기본 정보

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

총체적 안전 컨셉은 기계에서 안전과 산업 보안을 보장하기 위해 접근을 중시합니다.

맞춤형 권한 관리를 통한 총체적 안전 보장

2023년 2월 오스트필데른 – **필츠는 중요한 것을 보호하고자 할 때마다 게이트, 잠금 장치 및 키를 사용하여 접근을 제한합니다. 이는 궁극적인 자산인 모든 형태의 안전에도 마찬가지입니다. 산업 환경에서 목표는 한편으로는 사람을 보호하고(안전) 다른 한편으로는 기계류와 중요한 데이터를 보호하는 것입니다(산업 보안). 안전과 보안의 부재는 잘못된 작동에서부터 사고, 심각한 사이버 공격까지 다양한 결과를 불러올 수 있습니다. 접근 및 진입 권한을 명확하게 정의하는 포괄적인 신원 확인 및 접근 관리(I.A.M)는 총체적 안전 및 산업 보안 컨셉과 효율적인 절차에 기여합니다.**

안전 게이트 뒤는 위험하므로 주의해야 함을 사람에게 명확하게 알리는 가드는 생산 환경에서 흔히 볼 수 있는 광경입니다. 사람은 HMI(인간 기계 인터페이스) 또는 키를 통해 안전 펜스 뒤 공정에 접근합니다. 하지만 그럴 자격 또는 권한이 전혀 없는데 자신 또는 다른 사람을 위험에 빠뜨리는 경우 어떻게 해야 할까요? 또한 악의적인 의도를 가진 사람이 기계에 직접 또는 원격으로 접근하여 공정을 조작할 수도 있습니다. 접근 권한이라는 주제는 안전 및 산업

보안이 긴밀하게 연결되어 있음을 보여 줍니다. 여기서 한 발 더 나아가 산업 보안은 기계 안전의 무결성을 보장합니다. 예를 들어, 산업 보안은 외부의 무단 접근으로부터 공장 또는 생산 라인의 기계류를 보호하고, 중요한 공정 데이터 및 기계 데이터가 내부에서 위조, 손실되는 것을 막으며, 이러한 데이터에 무단으로 접근하지 못하도록 보호합니다. 여기에는 명백한 공격뿐만 아니라 의도치 않은 보안 사고도 포함됩니다.

안전 및 산업 보안은 하나입니다

공장 및 기계류의 운영자는 작업 및 권한을 명확하게 발급 및 할당하여 사실상 신원 확인 및 접근 관리(I.A.M)를 확립할 수 있어야 합니다. I.A.M은 작업 지침 또는 정기적인 절차 점검 등과 같은 조직 수준의 조치뿐만 아니라 생산 환경에서 적절한 보안 솔루션의 통합도 의미합니다. 이러한 조치가 제대로 이행되지 않으면 사고 또는 생산 중단 발생 시 기업 내 책임자가 개인적으로 책임을 져야 할 수 있습니다. 이전에 이러한 유형의 보안 솔루션은 기업 내부에서 자발적으로 적용했지만, 많은 곳에서 이러한 조치를 취할 필요를 느끼지 못했습니다. 그러나 이후 입법자들이 안전과 보안 간의 연결성을 인지하기 시작했습니다. 따라서 새로운 기계류 규정에 의무 보안 조치가 명시되었습니다.

작동 모드를 통한 안전 강화

또한 여러 C 규격에서 다양한 작동 모드 또한 관련 안전 기능을 포함해야 한다고 이미 규정해 두고 있습니다. 예를 들어, 작동 모드에는 자동 모드, 제한된 조건 하에서의 수동 개입, 서비스 모드 등이 있습니다. EN ISO 16090-1에서는 머시닝 센터 및 특수 목적용 기계류에 있어 기능 안전 보장을 위해 이러한 작동 모드 중 최소 두 가지 이상을 필수로 둘 것을 규정하고 있습니다. 한 번에 한 가지 작동 모드만 선택 및 활성화되어야 하며 선택된 작동 모드는 명확히 표시되도록 해야 합니다.

