Intelligent Information Management, **2009, 1, 150-158**
doi:10.4236/iim.2009.13022 Published Online December 2009 (http://www.scirp.org/journal/iim)

Probabilistic Analysis of a Robot System with Redundant Safety Units and Common-Cause Failures

B. S. DHILLON, Zhijian LI
Department of Mechanical Engineering, University of Ottawa, Ontario, Canada
Email: *dhillon@eng.uottawa.ca*

Abstract: This paper presents reliability and availability analyses of a model representing a system having one robot and n-redundant safety units with common-cause failures. At least k safety units must function successfully for the robot system success. The robot and other failure rates and the partially failed system repair rates are assumed constant and the failed robot-safety system repair time is assumed arbitrarily distributed. Markov and supplementary variable methods were used to perform mathematical analysis of this model. Generalized expressions for state probabilities, system availabilities, reliability, mean time to failure, and variance of time to failure are developed. Plots of some resulting expressions are shown.

Keywords: robot, safety, availability, reliability, common-cause failures, failure, repair, redundancy

1. Introduction

Robots are complex and sophisticated machines. Past experiences indicate that robots can constitute a source of great danger to humans. For example, over the years, a number of serious accidents and other safety-related problems involving robots have occurred [1–10]. This indicates that safety issues are a prime concern in the design, installation, operation, and maintenance of robots.

Needless to say, a robot not only has to be reliable, but also safe. Thus, the safety unit is an important element of the robot system. More specifically, a robot system is made up of a robot and its associated safety units. Therefore, in effective robot reliability analyses, the coupling between reliability and safety must be studied and the occurrence of common-cause failures considered. A common-cause failure may be defined as any instance where multiple units or elements fail due to a single cause [11].

The concept of redundancy is widely used to increase the safety and reliability of a system. It can also be applied to the robot system, in particular to safety units. Thus, this paper presents reliability and availability analyses of a robot system having one robot and n-redundant safety units subject to common-cause failures. At least k safety units must function normally for the successful operation of the robot system. The block diagram of this robot-safety system is shown in Figure 1, and its corresponding state space diagram is given in Figure 2. The numerals and letters n and k in the boxes and ellipse of Figure 2 denote system states.

At time t=0, the robot and all n safety units start operating. The robot-safety system can fail either due to the failure of the robot itself, the malfunction of the (n-k+1)th safety unit, or the occurrence of a common-cause failure. Nonetheless, the robot-safety system will function successfully until at least k safety units and the robot are operating normally. The system goes through (n-k+1) distinct operating states. A common-cause failure can occur only if at least k safety units and the robot are functioning successfully. The robot-safety system has a total of (n-k+4) distinct states. It means the array of numerals representing system states may be discontinuous. For example, for a 2-out-of-4 safety units, the array of numerals representing system states are 0, 1, 2, 5, 6, 7. More specifically, in this array of numerals, numerals 3 and 4 are missing. The degraded or fully failed robot-safety system is repaired.

The following assumptions are associated with this model:

1) The robot-safety system is composed of one robot and n identical safety units.

2) The robot and redundant safety units are operating simultaneously.

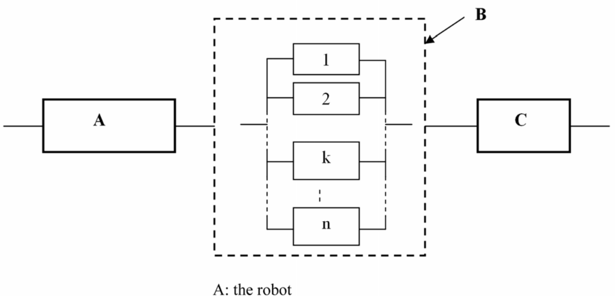
3) All failures are statistically independent.

4) All failure rates and the partially failed system repair rates are constant.

5) The failed robot-safety system repair rates can be constant or non-constant.

6) The repaired robot or a safety unit is as good as new.

7) The overall robot-safety system fails when the active



A: the robot
B: k-out-of-n safety units
C: common-cause failures

Figure 1. The block diagram of the robot-safety system with common-cause failures

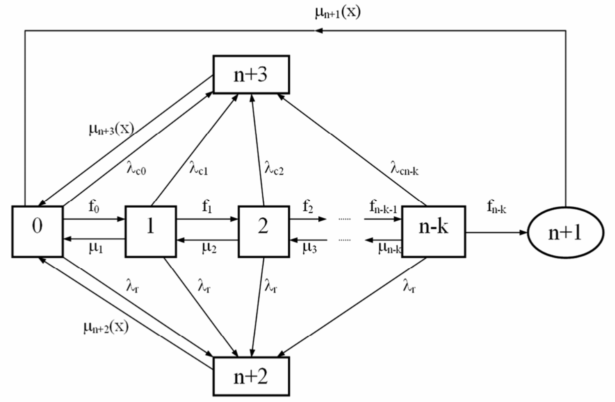


Figure 2. The state space diagram of the robot-safety system with common-cause failures. The numerals and letters n and k in squares, rectangles, and ellipse denote system states and f_i=(n-i)λ_s, for i=0, 1, 2,…, n-k

robot fails, a common-cause failure occurs, or the (n-k+1)th safety unit fails.

