技術解說

고장허용 전산체제

조 정 완*

——차 례——

1. 서 론

컴퓨터가 다양한 목적에 이용됨에 따라 신뢰도가 높은 즉 고장허용의 전산체계의 필요성은 증가되고 있다. 임상응용의 경우 컴퓨터의 오동작은 치명적일 수 있고 또 공정제어의 경우 귀중한 자원의 막대한 손실을 초래할 수 있다. 따라서 고장허용의 전산체계에 관한 연구는 필연적이다.

역사적으로 최초의 고장허용의 전산체계는 SAGE와 같은 군사적인 응용에 시도하였다. 2절에서는 이러한 신뢰도가 높은 기계의 시험적인 결과와 실제 운영의 경험에 입각한 고장허용의 전산체계의 설계원리를 논한다. 이어서 3절에서는 현재까지 설계된 고장허용 전산체계의 구조를 기술하며 4절에서는 현재까지 범용의 컴퓨터에 사용한 고장허용 기법을 소개한다.

2. 설계 원리

고장허용의 혹은 고장진단이 용이한 전산체계의 설계원리는 많이 발표되어 있다[9),16)]. 이러한 설계원리들은 일부는 실제 동작하는 컴퓨터의 경험에서 얻은 것들[16),17)]과 실험적 연구의 결과들[9),17),19)]이다.

최초의 설계원리는 redundancy기법으로서 고장진단의 편의를 위하여 각 소자단위의 redundancy 보다도 module단위의 redundancy기법이 많이 보급되었다. 따라서 논리회로 단계에서는 고도로 신뢰성있는 부품들과 설계방식이 요구되어 심지어 Manning[19)]은 고장진단이 용이하게 하기 위하여 pulse보다는 Level신호를 사용하는 비동기회로의 사용을 주장하였다.

물론 씨스템 단계에서는 modularity의 정도가 높은 것이 요망되며 module간의 상호연결 회선수가 작으며 적당한 곳에 test point의 설정이 요망된다.

*정회원 : 한국과학원교수·공학박사(당학회 편수위원)

3. 고장허용 전산체제의 구조

(가) 일반적인 고찰

현재 사용되고 있는 고장허용 전산체제의 구조는 대략 3가지가 있다. 첫째번 구조는 fault masking이라 하며 기계의 일부분에 고장이 있을 때에도 정상동작을 유지하도록 하는 구조이다. fault masking은 3중중복회로(TMR)와 다수결회로(majority voter)로 구성되어 있으며 3중중복회로 중에서 임의의 2개이상의 회로가 고장이 아니면 결과는 정상적으로 얻을 수 있도록 된 회로이다. 이러한 구조를 가진 컴퓨터에는 SATURN V[3)], NASA의 modular컴퓨터[8)], STAR컴퓨터[7)] 등이 있다. 이중에서 특히 STAR컴퓨터에서는 이의 시험 및 수리기(TARP)에 TMR을 적용하고 있다.

가장 많이 사용되고 있는 구조는 둘째번 구조인데 이것은 error switching이라 한다. 이 구조에서는 하나의 기계가 동작하고 있으며 이와 동일한 기계 한개 이상이 대기하고 있는 구조이다. 경우에 따라서 대기하고 있는 기계는 완전히 정지상태로 대기하거나[7)] 혹은 다른 중요하지 않은 처리를 하면서 대기할 수도 있다[4)]. 물론 본래의 기계에 고장이 발생시 대기 기계가 계속 처리를 하여 주고 본래의 기계는 고장진단을 위하여 off-line으로 한다. 이러한 구조는 장기에 걸쳐서 고도의 신뢰도가 요구되는 응용에 사용되었으며 그 예로는 No. 1 ESS[1)]와 STAR가 있다. No. 1 ESS의 경우 40년간의 신뢰도가 요구되었으며 STAR의 경우 10년간의 신뢰도가 요구되었다. error switching구조는 SAGE[1)]나 SABRE[2)]와 같이 상당히 오래된 기계에 이용하였으나 STAR나 No. 1 ESS와 같은 근대의 기계에도 이용하였다는 것은 특기할 만한 사실이다.

