Korean Chem. Eng. Res., 60(4), 492-498 (2022)
https://doi.org/10.9713/kcer.2022.60.4.492
PISSN 0304-128X, EISSN 2233-9558

공정제어시스템의 사이버보안 위험 노출 현황 및 대응방안 연구

김영세 · 박진형 · 김상기 · 김병직 · 이준원 · 박교식†

숭실대학교 안전보건융합대학원
06978 서울특별시 동작구 상도로 369
(2021년 12월 2일 접수, 2022년 6월 29일 수정본 접수, 2022년 7월 5일 채택)

A Research on the Exposure Status of Cybersecurity Risk of Process Control System and Its Counterplan

Youngse Kim, Jinhyung Park, Sangki Kim, Byungjick Kim, Joonwon Lee and Kyoshik Park†

Department of Safety & Health Convergence Engineering, Soongsil University, 369, Sangdo-ro, Dongjak-gu, Seoul, 06978, Korea
(Received 2 December 2021; Received in revised from 29 June 2022; Accepted 5 July 2022)

요 약

오늘날 대부분의 국내 석유화학 산업에서 사용되고 있는 공정제어시스템은 Windows 플랫폼 기반을 사용하고 있다. 개방형 기술에 따른 위험 노출이 증가하고 있지만, 사이버 공격에 대한 인식 부족과 오해로 인해 각종 사이버 공격에 대비하는 기업이 많지 않다. 본 연구는 석유화학 공정제어시스템이 OT 사이버보안 취약성에 얼마나 노출된 상태에서 운영 중인지를 조사하였으며, 보안 취약점을 감소시킬 수 있는 현실적인 방법을 제시하고자 하였다. 공정제어시스템의 사이버 위협 상태를 확인하기 위하여, 주요 사이버 위협 인자인 Windows 플랫폼에 대한 취약점을 확인하였으며 이를 위하여 국내 주요 3개 DCS 공급자와 635개 시스템의 Windows 플랫폼 단종 여부를 조사하였다. 조사결과 조사 대상의 77.5%가 아직도 이미 단종된 Windows 플랫폼으로 운영 중인 것으로 확인되어 공정제어 시스템이 보안 위협에 취약한 상태로 운영 중인 것으로 확인되었다. 이러한 사이버 위협에 능동적으로 대처하기 위해서는 미국과 같은 선진국에서 시행하고 있는 주요 석유화학 시설에 대한 중요기반시설 지정과 같은 법률적인 규제가 필요할 것으로 판단되며, 기존 DCS 공급자가 제공하는 보안 솔루션을 적극적으로 도입하여 공정제어시스템에 대한 보안 위협을 적극적으로 감소시키려는 노력이 필요한 시점이라고 판단된다.

Abstract − Process control systems used in most domestic petrochemical corporates today are based on the Windows platforms. As technology leans toward opened environment, the exposure risk of control systems is increasing. However, not many companies are preparing for various cyberattacks due to lack of awareness and misunderstanding of cyber intrusion. This study investigated the extent of how much exposed the petrochemical process control system is to security threats and suggested practical measures to reduce OT cybersecurity vulnerabilities. To identify the cyber threat status of process control systems, vulnerabilities of the Windows platform, a principal cyber threat factor, have been analyzed. For research, three major DCS providers in Korea and the discontinuation of Windows platform of 635 control systems were investigated. It was confirmed that 78% of the survey subjects were still operating in the discontinued windows platforms, and those process control systems were operated in a state vulnerable to cyber intrusions. In order to actively cope with these cyber threats, legal regulations such as designation of critical infrastructure for major petrochemical facilities which is implemented in advanced countries such as the United States are needed. Additionally, it is necessary to take the initiative in eradicating security threats to the process control systems by aggressively introducing security solutions provided from existing DCS suppliers. This paper was submitted to Professor Ko JaeWook's retirement anniversary issue.

Key words: OT Cybersecurity, Vulnerability, Windows platform, DCS (Distributed Control System), Critical infrastructure

1. 서 론

1990년대 초반 국내 석유화학산업에 대한 투자가 활성화되면서 컴퓨터 기반의 공정운전을 위한 자동제어시스템이 DCS(Distributed Control System)라는 이름으로 공급되기 시작했다. 1990년도에

†To whom correspondence should be addressed.
E-mail: safetyguy@ssu.ac.kr
‡이 논문은 광운대학교 고재욱 교수님의 정년을 기념하여 투고되었습니다.

Windows 3.0이 발표되었으나 이 시기 대부분의 DCS 공급자들은 자체적인 운영 체제와 하드웨어를 사용하여 시스템을 공급하고 있어 OT(Operational Technology) 영역의 사이버 공격에 대한 인식은 부각되지 않았던 시기였다. 1995년 Windows 95가 출시되고 산업제어시스템 영역 중 공정제어 시스템을 통한 데이터 통합, 분석 및 가공에 대한 필요성이 확대되면서 Windows 기반의 여러 가지 솔루션들이 개발되고 현장에 적용되기 시작했다. 이후 2002년에 Windows XP가 발표되면서 공정제어시스템의 많은 부분이 Windows 기반 솔루션으로 개발되어 현장에 적용됨에 따라 Windows가 가진 취약점을 통한 공정제어시스템의 사이버 공격이 증가하기 시작하였다[1]. 공정제어시스템이 사이버 공격의 주요 대상이 되면서 사이버보안에 대한 대책 마련이 필요하다는 논의가 시작되는 시기였다. 현재 국내 석유화학 산업에서 사용하고 있는 거의 모든 공정제어시스템은 Windows 플랫폼 기반으로 운영되고 있으나 사이버 공격 위험에 대한 인식 부족과 오해로 사이버 공격에 대한 대응책을 마련하고 준비하는 기업이 많지 않아 여러 가지 경로를 통한 사이버 공격 위험에 노출된 상황으로 판단된다. 특히 석유화학산업과 같은 다량의 위험물을 제조하고 취급하는 사업장의 공정제어시스템이 사이버 공격으로 인하여 갑작스러운 운전 불능상태 혹은 감시 불능상태가 될 경우, 이로 인하여 발생할 수 있는 사고는 여러 가지 이며 최악의 경우 사회, 국가적으로 큰 피해가 발생할 수도 있다. 특히 최근 코로나 펜데믹 상황에서 “원격” 혹은 “비대면”이라는 사회현상이 일상화되면서 공정제어 시스템에도 원격 솔루션에 대한 필요성이 요구되어 이와 관련된 솔루션들이 산업현장에 적용되면서 사이버보안 관점에서 또 하나의 큰 위험 요소로 작용하고 있다.

