ISO27014 기반 산업제어시스템 취약점 진단 프로그램 개발

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

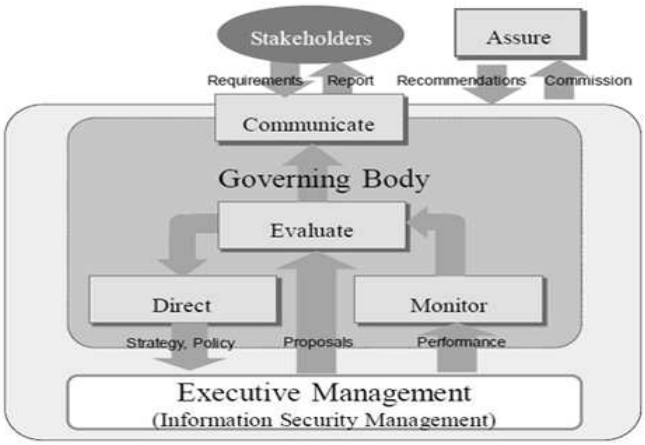
요 약

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 시스템의 보안 향상에 도움을 줄 수 있도록 한다.

1. 서 론

산업제어시스템(ICS, Industrial Control System)은 제조, 발전, 가공 등의 산업시설 뿐만 아니라 전력, 자원운송 등 주요정보통신 기반시설 및 빌딩, 공항 등의 시설에 적용된 시스템이다. 산업제어시스템은 SCADA(Supervisory Control And Data Acquisition System), 분산 제어시스템인 DCS(Distributed Control System), PLC(Programmable Logic Controller) 및 센서 등 다양한 구성요소 및 유형들로 이루어져 있다[1]. 이러한 산업제어시스템의 기능이 사이버 공격으로 인해 제 역할을 하지 못할 경우 시민의 안전에 위험을 초래하고, 국가 안보 및 경제의 안정에 심각한 피해를 줄 수 있다. 초기 산업제어시스템은 내·외부망으로 분리되어 운영되고 제어시스템 내 독자적인 통신프로토콜이 적용되어 폐쇄적으로 구축·운영되어 왔다. 하지만 최근 들어 다양한 분야의 적용을 위해 일반 업무용 시스템 망과 연계하는 추세이며, 이로 인해 ICS는 편리성을 위한 변화가 일어나게 되었다[2]. 이러한 상황에서 기존 인터넷망에서의 보안 사고에 대한 위협이 산업제어시스템으로 확산되던 중, 2010년 지멘스사의 SCADA 시스템을 공격하는 스턱스넷(Stuxnet) 악성코드가 발견되었다. 특정 SCADA를 노리는 스턱스넷은 산업제어시스템을 모니터링하거나 악성명령을 생성시키는 등 외부망과 내부망의 접점에서 발생할 수 있는 보안상 허점을 이용해 시스템을 장악하였다[3]. 이에 본 논문은 국내 산업제어시스템의 체계적인 보안수준 강화를 위해 ISO27014(정보보안 Governance표준)의 영역을 구현하는 프로그램을 제안한다. 또한 이러한 프로그램을 통해 향후 국내에 ICS 정보보안 거버넌스가 구축되어 국내 기업/기관의 지속적인 정보보안 수준 향상을 기대해볼 수 있다는 결론을 제시한다.

2.1. 시스템 기능



<그림 1> ISO27014 거버넌스 영역

ISO27014 거버넌스의 Body영역은 크게 네 가지 기능(Communicate, Evaluate, Direct, Monitor)으로 구분되어 있으며, 본 프로젝트에서는 이 기능을 프로그램에 접목시켜 구현하였다.[4].

ISO27014의 4가지 기능을 접목한 프로그램의 상세 기능은 다음 표와 같다.

제안 기능	기능 상세	ISO 27014 영역
통제항목 관리	• NEI 08-09 기반 통제항목 기입 • 통제항목에 대한 항목별 중요도 기입	Communicate
통제항목 기준 자산 평가	• Communicate 영역에서 정의된 통제항목에 대한 평가 결과 선택 • 점검항목 및 조치사항 기입	Evaluate

