(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년01월25일
(11) 등록번호 10-1010801
(24) 등록일자 2011년01월18일

(51) Int. Cl.
G06F 11/30 (2006.01) *G06F 13/28* (2006.01)
G06F 13/36 (2006.01) *H04L 9/00* (2006.01)
(21) 출원번호 10-2005-7022711
(22) 출원일자(국제출원일자) 2004년04월30일
심사청구일자 2009년04월10일
(85) 번역문제출일자 2005년11월28일
(65) 공개번호 10-2006-0032954
(43) 공개일자 2006년04월18일
(86) 국제출원번호 PCT/US2004/013369
(87) 국제공개번호 WO 2004/107176
국제공개일자 2004년12월09일
(30) 우선권주장
10/448,031 2003년05월29일 미국(US)
(56) 선행기술조사문헌
US6021455 A
US7073059 A
전체 청구항 수 : 총 5 항

(73) 특허권자
프리스케일 세미컨덕터, 인크.
미국 텍사스 오스틴 윌리암 캐논 드라이브 웨스트 6501
(72) 발명자
모이어, 윌리암, 씨.
미국 78620 텍사스주 드리핑 스프링스 피어 브랜치 로드 1005
맬리크, 아프잘, 엠.
미국 78759 텍사스주 오스틴 에이피티. 517 그레이트 힐스 트레일10050
(74) 대리인
주성민, 이중희, 백만기

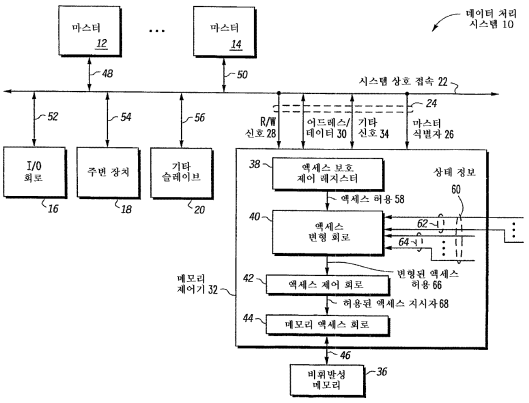
심사관 : 이경홍

(54) 액세스 허용을 결정하는 방법 및 장치

(57) 요 약

본 발명의 액세스 보호(96)를 결정하는 방법 및 장치는 다수의 마스터들(12,14)에 대응하는 다수의 액세스 요청(84)의 수신, 액세스 허용(86)의 결정, 상태 정보의 제공(60), 액세스 요청(84)에 근거하는 액세스 허용(86) 및 상태 정보(90)에 근거하는 선택적인 변형을 포함한다. 상태 정보(60)는 디버그 동작, 비보안 또는 비검증 메모리들로부터의 동작, 메모리 프로그래밍, 직접 메모리 액세스 동작, 부트 동작, 소프트웨어 보안 검증, 보안 레벨, 보안 모니터 동작, 동작 모드, 결함 모니터, 외부 버스 인터페이스 등(88)과 관련될 수 있을 것이다.

대 표 도



특허청구의 범위

청구항 1

제1 버스 마스터에 대응하는 제1 액세스 허용 정보를 저장하는 제1 액세스 보호 회로와,

제2 버스 마스터에 대응하는 제2 액세스 허용 정보를 저장하는 제2 액세스 보호 회로와,

상기 제1 및 제2 액세스 보호 회로에 결합되는 액세스 변형 회로와,

상기 액세스 변형 회로에 의해서 제공되는 액세스 허용 지시자를 포함하고,

상기 제1 버스 마스터에 의한 제1 액세스에 응답하여, 상기 액세스 변형 회로는 제1 상태 정보 및 상기 제1 액세스 허용 정보를 수신하며,

상기 제1 상태 정보에 기초하여 상기 액세스 변형 회로는 상기 제1 액세스 허용 정보를 선택적으로 변형하여 제1 변형 액세스 허용 정보를 생성하며,

상기 제1 변형 액세스 허용 정보는 상기 액세스 허용 지시자가 상기 제1 액세스를 허용하는지 여부를 판정하는데에 이용되며,

상기 제2 버스 마스터에 의한 상기 제2 액세스에 응답하여, 상기 액세스 변형 회로는 제2 상태 정보 및 상기 제2 액세스 허용 정보를 수신하며,

상기 제2 상태 정보에 기초하여, 상기 액세스 변형 회로는 상기 제2 액세스 허용 정보를 선택적으로 변형하여 제2 변형 액세스 허용 정보를 생성하며,

상기 제2 변형 액세스 허용 정보는 상기 액세스 허용 지시자가 상기 제2 액세스를 허용할 것인지 여부를 판정하는 데에 이용되며,

상기 제1 상태 정보 및 상기 제2 상태 정보는 상이한 소스(soruce)에 의해 제공되는 액세스 허용 회로.

청구항 2

제1항에 있어서,

상기 제1 상태 정보는 상기 제1 버스 마스터의 신뢰성을 나타내는 액세스 허용 회로.

청구항 3

제1항에 있어서,

상기 제1 상태 정보는 부트(boot) 동작과 관련되는 액세스 허용 회로.

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

제1 마스터에 대응하는 제1 액세스 요청을 수신하는 단계와,

상기 제1 마스터에 대응하는 제1 액세스 허용을 결정하는 단계와,

제1 상태 정보를 수신하는 단계와,

상기 제1 상태 정보에 기초하여 상기 제1 액세스 허용을 선택적으로 변형하는 단계와,

제2 마스터로부터 제2 액세스 요청을 수신하는 단계와,

상기 제2 마스터에 대응하는 제2 액세스 허용을 결정하는 단계와,

제2 상태 정보를 수신하는 단계와,

상기 제2 상태 정보에 기초하여 상기 제2 액세스 허용을 선택적으로 변형하는 단계를 포함하며,

상기 제1 상태 정보는 상기 제2 상태 정보와는 상이한 소스로부터 제공되는 액세스 보호 결정 방법.

청구항 10

제1 마스터에 대응하는 제1 액세스 요청을 수신하는 단계 - 상기 제1 액세스 요청은 슬레이브 장치에 대한 것임 - 와,

제1 상태 정보를 제공하는 단계와,

상기 제1 액세스 요청에 기초하여 제1 액세스 허용을 결정하는 단계 - 상기 제1 액세스 허용은 상기 제1 마스터가 상기 슬레이브 장치를 액세스하도록 허용하는지 여부를 나타냄 - 와,

상기 제1 상태 정보에 기초하여 상기 제1 액세스 허용을 선택적으로 변형하는 단계와,

제2 마스터에 대응하는 제2 액세스 요청을 수신하는 단계 - 상기 제2 액세스 요청은 상기 슬레이브 장치에 대한 것임 - 와,

제2 상태 정보를 제공하는 단계와,

상기 제2 액세스 요청에 기초하여 상기 제2 액세스 허용을 결정하는 단계 - 상기 제2 액세스 허용은 상기 제2 마스터가 상기 슬레이브 장치를 액세스하도록 허용하는지 여부를 나타냄 - 와,

상기 제2 상태 정보에 기초하여 상기 제2 액세스 허용을 선택적으로 변형하는 단계를 포함하며,

상기 제1 상태 정보는 상기 제2 상태 정보와는 상이한 소스로부터 제공되는 액세스 보호 결정 방법.

