(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년05월11일
(11) 등록번호 10-1857128
(24) 등록일자 2018년05월04일

(51) 국제특허분류(Int. Cl.)
G06F 21/71 (2013.01) *G06F 21/81* (2013.01)
G06F 21/85 (2013.01) *G06F 21/88* (2013.01)
(52) CPC특허분류
G06F 21/71 (2013.01)
G06F 21/81 (2013.01)
(21) 출원번호 10-2017-0126114
(22) 출원일자 2017년09월28일
심사청구일자 2017년09월28일
(56) 선행기술조사문헌
KR101730772 B1
KR1019980030737 A
KR1020090025846 A
KR1020100133256 A

(73) 특허권자
엘아이지넥스원 주식회사
경기도 용인시 기흥구 마북로 207 (마북동)
(72) 발명자
최원석
경기도 성남시 분당구 서판교로 147
이동훈
경기도 성남시 분당구 판교로 333
(74) 대리인
특허법인우인

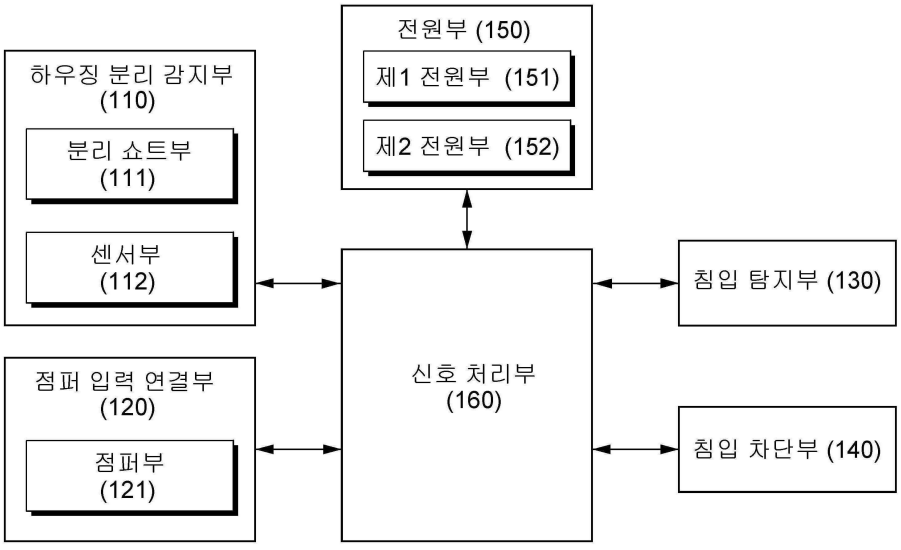
전체 청구항 수 : 총 11 항 심사관 : 구대성

(54) 발명의 명칭 **임베디드 시스템이 탑재된 무기를 보안하기 위한 장치**

(57) 요 약

본 발명은 임베디드 시스템을 탑재한 무기를 도난, 탈취당한 경우에 하우징의 분리를 검출하고, 임베디드 시스템이 해킹당하거나 악용되기 전에 보안 점퍼 코드를 이용하여 아군 여부를 확인함에 따라 조치를 취함으로써 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치를 제안한다.

대 표 도



(52) CPC특허분류
G06F 21/85 (2013.01)
G06F 21/86 (2013.01)
G06F 21/88 (2013.01)

명 세 서

청구범위

청구항 1

무기의 임베디드 시스템을 커버하는 하우징의 분리여부를 감지하는 하우징 분리 감지부;

상기 하우징의 분리를 감지한 경우, 외부로부터 소정 점퍼에 대한 연결시도를 입력받는 점퍼 입력 연결부;

상기 점퍼의 연결이 입력되는 단자를 구비하고, 상기 소정 점퍼에 대해 시도된 연결이 미리 설정된 보안 점퍼 코드와 일치하는지 여부에 따라 외부 침입 발생 여부를 판단하는 신호 처리부; 및

상기 신호 처리부에 의해 외부 침입이 발생한 것으로 판단된 경우, 상기 임베디드 시스템을 파괴하는 침입 차단부;를 포함하는 것을 특징으로 하는 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치.

청구항 2

제 1 항에 있어서,

상기 신호 처리부는,

상기 점퍼 입력 연결부를 통해 시도된 점퍼의 연결이 미리 설정된 보안 점퍼 코드와 일치하는지 비교하고, 일치하는 경우 아군에 의한 정상 동작으로 판단하고, 일치하지 않는 경우 적군에 의한 비정상적인 외부 침입으로 판단하는 침입 탐지부를 더 포함하는 것을 특징으로 하는 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치.

청구항 3

제 1 항에 있어서,

상기 점퍼 입력 연결부는,

다수의 점퍼 각각이 소정의 전압신호를 상기 신호 처리부의 단자로 전달하는 직렬 구조로 연결된 것을 특징으로 하는 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치.

청구항 4

제 3 항에 있어서,

상기 점퍼 입력 연결부는,

상기 각 점퍼의 일단이 상기 신호 처리부의 단자영역에 착탈형으로 접촉하는 구조로 구비되어, 사용자에 의해 각 점퍼가 상기 신호 처리부에 선택적으로 연결되는 것을 특징으로 하는 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치.

청구항 5

제 3 항에 있어서,

상기 점퍼 입력 연결부는,

상기 점퍼마다 온오프되는 스위치와 연결되어, 사용자에 의해 각 점퍼가 상기 신호 처리부에 선택적으로 연결되는 것을 특징으로 하는 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치.

청구항 6

제 1 항에 있어서,

상기 신호 처리부는,

상기 하우징 분리가 감지된 이후 미리 설정된 시간 이내에 상기 점퍼 입력 연결부를 통한 점퍼 연결 시도가 입력되지 않을 경우, 도난으로 간주하여 상기 침입 차단부를 가동시키는 것을 특징으로 하는 임베디드 시스템이

탑재된 무기를 보안하기 위한 장치.

청구항 7

제 1 항에 있어서,

상기 하우징 분리 감지부는,

분리 쇼트부로 구성되고, 상기 분리 쇼트부는 일단이 상기 하우징의 내측에 연결되고, 타단이 상기 신호 처리부와 연결되어, 상기 하우징에 분리가 없이 결합된 상태에서는 상기 일단 및 타단이 전기적으로 연결된 상태로 있고, 상기 하우징이 분리된 상태에서는 상기 일단과 타단의 전기적 연결이 끊어져 개방이 되는 것을 특징으로 하는 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치.

청구항 8

제 7 항에 있어서,

상기 하우징 분리 감지부는,

상기 하우징의 내측에서 일부분이 상기 신호 처리부와 연결되어 상기 하우징의 분리 중에 발생하는 물리적 변화를 감지하는 센서를 더 구비하고,

상기 분리 쇼트부에 의해 상기 하우징의 분리가 감지되고, 상기 센서에 의한 임계치 이상의 측정값을 둘 다 감지한 경우에만, 상기 하우징이 분리된 것으로 판단함으로써, 상기 분리 쇼트부의 감지 오류에 의한 오작동의 확률을 줄이는 것을 특징으로 하는 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치.

청구항 9

제 8 항에 있어서,

상기 하우징 분리 감지부는,

상기 하우징에 탑재된 적어도 하나의 영구자석을 구비하고,

상기 영구자석의 자성을 감지하는 자성감지센서를 포함하며,

상기 신호 처리부는 상기 자성감지센서로부터 입력되는 자성의 세기를 판단하여 미리 설정된 기준값 이하로 자성이 검출되지 않는 경우 상기 하우징에 변형 또는 분리가 발생한 것으로 판단하는 것을 특징으로 하는 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치.

