

# COMPUTING

## ControlSafe™ 확장 박스 플랫폼 철도 제어 및 철로 신호 적용을 위한 SIL4 COTS 페일 세이프 및 장애 내성(Fault-Tolerant) 시스템

### 데이터 시트

- TÜV SÜD 에 의해 SIL4 안전표준 인증을 받은 고도의 일체형COTS 솔루션
- 다양한 지상 장치 적용을 가능하게 하는 비용 효과적인 일반 플랫폼
- 더 큰 사시와 I/O 모듈을 갖춘 고도 I/O 용량
- Six nine (99.9999%) 플랫폼 하드웨어 유용성을 실행하도록 설계됨
- 새로운 구축과 업그레이드 프로젝트에 적합한 모듈식 확장성 솔루션
- 혁신적인 데이터 락스텝 (data lock-step) 도입으로 완벽한 기술 업그레이드 가능
- 하드웨어 기반 보팅 (voting) 메커니즘으로 애플리케이션 소프트웨어 투명성 극대화
- IEC 61373 및 EN 50155 준수의 러그드 디자인
- 15년의 계획된 제품 수명과 25년으로 확장된 지원 및 서비스 이용 가능
- 글로벌 서비스 조직에 의한 지원

30년 동안 높은 신뢰도의 고가용성 임베디드 컴퓨터 시스템을 개발해 온 전문 지식을 활용하여 Artesyn Embedded Technologies는 철도 시스템 통합업체와 철도 애플리케이션 공급업체들에게 COTS (Commercial Off-The-Shelf) 페일 세이프 컴퓨터 시스템을 제공하는 최우수 업체로 자리 매김하고 있습니다.

세계에서 가장 공신력 있는 인증 기관들 중 하나인 TÜV SÜD에 의해서 최고 안전 수준(SIL4)으로 인증 받기 위해 설계된 ControlSafe™ 확장 박스 플랫폼은 늘어나는 Artesyn ControlSafe 제품 포트폴리오를 크게 개선합니다. 포트폴리오에서 획기적인 플랫폼인 ControlSafe 플랫폼과 동일한 안전 아키텍처 및 기술을 활용하여 ControlSafe 확장 박스 플랫폼은 더 큰 I/O 모듈을 장착하는 더 큰 사시의 설계로 컴퓨터 기반 연동(CBI) 같은 지상 장치 적용을 주로 대상으로 하는 고도 일체형 및 비용 효과적 솔루션입니다.

철로 인프라에 전세계적 투자는 강력한 모멘텀으로 진행되기 때문에 철로 운송의 네트워크는 꾸준히 확대되면서 더욱 더 복잡해지고 있습니다. 이러한 도전을 취급하려면 더욱 안전하고 스마트한 열차 제어 및 철로 신호 솔루션뿐만 아니라 늘어가는 데이터 처리량을 취급할 더 높은 수준의 I/O 용량이 필요합니다. ControlSafe 확장 박스 플랫폼을 통해서 철로 시스템 통합자들과 철로 애플리케이션 제공자들은 최대 10개의 9U 확장 I/O 모듈(EIOU)과 1개의 4U I/O 모듈(XIOU)을 단 한 개의 사시에 통합할 수 있습니다. 다양한 I/O 유형을 수용하고 더 많은 포트와 채널을 각 I/O 모듈에 허용함으로써 이 개선된 I/O 처리 용량은 대규모 애플리케이션을 구축하는데 필요한 사시의 수를 효과적으로 줄일 수 있습니다.

안정성, 유용성, 유지관리성 및 안전(RAMS) 프로세스에 대해서는 EN 50126, 안전 관련 소프트웨어에 대해서는 EN 50128 그리고 안전 관련 전자 시스템에 대해서는 EN50129에 완전하게 인증을 받은 Artesyn의 ControlSafe 확장 박스 플랫폼은 SIL4 적용 환경에서 실행하도록 비용 효과적이고 적용 준비 플랫폼을 제공합니다. 스크래치를 통해 한 개를 설계하고 구축하는 것과 반대로, 코어 세이프티 처리 엔진으로서 ControlSafe 확장 박스 플랫폼을 채택하면 철로 애플리케이션 개발자들과 시스템 통합자들은 SIL4 COTS 플랫폼을 활용하여 비용과 리스크를 효과적으로 줄이고, 최종 솔루션을 위한 부가가치 제공과 최종 인증에 초점을 맞추어 출시 시간을 크게 가속화할 수 있습니다.



