한국철도학회 철도저널 18권 5호, 2015년 10월, pp. 29-32

철도분야에 적합한 SIL 4 자동화 솔루션, 필츠 PSS 4000-R

고 설 린
필츠코리아 기술컨설턴트 대리
S.Ko@pilzkorea.co.kr

1. 전 세계에서 검증된 필츠의 안전 솔루션

철도 산업의 솔루션 중 특히 신호 및 제어 시스템은 현재까지 자체적인 기술로 개발되어 공급되고 있습니다. 즉, 철도 교통의 특수하고 안정된 기술을 구현하기 위해 직접 설계, 개발, 공급이 이루어지고 있는 상황입니다.

오늘날, 전 세계 철도산업에서 필츠의 다양한 솔루션이 적용되고 있습니다. 신호 제어 시스템과 선로변환(선로전환기) 제어, 건널목 제어(Level Crossing) 시스템, 스크린 도어 시스템(PSD), 차상 안전 제어 시스템을 비롯하여 분기기 히팅(Point heater) 등의 솔루션이 있습니다.

철도 산업의 안전은 대중 교통분야에서 가장 중요한 사항입니다. 특히, 기차와 자동차가 교차하는 건널목 제어 부분을 비롯한 모든 제어 시스템은 최고 등급(SIL 4)의 안전 시스템이 적용되어야 합니다. 경제적이며 높은 안전 수준(SIL 등급)으로 시스템 구축 및 운영할 수 있는 필츠의 PSS 4000-R과 같은 PLC 기반의 안전 솔루션을 철도의 안전 및 통합 제어 시스템 뿐만 아니라 운영자 인터페이스 시스템까지 적용하는 사례가 최근 늘어나고 있습니다.

2. 철도 분야에 적합한 표준화된 자동화 솔루션

철도 분야의 신호 및 제어 솔루션은 상당 부분 자체 개발된 것을 사용하였습니다. 즉, 철도 분야 전용 제품들이 직접 설계, 개발 및 제조되었으며, 오늘날 이러한 방법은 규정 및 요구사항, 프로젝트별 특이 사항 적용의 필요성, 이에 따른 표준화 작업의 어려움 등이 비용 상승의 원인으로 작용하고 있습니다. 일반 철도분야에서 현존하는 신호 기술들은 기계식 방식이나 릴레이 방식과 같이 오래된 기술들을 기반으로 하고 있습니다. 최근에도 오래된 릴레이 방식을 사용한 기술이 철도 신호 분야에 널리 사용되고 있습니다. 반면에, 강력한 소프트웨어 기술로 마모성 및 케이블 집중 방식의 하드웨어 기술을 대체하는 방안도 현대화 방안의 일부로 적용되고 있습니다. 놀라운 사실은 이 방식이 결코 경제적으로나 안전성 면에서 손해를 보지 않는다는 것입니다.

현존하는 신호 박스 인프라와 새로운 방식의 전자식 신호 박스(ESB) 사이의 중계자 역할을 할 수 있는 제어 솔루션이 요구되는데, 일반 산업에서 사용되던 솔루션들도 고려되고 있습니다. 이러한 솔루션들은 신호 박스 어플리케이션의 구매, 엔지니어링, 운영 및 유지보수 측면에서 엄청난 비용 절감에 도움을 줄 수 있습니다.

3. 철도 분야를 위한 PLC의 적합성

실제로 공장과 같은 일반 산업 현장에서 쓰이던 PLC를 철도 분야에 적용하기 위해서는 철도 분야에서 요구하는 사항(안전 레벨)을 만족해야 하며 CENELEC 표준 EN 50155나 EN 5012x 시리즈가 이에 해당됩니다.

PLC 제어 시스템은 엄청난 양의 릴레이를 대체할 수 있는 안전한 플랫폼을 갖추고 있습니다. 이들은 상용 제품이

기 때문에 구매 비용도 저렴합니다. 또한, 소프트웨어 툴을 사용하여 시스템 구성 시간 단축, 확연히 개선된 진단 기능, 유지 보수의 단순화 등의 이점을 누릴 수 있고,

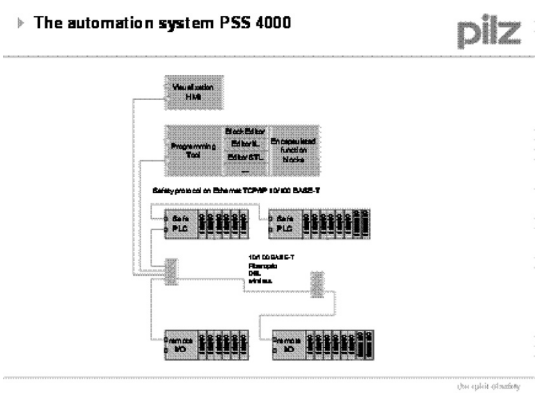
무엇보다도 사전에 승인된 제어 시스템을 사용함으로써 개발 비용이 상당히 감소합니다.

