논단 II

고신뢰도 제어시스템 기술

한국전기연구원
박사 권 순 만

1. 서 론

계측제어 기술은 크게 계측제어 시스템을 구성하는 H/W 및 S/W와 관련된 시스템 기술과 제어 및 진단 등을 위한 이론적인 제어 분야로 크게 나누어 생각할 수 있다. 본고에서는 계측제어 시스템 기술 중에서 국내 산업과 유관성이 큰 분야로서 고신뢰도/고안전도 제어시스템 기술에 관하여 기술하고자 한다. 계측제어 기술이 모든 국내외의 산업과 밀접한 관계를 가지고 있지만 결국 이 분야에서 해결이 요구되는 핵심 문제는 초정밀제어와 고신뢰도/고안전도 제어시스템(Dependable System) 기술이다. 초정밀제어 기술의 분야는 센서, actuator, 구조물 등의 복합적인 문제가 수반되지만 제어 기술의 관점에서는 자동제어 이론으로 집약되는 반면에, 고신뢰도/고안전도 기술은 제어시스템의 운용상의 관점에서 주로 논의되는 분야이다.

자동제어로 통칭되는 많은 제어 관련 기술들은 주로 feedback control로 대표되는 제어 이론의 연구와 교육이 주를 이루어 왔다. feedback control은 제어대상 기기 또는 플랜트가 외란과 잡음에 의한 출력의 영향이 커지는 것을 예방하기 위한 이론적 근거를 가지고 설계되는 것으로 모델링, controller design 등의 단계로 설계되는 것이다. 기본적으로는 모델의 선형/시불변/정확도 특성을 근거로 제어기를 설계하였으나 실제의 모든 제어대상은 비선형/시변 특형을 갖게되며 이론적으로 유한 차수로 정확한 모델링이 불가능하다는 현실속에서 Nonlinear Control, Adaptive Control, Robust Control, 그리고 Fuzzy, Neural Network 개념을 이용하는 제어 이론들이 급속히 발전되고 있다. 이러한 이론들은 때로는 상반되는 가정하에서 그 효용성을 입증하기도 하지만 상호 보완적으로 수학적으로 다양한 특성을 갖는 제어 대상들에 효과적인 대응 방법을 제시하면서 이론적인 체계를 갖추어 왔다. 특히 수학을 기본으로 하는 이론적인 접근에서 많은 주목할 만한 성과들을 나타내고 있으며 국내에서도 많은 관심속에 연구되고 있는 분야이다.

국내에서 그 해결책이 요구되는 또 하나의 분야인 제어 시스템 기술의 현실은 아직 그러하지 못하며, 초기적인 단계에 머물러 있다. 그 이유로는 제어시스템은 기본적인 계측과 제어기능, 다양한

통신 및 사용자 Interface, 진단 및 보호 기능의 구현 등이 필요하며 제어대상에 따라 요구되는 신뢰도와 안전도가 크게 달라지기 때문이다. 제어시스템의 규모는 제어 대상 기기나 Plant의 규모에 의해서 결정되지만 통상 대규모 시스템의 경우 제어시스템 기술은 I&C(Instrumentation and Control)로 불린다. 본고에서는 제어시스템의 다양한 요구 특성 중에서 신뢰도와 이용도, 안전도의 측면에서 기술하고자 한다.

제어시스템에 관해서 보통 신뢰도가 높고 안전을 보장할 수 있을 것 등과 같은 표현은 통상적으로 많이 사용되는 용어이지만 다분히 주관적이고 정성적인 내용이 되므로 좀 더 구체적이며 상대적인 특성 평가를 위해서는 정량적인 표현이 가능하여야 한다. 정량적인 특성을 나타내는 평가지수로는 RAMS(Reliability, Availability, Maintainability, Safety)가 사용되며 최근에는 좀 더 복합적인 개념의 TDP(Testability, Dependability, Performability)가 사용되고 있다. 다음 장에서 RAMS와 TDP에 대해서 소개한다.

2. 정량적 평가 기법과 구현 개념

가. RAMS & TDP 정의

RAMS 및 TDP의 정의는 다음과 같다 [1], [2].

