



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0025554  
(43) 공개일자 2016년03월08일

(51) 국제특허분류(Int. Cl.)  
G06F 21/71 (2013.01) G06F 21/74 (2013.01)  
G06T 1/20 (2006.01)  
(52) CPC특허분류  
G06F 21/71 (2013.01)  
G06F 21/74 (2013.01)  
(21) 출원번호 10-2016-7000555  
(22) 출원일자(국제) 2014년06월30일  
심사청구일자 없음  
(85) 번역문제출일자 2016년01월08일  
(86) 국제출원번호 PCT/US2014/044776  
(87) 국제공개번호 WO 2015/002851  
국제공개일자 2015년01월08일  
(30) 우선권주장  
61/841,881 2013년07월01일 미국(US)  
14/014,032 2013년08월29일 미국(US)

(71) 출원인  
켈컴 인코퍼레이티드  
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스  
드라이브 5775  
(72) 발명자  
정 토마스  
미국 92121 캘리포니아주 샌디에고 모어하우스 드  
라이브 5775  
투스니 아제딘  
미국 92121 캘리포니아주 샌디에고 모어하우스 드  
라이브 5775  
토르제브스키 윌리엄  
미국 92121 캘리포니아주 샌디에고 모어하우스 드  
라이브 5775  
(74) 대리인  
특허법인코리어나

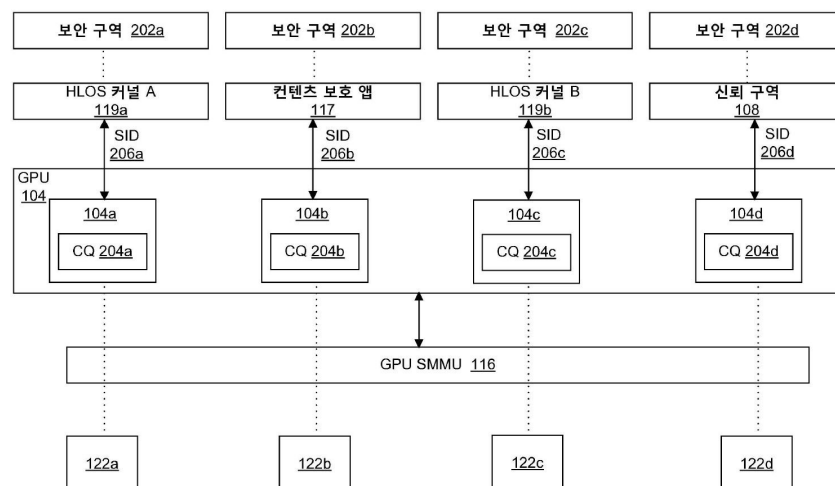
전체 청구항 수 : 총 40 항

(54) 발명의 명칭 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템 및 방법

(57) 요약

시스템들, 방법들 및 컴퓨터 프로그램들은 그래픽 프로세싱 유닛 (GPU) 에 보안 액세스 제어를 제공하기 위해 개시된다. 일 시스템은 GPU, 복수의 GPU 프로그래밍 인터페이스들, 및 커맨드 프로세서를 포함한다. 각각의 GPU 프로그래밍 인터페이스는 복수의 보안 구역들 중 상이한 보안 구역에 동적으로 할당된다. 각각의 GPU 프로그래밍 인터페이스는 대응하는 보안 구역과 연관된 하나 이상의 애플리케이션들에 의해 발행된 작업 오더들을 수신하도록 구성된다. 작업 오더들은 GPU 에 의해 실행될 명령들을 포함한다. 커맨드 프로세서는 복수의 GPU 프로그래밍 인터페이스들과 통신한다. 커맨드 프로세서는 별개의 보안 메모리 영역들을 사용하여 복수의 GPU 프로그래밍 인터페이스들에 의해 수신된 작업 오더들의 실행을 제어하도록 구성된다. 각각의 보안 메모리 영역은 복수의 보안 구역들 중 하나에 할당된다.

대표도



(52) CPC특허분류

*G06T 1/20* (2013.01)

*G06F 2221/2113* (2013.01)

---

## 명세서

### 청구범위

#### 청구항 1

그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 방법으로서,

그래픽 프로세싱 유닛으로의 액세스를 제어하기 위한 복수의 보안 구역들을 정의하는 단계;

GPU 에 의해 제공되는 복수의 GPU 프로그래밍 인터페이스들 중 대응하는 GPU 프로그래밍 인터페이스에 상기 보안 구역들의 각각을 할당하는 단계로서, 상기 GPU 프로그래밍 인터페이스들의 각각은 대응하는 상기 보안 구역과 연관된 하나 이상의 애플리케이션들에 의해 발행된 작업 오더들을 수신하기 위한 것이고, 상기 작업 오더들은 상기 GPU 에 의해 실행될 명령들을 포함하는, 상기 보안 구역들의 각각을 할당하는 단계; 및

별개의 보안 메모리 영역들을 사용하여 상기 복수의 GPU 프로그래밍 인터페이스들에 의해 수신된 상기 작업 오더들의 실행을 제어하는 단계로서, 각각의 상기 보안 메모리 영역은 상기 복수의 보안 구역들 중 하나에 할당되는, 상기 작업 오더들의 실행을 제어하는 단계를 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 방법.

#### 청구항 2

제 1 항에 있어서,

상기 GPU 프로그래밍 인터페이스들은 상기 대응하는 GPU 프로그래밍 인터페이스에 의해 수신된 작업 오더들을 저장하기 위한 개별 커맨드 큐를 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 방법.

#### 청구항 3

제 1 항에 있어서,

상기 작업 오더들은 중앙 프로세싱 유닛 (CPU) 에 의해 상기 보안 구역들에 따른 상기 대응하는 GPU 프로그래밍 인터페이스 내로 투입되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 방법.

#### 청구항 4

제 3 항에 있어서,

상기 작업 오더들은 상기 대응하는 GPU 프로그래밍 인터페이스를 식별하는 스트림 식별자를 사용하여 투입되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 방법.

#### 청구항 5

제 1 항에 있어서,

별개의 메모리 영역들은 보안 메모리 관리 유닛에 의해 할당되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 방법.

#### 청구항 6

제 5 항에 있어서,

상기 별개의 메모리 영역들 중 하나 이상은 상기 보안 메모리 관리 유닛에서 연관된 컨텍스트 뱅크를 사용하는 하드웨어-강제 보호들을 갖는 분리된 어드레스 공간을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 방법.

#### 청구항 7

제 6 항에 있어서,

상기 분리된 어드레스 공간은: 2 이상의 오퍼레이팅 시스템들을 관리하기 위한 하이퍼바이저 소프트웨어 계층;

및 신뢰 하드웨어와 비-신뢰 하드웨어 간의 분리 중 하나 이상을 통해 구현되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 방법.

#### 청구항 8

제 1 항에 있어서,

상기 보안 구역들 중 2 이상은 병렬로 관리되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 방법.

#### 청구항 9

제 1 항에 있어서,

상기 보안 구역들 중 하나 이상은 비-보안 구역 또는 보안 구역을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 방법.

#### 청구항 10

제 1 항에 있어서,

상기 작업 오더들을 발행하는 하나 이상의 애플리케이션들은, 콘텐츠 보호 구역 애플리케이션, 오퍼레이팅 시스템과 연관된 콘텐츠 보호 구역 커널, 하이 레벨 오퍼레이팅 시스템 커널, 및 신뢰 구역 보안 모니터 중 하나 이상을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 방법.

