

The Effect of Failure Detection Equipment on System Availability

Seongryong Na^{a,1} · Sung-Hwan Bang^a

^aDepartment of Information and Statistics, Yonsei University

(Received November 30, 2012; Revised December 27, 2012; Accepted January 3, 2013)

Abstract

In this paper we study the effect of failure detection equipment(FDE)s on system availability. A new repair scheme is considered for the step of repairing FDE which becomes out of order in the course of repairing the main system(MS). We compute and compare the availability of MS.

Keywords: System availability, failure detection equipment, sequential repair, reliability, Markov process.

1. 서론

전체 시스템을 본연의 주요 기능을 담당하는 주시스템(main system; MS) 부분과 고장을 감지하고 수리 작업을 가능하게 하는 고장감지장치(failure detection equipment; FDE) 부분으로 구분하는 것이 논리적 혹은 물리적으로 가능하다. 원격감시와 제어가 이루어지는 공장자동화설비와 통신 및 전력 시스템 등에서 시스템 상태관리를 위한 감시 장치의 예를 쉽게 볼 수 있다. 이때 FDE의 고장은 MS의 고장 미발견과 수리 지체를 야기하며 결과적으로 시스템 가용도의 감소를 초래할 수 있다. 고장 발견 여부를 고려한 안전시스템에 대한 신뢰도 연구가 Zhang 등 (2003)와 Guo와 Yang (2007) 등에서 이루어졌고 최근에 Na (2011)가 FDE의 고장이 시스템 가용도에 미치는 효과를 마코프 모델링을 통하여 분석하였다.

기존의 MS-FDE 시스템 분석에서는 MS 수리 과정 중에는 FDE 고장이 발생하지 않는다는 가정을 통하여 신뢰도 분석을 하였다. 즉, MS가 고장이 나면 FDE는 수행해야 할 업무가 없으므로 전원을 꺼두면 고장이 발생하지 않는다는 것인데, 현실적으로 전원을 켜고 끄는데 비용이 많이 들거나 시간이 오래 걸리면 FDE를 꺼둘 수가 없어 고장이 발생하게 되고 따라서 기존의 가정이 맞지 않을 수도 있는 것이 현실이다. 본 연구에서는 이러한 가능성을 반영하여 MS 수리 중에도 FDE 고장이 발생할 수 있는 경우를 다룬다.

MS 수리 중 FDE에 고장이 발생한다면 어떠한 순서로 수리를 할 것인가가 중요하다. 현실에서는 시스템의 복잡도, 수리 종사자 수 등의 요소를 고려하여 시스템의 수리정책을 결정하게 된다. 이 논문에서는 고장난 순서에 따라 수리가 이루어지는 순차수리 정책의 시스템에 대한 마코프 모델링을 통하여 시스템 가용도를 산출하고 이를 기존의 결과와 비교한다.

이 논문의 구성은 다음과 같다. 2절에서 고장감지장치, MS-FDE 시스템, 신뢰도 분석을 위한 가정을 서술하고 최근 연구 결과를 정리한다. 이 논문에서 새롭게 다루는 수리정책과 이에 기초한 시스템 가용도 분석 결과는 3절에서 다루고자 한다.

¹Corresponding author: Professor, Department of Information and Statistics, Yonsei University, 1 Yonseidaegil, Wonju, Gangwon-Do 220-710, Korea. E-mail: nasr@yonsei.ac.kr

2. MS-FDE 시스템 신뢰도 분석

고장감지장치를 고려하지 않는 신뢰도 분석에서는 시스템 고장에 대하여 즉시 수리가 개시됨을 가정하는데 이는 고장 발견이 즉시 이루어지든지 또는 고장 발견에 소요되는 시간을 별도로 구분하지 않고 수리시간에 포함시켜 모형화 하는 것이다. 하부시스템 구성을 고려하지 않고 주시스템을 정상과 고장의 2개의 상태를 가지는 교대재생과정으로 표현할 때 기존의 분석은 다음을 가정한다.