(1) Reliability : Reliability는 초기시각 t_0에서 정상으로 동작하던 시스템이 시구간$[t_0, t]$에서 정상으로 동작할 조건부 확률이며 시간 t의 함수인 R(t)로 표시된다.

(2) Availability : Availability는 t 시각에서 정상적으로 기능을 발휘할 확률이며 통상적으로는 시간 구간내에서 정상으로 동작하는 시간의 비율로 해석되며 A(t)로 표시된다.

(3) Maintainability : Maintainability는 고장난 시스템이 시간 t에 복구될 확률을 의미하며 M(t)로 표시된다.

(4) Safety : Safety는 주어진 시스템이 정상적으로 동작하거나 고장시에 안전측으로 동작할 확률을 의미하며 S(t)로 표시된다.

(5) Testability : Testability는 주어진 시스템 내에서 제반 요구 사항을 시험할 수 있는 정도를 나타내는 값으로 정량화된 표현의 체계에 관해서는 공감이 이루어지지 않은 상태이다.

(6) Dependability : Dependability는 Fault-Tolerance와 RAMS를 포함하는 복합적인 개념으로 주어진 시스템이 제공하는 기능의 질에 관한 정성적의미로 출발하였으나 최근에는 Dependable, Ultra Dependable 등의 초고신뢰도를 의미하는 형태로 많이 사용된다.

(7) Performability : Performability는 주어진 시스템이 설계의 초기 목적보다 어느 정도 성능이 저하된 상태에서 동작될 수 있는 확률을 의미한다. 즉 100%의 성능보다 낮은 L이상의 성능을 발휘할 수 있는 확률을 의미하므로 P(L,t)로 표시된다.

나. RAMS의 요구방법

시스템의 요구 Specification에서 상기의 RAMS & TDP를 모두 엄격하게 적용하는 구체적 수치를 제시하는 경우는 드물다. 그 이유는 대부분의 시스템이 사용되는 목적에 따라 그 요구되는 대표적 특성이 다르므로 그 목적에 맞는 대표적인 특성의 정

량적 값이 Specification에 기술된다. 고신뢰도/고안전도 제어시스템은 사용되는 목적에 따라 다음과 같은 구분이 가능하다.

(1) 장수명 운용 : 무인 인공 위성이나 우주선의 경우는 10년 동안 정상 동작할 확률을 0.95 이상으로 하면서 이 기간 동안에 전혀 유지보수가 불가능한 조건으로 설계되는 것이다.

(2) 초고신뢰도 운용 : 항공기의 경우는 1회 비행의 시간이 10-15시간 이내이지만 어떤 부분의 이상은 비행기를 추락시킬 수 있으며 이런 핵심적인 부분의 신뢰도는 10시간의 운전시 0.9_7의 신뢰도가 요구되고 있다.

(3) 초안전도 운용 : 원자력 발전소의 경우도 높은 신뢰도가 요구되지만 더 중요한 요소는 발전소 또는 원자로가 정지되더라도 방사능 유출 등의 대형 사고를 방지하는 것이 중요하다는 측면에서 앞의 항공기와 구분된다. 항공기의 경우는 비행중에 어떤 이상이 발견되어도 안전한 착륙이 이루어 질 때 까지는 제어 시스템의 기능을 계속 수행하는 것이 필수적이므로 다중화된 제어 시스템(대형기의 경우 통상 5중화)의 채널중 반수 이상에 이상이 발생해도 제어 기능을 계속 수행하는 반면에 원자로의 경우는 2 out of 4 Logic에서 원자로의 정지 판단 채널이 2개 이상이면 모든 제어 기능에 우선하여 원자로를 정지시키도록 설계되는 차이가 있다.

(4) 고이용률 운용 : 은행의 전산시스템의 경우가 높은 이용률이 요구되는 대표적 시스템의 예이다. 이 경우는 매우 짧은 순간의 정지는 허용이 되며 그 동안에 Data의 손망실이 일어나지 않도록 하는 것이 핵심 요구 조건이 된다.

다. RAMS의 구현방법

정량적 특성을 만족시키는 설계를 위한 개념적인 절차는 아래의 그림1에 나타나 있다. 그림1의 설계 과정의 단계별 내용을 살펴 보면 다음과 같다.