청구항 10

제 8 항에 있어서,

상기 센서는,

상기 하우징의 분리에 의해 접착되어 있던 센서의 이탈을 검출하는 탈부착 센서, 상기 하우징에 발생하는 임계치 이상의 압력을 검출하는 압력센서 및 임계치 이상의 흔들림을 검출하는 자이로 센서 또는 가속도 센서 중 적어도 하나를 포함하는 것을 특징으로 하는 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치.

청구항 11

제 1 항에 있어서,

상기 하우징 분리 감지부에 상시 전원을 공급하는 제1 전원부; 및

상기 시도된 점퍼의 연결이 미리 설정된 보안 점퍼 코드와 일치하는 경우, 상기 임베디드 시스템으로의 전원인가를 허여하는 제2 전원부;를 더 포함하여 구성되는 것을 특징으로 하는 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치로, 보다 상세하게는 임베디드 시스템을 탑재한 무기를 도난, 탈취당한 경우에 하우징의 분리를 검출하고, 임베디드 시스템이 해킹당하거나 악용되기 전에 보안 점퍼 코드를 이용하여 아군 여부를 확인함에 따라 조치를 취함으로써 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치에 관한 것이다.

배 경 기 술

[0002] 현대전이 갈수록 첨단화되어 감에 따라 무기에서 차지하는 전자 부품의 비중이 커지고 있으며, 드론, 탱크, 로봇 등과 같이 임베디드 시스템이 탑재된 무기들이 많아지고 있다.

[0003] 전시상황 또는 전시상황이 아니더라도 적군이 아군의 무기를 탈취하는 경우가 있다. 적군은 탈취한 무기를 분리해서 설계를 파악한 후, 최첨단 무기 구조 및 제조 기술을 도용하거나, 무기를 뜻대로 변형하여 자신들의 무기로 이용할 수도 있다.

[0004] 특히, 현대전의 무기는 전술한 바와 같이 임베디드 시스템을 탑재하는 무기들이 많기 때문에, 적군에 의해 하드웨어 기술뿐만 아니라 소프트웨어 기술을 해킹당한다면, 무기의 탈취가 심각한 무기기술 정보유출로 이어질 수 있으며, 아군에게 심각한 피해를 입힐 위험이 있게 된다.

[0005] 한국등록특허 제10-1041927호는 인증매체에 의하여 가압되는 전원스위치에 의해 동작중인 유도무기 시스템에 영향을 미치지 않는 인증매체의 유도무기의 보안인증 장치 및 이를 구비하는 보안인증 시스템에 대하여 기술하고 있다.

[0006] 그러나, 이 방법은 궁극적으로 적군에 의해 무기를 도난 또는 탈취당한 경우에 대비하여 무기의 임베디드 시스템을 스스로 보안할 수 있는 방법을 제시하고 있지 못하고 있기 때문에 전술한 문제점을 해결할 수가 없다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 상기한 문제점을 해결하기 위해 안출된 것으로서, 임베디드 시스템을 탑재한 무기를 도난, 탈취당한 경우에 하우징의 분리를 검출하고, 임베디드 시스템이 해킹당하거나 악용되기 전에 보안 점퍼 코드를 이용하여 아군 여부를 확인함에 따라 조치를 취함으로써 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치를 제안함을 목적으로 한다.

[0008] 그러나 본 발명의 목적은 상기에 언급된 사항으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0009] 본 발명은 상기한 목적을 달성하기 위해 안출된 것으로서, 무기의 임베디드 시스템을 커버하는 하우징의 분리여부를 감지하는 하우징 분리 감지부와, 상기 하우징의 분리를 감지한 경우, 외부로부터 소정 점퍼에 대한 연결시도를 입력받는 점퍼 입력 연결부와, 상기 점퍼의 연결이 입력되는 단자를 구비하고, 상기 소정 점퍼에 대해 시도된 연결이 미리 설정된 보안 점퍼 코드와 일치하는지 여부에 따라 외부 침입 발생 여부를 판단하는 신호 처리부 및 상기 신호 처리부에 의해 외부 침입이 발생한 것으로 판단된 경우, 상기 임베디드 시스템을 파괴하는 침입 차단부를 포함하는 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치를 제안한다.

발명의 효과

[0010] 본 발명의 실시 예에 따른 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치에 따르면, 임베디드 시스템을 탑재한 무기를 도난, 탈취당한 경우 아군의 원격 조정이 없더라도 스스로 하우징의 분리 상태를 검출하고, 임베디드 시스템이 해킹당하거나 악용되기 전에 보안 점퍼 코드를 이용하여 아군 인증 결과에 따라 조치를 취함으로써 임베디드 시스템이 탑재된 무기를 해킹, 악용 및 기술유출로부터 보안할 수 있다.

[0011] 또한, 본 발명은 아군의 무기가 적군에 의해 도난 또는 탈취 당하더라도 역공학(reverse engineering)의 난이도를 높임으로써, 하드웨어 및 소프트웨어를 포함하는 무기를 재활용하거나 해킹하기 어렵도록 구성할 수 있다.

도면의 간단한 설명

[0012] 도 1은 본 발명의 일실시예에 따른 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치의 구성을 개략적으로 도시하는 블록도이다.

도 2는 본 발명의 일실시예에 따른 하우징 분리 감지부의 분리 쇼트부를 도시하는 도면이다.

도 3은 본 발명의 일실시예에 따른 영구자석의 세기 변화 측정을 이용하는 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치의 일부 구성을 개략적으로 도시하는 도면이다.

도 4는 본 발명의 일실시예에 따른 점퍼 입력 연결부의 다수 점퍼로 구성된 점퍼부의 일예를 도시하는 도면이다.

도 5는 본 발명의 일실시예에 따른 침입 탐지부에 설정된 보안 점퍼 코드의 일예를 도시하는 도면이다.

도 6은 본 발명의 일실시예에 따른 침입 차단부를 구성하는 발열저항 및 스위치를 개략적으로 도시하는 도면이다.

도 7은 본 발명의 일실시예에 따른 임베디드 시스템이 탑재된 무기를 보안하기 위한 방법을 설명하기 위한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 이하, 본 발명의 바람직한 실시예를 첨부된 도면들을 참조하여 상세히 설명한다. 우선 각 도면의 구성요소들에 참조 부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다. 또한, 이하에서 본 발명의 바람직한 실시예를 설명할 것이나, 본 발명의 기술적 사상은 이에 한정하거나 제한되지 않고 당업자에 의해 변형되어 다양하게 실시될 수 있음은 물론이다.

[0014] 미사일, 드론, 탱크와 같은 거의 모든 첨단무기에는 컴퓨터 역할을 하는 프로세서가 탑재되고, 이를 위해서 임베디드 시스템이 탑재된다.

[0015] 이러한 임베디드 시스템이 탑재된 무기가 도난당했을 경우, 적에 의해서 악용되거나 해킹당하고 기술 유출되는 상황을 막기 위한 방법이 필요하다.

[0016] 보통 임베디드 시스템의 경우에는 임베디드 전자 보드를 외부에 노출시키지 않게 하고, 물리적인 충격이나 환경요소로부터 보호하기 위해 하우징 처리를 한다.

