산업제어시스템 자산 유형별 보안성 평가 연구

김은지*, 김혜진**, 박민지***, 박태영****, 이지은*
*성신여자대학교 융합보안공학과, **성신여자대학교 정보시스템공학과
***성신여자대학교 컴퓨터공학과, ****한국산업기술대학교 IT경영학과
eungimin@naver.com, hihello1208@naver.com, pmj7755@naver.com, ty990520@naver.com,
dlwldms30899@gmail.com

A study on security evaluation by type of ICS Asset

Eun-Ji Kim*, Hye-Jin Kim**, Min-Ji Park***, Tae-Young Park****, Ji-Eun Lee*
*Dept. of Convergence Security Engineering, Sung-Shin Women's University
**Dept. of Information System engineering, Sung-Shin Women's University
***Dept. of Computer Engineering, Sung-Shin Women's University
****Dept. of IT Business, Korea Polytechnic University

요 약

산업제어시스템에 침해사고가 발생하여 서비스 제공이 중단될 경우 사회에 큰 혼란을 야기할 수 있기 때문에 주기적으로 내부 자산의 보안 수준을 관리하는 것은 매우 중요하다. 위 논문은 산업제어시스템 내부 자산의 보안성 확립을 위한 산업제어시스템 자산 유형별 보안성 평가 프로그램을 제안한다. 동일 자산 그룹에 따라 보안조치를 선별적으로 적용하고 신규 취약점을 지속적으로 파악하는 프로세스를 프로그램에 적용하여 제어시스템 보안 수준을 안정적으로 유지하는 사내 프로그램으로 활용될 수 있도록 한다.