2. Notation

The following symbols are associated with the model:

1) ith state of the overall robot-safety system: for i=0, means robot and all n safety units are in perfect working condition; for i=1, means robot and n-1 safety units operating normally while one safety unit has failed; for i=m (where m=2,3,…,n-k-1 and k=1,2,…,n-1), means the robot and n-m safety units operating normally while m safety units have failed; for i=n-k (where k=1,2,…,n), means robot and k safety units operating normally while n-k safety units have failed.

2) jth state of the failed robot-safety system: for j=n+1, means robot-safety system failed due to the malfunction of the (n-k+1)th safety unit ; for j=n+2, means robot-safety system failed due to the failure of the robot itself; for j=n+3, means robot-safety system failed due to a common-cause failure.

3) time

λ_s: Constant failure rate of the safety unit.

λ_r: Constant failure rate of the robot.

λ_{ci}: Constant common-cause failure rate of the robot-safety system in state i; for i = 0,1,2,…,n-k.

μ_i: Constant repair rate of the safety unit in state i; for i = 1,2,…,n-k.

Δx: Finite repair time interval.

$\mu_j(x)$: Time-dependent repair rate when the failed robot-safety system is in state j and has an elapsed repair time of x; for j = n+1, n+2, n+3.

$p_j(x,t)\Delta x$: The probability that at time t, the failed robot-safety system is in state j and the elapsed repair time lies in the interval [x, x+Δx]; for j = n+1, n+2, n+3.

Pdf: Probability density function.

$z_j(x)$: pdf of repair time when the failed robot-safety system is in state j and has an elapsed time of x; for j = n+1, n+2, n+3.

$P_i(t)$: Probability that the robot-safety system is in state i at time t; for i = 0,1,…,n-k.

$P_j(t)$: Probability that the robot-safety system is in state j at time t; for j = n+1, n+2, n+3.

P_i: Steady-state probability that the robot-safety system is in state i; for i = 0,1,…,n-k.

P_j: Steady-state probability that the robot-safety system is in state j; for j = n+1, n+2, n+3.

s: Laplace transform variable.

$P_i(s)$: Laplace transform of the probability that the robot-safety system is in state i; for i = 0,1,…,n-k.

$P_j(s)$: Laplace transform of the probability that the robot-safety system is in state j; for j = n+1, n+2, n+3.

$AV_{rs}(s)$: Laplace transform of the robot-safety system availability when the robot working with at least k safety units.

$AV_{rs}(t)$: Robot-safety system time-dependent availability when the robot working with at least k safety units.

$SSAV_{rs}$: Robot-safety system steady state availability when the robot working with at least k safety units.

$R_{rs}(s)$: Laplace transform of the robot-safety system reliability when the robot working with at least k safety units.

$R_{rs}(t)$: Robot-safety system reliability when the robot working with at least k safety units.

$MTTF_{rs}$: Robot-safety system mean time to failure when the robot working with at least k safety units.

σ^2: Robot-safety system variance of time to failure when the robot working with at least k safety units.

3. Analysis

Using the supplementary method [12–13], the system of Equations associated with Figure 2 can be expressed as follows:

$$\frac{dP_0(t)}{dt}+a_0P_0(t)=\mu_1P_1(t)+\sum_{j=n+1}^{n+3}\int_0^{\infty}P_j(x,t)\mu_j(x)dx \quad (1)$$

$$\frac{dP_i(t)}{dt}+a_iP_i(t)=(n-i+1)\lambda_sP_{i-1}(t)+\mu_{i+1}P_{i+1}(t) \quad (for \quad i=1,2,...,n-k-1) \tag{2}$$

$$\frac{dP_{n-k}(t)}{dt}+a_{n-k}P_{n-k}(t)=(k+1)\lambda_sP_{n-k}(t) \tag{3}$$

$$\frac{\partial P_j(x,t)}{\partial t}+\frac{\partial P_j(x,t)}{\partial x}+\mu_j(x)P_j(x,t)=0 \quad (for \quad j=n+1,n+2,n+3) \tag{4}$$

where

$$a_0=n\lambda_s+\lambda_r+\lambda_{c0}$$

$$a_i=(n-i)\lambda_s+\lambda_r+\lambda_{ci}+\mu_i \quad (for \quad i=1,2,...,n-k-1)$$

$$a_{n-k}=k\lambda_s+\lambda_r+\lambda_{cn-k}+\mu_{n-k}$$

The associated boundary conditions are as follows:

$$P_{n+1}(0,t)=k\lambda_sP_{n-k}(t) \tag{5}$$

$$P_{n+2}(0,t)=\lambda_r\sum_{i=0}^{n-k}P_i(t) \tag{6}$$

$$P_{n+3}(0,t)=\sum_{i=0}^{n-k}\lambda_{ci}P_i(t) \tag{7}$$

At time t=0, P$_0$(0)=1, and all other initial condition state probabilities are equal to zero.