#### 청구항 11

그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템으로서,

그래픽 프로세싱 유닛 (GPU) 으로의 액세스를 제어하기 위한 복수의 보안 구역들을 정의하는 수단;

상기 GPU 에 의해 제공되는 복수의 GPU 프로그래밍 인터페이스들 중 대응하는 GPU 프로그래밍 인터페이스에 상기 보안 구역들의 각각을 할당하는 수단으로서, 상기 GPU 프로그래밍 인터페이스들의 각각은 대응하는 상기 보안 구역과 연관된 하나 이상의 애플리케이션들에 의해 발행된 작업 오더들을 수신하기 위한 것이고, 상기 작업 오더들은 상기 GPU 에 의해 실행될 명령들을 포함하는, 상기 보안 구역들의 각각을 할당하는 수단; 및

별개의 보안 메모리 영역들을 사용하여 상기 복수의 GPU 프로그래밍 인터페이스들에 의해 수신된 상기 작업 오더들의 실행을 제어하는 수단으로서, 각각의 상기 보안 메모리 영역은 상기 복수의 보안 구역들 중 하나에 할당되는, 상기 작업 오더들의 실행을 제어하는 수단을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

#### 청구항 12

제 11 항에 있어서,

상기 GPU 프로그래밍 인터페이스들은 상기 대응하는 GPU 프로그래밍 인터페이스에 의해 수신된 작업 오더들을 저장하기 위한 개별 수단을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

#### 청구항 13

제 11 항에 있어서,

상기 작업 오더들은 중앙 프로세싱 유닛 (CPU) 에 의해 상기 보안 구역들에 따른 상기 대응하는 GPU 프로그래밍 인터페이스 내로 투입되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

#### 청구항 14

제 13 항에 있어서,

상기 작업 오더들은 상기 대응하는 GPU 프로그래밍 인터페이스를 식별하는 스트림 식별자를 사용하여 투입되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

#### 청구항 15

제 11 항에 있어서,

별개의 메모리 영역들은 보안 메모리 관리 유닛에 의해 할당되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

#### 청구항 16

제 15 항에 있어서,

상기 별개의 메모리 영역들 중 하나 이상은 상기 보안 메모리 관리 유닛에서 연관된 컨텍스트 뱅크를 사용하는 하드웨어-강제 보호들을 갖는 분리된 어드레스 공간을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

#### 청구항 17

제 16 항에 있어서,

상기 분리된 어드레스 공간은: 2 이상의 오퍼레이팅 시스템들을 관리하기 위한 하이퍼바이저 소프트웨어 계층; 및 신뢰 하드웨어와 비-신뢰 하드웨어 간의 분리 중 하나 이상을 통해 구현되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

#### 청구항 18

제 11 항에 있어서,

상기 보안 구역들 중 2 이상은 병렬로 관리되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

#### 청구항 19

제 11 항에 있어서,

상기 보안 구역들 중 하나 이상은 비-보안 구역 또는 보안 구역을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

#### 청구항 20

제 11 항에 있어서,

상기 작업 오더들을 발행하는 하나 이상의 애플리케이션들은, 콘텐츠 보호 구역 애플리케이션, 오퍼레이팅 시스템과 연관된 콘텐츠 보호 구역 커널, 하이 레벨 오퍼레이팅 시스템 커널, 및 신뢰 구역 보안 모니터 중 하나 이상을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

#### 청구항 21

그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 컴퓨터 프로그램으로서,

상기 컴퓨터 프로그램은 프로세서에 의한 실행을 위해 컴퓨터 판독가능 매체에 수록되고, 상기 컴퓨터 프로그램은 로직을 포함하며,

상기 로직은,

그래픽 프로세싱 유닛 (GPU) 으로의 액세스를 제어하기 위한 복수의 보안 구역들을 정의하고;

상기 GPU 에 의해 제공되는 복수의 GPU 프로그래밍 인터페이스들 중 대응하는 GPU 프로그래밍 인터페이스에 상기 보안 구역들의 각각을 할당하는 것으로서, 상기 GPU 프로그래밍 인터페이스들의 각각은 대응하는 상기 보안 구역과 연관된 하나 이상의 애플리케이션들에 의해 발행된 작업 오더들을 수신하기 위한 것이고, 상기 작업 오더들은 상기 GPU 에 의해 실행될 명령들을 포함하는, 상기 보안 구역들의 각각을 할당하며; 그리고

별개의 보안 메모리 영역들을 사용하여 상기 복수의 GPU 프로그래밍 인터페이스들에 의해 수신된 상기 작업 오더들의 실행을 제어하는 것으로서, 각각의 상기 보안 메모리 영역은 상기 복수의 보안 구역들 중 하나에 할당되는, 상기 작업 오더들의 실행을 제어하도록

구성되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 컴퓨터 프로그램.

## 청구항 22

제 21 항에 있어서,

상기 GPU 프로그래밍 인터페이스들은 상기 대응하는 GPU 프로그래밍 인터페이스에 의해 수신된 작업 오더들을 저장하기 위한 개별 커맨드 큐를 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 컴퓨터 프로그램.

## 청구항 23

제 21 항에 있어서,

상기 작업 오더들은 중앙 프로세싱 유닛 (CPU) 에 의해 상기 보안 구역들에 따른 상기 대응하는 GPU 프로그래밍 인터페이스 내로 투입되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 컴퓨터 프로그램.

## 청구항 24

제 23 항에 있어서,

상기 작업 오더들은 상기 대응하는 GPU 프로그래밍 인터페이스를 식별하는 스트림 식별자를 사용하여 투입되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 컴퓨터 프로그램.

## 청구항 25

제 21 항에 있어서,

별개의 메모리 영역들은 보안 메모리 관리 유닛에 의해 할당되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 컴퓨터 프로그램.

## 청구항 26

제 25 항에 있어서,

상기 별개의 메모리 영역들 중 하나 이상은 상기 보안 메모리 관리 유닛에서 연관된 컨텍스트 뱅크를 사용하는 하드웨어-강제 보호들을 갖는 분리된 어드레스 공간을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 컴퓨터 프로그램.

## 청구항 27

제 26 항에 있어서,

상기 분리된 어드레스 공간은: 2 이상의 오퍼레이팅 시스템들을 관리하기 위한 하이퍼바이저 소프트웨어 계층; 및 신뢰 하드웨어와 비-신뢰 하드웨어 간의 분리 중 하나 이상을 통해 구현되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 컴퓨터 프로그램.

## 청구항 28

제 21 항에 있어서,

상기 보안 구역들 중 2 이상은 병렬로 관리되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 컴퓨터 프로그램.

## 청구항 29

제 21 항에 있어서,

상기 보안 구역들 중 하나 이상은 비-보안 구역 또는 보안 구역을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 컴퓨터 프로그램.

## 청구항 30

제 21 항에 있어서,

상기 작업 오더들을 발행하는 하나 이상의 애플리케이션들은, 콘텐츠 보호 구역 애플리케이션, 오퍼레이팅 시스템과 연관된 콘텐츠 보호 구역 커널, 하이 레벨 오퍼레이팅 시스템 커널, 및 신뢰 구역 보안 모니터 중 하나 이상을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 컴퓨터 프로그램.

### 청구항 31

그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템으로서,

그래픽 프로세싱 유닛 (GPU);

상기 GPU 에 의해 제공되는 복수의 GPU 프로그래밍 인터페이스들로서, 각각의 GPU 프로그래밍 인터페이스는 복수의 보안 구역들 중 상이한 보안 구역에 동적으로 할당되고 대응하는 상기 보안 구역과 연관된 하나 이상의 애플리케이션들에 의해 발행된 작업 오더들을 수신하도록 구성되며, 상기 작업 오더들은 상기 GPU 에 의해 실행될 명령들을 포함하는, 상기 복수의 GPU 프로그래밍 인터페이스들; 및

상기 복수의 GPU 프로그래밍 인터페이스들과 통신하는 커맨드 프로세서로서, 상기 커맨드 프로세서는 별개의 보안 메모리 영역들을 사용하여 상기 복수의 GPU 프로그래밍 인터페이스들에 의해 수신된 상기 작업 오더들의 실행을 제어하도록 구성되고, 각각의 상기 보안 메모리 영역은 상기 복수의 보안 구역들 중 하나에 할당되는, 상기 커맨드 프로세서를 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

### 청구항 32

제 31 항에 있어서,

상기 GPU 프로그래밍 인터페이스들은 대응하는 GPU 프로그래밍 인터페이스에 의해 수신된 작업 오더들을 저장하기 위한 개별 커맨드 큐를 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

### 청구항 33

제 31 항에 있어서,

상기 작업 오더들은 중앙 프로세싱 유닛 (CPU) 에 의해 상기 보안 구역들에 따른 상기 대응하는 GPU 프로그래밍 인터페이스 내로 투입되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

### 청구항 34

제 33 항에 있어서,

상기 작업 오더들은 상기 대응하는 GPU 프로그래밍 인터페이스를 식별하는 스트림 식별자를 사용하여 투입되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

### 청구항 35

제 31 항에 있어서,

별개의 메모리 영역들은 보안 메모리 관리 유닛에 의해 할당되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

### 청구항 36

제 35 항에 있어서,

상기 별개의 메모리 영역들 중 하나 이상은 상기 보안 메모리 관리 유닛에서 연관된 컨텍스트 뱅크를 사용하는 하드웨어-강제 보호들을 갖는 분리된 어드레스 공간을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

### 청구항 37

제 36 항에 있어서,

상기 분리된 어드레스 공간은: 2 이상의 오퍼레이팅 시스템들을 관리하기 위한 하이퍼바이저 소프트웨어 계층; 및 신뢰 하드웨어와 비-신뢰 하드웨어 간의 분리 중 하나 이상을 통해 구현되는, 그래픽 프로세싱 유닛에 보안

액세스 제어를 제공하는 시스템.