- (A1) MS가 고장이 발생하기 전까지 정상상태에 머무는 시간은 평균이 λ_M^{-1} 인 지수분포를 따른다.
- (A2) 고장난 MS를 수리하고 정상상태로 복귀시키는데 소요되는 시간은 평균이 μ_M^{-1} 인 지수분포를 따른다.
- (A3) MS의 고장이 발견되는 즉시 수리가 개시된다.
- (A4) MS가 정상상태에 머무는 시간들과 수리소요시간들은 서로 독립이다.
- (A5) MS의 고장은 즉시 발견된다.

교대재생과정의 기본 성질을 이용하면 다음의 시스템 가용도 결과를 얻을 수 있다 (Ross, 1996).

$$Av = \frac{\lambda_M^{-1}}{\lambda_M^{-1} + \mu_M^{-1}} = \frac{\mu_M}{\lambda_M + \mu_M}. \quad (2.1)$$

이 결과는 일반적인 분포 가정에서도 성립하지만 마코프 확률과정 표현을 위해서 (A1), (A2)의 지수분포 가정이 필요하다.

시스템 고장을 발견하는 기능의 FDE를 포함하는 시스템의 신뢰도 분석을 위하여 (A5) 대신 다음을 가정한다.

- (B1) FDE가 고장전까지 정상적으로 기능하는 시간은 평균 λ_D^{-1} 의 지수분포를 따른다.
- (B2) 고장난 FDE를 고쳐서 정상상태로 복귀하기에 소요되는 시간은 평균이 μ_D^{-1} 인 지수분포를 따른다.
- (B3) FDE가 정상적으로 기능하는 시간들과 고장수리시간들은 서로 독립이다.
- (B4) FDE의 고장은 즉시 발견되며 수리개시된다.
- (B5) FDE가 정상상태일 때만 MS의 고장이 즉시 발견되고 FDE가 수리중이면 MS의 고장은 발견되지 않는다.
- (B6) MS의 고장을 탐지해서 수리를 하는 동안에는 FDE에 고장이 발생하지 않는다.

조건 (A1)–(A4), (B1)–(B6)을 가정하는 MS-FDE 시스템은 마코프 모델링이 가능하다. MS와 FDE의 상태를 각각 $X(t)$, $Y(t)$ 로 정의하고 정상 상태를 1, 고장 상태를 0으로 표현하면 $(X(t), Y(t))$ 는 표본공간 $S = \{(1, 1), (0, 1), (1, 0), (0, 0)\}$ 의 연속시간 마코프 확률과정이고 상태전이도는 Figure 2.1과 같이 표현 가능하다.

MS-FDE 시스템의 가용도는 평형 상태에서 MS가 주어진 기능을 정상적으로 수행할 확률로 정의된다. 다음은 조건 (A1)–(A4), (B1)–(B6)이 만족하는 시스템의 가용도이다 (Na, 2011).

$$Av = \frac{\mu_M}{\lambda_M + \mu_M} \cdot \frac{\mu_D(\lambda_M + \mu_M)(\lambda_M + \lambda_D + \mu_D)}{\mu_D(\lambda_M + \mu_M)(\lambda_M + \lambda_D + \mu_D) + \lambda_M\lambda_D\mu_M}. \quad (2.2)$$

