

발명의 설명

발명의 명칭: 선박 사이버 공격 조기 경보 시스템 및 방법

기술분야

- [1] 본 발명은 선박 제어시스템을 환경을 고려하여 AMS(Alarm. Monitoring & Control System) 체계와 연동을 통해 이상행위를 탐지하여 선박 사이버 공격에 대한 조기 경보를 할 수 있는 선박 사이버 공격 조기 경보 시스템 및 방법에 관한 것이다.

배경기술

- [2] 일반적으로, 화재, 침수, 기계 오류 등과 같은 선박의 위험 상황이 발생하는 경우, 선박의 경보 시스템으로써 알람 램프, 스피커 등이 사용되고 있다.
- [3] 선박은 AMS(Alarm. Monitoring & Control System)을 통해서 필드 스테이션에 대한 입출력 값을 수집하여 감시 모니터링 체계를 구축하고 있다.
- [4] 또한, 종래의 AMS 시스템에서는 사이버 공격에 대한 탐지/모니터링 기능이 없었다.
- [5] 따라서, 현존하는 제어시스템(OT)의 사이버보안 장비는 선박 내 모든 OT체계에 위협 탐지를 위한 시스템 구현이 어려운 문제점이 있었다.
- [6] 관련선행문헌으로는 대한민국 공개특허공보 제10-2017-0110932호(2017.10.12.)이 공개되어 있다.

발명의 내용

기술적 과제

- [7] 본 발명의 목적은 선박 제어시스템 환경을 고려하여 AMS(Alarm. Monitoring & Control System) 체계와 연동을 통한 이상행위를 탐지하고 경보를 수행할 수 있는, 선박 사이버 공격 조기 경보 시스템 및 방법을 제공하는 것을 목적으로 한다.
- [8] 본 발명의 다른 목적은 육상에 구현된 선원 훈련 환경에서 선박 내 시스템의 이상행위 조건을 발생시키고 이에 대응하는 선원들의 행동, 입력 데이터를 학습하여 정상적인 대응조치와 비정상적인 대응조치를 분류하고 실제 해상에서 사이버 사고 발생 시 선원들의 행동, 입력 학습 데이터를 기반으로 비정상적인 대응조치 입력, 행동이 발생하는 경우 조기 경보할 수 있는, 선박 사이버 공격 조기 경보 시스템 및 방법을 제공하는 것을 목적으로 한다.

과제 해결 수단

- [9] 상기한 목적을 달성하기 위한 본 발명의 일측면에 따른 선박 사이버 공격 조기 경보 방법은, 선박의 사이버 이상행위에 대한 선원들의 조치 행동 및 입력 데이터를 학습부를 통해 학습하는 학습단계; 선박 기제자에 이상행위가 발생했는지 여부를 AMS(Alarm. Monitoring & Control System)와 연동된 탐지부를 통해 탐지하는 탐지 단계; 상기 탐지 단계를 통해 탐지된 이상행위에 대한 조치로 수행하는 선원들의 행동 및 입력 데이터를 저장부에 저장하는 저장 단계; 상기 저장부

에 저장된 데이터를 기반으로 조치내역을 시뮬레이션부를 통해 시뮬레이션하는 시뮬레이션 단계; 상기 시뮬레이션 단계를 통한 시뮬레이션 결과 이상행위에 대한 선원들의 행동 및 입력 데이터를 학습된 데이터와 비교하여 정상 또는 비정상 조치로 분류부를 통해 판단하여 분류하는 분류 단계; 및 상기 분류 단계를 통해 비정상 조치로 확인되는 경우, AMS(Alarm. Monitoring & Control System)와 선박 내 시각, 청각을 통한 경보체계와 연동하여 경보하는 경보부를 통해 조기 경보를 발생시키는 경보 단계를 포함할 수 있다.