#### 청구항 38

제 31 항에 있어서,

상기 보안 구역들 중 2 이상은 병렬로 관리되는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

#### 청구항 39

제 31 항에 있어서,

상기 보안 구역들 중 하나 이상은 비-보안 구역 또는 보안 구역을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

#### 청구항 40

제 31 항에 있어서,

상기 작업 오더들을 발행하는 하나 이상의 애플리케이션들은, 콘텐츠 보호 구역 애플리케이션, 오퍼레이팅 시스템과 연관된 콘텐츠 보호 구역 커널, 하이 레벨 오퍼레이팅 시스템 커널, 및 신뢰 구역 보안 모니터 중 하나 이상을 포함하는, 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 시스템.

### 발명의 설명

#### 기술 분야

[0001]

우선권 및 관련 출원들 서술

[0002]

본 출원은 2013 년 7 월 1 일자로 출원되고 가출원 번호 제 61/841,881 호가 할당된 "System and Method for Providing Secure Access Control to a Graphics Processing Unit" 라는 명칭의 미국 특허 가출원을 35 U.S.C. 119(e) 하에 우선권 주장하며, 그 전체 내용들은 참조에 의해 본원에 통합된다.

#### 배경 기술

[0003]

모바일 폰들과 같은 휴대용 컴퓨팅 디바이스들 ("PCD들") 은 점점 더 복잡해지고 있다. 기존의 PCD들은 중, 상이한 기능들을 수행하고 그러한 디바이스들에 대한 증가하는 요구들을 만족하는 다수의 프로세서들 (예컨대, 중앙 프로세싱 유닛 (CPU), 그래픽 프로세싱 유닛 (GPU), 디지털 신호 프로세서 (DSP) 등) 을 갖는다. 기존의 PCD들은 또한, DRM (digital rights management), 은행업무, 의료 기록들, 지문들 등등을 포함하는 애플리케이션들에 대한 기밀 데이터로의 액세스를 제어하는 것과 같은 사용 케이스들에 대한 액세스 제어 요건들을 일반적으로 지원하는 콘텐츠 보호 아키텍처들을 지원할 수도 있다. 콘텐츠 보호 아키텍처는 통상적으로, 애플리케이션들에 의한 민감한 콘텐츠로의 액세스를 제어하기 위해 메모리 영역들을 상이한 보안 구역들로 분리한다. 그러나, 기존의 PCD들 및 콘텐츠 보호 아키텍처들은 CPU-레벨 액세스 제어에 제한된다.

#### 발명의 내용

#### 해결하려는 과제

[0004]

따라서, 보안 액세스 제어를 GPU 에 제공하기 위한 개선된 메커니즘들이 당업계에 요구된다.

#### 과제의 해결 수단

[0005]

시스템들, 방법들 및 컴퓨터 프로그램들은 그래픽 프로세싱 유닛 (GPU) 에 보안 액세스 제어를 제공하기 위해 개시된다. 일 방법은: 그래픽 프로세싱 유닛 (GPU) 으로의 액세스를 제어하기 위한 복수의 보안 구역들을 정의하는 단계; GPU 에 의해 제공되는 복수의 GPU 프로그래밍 인터페이스들 중 대응하는 GPU 프로그래밍 인터페이스에 보안 구역들의 각각을 할당하는 단계로서, GPU 프로그래밍 인터페이스들의 각각은 대응하는 보안 구역과 연관된 하나 이상의 애플리케이션들에 의해 발행된 작업 오더들을 수신하기 위한 것이고, 작업 오더들은 GPU 에 의해 실행될 명령들을 포함하는, 상기 보안 구역들의 각각을 할당하는 단계; 및 별개의 보안 메모리 영역들을 사용하여 복수의 GPU 프로그래밍 인터페이스들에 의해 수신된 작업 오더들의 실행을 제어하는 단계로서, 각각의



보안 메모리 영역은 복수의 보안 구역들 중 하나에 할당되는, 상기 작업 오더들의 실행을 제어하는 단계를 포함한다.

[0006]

다른 실시형태는 그래픽 프로세싱 유닛에 보안 액세스 제어를 제공하는 컴퓨터 프로그램이다. 그 컴퓨터 프로그램은 프로세서에 의한 실행을 위해 컴퓨터 판독가능 매체에 수록된다. 컴퓨터 프로그램은 로직을 포함하고, 로직은: 그래픽 프로세싱 유닛 (GPU) 으로의 액세스를 제어하기 위한 복수의 보안 구역들을 정의하고; GPU 에 의해 제공되는 복수의 GPU 프로그래밍 인터페이스들 중 대응하는 GPU 프로그래밍 인터페이스에 보안 구역들의 각각을 할당하는 것으로서, GPU 프로그래밍 인터페이스들의 각각은 대응하는 보안 구역과 연관된 하나 이상의 애플리케이션들에 의해 발행된 작업 오더들을 수신하기 위한 것이고, 작업 오더들은 GPU 에 의해 실행될 명령들을 포함하는, 상기 보안 구역들의 각각을 할당하며; 그리고 별개의 보안 메모리 영역들을 사용하여 복수의 GPU 프로그래밍 인터페이스들에 의해 수신된 작업 오더들의 실행을 제어하는 것으로서, 각각의 보안 메모리 영역은 복수의 보안 구역들 중 하나에 할당되는, 상기 작업 오더들의 실행을 제어하도록 구성된다.

[0007]

또 다른 실시형태는 그래픽 프로세싱 유닛 (GPU) 에 보안 액세스 제어를 제공하는 시스템이다. 그 시스템은 복수의 GPU 프로그래밍 인터페이스들을 갖는 GPU 및 커맨드 프로세서를 포함한다. 각각의 GPU 프로그래밍 인터페이스는 복수의 보안 구역들 중 상이한 보안 구역에 동적으로 할당되고 대응하는 보안 구역과 연관된 하나 이상의 애플리케이션들에 의해 발행된 작업 오더들을 수신하도록 구성된다. 작업 오더들은 GPU 에 의해 실행될 명령들을 포함한다. 커맨드 프로세서는 복수의 GPU 프로그래밍 인터페이스들과 통신하고, 별개의 보안 메모리 영역들을 사용하여 복수의 GPU 프로그래밍 인터페이스들에 의해 수신된 작업 오더들의 실행을 제어하도록 구성된다. 각각의 보안 메모리 영역은 복수의 보안 구역들 중 하나에 할당된다.

### 도면의 간단한 설명

[0008]

도면들에 있어서, 동일한 참조부호들은, 달리 나타내지 않으면 다양한 도면들 전반에 걸쳐 동일한 부분들을 지칭한다. "102A" 또는 "102B" 와 같은 문자 지정을 갖는 참조부호들에 대해, 그 문자 지정은 동일한 도면에 존재하는 2개의 동일한 부분들 또는 엘리먼트들을 구별할 수도 있다. 참조부호들에 대한 문자 지정은, 참조부호가 모든 도면들에 있어서 동일한 참조부호를 갖는 모든 부분들을 포괄하도록 의도될 경우에 생략될 수도 있다.

도 1 은 그래픽 프로세싱 유닛 (GPU) 에 보안 액세스 제어를 제공하는 시스템의 일 실시형태를 예시하는 블록 다이어그램이다.

도 2 는 4 개의 보안 구역들 및 대응하는 GPU 프로그래밍 인터페이스들로 구성되고 메모리 영역들이 할당되는 도 1 의 시스템의 일 실시형태를 예시하는 블록 다이어그램이다.