[0017] 본 발명은 하우징에 의해 커버된 임베디드 시스템을 탑재한 무기를 보안하기 위한 장치를 제안하고자 한다.

[0018] 도 1은 본 발명의 일실시예에 따른 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치의 구성을 개략적으로 도시하는 블록도이다.

[0019] 도 1을 참조하면, 본 발명의 일실시예에 따른 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치(100)는 하우징 분리 감지부(110), 점퍼 연결 입력부(120), 침입 탐지부(130), 침입 차단부(140), 전원부(150) 및 신호 처리부(160)를 포함하여 구성된다.

[0020] 먼저, 신호 처리부(160)는 본 발명에 따른 임베디드 시스템이 탑재된 무기를 보안하기 위한 장치의 전체 기능 및 구성을 제어하는 역할을 하고, 사용자 요구에 맞게 프로그래밍하여 사용할 수 있는 일종의 주문형 반도체(ASIC)인 FPGA(Field programmable gate array)로 구성될 수 있다.(이하, 신호 처리부(160)를 FPGA와 혼용할 수 있다.)

[0021] 하우징 분리 감지부(110)는 무기의 임베디드 시스템을 커버하는 하우징의 분리를 감지하는 역할을 한다.

[0022] 상술한 바와 같이 대부분의 무기의 임베디드 시스템은 전자보드를 외부에 노출시키지 않게 하고, 물리적인 충격이나 환경요소로부터 보호하기 위해 하우징에 의해 커버된다.

[0023] 따라서, 적군이 무기를 탈취해서 임베디드 시스템을 분석하고자 한다면 먼저 하우징부터 분리할 것이기 때문에 본 발명의 장치는 임베디드 시스템을 커버하는 하우징의 분리를 우선 감지한다.

[0024] 이를 위해, 하우징 분리 감지부(110)는 다양한 방법으로 하우징의 분리 또는 분리를 감지할 수 있는데 먼저 도 2에 도시된 바와 같이, 분리 쇼트부(111)를 이용할 수 있다.

[0025] 분리 쇼트부(111)는 하우징(H)의 내측에 구비되되 일단(11)이 신호 처리부(160)과 연결되고, 타단(12)이 하우징(H)의 내벽에 연결되어, 하우징(H)에 분리가 없이 결합된 상태에서는 일단(11)과 타단(12)이 전기적으로 연결된 상태로 있고, 하우징(H)이 분리된 상태에서는 일단(11)과 타단(12)의 전기적 연결이 끊어져 개방(Open)이 된다.

[0026] 즉, 분리 쇼트부(111)에서 하우징의 분리에 의해 일단(11)과 타단(12)의 전기적 연결이 끊어지면 신호 처리부(160)는 개방을 감지하게 되는데 예를 들어, 하우징 결합을 1로 인식하고, 하우징의 분리를 0으로 인식하도록 신호 처리부(160) 내부에서 풀 다운(Pull down)처리할 수 있다.

[0027] 그런데 무기를 이용하다보면 지면의 불균일이나 바람, 주변 폭발에 의한 타격 등의 요인에 의해 무기가 크게 흔들리거나 이동 속도나 진행 방향에 큰 변경이 발생할 수 있다.

[0028] 이 때문에 무기가 도난이나 탈취당한 상황이 아닌데도 군사상황 또는 전시상황에서 분리 쇼트부(111)가 하우징이 분리된 것으로 감지 오류를 발생할 위험이 있을 수 있다.

[0029] 이와 같은 상황을 방지하기 위해 하우징 분리 감지부(110)는 센서부(112)를 더 구비하여, 신호 처리부(160)에서는 분리 쇼트부(111)에서 개방을 감지하고 이와 동시에 센서부(112)에 의해 하우징 분리에 의한 물리적 변화가 임계치 이상의 측정값으로 감지된 경우에만 하우징(H)이 분리된 것으로 판단함으로써, 분리 쇼트부(111)의 감지 오류에 의한 오동작의 확률을 줄일 수 있다.

[0030] 센서부(112)는 하우징(H)의 내측에서 일부분이 신호 처리부(160)과 연결되어 하우징(H)의 분리 중에 발생하는 물리적 변화를 감지하는 역할을 한다. 이를 위해, 센서부(112)는 도 3에 도시된 바와 같이 자성감지센서를 구비하여 하우징에 탑재된 적어도 하나의 영구자석(113)의 자성을 측정하며, 자성의 세기 변화를 검출한다.

[0031] 이와 같이 측정된 자성의 측정값 및 자성의 세기 변화를 신호 처리부(160)로 전송하면, 신호 처리부(160)는 자성의 세기를 판단하여 미리 설정된 기준값 이하로 자성이 검출되지 않는 경우를 하우징(H)에 변형 또는 분리가 발생한 것으로 판단한다.

[0032] 이외에도 센서부(112)는 하우징(H)에 발생하는 다른 물리적 변화를 감지하기 위해 하우징(H)의 분리에 의해 접착되어 있던 센서의 이탈을 검출하는 탈부착 센서, 하우징(H)에 발생하는 임계치 이상의 압력을 검출하는 압력센서 및 임계치 이상의 흔들림을 검출하는 자이로 센서 또는 가속도 센서 중 적어도 하나를 포함하여 구비될 수 있다.

[0033] 신호 처리부(160)는 하우징 분리 감지부(110)를 통해 하우징(H)이 분리된 것으로 판단되면, 신호 처리부(160)의 입력단자에 연결된 다수 점퍼로 구성된 점퍼 입력 연결부(120)에 전원을 인가하고, 외부로부터 소정 점퍼에 대한 연결시도를 입력받는다.

[0034] 하우징 분리 감지부(110)에는 제1 전원부(151)를 통해 저전력을 상시 공급하도록 한다.

[0035] 점퍼 입력 연결부(120)는 도 4에 도시된 바와 같이, 다수 점퍼로 구성된 점퍼부(121)를 포함한다. 점퍼부(121)는 외부로부터 각 점퍼를 연결시키기 위한 시도에 의해 해당 점퍼가 신호 처리부(160)의 단자영역에 연결되는 경우, 소정의 전압신호를 신호 처리부(160)의 단자영역으로 전달하는 직렬 구조로 연결되어 있다.

[0036] 점퍼 입력 연결부(120)는 각 점퍼의 일단이 신호 처리부(160)의 단자영역에 착탈형으로 접촉하는 단자구조로 구비되어, 사용자에 의해 각 점퍼가 신호 처리부(160)에 선택적으로 연결될 수 있다. 이에 의해, 사용자는 미리 설정된 보안 점퍼 코드를 맞추기 위한 점퍼 연결을 시도할 수 있다.

[0037] 이외에 점퍼 입력 연결부(120)는 점퍼마다 턴온 또는 턴오프되는 스위치와 연결되어, 스위치가 턴온되면 해당 점퍼는 신호 처리부(160)의 입력단자에 연결되고, 스위치가 턴오프되면 해당 점퍼는 신호 처리부(160)의 입력단자에 연결되지 않는 구조로 구비될 수도 있다.

[0038] 침입 탐지부(130)는 도 5에 도시된 바와 같이, 점퍼 입력 연결부(120)를 통해 시도된 점퍼의 연결이 미리 설정된 보안 점퍼 코드와 일치하는지 여부를 판단하여, 신호 처리부(160)에 보안 점퍼 코드와의 일치 여부 결과를 전달한다.

