OMRON

내환경 리모트 터미널

NXR-S 시리즈

심플 로직 세이프티 I/O 블록 CIP Safety 대응

유저 매뉴얼

NXR-SXD1204-CST
NXR-SXD1204B-CST

⚠ 안내 (For Reference Only)

본 문서는 AI 번역으로 작성된 참고용 국문자료 입니다.
일부 표현은 원문과 다소 다를 수 있으며,
중요한 내용은 원문과 함께 참고해 주시기 바랍니다.

세이프티 I/O 블록



원본 지침서

W645-E1-02

참고

· 모든 권리가 보호됩니다. 본 발행물의 어떠한 부분도 복제, 검색 시스템에 저장 또는 전송할 수 없으며, 그 방식은 기계적, 전자적, 복사, 녹음 또는 그 밖의 어떠한 형태나 수단이든 오므론의 사전 서면 허가 없이는 불가합니다.

· 본 문서에 포함된 정보의 사용과 관련하여 특허 책임을 지지 않습니다. 또한, 오므론은 고품질 제품의 개선을 위해 끊임없이 노력하고 있으므로, 본 매뉴얼에 포함된 정보는 예고 없이 변경될 수 있습니다.

· 본 매뉴얼의 작성에는 만전을 기했습니다. 그럼에도 불구하고 오므론은 오류나 누락에 대해 책임을 지지 않습니다. 또한 본 발행물에 포함된 정보의 사용으로 인해 발생하는 손해에 대해서도 책임을 지지 않습니다.

상표

· Sysmac 및 SYSMAC은 일본 및 그 밖의 국가에서 오므론 팩토리 오토메이션 제품에 대한 오므론 주식회사의 상표 또는 등록상표입니다.

· Smartclick은 일본 및 그 밖의 국가에서 오므론 주식회사의 상표 또는 등록상표입니다. 국가에서 통용됩니다.

· Microsoft, Windows, Excel, Visual Basic, Microsoft Edge는 다음의 등록상표 또는 미국 및 그 밖의 국가에서의 Microsoft Corporation의 상표입니다.

· EtherCAT®은 등록상표이자 특허 기술이며, 독일 Beckhoff Automation GmbH가 라이선스했습니다.

· Safety over EtherCAT®은 등록상표이자 특허 기술이며, Beckhoff Automation GmbH(독일)가 라이선스했습니다.

· ODVA, CIP, CompoNet, DeviceNet, EtherNet/IP, CIP Safety는 ODVA의 상표입니다.

· ODVA 및 CIP Safety 로고는 ODVA의 상표입니다.

· SD 및 SDHC 로고는 SD-3C, LLC의 상표입니다.

AI 번역본
-For Reference Only-

본 문서에 기재된 그 밖의 회사명 및 제품명은 각 회사의 상표 또는 등록상표입니다.

저작권

· Microsoft 제품의 화면 캡처는 Microsoft의 허가를 받아 사용되었습니다.

· 본 제품에는 일부 타사 소프트웨어가 포함되어 있습니다. 이 소프트웨어의 라이선스 및 저작권 정보는 http://www.fa.omron.co.jp/nj_info_e/ 및 http://www.fa.omron.co.jp/nx_info_e/ 에서 확인할 수 있습니다.

소개

내환경 리모트 터미널 NXR-S 시리즈 심플 로직 세이프티 I/O
블록 CIP Safety 대응 제품(이하 세이프티 I/O 블록이라 함)을 구입해 주셔서 감사합니다.
본 매뉴얼에는 세이프티 I/O 블록을 사용하는 데 필요한 정보가 수록되어 있습니다. IO-Link 시스템을 구축하기 전에 본 매뉴얼을 잘 읽고 유닛의 기능과 성능을 충분히 이해하시기 바랍니다.
본 매뉴얼은
운용 중에도 언제든지 참조할 수 있도록 안전한 장소에 보관하십시오.

대상 독자

본 매뉴얼은 전기 시스템에 관한 지식(전기 기술자 또는 이에 준하는 지식)을 갖춘 다음의 담당자를 대상으로 합니다.

- FA 시스템 도입 담당자
- FA 시스템 설계 담당자
- FA 시스템 설치 및 보수 담당자
- FA 시스템 및 설비 관리 담당자

프로그래밍과 관련하여, 본 매뉴얼은 국제 표준 IEC 61131-3 또는 일본 표준 JIS B 3503의 프로그래밍 언어 사양을 이해하는 담당자를 대상으로 합니다.

적용 제품

본 매뉴얼은 다음 제품을 다룹니다.

- 내환경 리모트 터미널 NXR-S 시리즈 심플 로직 세이프티 I/O 블록 CIP Safety 대응 NXR-SXD1204-CST

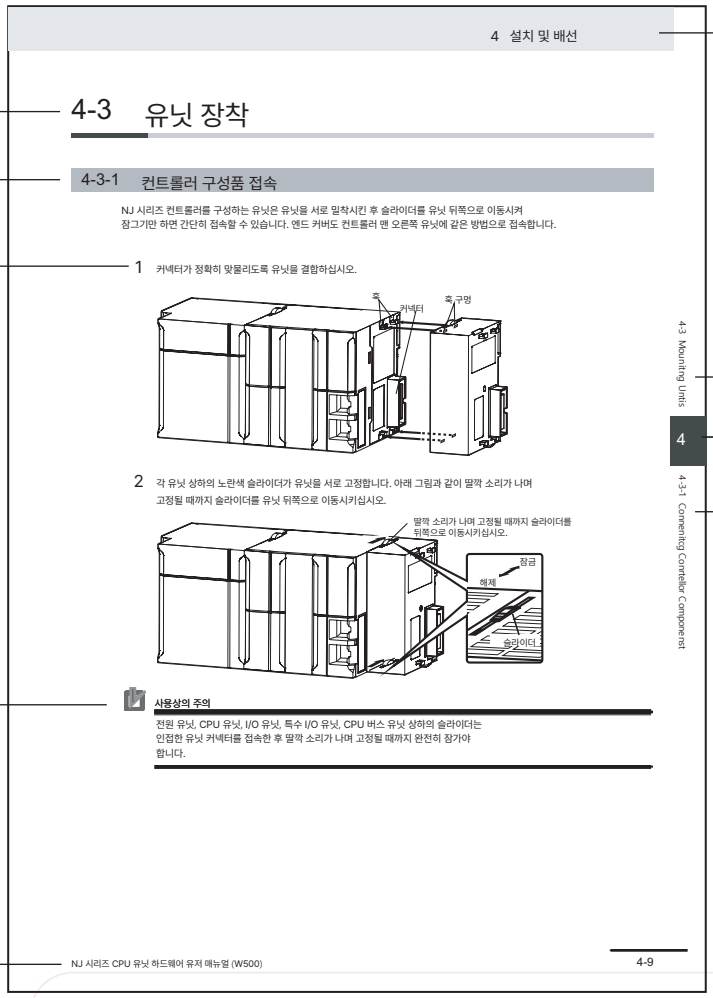
  NXR-SXD1204B-CST

AI 번역본
-For Reference Only-

매뉴얼 구성

페이지 구성

본 매뉴얼에서는 다음과 같은 페이지 구성을 사용합니다.



레벨 2 표제

레벨 3 표제

절차의 한 단계
절차를 나타냅니다.

특별 정보
아이콘은
주의사항, 추가 정보 또는
참조 정보를 나타냅니다.

매뉴얼명

레벨 1 표제

레벨 2 표제

레벨 3 표제
현재 표제를
표시합니다.

페이지 탭
주요 섹션의 번호를
표시합니다.

이 그림은 예시로만 제공된 것입니다. 본 매뉴얼에 그대로 나타나지 않을 수 있습니다.

AI 번역본
-For Reference Only-

특별 정보

본 매뉴얼의 특별 정보는 다음과 같이 분류됩니다.

안전 사용을 위한 주의사항

제품의 안전한 사용을 위해 해야 할 일과 하지 말아야 할 일에 관한 주의사항입니다.

사용상의 주의

올바른 동작과 성능을 위해 해야 할 일과 하지 말아야 할 일에 관한 주의사항입니다.

