ICS SW 보안 무결성 관리 프로그램 개발

주소영*, 권해나*, 김은지*, 양소영**
*성신여자대학교 융합보안(공)학과
**한국산업기술대학교 컴퓨터공학과
zoocinei@naver.com, ghana97@naver.com, eungimin@naver.com, maysoyoung@gmail.com

Development of an ICS SW Integrity Management System

Soyoung Joo*, Haena Kwon*, Kim EunJi*, Yang So Young**
*Dept. of Convergence Security (Engineering), Sung-Shin Women's University
**Dept. of Computer Engineering, Korea Polytechnic University

요 약

주요기반시설 산업제어시스템의 폐쇄 망 운영 환경에 따라 내부자 사이버 보안 위협으로 인한 피해가 다수 발생하고 있다. 따라서 이에 대응하기 위한 내부 보안 대책이 요구된다. 이에 본 논문은 산업제어시스템의 안전한 운용을 위한 SW 보안 무결성 관리 프로그램을 제안한다. 자산의 구매, 설치, 운영, 유지보수를 통합 관리함으로써 전반적인 라이프 사이클의 흐름 내에서 정보보안 강화를 확립하는 것을 목표로 한다. 이를 통하여 산업제어시스템의 특성을 반영한 효과적인 내부 보안 관리 프로그램으로 활용될 수 있을 것이다.

1. 서론

산업제어시스템(ICS, Industrial Control System)은 국가 주요 기반시설을 모니터링하고 제어하는 시스템으로 구성되어 있으며, 높은 보안성을 요구하고 있어 인터넷 및 기관의 업무망과는 격리된 형태의 폐쇄 망으로 운영된다.[1] 때문에, 외부자 공격보다는 내부자의 고의 또는 의도치 않는 공격으로 인해 발생하는 침해사고 사례가 많다.[2]

하지만 국내의 경우, 제어망과 업무망을 이분화하고 물리적인 대책만을 권고하고 있어 다양한 제어 망 연계에 대한 보안과 제어 망 내부 보안 대책이 추가적으로 필요하다.[3] 내부적으로, 산업제어시스템을 구성하는 디지털 자산의 보안성에 대한 보증이 필요하고 산업제어시스템의 보안성을 보증할 수 있는 보안 평가 절차 및 방법이 필요하다.[4] 따라서, 기술 중심적인 사이버 공격 라이프 사이클을 통합 관점에서 재구성하여 산업제어시스템을 구성하는 디지털 자산에 대한 라이프 사이클 관리가 요구된다.[2]

본 연구는 디지털 자산 라이프 사이클을 관리하기 위한 정보보안 거버넌스 측면의 4 가지 프로세스가 포함된 시스템을 제안하고자 한다. 디지털 자산의 라이프 사이클은 구매, 설치, 운영, 유지보수로 나눠질 수 있으며, 해당 사이클 별로 보안성을 확보하기 위한 프로세스가 필요하다.

본 프로그램의 주요 특징은 크게 네 가지로 구분된다. 첫째, 디지털 자산 구매 프로세스는 기술적 통제 요건 충족, Secure Coding 적용, 신규 취약점 및 악성코드 검사, 무결성 검증 기능 확인 등 V&V 관점의 활동을 수행한다.

둘째, 디지털 자산 설치 프로세스는 자산 별 무결성 유지 대상을 분류하여 무결성 유지 정보 등록 및 자산 관리를 수행한다.

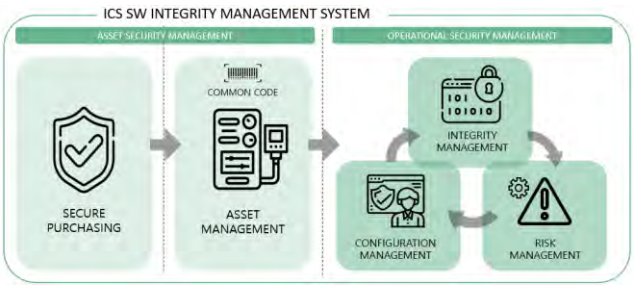
셋째, 디지털 자산 유지보수 프로세스는 자산의 소프트웨어 형상을 통제하기 위해 보안 영향도 측면 작업 검토, 소프트웨어 기능 V&V, 최소 기능성 점검 등 활동을 수행한다.

