ICS 27014 기반 산업제어시스템

취약점 진단 프로그램

:ICS 27014 Governing Body 영역을 구현하기 위한 프로그램

HelloSecurity Team

(김주연, 김은지, 윤주혜)

성신여자대학교 사회과학대학 융합보안학과

2018.09.07

****

목 차

1. 프로그램의 목적
2. 프로그램 구성도
3. 프로그램 기능

1 프로그램(기능) 목록

2 기능 흐름도

3 화면 설계서

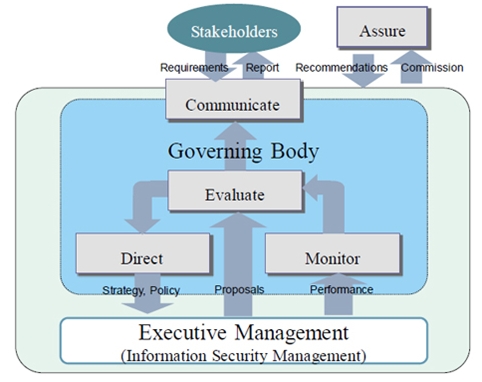
1. 관련 연구

1 항목별 중요도 기준

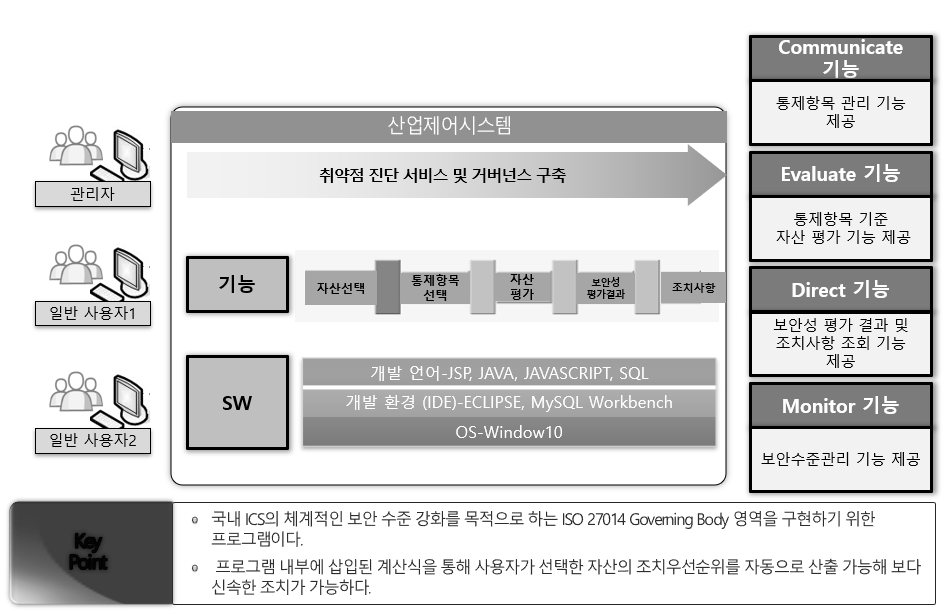
2 계산식

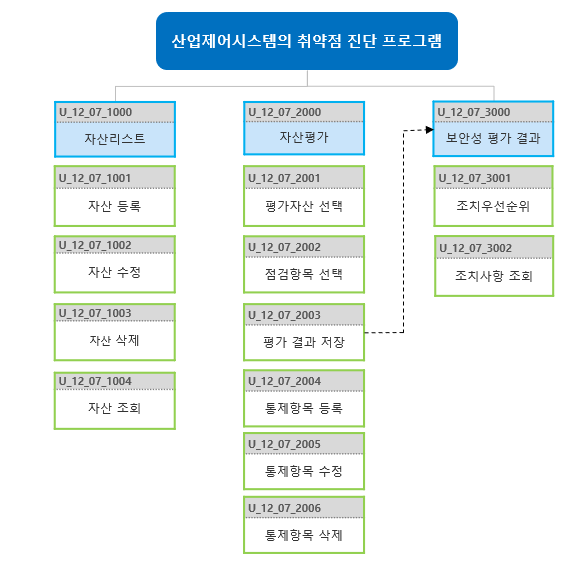
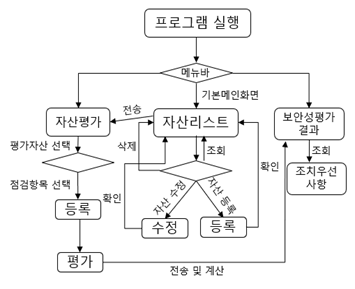
1. 결론
2. 참고 문헌
3. **프로그램의 목적**