이 연구의 목적은 국내 석유화학산업에서 사용하고 있는 Windows 플랫폼 기반의 공정제어시스템이 사이버 위협에 노출된 정도를 확인하고 그 대책을 제시하려는데 있다. 이를 판단하기 위하여 석유화학 공장의 공정제어시스템으로 사용하고 있는 DCS가 마이크로소프트사에서 현재 패치를 제공하지 않는 단종된 버전에서 운영되고 있는 수량을 파악하였다. 단종된 플랫폼은 취약점이 발견되어도 이를 해결하기 위한 패치를 지원하지 않아 더 많은 사이버 위협에 쉽게 노출될 수밖에 없으며, 점점 지능화되는 사이버 공격 목표가 되어 결국 국가나 사회적으로 큰 피해를 초래할 수 있는 사고로 이어질 수 있는 개연성이 증가하게 된다. DCS system의 cyber 보안 건전성에 가장 많은 영향을 미치는 3가지 요소는

1. Patch와 update를 하지 않아 발생한 취약점(32%)
2. ID와 접근제어 관리 부실로 발생한 취약점 (25%)
3. 망 분리 같은 network architecture 설계 잘못으로 인한 취약점 (11%)으로 조사되었다[1]. 두 번째와 세 번째 요소는 DCS 공급사가 control 할 수 있는 부분이 아니라 기업의 보안 정책에 따라 결정되는 영역이기 때문에 조사할 수 없었다. 보안 건전성에 가장 많은 부분을 차지하고 있는 Windows patch와 update 항목은 모든 DCS system에 공통으로 적용되어 Windows platform을 조사하게 되었다. 본 연구를 통하여 현재 주요 국가중요시설인 석유화학 공정제어시스템들이 취약점에 노출된 정도를 확인하고, 사이버 공격 위험에 적극적으로 대응하여 이로 인한 사고 위험성을 감소시키고, 안전한 공정운전을 확보할 방안을 제시하고자 한다.

2. 연구 대상 및 방법

본 연구는 석유화학 공정제어시스템으로 사용하고 있는 DCS에 적용된 Windows 플랫폼 버전을 조사하는 것으로 시작했다. 현재 DCS에 사용되고 있는 대부분의 공정제어시스템은 Windows 플랫폼을 기반으로 운영되고 있기 때문이다. Windows를 포함한 모든 소프트웨어는 태생적으로 자체적인 버그나 취약점을 갖고 있어 소프트웨어 개발 메이커는 버그나 취약점이 발견될 때마다 문제가 발견된 부분을 수정·보완하여 문제가 해결된 패치를 제작해 주기적으로 사용자에게 제공하고, 사용자는 문제가 해결된 보안 패치를 적용하여 발견된 버그나 취약점을 해결할 수 있게 된다. 사이버보안 위협에 대한 통계치를 확인하기 위하여 국제적인 보안기업이 발간한 보고자료와 마이크로소프트사의 연간 보고서 등을 인용하였으며, 전반적인 사이버보안 관련 기술 경향이나 국제규격의 방향을 확인하기 위하여 국내외 학술논문과 학위논문, 관련 서적 등을 참고하였다. 사이버 위험성 평가 방법에서는, 일반적인 위험성 평가 방법에 추가로 고려해야 할 요인들에 대하여 ‘CCPS guideline for analyzing and managing the security vulnerabilities of fixed chemical sites’에서 제시하는 방법을 소개하였다.

본 연구를 위하여 국내에서 사용 중인 공정제어시스템(DCS) 중 Windows 플랫폼으로 운영되고 있는 635개를 조사하였다. 공정제어시스템에서 사용하는 스테이션과 서버를 중심으로 조사하였고, 마이크로소프트사에서 보안 패치를 지원하지 않는 버전으로 공정을 운전하고 있는 시스템이 어느 정도인지를 파악하였다. 조사된 DCS 시스템은 국내 DCS를 70% 이상 공급하는 3개사의 지원을 받아 조사해서 국내 석유화학 공정에 사용하는 자동제어시스템의 현황을 대표한다고 판단된다. 취득된 정보는 2021년 6월 기준이며, 이후 변경된 내용은 반영하지 않았다.

3. 산업제어시스템에 대한 취약점 선행 연구

산업제어시스템의 정상적인 가동을 위협하는 취약점에 관한 연구는 주로 주요 기반 시설을 보호하기 위한 보호 정책 제도, 관리체계 그리고 동향 분석과 그에 따른 보안대책을 중심으로 이루어지고 있었다.

2014년 김도연의 ‘산업제어시스템의 사이버보안을 위한 취약점 분석’ 논문에서는 산업제어시스템의 취약점의 원인을 정책 및 절차, 플랫폼 그리고 네트워크 부분으로 나누어 각 취약점 대응방안에 대하여 설명하였다[2].

2107년 박미향의 ‘주요기반시설에 대한 주요국 사이버보안 수준 비교·분석’ 연구에서는 ICT 기술의 발달로 주요기반시설 간의 상호의존성이 증가하고 있으나, 기존 연구는 동향조사 및 보호 정책 논의 수준에 머물고 있어 정책의 효율적 추진을 위한 현황 진단 및 적절성 판단의 연구가 필요하다는 것을 주장하였다[3]. 또한 국가별 사이버보안 수준을 측정하는 국제전기통신연합(International Telecommunication Union, ITU)의 세계사이버보안지수(Global Cybersecurity Index, GCI), 소프트웨어연합(Business Software Alliance, BSA)의 사이버보안 대시 보드(Cybersecurity Dashboard, CSD), 그리고 호주전략정책연구소(Australian Strategic Policy Institute, ASPI)의 아·태지역 사이버성숙도(Cybersecurity Maturity in the APAC region, CSM) 등 3가지 지표를 선정하여 주요국과 한국의 현재 주요기반시설의 보호 수준을 비교 및 평가하여 매우 거시적인 측면에서 사이버보안 수준을 연구하였다.