넷째, 디지털 자산 운영 프로세스는 상시·주기적으로 NEI 08-09 보안통제 항목 기준으로 위험 관리, HW 접근통제 점검, 무결성 유지 점검 관리 활동을 수행한다.

본 논문 2 장에서는 ICS SW 보안 무결성 관리 시스템의 전반적인 프로세스와 시스템 알고리즘을 제시한다. 3 장에서는 이를 기반으로 한 프로그램의 주요 기능과 프로그램 구현 결과를 설명한다. 4 장에서는 프로그램의 기대효과를 기술하며 결론을 짓는다.

1. ICS SW 보안 무결성 관리 시스템

2.1. 서비스 측면의 프로세스 흐름도



(그림 1)ICS SW 보안 무결성 관리 프로세스

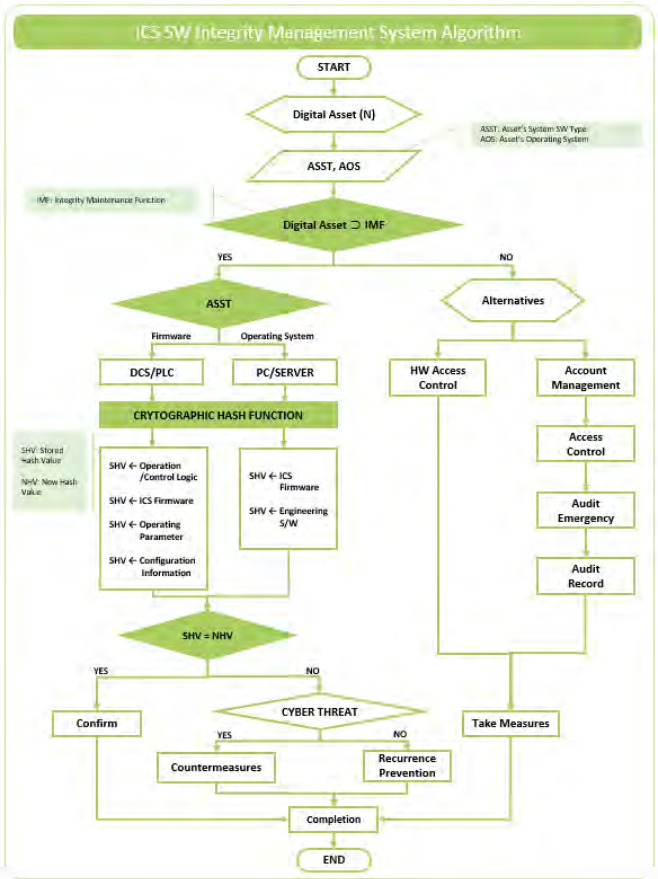
본 논문은 과학기술정보통신부 정보통신창의인재양성사업의 지원을 통해 수행한 ICT 멘토링 프로젝트 결과물입니다.

그림 1 은 본 논문에서 제시하는 ICS SW 보안 무결성 관리 시스템의 프로세스를 나타낸다. 위 프로세스를 기반으로 디지털 자산의 라이프 사이클 전반적인 흐름 내에 보안성을 확보하는 것을 목표로 한다.

서비스 관점에서의 프로세스는 크게 자산 보안 관리(Asset Security Management)와 운영 보안 관리(Operational Security Management)로 나눌 수 있다. 자산 보안 관리에서는 디지털 자산 구매, 디지털 자산 설치를 수행한다. 신규 디지털 자산의 보안 항목을 검사하여 구매 및 반입 프로세스를 진행하고 자산의 무결성 유지 정보를 등록하는 절차를 수행하여 자산을 관리한다.

운영 보안 관리에서는 디지털 자산 유지보수, 디지털 자산 운영을 실시한다. 자산 보안 관리 단계에서 등록한 자산의 무결성 유지 정보를 기반으로 무결성 유지 점검 관리를 정기적으로 실시한다. 또한, 위험관리와 형상 관리를 보안 측면에서 반복적으로 수행 및 관리하여 산업제어시스템 디지털 자산의 지속적인 정보 보안 관리를 가능하게 한다.

