(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
G06F 1/00

(11) 공개번호 특2003-0094396
(43) 공개일자 2003년12월11일

(21) 출원번호 10-2003-7014546
(22) 출원일자 2003년11월07일
번역문 제출일자 2003년11월07일
(86) 국제출원번호 PCT/US2002/11935
(87) 국제공개번호 WO 2002/93336
(86) 국제출원출원일자 2002년04월17일
(87) 국제공개일자 2002년11월21일

(30) 우선권주장 09/852,942 2001년05월10일 미국(US)
09/852,372 2001년05월10일 미국(US)
09/853,226 2001년05월11일 미국(US)

(71) 출원인 어드밴스드 마이크로 디바이시즈, 인코포레이티드
미국 캘리포니아 94088-3453 서니베일 원 에이엠디 플레이스 메일 스톱68

(72) 발명자 스트롱인제프리에스.
미국텍사스78731오스틴몬타나노르테7210

(74) 대리인 박장원

심사청구 : 없음

(54) 개인용 컴퓨터 시스템들에서 백도어 액세스 메커니즘들을막기 위한 메커니즘

요약

백도어 액세스 메커니즘들을 막기 위한 방법들, 디바이스들 및 시스템들이 개시된다. 프로세서는 1개 이상의 하드웨어-디버그-테스트(HDT) 인에이블 비트들을 저장하도록 구성된 제 1 레지스터, 다수의 HDT 입력 신호들을 수신하도록 결합된 제 1 제어 로직, 및 제 1 레지스터에 결합된 제 2 제어 로직을 포함한다. 제 1 제어 로직은 제 1 레지스터를 액세스하도록 결합된다. 제 2 제어 로직은 프로세서의 리셋에 응답하여 1개 이상의 디폴트 값들을 제 1 레지스터에 저장하도록 구성된다. 다른 프로세서는 다수의 마이크로코드 입력들을 수신하도록 결합된 제 1 제어 로직, 제 1 제어 로직에 결합된 제 1 레지스터, 및 제 1 레지스터에 결합된 제 2 제어 로직을 포함한다. 제 1 레지스터는 1개 이상의 마이크로코드 적재기 인에이블 비트들을 저장하도록 구성된다. 제 2 제어 로직은 프로세서의 리셋에 응답하여 1개 이상의 디폴트 값들을 제 1 레지스터에 저장하도록 구성된다.

대표도

도 4A

색인어

백도어 액세스, 개인용 컴퓨터, 마이크로코드, 디폴트 값, HDT 인에이블 비트

명세서

관련 출원

본 발명은, 2001년 5월 10일 출원되었고 발명자들이 Dale E. Gulick 및 Geoffrey S. Strongin이며 그 명칭이 '보안 실행 박스 및 방법(Secure Execution Box and Method)'인 동시 계류중인 미국 특허 출원 제09/852,382호의 부분 연속 출원이다. 본 발명은 또한, 2001년 5월 10일 출원되었고 발명자들이 Dale E. Gulick 및 Geoffrey S. Strongin이며 그 명칭이 '강화된 보안 및 제어성을 위한 컴퓨터 시스템 아키텍쳐(Computer System Architecture for Enhanced Security and Manageability)'인 동시 계류중인 미국 특허 출원 제09/852,942호의 부분 연속 출원이다.

기술분야

본 발명은 일반적으로 컴퓨팅 시스템들에 관한 것으로서, 특히 권한이 없는 백도어(back door) 액세스들로부터 개인용 컴퓨터 시스템들을 보호하기 위한 방법 및 장치에 관한 것이다.

배경기술

도 1은 예시적인 컴퓨터 시스템(100)을 도시한다. 이 컴퓨터 시스템(100)은 프로세서(102), 노쓰 브리지(north bridge)(104), 메모리(106), 진보형 그래픽 포트 (AGP) 메모리(108), 주변기기 접속 (PCI) 버스(110), 사우쓰 브리지(south bridge)(112), 배터리(113), AT 부착(ATA) 인터페이스(114)(집적 드라이브 일렉트로닉스 (IDE) 인터페이스로서 더 일반적으로 알려져있음), 범용 직렬 버스 (USB) 인터페이스(116), 로우 핀 카운트 (LPC) 버스(118), 입/출력 제어기 칩(SuperI/O ™)(120) 및 BIOS 메모리(122)를 포함한다. 주목할 사항으로서, 상기 노쓰 브리지(104) 및 사우쓰 브리지(112)는 단일 칩 만을 포함하거나 또는 다수의 칩들을 포함할 수 있어, 총체적으로 '칩셋(chipset)'이라는 용어를 이끌어낸다. 또한, 주목할 사항으로서, 요구에 따라서 다른 버스들, 디바이스들, 그리고/또는 서브 시스템들(예를 들어 캐시들, 모뎀들, 병렬 또는 직렬 인터페이스들, SCSI 인터페이스들, 네트워크 인터페이스 카드들 등)이 컴퓨터 시스템(100)에 포함될 수 있다. ['SuperI/O'는 캘리포니타 산타클라라에 소재하는 내셔널 세미컨덕터 코포레이션(National Semiconductor Corporation)의 상표이다.]

프로세서(102)는 노쓰 브리지(104)에 결합된다. 이 노쓰 브리지(104)는 프로세서(102), 메모리(106), AGP 메모리(108) 및 PCI 버스(110) 사이에 인터페이스를 제공한다. 사우쓰 브리지(112)는 IDE 인터페이스(114), USB 인터페이스(116) 및 LPC 버스(118)에 결합된 주변장치들, 디바이스들 및 서브 시스템들과 PCI 버스(110) 사이에 인터페이스를 제공한다. 배터리(113)는 사우쓰 브리지(112)에 결합된 것으로 도시된다. SuperI/O ™ 칩(120)은 LPC 버스(118)에 결합된다.

노쓰 브리지(104)는 프로세서(102)와, 메모리(106)와, AGP 메모리(108)와, PCI 버스(110)에 결합된 디바이스들과, 그리고 사우쓰 브리지(112)에 결합된 디바이스들 및 서브 시스템들 사이에 통신 액세스를 제공한다. 전형적으로, 컴퓨터 시스템(100)에 결합하기 위해 PCI 버스(110)에 연결되는 PCI '슬롯들'(도면 미도시) 내에는 제거가능한 주변 디바이스들이 삽입된다. 대안적으로, 마더보드(motherboard) 위에 위치하는 디바이스들이 PCI 버스(110)에 직접 연결될 수 있다.

사우쓰 브리지(112)는, 일반적으로 LPC 버스(118)(또는, X-버스 또는 ISA 버스와 같은 이전 것들(predecessors))를 통해 컴퓨터 시스템(100)에 결합되는 다양한 디바이스들 및 서브 시스템들(예를 들어, 모뎀, 프린터, 키보드, 마우스 등)과 PCI 버스(110) 사이에 인터페이스를 제공한다. 사우쓰 브리지(112)는 IDE 인터페이스(114), USB 인터페이스(116) 및 LPC 버스(118)를 통해 컴퓨터 시스템(100)의 나머지 부분에 디바이스들을 인터페이스하는 데에 이용되는 로직을 포함한다.

하드웨어의 관점에서, x86 동작 환경은 사용자의 사생활을 거의 보호하지 못하고, 법인의 비밀 및 자산에 대한 보안을 거의 제공하지 못하거나, 콘텐츠 제공자들(content providers)의 소유권을 거의 보호하지 못한다. 이러한 모든 목적들, 즉 사생활, 보안 및 소유권(총체적으로 PSO)은 인터넷 연결 컴퓨터 세대에서 점점 중요해지고 있다. 최초의 개인용 컴퓨터들은 PSO 요구들을 예상하여 설계되지 않았다.

소프트웨어의 관점에서 또한, x86 동작 환경은 PSO에 대해 불충분하다. 소프 트웨어를 통해 하드웨어를 용이하게 직접 액세스함으로써, 또는 개인용 컴퓨터의 커버를 단순히 오픈함으로써, 침입자 또는 도둑은 대부분의 보안 소프트웨어 및 디바이스들을 손상시킬 수 있다. 개인용 컴퓨터의 이용의 용이함이 결국 PSO 문제들을 부가하게 된다.

발명의 상세한 설명

본 발명은 프로세서를 제공한다. 이 프로세서는 1개 이상의 하드웨어-디버그-테스트(HDT) 인에이블 비트들을 저장하도록 구성된 제 1 레지스터, 다수의 HDT 입력 신호들을 수신하도록 결합된 제 1 제어 로직, 및 제 1 레지스터에 결

합된 제 2 제어 로직을 포함한다. 제 1 제어 로직은 제 1 레지스터를 액세스하도록 결합된다. 제 2 제어 로직은 프로세서의 리셋에 응답하여 제 1 레지스터 내에 1개 이상의 디폴트 값들을 저장하도록 구성된다.

