Journal of Korea Society of Industrial Information Systems Vol.29 No.4, Aug. 2024 :43-54
http://dx.doi.org/10.9723/jksiis.2024.29.4.043 ISSN:1229-3741

스마트팩토리 환경의 사이버보안 리스크 관리 체계 연구

(Research on Cybersecurity Risk Management System in Smart Factory Environment)

신 영 선[1)*]
(YoungSun Shin)

요 약 본 연구는 스마트팩토리 환경에서의 사이버 보안 리스크 관리 체계를 제시하였다. 스마트팩토리는 제조업에서 인공지능, 빅데이터, 사물인터넷(IoT), 자동화 등 첨단 기술을 활용하여 생산 시스템을 최적화하고 효율성을 높이는 공장을 의미한다. 이러한 기술들은 생산 프로세스를 자동화하고 데이터를 실시간으로 수집하여 분석하므로, 생산 과정에서의 결함을 빠르게 감지하고 조치할 수 있다. 그러나 이러한 디지털화된 환경은 사이버 공격에 취약하며, 생산 시스템의 중단이나 정보 유출로 인한 심각한 피해를 입을 수 있어 사이버 보안 리스크를 효과적으로 관리하는 체계적인 접근 방식이 필수적으로 요구된다. 본 연구에서는 비즈니스 프로세스 기반 보안 위험 평가와 더불어 스마트팩토리 환경에서의 사이버 보안 리스크 관리체계를 제안하였다. 이러한 연구들은 스마트팩토리의 사이버 보안 리스크 관리를 더욱 향상시키는 데 도움이 될 것이다. 또한 스마트팩토리가 안전하고 효율적으로 운영될 수 있도록 하는 데 중요한 역할을 할 것이다.

핵심주제어: 스마트팩토리, 보안리스크, 사이버 보안, 보안위험평가

Abstract This study presented a cybersecurity risk management system in a smart factory environment. A smart factory refers to a factory that optimizes the production system and increases efficiency. However, this digitized environment is vulnerable to cyber attacks, and manufacturing companies can suffer serious damage from disruptions in production systems or information leaks. Therefore, a systematic approach to effectively managing cyber security risks is essential in smart factories. In this study, a continuous security risk management system for each stage of the smart factory was proposed along with business process-based security risk assessment. These studies will help to further improve cybersecurity risk management in smart factories. It will also play an important role in ensuring that smart factories operate safely and efficiently.

Keywords: Smart Factory, Security Risk, Cybersecurity, Security Risk Assement

1. 서 론

최근 4차 산업의 발전으로 제조업 분야에서는

* Corresponding Author: pr20058@koje.ac.kr
Manuscript received May 20, 2024 / revised June 03, 2024 / accepted July 23, 2024
1) 거제대학교 기계공학과, 제1저자, 교신저자

인공지능, 빅데이터, 사물인터넷 등의 첨단 기술을 적용한 스마트팩토리 환경을 기반으로 생산 시스템이 활발히 도입되고 있다. 특히 제조업 분야에서는 스마트팩토리의 등장으로 효율성과 생산성을 크게 향상시킬 수 있지만, 기존의 제조산업이 비즈니스 시스템과 통합되고 개방형 환경으로 변화됨에 따라 사이버 공격, 개인정보 유출 등 정보보안 문제가 개인 사생활 침해뿐만 아니라 국가 안전을 위협하는 요인으로 작용하고 있어 보안 위협에 대한 보안대책 연구가 이루어지고 있다(Kim and Park, 2022).

Son(2023)이 제시한 디지털전환 환경에서의 사이버 보안 위협 분석에 관한 논문에 따르면 지난해 사이버안보와 디지털 보안 기술의 혁신 전략 포럼에서 실제로 전년대비 전 세계 사이버 공격은 38% 증가하였고, 국내에서는 사이버 공격이 49%로 지속해서 늘고 있으며, 주요 산업 분야별 디지털 전환 확대로 S/W 및 시스템 복잡성이 증가하고 AI 도입 확산 등에 따른 신기술 위험이 크게 늘어났다고 분석하였다. 이와 관련하여 한국과학기술기획평가원에서 2023년 국내 사이버 공격 및 침해사고 발생 현황을 Fig. 1과 같이 나타내고 있다. 국내 사이버 공격은 2022년 대비 2023년도에 49%가 증가하였고, 사이버공격 침해사고 국내발생 현황을 보면 악성코드 감염 32%, 중요정보유출 29%, 피싱/스캠이 20% 차지하고 있다.

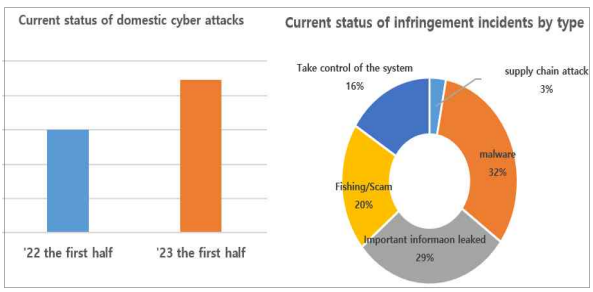

Fig. 1 Current Status of Domestic Cyber Attacks and Breaches

지금까지는 산업자동화, 인공지능 기술을 도입하기 위해 기술적인 부분에 대한 보안 대책을 강구하였다. 그러나 스마트팩토리 환경의 이동성과 즉각적인 가용성, 확장성, 복잡성과 다양성을 고려할 때, 기존 위험평가 프로세스에 대한 구조적인 평가 방법론의 변화와 새로운 보안 리스크 관리체계가 필요하다. 이러한 이유로 스마트팩토리 환경에서 보안 리스크를 최소화하기 위한 구조적인 관리체계 변화의 필요성에 대한 연구가 다양하게 이루어지고 있다(Lee, 2015). 특히 제조설비와 주요 사회기반 시설의 디지털 의존도가 심화됨에 따라 스마트팩토리 환경에서의 사이버 보안에 대한 필요성과 보안 리스크를 효과적으로 관리하는 것이 절대적으로 필요하다는 인식이 증가하고 있다.

Bae and Goh(2019)의 스마트팩토리 도입 기업의 보안강화 사례 연구에 따르면 인공지능, 클라우드 등의 혁신 기술을 제조업에 도입하여 운영하는 스마트팩토리 환경에서는 기존의 물리적, 관리적 측면의 보안 정책 및 기술 적용 뿐 아니라 지속적으로 변화하는 환경을 바탕으로 신기술이 내포하고 있는 위협요인들에 지속적으로 노출되는 문제를 해결하기 위한 보안강화 방안을 제시하고 있다.

