

실시간 시스템의 제어기 시간 제약성

이상문 · 김학배  
연세대학교 전기·컴퓨터공학과

Timing Constraints of the Controller in a Real-Time System

Sangmoon Lee and Hagbae Kim

Dept. of Electrical and Computer Engineering, Yonsei University

**Abstract** - 실시간 제어시스템은 데드라인(deadline)이라는 시간 제약성을 가지며, 데드라인 이내의 작업수행 여부에 따라서 시스템의 안정성 및 신뢰성 보장을 평가할 수 있다. 본 연구에서는 실시간 시스템 제어기의 시간 지연에 의한 시스템의 영향과 이에 따른 시간 제약성에 대한 연구가 수행된다. 정상상태의 제어기의 시간 지연은 그 효과가 미약하여 일반적으로 고려하지 않는다. 그러나, 시스템의 고장상태 즉, 비정상적인 상태의 시간지연은 비록 랜덤하게 발생되나 발생시에는 전체시스템에 미치는 영향이 매우 크므로 이를 반드시 고려하고, 이에 대한 분석이 필요하다. 먼저, 단일작업을 수행하는 선형시불변 및 비선형시스템에 대한 데드라인 유도하고, Path-space approach 기법에 의해 신뢰도 상위 및 하위 경계값을 유도한다.

정확한 데드라인값의 유도는 현재로는 미흡한 실정이다. 본 연구에서는 간단한 단일작업을 수행하는 선형시불변(LTI) 시스템에서 시간지연이 제어시스템의 안정성에 주는 영향분석과 이를 통한 시스템의 데드라인을 유도한다. 또한, 신뢰도 평가를 위해 일반함수를 확률밀도함수로 갖는 상태전이를 모델링할 수 있는 semi-Markov 모델을 활용하여 제어기의 고장과 고장 하에서도 데드라인 내의 시스템의 일시적인 안정성 유지 및 전체 시스템의 고장 등을 함축할 수 있는 모델 하에서 시스템 신뢰도를 유도하는 기법이 연구되었다.

2. 단일작업을 수행하는 선형시불변 시스템의 경성데드라인 유도

1. 서 론

최근들어 디지털컴퓨터는 속도와 성능면에서 기술발전이 거듭되고 있으며, 여러 응용분야에서 널리 사용되고 있다. 일반적으로 디지털컴퓨터 제어기는 시스템/플랜트의 안정성 유지와 성능향상을 위해서 주변장치를 이용하는데, 이때 케환루프에서 필연적으로 작지 않은 시간적 지연현상이 발생하게 되지만, 일반적으로 시스템이 정상 동작을 수행할 때 이는 상대적으로 작기때문에 시스템의 안정성 및 성능에 미세한 영향을 미친다. 그러나, 내·외적인 요인(부품결함, EMI등)으로 인해서 발생하는 제어기 고장은 상당한 시간지연과 함께 시스템의 안정성에 심각한 영향을 미치게 된다[1]. 일반적으로 실시간 제어시스템은 항공기, 핵발전소, 인공위성 등의 시스템에서 제어 및 감시기능을 위해서 널리 활용되고 있는데, 제어기의 정확성이 작업의 논리적 결과뿐만 아니라 그 결과와 생성된 시간에도 좌우된다는 기본 성질에 의해 특성 지어진다[2]. 그러므로, 실시간 시스템은 어떠한 상황에서도 이러한 시계수 제한성을 만족시킬수 있는 시스템 설계 및 평가가 이루어져야 한다. 고장포용 제어를 플랜트에 도입해서 사용하면 일시적인 제어기의 논리적 오류가 발생했을 경우에도 적절한 고장허용기법을 통해서 시스템의 안정성을 유지할 수 있다. 하지만, 엄격한 시계수제한성을 내포한 실시간 시스템의 경우에는 데드라인이내에 데이터를 전달할 수 없는 경우에는 고장포용기법이 시스템의 안정성을 보장할 수 없다. 그러므로, 기존에 안정도 및 성능지수로 표현되어지던 시스템의 특성은 데드라인이 요구되는 실시간 시스템에서는 큰 의미를 가지는 요소가 되지 못한다. 즉, 시스템의 고신뢰도를 보장하기 위해서는 고장허용기법 뿐만 아니라, 시스템의 데드라인을 만족시키는 새로운 시스템 설계 및 정확한 신뢰도 평가가 요구된다. [3],[4]에서는 실시간 제어시스템에서 제어기의 계산지연시간에 대한 분석을 원시/모의 실험 및 단순한 이론적 모델링을 이용하였다. [5]에서는 데드라인의 특성을 파악하여 시스템의 적절한 설계를 고려하기도 하였지만, 제어시스템의 설계를 위해서 필수적인 제어시스템에서 유동적 특성을 반영한