본 발명에 따르면, HDT 모드 인에이블 상태를 결정하는 방법이 제공된다. 이 방법은 HDT 모드를 시작 요구를 수신하는 단계와, HDT 모드 인에이블 상태를 결정하는 단계와, 그리고 HDT 모드 인에이블 상태가 인에이블 상태로 설정된 경우 HDT 모드를 시작하는 단계를 포함한다.

본 발명에 따르면, 마이크로코드를 변경하는 방법이 제공된다. 이 방법은 마이크로코드 변경 요구를 수신하는 단계와, 마이크로코드 적재기 인에이블 상태(microcode loader enable status)를 결정하는 단계와, 그리고 마이크로코드 적재기 인에이블 상태가 인에이블 상태로 설정된 경우 마이크로코드를 변경하는 단계를 포함한다.

본 발명에 따르면, HDT 모드 상태를 변경하는 방법이 제공된다. 이 방법은 HDT 모드 상태 변경 요구를 수신하는 단계와, HDT 모드 인에이블 로크 상태(HDT mode enable lock status)를 결정하는 단계와, 그리고 HDT 모드 인에이블 로크 상태가 언로크 상태(unlock status)로 설정된 경우 HDT 모드 상태를 변경하는 단계를 포함한다.

본 발명에 따르면, 마이크로코드 적재기 인에이블 상태를 변경하는 방법이 제공된다. 이 방법은 마이크로코드 적재기 인에이블 상태 변경 요구를 수신하는 단계와, 마이크로코드 적재기 인에이블 로크 상태를 결정하는 단계와, 그리고 마이크로코드 적재기 인에이블 로크 상태가 언로크 상태로 설정된 경우 마이크로코드 적재기 인에이블 상태를 변경하는 단계를 포함한다.

본 발명에 따르면, 프로세서 동작 방법이 제공된다. 이 방법은 1개 이상의 비휘발성 메모리 셀들로부터 1개 이상의 디폴트 값들을 읽는 단계 및 상기 1개 이상의 디폴트 값들을 풀업 또는 풀다운 레지스터를 통해 스트래핑 값(strapping value)으로서 수신하는 단계로 이루어진 그룹으로부터 선택된 1개 이상의 디폴트 값들을 얻는 단계를 포함한다. 이 방법은 프로세서의 리셋에 응답하여 1개 이상의 디폴트 값들을 1개 이상의 레지스터들에 1개 이상의 다양한 엔트리들로서 기입하는 단계를 포함한다. 상기 1개 이상의 다양한 엔트리들은, 1개 이상의 HDT 인에이블 비트들, 1개 이상의 HDT 인에이블 로크 비트들, 1개 이상의 마이크로코드 적재기 인에이블 비트들 및 1개 이상의 마이크로코드 적재기 인에이블 로크 비트들로 이루어진 그룹으로부터 선택된다.

도면의 간단한 설명

본 발명은 첨부 도면들을 참조하여 설명되는 하기의 상세한 설명으로부터 보다 명확해지는바, 도면들에서 동일한 부호들은 동일한 요소를 나타낸다.

도 1은 종래 기술의 컴퓨터 시스템의 블록도이다.

도 2는 본 발명의 일 양상에 따른, 보안 실행 박스를 갖는 컴퓨터 시스템에서의 데이터 및 커맨드의 흐름을 나타낸 흐름도이다.

도 3은 본 발명의 일 양상에 따른, SMM MSR들을 갖는 컴퓨터 시스템의 일 실시예의 블록도이다.

도 4A 내지 4D는 본 발명의 다양한 양상들에 따른, 로크 레지스터들 및 로직을 포함하는 프로세서들의 실시예들의 블록도들이다.

도 5는 본 발명의 일 양상에 따른, HDT 모드를 시작하는 방법의 일 실시예의 흐름도이다.

도 6은 본 발명의 일 양상에 따른, HDT 인에이블 상태를 변경하는 방법의 일 실시예의 흐름도이다.

도 7은 본 발명의 일 양상에 따른, 마이크로코드 적재기를 시작하는 방법의 일 실시예의 흐름도이다.

도 8은 본 발명의 일 양상에 따른, 마이크로코드 적재기 인에이블 상태를 변경하는 방법의 일 실시예의 흐름도이다.

본 발명은 많은 변형들 및 대안적인 형태들을 가질 수 있지만, 도면들에는 특정한 실시예들이 도시되어 있으며, 본원에서는 이에 대해 상세히 설명한다. 그러 나, 이러한 특정한 실시예들은 본 발명을 개시된 형태들로 한정하지 않으며, 본 발명은 첨부된 청구항들에 의해 정의되는 본 발명의 정신 및 범위 내에 있는 모든 변형들, 등가들 및 대안들을 포함한다.

실시예

이하, 본 발명의 예시적인 실시예들에 대해 설명한다. 명확성을 위해, 본원에서는 실제 실시에 있어서의 모든 특징들을 모두 설명하지는 않는다. 물론, 주목할 사항으로서, 이러한 모든 실제 실시예의 개발시, 예를 들어 시스템 관련 및 사업 관련 제약들을 따르는 것과 같이, 개발자의 특정한 목표들을 달성하기 위해서는 실시마다 특정한 많은 결정들이 이루어져야 하는바, 이는 실시 마다 달라질 것이다. 또한, 주목할 사항으로서, 이러한 개발 노력은 복잡하고 시간을 소모하지만, 그럼에도 불구하고 본원의 개시의 이득을 갖는 당업자들에게는 일상적인 작업이 된다. 참조 부호와 관련하여 글자를 이용한 것은, 그 참조 부호와 관련된 항목의 대안적인 실시예들 또는 예들을 보이기 위해서이다.

시스템 관리 모드(SMM)는 전력을 유지하기 위해 구현되었던 컴퓨터 시스템에서의 동작 모드이다. SMM은 제 4 세대 x86 프로세서들에 대해 생성되었다. 보다 새로운 x86 세대 프로세서들이 출현함에 따라, SMM은 운영 체재에 대해 비교적 투명하게 되었다. 즉, 컴퓨터 시스템은 운영 체재에 거의 또는 아예 영향을 주지 않으면서 SMM에 들어가고 나온다.

도 2는 본 발명의 일 양상에 따른, 보안 실행 박스(260)를 갖는 컴퓨터 시스템에서의 데이터 및 커맨드의 흐름을 보여주는 흐름도의 일 실시예의 블록도이다. 사용자 입력 및 출력(I/O) 데이터 그리고/또는 커맨드들(205)이 1개 이상의 애플리케이션들(210)에 제공되고, 이들(210)로부터 수신된다. 애플리케이션들(210)은, 컴퓨터 시스템(100) 또는 다른 어떠한 컴퓨터 시스템과 같은 컴퓨터 시스템 내에서 암호 서비스 제공자들(215)과 데이터 및 커맨드들을 교환한다. 암호 서비스 제공자들(215)은 API(애플리케이션 프로그래밍 인터페이스) 호출(call)들(220)을 이용하여, 하드웨어(230)에 대한 액세스를 제공하는 드라이버들(225)과 상호작용을 할 수 있다.

본 발명의 일 양상에 따르면, 드라이버들(225) 및 하드웨어(230)는 보안 실행 모드(SEM)(260)를 동작시키도록 구성된 보안 실행 박스의 일부를 구성한다. 신뢰성있는 사생활, 보안 및 소유권(PSO) 동작들(단순히 보안 동작들이라고도 함)은 컴퓨터 시스템이 SEM(260)에 있는 동안 일어날 수 있다. 사용자 입/출력(205) 그리고/또는 애플리케이션들(210)로부터 전달된 소프트웨어 호출들은 SMM에서 보안 실행 박스(260) 내에 놓여질 수 있다. 소프트웨어 호출들은 다양한 보안 하드웨어 자원들에 대해 SEM에서 보안 실행 박스(260)에 대한 액세스를 갖는다.

도 3은 본 발명의 여러 양상들에 따른, SMM MSR들을 갖는 컴퓨터 시스템(300)의 일 실시예의 블록도이다. 도 3은 프로세서(305), 노쓰 브리지(310), 메모리(306) 및 사우쓰 브리지(330)를 포함한다. 프로세서는 1개 이상의 SMM MSR들(머신 지정 레지스터들)(307)을 포함한다. 노쓰 브리지(310)는 메모리 제어기(315)를 포함한다. 노쓰 브리지(310)는 프로세서(305)와 사우쓰 브리지(330) 사이에 결합되는바, 로컬 버스(308)를 통해 프로세서(305)에 결합되고, PCI 버스(110)를 통해 사우쓰 브리지(330)에 결합된다. 노쓰 브리지(310)는 프로세서(305)로부터 SMIACT# 신호를 수신하도록 결합된다.