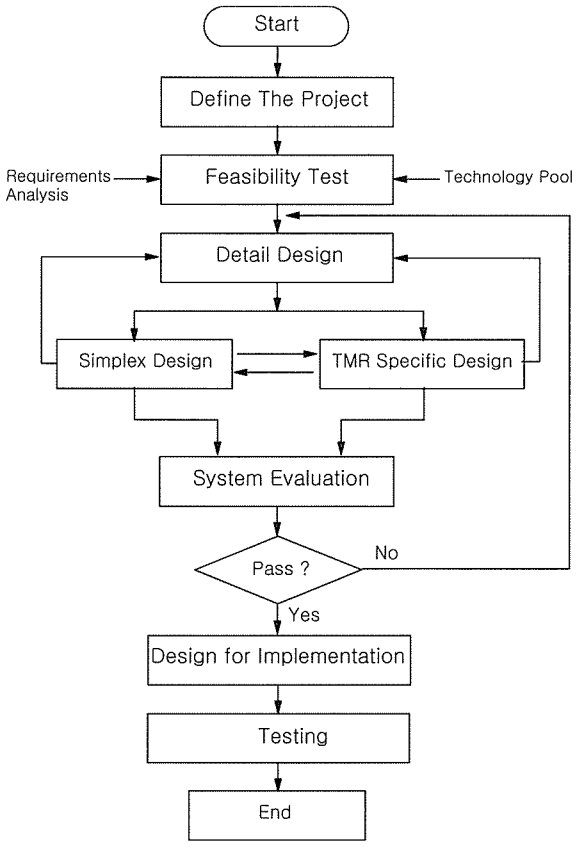
(1) 과제의 정의(Defining the project) : 이 단계에서는 대상플랜트에 대한 제어시스템의 기능적인 부분들이 정의된다. 또한 요구되는 정량적인 RAMS의 값들이 결정되어야 한다.

(2) 가능성 테스트 : 몇 개의 시작품을 개략적으로 설계한 후 RAMS 해석 tool을 이용하여 간단한 테스트를 통하여 설계 요건 충족의 가능성을 검토한 후 최종 하나의 시작 설계안을 확정한다.

(3) 상세 설계 : 이 단계에서는 부품을 고려한 상세한 설계가 이루어지는 데 앞에서 행한 가능성 테스트의 결과를 고려하여 Simplex 또는 N-modular 구조 등을 결정한다.

(4) 시스템 평가 및 판정 : 상세 설계된 시스템의 정략적인 평가가 상세히 이루어진다. 결과로서 나타나는 값의 설계 요건 충족 유무를 판정한 후 충족하지 못하면 새로운 시작 설계 단계로 돌아가서 앞서의 과정을 이 단계를 통과할 때까지 재반복한다.

(5) 제작 및 시험 : 시스템 평가 결과가 양호하면 실제 시스템을 제작하고 각종 규격에 맞추어 시험실 테스트를 행한 후 최종 field 테스트를 거친다. 이러한 테스트 중 필요에 따라 보완 작업을 거치며 경우에 따라 시스템의 설계 요건을 재평가한다.



(그림 1) 설계 과정

라. 디지털 시스템에서의 추가적인 문제

앞 절의 절차나 분석 Tool들은 대부분이 Component 또는 단위 시스템들의 정량적 특성이 알려진 경우에 사용이 가능하며 소프트웨어가 핵심을 이루는 디지털 시스템에서는 그 소프트웨어가 얼마나 Error가 없이 개발되었는가의 문제가 또 다른 문제로 남게되며 이에 대해서는 확인 및 검증 (V&V, Verification & Validation) 또는 Error 관련 영향을 정량적으로 분석해야 되는 거대한 연구 분야가 그 해결을 기다리고 있다.