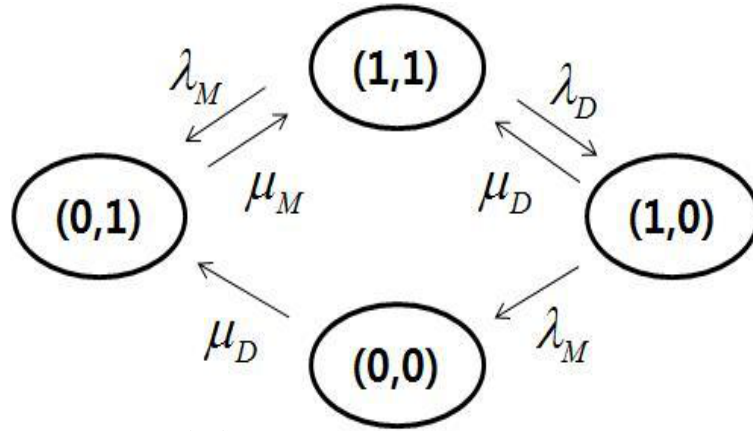


Figure 2.1. Transition diagram of MS-FDE system

앞의 식 (2.1), (2.2) 결과에서 FDE를 고려하는 MS-FDE 시스템의 가용도가 감소함을 알 수 있다. MS-FDE 시스템의 평균작동시간(mean time between failures; MTBF)은 $MTBF = \lambda_M^{-1}$ 으로 MS만을 고려하는 기존의 시스템과 변화가 없다. 반면에 평균수리시간(mean time to repair; MTTR)은

$$MTTR = \mu_M^{-1} + \mu_D^{-1} \cdot \frac{\lambda_D}{\lambda_M + \lambda_D + \mu_D} \tag{2.3}$$

식과 같은데 기존의 μ_M^{-1} 보다 증가함을 볼 수 있다. 시스템 가용도는 임의의 시간에 시스템이 주어진 기능을 수행할 확률인데 MS-FDE 시스템에서는 MS가 동작할 확률이다. 이 값은 MS가 작동하는 시간의 길이에 비례하기 마련인데 MS 작동시간의 평균에 해당하는 MTBF에 비례한다. 반면 고장수리시간이 길어지면 가용도는 감소하며 MS 고장수리 시간의 평균에 해당하는 MTTR에 반비례한다. 시스템 가용도가 높다는 것은 시스템이 항상 동작하고 있을 가능성이 높다는 것을 의미한다. 신뢰성 측면에서 가용도가 높은 시스템은 더 신뢰할 수 있는 시스템으로 해석되며 시스템 가용도는 수리가능 시스템의 신뢰도를 측정하는 가장 중요한 척도의 하나이다. 자세한 내용은 Na (2011)를 참고할 수 있다.

3. 순차수리 정책과 시스템 신뢰도 분석

수리가능 시스템의 고장을 감지해서 수리 개시를 가능하게 하는 고장감지장치를 고려한 시스템 신뢰도 산출에서 지금까지는 주시스템을 수리하는 과정에서는 고장감지장치에서 고장이 발생하지 않는다는 가정을 통하여 신뢰도 분석을 하였다. 즉, MS가 고장이 나면 FDE는 수행해야 할 업무가 없으므로 전원을 꺼두면 고장이 발생하지 않는다는 조건이 맞게 되나 현실적으로 전원을 켜고 끄는데 많은 비용이 들거나 시간이 오래 걸리면 FDE를 꺼둘 수가 없게 되고 고장 발생이 가능하다. 그러므로 FDE에 고장이 발생하지 않는다는 가정 (B6)에 변경이 필요해진다.

이미 사전에 고장난 MS와 추가로 고장이 발생한 FDE를 어떤 순서로 수리하느냐에 대한 수리정책을 고려해야 한다. 실제 상황에서는 여러 조건을 고려하여 다양한 수리정책을 운용할 수 있을텐데 이 논문에서는 실제 상황에서 쉽게 운용 가능한 순차수리(sequential repair) 정책을 고려하기로 한다. 순차수리 정책은 먼저 고장이 발생하는 것부터 수리를 시작하는 수리정책이다. 즉, MS가 먼저 고장나고 FDE가 나중에 고장나면 먼저 고장난 MS를 수리하고 그 다음 FDE를 수리하는 경우이다. 신뢰도 분석을 위하여 조건 (A1)-(A4), (B1)-(B5) 외에 다음을 가정한다.