추가 정보

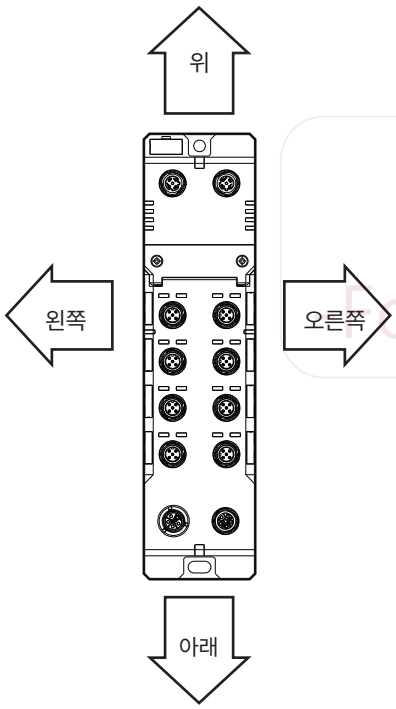
필요에 따라 참조할 추가 정보입니다.
이 정보는 이해를 돕거나 조작을 쉽게 하기 위해 제공됩니다.

버전 정보

유닛 버전이 다른 컨트롤러와 지원 소프트웨어의 버전이 다른 경우의 사양 및 기능 차이에 관한 정보입니다.

용어에 관한 주의사항

- 본 매뉴얼에서 "다운로드"는 지원 소프트웨어에서 실기기로 데이터를 전송하는 것을, "업로드"는 실기기에서 지원 소프트웨어로 데이터를 전송하는 것을 가리킵니다.
- 본 매뉴얼에서 유닛의 방향은 다음 그림과 같이 나타내며, 이는 유닛의 정면도를 나타냅니다.



AI 번역본
For Reference Only-

AI 번역본
-For Reference Only-

매뉴얼의 섹션 구성

1 특징 및 시스템 구성

2 사양 및 적용 절차

3 각부 명칭과 기능

4 전원 시스템 설계

5 설치 및 배선

6 세이프티 I/O 블록의 동작

7 세이프티 I/O 블록 설정

8 세이프티 I/O 블록의 기능

9 안전 응답 성능

10 보안 가이드라인

11 문제 해결

12 점검 및 보수

A 부록

I 색인

AI 번역본
-For Reference Only-

목차

소개 **1**
대상 독자 1
적용 제품 1

매뉴얼 구성 **2**
페이지 구성 2
특별 정보 3
용어에 관한 주의사항 3

매뉴얼의 섹션 구성 **5**

계약 조건 **13**
보증, 책임의 제한 13
적용 시 고려사항 14
면책사항 14
예상 사용 사례 및 위협에 대한 보안 책임에 관한 성명 15

안전상의 주의사항 **16**
주의 정보의 정의 16
기호 16
경고 17
주의 23

안전 사용을 위한 주의사항 **24**

사용상의 주의 **27**

법규 및 규격 **29**
EU 지침 및 규정 적합 29
EN ISO 13849-1 적합 30
UL 및 CSA 규격 적합 30
조선 규격 적합 31
KC 인증 적합 31

유닛 버전 **32**
유닛 버전 32

관련 매뉴얼 **34**

용어 **36**

개정 이력 **38**

AI 번역본
-For Reference Only-

섹션 1 특징 및 시스템 구성

1-1 세이프티 I/O 블록 개요 **1-2**
1-2 세이프티 I/O 블록의 특징 **1-3**
1-3 시스템 구성 **1-4**
1-3-1 세이프티 제어 시스템 1-4
1-3-2 네트워크 토폴로지 1-13
1-3-3 캐스케이드 접속 1-14
1-4 지원 소프트웨어 **1-16**

섹션 2 사양 및 적용 절차

2-1 사양 2-2
2-1-1 일반 사양 2-2
2-1-2 통신 사양 2-3
2-1-3 세이프티 사양 2-4
2-1-4 유닛 사양 2-6

2-2 사용 절차 2-9
2-2-1 Step 1. 시스템 설계 2-9
2-2-2 Step 2. 소프트웨어 설계 2-9
2-2-3 Step 3. 하드웨어 설계 2-10
2-2-4 Step 4. 안전 응답 성능 계산 및 검증 2-10
2-2-5 Step 5. 소프트웨어 설정 및 프로그래밍 2-11
2-2-6 Step 6. 설치 및 배선 2-11
2-2-7 Step 7. 동작 확인 2-12
2-2-8 Step 8. 운용, 보수 및 점검 2-13

섹션 3 각부 명칭과 기능

3-1 각부 명칭 3-2

3-2 표시등 3-5
3-2-1 상태 표시등 3-5
3-2-2 I/O 표시등 3-8
3-2-3 유닛 식별 표시등 3-9

3-3 로터리 스위치 3-10

3-4 커넥터 3-11
3-4-1 EtherNet/IP 통신 커넥터 3-11
3-4-2 전원 커넥터 3-11
3-4-3 I/O 커넥터 3-12

섹션 4 전원 시스템 설계

4-1 전원 종류 및 전원 시스템 4-2
4-1-1 전원 종류 및 용도 4-2
4-1-2 전원 시스템 4-2

4-2 전원 시스템 설계 4-6
4-2-1 전원 시스템 설계 절차 4-6
4-2-2 다이렉트 전원 공급 방식의 설계 방법 4-6
4-2-3 스루 배선을 이용한 전원 시스템의 설계 방법 4-13

4-3 전원 및 보호 장치 선정 4-21
4-3-1 외부 전원 선정 4-21
4-3-2 보호 장치 선정 4-21

AI 번역본
For Reference Only-

섹션 5 설치 및 배선

5-1 유닛 설치 5-2
5-1-1 설치 시 주의사항 5-2
5-1-2 설치 방향 5-2
5-1-3 설치 방법 5-3

5-2 EtherNet/IP 네트워크 배선 5-5
5-2-1 설치 시 주의사항 5-5
5-2-2 통신 케이블 접속 5-6

5-3 전원 배선 5-12
5-3-1 설치 시 주의사항 5-12

5-3-2 전원 케이블, 조임 공구 및 사용 조임 토크 5-12
5-3-3 외부 전원에 전원 케이블 접속 5-13
5-3-4 전원 케이블 접속 5-14

5-4 I/O 케이블 배선 5-19
5-4-1 설치 시 주의사항 5-19
5-4-2 I/O 케이블 접속 5-19
5-4-3 배선 예 5-24

5-5 접속 기기 5-29
5-5-1 Ethernet 케이블 5-29
5-5-2 전원 케이블 5-31
5-5-3 I/O 케이블 5-34
5-5-4 커넥터용 방수 커버 5-38

5-6 옵션 5-39
5-6-1 마커 5-39

섹션 6 세이프티 I/O 블록의 동작

6-1 동작 개요 6-2

6-2 CIP Safety 통신 6-4

6-3 EtherNet/IP 통신 6-6
6-3-1 태그 데이터 링크 통신 6-6
6-3-2 익스플리시트 메시지 통신 6-6

6-4 세이프티 입력 기능 6-8
6-4-1 접속 가능 기기 6-8
6-4-2 테스트 출력 기능 6-10
6-4-3 테스트 펄스 평가 기능 6-10
6-4-4 듀얼 채널 평가 6-11
6-4-5 세이프티 입력 단자의 진단 기능으로 검출 가능한 에러 6-12
6-4-6 입력 필터 기능 6-13
6-4-7 입력 에러 래치 시간 6-15

6-5 세이프티 출력 기능 6-16
6-5-1 접속 가능 기기 6-16
6-5-2 테스트 펄스 평가 기능 6-16
6-5-3 듀얼 채널 평가 6-17
6-5-4 세이프티 출력 단자의 진단 기능으로 검출 가능한 에러 6-18
6-5-5 출력 에러 래치 시간 6-18
6-5-6 EDM 피드백 6-19
6-5-7 출력 지연 6-19

6-6 로직 기능 6-20
6-6-1 논리 처리 6-20

6-7 세이프티 애플리케이션 6-23
6-7-1 세이프티 애플리케이션의 목적 6-23
6-7-2 세이프티 애플리케이션의 종류 6-23
6-7-3 고정 애플리케이션 상세 6-27