- [10] 또한, 본 발명의 일측면에 따른 선박 사이버 공격 조기 경보 방법에서, 상기 탐지 단계는, AMS(Alarm. Monitoring & Control System) 이상신호 발생기, AIS(Automatic Identification System) 이상신호 발생기, M/E(Main Engine) 이상신호 발생기, 센서 이상신호 발생기, 선박 전자해도시스템 및 로딩 컴퓨터를 포함하는 선박 내 주요 기자재 중 어느 하나에서 이상행위가 발생했는지 여부를 탐지할 수 있다.
- [11] 또한, 본 발명의 일측면에 따른 선박 사이버 공격 조기 경보 방법에서, 상기 탐지 단계는, 다양한 실제 이상행위와 조치내역을 비교하고, 초기 대응 조치에 대한 시뮬레이션을 통해 결과값을 확인하여, 대응 조치의 초기 단계에서 이상행위를 탐지하여 경보를 조기에 발생할 수 있는 것을 특징으로 한다.
- [12] 또한, 본 발명의 일측면에 따른 선박 사이버 공격 조기 경보 방법에서, 상기 분류 단계는, 이상신호 발생에 따른 조치에 대한 기자재 입력 값, 시간, 장소, 경로 및 통신 기록 등을 확인하여 선원들의 행동 및 입력 데이터를 비교하여 정상 또는 비정상 조치로 분류하는 것을 특징으로 한다.
- [13] 또한, 본 발명의 다른 측면에 따른 선박 사이버 공격 조기 경보 시스템은, 선박의 사이버 이상행위에 대한 선원들의 행동 및 입력 데이터를 학습하는 학습부; 선박 기재자에 이상행위가 발생했는지 여부를 AMS(Alarm. Monitoring & Control System)와 연동하여 탐지하는 탐지부; 상기 탐지부를 통해 탐지된 이상행위에 대한 조치로 수행하는 선원들의 행동 및 입력 데이터를 저장하는 저장부; 상기 저장부에 저장된 데이터를 기반으로 조치내역을 시뮬레이션하는 시뮬레이션부; 상기 시뮬레이션부를 통한 시뮬레이션 결과 이상행위에 대한 선원들의 행동 및 입력 데이터를 학습부를 통해 학습된 데이터와 비교하여 정상 또는 비정상 조치로 분류하는 분류부; 및 상기 분류부를 통해 비정상 조치로 확인되는 경우, AMS(Alarm. Monitoring & Control System)와 선박 내 시각, 청각을 통한 경보체계와 연동하여 조기 경보를 발생시키는 경보부를 포함하는 것을 특징으로 한다.
- [14] 또한, 본 발명의 다른 측면에 따른 선박 사이버 공격 조기 경보 시스템에서, 상기 탐지부는, AMS(Alarm. Monitoring & Control System) 이상신호 발생기, AIS(Automatic Identification System) 이상신호 발생기, M/E(Main Engine) 이상신호 발생기, 센서 이상신호 발생기, 선박 전자해도시스템 및 로딩 컴퓨터를 포함하는 선박 내 주요 기자재 중 어느 하나에서 이상행위가 발생했는지 여부를 탐지하는 것을 특징으로 한다.

- [15] 또한, 본 발명의 다른 측면에 따른 선박 사이버 공격 조기 경보 시스템에서, 상기 탐지부는, 다양한 실제 이상행위와 조치내역을 비교하고, 초기 대응 조치에 대한 시뮬레이션을 통해 결과값을 확인하여, 대응 조치의 초기 단계에서 이상행위를 탐지하여 경보를 조기에 발생할 수 있는 것을 특징으로 한다.
- [16] 또한, 본 발명의 다른 측면에 따른 선박 사이버 공격 조기 경보 시스템은, 상기 분류부는, 이상신호 발생에 따른 조치에 대한 기차제 입력 값, 시간, 장소, 경로 및 통신 기록 등을 확인하여 선원들의 행동 및 입력 데이터를 비교하여 정상 또는 비정상 조치로 분류하는 것을 특징으로 한다.