현재의 사이버 보안 환경은 매우 동적이고 복잡하여 전통적인 자산 중심의 위험 평가 방식만으로는 새로운 위협에 대응하기에 부족하다. 사이버 공격의 특성과 그로 인한 결과가 산업 분야마다 다르게 나타나고, 네트워크 취약성 및 직원 과실 등 예측할 수 없는 위험 요소가 존재하기 때문에 완전한 가시성을 기업이 확보하는 경우가 없다. 그럼에도 불구하고 지금까지의 위험평가는 자산을 중심으로 위협을 도출하고 위험평가 후 평가 결과에 따른 획일적인 보안대책 수립 방식을 적용하고 있다 (Lee, 2018; Kim and Shon, 2019). 따라서 높은 가용성이 요구되는 스마트팩토리 환경에서는 산업 자동화를 계획하는 단계에서부터 업무별 프로세스 과정에서의 보안 리스크 관리를 위한 보안 관리체계를 함께 수립하고 시스템을 구축해나가야 할 필요성이 있다.

즉, 스마트팩토리 제조 환경의 변화와 AI를 기반으로 한 시스템들의 운용데이터 등 디지털 전환으로 발생되는 다양한 데이터를 효과적으로 관리하고, 업무 프로세스 상에서 발생할 수 있는 위협 식별, 위험성 평가 및 대책 수립을 위한 체

계적인 보안 리스크 관리체계를 구축해야 한다. 이와 더불어 기존의 위험성 평가를 넘어서 역동적으로 변화하는 스마트팩토리 환경에 적시에 대응하기 위한 상시 보안리스크 관리체계를 구축하고, 다양한 업무 환경에서 발생하는 위협을 사전에 예방하고 적절히 대응할 필요가 있다.

본 논문에서는 기존의 보안 위험 평가 프로세스를 분석하고 지속적인 사이버보안 강화를 위해 스마트팩토리 환경에서의 업무별 취약점을 점검하고 업무 프로세스상의 위협 식별방안, 위험성 평가를 바탕으로 보안 대책을 수립하도록 하는 적극적이고 효과적인 보안 활동을 제공하기 위한 스마트팩토리 환경에서의 사이버보안 리스크 관리체계를 제안한다.

2. 관련연구

2.1 국내 사이버보안 대응에 관한 연구

국가사이버위협에 따른 국방사이버대응실태 연구에 따르면 국가적인 사이버 위협이 지속되는 상황에서 국방차원에서의 사이버 대응실태를 조사 분석하고 국방정보화를 촉진하기 위해 거버넌스 체계를 도입하고 체계적이고 전사적 차원의 국방 정보화를 추진해 나가고 있다. 하지만 국방정보화로 인해 사이버 보안 리스크의 가능성이 증가됨에 따라 국방 사이버 보안 대책의 발전도 함께 이루어져야 하는데 지금까지는 국방정보화가 이루어진 다음에 보안 대책을 수립 및 적용하고 있는 실정이다. 따라서 정보기술 의존도가 높아짐에 따라 국방정보화 과정에서 사이버 보안대책을 함께 수립하고 시스템을 구축해 나갈 필요가 있다. 국방정보화의 발전에 따라 위협 발생 빈도가 증가함으로써 이에 대한 연구가 진행되고 있으며, Choi(2012)의 국가사이버위협에 따른 국방사이버대응 실태 연구에서 국가적인 사이버위협이 지속되는 상황하에서 국방차원의 사이버대응 실태와 발전책을 제시하고 있다.

이와 더불어 중소기업의 사이버 보안 강화를 위한 연구가 이루어지고 있다. 중소기업은 보안인력 및 보안 기술이 부족하고 필요성 인식 부재 등 보안관리 체계가 부실한 중소기업의 경우 작은 보안 사고가 해당 기업과 연계된 모기업 및 동종 업체에까지 큰 영향을 미칠 수 있고, 특히 제조업의 경우 많은 중소업체들이 연관되어 있어 보안에 취약한 부분이 많다 Shin(2024).

Min(2014)의 중소기업의 보안 활동이 사이버 침해사고 대응에 미치는 영향에 대한 연구에서 사이버 침해사고에 유연하게 대응하기 위한 대응체계 구축 방안을 제시하고 있으며, 자산관리, IT관리 프로세스, 시스템 관리 프로세스에 관한 대응체계 구축을 제안하고 있다. Bae(2019)의 스마트팩토리 도입 기업의 보안강화 연구에서는 스마트팩토리 보안 관련 기업 실무 사례 분석과 해외 표준과 국내 표준에 대한 비교 분석 연구를 수행하였으며, You(2021)의 스마트팩토리 환경에 적합한 정보보안 정책 방향성에 대한 연구에서는 국내외 주요 스마트공장 보안 표준을 기반으로 주요 보안 특성을 변별하고 스마트공장 보안 평가 항목을 도출함으로써 보안 정책의 방향성을 제시하여 본 논문에서는 스마트공장의 보안관리 고도화를 위한 방안을 참고하였다.

2.2 국내외 취약점 분석 및 위험평가 정책 연구

가. 국내 취약점 분석·평가에 관한 기준 고시

주기적인 취약점 분석·평가는 새로운 사이버 보안 위협에 신속하게 대응하고 지속적으로 보안을 강화하는 중요한 활동으로 수행 주체에 따라 다양한 방식과 절차를 가지고 수행된다. 정보통신기반보호법(법률 제11690)에 의거 주요정보통신기반시설에 대해서 주기적으로 취약점 분석·평가를 수행하고, 이에 대한 보호대책을 수립하도록 하고 있다. 동법 제9조 4항은 '취약점 분석·평가에 관한 기준'을 정하여 고시토록 하고 있으며, 동법 시행령 제18조 4항에는 고시되는 해당 기준은 취약점 분석·평가의 절차, 범위 및 항목, 평가방법을 포함하도록 하고 있다.