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. 초기 산업제어시스템은 내·외부망으로 분리되어 작동하였고, 제어시스템 내 독자적인 통신프로토콜이 적용되어 폐쇄적으로 구축·운영되어 왔었다. 하지만 최근 들어 산업제어시스템과 일반 인터넷 망의 연계로 인해 기존 인터넷 망에서의 보안 사고에 대한 위협이 산업제어시스템으로 확산되었다.  이후, 2010년 지멘스사의 SCADA 시스템을 공격하는 스턱스넷 악성코드가 발견되는 등 산업제어시스템을 표적으로 한 지능화된 공격이 증가함에 따라 산업제어시스템의 보안 시스템을 좀 더 체계적으로 갖춰야 할 필요성이 대두되고 있다. 이러한 흐름에 따라 국내에서는 체계적인 정보보호 관리를 위해 정보보호관리체계(ISMS 등)를 도입하는 기업들이 증가하는 추세다. 그러나, 이러한 정보보호관리체계는 산업제어시스템에 특화된 요소들을 효과적으로 관리할 수 없다. 이러한 한계점을 보완하기 위해 우리는 ISO 27014 Governing Body 영역을 구현하기 위한 프로그램을 개발하여 산업제어시스템의 체계적이고 지속적인 보안 향상에 도움을 주는 것을 목표로 하였다.



**[그림1-1] ISO27014 정보보안 거버넌스 표준**

1. **프로그램 구성도**

**[그림2-1] 시스템 구성도**

**[그림 2-2] 시스템 흐름도** **[그림 2-3]  메뉴 구성도**

위 그림은 본 프로그램 개발에 앞서 프로그램 메뉴 흐름을 도식화한 시스템 구성도와 메뉴의 구체적인 기능을 보여주는 메뉴 구성도이다. 프로그램 상단 메뉴 바의 메뉴 순서에 따라 차례대로 자산 평가를 할 수 있다. 먼저, 사용자가 취약점 진단 프로그램을 실행시키면 메인화면으로 접속하게 된다. ‘자산 리스트’ 메뉴에서는 사용자가 평가하고 싶은 자산을 등록, 수정 및 삭제할 수 있다. 두번째로, ‘자산 평가’메뉴는 통제항목을 통해 자산의 보안성 평가를 할 수 있으며 보안성 평가의 기반이 되는 통제항목을 조회, 수정, 삭제 할 수 있는 메뉴이다. 자산을 등록한 사용자는 ‘자산평가’ 메뉴에서 평가하려는 자산과 통제항목을 선택하여 자산의 통제항목 이행여부를 체크한다. 마지막으로, ‘보안성 평가 결과’ 메뉴는 ‘자산 평가’에서 체크한 결과를 바탕으로 평가결과를 도출한다. 사용자는 평가한 자산의 취약점 조치우선순위 및 이에 대한 보안조치사항을 알 수 있다.

1. **프로그램 기능**

프로그램의 시스템 기능은 ISO 27014에서 제시한 4가지 기능(Communicate, Evaluate, Direct, Monitor)을 기반으로 이루어져있다. 4가지 기능에 대한 상세 기능은 아래 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 평가결과 | - 취약점 제거 위한 조치 사항 제시  - 조치우선순위 계산 | Direct |
| 보안수준 관리 | - 보안수준 정량적 표현 | Monitor |

첫째, Communicate(의사소통)는 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. NEI08-09를 기반으로한 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, Evaluate(평가)는 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.