도 3 은 GPU 에 보안 액세스 제어를 제공하기 위해 도 1 의 시스템에서 구현된 방법의 일 실시형태를 예시하는 플로우차트이다.

도 4 는 도 1 의 시스템을 통합하는 예시적인 휴대용 컴퓨팅 디바이스를 예시하는 블록 다이어그램이다.

### 발명을 실시하기 위한 구체적인 내용

[0009]

단어 "예시적인"은 본원에서 "실시형태인, 예시인 또는 예증인" 것을 의미하기 위해 사용된다. "예시적인"으로서 본원에서 설명된 임의의 양태는 다른 양태들에 비해 더 선호되거나 또는 더 유익한 것으로 해석될 필요는 없다.

[0010]

이 설명에 있어서, 용어 "애플리케이션" 은 또한 오브젝트 코드, 스크립트들, 바이트 코드, 마크업 언어 파일들, 및 패치들과 같은 실행가능 콘텐츠를 갖는 파일들을 포함할 수도 있다. 부가적으로, 본 명세서에서 지칭되는 "애플리케이션" 은 또한, 공개될 필요가 있을 수도 있는 문헌들 또는 액세스될 필요가 있는 다른 데이터 파일들과 같이 본질적으로 실행가능하지 않는 파일들을 포함할 수도 있다.

[0011]

용어 "컨텐츠" 는 또한 오브젝트 코드, 스크립트들, 바이트 코드, 마크업 언어 파일들, 및 패치들과 같은 실행가능 콘텐츠를 가진 파일들을 포함할 수도 있다. 또한, 본 명세서에서 지칭되는 "컨텐츠"는, 공개되어야 할 수도 있는 문헌들 또는 액세스되어야 하는 다른 데이터 파일들과 같이 본질적으로 실행가능하지 않는 파일들을 포함할 수도 있다.

[0012]

본 명세서에서 사용된 바와 같이, 용어 "컴포넌트", "데이터베이스", "모듈", "시스템" 등은 컴퓨터 관련 엔티티, 즉 하드웨어, 펌웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어, 또는 실행 중인 소프트웨어 중 하나를

가리키는 것으로 의도된다. 예를 들어, 컴포넌트는 프로세서 상에서 구동하는 프로세스, 프로세서, 오브젝트, 실행 가능물 (executable), 실행 스레드 (thread of execution), 프로그램, 및/또는 컴퓨터일 수도 있지만, 이에 한정되지 않는다. 예시로서, 컴퓨팅 디바이스 상에서 구동하는 애플리케이션 및 컴퓨팅 디바이스 양자는 컴포넌트일 수도 있다. 하나 이상의 컴포넌트들은 프로세스 및/또는 실행 스레드 내에 상주할 수도 있고, 컴포넌트는 하나의 컴퓨터에 국부화되고/되거나 2 이상의 컴퓨터들 사이에서 분산될 수도 있다. 부가적으로, 이들 컴포넌트들은 다양한 데이터 구조들이 저장된 다양한 컴퓨터 판독가능 매체로부터 실행할 수도 있다. 컴포넌트들은 하나 이상의 데이터 패킷들을 갖는 신호 (예를 들어, 로컬 시스템에서, 분산 시스템에서 및/또는 신호에 의한 다른 시스템들과의 인터넷과 같은 네트워크에 걸쳐 다른 컴포넌트와 상호작용하는 하나의 컴포넌트로부터의 데이터)에 따라서와 같은 로컬 및/또는 원격 프로세스들에 의해 통신할 수도 있다.

[0013] "휴대용 컴퓨팅 디바이스" ("PCD")는 예컨대, 셀룰러 전화기, 위성 전화기, 페이지, 개인 휴대정보 단말기, 스마트폰, 네비게이션 디바이스, 스마트북 또는 전자 리더, 미디어 플레이어, 태블릿 컴퓨터, 랩탑 컴퓨터, 또는 다른 기타 디바이스들을 포함할 수도 있다.

[0014] 도 1은 그래픽 프로세싱 유닛 (GPU; 102)에 보안 액세스 제어를 제공하기 위해 예컨대, PCD (도 4)에 통합될 수도 있는 시스템 (100)이다. 시스템 (100)은 하나 이상의 애플리케이션들 (118) 및/또는 하나 이상의 오퍼레이팅 시스템들 (120)과 연관된 그래픽들 및/또는 계산 명령들을 실행하기 위해 하나 이상의 중앙 프로세싱 유닛들 (CPU; 402) 및 하나 이상의 GPU들 (102)을 포함한다. CPU (402) 및 GPU (102)는 하드웨어 버스, 커넥션 또는 다른 인터페이스에 의해 접속될 수도 있다. 시스템 (100)은 복수의 보안 및/또는 콘텐츠 보호 구역들 ("보안 구역들")에 GPU 액세스 제어를 제공한다.

[0015] GPU 하드웨어 및/또는 소프트웨어는 복수의 GPU 프로그래밍 인터페이스들 (104)을 CPU (402)에 제공한다. GPU 프로그래밍 인터페이스들 (104)의 각각은 상이한 보안 구역들에 상주중인 오퍼레이팅 시스템들 (120) 및 하나 이상의 애플리케이션들 (118)에 의해 발행된 작업 오더들을 수신하기 위해 상이한 보안 구역과 연관된다. 보안 구역들은 임의의 바람직한 보안 사용 케이스에 기초하여 보안 정책 관리자 (106)에 의해 정의될 수도 있다. 각각의 보안 구역은 별개의 GPU 프로그래밍 인터페이스 (104)에 할당되고, 별개의 메모리 영역에 할당된다. 도 1의 실시형태에서, 시스템 (100)은 대응하는 보안 메모리 영역들을 갖는 4개의 GPU 프로그래밍 인터페이스들 (104a, 104b, 104c, 및 104d)을 포함한다. 컨텍스트 बैं크들 (122a, 122b, 122c, 및 122d)은 대응하는 보안 구역들에서 작업 오더들을 실행하기 위한 메모리 리소스들로서 할당될 수도 있다. 이와 관련하여, 보안 메모리 영역들은 시스템 메모리 관리 유닛 (SMMU; 116)에서 컨텍스트 बैं크들 (122a, 122b, 122c, 및 122d)을 사용하는 하드웨어-강제 (hardware-enforced) 보호들을 갖는 분리된 어드레스 공간을 포함할 수도 있다. 각각의 컨텍스트 बैं크 (122)는 특정 보안 및 분리된 어드레스 공간을 강제하기 위한 하드웨어 리소스들을 포함할 수도 있다.

[0016] 작업 오더들은 GPU (102)에 의해 실행될 그래픽 명령들을 포함한다. 애플리케이션들 (118)이 GPU (102)로부터 리소스들을 요청하는 임의의 적절한 애플리케이션을 포함할 수도 있는 것이 인식되어야만 한다. 오퍼레이팅 시스템 (120)은 예컨대, 하이-레벨 오퍼레이팅 시스템 (HLOS)과 같은 하나 이상의 오퍼레이팅 시스템들을 포함할 수도 있다. 일 실시형태에서, GPU (102)는 특수 구성된 콘텐츠 보호 애플리케이션들 (예컨대, 콘텐츠 보호 애플리케이션 (117), 또는 오퍼레이팅 시스템들 (120)과 연관된 콘텐츠 보호 커널 (119))로부터 작업 오더들을 수신할 수도 있다.

[0017] GPU 프로그래밍 인터페이스 (104)가 제어 리소스를 포함하는 것을 담당자는 인식할 것이다. 일 실시형태에서, 제어 리소스는 대응하는 보안 구역에서의 애플리케이션들로부터 작업 오더들을 수용하기 위한 레지스터 리소스들 및 작업 오더의 실행의 완료 또는 실패 상태를 표시하기 위한 하나 이상의 중단 리소스들을 포함할 수도 있다. GPU 프로그래밍 인터페이스들 (104)은 예컨대, 가상 머신들의 사이즈 및 보안 정책 관리자 (106) 또는 신뢰 구역 컴포넌트 (108) (즉, 시스템 (100)에서 "신뢰 루트 (root of trust)")가 GPU (402)로의 액세스를 요구하는지 여부에 기초하여, 가상 머신 관리자 (VMM; 110)에 의해 구성가능할 수도 있다. 시스템 (100)에서의 "신뢰 루트"는 보안 사용 케이스 시작 시간에 발생할 수도 있는 보안 정책 관리자 (106)의 시스템 보안 정책들에 기초하여, GPU 프로그래밍 인터페이스들 (104)을 지정된 보안 구역들에 동적으로 할당한다.