3. 제어 시스템 평가 및 설계 구현 예

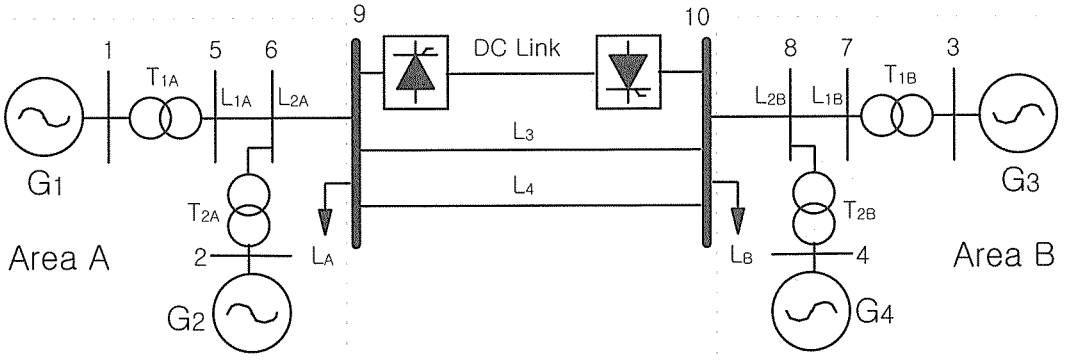
앞에서 설명한 제어 시스템의 신뢰도 평가와 고신뢰도 설계 과정을 실제 제어 시스템의 예를 들어 살펴보기로 한다.

가. 시스템 평가 예 (HVDC 시스템)

평가 기술의 한 예로서 현재 새로운 전력 기술의 한 주요 분야로 거대 전력 연계 시스템 상에서 중요도가 증가하고 있는 HVDC (High-Voltage

Direct-Current) 송전 시스템을 고려해 보자.

HVDC 송전의 목적은 장거리 대용량 전송, 격리된 대규모 교류 송전 계통 사이의 연계, 비동기 연계 등에 있다. 또 AC 송전과 병렬 연결된 HVDC link는 HVDC의 장점과 AC 설비를 이용한 송전단과 수전단 사이의 부하 공급 능력 결합을 이용하여 외란 시 전력 조류(power flow)의 목적으로 이용될 수 있다. 따라서 이러한 목적상의 각종 scheme에 대한 포괄적인 신뢰도 평가 절차의 필요성이 제기되고 있다. 이 HVDC 시스템의 신뢰도는 1개 혹은 다수 개의 지표로 예측되는 데 가장 일반적인 것들로는 availability와 송전 capacity-level에 따르는 performance를 들 수 있다. 다음 그림 2에 HVDC 시스템의 한 예를 나타내었는데 2개의 AC와 1개의 bipolar DC link로 구성된 병렬 AC/DC 전송계통이다.

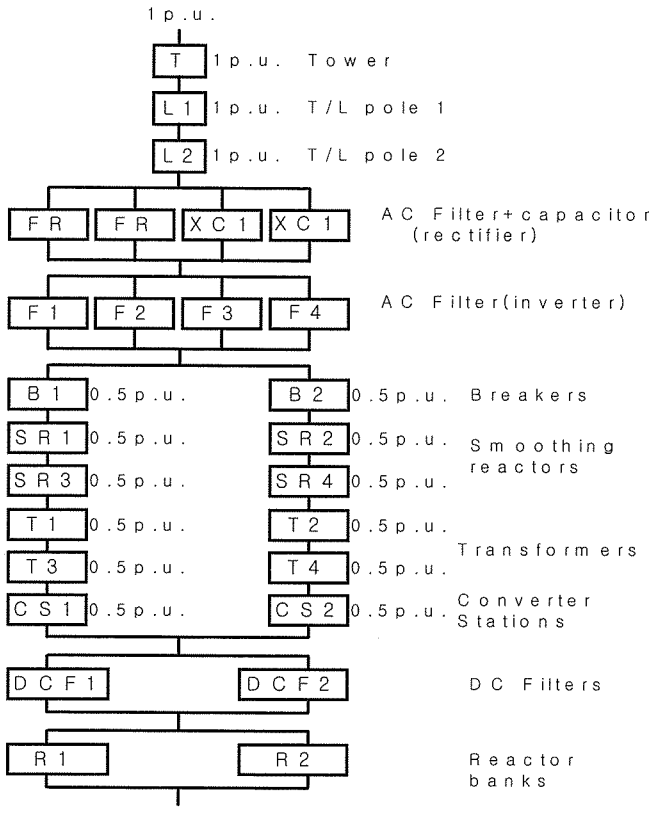


(그림 2) HVDC 시스템의 예

이 시스템의 운용상의 기본적인 평가는 이 시스템이 필요시 (즉, 두 전력 계통 지역간에 전력 수수가 필요하게 될 때) 즉시 운용될 수 있는 상태에 있는 가 하는 것과 만약 component가 고장시에도 어느 정도까지 전력전송이 가능한가 하는 것일 것이다. 첫 번째 항목은 RAMS 관점에서 보면 정상상태 availability(A_{SS})로 표시될 수 있고 두 번째는 performability와 관련된 항목으로써 이 HVDC 시스템에서는 capacity-level로 표시 가능하다. 이를 위한 평가 모델은 다음 그림 3과 같이 나타낼 수 있다 [5].