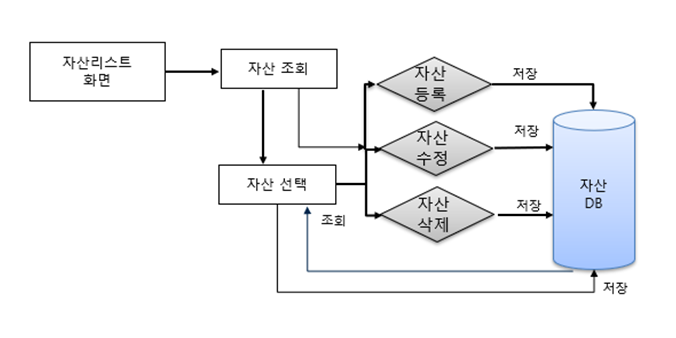
셋째, Direct(지시)는 자산우선순위와 항목별 중요도를 통해 도출된 조치우선순위를 직관적으로 사용자에게 보여주고, 취약점을 감소 및 제거할 수 있도록 조치사항을 제시하는 기능이다. Evaluate에서 기입한 데이터 중 평가 결과가 ‘N’으로 기입된 데이터에 한해서만 보안성 평가 결과가 보여진다. ‘보안성 평가 결과’ 탭에서는 통제항목 순과 조치우선순위 순, 두 가지로 필요에 따라 선택하여 볼 수 있다. 조치우선순위 순으로 정렬하기 위해 프로그램에 내장한 계산식은 데이터베이스 내부에 존재하고 있는 자산리스트 데이터와 자산평가 데이터, 프로그램 소스 코드 내 자바스크립트 함수를 통해 구현했다. 또한, Bottom-up방식으로 정렬되었기 때문에 사용자는 산정된 조치우선순위를 통해 가장 취약한 자산을 파악할 수 있으며 이에 따른 보안조치사항을 이행해서 해당 취약점을 보완할 수 있다. 즉, 이 단계는 정보보안 목표와 전략 방향을 제공하는 기능을 한다.

넷째, Monitor(모니터)는 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.

프로그램의 목록은 4가지 기능을 포함하고 있는 각 화면별 구성도를 나타내는 것으로 아래와 같다.

