

발명의 설명

발명의 명칭: 선박 사이버보안 상태 측정 방법, 그리고 선박 사이버보안 위험 평가 및 이상징후 탐지 방법

기술분야

- [1] 본 발명은 다양한 경로로 수집되는 위험 데이터는 위험 발생 정도 등 다양한 기준에 따라 인덱싱 되어 점수화 하며, 선박의 선실, 브릿지룸, 엔진룸 등 중요도에 따라 구역을 구분하며, 각 구역의 CBS의 정량화된 위험 스코어링을 제공하는, 선박 사이버보안 상태 측정 방법, 그리고 선박 사이버보안 위험 평가 및 이상징후 탐지 방법에 관한 것이다.

배경기술

- [2] 종래의 사이버 리스크에 대한 평가 또는 정량화에 대한 기술은 네트워크에 연결된 상황에서 정량화 한다. 해당 정량화 방법은 일반적인 네트워크에 연결된 상태에 대한 정량화하는 방법이기 때문에 산업에 따라 일반적인 적용에 제한사항이 존재한다.
- [3] 현재 사이버 위협에 대한 종래의 기술은 네트워크의 각 노드에 대해 가중치를 부여하여 노드간 확률을 계산하여 전체적인 사이버 위협 확률을 계산하는 방식과 엔드 포인트에 에이전트를 설치하여 시스템에서 가져올 수 있는 데이터를 수집하여 정량화 한다.
- [4] 다양한 사이버 리스크에 대한 스코어링 방법은 확률적인 계산이 필요한 페이지안 확률/통계를 사용해 과거의 네트워크 행위와 비교하여 최종적인 위험 발생 가능성을 도출하거나, 각 클라이언트에서 발생 가능한 사이버 위협을 추정하여 합산하는 방식을 가진다.
- [5] 그러나 종래 기술은 엔드 포인트에 위험 스코어링을 위한 에이전트가 배포되어 발생 가능한 위험 데이터를 수집하거나, 네트워크를 모니터링하여 과거 행동 양상과 비교하여 분석을 수행하는 방식이므로, 선박 네트워크를 분석하는 방식은 네트워크의 과도한 트래픽을 발생시킬 수 있으며, 엔드 포인트에 에이전트를 설치하는 방식은 선박 가용성에 위배될 수 있어 사용에 제한이 있다는 문제점이 있었다.
- [6] 또한, 일반적으로 금융분야, 원자력시설, 일반기업, 기반시설 등 육상에서 사이버보안 위험 평가하는 방법들은 육상에서의 사이버보안 위험 평가를 하고 있다. 선박은 해상에서의 사이버보안 위험 평가를 하여야 하고 이를 위해 국제선급협회 및 각 선급에서 사이버보안 위험 평가 방법을 고시하고 있다.
- [7] 도 6에 도시된 바와 같이, ISO 27001과 IACS Rec 171을 비교한 도면으로 ISO 27001 정보보호관리체계(Information Security Management System)에서 정보보호의 통제항목을 표준으로 한다. IACS Rec 171은 선박의 위험 평가를 제시한다.

- [8] 따라서 ISO 27001 정보보호의 통제항목을 바탕으로 각 단계별로 IACS Rec 171을 통해 선박의 위험 평가를 할 수 있다.
- [9] 이와 관련하여, 국제표준기구(ISO) ISO 31000:2018 “Risk management - Guidelines”에서 위험관리 절차는 (1)Communication and consultation, (2)scope, context and criteria, (3)risk assessment, (4)risk treatment, (5)monitoring and review, (6)recoding and reporting으로 진행된다. 여기서 risk assessment는 위험 식별, 위험 분석, 위험 평가의 단계로 설명되어 있다.
- [10] 국제선급협회(IACS, International Association of Classification Societies) Rec 171 “Recommendation on incorporating cyber risk management into Safety Management Systems”에서 선박의 위험 평가 방법은 도 7에 도시된 바와 같이, (1)범위 정의(S10), (2)UR E22 카테고리 분류(S20), (3)위험 목록 식별(S30), (4)위험·공격·기술의 영향도(S40), (5)운영 위험(S50), (6)발생가능성평가(S60), (7)위험 수준 평가(S70), (8)위험 조치에 대한 결정(S80), (9)위험 완화(S90), (10)잔여 위험(S92)의 절차로 되어있다. 영국의 Lloyd's Register, 프랑스 Bureau Veritas, 노르웨이 Det Norske Veritas, 한국 선급 등 각 선급에서 고시하는 선박 사이버보안 위험 평가 방법은 IACS Rec 171를 벗어나지 않는다.
- [11] 보안의 3대 요소는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)이며, 육상에서는 보안의 3대 요소 중 기밀성과 무결성을 우선으로 하고 있다.
- [12] 육상에서 위험 평가를 하기 위한 자산으로는 서버, 네트워크 장비, 보안시스템, DBMS, 응용프로그램, 단말기, 소프트웨어, 저장매체, 제어시스템 등을 분류하고 있다.
- [13] 따라서, IACS 또는 각 선급에서 제시하고 있는 위험 평가 방법에서 위험의 발생가능성을 도출하는 과정 중 엔드유저(End-User) 및 공격자 그룹(Attacker Group)의 등급을 평가하기에는 선박의 건조 과정에서 위험평가를 하거나 선박 운항중에 위험평가를 하는 경우 해양의 특수성으로 인한 위험 평가 기간이 물리적, 시간적으로 부족하고 사람의 주관적인 기준으로 등급 평가가 모호하여 위험평가를 위한 정량적인 평가 수단이 필요하다.
- [14] 또한, 선박은 다수의 CBS가 설치되어 있는 복합적인 체계로 구성된다. 최근에는 ICT 환경의 선박 기자재가 탑재되는 비중이 높아지면서 해킹, 악성코드 공격에 대한 위험이 증가하고 있다.
- [15] 선박은 육상 체계와 다르게 선박 안전운전을 저해하는 요인들에 대해 사이버 위험을 차단하는 방안이 적용하기 쉽지 않다.
- [16] 침입차단시스템 등과 같은 보안장비의 오동작, 오탐, 과탐으로 인해 정상 운항 데이터가 차단되는 경우 충돌, 좌초와 같은 심각한 물리적 피해가 발생할 수 있다.

- [17] ICT 기반으로 급격히 변화하고 있는 선박에서 선박 고유의 환경에 특화된 사이버 공격 탐지 기술이 보편화되지 않은 시점에서 실시간으로 선박 환경과 선박 기자재에 대한 사이버위험을 차단하기 어렵다.
- [18] 따라서, 사전 예방적 관점에서 선박 환경에서 발생할 수 있는 사이버위험을 사전에 예측하고 피해 가능 경로, 피해 범위를 산정하여 예방활동을 취하는 것이 효율적이다.
- [19] 관련 선행문헌으로는 대한민국 공개특허 제10-2020-0029266호(2020.03.18.), 대한민국 등록특허 제10-2406756호(2022.06.10.), 대한민국 공개특허 제10-2020-0141774호(2020.12.21.), 대한민국 등록특허 제10-0604604호(2006.07.24.)가 공개되어 있다.