명 세 서

[0001] 관련출원

[0002] 본 발명은 2002년 3월 8일 출원된 "Data Processing System with Peripheral Access Protection and Method Therefor"라는 발명의 명칭을 가지는 미국 특허 출원 제10/094,082호 및 2003년 3월 7일 출원된 "Data Processing System with Peripheral Access Protection and Method Therefor"라는 발명의 명칭의 미국 특허 출원 제10/384,024호와 관련되며, 이들은 모두 본원의 출원인에게 양도되었다.

기 술 분 야

[0003] 본 발명은 액세스 허용에 관한 것으로, 보다 구체적으로, 예컨대 데이터 처리 시스템 내에서의 액세스 허용을 결정하는 액세스 허용 회로에 관한 것이다.

배 경 기 술

[0004] 시스템 온 칩(system on chip, SoC) 솔루션에 있어서, 예컨대 메모리와 같이 공유되는 주변 및 슬레이브(slave) 장치들을 가지는 다수의 마스터(master)를 가지는 것은 통상적인 것이다. 공유된 주변 및 슬레이브 장치들 모두 또는 그 중 몇몇의 컨텐츠는 템퍼링(tampering), 모방 또는 시스템을 손상시킬 수 있는 소정의 마스터에서 실행되는 잘못되거나 혹은 적대적인 소프트웨어와 같은 가로채기(interrogation)에 대하여 보호될 필요가 있을

것이다. 예컨대, 시스템의 주변 및 슬레이브 장치들 내의 보안 정보에의 액세스를 획득하는 데에 이용될 수 있는 보안되지 않은 마스터 상에서 실행되는 소프트웨어에 의해서 바이러스가 유입될 수 있을 것이다. 더욱이, 시스템 내의 소정의 버스 마스터들은 보안이 이루어진 것으로 간주되고, 다른 버스 마스터들은 보안이 이루어지지 않은 것으로 간주될 수 있을 것이며, 이러한 고려는 시스템의 상태가 변경됨에 따라 변할 수 있을 것이다. 따라서, 시스템의 무결성과 보안을 위하여, 보안되지 않은 마스터 상에서 실행되는 잘못되거나 혹은 적대적인 소프트웨어로부터 시스템을 보호할 필요가 있다.

발명의 상세한 설명

[0010] 본 명세서에서 이용되는 "버스"라는 용어는 데이터, 어드레스, 제어 또는 상태와 같은 하나 이상의 다양한 타입의 정보를 전송하는 데에 이용될 수 있는 복수의 신호들 또는 도전체들을 일컫는 데에 이용된다. 본 명세서에서 논의되는 도전체들은 단일의 도전체, 다수의 도전체들, 단방향 도전체들 또는 양방향 도전체들을 일컫는 것으로 도시되거나 기술될 수 있을 것이다. 그러나, 상이한 실시예들은 도전체의 구현을 달리할 수 있을 것이다. 예컨대, 양방향 도전체 대신에 별개의 단방향 도전체들이 이용될 수 있을 것이며, 그 반대로 이용될 수도 있을 것이다. 또한, 다수의 도전체들이 다수의 신호들을 직렬 또는 다중화된 방식으로 전송하는 단일 도전체로 대체될 수 있을 것이다. 마찬가지로, 다수의 신호들을 운반하는 단일의 도전체가 이들 신호들의 부분집합들을 운반하는 다양한 상이한 도전체들로 분리될 수 있을 것이다. 따라서, 신호들을 전송하는 데에는 많은 옵션들이 존재할 수 있을 것이다.

[0011] 시스템 무결성과 보안을 보장하기 위하여, 예컨대 다수의 마스터 데이터 처리 시스템과 같은 시스템이 보안되지 않은 프로세서 또는 다른 마스터에서 실행되는 잘못되거나 혹은 적대적인 소프트웨어에 의해서 위험에 노출되지 않도록 보장하는 것이 바람직하다. 예컨대, 다수의 마스터 시스템 내의 다수의 마스터들은, 예컨대 시스템의 주변 또는 슬레이브 장치와 같은 동일한 자원을 공유할 수 있을 것이다. 다수의 마스터들 중 몇몇은 보안이 이루어진 것으로, 다른 것들은 보안이 이루어지지 않은 것으로 간주될 수 있을 것이다. 본 명세서에서 사용된 보안 마스터는 통상적으로 보다 액세스가 용이하며 손상에 보다 영향을 많이 받는 비보안 마스터보다 통상적으로 적게 액세스가능하며, 보다 손상에 영향을 적게 받는 마스터를 일컫는다. 예컨대, 보안 마스터는 제한된 액세스를 가지거나 마스터 또는 SoC의 제조자에 의해서 전적으로 명령을 수행할 수 있을 것이다(즉, 보안 마스터 상에서 실행되는 소프트웨어는 신뢰되거나 보안 소프트웨어인 것으로 간주될 수 있을 것이다). 그러나, 비보안 마스터는 제3자 소프트웨어(예컨대, 사용자 개발 소프트웨어) 또는 (소프트웨어의 컨텐츠 및 함수가 일반적으로 알려지지 않은)임의의 다른 신뢰되지 않은 소프트웨어를 수신하고 실행할 수 있을 것이다. 소프트웨어가 신뢰되지 않았기 때문에, 잘못되거나, 시스템의 다른 부분을 손상시키려 하거나 보안 정보에의 액세스를 획득하려고 시도하는 적대적인 소프트웨어일 수 있을 것이다. 더욱이, 보안 또는 비보안으로서의 특정 마스터의 상태를 데이터 처리 시스템의 상태가 변경됨에 따라 변경할 수 있을 것이다.

[0012] 따라서, 본 발명의 일 실시예는 슬레이브 또는 비휘발성 메모리와 같은 주변 장치의 컨텐츠가 보안 상태에서 동작하는 때에는 비휘발성 메모리로부터 프로그램 실행이 진행되지만, 보안성이 보다 약한 상태에서 동작하는 때에는 권한없는 액세스가 발생하는 것을 방지하는 것을 가능하게 하는 방식으로 보안이 이루어지는 것을 가능하게 한다. 도 1 내지 3을 참조하여 아래에 기술될 바와 같이, 일 실시예는 시스템 상태가 이전에 프로그래밍된 데이터 처리 시스템의 액세스 보호 정책을 변경하거나 오버라이드(override)하는 것을 가능하게 하는 방법을 제공한다. 이러한 오버라이드는, 예컨대 각각의 마스터의 (예컨대, 슬레이브 장치, 주변 장치, 메모리, 공유 자원 등과 같은)시스템 자원에 대한 판독 및 기록 액세스를 함께 또는 독립적으로 제한하는 데에(또는 반대로 이러한 액세스 허용을 넓히는 데에) 이용될 수 있을 것이다. 더욱이, 이들 오버라이드는 상태 정보의 변경이 있는 때에 동적으로 변경될 수 있을 것이다. 또한, 아래에서 보다 상세히 기술될 바와 같이, 상태 정보는, 예컨대 디버그 모드의 인에이블, 비보안 또는 비검증 메모리 영역으로부터의 프로그램의 실행, 비휘발성 메모리의 일부의 재프로그래밍 등과 관련된 정보와 같은 데이터 처리 시스템의 상태와 관련된 임의의 타입의 정보를 포함할 수 있을 것이다.

