

기본 정보

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern,
Germany
Deutschland/Germany
www.pilz.com

2026년 7월
1 / 9페이지

자동화 네트워크의 “구역 및 통로”: 보안으로 안전을 지키다.

안전이 최우선입니다

Ostfildern, 2026년 7월 – 기계류 규정(Machinery Regulation, MR)에서는 안전 관련 기능의 무단 조작을 방지하는 방식으로 산업 보안을 설계해야 한다고 의무적으로 규정합니다. 즉, 보안은 안전 기능이 제대로 작동하는 데 필요한 사전 조건입니다. 하지만 자동화 네트워크에 대한 총체적인 보호는 어떻게 달성할 수 있을까요? IEC 62443-3-2 및 곧 제정될 EN 50742와 같은 규격들은 시스템을 구역으로 구분하고 연결 통로를 모니터링해야 한다는 명확한 방향을 제시하고 있으며, 이는 업계 단체와 전문가들이 현재 제시하는 권고 사항 전반에 걸쳐 적용되는 원칙입니다. 필츠는 안전을 이룬바 표준 자동화로부터 엄격하게 분리하는 것이 효과적인 기계류 안전의 핵심이라고 확신합니다. 이는 '심층적 방어'(Defence-in-Depth) 원칙에 기반을 두고 구역 및 통로 접근법을 활용해 구현할 수 있습니다.

집은 튼튼하고 안전하게 지을 수 있습니다. 견고한 벽, 난연성 자재, 신뢰할 수 있는 전기 설비, 그리고 제대로 작동하는 경보 장치를

갖추면 됩니다. 이러한 구조적 안전성은 기계류 안전의 대표적인 사례로, 설계 조치, 센서 기술 및 보호 장치를 통해 의도하지 않은 위험을 예방하도록 되어 있습니다. 하지만 그런 집은 고의적인 간섭이 없을 때에만 안전할 수 있습니다. 난방 제어 장치의 조작, 전기 회로의 고의적 손상, 또는 경보 시스템의 무력화는 안전을 고려하여 설계된 건물조차 위험 요소로 변모시킬 수 있습니다. 기계류 분야에서는 안전 관련 부품이 무단으로 조작되거나 무력화될 경우, 아무리 뛰어난 안전성 설계라도 그 효과를 발휘하지 못하게 됩니다.

이러한 맥락에서 보안은 외부로부터 보호해주는 역할을 담당합니다. 견고한 문, 안전한 출입 지점, 감시받는 연결 통로, 그리고 무단 침입을 막는 장벽 등이 이에 해당합니다. 따라서 보안은 사고 자체를 막아주는 것이 아니라, 예를 들어 무단 작동 모드 선택이나 조작을 통해 접근 권한을 얻은 개인에 의해 보호 메커니즘이 무력화되는 것을 방지합니다. 안전을 확실하게 유지하는 유일한 방법은 바로 ‘보안을 통한 안전’(Security for Safety)입니다.

규제 요건부터 해결책 제안까지

‘기계류 규정 (EU) 2023/1230’은 최초로 보안을 공장 및 기계류의 안전 기능에 있어 필수 요건으로 규정하고 있습니다. 즉, 안전 기능은

의도적이든 아니든 간에 어떠한 무단 조작으로도 훼손되어서는 안 됩니다. 바로 이 지점에서 새롭게 제정될 EN 50742 규격이 역할을 하게 됩니다. 이 규격은 기계류 규정(MR)의 핵심적인 보안 요구사항을 명확히 하는 데 도움을 줄 것입니다. 이 규격은 부정 행위로부터 보호하기 위한 기술적 세부 사항을 규정하며, 안전 관련 기능에 영향을 미칠 수 있는 하드웨어, 소프트웨어 및 데이터에 대한 명확한 요구사항을 제시합니다. 이 규격은 개발 단계부터 운영 및 해체 단계까지 전체 라이프사이클을 다룹니다. 산업 자동화 및 제어 시스템의 사이버 보안을 위한 체계적인 접근 방식을 제시하는 기존의 IEC 62443 규격 시리즈 또한 중요한 역할을 담당합니다. 이 규격은 위험성 분석, 심층적 방어(Defence-in-Depth) 및 구역 분할 원칙(구역 및 통로)을 위한 체계적인 프레임워크를 제공하며, EN 50742에서 보안을 보장하기 위한 대체 또는 보완 접근법으로 명시적으로 인정하고 있습니다. 이 규격들은 함께 '보안을 통한 안전'(Security for Safety)의 규범적 핵심을 이룹니다. 이 규격들은 기계의 디지털 무결성을 기능 안전의 사전 요건으로 인정하고 그에 따라 적절히 보호할 것을 의무 사항으로 규정합니다.