보안성 평가 결과	• 취약점 제거 위한 조치 사항 제시 • 조치우선순위 계산	Direct
보안수준 관리	• 보안수준 정량적 표현	Monitor

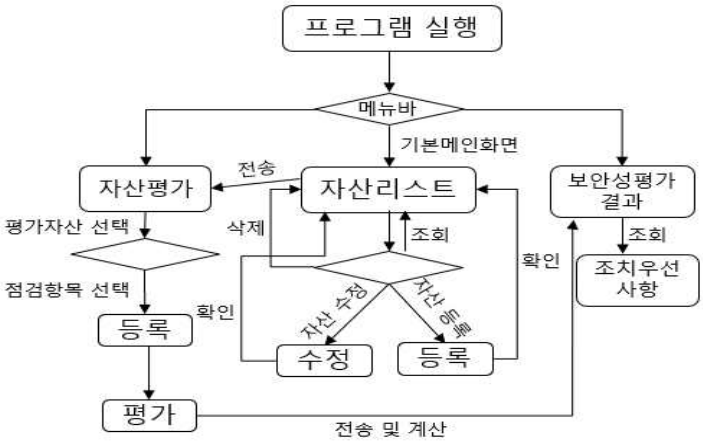
첫째, Communicate는 관리·운영·기술적 통제항목 등록 및 이에 대한 항목별 중요도를 등록하는 기능을 한다. 통제항목은 NEI 08-09을 기반으로 한다. 사용자는 새로운 위협이나 분석에 따라 통제항목을 추가, 수정, 삭제할 수 있다. 하지만, 관리자가 NEI 08-09를 기반으로 기입한 통제항목 및 항목별 중요도는 프로그램 개발 시 사전에 등록해두고 사용자가 데이터를 무단으로 수정 및 삭제할 수 없도록 한다. NEI 08-09를 기반으로 한 통제항목을 사용자가 임의로 수정, 삭제하게 될 경우, 보다 체계적으로 취약점을 진단하고자 하는 프로그램 제작의도에 어긋나기 때문이다. 이 단계를 통해 각 사용자들은 정보보안 관련 정보를 서로 교환할 수 있으며, 뿐만 아니라 정보보안 요구사항도 이해하는 데 도움을 준다.

둘째, Evaluate는 Communicate 영역에서 정의된 통제항목을 기반으로 사용자가 자산의 통제항목 내 세부점검항목 이행여부를 Y/N으로 평가하는 기능이다. 이 기능을 통해 사용자는 정보보안 성과 결과를 고려하고 예측하여 전략적으로 비즈니스 목적을 달성할 수 있다.

셋째, Direct는 자산우선순위와 항목별 중요도를 통해 도출된 조치우선순위를 직관적으로 사용자에게 보여주고, 취약점을 감소 및 제거할 수 있도록 조치사항을 제시하는 기능이다. Evaluate에서 기입한 데이터 중 평가 결과가 'N'으로 기입된 데이터에 한해서만 보안성 평가 결과가 보여진다. '보안성 평가 결과' 탭에서는 통제항목 순과 조치우선순위 순, 두 가지로 필요에 따라 선택하여 볼 수 있다. 조치우선순위 순으로 정렬하기 위해 프로그램에 내장된 계산식을 통해 계산 후 Bottom-up 방식으로 정렬되었기 때문에 사용자는 산정된 조치우선순위를 통해 가장 취약한 자산을 파악할 수 있다. 또한, 사용자는 이에 따른 보안조치사항을 이행해서 해당 취약점을 보완할 수 있다. 즉, 이 단계는 정보보안 목표와 전략 방향을 제공하는 기능을 한다.

넷째, Monitor는 Direct의 결과를 시각적으로 보여주는 기능을 포함한다. Direct에서 사용한 계산식의 통제항목별 조치우선순위를 그래프로 나타낸다. 또한, 'N'으로 체크했던 통제항목의 중요도별 개수를 그래프로 보여주어 지표를 한 눈에 알아볼 수 있도록 하였다.

2.2 시스템 흐름도



위 그림은 프로그램 메뉴 흐름을 도식화한 시스템 흐름도이다. 프로그램 상단 메뉴 바의 순서에 따라 차례대로 자산 평가를 할 수 있다. 먼저, 사용자가 취약점 진단 프로그램을 실행시키면 메인화면으로 접속하게 된다. '자산 리스트' 메뉴에서는 사용자가 택한 자산을 등록, 수정 및 삭제할 수 있다. 둘째, '자산 평가'메뉴는 보안성 평가의 기반이 되는 통제항목을 조회, 추가, 삭제할 수 있으며, 최종적으로 점검항목을 통해 자산의 보안성 평가를 할 수 있는 메뉴이다. 사용자는 '자산평가' 메뉴에서 평가하려는 자산과 통제항목을 선택하여 자산의 점검항목 이행여부를 체크한다. 셋째, '보안성 평가 결과' 메뉴는 '자산 평가'에서 체크한 결과를 바탕으로 이행되지 않은 점검항목만을 도출한다. 또한, 사용자는 평가한 자산의 조치우선순위 및 이에 대한 보안조치사항을 알 수 있다.

2.3 항목별 중요도 선정 기준

기업 내 정보보안 활동은 흔히 세 가지(취약점 분석 및 대응, 취약점 발견 및 예방, 취약점 검토 및 보고)로 구분된다. 본 프로그램에서는 여기서 분류된 활동을 기준으로 통제항목의 중요도(상, 중, 하)를 고정된 값으로 하였다. 통제항목별 중요도는 주요 정보통신 기반 시설 취약점 분석·평가 점검항목에 명시된 등급 및 관련 연구결과를 기준으로 설정하였다. 통제항목별 중요도기준은 다음과 같다.