세째번째 구조는 LSI기술의 개발과 마이크로프로그램 기법의 발전에 기인한 것으로서 위축시킬 수 있는 다중처리(degradable multiprocessing) 방식이다. 이 구조에는 몇가지 방식이 있는데 이중에서 대표적인 것

으로는 NASA의 modular컴퓨터와 같이 여러개의 처리장치가 다중처리를 하다가 1개의 처리장치에 고장이 발생할 경우 그 처리장치를 제외한 나머지로서 위축된 동작을 계속할 수 있는 구조가 있다. 다른 방식으로는 RCA의 VIC[5]와 Model 215[6]와 같이 마이크로프로그램된 기계로서 마이크로프로그램의 알고리즘을 변환하여 고장난 부분의 사용을 회피하도록 하는 구조가 있다.

(나) Fault Masking 컴퓨터

ㄱ. SATURN V[3]

SATURN V 컴퓨터는 SATURN유도탄 유도장치의 일부분으로서 A/D와 D/A변환기를 통하여 유도장치와 연결되어 있다.

이 체제에서 컴퓨터와 A/D 및 D/A변환기는 TMR과 majority voter 그리고 disagreement탐지기 형식으로 구성되어 있고 만일 disagreement가 탐지될 경우 지상에 있는 통제부에 이 결과를 송신하여 TMR형태를 유지할 것인가 혹은 고장부분을 제거하고 simplex로 동작시킬 것인가를 결정하도록 한다. 이 컴퓨터에서 기억장치에는 TMR을 사용하지 않고 duplex로 구성되어 있어서 각 module은 동일한 자료를 기억하고 있다. 이 기억장치의 고장 진단은 parity검사에 의하며 한 module의 고장이 발견되면 새로운 module을 연결한다. SATURN V의 MTBF는 45,000시간이다.

ㄴ. STAR[7]

STAR컴퓨터의 기본적인 원리는 error switching이며 이에 관하여는 후에 기술한다. 그러나 이 컴퓨터의 TARP는 TMR과 majority voter 그리고 spare module 형태이다. TARP의 주 목적은 고장후 복구 그리고 나머지 부분에 clock과 동기용 pulse를 발생하는 것이다. 만일 TARP의 고장이 발견될 경우 고장부분을 제거하고 새로운 것을 연결하여 다시 TMR을 형성한다.

(다) Error Switching 컴퓨터

ㄱ. SAGE[1]

SAGE는 1950년대에 국방부와의 계약에 의하여 IBM이 제작한 방공자료 처리용 컴퓨터체제이다. SAGE는 FSQ-7이라는 컴퓨터가 주축을 이루고 있으며 고장발견시 대기하고 있는 컴퓨터가 자료처리를 계속하고 고장난 컴퓨터의 고장진단을 시작한다.

ㄴ. SABRE[2]

SABRE는 1960년대에 American Airlines와 IBM 공동으로 개발한 비행기 좌석예약용 전산체제이다. 기본적인 컴퓨터는 2개의 IBM 7090과 통신을 위한 자기 drum이다. SAGE와 같이 하나의 컴퓨터는 본래의 좌석예약 업무를 처리하고 다른 컴퓨터는 대기한다.

ㄷ. No. 1 Ess[4]

No. 1 Ess는 1960년대에 Bell연구소에서 개발하고 Western Electric에서 제작한 컴퓨터 제어에 의한 전화교환 체제이다.

SAGE나 SABRE와 같이 이 전산기에 의한 제어체제도 2중전산체제이다. 그러나 No.1 ESS는 Subsystem 단계에까지 error switching을 도입한 기계로는 처음이다. 이 전산체계는 2중의 processor와 matching회로 그리고 프로그램 기억장치와 호출 혹은 데이타 기억장치 그리고 전화교환용의 특수한 주변접합기로 구성되어 있으며 기억장치와 주변장치용의 bus들은 모두 2중으로 되어 있다. 이 전산체계에서 고장발견을 위하여는 두가지 방법을 사용한다. 첫째로는 두개의 processor를 모두 사용하여 matching회로를 이용하는 방법이고 둘째 방법은 error code를 사용하는 것이다.