발명의 내용

기술적 과제

- [20] 본 발명의 목적은 선박의 CBS(Computer Based System)을 다양한 소스로부터 수집되는 위험과 비교하여 위험 척도를 계산하는 방식으로 선박의 네트워크에 설치 또는 접근하지 않는 방식으로 가용성을 유지하고, 다양한 경로로 수집되는 위험 데이터는 위험 발생 정도 등 다양한 기준에 따라 인덱싱 되어 점수화 한다. 선박의 선실, 브릿지룸, 엔진룸 등 중요도에 따라 구역을 구분하며, 각 구역의 CBS의 정량화된 위험 스코어링을 제공할 수 있는 선박 사이버보안 상태 측정을 위한 방법을 제공하는 것을 목적으로 한다.
- [21] 본 발명의 다른 목적은 사이버보안 위험 평가 시 위험의 심각도와 노출정도를 통해 위험 노출 등급을 도출하고 위험 발생가능성을 도출하는 요소로 활용하여 위험 평가의 정량화가 가능하고, 정량화된 선박 사이버 보안 위험 평가 방법을 시스템으로 구축하여 위험 평가에 적용하여 해양의 특수성으로 인한 위험 평가의 문제점 해소에 기여할 수 있는 선박 사이버 보안 위험 평가를 위한 방법을 제공하는 것을 목적으로 한다.
- [22] 본 발명의 또 다른 목적은 선급별 사이버 보안 요구사항에 맞춰 위험 평가를 수행하여 선급 인증 시 사이버 보안에 대한 요건을 갖출 수 있는 선박 사이버 보안 위험 평가를 위한 방법을 제공하는 것을 목적으로 한다.
- [23] 본 발명의 또 다른 목적은 선박 네트워크 토폴로지(Network Topology) 및 CBS(Computer based System) 특성 정보, 실시간 탐지된 위협정보를 기반으로 발생가능한 사이버위험을 예측함으로써 보안사고 예방과, 보안장비의 오탐, 과탐 등 실시간 침입차단으로 인해 발생할수 있는 위험요소를 방지할수 있는 기계학습 기반 선박 사이버보안 이상징후 탐지 방법을 제공하는 것을 목적으로 한다.

과제 해결 수단

- [24] 상기 기술적 과제를 달성하기 위한 본 발명의 일측면에 따른 선박 사이버보안 상태 측정을 위한 방법은, 선박 CBS 데이터를 수집하고 CBS에 대한 사이버위험

및 해양 인텔리전스 데이터를 수집하는 데이터 수집 단계; 선박 구역에 따른 CBS 수집 및 관리 단계; 사이버위협 스코어 기준을 통한 데이터 인덱싱 단계; 선박 구역별 위험 스코어 계산 단계; 및 위험 스코어에 따른 선박 사이버보안 상태를 도출하고 위험도를 완화하는 위험도 완화 단계를 포함할 수 있다.

- [25] 또한, 본 발명의 일측면에 따른 선박 사이버보안 상태 측정을 위한 방법에서, 사이버위협 및 해양 인텔리전스 수집 단계는, IT 사이버 위협 인텔리전스 및 OT사이버 위협 인텔리전스를 사전에 수집하고, 인텔리전스 데이터의 유효성을 검사할 수 있다.
- [26] 또한, 본 발명의 일측면에 따른 선박 사이버보안 상태 측정을 위한 방법에서, 상기 선박 구역에 따른 CBS 수집 및 관리 단계는, 구획별 CBS 관리 단계; 구획별 CBS 구분 단계; 구획별 CBS 리스팅 단계; 및 구획별 위험 평가 단계를 포함할 수 있다.
- [27] 또한, 본 발명의 일측면에 따른 선박 사이버보안 상태 측정을 위한 방법에서, 상기 사이버위협 스코어 기준을 통한 데이터 인덱싱 단계는, 사이버 위협 분류 단계;
- [28] 사이버 위협의 우선순위 지정 단계; 사이버 위협 획일화 단계; 및 우선순위별 스코어링 단계를 포함할 수 있다.
- [29] 또한, 본 발명의 일측면에 따른 선박 사이버보안 상태 측정을 위한 방법에서, 상기 선박 구역별 위험 스코어 계산 단계는, 선박의 선실, 브릿지룸, 엔진룸 등 선박 구역별 중요도에 따른 구역을 구분하여 가중치를 부여하는 가중치 부여 단계를 더 포함할 수 있다.
- [30] 또한, 상기 기술적 과제를 달성하기 위한 본 발명의 다른 측면에 따른 선박 사이버 보안 위험 평가를 위한 방법은 위험평가 대상 선박이 인증 받을 선급의 사이버보안 요구사항을 위험평가 수행 시 조회하고 선박의 자산을 식별하여 사이버 보안 범위를 선정하는 범위 선정 단계; 상기 범위 선정 단계를 통해 선정된 보안 범위 내에 선박의 자산을 CBS(Computer Based System)에 따라 분류하고, 분류된 자산에 연결되는 복수의 네트워크에 대한 송수신 데이터를 데이터 수집부에서 수집하는 데이터 수집 단계; 및 상기 데이터 수집 단계에서 수집된 데이터에서 위협 목록을 식별하고 분석하여 복수의 네트워크 각각의 사이버보안 위협에 대한 사이버보안 위험 평가를 수행하는 위험 평가 단계를 포함할 수 있다.
- [31] 또한, 본 발명의 다른 측면에 따른 선박 사이버 보안 위험 평가를 위한 방법에서, 상기 범위 선정 단계는, 선박을 인증하는 각 선급들이 요구하는 사이버보안 규칙(rule)이 저장된 데이터베이스(DB)로부터 조회하고, 위험 평가 시 선박이 인증 받을 선급의 사이버보안 요구사항에 맞춰 선박의 자산을 식별하여 사이버보안 위험 평가 범위를 선정할 수 있다.