[0013] 도 1은 데이터 처리 시스템(10)의 일부를 도시한다. 데이터 처리 시스템(10)은 마스터(상호접속 또는 버스 마스터라고도 불림)(12), 마스터(14)(상호접속 또는 버스 마스터라고도 불림), 메모리 제어기(32), 비휘발성 메모리(36), 시스템 상호접속부(22), I/O 회로(16), 주변 장치(18) 및 기타 슬레이브(20)를 포함한다. 마스터(12)는 도전체(48)를 통해서 시스템 상호접속부(22)에 양방향성으로 결합되며, 마스터(14)는 도전체(50)를 통해서 시스템 상호접속부(22)에 양방향성으로 결합되며, I/O 회로는 도전체(52)를 통해서 시스템 상호접속부(22)에 양방향성으로 결합되며, 주변 장치(18)는 도전체(54)를 통해서 시스템 상호접속부(22)에 양방향성으로 결합되며,

기타 슬레이브(20)는 도전체(56)를 통해서 시스템 상호접속부에 양방향성으로 결합되며, 메모리 제어기(32)는 도전체(24)를 통해서 시스템 상호접속부(22)에 양방향성으로 결합된다. 도전체(24)는 마스터 식별자(26), 어드레스/데이터(30), R/W 신호(28) 및 기타 신호(34)와 통신하는 도전체들을 포함한다.

[0014] 메모리 제어기(32)는 액세스 보호 제어 레지스터(38), 액세스 변형 회로(40), 액세스 제어 회로(42) 및 메모리 액세스 회로(44)를 포함하며, 도전체(46)를 통해서 비휘발성 메모리(36)에 양방향성으로 결합된다. 액세스 보호 제어 레지스터는 액세스 변형 회로(40)에의 액세스 허용(58)을 제공한다. 액세스 변형 회로(40)는 도전체(62)를 통해서 데이터 처리 시스템(10) 내의 정보로부터, 그리고 도전체(64)를 통해서 메모리 제어기(32) 내의 정보로부터 상태 정보(60)를 수신하며, 변형된 액세스 허용(66)을 액세스 제어 회로(42)에 제공한다. 다른 실시예에서, 상태 정보(60)는 (도전체(62)를 통해서)데이터 처리 시스템(10)으로부터 제공되는 정보만을 포함하거나 메모리 제어기(32) 내로부터 제공되는 정보만을 포함할 수 있음에 주목하여야 한다. 더욱이, 상태 정보(60)는 (몇몇 또는 모든 도전체(62)를 통해서)데이터 처리 시스템(10) 외부의 소스들로부터 제공되는 정보를 포함할 수 있을 것이다. 따라서, 아래에서 보다 상세히 설명될 바와 같이 상태 정보(60)는 액세스 변형 회로(40)에 원하는 상태 정보를 제공하는 임의의 타입의 신호 또는 지시자를 포함할 수 있을 것이다. 액세스 제어 회로(42)는 메모리 액세스 회로(44)에 (하나 이상의 지시자를 포함할 수 있는)액세스 허용 지시자(68)를 제공한다.

[0015] 비록 도 1에는 하나의 주변 장치(18)만이 도시되어 있지만, 데이터 처리 시스템(10)은 시스템 상호접속부(22)에 결합되는 임의의 수의 주변 장치를 포함할 수 있을 것이다. 유사하게, 임의의 수의 마스터 및 슬레이브가 시스템 상호접속부(22)에 결합될 수 있을 것이며, 도 1에 도시된 것에 한정되지 않는다. 일 실시예에서 데이터 처리 시스템(10)은 단일의 집적 회로 또는 동일한 장치상에 위치할 수 있을 것임에 주목하라. 이와 달리, 데이터 처리 시스템(10)은 서로 상호접속되는 임의의 수의 별개의 집적 회로 또는 별개의 장치를 포함할 수 있을 것이다. 예컨대, 일 실시예에서, (예컨대, 비휘발성 메모리(36) 및 메모리 제어기(32)와 같은)메모리 및 메모리 제어기는 데이터 처리 시스템(10)의 나머지 부분과는 별도의 하나 이상의 집적 회로들 상에 위치할 수 있을 것이다.

[0016] 일 실시예에서, 마스터(12) 및 마스터(14)는, 마이크로프로세서, 디지털 신호 프로세서 등과 같이 명령을 실행할 수 있는 프로세서이거나, DMA(direct memory access) 회로 또는 디버그 회로와 같은 임의의 다른 타입의 상호접속부 또는 버스 마스터일 수 있을 것이다. 또한, 단지 2개의 마스터만이 기술되었지만, 데이터 처리 시스템(10)은 필요한 만큼의 (하나 이상의)임의의 수의 마스터들을 포함할 수 있을 것이다. 소정의 동작 포인트에서 각각의 마스터(12,14)는 상이한 보안 레벨을 가실 수 있음 또한 주의하라. 예컨대, 특정 동작 포인트에서의 데이터 처리 시스템(10)의 상태에 따라, 각각의 마스터(12,14)는 보안 또는 비보안 마스터일 수 있을 것이다. 주변 장치(18)는 UART(universal asynchronous receiver transmitter), RTC(real time clock), 키보드 제어기, 임의의 타입의 메모리 등과 같은 임의의 타입의 주변 장치일 수 있을 것이다. 기타 슬레이브(20)는, 예컨대 마스터(12,14)에 의해서 액세스가능한 메모리와 같은 임의의 타입의 상호접속 슬레이브 및 주변 장치(18)와 동일한 타입을 포함하는 시스템 버스 상에 상주하는 임의의 타입의 주변 장치를 포함할 수 있음에 주목하라. I/O 회로(16)는 데이터 처리 시스템(10)의 내부 혹은 회부의 정보를 수신하거나 제공하는 임의의 타입의 I/O 회로를 포함할 수 있을 것이다.

[0017] 예시된 실시예에서, 메모리 제어기(32) 및 비휘발성 메모리(36)는 시스템 상호접속부(36)에 결합되는 다른 슬레이브에 대응한다. 일 실시예에서, 비휘발성 메모리(36)는 (예컨대, 미스터(12,14)와 같은)시스템 상호접속부(22)에 결합되는 적어도 2개의 마스터에 의해서 공유될 수 있음에 주목하라. 비휘발성 메모리(36)는 마스터(12,14)와 동일한 집적 회로 상에, 또는 별도의 집적 회로 상에 위치할 수 있을 것이다. 더욱이, 메모리(36)가 (플레쉬 메모리와 같은)비휘발성 메모리로 도시되어 있지만, 메모리(36)는, 예컨대 ROM, RAM, DRAM, SRAM, (예컨대, 플래쉬, MRAM과 같은)비휘발성 메모리 등과 같은 임의의 타입의 메모리일 수 있을 것이다. 또한, 메모리(36)는 다른 주변 장치 또는 슬레이브 내에 위치한 메모리 또는 다른 저장 장치일 수 있을 것이다. 또 다른 실시예에서, 메모리(36)는 보호될 필요가 있는 보안 정보를 가지는 임의의 타입의 자원일 수 있을 것이며, 메모리 제어기(32)는 자원을 보호하기 위한 액세스 보호 회로를 가지는 임의의 타입의 제어기로 대체될 수 있을 것이다.

