

발명의 설명

발명의 명칭: 선박의 사이버보안 유무선 패치 방법 및 시스템

기술분야

- [1] 본 발명은 선박의 사이버보안 유무선 패치방법 및 장치에 관한 것으로 선박용 CBS 패치 업데이트 방법 정립 및 장치의 필요성이 대두됨에 있어 IACS UR E26 요구사항에 따른 패치 업데이트를 수행할 수 있는 선박의 사이버보안 유무선 패치 방법 및 시스템에 관한 것이다.

배경기술

- [2] 국제해사기구(IMO) 및 선급 룰이 강화됨에 따라 선박 내 사이버보안이 요구된다. 이러한 사이버보안에 관한 규정 중 특히 선박 내 컴퓨터 베이스 시스템(Computer Based System)(예: 서버 혹은 컴퓨터 등)에 대한 보안 패치 및 소프트웨어 업데이트가 중요하다. 이를 위한 패치방안으로 PMS (Patch Management System)을 이용하거나, USB 등을 이용한 수동 패치 방식으로 크게 나눌 수 있다. 그러나 선박의 특성상 위성을 이용하여 패치를 수행하는 것이 용이하지 못한 문제점이 있었다.
- [3] 관련선행문헌으로는 대한민국 공개특허 제10-2023-0045769호(2023.04.05.)이 공개되어 있다.

발명의 내용

기술적 과제

- [4] 본 발명의 목적은 무선 패치 업데이트 방안 정립을 통해 향후, 엔지니어 방문 없이 원격으로 패치 업데이트 수행이 가능한 선박의 사이버보안 유무선 패치방법 및 시스템을 제공하는 것을 목적으로 한다.
- [5] 또한, 본 발명의 다른 목적은 스마트 십 및 자율운항 시스템을 위한 선박 사이버보안이 적용된 선박의 사이버보안 패치가 가능하며, 선박의 운항 상황 및 선박 위치에 따라 지속적으로 사이버보안 패치 업데이트를 수행할 수 있는 선박의 사이버보안 유무선 패치방법 및 시스템을 제공하는 것을 목적으로 한다.

과제 해결 수단

- [6] 상기한 목적을 달성하기 위한 본 발명의 일측면에 따른 선박 사이버보안 패치 시스템은, 선박 사이버보안 패치 업데이트 시스템에 있어서, 선박의 복수의 CBS에 대하여 패치 대상의 CBS가 있는 경우 해당 CBS의 패치를 각 CBS의 공급자 서버로부터 패치를 수신하여 통합하는 시스템 통합 서버; 상기 시스템 통합 서버에서 수신된 패치를 인증하고 암호화하며, 암호화된 패치를 배포하는 패치 배포 서버; 및 선박에 구비되며, 상기 패치 배포 서버로부터 수신된 패치를 인증하고 복호화하며, 해시, 타임 스탬프 및 패치 버전을 확인하여 패치 업데이트를 수행하는 패치 업데이트 서버를 포함하며; 상기 패치 업데이트 서버는 선박의 운항 상

황 및 선박 위치에 따라 지속적으로 사이버보안 패치 업데이트를 수행하는 것을 특징으로 한다.