6-8 운용 모드 6-47
6-8-1 운용 모드 종류 6-47
6-8-2 각 운용 모드에서 실행 가능한 기능 6-48
6-8-3 각 운용 모드에서 실행 가능한 Web UI 기능 6-50
6-8-4 운용 모드 변경 및 전원 투입 모드 6-51

섹션 7 세이프티 I/O 블록 설정

7-1 설정 절차 7-3
7-1-1 세이프티 컨트롤러가 제어를 수행하도록 하는 컨피규레이션 설정 절차 (Type 1 Safety Open을 사용한 컨피규레이션) 7-3

AI 번역본
For Reference Only

7-1-2 세이프티 컨트롤러가 제어를 수행하도록 하는 컨피규레이션 설정 절차 (Web UI를 사용한 컨피규레이션) 7-6
7-1-3 프리셋 세이프티 애플리케이션을 사용하여 제어를 수행하도록 하는 세이프티 I/O 블록의 컨피규레이션 설정 절차 7-9
7-1-4 사용자가 설계한 세이프티 애플리케이션으로 제어를 수행하도록 하는 세이프티 I/O 블록의 컨피규레이션 설정 절차 (집중 관리 방식) 7-11
7-1-5 사용자가 설계한 세이프티 애플리케이션으로 제어를 수행하도록 하는 세이프티 I/O 블록의 컨피규레이션 설정 절차 (분산 관리 방식) 7-14

7-2 Web UI 개요 7-17
7-2-1 Web UI의 각종 사양 7-17
7-2-2 Web UI의 조작 권한 7-17
7-2-3 Web UI의 화면 구성 7-17
7-2-4 메인 메뉴 일람 7-18
7-2-5 Web UI 시작 절차 7-21
7-2-6 로그인 7-22
7-2-7 로그아웃 7-24
7-2-8 최초 로그인 시 주의사항 7-24

7-3 CIP Safety 통신 설정 7-27
7-3-1 CIP Safety 통신 접속 설정 7-27
7-3-2 세이프티 I/O 블록 설정의 익스포트 및 임포트 7-36

7-4 EtherNet/IP 통신 설정 7-38
7-4-1 태그 데이터 링크 통신 설정 7-38
7-4-2 LLDP 기능 7-42

7-5 세이프티 입력 기능 설정 7-44
7-5-1 세이프티 입력 기능 설정 절차 7-44
7-5-2 표준 출력 기능 설정 절차 7-47

7-6 세이프티 출력 기능 설정 7-50
7-6-1 세이프티 출력 기능 설정 절차 7-50

7-7 로직 기능 설정 7-53
7-7-1 로직 설정 절차 7-53
7-7-2 파라미터 리스트 표시 7-58
7-7-3 고려해야 할 입력 기기의 이상 동작 예 7-59

7-8 세이프티 시그니처 설정 7-63

7-9 세이프티 애플리케이션 파일 작성 7-65
7-9-1 세이프티 I/O 블록 등록 7-65
7-9-2 세이프티 애플리케이션 설정 7-66
7-9-3 세이프티 I/O 기능 설정 7-68
7-9-4 로직 기능 설정 7-68
7-9-5 세이프티 애플리케이션 파일 익스포트 7-68

7-10 IP 주소 설정 7-71
7-10-1 IP 주소 구성 7-71
7-10-2 로터리 스위치를 이용한 IP 주소 설정 방법 선택 7-73
7-10-3 Sysmac Studio를 이용한 설정 7-74
7-10-4 Web UI를 이용한 설정 7-76

7-11 TUNID 설정 7-78
7-11-1 TUNID의 목적 7-78
7-11-2 TUNID 설정 절차 7-78

7-12 세이프티 애플리케이션 선택 7-83

7-13 리스타트 7-84
7-13-1 리스타트의 목적 7-84
7-13-2 리스타트 사용 절차 7-84

7-14 컨피규레이션 7-87
7-14-1 세이프티 컨트롤러 컨피규레이션 7-87
7-14-2 세이프티 I/O 블록의 컨피규레이션 7-87

7-15 자동 시각 조정 설정 7-91
7-15-1 자동 시각 조정의 목적 7-91
7-15-2 자동 시각 조정 사용 절차 7-91

AI 번역본
-For Reference Only-

7-15-3 자동 시각 조정 상세 7-94

7-16 운용 모드 변경 7-95
7-16-1 운용 모드 변경 사용 절차 7-95

7-17 컨피규레이션 잠금 7-99
7-17-1 컨피규레이션 잠금의 목적 7-99
7-17-2 컨피규레이션 잠금 사용 절차 7-99
7-17-3 컨피규레이션 잠금 상세 7-103

7-18 세이프티 비밀번호 설정 7-104
7-18-1 세이프티 비밀번호의 목적 7-104
7-18-2 세이프티 비밀번호 설정 사용 절차 7-104
7-18-3 세이프티 비밀번호 상세 7-106

7-19 백업 7-108
7-19-1 백업의 목적 7-108
7-19-2 백업 사용 절차 7-108
7-19-3 백업 상세 7-111

섹션 8 세이프티 I/O 블록의 기능

8-1 기능 일람 8-3

8-2 전체 메모리 클리어 기능 8-4
8-2-1 전체 메모리 클리어 기능의 목적 8-4
8-2-2 전체 메모리 클리어 기능 사용 절차 8-4
8-2-3 전체 메모리 클리어 기능 상세 8-7

8-3 HTTPS 통신 기능 8-8
8-3-1 HTTPS 통신 기능의 목적 8-8
8-3-2 HTTPS 통신 기능 사용 절차 8-8
8-3-3 HTTPS 통신 기능 상세 8-9

8-4 디바이스 레벨 링(DLR) 기능 8-10
8-4-1 DLR 기능의 목적 8-10
8-4-2 DLR 기능 사용 절차 8-10
8-4-3 DLR 기능 상세 8-10

8-5 스루 배선 출력용 전원 OFF 기능 8-11
8-5-1 스루 배선 출력용 전원 OFF 기능의 목적 8-11
8-5-2 스루 배선 출력용 전원 OFF 기능 사용 절차 8-11

8-6 I/O 배선 점검 기능 8-13
8-6-1 I/O 배선 점검 기능의 목적 8-13
8-6-2 I/O 배선 점검 기능의 동작 8-13
8-6-3 I/O 배선 점검 기능을 위한 I/O 구성 설정 8-13
8-6-4 I/O 배선 점검 기능 사용 절차 8-14

8-7 범용 CIP 커맨드 전송 기능 8-15
8-7-1 범용 CIP 커맨드 전송 기능의 목적 8-15
8-7-2 범용 CIP 커맨드 전송 기능 사용 절차 8-15

8-8 유닛 식별 기능 8-16
8-8-1 유닛 식별 기능의 목적 8-16
8-8-2 유닛 식별 기능 사용 절차 8-16
8-8-3 유닛 식별 기능 상세 8-18

8-9 IP 주소 표시 기능 8-19
8-9-1 IP 주소 표시 기능의 목적 8-19
8-9-2 IP 주소 표시 기능 사용 절차 8-19
8-9-3 IP 주소 표시 기능 상세 8-19

8-10 전원 모니터 기능 8-22
8-10-1 전원 모니터 기능의 목적 8-22
8-10-2 전원 모니터 기능 사용 절차 8-22
8-10-3 전원 모니터 기능 상세 8-24

8-11 I/O 모니터 기능 8-27

AI 번역본
-For Reference Only-

8-11-1 I/O 모니터 기능의 목적 8-27
8-11-2 I/O 모니터 기능 사용 절차 8-27

8-12 접점 동작 횟수 모니터 기능 8-29
8-12-1 접점 동작 횟수 모니터 기능의 목적 8-29
8-12-2 세이프티 입력 단자에서의 사용 절차 8-29
8-12-3 세이프티 출력 단자에서의 사용 절차 8-29

8-13 통신 케이블 진단 기능 8-31
8-13-1 통신 케이블 진단 기능의 목적 8-31
8-13-2 통신 케이블 진단 기능 사용 절차 8-31
8-13-3 통신 케이블 진단 기능 상세 8-33

8-14 펌웨어 업데이트 기능 8-35
8-14-1 펌웨어 업데이트 기능의 목적 8-35
8-14-2 펌웨어 업데이트 기능 사용 절차 8-35
8-14-3 펌웨어 업데이트 기능 상세 8-36