[0039] 침입 탐지부(130)는 신호 처리부(160)의 일부 구조로 구비되거나, 분리될 수 있음에 한정하지 않는다.

[0040] 침입 탐지부(130)는 시도된 점퍼의 연결이 미리 설정된 보안 점퍼 코드와 일치하는 경우, 이를 아군에 의한 정상 동작으로 판단한다.

[0041] 반면, 시도된 점퍼의 연결이 미리 설정된 보안 점퍼 코드와 일치하지 않는 경우, 이를 적군에 의한 도난, 탈취

또는 외부 침입이 탐지된 것으로 판단하여 침입 차단부(140)를 동작시킨다.

[0042] 예를 들어, 도 5에 도시된 바와 같이 보안 점퍼 코드가 '1000100100'가 설정되어 있는 무기에 사용자가 점퍼 입력 연결부(120)를 통해 1번째, 5번째, 8번째 점퍼를 신호 처리부(160)의 입력단자에 연결시키는 경우, 침입 탐지부(130)는 이 연결시도를 정상으로 판단할 것이다. 점퍼 연결시도가 정상으로 판단된 경우, 신호 처리부(160)는 제2 전원부(152)를 통해 신호 처리부(160)의 다양한 장치들에 해당하는 전원들이 공급되도록 허여하고, 정상 모드가 실행되게 한다.

[0043] 보안 점퍼 코드는 무기를 개발한 사람 또는 아군만 알도록 관리된 보안 정보이다. 또한, 아군만이 무기의 하우징을 분리한 후에는 미리 설정된 시간 이내에 점퍼부(121)를 보안 점퍼 코드에 따라 연결시켜야 하는 보안 단계를 알고 있을 것이다.

[0044] 또한, 침입 탐지부(130)는 하우징 분리가 감지된 이후 미리 설정된 시간 이내에 점퍼 입력 연결부(120)를 통한 점퍼 연결 시도가 발생하지 않을 경우, 이를 적군에 의한 탈취 또는 도난 상태 또는 외부 침입이 탐지된 것으로 간주하여 침입 차단부(140)를 동작시킨다.

[0045] 침입 차단부(140)는 침입 탐지부(130) 또는 신호 처리부(160)에 의해 무기가 외부 침입 또는 도난, 탈취된 상태로 탐지된 경우, 임베디드 시스템을 파괴모드를 실행한다. 이를 위해, 침입 차단부(140)는 도 6에 도시된 바와 같이, 스위치(141와 발열저항(142)으로 구성될 수 있다.

[0046] 상기 파괴모드는 신호 처리부(160)이 회로카드의 적어도 일부를 스위치(141)를 통해 연결하여 쇼트시킴으로써 임베디드 시스템을 파괴시키거나, 구비된 발열저항(142)을 동작시켜 보드의 중요한 부분을 태워버리는 실행일 수 있다.

[0047] 여기서, 스위치(141)는 디지털 스위치에 비해 비교적 큰 전력 전달이 가능한 기계적 아날로그 스위치가 채용됨이 바람직하다.

[0048] 즉, 디지털 스위치로 파괴모드를 실행할 경우, 디지털 스위치가 먼저 파손되거나 보드를 파손시킬 수준의 전력 전달이 안 될 수 있기 때문에 상대적으로 큰 전력 전달이 가능한 아날로그 스위치를 이용한다.

[0049] 여기서, 파괴모드가 실행될 회로카드의 일부란, 설계상 전압 또는 전류 인가 시 파손을 야기할 수 있는 전자장치의 입출력 단자 또는 전원단자를 일컫는다.

[0050] 이와 같이 본 발명은 아군의 무기가 적군에 의해 도난 또는 탈취 당하더라도 역공학(reverse engineering)의 난이도를 높일 수 있어, 하드웨어 및 소프트웨어를 포함하는 무기를 재활용하거나 해킹하기 어렵도록 구성할 수 있다.

[0051] 도 7은 본 발명의 실시 예에 따른 임베디드 시스템이 탑재된 무기에 대한 보안 방법을 설명하기 위한 순서도이다.

[0052] 이하, 도 7을 참조하여 본 발명의 실시 예에 따른 임베디드 시스템이 탑재된 무기에 대한 보안 방법을 설명하기로 한다.

[0053] 먼저, 제1 전원부를 통해 하우징 분리 감지부(110)에 상시전원을 공급하여 무기의 임베디드 시스템을 커버하는 하우징에 발생하는 물리적 변화를 감지한다(S701).

[0054] 대부분의 무기의 임베디드 시스템은 전자보드를 외부에 노출시키지 않게 하고, 물리적인 충격이나 환경요소로부터 보호하기 위해 하우징에 의해 커버된다. 따라서, 적군이 무기를 탈취해서 임베디드 시스템을 분석하고자 한다면 먼저 하우징부터 분리할 것이기 때문에 본 발명의 장치는 임베디드 시스템을 커버하는 하우징의 분리를 우선 감지한다.

[0055] 이를 위해, 하우징 분리 감지부(110)는 다양한 방법으로 하우징의 분리를 감지할 수 있는데 먼저 도 2에 도시된 바와 같이, 분리 쇼트부(111)를 이용할 수 있다.

[0056] 분리 쇼트부(111)는 하우징(H)의 내측에 구비되되 일단(11)이 신호 처리부(160)과 연결되고, 타단(12)이 하우징(H)의 내벽에 연결되어, 하우징(H)에 분리가 없이 결합된 상태에서는 일단(11)과 타단(12)이 전기적으로 연결된 상태로 있고, 하우징(H)이 분리된 상태에서는 일단(11)과 타단(12)의 전기적 연결이 끊어져 개방이 된다.

[0057] 즉, 분리 쇼트부(111)에서 하우징의 분리에 의해 일단(11)과 타단(12)의 전기적 연결이 끊어지면 신호 처리부(160)는 개방을 감지하게 되는데 예를 들어, 하우징 결합을 1로 인식하고, 하우징의 분리를 0으로 인식하도록

신호 처리부(160) 내부에서 풀 다운(Pull down)처리할 수 있다.

[0058] 그런데 무기를 이용하다보면 지면의 불균일이나 바람, 주변 폭발에 의한 타격 등의 요인에 의해 무기가 크게 흔들리거나 이동 속도나 진행 방향에 큰 변경이 발생할 수 있다.

[0059] 이 때문에 무기가 도난이나 탈취당한 상황이 아닌데도 군사상황 또는 전시상황에서 분리 쇼트부(111)가 하우징이 분리된 것으로 감지 오류를 발생할 위험이 있을 수 있다.

[0060] 이와 같은 상황을 방지하기 위해 하우징 분리 감지부(110)는 센서부(112)를 더 구비하여, 신호 처리부(160)에서는 분리 쇼트부(111)에서 개방을 감지하고 이와 동시에 센서부(112)에 의해 하우징 분리에 의한 물리적 변화가 임계치 이상의 측정값으로 감지된 경우에만 하우징(H)이 분리된 것으로 판단함으로써, 분리 쇼트부(111)의 감지 오류에 의한 오동작의 확률을 줄일 수 있다.

[0061] 센서부(112)는 하우징(H)의 내측에서 일부분이 신호 처리부(160)과 연결되어 하우징(H)의 분리 중에 발생하는 물리적 변화를 감지하는 역할을 한다. 이를 위해, 센서부(112)는 도 3에 도시된 바와 같이 자성감지센서를 구비하여 하우징에 탑재된 적어도 하나의 영구자석의 자성을 측정하며, 자성의 세기 변화를 검출한다.