2017년 오형준의 ‘기반 시설 침해사고 및 제어시스템 표준 동향’

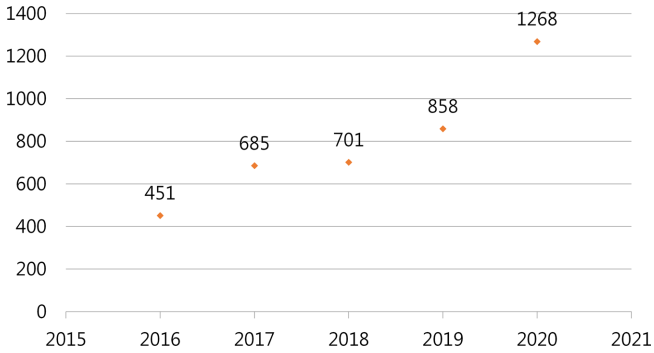

Fig. 1. Total vulnerabilities from 2016 to 2020 [5].

논문에서는 증가하고 있는 기반 시설의 사이버 피해사례와 산업제어시스템 보안에 대한 중요성이 증가하면서 새롭게 만들어지고 개정되고 있는 국내외 보안 표준을 설명하고 있다[4]. 사이버 공격의 경향이나 추세에 따라 지속해서 국제표준이 개정 또는 새로 제정되고 있으나 국내 정보보호 관리체계는 상대적으로 잘 이루어지고 있지 않아 변화하는 사이버 환경에 적합한 정보보호 관리체계가 요구된다는 것을 주장하고 있다.

2018년 이재명의 '산업제어시스템(ICS) 보안 취약점 제거 시 한 계점 사례분석' 논문에서는 보안패치 적용 시 가용성에 영향을 미칠 가능성으로 인하여 현장에서 주기적으로 보안패치를 적용하는 데 어려움이 있으며[1], 향후 가용성에 영향을 미치는 구체적인 인자들을 연구하여 안전한 패치 적용을 할 수 있는 연구가 필요하다고 주장했다. 2021년 마이크로소프트의 취약점 보고서에 따르면 전 세계적으로 3건 중 1건이 patch 되지 않은 취약점으로부터 침해사고가 발생한다고 보고되고 있다[5].

이전 선행 연구를 검토한 결과 산업제어시스템에 대한 취약점이 어디서 발생하고 있는지, 어떤 기준으로 관리하고 평가해야 하는지 그리고 관련 국제표준은 어떠한지 등에 대하여 상당히 다양한 측면에서 연구된 논문이 많았다. 본 논문의 연구 방향은 여러 가지 산업제어시스템 중 석유화학산업에 사용되고 있는 DCS 혹은 PCS(Process Control System)가 이미 단종되어 패치가 지원되지 않은 플랫폼상에서 운전되고 있는 현황을 조사하였다.

이는 선행 연구에서도 언급된 주요 취약점 중의 하나인 플랫폼에 관한 부분에 해당하며, Fig. 1은 지속적인 취약점 증가추세를 나타내고 있다. 본 논문은 현재 석유화학공장을 운전하고 있는 공정제어시스템의 실제 현장 데이터를 기초로 조사한 부분에 의미가 있다고 판단된다.

4. 산업제어시스템에 대한 사이버 공격 피해사례

4-1. 국내 피해사례

1. 전산망 장애[6] - 2017년 발생한 랜섬웨어 워너크라이(Wannacry)는 전 세계 100여 개국에 약 12만 대 이상 피해를 줬다. 국내에서도 2016년 랜섬웨어 피해자만 13만명에 달했으며, 피해 규모도 약 3,000억 원에 달하는 것으로 보고되고 있다. 랜섬웨어는 Windows SMB(Server Message Block) 취약점을 통해 감염되며, 국내 사례의 대부분이 해당 취약점을 통해 감염된 사례다. 국내 석유화학 공장에도 공정 데이터 최적화를 위한 OPC 통신 서버에서 랜섬웨어에 감염되는 사례가 DCS 제조사를 통해 확인되고 있다.

2. 한수원 해킹공격[5] - 2014년 12월, 공격자들은 한국수력원자력 직원들에게 악성코드가 담긴 피싱 메일을 보내 시스템 파괴를 시도하였다. 이 사건은 미리 확보한 원전 관련 자료를 미끼로 협박한 최초의 심리전 형태의 사이버 공격으로 알려져 있다. 특히 이 공격은 북한 해커들이 사용하는 것으로 알려진 킴수키 계열의 악성코드와 유사하여 북한의 소행으로 추정하고 있다.

4-2. 해외 피해사례

1. 사우디 아람코 사이버 공격[7] - 2012년 8월, 세계 최대 규모의 정유 회사인 사우디 아람코의 컴퓨터 3만 5천 대가 감염되어 손상되는 일이 발생하였다. 이것은 샤문(Shamoon) 바이러스의 공격으로 발생했으며 사우디 아람코의 사이버보안 관련 투자는 많이 이루어진 편이었지만 대부분이 생산 시스템에 집중되어 사무 환경 시스템은 상대적으로 취약한 상태였다. 사우디 아람코를 침투했던 악성코드는 아람코 본사에 있던 3만 5천여 대의 컴퓨터 하드 드라이브를 일부 혹은 전부 삭제하는 기능이 있었다.

2. 미국 콜로니얼 파이프라인 중단사태[8] - 콜로니얼 파이프라인의 인프라는 휴스턴에서 텍사스, 뉴저지까지 약 8,800 km에 달하며, 하루에도 수백만 갤런의 석유가 이 파이프라인으로 이동한다. 2021년 5월 7일, 사이버 공격이 콜로니얼 파이프라인으로 침투했고, 이후 모든 인프라가 일시에 마비됐다. FBI는 이것이 다크사이드(DarkSide)라는 랜섬웨어 범죄 집단의 소행이라고 발표했지만, 사건이 더 확대될 것으로 보도되었다.