'구역 및 통로' 접근법이 기계류 안전을 높이는 이유

집의 비유로 돌아가 보자면, 보일러실은 ‘구역’을 나타내고, 스마트 홈 게이트웨이 연결은 이를 잇는 ‘통로’를 나타냅니다. 이 연결이 무단 조작될 경우, 방 자체의 보안이 완벽하더라도 시스템 전체가 영향을 받을 수 있습니다. 따라서 개별 구역을 보호하는 것뿐만 아니라, 이들 구역을 연결하는 통로의 보안을 확보하는 것 또한 매우 중요합니다. 바로 이 지점에서 '구역 및 통로' 원칙이 적용됩니다. 구역들은 서로 명확하게 구분되며, 구역 간의 이동 통로는 감시받도록 설계됩니다. 집에서는 문과 열쇠가 누가 어디로 갈 수 있는지를 결정하듯이, 산업 플랜트 내에서도 내부 보호(안전)와 외부 조작으로부터의 보호(보안)가 구조적으로 서로 밀접하게 연관되어 있습니다.

그 결과, 심층적 방어(Defence-in-Depth) 원칙에 기반한 보호 개념이 도출되었습니다. 안전은 단일 장벽만으로는 달성될 수 없으며, 여러 층의 보호 장치를 서로 앞뒤로 배치함으로써 비로소 확보될 수 있습니다. 이 경우, 한 층을 뚫고 들어가도 다음 층이 여전히 견고하게 버티고 있습니다. 구역들은 이러한 계층적 공간을 형성하며, 연결 통로는 이들 구역 사이를 오가는 감시 대상 경로가 됩니다. 이렇게 하면, 하나의 취약점만으로는 전체 시스템이 침해될 수 없습니다. 특히 안전과 관련되어 사람들을 보호하는 사안의 경우 더욱 그러합니다.

필츠는 '보안을 통한 안전'(Security for Safety)이라는 접근 방식을 일관되게 추구하며, 여기서 '안전'은 '보안'의 최우선 보호 목표입니다. 가장 중요한 것은 안전을 지키는 것이며, 이는 결국 사람을 보호하는 것입니다. 이 때문에 필츠는 안전을 일반 기계 제어, 즉 표준 자동화와 분리하여 안전 관련 기능이 노출되는 정도를 줄이려고 합니다. 이러한 '자산'들이 기능적으로 명확하게 구분될수록, 신뢰할 수 있는 보호를 제공하기 위해 필요한 추가적인 안전 조치는 줄어들게 됩니다.

이 접근 방식의 장점은 기계의 전체 라이프사이클 전반에 걸쳐 분명하게 드러납니다. 안전 기능과 표준 기능이 분리되어 있다면, 표준 기능이 업데이트되더라도 안전 기능을 함께 재인증하거나 수정할 필요가 없습니다. 이 덕분에 유지보수 및 정비 작업이 크게 줄어듭니다. 기존의 안전 컨트롤러는 표준 컨트롤러에 비해 안전에 중요한 업데이트가 훨씬 적게 필요하므로, 이러한 분리를 통해 불필요한 개입을 크게 줄일 수 있습니다. 이러한 분리 방식은 기술적인 이점도 제공합니다. 안전 컨트롤러 PNOZmulti 2와 같은 독립형 안전 시스템은 다양한 제조사의 제어 시스템과 자유롭게 결합할 수 있는

반면, 통합형 시스템은 특정 기술에 종속되는 경우가 많습니다.

동시에, 별도의 안전 솔루션을 도입하면 공격자가 극복해야 할 장벽이 높아지는데, 이는 개별 시스템을 하나씩 해킹해야 하므로 시스템을 조작하기가 훨씬 더 어려워지기 때문입니다. 게다가 표준 시스템은 필요할 때 온라인 상태로 전환할 수 있지만 실제 안전 기능은 분리된 상태로 유지되므로 공격 노출 면적을 대폭 줄일 수 있습니다.

각각 완벽하게 조율된 보안 레벨을 유지하면서 안전과 보안 자동화를 이처럼 분리하면 안전, 유지보수 및 확장 계획을 수립하는 것이 쉬워져 효율성을 높일 수 있습니다. 따라서 표준 프로그램을 변경할 때 안전 관련 부분에 대한 개입이 필요하지 않아, 필요한 프로그래밍 및 수정 작업량이 크게 줄어듭니다. 동시에, 이러한 분리 방식은 별도의 시스템을 사용할 경우 라이선스 비용과 서비스 요금이 더 저렴해지는 경우가 많기 때문에 소프트웨어 및 지원 비용 측면에서도 긍정적인 영향을 미칩니다.