[0018] 시스템 상호접속부(22)는 마스터(12), 마스터(14), I/O 회로(16), 주변 장치(18), 기타 슬레이브(20) 및 메모리 제어기(32)를 상호접속한다. 일 실시예에서, 도 1에 도시된 바와 같이, 시스템 상호접속부(22)는 시스템 버스 프로토콜에 따라 동작하는 시스템 버스로 구현된다. 이와 달리, 시스템 상호접속부(22)는 다양한 장치들 사이

에서 정보를 라우팅하는 스위칭 회로와 같은 상호접속 회로를 이용하여 구형될 수 있다.

[0019] 동작시에, 마스터(12,14)는 기타 슬레이브(20), 주변 장치(18) 또는 비휘발성 메모리(36)에의 액세스를 요청하기 위하여 메모리 제어기(32)를 통해서 시스템 상호접속부(22)의 사용을 요청한다. 요청 마스터는 시스템 상호접속부(22)를 통해서 메모리 제어기(32)에 액세스 요청을 제공할 수 있다. 액세스 요청은, 예컨대 데이터 또는 명령에 대한 판독 요청 또는 기록 요청일 수 있다. 메모리 제어기(32)는 요청 마스터가 충분한 액세스 허용을 가지는 것으로 가정하여 판독 액세스 요청에 응답하여 요청된 정보(데이터 또는 명령)를 시스템 상호접속부(22)를 통해서 요청 마스터에 다시 제공한다. 일 실시예에서, 액세스 요청에 대하여, 어느 마스터가 현재 액세스를 요청하는지를 식별하는 마스터 식별자(26)가 메모리 제어기(32)에 제공된다. 현재 액세스 요청이 판독 또는 기록 타입의 액세스인지를 나타내기 위하여 R/W 신호(28)가 메모리 제어기(32)에 제공될 수 있을 것이다. 메모리 제어기(32)는 현재 액세스 요청에 대응하는 어드레스 정보 또한 수신하고, 요청된 정보를 어드레스/데이터(30)를 통해서 제공한다. 메모리 제어기(32)와 통신하는 데에 필요한 (상태, 데이터 등과 같은)임의의 다른 신호들이 다른 신호들(34)을 통해서 제공될 수 있을 것이다.

[0020] 마스터(12,14)와 같은 각각의 마스터는 비휘발성 메모리(36)에의 특정 액세스 요청이 허용가능한지를 결정하는 데에 이용될 수 있는 대응하는 액세스 허용을 가질 수 있을 것이다. 예컨대, 특정 마스터는 비휘발성 메모리(36)에의 기록 액세스 또는 판독 액세스에 대하여 상이한 액세스 허용을 가질 수 있을 것이다. 일 실시예에서, 이들 액세스 허용은 액세스 보호 제어 레지스터(38)에 저장된다.

[0021] 도 2는 도 1의 액세스 보호 제어 레지스터(38)의 일 실시예를 도시한다. 일 실시예에서, 액세스 보호 제어 레지스터(38)는 데이터 처리 시스템(10) 내의 각각의 마스터에 대한 하나의 액세스 보호 필드를 포함한다. 예컨대, 액세스 보호 제어 레지스터(38)는 마스터(12) 및 마스터(14)에 각각 대응하는 마스터(12) 액세스 보호 필드(70) 및 마스터(14) 액세스 보호 필드(76)를 포함한다. 액세스 보호 필드는 특정 마스터에 의한 비휘발성 메모리(36)에 대한 특정 타입의 액세스가 허용되는지 여부를 나타낸다. 예컨대, 예시된 실시예에서, 각각의 액세스 보호 필드(70,76)는 각각의 마스터에 대한 판독 액세스 및 기록 액세스의 허용을 나타내기 위하여 판독 액세스 보호 필드 및 기록 액세스 보호 필드를 포함한다.

[0022] 마스터(12) 액세스 보호 필드(70)는 마스터(12)가 비휘발성 메모리(36)에의 판독 액세스를 수행하는 것이 허용되었는지 여부를 나타내는 마스터(12) 판독 액세스 보호 필드(72) 및 마스터(12)가 비휘발성 메모리(36)에의 기록 액세스를 수행하는 것이 허용되었는지 여부를 나타내는 마스터(12) 기록 액세스 보호 필드(74)를 포함한다. 따라서, 마스터(12)는 비휘발성 메모리(36)에의 판독 또는 기록 액세스 중 하나만을 수행하도록 허용될 수 있을 것이다. 이와 달리, 마스터(12)는 팔드(72,74)의 값에 따라 비휘발성 메모리(36)에의 판독 및 기록 액세스 모두에 대하여 허용하거나, 이들 모두에 대하여 허용하지 않을 수 있을 것이다. 일 실시예에서, 각각의 필드(72,74)는 대응하는 액세스 타입(기록 또는 판독)이 허용되는지 여부를 나타내는 1 비트 필드이다. 유사하게, 마스터(14) 액세스 보호 필드(76)는 마스터(14)가 비휘발성 메모리(36)에의 판독 액세스를 수행하는 것이 허용되는지 여부를 나타내는 마스터(14) 판독 액세스 보호 필드(78) 및 마스터(14)가 비휘발성 메모리(36)에의 기록 액세스를 수행하는 것이 허용되는지 여부를 나타내는 마스터(14) 기록 액세스 보호 필드(80)를 포함한다. 따라서, 마스터(14)는 비휘발성 메모리(36)에의 기록 또는 판독 액세스 중 단지 하나만을 수행하는 것이 허용될 수 있을 것이다. 이와 달리, 마스터(14)는 필드(78,80)의 값에 따라 비휘발성 메모리(36)에의 판독 및 기록 액세스 모두가 허용되거나, 이들 모두가 허용되지 않을 수 있을 것이다. 일 실시예에서, 각각의 필드(78,80)는 대응하는 액세스 타입(판독 또는 기록)이 허용되는지 여부를 나타내는 1 비트 필드이다.

[0023] 다른 실시예에서, 액세스 보호 제어 레지스터(38)는 필드(70,76)와 같은 임의의 수의 액세스 보호 필드를 포함할 수 있음에 주목하라. 예컨대, 액세스 보호 제어 레지스터(38)는 데이터 처리 시스템(10) 내의 모든 마스터에 대하여. 혹은 데이터 처리 시스템(10) 내의 마스터들의 부분집합에 대해서만 하나의 액세스 보호 필드를 포함할 수 있을 것이다. 또한, 각각의 액세스 보호 필드(70,76)는 판독 기록 액세스를 대신하여, 혹은 이에 추가하여 (예컨대, 버스트 액세스와 같은)상이한 타입의 액세스에 기초하는 허용을 식별하기 위하여 임의의 수의 필드들을 포함할 수 있음에 주목하라. 더욱이, 필드(70,72,76,78,80)는 상이한 필드 정의, 상이한 비트 할당 또는 상이한 수의 비트를 이용하는 것과 같은 다양한 상이한 방식으로 구현될 수 있을 것이다. 이와 달리, 별개의 레지스터들 또는 다른 레지스터 또는 데이터 처리 시스템(10) 내의 다른 메모리 위치 내와 같이 상이하게 구성될 수 있을 것이다. 통상적으로, 액세스 보호 제어 레지스터(38)는 보안 마스터에 의해서 프로그램가능한 소프트웨어이다. 일 실시예에서, 액세스 보호 제어 레지스터(38)는 리셋시에 프로그램될 수 있을 것이다.