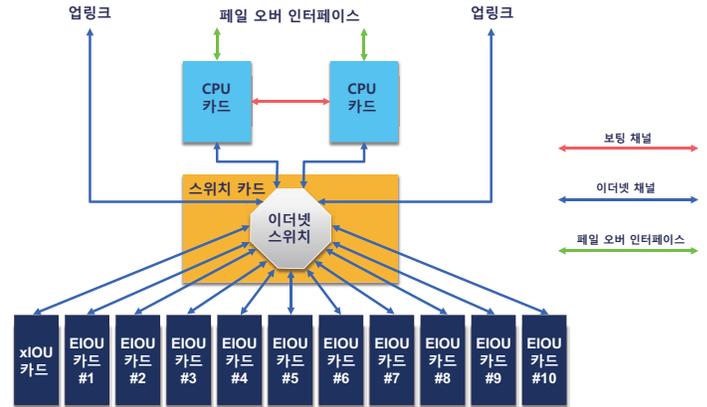
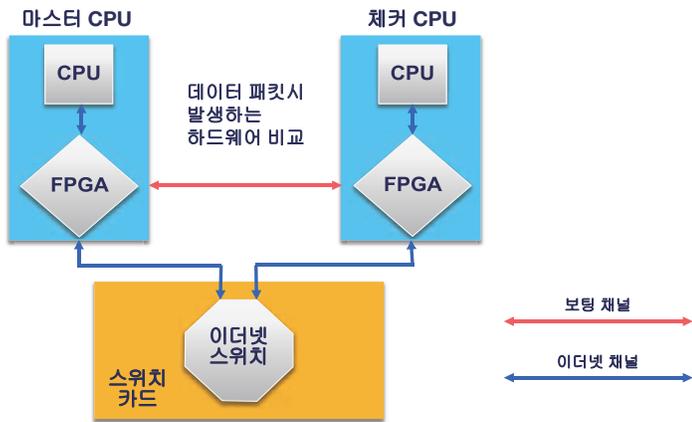
혁신적 데이터 락-스텝 및 하드웨어 기반 보팅을 갖추고 있는 공유 안전 아키텍처는 ControlSafe 확장 박스 플랫폼 및 ControlSafe 플랫폼 사이에 적용을 변환하는 것을 용이하게 만듭니다. 또한 이것은 “일반 플랫폼”을 제공함으로써 Artesyn의 설계 철학을 더욱 강화하여 다양한 적용을 가능하므로 고객들의 투자에 대한 수익을 최대화하도록 지원합니다. 또한 ControlSafe 확장 박스 플랫폼은 특정 적용 요건을 충족하도록 I/O 확장 서브시스템으로 구축할 수 있습니다.

Artesyn은 일관된 성능을 보이는 입증되고 신뢰할 수 있는 시스템을 바탕으로 당사 고객과 장기적 협력 관계를 구축하기 위해 노력합니다. 또한 ControlSafe Platform은 철도 산업 고객에게 15년의 기본 제품 수명과 25년의 장기 지원 및 서비스를 특징으로 하는 신뢰성 높은 플랫폼을 제공함으로써 이러한 의지를 더욱 공고히 하고 있습니다.

Artesyn의 미래 보장 개발 철학을 고수하는 ControlSafe 플랫폼은 제품 수명 주기 내내 새 프로세서 아키텍처뿐만 아니라 별도의 I/O 인터페이스를 무리 없이 수용하기 위해 모듈식 그리고 확장식으로 디자인되었습니다. Artesyn은 다양한 철로 신호 적용에 있어서 고객들이 당사의 ControlSafe 제품을 완벽하게 통합시킬 수 있도록 광범위한 제품 라인을 구축할 지속적인 개발에 초점이 맞춰져 있습니다. Artesyn의 궁극적 목적은 고객들이 최종 애플리케이션을 차별화하는데 개발 노력을 집중하게 함으로써 고객들의 경쟁적 위치를 고양시키는 것입니다.