2.2. 시스템 측면의 무결성 검증 알고리즘



(그림 2)ICS SW 보안 무결성 관리 시스템 알고리즘

그림 2 는 ICS SW 보안 무결성 관리 프로그램의 디지털 자산에 대한 무결성을 검증하는 시스템 알고리즘을 도식화한 것이다.

프로그램은 크게 3 단계의 보안 무결성 검증 과정을 수행한다. 1 단계, 주요기반시설 환경 內 디지털 자산 정보를 등록한다. 2 단계, 등록한 N 개의 자산을 시스템 SW 타입에 맞게 분류하여 무결성 유지 정보를 해시 값으로 저장한다. 3 단계, 저장된 해시 값과 생성된 해시 값의 비교를 통하여 무결성 점검을 실시한다.

프로그램의 디지털 자산 구매 프로세스를 통하여 반입이 완료된 신규 자산에 대하여 자산의 시스템 SW 타입(ASST, Asset's System SW Type)과 자산의 운영체제(AOS, Asset's Operating System) 정보를 등록한다. 다음으로 등록된 자산이 무결성 유지 기능(IMF, Integrity Maintenance Function)이 있는지 판단하는 과정을 거친다. 자산이 무결성 유지 기능을 지원하고 있다면 무결성 유지 정보 등록 단계로 넘어간다. 자산이 무결성 유지 기능을 지원하지 않을 경우에는 결과가 NO 가 되며 무결성 유지를 위한 대안 조치를 제시한다. 대안 조치에는 물리적인 HW 접근 통제 또는 관리적 통제 조치인 계정 관리, 접근 통제, 감사 대상 비상사건 조치, 감사 기록의 대상 조치를 제시한다. 제안된 대안 조치들을 수행하는 것으로 디지털 자산에 대한 무결성이 지속적으로 유지 및 점검되어야 한다.

무결성 유지 정보 등록 단계에서는 앞서 등록한 자산에 대한 시스템 SW 타입 정보를 확인하여 Firmware 인 경우 DCS/PLC 로 분류하고 Operating System 인 경우 PC/SERVER 로 분류한다. DCS/PLC 로 분류한 자산은 운영/제어로직, 제어시스템 펌웨어, 운영 매개변수, 설정정보를 해시 값으로 저장한다. 이때, 해시 값은 기준 해시 값으로 SHV(Stored Hash Value)로 저장한다. PC/SERVER 로 분류한 자산에 대해서는 운영/제어로직과 엔지니어링 S/W 값을 SHV 로 저장한다.

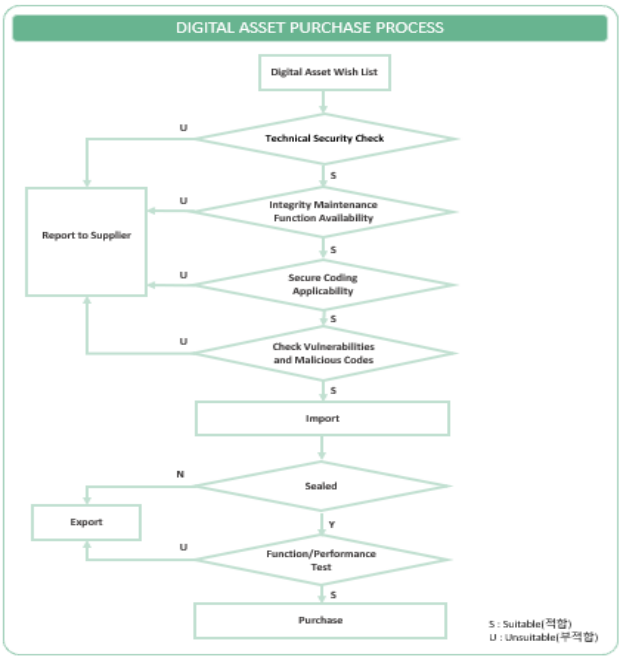
마지막 단계에서는 저장한 SHV 값과 무결성 검증을 위해 새로 생성한 NHV(New Hash Value) 값이 동일한지 비교한다. 비교 결과가 동일할 경우에는 평가결과가 Yes 가 되고 안전한 자산으로 무결성 검증을 완료한다. 해시 값이 동일하지 않을 경우에는 평가결과가 No 가 되고 사이버 공격의 여부를 판단한다. 사이버 공격이 아닐 경우에는 재발 방지 대책 수립 및 이행을 해야 하고 사이버 공격일 경우에는 사이버 공격 대응 조치를 수행한다.