5. 사이버보안 위협 위험성 분석

Clint Bodungen의 사이버 위험에 대한 정의를 보면 "위험은 위협요인(threat source)이 가진 잠재적 취약점으로 인한 위협인자(threat vector)를 통해 위협 이벤트를 발생시킬 가능성(likelihood)이자, 이에 따라 발생할 결과(consequence)와 영향도(impact) 이다"로 정의하고 있다[9].

산업제어시스템의 사이버 공격에 대한 위험성을 여러 가지 측면에서 분석 연구한 자료가 다양한 연구 기관에서 소개되고 있다. 산업제어시스템이 Windows 플랫폼으로 전환됨에 따라 2010년 이후 보안 취약성이 기하급수적으로 늘어났고, 현재도 보안 취약점을 노리는 해커들의 지속적인 침투 시도가 이루어지고 있다. Fig. 2를 보면 컴퓨터시스템을 산업제어시스템에 적용하기 시작한 초기에는 침입자들의 시스템에 대한 지식이 높았던 반면에 해킹 관련 기술력은 그리 높지 않은 시기였다. 그러나 점차 해킹에 대한 방법이나 기술이 발전하고 일반인들도 관련 기술을 쉽게 접할 수 있게 되면서 해킹에 대한 특별한 지식이 없는 불특정 다수에 의해 쉽게 시도될 수 있는 잠재적인 위험성이 증가하고 있음을 의미한다.

Fig. 3에 조사되었듯이 글로벌 백신 회사 카스퍼스키의 2015년 산업제어 시스템에 대한 보안 취약점이 대부분의 DCS 제조사에서 확인되었으며, 제어시스템이 가진 취약점 유형으로 분류했을 때 Windows 플랫폼이 가진 취약점 부분이 가장 높게 나타났다[1]. 이것은 여러 가지 침투 경로 중 취약한 플랫폼을 통해 침투할 가능성이 매우 크다는 것을 시사한다.

Fig. 3은 산업제어시스템 제조사별 보안 취약점 통계를 나타내고 있으며, 대부분의 제조사가 Windows 플랫폼을 채택하고 있어 비슷한 수준의 high risk level 보안 취약점에 노출되어 있음을 보여주고

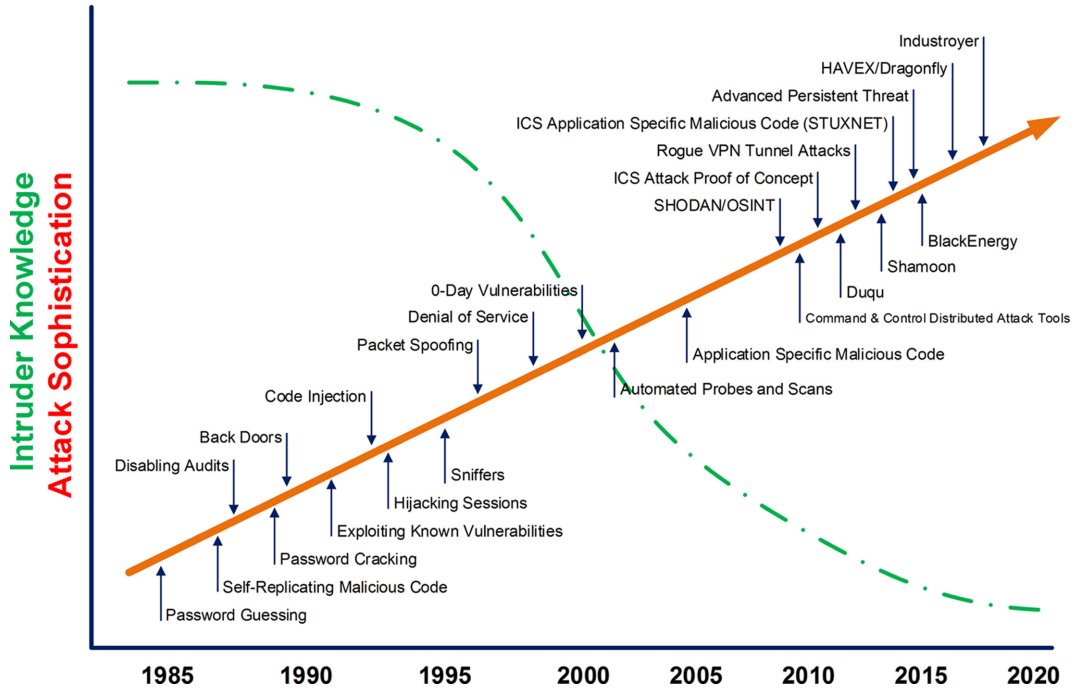

Fig. 2. Attack sophistication vs. intruder technical knowledge [10].

Table 1. The status of vulnerabilities on ICS [1]

High-Critical Risk Category	Rate
Vulnerabilities, Patched and Update	32%
Identity and Access Management	25%
Architecture and Network Segmentation	11%
Encryption and Authentication	8%
Network Management and Monitoring	7%
Insecure Service Enabled	5%
Misconfigurations	5%
Cybersecurity Governance and Best Practices	4%
Others	2%

있다.

Fig. 2에 나타난 바와 같이, 산업제어시스템에 침투할 수 있는 도구와 다양한 기술들이 발달하여 이 분야에 대한 특별한 지식이 없는 사람들도 쉽게 시도해 볼 수 있는 환경이 되면서 Windows 플랫폼으로 운영되는 산업제어시스템은 수많은 공격에 노출되어 있다는 것을 현실로 받아들여야 한다. 공정제어 데이터들이 IT와 결합하면서 기술적으로 IT와 OT의 구분이 모호해지고 있으나, IT와 OT가 중요시하는 보안의 우선순위는 서로 다르다. IT는 개인정보와 같이 기밀이 요구되는 정보를 주로 취급하기 때문에 정보의 3요소인 CIA 즉 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 우선순위로 하고, OT의 경우는 AIC로 24시간 365일 공정의 정상 가동이 보장되어야 하므로 가용성과 무결성 유지를 가장 중요한 목표로 하고 있다.