분리를 통한 보호 – 교육을 통한 역량 강화

안전과 표준 자동화를 명확하게 분리함으로써 기술적 안정성을 보장할 뿐만 아니라 작업자의 실수를 줄이고 교육 요건도 낮출 수 있습니다. 안전 관련 기능은 전용 하드웨어에서 실행되며

조직적으로도 명확히 분리되므로, 표준 프로그램에 변경 사항이 발생하더라도 계속해서 보호됩니다. 그 결과, 일상 업무에서 발생하는 오류가 안전에 지장을 주지 않으며, 책임을 보다 명확하게 할당할 수 있습니다.

필츠는 기업들이 이러한 아키텍처를 도입할 수 있도록 포괄적인 교육 및 서비스 프로그램을 제공합니다. 여기에는 '산업 보안 기초' 및 'CESA – Certified Expert for Security in Automation' 교육 과정과 산업 보안 서비스가 포함됩니다. 이러한 교육 과정은 개별 블록에 기반해 견고한 '보안을 통한 안전'(Security for Safety) 개념을 개발하는 방법을 설명하는 것은 물론 그 이상도 다룹니다 - 보안 위험을 체계적으로 관리하고 종합적인 안전 개념을 개발하는 방법, IEC 62443의 요구사항을 반영하는 방법, 안전한 기계 네트워크 아키텍처를 구성하는 방법, 그리고 취해진 조치의 효과성을 평가하고 지속적으로 개선하는 방법을 보여줍니다.

이 접근 방식의 주요 장점 중 하나는, 안전 기능의 보호가 이미 아키텍처 설계 단계에서 보장되므로 최종 사용자의 운영 담당자가 보안 사안에 깊이 관여할 필요가 없다는 점입니다. 이러한 이유로 이들 교육 과정은 주로 보안 관련 의사결정을 내리거나 시스템을 설계하는 담당자를 대상으로 하며, 운영 담당자의 경우 산업 보안에 대한 추가적

교육 없이도 안전하게 업무를 수행할 수 있습니다. 그 결과, 다양한 역할이 실용적으로 분담되어 공장 운영이 간소화되는 동시에 안전 레벨도 지속적으로 향상됩니다.

명확한 체계와 적절한 전문성을 바탕으로 한 안전 강화

효과적인 '보안을 통한 안전' 전략은 개별적인 조치만으로는 달성될 수 없으며, 치밀하게 설계된 체계, 명확한 책임 소재, 그리고 목표 지향적인 역량 개발을 통해 실현됩니다. 바로 이 지점에서 필츠가 역할을 합니다. 필츠는 '심층적 방어'에 철저히 집중하고 안전과 표준 자동화를 명확히 분리함으로써 견고한 기계류 시스템을 위한 토대를 마련합니다. 또한 기업들이 이 길을 자신 있게 걸어갈 수 있도록 실질적인 교육과 컨설팅을 제공하여 이를 뒷받침합니다. 그 결과, 단순히 규격 요건을 충족하는 데 그치지 않고 일상적인 운영에서 실질적인 부가가치를 제공하는 안전 레벨을 달성할 수 있게 됩니다. 이는 더 단순하고, 더 견고하며, 장기적으로도 효과적인 솔루션입니다.

((글자 수: 9.640))

필츠는 자동화 기술을 위한 제품, 시스템, 서비스를 제공하는 글로벌 기업입니다. 안전 자동화 분야의 선구자로서 필츠는 인간, 기계, 환경을 위한 안전을 도모합니다.

1948년에 설립되어 독일 오스트필데른에 본사를 두고 있는 이 가족 기업은 오늘날 전 세계 42개 지사와 지점에 2,500명 가량의 직원을 보유하고 있습니다.

이 기술 선도 업체는 기계의 안전과 산업 보안을 위한 완전한 자동화 솔루션을 제공합니다. 이러한 솔루션에는 산업용 통신, 진단 및 시각화 시스템은 물론 센서와 제어 및 드라이브 기술도 포함됩니다. 필츠의 포트폴리오는 컨설팅, 엔지니어링, 교육과 관련한 국제적 서비스까지 포함하고 있습니다. 필츠 솔루션은 기계 공학을 넘어 예를 들어, 내부 물류, 패키징, 철도 기술, 로봇 공학 분야 같은 많은 산업 분야에서 사용되고 있습니다.

www.pilz.com

소셜 미디어를 통해 보는 필츠:

필츠는 소셜 미디어 채널을 통해 필츠의 이야기와 사람들에 대한 다양한 정보를 소개하고, 최신 자동화 기술 소식을 전달합니다.

 www.pilz.com/facebook
 www.pilz.com/xing
 www.pilz.com/youtube
 www.pilz.com/linkedin

홍보 담당자:

Martin Kurth

기업 및 기술 홍보 담당
전화: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

기술 및 기업 홍보 담당
전화: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

기술 홍보 담당
전화: +49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rößle

기술 홍보 담당
전화: +49 711 3409-7147
e.roessle@pilz.de