3.1. Time Dependant Availability Analysis

Using the Laplace Transform technique and the initial conditions in Equations (1) – (7), we get

$$(s+a_0)P_0(s)=1+\mu_1P_1(s)+\sum_{j=n+1}^{n+3}\int_0^\infty P_j(x,s)\mu_j(x)dx \tag{8}$$

$$(s+a_i)P_i(s)=(n-i+1)\lambda_sP_{i-1}(s)+\mu_{i+1}P_{i+1}(s) \quad (for \quad i=1,2,...,n-k-1) \tag{9}$$

$$(s+a_{n-k})P_{n-k}(s)=(k+1)\lambda_sP_{n-k-1}(s) \tag{10}$$

$$sP_j(x,s)+\frac{\partial P_j(x,s)}{\partial x}+\mu_j(x)P_j(x,s)=0 \tag{11}$$

$$(for \quad j=n+1,n+2,n+3)$$

$$P_{n+1}(0,s)=k\lambda_sP_{n-k}(s) \tag{12}$$

$$P_{n+2}(0,s)=\lambda_r\sum_{i=0}^{n-k}P_i(s) \tag{13}$$

$$P_{n+3}(0,s)=\sum_{i=0}^{n-k}\lambda_{ci}P_i(s) \tag{14}$$

Solving differential Equation (11), we get the following expression:

$$P_j(x,s)=P_j(0,s)e^{-sx}\exp[-\int_0^x\mu_j(\delta)d\delta] \tag{15}$$

$$(for \quad j=n+1,n+2,n+3)$$

Since

$$P_j(s)=\int_0^\infty P_j(x,s)dx \qquad (for \quad j=n+1,n+2,n+3) \tag{16}$$

and together with Equation (15), we get

$$P_j(s)=P_j(0,s)\frac{1-Z_j(s)}{s} \quad (for \quad j=n+1,n+2,n+3) \tag{17}$$

where

$$\frac{1-Z_j(s)}{s}=P_j(0,s)\int_0^\infty e^{-sx}\exp[-\int_0^x\mu_j(\delta)d\delta]dx \tag{18}$$

$$(for \quad j=n+1,n+2,n+3)$$

$$Z_j(s)=\int_0^\infty e^{-sx}z_j(x)dx \quad (for \quad j=n+1,n+2,n+3) \tag{19}$$

$$z_j(x)=\exp[-\int_0^x\mu_j(\delta)d\delta]\mu_j(x)$$

where z$_j$(x) is the failed robot-safety system repair time probability density function.

Using Equations (9) – (10), and (17), together with

$$\sum_{i=0}^{n}P_i(s)+\sum_{j=n+1}^{n+4}P_j(s)=\frac{1}{s} \tag{20}$$

we get the following Laplace Transforms of state probability solutions:

$$P_i(s)=\frac{N_i(s)}{M_0(s)} \qquad (for \quad i=0,1,...,n-k) \tag{21}$$

$$P_j(s)=\frac{N_j(s)}{M_0(s)} \qquad (for \quad j=n+1,n+2,n+3) \tag{22}$$

where

$$k_1=\frac{n\lambda_s\mu_1}{s+a_1-k_2}$$

$$k_i=\frac{(n-i+1)\lambda_s\mu_i}{(s+a_i)-k_{i+1}} \qquad (for \quad i=1,2,...,n-k-1)$$

$$k_{n-k}=\frac{(k+1)\lambda_s\mu_{n-k}}{s+a_{n-k}}$$

$$a_{n+1}=k\lambda_s\prod_{i=1}^{n-k}\frac{k_i}{\mu_i}$$

$$a_{n+2} = \lambda_r[1 + \sum_{m=1}^{n-k}(\prod_{i=1}^{m}\frac{k_i}{\mu_i})]$$

$$a_{n+3} = \lambda_{c0} + \sum_{m=1}^{n-k}(\lambda_{cm}\prod_{i=1}^{m}\frac{k_i}{\mu_i})$$

$$M_0(s) = s(1 + \sum_{i=1}^{n-k}\prod_{m=1}^{i}\frac{k_m}{\mu_m} + \sum_{j=n+1}^{n+3} a_j\frac{1-Z_j(s)}{s}) \quad (23)$$

$$N_0(s) = 1 \quad (24)$$

$$N_i(s) = \prod_{m=1}^{i}\frac{k_m}{\mu_m}N_0(s) \qquad (for \quad i = 0,1,2,...,n-k) \quad (25)$$

$$N_j(s) = \frac{a_j[1-Z_j(s)]}{s}(for \quad j = n+1, n+2, n+3) \quad (26)$$

Thus, the Laplace transform of the robot-safety system availability with at least k working safety units is

$$AV_{rs}(s) = \sum_{i=0}^{n-k}P_i(s) = \frac{\sum_{i=0}^{n-k}N_i(s)}{M_0(s)} \quad (27)$$

Substituting the Laplace transform of $z_j(x)$ for different repair time distributions in Equation (27), and taking the inverse Laplace transform of the resulting equation, we can get the time-dependent robot-safety system availability, $AV_{rs}(t)$.