익명 접근 차단

그런데 누가 어떤 작동 모드에서 접근할 수 있는지 또는 누가 작동 모드를 변경할 수 있는지 어떻게 결정할 수 있을까요? 이러한 결정을 하려면 작동, 세척 또는 정비 직원 등과 같이 기계에 접근하는 다양한 그룹을 정의해야 합니다. 그런 다음 작업 또는 자격에 따라 직원을 그룹에 할당합니다. 또한 기업의 규모에 따라 다양한 사용자 그룹 또는 예를 들어, 회사 전체에서 사용되는 기계 유형에도 활성화 권한 또는 접근 권한을 발급할 수 있습니다. 위험성 평가 시 안전 전문가는 모든 위험에 대해 익명 접근의 위험성을 평가하고 등급을 매깁니다.

위험을 줄이기 위한 조치는 최신 기술에 따라 통일된 규격을 고려하여 최종적으로 정의됩니다.

임의 조작을 방지하는 사용자 편의성

조치를 이행할 때 임의 조작을 방지하기 위해 기업에서는 사용자에게 취급의 편이성과 사용성을 보장하는 것이 중요합니다. 이는 기계 제조업체의 개발 공정에 이미 적용되어 있습니다. 사용자가 쉽게 다룰 수 있는 직관적인 운영 시스템은 작업자가 안전 예방 조치를 건너 뛰거나 기계류를 잘못 작동하는 것을 막아줍니다. 많은 것들을 충분히 고려해 만든 안전 시스템은 또한 불필요한 가동 중단 없이 효율적인 절차에 기여합니다. EN ISO 14119의 핵심 측면은 바로 "안전 장치 무력화" 문제입니다. 이 규격은 안전 게이트 시스템의 설계 및 선택에 대한 안내 지침을 정의하므로 임의 조작을 방지하는 방법에 대한 실질적인 가이드를 제공합니다.

개별 안전 컨셉

의도적이든 실수든 상관없이 액세스 도어가 열려 있을 때 위험이 발생하지 않도록 하려면 안전 게이트 시스템을 사용하여 보호해야 합니다. 여기서는 안전 관점에서 위험한 기계 움직임으로부터 작업자를 보호하는 데 특히 주안점을 두었습니다. 단독으로 작동하는 기계이냐 복잡하게 상호 연결된 공장이냐에 따라 적절한 맞춤 안전

컨셉이 필요합니다. 기계류에서 위험한 오버런이 발생하는 경우 가드 락킹 기능이 중요합니다. 게이트에 접근할 수 있는 경우에는 이스케이프 릴리즈가 있어야 합니다.

안전 게이트의 맞춤형 보호

필츠의 PSENmlock 등과 같은 모듈형 안전 게이트 시스템은 단일 시스템 내에서 안전 게이트 모니터링을 안전 가드 락킹과 결합하고 비상 정지, 이스케이프 릴리즈 및 기계식 재시작 인터록 등과 같은 안전 기능도 제공합니다. 또한 광범위한 어플리케이션을 보호하기 위한 유연성과 분산형 인텔리전스를 제공합니다. 개별 솔루션은 센서, 이스케이프 릴리즈, 도어 핸들과 제어 및 푸시버튼 유닛의 결합으로 구성됩니다. 사용자는 어플리케이션에 따라 나만의 맞춤형 안전 게이트 솔루션을 설계할 수 있습니다. 산업 보안을 위한 요구 사항을 충족하기 위해 이제는 접근 및 권한에 집중해야 합니다.

안전 및 산업 보안 모두를 제공하는 하나의 시스템

무단 접근 방지는 작동 모드 선택 및 접근 권한 시스템을 사용하여 실제로 구현할 수 있습니다. 이 시스템은 작동 모드 선택 및 접근 권한 제어 등 산업 보안과 안전을 결합합니다. 이러한 유형의 솔루션은 필츠 PITmode 제품군의 기기에서 제공합니다. 따라서 정의된 작동 모드 간에 전환하고 접근 권한을 제어할 수 있습니다. 각

사용자가 명확한 사용자 인증을 지원하고 임의 조작을 방지해주는 개별 트랜스폰더를 받게 되므로 직관적인 작동이 보장됩니다.