**CONTROLSAFE 확장 박스 아키텍처**

데이터 락스텝 모드에서는 두 CPU에서 외 부와 주고 받는 모든 데이터 패킷에 대해서 두 CPU의 올바른 작동을 확인하기 위해 비교됩니다. 데이터 락스텝 모드에서는 두 CPU에서 외 부와 주고 받는 모든 데이터 패킷에 대해서 두 CPU의 올바른 작동을 확인하기 위해 비교됩니다. 프로세서 클럭이 동기화되고 결정적 경계가 프로세서의 주소와 데이터 버스에서 생성되는 하드 락스텝 모드와는 반대로, 데이터 락스텝 모드는 하드 락스텝 세이프티 아키텍처에 대해 실행 가능한 옵션이 아닌 현대 고성능 프로세서를 사용하여 실행할 수 있습니다.



데이터 패브릭 바운드 거래의 비교는 이 2개의 CPU 사이의 불일치가 실패로 간주되어 EXB를 페일 세이프 모드로 들어가게 만드는 2oo2 보팅 메커니즘을 사용하여 실행합니다. 페일 세이프 모드에서는 기본적으로 모든 출력 포트가 차단되므로 외부 장비로 잘못된 출력이 보내질 가능성을 없애줍니다.

EXB 데이터 락-스텝 아키텍처를 통해서 동일한 I/O를 유지하면서 시간 내내 프로세서 아키텍처를 업그레이드 할 수 있습니다. 하드웨어에 2oo2 보팅 기능을 구현함으로써 애플리케이션 개발자는 기존 애플리케이션 소프트웨어를 최소한의 수정으로 마이그레이션할 수 있습니다.

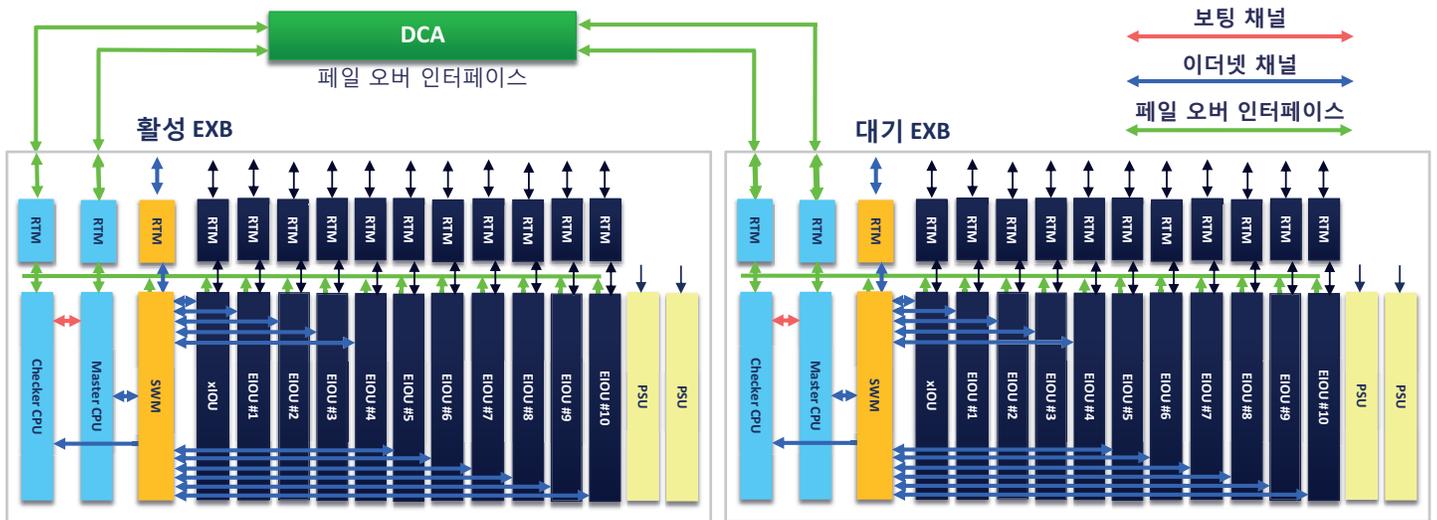
주로 지상 장치 적용을 대상으로 하는 Artesyn ControlSafe 확장 박스 플랫폼은 CAN, 이더넷, 이더넷 링, UART, 디지털 및 아날로그 같은 다양한 I/O 모듈을 지원하도록 설계되어 있어서 솔루션 통합자들은 손쉽게 새 설치를 취급하고 프로젝트를 업그레이드할 수 있습니다. 모든 커뮤니케이션 I/O 모듈은 동일한 NXP CPU 코어 및 동일한 Wind River VxWorks 653 운영 시스템에 기반한 공통 아키텍처를 갖추고 있으므로 소프트웨어 개발 환경을 단순화시킨다. 추가 확장을 원격 사시에 포함할 수 있는 순 조로운 분산 프로그래밍 모델을 허용하는 이더넷 상에서 모든 I/O 모듈에 액세스한다. 모든 모듈은 시스템이 작동 불가로 만드는 리스크 없이 원격 온라인 소프트웨어 및 펌웨어 업그레이드를 지원 한다. 모든 I/O 포트는 안전 또는 비안전 관련하여 사용자가 프로그램화할 수 있다. 또한 스위치 모듈은 애플리케이션 네트워크의 다른 프로세싱 노드나 동종 EXB에 직접적 이더넷/IP 액세스를 위해 자체의 후면 전환 모듈(RTM)을 통해 3개의 10/100/1000Base-T 포트를 제공합니다.

