IACS UR E26 검증 자동화를 위한 워크플로우 기반 점검 방법론 설계

차한솔*, 김영민*, 김정호*, 조해성*, 박기웅†
세종대학교 (학부생, 교수†)

Design of a Workflow-Based Inspection Methodology for IACS UR E26 Verification Automation

Han-Sol Cha*, Young-Min Kim*, Jeong-Ho Kim*, Hae-Seong Cho*, Ki-Woong Park†
Sejong University(Undergraduate student, Professor†)

요 약

IACS UR E26은 2024년 7월부터 신조선에 강제 적용되는 선박 사이버 복원력 규정으로, 자산 관리, 네트워크 분리 등 15개 검증 항목을 요구한다. 그러나 현재 진행 중인 적합성 검증은 검사관이 방화벽 CLI에서 수동으로 정책을 조작하고 스크린샷을 캡처하여 수기 보고서를 작성하는 방식에 의존하고 있다. 이러한 수동 점검 방식은 항목당 30분에서 1시간이 소요되어 막대한 시간이 지연될 뿐만 아니라, 점검자의 역량에 따라 재현성 부재 및 품질 편차가 발생한다는 치명적인 한계가 존재한다. 본 논문에서는 이러한 수동 점검 워크플로우의 병목 지점을 분석하고, 이를 개선하기 위해 IACS UR E26의 핵심 4개 항목 (자산 목록 관리, 보안 영역 및 네트워크 분리, 네트워크 보호 수단, 네트워크 운영 모니터링)에 대한 워크플로우 기반 자동화 점검 방법을 제안한다. 검증 워크플로우에 내재된 단순 반복적이고 정형화 가능한 요소를 도출하여, 점검 과정을 자동 점검(Trigger), 결과 수집(Collect), Pass/Fail 판정(Judge)의 3단계로 표준화하였다. 제안하는 방법은 기존에 개별 도구와 물리적 확인에 의존하던 점검 과정을 병렬화 및 자동화하여 End-to-End 소요 시간을 획기적으로 단축할 수 있는 구조를 제공한다. 또한, 사전에 정의된 합격 기준과의 자동 대조를 통해 정량적인 Pass/Fail 판정을 내리고 PDF 보고서를 자동 생성함으로써 검증의 객관성과 재현성을 보장할 수 있도록 설계하였다. 본 연구는 물리적 제약이 큰 선박 환경의 보안 검증 체계에서, 시간적 효율성과 결과의 신뢰성을 동시에 확보할 수 있는 실무적 가이드라인을 제시한다는 점에서 의의가 있다.

I. 서론

IACS UR E26은 2024년 7월부터 신조선에 강제 적용되는 선박 사이버 복원력 규정으로, 자산 관리, 네트워크 분리 등 15개 검증 항목을 요구한다. 그러나 현재 진행 중인 적합성 검증은 검사관이 방화벽 CLI에서 수동으로 정책을 조작하고 스크린샷을 캡처하여 수기 보고서를 작성하는 방식에 의존하고 있다. 이러한 수동 점검 방식은 항목당 30분에서 1시간이 소요되어 막대한 시간이 지연될 뿐만 아니라, 점검자의 역량에 따라 재현성 부재 및 품질 편차가 발생한다는 치명적인 한계가 존재한다.

본 논문에서는 이러한 수동 점검 워크플로우의 병목 지점을 분석하고, 이를 개선하기 위해 IACS UR E26의 항목에 대한 워크플로우 기반 자동화 점검 방법을 제안한다. 검증 워크플로우에 내재된 단순 반복적이고 정형화 가능한 요소를 도출하여, 점검 과정을 자동 점검(Trigger), 결과 수집(Collect), Pass/Fail 판정(Judge)의 3단계로 표준화하였다. 제안하는 방법은 기존에 개별 도구와 물리적 확인에 의존하던 점검 과정을 병렬화 및 자동화하여 End-to-End 소요 시간을 획기적으로 단축할 수 있는 구조를 제공한다. 또한, 사전에 정의된 합격 기준과의 자동 대조를 통해 정량적인 Pass/Fail 판정을 내리고 보고서를 자동 생성함으로써 검증의 객관성과 재현성을 보장할 수 있도록 설계하였다.

본 연구는 물리적 제약이 큰 선박 환경의 보안 검증 체계에서, 시간적 효율성과 결과의 신뢰성을 동시에 확보할 수 있는 실무적 가이드라인을 제시한다는 점에서 의의가 있다.