사이버 위협의 상당 부분을 차지하고 있는 플랫폼에 대한 취약점은 사이버보안 위협에 비교적 적극적으로 대응하고 있는 기업에서도 가용성이 너무 강조된 나머지 현장에서 보안패치의 실제 적용이 쉽지 않아 또 다른 위협요인으로 작용하고 있다[1]. 특히 이와 같은 상황에서 공정제어시스템이 공격을 당하면 다음과 같은 두 가지 종

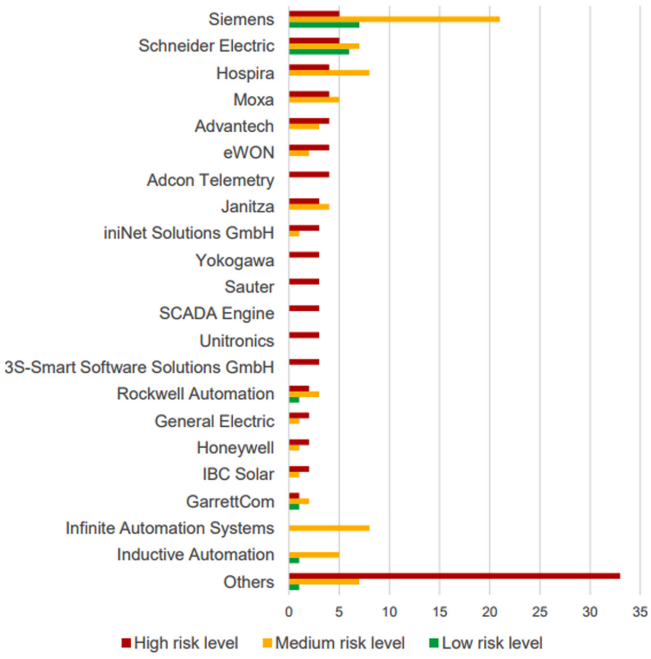

Fig. 3. Industrial control system vulnerability statistics by makers [11].

류의 대표적인 현상이 발생하게 된다. 첫 번째는 Loss of view로 언급되는 감시 불능상태이다. 이 문제는 사이버 공격으로 인하여 공정 운전화면이 갑자기 블랙아웃 되는 경우이며, 운전자들이 공황상태에 빠져 신속하게 적절한 조치를 하기 어려운 상황이 되면서 더 큰 문제로 확대될 가능성이 커진다.

이러한 문제가 발생했을 때 어떤 조치를 해야 하는지에 대한 SOP(Standard Operating Procedure)가 준비된 공정이 많지 않으리라고 판단되며, 이 경우 대부분은 정상적인 공정 shutdown SOP 과정

Table 2. Distribution of windows platform on DCS

Platform	Win XP	Wind 7	Wind 10	Win Server 2003	Win Server 2008	Win Server 2008	Total
No. of Node	727	2157	832	151	388	163	4418
%	16.5%	48.8%	18.8%	3.4%	8.8%	3.7%	

을 거치지 않은 비정상적인 shutdown이 발생하여, 물적인 피해뿐만 아니라 인적, 환경적인 측면에서도 위험한 상황이 발생할 가능성이 커진다.

두 번째는 감시 불능상태인 Loss of view보다 더 심각한 상황을 초래할 수 있는 Loss of control(제어 불능상태) 이다. Loss of control은 공정제어시스템이 사이버 공격으로 공정운전에 대한 통제권을 상실하는 경우이다. 더욱 위험한 요인은 운전자에게 보이는 화면에는 모든 것이 정상으로 나타나지만 실제로는 현장의 모든 조작이 공격자에 의해 조작되는 경우이다.

사이버 공격의 위험성 평가는 시스템의 구체적인 구성 및 설정과 같은 특정 상황에서 잠재적으로 문제가 될 수 있는 모든 것을 탐지하는 것으로 시작한다. 시스템에 대한 단점이나 취약점이 발견되면 문제가 발생할 가능성(possibility)과 발생에 따른 잠재적 영향도를 고려하여 평가할 수 있다. 산업계가 직면하고 있는 보안 위협에 대한 위험성은 다음과 같이 계산될 수 있다.

$$R = L_{AS} \times C \quad (1)$$

- Risk(R) : 자산이 소실되거나 손상이 발생할 가능성
- Likelihood of Successful Attack(L_{AS}) : 공격으로 인한 피해가 발생할 가능성
- Consequence(C) : 시스템에 문제가 발생하거나 손실이 발생할 경우, 발생할 수 있는 재정적인 피해, 기업 이미지 손실, 환경에 대한 잠재적 영향 그리고 직원과 공공의 건강 및 안전과 관련된 위험들을 반영한다.

사이버 공격으로 인한 피해 발생 가능성(L_{AS})은 다음과 같은 추가적인 세 가지 요인에 의해 영향을 받는다

$$L_{AS} = T \times V \times A_T \quad (2)$$

- 위협 인자(Threat, T) : 자산의 손실 혹은 손상을 초래할 가능성이 있는 사람, 증상, 상황 또는 사건 등과 같은 요인
- 취약점(Vulnerabilities, V) : 공격자들이 목적을 달성하기 위해 접근하는 대상물이 가진 약점
- 목표물에 관한 관심도(Target Attractiveness, A_T) : 공격자가 목표로 한 자산으로부터 취득이 예상되는 이익[12]

위험성 평가의 정확도는 가능성 계산에 크게 의존하게 되며, 가능성 산정을 통해서 취약점에 대한 공격으로 이벤트가 될 가능성을 예측할 수 있다.