[0024] 도 1을 다시 참조하면, 액세스 변형 회로(70)는 제어 레지스터(38) 내에 저장된 하나 이상의 액세스 허용을 변

형하는 데에(또는 오버라이드하는 데에) 이용될 수 있을 것이다. 예컨대, 상태 정보(60)에 따라, 액세스 변형 회로(40)는 액세스 보호 제어 레지스터(38)로부터의 액세스 허용(58)을 선택적으로 변형하여 변형된 액세스 허용을 제공할 수 있을 것이다. 즉, 어떤 경우에 변형된 액세스 허용(66)을 생성하도록 모든 액세스 허용(58)이 변형되거나, 변형된 액세스 허용(66)이 단지 하나 또는 몇몇 변형된 허용만을 포함하도록 하나 또는 몇몇 액세스 허용(58)만이 변형될 수 있을 것이다. 즉, 변형된 액세스 허용(66)은 현재 변형되지 않은 액세스 보호 제어 레지스터(38)로부터의 허용을 포함할 수 있을 것이다. 또한, 변형된 액세스 허용(66)은 특정 마스터에 대하여 메모리(36)에의 보다 광범위한(또는 덜 제한적인) 액세스를 제공하거나, 특정 마스터에 대하여 메모리(36)에의 액세스를 제한할 수 있을 것임에 주목하라.

[0025] 도 1을 다시 참조하면, 그 후에, 액세스 제어 회로(42)는 현재 액세스 요청이 허용되었는지 여부를 결정할 수 있을 것이다. 예컨대, 데이터 처리 시스템(10)내의 (마스터(12,14)와 같은)각각의 마스터는 대응하는 마스터 식별자를 가실 수 있을 것이다. 일 실시예에서, 마스터(12)는 마스터 식별자 0에 대응하고, 마스터(14)는 마스터 식별자(1)에 대응하여 각각의 마스터가 대응하는 숫자로 특유하게 식별될 수 있을 것이다. 다른 실시예에서, 임의의 타입의 식별자가 이용될 수 있을 것이며, 다른 방식으로 할당될 수도 있을 것이며, 0부터 시작하거나, 한자리 수까지와 같이 순서에 제한되지도 않을 것이다. 따라서, 다른 실시예에서, 다수의 마스터들은 동일한 마스터 식별자를 공유할 수 있을 것이다. 따라서, 액세스 제어 회로(42)는 (마스터 식별자(26)에 의해서 액세스 제어 회로(42)로 지시되는)어느 마스터가 현재 액세스를 요청하는지에 기초하여, 그리고 (변형된 액세스 허용(66)에 의해서 액세스 제어 회로(42)로 지시되는)액세스 허용에 기초하여, 비휘발성 메모리(36)로의 액세스가 허용되는지 여부를 결정한다. 액세스가 허용되는 경우에는, 액세스 허용 지시자(68)는 메모리 액세스 회로(44)로의 액세스가 허용되었음을 나타내며, 메모리 액세스 회로(44)는 그 후에 필요한 신호들 및 정보를 비휘발성 메모리(36)에 제공하여 요청된 액세스를 완료(예컨대, 요청된 판독 또는 기록을 완료)할 수 있을 것이다. 그러나, 현재 요청 마스터에 대한 변형된 액세스 허용(66)에 기초하는 경우에는, 액세스 제어 회로(42)가 액세스가 허용되었는지를 결정하며, 액세스 허용 지시자(68)는 액세스가 허용되지 않았음을 지시하고, 메모리 액세스 회로(44)는 요청된 액세스를 완료하지 않는다. 메모리 제어기(32)의 동작은 도 3을 참조하여 더 상세히 설명될 것이다.

[0026] 도 3은 본 발명의 일 실시예에 따른 메모리 제어기(32)의 동작에 대응하는 흐름(96)을 도시한다. 흐름(96)은 개시(82)에서 시작하고, 액세스 요청이 수신되는 블럭(84)으로 진행한다. 예컨대, 마스터(12,14)는 시스템 상호접속부(22)를 통해서 비휘발성 메모리(36)에 액세스 요청을 제공할 수 있을 것이며, 액세스 요청은, 예컨대 R/W 신호(28)에 의해서 지시되는 바와 같은 판독 또는 기록 요청일 수 있을 것이다. 그 후에, 블럭(86)으로 진행하여 액세스 허용이 결정된다. 예컨대, 이들 액세스 허용은 액세스 보호 제어 레지스터(38) 내의 필드(필드(70,76))에 의해서 제공될 수 있을 것이다. 그 후에, 흐름은 블럭(88)으로 진행하여 (상태 정보(60))와 같은 상태 정보가 수신된다. 상태 정보는, 예컨대, 디버그 동작, 비보안 또는 비검증 메모리로부터의 동작, 메모리 프로그래밍, DMA(direct memory access) 동작, 동작 모드, 폴트 모니터, 외부 버스 동작 등과 관련될 수 있을 것이다. 즉, 하나 이상의 상기 조건들, 상태들 또는 동작들을 나타내거나, 또는 하나 이상의 조건들, 상태들 또는 동작들과 관련된 정보를 나타낼 수 있는 정보가 상태 정보(60)를 통하여 액세스 변형 회로(40)에 제공될 수 있을 것이다. 따라서, 상태 정보(60)는 (마스터(12), 마스터(14), I/O 회로(16), 주변 장치(18) 또는 기타 슬레이브(20)와 같은)데이터 처리 시스템(10) 내의 다양한 장소, 혹은 메모리 제어기(32) 내의 장소 또는 데이터 처리 시스템(10) 외부의 장소 또는 이들의 조합으로부터 수신될 수 있을 것이다.

[0027] 예컨대, 디버그 동작과 관련된 상태 정보에 대하여, 하나 이상의 상태 정보들의 신호들(60)이 별도의 유닛으로서, 또는 예컨대 마스터(12,14)의 일부로서 상호 접속부(22)에 결합되는 디버그 회로(도시되지 않음)로부터 수신될 수 있을 것이다. 상태 정보(60) 내의 신호들은 다양한 상이한 방식으로 결합되어 결합된 상태 정보 또는 액세스 변형 회로(40)에의 하나 이상의 자원에 기초하는 상태 정보를 제공한다. 이러한 결합 회로는 액세스 변형 회로(40) 내에 위치하거나, 액세스 변형 회로(40) 외부에 위치하거나, 심지어는 메모리 제어기(32) 외부에 위치할 수 있을 것이다.