섹션 9 안전 응답 성능

9-1 세이프티 I/O 블록의 안전 응답 성능 9-2
9-1-1 안전 응답 성능 계산 9-2
9-1-2 안전 응답 성능 검증 9-5

섹션 10 보안 가이드라인

10-1 세이프티 I/O 블록이 제공하는 심층 방어 10-2
10-1-1 세이프티 I/O 블록의 동작 환경 10-2
10-1-2 세이프티 I/O 블록을 이용한 기술 계층 보안 대책 10-3

10-2 자산을 보호하기 위한 세이프티 I/O 블록의 보안 기능 10-5
10-2-1 통신 회선상의 데이터 보호 10-5
10-2-2 세이프티 I/O 블록에 대한 외부 공격 차단 10-7
10-2-3 세이프티 I/O 블록에 대한 무단 조작 방지 10-9
10-2-4 세이프티 I/O 블록 자산의 변조 방지 10-10
10-2-5 세이프티 애플리케이션 파일 및 백업 파일 보호 10-11
10-2-6 부인 방지 10-12

10-3 보안 패치 적용 10-13
10-3-1 세이프티 I/O 블록 업데이트 10-13
10-3-2 Sysmac Studio 업데이트 10-13
10-3-3 PC의 OS 업데이트 10-13

10-4 기기의 안전한 폐기 10-14
10-4-1 세이프티 I/O 블록 내 자산 삭제 10-14

AI 번역본
-For Reference Only-

섹션 11 문제 해결

11-1 에러 확인 11-2
11-1-1 에러 통지 방법 및 확인해야 할 정보 11-2
11-1-2 에러 확인 방법 11-2
11-1-3 동작 상태 모니터 기능 11-3

11-2 이벤트를 이용한 에러 확인 및 문제 해결 11-6
11-2-1 이벤트 로그 기능 11-6
11-2-2 Sysmac Studio를 이용한 이벤트 확인 11-6
11-2-3 Web UI를 이용한 이벤트 확인 11-9
11-2-4 이벤트 상세 및 문제 해결 11-12

섹션 12 점검 및 보수

12-1 청소 및 점검 12-2
12-1-1 청소 12-2
12-1-2 점검 절차 12-2

12-2 유닛 교체 12-4
12-2-1 유닛 교체 시 주의사항 12-4
12-2-2 백업 기능을 이용한 유닛 교체 12-4
12-2-3 백업 기능을 사용하지 않는 유닛 교체 12-5

부록

A-1 외형 치수 A-2

A-2 세이프티 I/O 어셈블리 데이터 A-4
A-2-1 세이프티 입력 어셈블리 데이터 A-4
A-2-2 세이프티 출력 어셈블리 데이터 A-6
A-2-3 컨피규레이션 어셈블리 데이터 A-7

A-3 I/O 어셈블리 포트 및 대응하는 세이프티 I/O 어셈블리 데이터 요소 A-14

A-4 지원 CIP 오브젝트 A-16
A-4-1 아이덴티티 오브젝트(Class ID: 01 Hex) A-17
A-4-2 어셈블리 오브젝트(Class ID: 04 Hex) A-19
A-4-3 유닛 매니저 오브젝트(Class ID: 380 Hex) A-22
A-4-4 이벤트 히스토리 로그 오브젝트(Class ID: 34B Hex) A-27
A-4-5 에러 이벤트 오브젝트(Class ID: 34C Hex) A-30
A-4-6 세이프티 디스크리트 입력 포인트(SDIP) 오브젝트(Class ID: 3D Hex) A-33
A-4-7 세이프티 디스크리트 출력 포인트(SDOP) 오브젝트(Class ID: 3B Hex) A-35
A-4-8 디바이스 레벨 링(DLR) 오브젝트(Class ID: 47 Hex) A-37
A-4-9 QoS 오브젝트(Class ID: 48 Hex) A-39
A-4-10 TCP/IP 인터페이스 오브젝트(Class ID: F5 Hex) A-41
A-4-11 이더넷 링크 오브젝트(Class ID: F6 Hex) A-45
A-4-12 LLDP 관리 오브젝트(Class ID: 109 Hex) A-51
A-4-13 LLDP 데이터 테이블 오브젝트(Class ID: 10A Hex) A-53
A-4-14 로직 프로세스 오브젝트(Class ID: 309 Hex) A-58

A-5 적합성 선언 A-60

색인

AI 번역본
-For Reference Only-

계약 조건

보증, 책임의 제한

보증

● 배타적 보증

오므론의 배타적 보증은, 오므론의 판매일(또는 오므론이 서면으로 명시한 그 밖의 기간)로부터 12개월 동안 제품에 재료 및 제작상의 결함이 없다는 것입니다. 오므론은 그 밖의 명시적 또는 묵시적 보증을 일체 부인합니다.

● 제한 사항

오므론은 제품의 비침해, 제품성 또는 특정 목적에의 적합성에 대해 명시적이든 묵시적이든 어떠한 보증이나 진술도 하지 않습니다. 구매자는 제품이 자신의 의도된 용도의 요구사항을 적절히 충족하는지를 오로지 자신이 판단했음을 인정합니다.

오므론은 또한 제품 또는 그 밖의 지적재산권 침해에 근거한 청구나 비용에 대한 모든 형태의 보증 및 책임을 부인합니다.

● 구매자의 구제 수단

오므론이 부담하는 유일한 의무는, 오므론의 선택에 따라 (i) 부적합 제품을 (원래 출하된 형태로, 제거 또는 교체에 따른 인건비는 구매자 부담으로) 교체하거나, (ii) 부적합 제품을 수리하거나, 또는 (iii) 부적합 제품의 구매 가격에 상당하는 금액을 환불 또는 credit 처리하는 것입니다. 다만 오므론의 분석 결과 해당 제품이 올바르게 취급, 보관, 설치 및 유지보수되었고 오염, 남용, 오용 또는 부적절한 개조의 대상이 되지 않았음이 확인된 경우에 한해서만 오므론은 제품에 관한 보증, 수리, 배상 또는 그 밖의 청구나 비용에 대해 책임을 집니다. 구매자에 의한 제품 반품은 출하 전에 오므론의 서면 승인을 받아야 합니다. 오므론 관계사는 제품을 그 밖의 전기 또는 전자 부품, 회로, 시스템 어셈블리, 그 밖의 자재나 물질 또는 환경과 조합하여 사용한 경우의 적합성 또는 부적합성이나 그 결과에 대해 책임을 지지 않습니다. 구두 또는 서면으로 제공된 어떠한 조언, 권고 또는 정보도 위 보증에 대한 수정이나 추가로 해석되지 않습니다.

AI 번역 본
For Reference Only-

공개된 정보는 https://www.omron.com/global/ 을 참조하거나 오므론 담당자에게 문의하십시오.

책임의 제한 등

오므론 관계사는 특별 손해, 간접 손해, 부수적 손해 또는 결과적 손해, 이익 손실 또는 생산 손실이나 상업적 손실에 대해, 그 청구가 계약, 보증, 과실 또는 엄격 책임 중 어느 것에 근거하든 관계없이 책임을 지지 않습니다.

또한 오므론 관계사의 책임은 어떠한 경우에도 책임이 제기된 해당 제품의 개별 가격을 초과하지 않습니다.

적용 시 고려사항

적합성

오므론 관계사는 구매자의 용도나 제품 사용에 적용되는 어떠한 표준, 코드 또는 규정에 대한 적합성에 대해서도 책임을 지지 않습니다. 구매자의 요청이 있는 경우, 오므론은 제품에 적용되는 정격 및 사용 제한 사항을 명시한 제3자 인증 문서를 제공합니다. 이 정보만으로는 최종 제품, 기계, 시스템, 그 밖의 용도나 사용과 조합한 제품의 적합성을 완전히 판단하기에 충분하지 않습니다. 구매자의 용도, 제품 또는 시스템에 대한 해당 제품의 적합성을 판단하는 것은 전적으로 구매자의 책임입니다. 구매자는 모든 경우에 적용상의 책임을 집니다.

생명이나 재산에 중대한 위험이 따르는 용도나 대량 사용에는, 시스템 전체가 그러한 위험에 대응하도록 설계되었고 오므론 제품이 전체 설비나 시스템 내에서 의도된 용도에 맞게 올바르게 정격이 부여되고 설치되었음을 확인하지 않는 한 제품을 절대 사용하지 마십시오.