[0062] 이와 같이 측정된 자성의 측정값 및 자성의 세기 변화를 신호 처리부(160)로 전송하면, 신호 처리부(160)는 자성의 세기를 판단하여 미리 설정된 기준값 이하로 자성이 검출되지 않는 경우를 하우징(H)에 변형 또는 분리가 발생한 것으로 판단한다.

[0063] 이외에도 센서부(112)는 하우징(H)에 발생하는 다른 물리적 변화를 감지하기 위해 하우징(H)의 분리에 의해 접착되어 있던 센서의 이탈을 검출하는 탈부착 센서, 하우징(H)에 발생하는 임계치 이상의 압력을 검출하는 압력센서 및 임계치 이상의 흔들림을 검출하는 자이로 센서 또는 가속도 센서 중 적어도 하나를 포함하여 구비될 수 있다.

[0064] 다음으로, S710 단계에서하우징 분리 감지부(110)를 통해 하우징의 분리를 감지한 경우, 점퍼 입력 연결부(120)가 다수 점퍼로 구성된 점퍼부에 전원을 인가하고, 외부로부터 소정 점퍼에 대한 연결시도를 입력받는다(S720).

[0065] 여기서, 점퍼 입력 연결부(120)는 도 4에 도시된 바와 같이, 다수 점퍼로 구성된 점퍼부(121)를 포함한다. 점퍼부(121)는 외부로부터 각 점퍼를 연결시키기 위한 시도에 의해 해당 점퍼가 신호 처리부(160)의 단자영역에 연결되는 경우, 소정의 전압신호를 신호 처리부(160)의 단자영역으로 전달하는 직렬 구조로 연결되어 있다.

[0066] 점퍼 입력 연결부(120)는 각 점퍼의 일단이 신호 처리부(160)의 단자영역에 착탈형으로 접촉하는 단자구조로 구비되어, 사용자에 의해 각 점퍼가 신호 처리부(160)에 선택적으로 연결될 수 있다. 이에 의해, 사용자는 미리 설정된 보안 점퍼 코드를 맞추기 위한 점퍼 연결을 시도할 수 있다.

[0067] 이외에 점퍼 입력 연결부(120)는 점퍼마다 턴온 또는 턴오프되는 스위치와 연결되어, 스위치가 턴온되면 해당 점퍼는 신호 처리부(160)의 입력단자에 연결되고, 스위치가 턴오프되면 해당 점퍼는 신호 처리부(160)의 입력단자에 연결되지 않는 구조로 구비될 수도 있다.

[0068] 다음으로, 침입 탐지부(130)가 시도된 점퍼의 연결이 미리 설정된 보안 점퍼 코드와 일치하는지 여부를 판단하여(S730) 외부 침입을 탐지한다.

[0069] 즉, 침입 탐지부(130)는 도 5에 도시된 바와 같이, 점퍼 입력 연결부(120)를 통해 시도된 점퍼의 연결이 미리 설정된 보안 점퍼 코드와 일치하는지 여부를 판단하여, 신호 처리부(160)에 보안 점퍼 코드와의 일치 여부 결과를 전달한다. 침입 탐지부(130)는 신호 처리부(160)의 일부 구조로 구비되거나, 분리될 수 있음에 한정하지 않는다.

[0070] 침입 탐지부(130)는 시도된 점퍼의 연결이 미리 설정된 보안 점퍼 코드와 일치하는 경우, 이를 아군에 의한 정상 동작으로 판단하고 제2 전원부를 통해 FPGA의 다양한 장치들에 해당하는 제2 전원들을 공급하고(S732), 정상 모드를 실행한다(S734).

[0071] 반면, 시도된 점퍼의 연결이 미리 설정된 보안 점퍼 코드와 일치하지 않는 경우, 이를 적군에 의한 도난, 탈취 또는 외부 침입이 탐지된 것으로 판단하여 침입 차단부(140)를 동작시켜 임베디드 시스템 파괴모드를 실행한다(S740).

[0072] 예를 들어, 도 5에 도시된 바와 같이 보안 점퍼 코드가 ‘1000100100’ 가 설정되어 있는 무기에 사용자가 점퍼

입력 연결부(120)를 통해 1번째, 5번째, 8번째 점퍼를 신호 처리부(160)의 입력단자에 연결시키는 경우, 침입 탐지부(130)는 이 연결시도를 정상으로 판단할 것이다.

[0073] 이와 같은 보안 점퍼 코드는 무기를 개발한 사람 또는 아군만 알도록 관리된 보안 정보이다. 또한, 아군만이 무기의 하우징을 분리한 후에는 미리 설정된 시간 이내에 점퍼부(121)를 보안 점퍼 코드에 따라 연결시켜야 하는 보안 단계를 알고 있을 것이다.

[0074] 이 S740 단계의 임베디드 시스템을 파괴하는 모드를 실행하기 전에, 무기 주변정보를 수집하여 미리 설정된 아군의 주소로 전송한 뒤에 임베디드 시스템을 파괴한다.

[0075] 여기서, 무기 주변정보는 무기 주변에 대한 영상 데이터, 이미지 데이터, 음성 데이터 및 위치 정보 데이터 중 적어도 하나를 포함할 수 있고, 이러한 데이터는 각 데이터를 획득할 수 있는 카메라 모듈, GIS(지리정보시스템 또는 공간정보시스템), GPS(위성항법시스템) 및 RS(원격탐사) 중 적어도 하나를 이용하여 획득할 수 있다.

[0076] 여기서, 무기는 탑재된 통신단말기를 통해 이동위성통신체계를 이용하여 무기 주변정보를 미리 설정된 아군의 통신장치로 전송되게 할 수 있다. 구체적으로, 무기는 MOUS(Mobile User Objective System)과 같이 이동위성통신을 지원하기 위한 narrowband 위성통신체계를 채용하여 원거리에서도 아군의 장치로 음성 및 저속의 데이터(~384Kbps) 통신을 지원할 수 있다. MOUS는 전 세계를 대상으로 작전을 수행하기 위해 정지궤도에 다수의 위성을 배치시켜 음성 및 저속의 데이터(~384Kbps) 통신을 지원하고, 무기는 MOUS 단말기를 탑재한다.

[0077] 이러한 부가 기능 실행을 통해, 아군은 무기를 도난, 탈취당하더라도 무기 주변을 찰나라도 촬영한 이미지 데이터 또는 영상 데이터를 통해 사병들의 전투복 등을 확인할 수 있어 적군의 정체를 판가름할 수 있고, 녹취된 음성 데이터를 통해 적군의 국적이나 적군의 정체 등을 확인할 수 있으며, 위치 정보 데이터를 통해 적군 기지의 위치를 파악하는 데에 도움이 될 수 있다.

[0078] 구체적으로, 침입 차단부(140)는 침입 탐지부(130) 또는 신호 처리부(160)에 의해 무기가 외부 침입 또는 도난, 탈취된 상태로 탐지된 경우, 임베디드 시스템을 파괴모드를 실행하는데, 이를 위해 침입 차단부(140)는 도 6에 도시된 바와 같이, 스위치(141)와 발열저항(142)으로 구성될 수 있다.