- [7] 또한, 본 발명의 일측면에 따른 선박 사이버보안 패치 시스템에서, 상기 패치 배포 서버는, 선박의 운항 상황 및 선박 위치에 따라 VSAT, LTE, Port LAN 중 어느 하나의 통신 방식으로 연결하여 패치를 배포하는 것을 특징으로 한다.
- [8] 또한, 본 발명의 일측면에 따른 선박 사이버보안 패치 시스템에서, 상기 패치 업데이트 서버는, 백업 업데이트 서버를 더 구비하며; 상기 패치 업데이트 서버를 통해 패치 업데이트 수행 중 통신 연결이 중단된 경우에, 백업 업데이트 서버를 통해 중단 전 패치 상태를 저장하고, 통신 연결이 재개된 후 중단된 시점부터 업데이트를 수행하는 것을 특징으로 한다.
- [9] 또한, 본 발명의 다른 측면에 따른 선박 사이버보안 패치 방법은, 선박 사이버보안 패치 업데이트 방법에 있어서, 선박의 복수의 CBS에 대하여 패치 대상의 CBS가 있는 경우 시스템 통합 서버에서 해당 CBS의 패치를 각 CBS의 공급자 서버로부터 패치를 수신하여 통합하는 패치 수신 단계; 상기 패치 수신 단계를 통해 수신된 패치를 인증하고 암호화하며, 암호화된 패치를 패치 배포 서버에서 패치를 배포하는 패치 배포 단계; 및 상기 패치 배포 단계를 통해 배포된 패치를 선박의 패치 업데이트 서버에서 수신하여, 수신된 패치를 인증하고 복호화하며, 해시, 타임 스탬프 및 패치 버전을 확인하여 패치 업데이트를 수행하는 패치 업데이트 단계를 포함하며; 상기 패치 업데이트 단계는, 선박의 운항 상황 및 선박 위치에 따라 지속적으로 사이버보안 패치 업데이트를 수행하는 것을 특징으로 한다.
- [10] 또한, 본 발명의 다른 측면에 따른 선박 사이버보안 패치 방법에서, 상기 패치 배포 단계는, 선박의 운항 상황 및 선박 위치에 따라 VSAT, LTE, Port LAN 중 어느 하나의 통신 방식으로 연결하여 패치를 배포하는 것을 특징으로 한다.
- [11] 또한, 본 발명의 다른 측면에 따른 선박 사이버보안 패치 방법은, 상기 패치 업데이트 단계에서, 패치 업데이트 서버는 백업 업데이트 서버를 더 구비하며; 상기 패치 업데이트 서버를 통해 패치 업데이트 수행 중 통신 연결이 중단된 경우에, 백업 업데이트 서버를 통해 중단 전 패치 상태를 저장하고, 통신 연결이 재개된 후 중단된 시점부터 업데이트를 수행하는 것을 특징으로 한다.

발명의 효과

- [12] 본 발명에 따르면, 무선 패치 업데이트 방안 정립을 통해 향후, 엔지니어 방문 없이 원격으로 패치 업데이트 수행이 가능한 효과를 갖는다.
- [13] 또한, 본 발명에 따르면, 스마트 ship 및 자율운항 시스템을 위한 선박 사이버보안이 적용된 선박의 사이버보안이 가능하며, 선박의 운항 상황 및 선박 위치에 따라 지속적으로 사이버보안 패치 업데이트를 수행할 수 있는 효과를 갖는다.

도면의 간단한 설명

- [14] 도 1은 본 발명에 따른 선박의 사이버보안 유무선 패치 시스템을 나타내는 도면이다.

- [15] 도 2는 본 발명에 따른 선박의 사이버보안 유무선 패치 방법을 나타내는 순서도이다.