**사시 레벨의 장애 관리**

Artesyn의 ControlSafe 확장 박스 플랫폼은 런타임과 인라인 진단을 활용하여 사시 레벨의 장애 관리 기능을 제공합니다. 각 모듈은 시동에 적극적인 진단 점검(POST)을 실행하여 준비를 확실하게 합니다. 하드웨어 기반의 건강 및 안전 모니터링 서브시스템은 I/O 모듈을 포함하여 하나의 사시에 모든 모듈을 연결합니다. 하드웨어 기반의 인라인 진단은 사시의 전체 안전 경로에서 안전 기능에 대한 잠재적 결함을 지속적으로 점검하고 소프트웨어 런타임 진단에서는 진단 기능의 올바른 작동을 점검합니다. 하드웨어 탐지와 안전 관련 장애가 일어나면 모든 안전 기능이 자동안전장치 상태로 즉각 변환됩니다.

### CONTROLSAFE 확장 박스 플랫폼 아키텍처

Artesyn의 ControlSafe 확장 박스 플랫폼은 2개의 리던던트 EXB로 구성되어 있고 이 각각은 페일 세이프 운영을 실행할 뿐만 아니라 고도로 유용한 플랫폼을 제공합니다. 이 부품들은 2개의 EXB의 건전 상태를 모니터하고, 한 개는 ‘활성화’로 그리고 다른 한 개는 ‘대기’로 지정하는 직접 연결 알고리즘(DCA)에 의해 연결되어 있습니다. 활성 EXB에 작동하는 사용자 애플리케이션은 모든 I/O를 완전하게 제어합니다. 대기 EXB에 작동하는 동일한 사용자 애플리케이션은 안전 관련 입력을 모니터 할 수 있지만 기본적으로 어떤 안전 관련 출력도 구동할 능력이 없습니다. 활성 EXB에 문제가 생기면 안전 관련 출력이 중단되며, 상태 신호를 DCA를 통해 보내고, 이로 인해 대기 EXB가 활성화되고 안전 관련 출력 구동을 시작합니다. 결함이 있는 EXB는 작동을 중단하고 서비스 직원이 수리한 후 다시 서비스를 시작할 수 있습니다. 두 EXB의 건전 상태를 모니터하고 둘 사이의 페일오버 작동을 제어함으로써 고도로 유용한 페일 세이프 컴퓨팅 시스템을 제공합니다.



### 활성/대기 제어

Artesyn의 ControlSafe 확장 박스 플랫폼은 직접 연결 케이블링 방식으로 활성/대기 제어를 지원합니다.

### 직접 연결

직접 연결 방식은 특허 받은 알고리즘과 특수 케이블을 사용하여 2개의 EXB를 연결합니다. 건전 상태는 활성 및 대기 역할을 제어하기 위해 모든 CPU 모듈에서 작동하는 상태 머신에서 교환되고 추적됩니다. 전원을 공급하면 양 CPU에 건전 신호가 있는 첫 EXB가 활성화됩니다. 직접 연결 알고리즘(DCA)은 한 번에 한 EXB만 활성화되고 상태가 양호한 한 EXB만 활성화될 수 있도록 설계되어 있습니다.