[0028] 도 3을 참조하면, 흐 후에 흐름은 블럭(90)으로 진행하여 수신된 상태 정보에 기초하여 액세스 허용이 선택적으로 변형될 수 있을 것이다. 예컨대, 일 실시예에서, 하드웨어 오버라이드가 액세스 허용을 변형하는 데에 이용되어, 상태 정보(60)를 통해서 통신되는 소정의 조건들 또는 상태들이 액세스 보호 제어 레지스터(38) 내에 저장되는 허용이 하드웨어에 의해서 오버라이드되도록 야기할 수 있을 것이다. 예컨대, 일 실시예에서, 상태 정보(60)는 원하는 대로 결합되어(혹은 직접), 하드웨어 오버라이드 회로에 입력될 수 있을 것이며, 소정의 조건들이 충족되는 때에 액세스 보호 제어 레지스터(38)의 값들이 하드웨어에 의해서 변형되거나 대체되어 변형된

액세스 허용(66)과 같은 변형된 액세스 허용을 생성할 수 있을 것이다. 이와 달리, 액세스 허용(58)은 상태 정보(60)에 기초하여 다른 하드웨어 또는 다른 소프트웨어 방법에 의한 것과 같은 다른 방식으로 선택적으로 변형되어 변형된 액세스 허용(66)을 생성할 수 있을 것이다.

[0029] 흐름은 그 후에 블럭(92)로 진행하여 변형된 액세스 허용에 기초하여 요청된 액세스가 선택적으로 수행된다. 예컨대, 마스터(12)가 비휘발성 메모리(36)에의 판독 액세스를 요청하고, 마스터(12) 판독 액세스 보호 필드(72)가 마스터(12)에 의한 판독 액세스가 허용되었음을 나타내는 경우에, (이것이 액세스 변형 회로(40)에 의해서 변형되지 않는다고 가정하면)마스터(12)의 요청이 수행될 것이다. 그러나, 상태 정보(60)가 마스터(12)의 판독 액세스 허용이 변형되어야할 것을 나타내면(예컨대, 허용하지 않고 부인하는 경우에), 액세스 변형 회로(40)는 판독 액세스 허용을 변형하여(그리고, 이것을 변형된 액세스 허용(66)을 일부로서 제공하여) 요청된 판독 액세스는 허용되지 않고 부인될 것이며, 이리하여 마스터(12) 판독 액세스 보호 필드(72)를 오버라이드한다. 흐름은 종료(94)에서 종료한다.(도 3의 흐름은 메모리 제어기(32)를 통한 메모리(36)에의 액세스 요청시마다 반복될 수 있음에 주목하라.)

[0030] 따라서, 마스터(12,14)와 같은 마스터에 의한 비휘발성 메모리(36)에의 액세스마다, 액세스 보호 제어 레지스터들(38)은 현재 액세스가 허용되는지 여부를 결정하는 데에 이용될 수 있는 액세스 허용(58)을 제공한다. 그러나, 데이터 처리 시스템(10)의 상태 정보에 따라 이들 소프트웨어 프로그램가능 레지스터들의 오버라이드가 바람직한(그래서 변형된 액세스 허용(66)을 야기하는) 상황이 존재한다. 예컨대, 액세스 보호 제어 레지스터(38)가 소프트웨어 프로그램가능한 경우에, 액세스 보호 제어 레지스터(38) 내에 저장된 허용은 비보안 소프트웨어에 의해서 보호받을 필요가 있는 보안 정보에 대한 액세스를 잘못 허용하도록 변경되었을 수 있을 것이다. 따라서, 액세스 변형 회로(40)는 소정의 상태 정보 또는 데이터 처리 시스템(10)의 조건들에 따라 보안 정보에의 액세스를 방지하기 위하여 액세스 보호 레지스터(38)의 액세스 허용을 변형하는 데에 이용될 수 있는 (오버라이드와 같은)변형을 제공하는 데에 이용될 수 있을 것이다.

[0031] 일 실시예에서, 데이터 처리 시스템(10)은 통상적으로 디버그동안에 보다 액세스가능하기 때문에 디버그 동작동안에는 액세스가 제한될 수 있을 것이다. 따라서, 일 실시예에서 상태 정보(60)는 언제 디버그가 인에이블되는지를 나타내는 디버그 회로(도시되지 않음)로부터의 정보를 포함한다. 이 경우에, 액세스 보호제어 레지스터(38) 내의 몇몇 또는 모든 마스터들(12,14)의 허용은 액세스 변형 회로(40)에 의해서 변형될 수 있을 것이다.

[0032] 다른 실시예에서, 비보안 또는 비검증 메모리로부터의 동작 동안에, 데이터 처리 시스템(10)의 보안을 보장하고, 예컨대 이들 비보안 또는 비검증 메모리들 내에 저장된 잘못되거나 적대적인 소프트웨어에 기인하여 야기될 수 있는 손상을 방지하기 위하여 액세스가 변형될 필요가 있을 것이다.

[0033] 다른 실시예에서, 액세스 허용은 메모리가 프로그래밍되는 경우에 변형될 필요가 있을 것이다. 예컨대, 도 1을 참조하면, 비휘발성 메모리(36)가 변형되는 경우에, 비휘발성 메모리(36)의 변형된 부분의 보안을 보장하는 것이 가능하지 않기 때문에 비휘발성 메모리(36)로의 액세스 허용이 변경될 수 있을 것이다. 예컨대, 비휘발성 메모리(36)는 불량 데이터, 오정보를 포함하도록 변형되거나, 또는 잘못되거나 적대적인 소프트웨어를 저장하도록 변형되었을 수 있을 것이다. 이러한 경우에, 상태 정보(60)는 도전체(64)와 같은 메모리 제어기(32) 내로부터 제공되는 정보를 포함할 수 있을 것이다.

[0034] 또 다른 실시예에서, 액세스 허용은 DAM 동작을 위하여 변형될 수 있을 것이다. 이러한 예에서, 상태 정보(60)는 DMA 동작의 발생을 나타내는 DMA로부터의 신호를 포함할 수 있을 것이다(예컨대, 마스터(12,14)는 DMA이거나 이를 포함할 수 있을 것이다). 다른 실시예에서, 액세스 허용은 시스템이 잘못된 펌웨어, 소프트웨어 또는 설정에 의해서 미지의 상태로 부트될 수 있기 때문에 보안 정보가 보안 상태로 남는 것을 보장하도록 부트 동작시에 변형될 수 있을 것이다. 액세스 허용은 소프트웨어가 검증될 때까지 액세스 보호 제어 레지스터(38) 내에 저장된 액세스 허용이 액세스를 제어하는(즉, 오버라이드되거나 변형되는) 것을 허용하지 않도록 소프트웨어 보안 검증에 기초하여 변경될 수도 있을 것이다. 액세스 허용은 데이터 처리 시스템(10) 또는 마스터(12,14)의 보안 레벨에 기초하여 변형될 수 있을 것이다. 예컨대, 각각의 마스터는 (보안 및 비보안이 아닌)가변 보안 레벨을 가질 수 있을 것이며, 특정 액세스 요청 동안의 보안 레벨에 기초하여 제어 레지스터(38)의 액세스 허용이 변형될 수 있을 것이다. 액세스 허용은 보안 모니터 동작에 기초하여 변형될 수도 있을 것이다. 예컨대, 보안이 침해되지 않았음을 보장하기 위하여 데이터 처리 시스템(10) 내의 동작을 감독하는 보안 모니터(도시되지 않음)가 데이터 처리 시스템(10)에 존재할 수 있을 것이다. 따라서, 보안 모니터에 의한 소정의 조건의 검출시에, 액세스가 적절히 변형될 수 있을 것이다. 따라서, 상태 정보(60)는 이들 상태, 조건 및 동작에 관련

된 정보를 액세스 변형 회로(40)에 제공하는 데에 이용될 수 있을 것이다.