[0079] 상기 파괴모드는 신호 처리부(160)이 회로카드의 적어도 일부를 스위치(141)를 통해 연결하여 쇼트시킴으로써 임베디드 시스템을 파괴시키거나, 구비된 발열저항(142)을 동작시켜 보드의 중요한 부분을 태워버리는 실행일 수 있다.

[0080] 여기서, 스위치(141)는 디지털 스위치에 비해 비교적 큰 전력 전달이 가능한 기계적 아날로그 스위치가 채용됨이 바람직하다.

[0081] 즉, 디지털 스위치로 파괴모드를 실행할 경우, 디지털 스위치가 먼저 파손되거나 보드를 파손시킬 수준의 전력 전달이 안 될 수 있기 때문에 상대적으로 큰 전력 전달이 가능한 아날로그 스위치를 이용한다.

[0082] 여기서, 파괴모드가 실행될 회로카드의 일부란, 설계상 전압 또는 전류 인가 시 파손을 야기할 수 있는 전자장치의 입출력 단자 또는 전원단자를 일컫는다.

[0083] 한편, 침입 탐지부(130)는 하우징 분리가 감지된 이후 미리 설정된 시간 이내에 점퍼 입력 연결부(120)를 통한 점퍼 연결 시도가 발생하지 않을 경우, 이를 적군에 의한 탈취 또는 도난 상태 또는 외부 침입이 탐지된 것으로 간주하여 침입 차단부(140)를 동작시킨다.

[0084] 이상에서 설명한 본 발명의 실시예를 구성하는 모든 구성요소들이 하나로 결합하거나 결합하여 동작하는 것으로 기재되어 있다고 해서, 본 발명이 반드시 이러한 실시예에 한정되는 것은 아니다. 즉, 본 발명의 목적 범위 안에서라면, 그 모든 구성요소들이 하나 이상으로 선택적으로 결합하여 동작할 수도 있다. 또한, 그 모든 구성요소들이 각각 하나의 독립적인 하드웨어로 구현될 수 있지만, 각 구성요소들의 그 일부 또는 전부가 선택적으로 조합되어 하나 또는 복수개의 하드웨어에서 조합된 일부 또는 전부의 기능을 수행하는 프로그램 모듈을 갖는 컴퓨터 프로그램으로서 구현될 수도 있다. 또한, 이와 같은 컴퓨터 프로그램은 USB 메모리, CD 디스크, 플래쉬 메모리 등과 같은 컴퓨터가 읽을 수 있는 기록매체(Computer Readable Media)에 저장되어 컴퓨터에 의하여 읽혀지고 실행됨으로써, 본 발명의 실시예를 구현할 수 있다. 컴퓨터 프로그램의 기록매체로서는 자기 기록매체, 광 기록매체 등이 포함될 수 있다.

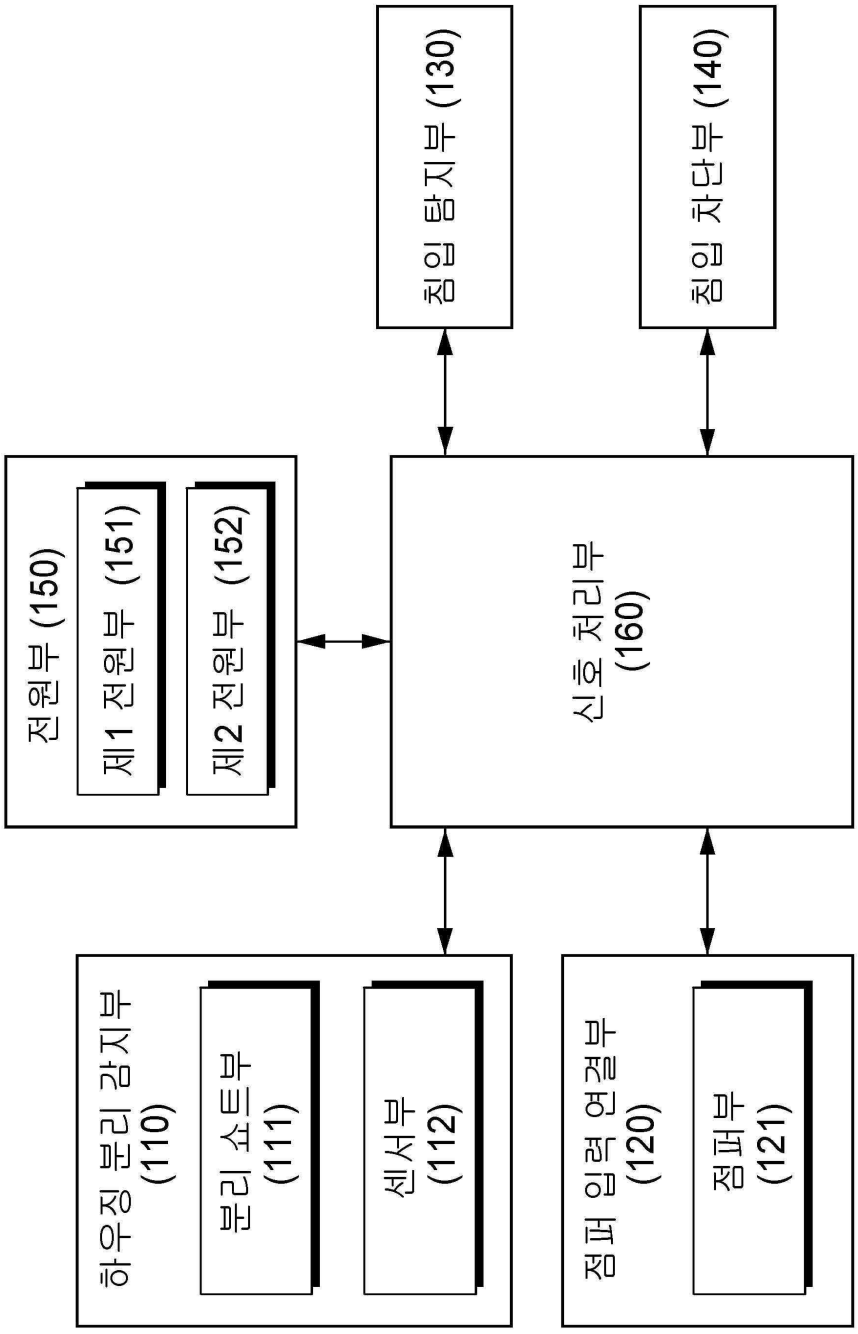
[0085] 또한, 기술적이거나 과학적인 용어를 포함한 모든 용어들은, 상세한 설명에서 다르게 정의되지 않는 한, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 갖는다. 사

전에 정의된 용어와 같이 일반적으로 사용되는 용어들은 관련 기술의 문맥상의 의미와 일치하는 것으로 해석되어야 하며, 본 발명에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