접근 및 작동 모드의 개별 관리

PITmode는 다양한 버전으로 제공되어 안전 컨셉의 개별 설계가 가능합니다. PITmode는 작동 모드 선택을 위한 푸시버튼과 평가 유닛을 포함한 컴팩트 올인원 장치로서, 설치 공간을 절약할 수 있습니다. 한편, 모듈형 시스템인 PITmode fusion은 RFID 기술과 통합 웹 서버가 적용된 판독 유닛 PITreader와 안전 평가 유닛(SEU)으로 구성되어 있습니다. 또 다른 버전은 PITmode flex입니다. 이 버전에서 PITreader는 필츠 컨트롤러 및 안전 평가용 소프트웨어 블록과 함께 사용됩니다. 모듈형 셋업 덕분에 접근 권한 및 작동 모드 선택 기능을 기존 제어 콘솔의 설계에 통합할 수 있습니다. 작동 모드 선택에 기존의 버튼을 사용할 수 있어 사용자가 쉽게 조작할 수 있습니다. 트랜스폰더를 사용한 신원 확인은 판독 기기 PITreader에서 수행합니다. PITmode 및 PITmode fusion은 PL d에 따른 기능 안전 작동 모드 선택 및 접근 권한 기능을 제공합니다.

간편 인증 – 원격으로도 가능

작동 모드를 선택하려면 사용자는 트랜스폰더를 PITmode에 직접 연결하고 작동 모드에 대해 정의된 버튼이나 HMI의 해당 버튼을

누릅니다. 사용자에게 권한이 있으면 해당 공정에 대한 접근이 허용됩니다. 서비스 직원이 원격 유지보수를 통해 기계에 접근하고자 하는 경우에도 마찬가지입니다. 현장에 있는 사람이 시스템에서 해당하는 권한을 부여하는 경우에만 원격 유지보수를 시작할 수 있습니다. 유지보수 작업을 마치면 이 접근이 다시 차단되고 기계가 백업을 시작합니다. 따라서 유지보수 작업 이후 권한 없는 사람의 임의 조작 또는 실수로 열려 있는 포트 등의 문제가 발생할 수 없습니다. 운영 회사는 누가 어떤 권한을 가질지 즉, 누구에게 공정에 대한 접근 권한을 제공할지 제어하기 때문에 산업 보안이 강화됩니다.

접근 관리를 위한 완벽한 솔루션

접근 제어만 수행하려는 경우 PITreader는 독립 실행형 장치로써 또는 필츠의 컨트롤러와 함께 접근 권한 시스템으로 사용할 수 있습니다. 소형 컨트롤러 PNOZmulti 2와 함께 사용하면 관리자는 연결된 구성 도구인 PNOZmulti Configurator에서 "드래그 앤 드롭"을 통해 간단하게 공장 및 기계류에 대한 접근 권한을 구성할 수 있습니다. 그러면 구성된 권한이 판독 기기 PITreader를 통해 RFID 트랜스폰더 키로 전송됩니다. 또한 PITreader S 버전은 OPC UA 규격을 통합하였으므로 필츠 컨트롤러와 독립적으로 타사 장치와

함께 사용할 수 있습니다. 앞서 말씀드린 것처럼 PITmode 기기는 기존 제어 패널에 쉽게 통합할 수 있습니다.

키, 카드 또는 스티커 중 선택

PITreader 카드 유닛 버전은 운영자 및 사용자를 위한 추가 유연성을 제공합니다. RFID 지원 카드 및 스티커는 RFID 트랜스폰더 키와 함께 또는 그 대신에 사용할 수 있습니다. 회사에서 RFID 지원 카드를 이미 사용하고 있는 경우에는 PITreader 카드 유닛과 함께 사용할 수도 있습니다. 이 경우 사용자는 여러 기능을 사용하기 위해 하나의 카드만 있으면 됩니다. 일반적으로, 키, 카드 또는 스티커이든 상관없이 RFID 트랜스폰더의 이점은 여러 기능을 하나의 트랜스폰더에 결합하여 전체 기계식 키 링을 통합한다는 점입니다. 신원 확인 매체를 하나만 소지하면 되기 때문에 이는 사용자에게 매우 편리합니다. 또한 키 관리 및 유지보수에 드는 관리자의 시간과 노력이 줄어듭니다.