- [32] 또한, 본 발명의 다른 측면에 따른 선박 사이버 보안 위험 평가를 위한 방법에서, 상기 데이터 수집 단계는, 선박의 자산을 식별하고, CBS 분류에 따른 자산 중요도를 고려하여 데이터 수집 시기를 설정할 수 있다.
- [33] 또한, 본 발명의 다른 측면에 따른 선박 사이버 보안 위험 평가를 위한 방법에서, 상기 위험 평가 단계는, 영향도 평가 단계, 공격 표면 평가 단계, 위험 노출 평가 단계 및 발생 가능성 평가 단계를 포함할 수 있다.
- [34] 또한, 본 발명의 다른 측면에 따른 선박 사이버 보안 위험 평가를 위한 방법에서, 상기 위험 노출 평가 단계는, 휴먼 팩터(Human Factor)를 산정하는 엔드유저(End-User)와 공격자 그룹(Attacker Group)을 대체하여, 심각도와 노출정도를 평가하여 산정된 노출 등급을 통해 위험 노출을 평가를 하는 것을 특징으로 한다.
- [35] 또한, 본 발명의 다른 측면에 따른 선박 사이버 보안 위험 평가를 위한 방법에서, 상기 위험 노출(Threat Exposure)은 심각도(Severity)와 노출정도(Degree of Exposure)의 두 요소에 각 등급에 따라 산정되는 것으로, 먼저 심각도(Severity)는 Low, Medium, High, Critical 1~4등급으로 분류되며; 노출정도(Degree of Exposure)는 None, CVE, MCTI, 다크웹, Naval 1~5등급으로 분류되며; 상기 심각도(Severity)와 노출정도(Degree of Exposure)의 등급이 판별되면 각 요소의 등급의 수치를 더하여 위험 노출(Threat Exposure) 등급을 1~5등급으로 분류하여 산정할 수 있다.
- [36] 또한, 상기 기술적 과제를 달성하기 위한 본 발명의 일측면에 따른 기계학습 기반 선박 사이버보안 이상징후 탐지 방법은, CBS 정의부를 통해 실시간 CBS 공격표면의 정보를 스캐닝 하는 CBS 공격표면 정보 스캐닝 단계; 상기 CBS 공격표면 정보 스캐닝 단계를 통해 스캐닝된 CBS 공격표면 정보에 대하여 CBS 정의부는 CBS 공격표면을 정량화하는 CBS 공격표면 정량화 단계; 상기 CBS 공격표면 정량화 단계를 통해 정량화된 CBS에 대하여 기계학습을 통해 위험분석부에서 사이버위험 지수를 산출하는 사이버위험 지수 산출 단계; 및 상기 사이버위험 지수 산출 단계를 통해 산출된 사이버위험지수를 분석하여 위험분석부에서 CBS에 해킹이 발생할 위험도가 높은 경로를 생성하는 이상징후 그래프 생성 단계를 포함할 수 있다.
- [37] 또한, 본 발명의 일측면에 따른 기계학습 기반 선박 사이버보안 이상징후 탐지 방법에서, 상기 사이버위험 지수 산출 단계는, 선박 내부에 탑재된 CBS 보안 취약성 정보를 CVE와 선박의 공격표면 정보, 선박 내부 네트워크에 설치된 침입탐지시스템으로부터 식별되는 정보를 통해 위험도 테이블을 생성하는 것을 특징으로 한다.
- [38] 또한, 본 발명의 일측면에 따른 기계학습 기반 선박 사이버보안 이상징후 탐지 방법은, 상기 사이버위험 지수 산출 단계에서, 상기 식별되는 정보는, 소스(source) IP와 데스티네이션(destinaion) IP 및 탐지 룰(rule) 중요도 정보를

포함하여, 위험도 테이블을 생성하며; CBS 보안통제가 설정된 경우 보안통제 테이블을 포함하여 사이버위험 지수를 산출할 수 있다.

[39] 또한, 본 발명의 일측면에 따른 기계학습 기반 선박 사이버보안 이상징후 탐지 방법은, 상기 이상징후 그래프 생성단계에서, 네트워크 토폴로지 상에 위험도 테이블 및 보안통제 테이블을 대입하여 경로상에 CBS에서 해킹이 발생할 위험도가 높은 경로를 맵핑할 수 있다.

[40] 또한, 본 발명의 일측면에 따른 기계학습 기반 선박 사이버보안 이상징후 탐지 방법은, 상기 이상징후 그래프 생성 단계에서, 네트워크 토폴로지는, 트리 토폴로지를 통해 이상징후 그래프를 생성할 수 있다.

발명의 효과

[41] 본 발명에 따르면, 선박의 CBS(Computer Based System)을 다양한 소스로부터 수집되는 위험과 비교하여 위험 척도를 계산하는 방식으로 선박의 네트워크에 설치 또는 접근하지 않는 방식으로 가용성을 유지하고, 다양한 경로로 수집되는 위험 데이터는 위험 발생 정도 등 다양한 기준에 따라 인덱싱 되어 점수화 한다. 선박의 선실, 브릿지룸, 엔진룸 등 중요도에 따라 구역을 구분하며, 각 구역의 CBS의 정량화된 위험 스코어링을 제공할 수 있는 효과를 갖는다.

[42] 또한, 본 발명에 따르면 사이버보안 위험 평가 시 위협의 심각도와 노출정도를 통해 위험 노출 등급을 도출하고 위험 발생가능성을 도출하는 요소로 활용하여 위험 평가의 정량화가 가능한 효과를 갖는다.

[43] 또한, 본 발명에 따르면 정량화된 선박 사이버 보안 위험 평가 방법을 시스템으로 구축하여 위험 평가에 적용하여 해양의 특수성으로 인한 위험 평가의 문제점 해소에 기여할 수 있는 효과를 가진다.

[44] 또한, 본 발명에 따르면 선급별 사이버 보안 요구사항에 맞춰 위험 평가를 수행하여 선급 인증 시 사이버 보안에 대한 요건을 갖출 수 있는 효과를 가진다.

[45] 또한, 본 발명에 따르면, 선박 네트워크 토폴로지(Network Topology) 및 CBS(Computer based System) 특성 정보, 실시간 탐지된 위협정보를 기반으로 발생가능한 사이버위험을 예측함으로써 보안사고 예방과, 보안장비의 오탐, 과탐 등 실시간 침입차단으로 인해 발생할수 있는 위험요소를 방지할수 있는 효과를 갖는다.

도면의 간단한 설명

[46] 도 1은 본 발명에 따른 선박 사이버보안 상태 측정을 위한 방법에서 선박 구역별 위험 스코어 계산 및 구역별 중요도에 따른 가중치 부여 방법을 나타내는 도면이다.

[47] 도 2는 본 발명에 따른 선박 사이버보안 상태 측정을 위한 방법을 개략적으로 나타내는 블록도이다.

[48] 도 3은 본 발명에 따른 선박 사이버보안 상태 측정을 위한 방법에서, 선박 구역에 따른 CBS 수집 및 관리 단계를 나타내는 도면이다.