적절한 실시간 제어시스템의 설계를 위해서 필수 정보인 데드라인을 유도하기 위해 이에 영향을 주는 시스템의 동적특성, 외부환경변수, 그리고 제어법칙 등을 모두 고려하여 데드라인을 유도하는 것은 거의 불가능하다. 따라서 단일작업을 수행하는 선형시불변 시스템의 동적특성을 고려한 데드라인을 유도한다. 즉, 시스템의 동적특성을 반영하는 상태제한조건, 종료조건, 수행시간, 표본추출주기, 자원제한조건, 그리고 고장검출 및 회복기법 등을 포함하여 순차적회귀기법 즉,  $i$ -반복기법으로 데드라인을 유도하였다.

2.1 단일작업수행 선형시불변(LTI) 시스템

단일작업을 수행하는 선형시불변 시스템의 상태방정식은 식(1)과 같다.

$$x(k+1) = Ax(k) + Bu(k) \tag{1}$$

$$u(k) = -Fx(k)$$

여기서,  $A = e^{A_c T_s}$ ,  $B = \int_0^{T_s} e^{A_c (T_s-\tau)} B_c d\tau$ 이다.  $A_c$ ,  $B_c$ 는 각각 연속시간모델의 계수행렬이고,  $T_s$ 는 표본추출주기이다. 케환루프에서 지연시간은 제어시스템/플랜트의 성능을 저하시키며, 고장회복지연시간이 연장되어 데드라인을 초과한다면 회복불가능한 시스템/플랜트의 고장이 발생될 것이다.  $X_A$ 는 허용상태공간이고,  $U_A$ 는 허용가능입력공간이라 정의할 때, 시간  $k_0$ 에서 제어기의 일시적 고장으로 인해서 계산지연시간  $NT_s$ 가 발생한다면, 시간  $k$ 에서의 상태 방정식은 식(2)와 같다.

$$x(k) = \Phi(k, k_0, x(k_0), u(k-M)) \tag{2}$$

여기서  $\Phi$ 는 상태변화함수이고, 시간  $k_0$ 에서 시작하는 제어작업의 데드라인은 식(3)으로 정의된다.

$$D(x(k_0)) = u(k-M) \in U_A \{N\Phi(k, k_0, x(k_0), u(k-M)) \in X_A\} \tag{3}$$

즉, 시간  $k_0$ 에서 시작하는 작업의 데드라인은 제어시스템이 이 시간에서 고장이 발생했음이라도 안정성을 유지시켜 줄 수 있는 허용 가능한 최대계산지연시간으로 정의된다. 제어기의 입력신호가  $t = mT_s$ 마다 구동기를 갱신한다면 제어기에서 일시적 고장이 발생즉시 검출된다고 가정하고 지연시간이  $iT_s$ 주기동안 지속될 때, 구동

기의 값은 hold-and-latch회로의 특성 때문에 고장발생 이전에 갱신된 값으로 유지될 것이고, 이 때 시스템의 상태방정식은 식(4)과 같다.

$$\begin{aligned} x(mN+1) &= A x(mN) + B u(mN) \\ x(mN+2) &= A^2 x(mN) + (A+I) B u(mN) \\ &\vdots \\ x(mN+i) &= A^i x(mN) + \sum_{j=0}^{i-1} A^j B u(mN+j) \\ x(mN+i+1) &= A^{i+1} x(mN) + \sum_{j=0}^i A^j B u(mN+j) + B u(mN+i) \\ &\vdots \\ x((m+1)N) &= A^N x(mN) + \sum_{j=0}^{N-1} A^j B u(mN+j) \\ &\quad + \sum_{j=0}^{N-1} A^j B u(mN+N-j-1) \end{aligned} \quad (4)$$

여기서,  $m$ 은  $N$ (최대고장지속시간,  $NT_s$ ) 표본추출기간을 통합하기 위한 시간지표이다.  $X(m)$ 과  $U(m)$ 을 다음과 같이 재정의한다.