4. 자동화 시스템 PSS 4000

자동화 회사 필츠는 수 십 년간 안전 자동화 및 안전 제어 솔루션 제공 및 기술 개발에 경험이 있습니다. 또한 철도 산업 어플리케이션에도 다양한 경험이 있습니다.

필츠는 EN 61508 기준을 만족하는 PSS 4000을 개발하였습니다. 또한 철도 분야에 특별한 요구 사항들을 만족하는 제품인 R(Railway)제품도 개발하였습니다. PSS 4000-R은 전자파(EMC) 간섭에도 강한 내성을 가지고 있으며, 넓은 범위의 온도 조건 및 기계 진동에 대하여도 강한 내성을 가지고 있어 철도 분야에 적용하기 적합합니다. PSS 4000–R은 이미 철도 인증 EN 50126, EN 50128, EN 50129, 또한 EN 50155의 요구사항들을 만족합니다. 또한 전체 시스템의 안전 등급을 SIL 4까지 구성할 수 있습니다.

PSS 4000의 하드웨어는 PLC부분, 분산 I/O부분과 Failsafe 및 Standard I/O 확장 모듈 부분으로 구성됩니다. 노드 간의 통신은 리얼타임 이더넷 기반의 SafetyNET p 프로토콜을 사용합니다. SafetyNET p는 이더넷 스위치나 DSL 모뎀을 사용하여 다양한 토폴로지의 네트워크를 구성할 수도 있습니다.



〈그림 1〉 PSS 4000–R

소프트웨어 플랫폼 PAS4000은 제어 시스템 구성 및 제어 로직 개발, 프로그램 다운로드 및 시운전 등을 수행할 수 있는 PSS 4000용 툴입니다. PAS4000은 IEC 61131-3(프로그래밍 언어) 표준에 부합하는 개발 방식(IL, STL, Ladder)을 지원하며, PASmulti라는 그래픽 요소의 간편한 개발 방식도 지원합니다.

5. 철도 분야를 위한 PLC 아키텍처

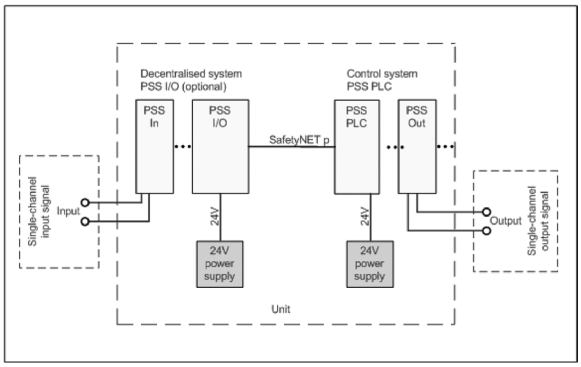
철도 분야의 어플리케이션들은 대부분 안전 무결성 레벨 SIL 2, SIL 3, SIL 4로 구성됩니다.

철도 분야의 PLC플랫폼을 적용하기 위한 중요한 요구사항은 사용하기 쉬운 모듈화된 시스템, 즉 가용성입니다. 개발자뿐만 아니라 End-user도 사용이 쉬워야 합니다. PSS 4000-R은 이미 철도 분야 인증의 요구사항을 모두 만족하여 인증 업체에서 검증 업무가 확연히 줄어들기 때문에 안전 인증에 소요되는 시간을 매우 감소시킬 수 있습니다. 이를 위해 필츠는 세 가지의 승인된 아키텍처 모델을 제공합니다. 사용자(개발자)는 아키텍처 모델을 선택하여 센서 사양 및 엑추에이터 사양만 선정하면 됩니다. 또한 필츠는 THR(Tolerable Hazard Rate)의 정량적 평가를 위한 적절한 HR(Hazard Rate)을 각 아키텍처 모델마다 제공합니다.

6. SIL 2 아키텍처

SIL 2 아키텍처는 재해의 심각성 수준이 '낮음'인 어플리케이션에 적용될 수 있습니다. EN 50129에서 SIL 2 내용을 보면 단일 결함에 대한 요구사항이 없기 때문에 SIL 2 아키텍처는 단일 채널로 구성이 가능합니다. 따라서 하나의 PLC 및 단일 채널의 디바이스로 SII 2 아키텍처 구성이 가능합니다. (<그림 2> 참조)

기본 구성요소를 보면 단일 입력 모듈, 파워 서플라이, 출력 모듈로 구성이 됩니다. Failsafe 모듈은 PLC 내부에 기본적으로 리던던트 시스템이 구성되어 있습니다. 또한 SafetyNET p 네트워크를 사용하여 Failsafe 관련 데이터들을 신뢰성 있게 처리할 수 있습니다. 따라서 SIL 2 아키



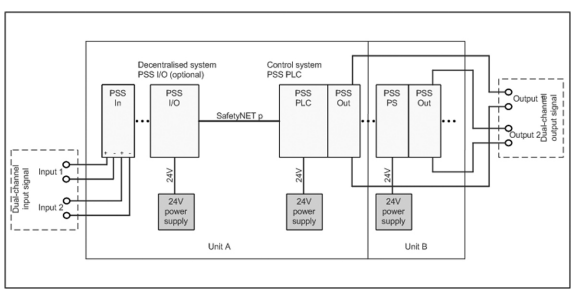
〈그림 2〉 SIL 2 아키텍처

텍처 구성을 위해서는 단일 채널의 입력 디바이스와 단일 채널의 출력 디바이스가 필요할 것입니다.