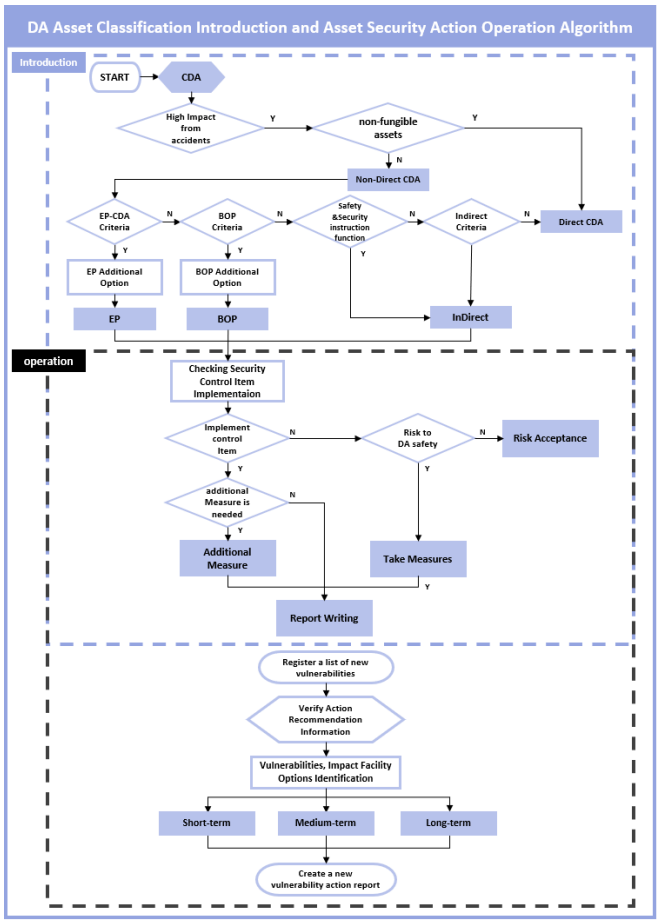
Ⅰ. 서론

산업제어시스템은 산업시설 또는 사회의 중요한 인프라와 관련된 물리적 프로세스를 제어하는 시스템이다. 이로 인해 서비스 제공이 중단될 경우 심각한 경제적 피해와 사회 혼란으로 이어질 수 있다[1]. 현재 산업제어시스템의 보안조치 규제는 안전/보안/비상대응 기능에서 동일한 사이버 보안조치 기준에 의해 규제되고 있기 때문에 관리의 효율성이 저하되고 있다[2]. 또한 기술의 발전에 따라 산업제어시스템이 디지털 시스템으로 변경되면서, 이전에는 없었던 사이버 보안 취약점 및 관련 위협이 지속적으로 발견되고 있다[2]. 이에 따라 각 디지털 자산의 특성을 반영한 개별적인 보안조치를 적용하여 기존 취약점 보안조치 관리의 효율성을 극대화할 필요성이 생겼다. 뿐만 아니라, 기존/신규 취약점을 지속적으로 파악하고 취약점에 맞는 대응 조치를 마련하여 제어시스템 사고로 인한 피해를 최소화할 필요성이 존재한다. 본 논문에서는 자산의 특성 및 침해영향도를 단계적으로 평가하여 동일한 속성에 따라 자산을 그룹화하고, 최적화된 보안조치를 선별적으로 적용하고자 한다. 또한, CVE 항목과 디지털자산 제조사를 통해 수집한 신규 취약점에 해당하는 영향설비에 단계별 보안조치를 적용하여 효과적인 취약점 관리가 가능하도록 한다. 이를 바탕으로 관리적/운영적/기술적인 측면에서 디지털 자산 보안조치의 전 과정을 효율적으로 시행할 수 있도록 하는 통합관리체계를 제시하여 제어시스템 내부 취약점을 체계적으로 관리하는 프로세스를 제안한다.

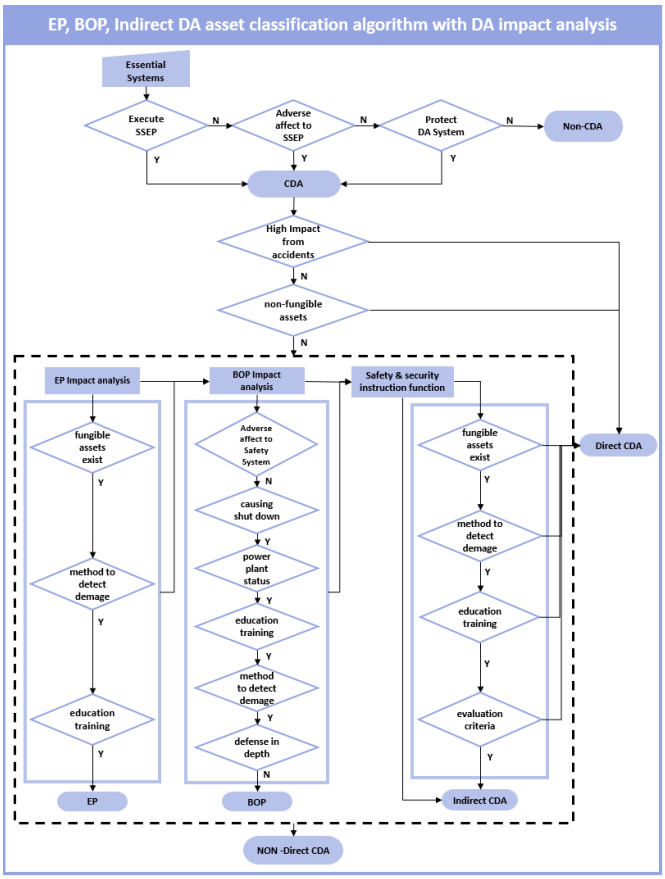
Ⅱ. 본론

1. DA 영향도에 따른 보안성 평가 관리 프로세스

본 논문에서 제시하는 DA 보안성 평가 및 관리 프로그램은 다음과 같은 프로세스로 작동하여 전체 프로세스는 아래 (그림 1)에서 확인할 수 있다. (1) DA 도입 단계에는 디지털 자산을 Direct DA, BOP(Balance Of Plant), Indirect DA, EP(Emergency Preparedness)로 분류한다. (2) 분류결과에 따라 그룹별로 통제항목을 적용하여 그룹의 특성 반영한 보안조치 수행 (3) DA 운영단계에서 영향 설비에 따라 신규 취약점 조치 계획 및 이행을 통하여 효율적인 취약점 조치를 제공한다. 이에 디지털자산의 보안성을 도입부터 운영단계까지 유지하도록 한다.