$$X(m) = [x(mN+1), x(mN+2), \dots, x((m+1)N)]^T \quad (5)$$

$$U(m) = [u(mN+1), u(mN+2), \dots, u((m+1)N)]^T \quad (6)$$

위 식에서  $X(m)$ 과  $U(m)$ 은 누적상태벡터이고, 고장으로 인한 시간지연이  $iT_s$  동안 지속된다면, 누적상태방정식은 식(7)과 같은 형태로 표현된다.

$$X(m+1) = A_D X(m) + B_D U(m) + B_D^2 U(m+1) \quad (7)$$

$$U(m) = -F_D X(m)$$

식(7)에서 각각의 누적상태방정식의 새로운 계수행렬  $A_D$ ,  $B_D^1$ , 및  $B_D^2$ , 는 각각 행렬 값들로 얻을 수 있다. 만일, 고장이 매주기 이진 분포에 의해 발생한다고 가정하면,  $q_0, q_1, \dots, q_N$ 은  $0, T_s, \dots, NT_s$ 의 지연시간의 확률로 각각 표현되고, 최대지연시간이  $NT_s$ 라고 가정하면  $\sum_{i=0}^N q_i = P$ 가 된다. 여기서,  $P$ 는 고장발생을 지배하는 이진분포함수의 변수가 된다. 지연시간 분포는 외부환경 특성에 대한 분석 및 통계기법으로부터 실제적으로 추정될 수 있다. 이러한 지연시간 분포와 앞서 수정된 상태방정식을 결합함으로써 지연시간의 효과가  $NT_s$ 보다 작거나 같을 때의 상태방정식은 다음과 같이 보안된다.

$$X(m+1) = A_D X(m) + \sum_{i=0}^N \xi_i (B_D^1 U(m) + B_D^2 U(m+1)) \quad (8)$$

여기서  $\xi_i \in \{0, 1\}$ 는 확률 파라미터  $q_i$ 를 갖는 이진분포를 갖는 랜덤변수이다(즉,  $\Pr\{\xi_i=1\} = q_i$ ). 그러므로, 계관지연이 정상확률모델에 의해 일정하게 발생할 때 제어시스템의 특성방정식은 식(8)로부터 다음과 같이 유도될 수 있다.

$$\det[(I + \sum_{i=0}^N q_i B_D^2) z^N - A_D + \sum_{i=0}^N q_i B_D^1] = 0 \quad (9)$$

식(9)에서  $i$ 의 값을 증가시키면서 극점위치를 검사하여 그 값이 시스템 안정성 유지를 위해 필요한 허용상태공간을 벗어나게 하는 최소의 지연시간  $N$ (즉, 시스템안정성을 유지시키는 최대지연시간)을 유도할 수 있다.

### 3. Semi-Markov 모델링

일반적으로 랜덤이산사건에 의한 제어시스템의 유동적인 상태를 모델링할 때 Markov model을 이용한 방법이 널리 활용되어 왔다. 하지만, Markov model의 경우 데드라인 정보를 포함해야 할 있는 실시간 제어시스템의 상태에서 비지수함수를 확률밀도로 하는 상태천이 시간을 표현하기 불가능하고 이를 확장한 semi-Markov 모델 또한 각각의 정상상태 확률을 유도하기가 난해하다. 즉, Chapman-Kolmogorov 방정식을 이용해서 회귀적인(recursive) 적분방정식을 이용하여 수학적 해석이 가능하지만 상태 수가 증가하는 경우에 Chapman-Kolmogorov 방정식에 의한 계산량이 급격하게 많아져 계산이 불가능하게 된다. 비실시간 시스템의 유동적인 상태천이는 고장발생 및 회복시간이 지수분포를 갖는다는 가정 하에 그림 1.(a)과 같은 two-state Markov 모델에 의해 표현될 수 있으나 실시간

제어시스템의 이산사건들(고장 발생 및 회복)에 의한 상태천이는 데드라인을 경과함으로써 천이되는 시스템고장으로의 과정이 지수분포로는 더 이상 표현할 수 없기 때문에 그림 1.(b)과 같이 Markov process의 개념을 확장한 semi-Markov 모델을 이용해서 표현하였다. 여기에서 시스템의 정상상태, 제어기고장 및 전체 시스템고장 상태는 각각  $S_0, S_1, S_2$ 에 의해 그려졌고 각각의 상태천이 시간은  $f(t), g(t)$ (이상 지수분포) 및  $d(t)$ 에 의해 표현되었다. 제어기 고장은 일시적일 수 있기에 회복될 수 있지만(loop 형성), 데드라인을 경과한 긴 제어기 고장상태는 흡수(absorbing)상태인 시스템고장으로 이끌게 됨을 아래 그림에서 확인할 수 있다.