[0018] 전술된 것과 같이, 각각의 GPU 프로그래밍 인터페이스 (104)는 특정 사용 시나리오에 의존하여 대응하는 컨텍스트 बैं크 (122)에 맵핑된 메모리일 수도 있고, 이 경우 그들은 메모리 맵핑된 입력/출력 (MIMO) 레지스터를 포함할 수도 있다. GPU 프로그래밍 인터페이스들 (104)은 하나 이상의 가상 머신들 또는 VMM (110)에 직접 할당가능할 수도 있다. 각각의 GPU 프로그래밍 인터페이스 (104)는 시스템 메모리 관리 유닛 (SMMU;

116) 을 사용하여 하드웨어-강제 액세스 제어에 의해 보호될 수도 있음이 추가로 인식되어야만 한다. 이러한 방식으로, 각각의 보안 구역은 레지스터에 대하여 완전히 제어할 수도 있고, 특정 사용 케이스가 시작한 후에 GPU 프로그래밍 인터페이스 (104) 와 연관된 리소스들을 중단할 수도 있다.

[0019]

도 1 에 추가로 도시된 것과 같이, GPU (102) 는 복수의 GPU 프로그래밍 인터페이스들 (104) 과 통신하는 커맨드 프로세서 (114) 를 포함할 수도 있다. 커맨드 프로세서 (114) 는 GPU 프로그래밍 인터페이스 (104) 와 연관된 컨텐츠 큐 (204; 도 2) 로부터 작업 오더들을 선택하도록 구성될 수도 있다. 이와 관련하여, 커맨드 프로세서 (114) 는 예컨대, GPU 스케줄링 정책들에 기초하여 어떤 작업 오더들을 프로세싱할 것인지를 결정할 수도 있고, 그 후에 보안 구역에 할당된 적절한 컨텍스트 뱅크 (122) 를 사용하여 작업 오더들의 실행을 제어할 수도 있다.

[0020]

일 실시형태에서, 다수의 보안 구역들은 CPU (402) 상에 동시에 실행중인 애플리케이션들 (118) 에 의해 병렬로 관리될 수 있다. 각각의 애플리케이션 (118) 은 연관된 커맨드 큐를 직접 관리할 수도 있다. 보안 구역들 중 하나 이상은 또한, 보안 및/또는 비-보안일 수도 있다. 애플리케이션 (118) (및 그 연관된 메모리) 이 보안 및/또는 비-보안인 보안 정책은, GPU (102) 를 제어중인 프로세서 (예컨대, CPU (408)) 에 의해 결정될 수도 있다. CPU (402) 에 의해 수행되고 및/또는 관리되는 세그멘테이션은 예컨대, 다음의 예시적인 방식들을 포함하는 다양한 방식으로 구현될 수도 있다: (1) 하이퍼바이저 계층 (예컨대, 다수의 게스트 오퍼레이팅 시스템들 (120) 을 관리하기 위한 소프트웨어 계층) 과의 분리; 및/또는 (2) 메모리 액세스 및 GPU 커맨드들을 트래킹하고 요청 소스를 분리하기 위한 명령들의 추가의 하드웨어 태깅 (tagging) 을 통해 신뢰 하드웨어와 비-신뢰 하드웨어 간의 분리를 제어할 수도 있는, 하드웨어 보안 도메인 (예컨대, ARM 아키텍처들에서 사용된 "신뢰 구역" 보안 확장들) 을 정의하는 하드웨어 프로세스 구성. 하이퍼바이저 계층은 제어 유닛의 메모리 액세스 분리에 제한될 수도 있는, 하드웨어에서의 소프트웨어 관념을 포함할 수도 있다.

[0021]

시스템 (101) 은 GPU 액세스 제어에 관련된 임의의 바람직한 보안 사용 케이스들을 지원할 수도 있다. 예를 들어, 시스템 (101) 은, DRM (digital rights management), 및 예컨대, 은행업무, 의료 기록들, 지문들 등등을 포함하는 애플리케이션들에 대한 기밀 데이터로의 액세스를 제어하는 것과 같은 사용 케이스를 지원할 수도 있다. 일 실시형태에서, 개별 보안 구역들과 연관된 4 개의 예외 레벨들을 제공할 수도 있으며, 각각의 레벨은 시스템 (101) 은 상이한 또는 랭크된 보안 권한들을 갖는다. 제 1 예외 레벨 (EL0) 은 대략 사용자 모드에 대응할 수도 있다. 제 2 예외 레벨 (EL1) 은 커널 모드에 대응할 수도 있다. 제 3 예외 레벨 (EL2) 은 하이퍼바이저들에 대응할 수도 있다. 제 4 예외 레벨 (EL3) 은 최고 기밀의 보안 구역을 포함하는, 신뢰 구역 컴포넌트 (108) 에 대응할 수도 있다.

[0022]

도 2 는 4 개의 보안 구역들 (202a, 202b, 202c, 및 202d) 을 수반하는 예시적인 사용 케이스를 도시한다. 보안 구역 (202a) 은 제 1 HLOS 커널 (119a) 에 대하여 구성되고 컨텐츠 큐 (204a) 를 갖는 GPU 프로그래밍 인터페이스 (104a) 에 할당된다. 컨텐츠 뱅크 (122a) 는 보안 구역 (202a) 에 할당된다. 보안 구역 (202b) 은 컨텐츠 보호 애플리케이션 (117) 에 대하여 구성되고 컨텐츠 큐 (204b) 를 갖는 GPU 프로그래밍 인터페이스 (104b) 에 할당된다. 컨텐츠 뱅크 (122b) 는 보안 구역 (202b) 에 할당된다. 보안 구역 (202c) 은 제 2 HLOS 커널 (119b) 에 대하여 구성되고 컨텐츠 큐 (204c) 를 갖는 GPU 프로그래밍 인터페이스 (104c) 에 할당된다. 컨텐츠 뱅크 (122c) 는 보안 구역 (202c) 에 할당된다. 보안 구역 (202d) 은 신뢰 구역 컴포넌트 (108) 와 연관되고 컨텐츠 큐 (204d) 를 갖는 GPU 프로그래밍 인터페이스 (104c) 에 할당된다. 신뢰 구역 컴포넌트 (108) 는, 오직 신뢰 구역 컴포넌트 (108) 에만 보이는 분리된 어드레스 공간을 포함하는 신뢰 컨텍스트 뱅크 (122d) 를 갖는다.

[0023]

보안 구역들 (202) 은 적절한 애플리케이션들 (118) 을 갖는 임의의 바람직한 사용 케이스들을 지원할 수도 있는 것이 인식되어야만 한다. 예를 들어, 일 실시형태에서, 보안 구역 (202a) 은 게이밍 애플리케이션 및 연관된 가상 메모리 공간과 연관될 수도 있다. 보안 구역 (202b) 은 비디오 애플리케이션 및 연관된 프리미엄 비디오 가상 메모리 공간과 연관될 수도 있다. 보안 구역 (202c) 은 브라우저 애플리케이션 및 연관된 가상 메모리 공간과 연관될 수도 있다. 보안 구역 (202d) 은 बैं킹 애플리케이션 및 연관된 가상 메모리 공간과 연관될 수도 있다.

[0024]

도 2 에 추가로 도시된 것과 같이, 각각의 GPU 프로그래밍 인터페이스 (104a, 104b, 104c, 및 104d) 는 별개의 데이터 스트림 식별자 (각각 SID (206a), SID (206b), SID (206c), 및 SID (206d)) 에 의해 식별될 수도 있다. 스트림 식별자들은 예컨대, CPU (402) 에 의해, 작업 오더들을 적절한 GPU 프로그래밍 인터페이스에 투입하는데 사용될 수도 있다. 커맨드 프로세서 (114) 는 스트림 식별자들에 따라 작업 오더들을 선택할 수도 있

고, SMMU (116) 는 스트림 식별자들에 따라 메모리 리소스들을 관리할 수도 있다.