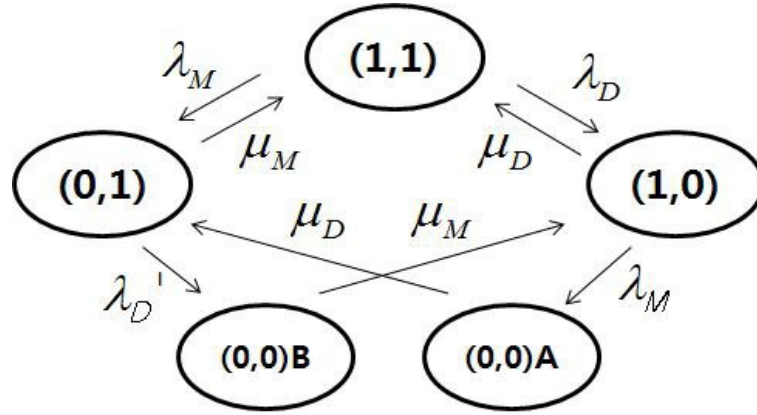


Figure 3.1. Transition diagram of MS-FDE system with sequential repair

(B7) MS의 고장을 탐지해서 수리를 하는 동안에 FDE는 λ'_D 의 비율로 고장나며 이 경우 순차수리를 시행한다.

MS 수리 중 FDE의 고장률을 기존의 λ_D 과 달리 λ'_D 로 별도로 표기한다. 조건 (A1)–(A4), (B1)–(B5), (B7)을 가정하는 MS-FDE 시스템의 상태전이도는 Figure 3.1과 같다. 여기에서 상태 (0,0)A는 Figure 2.1의 (0,0)와 같은 상태이며 FDE가 고장나고 MS가 고장난 상태이다. 반면 상태 (0,0)B는 MS 수리 중에 FDE가 고장난 상태로 순차수리가 적용되는 상태이다. 다음은 시스템 가용도 분석 결과이다.

정리 3.1 조건 (A1)–(A4), (B1)–(B5), (B7)을 만족하는 순차수리 정책의 MS-FDE 시스템을 가정할 때 시스템 가용도는

$$Av = \mu_M \mu_D (\lambda_M + \lambda_D + \mu_D) (\lambda'_D + \mu_M) \cdot C^{-1} \quad (3.1)$$

이다. 여기에서 정규화 상수 C 는

$$C = \mu_M \mu_D (\lambda'_D (\lambda_M + \lambda_D) + \lambda_D \mu_M) + \lambda_M \mu_M \mu_D (\lambda_M + \lambda_D + \mu_D) + \mu_M \mu_D (\lambda_M \mu_M + \mu_M \mu_D + \lambda'_D \mu_D) \\ + \lambda_M \lambda'_D \mu_D (\lambda_M + \lambda_D + \mu_D) + \lambda_M \mu_M (\lambda'_D (\lambda_M + \lambda_D) + \lambda_D \mu_M)$$

식과 같다.

증명: Figure 3.1의 상태를 11, 10, 01, 00A, 00B로 표기하기로 하고 다음의 평형방정식을 얻는다.

$$\begin{aligned} (1,1) : p(11)(\lambda_M + \lambda_D) &= p(01)\mu_M + p(10)\mu_D \\ (1,0) : p(10)(\lambda_M + \mu_D) &= p(11)\lambda_D + p(00B)\mu_M \\ (0,1) : p(01)(\mu_M + \lambda'_D) &= p(11)\lambda_M + p(00A)\mu_D \\ (0,0)A : p(00A)\mu_D &= p(10)\lambda_M \\ (0,0)B : p(00B)\mu_M &= p(01)\lambda'_D \end{aligned}$$

위 평형방정식에서 다음의 극한확률을 유도할 수 있다.