3.2. Steady State Availability Analysis

As time t approaches infinity, state probabilities reach the steady state. Thus, Equations (1) – (7) reduce to Equations (28) – (34), respectively.

$$a_0P_0 = \mu_1P_1 + \sum_{j=n+1}^{n+3}\int_0^{\infty}P_j(x)\mu_j(x)dx \quad (28)$$

$$a_iP_i = (n-i+1)\lambda_sP_{i-1} + \mu_{i+1}P_{i+1} \qquad (for \quad i = 1,2,...,n-k-1) \quad (29)$$

$$a_{n-k}P_{n-k} = k\lambda_sP_{n-k} \quad (30)$$

$$\frac{dP_j(x)}{dx} + \mu_j(x)P_j(x) = 0 \qquad (for \quad j = n+1, n+2, n+3) \quad (31)$$

$$P_{n+1}(0) = k\lambda_sP_{n-k} \quad (32)$$

$$P_{n+2}(0) = \lambda_r\sum_{i=0}^{n-k}P_i \quad (33)$$

$$P_{n+3}(0) = \sum_{i=0}^{n-k}\lambda_{ci}P_i \quad (34)$$

Solving Equation (31), we get

$$P_j(x) = P_j(0)\exp[-\int_0^x\mu_j(\delta)d\delta] \qquad (for \quad j = n+1, n+2, n+3) \quad (35)$$

The steady state condition of the probability, P_j, that due to a failure the robot-safety system is under repair, is

$$P_j = \int_0^{\infty}P_j(x)dx \qquad (for \quad j = n+1, n+2, n+3) \quad (36)$$

Substituting Equation (35) into Equation (36), yields

$$P_j = P_j(0)E_j[x] \qquad (for \quad j = n+1, n+2, n+3) \quad (37)$$

where

$$E_j(x) = \int_0^{\infty}\exp[-\int_0^x\mu_j(\delta)d\delta]dx = \int_0^{\infty}xz_j(x)dx \quad (38)$$

which is the mean time to robot-safety system repair when the failed robot-safety system is in state j and has an elapsed repair time of x.

Substituting Equations (32) – (34) into Equation (37), we get:

$$P_{n+1} = k\lambda_sP_{n-k}E_{n+1}[x] \quad (39)$$

$$P_{n+2} = \lambda_r\sum_{i=0}^{n-k}P_iE_{n+2}[x] \quad (40)$$

$$P_{n+3} = \sum_{i=0}^{n-k}\lambda_{ci}P_iE_{n+3}[x] \quad (41)$$

Solving Equations (29), (30), and (39) - (41), together with

$$\sum_{i=0}^{n}P_i + \sum_{j=n+1}^{n+4}P_j = 1 \quad (42)$$

yield the following steady state probabilities:

$$P_0 = (L + \sum_{j=n+1}^{n+3}L_jE_j[x])^{-1} = \frac{1}{G} \quad (43)$$

$$P_i = \frac{L_i}{\mu_i}P_{i-1} = \prod_{m=1}^{i}\frac{L_m}{\mu_m}P_0 \quad (for \quad i = 1,2,...,n-k-1) \quad (44)$$

$$P_{n-k} = \frac{L_{n-k}}{\mu_{n-k}}P_{n-k-1} = \prod_{i=1}^{n-k}\frac{L_i}{\mu_i}P_0 \quad (45)$$

$$P_j = L_j E_j[x] P_0 \qquad (for \quad j = n+1, n+2, n+3) \quad (46)$$

where

$$L = 1 + \sum_{m=1}^{n-k} \prod_{i=1}^{m} \frac{L_i}{\mu_i}$$

$$L_i = \frac{(n-i+1)\lambda_s \mu_i}{a_i - L_{i+1}} \qquad (for \quad i = 1, 2, ..., n-k-1)$$

$$L_{n-k} = \frac{(k+1)\lambda_s \mu_{n-k}}{a_{n-k}}$$

$$L_{n+1} = k\lambda_s \prod_{i=1}^{n-k} \frac{L_i}{\mu_i}$$

$$L_{n+2} = \lambda_r (1 + \sum_{m=1}^{n-k} \prod_{i=1}^{m} \frac{L_i}{\mu_i})$$

$$L_{n+3} = \lambda_{c0} + \sum_{m=1}^{n-k} \lambda_{cm} \prod_{i=1}^{m} \frac{L_i}{\mu_i}$$

$$G = L + \sum_{j=n+1}^{n+3} L_j E_j[x] \quad (47)$$

The steady state availability of the robot-safety system with at least k working safety units is

$$SSAV_{rs} = \sum_{i=0}^{n-k} P_i = \frac{L}{G} \quad (48)$$

For different failed system repair time distributions, the values of G are obtained as follows:

1). When the failed robot-safety system repair time x is exponentially distributed, then the probability density function of the repair time is

$$z_j(x) = \mu_j e^{-\mu_j x} \qquad (\mu_j > 0, \quad j = n+1, n+2, n+3) \quad (49)$$

where x is the repair time, and μ_j is the constant repair rate of state j. Thus, the mean time to robot-safety system repair, $E_j[x]$, for the exponential distribution is

$$E_j[x] = \int_0^\infty x z_j(x) dx = \frac{1}{\mu_j} \quad (for \quad j = n+1, n+2, n+3) \quad (50)$$