- [49] 도 4는 본 발명에 따른 선박 사이버보안 상태 측정을 위한 방법에서, 사이버위협 스코어 기준을 통한 데이터 인덱싱 단계를 나타내는 도면이다.
- [50] 도 5는 본 발명에 따른 선박 사이버보안 상태 측정을 위한 방법을 나타내는 흐름도이다.
- [51] 도 6은 국제표준기구(ISO)의 정보보호 항목과 국제선급협회(IACS)의 위험 평가 항목을 비교하여 나타내는 도면이다.
- [52] 도 7는 국제선급협회(IACS)에서 위험 평가를 수행하는 절차를 나타내는 블록 구성도이다.
- [53] 도 8은 본 발명의 실시예에 따른 선박 사이버 보안 위험 평가를 수행하는 절차를 나타내는 블록 구성도이다.
- [54] 도 9는 본 발명의 선박 사이버 보안 위험 평가를 수행하기 위한 평가 시스템의 구성을 나타내는 블록 구성도이다.
- [55] 도 10는 본 발명의 실시예에 따른 선박 사이버 보안 위험 평가 방법의 세부 구성을 나타내는 도면이다.
- [56] 도 11은 본 발명에 따른 기계학습 기반 선박 사이버보안 이상징후 탐지 방법의 순서를 나타내는 순서도이다.
- [57] 도 12는 본 발명에 따른 기계학습 기반 선박 사이버보안 이상징후 탐지 방법에서 보안통제 테이블을 포함한 위험도 테이블을 나타내는 도면이다.
- [58] 도 13은 본 발명의 일 실시예에 따른 선박 네트워크 토폴로지 상에 위험 도 및 보안통제 테이블을 대입하여 경로상에 CBS에서 해킹이 발생할 위험도가 높은 경로를 맵핑하여 나타내는 도면이다.

발명의 실시를 위한 형태

- [59] 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.
- [60] 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.
- [61] 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.

- [62] 도 1은 본 발명에 따른 선박 사이버보안 상태 측정을 위한 방법에서 선박 구역별 위험 스코어 계산 및 구역별 중요도에 따른 가중치 부여 방법을 나타내는 도면이고, 도 2는 본 발명에 따른 선박 사이버보안 상태 측정을 위한 방법을 개략적으로 나타내는 블록도이고, 도 3은 본 발명에 따른 선박 사이버보안 상태 측정을 위한 방법에서, 선박 구역에 따른 CBS 수집 및 관리 단계를 나타내는 도면이고, 도 4는 본 발명에 따른 선박 사이버보안 상태 측정을 위한 방법에서, 사이버위험 스코어 기준을 통한 데이터 인덱싱 단계를 나타내는 도면이고, 도 5는 본 발명에 따른 선박 사이버보안 상태 측정을 위한 방법을 나타내는 흐름도이다.
- [63] 도 1 내지 도 5를 참조하면, 본 발명에 따른 선박 사이버보안 상태 측정을 위한 방법은 사이버 위협/해양 인텔리전스를 수집한다.
- [64] 사이버 위협 인텔리전스(CTI: Cyber Threat Intelligence)는 위협 정보를 수집해 상황을 분석하고, 위협에 효과적으로 대응하는 방법을 의미한다.
- [65] 이때, 선박 구역에 따른 CBS(Computer Based System) 데이터를 수집 및 관리하며, 사이버 위협 스코어 기준을 통한 데이터를 인덱싱하고, 선박 구역별 위험 스코어를 계산한다.
- [66] 이때, 선박 구역별 중요도에 따른 가중치를 부여하여 선박 구역별 위험 스코어를 계산할 수 있다.
- [67] 또한, 본 발명의 선박 사이버보안 상태 측정을 위한 방법을 수행하기 위한 선박 사이버보안 상태 측정 시스템은 사이버 위협/해양 인텔리전스 데이터 수집부(10)와, CBS 데이터 관리부(20), 사이버 위협 인덱싱부(30), 선박 구역별 위험 스코어 계산부(40) 및 사이버보안 상태 도출 및 위험도 완화부(50)를 포함할 수 있다.
- [68] 도 1에서와 같이, 사이버 위협/해양 인텔리전스를 수집하고 선박 구역별 중요도(A 내지 D 단계)에 따라 가중치를 부여하여 0점 내지 100점으로 위험 스코어를 계산할 수 있다.
- [69] 또한, 본 발명에 따른 선박 사이버보안 상태 측정을 위한 방법은, 도 2를 참조하면, 선박 전체 CBS 데이터를 수집하고 CBS에 대한 사이버위협 및 해양 인텔리전스 데이터 수집 단계(10)와, 선박 구역에 따른 CBS 수집 및 관리 단계(20)와, 사이버위협 스코어 기준을 통한 데이터 인덱싱 단계(30)와, 선박 구역별 위험 스코어 계산 단계(40); 및 위험 스코어에 따른 선박 사이버보안 상태를 도출하고 위험도를 완화하는 위험도 완화 단계(50)를 포함할 수 있다.
- [70] 또한, 사이버위협 및 해양 인텔리전스 데이터 수집 단계(10)는, IT(Information Technology) 사이버 위협 인텔리전스 및 OT(Operational Technology)사이버 위협 인텔리전스 데이터를 수집하고, 인텔리전스 데이터의 유효성을 검사할 수 있다.

- [71] 또한, 선박 구역에 따른 CBS 데이터 수집 및 관리 단계(20)는, 도 3에 도시된 바와 같이, 구역별 CBS 관리 단계(21)와, 구역별 CBS 구분 단계(22)와, 구역별 CBS 리스팅 단계(23) 및 구역별 위험 평가 단계(24)를 포함할 수 있다.
- [72] 또한, 사이버위협 스코어 기준을 통한 데이터 인덱싱 단계(30)는, 도 4에 도시된 바와 같이, 사이버 위협 분류 단계(31)와, 사이버 위협의 우선순위 지정 단계(32)와, 사이버 위협 획일화 단계(33) 및 우선순위별 스코어링 단계(34)를 포함할 수 있다.
- [73] 또한, 선박 구역별 위험 스코어 계산 단계(40)는, 선박의 선실, 브릿지룸, 엔진룸 등 선박 구역별 중요도에 따른 구역을 구분하여 가중치를 부여하는 가중치 부여 단계(45)를 더 포함할 수 있다.
- [74] 도 5를 참조하여 보다 구체적으로 살펴보면, 본 발명에 따른 선박 사이버보안 상태 측정을 위한 방법은, 사이버위협 및 해양 인텔리전스 데이터를 수집하는 데이터 수집 단계(S1)는, 데이터소스를 통해 IT(Information Technology) 사이버 위협 인텔리전스 및 OT(Operational Technology) 사이버 위협 인텔리전스를 수집하고, 인텔리전스 데이터의 유효성을 검사(S11)할 수 있다.
- [75] 이때, 데이터 수집 단계(S1)에서, 해양 인텔리전스 데이터는 사전에 수집되어 데이터소스에 저장될 수 있고, 저장된 데이터를 수신하여 수집될 수 있다.
- [76] 선박 구역에 따른 CBS 수집 및 관리 단계(S2)는, 데이터 소스를 통해 선박 CBS 데이터를 수집(S21)하고, CBS 분류/기능을 분석(S22)하며, 분류된 CBS의 유효성을 검사(S23)하고, 유효하지 않는 경우 CBS 데이터를 수정(S24)할 수 있으며, CBS 시스템을 관리(S25)할 수 있다.
- [77] 사이버위협 스코어 기준을 통한 데이터 인덱싱 단계(S3)는, 다차원 리스크 매트릭스는 등록된 CBS에서 발생 가능한 리스크 매트릭스를 나열하고 등급 부여를 위한 점수를 매기는 과정으로 CBS 카테고리 분류, 접근 권한, 침해 사례, 취약점, 외부 연결 상태, 접근 가능 포트, 파워에 대해 각각 리스크 스코어가 부여된다.
- [78] 따라서, 사이버위협 스코어 기준을 통한 데이터 인덱싱 단계(S3)는 다차원 리스크 매트릭스를 생성(S31)하고, 매트릭스 팩터 유효성을 검사(S32)하며, 최종적으로 단일 리스크 매트릭스를 생성(S33)단계에서는 등록된 모든 CBS의 스코어를 통합한 매트릭스를 도출한다.
- [79] 이때 단일 매트릭스 생성이 불가능한 경우, 매트릭스 요소를 재탐색(S34)하거나 다차원 리스크 매트릭스에 부합하지 않는 CBS가 등록될 경우 예외로 계산되어 N/A 등급을 부여한다.
- [80] 선박 구역별 위험 스코어 계산 단계(S4)는, 구역별 위험도/심각도를 측정(S41)한다.
- [81] 이때, 구역별 중요도에 따라 가중치를 설정(S45)할 수 있으며, 구역 구분 시 구역(룸)이 외부와 단절(폐쇄성)이 있는 경우 보다 낮은 가중치를 설정할 수 있다.