프로그래머블 제품

오므론 관계사는 프로그래머블 제품에 대한 사용자의 프로그래밍이나 그로 인한 결과에 대해 책임을 지지 않습니다.

면책사항

성능 데이터

오므론 관계사의 웹사이트, 카탈로그, 그 밖의 자료에 제시된 데이터는 사용자가 적합성을 판단하는 데 참고하기 위한 것이며 보증을 구성하지 않습니다. 이는 오므론의 시험 조건에 따른 결과일 수 있으므로 사용자는 실제 적용 요구사항과 대조해야 합니다. 실제 성능은 오므론의 보증 및 책임의 제한을 따릅니다.

사 번역본
-For Reference Only-

사양 변경

제품 사양 및 부속품은 개선 및 그 밖의 사유로 예고 없이 변경될 수 있습니다. 공표된 정격이나 기능이 변경되거나 중요한 구조 변경이 있는 경우 형번을 변경하는 것이 당사의 관례입니다. 다만 제품의 일부 사양은 예고 없이 변경될 수 있습니다. 확신이 서지 않는 경우, 귀하의 용도에 필요한 사양을 확정하거나 고정하기 위해 특수 형번이 부여될 수 있습니다. 구매한 제품의 실제 사양을 확인하려면 언제든지 오므론 담당자에게 문의하십시오.

오류 및 누락

오므론 관계사가 제공하는 정보는 확인을 거쳐 정확하다고 판단되지만, 사무적 오류, 오타 또는
교정상의 오류나 누락에 대해서는 책임을 지지 않습니다.

예상 사용 사례 및 위협에 대한 보안 책임에 관한 성명

오므론은 오므론 제품, 그에 설치된 소프트웨어, 또는 그와
연결된 컴퓨터 기기, 컴퓨터 프로그램, 네트워크,
데이터베이스, 그 밖의 독점 자료에 대한 분산 서비스 거부 공격,
컴퓨터 바이러스, 그 밖의 기술적으로 유해한 자료 및/또는
무단 접근으로 인해 직간접적으로
발생하는 어떠한 손실, 손해 또는 비용에 대해서도 책임을 지지 않습니다.

사용자는 (i) 바이러스 방지, (ii) 데이터 입출력, (iii) 손실된 데이터의 복구 수단 유지, (iv) 오므론 제품 및/또는
그에 설치된 소프트웨어의 컴퓨터 바이러스 감염 방지, (v) 오므론 제품을 무단
접근으로부터 보호하기 위한 사용자 고유의 요구사항을 충족하는 적절한 조치와 점검 사항을
판단하고 사용하는 것에 대해 전적으로 책임을 집니다.

AI 번역본
-For Reference Only-

안전상의 주의사항

주의 정보의 정의

본 매뉴얼에서는 내환경 리모트 터미널 NXR-S 시리즈 심플 로직 세이프티 I/O 블록 CIP Safety 대응 제품을 안전하게 사용하기 위해 필요한 주의사항을 제공하기 위해 다음의 표기를 사용합니다.
여기에 제공된 안전상의 주의사항은 안전을 위해 매우 중요합니다. 모든 안전상의 주의사항에 제공된 정보를 항상 읽고 유의하십시오.
다음과 같은 표기를 사용합니다.

⚠ 경고	회피하지 않으면 사망 또는 중상을 초래할 수 있는 잠재적으로 위험한 상황을 나타냅니다. 또한 심각한 재산 피해가 발생할 수 있습니다.
⚠ 주의	회피하지 않으면 경상이나 중등도의 부상 또는 재산 피해를 초래할 수 있는 잠재적으로 위험한 상황을 나타냅니다.

기호

	원과 사선 기호는 해서는 안 되는 조작을 나타냅니다. 구체적인 조작은 원 안에 나타내고 문장으로 설명합니다. 이 예시는 분해 금지를 나타냅니다.
	삼각형 기호는 (경고를 포함한) 주의사항을 나타냅니다. 구체적인 조작은 삼각형 안에 나타내고 문장으로 설명합니다. 이 예시는 감전에 대한 주의사항을 나타냅니다.
	삼각형 기호는 (경고를 포함한) 주의사항을 나타냅니다. 구체적인 조작은 삼각형 안에 나타내고 문장으로 설명합니다. 이 예시는 일반적인 주의사항을 나타냅니다.
	채워진 원 기호는 반드시 해야 하는 조작을 나타냅니다. 구체적인 조작은 원 안에 나타내고 문장으로 설명합니다. 이 예시는 반드시 해야 하는 사항에 대한 일반적인 주의사항을 나타냅니다.

AI 번역본
-For Reference Only-

경고

⚠ 경고

전원 공급 중

전원이 ON 상태일 때 단자부를 만지지 마십시오.
감전될 수 있습니다.



어떠한 유닛도 분해하지 마십시오.
특히 전원이 공급 중이거나 전원을 끈 직후에는 전원을 공급하는 유닛 내부에 고전압 부품이 존재합니다. 이러한 부품에 접촉하면 감전될 수 있습니다. 유닛 내부에는 부상을 유발할 수 있는 날카로운 부품이 있습니다.



페일세이프 대책

CPU 유닛, 그 밖의 유닛 또는 슬레이브의 오동작이나 그 밖의 외부 요인으로 인해 이상이 발생한 경우에도 시스템의 안전을 확보할 수 있도록 외부 회로에 안전 대책을 마련하십시오.
그렇게 하지 않으면 오동작으로 인해 중대한 사고가 발생할 수 있습니다.



비상 정지 회로, 인터록 회로, 리밋 회로 등의 안전 대책을 외부 제어 회로에 반드시 마련해야 합니다.



출력 릴레이의 융착이나 소손 또는 출력 트랜지스터의 파손으로 인해 출력이 ON 또는 OFF 상태로 유지될 수 있습니다. 이러한 문제에 대한 대책으로, 시스템의 안전한 동작을 보장하기 위한 외부 안전 대책을 마련해야 합니다.



다음의 경우 CPU 유닛은 기본 출력 유닛의 모든 출력을 OFF 합니다. 리모트 I/O 슬레이브는 슬레이브에 설정된 내용에 따라 동작합니다.

- 전원 이상이 발생한 경우.
- 전원 접속에 이상이 발생한 경우.
- CPU 워치독 타이머 에러 또는 CPU 리셋이 발생한 경우.
- 메이저 폴트 레벨의 컨트롤러 에러가 발생한 경우.
- 전원 투입 후 RUN 모드로 진입할 때까지 CPU 유닛이 대기 중인 동안.

이러한 경우에도 시스템의 안전한 동작을 보장하기 위한 외부 안전 대책을 마련해야 합니다.



AI 번역본
For Reference Only

신호선 단선, 순간 정전, 그 밖의 원인으로 인한 잘못되거나 누락되거나 이상이 있는 신호에 대비해 안전을 확보하는 페일세이프 대책을 취해야 합니다.
그렇게 하지 않으면 오동작으로 인해 중대한 사고가 발생할 수 있습니다.



전압 및 전류 입력

유닛 및 슬레이브에 입력되는 전압 및 전류가 지정된 범위 이내인지 확인하십시오.
지정된 범위를 벗어나는 전압이나 전류를 입력하면 사고나 화재가 발생할 수 있습니다.



전원 설계

본 매뉴얼의 지침에 따라 전원 설계 및 배선을 올바르게
수행하십시오. 지정된 범위를 벗어나는
전압이나 전류의 입력, 또는 잘못된 배선은 고장이나 화재를 초래할 수 있습니다.

CIP Safety 통신

세이프티 I/O 블록을 기기나 설비에 설치하거나 네트워크에 접속하기 전에, 메모리 전체
클리어를 실행하여 세이프티 I/O 블록에 이전에 저장된 설정 데이터를 삭제하십시오.
최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.

세이프티 I/O 블록을 네트워크에 접속하기 전에 적절한 IP 주소 및 통신
속도를 설정하십시오.
최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.

산출된 응답 시간이 모든 세이프티 체인에 대해 요구되는
사양을 충족하는지 확인하십시오. 최악의
경우 안전 기능이 상실되어 사망에 이르는 인신 상해로 이어질 위험이 있습니다.