Substituting Equation (50) into Equation (47), we get

$$G = G_e = L + \sum_{j=n+1}^{n+3} (L_j \frac{1}{\mu_j}) \quad (51)$$

2). When the failed robot-safety system repair time x is gamma distributed, then the probability density function of the repair time is

$$z_j(x) = \frac{\mu_j (\mu_j x)^{\beta-1} e^{-\mu_j x}}{\Gamma(\beta)} \quad (\beta > 0, j = n+1, n+2, n+3) \quad (52)$$

where x is the repair time, Γ(β) is the gamma function, and β and μ_j are the shape and scale parameters, respectively. Thus, the mean time to robot-safety system repair, $E_j[x]$, for the gamma distribution is

$$E_j[x] = \int_0^\infty x z_j(x) dx = \frac{\beta}{\mu_j} \quad (for \quad j = n+1, n+2, n+3) \quad (53)$$

Substituting Equation (53) into Equation (47), we get

$$G = G_g = L + \sum_{j=n+1}^{n+3} (L_j \frac{\beta}{\mu_j}) \quad (54)$$

3). When the failed robot-safety system repair time x is Weibull distributed, then the probability density function of the repair time is expressed by

$$z_j(x) = \mu_j \beta x^{\beta-1} e^{-(\mu_j x)^\beta} \quad (\beta > 0, j = n+1, n+2, n+3) \quad (55)$$

where x is the repair time, and β and μ_j are the shape and scale parameters of the Weibull distribution, respectively. Thus, the mean time to robot-safety system repair, $E_j[x]$, for the Weibull distribution is given by

$$E_j[x] = \int_0^\infty x z_j(x) dx = (\frac{1}{\mu_j})^{1/\beta} \frac{1}{\beta} \Gamma(\frac{1}{\beta}) \quad (56)$$

$$(for \quad j = n+1, n+2, n+3)$$

Substituting Equation (56) into Equation (47), we get

$$G = G_w = L + \sum_{j=n+1}^{n+3} [L_j (\frac{1}{\mu_j})^{1/\beta} \frac{1}{\beta} \Gamma(\frac{1}{\beta})] \quad (57)$$

4). When the failed robot-safety system repair time x is Rayleigh distributed, then the probability density function of the Rayleigh distribution is expressed by

$$z_j(x) = \mu_j x e^{-\mu_j x^2/2} \quad (\mu_j > 0, j = n+1, n+2, n+3) \quad (58)$$

where x is the repair time, and μ_j is the scale parameter. Thus, the mean time to robot-safety system repair, $E_j[x]$, for the Rayleigh distribution is

$$E_j[x] = \int_0^\infty x z_j(x) dx = \sqrt{\frac{\pi}{4\mu_j}} \quad (59)$$

$$(for \quad j = n+1, n+2, n+3)$$

Substituting Equation (59) into Equation (47), we get

$$G = G_r = L + \sum_{j=n+1}^{n+3} (L_j \sqrt{\frac{\pi}{4\mu_j}}) \quad (60)$$

5). When the robot-safety system repair time x is lognormal distributed, then the probability density function of the repair time is

$$z_j(x) = \frac{1}{x\sigma_{y_j}\sqrt{2\pi}} e^{[\frac{-(\ln x - \mu_{y_j})^2}{2\sigma_{y_j}^2}]} \quad (61)$$

$$(for \quad j = n+1, n+2, n+3)$$

where x is the repair time, and lnx is the natural logarithms of x with a mean and variance μ and σ^2, respectively. The conditions on parameters are as follows:

$$\sigma_{y_j} = \ln\sqrt{1 + (\frac{\sigma_{x_j}}{\mu_{x_j}})^2} \ ,$$

$$\mu_{y_j} = \ln\sqrt{\frac{\mu_{x_j}^{\ 4}}{\mu_{x_j}^{\ 2} + \sigma_{x_j}^{\ 2}}} \quad (62)$$

$$(for \quad j = n+1, n+2, n+3)$$

Hence, the failed robot-safety system mean time to repair, $E_j[x]$, for the lognormal distribution is

$$E_j[x] = e^{(\mu_{y_j} + \frac{\sigma_{y_j}{}^2}{2})} \quad (for \quad j = n+1, n+2, n+3) \quad (63)$$

Substituting Equation (63) into Equation (47), we get

$$G = G_l = L + \sum_{j=n+1}^{n+3} [L_j e^{(\mu_{y_j} + \frac{\sigma_{y_j}{}^2}{2})}] \quad (64)$$