취약점 분석·평가 기준은 계획 수립, 평가 대상 선별하는 현황분석, 취약점 분석, 취약점 보호대책 수립의 4단계 절차를 제시하고 관리적, 물리적, 기술적 취약점 분석을 수행토록 하고

있으며, 대부분의 취약점 분석·평가시 적용되고 있다(Kang, 2021). 하지만 고시된 취약점 분석 기준 항목은 사이버보안 위협 변화에 대한 점검은 가능하나 사이버 보안 위협 변화에 따른 취약점 분석 절차의 세부적 제시가 부족하고, 자산 중심의 분석 평가가 이루어져 업무 프로세스에서 발생되는 여러 가지 변화되는 환경을 고려한 취약점을 식별하고 분석 및 평가를 하기에는 부족하다.

나. 국외 취약점 분석 및 위험평가 정책 연구

미국은 미국 연방 정보 보안 관리법(FISMA, Federal Information System Management Act)을 제정하고, 정부기관의 정보시스템에 대하여 매년 취약점 분석 · 평가를 수행하고 보호계획을 작성하고 있다. FISMA의 목표는 정보보안 수준을 향상시키고 사이버공격으로부터 보호하기 위한 기관들이 적절한 보안 프레임워크를 구현하도록 가이드라인을 제시하고 있다. 또한 제어시스템에 대한 보안 위협 증가로 미 NIST는 2011년 제어시스템 보안을 위한 프레임워크와 보안항목을 제시한 NIST SP80－82(Guide to Industrial Control System(ICS) Security)를 발표하고 2013년 이를 다시 개정하여 NIST SP800-82 Rev.1를 발표하였다(Lee, 2017). NIST SP800-82는 ICS의 보안 강화를 위해 위험관리 프레임워크와 관리, 운영, 기술적 측면의 보안 항목을 제시하고 있다.

Jin(2021)의 IEC 62443 표준 적용을 통한 산업제어 시스템 보안성 강화 연구에서는 SME (Small and Medium sized Enterprise) 환경의 스마트공장 보안 내재화를 이루기 위해 보안 프로세스 정립 및 보안 요구사항과 보안 요구사항에 적합한 개발 방법론의 도입의 필요성에 대해서 강조하고 있다. 또한 ISO/IEC 27001은 정보보안 관리 시스템(Information Security Management System, ISMS)을 위한 국제 표준으로, 정보자산을 보호하기 위한 위험 관리 절차를 제시하고 있으며, ISO/IEC 31000(Risk Management-Principles and Guidelines)은 조직 전반의 위험관리 프레임웍을 토대로 기록 관리의 위험관리 요소와 대응 전략을 제시하고 있다(Kim, 2015).

다. ISO/IEC 31000 리스크 관리 가이드라인 분석

ISO/IEC 31000은 보편적인 보안관리 프레임워크 및 가이드라인을 제시함으로써 다양한 산업 분야에 조직의 특성을 고려하여 보안관리 프레임워크 및 위험관리 체계를 수립하기 위한 기준을 제시하고 있다. 제조산업의 경우 디지털 전환 환경에서 자산의 식별과 분류를 위한 체계 및 접근 방식 미흡, 스마트팩토리화로 인한 생산 라인의 복잡성과 변동성으로 인해 리스크 평가 및 모니터링이 쉽지 않다. 또한 스마트팩토리 특성상 실시간으로 운영되고 연결되어 있는 장비들, IT장비와의 연동에 따른 사이버 공간상에 발생되는 위협들을 고려하지 않는 등 변화되는 환경에 상시 적용가능한 적절한 보안 조치를 취하지 않은 채로 시스템을 운영하고 있어, 중요한 제어 시스템에 대한 취약점이 노출되어 있다. Lee(2015)와 Lee(2017)는 실제 스마트팩토리 환경에서 ISO/IEC 27001 및 ISO/IEC 31000을 충족하지 못하는 사례를 연구하였는데, 이러한 사례들은 ISO/IEC 27001 및 ISO/IEC 31000 표준의 적용이 스마트팩토리에서 어려움을 겪고 있음을 보여준다.

본 논문에는 사이버 보안리스크 관리체계를 제안하기 위한 ISO/IEC 31000의 가이드라인에서 제시하는 위험관리 프로세스를 바탕으로 위협 식별 방안, 분석, 평가, 처리 방안에 대해 스마트팩토리 환경의 특성을 고려한 보안 리스크 관리체계를 제안하고자 하였다. 이를 위해 Kim (2015)이 제안한 ISO/IEC 31000과 ISO/IEC 27001에 기반한 위험관리시스템의 방법론 연구에서 제시한 내용을 분석하였고, 위의 표준에서 제시하는 요구사항을 실제 운영 환경에 맞게 유연하게 적용하기 위한 보안 리스크 관리체계를 연구하였다.

ISO/IEC 31000은 리스크 경영의 원칙과 가이드라인을 제시한 위험관리를 위한 표준으로 리스크 관리를 어떻게 하면 좀 더 효율적으로 다룰 수 있는가에 대한 표준을 제공하고 있다. 어떤 특정 산업분야를 위해 개발된 것은 아니고, 포괄적 리스크 관리를 다루고 있는 있으며, 전략수립, 의사결정, 운영, 프로세스, 프로젝트, 자

산 등과 같은 다양하고 넓은 분야에 적용이 가능하다. 또한 ISO/IEC 31000에서 제시하고 있는 리스크 관리 프로세스는 리스크와 연관하여 조직을 지휘하고 관리하기 위한 조직적인 활동을 말하는 것으로 효과적인 위험관리를 위해 범용적으로 적용가능하며 스마트팩토리 환경에서의 사이버 보안 리스크 관리체계를 구축하는데 중요한 역할을 한다. ISO/IEC 31000에서는 위험도(Risk)를 특정한 위험요인이 사고를 일으킬 가능성(빈도)와 사고결과의 중대성(손실크기)를 조합하여 위험요소를 정량화한 위험의 크기 또는 정도를 위험도라고 정의하고 있다. 본 논문에서는 이를 바탕으로 업무 수행시 발생할 수 있는 보안 위협들이 보안사고에 끼치는 영향도와 위험발생가능도에 대한 기준을 제시하였다.

Fig. 2는 ISO/IEC 31000에서 제시하는 리스크 관리 프로세스이다. Fig. 2에서 보는바와 같이 해당 표준에는 리스크 관리를 위해 상황설정, 리스크 식별, 분석, 평가, 처리 단계로 구성하고 이를 모니터링 및 검토하고 있는 프로세스를 제공하고 있다.