- [82] 위험도 완화 단계(S5)은 위험 수준에 따른 등급을 부여하여 위험 스코어에
- [83] 위험 스코어에 따른 선박 사이버보안 상태를 도출하고 위험도를 완화하도록 할 수 있다.
- [84] 따라서 본 발명에 따르면, 선박의 CBS(Computer Based System)을 다양한 소스로부터 수집되는 위험과 비교하여 위험 척도를 계산하는 방식으로 선박의 네트워크에 설치 또는 접근하지 않는 방식으로 가용성을 유지하고, 다양한 경로로 수집되는 위험 데이터는 위험 발생 정도 등 다양한 기준에 따라 인덱싱되어 점수화 한다. 선박의 선실, 브릿지룸, 엔진룸 등 중요도에 따라 구역을 구분하며, 각 구역의 CBS의 정량화된 위험 스코어링을 제공할 수 있는 효과를 갖는다.
- [85] 도 8 내지 도 10을 참조하면, 본 발명에 따른 선박 사이버 보안 위험 평가를 위한 방법은, 위험평가 대상 선박이 인증받을 선급의 사이버보안 요구사항을 위험평가 수행 시 조회하고 식별된 선박의 자산 중 사이버 보안 범위를 선정하는 범위 선정 단계; 범위 선정 단계를 통해 선정된 사이버 보안 범위 내에 CBS 카테고리를 분류하는 CBS 분류 단계; 상기 CBS 분류 단계를 통해 분류된 자산에 연결되는 복수의 네트워크에 대한 송수신 데이터를 데이터 수집부에서 수집하는 데이터 수집 단계; 및 상기 데이터 수집 단계에서 수집된 데이터에서 위험 목록을 식별하고 분석하여 복수의 네트워크 각각의 사이버보안 위협에 대한 사이버보안 위험 평가를 수행하는 위험 평가 단계를 포함할 수 있다.
- [86] 보다 구체적으로는, 도 8에 도시된 바와 같이, (1)범위 선정 단계(S110), (2)CBS(Computer Based System) 카테고리 분류(S120), (3)위험 목록 식별(S130), (4)위험 영향도(S140), (5)운영 위험(S150), (6)발생가능성평가(S160), (7)위험 수준 평가(S170), (8)위험 조치에 대한 결정(S180), (9)위험 완화(S190), (10)잔여 위험(S192)의 절차로 구성될 수 있다.
- [87] 범위 선정 단계(S110)는 위험평가 대상 선박이 인증 받을 선급의 사이버보안 요구사항을 위험평가 수행 시 조회하고 선박의 자산을 식별하여 사이버 보안 범위를 선정할 수 있다.
- [88] CBS(Computer Based System) 카테고리 분류 단계(S120)는 선박 내의 자산 중 CBS(Computer Based System)의 카테고리에 해당하는 자산을 분류한다.
- [89] 선박에서는 보안의 3대 요소 중 가용성을 중시하고 있다. 그리고 선박의 자산은 CBS(Computer Based System) 범주에 포함되는 시스템으로 분류된다. 따라서 선박 사이버보안 위험 평가 시 자산을 식별하고 분류할 때 CBS에 따라 분류되어야 하고 가용성을 고려한 위험 분석과 위험 조치를 수행한다.
- [90] 위험 목록 식별 단계(S130)는 분류된 CBS 카테고리에서 사이버보안 위협이 가능한 자산의 목록을 식별하고, 해당 자산이 연결된 복수의 네트워크에 대한 송수신 데이터를 수집할 수 있다.
- [91] 핵심 장비 및 시스템 식별은 사이버 공격에 취약한 선내 주요 자산을 식별하고 평가할 수 있다.