3.3. Robot-Safety System Reliability, MTTF, and Variance of time to failure

Setting $\mu_{n+1}(x)=\mu_{n+2}(x)=\mu_{n+3}(x)=0$ in Figure 2 and applying the Markov method, we get the following differential equations:

$$\frac{dP_0(t)}{dt} + a_0 P_0(t) = \mu_1 P_1(t) \quad (65)$$

$$\frac{dP_i(t)}{dt} + a_i P_i(t) = (n-i+1)\lambda_s P_{i-1}(t) + \mu_{i+1} P_{i+1}(t) \quad (66)$$

$$(for \quad i = 1, 2, ..., n-k-1)$$

$$\frac{dP_{n-k}(t)}{dt} + a_{n-k} P_{n-k}(t) = (k+1)\lambda_s P_{n-k-1}(t) \quad (67)$$

$$\frac{dP_{n+1}(t)}{dt} = k\lambda_s P_{n-k}(t) \quad (68)$$

$$\frac{dP_{n+2}(t)}{dt} = \lambda_r \sum_{i=0}^{n-k} P_i(t) \quad (69)$$

$$\frac{dP_{n+3}(t)}{dt} = \sum_{i=0}^{n-k} \lambda_{ci} P_i(t) \quad (70)$$

At time t=0, $P_0(0)=1$, and all other initial condition state probabilities are equal to zero. Taking the Laplace transforms of Equations (65) – (70) and solving the resulting set of equations, we obtain the following Laplace transforms of state probabilities:

$$P_0(s) = [s(1 + \sum_{i=1}^{n-k} \prod_{m=1}^{i} \frac{k_m}{\mu_m} + \sum_{j=n+1}^{n+3} \frac{a_j}{s})]^{-1} \quad (71)$$

$$P_i(s) = \prod_{m=1}^{i} \frac{k_m}{\mu_m} P_0(s) \qquad (for \quad i = 1, 2, ..., n-k) \quad (72)$$

$$P_j(s) = \frac{a_j}{s} P_0(s) \qquad (for \quad j = n+1, n+2, n+3) \quad (73)$$

The Laplace transform of the robot-safety system reliability with at least k working safety units is

$$R_{rs}(s) = \sum_{i=0}^{n-k} P_i(s) = (1 + \sum_{m=1}^{n-k} \prod_{i=1}^{m} \frac{k_i}{\mu_i}) P_0(s) \quad (74)$$

Using Equation (74), the robot-safety system mean time to the failure is obtained as follows [14]:

$$MTTF_{rs} = \lim_{s \to 0} R_{rs}(s) = \frac{1 + \sum_{m=1}^{n-k} \prod_{i=1}^{m} \frac{L_i}{\mu_i}}{\sum_{j=n+1}^{n+3} L_j} \quad (75)$$

The time-dependant robot-safety system reliability, $R_{rs}(t)$, can be obtained by taking the inverse Laplace transform of Equation (74).

The robot-safety system variance of time to failure is expressed by

$$\sigma^2 = -2 \lim_{s \to 0} R_{rs}'(s) - (MTTF_{rs})^2$$

$$= \frac{2(1 + \sum_{m=1}^{n-k} \prod_{i=1}^{m} \frac{L_i}{\mu_i})(1 + \sum_{m=1}^{n-k} \prod_{i=1}^{m} \frac{L_i}{\mu_i} + \sum_{j=n+1}^{n+3} a_{dj})}{(\sum_{j=n+1}^{n+3} L_j)^2} \quad (76)$$

$$- \frac{2\sum_{m=1}^{n-k} k_{dm}}{\sum_{j=n+1}^{n+3} L_j} - (MTTF_{rs})^2$$

where

$R_{rs}'(s)$ denotes the derivative of $R_{rs}(s)$ with respect to s.

$$k_{dm} = \lim_{s\to 0}\left(\prod_{i=1}^{m}\frac{k_i}{\mu_i}\right)' \qquad (for \quad m = 1,2,...,n-k)$$

$$a_{dj} = \lim_{s\to 0} a_j{}' \qquad (for \quad j = n+1, n+2, n+3)$$

$$a_{dn+1} = \lim_{s\to 0} a_{n+1}^{'} = k\lambda_s k_{dn-k}$$

$$a_{dn+2} = \lim_{s\to 0} a_{n+2}^{'} = \lambda_r \sum_{m=1}^{n-k} k_{dm}$$

$$a_{dn+3} = \lim_{s\to 0} a_{n+3}^{'} = \sum_{m=1}^{n-k} \lambda_{cm} k_{dm}$$

$(\prod_{i=1}^{m}\frac{k_i}{\mu_i})'$ denotes the derivative of $\prod_{i=1}^{m}\frac{k_i}{\mu_i}$ with respect to s.

a_j' denotes the derivative of a_j with respect to s.

The number of safety units incorporated within the robot-safety system is the matter of desired level of safety. More safety units we use, the better system safety, reliability, and MTTF we can achieve.

4. Special Case Model: (k=2, n=3)

For k=2 and n=3 in Figures 1 and 2, the model becomes for a system having one robot and three redundant safety units. However, at least two safety units must function successfully for the robot-safety system success. The corresponding system of Equations can be obtained from Equations (1) –(7) by setting k=2 and n=3. Furthermore, robot-safety system state probabilities [$P_i(t)$, $P_j(t)$, P_i, P_j], availabilities [$AV_{rs}(t)$, $SSAV_{rs}$], reliability [$R_{rs}(t)$], mean time to failure [$MTTF_{rs}$], and variance of time to failure [σ^2] for the special case model can also be obtained by inserting k=2 and n=3 into the corresponding generalized Equations.