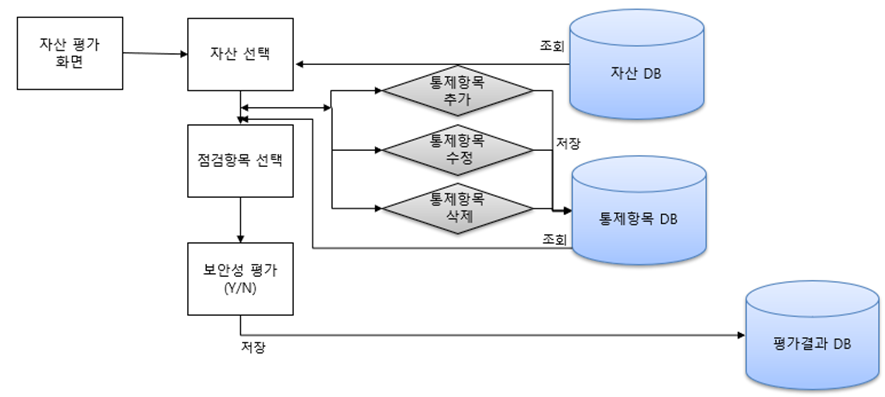


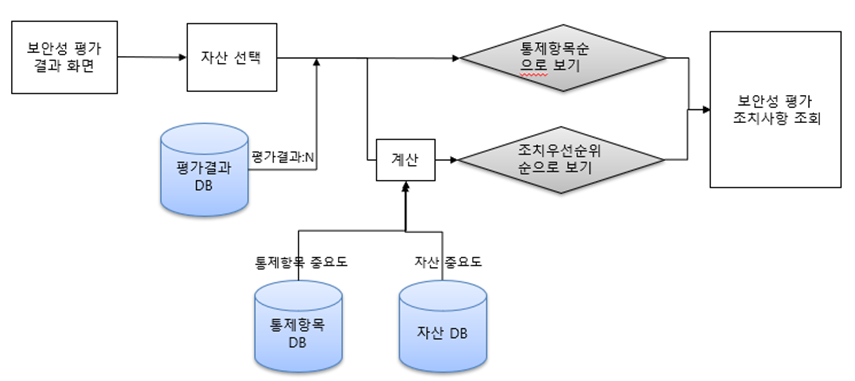
**[그림 3-1]  프로그램(기능) 목록**



**[그림 3-2] 자산리스트 기능 흐름도**

먼저 사용자는 로그인을 한 후 자산리스트 화면에 접속해 자산을 조회한다. 프로그램은 여기서 등록된 자산들을 가지고 조치우선순위를 계산하기 때문에 사용자가 화면에서 자산 정보를 변경(등록, 수정, 삭제)하기만 하면 즉각적으로 자산DB에 반영되어 자산 평가 화면에서 불러올 수 있다.