본 무결성 검증 알고리즘은 주요기반시설 內 산업제어시스템의 구성 정보 및 소프트웨어가 정확하고 일관성 있게 유지되는 것을 보증하는 무결성을 정기적으로 검증하여 보안성을 향상시킨다.

3. ICS SW 보안 무결성 관리 프로그램 개발

3.1. 프로그램 주요 기능

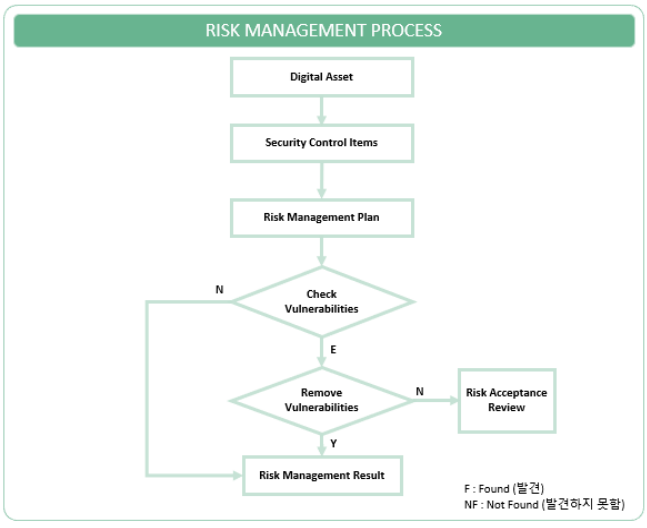
본 절에서는 ICS SW 무결성 관리 프로그램의 주요 핵심 기능인 디지털 자산 구매 기능, 위험 관리 기능, 형상 관리 기능을 살펴본다. 핵심 기능 중 하나인 자산 무결성 유지 점검 기능은 2-2 시스템 측면의 무결성 검증 알고리즘을 통해 기능과 프로세스를 확인할 수 있기 때문에 위 절의 내용으로 대체한다.



(그림 3) 디지털 자산 구매 기능 프로세스

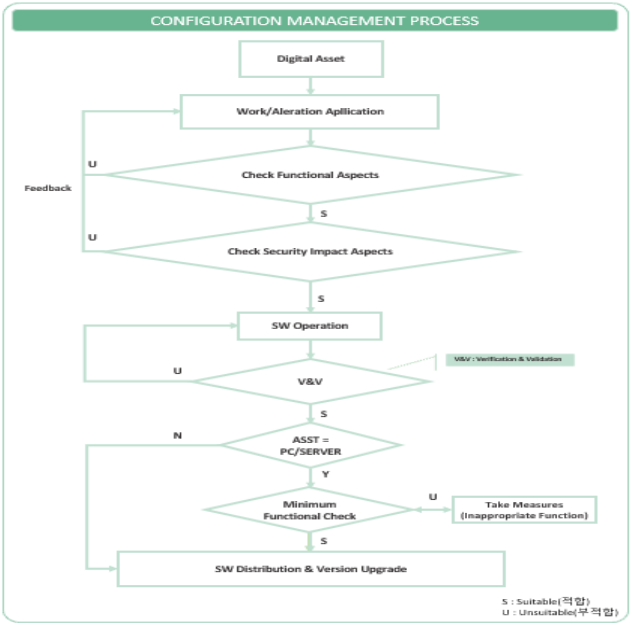
첫 번째 주요 기능은 디지털 자산 구매 기능이다. 그림 3 은 디지털 자산 구매 프로세스(Digital Asset Purchase Process)를 도식화한 것이다. 해당 프로세스는 주요기반시설 환경 내부에 신규 디지털 자산을 반입하기 전, 구매하고자 하는 자산의 보안성 만족 여부를 검토한 후 반입 및 구매를 확정하는 기능이다.