Open Type을 "Open Only"로 설정한 경우, 사용 전에 오리지네이터와 타겟이 올바르게 구성되었는지 확인하십시오.

최악의 경우 안전 기능이 상실되어 사망에 이르는 인신 상해로 이어질 위험이 있습니다.

세이프티 I/O 블록을 디버깅할 때는, 오리지네이터 기기에서
프로그래밍된 동작에 따라 유닛과
접속된 외부 기기가 올바르게 동작하는지 확인하십시오. 최악의
경우 안전 기능이 상실되어 사망에 이르는 인신 상해로 이어질 위험이 있습니다.

시스템을 시작하기 전에, 모든 기기의 구성 데이터와 동작이 올바른지 확인하는 사용자 테스트를 실시하십시오.

최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.

SIL이 다른 세이프티 기기가 하나의 세이프티 네트워크에 공존하는 경우, 이로 인한 영향을
철저히 평가하고 시스템 전체에 요구되는 안전 수준을 확보할 수 있는지 확인하십시오.
최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.

각 세이프티 네트워크 또는 세이프티 서브넷에 할당되는 SNN은
시스템 전체에서 고유하도록
구성해야 합니다. 최악의
경우 안전 기능이 상실되어 사망에 이르는 인신 상해로 이어질 위험이 있습니다.

사용 설명서 번역본
-For Reference Only-

Web UI에 표시되는 정보를 바탕으로 세이프티 I/O 블록의 구성 데이터가 올바르게
다운로드되었는지 확인하십시오.
최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.

Type1 Safety Open을 사용하여 구성하는 경우, 최종 검증 절차의 일환으로 소유권(CFUNID)
할당이 올바르게 구성되었는지 반드시 확인하십시오.
최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.

오리지네이터의 커넥션 데이터 세트 및/또는 타겟의 구성 데이터를 반드시 타겟에 다운로드한
후 테스트와 검증을 수행하십시오.
타겟의 SCID는 테스트와 검증이 완료된 후에만 확인하십시오.
최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.

세이프티 I/O 블록에 전송된 SCID 및 구성 데이터를, 구성 시점에 컨피규레이션 도구에 표시되어 확인된
SCID 및 구성 데이터와 반드시 비교하십시오.
최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.

세이프티 I/O 블록을 교체하는 경우, 교체 기기가 올바르게 구성되었는지 확인해야 하며, 교체 후에는 사용자가 직접 기기의 동작을 확인해야 합니다.
최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.



세이프티 I/O 블록을 잠그기 전에 해당 기기의 동작을 반드시 충분히 테스트하십시오.
최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.



접지

24-V 측을 절대 접지하지 마십시오. 세이프티 출력의 단락으로 인해 안전 기능이 상실될 위험이 있습니다.
최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.



시스템 구축

시스템을 구축할 때는, 안전 관련 구성요소의 완전성을 확보하기 위해 다음의 경고사항을 준수하십시오.
최악의 경우 안전 기능이 상실되어 사망에 이르는 인신 상해로 이어질 위험이 있습니다.



리스크 평가 시스템 구축

이러한 제품을 선정하는 과정에는, 설비의 잠재적 위험을 파악하고 안전 제품 선정을 최적화하기
위해 설계 개발 단계 초기에 리스크 평가 시스템을 개발하고 실행하는 것이 포함되어야 합니다.
관련 국제 표준

- ISO 12100 설계를 위한 일반 원칙 - 리스크 평가 및 리스크 저감



보호 대책

안전 제품을 사용하는 설비 및 기기의 안전 시스템을 개발할 때는, 아래에 제시된 예를 비롯하여 이용
가능한 일련의 국제 및 산업 표준 전체를 이해하고 준수하기 위해 최선을 다하십시오.
관련 국제 표준

- ISO 12100 설계를 위한 일반 원칙 - 리스크 평가 및 리스크 저감
- IEC 60204-1 기계류의 전기 설비 - 제1부: 일반 요구사항
- ISO 13849-1, -2 제어 시스템의 안전 관련 부품
- ISO 14119 가드와 연동된 인터록 장치 - 설계 및 선정 원칙
- IEC/TS 62046 사람의 존재를 검출하기 위한 보호 장비의 적용
- IEC 62061 안전 관련 전기, 전자, 프로그래머블 전자 제어 시스템의 기능 안전
- IEC 61508 전기/전자/프로그래머블 전자 안전 관련 시스템의 기능 안전



사본 역본
-For Reference Only-

안전 제품의 역할

안전 제품에는 표준화된 안전 기능 및 메커니즘이 내장되어 있지만, 이러한 기능 및 메커니즘의 이점은 올바르게 설계된 안전 관련 시스템 내에서만 최대한으로 발휘되도록 설계되어 있습니다. 모든 기능 및 메커니즘을 충분히 이해하고, 이를 바탕으로 최적의 사용을 보장하는 시스템을 개발하십시오.
관련 국제 표준

- ISO 14119 가드와 연동된 인터록 장치 - 설계 및 선정 원칙
- ISO 13857 상하지가 위험 구역에 도달하지 못하도록 하는 안전 거리



안전 제품 설치

자격을 갖춘 엔지니어가 안전 관련 시스템을 개발하고 기기와
설비에 안전 제품을 설치해야 합니다.
기계 커미셔닝에 앞서 안전 제품이 예상대로 동작하는지 테스트를 통해 확인하십시오.
관련 국제 표준

- ISO 12100 설계를 위한 일반 원칙 - 리스크 평가 및 리스크 저감
- IEC 60204-1 기계류의 전기 설비 - 제1부: 일반 요구사항
- ISO 13849-1, -2 제어 시스템의 안전 관련 부품
- ISO 14119 가드와 연동된 인터록 장치 - 설계 및 선정 원칙
- IEC 62061 안전 관련 전기, 전자,
  프로그래머블 전자 제어 시스템의 기능 안전
- IEC 61508 전기/전자/프로그래머블 전자 안전 관련 시스템의 기능 안전

법규 및 규정 준수

안전 제품은 해당되는 법규, 규정 및 표준을 준수해야 합니다. 이러한
제품이 통합된 기기와 설비가
유통되는 국가의 법규, 규정 및 표준에 따라 설치 및 사용되고 있는지 확인하십시오.

사용상의 주의사항 준수

안전 제품의 올바른 사용 절차를 익히기 위해, 취급 설명서와 유저 매뉴얼에 제공된 사양 및 주의사항을
주의 깊게 읽으십시오.
지침을 벗어난 사용은 안전 관련 시스템이 예상하지 못한 기기나 설비의 뜻밖의 고장으로
이어질 수 있습니다.

기기 및 설비의 이전

기기와 설비를 이전할 때는, 취급 설명서 사본 1부를 반드시 보관하고
다른 1부를 기기나 설비와 함께
제공하여 이를 인수받는 사람이 조작과 유지보수에 문제가 없도록 하십시오.
관련 국제 표준

- ISO 12100 설계를 위한 일반 원칙 - 리스크 평가 및 리스크 저감
- IEC 60204-1 기계류의 전기 설비 - 제1부: 일반 요구사항
- ISO 13849-1, -2 제어 시스템의 안전 관련 부품
- IEC 62061 안전 관련 전기, 전자,
  프로그래머블 전자 제어 시스템의 기능 안전
- IEC 61508 전기/전자/프로그래머블 전자 안전 관련 시스템의 기능 안전

세이프티 I/O 블록 사용 시

표시등은 신뢰할 수 있는 표시가 아니며 정확한 정보를 제공하는 것이 보장되지 않습니다.
시운전이나 문제 해결 중의 일반적인 진단 용도로만 사용하십시오. 운용 중에는
표시등을 표시 용도로 사용하지 마십시오.
최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.

익스플리시트 메시지 및 노출된 변수를 포함하여 비안전 신호를
안전 신호로 사용하지 마십시오. 최악의
경우 안전 기능이 상실되어 사망에 이르는 인신 상해로 이어질 위험이 있습니다.

유닛의 테스트 출력을
안전 출력으로 사용하지 마십시오. 최악의
경우 안전 기능이 상실되어 사망에 이르는 인신 상해로 이어질 위험이 있습니다.