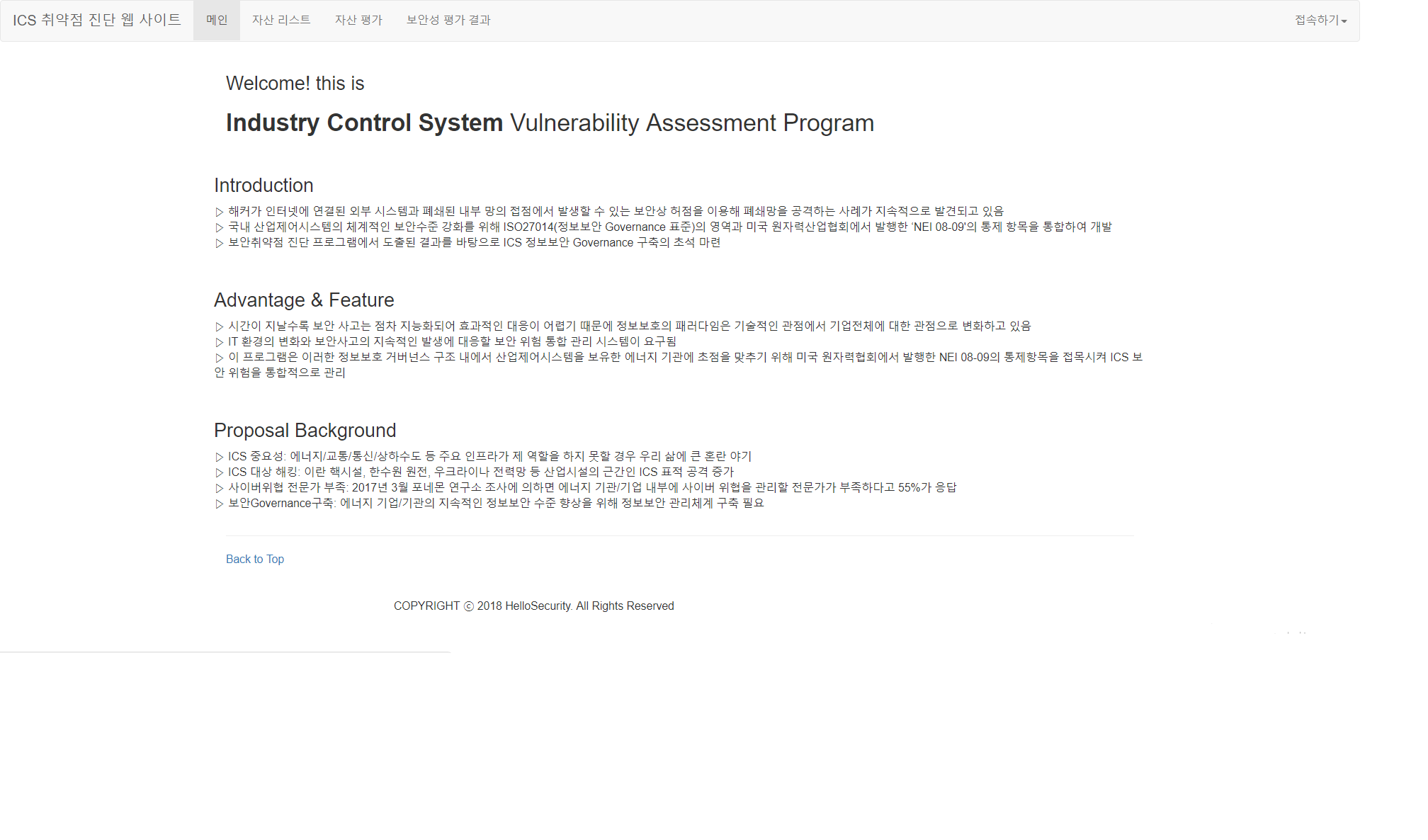
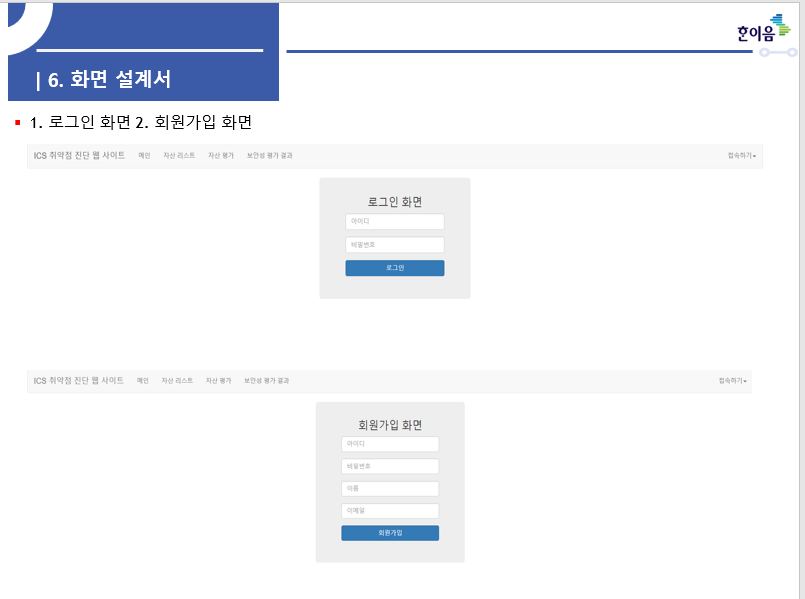
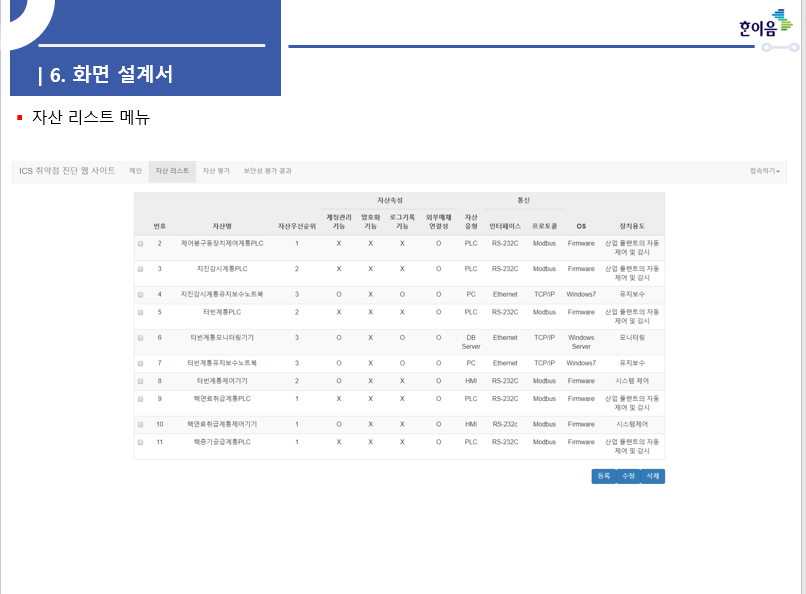
**[그림 3-3] 자산 평가 기능 흐름도**

