ISO27014 기반 산업제어시스템 취약점 진단 프로그램 개발

Development of a Vulnerability Diagnosis Program for the Industrial Control System Based on ISO27014

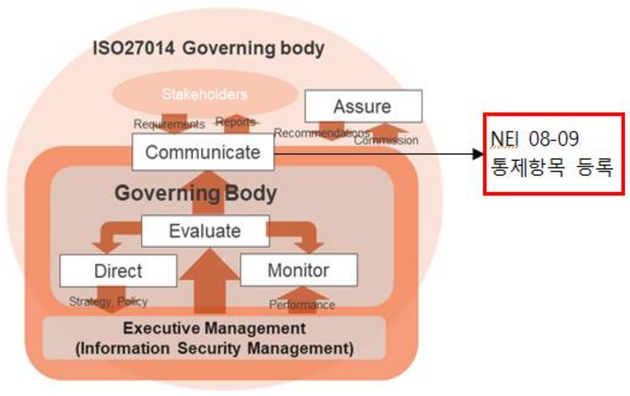
김은지, 김주연, 윤주혜
성신여자대학교
eungimin@naver.com

요약

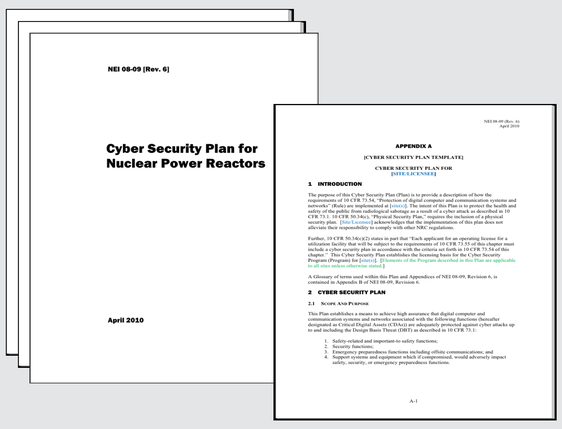
주요정보통신 기반 시설 및 빌딩, 공항 등에 적용된 시스템인 산업제어시스템은 인터넷 망과의 연계로 인해 사이버 보안사고의 위협에 노출되고 있다. 하지만, 이러한 위협에 앞서 현재 국내에는 체계적인 ICS 보안 표준이 구축되어 있지 않은 현황이다. 이에 본 논문은 국내 산업제어시스템의 체계적인 보안수준 강화를 위해 ISO 27014 Governing Body 영역을 구현하기 위한 프로그램을 개발하여 시스템 보안 향상에 도움을 줄 수 있도록 한다.

연구목적

산업제어시스템의 체계적인 보안수준 강화를 위해 ISO27014(정보보안 Governance 표준)의 영역과 미국 원자력산업협회에서 발행한 'NEI 08-09'의 통제항목을 통합하여 산업제어시스템 보안취약점 진단 프로그램을 개발하고 이를 통해 도출된 결과를 바탕으로 국내 산업제어시스템 정보보안 Governance 구축의 초석 마련을 위함



연구방법



	ISO 27014	프로그램 기능
Communicate	조직, 이해관계자 요구에 따라 정보보안 내용을 공유, 교환	기업의 필요, 요구사항에 따라 통제항목을 수정, 추가, 삭제
Evaluate	보안 현황을 고려하여 정보보호 활동 목표의 성취여부 측정	통제항목을 바탕으로 현재 ICS 보안성을 평가
Direct	보안 목적 전략 달성에 필요한 사항을 제시	계산식을 통해 보안 조치사항 우선순위를 도출, 조치방안을 제안
Monitor	보안관리 활동을 위한 적절한 성과지표를 관리하여 목적을 달성	우선순위를 이용하여 그래프, 인포그래픽을 이용한 가시화(정량화)

구분	가중치(중요도)			합계
	3점(상)	2점(중)	1점(하)	
통제항목별 점검 항목 개수	4개 (36%)	3개 (27%)	4개 (36%)	11개 (100 %)
가중치 총합	12	6	4	22

(통제항목별)조치우선순위
= 자산우선순위 × {(3×중요도'상'인 세부점검항목수)+(2×중요도'중'인 세부점검항목수)+(1×중요도'하'인 세부점검항목수)}