- [92] 영향도 평가는 시스템에 대한 가용성 측면에서의 위협 결과를 고려할 수 있다.
- [93] 이때 네트워크는 위성과 연동하는 VSAT(Very Small Aperture Terminal), IT(Information Technology) 네트워크, OT(Operational Technology) 네트워크 등을 포함할 수 있다.
- [94] 또한, 위협 목록 식별 단계(S130)를 통해 식별된 위협 목록을 분석하여 복수의 네트워크 각각의 사이버보안 위협에 대한 사이버보안 위협 평가를 수행하는 위협 평가 단계를 포함할 수 있다.
- [95] 이때 위협 평가 단계는, 위협 영향도 평가 단계(S140)와, 운영 위협 평가 단계(S150) 및 발생가능성 평가 단계(S160)를 포함할 수 있다.
- [96] 또한, 운영 위협 평가 단계(S150)는 제1 평가 단계인 공격 표면 평가 단계(S155)와 제2 평가 단계인 위협 노출 평가 단계(S159)를 포함할 수 있다.
- [97] 또한, 공격 표면 평가 단계(S155)는 연결성(S152)과 복잡성(S154)을 고려하여 공격 표면을 평가할 수 있다.
- [98] 또한, 위협 노출 평가 단계(S159)는 위협의 심각도(severity)(S157)와 노출정도(Degree of Exposure)(S158)를 통해 노출 등급을 도출하여 위협 노출(Threat Exposure)을 평가할 수 있다.
- [99] 즉, 육상과 해상의 차이점을 고려한 IACS Rec 171에서 위협 평가 시 측정기 어려운 엔드유저(End-User), 공격자 그룹(Attacker Group), 휴먼 팩터(Human Factor) 요소들을 대체할 수 있는 요소로 심각도(Severity), 노출 정도(Degree of Exposure), 위협 노출(Threat Exposure)을 제시하고 제시된 요소가 선박에서 명확하고 정량화된 위협 수준을 평가할 수 있는 효과를 갖는다.
- [100] 따라서, 본 발명에 따르면 IACS Rec 171의 위협평가(Risk Assessment)에서 휴먼 팩터(Human Factor)를 산정하는 엔드유저(End-User)와 공격자 그룹(Attacker Group)을 명확하게 판별하기 어렵기 때문에 이를 위협 노출 평가(Threat Exposure)로 대체하여 명확하고 정량화된 위협 수준을 평가할 수 있다.
- [101] 도 9를 참조하면, 선박 사이버 보안 위협 평가 시스템(100)은 선급별 사이버보안에 따른 사이버 보안 범위를 설정하여 위협 평가 범위를 선정하는 위협 평가 범위 선정부(110)와, 복수의 네트워크에 대한 송수신 데이터를 수집하는 데이터 수집부(120)와, CBS 카테고리에서 위협 목록을 식별하고 분석하여 복수의 네트워크 각각의 사이버보안 위협에 대한 사이버보안 위협 평가를 수행하는 분석부(130)와 각 선급들이 요구하는 사이버보안 규칙을 저장하는 데이터베이스부(140) 및 자산의 중요도에 따라 위협 평가 시점을 제어하는 제어부(150)를 포함할 수 있다.
- [102] 따라서, 본 발명에 따른 선박 사이버보안 위협 평가 방법은, 선급별 사이버보안에 따른 사이버 보안 범위를 선박 사이버 보안 위협 평가 시스템(100)의 위협 평가 범위 선정부(110)에서 설정하여 데이터베이스화 하는 범위 선정 단계와, 범위 선정 단계를 통해 선정되어 데이터베이스부(140)에 저장된 보안 범위 내에 선박의 자산을 CBS(Computer Based System)에 따라 분류하고, 분류된 자산에

연결되는 복수의 네트워크에 대한 송수신 데이터를 데이터 수집부(120)에서 수집하는 데이터 수집 단계 및 데이터 수집 단계에서 수집된 데이터에서 위협 목록을 식별하고 가용성을 고려한 위협을 분석부(130)에서 분석하여 복수의 네트워크 각각의 사이버보안 위협에 대한 사이버보안 위협 평가를 수행하는 위협 평가 단계를 포함한다.

- [103] 또한, 범위 선정 단계는, 선박을 인증하는 각 선급들이 요구하는 사이버보안 규칙(rule)을 데이터베이스(DB)화하고 위협 평가 시 선박이 인증 받을 선급의 사이버보안 요구사항에 맞춰 사이버보안 위협 평가 범위를 선정할 수 있다.
- [104] 또한, 데이터 수집 단계는, 선박의 자산을 식별하고, CBS 분류에 따른 자산 중요도를 고려하여 데이터 수집 시기를 제어부(150)에서 설정할 수 있다.
- [105] 또한, 위협 평가 단계는, 영향도(Impact grade) 평가 단계와, 공격 표면(Attack Surface) 평가 단계와, 위협 노출(Threat Exposure) 평가 단계 및 발생 가능성(Likelihood) 평가 단계를 포함할 수 있으며, 위협 노출 평가 단계는,
- [106] 위협의 심각도(severity)와 노출정도(Degree of Exposure)를 통해 노출 등급을 도출하여 위협 노출(Threat Exposure)을 평가할 수 있다.
- [107] 도 10에 도시된 바와 같이, 본 발명의 실시예에 따른 선박 사이버 보안 위협 평가 방법의 세부 구성을 살펴보면, 사전 협의 및 범위 선정 단계(S100)와, 위협분석 단계(S150)와, 종료 단계(S200)를 포함할 수 있으며, 사전협의 및 범위 선정 단계(S100)는, 사전준비(S101), 프로젝트 수행 요청(S102), 인증 선급 협의(S103), 법률 준수 국가 협의(S104), 대상 및 범위, 기간 협의(S105), 위협 분석 절차 협의(S106), CBS 식별 요청(S107) 단계를 포함할 수 있다.
- [108] 또한, 위협분석 단계(S150)는, 사전분석과 실선분석 및 평가 단계를 포함할 수 있다.
- [109] 사전분석 단계는 CBS 분류(S120), 영향도 평가(S140), 공격 표면 등급 평가(S155), 위협 노출 등급 평가(S159), 발생 가능성 등급 평가(S160) 및 위협 수준 산정(S170) 단계를 포함할 수 있다.
- [110] 또한, 위협 노출(Threat Exposure) 등급 평가(S159)는 심각도(Severity)와 노출정도(Degree of Exposure)의 두 요소에 각 등급에 따라 산정되는 것으로, 먼저 심각도(Severity)는 Low, Medium, High, Critical 1~4등급으로 분류되며, 노출정도(Degree of Exposure)는 None, CVE, MCTI, 다크웹, Naval 1~5등급으로 분류되고, 상기 심각도(Severity)와 노출정도(Degree of Exposure)의 등급이 판별되면 각 요소의 등급의 수치를 더하여 위협 노출(Threat Exposure) 등급을 1~5등급으로 분류하여 산정하는, 노출정도(Degree of Exposure)가 Naval은 심각도(Severity)와 상관없이 5등급으로 산정할 수 있다.
- [111] 또한, 실선분석 단계는 위협 확인(S171), 침투 테스트(S172), 위협 분석 체크리스트(S173) 위협 식별 및 분석(S174) 단계를 포함할 수 있다.