발명의 효과

- [17] 본 발명에 따르면 선박 제어시스템 환경을 고려하여 AMS(Alarm. Monitoring & Control System) 체계와 연동을 통한 이상행위를 탐지하고 경보를 수행할 수 있는 효과를 갖는다.
- [18] 또한, 본 발명에 따르면, 육상에 구현된 선원 훈련 환경에서 선박 내 시스템의 이상행위 조건을 발생시키고 이에 대응하는 선원들의 행동, 입력 데이터를 학습하여 정상적인 대응조치와 비정상적인 대응조치를 분류하고 실제 해상에서 사이버 사고 발생 시 선원들의 행동, 입력 학습 데이터를 기반으로 비정상적인 대응조치 입력, 행동이 발생하는 경우 조기 경보할 수 있는 효과를 갖는다.
- [19] 또한, 본 발명에 따르면, 선박 내 IT/OT 체계에 대한 보안 적용 한계사항을 극복하여 새로운 선박 IT/OT 보안 탐지를 수행할 수 있는 효과를 갖는다.

도면의 간단한 설명

- [20] 도 1은 종래의 AMS(Alarm. Monitoring & Control System)을 나타내는 도면이다.
- [21] 도 2는 본 발명에 따른 선박 사이버 공격 조기 경보 시스템의 구성을 나타내는 도면이다.
- [22] 도 3은 본 발명에 따른 선박 사이버 공격 조기 경보 방법에서 학습 단계를 나타내는 도면이다.
- [23] 도 4는 본 발명에 따른 선박 사이버 공격 조기 경보 방법의 순서를 나타내는 도면이다.
- [24] 도 5 및 도 6은 본 발명에 따른 선박 사이버 공격 조기 경보 방법에서 탐지부를 고도화하는 학습 단계를 나타내는 도면이다.

발명의 실시를 위한 형태

- [25] 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.
- [26] 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.

- [27] 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.
- [28] 선박은 AMS(Alarm. Monitoring & Control System)을 통해서 필드 스테이션에 대한 입출력 값을 수집하여 감시 모니터링 체계를 구축하고 있다.
- [29] 도 2 내지 도 6을 참조하면, 본 발명은 선박 제어시스템(OT) 환경을 고려하여 AMS(Alarm. Monitoring & Control System) 체계와 연동을 통한 이상행위 탐지가 가능한 선박 사이버 공격 조기 경보 시스템 및 방법에 관한 것이다.
- [30] 보다 구체적으로는 또한, 본 발명에 따른 선박 사이버 공격 조기 경보 시스템(100)은, 도 2에 도시된 바와 같이, 학습부(110), 탐지부(120), 저장부(130), 시뮬레이션부(140), 분류부(150) 및 경보부(160)를 포함할 수 있다.
- [31] 육상에 구현된 선원 훈련 환경 등 선박 외부에서 사이버 이상행위 생성(50)하여, 선박에 전송하면 선박 사이버 공격 조기 경보 시스템(100)의 학습부(110)에서 선박의 사이버 이상행위에 대하여 대응하는 선원들의 행동 및 입력 데이터를 학습한다.
- [32] 또한, 탐지부(120)는 선박 기제자에 이상행위가 발생했는지 여부를 AMS(Alarm. Monitoring & Control System)와 연동하여 탐지할 수 있다.
- [33] 즉, AMS(Alarm. Monitoring & Control System) 이상신호 발생기, AIS(Automatic Identification System) 이상신호 발생기, M/E(Main Engine) 이상신호 발생기, 센서 이상신호 발생기, 선박 전자해도시스템 및 로딩 컴퓨터를 포함하는 선박 내 주요 기자재 중 어느 하나에서 이상행위가 발생했는지 여부를 탐지부를 통해 탐지할 수 있다.
- [34] 또한, 저장부(130)는 탐지부(120)에서 탐지된 이상행위에 대한 조치로 수행하는 선원들의 행동 및 입력 데이터를 저장할 수 있다.
- [35] 시뮬레이션부(140)는, 저장부(130)에 저장된 데이터를 기반으로 조치내역을 시뮬레이션할 수 있다.
- [36] 분류부(150)는 시뮬레이션부(140)를 통한 시뮬레이션 결과 이상행위에 대한 선원들의 행동 및 입력 데이터를 학습부(110)를 통해 학습된 데이터와 비교하여 정상 또는 비정상 조치로 분류할 수 있다.
- [37] 경보부(160)는 분류부(150)를 통해 비정상 조치로 확인되는 경우, AMS(Alarm. Monitoring & Control System) 등 선박내 시각, 청각을 통한 경보체계와 연동하여 경보를 발생할 수 있다.