[0025]

도 3 은 시스템 (100) 에서 GPU 액세스 제어를 제공하기 위한 방법 (300) 의 일 실시형태를 예시한다. 블록 (301) 에서, GPU (104) 에 의해 실행될 명령들에 대하여 복수의 보안 구역들 (202) 이 정의된다. 보안 구역들 (202) 은 보안 정책 관리자 (106), 신뢰 구역 컴포넌트 (108), 또는 시스템 (101) 과 연관된 다른 소프트웨어 및/또는 하드웨어에 의해 정의될 수도 있다. 일 실시형태에서, 보안 구역들 (202) 중 2 이상이 병렬로 관리될 수도 있다. 또한, 일부 실시형태들에서, 보안 구역 및 비-보안 구역 양자가 구현될 수도 있음이 인식되어야 한다. 블록 (303) 에서, 각각의 보안 구역 (202) 은 별개의 GPU 프로그래밍 인터페이스 (104) 에 할당되고, 별개의 메모리 영역 (예컨대, 컨텍스트 बैं크들 (122a, 122b, 122c, 및 122d)) 에 할당된다. 전술된 것과 같이, GPU 프로그래밍 인터페이스들 (104) 은 예컨대, 가상 머신들의 사이즈 및 보안 정책 관리자 (106) 또는 신뢰 구역 컴포넌트 (108) 가 GPU (104) 로의 액세스를 요구하는지 여부에 기초하여, VMM (110) 에 의해 구성가능할 수도 있다. 일 실시형태에서, 시스템 (100) 에서의 "신뢰 루트" 는 보안 사용 케이스 시작 시간에 발생할 수도 있는 보안 정책 관리자 (106) 의 시스템 보안 정책들에 기초하여, GPU 프로그래밍 인터페이스들 (104) 을 지정된 보안 구역들에 동적으로 할당한다. 블록 (305) 에서, 보안 구역들 (202) 중 하나에 상주중인 애플리케이션들 (118) 은 작업 오더들을 적절한 GPU 프로그래밍 인터페이스 (104) 에 발행할 수도 있다. CPU (402) 는 스트림 식별자들 (206) 을 사용하여 작업 오더들을 투입할 수도 있다. 블록 (307) 에서, 작업 오더들은 대응하는 보안 구역 (202) 에 기초하여 적절한 GPU 프로그래밍 인터페이스 (105) 에 제공될 수도 있다. 블록 (309) 에서, 커맨드 프로세서 (114) 및/또는 SMMU (116) 는 대응하는 보안 구역 (202) 및 GPU 프로그래밍 인터페이스 (104) 에 할당된 별개의 메모리 영역들 (예컨대, 컨텍스트 बैं크들 (122a, 122b, 122c, 및 122d)) 을 사용하여 작업 오더들의 실행을 제어할 수도 있다.

[0026]

대안적인 사용 케이스들이 구현될 수도 있음을 당업자는 인식할 것이다. 신뢰 구역 컴포넌트 (108) 를 수반하는 예시적인 "신뢰 구역" 사용 케이스는 GPU 액세스 제어 기능의 특정 양태들을 추가로 예시하기 위해 기술될 것이다. 신뢰 구역 컴포넌트 (108) 는 신뢰 컨텍스트 बैं크 (122d; 도 2) 의 소유권을 주장할 수도 있다. SMMU 컨텍스트 बैं크와 연관된 페이지 테이블이 구성될 수도 있다. 페이지 테이블은 신뢰 구역 (즉, 보안 구역 (202d) 에 의해 소유되는 버퍼들로 채워질 수도 있고, 다른 보안 구역 (202a, 202b, 또는 202c) 과 공유되는 버퍼들을 제외하여 임의의 다른 컴포넌트들에게는 보이지 않는다. 보안 정책은 신뢰 구역 컴포넌트 (108) 가 GPU 프로그래밍 인터페이스 (104d) 의 소유권을 주장하는 것을 명시할 수도 있다. SID (206d) 는 신뢰 컨텍스트 बैं크 (122d) 에 맵핑하는 보안 SID 로서 구성될 수도 있다. 동작시, 신뢰 구역 컴포넌트 (108) 는 커맨드 큐 (104d) 에 요청들을 투입함으로써 GPU 작업 오더들을 발행한다.

[0027]

작업 오더들이 커맨드 큐 (204d) 에 투입될 경우, 커맨드 프로세서 (114) 는 (예컨대, "도어벨" 레지스터에 의해) 프로세싱을 시작하도록 촉구될 수도 있다. 커맨드 프로세서 (114) 는 어느 것이 작업할지를 선택하기 위해 GPU 프로그래밍 인터페이스(들) (104d) 을 스캔한다. 작업 오더는, SID (206d) 가 GPU 프로그래밍 인터페이스 (104d) 에 따라 세팅되는 동안, 프로세싱될 수도 있다. SID (206d) 는 적절한 메모리 보호를 셋업하는 특정 컨텍스트 बैं크를 선택한다. 작업이 성공적으로 완료될 경우 또는 에러의 경우에, 커맨드 프로세서 (114) 는 CPU (402) 를 중단하고 및/또는 신뢰 구역 컴포넌트 (108) 는 그 중단을 수신한다. 작업 오더의 완료 이후에, 신뢰 구역 컴포넌트 (108) 는 추가의 작업 오더들을 발행할 수도 있다. 중단이 에러를 표시한다면, 신뢰 구역 컴포넌트 (108) 는 추가의 프로세싱을 중지하고, 에러 핸들링 정책들에 따라 에러를 핸들링할 수도 있다.

[0028]

도 4 는 예시적인 휴대용 컴퓨팅 디바이스 (PCD; 400) 에 통합된, 전술된 시스템 (100) 을 도시한다. 시스템 (100) 의 일부 컴포넌트들이 SoC (322) 상에 포함되는 반면, 다른 컴포넌트들은 오프칩으로 상주할 수도 있음이 인식되어야만 한다. SoC (322) 는 별도로 제작될 수도 있고 휴대용 컴퓨팅 디바이스 (400) 에 대한 설계들로 통합될 수도 있는 임의의 임베디드 시스템을 포함할 수도 있다.

[0029]

도시된 것과 같이, PCD (400) 는 멀티코어 CPU (402A) 를 포함하는 SoC (322) 를 포함한다. 멀티코어 CPU (402A) 는 제 0 코어 (410), 제 1 코어 (412), 및 제 N 코어 (414) 를 포함할 수도 있다. 디스플레이 제어기 (328) 및 터치스크린 제어기 (330) 는 CPU (402) 상에 상주하거나 그에 접속될 수도 있는, GPU (104) 에 커풀링될 수도 있다. 차례로, SoC (322) 외부의 터치스크린 디스플레이 (108) 는 디스플레이 제어기 (328) 및 터치스크린 제어기 (330) 에 커풀링될 수도 있다.

[0030]

도 4 는 비디오 인코더 (334), 예컨대 PAL (phase alternating line) 인코더, SECAM (sequential color a memoire) 인코더, 또는 NTSC (national television system(s) committee) 인코더가 멀티코어 CPU (402A) 에 커



플러링되는 것을 추가로 도시한다. 추가로, 비디오 증폭기 (336) 가 비디오 인코더 (334) 및 터치스크린 디스플레이 (108) 에 커플링된다. 또한, 비디오 포트 (338) 가 비디오 증폭기 (336) 에 커플링된다. 도 4 에 도시된 바와 같이, 범용 직렬 버스 ("USB") 제어기 (340) 및 다른 트레이스 싱클들 (109) 및 트레이스 덤프들 (110) 이 멀티코어 CPU (402A) 에 커플링될 수도 있다. 또한, USB 포트 (342) 가 USB 제어기 (340) 에 커플링된다. 메모리 (404A) 및 가입자 아이덴티티 모듈 (SIM) 카드 (346) 가 또한 멀티코어 CPU (402A) 에 커플링될 수도 있다.

[0031] 추가로, 도 4 에 도시된 바와 같이, 디지털 카메라 (348) 가 멀티코어 CPU (402A) 에 커플링될 수도 있다. 예시적인 양태에 있어서, 디지털 카메라 (348) 는 전하 결합형 디바이스 (CCD) 카메라 또는 상보적 금속 산화물 반도체 (CMOS) 카메라이다.