상	- 취약점 **분석 및 대응절차**와 관련된 정책·지침 **수립** - ASSET의 접근 통제 등의 통제항목
중	- 취약점 **발견 및 예방**에 관련된 세부적인 정책·지침 **이행 및 승인·감독** - 보완통제·대체보완장치, 권한 부여, 문서화, 구현 및 개발 등의 통제항목
하	- 취약점 **검토 및 예방**에 관련된 정책 및 지침의 **감사** - 모니터링, 검토/테스트 등의 통제항목

중요도를 '상'으로 지정한 항목들은 취약점 분석 및 대응절차와 관련된 정책·지침 수립, ASSET의 접근 통제 등의 통제항목이다. 정책 및 지침 수립은 관리적 보안 측면에서 전체를 포괄할 수 있는 근본이 되므로 거버넌스 내에서 기본적으로 갖춰져야 할 부분이기 때문이다. 산업제어시스템의 통상적인 취약점들은 정책 및 절차를 포함하는 문서들의 부재 및 불완전·부

적절성에서 기인한다.[5]

또한, 기술적·물리적 보안 측면에서 ASSET의 물리·논리적 접근통제 항목이 경외시될 경우 ICS에 비인가적 접근 및 내부자 유출이 발생함에 따라 중요 시스템에 대한 접근이 용이해져 통제의 접근권한이 오·남용될 수 있다. 따라서, 중요 시스템에 대한 접근권한 관리와 관리자 식별 등에 있어 더 엄격하고 강화된 보안이 이루어져야 한다.

'중'으로 지정한 항목은 세부적인 정책·지침 이행 및 승인·감독, 보완통제·대체보완장치, 권한 부여, 문서화, 구현 및 개발 등 취약점 발견 및 예방에 관련된 항목이다. 이 단계는 직접적인 사이버 공격에 대한 대응보다는 보안을 더욱 체계적으로 보완하는 단계기 때문에 상대적으로 중요도가 떨어진다.

마지막으로, '하'로 지정한 항목은 정책 및 지침의 감사, 모니터링, 검토/테스트 등과 같은 취약점 검토 및 보고 단계이다. 이 단계는 향후 프로그램의 설계보완 및 ICS의 현황을 파악하는 데 도움을 줄 수 있지만, ICS의 보안성 향상에 있어서는 크게 영향을 끼치지 않는 항목들이다.

2.4 조치우선순위 계산식

자산명	우선순위
터빈계통 PLC	2
터빈계통 모니터링기기	3
지진감시계통 PLC	2
핵연료취급계통 PLC	1
핵증기공급계통 제어기기	1

<표1-1> 자산우선순위

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

<표1-2> 계산식 도출 표

$$(\text{통제항목별})\text{조치우선순위} = \text{자산우선순위} \times \left\{ \begin{array}{l} (3 \times \text{중요도 '상'인 세부점검항목수}) + \\ (2 \times \text{중요도 '중'인 세부점검항목수}) + \\ (1 \times \text{중요도 '하'인 세부점검항목수}) \end{array} \right\}$$

<수식1-1> 조치우선순위 계산식

본 프로그램은 프로그램 내부에 삽입되어 있는 계산식을 통해 조치우선순위를 자동으로 산출하는 방식을 채택했다. 예시는 표1-1과 같다. 조치우선순위를 정량적 수치로 도출하기 위하여 자산 우선순위(1순위/2순위/3순위)와 통제항목별 중요도(상/중/하)를 각각 3, 2, 1점으로 부여하였다. 최종적으로 조치우선순위 도출을 위한 자산별 결과 값은 자산 우선순위 별 가중치에 통제항목 가중치 합계를 곱하여 도출된다. 예를 들어, '터빈계통 PLC' 자산을 NEI 08-09의 통제항목인 'E.12 사이버 위험 평가 및 관리' 항목을 통해 도출된 우선순위 계산식 결과는 2(자산 우선순위) X 가중치 총합 합계(22점) =44(점) 이다. 이 결과를 통해 상대적으로 아래 그림과 같이 조치우선순위가 매겨진다.

3. 결 론

본 논문에서는 산업제어시스템의 무중단 운영 특성상 사전예방 및 관리가 중요하게 부각되고 있는 추세에 따른 취약점 진단 프로그램을 제안했다. 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 개발이야말로 ICS보안 분야의 연구과제로 생각된다.

4. 참 고 문 헌

[1] 손경호, "산업제어시스템 보안성 평가·인증 동향 분석", 한국정보보호학회, 2014

[2] 김일용, 임희택, 지대범, 박재표, "산업제어시스템 환경에서 효과적인 네트워크 보안 관리 모델", 한국산학기술학회, 2018

[3] 조용현, 이은경, "산업제어시스템을 위한 정보보호 관리체계 설계 방안 연구", 한국컴퓨터정보학회, 2016

[4] 김정덕, 이성일, "정보보호 거버넌스 국제표준화와 국내 도입 사례 연구", 한국정보보호학회, 2012

[5] 김도연, "산업제어시스템의 사이버보안을 위한 취약점 분석", JKIECS, vol. 9, no. 1, pp. 140, 2014

본 논문은 과학기술정보통신부 정보통신창의인재양성사업의 지원을 통해 수행한 ICT멘토링 프로젝트 결과물입니다.