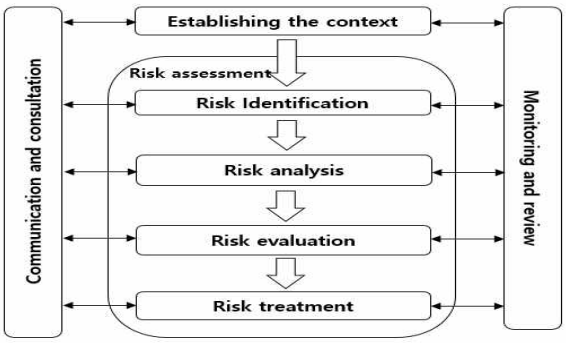

Fig. 2 ISO 31000 Risk Management Process

리스크 관리 프로세스에서는 각 단계별 보편적 가이드라인을 제시하고 있으며, 이를 바탕으로 조직의 특성에 맞게 위험도를 평가하기 위한 프로세스를 수립할 수 있다.

첫 번째 단계는 상황설정 단계로 조직의 목표 달성에 영향을 미치는 외부 및 내부 환경에 따른 상황을 설정하여 내부/외부 이슈를 바탕으로 리스크 관리 프로세스를 기획하고 리스크 평가 방법을 결정하도록 제안하고 있다. 두 번째 단계는 리스크 식별단계로 포괄적인 리스크의 리스트를 작성하는 단계이다. 조직의 모든 리스크 식별하고 모든 심각한 원인과 결과를 모두 고려하여, 조직의 목표와 능력에 적합한 리스크를 식별하는 수단과 기술을 적용하고 관련된 정보의 최신화를 통한 효과적인 리스크 식별하도록 한다. 이때 적절한 지식을 가진 인원이 리스크의 식별에 참여를 하도록 제안하고 있다. 세 번째 단계는 리스크 분석 단계로 위험발생 발생결과가 미치는 영향(심각도) 및 발생가능성에 따라 위험도를 분석하고 위험 요소별 영향 및 발생가능성을 정량화하도록 제시하고 있다. 네 번째 단계는 리스크 평가 단계로 리스크 분석 결과를 바탕으로 조치가 필요한 리스크를 위험평가 기준에 따라 도출하고 보안 조치의 우선순위 결정를 지원하도록 하고 있다. 리스크 분석을 통해 식별된 리스크 수준을 리스크 평가 기준과 비교하여 조치의 필요성을 결정하는데 법적, 규제적 및 기타 요구 사항등에 따라 이루어져야 하며 리스크 평가 기준에 따른 리스크 수준의 비교 및 조치의 우선순위 결정한다. 마지막으로 리스크 처리 단계에서는 적절한 리스크 조치 옵션의 결정은 비용과 법적, 규제적 요구사항 및 기타 요구사항의 충족간의 균형을 고려하여 이루어지도록 제안하고 있다.

본 논문에서는 ISO/IEC 31000의 리스크 관리 프로세스 가이드라인에서 제시한 위험식별, 분석, 평가, 처리 단계의 내용을 참고하여, 스마트팩토리의 특성을 고려하고 환경에 적용 가능한 보안 리스크 관리체계 연구의 필요성과 사이버 보안 리스크 관리체계를 제안하였다.

2.3 일반적 위험평가 모델과의 차이점

일반적인 위험평가 모델은 조직의 중요 자산을 보호하기 위한 대책 수립을 목표로 자산별 취약점을 분석하고 정기적인 점검을 통해 보안 리스크를 감소시키기 위한 대책을 수립하고 있다(Kim, 2019; Jeon, 2024).

하지만 물리적 취약점 외에 네트워크망 연동, 인공지능 기술 도입 등으로 인해 산업 전반에 시공간을 초월한 새로운 보안 위협들이 발생함

에 따라 전통적인 보안위험 평가 방법론은 새로운 사이버보안 위협 변화에 대응하기 어려워지고 있다. 또한 내부 사용자 영역에서도 외부로부터의 침입경로가 형성될 수 있음을 인식하고, 내외부의 다양한 위험에 대한 분석이 필요하며, 지속적이고 전방위적이며, 입체적인 관리 프레임워크가 필요하다. 특히 스마트팩토리와 같은 산업 환경에서는 보안 목적 우선순위가 IT시스템과는 다르게 가용성이 중시되고 있어, 중요 인프라를 모니터링 및 제어하는 시스템 운용에 영향을 최소화하는 보안 리스크 관리체계가 만들어져야 한다. 이유로는 시스템 정지에 따른 여파는 단순 불편을 넘어, 막대한 물리적 파급효과로 이어지기 때문이다 (Hwang, 2021; Kim and Park, 2022). Fig. 3은 기존의 위험평가 방법과 제안하는 보안 리스크 관리체계 방법의 차이점을 제시한 그림이다.

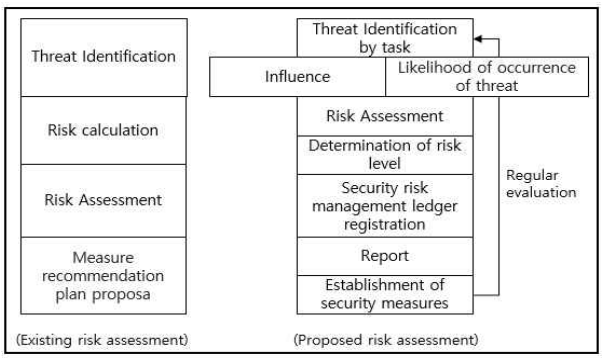

Fig. 3 Proposed Risk Assessment Model

기존의 위험평가 방법은 자산을 기반으로 위협을 식별하고 위험 평가를 통해 보안 대책을 수립하는 단계로 이루어진다. 본 논문에서 제시한 위험평가 모델은 업무 수행 과정 중에 발생할 수 있는 위협들을 식별하고, 보안성 수준에 영향을 주는 정도를 평가하고 수용할 수 있는 위험과 그렇지 않은 위험을 구분한 후 보안 대책을 수립할 수 있는 보안 리스크 관리체계를 제안하였다. 또한 스마트팩토리 환경의 특성을 고려해 정기적 위험 평가 외에 상시적으로 보안 리스크를 관리하기 위한 방안을 제시하였다. 이를 위해 Kim(2018)의 위협 분석 및 리스크 평가를 위한 종속 공격 문석 모델에서 보 안 위험 수준을 결정하는 심각도, 공격 가능성, 제어 가능성의 정의와 분류 단계를 참조하였다.