글로벌 주소를 통해 인트라넷 환경을 사용하는 경우, SCADA나 HMI 등 권한이 없는 단말이나
권한이 없는 서버에 접속하면 스푸핑이나 변조 등의 네트워크 보안 문제가 발생할 수 있습니다.
단말에 대한 접근 제한, 보안 기능을 갖춘 단말의 사용, 설치 구역의 잠금 등 충분한 대책을 직접 마련해야
합니다.

AI 번역본
-For Your Reference Only-

유닛에 접속되는 모든 안전 기기 및 구성요소는 요구되는 안전 수준 및 해당 세이프티 카테고리를 충족하도록 선정하여 사용해야 합니다.
요구되는 안전 기능의 상실로 인해 중대한 부상이 발생할 수 있습니다.



시스템을 시작하기 전에, 모든 안전 기기가 올바르게 동작하는지 확인하는 사용자 테스트를 실시하십시오.
세이프티 시그니처는 사용자 테스트 완료 시 검증됩니다.
요구되는 안전 기능의 상실로 인해 중대한 부상이 발생할 수 있습니다.



유닛을 교체할 때는, 유닛의 모델, 유닛 및 커넥터 장착 위치, 유닛 구성 및 그 동작이 올바른지 확인하십시오.



스루 배선 출력용 전원 OFF 기능은 비안전 기능입니다. 안전 출력으로 사용하지 마십시오. 최악의 경우 안전 기능이 상실되어 사망에 이르는 인신 상해로 이어질 위험이 있습니다.



유닛의 세이프티 애플리케이션 기능을 사용할 때는, 로터리 스위치 설정이 올바른지 확인하고 장비를 조작하기 전에 항상 실제 장비에서 동작을 확인하십시오. 최악의 경우 안전 기능이 상실되어 사망에 이르는 인신 상해로 이어질 위험이 있습니다.



Sysmac Studio나 그 밖의 지원 소프트웨어에서 유닛 구성 정보, 파라미터, 설정값 또는 그 밖의 데이터를 전송하기 전에 반드시 전송 대상의 안전을 확인하십시오. 컨트롤러의 운용 모드와 관계없이 기기나 기계가 예상치 못하게 동작할 수 있습니다.



구성이 의도치 않게 변경되는 것을 방지하기 위해, 안전 검증이 완료되면 구성을 잠그십시오.



단일 채널 출력으로 세이프티 체인을 구축하는 경우, 세이프티 카테고리 2/PLc까지만 달성할 수 있습니다. 단일 채널 입력 및 출력을 사용하는 경우, 세이프티 카테고리, PL 제약조건, 에러 검출을 포함하여 시스템에 요구되는 사항을 충족해야 합니다. 이러한 요구사항과 제약조건에 따라 시스템을 구축하십시오.



다음의 기능을 실행할 때는 항상 시스템 주변의 안전을 확인하십시오.

- 해당 유닛의 운용 모드 변경
- 세이프티 I/O 접점의 설정/리셋
- 세이프티 I/O 접점의 강제 리프레시
- 세이프티 I/O 데이터의 현재값 변경

출력이 동작하여 중대한 부상을 초래할 수 있습니다.



유닛을 복원할 때는, 복원된 프로그램의 세이프티 시그니처가 올바른지 확인하십시오. 요구되는 안전 기능의 상실로 인해 중대한 부상이 발생할 수 있습니다.



안전 검증이 완료되면 구성을 잠그십시오. 구성이 잠금 해제된 상태에서 세이프티 애플리케이션의 로터리 스위치를 변경하고 전원을 재시작하면, 시스템이 다른 세이프티 구성으로 재시작됩니다. 요구되는 안전 기능의 상실로 인해 중대한 부상이 발생할 수 있습니다.

AI 번역본
-For Reference Only-

운용 전 및 운용 중

최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.
시스템 전체에 대한 리스크 평가를 직접 실시하십시오. 리스크 평가를 통해, 전원 투입 후 자동 운용 상태 전환이 위험한 상태로 이어지지 않도록 하십시오.



전원 투입 모드가 Executing으로 설정된 경우, 본 제품은 전원 투입 후 또는 Type1 Safety Open을 통한 구성 후 자동으로 운용 상태(Executing)로 진입합니다. 전원 투입 모드가 Executing이 되는 조건은 다음과 같습니다.

- 고정 애플리케이션을 사용하는 경우.
- 애드온 애플리케이션 또는 사용자 정의 애플리케이션의 로직을 설계할 때, 전원 투입 모드가 Executing으로 설정된 경우.



최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.
사용자 정의 애플리케이션 및 애드온 애플리케이션은 설비의 안전 무결성 수준(SIL) 요구사항에 따라 설계, 테스트 및 검증되어야 합니다.
Sysmac Studio를 사용하여 애플리케이션 파일을 작성하십시오. Sysmac Studio 사용 방법은 본 매뉴얼 및 Sysmac Studio Version 1 오퍼레이션 매뉴얼 (Cat. No. W504)에서 확인할 수 있습니다.



최악의 경우 사망에 이르는 인신 상해의 위험이 있습니다.
본 제품은 최소 8시간 연속으로 운용되도록 하십시오.
본 제품은 일부 하드웨어 자기진단에 최대 8시간이 소요될 수 있습니다. 연속 운용 시간이 8시간 미만인 경우, 특정 기능이나 영역에 대한 진단이 수행되지 않아 해당 영역에서 발생하는 결함을 검출하지 못할 수 있습니다.

보안 대책

바이러스 방지



제어 시스템에 접속된 컴퓨터에 최신 상용 품질의 바이러스 방지 소프트웨어를 설치하고 최신 상태로 유지 관리하십시오.

무단 접근 방지를 위한 보안 대책

당사 제품에 대한 무단 접근을 방지하기 위해 다음의 대책을 취하십시오.

- 권한이 있는 담당자만 제어 시스템 및 설비에 접근할 수 있도록 물리적 통제를 설치하십시오.
- 신뢰할 수 없는 기기로부터의 접근을 방지하기 위해 네트워크를 통한 제어 시스템 및 설비로의 접속을 줄이십시오.
- 사용하지 않는 통신 포트를 차단하고 통신 호스트를 제한하며 제어 시스템 및 설비를 IT 네트워크에서 분리하기 위해 방화벽을 설치하십시오.
- 제어 시스템 및 설비에 대한 원격 접속에는 가상 사설망(VPN)을 사용하십시오.
- 제어 시스템 및 설비에 원격으로 접속하는 기기에는 다요소 인증을 적용하십시오.
- 강력한 비밀번호를 설정하고 자주 변경하십시오.
- USB 드라이브 등의 외부 저장장치를 제어 시스템 및 설비에 접속하기 전에 바이러스 검사를 실시하여 안전을 확인하십시오.



AI 번역본
-For Reference Only-

데이터 입출력 보호

제어 시스템 및 설비에 대한 입출력 데이터의 의도치 않은 수정에 대응하기 위해 백업과 범위를 검증하십시오.

- 데이터 범위 확인
- 변조 및 이상 발생 시를 대비한 백업의 유효성 확인 및 복원용 데이터 준비
- 데이터 변조 및 이상 발생 시 비상 정지 및 페일소프트 운용 등의 안전 설계



데이터 복구

데이터 손실에 대비하여 데이터를 백업하고 정기적으로 최신 상태로 유지하십시오.



글로벌 주소를 통해 인트라넷 환경을 사용하는 경우, SCADA나 HMI 등 권한이 없는 단말이나 권한이 없는 서버에 접속하면 스푸핑이나 변조 등의 네트워크 보안 문제가 발생할 수 있습니다. 단말에 대한 접근 제한, 보안 기능을 갖춘 단말의 사용, 설치 구역의 잠금 등 충분한 대책을 직접 마련해야 합니다.



인트라넷을 구축할 때는, 케이블 단선이나 무단 네트워크 기기의 영향으로 통신 장애가 발생할 수 있습니다. 설치 구역의 잠금 등의 수단으로 네트워크 기기에 대한 물리적 접근을 제한하는 등 적절한 대책을 취하십시오.