### 세이프티 릴레이 박스

세이프티 릴레이를 선호하거나 필요로 하는 고객들에게 세이프티 릴레이 박스(SRB)는 ControlSafe 확장 박스 플랫폼의 리던던트 EXB 2개를 연결하는 대체 방식을 제공할 수 있습니다. 이 경우에 SRB는 Artesyn ControlSafe 포트폴리오의 첫 SIL4 인증 안전 플랫폼인 ControlSafe 플랫폼과 동일한 방식으로 가능합니다. SRB 사용자는 릴레이와 개별 로직을 사용하여 활성 EXB를 선택하고, 활성 EXB가 고장일 때 제어를 대기 EXB로 전환합니다. 또한 SRB는 오직 한 개의 EXB만 한 번에 활성화 하고 결함이 있는 EXB는 활성화될 수 없도록 합니다. 그러나 ControlSafe 확장 박스 플랫폼의 초기 출시에 대한 SIL4 인증은 직접 연결 기반의 구성만을 커버합니다. 고객이 SRB-기반 EXB 솔루션을 SIL4 적용 환경에 설치할 필요가 있을 경우, 이 옵션에 더욱 상세한 토론을 위해 Artesyn 지역 판매 팀에게 연락하십시오.

### 전원 서브시스템

EXB에는 리던던트 (1+1) AC 전원 공급 FRU(PSU)가 포함되어 있습니다. 둘 중 어느 것도 완전히 장착된 EXB에 전원을 공급할 수 있습니다. 한 개의 PSU에 문제가 생기면 다른 부품이 전원을 공급하여 계속 작동하도록 합니다. 소프트웨어는 PSU의 건전 상태를 모니터 할 수 있습니다.

### 냉각 서브시스템

팬 트레이 FRU가 포함되어 있어서 자율적으로 작동하도록 합니다. 주변의 유입구 온도가 설정 온도에 도달하면 팬 트레이가 켜집니다. 팬은 약 55°C에서 전속도로 올라갑니다. 소프트웨어는 팬 트레이의 건전상태와 작동 상태를 모니터 할 수 있습니다. 팬 트레이는 어느 단일 팬에 결함이 있어도 충분히 냉각시킬 수 있습니다.

### EIOU 개발

ControlSafe 확장 박스 플랫폼은 일반 베이스 플랫폼으로 설계되어 있어서 Artesyn EIOU 모듈의 지속적인 추가를 통해 다양한 적용이 가능하게 됩니다. 또한, Artesyn은 EIOU 모듈과 I/O 뒤판을 개발하고, 필요한 모든 기술 사양, 제품 지원 및 서비스를 제공함으로써 특정 수요를 충족할 수 있도록 고객들에게 유연성을 제공합니다. 비즈니스 모델은 Artesyn과 고객 사이의 협력을 증진하고 그들이 유용한 자원을 효과적이며 효율적으로 활용하여 새 개발을 취급하고 프로젝트를 업그레이드 할 수 있게 합니다.

### 운영 체제

ControlSafe Platform의 모든 모듈은 Wind River의 VxWorks 653 운영 체제를 지원합니다. 이 운영 체제는 리소스 관리와 파티션 환경을 모두 제공하므로 임계 수준이 다른 여러 독립된 애플리케이션을 보호된 조건의 단일 대상 플랫폼에서 실행할 수 있습니다. VxWorks 653의 핵심은 Core OS입니다. Core OS 구성 요소는 대상 아키텍처의 기능을 이용하여 별도의 파티션에 상주하고 있는 애플리케이션을 서로 격리시켜 줍니다. 파티션은 VxWorks 기반 API, APEX 인터페이스 (ARINC 653 인터페이스) 또는 POSIX API의 세 가지 인터페이스 레이어 중 하나를 지원합니다. 이러한 인터페이스 레이어는 애플리케이션에 다양한 수준의 스케줄링과 스레드 관리 기능을 제공합니다. 파티션 메모리와 CPU 시간 사용을 제어 외에 Core OS는 I/O 같은 시스템 리소스를 관리하는 서비스도 제공합니다.



Core OS는 CPU 사이클을 각 파티션에 할당하고 파티션 실행 순서를 지정하는 정적으로 정의된 구성 테이블을 사용하여 파티션 스케줄러를 구현합니다. Core OS는 시스템 시간과 메모리를 포함하여 애플리케이션 파티션을 대신하여 모든 공유 리소스를 관리합니다. Core OS는 파티션 전환 후에 애플리케이션이 서로 방해하지 않도록 해줍니다. 파티션간의 통신, 파티션과 Core OS 간의 통신은 적절한 통신 채널이 사용되고 시스템 구성 테이블에서 허용되는 경우에만 수행됩니다.