[0035] 또한, 다른 예에서, 액세스 허용은 데이터 처리 시스템 또는 메모리 제어기(32)의 동작 모드에 기초하여 상태 정보(60)에 의해서 지시되는 대로 변형될 수 있을 것이다. 예컨대, 데이터 처리 시스템(10)이 (동작의 기본 세트만이 지원되는 최소 동작 상태와 같은)감소된 레벨 동작 상태에 진입하는 경우에, 제어 레지스터(38)의 프로그래밍된 액세스 허용은 감소된 레벨에서 동작하는 동안 데이터 처리 시스템(10)을 보호하도록 변형될 수 있을 것이다. 다른 실시예에서, 액세스 허용은 데이터 처리 시스템(10)의 폴트 모니터(도시되지 않음)에 기초하여 변형될 수 있을 것이다. 예컨대, 데이터 처리 시스템(10)의 임의의 부분 내의 폴트 모니터에 응답하여, 제어 레지스터(38)의 액세스 허용은 폴트 검출시에 액세스를 제한하도록 변형될 수 있을 것이다. 본 실시예에서, 폴트 모니터로부터의 신호는 상태 정보(60)를 통해서 액세스 변형 회로(40)에 제공될 수 있을 것이다. 또 다른 실시예에서, 액세스 허용은 외부 버스 동작에 기초하여 변형될 수 있을 것이다. 예컨대, 외부 버스 동작 동안에, 외부 소스는 보안 정보를 액세스하거나 변형하려고 하거나, 메모리(36) 또는 데이터 처리 시스템(10)을 손상시키려고 할 것이다. 따라서, 액세스 허용은 데이터 처리 시스템(10)의 보안을 보장하기 위하여 외부 버스 동작 동안에 액세스를 제한할 수 있을 것이다.

[0036] (예컨대, 상태 정보(60)를 통하여 제공되는)상태 정보가 제어 레지스터(38)의 액세스 허용을 선택적으로 이용될 수 있는 상이한 상황에 대하여 위에서 많은 예들이 제공되었음에 주목하라. 전술한 것과 다른 실시예들이 이용될 수 있다. 더욱이, 데이터 처리 시스템(10)의 필요에 따라 액세스 허용이 변경되어야 하는 상태 정보(60)가 다양한 방식으로 결합될 수 있는 상기 상황들의 조합이 이용될 수 있을 것이다. 즉, 상태 정보(60)는 액세스 변형 회로(40)가 액세스 허용의 변형 여부를 올바르게 결정하도록 하기 위하여 액세스 변형 회로(40)에의 필요한 상태 정보를 나타내기 위하여 메모리 제어기(32) 내의 자원들 또는 소스들을 포함하는 다양한 상이한 자원 또는 소스들로부터 취해질 수 있을 것이다. 더욱이, 상태 정보는 데이터 처리 시스템(10) 또는 그 구성요소의 상태 또는 조건을 반영하는 임의의 타임의 정보를 포함할 수 있을 것이다. 또한, 상태 정보는 (마스터(12,14)와 같은)하나 이상의 마스터들의 신뢰도를 나타낼 수 있을 것이다. 또한, 비록 전술한 대부분의 예들이 액세스 허용을 제한하는 것을 참조하여 제공되었지만, 액세스 변형 회로(40)는 데이터 처리 시스템(10)의 설계에 따라 액세스 허용을 증가시키거나 넓히는 데에 상태 정보를 이용할 수도 있을 것이다.

[0037] 따라서, 다수의 마스터 데이터 처리 시스템을 포함하는 데이터 처리 시스템의 보안을 어떻게 향상시킬 수 있는지를 이해할 수 있을 것이다. 액세스 변형 호로는 다양한 상이한 타입의 상태 정보에 기초하여 액세스 허용을 선택적으로 변형하는 데에 이용될 수 있을 것이다. 따라서, 데이터 처리 시스템(10)의 상태가 변함에 따라, 액세스 단위마다 액세스 허용을 제한하거나 넓힘으로써 필요한 만큼의 보안이 유지될 수 있을 것이다. 더욱이, 이러한 변형은 마스터 단위 및 액세스 타입 단위로 수행될 수 있을 것이다. 상태 정보는 메모리 제어기(32) 내의 정보를 포함하는 데이터 처리 시스템(10)의 다양한 부분으로부터 수신된 정보를 포함할 수 있을 것이며, 데이터 처리 시스템(10)의 외부 소스로부터의 정보를 포함할 수 있을 것이다. 또한, 액세스 변형 회로는 액세스 허용을 하드웨어 오버라이드 메커니즘을 이용하여 선택적으로 변형할 수 있을 것이다. 이와 달리, 다른 하드웨어, 소프트웨어 또는 이들의 조합, 메커니즘이 변형된 액세스 허용(66)을 생성하는 데에 이용될 수 있을 것이다.

[0038] 명세서에서, 본 발명은 특정 실시예를 참조하여 기술되었다. 그러나, 본 기술 분야의 당업자는 청구의 범위에 기술된 본 발명의 범위를 벗어나지 않고서 다양한 변경과 변화가 이루어질 수 있음을 이해할 것이다. 예컨대, 데이터 처리 시스템(10) 및 메모리 제어기(32)는 도 1의 실시예에 나타난 것과는 다르게 구성될 수 있을 것이다. 더욱이, 회로는 하드웨어, 소프트웨어 및 펌웨어의 조합으로 구현될 수 있을 것이다. 따라서, 명세서 및 도면은 제한적인 의미가 아니라 예시적인 의미로 간주되며, 이러한 모든 변형은 본 발명의 범위 내에 포함된다.

[0039] 특정 실시예에 관하여 장점, 다른 이점 및 문제점에 대한 해결책이 전술되었다. 그러나, 장점, 이점, 문제점에 대한 해결책 및 장점, 이점 또는 해결책을 발생시키거나, 보다 강조하는 임의의 요소는 임의의 청구항 또는 모든 청구항에서 중요하거나, 요청되거나 필수적인 특질 또는 요소로 해석되지 않는다. 본 명세서에서 사용된 "하나의(a(n))"는 하나 이상을 정의한다. 본 명세서에 사용된 "포함하는"이라는 용어는 포함하는 것을 의미한다. 본 명세서에 사용된 "포함하는" 또는 그 변형은 요소들의 리스트를 포함하는 프로세스, 방법, 물건 또는 장치가 이들뿐만 아니라 명시적으로 리트스되지 않거나 이러한 프로세스, 방법, 물건 또는 장치에 고유한 다른 요소들도 포함하도록 하는 비배타적인 포함을 커버한다.