<수식1-1> 조치우선순위 계산식

1. NEI 08-09의 항목분석

미국 원자력 산업협회에서 발행한 NEI 08-09를 기반으로 산업제어시스템에 특화된 통제항목을 개발하여 산업 환경을 더욱 정확하게 진단하는 기반을 마련하였음

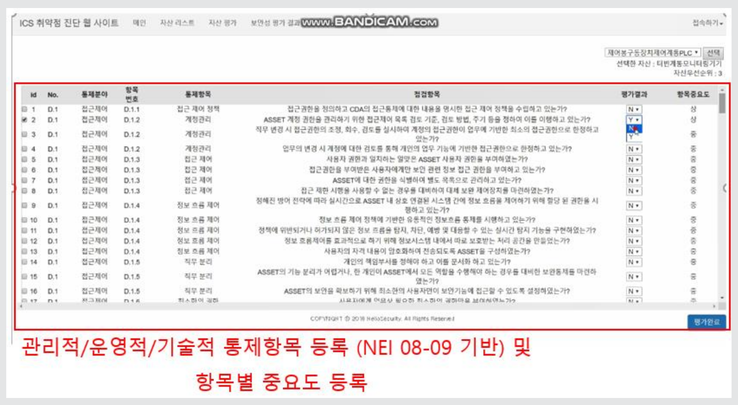
2. ISO 27014 거버넌스 영역 분석

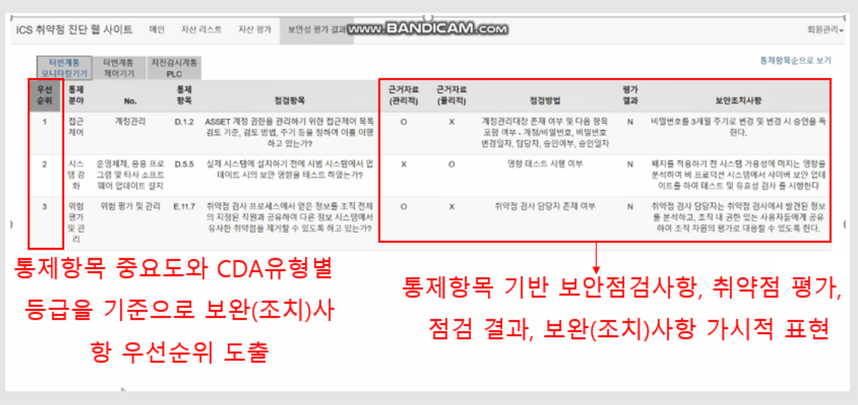
ISO27014를 모델로 한 취약점 진단 프로그램을 만들기 위해 ISO 27014를 구성하는 거버넌스 영역의 기능과 의의를 분석, 프로그램 기능에 접목시킴

3. 조치우선순위 산출을 위한 연구

사용자가 평가한 자산의 통제항목별 조치우선순위를 자동으로 산출할 수 있는 계산식을 개발하였음
세부 점검항목의 중요도는 주요 정보통신 기반 시설 취약점 분석·평가 점검항목에 명시된 등급 및 관련 연구결과를 참고하여 산정하였음

연구결과





우선순위 도출 계산식을 통해 자산별 통제항목 우선순위를 도출해낼 수 있었다. 조치가 시급한 항목이 무엇인지 알 수 있어 이를 응용하여 각종 분야에서 활용할 수 있을 것으로 사료된다.

결론

본 논문에서는 산업제어시스템의 무중단 운영 특성상 사전예방 및 관리가 중요하게 부각되고 있는 추세에 따른 취약점 진단 프로그램을 제안했다. 본 프로그램에서 가장 중심이 되는 기능은 계산식을 통한 조치우선순위 도출기능이다. 현재 국내에서는 CCE(규제준수를 위한 패턴매칭 방식의 취약점 점검)에 초점을 맞춰 발전하고 있는 실정이지만, 지능형 공격이 증가하고 있는 요즈음에는 취약점 자체를 찾아내어 실제 공격에 대응하기 위한 CVE방식 역시 필요하다. 본 프로그램 역시 CCE에 초점을 맞춰 개발되었다. 향후 CVE와 CCE방식을 융합한 개발이야 말로 ICS보안 분야의 연구과제로 생각된다.