4.1. Time Dependant Availability Plots for k=2 and n=3

Setting:

λ_s=0.0006, λ_r=0.0006, λ_{c0}=0.0002, λ_{c1} =0.0001,
μ_1=0.0009, μ_4=0.0011, μ_5=0.0012, μ_6=0.0006

in Equations (21) –(22) and (27), and for gamma distributed failed system repair times using Maple computer program [15], the time-dependant plots of robot-safety system state probabilities and availability are shown in Figures 3 and 4, respectively.

4.2. Steady State Availability Plots for k=2 and n=3

Setting:

λ_s=0.0006, λ_r=0.0006, λ_{c1} =0.0001,
μ_1=0.0009, μ_4=0.0011, μ_5=0.0012, μ_6=0.0006

in Equation (48), and for gamma and Weibull distributed failed system repair times using Maple computer program [15] plots for $SSAV_{rs}$ are shown in Figures 5 and 6, respectively.

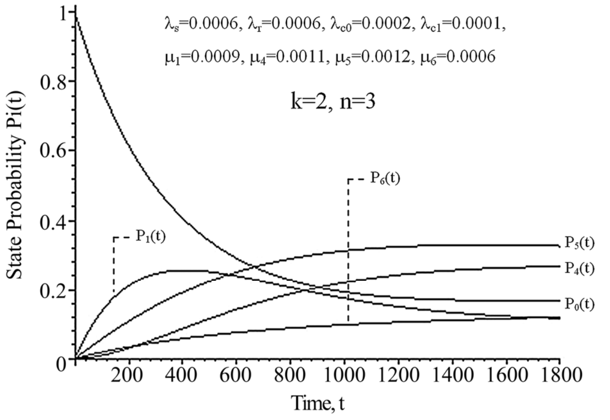


Figure 3. Time-dependent probability plots for a robot-safety system with gamma distributed (β=2) failed system repair times

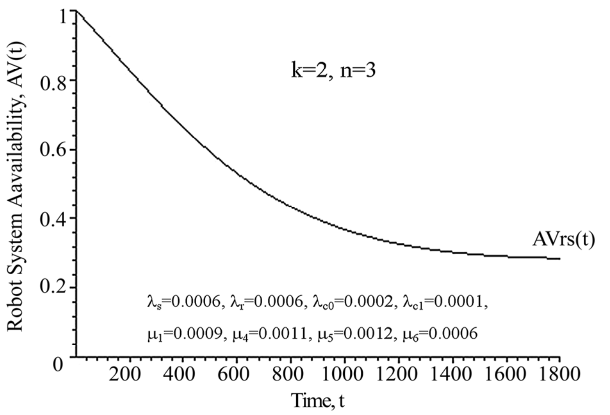


Figure 4. Time-dependent availability plots for a robot-safety system with gamma distributed (β=2) failed system repair times

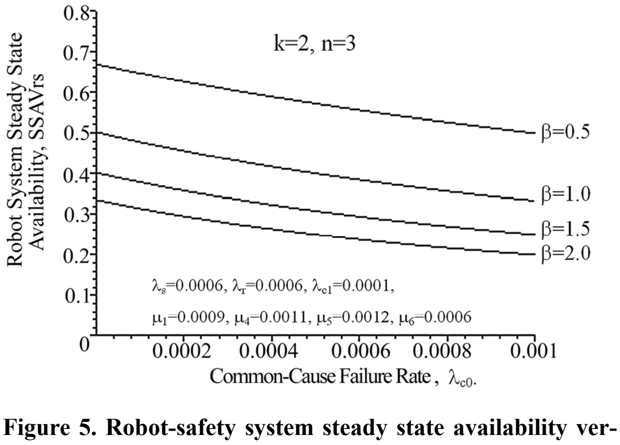


Figure 5. Robot-safety system steady state availability versus common-cause failure rate (λ_{c0}) plots with gamma distributed (β=0.5, 1, 1.5, 2) failed system repair times.

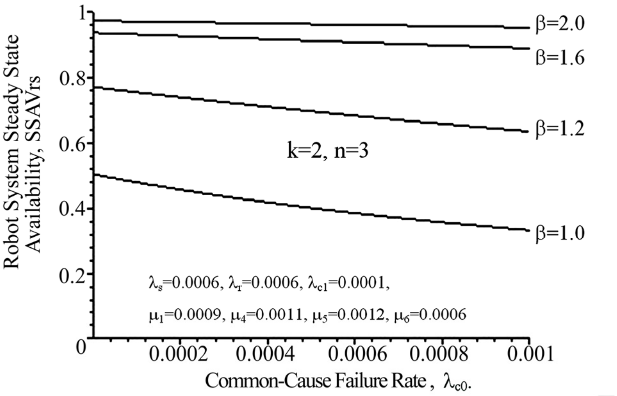


Figure 6. Robot-safety system steady state availability versus common-cause failure rate (λ_{c0}) plots with Weibull distributed (β=1.0, 1.2, 1.6, 2) failed system repair times.