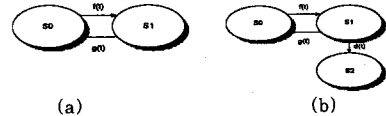


그림 1. (a) 데드라인 정보를 가지지 않는 시스템의 Markov model  
(b) 데드라인 정보를 갖는 시스템의 semi-Markov model

### 4. Path-space 기법을 적용한 시스템 신뢰도의 경계치 유도

그림 1.(b)에서  $f(t), g(t), d(t)$ 는 제어기고장의 inter-arrival 시간과 회복시간 그리고 데드라인을 경과할 수 있는 시간들을 나타내는 확률밀도함수라 정의하였다. 만약  $F(t), G(t), D(t)$ 가  $f(t), g(t), d(t)$ 의 cumulative 확률분포(distribution)함수를 나타내고  $f_{ij}(t)$ 가 상태  $S_i$ 에서  $S_j$ 로 천이될 때의 확률밀도함수로 정의된다면,

$$\begin{aligned} P_{02}(T) &= \int_0^T f_{01}(x) P_{12}(T-x) dx \\ P_{12}(T) &= \int_0^T f_{10}(x) P_{02}(T-x) dx + \int_0^T f_{12}(x) dx \end{aligned} \quad (10)$$

와 같은 계산 결과를 얻을 수 있다. 위의 식에서  $P_{02}(T)$ 를 계산하기 위해  $P_{12}(T)$ 를 대입하면, 반복적(회귀적)으로 식의 대입을 요구하게 되고, 적분횟수의 증가로 인해 실질적인 계산이 불가능하게 된다. 이론적으로 Markov 모델에서 모든 상태는 이전의 모든 상태에 비의존적이면서(memoryless), 바로 전 상태 및 그 때의 사건 발생 종류에만 의존하므로, 그림 2와 같이 가능한 sample path를 이루는 상태 sequence에서 각 상태들의 배열순서를 바꿀 수가 있다. 이렇게 이산사건에 발생 시퀀스에 의한 시스템 상태 sequence를 모두 배열한 path를 중심으로 상태확률을 구하는 방법이 path-space 기법의 시작이다.

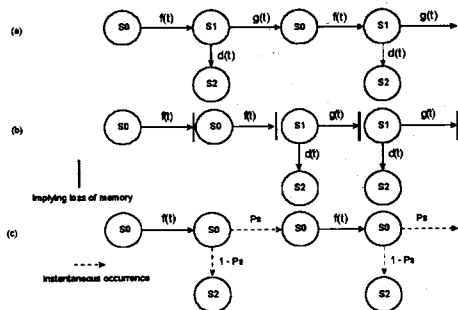


그림 2. (a) transitions ordered originally  
(b) transition reordered using the property of semi-Markov models(independent of the global time)  
(c) Transitions approximated by instantaneous coverage

이러한 상태 확률의 정확한 값을 유도하기 위해선 path-space 기법 또한 무한히 많은 적분을 해야하는 어려움이 있으나 (semi-) Markov process의 개념에 의한 path상에서의 순서 변동(적분순서 변경) 및 적분

구간 변경을 통한 상위 및 하위 경계값의 유도는 계산과정을 눈에 띄게 단순화 시켜준다. 이렇게 유도된 상·하위의 경계값들의 차이가 극히 미소하다면 그 tightness에 의해 정확한 값의 위치 구간을 쉽게 추정할 수 있다. path-space 기법은 이러한 여러 가지의 기본 개념에 근거해서 초기 시간부터 임의의 시간 T(mission time)까지 시스템고장에 도달하는 모든 가능한 path를 설정해서 이러한 path들의 확률값들을 더함으로써 전체 시스템고장의 확률을 유도할 수 있게 된다. 임의의 시간 T까지 시스템고장이 일어날 확률은 상태 및 path간의 비의존성에 의해서 시스템고장 상태로 흡수되는 모든 path들의 확률의 합과 같다.  $P_n$ 이 n-1번째 상태간의 루프를 경유한 이후에 시스템 고장 상태로 천이될 확률이라고 정의한다면,