6. 연구 결과

보안 침해사고의 상당 부분이 Windows 플랫폼이 가진 취약점을 통해서 침투한다는 것이 선행 연구를 통해 확인되었다[1]. 마이크로소프트사에서 발표하고 있는 통계자료에서도 플랫폼이 가진 취약점 발견 건수는 해마다 증가하고 있다[5]. 공정제어시스템이 취약점에 대한 패치가 제공되지 않은 단종된 버전에서 운전된다는 것은 사이버 위협에 거의 무방비 상태로 노출된 것으로 판단된다. 앞에서 소개한 식 (2)에서 공정제어시스템과 같은 관심도가 높은 대상이 가진 취약점(V)이 공격당한다면 결과적으로 식 (1)에서 자산이 소실되거나 CR이 커지게 된다. 마이크로소프트사에서 발간한 2021년 취약점 보고서에 따르면 Windows 10의 적용을 통하여 2020년 발견된 치명적인 취약점 132건의 70%를 완화할 수 있다고 보고하였다[5]. 이 연구는 국내 주요 DCS 공급업체 3곳이 참여하여 현재 Windows platform으로 운전 중인 총 635개의 DCS 시스템에서 사용하고 있는 스테이션과 서버의 버전을 확인하였다. 조사된 635개의 시스템은 국내 주요 석유화학 공장의 공정제어시스템의 70% 이상을 공급하고 있는 주요 3개사의 데이터를 기반으로 하였다.

조사 대상 635개 공정에 설치된 4,418대의 워크스테이션과 서버 중 마이크로소프트사에서 현재 서비스를 제공하는 버전으로 운영 중인 스테이션은 832대로 18.8%이고 서버는 163대로 3.6%로 확인되었다. 2008년 단종된 Windows XP를 사용하고 있는 스테이션은 16.5%, 2020년 1월 단종된 Windows 7을 사용하고 있는 스테이션은 48.8%로 확인되었다. DCS 시스템 중 22.5%만이 마이크로소프트사의 Windows 현재 버전으로 운영 중인 시스템으로 확인되었고, 나머지 77.5%는 아직 단종된 버전에서 운영 중인 것으로 확인되었다. 한국인터넷진흥원(KISA)과 스탯카운터 등에서 2019년 11월 조사한 국내 Windows 사용자 중 Windows 7 사용률은 21.9%였으며, 현재 버전인 Windows 10 사용자는 73.5%로 확인되었다[13]. 이는 산업제어 시스템에서 사용하는 장비에 적용된 Windows 플랫폼에 대한 대응 속도가 상당히 늦음을 알 수 있고, 앞에서 언급한 설비의 가용성 확보를 최우선시하는 기업의 생리와 관련되어 있다.

7. 사이버보안 위협 대응방안

공정제어시스템의 운영체계인 Windows 플랫폼이 가진 취약점 발견 건수가 지속해서 증가하고 있고 취약점을 통한 침투 시도 이외에도 다양한 경로를 통하여 시스템에 침투하려는 시도가 이루어지고 있다. 현재 석유화학산업에 사용되고 있는 거의 모든 공정제어시스템은 Windows 기반으로 운영되고 있어 플랫폼이 가진 취약점을 통한 사이버 공격 가능성은 어느 때 보다 높다고 하겠다. 또한, 코로나 19 환경에서 사회적 거리 두기로 인한 원격 감시 혹은 원격 제어에 대한 필요성이 증가하면서 관련된 솔루션의 등장도 사이버 공격 가능성을 높이는 계기가 되고 있다.

최근 마이크로소프트사에서 발표한 2021 Microsoft 취약점 보고서에서 발표된 결과는(Fig. 4)와 같다. 이에 의하면 Windows 플랫폼에 대한 취약점 건수가 지속해서 증가하였고 2020년에는 907건이 발견되었다. 최근 산업제어 시스템을 사이버 위협으로부터 보호하기 위한 준비 과정이 더 복잡해지고 식별하지 못한 많은 위협 인자들이 매일 발생하는 상황에서, 일회성 위험성 평가의 효율성에 문제의식을 갖기 시작했다. OT 보안 측면에서 대응방안을 구축하는데 어려움을 발생시키는 주요 요인들은 다음과 같다.

첫째 OT 자산에 대한 가시성 확보에 어려움이 있다. 일반적으로

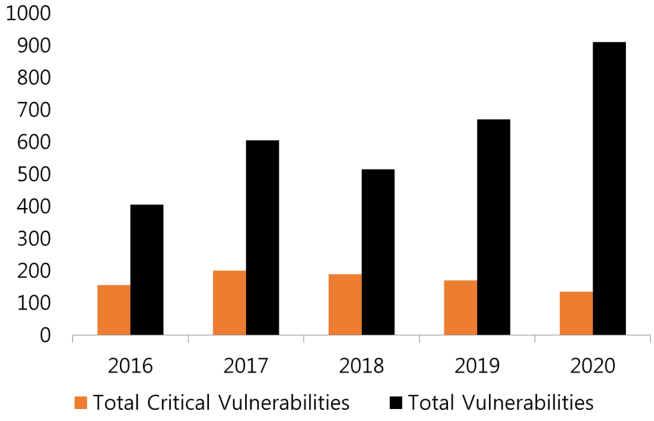

Fig. 4. Microsoft windows vulnerabilities (2016~2020) [5].

공정제어시스템에는 다양한 장비들이 통신으로 연결되어 데이터를 교환하고 그 결과로 목적하는 생산활동이 이루어진다. 석유화학산업의 공정제어시스템 또한 수많은 현장 계기로부터 데이터를 취합하는 서버, 네트워크 스위치, 소형 컨트롤러, 운전자용 스테이션, 히스토리안 및 특별한 목적을 수행하는 장비 등 많은 자산이 서로 연결되어 제품 생산에 사용되고 있다. 현재와 같은 상태에서 생산에 사용되는 자산들이 사이버보안 측면에서 보안 패치가 어디까지 되어 있는지, 어느 장비가 더 취약점에 노출되어 있는지 혹은 통신 부하는 얼마나 되는지 등에 대한 정보를 전체적으로 파악하기가 매우 어렵기 때문이다. 다시 말해서 보이지 않은 자산을 사이버 위협으로부터 보호하기가 매우 어렵다는 의미이다.