VxWorks 653 Health Monitor (HM)는 시스템에서 알람이나 메시지 같은 이벤트를 발생시키고 처리하는 프레임워크를 제공합니다. 이 프레임워크는 ARINC API를 지원하며 독립 실행형 API를 포함합니다. HM은 모듈, 파티션 및 프로세스 세 가지 수준에서 작동합니다. 결함 응답과 회복 동작은 파티션과 모듈 수준에서 테이블 중심으로 이루어지는 반면 애플리케이션 작동은 프로세스 수준에서 이루어집니다. 파티션 또는 모듈 수준 처리기는 해당 이벤트를 통보함으로써 다른 파티션에 정보를

### 애플리케이션 개발 환경

명령 라인 도구는 프로젝트를 구축하거나, XML 및 부품을 사용하여 구성하거나, 운영 시스템을 모니터링하고 디버그 하도록 제공됩니다. VxWorks 653 애플리케이션을 작성하고 특정 참조 하드웨어 필요 없이 Windows 플랫폼에서 테스트하는 기능을 제공하는 VxWorks 653 시뮬레이터도 포함되어 있습니다. VxWorks 653 환경은 호스트 애플리케이션이 호스트 컴퓨터에 상주하고 있는 대상 서버와 통신할 수 있는 WTX (Wind River tool exchange) 프로토콜을 지원합니다.

- 제어/상태
- DRAM 스크레버
- 펌웨어 업그레이드
- 플래시 무결성
- 링크 상태 확인
- 로깅
- 유지관리 모드 감시
- 네트워크 라우팅
- 지속적 DRAM
- 플랫폼 관리
- 런타임 진단
- 스위치 관리
- 안전 레이어
- 중요 제품 데이터(MPD)
- 보팅 로직

### 인증 증거

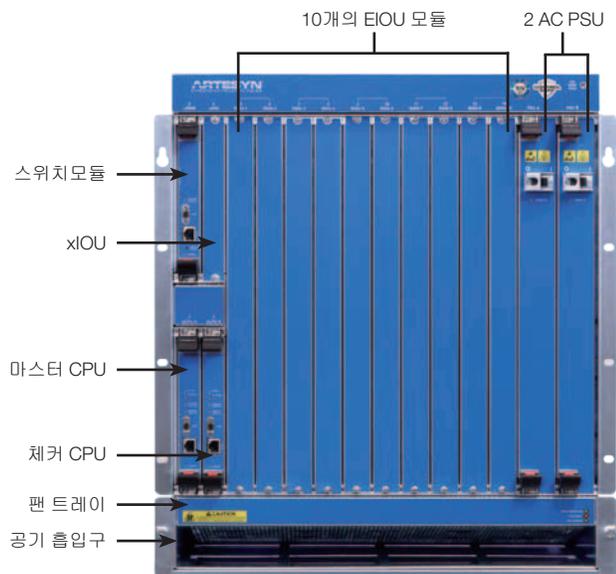
Artesyn의 ControlSafe 확장 박스 플랫폼은 현대적인 안전 적용을 위해 고도로 안정적이며 유용한 플랫폼을 제공하는 필요한 모든 산업 사양 및 표준을 엄격하게 준수합니다. Artesyn은 통합 시스템에서 인증 프로세스가 용이하도록 완벽한 인증 증거 패키지를 고객에게 제공합니다.

인증 증거 패키지는 다음과 같습니다.

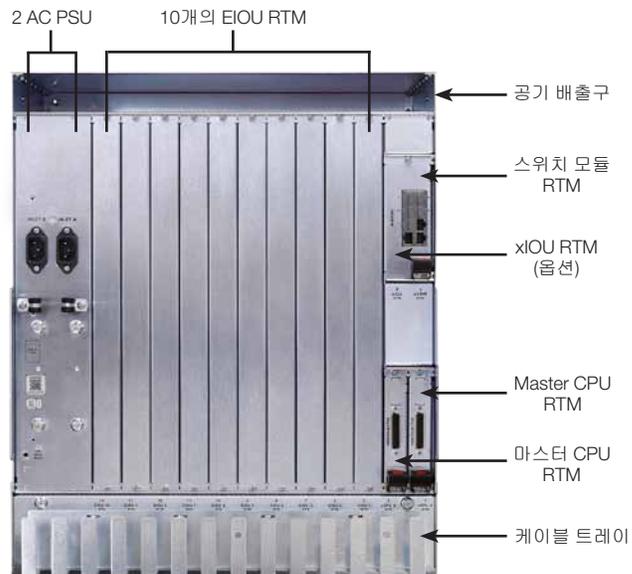
- 안전 사례
  - 시스템 정의
  - 품질 관리 보고서
  - 안전 관리 보고서
  - 기술 안전 보고서
- 안전 평가 보고서
- 안전 매뉴얼
  - 또한 이 부품은 Artesyn의 ControlSafe 확장 박스 플랫폼을 안전 관련 시스템에 통합하는데 필요한 사용자 조치를 명시합니다
- TÜV SÜD에 의해 발행된 안전 인증 번호 Z10 16 10 87324 011