† 교신저자: 박기웅(세종대학교 정보보호학과 교수)

본 연구는 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 정보보호핵심원천기술개발(Project No. RS-2026-25519773, 30%; RS-2024-00438551, 10%), 실감콘텐츠핵심기술개발(Project No. RS-2023-00228996, 20%), 대학ICT연구센터(ITRC) (Project No. , 10% IITP-2026-RS-2021-II211816, 10%), 한국연구재단(NRF) 핵심연구사업(Project No. RS-2026-25481431 30%)의 지원을 받아 수행된 연구임.

II. 관련 연구

2.1 선박 네트워크 보안 및 테스트베드 연구

Son 등은 IACS UR E26과 IEC 62443 참조 모델을 기반으로 선박 네트워크를 Enterprise,

DMZ, Control System 중심의 보안 구역으로 분류하고, 실선 환경에 적용 가능한 네트워크 토폴로지를 제안하였다. 이 연구는 구역 분리와 방화벽 기반 접근 통제를 실제 선박 환경에 매핑하였다는 점에서 의미가 있으나, 검증 수행은 주로 수동 절차에 의존하였고, 검증 결과의 자동 판정이나 보고서 자동화까지는 다루지 않았다.

해사 사이버보안 테스트베드 측면에서는 MaCySTe와 MariOT와 같은 연구가 대표적이다. 이들 연구는 선박 네트워크를 가상 또는 혼합 환경으로 재현하여 해사 프로토콜, 장비 상호작용, 공격 시나리오를 실험할 수 있는 기반을 제공하였다. 국내에서도 상용 보안 장비를 활용한 선박 사이버 테스트베드와 E26 시현 시험 절차가 정리되어 있다. 다만 이들 환경은 공격 재현, 교육, 기능 검증에 비중을 두고 있으며, 시험 절차를 정형 데이터로 환원하여 자동 판정하는 구조는 충분히 제시되지 않았다.

III. 수동점검 워크플로우 분석 및 한계점

3.1 수동 검증 절차 분해

UR E26 핵심 항목의 수동 검증 절차는 세부 내용과 무관하게 준비, 실행, 수집, 판정, 기록의 공통 구조로 추상화할 수 있다. 준비 단계에서는 장비 접속 및 점검 조건 확인이 수행되고, 실행 단계에서는 CLI 또는 관리 콘솔을 통해 점검 명령이 직접 입력된다. 이후 수집 단계에서 결과 화면, 로그, 이벤트가 확보되며, 판정 단계에서는 절차서와 육안 대조를 통해 합격 여부가 결정된다. 마지막으로 기록 단계에서 결과가 수기 보고서 양식에 전사된다.

이 중 기술적 가치가 높은 단계는 실행과 수집이지만, 실제 병목은 판정과 기록에서 발생한다. 검사관은 동일한 로그와 화면을 반복 해석해야 하며, 결과를 다시 문서 양식으로 옮겨 적는 과정에서 시간이 소모된다. 따라서 자동화 설계의 핵심은 단순 반복적 행위를 제거하고, 수집된 증적을 정형 데이터로 전환하는 데 있다.

3.2 단계별 자동화 가능 요소 도출

시현 시험 절차를 기준으로 보면 자산 목록 관리는 방화벽 ARP/DHCP 조회와 스위치 MAC 테이블 확인, 네트워크 분리는 Zone 간 통신 시도와 방화벽 로그 확인, 네트워크 보호 수단은 포트 스캔 또는 이상 트래픽 유발과 IDS/IPS 이벤트 확인, 네트워크 운영 모니터링은 테스트 이벤트 발생과 SIEM 경보 확인으로 구성된다. 즉, 점검 행위의 상당 부분이 명령 실행과 로그 확인이라는 정형 구조를 갖는다.

준비 및 실행 단계는 스크립트 또는 API 호출로 대체 가능하고, 수집 단계는 JSON 또는 이벤트 로그 수집기로 자동화할 수 있다. 판정 단계는 사전에 정의된 기준과의 비교 로직으로 치환 가능하며, 기록 단계는 결과 템플릿과 PDF 생성기로 자동화될 수 있다. 다만 물리적 단절 조작, 현장 장비 상태 전환, 수동 운전 확인과 같이 물리 개입이 요구되는 항목은 완전 자동화보다 반자동 절차가 적절하다.