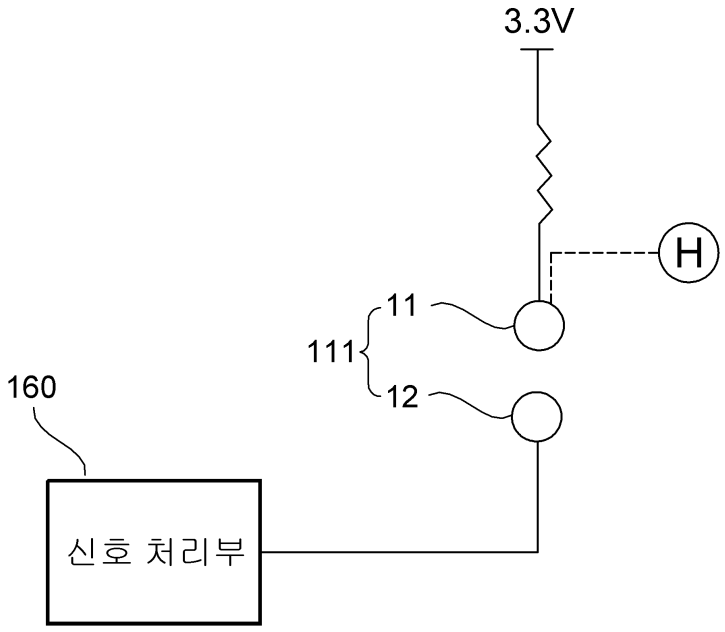
[0086] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위 내에서 다양한 수정, 변경 및 치환이 가능할 것이다. 따라서, 본 발명에 개시된 실시예 및 첨부된 도면들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예 및 첨부된 도면에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구 범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리 범위에 포함되는 것으로 해석되어야 할 것이다.