시스템 새시

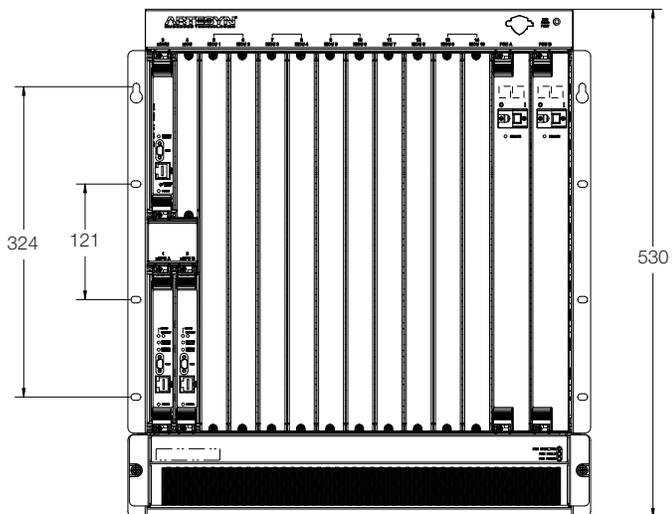
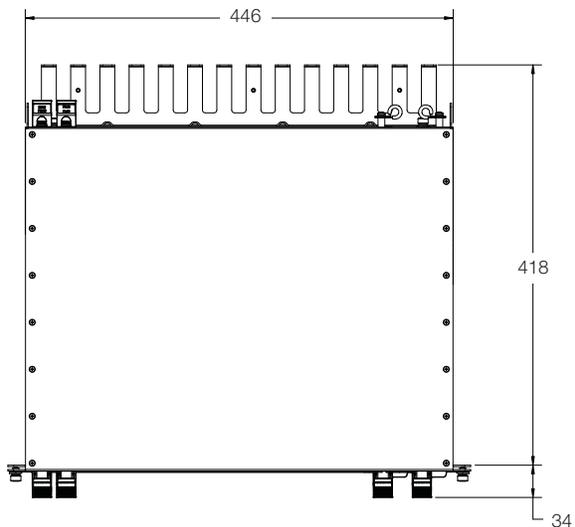
정면 뷰



후면 뷰

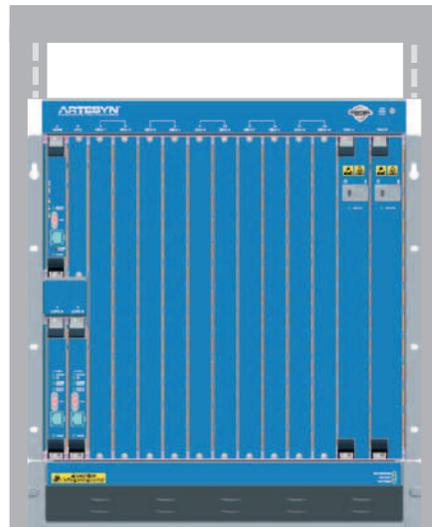


EXB 치수 (단위: mm)