IV. Trigger-Collect-Judge 자동화 점검 방법론

4.1 점검 단계 표준화 모델

제안 방법론의 핵심은 검사관의 수동 행위를 Trigger, Collect, Judge의 3단계로 구성하는 것이다.

Trigger 단계에서는 관리 스크립트를 통해 점검 절차를 자동 기동한다. 예를 들어 자산 목록 관리는 장비 인터페이스 조회, 네트워크 분리는 사전 정의된 경로에 대한 통신 시도, 네트워크 보호 수단은 포트 스캔이나 이상 트래픽 생성, 운영 모니터링은 테스트 이벤트 주입으로 구성할 수 있다.

Collect 단계에서는 Wazuh, Suricata, 방화벽 로그, 자산 스캔 결과와 같이 기계 판독 가능한 증적을 자동 수집한다. 수집 데이터는 JSON 또는 구조화된 이벤트 포맷으로 변환되어 Judge 단계의 입력으로 제공된다.

Judge 단계에서는 항목별 합격 기준과 수집 데이터를 자동 대조하여 Pass/Fail을 판정하고, 판정 결과를 표준 보고서 템플릿에 매핑한다. 이로써 기존의 "실행 – 화면 확인 – 수기 기록" 절차는 "자동 실행 – 자동 수집 – 자동 판정 – 자동 보고"의 통합 워크플로우로 재구성된다.

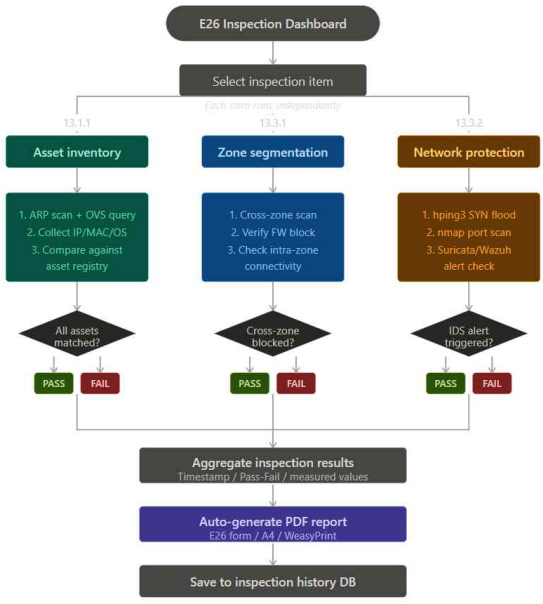

그림 1. 제안하는 3단계 자동화 검증 구조

4.2 항목별 Pass/Fail 판정 기준 설계

자동 판정을 위해서는 각 항목의 합격 기준을 기계 판독 가능한 규칙으로 정식화해야 한다.

자산 목록 관리는 스캔 결과와 기준 목록의 일치율, 미등록 자산 존재 여부로 판정할 수 있고, 네트워크 분리는 비허가 경로에 대한 차단 로그의 존재 여부로 판정할 수 있다. 네트워크 보호 수단은 공격 이벤트에 대한 탐지·차단 로그, IDS 또는 SIEM 수집 여부를 기준으로 하며, 네트워크 운영 모니터링은 테스트 이벤트 발생 후 경보 생성과 표시 여부를 기준으로 한다.

이와 같은 규칙 기반 판정은 결과 해석 과정에서의 주관 개입을 줄이고, 동일 입력에 대해 동일 결과를 반환하는 재현성을 확보하는 데 유리하다. 또한 판정 결과가 템플릿에 직접 반영되므로, 보고서 작성 단계 역시 사람이 결과를 다시 요약하거나 전사하는 부담을 줄일 수 있다.

V. 절차 분석 기반 기대 효과

5.1 기대 효과

수동 점검은 장비 접속, 명령 입력, 결과 대기, 화면 확인, 캡처, 수기 판정, 보고서 작성이 직렬적으로 수행되므로 반복 작업과 행정성 작업이 누적된다. 반면 제안 방식은 스크립트 실행, 로그 수집, 규칙 대조, 결과 템플릿 반영을 하나의 워크플로우로 통합한다. 따라서 본 연구는 실측 수치가 아닌 절차 분석 관점에서, 검사관의 개입 횟수 감소, 수기 전사 제거, 판정 일관성 향상이라는 실무적 효율을 기대할 수 있다.