$$\begin{aligned} p(11) &= \mu_M \mu_D (\lambda_M \mu_M + \mu_M \mu_D + \lambda'_D \mu_D) \cdot C^{-1} \\ p(10) &= \mu_M \mu_D (\lambda'_D (\lambda_M + \lambda_D) + \lambda_D \mu_M) \cdot C^{-1} \end{aligned}$$

$$\begin{aligned}
p(01) &= \lambda_M \mu_M \mu_D (\lambda_M + \lambda_D + \mu_D) \cdot C^{-1} \\
p(00A) &= \lambda_M \mu_M (\lambda'_D (\lambda_M + \lambda_D) + \lambda_D \mu_M) \cdot C^{-1} \\
p(00B) &= \lambda_M \lambda'_D \mu_D (\lambda_M + \lambda_D + \mu_D) \cdot C^{-1}
\end{aligned}$$

위 결과를 이용하여 시스템 가용도는

$$\begin{aligned}
A_v &= p(11) + p(10) \\
&= \{ \mu_M \mu_D (\lambda_M \mu_M + \mu_M \mu_D + \lambda'_D \mu_D) + \mu_M \mu_D (\lambda'_D (\lambda_M + \lambda_D) + \lambda_D \mu_M) \} \cdot C^{-1} \\
&= \mu_M \mu_D (\lambda_M + \lambda_D + \mu_D) (\lambda'_D + \mu_M) \cdot C^{-1}
\end{aligned}$$

으로 주어지며, 식 (3.1)이 증명된다. \square

시스템 가용도 식 (3.1)은 다음과 같이 변형이 가능하다.

$$\begin{aligned}
A_v &= \frac{\mu_M}{\lambda_M + \mu_M} \cdot \frac{\mu_D (\lambda_M + \mu_M) (\lambda_M + \lambda_D + \mu_D)}{\mu_D (\lambda_M + \mu_M) (\lambda_M + \lambda_D + \mu_D) + \lambda_M \lambda_D \mu_M} \\
&\quad \cdot (\lambda'_D + \mu_M) \{ \mu_D (\lambda_M + \mu_M) (\lambda_M + \lambda_D + \mu_D) + \lambda_M \lambda_D \mu_M \} \cdot C^{-1}.
\end{aligned}$$

조건 (B7)에 의하여 FDE의 고장을 가정하는 경우에 시스템 가용도가 식 (2.2)의 가용도에 비하여 감소함을 알 수 있다. 한편 $\lambda'_D = 0$ 이면 식 (2.2)와 (3.1)은 같은 식이 된다.

다른 신뢰도 척도 평균작동시간(mean time between failures; MTBF)과 평균수리시간(mean time to repair; MTTR)은 다음과 같다.

정리 3.2 정리 3.1의 시스템을 가정할 때 $MTBF = \lambda_M^{-1}$ 과

$$MTTR = \mu_M^{-1} + \mu_D^{-1} \cdot \frac{\lambda_D (\mu_M + \lambda'_D) + \lambda_M \lambda'_D}{(\mu_M + \lambda'_D) (\lambda_M + \lambda_D + \mu_D)} \quad (3.2)$$

이 성립한다.

증명: 고장난 MS를 복구하면 11 혹은 10 상태에서 동작을 시작하며 고장이 발생하기까지 FDE와 관계없이 동작이 이루어진다. 따라서 조건 (A1)에 의하여 $MTBF = \lambda_M^{-1}$ 성립한다. 반면 시스템 고장은 01 혹은 00A 상태에서 시작되며 복구까지의 시간이 영향을 받는다. 상태 01, 00A에서 시작해서 상태 11 혹은 10까지의 평균수리시간을 각각 $MTTR(01)$, $MTTR(00A)$ 로 정의하자. 먼저 상태전이도 Figure 3.1과 지수분포의 비기억성을 이용하면

$$MTTR(00A) = \mu_D^{-1} + MTTR(01)$$

이 성립한다. 한편 $MTTR(01)$ 은 11 혹은 10까지의 상태 전이를 추적하여 다음과 같이 구할 수 있다.