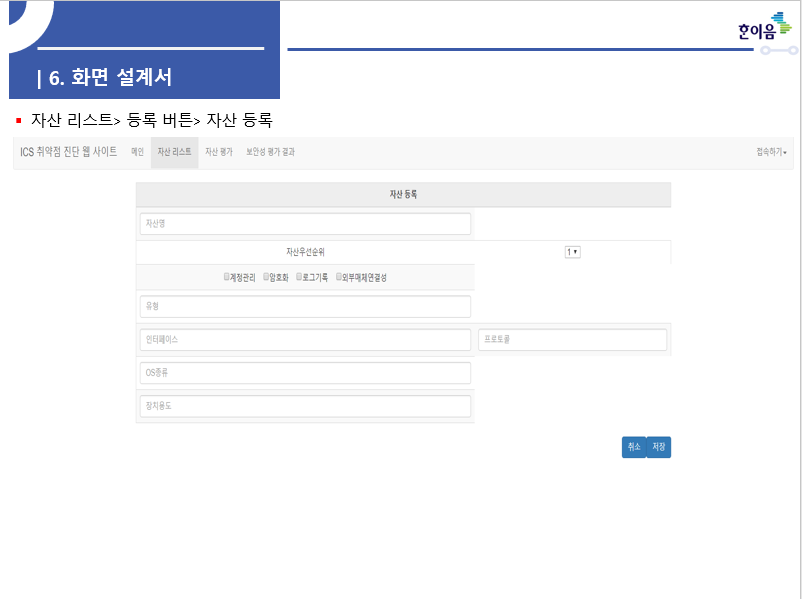
****자산평가에서 사용자는 평가기준이 되는 통제항목을 추가, 수정, 삭제할 수 있다. 이때 프로그램에 기본적으로 저장된 통제항목은 수정과 삭제 기능이 적용되지 않는다. 자산리스트 기능과 연동된 자산DB의 자산 항목을 불러와 평가하려는 자산을 선택한다. 그 다음 점검하고자 하는 통제항목을 선택하고 해당 항목의 이행여부를 평가한다. 평가완료 버튼을 누르면 사용자가 선택한 자산과 통제항목, 해당 항목의 이행 결과가 평가결과 DB로 저장된다.

**[그림 3-4]  보안성 평가 결과 기능 흐름도**

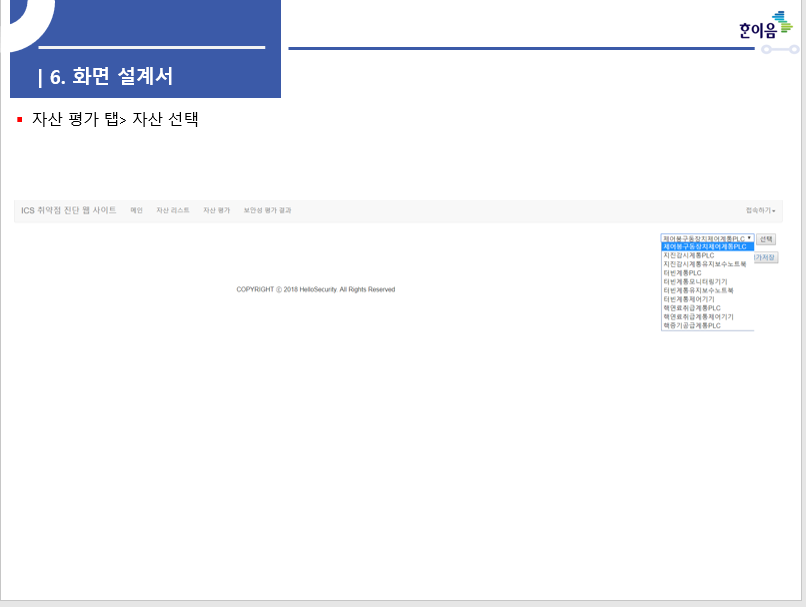
보안성 평가 결과 화면은 사용자가 평가완료 버튼을 누른 후 그 결과 값을 나타내는 화면이다.  평가결과 DB에 저장된 항목 중에서 평가결과가 ‘N’으로 기입된 항목에 대해서만 계산식을 사용해 조치우선순위 및 보안조치사항을 알려준다. 계산식은 통제항목 DB에 저장된 통제항목내 점검항목의 중요도와 자산 DB에 저장된 자산 우선순위를 이용하여 구현했다. 기본 화면은 통제항목의 번호를 오름차순으로 정렬한 결과창이다. 반면, ‘조치우선순위순으로 보기’버튼을 누르면 탭에서 택한 자산에 대해 조치우선순위가 높은 순서대로 통제항목을 정렬하여 보여준다.