$$P_0 = \int_0^T f_{01}(t_1) \int_0^{T-t_1} f_{12}(t_2) dt_2 dt_1 \quad (11)$$

$$P_1 = \int_0^T f_{01}(t_1) \int_0^{T-t_1} f_{10}(t_2) \int_0^{T-t_1-t_2} f_{01}(t_3) * \int_0^{T-t_1-t_2-t_3} f_{12}(t_4) dt_4 dt_3 dt_2 dt_1$$

$$\vdots$$

$$P_n = \int_0^T f_{01}(t_1) \int_0^{T-t_1} f_{10}(t_2) \int_0^{T-t_1-t_2} f_{01}(t_3) * \int_0^{T-t_1-t_2-t_3} f_{10}(t_4) \int_0^{T-t_1-t_2-t_3-t_4} f_{01}(t_{2n-1}) * \int_0^{T-t_1-t_2-t_3-t_4-t_{2n-1}} f_{12}(t_{2n}) dt_{2n} dt_{2n-1} \dots dt_2 dt_1$$

와 같이 된다. 또한 이 식을 그림 2.(b)에서 보는 것과 같이 전체시간에 대한 상태의 독립성을 바탕으로 식을 재배열하면 일반적인 n에 대한  $P_n$ 은 적분순서를 재배열하는 결과로 인해 식(12)와 같은 동일한 계산식으로 나타내어진다.

$$P_n = \int_0^T f_{01}(t_1) \int_0^{T-t_1} f_{01}(t_2) \dots \int_0^{T-t_1-t_2-t_{n-1}} f_{01}(t_n) * \int_0^{T-t_1-t_2-t_{n-1}} f_{12}(t_{2n-1}) \int_0^{T-t_1-t_2-t_{n-1}-t_{2n-1}} dt_{2n} \dots dt_2 dt_1 \quad (12)$$

위에서 얻어진  $P_n$ 에서 적분 영역을 바꾸면 시계수 제한성을 포함한 실시간 시스템 신뢰도의 상·하위 경계치를 유도할 수 있게 된다. 이러한 bounding과정은 식(13)과 같은 부등식들에 의해 표현된다.

$$P_0 \leq \int_0^T f_{01}(t_1) \int_0^\infty f_{12}(t_2) dt_2 dt_1$$

$$\vdots$$

$$P_n \leq \int_0^T f_{01}(t_1) \int_0^{T-t_1} f_{01}(t_2) \dots \int_0^{T-t_1-t_2-t_{n-1}} f_{01}(t_n) dt_n \dots dt_2 dt_1 * \int_0^\infty f_{12}(x) dx \int_0^\infty f_{12}(x) dx \quad (13)$$

여기서  $\Pr[k \leq n | T]$ 는 제어가 T시간 동안에 최소한 n번 실패할 확률을 의미하며  $G(\tau)$ 는 데드라인 이내에 제어기가 회복될 확률값이다. 그러므로, 전체 시스템 고장의 상위(UB) 및 하위 경계치(LB)는 다음과 같이 유도된다.

$$UB = [1 - G(\tau)] \sum_{n=1}^{\infty} \Pr[k \leq n | T] G^{n-1}(\tau) \quad (14)$$

$$LB = [1 - G(\tau)] \sum_{n=1}^{\infty} \Pr[k \leq n | T - n\tau] G^{n-1}(\tau) \quad (15)$$

위의 식(14)와 (15)에서 상·하위의 경계치 등의 차이는 단순히 제어기 고장 및 전체시스템고장을 관찰할 mission time구간이 되는 시간간격이 각각 T와  $T - n\tau$ 로 해서 전체합을 구한다는 것이다. 임의의 시간구간 T에 대해 제어기 고장이 여러번 일어날 확률은 아주 작으므로 큰 값의 n에 의한 UB 및 LB 값에의 기여도는 무시할 만큼 작음을 고려할 때 전체적으로 근사된 상·하위의 값 차이가 미소함을 직관적으로도 알 수 있다.