도 3의 실시예에서, 컴퓨터 시스템(300)은 표준 프로세서 신호들(예를 들어, 노쓰 브리지(310)로의 SMIACT#) 그리고/또는 로컬 버스(308) 및 PCI 버스(110) 상의 버스 주기들을 이용하여 프로세서(305)가 SMM에 있음을 신호한다.

본 발명의 다양한 실시예들에서는, SMM의 보안을 가정한다. 주목할 사항으로서, 1개 이상의 소위 '백도어들'이 존재할 수 있는바, 이들은 SMM의 보안을 잃게하는 데에 이용될 수 있다. 고려되는 문제(issue)들은 프로세서(305)의 하드웨어 디버그 테스트(HDT) 모드의 오용 뿐 아니라 마이크로코드를 로드하고 대체할 수 있는 프로세서(305)의 성능이다. 도 4A 내지 4D는 프로세서(305)의 다양한 실시예들(305A, 305B, 305C 및 305D)을 도시하는바, 이들은 각각 1개 이상의 백도어 공격에 대한 다양한 보안 보호물들을 포함한다.

도 4A에서, 프로세서(305A)는 HDT 제어 로직(410A), HDT 리셋 로직(420A), 및 (HDT 인에이블 레지스터(415) 및 비휘발성 랜덤 액세스 메모리(NVRAM)(430)를 포함하는) 1개 이상의 레지스터들을 포함한다. 도시된 바와 같이, HDT 제어 로직(410A)은 다양한 HDT 핀들(405)을 통해 다수의 입력 신호들을 수신하도록 결합된다. HDT 제어 로직(410A)은 또한 HDT 인에이블 레지스터(415)에 결합된다. HDT 리셋 로직(420A)은 라인(425)을 통해 RESET 신호를 수신하고, HDT 인에이블 레지스터(415) 및 NVRAM(430)을 액세스하도록(즉, 읽기 및 쓰기) 결합된다.

도 4B에서, 프로세서(305B)는 HDT 제어 로직(410B), HDT 리셋 로직(420B), 및 (HDT 인에이블 레지스터(415) 및 HDT 인에이블 로크 레지스터(435)를 포함하는) 2개의 레지스터들을 포함한다. 도시된 바와 같이, HDT 제어 로직(410B)은 다수의 HDT 핀들(405)을 통해 다수의 입력 신호들을 수신하도록 결합된다. HDT 제어 로직(410B)은 또한 HDT 인에이블 레지스터(415) 및 HDT 인에이블 로크 레지스터(435)에 결합된다. HDT 리셋 로직(420B)은 라인(425) 상으로 RESET 신호를 수신하고, 풀럽(또는 풀다운) 레지스터(445)를 통해 라인(440) 상으로 신호를 수신하도록 결합된다.

도 4C에서, 프로세서(305C)는 마이크로코드 제어 로직(455), 마이크로코드 적재기 인에이블 리셋 로직(465), 및 (마이크로코드 적재기 인에이블 레지스터(460)를 포함하는) 1개 이상의 레지스터들을 포함한다. 도시된 바와 같이, 마이

크로코드 제어 로직(455)은 다수의 마이크로코드 입력 핀들(450)을 통해 다수의 입력 신호들을 수신하도록 결합된다. 마이크로코드 제어 로직(455)은 또한 마이크로코드 적재기 인에이블 레지스터(460)에 결합된다. 마이크로코드 적재기 인에이블 리셋 로직(465)은 RESET 신호를 수신하고 마이크로코드 적재기 인에이블 레지스터(460)를 액세스하도록 결합된다.

도 4D에서, 프로세서(305D)는 제어/리셋 로직(475)을 형성하기 위해 마이크로코드 제어 로직(455), HDT 리셋 로직(420) 및 MLE 리셋 로직(465)과 통합된 HDT 제어 로직(410)을 포함한다. HDT 인에이블 레지스터(415) 및 마이크로코드 적재기 인에이블 레지스터(460)는 멀티비트 로크 레지스터(480)로 통합된다. 제어/리셋 로직(475)으로의 다수의 입력들(470)이 도시된다. 이 다수의 입력들(470)은 HDT 입력 들(405), 마이크로코드 입력들(450) 그리고/또는 리셋 시그널링 수단(reset signaling means)을 포함할 수 있다. 다른 실시예들(미도시)은 HDT 제어 로직(410)과 마이크로코드 제어 로직(455) 만을 통합하거나, 단지 HDT 리셋 로직(420)과 MLE 리셋 로직(465) 만을 통합한다.

본 발명의 다양한 실시예들에 따르면, 레지스터들(415, 435 및 460) 뿐 아니라 NVRAM(430)은 1개 이상의 비트들에 대한 저장 공간을 포함한다. 일 실시예에서, 각 레지스터는 단일 비트를 저장하도록 구성된다. 주목할 사항으로서, 인에이블 레지스터들(415 및 460) 또한 단일 로크 레지스터 내에 통합될 수 있으며, HDT 인에이블 로크 레지스터(435)는 마이크로코드 인에이블 로크 레지스터로서 이용될 수 있다. 레지스터들(415, 435, 460 그리고/또는 480)은 SMM MSR들(307)에 포함될 수 있는 것으로 여겨진다.

다양한 실시예들에서, HDT 인에이블 레지스터(415)는 HDT 모드가 인에이블 상태인지 아니면 디스에이블 상태인지를 나타내는 1개 이상의 HDT 인에이블 비트들을 저장하도록 구성된다. HDT 리셋 로직(420)은 프로세서(305)의 리셋시 1개 이상의 HDT 인에이블 비트들을 디폴트 상태로 설정하도록 구성된다.

도 4A 및 4B에 도시된 것들과 같은, HDT 모드들을 제어하기 위한 많은 실시예들이 고려된다. 일 실시예에서, HDT 모드는 엔지니어링(engineering) 및 테스팅에 이용되는 비생성 프로세서들(non-production processors)(305)에서 디폴트로서 인에이블된다. HDT 모드는 표준 생성 프로세서들(305)에서는 디폴트로서 디스에이블될 수 있다. 도 4A에 도시된 다른 실시예에서, 디폴트 상태는 NVRAM(430)에 저장 되며 이로부터 읽혀질 수 있다. 본 실시예에서, 디폴트 상태는 변경가능하지만, 도시된 실시예에서, 디폴트 상태는 디스에이블되는 것으로 설정된다. 도 4B에 도시된 또 다른 실시예에서, 디폴트 상태는 스트래핑 옵션(strapping option)을 이용하여 설정된다. 디폴트 값은 풀업(또는 풀다운) 레지스터(445)를 통해 HDT 리셋 로직(420B)에 제공된다.

도 4C 및 4D에 도시된 것들과 같은, 마이크로코드 적재기 모드들을 제어하는 많은 실시예들이 또한 고려된다. 미도시된 일 실시예에서, 마이크로코드 갱신 모드는 엔지니어링 및 테스팅에 이용되는 비생성 프로세서들(305)에서 디폴트로서 인에이블된다. 마이크로코드 갱신 모드는 표준 생성 프로세서들(305)에서는 디폴트로서 디스에이블될 수 있다. 도 4A에 도시된 것과 유사한 다른 실시예에서, 디폴트 상태는 NVRAM(430)에 저장되고 이로부터 읽혀질 수 있다. 본 실시예에서, 디폴트 상태는 변경가능하지만, 도시된 실시예에서, 디폴트 상태는 디스에이블되는 것으로 설정된다. 도 4B에 도시된 또 다른 실시예에서, 디폴트 상태는 스트래핑 옵션을 이용하여 설정된다. 디폴트 값은 풀업(또는 풀다운) 레지스터(445)를 통해 MLE 리셋 로직(465)에 제공된다.

도 5는 HDT 모드를 시작하는 방법(500)을 도시한다. HDT 모드에 들어가라는 요구의 수신(단계 505)에 응답하여, HDT 제어 로직(410)은 HDT 모드가 인에이블 상태인지 아니면 디스에이블 상태인지를 확인하기 위해 1개 이상의 HDT 인에이블 비트들의 상태를 체크한다(단계 510). HDT 모드가 인에이블 상태이면(단계 515), HDT 제어 로직(410)은 HDT 모드를 시작한다(단계 520). HDT 모드가 디스에이블 상태이 면(단계 515), HDT 제어 로직(410)은 HDT 모드를 시작하지 않는다.