그림 3의 평가 모델을 바탕으로 한 해석은 SHARPE[3]나 Isograph[6] 등과 같은 다양한 tool을 이용하면 쉽게 가능하다. 그 결과의 한 예가 다음 표 1에 표시되어 있는 데 performance level은 capacity와 관련되어 짐을 알 수 있다. 이 표에서 나타난 이 시스템을 평가해 보면 예를 들어 이 시스템이 100MW(50% 정격)이상을 전송할 수 있는 availability는 99.8% 이상임을 보여주고 있다.

이 HVDC의 설계와 관련된 사항으로는 위의 예에서와 같이 이 HVDC 시스템이 적용되어 기본적으로 꼭 보장해야 할 capacity-level과 그에 따른 A_{SS} 등이 하나의 주요 평가지수로 사용될 수 있다. 이러한 조건에 따르는 설계기법에 관한 연구는 현재 진행 중이다.



(그림 3) HVDC 시스템 평가를 위한 모델

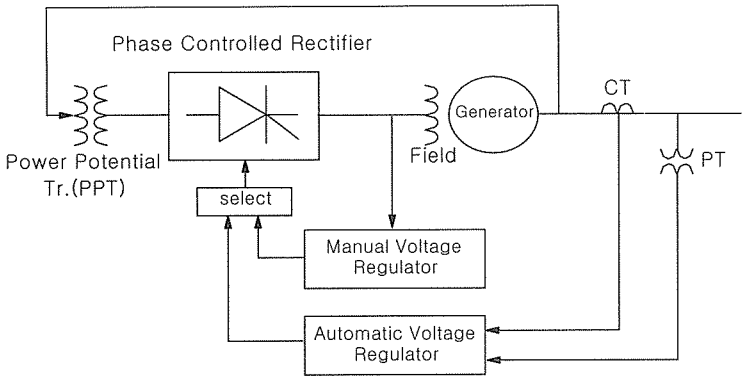
〈표 1〉 HVDC 시스템 평가 예

Performance Level	Capacity[MW]	*Ass*
100%	200	0.972728428
80%	160	5.34466E-06
63%	126	7.34157E-12
60%	120	0.001002474
50%	100	0.025201308
37%	74	0.000411650
22%	44	9.89198E-08
0%	0	0.000650696

나. 시스템 설계 예(발전소용 여자 제어 시스템)

두 번째의 예로는 발전소의 동기발전기의 여자 제어 시스템 설계에 관한 것이다. 전력계통에 연결되어 있는 수많은 수용가들에게 고품질 고신뢰 의 전력을 공급하기 위해서는 발전소의 전력 생산

설비는 고신뢰성이 요구된다. 이 고신뢰 발전 시스템의 요건에 핵심적인 부분의 하나가 여자제어 시스템이다. 이 여자 제어 시스템 구조의 한 예를 다음 그림 4에 나타내었다.



(그림 4) 여자 제어 시스템 예

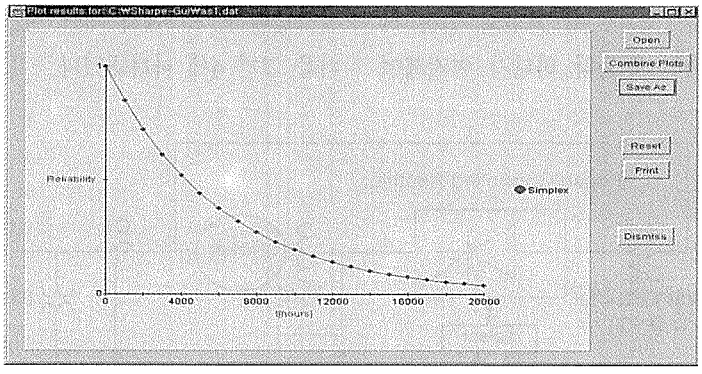
이 제어기의 설계 과정을 그림1에서 나타낸 과정의 단계별로 구분하여 살펴보자.