$$MTTR(01) = \frac{\mu_M}{\mu_M + \lambda'_D} (\mu_M + \lambda'_D)^{-1} + \frac{\lambda'_D}{\mu_M + \lambda'_D} \{ (\mu_M + \lambda'_D)^{-1} + \mu_M^{-1} \} = \mu_M^{-1}.$$

시스템이 정상 혹은 고장 상태를 상태 i 에서 시작할 확률을 $p^*(i)$ 로 표기하자. 또 정상 상태를 j 에서 시작한 시스템이 다음 고장 상태를 k 에서 시작할 확률을 $p^*(k|j)$ 로 표기한다. 정상 상태에 대하여 다음 확률을 어렵지 않게 알 수 있다.

$$p^*(11) = 1 - p^*(10) = \frac{\mu_M}{\mu_M + \lambda'_D}.$$

고장 상태 01에 대하여 다음 식이 성립한다.

$$p^*(01) = p^*(11)p^*(01|11) + p^*(10)p^*(01|10).$$

조건부 확률에 대하여

$$\begin{aligned} p^*(01|11) &= \frac{\lambda_M}{\lambda_M + \lambda_D} + \frac{\lambda_D}{\lambda_M + \lambda_D} p^*(01|10) \\ &= \frac{\lambda_M}{\lambda_M + \lambda_D} + \frac{\lambda_D}{\lambda_M + \lambda_D} \cdot \frac{\mu_D}{\lambda_M + \mu_D} p^*(01|11) \end{aligned}$$

이 성립하고 이를 풀면

$$p^*(01|11) = \frac{\lambda_M + \mu_D}{\lambda_M + \lambda_D + \mu_D}$$

값을 얻을 수 있다. 또한

$$p^*(01|10) = \frac{\mu_D}{\lambda_M + \mu_D} p^*(01|10) = \frac{\mu_D}{\lambda_M + \lambda_D + \mu_D}$$

확률을 구할 수 있다. 따라서

$$p^*(01) = 1 - p^*(00A) = \frac{\mu_M(\lambda_M + \mu_D) + \lambda'_D \mu_D}{(\mu_M + \lambda'_D)(\lambda_M + \lambda_D + \mu_D)}$$

값을 얻게 되고 이를 이용하여

$$\begin{aligned} \text{MTTR} &= p^*(01) \cdot \text{MTTR}(01) + p^*(00A) \cdot \text{MTTR}(00A) \\ &= \frac{\mu_M(\lambda_M + \mu_D) + \lambda'_D \mu_D}{(\mu_M + \lambda'_D)(\lambda_M + \lambda_D + \mu_D)} \cdot \mu_M^{-1} + \frac{\lambda_D \mu_M + \lambda'_D(\lambda_M + \lambda_D)}{(\mu_M + \lambda'_D)(\lambda_M + \lambda_D + \mu_D)} \cdot (\mu_M^{-1} + \mu_D^{-1}) \\ &= \mu_M^{-1} + \mu_D^{-1} \cdot \frac{\lambda_D(\mu_M + \lambda'_D) + \lambda_M \lambda'_D}{(\mu_M + \lambda'_D)(\lambda_M + \lambda_D + \mu_D)} \end{aligned}$$

결과를 얻을 수 있고, 식 (3.2)가 증명된다. \square

FDE의 고장 가능성을 가정하는 조건 (B7)에 의하여 식 (3.2)의 값이 식 (2.3)보다 증가함을 쉽게 확인할 수 있으며 $\lambda'_D = 0$ 이면 두 식은 동일하다. 한편 식 (3.2)의 값은 식 (3.1) 가용도와 정리 3.2의 MTBF를 교대재생과정의 가용도에 대한 기본 성질에 대입하여 얻는 결과와 동일하다. 이 사실은 순차 수리 MS-FDE 시스템이 교대재생과정 특성을 가짐을 보여주는 좋은 예라 하겠다.