또한 공통적으로 "조건 확인 – 명령 수행 – 로그 확인 – 합격 기준 대조"와 같은 구조를 가지는데, 이는 자동화에 적합한 패턴이며, 점검 결과를 정형 데이터로 남길 수 있다는 점에서 향후 통합 대시보드, 감사 추적, 보고서 자동 생성까지 자연스럽게 확장될 수 있다.

5.2 한계와 적용 범위

본 연구는 자동화 가능한 항목을 중심으로 방법론을 정립한 설계 연구이며, 물리적 네트워크 단절 조작이나 상용 장비 종속 인터페이스가 요구되는 항목까지 실증적으로 포함하지는 않았다. 또한 실제 조선소 시운전 환경의 장비 편차가 모두 반영된 것은 아니다. 그럼에도 불구하고 본 방법론은 현행 수동 점검 절차의 병목을 구조적으로 분석하고, 자동화 가능 영역을 명확히 구획하였다는 점에서 의미가 있다. 향후 통합 구현과 현장 검증이 수행된다면, 절차 분석 단계에서 제시한 기대 효과를 정량화하고 상용 방화벽 API, PLC 인터페이스, 격리·복구 절차까지 자동화 범위를 확장할 수 있다.

VI. 결론

본 논문은 IACS UR E26 적합성 검증에서 반복적으로 수행되는 수동 점검 절차를 분석하고, 이를 Trigger–Collect–Judge의 3단계 워크플로우로 표준화하는 자동화 점검 방법론을 제안하였다. 특히 각 자동화 가능한 항목들에 대해 자동 실행, 자동 수집, 규칙 기반 판정, 보고서 생성까지 연결되는 구조를 정립하였다.

제안 방법은 실측 성능평가보다는 절차 분석과 설계 관점에 초점을 두지만, 시운전 단계에서 반복되는 수작업과 수기 전사를 줄이고, 판정 기준을 명시적으로 코드화함으로써 객관성과 재현성을 높일 수 있는 실무적 가능성을 보여준다. 또한 실제 선박 환경에 앞서 사전 검증 및 자동화 로직 검토에 활용할 수 있는 기반을 제시하였다.

향후 연구에서는 물리적 끊김, 격리, 독립 운전, MRC 폴백, 복구 항목과 같이 현장 제약이 큰 절차로 자동화 범위를 확장하고, FortiGate 등 상용 장비 API 및 실제 운용 장비와의 연동을 통해 현장 적용성을 높일 계획이다. 이를 통해 해사 사이버보안 검증을 단순 시현 절차가 아닌 반복 가능하고 감사 가능한 자동화 검증 체계로 발전시키는 것이 목표이다.

VII. 참고문헌

[1] IMO, "Maritime Cyber Risk Management in Safety Management Systems," MSC.428(98), 2017.
[2] IACS, "Unified Requirement E26: Cyber Resilience of Ships," Rev.1, 2023.
[3] IACS, "Unified Requirement E27: Cyber Resilience of On-board Systems and Equipment," Rev.1, 2023.
[4] G. Son, S. Choi, N. Kang, and S. Kim, "Design of Ship Network Topology Considering IACS UR E26," J. Soc. Naval Architects of Korea, vol. 61, no. 6, pp. 427-436, Dec. 2024.
[5] G. Longo et al., "MaCySTe: A Maritime Cyber Security Testbed," SoftwareX, vol. 23, 101426, Jul. 2023.
[6] MPA, "MPA Commissions MariOT Training Facility," Maritime and Port Authority of Singapore, Mar. 2025.
[7] Pen Test Partners, "Hacking Serial Networks on Ships," Jun. 2018.
[8] DNV, "Maritime Cyber Priority 2024/25: Managing Cyber Risk to Enable Innovation," 2024.
[9] USCG, "Cyber Trends and Insights in the Maritime Environment (CTIME) 2025," May 2025.
[10] Marlink, "Global Maritime Cyber Threat Report H2 2024," May 2025.
[11] IEC-62443-2-1, "Industrial communication networks – Network and system security," Ed. 2, 2024.
[12] KISA, "Smart Ship Cyber Risk Assessment Guide," 2025.
[13] Dragos, "OT Cybersecurity Year in Review: 8th Annual Report," 2025.