도 6은, HDT 로크 모드를 포함하는, HDT 모드 인에이블 상태를 변경하는 방법(600)을 도시한다. HDT 모드에 들어가라는 요구의 수신에 응답하여(단계 605), HDT 제어 로직(410)은 HDT 로크 모드가 로크 상태인지 아니면 언로크 상태인지를 결정하기 위해 1개 이상의 HDT 인에이블 로크 비트들의 상태를 체크한다(단계 615). HDT 로크 모드가 언로크 상태이면(단계 615), HDT 제어 로직(410)은 HDT 모드를 시작한다(단계 635). HDT 로크 모드가 로크 상태이면(단계 615), HDT 제어 로직(410)은 HDT 로크 모드 상태 변경에 대한 인증을 요구한다(단계 620). 변경이 인증되면(단계 625), HDT 제어 로직(410)은 HDT 모드 로크 비트를 언로크 상태로 변경한다(단계 630). 변경이 인증되지 않으면(단계 625), HDT 제어 로직(410)은 HDT 모드 로크 비트를 변경하지 않는다.

다양한 실시예들에서, HDT 인에이블 상태는 1개 이상의 HDT 인에이블 상태 비트들을 설정함으로써, 또는 리셋함으로써 변경될 수 있다. 예를 들어, HDT 모드는 디스에이블될 수 있지만, SMM 내에서, HDT 제어 로직(410)에 대한 소정의 입력은 HDT 제어 로직(410)에 HDT 모드 상태를 인에이블 상태로 변경할 것을 신호할 수 있다. 도 4A의 실시예에서, 예를 들어, 일단 신호가 되면, HDT 제어 로직(410)은 HDT 인에이블 비트의 상태를 디스에이블 상태에서 인에이블 상태로 변경한다.

도 4B의 실시예를 다시 참조하여, 예를 들어, HDT 모드 상태 변경 요구의 수신에 응답하여, HDT 제어 로직(410)은 HDT 로크 모드가 인에이블 상태인지 아니면 디스에이블 상태인지를 확인하기 위해 1개 이상의 HDT 인에이블 로크 비트들의 상 태를 체크한다. HDT 로크 모드가 디스에이블 상태이면, HDT 제어 로직(410)은 HDT 모드 상태를 변경할 수 있다. HDT 로크 모드가 인에이블 상태이면, HDT 제어 로직(410)은 HDT 모드 상태를 변경하지 않는다.

주목할 사항으로서, 상기 방법(600)은 HDT 로크 모드 상태 변경에 대한 인증을 요구하는 단계(단계 620) 대신, 대안적으로 HDT 로크 모드가 로크 상태에 있는 지를 확인하는 단계(단계 615)를 종료할 수 있다. 방법(600)은 또한, 인증을 요구하기 전에(단계 620), HDT 로크 모드 상태의 변경 요구를 수신하는 단계(미도시)를 포함할 수 있다.

다음으로, 도 7은 마이크로코드 적재기를 시작하는 방법(700)을 도시한다. 마이크로코드 갱신 모드 시작 요구의 수신에 응답하여(단계 705), 마이크로코드 제어로직(455)은 마이크로코드 갱신 모드가 인에이블 상태인지 아니면 디스에이블 상태인지를 확인하기 위해 1개 이상의 마이크로코드 인에이블 비트들의 상태를 체크한다(단계 710). 마이크로코드 갱신 모드가 인에이블되면(단계 715), 마이크로코드 제어 로직(455)은 마이크로코드 갱신 모드를 시작한다(단계 720). 마이크로코드 갱신 모드가 디스에이블되면(단계 715), 마이크로코드 제어 로직(455)은 마이크로코드 갱신 모드를 시작하지 않는다.

다음으로 도 8은, 마이크로코드 로크 모드를 포함하는, 마이크로코드 갱신 모드 인에이블 상태를 변경하는 방법(800)을 도시한다. 마이크로코드 모드에 들어가라는 요구의 수신에 응답하여(단계 805), 마이크로코드 제어 로직(455)은 마이크로코드 모드가 로크 상태인지 아니면 언로크 상태인지를 확인하기 위해 1개 이상의 마이크로코드 인에이블 로크 비트들의 상태를 체크한다(단계 810). 마이크로코드 로크 모드가 언로크 상태이면(단계 815), 마이크로코드 제어 로직(455)은 마이크로 모드를 시작한다(단계 835). 마이크로코드 로크 모드가 로크 상태이면(단계 815), 마이크로코드 제어 로직(455)은 마이크로코드 모드 로크 상태 변경에 대한 인증을 요구한다(단계 820). 변경이 인증되면(단계 825), 마이크로코드 제어 로직(455)은 마이크로코드 모드 로크 비트를 언로크 상태로 변경한다(단계 830). 변경이 인증되지 않으면(단계 825), 마이크로코드 제어 로직(455)은 마이크로코드 모드로크 비트를 변경하지 않는다.

다양한 실시예들에서, 마이크로코드 인에이블 상태는 1개 이상의 마이크로코드 인에이블 상태 비트들을 설정함으로써 또는 리셋함으로써 변경될 수 있다. 예를 들어, 마이크로코드 모드는 디스에이블될 수 있지만, SMM 내에서, 마이크로코드 제어 로직(455)에 대한 소정의 입력은 마이크로코드 제어 로직(455)에 마이크로코드 모드 상태를 인에이블 상태로 변경할 것을 신호할 수 있다. 도 4C의 실시예에서, 예를 들어, 일단 신호가 되면, 마이크로코드 제어 로직(455)은 1개 이상의 마이크로코드 인에이블 비트들의 상태를 디스에이블 상태로부터 인에이블 상태로 변경한다.

마이크로코드 모드 상태의 변경 요구의 수신에 응답하여, 마이크로코드 제어 로직(455)은 마이크로코드 로크 모드가 인에이블 상태인지 아니면 디스에이블 상태인지를 결정하기 위해 1개 이상의 마이크로코드 인에이블 로크 비트들의 상태를 체크할 수 있다. 마이크로코드 로크 모드가 디스에이블되면, 마이크로코드 제어 로직(455)은 마이크로코드 모드 상태를 변경할 수 있다. 마이크로코드 로크 모드가 인에이블되면, 마이크로코드 제어 로직(455)은 마이크로코드 모드 상태를 변경하지 않는다.

주목할 사항으로서, 상기 방법(800)은, 마이크로모드 갱신 로크 상태 변경에 대한 인증을 요구하는 단계(단계 820) 대신, 대안적으로 마이크로코드 갱신 로크 상태가 로크 상태에 있는 지를 결정하는 단계(단계 815)를 종료할 수 있다. 방법(800)은 또한, 인증을 요구하는 단계(단계 820) 이전에, 마이크로코드 갱신 로크 상태 변경 요구를 수신하는 단계(미도시)를 포함할 수 있다.

본 개시의 목적을 위해, ROM에 대한 언급은 플래시 메모리 및 실질적으로 비휘발성인 다른 메모리 타입들에 대해 적용한 것으로서 해석되어야 한다. 주목할 사항으로서, 본원에 개시된 본 발명의 방법들이 흐름도로서 설명되었지만, 이러한 흐름도의 다양한 요소들은 다양한 실시예들에서 생략되거나 또는 다른 순서로 수행될 수 있다. 또한, 주목할 사항으로서, 본원에서 개시된 본 발명의 방법들은 변형되어 구현될 수 있다.

상기 설명된 본 발명의 일부 양상들은 하드웨어 또는 소프트웨어로 구현될 수 있다. 따라서, 본원의 상세한 설명의 일부는 하드웨어 구현 프로세스에 관련하여 제시되었으며, 상세한 설명의 일부는 컴퓨팅 시스템 또는 컴퓨팅 디바이스의 메모리 내에서의 데이터 비트들에 대한 상징적인 동작 표현들을 포함하는 소프트웨어 구현 프로세스에 관련하여 제시되었다. 이러한 설명들 및 표현들은 당업자들이 하드웨어 및 소프트웨어를 이용하여 그들의 작업 내용을 다른 당업자들에게 전달하기 위해 이용되는 수단이다. 프로세스 및 동작은 모두 물리량들의 물리적인 처리를 필요로 한다. 소프트웨어에서, 반드시 그런 것은 아니지만, 이러한 물리량들은 저장, 전달, 결합, 비교될 수 있는(그렇지 않으면 처리될 수 있는) 전기, 자기 또는 광학 신호들의 형태를 가질 수 있다. 주로 공통 이용을 위해, 이러한 신호들을 비트들, 값들, 요소들, 심볼들, 기호들, 용어들, 숫자들 등으로서 설명하는 것이 종종 편리함이 입증되었다.