3. 스마트팩토리 환경의 사이버보안 리스크 관리체계 구축 방안

3.1 사이버보안 리스크 관리체계 모델

스마트팩토리에서의 업무 프로세스는 다양한 IoT 기기와 센서, 로봇 등의 자동화 장비가 연동되어 생산라인을 구성하고 데이터를 실시간으로 수집하고 분석하여 생산량을 최적화하는데 중요한 역할을 한다. 이러한 프로세스는 동시에 사이버보안의 취약점을 내포할 수 있는데 생산라인에 연결된 IoT 기기나 센서는 외부 공격자에 의해 해킹될 수 있으며, 데이터 전송 과정에서의 암호화 문제, 생산 프로세스에 대한 권한 부여 및 제어에 대한 문제는 생산 프로세스의 중단이나 오작동으로 이어질 수 있다. 따라서 업무를 수행하는 과정에서 발생되는 보안 위협들을 분석하기 위한 대책이 필요하다.

Fig. 4는 본 논문에서 제시한 사이버보안 리스크 관리체계 모델이다.

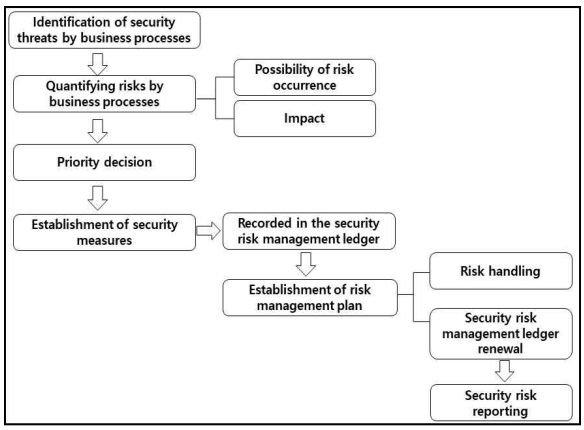

Fig. 4 Cyber Security Risk Assessment Model

업무별 공정라인의 각 단계별 위험도를 산정하고, 우선순위에 따른 대책 수립 마련과 보안 리스크 목록 관리, 위험처리 내용 및 결과, 보고

체계에 대한 전반적인 프로세스를 진행하기 위해 보안 리스크 평가 모델을 도식화 하였다.

Fig. 4에서 제안한 모델의 프로세스를 살펴보면 첫 번째 단계로 3.1에서 설명한 것과 같이 업무 프로세스상 보안 위협 식별과 조직을 대상으로 주기적인 보안 이슈를 식별한다. 두 번째 단계로 식별된 보안 위협에 대하여 현업팀 담당자 및 보안 리스크 담당자의 협의와 보안 리스크 평가가 필요하다. 위험성 평가는 위험발생가능도와 영향도를 기준으로 평가하고 우선순위를 정한 후 보안대책을 마련할 수 있다. 세 번째로 위험평가 결과를 보안 리스크 관리 대장에 기록되고, 네 번째로는 평가결과를 토대로 위험관리 계획이 수립되어야 한다. 위험관리 계획은 보안 리스크를 다루는데 있어서 필수적으로 수립되어야 하며, 이에 따라 상시 위험 평가 및 처리, 보안 리스크 관리대장을 갱신해야 한다. 마지막으로 경영진에게 보안 리스크 관리 활동에 대한 보고가 필요하다.

본 논문에서 제안한 모델과 기존의 보안 위험 평가 모델과의 차이점으로는 자산 중심의 보안 위험 평가가 아닌 스마트팩토리 환경의 특성을 고려하여 업무 프로세스 단계별 보안 위협을 식별한다는 점이다.

3.2 업무 프로세스별 보안 리스크 식별

가. 업무 프로세스별 위협 식별

업무 프로세스 상의 보안 위협을 식별하기 위해서는 스마트팩토리 환경에서의 공정라인의 각 구성 요소의 취약점과 데이터 흐름을 면밀히 살펴보고, 외부로부터의 공격이나 내부적인 오류로 인해 발생할 수 있는 위협들을 업무 담당자 및 팀별로 위협을 식별하고 새로운 위협이 발생할 경우 수정 관리하기 위한 위협에 대한 목록화가 필요하다.

Table 1은 업무 프로세스 상에서의 위협을 식별하기 위해 다섯가지 방안을 제시하였으며, 업무 담당자 및 보안담당자의 인터뷰와 체크리스트 활용, 보안 인력풀 활용 방안에 대해 제시하였다.

Table 1 Identify Security Threats in Business Processes

No	Security Threat Identification Method
1	Interview with business personnel and security personnel
2	Constructing a security risk pool
3	Periodic security inspection activities by field teams
4	List security risks by business team
5	Periodic addition and deletion of security risks

현업 부서 보안담당자에 의한 업무 프로세스 분석을 통해 팀 업무에 대한 전문성을 확보하고 발생 가능한 보안 위협을 식별한다. 또한 주기적인 점검활동을 통해 분석한 리스크 요인을 목록화하고, 업무 담당자들이 업무 수행 조건과 상황에 맞는 실무 사례들을 지속적이고 주기적으로 추가, 삭제함으로써 현실성을 높이고, 위험관리 항목을 꾸준히 개선하기 위해 리스크를 분류하고 핵심 리스크 지표를 설정하여 관리하여야 한다. 또한 보안 리크스와 관련한 전문성이 부족한 부분은 보안 리스크풀 등의 제공을 통해 해소할 수 있는 방안이 필요하다.

나. 보안 이슈 식별

기업내 정기적/상시적 주요 보안 관리 활동을 통해 식별된 보안 이슈를 체계적으로 관리하여야 한다. 주요 보안 관리 활동은 보안성 검토, 보안 점검, 주요 회의/협의 등으로 이뤄지는데 이러한 활동들은 스마트팩토리의 다양한 부문에서 진행되며, 보안 이슈를 식별하는데 중요한 역할을 한다.

보안 이슈는 단순히 기술적인 측면뿐만 아니라 조직문화, 정책 및 절차, 외부 환경 변화 등 다양한 요소에서 발생할 수 있다. 따라서 보안성 검토나 보안 점검뿐만 아니라 조직 내의 다양한 활동과 프로세스에서도 보안 이슈를 발견하고 보안 이슈별 목록화 및 갱신 대장을 갖추어야 한다.