(그림 1) DA 자산 분류 도입 및 자산 보안 조치 운영 알고리즘



(그림 2) DA 영향도 분석으로 EP, BOP, Indirect DA 자산 분류 알고리즘

2. 기능별 세부 프로세스

2.1. EP, BOP, Indirect DA 자산 분류 프로세스

(그림 2)는 필수디지털자산의 침해영향도에 따라 자산을 분류하는 시스템 알고리즘을 도식화한 것이다. 프로그램은 크게 3 단계의 DA 영향도 분류 과정을 수행한다. (1) DA 분류, (2) DA 를 직접 디지털 자산과 간접디지털 자산으로 분류, (3) 영향성 분석을 통해 간접디지털 자산을 EP, BOP, Indirect DA 그룹으로 세분화

1 단계, 제어시스템 내부의 디지털 자산 중 DA 분류를 진행한다. DA 는 발전소가 반드시 유지해야하는 안전, 보안, 비상대응 기능을 수행하거나 해당 기능에 악영향을 미칠 수 있는 자산이다. 이후 식별된 CDA 를 사이버 공격 발생 시 SSEP 기능에 부정적인 영향이 발생하는 직접필수디지털자산(이하, Direct CDA)와 부정적인 영향이 발생하지 않는 간접필수디지털자산(이하, Non-Direct CDA)로 분류한다.

2 단계로 Direct CDA 와 Non-Direct CDA 를 분류한다. Direct CDA 와 Non-Direct CDA 는 SSEP 침해영향도의 수준과 SSEP 관련 기능을 대안적으로 수행하는 설비의 존재 여부로 분류할 수 있다.

3 단계로 Non-Direct CDA 에서 수행기능과 SSEP 의 침해영향도를 기반으로 EP, BOP, Indirect DA 로 분류한다. EP 자산은 SSEP 기능 중 EP 기능을 보조하는 자산이다. 먼저 EP 영향도 분석을 통해 해당 자산이 EP 기능을 수행하는 자산인지 파악한다. 또한 특정 설비가 마비되었을 경우 EP 기능을 대신 수행할 수 있는 대체수단이 존재하는지 파악한다. 또한, 사고가 발생한 후 손상을 탐지하거나 사고를 예방하기 위한 훈련이 존재한다면 사고를 미리 예방할 수 있거나 사고 후 SSEP 손상에 대한 영향이 극히 적다고 판단할 수 있어 최종적으로 EP 로 분류할 수 있다. BOP 는 발전소의 반응도에 직간접적으로 영향을 줄 수 있는 자산으로, 발전소의 현재 상태를 확인할 수 있는 상태정보를 제공하기 위해 작동하는 비안전 관련 설비이다. 먼저 BOP 영향도 분석을 통해 발전소 반응도의 침해영향도를 파악한다. 안전시스템의 악영향 발생 여부, 발전소 상태정보의 제공 여부, 발전정지의 유발여부, 심층 방호 기능을 제공 여부를 파악한 후, BOP 또한 손상 탐지 여부와 교육 훈련 존재

여부를 확인하여 SSEP 기능에 악영향을 미치지 않는다는 점을 확인하고 BOP 로 분류한다. Indirect 자산은 발전소 내부의 지시 및 경보를 제공하는 설비로 사이버 공격이 발생하더라도 안전/보안 기능에 악영향을 미치지 않으며 사용자가 대체할 수 있는 수단이 있는 자산이다.