ㄹ. STAR[7]

STAR는 NASA와의 계약에 의하여 JPL이 제작한 컴퓨터이다. STAR의 주목적은 장기간의 무인조종의 우주비행에의 응용이다. 이 컴퓨터에서는 error switching, error coding과 fault masking방식을 혼용하였다. 이 컴퓨터의 기본적인 이념은 고장을 검출하여 수선하여 고장발생시의 계산을 반복하므로서 고도의 정확성을 유지하는 것이다. 이러한 기능은 TARP가 가지고 있다. ESS와 같이 STAR는 module로 구성되어 있으며 module단위로 switching이 가능하다. 그러나 ESS와는 달리 대기하고 있는 module들은 전원이 공급되어 있지 않은 상태로 대기한다. 그리고 ESS와는 달리 고장검출을 위하여는 arithmetic code를 사용한다. 기억장치로는 극히 소중한 자료들은 2중 혹은 3중의 기억장치에 보관한다.

(라) Degradable Processing

ㄱ. VIC[5]

VIC-36A는 국방부와의 계약에 의하여 RCA가 1965년경에 제작한 컴퓨터이다. 이 컴퓨터는 마이크로프로그램의 제어기능을 갖인 컴퓨터로서 기억장치와 register들은 2중으로 되어 있다. 이 컴퓨터의 특징은 어느 회로부분의 고장이 발생시 그 부분을 사용하지 않는 마이크로프로그램된 알고리즘을 이용하여 다소 위축된 기능으로라도 동작을 계속하도록 하는 것이다. 따라서 하드웨어의 중복을 피할 수 있으므로 비용을 줄일 수 있다는 특징이 있다.

ㄴ. RCA Model 215[6]

Model 215는 VIC을 개량한 것으로 1960년대 후기에 RCA에서 제작한 것이다.

M 215는 2개의 완전한 processor가 공동의 기억장치를 갖고 있는 체제이다. 정상적인 운영을 할 때에는 두개의 processor가 독립된 기능을 하고 있으나 일단 어느 processor에 고장이 발생하면 그 processor를 제거하고 단일 전산체제로서 운영된다.

ㄷ. Modular 컴퓨터[8),10)]

Modular 컴퓨터는 NASA와의 계약에 의하여 Hughs가 설계한 것이다. 이는 주로 LSI부품으로 제작하였으며 이 컴퓨터는 우주선 유도용으로 제작되었다. 이 전산체제는 3개의 컴퓨터로 구성되어 있으며 이들 각 컴퓨터는 각각 독립된 연산, 제어, 기억, 입출력 module들로 구성되어 있다. 이 체제는 지극히 높은 신뢰도를 요구하는 시간에는 TMR형태로 운영되며 이 시간이 지나면 오직 하나의 컴퓨터만이 운영된다. 그리고 이 체제에는 CAU가 있어서 만일 컴퓨터내의 고장이 각 컴퓨터마다 서로 다른 module에 있을 때에도 각 컴퓨터로부터 정상적인 module들만 모아서 하나의 정상동작을 할 수 있는 컴퓨터를 형성할 수 있다.

ㄹ. Hopkins[9)]

Hopkins는 1970년대 초반에 MIT의 A.L. Hopkins가 NASA와의 계약에 의하여 수행한 고장허용 전산체제에 관한 연구결과이다. 이 기계는 실제로 제작되지는 못하였으나 우주선에 사용하기 위하여 여러개의 작은 processor들로 구성되어 있다. 이 컴퓨터는 6~9개의 processor들로 구성되어 있으며 time share된 bus를 통하여 기억장치를 공유한다. 각 processor들은 2중의 CPU와 match회로 TMR형태의 buffer를 갖고 있다. processor의 동작은 계산과 저장 2단계로 구분되어 계산시에 고장이 발생할 경우 scratch pad에 저장된 내용 즉 고장발생이전의 상태를 기억장치로 보내어 다른 processor로 하여금 정상동작을 계속하도록 한다.