- [38] 이때, 탐지부(120)는, 다양한 실제 이상행위와 조치내역을 비교하고, 초기 대응 조치에 대한 시뮬레이션을 통해 결과값을 확인하여, 대응 조치의 초기 단계에서 이상행위를 탐지하여 경보를 조기에 발생할 수 있는 것을 특징으로 한다.
- [39] 또한, 본 발명에 따른 선박 사이버 공격 조기 경보 시스템에서 분류부(150)는, 이상신호 발생에 따른 조치에 대한 기자제 입력 값, 시간, 장소, 경로 및 통신 기록 등을 확인하여 선원들의 행동 및 입력 데이터를 비교하여 정상 또는 비정상 조치로 분류할 수 있다.
- [40] 또한, 본 발명에 따른 선박 사이버 공격 조기 경보 방법은, 도 3 내지 6에 도시된 바와 같이, 학습 단계(S10), 탐지 단계(S110), 저장 단계(S120), 시뮬레이션 단계(S130), 분류 단계(S140) 및 경보 단계(S150)를 포함할 수 있다.
- [41] 학습단계(S10)는 선박의 사이버 이상행위에 대한 선원들의 조치 행동 및 입력 데이터를 학습부를 통해 학습할 수 있다.
- [42] 보다 구체적으로 학습 단계(S10)는 선박 사이버 이상행위 조건을 생성하여 육상 또는 선박 외부에서 생성하여 선박으로 전송(S11)할 수 있다.
- [43] 선박 사이버 이상행위에 대하여 선박 기자제에 이상행위 발생여부를 AMS(Alarm. Monitoring & Control System)와 연동하여 탐지(S12)하고, 승선자 또는 육상 근무자의 조치(S13)하고, 조치된 행동 및 입력 데이터를 저장(S14)하며, 조치 데이터를 시뮬레이션을 수행(S15)하여, 선박 기자제에 대한 영향과 조치내역을 분석(S16)한다.
- [44] 따라서, 선박 사이버 이상행위에 대하여 조치가 정상적으로 진행되었는지 또는 비정상적으로 진행되었는지 선박 기자제에 대한 영향에 따라 확인할 수 있다.
- [45] 탐지 단계(S110)는 선박 기재자에 이상행위가 발생했는지 여부를 AMS(Alarm. Monitoring & Control System)와 연동된 탐지부를 통해 탐지할 수 있다.
- [46] 또한, 탐지 단계(S110)는 학습 단계를 통해 학습된 데이터를 다양한 실제 이상행위와 조치내역을 비교하고 업데이트(S70)하여, 초기 대응 조치에 대한 시뮬레이션(S80)을 통해 결과값을 확인하여, 대응 조치의 초기 단계에서 이상행위를 탐지하여 경보를 조기에 발생(S90)할 수 있다.
- [47] 저장 단계(S120)는 탐지 단계(S110)를 통해 탐지된 이상행위에 대한 조치로 수행하는 선원들의 행동 및 입력 데이터를 저장부에 저장할 수 있다.
- [48] 시뮬레이션 단계(S130) 저장부에 저장된 데이터를 기반으로 조치내역을 시뮬레이션부를 통해 시뮬레이션할 수 있다.
- [49] 분류 단계(S140)는 시뮬레이션 단계(S130)를 통한 시뮬레이션 결과 이상행위에 대한 선원들의 행동 및 입력 데이터를 학습된 데이터와 비교하여 정상 또는 비정상 조치로 분류부를 통해 판단하여 분류할 수 있다.
- [50] 경보 단계(S150)는 분류 단계(S140)를 통해 비정상 조치로 확인되는 경우, 경보부를 통해 조기 경보를 발생할 수 있다.
- [51] 또한, 탐지 단계(S110)는, AMS(Alarm. Monitoring & Control System) 이상신호 발생기, AIS(Automatic Identification System) 이상신호 발생기, M/E(Main Engine)