구현한 프로그램의 화면설계서는 다음과 같다.

* **메인화면> 상단 좌측 접속하기**
* **1. 로그인화면 2. 회원가입 화면**
* **자산리스트 메뉴**
* **자산리스트 > 등록버튼 > 자산 등록**



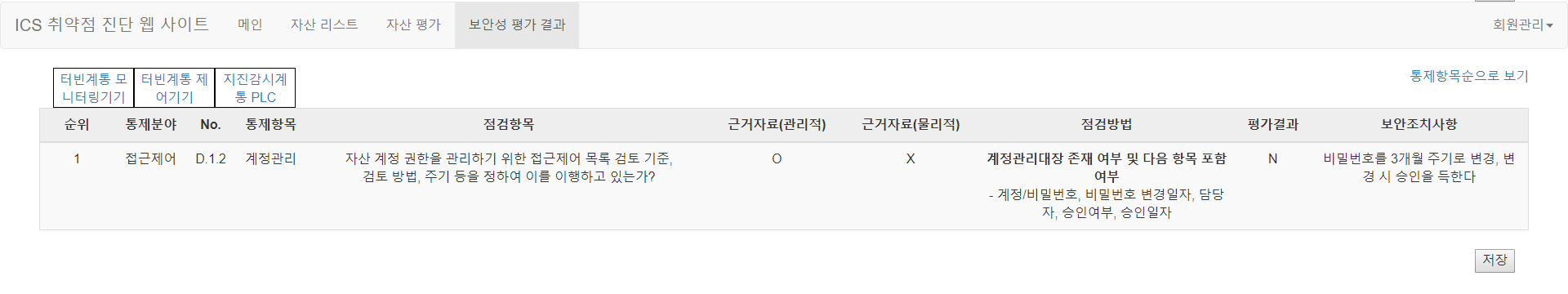
* **자산 평가 탭 > 자산 선택**



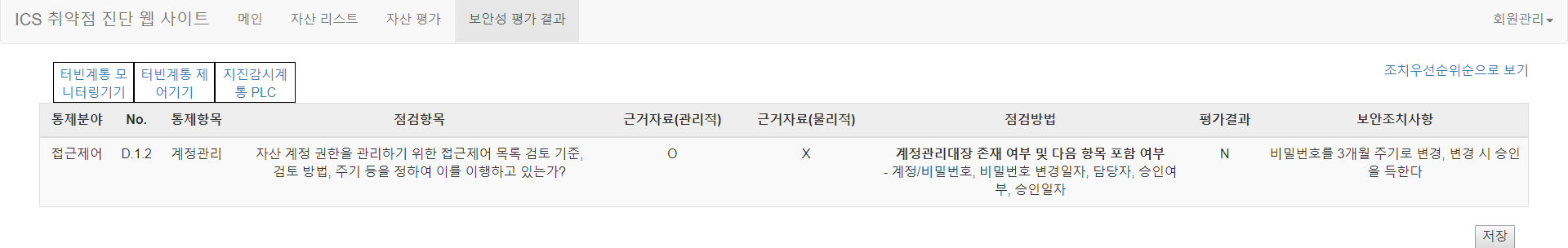
* **자산 평가 탭 > 자산 선택 > 통제항목 선택 > 평가결과 기입(Y/N) > 평가저장**



* **보안성 평가 결과 탭> 터빈계통 모니터링기기> 저장**



* **통제항목순으로 보기**

****

마지막으로 본 프로그램은 다음과 같은 개발환경에서 구현하였다.

|  |  |  |
| --- | --- | --- |
| S/W 개발환경 | OS | Windows 10 |
| 개발환경(IDE) | Eclipse |
| 개발도구 | Eclipse, Tomcat, Mysql |
| 개발언어 | JAVA, JSP, JAVASCRIPT |
| 기타사항 | 서버구축 - AWS EC2 |

1. **관련 연구**

1. 항목별 중요도 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.