발명의 실시를 위한 형태

- [16] 본 발명의 목적과 기술적 구성 및 그에 따른 작용 및 효과에 관한 자세한 사항은 본 발명의 명세서에 첨부된 도면에 의거한 상세한 설명에 의해 보다 명확하게 이해될 것이다.
- [17] 본 명세서에서 사용되는 용어는 단지 특정한 실시예를 설명하기 위해 사용되는 것으로 본 발명을 한정하려는 의도가 아니다. 예컨대, 본 명세서에서 사용되는 '구성된다' 또는 '포함한다' 등의 용어는 발명에 기재된 여러 구성요소들 또는 여러 단계들을 반드시 모두 포함하는 것으로 해석되지 않아야 하며, 그 중 일부 구성요소들 또는 일부 단계들을 포함하지 않거나 또는 추가적인 구성요소들 또는 단계들을 더 포함할 수 있는 것으로 해석되어야 한다. 또한, 본 명세서에서 사용되는 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한 복수의 표현을 포함한다.
- [18] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 설명함으로써 본 발명을 상세히 설명한다. 이하에서 설명되는 실시예들은 본 발명의 기술사상을 당업자가 용이하게 이해할 수 있도록 제공되는 것으로서, 이에 의해 본 발명이 한정되는 것으로 해석되어서는 안되며, 본 발명의 실시예들은 이 분야의 통상의 기술자에게 다양한 응용을 가질 수 있음은 당연하다.
- [19] 도 1 내지 도 2를 참조하여 본 발명에 따른 선박의 사이버보안 유무선 패치 방법 및 시스템을 살펴보기로 한다.
- [20] 본 발명의 일측면에 따른 선박의 사이버보안 유무선 패치 시스템은, IACS UR E26 요구 사항에 따라, 선박용 CBS 패치 업데이트 방법 및 시스템을 정립한다.
- [21] 본 발명에 따른 선박 사이버보안 패치 업데이트 시스템은 선박의 복수의 CBS(Computer Based System)에 대하여 패치 대상의 CBS가 있는 경우 해당 CBS의 패치를 각 CBS의 공급자 서버(10)로부터 패치를 수신하는 시스템 통합 서버(100)와, 시스템 통합 서버(100)에서 수신된 패치를 인증하고 암호화하며, 암호화된 패치를 선박의 운항 상황 및 선박 위치에 따라 통신 연결 방식을 다르게 하여 패치를 배포하는 패치 배포 서버(200) 및 선박(400)에 구비되며, 패치 배포 서버(200)로부터 수신된 패치를 인증하고 복호화하며, 해시, 타임 스탬프 및 패치 버전을 확인하여 패치 업데이트를 수행하는 패치 업데이트 서버(450)를 포함할 수 있다.
- [22] 패치 업데이트 서버(450)는 선박의 운항 상황 및 선박 위치에 따라 지속적으로 사이버보안 패치 업데이트를 수행하는 것을 특징으로 한다.
- [23] 즉, 선박의 특성상 항해 또는 정박 시 패치 업데이트는 무선통신을 통해 적용할 수 있다.

- [24] 예를 들어 항해 시 VSAT(very small aperture terminal)로 정박 시 5G 또는 LTE(long term evolution)로 업데이트를 수행할 수 있다.
- [25] 따라서, 패치 배포 서버(300)는, 선박의 운항 상황 및 선박 위치에 따라 VSAT, LTE, Port LAN(local area network) 중 어느 하나의 통신부(300) 연결 방식으로 연결하여 패치를 배포하는 것을 특징으로 한다.
- [26] 또한, 키 관리 시스템을 통해 암호화된 패치를 배포함으로써 다른 선박이 패치 데이터를 수신하는 경우에도 보안을 유지하여 패치를 수행할 수 있는 것을 특징으로 한다.
- [27] 보다 구체적으로는, 선박의 복수의 CBS에 대하여 패치 대상의 CBS가 있는 경우 시스템 통합 서버(100)에서 해당 CBS의 패치를 각 CBS의 공급자 서버(11 내지 13)로부터 패치를 수신한다.
- [28] 이어서, 패치 배포 서버(200)는 시스템 통합 서버(100)로부터 수신된 패치를 방화벽(Firewall, 210)을 통해 인증하고 키 관리 시스템(230)을 통해 암호화하며, 암호화된 패치를 선박의 운항 상황 및 선박 위치에 따라 통신 연결 방식을 다르게 하여 패치를 배포할 수 있다.
- [29] 즉 선박의 운항 상황 및 선박 위치에 따라 VSAT, LTE, Port LAN(local area network) 중 어느 하나의 통신부(300)를 통해 패치를 배포할 수 있다.
- [30] 선박(400)에서 수신된 패치를 방화벽(firewall, 410)을 통해 인증하고 키 관리 시스템(430)을 통해 복호화하며, 해시(hash), 타임 스탬프(Timestamp)를 확인하며, 패치 업데이트 서버(450)에서 패치 버전(Patch Version)을 확인하고 각 선박 CBS의 OT(Operational Technology) 시스템에 대하여 패치 업데이트를 수행한다.
- [31] 또한, 패치 업데이트 서버(450)는, 백업 업데이트 서버(460)를 더 구비할 수 있으며, 패치 업데이트 서버(450) 통해 패치 업데이트 수행 중 통신 연결이 중단된 경우에, 백업 업데이트 서버(460)를 통해 중단 전 패치 상태를 저장하고, 통신 연결이 재개된 후 중단된 시점부터 업데이트를 수행할 수 있다.
- [32] 이때 패치 업데이트는, 선박의 운항 상황 및 선박 위치에 따라 지속적으로 사이버보안 패치 업데이트를 수행할 수 있다.
- [33] 또한, 도 2를 참조하여, 본 발명에 따른 선박 사이버보안 패치 방법을 살펴보면, 선박의 복수의 CBS에 대하여 패치 대상의 CBS가 있는 경우 시스템 통합 서버에서 해당 CBS의 패치를 각 CBS의 공급자 서버로부터 패치를 수신하는 패치 수신 단계(S100)와, 패치 수신 단계(S100)를 통해 수신된 패치를 인증하고 암호화하며, 암호화된 패치를 선박의 운항 상황 및 선박 위치에 따라 통신 연결 방식을 다르게 하여 패치 배포 서버에서 패치를 배포하는 패치 배포 단계(S200) 및 패치 배포 단계(S200)를 통해 배포된 패치를 선박의 패치 업데이트 서버에서 수신하여, 수신된 패치를 인증하고 복호화하며, 해시, 타임 스탬프 및 패치 버전을 확인하여 패치 업데이트를 수행하는 패치 업데이트 단계(S300)를 포함할 수 있다.
- [34] 패치 업데이트 단계(S300)는, 선박의 운항 상황 및 선박 위치에 따라 지속적으로 사이버보안 패치 업데이트를 수행하는 것을 특징으로 한다.