ㅁ. D825[11)]

D825는 degradable 다중처리 전산체계로는 제일 처음 제작한 것으로서 1960년대 초기에 국방부의 계약에 의하여 Burroughs가 제작한 것이다. 이 전산체계는 몇개의 범용컴퓨터와 기억장치 module들과 주변장치들이 cross bar switch로 연결되어 있다. 어느 module에도 고장허용을 위한 특별한 회로는 없으나 어느 module이든지 서로 연결이 가능하므로 앞서 논한 고장허용 전산체계에 속한다. 즉 한 processor 혹은 임의의 module에 고장이 발생시 그와 같은 기능을 가진 다른 module을 연결함으로 정상동작을 계속할 수 있다. 이 컴퓨터의 processor들은 stack processor라는 특징이 있다.

(마) 고장진단이 가능한 컴퓨터

IBM의 DX-1[15)]은 고장허용 전산체계는 아니나 제 자신이 고장진단을 할 수 있다는 특징이 있다. DX-1은 IBM이 1960년대 중반에 설계하고 제작은 하지 않은 컴퓨터이다. 이 컴퓨터의 기본 이념은 자체 고장진단력을 최대로 하며, MTTD를 최소화하며, 하드웨어 보강을 최소화하고 hardcore를 최소로 줄이는 것이다. 이 컴퓨터 고유의 고장진단은 8-bit짜리 기계 전체를 4-bit짜리로 나누어서 두개의 독립된 기계로 사용할 수 있도록 한 것이다. 이 컴퓨터가 정상동작을 할 경우에는 8-bit기계로 동작하며, 고장발생시에는 4-bit짜리 기계 2개로서 동작하여 그중 하나가 다른 부분을 시험하도록 한다.

4. 범용 컴퓨터의 고장허용

(가) 일반적인 고찰

일반적으로 범용 컴퓨터에서 고장허용체제는 그다지 많이 요구되지 않았다. 그것은 고장이 의심될 경우 컴퓨터 보수요원이 diagnostic 프로그램의 도움으로 고장을 진단하고 수선하며 이 경우 job의 turn-around 시간에 영향을 미칠 뿐이기 때문이다. 따라서 우주비행, 방어, 공정제어와 같은 응용과는 차이점이 많다.

(나) 초창기

1세대 컴퓨터는 진공관이나 diode로 된 논리회로로 만들었으므로 그 신뢰도는 매우 낮았다. 따라서 고장진단을 도울 수 있는 기능이 요구되었다. 예를 들면 UNIVAC I[11)]은 연산기와 제어기를 2중으로 하고 match회로를 두어서 고장발생시 정지하도록 하였고 기억장치와 bus에는 parity를 사용하고 주기적으로 기억장치 전부를 시험하였다.

(다) 중반기

2세대 컴퓨터부터는 부품의 신뢰도가 좋아짐에 따라 완전한 2중회로의 필요성은 없어졌다. 예를들면 IBM의 Stretch[11)]는 연산기만 2중으로 하고 error code와 계산후 비교하는 회로를 도입하였다. 1950년대 중반기에는 기억장치와의 데이타 전송에는 error code를 사용하는 것이 거의 표준에 가까웠다. 또 이 시대의 컴퓨터들은 제어회로의 중복보다도 overflow나 underflow, floating point수의 연산에서 지수부분의 유효여부 등의 시험 등과 같은데 더 치중하였다. 중반기에 또한가지 특기할 만한 것은 고장을 검사하여 발견하고 실제 고장부분을 찾는 방법이 상당히 진보되어 고장수선이 신속하여졌으므로 down time이 줄어들었다.