3.3 사이버보안 리스크 평가 및 처리

보안 리스크 평가를 위해 업무 프로세스별 보안 위협과 정기적/상시적 보안 이슈들을 평가 기준에 따라 위협의 정도를 산출하고 보안 리스크를 산정한다. 스마트팩토리 환경에서의 보안 리스크 평가는 전체적인 생산 과정을 고려하여 이루어져야 하며,각 구성요소와 데이터 흐름을 종합적으로 분석하고, 보안 취약점을 최소화하기 위한 방안을 마련해야 한다. 이를 통해 업무별 안전성을 보장할 수 있으며, 사이버 보안 위협으로부터 생산 시스템을 보호할 수 있다.

보안 리스크 평가 기준은 해당 업무가 위협에 노출되었을 때 기업에 미치는 영향도(Impact)와 위험발생가능도(Likelihood)를 기준으로 평가하도록 제시하였다. 영향도와 위험발생가능도를 평가하기 위한 기준에 대한 정의로 기업의 특성에 맞게 3단계에서 5단계로 구분하여 나타낼 수 있으며, 본 논문에서는 ISO/IEC 31000을 기준으로 3단계로 구분하였다.

Table 2는 업무가 위협에 노출되었을 때의 영향도를 확인하기 위한 평가 기준을 정의한 표로 업무의 특성을 고려하고 기업에 미치는 중요도와 피해손실규모 정도를 평가하는 항목으로 구성하였다.

Table 2 Impact Evaluation Criteria

Impact		
Import-ance	1	Not significantly related to major services
	2	Other major services and related tasks, services, information, assets
	3	Tasks and services, information, assets, etc. related to core business
Damage loss	1	Little or no loss in case of problems
	2	When problems arise, they can result in financial and reputational losses
	3	causing significant financial and reputational damage

중요도와 피해손실규모의 1단계는 업무의 중요도와 업무 수행 중 위협이 발생하여도 피해규모가 거의 없는 정도를 말하고 3단계를 업무의 중요도가 높고 문제 발생시 막대한 손실을 초래할 수 있는 단계로 정의하였다.

Table 3은 위험발생가능성을 도출하기 위한 평가 기준 정의로 취약성과 위험노출정도로 구성하였다.

Table 3 Risk Occurrence Probability Assessment Criteria

Possibility of Risk Occurrence		
vulner ability	1	No security controls at all
	2	Security controls exist, but are applied/enforced in specific cases
	3	Security controls exist, are applied, and are being enforced.
Degree of risk exposure	1	Cases that may occur in some tasks throughout the organization
	2	Cases that can occur in most tasks throughout the organization
	3	Cases that can occur throughout the entire organization

취약성과 위험노출 1단계는 관련 보안통제 및 제약 사항이 전여 없고 해당 위험이 극히 일부 서비스에만 영향을 주는 단계를 말하며, 3단계는 관련 보안 통제 및 제약사항이 존재하며, 해당 위험이 조직의 전체 서비스 및 업무에 모두 발생한 경우로 정의하였다.

Fig. 5는 영향도와 위험발생가능도를 도출하기 위한 매트릭스이다.

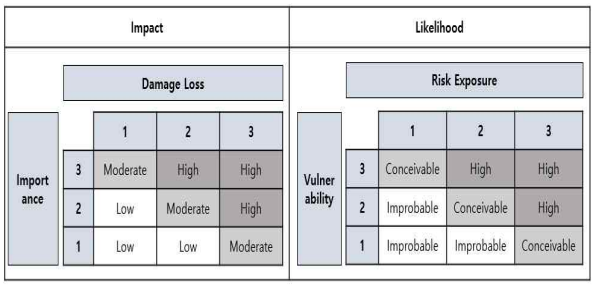

Fig. 5 Impact and Likelihood Assessment Criteria

Table 2에서 제시한 기준을 바탕으로 업무별

중요도와 피해손실규모 값을 측정하고 영향도를 측정하기 위한 평가 기준 매트릭스에 적용하여 High, Moderate, Low의 3가지 측정값 중 한 개의 값을 도출한다. High의 경우 위협으로 인해 기업에 미치는 영향정도가 높은 경우이고, Low의 경우 위험은 발생하지만 기업의 업무에 크게 영향을 끼치지 않는 정도를 말한다.

또한 Table 3에서 제시한 기준을 바탕으로 취약성과 위험노출정도를 측정한 값을 위험발생가능도를 측정하기 위한 매트릭스에 적용하여 High, Conceivable, Improbable 중 한 개의 값을 도출한다. 위험발생가능도가 높은 경우 High의 값을, 위험이 발생할 가능성이 적은 경우는 Conceivable 또는 Improbable의 값을 도출한다. 즉, 업무의 중요도가 높고 위협으로 인한 피해손실규모가 클수록, 업무별 취약성이 높고 위험노출정도가 높은 단계의 경우 High 수준의 위험평가 결과를 도출하게 된다. 이후 수용 가능한 위험 수준을 판단하기 위해 위험도 산정 및 수용 가능한 위험수준을 결정한다.

Fig. 6은 앞에서 도출한 영향도와 위험 발생가능도 결과를 이용하여 위험도를 산정하고 수용 가능한 위험 수준을 결정하는데, 위험도는 High, Medium, Low 3단계의 수준으로 측정한다. 위험도 산정 결과 값을 바탕으로 위험처리 방안을 수립할지, 수용 가능한 위험수준인지를 판단한다.

		Likelihood of occurrence		
		Frequent	Conceivable	Improbable
Influence	High	High	High	Medium
	Moderate	Medium	Medium	Low
	Low	Medium	Low	Low

Fig. 6 Risk Calculation and Acceptable Risk Level Decision Table

Fig. 6에서 보는바와 같이 영향도와 위험발생가능도가 높을수록 위험도는 높고, 낮을수록 위험도가 낮도록 위험도 산정표를 제시하였다. 위험도 산정 결과를 바탕으로 위험수준에 대한 위험처리방안을 수립할지, 수용 가능한 위험수준인지를 판단하기 위해 Fig. 7과 같이 평가표를 제시하였다.

위험수용수준은 위험분석 결과 나타난 정보보호관리체계 범위 내의 정보자산별 위험에 대해 수용 가능한 위험도의 수준을 결정하는 것을 말하는 것으로 본 논문에서는 위험수용수준을 위험에 대한 별도 조치는 취하지 않으며, 지속적인 '잔여위험' 모니터링을 실시하는 내용으로 정의하였다.