- [35] 또한, 선박 사이버보안 패치 방법에서, 패치 배포 단계(S200)는, 선박의 운항 상황 및 선박 위치에 따라 VSAT, LTE, Port LAN 중 어느 하나의 통신 방식으로 연결하여 패치를 배포할 수 있다.
- [36] 또한, 패치 업데이트 단계(S300)에서, 패치 업데이트 서버(450)는 백업 업데이트 서버(460)를 더 구비할 수 있으며, 패치 업데이트 서버(450)를 통해 패치 업데이트 수행 중 통신 연결이 중단된 경우에, 백업 업데이트 서버(460)를 통해 중단 전 패치 상태를 저장하고, 통신 연결이 재개된 후 중단된 시점부터 업데이트를 수행할 수 있다.
- [37] 따라서, 본 발명에 따르면, 무선 패치 업데이트 방안 정립을 통해 향후, 엔지니어 방식 없이 원격으로 패치 업데이트 수행이 가능한 효과를 갖는다.
- [38] 또한, 본 발명에 따르면, 스마트 ship 및 자율운항 시스템을 위한 선박 사이버보안이 적용된 선박의 사이버보안이 가능하며, 선박의 운항 상황 및 선박 위치에 따라 지속적으로 사이버보안 패치 업데이트를 수행할 수 있는 효과를 갖는다.
- [39] 이상 설명된 본 발명에 따른 실시예는 다양한 컴퓨터 구성요소를 통하여 실행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수 있다. 컴퓨터 판독 가능한 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM 및 DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical medium) 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 실행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령어의 예에는 컴파일러에 의하여 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용하여 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위하여 하나 이상의 소프트웨어 모듈로 변경될 수 있으며 그 역도 마찬가지이다.
- [40] 이상에서 설명되는 실시예들은 본 발명의 기술사상을 당업자가 용이하게 이해할 수 있도록 제공되는 것으로서, 이에 의하여 본 발명이 한정되는 것으로 해석되어서는 안되며, 본 발명의 실시예들은 본 발명의 사상 및 범위를 벗어나지 않는 범위 내에서 다양하게 수정 및 변형될 수 있음은 이 기술의 분야에서 통상의 지식을 가진 자에게 자명하다. 따라서 그러한 수정예 또는 변형예들은 본 발명의 특허청구범위에 속한다 하여야 할 것이다.