향상된 보안

사용자 인증, 자격 부여 및 접근 보호 관점에서 보안 측면도 고려해야 합니다. 모든 안전 및 보안 조치에도 불구하고 기계에서 사건 또는 보안 사고가 발생하는 경우 RFID 트랜스폰더를 읽어 누가 무엇을 변경했는지 확인할 수 있습니다. 이 옵션 기능이 필요한 경우

컨트롤러에서는 인증 기능을 사용하여 수정이 불가능한 내부 감사 추적 기록(이벤트 로그)에 접근 시간을 기록합니다.

세심한 관리가 열쇠입니다

어플리케이션의 라이프사이클 전반에서 안전 및 산업 보안을 보장하기 위해 관리자는 권한을 유지관리하는 데 많은 노력을 기울입니다. 간편한 관리를 위해 필츠의 적절한 소프트웨어 도구가 사용자 및 트랜스폰더 구성을 지원합니다. 즉, 작은 RFID 키 내에 복잡한 권한 매트릭스 또는 그룹 전반 사양을 숨길 수 있음을 의미합니다. 통합 PITreader 웹 서버를 통해 관리자는 PITmode 또는 PITreader에 속하는 RFID 트랜스폰더를 프로그래밍하고 여기에 사용자 데이터 및 권한을 저장합니다. 중요한 모든 설정은 판독 유닛에서 직접 수행하므로 인터페이스 구성을 비롯한 시운전 시간이 단축됩니다.

인터페이스에 대한 접근 제한

보안 사고의 주요 관문인 산업용 특수 USB 포트를 사용하는 데까지 신원 확인 및 접근 관리 기능을 확장할 수 있습니다. 접근 권한 시스템 PITreader에는 활성화 가능한 USB 2.0 호스트 인터페이스가 있는 PIT oe USB 등과 같은 작동 요소가 결합됩니다. 이러한 솔루션은 임의 조작이 불가능한 프로그램 가져오기, 데이터

내보내기, 키보드 또는 마우스 연결 기능을 지원합니다. 해당 권한이 있는 경우에만 인터페이스를 활성화할 수 있기 때문에 생산 시설의 데이터 흐름을 보호할 수 있습니다. 산업 자동화 네트워크 내에서의 데이터 통신을 제어하는 필츠의 SecurityBridge와 같은 산업용 방화벽을 결합하여 무단 접근 및 임의 조작으로부터 기계를 보호할 수 있습니다.

기존 기계류 - 안전과 보안

기존 기계류가 최신 상태로 업데이트되거나 위험성 평가의 일부로 조치를 취할 필요가 식별되면 접근 권한 시스템 PITreader을 쉽게 개조할 수 있습니다. 직경이 22.5mm인 키 스위치에 표준화된 컷아웃(cut-out)을 사용하여 기기를 직접 장착할 수 있습니다. 필츠 컨트롤러와 결합하면 원하는 보안 기능을 직접 설정할 수 있습니다. 타사 컨트롤러를 사용하는 경우에는 접근 권한 및 작동 모드 평가를 통합하는 데 PITmode fusion이 사용됩니다. 고려 중인 트랜스폰더 매체에 따라 기업에서 사용 중인 기존 RFID 키 카드를 인증에 사용할 수 있습니다.

결론

궁극적인 자산 즉, 안전을 보호하기 위해서는 총체적인 안전 컨셉을 설계하고 최신 상태인지 정기적으로 확인해야 합니다. 여기서 중요한

요소는 기업에서 권한 및 접근을 명확하게 규제하는 신원 확인 및 접근 관리(I.A.M)입니다. 이 솔루션은 조치 및 사양과 적절한 안전 및 보안 기능을 포함하는 컨셉입니다. PITreader 등과 같은 접근 권한 시스템은 사용자 및 트랜스폰더를 구성하기 위한 추가 소프트웨어 구성요소와 함께 사용되는 경우 이러한 목적에 적합한 하드웨어 블록입니다. 안전 게이트 시스템, 컨트롤러 및 소프트웨어 등과 같은 추가 구성요소와 작동 모드 선택 등과 같은 기능은 총체적인 안전 및 산업 보안 컨셉을 구성하는 솔루션을 향상시킵니다. 이 시스템은 사용자 손 안에 있는 개별 키로 작동하기 때문에 사용자가 다루기 쉽습니다.

