\widetilde{F}_\omega(s) = \int_0^\infty e^{-st} dF_\omega(t) = E\left[e^{-s\omega}\right]$, $\Pr(\nu = n) = q(1 - q)^{n-1}$ and q is the probability of an accident during a renewal interval. We see that

$$E\left[e^{-s\omega} \mid \nu = n\right] = E\left[e^{-s\left(\sum_{i=1}^{\nu-1}\sigma_i + \sigma'_\nu\right)} \middle| \nu = n \right] = \left(\widetilde{F}_\sigma(s)\right)^{n-1} \widetilde{F}_{\sigma'}(s) .$$

Therefore

$$\widetilde{F}_\omega(s) = \sum_{n=1}^{\infty} \left(\widetilde{F}_\sigma(s)\right)^{n-1} \widetilde{F}_{\sigma'}(s) q(1-q)^{n-1} = \frac{q\widetilde{F}_{\sigma'}(s)}{1-(1-q)\widetilde{F}_\sigma(s)}$$

Since $E[\omega] = -\left.\frac{d\widetilde{F}_\omega(s)}{ds}\right|_{s=0}$, it follows that

$$E[\omega] = E[\sigma'] + \frac{1-q}{q} E[\sigma].$$

Variable β has an unknown distribution. Therefore variable σ also has an unknown distribution. Using stochastic ordering (Stoyan, 1983), we get the following estimation

$$E[\sigma'] + \frac{1-q}{q}\left(E[\min(\chi,\varphi)] + \left(E[\gamma]\Pr(B) + \left(E[\delta] + E[\alpha]\right)\Pr(\overline{B})\right)\Pr(\chi \le \varphi)\right) + E[\psi]\Pr(\varphi < \chi) \le E[\omega] \le$$

$$\le E[\sigma'] + \frac{1-q}{q}\left(E[\min(\chi,\varphi)] + \left((E[\delta] + E[\gamma]\right)\Pr(B) + \left(E[\delta] + E[\alpha]\right)\Pr(\overline{B})\right)\Pr(\chi \le \varphi)\right) + E[\psi]\Pr(\varphi < \chi),$$

where

$$E[\sigma'] = E[\min(\chi,\varphi)] + E[\delta]\Pr(\chi \le \varphi) .$$

By U_n denote the moment of the n-th failure of the power safety subsystem. By V_n denote the moment of the n-th repair of the power safety subsystem. Then the corresponding accident takes place when

$$U_n \le \chi < V_n - \delta,$$
$$\delta \le V_n - U_n$$

or when

$$V_{n-1} + T^p \le \chi < V_{n-1} + (T^p + \theta^p) - \delta;$$
$$V_{n-1} + (T^p + \theta^p) + T^p \le \chi < V_{n-1} + 2(T^p + \theta^p) - \delta;$$
$$\ldots$$
$$V_{n-1} + \left(\left\langle \frac{\xi_n}{T^p + \theta^p} \right\rangle - 1\right)(T^p + \theta^p) + T^p \le \chi < V_{n-1} + \left\langle \frac{\xi_n}{T^p + \theta^p} \right\rangle (T^p + \theta^p) - \delta;$$
$$\delta < \theta^p$$

where $<x>$ is an integer part of x.

Since the operation process of the safety system is an alternating renewal process, it follows that

$$U_n = \sum_{i=1}^{n} \xi_i^p + \sum_{i=1}^{n-1}\left((T^p + \theta^p) - \left\{ \frac{\xi_i^p}{T^p + \theta^p} \right\} (T^p + \theta^p) \right) + \sum_{i=1}^{n-1} \eta_i^p ,$$

$$V_n = \sum_{i=1}^{n} \xi_i^p + \sum_{i=1}^{n} \left((T^p + \theta^p) - \left\{ \frac{\xi_i^p}{T^p + \theta^p} \right\} (T^p + \theta^p) \right) + \sum_{i=1}^{n} \eta_i^p ,$$

where $\{x\}$ is a fractional part of x. Taking into account the condition of accident, we obtain:

$$\Pr(\overline{B}) = \sum_{n=1}^{\infty} \int_{0}^{\infty} \left(E \left[J_{U_n \le x < V_n - \delta} J_{\Delta_n > 0} + \sum_{i=1}^{\left\langle \frac{\xi_n^p}{T^p + \theta^p} \right\rangle} J_{V_{n-1} + (i-1)(T^p + \theta^p) + T^p \le x < V_{n-1} + i(T^p + \theta^p) - \delta} J_{\zeta > 0} \right] \right) dF_{\chi}(x)$$

where

$$\varDelta_n = \eta_n + \varepsilon_n - \delta,$$

$$\varepsilon_n = T^p + \theta^p - \left\{ \frac{\xi_n^p}{T^p + \theta^p} \right\} (T^p + \theta^p),$$

$$\zeta = \theta^p - \delta$$

It now follows that

$$\Pr(\overline{B}) = \sum_{n=1}^{\infty} \int_{0}^{\infty} \Pr\big(\min(U_n, (U_n + \Delta_n)) \le x\big) dF_{\chi}(x) - \sum_{n=1}^{\infty} \int_{0}^{\infty} \Pr\big(U_n + \Delta_n \le x\big) dF_{\chi}(x) +$$

$$+ \sum_{n=1}^{\infty} \int_{0}^{\infty} E \left[\sum_{i=1}^{\left\langle \frac{\xi_n^p}{T^p + \theta^p} \right\rangle} \Pr\big(\min((V_{n-1} + i(T^p + \theta^p) - \theta^p), (V_{n-1} + i(T^p + \theta^p) - \theta^p + \zeta)) \le x\big) \right] dF_{\chi}(x) -$$

$$- \sum_{n=1}^{\infty} \int_{0}^{\infty} E \left[\sum_{i=1}^{\left\langle \frac{\xi_n^p}{T^p + \theta^p} \right\rangle} \Pr\big(V_{n-1} + i(T^p + \theta^p) - \theta^p + \zeta \le x\big) \right] dF_{\chi}(x) = q_1 + q_2.$$