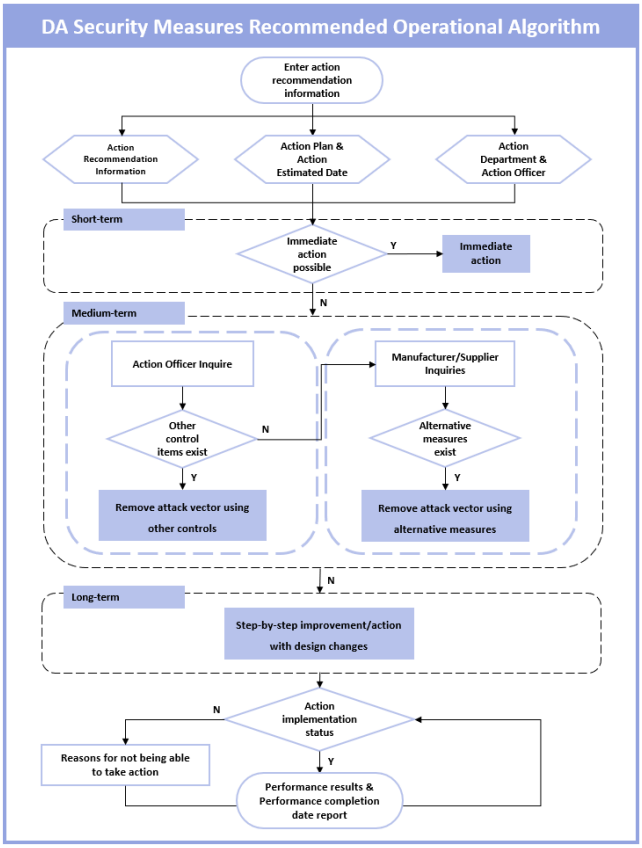
따라서 안전보안지시 기능이 존재한다면 Indirect 자산으로 분류할 수 있다. 해당 설비가 마비되었을 경우 기능을 대신 수행할 수 있는 대체 자산이 존재하는지 확인하고, 손상 탐지 여부와 교육 훈련 존재 여부를 확인하여 최종적으로 Indirect DA 로 분류한다. 위 3 가지 분류에 해당되지 않는 자산은 SSEP 기능에 악영향을 미칠 수 있다고 판단하여 Direct DA 으로 분류한다. 이후 분류한 자산은 통제항목을 이행하고 있는지 점검하는 과정을 거친다. 통제항목은 자산별 특성을 반영하였기 때문에 자산의 보안성을 더욱 정확하게 판단할 수 있으며 자산 내부에 존재하는 취약점을 조기에 파악할 수 있다.

통제항목을 이행하지 않은 경우, 항목의 미이행이 안전에 영향을 미치지 않는다면 위협을 수용하고, 미치는 경우 해당 통제항목을 이행하도록 한다. 통제항목을 이행했음에도 잔존 위험이 존재하는 경우 추가 이행조치를 적용한다. 모든 과정 이후에는 통제항목 적용관리 보고서를 작성하여 현시점의 보안성을 기록하도록 한다.

2.2. 신규 취약점에 따른 보안성 조치 권고 운영 프로세스

도입단계에서 CVE 항목과 디지털자산 제조사를 통해 얻은 신규 취약점과 이에 영향을 받는 설비 정보를 활용하여 정보보안부서 담당자는 취약점 영향 설비에 한하여 취약점 조치 권고를 발행한다.

조치권고 정보와 각 취약점 조치 이행 기간에 따라 조치방법은 단기, 중기, 장기로 선정한다. 취약점 조치 이행 기간에 따른 선정 기준은 다음과 같으며 (그림 3)에서 기준 선정 흐름을 확인할 수 있다. 첫 번째로, 조치 권고가 취약점 조치 담당자에 의해 즉시 조치가 가능하다면 단기 조치를 선정하여 즉시 조치를 이행한다. 그러나 즉시조치가 불가능하다고 판단된다면 두 번째로, 조치 담당자를 통하여 취약점을 해결할 수 있는 타 통제항목을 기준으로 중기 조치를 적용하여 취약점을 제거한다. 만약 타 통제항목이 존재하지 않는다면 설비의 제조사 및 공급사로부터 취약점에 대한 대안조치의 존재 여부를 확인하여 중기 조치를 통해 취약점 공격벡터를 제거한다. 두 번째 단계까지 취약점 조치 구분조건에 부합하지 않은 경우 세 번째 단계에서, 필수적으로 설계를 변경한다. 이를 통하여 단계적으로 개선하는 방향으로 장기 과정을 수행해야 한다.



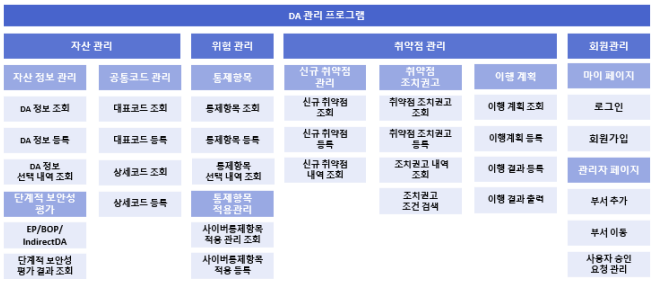
(그림 3) DA 보안성 조치 권고 운영 알고리즘

(그림 3)의 흐름에 따라 조치권고를 발행하고 수행된 단기, 중기, 장기 조치 수행방법은 공통된 최종 단계를 수행한다. 취약점 조치 담당자는 조치 권고 취약점에 대하여 조치이행 여부를 확인함으로써 취약점 조치가 정상적으로 이행되었는지 검토한다. 이행되었다면 이행결과와 이행완료일자를 보고한다. 조치 권고 미이행의 경우에는 이행불가사유와 이에 대한 대안조치를 입력한 후 다시 이행여부를 확인하는 과정을 반복한다. 이 때 조치부서가 선택할 수 있는 대안조치는 통제항목에서 선택하는 것을 원칙으로 한다. 본 과정은 취약점 조치 권고가 정상적으로 이행되었을 때까지 반복된다.