글자 수: 14.675

<u>그림</u>

그림 1:
F_Press_IAM_Man_using_PITreader_Key_cold1.jpg(© Pilz GmbH & Co. KG)

사진 설명: 포괄적인 신원 확인 및 접근 관리(I.A.M)는 어플리케이션에 대한 접근을 제어하므로 안전과 산업 보안을 비롯한 안전 기능 및 조치의 무결성을 보장합니다.

그림 2:
F_Press_PITmode_fusion_402251_PIT_oe_4023311_P1_B_8_2_cold_2020_01.jpg(Pilz GmbH & Co. KG)

사진 설명: 필츠의 PITmode fusion은 모듈형 작동 모드 선택 및 접근 권한 시스템으로, 안전 및 산업 보안을 단일 시스템에 결합합니다.

그림 3:
F_Press_PITreader_S_card_unit_402321_and_PITreader_card_ye_g_402330_P1_B8_2_cold.jpg(Pilz GmbH & Co. KG)

사진 설명: RFID 기반 카드 PITreader card 및 스티커 PITreader sticker와 결합된 필츠의 접근 권한 시스템 PITreader 카드 유닛은 효율적인 접근 권한 시스템을 구현하기 위한 추가 형식을 제공합니다.

그림 4:
F_Press_PITreader_Webserver.jpg(© Pilz GmbH & Co. KG)

사진 설명: RFID 트랜스폰더 키는 PITreader에서 판독 및 학습됩니다. 접근 권한 및 작동 모드는 연결된 웹 서버를 사용하여 쉽게 할당할 수 있습니다.

그림 5:
F_Press_Group_7_Modular_safety_gate_system_with_diagnostic_and_evaluation_P1_B8_2_cold.jpg(© Pilz GmbH & Co. KG)

사진 설명: 적절한 핸들 모듈이 장착된 안전 게이트 시스템 PSENmlock(왼쪽 위), 일체형 접근 권한 시스템 PITreader가 탑재된 푸시버튼 유닛 PITgatebox(오른쪽 위), 소형 안전 컨트롤러 PNOZmulti 2(오른쪽 아래) 및 진단 솔루션 SDD(Safety Device

Diagnostics)(왼쪽 아래)를 유연하게 결합하면 접근 권한 할당이 가능한 완전한 안전 게이트 솔루션이 구성됩니다.

박스: 디지털 유지보수 안전 가딩 시스템 key-in-pocket

소형 안전 컨트롤러 PNOZmulti 2 또는 자동화 시스템 PSS 4000 등과 같은 필츠 컨트롤러와 결합되면 PITreader는 단순한 접근 권한 할당을 뛰어넘어 효과적인 디지털 “Key-in-pocket” 유지보수 안전 가딩에 사용할 수 있습니다. 이 솔루션은 유지보수 작업이 진행되는 동안 기계가 재가동되는 것을 막고 권한 없는 사람은 접근하지 못하게 합니다. 이는 실제로 유지보수 작업을 수행할 권한을 가진 한 명 이상의 사용자가 공장에서 자신을 인증하도록 하여 구현됩니다. 인증에 성공하면 개인화된 보안 ID가 사용자를 위해 필츠 컨트롤러의 안전 목록에 저장됩니다. 그러면 이제 기계를 셧다운하고 안전 게이트를 개방한 뒤 기계에 접근할 수 있습니다. 이 시간 동안 RFID 키는 각 사용자가 소유하고 있습니다. 이 개념이 “key in pocket”입니다. 유지보수가 완료되면 사람들이 위험 구역에서 빠져나간 후 모두 로그아웃합니다. 그러면 보안 ID들이 필츠 컨트롤러의 안전 목록에서 삭제되고, 기계를 재가동할 수 있게 됩니다. 기계식 키를 사용하는 유지보수 안전 가딩과는 달리, 어떤 안전 게이트를 통해서든 공장에 들어가거나 공장에서 나올 수

있습니다. 이러한 방식으로 “key-in-pocket”은 유지보수 중 작업자에게 더 큰 유연성을 제공하고 시간을 절감해줍니다. 디지털 유지보수 안전 가딩은 안전 펜스로 보호되는 위험 구역이 있는 기계를 위해 특별히 설계된 기능입니다. 운영자는 누가 어떤 작업을 위한 접근 권한을 가졌는지 항상 파악할 수 있습니다. 임시 권한을 할당할 수도 있습니다.