그러나, 이들 및 유사한 용어들 모두는 적절한 물리량들과 관련되며 이러한 물리량들에 적용된 단지 편리한 라벨들일 뿐 이라는 것을 염두해야한다. 특별하게 지정하지 않는한, 그렇지 않으면 명백한 것으로서, 본 개시 전체를 통해, 이러

한 설명들은 어떠한 전자 디바이스의 저장 장치 내의 물리(전기, 자기 또는 광학)량들로서 표현된 데이터를 처리하고, 저장 장치, 또는 전송 또는 디스플레이 디바이스들 내의 물리량들로서 유사하게 표현되는 다른 데이터로 변환하는 전자 디바이스의 실행 및 프로세스들을 설명한다. 이러한 설명을 나타내는 용어들의 예로는, 한정하는 것은 아니지만, '프로세싱', '컴퓨팅', '계산(calculating)', '결정', '디스플레잉' 등이 있다.

또한, 주목할 사항으로서, 본 발명의 소프트웨어 구현 양상들은 전형적으로 어떠한 형태의 프로그램 저장 매체에 엔코드되거나, 어떠한 타입의 전송 매체에 대해 구현된다. 프로그램 저장 매체는 자기적이거나(예를 들어, 플로피 디스크 또는 하드드라이브) 광학적이며(예를 들어, 컴팩 디스크 판독 전용 메모리, 또는 'CD-ROM'), 판독 전용이거나 랜덤 액세스가 될 수 있다. 유사하게, 전송 매체는 꼬임쌍 선, 동축 케이블, 광섬유, 또는 종래에 알려진 다른 어떠한 적절한 전송 매체가 될 수 있다. 본 발명은 이러한 어떠한 소정의 실시 양상들에 한정되지 않는다.

상기 개시된 특정한 실시예들은 단지 예시적인 것으로서, 본 발명은 다르지만 등가의 방법들, 즉 본원의 개시의 이득을 갖는 당업자들에게 명백한 방법들로 변형 및 실행될 수 있다. 또한, 하기의 청구항들에 정의되는 것 외에는, 본원에 개시된 구성 또는 설계의 세부 사항들에 대한 어떠한 한정도 의도되지 않는다. 따라서, 상기 개시된 특정 실시예들은 변경 또는 수정될 수 있으며, 이러한 모든 변경들은 본 발명의 범위 및 정신 내에 있는 것으로 간주된다. 따라서, 본원이 보호를 받고자 하는 바는 하기의 청구항들에서 설명된다.

(57) 청구의 범위

청구항 1.
프로세서로서,

1개 이상의 하드웨어-디버그-테스트(HDT) 인에이블 비트들을 저장하도록 구성된 제 1 레지스터와;

복수의 HDT 입력 신호들을 수신하도록 결합되며, 상기 제 1 레지스터를 액세스하도록 구성된 제 1 제어 로직과; 그리고

상기 제 1 레지스터에 결합되며, 상기 프로세서의 리셋에 응답하여 상기 제 1 레지스터에 1개 이상의 디폴트 값들을 저장하도록 구성된 제 2 제어 로직을 포함하는 것을 특징으로 하는 프로세서.

청구항 2.
제 1 항에 있어서,

상기 제 1 제어 로직은 또한 HDT 모드에 들어가라는 요구를 수신하도록 구성되고, 상기 HDT 모드에 들어가라는 요구에 응답하여 상기 제 1 레지스터에 저장된 상기 1개 이상의 HDT 인에이블 비트들의 선택된 엔트리들을 읽도록 구성되며, 그리고 상기 1개 이상의 HDT 인에이블 비트들의 선택된 엔트리들에 기초하여 상기 HDT 모드에 들어가라는 요구를 승인 또는 거절하도록 구성되는 것을 특징으로 하는 프로세서.

청구항 3.
제 1 항에 있어서,

상기 1개 이상의 HDT 인에이블 비트들에 대한 상기 1개 이상의 디폴트 값들을 저장하도록 구성된 1개 이상의 비휘발성 메모리 셀들을 더 포함하며,

상기 제 2 제어 로직은 또한 상기 1개 이상의 비휘발성 메모리 셀들로부터 상기 1개 이상의 HDT 인에이블 비트들에 대한 상기 1개 이상의 디폴트 값들을 읽고, 상기 프로세서의 리셋에 응답하여 상기 1개 이상의 HDT 인에이블 비트들에 대한 상기 1개 이상의 디폴트 값들을 상기 제 1 레지스터에 기입하도록 구성되는 것을 특징으로 하는 프로세서.

청구항 4.
제 1 항에 있어서,

상기 제 2 제어 로직은 또한 상기 1개 이상의 HDT 인에이블 비트들에 대한 상기 1개 이상의 디폴트 값들을 나타내는 신호를 수신하고, 상기 프로세서의 리셋에 응답하여 상기 1개 이상의 HDT 인에이블 비트들에 대한 상기 1개 이상의 디폴트 값들을 상기 제 1 레지스터에 기입하도록 구성되는 것을 특징으로 하는 프로세서.

청구항 5.
제 1 항에 있어서,

1개 이상의 마이크로코드 적재기 인에이블 비트들을 저장하도록 구성된 제 3 레지스터와;

복수의 마이크로코드 입력들을 수신하도록 결합되며, 상기 제 3 레지스터를 액세스하도록 결합된 제 3 제어 로직과; 그리고

상기 제 3 레지스터에 결합되고, 상기 프로세서의 리셋에 응답하여 상기 1개 이상의 디폴트 값들을 상기 제 3 레지스터에 저장하도록 구성된 제 4 제어 로직을 더 포함하는 것을 특징으로 하는 프로세서.

청구항 6.
제 5 항에 있어서,

상기 제 3 제어 로직은 또한 마이크로코드 변경 요구를 수신하도록 구성되고, 상기 마이크로코드 변경 요구에 응답하여 상기 제 3 레지스터에 저장된 상기 1개 이상의 마이크로코드 적재기 인에이블 비트들의 선택된 엔트리들을 읽도록 구성되며, 그리고 상기 1개 이상의 마이크로코드 적재기 인에이블 비트들의 선택된 엔트리들에 기초하여 상기 마이크로코드 변경 요구를 승인 또는 거절하도록 구성되는 것을 특징으로 하는 프로세서.

청구항 7.
제 1 항에 있어서,

상기 제 1 제어 로직에 결합되고, 1개 이상의 HDT 인에이블 로크 비트들을 저장하도록 구성된 제 2 레지스터를 더 포함하는 것을 특징으로 하는 프로세서.

청구항 8.
제 7 항에 있어서,

상기 제 1 제어 로직은 또한 HDT 모드 상태 변경 요구를 수신하도록 구성되고, 상기 HDT 모드 상태 변경 요구에 응답하여 상기 제 2 레지스터에 저장된 상기 1개 이상의 HDT 인에이블 로크 비트들의 선택된 엔트리들을 읽도록 구성되며, 그리고 상기 1개 이상의 HDT 인에이블 로크 비트들의 선택된 엔트리들에 기초하여 상기 HDT 모드 상태 변경 요구를 승인 또는 거절하도록 구성되는 것을 특징으로 하는 프로세서.

청구항 9.
프로세서로서,

복수의 마이크로코드 입력들을 수신하도록 결합된 제 1 제어 로직과;

상기 제 1 제어 로직에 결합되며, 1개 이상의 마이크로코드 적재기 인에이블 비트들을 저장하도록 구성된 제 1 레지스터와; 그리고

상기 제 1 레지스터에 결합되며, 상기 프로세서의 리셋에 응답하여 1개 이상의 디폴트 값들을 상기 제 1 레지스터에 저장하도록 구성된 제 2 제어 로직을 포함하는 것을 특징으로 하는 프로세서.

청구항 10.
제 9 항에 있어서,

상기 제 1 제어 로직은 또한 마이크로코드 변경 요구를 수신하도록 구성되고, 상기 마이크로코드 변경 요구에 응답하여 상기 제 1 레지스터에 저장된 상기 1개 이상의 마이크로코드 적재기 인에이블 비트들의 선택된 엔트리들을 읽도록 구성되며, 그리고 상기 1개 이상의 마이크로코드 적재기 인에이블 비트들의 선택된 엔트리들에 기초하여 상기 마이크로코드 변경 요구를 승인 또는 거절하도록 구성되는 것을 특징으로 하는 프로세서.

청구항 11.
제 9 항에 있어서,

상기 1개 이상의 마이크로코드 적재기 인에이블 비트들에 대한 상기 1개 이상의 디폴트 값들을 저장하도록 구성된 1개 이상의 비휘발성 메모리 셀들을 더 포함하며,

상기 제 2 제어 로직은 또한 상기 1개 이상의 비휘발성 메모리 셀들로부터 상기 1개 이상의 마이크로코드 적재기 인에이블 비트들에 대한 상기 1개 이상의 디폴트 값들을 읽고, 상기 프로세서의 리셋에 응답하여 상기 1개 이상의 마이

크로코드 적재기 인에이블 비트들에 대한 상기 1개 이상의 디폴트 값들을 마이크로코드 적재기 레지스터에 기입하도록 구성되는 것을 특징으로 하는 프로세서.