Ⅲ. DA 보안성 평가에 따른 보안조치 프로그램 개발

1. 프로그램 주요 기능

본 프로그램은 크게 자산 관리, 위험 관리, 취약점 관리 3 가지 관리 기능을 가지고 있다. 이에 세부 기능으로는 효율적으로 산업제어시스템의 자산을 유형별로 보안성 및 취약점 관리할 수 있는 기능으로 구성되어 있다. 세부 기능 중 주요 기능 4 가지를 다음 장에서 소개한다.



(그림 4) 프로그램 기능 구성도

2. 기능별 화면 설명

2.1. 도입 과정 기능

(그림 5) 자산관리 기능

(그림 5)는 자산관리 탭의 자산 단계적 보안성 평가 메뉴이다. 자산을 선택하하면 자산 영향성 분석 결과에 따라 EP. BOP. Indirect DA에 해당하는 평가화면이 나온다. 해당 단계의 분류 조건을 충족하면 즉시 결과가 반환, 평가가 종료된다. 이 기능을 통해 자산을 EP, BOP, Indirect 별로 한눈에 파악할 수 있다.

(그림 6) 위험관리 기능

(그림 6)은 위험관리 탭의 사이버 보안항목 적용관리 메뉴이다. 점검하려는 자산을 선택한 후 자산의 보안항목 준수 여부를 체크하여 보고서 형태로 저장할 수 있다. 점검이 완료되면 적용관리 보고서는 시간순으로 누적되어 향후 이력관리가 가능하며 과거 보안상태를 추적할 수 있다.

2.2. 운영 과정 기능

(그림 7) 취약점 관리 기능

(그림 7)은 취약점 관리 탭의 조치권고 메뉴이다. 앞서 등록한 신규 취약점을 조치할 영향설비 및 담당 부서, 조치 유형을 등록하여 각 설비 상황에 맞는 취약점 조치권고를 발행할 수 있다. 조치 권고 내역은 발행일자별로 정렬되어 시급한 조치를 직관적으로 파악할 수 있다.

(그림 8) 취약점 조치 이행계획 기능

(그림 8)은 (그림 7)에서 발행한 취약점 조치권고를 수행하는 이행계획을 등록하는 메뉴이다. 취약점 조치권고를 화면 좌측에 불러와 우측에서 조치 제목, 조치방법, 조치 부서 등이 포함된 이행계획을 등록한다. 등록된 이행계획은 다른 조치이행계획과 함께 리스트로 확인 가능하며, DA 취약점 관리를 거시적인 관리가 가능하기에 관리적/운영적 측면에서 효율성을 가져올 수 있다.

Ⅳ. 결론

본 논문에서는 동일한 침해 영향도를 가진 자산 그룹에 개별 점검항목으로 보안성을 평가하고 신규 취약점을 파악하여 단계별 보안조치를 적용하는 프로세스를 제안한다. 이로 인하여, 산업제어시스템 내에 디지털 자산을 도입 시점부터 운영 과정 전반에 걸쳐 프로세스를 적용함으로써 디지털 자산 보안 수준 향상을 기대한다.

Acknowledgement

※ 본 논문은 과학기술정보통신부 정보통신창의인재양성사업의 지원을 통해 수행한 ICT 멘토링 프로젝트 결과물입니다.

참고문헌

[1] 차기종, 노재희, 김기황, 채명은, “원자력발전소 필수디지털자산에 대한 효율적인 보안조치 적용에 관한 연구”, 정보 및 제어 논문집, 271-271, 2017.

[2] 김우년, 이수연. "국외 산업제어시스템 보안기술 연구개발 동향." 정보보호학회지 25.5 (2015): 5-11.