둘째 보유 자산에 대한 지속적인 감시가 어렵다. OT 자산에 대한 가시성이 확보되지 않기 때문에 당연하게 겪는 어려움이라 할 수 있겠다. 보안 위협도 마찬가지로 보호해야 할 대상이 보이지 않으면 감시할 수 없고 결국 위험에 처했을 때 적절한 대응을 할 수 없게 된다. 이런 OT 자산을 사이버 위협으로부터 보호하고 대응하기 위해 보안 시스템의 도움을 받는 것이 현실적이다. 대부분의 DCS 메이커들이 이런 문제를 조기에 인식하고 이 부분에 대한 솔루션들을 이미 개발하여 DCS에 접목하고 있다. 시장에서 소개되고 있는 솔루션들은 국제표준기술기구인 NIST에서 제시하고 있는 CSF(cybersecurity framework)의 지침에 따라 개발되고 있다[14].

CFS에서 보여주고 있는 OT 보안에 대한 전체적인 체계는 단계별로 다섯 가지로 구분하고 있으며(Fig. 5), 처음으로 선행돼야 할 조치는 보호해야 할 자산들을 식별하는 단계이다. 이때 보호해야 할 자산에 대한 가시성을 확보해야 한다. 첫 번째 단계에서 보호해야 할 자산들이 결정되고 가시성이 확보되었다면 두 번째 단계에서는 이 자산들을 어떤 방법으로 그리고 어떤 수준까지 보호할 것인지에 대한 정책과 솔루션들이 결정되어야 한다. 이 단계에서 구축된 자산 보호 솔루션을 통해 실질적인 감시 및 감지 활동이 24시간 진행되게 된다.

다음 단계는 구축된 보안 솔루션에 의해 사이버 침해사고가 감지되었을 때 미리 준비된 대응 SOP를 통해 사고로 인한 영향을 최소화할 방안을 모색하고 재발 방지를 위한 보완책을 마련하는 단계이다. 마지막으로 보안 침해사고로 인해 발생한 피해를 복구하는 단계로 얼마나 신속하게 복구할 수 있는지가 매우 중요한 목표가 되고 있다. NIST CSF 단계 중 식별-보호-감지 단계를 통해서는 사전 위협 가능성을 감소시키고, 감지-반응-복구 단계를 통해서 사고에 따른 피해 영향도를 최소화할 수 있게 된다. Fig. 2에 언급되었듯이 사이버 공격자들이 침투할 수 있는 경로가 매우 다양하고 복잡해져, 시스템적인 지원 없이는 공정제어시스템을 사이버 위협으로부터 효과적으로 보호하기는 매우 어렵다고 판단된다. 따라서 이에 대응할 수 있는 방법은 시스템 메이커가 제공하는 보안 솔루션을 도입하여 대응하는 것이 현실적이라고 판단된다. DCS 제조사에서 개발한 보안 솔루션들은 기본적으로 NIST의 cybersecurity framework의 가이드라인을 기준으로 개발되고 있으며 OT 보안 소프트웨어가 갖춰야 할 기능은 다음과 같다. 첫째, 보호해야 할 자산을 인식하고 실시간으로 자산의 상태를 모니터링 할 수 있어야 한다. 둘째, 보호해야 할 자산을 사이버 위협으로 보호하기 위하여 위협 인자에 대한 최신정보를 유지해야 하며, 지속적인 업데이트를 받을 수 있어야 한다. 이 부분에는 추가적으로 통신 부하 혹은 패턴과 같은 정보를 통하여 이상 징후를 파악할 수 있는 기능이 포함될 수 있다. 셋째, 사이버 공격이나 이상 징후가 감지되었을 때 해당 이벤트에 대한 정보를 신속히 리포트하고 경보하는 기능이 포함되어야 한다. 넷째, 사이버 공격으로 인한 침해사고가 발생 되었다면 언제 어떤 경로를 통해 침투되었는지를 식별할 수 있어야 하며 마지막으로 발생한 피해를 신속하게 복구할 수 있는 백업 기능도 포함되는 것이 바람직하다.

Identify (식별)	Protect (보호)	Detect (감지)	Respond (반응)	Recovery (복구)
What processes and assets need protection?	Implement appropriate safeguards to ensure protection of the enterprise's assets	Implement appropriate mechanisms to identify the occurrence of cybersecurity Incident	Develop techniques to contain the impacts of cybersecurity events	Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events
CATEGORY	CATEGORY	CATEGORY	CATEGORY	CATEGORY
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Supply Chain Risk Management	• Identify & Manage Access Control • Awareness and Training • Data Security • Information Protection Processes & Procedures • Maintenance • Protective Technologies	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvement • Communications

Fig. 5. NIST cybersecurity framework chart [14].

8. 결 론

본 연구를 통해서 국내 석유화학산업에서 사용 중인 공정제어시스템의 많은 부분이 사이버보안 위협에 매우 취약한 상태에 놓여 있음이 확인되었다. 석유화학산업의 특성상 공정 가동 중지에 매우 민감할 수밖에 없어 가용성 확보가 최우선시됐지만, 이것으로 인하여 사이버보안 위협으로 인해 더 큰 위험에 처할 수 있다는 인식이 필요한 시기라고 생각된다. 공정제어시스템의 사이버보안 대응에 대한 인식은 아직 초기 단계이나, 일부 기업에서는 이 부분에 대한 심각성을 인식하고 공정제어시스템 메이커들과 전담반을 구성하여 대응방안을 협의하고 공장에 적합한 솔루션을 도입하여 사이버보안 시스템을 구축하기 시작한 것은 긍정적인 변화다.