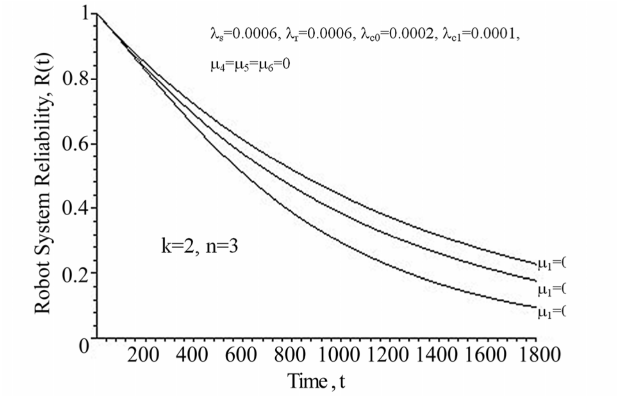


Figure 7. Reliability plots of the robot-safety system

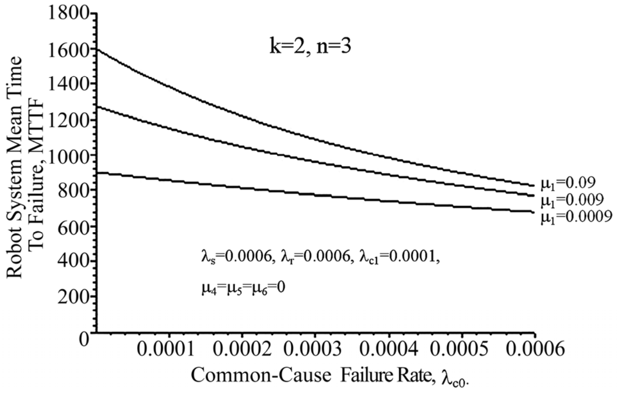


Figure 8. Mean time to failure plots of the robot-safety system as a function of common-cause failure rate (λ_{c0})

4.3. Reliability and MTTF Plots for k=2 and n=3

Setting:

λ_s=0.0006, λ_r=0.0006, (λ_{c0}=0.0002), λ_{c1} =0.0001,

$\mu_4 = \mu_5 = \mu_6 = 0$

in Equation (74) and using Maple computer program [15], the time-dependant reliability plots of the robot-safety system are shown in Figure 7. Similarly, plots of the robot-safety system mean time to failure, using Equation (75), as a function of common-cause failure rate (λ_{c0}), are shown in Figures 8.

5. Conclusions

This paper presented reliability analyses of a system having one robot and n-redundant safety units with common-cause failures. The results of the analysis indicate that redundant safety units help to improve robot system reliability and the occurrence of common-cause failures decrease the robot system reliability.

It is contended that the results of this study will be useful to management and engineering professionals to make various robot system reliability, availability, and safety-related decisions.

REFERENCES

[1] P. Nicolaisen, "Safety problems related to robots," Robotics, Vol. 3, pp. 205–211, 1987.

[2] M. Nagamachi, "Ten fatal accidents due to robots in Japan," in Ergonomics of Hybird Automated Systems I, eds. H. R. Karwowski and M. R. Parsaei, Elsevier, Amsterdam, pp. 391–396, 1988.

[3] B. S. Dhillon, "Robot reliability and safety," Springer-Verlag, New York, 1991.

[4] J. Fryman, "Future expectations in international robot safety," Robotic World, Vol. 24, No. 2, pp. 12–13, 2006.

[5] S. Neil, "Improving robot safety, managing automation," Vol. 18, No. 10, pp. 18–21, 2003.

[6] D. Kulic and E. Croft, "Pre-collision safety strategies for human-robot interaction," Autonomous Robots, Vol. 22, No. 2, pp. 149–164, 2007.

[7] E. J. Vanderperre and S. S. Makhanov, "Overall availability of a robot with internal safety device," Computers and Industrial Engineering, Vol. 56, No. 1, pp. 236–240, 2009.

[8] S. Haddadin, S. A. Albu-SuchaCurrency, and G. Hirzinger, "Requirements for safe robots: measurements, analysis and new insights," International Journal of Robotics, Vol. 28, No. 11–12, pp. 1507–1527, 2009.

[9] J. P. Merlet, "Interval analysis and reliability in robotics," International Journal of Reliability and Safety, Vol. 3, No. 1–3, pp. 104–130, 2009.

[10] B. S. Dhillon and S. Cheng, "Probabilistic analysis of a repairable robot-safety system composed of (n-1) standby robots, A Safety Unit, and a Switch," Journal of Quality in Maintenance Engineering, Vol. 14, No. 3, pp. 306–323, 2009.

[11] B. S. Dhillon, "Reliability engineering in systems design and operation," Van Nostrand Reinhold, New York, 1983.

[12] D. P. Gaver, "Time to failure and availability of paralleled

systems with repair," IEEE Transactions on Reliability, Vol. 12, pp. 30–38, 1963.

[13] R. C. Grag, "Dependability of a complex system having two types of components," IEEE Transactions on Reliability, Vol. 12, pp. 11–15, 1963.

[14] B. S. Dhillon, "Design reliability: fundamentals and applications," CRC Press, Boca Raton, Florida, 1999.

[15] R. M. Corless, "Essential MAPLE: An introduction to scientific programmers," Springer–Verlag, New York, 1995.