청구항 12.
제 9 항에 있어서,

상기 제 2 제어 로직은 또한 상기 1개 이상의 마이크로코드 적재기 인에이블 비트들에 대한 상기 1개 이상의 디폴트 값들을 나타내는 신호를 수신하고, 상기 프로세서의 리셋에 응답하여 상기 1개 이상의 마이크로코드 적재기 인에이블 비트들에 대한 상기 1개 이상의 디폴트 값들을 상기 제 1 레지스터에 저장하도록 구성되는 것을 특징으로 하는 프로세서.

청구항 13.
제 9 항에 있어서,

상기 제 1 제어 로직에 결합되며, 1개 이상의 마이크로코드 적재기 인에이블 로크 비트들을 저장하도록 구성된 제 2 레지스터를 더 포함하는 것을 특징으로 하는 프로세서.

청구항 14.
제 13 항에 있어서,

상기 제 1 제어 로직은 또한 마이크로코드 적재기 로크 상태 변경 요구를 수신하도록 구성되고, 상기 마이크로코드 적재기 로크 상태 변경 요구에 응답하여 상기 제 2 레지스터에 저장된 상기 1개 이상의 마이크로코드 적재기 인에이블 로크 비트들의 선택된 엔트리들을 읽도록 구성되며, 그리고 상기 1개 이상의 마이크로코드 적재기 인에이블 로크 비트들의 선택된 엔트리들에 기초하여 상기 마이크로코드 적재기 로크 상태 변경 요구를 승인 또는 거절하도록 구성되는 것을 특징으로 하는 프로세서.

청구항 15.
HDT 모드 인에이블 상태를 결정하는 방법으로서,

HDT 모드 시작 요구를 수신하는 단계와;

상기 HDT 모드 인에이블 상태를 결정하는 단계와; 그리고

상기 HDT 모드 인에이블 상태가 인에이블 상태로 설정된 경우, 상기 HDT 모드를 시작하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 16.
제 15 항에 있어서,

상기 HDT 모드 인에이블 상태를 결정하는 단계는 레지스터로부터 1개 이상의 HDT 인에이블 비트들에 대응하는 1개 이상의 엔트리들을 읽는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 17.
마이크로코드 변경 방법으로서,

마이크로코드 변경 요구를 수신하는 단계와;

마이크로코드 적재기 인에이블 상태를 결정하는 단계와; 그리고

상기 마이크로코드 적재기 인에이블 상태가 인에이블 상태로 설정된 경우, 상기 마이크로코드를 변경하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 18.
제 17 항에 있어서,

상기 마이크로코드 적재기 인에이블 상태를 결정하는 단계는 레지스터로부터 1개 이상의 마이크로코드 적재기 인에이블 비트들에 대응하는 1개 이상의 엔트리들을 읽는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 19.
HDT 모드 상태 변경 방법으로서,

HDT 모드 상태 변경 요구를 수신하는 단계와;

HDT 모드 인에이블 로크 상태를 결정하는 단계와; 그리고

상기 HDT 모드 인에이블 로크 상태가 언로크 상태로 설정된 경우, 상기 HDT 모드 상태를 변경하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 20.
제 19 항에 있어서,

상기 HDT 모드 인에이블 로크 상태를 결정하는 단계는 레지스터로부터 1개 이상의 HDT 인에이블 로크 비트들에 대응하는 1개 이상의 엔트리들을 읽는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 21.
제 19 항에 있어서,

상기 HDT 모드 상태를 변경하는 단계는 1개 이상의 HDT 인에이블 비트들에 대응하는 1개 이상의 엔트리들을 레지스터에 기입하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 22.
마이크로코드 적재기 인에이블 상태를 변경하는 방법으로서,

마이크로코드 적재기 인에이블 상태 요구를 수신하는 단계와;

마이크로코드적재기 인에이블 로크 상태를 결정하는 단계와; 그리고

상기 마이크로코드 적재기 인에이블 로크 상태가 언로크 상태로 설정된 경우, 상기 마이크로코드 적재기 인에이블 상태를 변경하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 23.
제 22 항에 있어서,

상기 마이크로코드 적재기 인에이블 로크 상태를 결정하는 단계는 레지스터로부터 1개 이상의 마이크로코드 적재기 인에이블 로크 비트들에 대응하는 1개 이상의 엔트리들을 읽는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 24.
제 22 항에 있어서,

상기 마이크로코드 적재기 인에이블 상태를 변경하는 단계는 1개 이상의 마이크로코드 적재기 인에이블 비트들에 대응하는 1개 이상의 엔트리들을 레지스터에 기입하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 25.
프로세서 동작 방법으로서,

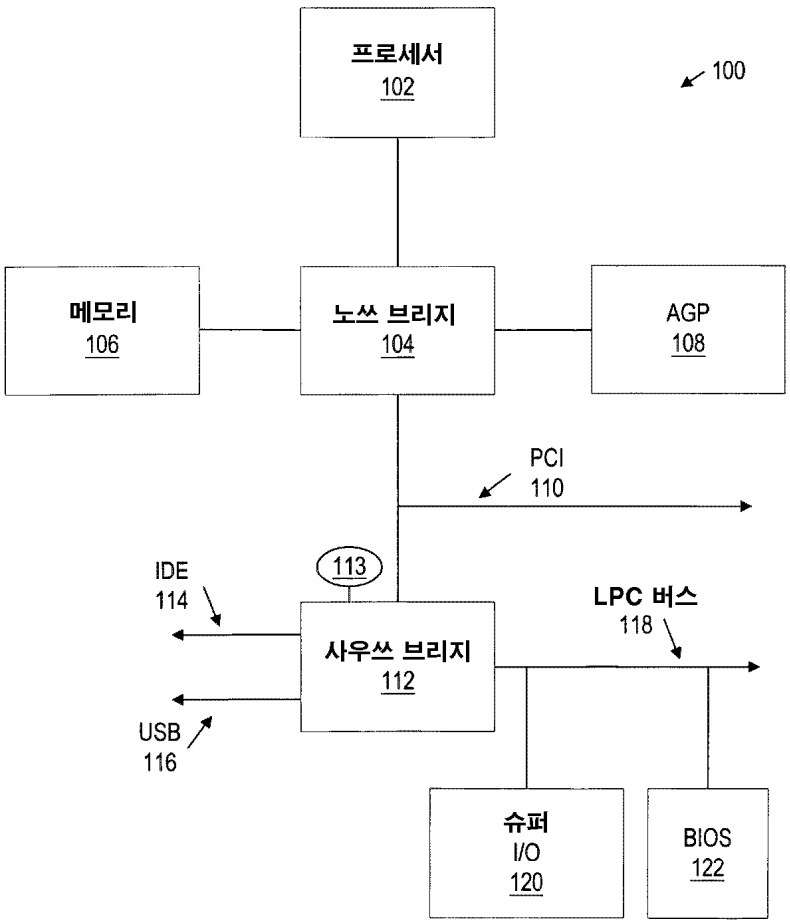
1개 이상의 비휘발성 메모리 셀들로부터 1개 이상의 디폴트 값들을 읽는 단계 및 풀업 또는 풀다운 레지스터를 통해 상기 1개 이상의 디폴트 값들을 스트래핑 값으로서 수신하는 단계로 이루어진 그룹으로부터 선택되는 상기 1개 이상의 디폴트 값들을 얻는 단계와; 그리고

상기 프로세서의 리셋에 응답하여 상기 1개 이상의 디폴트 값들을 1개 이상의 레지스터들에 1개 이상의 다양한 엔트리들로서 기입하는 단계를 포함하며,

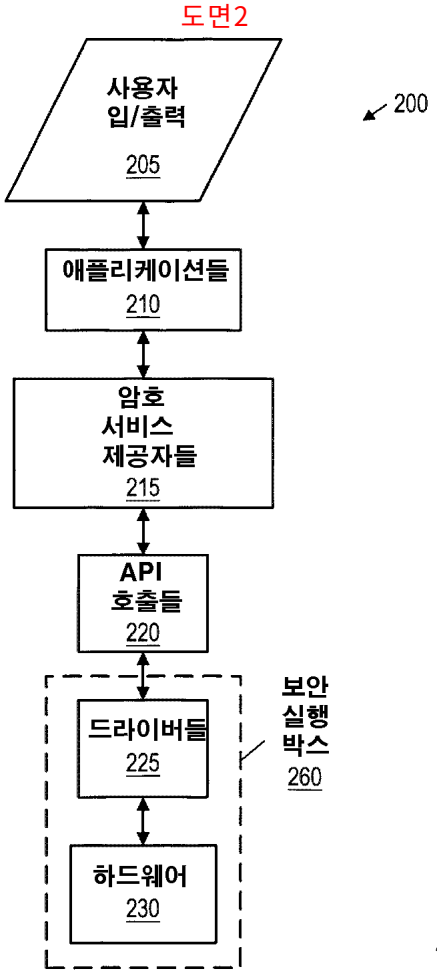
상기 1개 이상의 다양한 엔트리들은 1개 이상의 HDT 인에이블 비트들, 1개 이상의 HDT 인에이블 로크 비트들, 1개 이상의 마이크로코드 적재기 인에이블 비트들 및 1개 이상의 마이크로코드 적재기 인에이블 로크 비트들로 이루어진 그룹으로부터 선택되는 것을 특징으로 하는 방법.