신규 자산에 대하여 일차적으로 검토하는 항목은 기술적 보안 항목, 무결성 유지 기능, Secure Coding, 신규 취약점 및 악성코드 존재 여부이다. 이를 확인하는 보안 점검 절차를 통과해야 봉인된 채로 발전소 내부로 반입된다. 발전소 내부로 반입된 후, 봉인 훼손 여부, 내부적인 기능/성능 시험을 거쳐 적합성을 판단한다. 모든 항목에 대하여 적합하다고 평가된 자산에 한하여 구매를 확정 지을 수 있다.



(그림 4) 위험 관리 기능 프로세스

두 번째 주요 기능은 위험 관리 기능으로 위험 관리 계획에 따라 자산 취약점을 점검하고 사후 조치를 취하는 기능이다. 그림 4 는 프로그램의 위험 관리 프로세스(Risk Management Process)를 도식화한 것이다. 우선, 사전에 등록한 통제 항목을 기반으로 위험 관리 계획을 수립하여 정기적으로 위험 관리를 수행한다. 분기마다 자산 별 취약점 존재 여부를 검사함으로써 자산의 위험도를 수용 가능한 위험 수준(Degree of Assurance)으로 유지한다. 자산에 취약점이 발견되면 취약점을 제거하거나 위험 수용 검토서를 작성하여 위험 발생에 따르는 피해를 최소화하도록 한다. 모든 프로세스를 진행하면 위험 관리 결과를 등록하여 위험 관리 내역을 업데이트 한다.

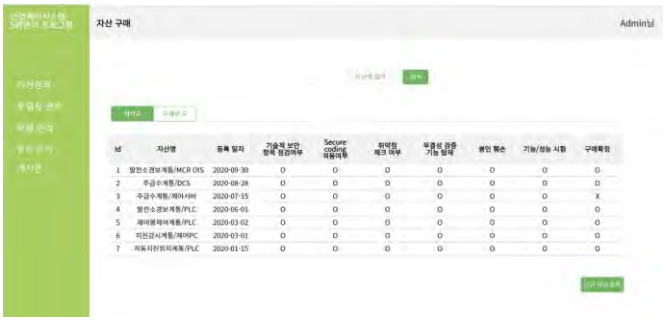


(그림 5) 형상 관리 기능 프로세스

세 번째 주요 기능은 형상 관리 기능이다. 그림 4 는 형상 관리 프로세스(Configuration Management Process)를 나타낸다. 담당자는 프로그램 업데이트, 로직 변경 등의 설비 작업 필요 시 작업신청서를 작성하여 해당 작업을 신청하는 절차를 수행하고, 관리자는 작업의 적합 여부를 기능, 보안 영향도 측면에서 평가한 후 해당 작업을 승인할 수 있다. 승인 완료된 작업에 한하여 SW 기능적 V&V(SW Functional Verification & Validation) 과정을 거치고 최종적으로 SW 업데이트를 진행한다. 예외적으로, 작업 대상 자산이 PC/Server 인 경우에는 최소 기능성 점검을 통과한 후 업데이트 된다.

3.2. 프로그램 구현 결과

본 프로그램은 자산 관리 탭(Asset Management Tab), 무결성 관리 탭(Integrity Management Tab), 위험 관리 탭(Risk Management Tab), 형상 관리 탭, 게시판 탭(Board Tab)으로 구성된다.