(1) 설계상의 제어대상은 500MW급 화력발전소이며 특징은
- 104 디지털 I/O 단자와 68 아날로그 단자를 필요로 하며 이 중 50개는 critical이고 나머지 122개는 noncritical 형식이다. EH 4개의 통신 포트가 필요하다.
- 구동부(actuator)는 static형인 phase-controlled rectifier이다.
- PID 제어 루프를 가지며 4millisecond의 샘플링 주기와 0.5%이내의 제어 정도가 요구된다.
- RAMS와 관련된 평가지수로는 reliability가 2년의 기간에 대해 0.99이상 보장되어야 한다.

(2) 위에서 설명한 기능을 수행하기 위해서 모든 component는 COTS(commercial-off-the-self) 기반의 component pool에서 선택한다는 원칙하에서 다음과 같은 구조가 채택된다.
- Simplex 디지털 제어기로서 VMEbus 구조를 기반으로 구성한다.
- 1 CPU 모듈
- 1 analog-to-digital 변환기 모듈(32 단자)
- 2 digital 입력 모듈 (총 64 단자)
- 1 counter/timer 모듈 (PCR firing 신호 발생용)
- 1 digital 출력 모듈 (40 단자)
- 1 통신 모듈 (2 RS-422, 2 RS-485).

(3) 위 구조에 대한 가능성을 검토하기 위해 간단히 reliability를 테스트한 결과는 다음 그림 5와 같이 나타난다.

그림에서 알 수 있는 바와 같이 위에서 선택한 시스템 구조로는 0.99이상의 reliability는 오직 61시간 정도 이내로 나타난다. 이 경우 제어기의 요구 설계 조건과는 너무나 차이가 많이 남을 알 수 있다. 여러 가지의 보다 고신뢰성을 가진 모듈



(그림 5) 초기 평가 결과

들을 이용한다고 하더라도 요구 조건의 충족은 불가능한 것으로 판단된다. 따라서 이 경우 우리는 기본적인 구조를 변경하는 방법을 선택함에 의해서 이 문제의 해결을 시도한다. 즉, simplex 구조상의 한계를 다음 그림 6에 나타낸 것과 같은 3중화 구조를 선택함에 의해 극복한다.

(4) 이 구조상의 상세 설계상의 특징의 주요 부분은 다음과 같다.

- 세 단위 제어기간의 상호 작용을 최소화하기 위해 비동기 구조를 가지며 최종 동기는 voter에서 이루어진다.
- Majority voting mechanism과 함께 "heartbeat"라는 신호를 이용하여 각 단위 제어기의 상태를 상호 인식하게 한다.

이러한 구조에 의해 이 3중화 제어기는 최악의 경우 하나의 단위 제어기만으로도 계속적인 동작이 가능하며 기본적으로 운전 중 고장난 단위제어기의 수리가 가능하다는 특징이 있다.

(5) 이 3중화 제어 시스템에 대한 reliability 해석 결과는 다음 그림 7과 같이 나타난다.

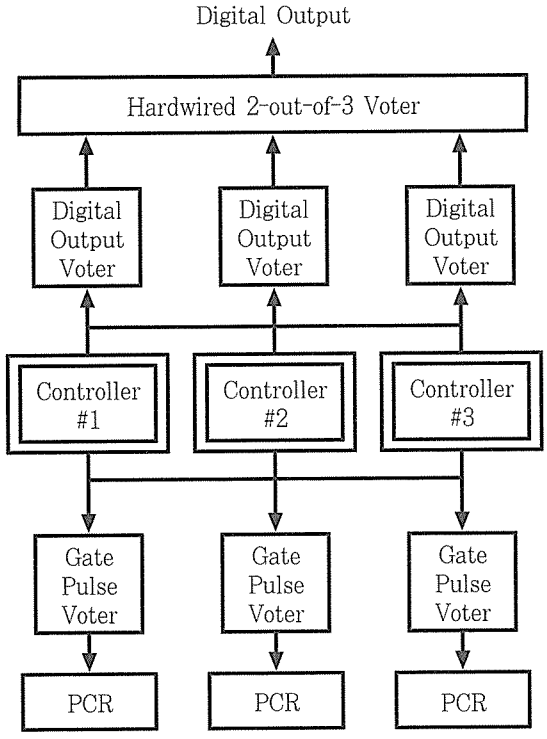
그림에서 보면 이 제어 시스템의 경우 0.99이상의 reliability를 2.5년 이상 유지함을 알 수 있다. 또한 4000시간 운전시간에 대해서도 0.999이상의 reliability를 나타냄을 주목하라. 결론적으로 제어기의 구조를 바꿈에 의해 상용(COTS) 모듈로도 아주 높은 RAMS를 성취할 수 있음을 알 수 있다.