[0032] 도 4 에 추가로 도시된 바와 같이, 스테레오 오디오 코더-디코더 (코덱; 350) 이 멀티코어 CPU (402A) 에 커플링될 수도 있다. 더욱이, 오디오 증폭기 (352) 가 스테레오 오디오 코덱 (350) 에 커플링될 수도 있다. 예시적인 양태에 있어서, 제 1 스테레오 스피커 (354) 및 제 2 스테레오 스피커 (356) 가 오디오 증폭기 (352) 에 커플링된다. 도 4 는, 마이크로폰 증폭기 (358) 가 또한 스테레오 오디오 코덱 (350) 에 커플링될 수도 있는 것을 도시한다. 부가적으로, 마이크로폰 (360) 이 마이크로폰 증폭기 (358) 에 커플링될 수도 있다. 특정 양태에 있어서, 주파수 변조 (FM) 라디오 튜너 (362) 가 스테레오 오디오 코덱 (350) 에 커플링될 수도 있다. 또한, FM 안테나 (364) 가 FM 라디오 튜너 (362) 에 커플링된다. 추가로, 스테레오 헤드폰들 (366) 이 스테레오 오디오 코덱 (350) 에 커플링될 수도 있다.

[0033] 도 4 는 무선 주파수 (RF) 트랜시버 (368) 가 멀티코어 CPU (402A) 에 커플링될 수도 있음을 추가로 도시한다. RF 스위치 (370) 가 RF 트랜시버 (368) 및 RF 안테나 (372) 에 커플링될 수도 있다. 도 4 에 도시된 바와 같이, 키패드 (204) 가 멀티코어 CPU (402A) 에 커플링될 수도 있다. 또한, 마이크로폰을 갖는 모노 헤드셋 (376) 이 멀티코어 CPU (402A) 에 커플링될 수도 있다. 추가로, 바이브레이터 디바이스 (378) 가 멀티코어 CPU (402A) 에 커플링될 수도 있다.

[0034] 도 4 는 또한, 전원 (380) 이 SoC (322) 에 커플링될 수도 있는 것을 도시한다. 특정 양태에서, 전원 (380) 은 전력을 요구하는 PCD (400) 의 다양한 컴포넌트들에 전력을 제공하는 직류 (DC) 전원이다. 추가로, 특정 양태에 있어서, 전원은, AC 전력 소스에 접속되는 교류 (AC)-DC 변환기로부터 도출되는 DC 전원 또는 재충전식 DC 배터리이다.

[0035] 도 4 는, PCD (400) 가 또한 데이터 네트워크, 예컨대 로컬 영역 네트워크, 개인 영역 네트워크, 또는 임의의 다른 네트워크를 액세스하는데 사용될 수도 있는 네트워크 카드 (388) 를 포함할 수도 있는 것을 추가로 표시한다. 네트워크 카드 (388) 는 블루투스 네트워크 카드, WiFi 네트워크 카드, 개인 영역 네트워크 (PAN) 카드, 개인 영역 네트워크 초저전력 기술 (PeANUT) 네트워크 카드, 또는 당업계에 잘 알려진 임의의 다른 네트워크 카드일 수도 있다. 추가로, 네트워크 카드 (388) 는 칩 내에 통합될 수도 있고, 즉 네트워크 카드 (388) 는 칩 내의 완전 솔루션일 수도 있고, 별개의 네트워크 카드 (388) 가 아닐 수도 있다.

[0036] 도 4 에 도시된 바와 같이, 터치스크린 디스플레이 (108), 비디오 포트 (338), USB 포트 (342), 카메라 (348), 제 1 스테레오 스피커 (354), 제 2 스테레오 스피커 (356), 마이크로폰 (360), FM 안테나 (364), 스테레오 헤드폰들 (366), RF 스위치 (370), RF 안테나 (372), 키패드 (374), 모노 헤드셋 (376), 바이브레이터 (378), 및 전원 (380) 은 온-칩 시스템 (322) 외부에 있을 수도 있다.

[0037] 특정 양태에 있어서, 본원에서 기술된 방법 단계들 중 하나 이상은, 도 1 에 도시된 것과 같은 시스템 (100) 과 관련하여 전술된 모듈들과 같은 컴퓨터 프로그램 명령들로서 메모리 (404) 에 저장될 수도 있다.

[0038] 이들 명령들은 멀티코어 CPU (402A) 및/또는 GPU (102) 에 의해, 본원에 기술된 방법들을 수행하도록 실행될 수도 있다. 추가로, 멀티코어 CPU (402A), GPU (102), PCD (400) 의 메모리 (404A), 또는 이들의 조합은 본원에 기술된 방법 단계들 중 하나 이상을 실행하기 위한 수단들로서 기능할 수도 있다.

[0039] 본 명세서에 설명된 프로세스들 또는 프로세스 플로우들에서의 특정 단계들은 자연스럽게, 본 발명이 설명된 바와 같이 기능하도록 다른 것들보다 선행한다. 하지만, 본 발명은, 그러한 순서 또는 시퀀스가 본 발명의 기능을 변경하지 않는다면, 설명된 단계들의 순서로 한정되지 않는다. 즉, 일부 단계들은 본 발명의 범위 및 사상으로부터 이탈할 없이 다른 단계들 이전에, 그 이후에 또는 그와 병렬로 (실질적으로 동시에) 수행될 수도 있음이 인식된다. 일부 경우들에 있어서, 특정 단계들은 본 발명으로부터 이탈함없이 생략되거나 또는 수행되지 않을 수도 있다. 추가로, "그 이후", "그 후", "다음으로" 등과 같은 단어들은 단계들의 순서를 한정

하도록 의도되지 않는다. 이들 단어들은 단순히, 예시적인 방법의 설명을 통해 독자를 가이드하도록 사용된다.

[0040] 부가적으로, 프로그래밍에 있어서의 당업자는, 예를 들어, 본 명세서에 있어서의 플로우 차트들 및 관련 설명에 기초하여 어려움 없이, 개시된 발명을 구현하기 위해 컴퓨터 코드를 기입하거나 적절한 하드웨어 및/또는 회로들을 식별할 수 있다.

[0041] 따라서, 프로그램 코드 명령들 또는 상세한 하드웨어 디바이스들의 특정 세트의 개시는 본 발명을 제조 및 이용하는 방법의 적절한 이해에 필수적인 것으로 고려되지 않는다. 청구된 컴퓨터 구현 프로세스들의 본 발명의 기능은, 다양한 프로세스 플로우들을 예시할 수도 있는 도면들과 함께 설명에서 더 상세히 설명된다.

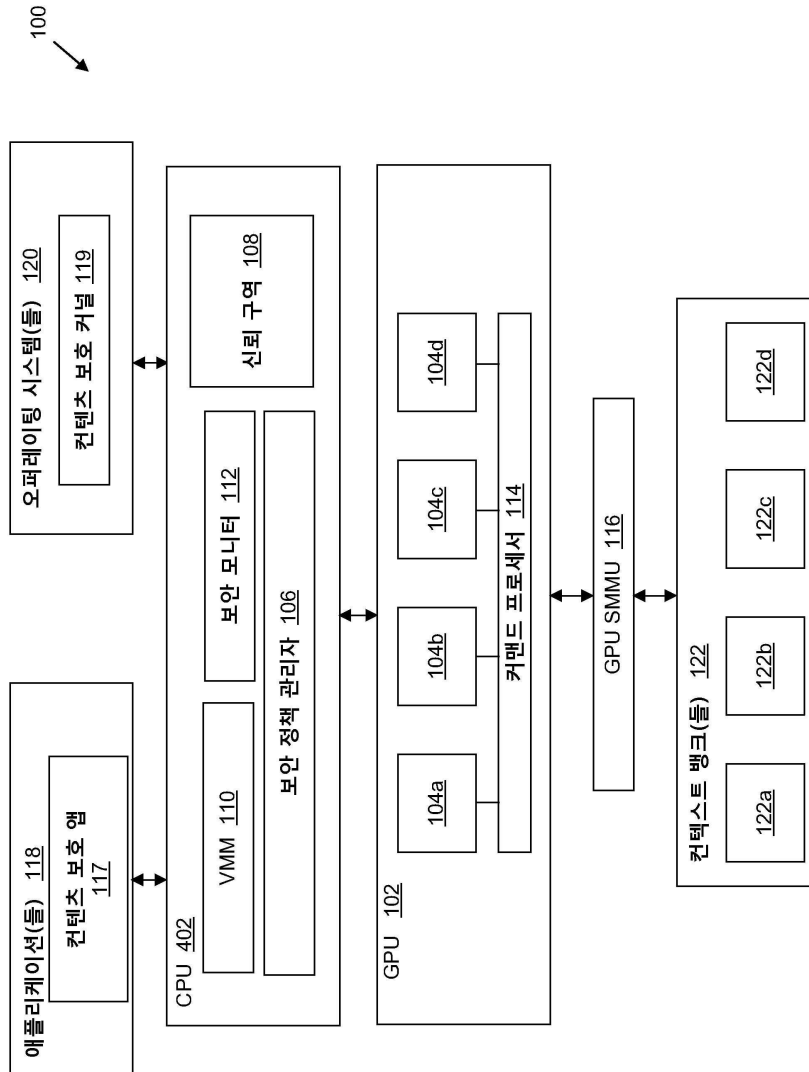
[0042] 하나 이상의 예시적인 양태들에 있어서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어, 또는 이들의 임의의 조합에서 구현될 수도 있다. 소프트웨어에서 구현된다면, 그 기능들은 하나 이상의 명령들 또는 코드로서 컴퓨터 판독가능 매체 상으로 저장 또는 전송될 수도 있다. 컴퓨터 판독가능 매체는, 일 장소로부터 다른 장소로의 컴퓨터 프로그램의 전송을 용이하게 하는 임의의 매체를 포함하는 컴퓨터 저장 매체 및 통신 매체 양자를 포함한다. 저장 매체는, 컴퓨터에 의해 액세스될 수도 있는 임의의 가용 매체일 수도 있다. 한정 이 아닌 예로서, 그러한 컴퓨터 판독가능 매체는 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 저장부, 자기 디스크 저장부 또는 다른 자기 저장 디바이스들, 또는 원하는 프로그램 코드를 명령들 또는 데이터 구조들의 형태로 수록 또는 저장하는데 이용될 수도 있고 컴퓨터에 의해 액세스될 수도 있는 임의의 다른 매체를 포함할 수도 있다.