서열목록

- [41] 10: 공급자 서버
- [42] 100: 시스템 통합 서버

WO 2025/143898**PCT/KR2024/021324**

- [43] 200: 패치 배포 서버
- [44] 300: 통신부
- [45] 400: 선박
- [46] 450: 패치 업데이트 서버

청구범위

- [청구항 1] 선박 사이버보안 패치 업데이트 시스템에 있어서,
선박의 복수의 CBS에 대하여 패치 대상의 CBS가 있는 경우 해당 CBS의 패치를 각 CBS의 공급자 서버로부터 패치를 수신하여 통합하는 시스템 통합 서버;
상기 시스템 통합 서버에서 수신된 패치를 인증하고 암호화하며, 암호화된 패치를 배포하는 패치 배포 서버; 및
선박에 구비되며, 상기 패치 배포 서버로부터 수신된 패치를 인증하고 복호화하며, 해시, 타임 스탬프 및 패치 버전을 확인하여 패치 업데이트를 수행하는 패치 업데이트 서버를 포함하며;
상기 패치 업데이트 서버는 선박의 운항 상황 및 선박 위치에 따라 지속적으로 사이버보안 패치 업데이트를 수행하는 것을 특징으로 하는, 선박 사이버보안 패치 시스템.
- [청구항 2] 청구항 1에 있어서,
상기 패치 배포 서버는,
선박의 운항 상황 및 선박 위치에 따라 VSAT, LTE, Port LAN 중 어느 하나의 통신 방식으로 연결하여 패치를 배포하는 것을 특징으로 하는, 선박 사이버보안 패치 시스템.
- [청구항 3] 청구항 1에 있어서,
상기 패치 업데이트 서버는, 백업 업데이트 서버를 더 구비하며;
상기 패치 업데이트 서버를 통해 패치 업데이트 수행 중 통신 연결이 중단된 경우에, 백업 업데이트 서버를 통해 중단 전 패치 상태를 저장하고, 통신 연결이 재개된 후 중단된 시점부터 업데이트를 수행하는 것을 특징으로 하는, 선박 사이버보안 패치 시스템.
- [청구항 4] 선박 사이버보안 패치 업데이트 방법에 있어서,
선박의 복수의 CBS에 대하여 패치 대상의 CBS가 있는 경우 시스템 통합 서버에서 해당 CBS의 패치를 각 CBS의 공급자 서버로부터 패치를 수신하여 통합하는 패치 수신 단계;
상기 패치 수신 단계를 통해 수신된 패치를 인증하고 암호화하며, 암호화된 패치를 패치 배포 서버에서 패치를 배포하는 패치 배포 단계; 및
상기 패치 배포 단계를 통해 배포된 패치를 선박의 패치 업데이트 서버에서 수신하여, 수신된 패치를 인증하고 복호화하며, 해시, 타임 스탬프 및 패치 버전을 확인하여 패치 업데이트를 수행하는 패치 업데이트 단계를 포함하며;
상기 패치 업데이트 단계는, 선박의 운항 상황 및 선박 위치에 따라 지속적으로 사이버보안 패치 업데이트를 수행하는 것을 특징으로 하는, 선박 사이버보안 패치 방법.

- [청구항 5] 청구항 4에 있어서,
상기 패치 배포 단계는,
선박의 운항 상황 및 선박 위치에 따라 VSAT, LTE, Port LAN 중 어느 하나의 통신 방식으로 연결하여 패치를 배포하는 것을 특징으로 하는, 선박 사이버보안 패치 방법.
- [청구항 6] 청구항 4에 있어서,
상기 패치 업데이트 단계에서, 패치 업데이트 서버는 백업 업데이트 서버를 더 구비하며;
상기 패치 업데이트 서버를 통해 패치 업데이트 수행 중 통신 연결이 중단된 경우에, 백업 업데이트 서버를 통해 중단 전 패치 상태를 저장하고, 통신 연결이 재개된 후 중단된 시점부터 업데이트를 수행하는 것을 특징으로 하는, 선박 사이버보안 패치 방법.