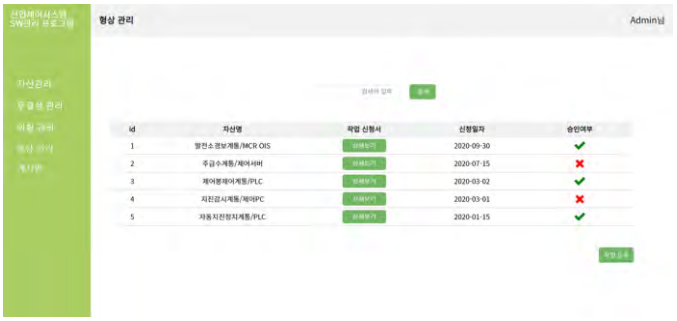
(그림 6) 디지털 자산 구매 기능 구현 결과

그림 6 은 자산 관리 탭의 자산 구매 메뉴이다. 자산 구매 페이지에서는 구입하고자 하는 자산이 위시 리스트(Wish List) 형태로 시간 순으로 목록화 되어 조회할 수 있다. 구매할 자산을 선택하면 해당 자산의 보안 항목을 체크할 수 있는 평가 창이 나타난다. 평가 시 부적합 결과를 받으면 구매를 진행할 수 없도록 경고 창이 뜨고 적합으로 평가를 모두 완료하면 구매 확정으로 표시된다. 구매가 완료된 자산은 자동적으로 자산 관리 탭의 자산 목록으로 추가되어 자산 무결성 관리 메뉴에서 무결성 유지 정보를 등록할 수 있다.

(그림 7) 무결성 유지 점검 기능 구현 결과

그림 7 은 무결성 관리 탭의 무결성 유지 점검 메뉴이다. 해당 페이지에서는 무결성 점검 보고서를 추가함으로써 자산에 대한 보안 무결성 검증을 수행할 수 있다. 앞서 등록한 무결성 유지 정보를 기준 값으로 점검 시점의 생성 값과 비교하는 절차를 진행한다. 점검을 완료하면 자동으로 생성된 보고서에서 점검연도, 점검일자, 점검설비, 담당자, 점검결과 확인이 가능하다.

(그림 8) 위험 관리 기능 구현 결과



(그림 9) 형상 관리 기능 구현 결과

그림 8 은 위험 관리 탭의 위험 관리 메뉴이고, 그림 9 는 형상 관리 탭의 형상 관리 메뉴이다. 위험 관리 탭에서는 통제 항목 등록 메뉴를 통해 통제항목을 등록하고, 위험 관리 메뉴에서 앞서 등록한 통제항목을 활용하여 취약점 점검 및 보고를 할 수 있다. 형상 관리 탭에서는 담당자가 작업 신청서를 작성할 수 있고, 관리자가 작업 신청서 내역을 검토하고 승인할 수 있다. 작업 신청 내역은 테이블 형태로 승인 여부를 직관적으로 확인할 수 있다.

4. 결론

산업제어시스템은 높은 보안성을 유지하기 위하여 폐쇄망으로 운영되어 내부자의 고의 또는 의도치 않는 공격으로 인한 침해사고의 위험성이 높다. 이에 본 논문은 산업제어시스템 내부 보안 대책을 마련하기 위하여 자산의 라이프 사이클 전반에 보안성을 향상시키는 SW 보안 무결성 관리 프로그램을 제안한다. 구매 프로세스부터 무결성 유지, 위험 관리, 형상 관리를 통합적으로 관리함으로써 높은 보안 수준을 유지할 수 있고 정기적인 점검을 통하여 자산의 보안 운영 관리가 가능하다. 또한, 기존의 체크리스트 형식의 보안 평가 절차가 아닌 무결성 검증 알고리즘을 통해 사이버 위협을 신속하게 감지, 조치할 수 있다는 점에서 차별성을 갖는다. 따라서 본 논문은 내부자 위협에 대응할 수 있도록 체계적인 검증 알고리즘을 제시하며 다양한 관리 프로세스를 갖추고 있기 때문에 산업제어시스템 보안성 강화를 기대한다.

참고문헌

[1] 이명신, 현대환, 정대원 “능동공격에 대한 계층방어 시험 및 최적 보안구현 방안”, KNOM Vol.14, 2011

[2] 박형민 “공격 라이프 사이클에 기반한 발전제어시스템 보안강화 방안 연구”, 고려대학교 정보보호대학원 사이버보안학과, 2017

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

[4] 최명길, “제어시스템 보안성 평가 방법에 관한 연구”, 한국정보보호학회, 2013