7. SIL 3 아키텍처

EN 50129에서 SIL 2와는 달리 SIL 3에서는 단일 결함이 관리되어야 한다는 내용이 있습니다. 따라서 단일 결함은 리던던트 시스템에 의해 감지가 되어야 하며 적절한 조치 또한 필요합니다.

기본적으로 외부 입/출력 디바이스들도 이중 채널이어야 합니다. <그림 3>을 참조하면, 아키텍처는 유닛 A 부분과 B 부분으로 구성됩니다. I/O 수량은 두 배로 구성이 되어야 하며, 파워 서플라이 역시 별도로 공급됩니다. PLC 제품 내부적으로 이미 다양성을 가진 리던던트가 구성이 되어있기 때문에, 사용자는 입/출력을 원하는 포트에 구성할 수 있습니다. SafetyNET p를 사용하여 네트워크로



〈그림 3〉 SIL 3 아키텍처

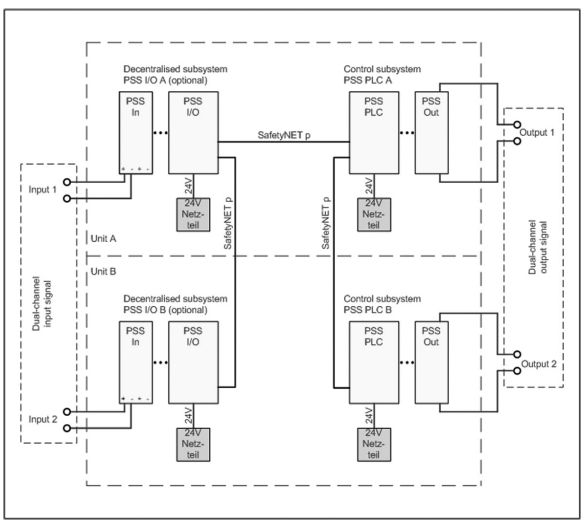
데이터를 처리할 수도 있습니다. 물론 파워 서플라이는 별도로 공급되어야 합니다.

8. SIL 4 아키텍처

가장 높은 수준인 SIL 4는 주로 신호 제어 시스템이나 선로 변환기같은 어플리케이션에서 요구됩니다. 이러한 경우, 각 유닛들은 더욱 엄격하게 분리됩니다.

일반적으로 SIL 4 아키텍처를 구성하기 위해 PLC 2개를 이용하여 리던던트 시스템을 구성합니다.

필츠는 SIL 4 어플리케이션 컨셉의 개발을 탈레스와 협업하고 있습니다. 탈레스의 SPZA(memory-programmable central block adaptation)는 엄청난 양의 릴레이시스템과 전자 신호 박스의 중계 역할을 대체 할 수 있는 탈레스의 솔루션입니다. 단독으로 구성된 유닛들은 일반 원인 고장(Common Cause Failure)으로부터 상당히 강한 내성을 가질 수 있습니다. 분산 I/O 시스템 구성 시에는 분산 I/O 시스템 역시 리던던트로 구성이 되어야 하며, 각각의 PLC는 각각의 연산 결과 값을 비교하여 동일할 경우 유효한 출력을 보내게 됩니다. 두 개의 PLC는 역시 SafetyNET p 프로토콜에 의해 연결이 됩니다. 두 개의 리던던트 시스템이 구성되었을지라도 동일한 로직이 두 개의 시스템에 적용



〈그림 4〉 SIL 4 아키텍처

되기 때문에 어플리케이션 프로그램은 한 쪽만 개발되면 됩니다.

9. 요약

PSS 4000과 같이 표준화된, 또한 사용이 쉬운 자동화 시스템은 사용자들의 초기 투자 비용은 물론 운영 비용도 감소시킬 수 있습니다. PSS 4000–R은 철도 분야 관련 승인이 된 제품이기 때문에 인증 작업량도 상당 부분 줄일 수 있습니다. PSS 4000-R은 같은 제품을 다양한 아키텍처로 구성하여 원하는 안전 무결성 등급(SIL 2, 3, 및 4)을 만족할 수 있습니다. 이러한 어플리케이션은 철도 건설 장비는 물론 레벨 크로싱 신호 감시와 같은 신호 제어 부분에도 사용될 수 있습니다. 각 프로젝트에 적용될 다양한 조건들을 손쉽게 적용 가능함 물론 복잡한 인증 업무도 파격적으로 줄여 줄 수 있는 PSS 4000-R 솔루션은 사용자에게 엄청난 비용절감 효과를 안겨 줄 것입니다.