- [112] 또한, 평가 단계는 위험 완화 수준 평가(S191a), 위험 완화 기간 평가(S191b), RRL(Response Rate Limiting) 산정(S191c) 및 보호대책 수립(S191d) 단계를 포함할 수 있다.
- [113] 또한, 종료 단계는 대응 방안 수립(S201), 보고서 작성(S202), 보고서 리뷰(S203), 보고서 제출(S204) 및 프로젝트 종료(S205) 단계를 포함할 수 있다.
- [114] 본 발명에 따르면 사이버보안 위험 평가 시 위협의 심각도와 노출정도를 통해 위험 노출 등급을 도출하고 위험 발생가능성을 도출하는 요소로 활용하여 위험 평가의 정량화가 가능한 효과를 갖는다.
- [115] 또한, 본 발명에 따르면 정량화된 선박 사이버 보안 위험 평가 방법을 시스템으로 구축하여 위험 평가에 적용하여 해양의 특수성으로 인한 위험 평가의 문제점 해소에 기여할 수 있는 효과를 가진다.
- [116] 또한, 본 발명에 따르면 선급별 사이버 보안 요구사항에 맞춰 위험 평가를 수행하여 선급 인증 시 사이버 보안에 대한 요건을 갖출 수 있는 효과를 가진다.
- [117] 도 11은 본 발명에 따른 기계학습 기반 선박 사이버보안 이상징후 탐지 방법의 순서를 나타내는 순서도이고, 도 12는 본 발명에 따른 기계학습 기반 선박 사이버보안 이상징후 탐지 방법에서 보안통제 테이블을 포함한 위험도 테이블을 나타내는 도면이고, 도 13은 본 발명의 일 실시예에 따른 선박 네트워크 토폴로지 상에 위험도 및 보안통제 테이블을 대입하여 경로상에 CBS에서 해킹이 발생할 위험도가 높은 경로를 맵핑하여 나타내는 도면이다.
- [118] 도 11 내지 도 13을 참조하면, 본 발명의 일측면에 따른 기계학습 기반 선박 사이버보안 이상징후 탐지 방법은, CBS 공격표면 정보 스캐닝 단계(S300)와, CBS 공격표면 정량화 단계(S310)와, 사이버위험 지수 산출 단계(S320) 및 이상징후 그래프 생성 단계(S330)를 포함할 수 있다.
- [119] 보다 구체적으로는, 도 11에 도시된 바와 같이, CBS(Computer Based System) 공격표면 정보 스캐닝 단계(S300)는, CBS 정의부(310)를 통해 CBS 공격표면의 정보를 스캐닝 한다.
- [120] CBS 공격표면 정량화 단계(S310)는, CBS 공격표면 정보 스캐닝 단계(S300)를 통해 스캐닝된 CBS 공격표면 정보에 대하여 CBS 정의부(310)는 CBS 공격표면을 정량화할 수 있다.
- [121] 즉, ICT 환경의 선박 기자재가 탑재되는 비중이 높아짐에 따라, 선박 고유의 환경에 특화된 CBS의 공격표면을 정량화하고, 사이버위험을 사전에 예측하고 피해 가능경로, 피해 범위를 산정하여 예방할 수 있다.
- [122] 또한, 사이버위험 지수 산출 단계(S320)는 CBS 공격표면 정량화 단계(S310)를 통해 정량화된 CBS에 대하여 기계학습을 통해 위험분석부(320)에서 사이버위험 지수를 산출할 수 있다.
- [123] 사이버위험이 발생할 확률은 다음 수식으로 계산할 수 있다.
- [124]

$$P(hack|cbs) = \frac{P(hack|cbs) \cdot P(hack)}{P(cbs)}$$

- [125] 또한, 다음 수식은 선박 내부에 탑재된 CBS가 원인이되어 사이버공격의 피해가 발생할 수 있는 확률을 나타낸다.
- [126] $P(hack|cbs)$
- [127] 또한, 이상징후 그래프 생성 단계(S330)는, 사이버위험 지수 산출 단계(S320)를 통해 산출된 사이버위험 지수를 분석하여 위험분석부(320)에서 CBS에 해킹이 발생할 위험도가 높은 경로를 생성하고 맵핑하여 표시할 수 있다.
- [128] 이때 CBS 값은 선박 내부에 탑재된 CBS의 보안 취약성 정보를 CVE와 선박의 공격표면 정보, 선박 내부 네트워크에 설치된 침입탐지시스템으로부터 식별되는 정보를 통해 위험도 테이블을 생성할 수 있다.
- [129] 선박의 공격표면 정보는 오픈된 포트 정보, 가동중인 서비스 정보, 가동중인 데몬 정보 등을 통해 데이터를 획득할 수 있다.
- [130] 또한, 사이버위험 지수 산출 단계(S320)에서, 식별되는 정보는, 소스(source) IP와 테스트네이션(destinaion) IP 및 탐지 룰(rule) 중요도 정보를 포함하여, 위험도 테이블을 생성할 수 있다.
- [131] 또한, CBS 보안통제가 설정된 경우 보안통제 테이블을 포함하여 사이버위험 지수를 산출할 수 있다.
- [132] 즉, CBS 보안통제가 설정된 경우 위험도는 경감될 수 있기 때문에 도 12에 도시된 바와 같이, 보안통제 테이블을 포함하여 위험도 테이블을 생성할 수 있다.
- [133] 또한, 도 13에 도시된 바와 같이, 선박 네트워크 본 발명의 일측면에 따른 기계학습 기반 선박 사이버보안 이상징후 탐지 방법은, 이상징후 그래프 생성단계(S130)에서, 네트워크 토폴로지(Network Topology) 상에 위험도 테이블 및 보안통제 테이블을 대입하여 경로상에 CBS에서 해킹이 발생할 위험도가 높은 경로를 맵핑할 수 있다.
- [134] 네트워크 토폴로지는 네트워크 장치와 컴퓨터 시스템이 서로 연결되는 패턴이나 배열을 의미하며, 네트워크는 정보와 데이터를 공유하기 위해 연결되어 있는 컴퓨터 또는 장치를 나타내는 노드를 의미한다.
- [135] 또한, 토폴로지는 정보 흐름을 감독하는 상호 연결된 여러 노드 간의 연결 패턴 및 디자인을 나타낸다.
- [136] 또한, 이상징후 그래프 생성 단계(S330)에서, 네트워크 토폴로지는, 트리 토폴로지(Tree Topology)를 통해 이상징후 그래프를 생성할 수 있다.
- [137] 트리 토폴로지는 스타와 버스 토폴로지의 조합으로 형성될 수 있다.

- [138] 트리 토폴로지는, 토폴로지의 스타 특성으로 인해 새로운 확장 네트워크 설치가 쉬우며, 결합이 있는 노드의 문제 해결 용이성은 네트워크의 효율성을 높이고 주 네트워크에 영향을 미치지 않는 효과를 갖는다.
- [139] 또한, 트리 토폴로지는 신호 손실 없이 먼 거리에 걸쳐 신호를 전송할 수 있는 장점을 갖는다.
- [140] 따라서, 본 발명에 따르면, 선박 네트워크 토폴로지(Network Topology) 및 CBS(Computer based System) 특성 정보, 실시간 탐지된 위협정보를 기반으로 발생가능한 사이버위험을 예측함으로써 보안사고 예방과, 보안장비의 오탐, 과탐 등 실시간 침입차단으로 인해 발생할수 있는 위험요소를 방지할수 있는 효과를 갖는다.
- [141] 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.
- [142] 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.