도면의 간단한 설명

[0005] 본 발명은 예시적으로 기술되며, 동일한 참조 부호가 동일한 요소를 나타내는 첨부된 도면에 의해서 제한되는 것은 아니다.

[0006] 도 1은 본 발명의 일 실시예에 따른 데이터 처리 시스템을 도시하는 블럭도.

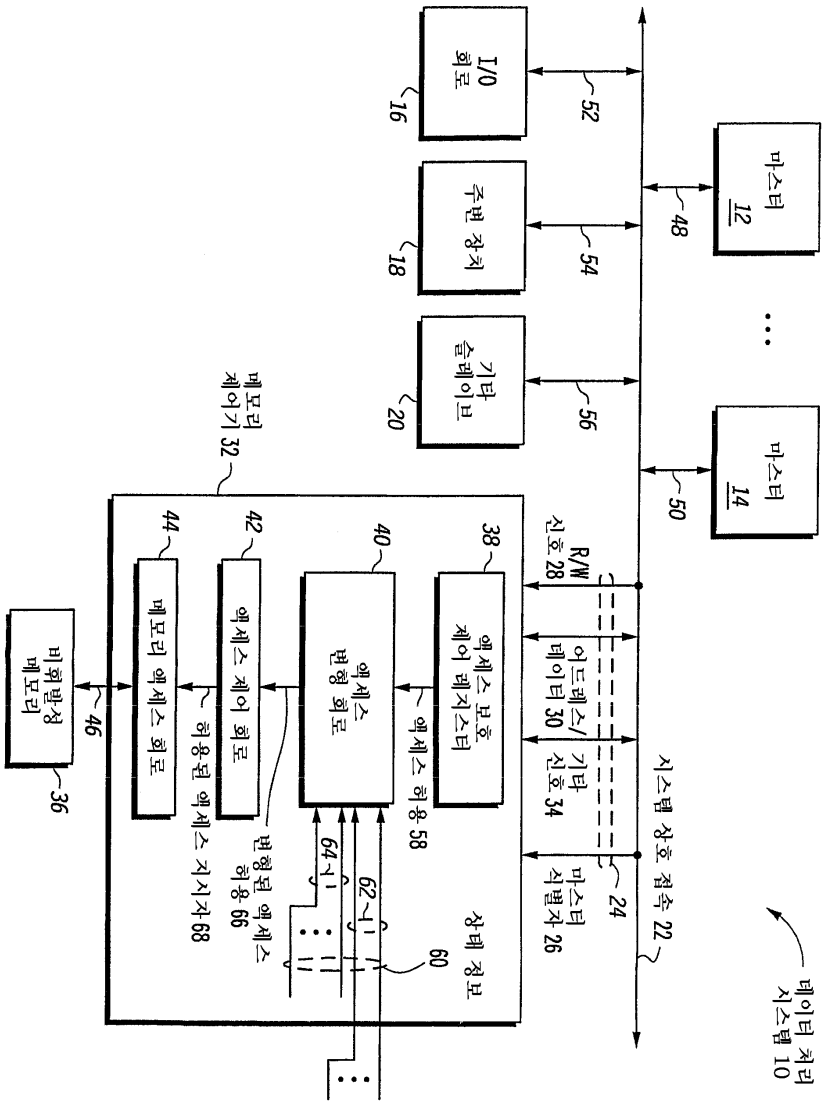
[0007] 도 2는 본 발명의 일 실시예에 따른 도 1의 데이터 처리 시스템의 액세스 보호 제어 레지스터를 도시하는 블럭도.

[0008] 도 3은 본 발명의 일 실시예에 따른 도 1의 데이터 처리 시스템의 동작을 도시하는 흐름도.

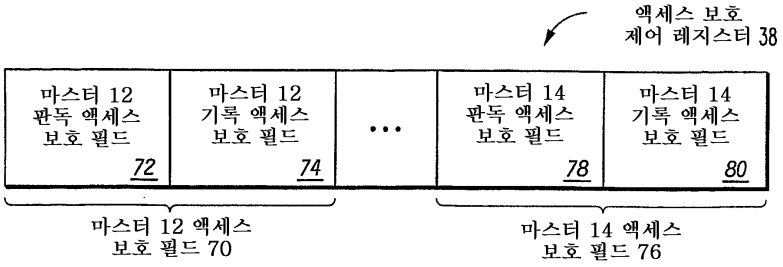
[0009] 본 발명의 기술 분야의 당업자는 도면의 요소들은 간단 명료하게 도시하기 위하여 반드시 실제 크기대로 도시되지 않았음을 이해할 것이다. 예컨대, 본 발명의 실시예의 이해를 돕기 위하여 도면의 몇몇 요소들의 치수는 다른 요소들에 비하여 과장될 수 있을 것이다.

도면

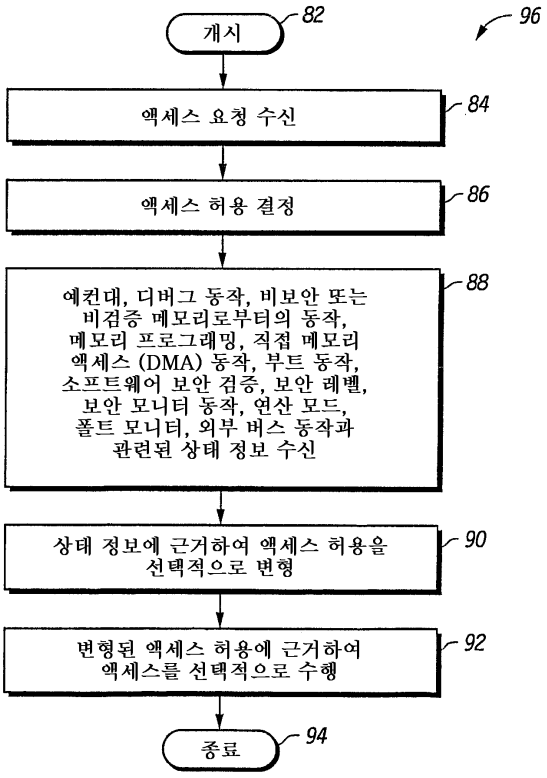
도면1



도면2


액세스 보호
제어 레지스터 38
마스터 12
판독 액세스
보호 필드
72
마스터 12
기록 액세스
보호 필드
74
...
마스터 14
판독 액세스
보호 필드
78
마스터 14
기록 액세스
보호 필드
80
마스터 12 액세스
보호 필드 70
마스터 14 액세스
보호 필드 76

도면3


개시
82
96
액세스 요청 수신
84
액세스 허용 결정
86
예컨대, 디버그 동작, 비보안 또는
비검증 메모리로부터의 동작,
메모리 프로그래밍, 직접 메모리
액세스 (DMA) 동작, 부트 동작,
소프트웨어 보안 검증, 보안 레벨,
보안 모니터 동작, 연산 모드,
폴트 모니터, 외부 버스 동작과
관련된 상태 정보 수신
88
상태 정보에 근거하여 액세스 허용을
선택적으로 변형
90
변형된 액세스 허용에 근거하여
액세스를 선택적으로 수행
92
종료
94