## 5. 예 제

우리는 상·하위 경계치들의 엄정함을 알아보기 위해서 (상위 경계치-하위 경계치)에서 상위 경계치를 나눈 값을 상대적차이비율(Relative Ratio Difference, RRD)이라고 정의하고 그 값들을 측정하였고 이 값이 극히 작은 경우 두 경계치가 근사함을 보인다고 말할 수 있다. 예로는 자동화된 생산 시스템에서 제어기에 의해 관측되고 운영되는 생산 라인이 있고 이 라인의 제어기

가 10일의 평균과 회복 확률이 0.95인 지수 분포의 실패 확률 분포를 가지고 있다고 하자. (즉  $G(\tau)$ : 0.95,  $1/\lambda$ : 10일,  $\tau$ : 15분, T: 1일.) 또한, 작업시간이 하루를 주기로 완결된다고 하자. 그러면, 이러한 경우 제안된 모델 및 계산기법에 의해 유도된 전체 시스템고장 확률의 상위 및 하위 경계치는 다음 표1과 같다. 이때의 RRD는 경계치의 엄정함을 보여줄 만큼 충분히 작다.

표 1. 생산 라인 제어의 상·하위 경계치와 상대 차이 비율

1/λ	5일	10일	30일
상위경계치	0.009950	0.004988	0.001665
하위경계치	0.009828	0.004931	0.001647
상대/비율	0.01228	0.01134	0.01072
G(τ)	0.9	0.95	0.99
상위경계치	0.009950	0.004988	0.000100
하위경계치	0.009238	0.004931	0.0009881
상대/비율	0.01127	0.01134	0.01141
τ	5분	15분	30분
상위경계치	0.004988	0.004988	0.004988
하위경계치	0.004969	0.004931	0.004875
상대/비율	0.00379	0.01134	0.02266
T	12시간	1일	2일
상위경계치	0.002497	0.004988	0.009950
하위경계치	0.002443	0.004931	0.009889
상대/비율	0.02173	0.01134	0.00615

## 6. 결 론

본 논문은 실시간 시스템의 시계수 제한성 정보를 제어기의 유동적 상태에 포함시켜 전체 시스템의 신뢰도를 평가하기 위한 기본 모델링과 이의 계산을 위한 기법을 검토하였다. 시계수 제한성을 이용하여 보다 정확한 전체 시스템의 고장 확률을 분석하고, 이를 포함한 시스템 신뢰도를 해석적으로 유도하였다. 먼저, 단일작업을 수행하는 선형시불변(LTI) 시스템에서 시간지연에 대한 안정성 분석과 이를 통한 시스템의 데드라인을 유도하였으며, 시계수 제한성과 회복 시간에 의한 제어기 고장과 시스템고장을 구분하여 semi-Markov model로 제시하였다. 또한 제안된 모델에 semi-Markov 특성을 고려한 path-space 기법을 적용하였다. Semi-Markov 특성을 결합한 path-space 기법은 신뢰도 계산에 있어 편리하고 직접적인 기법이며 많은 parameter를 필요로 하지 않기 때문에 복잡한 모델을 해석하기 간단하게 만들 수 있다. Path-space 기법에 의해 구해진 식을 수치 해석적으로 계산하기는 쉬우며, 예제를 통해 유도된 경계치의 상대 비율차이가 얼마나 엄정함을 보여주었다.

## (참 고 문 헌)

- [1] S. McConnel, D. Siewiorek, and M. Tsao, "The measurement and analysis of transient errors in digital computer systems," *Digest of Papers, FTCS-9*, pp. 67-70, Jun. 1979.
- [2] K. Shin and X. Cui, "Effects of computing time delay on real-time control systems," *Proc. of 1988 American Control Conf.*, pp. 1071-1076, Jun. 1988.
- [3] H. Kim and K. Shin, "On reconfiguration latency in fault-tolerant systems," in *IEEE 1995 Aerospace Applications Conference*, pp. 287-301, Snowmass at Aspen, CO, Feb. 1995.
- [4] K. Shin, C. Krishna, and Y. Lee, "A unified method for evaluating real-time computer controller and its application," *IEEE Trans. on Automat. Contr.*, vol. AC-30, no. 4, pp. 357-366, Apr. 1985.
- [5] H. Kim and K. Shin, "On the maximum feedback delay in a linear/nonlinear control system with input disturbances caused by controller-computer failures," *IEEE Trans. on Control Systems Technology*, vol. 2, no. 2, pp. 110-122, Jun. 1994.