청구범위

- [청구항 1] 선박 CBS 데이터를 수집하고 CBS에 대한 사이버위협 및 해양 인텔리전스 데이터 수집 단계;
선박 구역에 따른 CBS 데이터 수집 및 관리 단계;
사이버위협 스코어 기준을 통한 데이터 인덱싱 단계;
선박 구역별 위험 스코어 계산 단계; 및
위험 스코어에 따른 선박 사이버보안 상태를 도출하고 위험도를 완화하는 위험도 완화 단계를 포함하는, 선박 사이버보안 상태 측정을 위한 방법.
- [청구항 2] 청구항 1에 있어서,
사이버위협 및 해양 인텔리전스 데이터 수집 단계는,
IT 사이버 위험 인텔리전스 및 OT사이버 위험 인텔리전스를 수집하고,
인텔리전스 데이터의 유효성을 검사하는, 선박 사이버보안 상태 측정을 위한 방법.
- [청구항 3] 청구항 1에 있어서,
상기 선박 구역에 따른 CBS 데이터 수집 및 관리 단계는,
구획별 CBS 관리 단계;
구획별 CBS 구분 단계;
구획별 CBS 리스팅 단계; 및
구획별 위험 평가 단계를 포함하는, 선박 사이버보안 상태 측정을 위한 방법.
- [청구항 4] 청구항 1에 있어서,
상기 사이버위협 스코어 기준을 통한 데이터 인덱싱 단계는,
사이버 위험 분류 단계;
사이버 위험의 우선순위 지정 단계;
사이버 위험 획일화 단계; 및
우선순위별 스코어링 단계를 포함하는, 선박 사이버보안 상태 측정을 위한 방법.
- [청구항 5] 청구항 1에 있어서,
상기 선박 구역별 위험 스코어 계산 단계는,
선박의 선실, 브릿지룸, 엔진룸 등 선박 구역별 중요도에 따른 구역을 구분하여 가중치를 부여하는 가중치 부여 단계를 더 포함하는, 선박 사이버보안 상태 측정을 위한 방법.
- [청구항 6] 위험평가 대상 선박이 인증 받을 선급의 사이버보안 요구사항을 위험평가 수행 시 조회하고 선박의 자산을 식별하여 사이버 보안 범위를 선정하는 범위 선정 단계;

상기 범위 선정 단계를 통해 선정된 보안 범위 내에 선박의 자산을 CBS(Computer Based System)에 따라 분류하고, 분류된 자산에 연결되는 복수의 네트워크에 대한 송수신 데이터를 데이터 수집부에서 수집하는 데이터 수집 단계; 및
 상기 데이터 수집 단계에서 수집된 데이터에서 위협 목록을 식별하고 분석하여 복수의 네트워크 각각의 사이버보안 위협에 대한 사이버보안 위협 평가를 수행하는 위협 평가 단계를 포함하는, 선박 사이버보안 위협 평가 방법.

- [청구항 7] 청구항 6에 있어서,
 상기 범위 선정 단계는,
 선박을 인증하는 각 선급들이 요구하는 사이버보안 규칙(rule)이 저장된 데이터베이스(DB)로부터 조회하고, 위협 평가 시 선박이 인증 받을 선급의 사이버보안 요구사항에 맞춰 선박의 자산을 식별하여 사이버보안 위협 평가 범위를 선정하는, 선박 사이버보안 위협 평가 방법.
- [청구항 8] 청구항 6에 있어서,
 상기 데이터 수집 단계는,
 선박의 자산을 식별하고, CBS 분류에 따른 자산 중요도를 고려하여 데이터 수집 시기를 설정하는, 선박 사이버보안 위협 평가 방법.
- [청구항 9] 청구항 6에 있어서,
 상기 위협 평가 단계는,
 영향도 평가 단계, 공격 표면 평가 단계, 위협 노출 평가 단계 및 발생 가능성 평가 단계를 포함하는, 선박 사이버보안 위협 평가 방법.
- [청구항 10] 청구항 9에 있어서,
 상기 위협 노출 평가 단계는, 휴먼 팩터(Human Factor)를 산정하는 엔드유저(End-User)와 공격자 그룹(Attacker Group)을 대체하여, 심각도(Severity)와 노출정도(Degree of Exposure)를 평가하여 산정된 노출 등급을 통해 위협 노출 평가를 하는 것을 특징으로 하는, 선박 사이버보안 위협 평가 방법.
- [청구항 11] 청구항 10에 있어서,
 상기 위협 노출(Threat Exposure)은 심각도(Severity)와 노출정도(Degree of Exposure)의 두 요소에 각 등급에 따라 산정되는 것으로, 먼저 심각도(Severity)는 Low, Medium, High, Critical 1~4등급으로 분류되며;
 노출정도(Degree of Exposure)는 None, CVE, MCTI, 다크웹, Naval 1~5등급으로 분류되며;
 상기 심각도(Severity)와 노출정도(Degree of Exposure)의 등급이 판별되면 각 요소의 등급의 수치를 더하여 위협 노출(Threat Exposure) 등급을 1~5등급으로 분류하여 산정하는, 선박 사이버보안 위협 평가 방법.

- [청구항 12] CBS 정의부를 통해 실시간 CBS 공격표면의 정보를 스캐닝 하는 CBS 공격표면 정보 스캐닝 단계;
 상기 CBS 공격표면 정보 스캐닝 단계를 통해 스캐닝된 CBS 공격표면 정보에 대하여 CBS 정의부는 CBS 공격표면을 정량화하는 CBS 공격표면 정량화 단계;
 상기 CBS 공격표면 정량화 단계를 통해 정량화된 CBS에 대하여 기계학습을 통해 위험분석부에서 사이버위험 지수를 산출하는 사이버위험 지수 산출 단계; 및
 상기 사이버위험 지수 산출 단계를 통해 산출된 사이버위험지수를 분석하여 위험분석부에서 CBS에 해킹이 발생할 위험도가 높은 경로를 생성하는 이상징후 그래프 생성 단계를 포함하는, 기계학습 기반 선박 사이버보안 이상징후 탐지 방법.
- [청구항 13] 청구항 12에 있어서,
 상기 사이버위험 지수 산출 단계는,
 선박 내부에 탑재된 CBS 보안 취약성 정보를 CVE와 선박의 공격표면 정보, 선박 내부 네트워크에 설치된 침입탐지시스템으로 부터 식별되는 정보를 통해 위험도 테이블을 생성하는 것을 특징으로 하는, 기계학습 기반 선박 사이버보안 이상징후 탐지 방법.
- [청구항 14] 청구항 13에 있어서,
 상기 사이버위험 지수 산출 단계에서,
 상기 식별되는 정보는, 소스(source) IP와 테스트네이션(destinaion) IP 및 탐지 룰(rule) 중요도 정보를 포함하여, 위험도 테이블을 생성하며;
 CBS 보안통제가 설정된 경우 보안통제 테이블을 포함하여 사이버위험 지수를 산출하는, 기계학습 기반 선박 사이버보안 이상징후 탐지 방법.
- [청구항 15] 청구항 12에 있어서,
 상기 이상징후 그래프 생성단계에서,
 네트워크 토폴로지 상에 위험도 테이블 및 보안통제 테이블을 대입하여 경로상에 CBS에서 해킹이 발생할 위험도가 높은 경로를 맵핑하는,
 기계학습 기반 선박 사이버보안 이상징후 탐지 방법.
- [청구항 16] 청구항 12에 있어서,
 상기 이상징후 그래프 생성 단계에서,
 네트워크 토폴로지는, 트리 토폴로지를 통해 이상징후 그래프를 생성하는, 기계학습 기반 선박 사이버보안 이상징후 탐지 방법.