도면

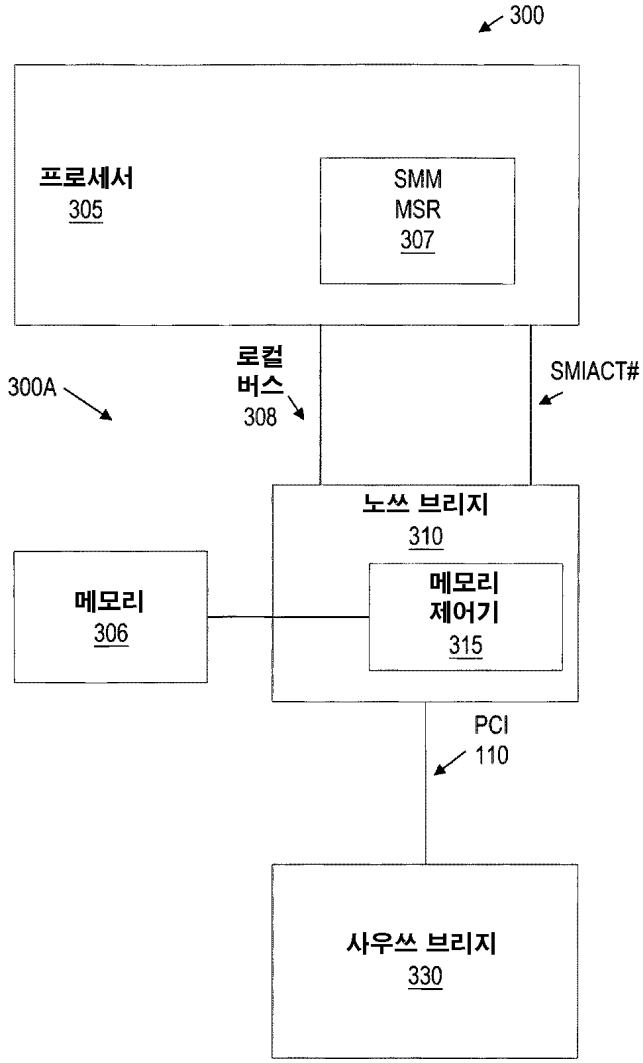
도면1


프로세서
102
100
메모리
106
노쓰 브리지
104
AGP
108
PCI
110
113
IDE
114
LPC 버스
118
사우쓰 브리지
112
USB
116
슈퍼
I/O
120
BIOS
122

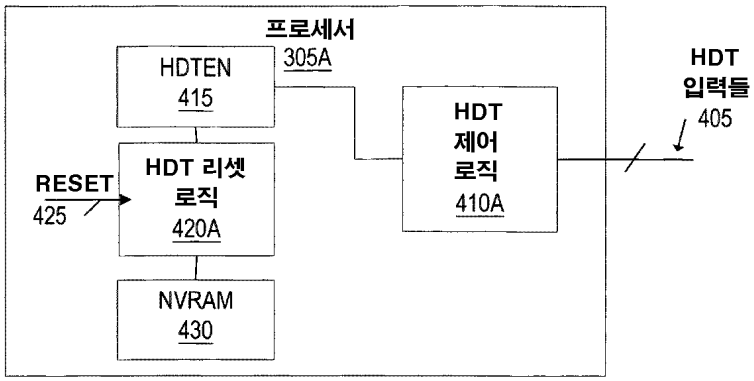
도면2


사용자
입/출력
205
200
애플리케이션들
210
암호
서비스
제공자들
215
API
호출들
220
보안
실행
박스
260
드라이버들
225
하드웨어
230

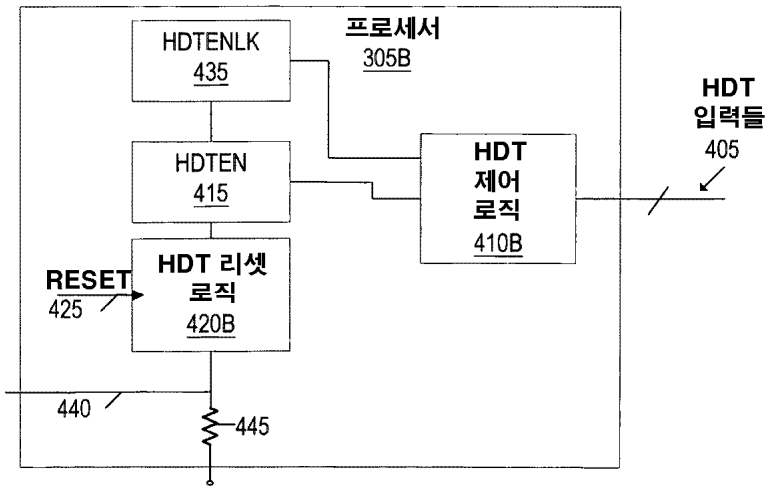
도면3


300
프로세서
305
SMM
MSR
307
300A
로컬
버스
308
SMIACT#
노쓰 브리지
310
메모리
306
메모리
제어기
315
PCI
110
사우쓰 브리지
330

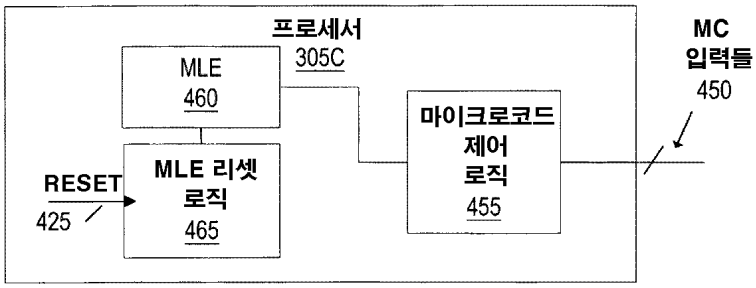
도면4A


프로세서
305A
HDTEN
415
HDT 리셋
로직
420A
RESET
425
NVRAM
430
HDT
제어
로직
410A
HDT
입력들
405