2010년 개정되어 시행된 '과학기술정보통신부 정보통신 기반 보호법'에 따라 우리나라 정부는 행정, 국방, 치안, 금융, 통신, 운송, 에너지 등 국민에게 공공성격의 서비스를 제공하는 300여 개 기업을 대상으로'주요정보통신기반시설'로 지정하여 관리하고 있다. 이 중 민간기업은 통신과 금융에 해당하는 30개이고 그 외에는 공공서비스를 제공하는 공기업들이다. '주요정보통신기반시설'로 지정된 기업들은 사전 정의된 '정보시스템, 제어시스템, 관리시스템, 정보통신망' 자산과 이와 연계된 내부 시스템과 외부 연계망, 인터넷을 포함한 영역에 대해서 물리적, 관리적, 기술적인 취약점을 매년 분석, 평가하여 해당 결과에 대한 보호 대책을 수립하고 시행하도록 법적으로 강제하고 있다[15]. 이에 대한 상세한 평가 및 실행 방법은 한국인터넷진흥원(KISA)에서 발간하는 '주요정보통신기반시설 취약점 분석 평가 기준'에서 제시하고 있다. 또한, 2021년 4월 새로운 개정안을 공표하여 클라우드, 제어시스템 등 최근 기술변화에 따른 신규 취약점에 대한 분석, 평가 항목을 추가하는 등 새로운 기준을 수립하여, 주요정보통신 기반 시설의 사이버 공격에 대한 대응능력을 강화하고 있다[15].

본 논문의 결론으로 시사하고자 하는 바로는 첫째, 국내 주요 석유화학단지인 울산, 여수 그리고 대산 단지에서 사용 중인 공정제어시스템이 많은 보안 취약점에 노출된 상태로 운전되고 있다는 것이 조사를 통하여 확인되었고, 가용성을 최우선시하는 기업의 특성상 자발적으로 사이버보안에 대한 대책을 추진하는 데는 한계가 있을 것으로 판단된다.

둘째, 국내 화학, 오일, 가스와 같은 시설의 사이버보안에 대한 심각성을 주목하여야 한다. 미국, EU를 비롯한 해외 여러 나라에서 기반 시설 (Critical Infrastructure)'로 지정하여 관리하는 반면 한국에서는 아직 기반 시설로 지정하지 않은 민간 분야의 화학, 에너지, 발전 분야 기업 중 국민안전과 공공에 영향을 미칠 수 있는 주요한 기업들에 대한 '국가 기반 시설' 지정 여부를 신속히 판단하여 실행하여야 할 것이다. 화학, 오일, 가스에 관련된 분야의 사이버안전은 사이버공간에서만 영향을 주는 것이 아니라, 실제 산업현장의 디지털 안전에 지대한 영향을 끼치는 매우 중요한 과제이며, 이러한 인식을 정부와 모든 해당 기업이 공유하고 대응체계를 갖추어 디지털로 변화하는 산업현장을 보호하고 사고를 예방하여야 할 것이다.

셋째, 사이버보안을 강화하기 위한 대책을 준비하는 과정에서 당면하게 되는 기술적인 문제를 해결하기 위한 현실적인 방안은 공정운전에 사용하고 있는 제어시스템 메이커들이 제공하는 솔루션을 통한 자산의 가시성 확보 및 24시간 감시할 수 있는 시스템을 구축하는 것이라고 판단된다.

References

1. Lee, J. M., "Security Vulnerability Management in Industrial Control System (ICS) Environment and Its Limitations; Focus on Security Patching," Master's thesis, Korea University, 1,2,5,19,40(2018).
2. Kim, D. H., "Vulnerability Analysis for Industrail Contrl System Cybersecurity," *Korea Institute of Electronc Commuication Science*, **9**(1), 140(2014).
3. Park, M. H. and Yoo, J. Y., "A Study on Major Counteies's Level of Cybersecurity for Critical Infrastructure," *Korea Institute of Information Decurity & Cryptology*, **27**(1), 165(2017).
4. Oh, H. J., Yoo, Y. I. and, Lee, K. H., "Infrastructure Infringement Accidents and Standard Trend in Control System," *Korea Institute of Information Decurity & Cryptology*, **27**(2), 5,7(2017).
5. Beyond Trust Microsoft – Vulnerabilities – Report, 4,7,12(2021).
6. Korea Inernet & Security Agency https://www.boho.or.kr/data/secNoticeView.do?bulletin_writing_sequence=25705G, (Accessed 06 Sep 2021).
7. Security News on Security World Magazine https://www.boannews.com/media/view.asp?idx=47370,(Accessed 01 Sep 2021).
8. Security News on Security World Magazine https://www.boannews.com/media/view.asp?idx=97355 (Accessed 20 Aug 2021).
9. P. Ackerman, Kim, J. W. and, Lee, D. K., "Industrial Control System Cybersecurity," Acorn Publishing, 207(2021).
10. Howard F. Lipson, Ph. D. "Tracking and Tracing Cyber-Attacks: Techincal Challenges and Global Policy Issues," CERT Coordination Center 24(2002).
11. Kaspersky Lab, Industrial Control System Vulnerabilities Statistics, 12(2015).
12. Center for Chemical Process Safety(CCPS) Guideline for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites (2003).
13. Korea Inernet & Security Agency https://www.boho.or.kr/cyber/window7Finish.do (Accessed 3rd Sep 2021).
14. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 National Institute of Standards Technology. Feb. 2014.
15. Ministry of Science and ICT public notice 2021-28, 2021-103 Partial revision of the criteria for the analysis and evaluation of technical vulnerabilities in major information and communication infrastructure.

Authors

Youngse Kim: Doctor's course, Department of Safety & Health Convergence Engineering, Soongsil University, Seoul 06978, Korea; youngse.kim@honeywell.com

Jinhyung Park: Doctor's course, Department of Safety & Health Convergence Engineering, Soongsil University, Seoul 06978, Korea; jinhyung.park@yokogawa.com

Sangki Kim: Doctor's course, Department of Safety & Health Convergence Engineering, Soongsil University, Seoul 06978, Korea; sangki.kim@se.com

Byungjick Kim: Professor, Department of Safety & Health Convergence Engineering, Soongsil University, Seoul 06978, Korea; bjkim60@naver.com

Joonwon Lee: Professor, Department of Safety & Health Convergence Engineering, Soongsil University, Seoul 06978, Korea; joonwonlee@ssu.ac.kr

Kyoshik Park: Professor, Department of Safety & Health Convergence Engineering, Soongsil University, Seoul 06978, Korea; safetyguy@ssu.ac.kr