이상신호 발생기, 센서 이상신호 발생기 중 어느 하나에서 이상행위가 발생했는지 여부를 탐지할 수 있으며, 다양한 실제 이상행위와 조치내역을 비교하고, 초기 대응 조치에 대한 시뮬레이션을 통해 결과값을 확인하여, 대응 조치의 초기 단계에서 이상행위를 탐지하여 경보를 조기에 발생할 수 있는 것을 특징으로 한다.

- [52] 또한, 분류 단계(S140)는, 이상신호 발생에 따른 조치에 대한 기자재 입력 값, 시간, 장소, 경로 및 통신 기록 등을 확인하여 선원들의 행동 및 입력 데이터를 비교하여 정상 또는 비정상 조치로 분류할 수 있다.
- [53] 이것에 의해 실제 해상에서 사이버 사고 발생시 선원들의 행동, 입력 학습 데이터를 기반으로 비정상적인 대응조치 입력, 행동이 발생하는 경우 조기 경보할 수 있다.
- [54] 따라서 본 발명에 따르면, 선박 제어시스템 환경을 고려하여 AMS(Alarm. Monitoring & Control System) 체계와 연동을 통한 이상행위를 탐지하고 경보를 수행할 수 있는 효과를 갖는다.
- [55] 또한, 본 발명에 따르면, 육상에 구현된 선원 훈련 환경에서 선박 내 시스템의 이상행위 조건을 발생시키고 이에 대응하는 선원들의 행동, 입력 데이터를 학습하여 정상적인 대응조치와 비정상적인 대응조치를 분류하고 실제 해상에서 사이버 사고 발생 시 선원들의 행동, 입력 학습 데이터를 기반으로 비정상적인 대응조치 입력, 행동이 발생하는 경우 조기 경보할 수 있는 효과를 갖는다.
- [56] 또한, 본 발명에 따르면, 선박 내 IT(Information Technology)/OT(Operational Technology) 체계에 대한 보안 적용 한계사항을 극복하여 새로운 선박 IT/OT 보안 탐지를 수행할 수 있는 효과를 갖는다.
- [57] 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.

- [58] 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

- [59] 50: 선박 외부에서 사이버 이상행위 생성
[60] 100: 선박 사이버 공격 조기 경고 시스템
[61] 110: 학습부
[62] 120: 탐지부
[63] 130: 저장부
[64] 140: 시뮬레이션부
[65] 150: 분류부
[66] 160: 경보부