4. 결론

별도의 고장감지장치 등을 통하여 고장 여부의 상태를 관리하는 시스템을 쉽게 접할 수 있다. 가령 원격감시와 제어가 이루어지는 공장자동화 설비, 원격 감시가 이루어지는 통신 및 전력 시스템, 원격 의료진단 장비 등을 생각할 수 있다. 이러한 시스템을 적절히 모델링하기 위해서 주시스템(MS)과 함께 별도의 고장감지장치(FDE)를 고려한다. MS의 상태를 모니터하는 FDE가 제기능을 수행하지 못하면 MS에 대한 고장 수리가 지체되고 이의 결과로 시스템 가용도가 감소하리라 예상할 수 있다. 기존의 연구는 MS의 고장을 발견하고 수리하는 과정에서 FDE의 고장이 발생하지 않는다는 가정을 통하여 분석을 실시하였다.

하지만 MS 수리중에 FDE의 고장이 발생하지 않는다는 가정이 현실적으로 적절치 않을 수 있고, 이러한 점을 고려한 모델링을 이 논문에서 연구하였다. 특히 MS와 FDE를 고장난 순서대로 수리하는 순차수리 정책을 반영한 시스템을 고려하였다. 마코프 과정 표현을 위하여 MS, FDE 모두 고장난 상태를 세분화할 필요가 있었고 순차수리 정책에 따른 상태전이도를 완성하였다. 마코프 모델링을 통하여 이론적으로 산출한 시스템 가용도는 고장 메카니즘의 변화에 따라 감소함을 확인할 수 있다. 순차수리 MS-FDE 시스템의 상태 전이를 바탕으로 MTBF, MTTR 등을 직접 계산하고 교대재생과정의 가용도를 이용하여 유도한 값과 동일함을 볼 수 있었다.

이 논문은 FDE를 고려한 신뢰도 분석을 현실성이 있는 새로운 상황에 적용한 의미가 있다. 한편 시스템 복잡도, 수리 인원 등의 요소를 고려한 또 다른 수리 정책이 가능할 수 있다. MS-FDE 시스템에 대하여 현실성 있는 다양한 수리정책을 설정하고 분석 결과를 비교하는 작업도 가능할 것이다.

References

- Guo, H. and Yang X. (2008). Automatic creation of Markov models for reliability assessment of safety instrumented systems, *Reliability Engineering and System Safety*, **93**, 807-815.
- Na, S. (2011). Reliability analysis of repairable systems considering failure detection equipments, *The Korean Journal of Applied Statistics*, **24**, 515-521.
- Ross, S. M. (1996). *Stochastic Processes*, 2nd Edition, Wiley, New York.
- Zhang, T., Long, W. and Sato, Y. (2003). Availability of systems with self-diagnostic components – applying Markov model to IEC 61508-6, *Reliability Engineering and System Safety*, **80**, 133-141.

시스템 가용도에 미치는 고장감지장치의 영향

나성룡^{a,1} · 방성환^a

^a연세대학교 정보통계학과

(2012년 11월 30일 접수, 2012년 12월 27일 수정, 2013년 1월 3일 채택)

요약

이 논문에서는 고장감지장치(FDE)가 시스템 가용도에 미치는 영향을 연구한다. 주시스템(MS) 수리 도중에 고장이 발생한 FDE를 수리하기 위한 새로운 수리 정책을 고려한다. 이 논문의 주요 목적은 MS의 가용도를 계산하고 비교하는 데에 있다.

주요용어: 시스템 가용도, 고장감지장치, 순차수리, 신뢰도, 마코프 과정.

¹교신저자: (220-710) 강원도 원주시 연세대길 1, 연세대학교 정보통계학과, 교수. E-mail: nasr@yonsei.ac.kr