[0043] 또한, 임의의 커넥션이 컴퓨터 판독가능 매체로 적절히 명명된다. 예를 들어, 동축 케이블, 광섬유 케이블, 꼬임쌍선, 디지털 가입자 라인 ("DSL"), 또는 적외선, 무선, 및 마이크로파와 같은 무선 기술들을 이용하여 웹사이트, 서버, 또는 다른 원격 소스로부터 소프트웨어가 송신된다면, 동축 케이블, 광섬유 케이블, 꼬임쌍선, DSL, 또는 적외선, 무선, 및 마이크로파와 같은 무선 기술들은 매체의 정의에 포함된다.

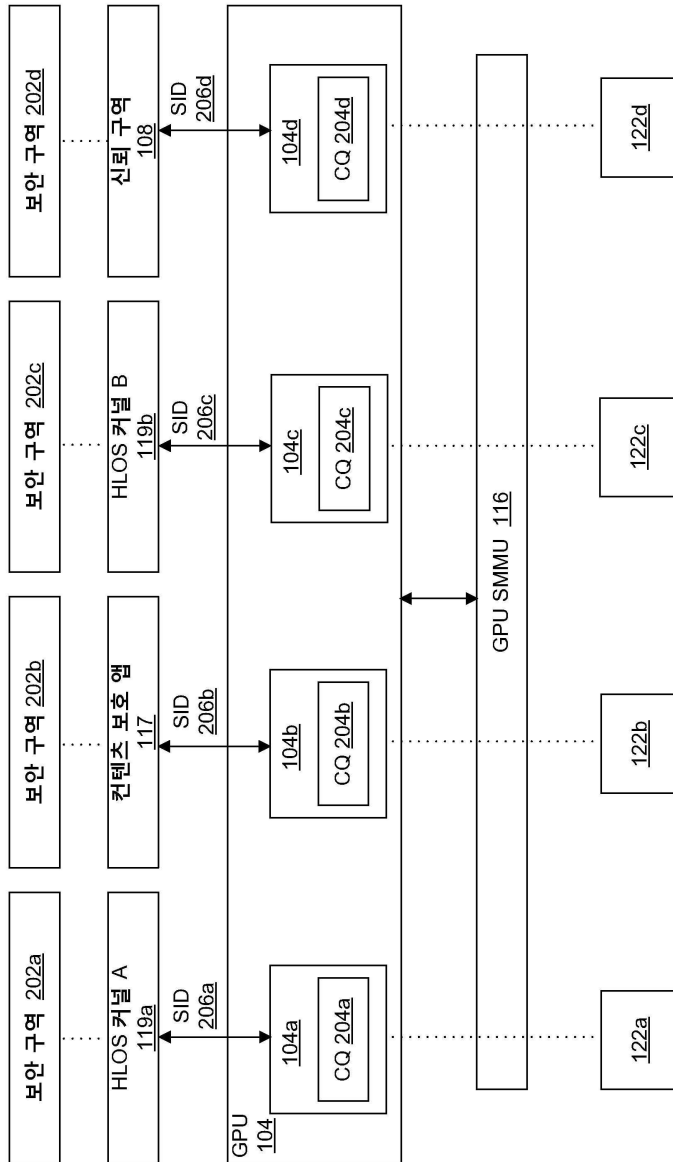
[0044] 본 명세서에서 사용되는 바와 같은 디스크 (disk) 및 디스크 (disc) 는 콤팩트 디스크 ("CD"), 레이저 디스크, 광학 디스크, 디지털 다기능 디스크 ("DVD"), 플로피 디스크 및 블루레이 디스크를 포함하며, 여기서, 디스크 (disk) 는 통상적으로 데이터를 자기적으로 재생하지만 디스크 (disc) 는 레이저를 이용하여 데이터를 광학적으로 재생한다. 상기의 조합들이 또한, 컴퓨터 판독가능 매체의 범위 내에 포함되어야 한다.

도면

도면1

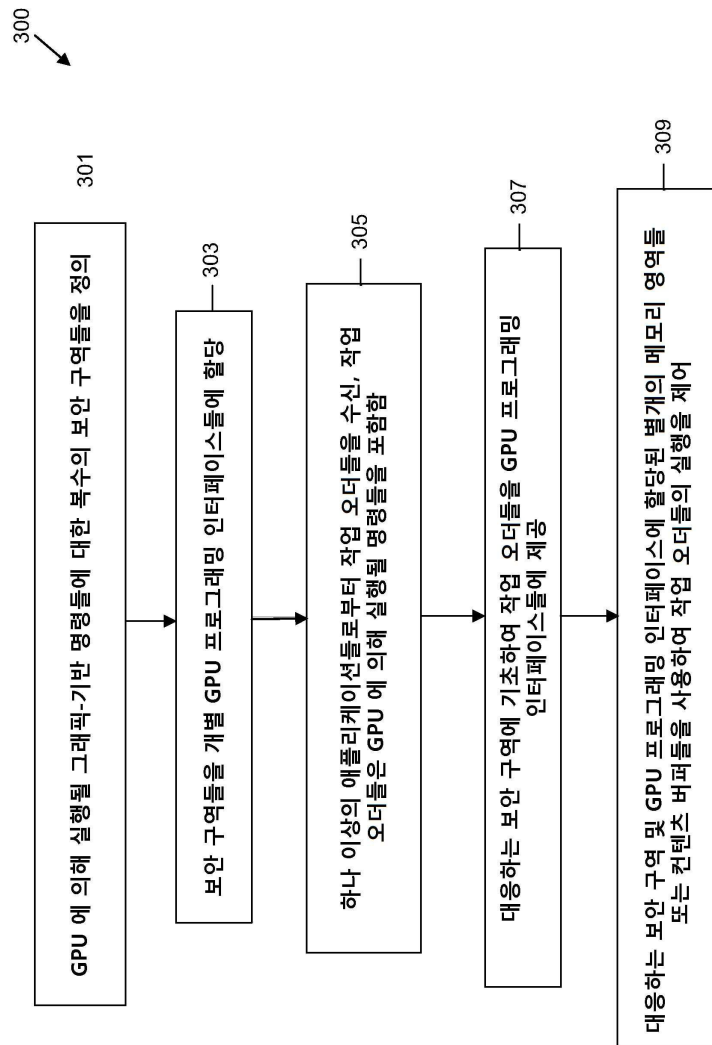


도면2





도면3



도면4