	Impact	Likelihood	Risk
Risk handling plan establish	High	Frequent	High
	High	Conceivable	High
	High	Improbable	Medium
	Moderate	Frequent	Medium
	Moderate	Conceivable	Medium
	Low	Frequent	Medium
Acceptable risk level	Moderate	Improbable	Low
	Low	Conceivable	Low
	Low	Improbable	Low

Fig. 7 Estimating Risk and Determining Acceptable Risk Levels

3.4 보안 리스크 평가 결과 관리

보안 리스크 평가 결과는 보안 리스크 관리대장에 기록되고, 이를 토대로 위험관리 계획이 수립되어야 한다. 위험관리계획은 보안 리스크를 다루는데 있어서 필수적으로 수립되고 주기적으로 관리대장을 갱신해야 한다.

먼저, 스마트팩토리 운용 장비 및 시스템은 보안 리스크의 상태와 추이를 실시간으로 모니터링하고, 보안 이벤트와 위험 평가 결과 등의 데이터가 시각화되도록 대시보드 형태로 작성되어야 한다. 또한 보안 위협의 세부 내용, 조치 계획, 조치 결과 등을 기록하고 경영진에게 적시에 보고되어야 한다. 또한, 보고서 작성시 경영진이 신속하게 이해하고 결정을 내릴 수 있도록 간결하고 명확하게 작성되어야 하며, 주요 보안 이슈와 대응 조치, 이로 인한 영향 등을 명확히 기술해야 한다. 이러한 절차를 통해 보안 리스크 관리 체계를 통해 스마트팩토리 환경에서의 보안 리스크를 효과적으로 관리하고 경영진에게 적절한 레포트를 제공해야 한다.

3.5 상시 보안 리스크 평가 체계 구축

스마트팩토리에서의 상시 보안 리스크 평가는 지속적으로 변화하는 사이버보안 위협에 대응하기 위한 핵심적인 활동이다. 따라서 스스로 보안 리스크를 예방, 관리하기 위한 통합적 접근으로 스마트팩토리 환경에서 리스크를 관리하기 위한 상시 보안 리스크 평가 체계를 구축하고 리스크 관리 활동을 스스로 이행해야할 필요가 있다. 즉, 기존의 IT정보시스템 보안 위험 평가와 업무 프로세스 기반 보안 위험 평가를 포함하여 정기적 또는 상시 위험평가를 보완하는 방안으로 수립되어야 하며 기업에 미치는 영향도와 위험발생가능도를 기준으로 위험도를 평가하여 실제 보안 리스크에 대한 상시 관리가 가능하도록 해야 한다. Table 4는 상시 보안리스크 평가 관리 체계를 제안한 것으로, 기존의 위험분석에 추가적으로 상시 보안 리스크를 정량적으로 평가해야 함을 제시하였다.

Table 4 Permanent Security Risk Assessment System Model

Division	Description
Constant security review	Self-security check External security check/screening Major meetings and regular consultations
Security Issue discrimination	Includes issues identified from key security-related activities
Security Risk assessment	Security risk assessment through consultation between security manager and security risk manager Mainly evaluated based on probability of occurrence and impact
Security Risk management ledgerregistration	Describe security risk details, action plan, action results, person in charge, etc. Reporting to management on security risk management activities is required.

상시 보안 리스크 평가를 위한 방안은 다음과 같다. 첫 번째, 자동화된 시스템을 통해 생산라인의 모든 보안 관련 이슈가 시스템에 기록되어야 한다. 이상 징후를 탐지하는 센서 네트워크나 로그 분석 시스템을 활용하여 보안 이벤트를 실시간으로 감지하고 기록하고 담당자에게 알림을 통해 보고되고 내·외부 보안 점검이 이루어져야 한다.

두 번째, 상시 뿐 아니라 정기적인 위험 평가를 위해 스마트팩토리의 보안 리스크를 주기적으로 평가해야 한다. 이 과정에서는 보안업무 담당자와 보안 리스크 담당자간의 협의를 통해 생산 시스템의 취약점과 위협을 식별한다. 위험평가는 전문가들에 의해 시행되어야 하며, 업무별 영향도와 위험발생가능도를 기반으로 표준화된 평가 도구 및 방법론이 활용될 수 있다.

세 번째로, 보안 리스크 내용 및 조치 계획, 조치 결과 등이 보안 리스크 관리 대장에 등록되어야 한다. 또한 보안 대책 수립은 위험 관리의 핵심 요소로 평가 결과를 바탕으로 수립하고 실행하는 것은 중요하다. 이 과정에서 생산 시스템의 운영에 불필요한 중단을 최소화하기 기업의 특성을 고려해 적절한 계획 및 우선순위를 설정해야 한다. 마지막으로 경영진 요약보고서를 통해 핵심 보안 리스크에 대한 요약과 상세한 내용을 제공하여 의사 결정에 적극적으로 기여할 수 있도록 함으로써 보안 업그레이드나 추가 보안 투자 등의 의사 결정을 지원하기 위한 리스크 대응 전략의 효율성을 높이기 위한 권고사항도 제공되어야 한다.

4. 결 론

본 논문에서는 스마트팩토리 환경의 사이버 보안 리스크 관리 체계를 연구하였다. 스마트팩토리 환경에서는 기업의 업무가 자동화되고 네트워크로 연결되는 등 IT와 OT 환경의 결합으로 폐쇄적이었던 작업환경이 개방됨에 따라 다양한 위협이 새롭게 발생되고 있다. 하지만 기존의 위험평가 및 관리 방법은 정기적인 보안 위협 점검 및 대책 수립 등 정적인 대응방식으

로 시시각각 동적으로 변화하는 스마트팩토리 환경에서 지속적이고 상시적인 관리 및 대응을 하기에는 다소 무리가 있다. 따라서 스마트팩토리 환경에서 사이버보안 리스크를 효과적으로 관리하기 위한 체계적인 접근 방식이 필요하다.

본 논문에서는 ISO/IEC 31000의 리스크 관리 프로세스에서 제시한 위험관리체계 수립을 위한 가이드라인을 기반으로 스마트팩토리의 특성을 고려한 사이버보안 관리체계를 제안하였다.