Note that

$$q_1 = \sum_{n=1}^{\infty} \int_{0}^{\infty} \int_{0}^{\infty} \Big((F_{\xi^p} * (F_{\xi^p} * F_{\eta^p} * F_{\varepsilon})^{*(n-1)})(x) - (F_{\xi^p} * (F_{\xi^p} * F_{\eta^p} * F_{\varepsilon})^{*(n-1)})(x - y) \Big) dF_{\Delta}(y) dF_{\chi}(x),$$

where $F_{\xi^p} * F_{\eta^p}(t) = \int_{0}^{t} F_{\xi^p}(t - z) dF_{\eta^p}(z)$ and $F^{*(2)}(t) = F * F(t)$. Equivalently

$$q_1 = \int_{0}^{\infty} \int_{0}^{\infty} (H_0(x) - H_0(x - y)) dF_{\Delta}(y) dF_{\chi}(x)$$

where $H_0(x) = \sum_{n=1}^{\infty} F_{\xi^p} * (F_{\xi^p} * F_{\eta^p} * F_{\varepsilon})^{*(n-1)}(x)$. Furthermore

$$q_2 = \sum_{n=1}^{\infty} \int_{0}^{\infty} \int_{0}^{\infty} E \left[\sum_{i=1}^{\left\langle \frac{\xi_n^p}{T^p + \theta^p} \right\rangle} \Big(\Pr\big(V_{n-1} + i(T^p + \theta^p) - \theta^p \le x\big) - \Pr\big(V_{n-1} + i(T^p + \theta^p) - \theta^p \le x - y\big) \Big) \right] dF_{\zeta}(y) dF_{\chi}(x).$$

In other notation,

$$q_2 = \int_{0}^{\infty} \int_{0}^{\infty} E \left[\sum_{i=1}^{\left\langle \frac{\xi^p}{T^p + \theta^p} \right\rangle} (H_{0i}(x) - H_{0i}(x - y)) \right] dF_{\zeta}(y) dF_{\chi}(x),$$

where $H_{0i}(x)=\sum_{n=1}^{\infty}F_{2i,n}(x)$ and $F_{2i,n}(x)=\Pr(V_{n-1}+i(T^p+\theta^p)-\theta^p\le x)$. The application of renewal limit theorems (Rausand & Høyland 2004) yields

$$q_1\approx\frac{1}{E\left[\eta^p\right]+(T^p+\theta^p)+(T^p+\theta^p)E\left[\left\langle\frac{\xi^p}{T^p+\theta^p}\right\rangle\right]}\int_0^{\infty}ydF_{\Delta}(y),$$

$$q_2\approx\frac{E\left[\left\langle\frac{\xi^p}{T^p+\theta^p}\right\rangle\right]}{E\left[\eta^p\right]+(T^p+\theta^p)+(T^p+\theta^p)E\left[\left\langle\frac{\xi^p}{T^p+\theta^p}\right\rangle\right]}\int_0^{\infty}ydF_{\zeta}(y).$$

Finally,

$$\Pr(\overline{B})\approx\frac{1}{E[\eta^p]+(T^p+\theta^p)+(T^p+\theta^p)E\left[\left\langle\frac{\xi^p}{T^p+\theta^p}\right\rangle\right]}\left(\int_0^{\infty}ydF_{\Delta}(y)+E\left[\left\langle\frac{\xi^p}{T^p+\theta^p}\right\rangle\right]\int_0^{\infty}ydF_{\zeta}(y)\right).$$

The Monte-Carlo method can be used to estimate $\int_0^{\infty}ydF_{\Delta}(y)$ and $\int_0^{\infty}ydF_{\zeta}(y)$:

$$\Pr(\overline{B})\approx\frac{1}{E\left[\eta^p\right]+(T^p+\theta^p)+(T^p+\theta^p)E\left[\left\langle\frac{\xi^p}{T^p+\theta^p}\right\rangle\right]}\times$$
$$\times\left(E\left[\max\left(\eta^p+T^p+\theta^p-\left\{\frac{\xi^p}{T^p+\theta^p}\right\},0\right)\right]+E\left[\left\langle\frac{\xi^p}{T^p+\theta^p}\right\rangle\right]E\left[\max\left(\theta^p-\delta,0\right)\right]\right).$$

Note that

$$\Pr(B)=1-\Pr(\overline{B}).$$

We obviously have

$$q=q^{pt}\Pr(\chi\le\varphi)+q^t\Pr(\chi>\varphi),$$

where q^{pt} is the probability of failure of both safety subsystems and q^t is the probability of failure of the temperature safety subsystem. Furthermore

$$q^{pt}=\Pr(\overline{B})q^t.$$

Using the same technique as earlier we obtain the following estimation of q^t

$$q^t\approx1-\frac{E\left[\xi^t\right]-\theta^tE\left[\left\langle\frac{\xi^t}{T^t+\theta^t}\right\rangle\right]}{E\left[\eta^t\right]+(T^t+\theta^t)+(T^t+\theta^t)E\left[\left\langle\frac{\xi^t}{T^t+\theta^t}\right\rangle\right]}.$$

Therefore we managed to estimate all variables necessary to evaluate mean time to accident. Though some of them should be evaluated numerically the required techniques are pretty much straightforward.

3 CONCLUSIONS

The proposed model permits to assess the reliability of one specific class of technological systems with time redundancy. In particular the suggested approach allows to evaluate the mean time to accident for the "safety system-protected object" complex. The proposed approach allows to