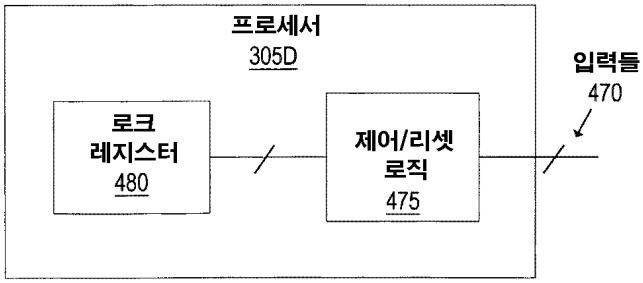
도면4B



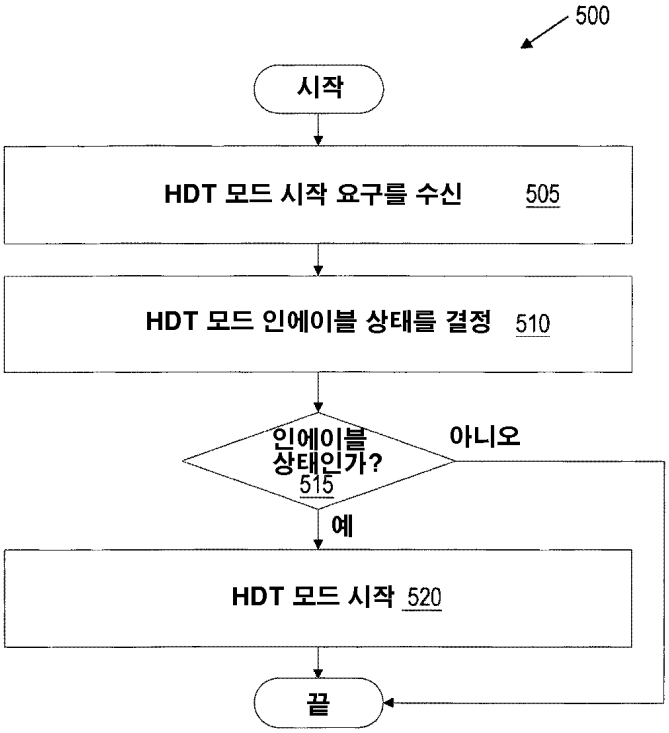
도면4C



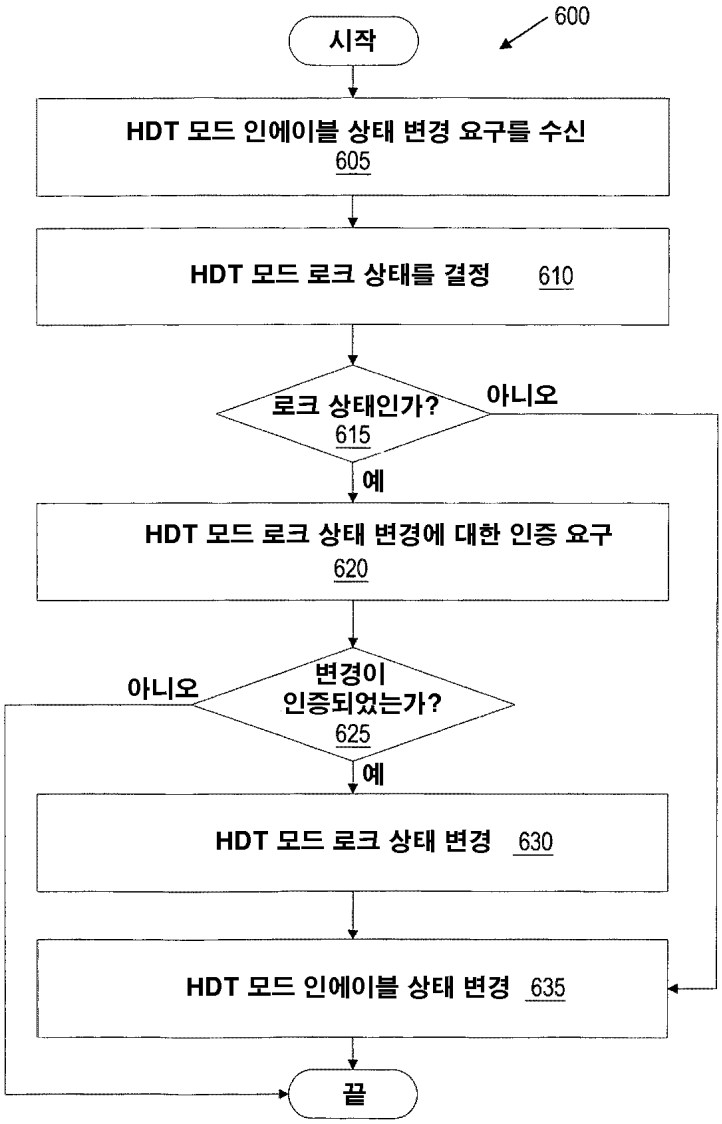
도면4D



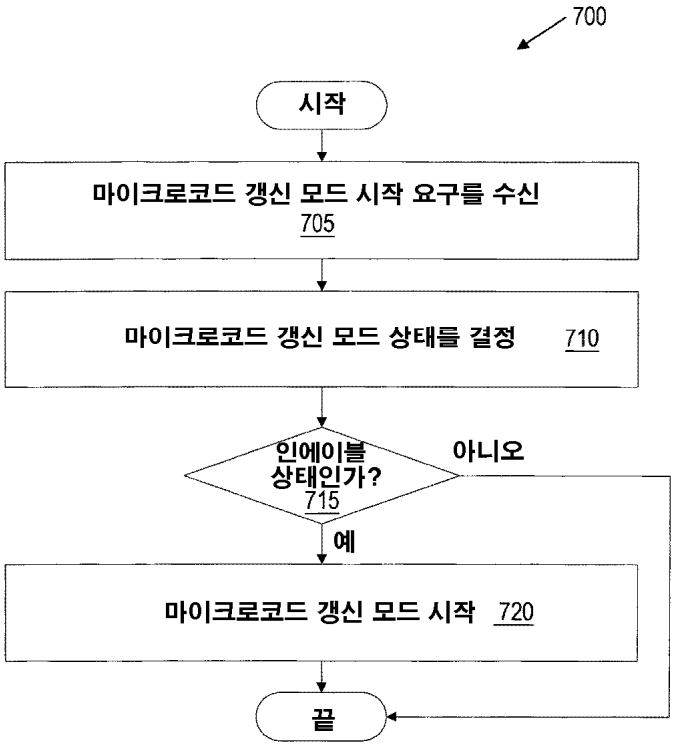
도면5


500
시작
HDT 모드 시작 요구를 수신 505
HDT 모드 인에이블 상태를 결정 510
인에이블 상태인가? 515
아니오
예
HDT 모드 시작 520
끝

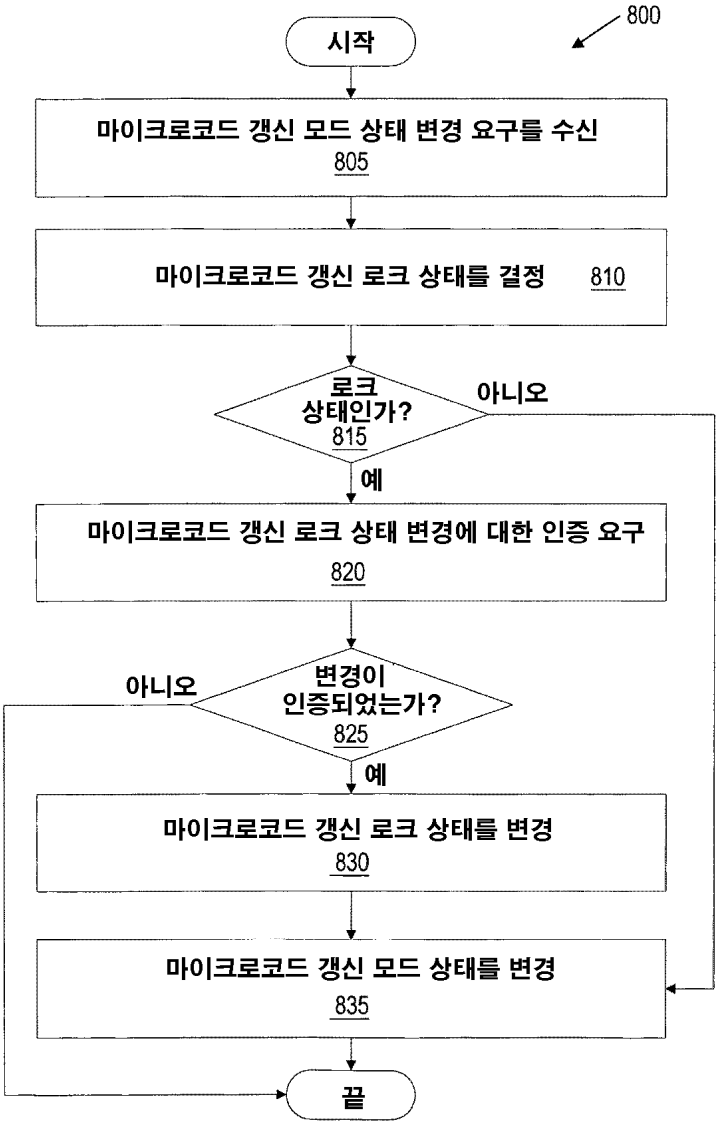
도면6


600
시작
HDT 모드 인에이블 상태 변경 요구를 수신 605
HDT 모드 로크 상태를 결정 610
로크 상태인가? 615
아니오
예
HDT 모드 로크 상태 변경에 대한 인증 요구 620
변경이 인증되었는가? 625
아니오
예
HDT 모드 로크 상태 변경 630
HDT 모드 인에이블 상태 변경 635
끝

도면7


700
시작
마이크로코드 갱신 모드 시작 요구를 수신
705
마이크로코드 갱신 모드 상태를 결정
710
인에이블 상태인가?
715
아니오
예
마이크로코드 갱신 모드 시작
720
끝

도면8


800
시작
마이크로코드 갱신 모드 상태 변경 요구를 수신
805
마이크로코드 갱신 로크 상태를 결정
810
로크 상태인가?
815
아니오
예
마이크로코드 갱신 로크 상태 변경에 대한 인증 요구
820
변경이 인증되었는가?
825
아니오
예
마이크로코드 갱신 로크 상태를 변경
830
마이크로코드 갱신 모드 상태를 변경
835
끝