(6) 위에서 설계된 제어기는 실제 제작 및 시험을 거쳐 현재 5세트가 현장에서 상용 운전되고 있다 [4],[7].

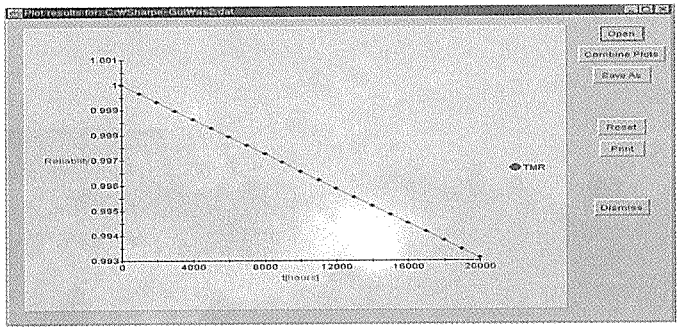
참고로 위의 시스템의 MTTF(Mean-Time-To-Failure)는 약 12×10^6시간으로 나타났다.

4. 결론 및 앞으로의 방향

이제까지 간략하게 소개한 고신뢰도 제어 기술은 원자력 발전설비, 화력 발전설비, 화공 플랜트 등과 같은 대형 플랜트, 철도, 항공·우주 산업 등과 같은 첨단 산업 관련 기술 등에서 핵심적인 기술의 한 분야이다. 지금 외국의 관련 기술의 추세는 재래의 고유브랜드 형태의 customized 시스템 기술에서 벗어나 COTS 제품에 기반을 둔 보다 개방된 시스템 구조 형태로 발전하고 있다. 따라서 이 경우에의 핵심 기술은 재래와 같은 compo-



(그림 6) 3중화 여자 제어 시스템



(그림 7) 3중화 시스템의 reliability

nent 기술이 아니라 설계 및 integration 기술이 그 핵심이 되며 특히 시스템 내부의 S/W의 비중이 높아감에 따라 S/W의 V&V 등이 기술발전의 관건이 되고 있다. 또한 앞에서의 여자 제어 시스템의 예에서 알 수 있었던 바와 같이 COTS 제품을 기반으로 한 시스템 설계에서의 신뢰성의 향상

은 하드웨어관련 기술로는 한계가 있다. 따라서 추후의 연구 방향은 초고신뢰 시스템 설계 기술 개발을 위해서는 하드웨어의 최적설계와 병행하여 관련 S/W 기술의 최적화를 통한 신뢰성 향상 기술 개발에 중점이 두어질 것으로 생각된다 .

참고문헌

[1] B. W. Johnson, *Design and Analysis of Fault-Tolerant Digital Systems*, Addison-Wesley Publishing Company, 1989

[2] R. Sahner and K. S. Trivedi and A. Puliafito, *Performance and Reliability Analysis of Computer Systems*, Kluwer Academic Publishers, 1996

[3] K. S. Trivedi, *"SHARPE Interface" User's Manual Version 1.01*, Duke University, 1999

[4] KERI Report, *A study on Environmental Testing of Digital Excitation System*, 1997

[5] "Incorporating a DC Link in Composite System reliability Evaluation", M. Fotuhi-Firuzabad, R. Billinton, S.O. Faried, 2000 IEEE PES Power Meeting, Singapore.

[6] Isograph, "AvSim+ for Windows 95 and Windows NT, Version 7.0, User Manual."

[7] 한국전기연구원 보고서, "발전기 여자 제어 시스템 개발," 1998.