(라) 현　　재

근대에 들어와서 집적회로의 발달로 인하여 부품의

신뢰도는 상당히 개량되었고 따라서 전산체제는 성능이 좋아졌고 그 구조는 매우 복잡하게 되었다. 따라서 전산체제의 가격이 매우 높아져서 장기간의 down time을 불허한다. 이러한 시점에서 전산체계는 modular 형의 다중처리형식이 많이 이용되고 있다. 이러한 체제는 한개 혹은 몇개의 module에 고장이 있더라도 전산체제 전체가 그 기능을 멈추는 것이 아니라 위축된 형태로라도 그 기능을 살릴 수 있기 때문이다. 이러한 컴퓨터의 대표적인 것은 하나의 커다란 중앙연산장치에 여러개의 주변 processor들이 부착되어 있는 CDC 6600[11], CDC 7600[12] 그리고 3개의 CPU가 다중처리 형태로 동작하는 UNIVAC 1108[13]이 있다.

참 고 문 헌

1) R.R. Everett, C.A. Zraket and H.D. Benington, "SAGE-A Data Processing System for Air Defense," Eastern Joint Computer Conf. Proc., 1957, pp. 148~155.
2) W.R. Plugge and M.N. Perry, "American Airlines' SABRE Electronic Resevation System," Western Joint Computer Conf. Proc., 1961, pp. 593~601.
3) M.M. Dickinson, J.B. Jackson and G.C. Randa, "SATURN V Launch Vehicle Digital Computer and Data Adaptor," FJCC Proc., 1964, p. 501.
4) R.W. Downing, J.S. Nowak and L.S. Tuomenoksa, "No. 1 ESS Maintenance Plan," BSTJ, Vol. 43, Sept. 1964, pp. 1961~2019
5) H.A. Miller, "Reliability Aspects of the Variable Instruction Computer," IEEE Trans. on Elect. Computers, Vol. EC-16, No. 5, Oct. 1967, pp. 596~602.
6) E.J. Dietrich and L.C. Kaye, "A Compatible Airborne Multiprocessor," FJCC Proc., 1969, pp. 347~357.
7) A. Avizienis, G.C. Gilley, F.P. Mathur, D.A. Rennels, J.A. Rohr and D.K. Rubin, "The STAR(Self-Testing-And-Repairing) Computer: An Investigation of the Theory and Practice of Fault-Tolerant Computer Design," IEEE Trans. on Computers, Vol. C-20, No.11, Nov. 1971, pp. 1312~1321.
8) J.J. Pariser and H.E. Maurer, "Implementation of the NASA Modular Computer with LSI Functional Characters," FJCC Proc. 1969, pp. 231~245.
9) AL. Hopkins, "A Fault-Tolerant Information Processing Concept for Space Vehicles," IEEE Trans. on Computers, Vol. C-20, No. 11, Nov. 1971, pp. 1394~1403.
10) F.D. Erwin and E. Bersoff' "Modular Computer Architecture Strategy for long Term Missions," FJCC Proc., 1969.
11) C.G. Bell and A. Newell, Computer Structures: Readings and Examples, McGraw-Hill Book Co., N.Y., 1971
12) P. Bonseigneur, "Description of the 7600 Computer System," Computer Group News, May, 1969, pp. 11~15.
13) D.C. Stanga, "Univac 1108 Multiprocessor System. SJCC Proc., 1967, pp. 67~74.
14) IBM Systems Reference Library-IBM S/360 Principles of Operation, Manual 5360~01, June 1970.
15) R.E. Forbes, D.H. Rutherford, C.B Stieglitz and L.H. Tung, "A Self Diagnosable Computer," FJCC Proc., 1965, pp. 1073~1086.
16) H.Y. Chang and J.M. Scanlon, "Design Principles for Processor Maintainability in Real Time Systems," FJCC Proc., 1969, pp. 319~328.
17) A. Avizienis, "Design of Fault-Tolerant Computers," FJCC Proc., 1967, pp. 733~743.
18) R.A. Short, "The Attainment of Reliable Digital Systems Through the use of Redundancy-A Survey," Compute Group News, Mar. 1968, pp. 2~17.
19) E. Manning, "On Computer Self-Diagnosis: Part II-Generalizations and Design Principles," IEEE Trans. on Computers, Vol. EC-15, Dec. 1966, pp. 882~891.