1,578자

key-in-pocket 그림 상자:
F_Press_Group_PIT_Key_in_pocket_solutions_P1_B8_2_cold.jpg(© Pilz GmbH & Co. KG)

사진 설명: 유지보수 안전 가딩 시스템 “key-in-pocket”은 접근 권한 시스템 PITreader, 푸시버튼 유닛 PITgatebox 및 필츠 컨트롤러(예: 소형 컨트롤러 PNOZmulti 2 또는 자동화 시스템 PSS 4000)로 구성됩니다.

PILZ
THE SPIRIT OF SAFETY

박스: 권한 할당 및 유지

기업에서 접근 권한 시스템을 사용하는 경우, 높은 수준의 안전 및 보안을 보장하기 위해서는 정기적인 유지보수와 권한 및 사용자 데이터의 관리가 정말 중요합니다. 필츠는 이 용도로 소프트웨어 도구 PTM(PIT 트랜스폰더 매니저)을 제공합니다. 따라서 관리자는 그래픽 인터페이스에서 사용자 설정, 차단 목록 및 사용자 데이터를 관리할 수 있습니다. 미리 구성된 템플릿과 가져오기 기능을 사용하여 단지 몇 단계만으로 트랜스폰더 키에 개별 사용자 권한을 기록할 수 있습니다.

기업에서 PITmode 또는 PITreader 기기를 여러 개 사용하는 경우 필츠의 PIT User Authentication Service(UAS) 소프트웨어를 사용하여 이들을 구성할 수 있습니다. 이 소프트웨어는 PTM 또는 다른 사용자 관리 소프트웨어와 같은 관리 시스템을 PITreader와 연결할 수 있습니다. PIT UAS에는 사용자를 위한 중앙 인증 데이터베이스가 있어 PTM에서 데이터를 가져와 모든 PITreader 기기로 할당할 수 있습니다. 관리자는 모든 PITreader의 현재 상태를 확인하고 진단 목록을 표시할 수 있습니다. 이러한 방식으로 여러 기기를 사용하는 중에도 빠르게 상태를 살펴볼 수 있습니다.

1,218자

사용자 관리 그림 상자:

((표시될 이미지)).jpg(© Pilz GmbH & Co. KG)

사진 설명: 기업에서 판독 기기 PITreader를 여러 대 사용하는 경우,
UAS(User Authentication Service)
소프트웨어 도구를 사용하여 이들을 구성합니다.

필츠 그룹

필츠 그룹은 자동화 기술을 위한 제품, 시스템 및 서비스를 제공하는 글로벌 기업입니다. 이 가족 기업의 본사는 독일 Ostfildern에 위치하며

직원 수는 약 2,500명입니다. 필츠는 전세계적으로 42개 자회사와 지사를 두고 있으며, 인간, 기계, 환경을 위한 안전 솔루션을 공급합니다.
기술 리더 기업인 필츠는 산업 통신, 진단 및 시각화 시스템을 포함하여 센서, 제어 및 드라이브 기술로 구성된 완전 자동화 솔루션을 제공합니다. 컨설팅, 엔지니어링, 교육을 포괄하는 국제적인 일련의 서비스가 필츠 포트폴리오를 완성합니다. 필츠의 솔루션은 내부물류, 철도 기술, 로봇 공학 분야 같은 기계 공학 이외의 많은 산업 분야에서 사용되고 있습니다.

www.pilz.com

홍보 관련 담당자:

Martin Kurth

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

Sabine Karrer

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

Jenny Skarman

기술 홍보 담당

전화 번호: +49 711 3409-1067
j.skarman@pilz.de

Sabrina Schilling

기술 홍보 담당

전화 번호: +49 711 3409-7147
s.schilling@pilz.de

Hansjörg Sperling-Wohlgemuth
컨퍼런스 및 프레젠테이션 관리 담당
전화 번호: +49 711 3409-239
h.sperling@pilz.de