도면

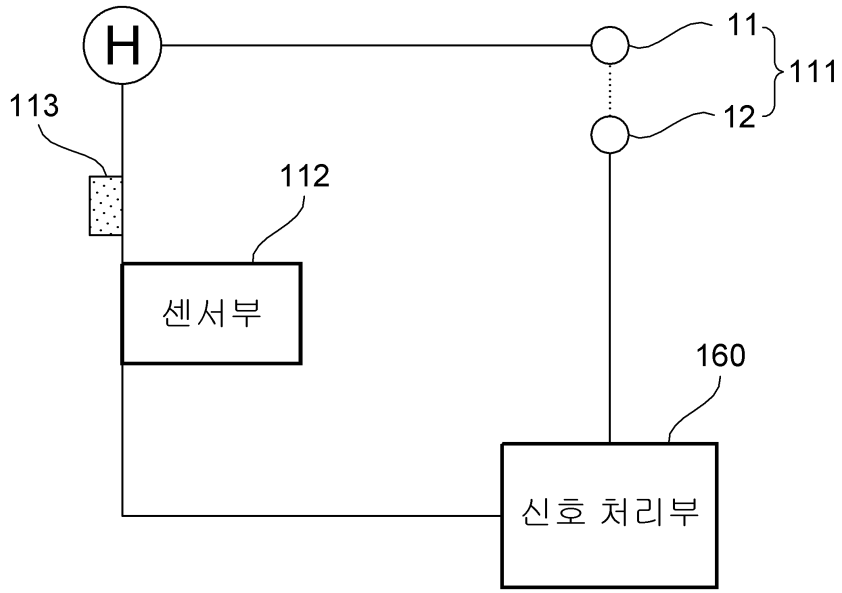
도면1



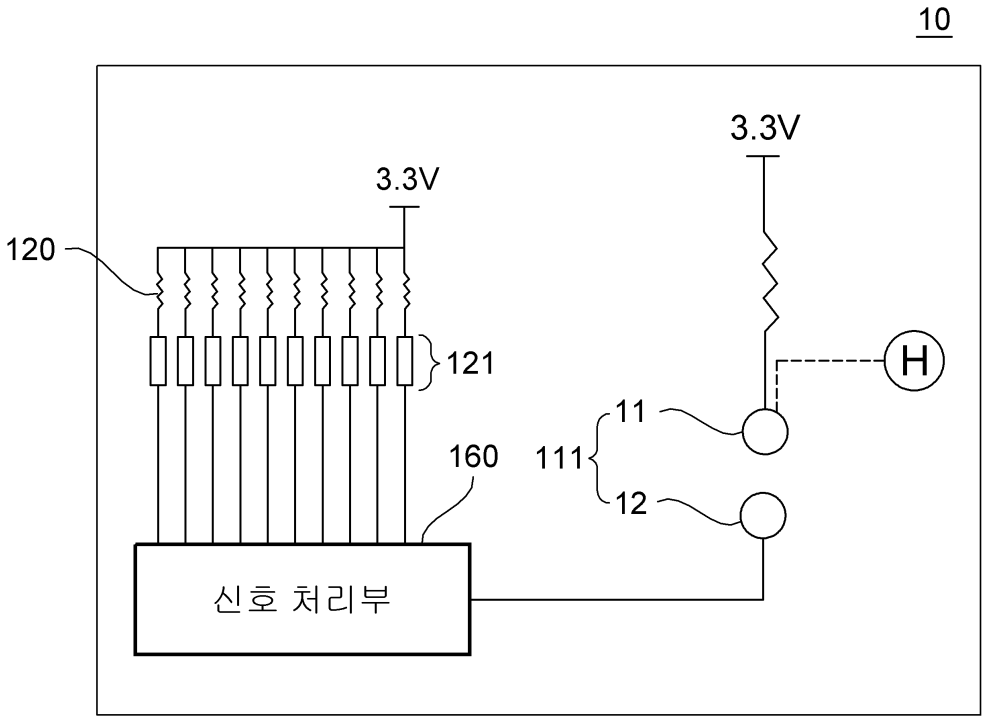
도면2



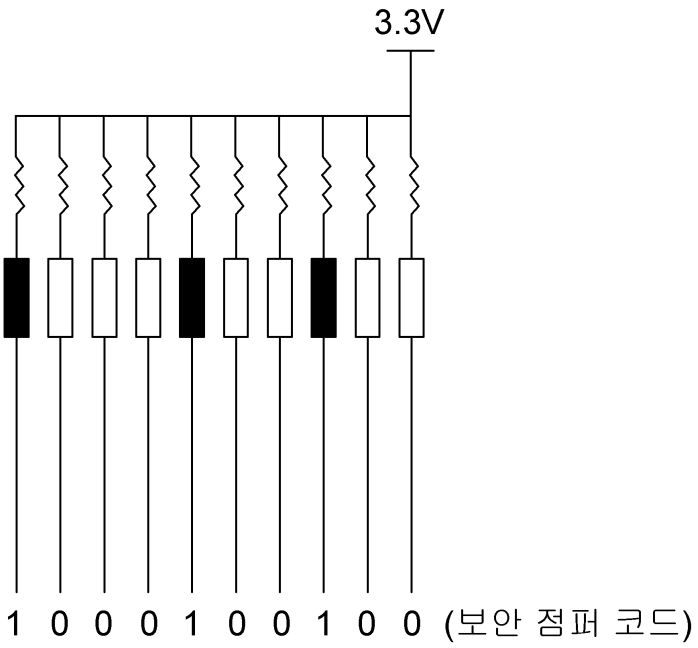
도면3



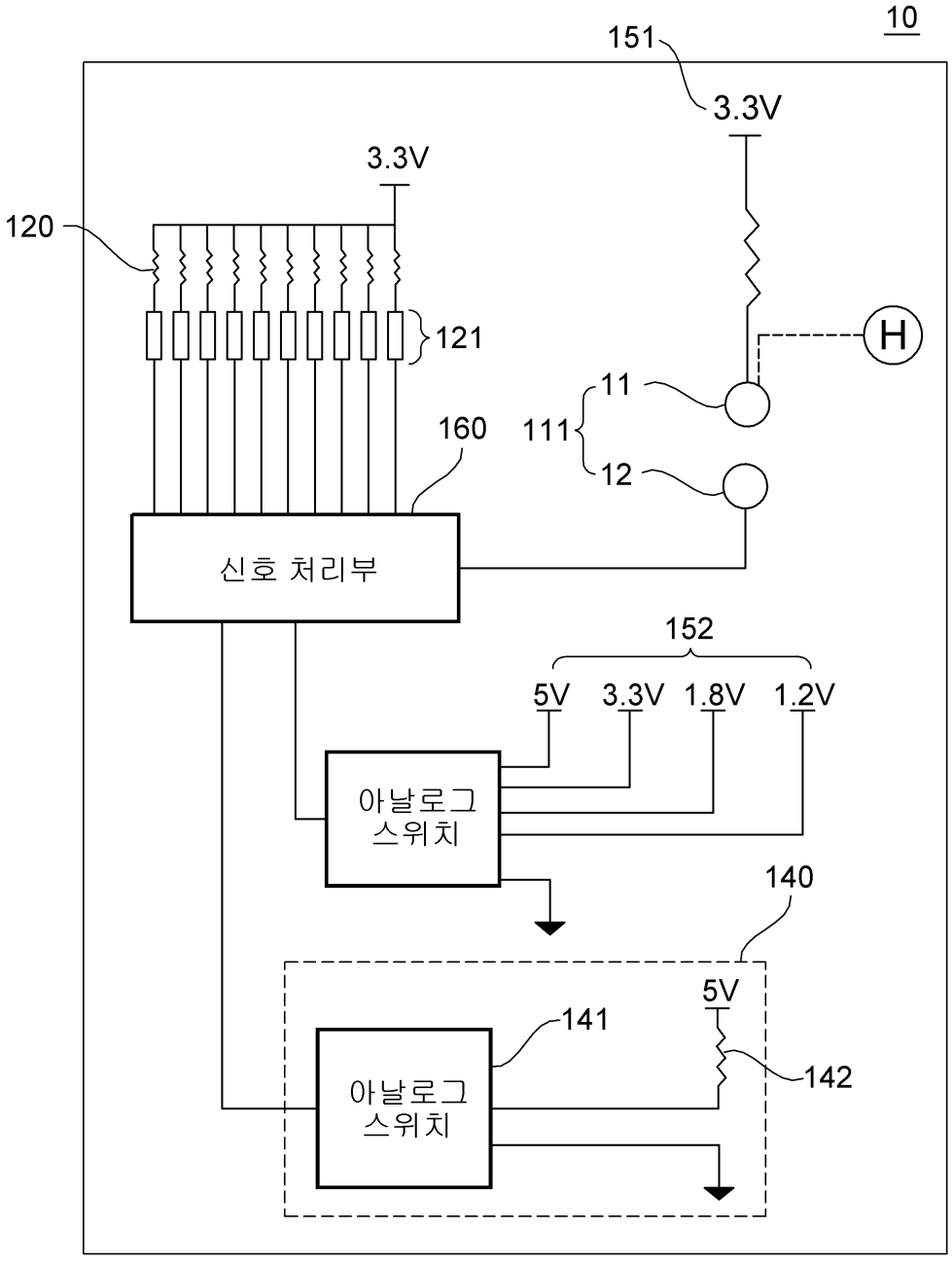
도면4



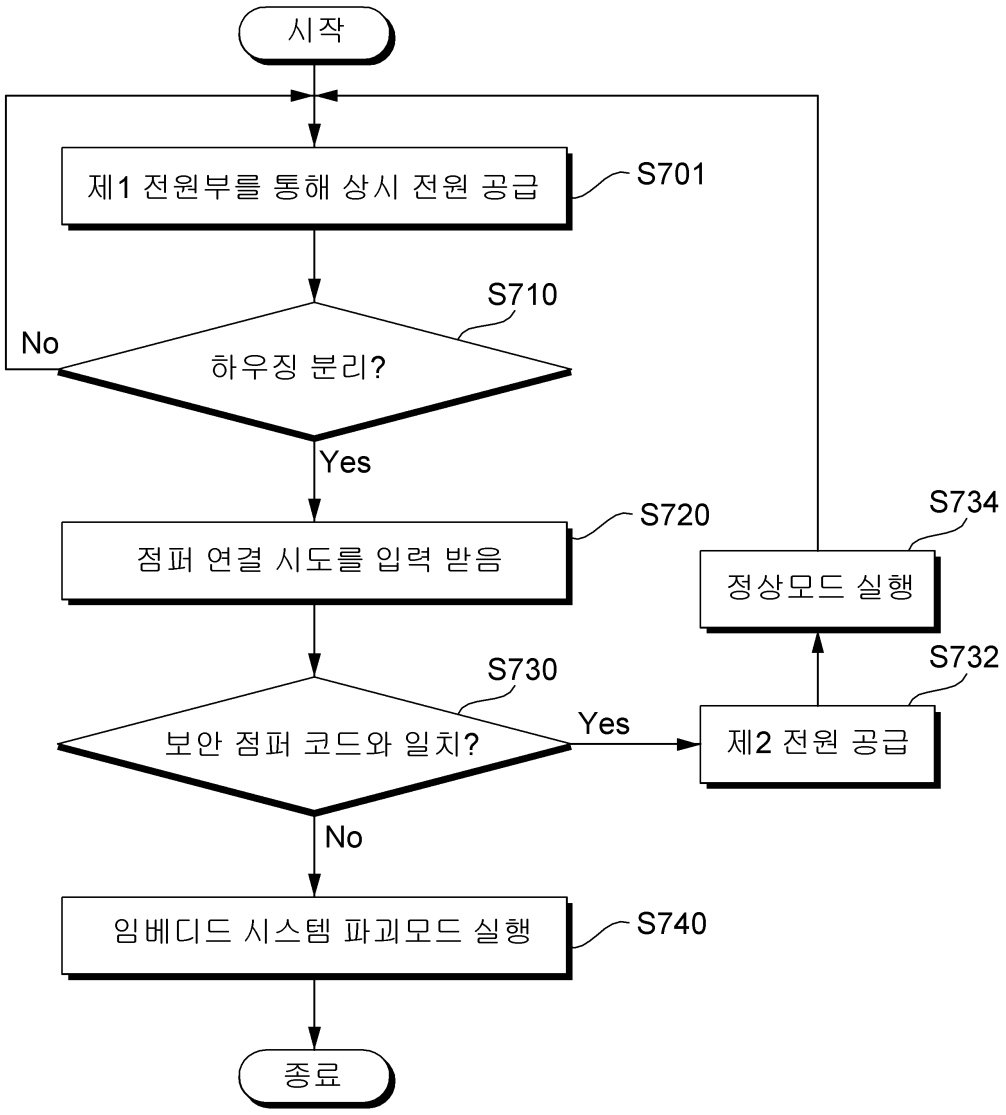
도면5



도면6


10
151
3.3V
3.3V
120
121
H
11
111
12
160
신호 처리부
152
5V
3.3V
1.8V
1.2V
아날로그
스위치
140
5V
141
142
아날로그
스위치

도면7


시작
제1 전원부를 통해 상시 전원 공급
S701
S710
하우징 분리?
No
Yes
S720
점퍼 연결 시도를 입력 받음
S730
보안 점퍼 코드와 일치?
Yes
No
제2 전원 공급
S732
정상모드 실행
S734
임베디드 시스템 파괴모드 실행
S740
종료