중요도를 ‘상’으로 지정한 항목들은 ‘취약점 분석 및 대응절차’와 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·부적절성에서 기인한다.[2]

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

‘중’은 ‘취약점 발견 및 예방’에 관련된 세부적인 정책·지침 이행 및 승인·감독, 보완통제·대체보완장치, 권한 부여, 문서화, 구현 및 개발 등의 통제항목이 해당된다. 직접적인 사이버 공격에 대한 대응보다는 보안을 더욱 체계적으로 보완하는 단계기 때문에 상대적으로 중요도가 떨어진다.

‘하’는 취약점 검토 및 예방에 관련된 정책 및 지침의 감사, 모니터링, 검토/테스트 등의 통제항목이 해당된다. 향후 프로그램의 설계보완 및 ICS의 현황을 파악하는 데 도움을 줄 수 있지만, ICS의 보안성 향상에 있어서는 크게 영향을 끼치지 않는 항목들이다.

2. 계산식

본 프로그램은 프로그램 내부에 삽입되어 있는 계산식을 통해 조치우선순위를 자동으로 산출하는 방식을 채택했다. 조치우선순위는 평가대상 자산에 대한 통제항목별로 계산이 이루어진다. 예를 들어, D.1과 같은 통제분야에는 D,1.1, D.1.2와 같은 통제항목이 있으며, 각각의 통제항목에는 세부점검항목이 있다. 이 세부점검항목은 각 항목마다 중요도가 상이하다. (

이렇게 각각 상이한 중요도를 고려하여 통제항목의 조치우선순위를 정량적 수치로 도출하기 위하여 점검항목별 중요도(상/중/하)를 각각 3점, 2점, 1점으로 부여하였다. 예를 들어, 사용자가 N으로 평가한 점검항목의 중요도가 ‘상-중-중-중’ 이면 점수는 6점이 되고, 중요도가 ’하-하-하’ 이면 점수는 3점이 된다. 자산 우선순위(1순위/2순위/3순위) 를 각각 3점, 2점 1점으로 부여하여 계산한 통제항목 점수에 우선순위 별 가중치 점수를 곱하였다.

1. **결론**

이러한 프로그램을 통해 향후 국내에 ICS 정보보안 거버넌스가 구축되어 국내 기업/기관의 지속적인 정보보안 수준 향상을 기대해 볼 수 있다는 결론을 제시한다. 앞서 설명한 바와 같이, 해당 프로그램을 사용하는 사용자는 별 다른 설정 없이 선택 후 버튼만 눌러 해당 자산의 취약점 조치우선순위 및 이에 대한 보안조치사항을 간편하게 알 수 있다는 장점이 있다. 또한, 선택한 자산에 대해서만 평가를 진행하기 때문에 평가 시간이 비교적 짧아서 사용자는 취약점에 신속하게 대응할 수 있어 해당 제어시스템에 대한 신뢰성 있는 보안을 유지할 수 있다. 다만, 이 프로그램에 있어 개선방안을 제시하자면, 현재 국내에서는 CCE(규제준수를 위한 패턴매칭 방식의 취약점 점검)에 초점을 맞춰 발전하고 있는 실정이다. 우리 프로젝트 팀원들도 위 프로그램을 개발하기 위해 이 프로그램에 들어갈 데이터(자산, 통제항목 등)의 전문성을 강화시키고자 NEI 08-09의 번역작업 및 통제항목에 대한 조치방안 강구, 산업제어시스템의 구성요소(SCADA, PLC 등)에 대한 스터디를 팀원들과 2월 달부터 매주 꾸준히 진행했기 때문에 다른 프로그램보다 ICS 보안 위험을 통합적으로 관리할 수 있는 프로그램을 개발할 수 있었다. 하지만, 지능형 공격이 증가하고 있는 요즈음에는 취약점 자체를 찾아내어 실제 공격에 대응하기 위한 CVE방식 역시 필요하다. 본 프로그램 역시 CCE에 초점을 맞춰 개발되었지만 향후 CVE와 CCE방식을 융합한 개발이야말로 ICS 보안 분야의 연구과제로 생각된다.

1. **참고문헌**

[1] 김일용, 임희택, 지대범, 박재표, “산업제어시스템 환경에서 효과적인 네트워크 보안 관리 모델”, 2018, 한국산학기술학회

[2] 김도연, “산업제어시스템의 사이버보안을 위한 취약점 분석”, 2014, 한국전자통신학회