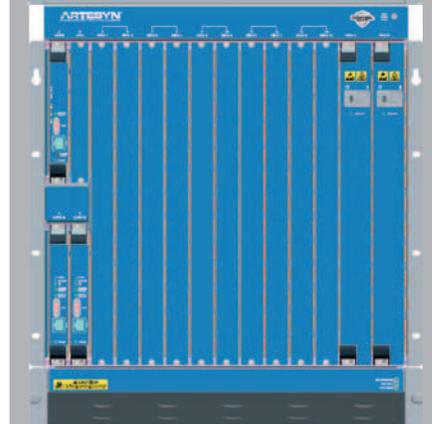


시스템 랙 마운팅 예

EXB #1 - 12U



EXB #2 - 12U



싱글 EXB - 12U



**기술 사양**

	<i>프로세서 모듈</i>	<i>스위치 모듈 및 IOU 모듈</i>
프로세서	NXP P2020 (1 GHz)	NXP P1011 (800 MHz)
운영 체제	VxWorks 653	VxWorks 653
메모리	1GB (옵션 4GB) DDR3-800 SDRAM, ECC	512MB (옵션 2GB) DDR3-667 SDRAM, ECC
플래시	2 X 128MB NOR	2 X 64MB NOR
MRAM	2 X 2MB MRAM	1 X 2MB MRAM
전면 패널 유지관리 포트	10/100/1000 BASE-T 및 RS232	10/100/1000 BASE-T 및 RS232 (스위치 모듈만 해당)
데이터 구조	14개의 GigE 링크	
보드 관리	전압과 온도 센서	

**I/O 인터페이스**

IOU 슬롯 숫자	10개의 9U 확장 IOU(EIOU); 1개의 4U (1) xIOU
10/100/1000 BASE-T 이더넷 포트	표준: 스위치 모듈 3개

**물리적 사양**

작동 온도	-40°C ~ 70°C
냉각	강제 공기 및 대류 냉각
전원	AC: 90-264V, 47-63Hz
진동	EN 61373, 카테고리 1, 등급 B(EN 50155 12.2.11) 준수
충격	EN 61373, 카테고리 1, 등급 B(IEC 60068-2-27) 준수
새시 씰링	표준: IP20; 옵션: IP30
보호 코팅	EN 50155 Section 12.2.10의 경우 ST1 등급 (소금 분무 테스트)
표준	EN50121, EN50124, EN50155, EN50126, EN50128, EN50129, EN55024, EN60529, EN60571, IEC61508에 따라 고안됨. 특정 준수 내용을 보려면 문서 참조.
안전 인증	EN50126, EN 50128, EN50129(SIL4) 및 IEC61508(SIL3) (TÜV SÜD에 의해 발행된 안전 인증 번호 Z10 16 10 87324 011)

주문 정보	
부품 번호	설명
CSP-EXB-CORE-AC-01	1개의 샤시, 2개의 AC 전원 공급장치, 2개의 CPU 모듈, 1개의 스위치 모듈과 1개의 팬 트라이로 구성된 ControlSafe 확장 박스 플랫폼 코어
CSP-EXB-FILL-01	4U 전면 필러 패널
CSP-EXB-FILL-02	9U 전면 필러 패널
CSP-EXB-FILL-RTM-01	3U 후면 필러 패널
CSP-EXB-FILL-RTM-02	9U 후면 필러 패널
CSP-CBL-DIRECT-01	직접 연결(DCA) 작동을 위한 2개의 케이블
CSP-CBL-PWR-B-01	미국/캐나다/일본 용도의 전원 코드
CSP-CBL-PWR-EU-01	한국/독일/프랑스 용도의 전원 코드
CSP-CBL-PWR-I-01	중국 용도의 전원 코드
SERIAL-MINI-D2	시리얼 케이블 - 표준 DE9에 마이크로 D-서브 커넥터

참고: ControlSafe 확장 박스 플랫폼 코어의 부품은 이 표에는 열거되어 있지 않지만 예비 부품으로 별도 주문할 수 있습니다. 더욱 상세내용에 대해서는 Artesyn 지역 판매팀에 연락하십시오.

## SOLUTION SERVICES

Artesyn Embedded Technologies provides a portfolio of solution services optimized to meet your needs throughout the product lifecycle. Design services help speed time-to-market. Deployment services include global 24x7 technical support. Renewal services enable product longevity and technology refresh.

## WORLDWIDE OFFICES

<b>United States</b>	+1 888 412 7832	<b>Japan</b>	+81 3 5403 2730
<b>Hong Kong</b>	+852 2176 3540	<b>Korea</b>	+82 2 6004 3268
<b>China</b>	+86 400 8888 183		

Artesyn Embedded Technologies, Artesyn and the Artesyn Embedded Technologies logo are trademarks and service marks of Artesyn Embedded Technologies, Inc. All other names and logos referred to are trade names, trademarks, or registered trademarks of their respective owners. © 2017 Artesyn Embedded Technologies, Inc.  
All rights reserved. For full legal terms and conditions, please visit [www.artesyn.com/legal](http://www.artesyn.com/legal).



[www.artesyn.com](http://www.artesyn.com)

ControlSafe EXB Platform-DS\_K 06Sep2017