특히 기존의 자산 중심의 위험평가 방법론을 기반으로 상시로 변화하는 스마트팩토리 환경에서 업무 수행 과정을 중심으로 한 보안 리스크 관리체계 모델을 연구하였다.

첫째, 기업의 자산 중심의 위험관리가 아닌 업무 프로세스 진행 중 발생되는 보안 위협을 업무 담당자와 보안 담당자를 통해 업무별로 식별하고, 기업에 보안 이슈를 상시 또는 정기적으로 식별해야 함을 제시하였다.

둘째, 업무별로 식별된 위협이 기업 운영에 심각한 영향을 끼치는 정도와 위험발생가능도의 기준과 정의를 제시하고 업무별로 영향도와 위험발생가능도를 측정하도록 하였다.

셋째, 영향도와 위험발생가능도 측정 값을 기반으로 위험도를 평가한 후 보안대책 우선순위를 정한다.

넷째, 위험도 평가 결과가 기업의 특성을 고려하여 허용 가능한 위험인지 그렇지 않은지를 판단하고 대책을 수립하고 경영자의 의사결정에 도움을 줄 수 있도록 상시 보고체계를 갖추도록 한다.

또한 보안 리스크 평가 과정은 정기적/상시적으로 수행되어야 하며, 업무 수행과정중에 발생되는 새로운 보안 위협, 보안 이슈에 대해 목록화 하고 수정, 갱신하는 체계가 갖추어져야 한다. 따라서 제안한 보안 리스크 관리체계를 통해 다양한 위협에 노출되어 있는 스마트팩토리 환경에서 업무 수행과정 중 생산 시스템의 안정성을 보다 유지시키고 지속적이고 상시적으며, 적극적인 보안대책을 수립할 수 있다.

본 연구의 한계점으로는 제조산업의 디지털화가 가속되면서 많은 보안 위협들이 발생하고 있지만 산업 분야의 다양성과 기업의 규모등을 고려할 때 보안 리스크 감소를 위한 관리체계 적용이 다소 어려울 수 있어 중소기업을 대상으로 한 국가 차원의 지원이 필요하다고 생각된다.

향후 연구 방향으로는 본 논문에서 제안한 보안 리스크 관리 체계의 효과성 평가에 대한 연구가 필요하며 이를 위해, 스마트팩토리 보안 요구사항 항목을 구체화 하고, 실제 스마트팩토리 환경에 적용하여, 그 결과를 분석하는 연구가 필요하다.

References

Bae, C. S. and Goh, S. C. (2019). Case Study on Security Enhancement of Smart Factory, *Korea Institute of Information Security & Cryptology*, 29(3), 675-684.

Choi, G. B. (2012). Status of Defense Cyber Response According to National Cyber Threats, *Journal of Korea Institute of Information Security & Cryptology*, 22(8), 36-40.

Hwang, I. H. (2021). The Influence of Security Motivation and Organization Trust on Information Security Compliance : Focusing on Moderation Effects of Work Promotion Focus, *Journal of Korea Society of Industrial Information Systems*, 26(3). 23-39.

Jeon, G. H. and Kim, K. S. (2024). Study on Method to Develop Case-based Security Threat Scenario for Cybersecurity Training in ICS Environment, *Journal of Platform Technology*, 12(1), 91-105.

Jin, J. H. and Kim, J. T. (2021). A Study on the Security Enhancement of the Industrial Control System through the Application of IEC62443 Standards, *Journal of Korea Information Processing Society*, 28(2), 280-283.

Kang, D. Y. (2021). Analysis of Threat Information Priorities for Effective Security

Monitoring & Control, *Journal of Korea Society of Industrial Information Systems*, 26(5), 69-77.

Kim, D. I. (2015). *Aphased Strategy for Application of the Risk Management System based on ISO 31000 in the Domestic Construction Companies*, Dissertation, Graduate School of Korea University, Seoul, Korea.

Kim, E. J. and Park, I. C. (2023). The Impact of SMEs' Security Activities on Cyber Incident Response. *Korean Journal of Industry Security*, 13(1), 7-28.

Kim, E. Y. (2015). Cyber Security Risk Analysis and Response Strategy Research in Smart Factories, *Journal of Information Security Society*, 25(1), 89-97.

Kim, G. Y. (2018). *Dependent Attacks Anaylsis for Threat Analysis and Risk Assessment (TARA)*, Thesis, Graduate School of Hanyang University, Seoul, Korea.

Kim, H. J., Kim, S. J., Kim, Y. S., Kim, S. K. and Shon, T. H. (2019). Cybersecurity Architecture for Reliable Smart Factory, *Journal of The Korea Institute of Information Security & Cryptololgy*, 29(3), 629-643.

Kim, Y. S. and Park, J. H. (2022). A Research on the Exposure Status of Cybersecurity Risk of Process Control System and Its Counterplan, *The Korean Institute of Chemical Engineers*, 60(4), 492-498.

Kim, W. N. and Park, E. K. (2019). Current Control System Security Evaluation System Trend, *Journal of Information Security*, 29(2), 5-11.

Lee, H. S. (2015). Research on Smart Factory Security Threat Response Measures, *Journal of Information Security Society,* 25(4), 305-313.

Lee, J. M. (2018). *Security Vulnerability Management in Industrial Control System (ICS) Environment and Its Limitations; Focus on Security Patching*, Thesis, Graduate School of Korea University, Seoul, Korea.

Min, B. G. (2014). Vulnerability Analysis Plan According to Changes in Cybersecurity Threats, *Korea Institute of Information Security & Cryptology*, 24(1), 7-12.

Shin, Y. S. (2024). A Study on the Establishment of Security Areas and Guidelines for Small and Medium Manufacturing Enterprises in the DX Process Environment, *Journal of Industrial Technology Research*, 29(2), 29-37.

Son, B. J. (2023). *Trend Analysis on Cybersecurity in the Era of Digital Transformation: Policy Implications,* Dissertation, Graduate School of Seoul Venture University, Seoul, Korea.

You, K. S. (2019). *Smart Factory Information Security Policy Directional Suggestions*, Thesis, Graduate School of Ajou University, Suwon, Korea.

신 영 선 (YoungSun Shin)

- 정회원
- 대전대학교 컴퓨터공학과 공학사
- 대전대학교 컴퓨터공학과 공학석사
- 대전대학교 컴퓨터공학과 공학박사
- (현재) 거제대학교 기계공학과 초빙교수
- 관심분야 : 정보보안, 보안평가, 정보보안정책