청구범위

- [청구항 1] 선박의 사이버 이상행위에 대한 선원들의 조치 행동 및 입력 데이터를 학습부를 통해 학습하는 학습단계;
선박 기재자에 이상행위가 발생했는지 여부를 AMS(Alarm, Monitoring & Control System)와 연동된 탐지부를 통해 탐지하는 탐지 단계;
상기 탐지 단계를 통해 탐지된 이상행위에 대한 조치로 수행하는 선원들의 행동 및 입력 데이터를 저장부에 저장하는 저장 단계;
상기 저장부에 저장된 데이터를 기반으로 조치내역을 시뮬레이션부를 통해 시뮬레이션하는 시뮬레이션 단계;
상기 시뮬레이션 단계를 통한 시뮬레이션 결과 이상행위에 대한 선원들의 행동 및 입력 데이터를 학습된 데이터와 비교하여 정상 또는 비정상 조치로 분류부를 통해 판단하여 분류하는 분류 단계; 및
상기 분류 단계를 통해 비정상 조치로 확인되는 경우, AMS(Alarm, Monitoring & Control System)와 선박내 시각, 청각을 통한 경보체계와 연동하여 경보하는 경보부를 통해 조기 경보를 발생하는 경보 단계를 포함하는 것을 특징으로 하는, 선박 사이버 공격 조기 경보 방법.
- [청구항 2] 청구항 1에 있어서,
상기 탐지 단계는,
AMS(Alarm, Monitoring & Control System) 이상신호 발생기, AIS(Automatic Identification System) 이상신호 발생기, M/E(Main Engine) 이상신호 발생기, 센서 이상신호 발생기, 선박 전자해도시스템 및 로딩 컴퓨터를 포함하는 선박 내 주요 기자재 중 어느 하나에서 이상행위가 발생했는지 여부를 탐지하는 것을 특징으로 하는, 선박 사이버 공격 조기 경보 방법.
- [청구항 3] 청구항 1에 있어서,
상기 탐지 단계는,
다양한 실제 이상행위와 조치내역을 비교하고, 초기 대응 조치에 대한 시뮬레이션을 통해 결과값을 확인하여, 대응 조치의 초기 단계에서 이상행위를 탐지하여 경보를 조기에 발생할 수 있는 것을 특징으로 하는, 선박 사이버 공격 조기 경보 방법.
- [청구항 4] 청구항 1에 있어서,
상기 분류 단계는,
이상신호 발생에 따른 조치에 대한 기자재 입력 값, 시간, 장소, 경로 및 통신 기록 등을 확인하여 선원들의 행동 및 입력 데이터를 비교하여 정상 또는 비정상 조치로 분류하는 것을 특징으로 하는, 선박 사이버 공격 조기 경보 방법.

- [청구항 5] 선박의 사이버 이상행위에 대한 선원들의 행동 및 입력 데이터를 학습하는 학습부;
 선박 기재자에 이상행위가 발생했는지 여부를 AMS(Alarm, Monitoring & Control System)와 연동하여 탐지하는 탐지부;
 상기 탐지부를 통해 탐지된 이상행위에 대한 조치로 수행하는 선원들의 행동 및 입력 데이터를 저장하는 저장부;
 상기 저장부에 저장된 데이터를 기반으로 조치내역을 시뮬레이션하는 시뮬레이션부;
 상기 시뮬레이션부를 통한 시뮬레이션 결과 이상행위에 대한 선원들의 행동 및 입력 데이터를 학습부를 통해 학습된 데이터와 비교하여 정상 또는 비정상 조치로 분류하는 분류부; 및
 상기 분류부를 통해 비정상 조치로 확인되는 경우, AMS(Alarm, Monitoring & Control System)와 선박내 시각, 청각을 통한 경보체계와 연동하여 조기 경보를 발생하는 경보부를 포함하는 것을 특징으로 하는, 선박 사이버 공격 조기 경보 시스템.
- [청구항 6] 청구항 5에 있어서,
 상기 탐지부는,
 AMS(Alarm, Monitoring & Control System) 이상신호 발생기,
 AIS(Automatic Identification System) 이상신호 발생기, M/E(Main Engine) 이상신호 발생기, 센서 이상신호 발생기, 선박 전자해도시스템 및 로딩 컴퓨터를 포함하는 선박 내 주요 기자재 중 어느 하나에서 이상행위가 발생했는지 여부를 탐지하는 것을 특징으로 하는, 선박 사이버 공격 조기 경보 시스템.
- [청구항 7] 청구항 5에 있어서,
 상기 탐지부는,
 다양한 실제 이상행위와 조치내역을 비교하고, 초기 대응 조치에 대한 시뮬레이션을 통해 결과값을 확인하여, 대응 조치의 초기 단계에서 이상행위를 탐지하여 경보를 조기에 발생할 수 있는 것을 특징으로 하는, 선박 사이버 공격 조기 경보 시스템.
- [청구항 8] 청구항 5에 있어서,
 상기 분류부는,
 이상신호 발생에 따른 조치에 대한 기자재 입력 값, 시간, 장소, 경로 및 통신 기록 등을 확인하여 선원들의 행동 및 입력 데이터를 비교하여 정상 또는 비정상 조치로 분류하는 것을 특징으로 하는, 선박 사이버 공격 조기 경보 시스템.