SD 메모리 카드 기능을 갖춘 기기를 사용하는 경우, 이동식 미디어를 분리하거나 마운트 해제함으로써 제3자가 이동식 미디어 내의 파일과 데이터를 취득, 변경 또는 교체할 보안 위험이 있습니다. 설치 구역의 잠금, 입퇴실 관리 등의 수단으로 컨트롤러에 대한 물리적 접근을 제한하거나 이동식 미디어에 대한 적절한 관리 조치를 취하는 등 충분한 대책을 직접 마련하십시오.



주의

⚠ 주의

IP 주소 취득

DHCP 서버에서 IP 주소를 취득하는 경우, DHCP 서버가 다음과 같이 설정되어 있는지 확인하십시오. 그렇지 않으면 제어 시스템이 예상치 못하게 동작할 수 있습니다.

- IP 주소 할당 방식: 고정 할당
- 임대 기간: 무기한



AI 번역본
-For Reference Only-

전원 공급 중 및 전원 OFF 시

전원 공급 중 및 전원을 끈 직후에는 기기를 만지지 마십시오.
화상을 입을 수 있습니다.



안전 사용을 위한 주의사항

운반

· 유닛을 운반할 때는 전용 포장 상자를 사용하십시오.
또한 운반 중에 유닛에 과도한 진동이나 충격이 가해지지 않도록 하십시오.

· 유닛을 떨어뜨리거나 비정상적인 진동이나 충격을 가하지 마십시오.
유닛 고장이나 오동작의 위험이 있습니다.

설치

· 제품을 만지기 전에, 정전기를 방전하기 위해 반드시 먼저 접지된 금속 물체를
만지십시오.

· 제품의 장착 나사와 스위치 커버 나사가 모두 본 매뉴얼에 지정된 토크로 조여져 있는지 확인하십시오.

장착

· 단자대, 통신 케이블, 그 밖의 잠금 장치가 있는 부품이 모두 올바르게 잠겨 있는지 확인하십시오.

배선

· 본 매뉴얼에 지정된 케이블, 커넥터, 방수 커버를 사용하십시오.

· 모든 케이블 커넥터 나사와 방수 커버 나사가 본 매뉴얼에 지정된 토크로 조여져 있는지 확인하십시오.

· 전원을 켜기 전에 모든 스위치와 그 밖의 설정을 재확인하고 모든 배선이 올바른지
재확인하십시오. 시스템을 배선할 때는 올바른 배선 부품과 공구를 사용하십시오.

· 케이블을 잡아당기거나 자연스러운 한계를 넘어 구부리지 마십시오.

· 케이블 위에 무거운 물건을 올려놓거나 밟지 마십시오.

· 유닛을 두 개 이상의 시스템에서 사용하는 경우, 간섭으로 인한 불안정한 동작을 방지하기 위해 케이블 사이에 최소 5 mm의 간격을 두십시오.
케이블을 함께 묶지 마십시오.

· 통신 케이블을 배선할 때는 다음의 주의사항을 준수하십시오.
a) 통신 케이블을 전원선 및 고압선에서 멀리 떨어뜨려 배선하십시오.
b) 통신 케이블은 항상 덕트 안에 배선하십시오.
c) 본 매뉴얼에 지정된 권장 통신 케이블을 사용하십시오.
d) 통신 케이블 실드선의 양 끝을 커넥터 후드에 접속하십시오.

AI 번역본
-For Reference Only-

전원 설계

· 본 매뉴얼에 지정된 전원 전압을 사용하십시오.

- 최대 전원 공급 전류는 유닛/입력 전원 전류와 출력 전원 전류의 합인 9 A입니다. 최대 전원 공급 전류를 초과하여 유닛을 사용하지 마십시오. 그렇지 않으면 전원 케이블에 과전류가 흘러 화재를 초래할 수 있습니다.
- 다음의 경우 유닛/입력 전원 및 출력 전원에 돌입전류가 흐를 수 있습니다.
  a) 전원을 켤 때.
  b) 접속된 외부 기기의 전원 공급이 시작될 때.
  c) 접속된 외부 기기의 전원이 ON/OFF될 때.

  또한 I/O 케이블에 단락이 발생한 경우 보호 기능이 작동할 때까지 과전류가 흐를 수 있습니다. 이러한 전류를 고려하여 충분한 여유 용량을 가진 전원을 선정하십시오. 돌입전류로 인해 전원이 올바르게 동작하지 못하거나 전원이 꺼질 수 있습니다.

EtherNet/IP 통신

- EtherNet/IP의 통신 거리, 접속 노드 수, 접속 방법이 사양 범위 내에 있는지 확인하십시오.
- EtherNet/IP 통신은 전원 투입 직후 항상 확립되는 것은 아닙니다. 제어 조작을 시도하기 전에, CPU 유닛의 시스템 정의 변수나 상태를 사용자 프로그램에서 사용하여 통신이 확립되었는지 확인하십시오.

실제 운용

- 실제 운용에 사용하기 전에 사용자 프로그램, 데이터, 파라미터 설정이 올바르게 실행되는지 확인하십시오.
- 전원이 불안정한 장소에서는 정격 전압과 주파수를 만족하는 전원이 공급되도록 적절한 대책을 취하십시오.

전원 끄기

- 통신 케이블을 배선하기 전에, 유닛에 대한 외부 전원과 유닛과 통신하는 기기에 대한 전원을 끄십시오.

AI 번역본
-For Reference Only-

- 다음의 작업을 수행하기 전에는 항상 유닛에 대한 외부 전원을 끄십시오.
  a) 접속된 기기를 포함한 유닛 조립
  b) 로터리 스위치 설정
  c) 케이블 접속 또는 배선
  d) 단자대나 커넥터의 장착 또는 분리

운용

- 다음의 조작을 수행하기 전에, 제어 대상 시스템에 악영향이 없는지 확인하십시오.
  a) CPU 유닛의 운용 모드 변경 (시작 모드 설정 변경 포함)

b) 사용자 프로그램이나 설정 변경

c) 설정값이나 현재값 변경

d) 강제 리프레시

· CPU 유닛은 운용이 정지된 상태(즉 PROGRAM 모드)에서도 I/O를 리프레시합니다.
따라서 본 제품에 할당된 출력 메모리의 데이터나 특수 I/O 유닛 또는 CPU 버스 유닛에 할당된 메모리의 데이터를 변경하는 다음의 조작을 수행하기 전에는 안전을 충분히 확인하십시오. 본 제품이나 특수 I/O 유닛 또는 CPU 버스 유닛에 접속된 부하가 예상치 못하게 동작할 수 있습니다.

a) 프로그래밍 장치(PC 툴)로 CPU 유닛에 I/O 메모리 데이터를 전송하는 경우.

b) 프로그래밍 장치로 메모리의 현재값을 변경하는 경우.

c) 프로그래밍 장치로 비트를 강제 세트 또는 강제 리셋하는 경우.

d) 메모리 카드나 EM 파일 메모리에서 CPU 유닛으로 I/O 메모리 파일을 전송하는 경우.

e) 호스트 컴퓨터나 네트워크상의 다른 PLC에서 I/O 메모리를 전송하는 경우.

보수

· 청소 시 페인트 시너를 사용하지 마십시오. 시판되는 알코올을 사용하십시오.

· 고압 세척을 사용하지 마십시오.

폐기

· 제품의 폐기는 지역 당국이 정한 규정의 적용을 받을 수 있습니다. 해당 지역의 조례에 따라 제품을 폐기하십시오.

· 정보 유출을 방지하기 위해, 폐기 전에 모든 사용자 데이터를 삭제하십시오.

AI 번역본
-For Reference Only-

사용상의 주의

보관, 장착 및 배선

- 다음의 장소에서는 유닛을 사용하거나 보관하지 마십시오. 그렇게 하면 동작 정지나 오동작이 발생할 수 있습니다.
  a) 직사광선을 받는 장소
  b) 사양에 지정된 범위를 벗어나는 온도나 습도의 영향을 받는 장소
  c) 심한 온도 변화로 인해 결로가 발생하는 장소
  d) 부식성 또는 가연성 가스의 영향을 받는 장소
  e) 먼지(특히 철분)나 염분의 영향을 받는 장소
  f) 산, 오일 또는 화학물질에 노출되는 장소
  g) 진동이나 충격이 유닛에 직접 전달되는 장소
  h) 전원선 부근
- 다음의 장소에 유닛을 설치할 때는 충분한 차폐 대책을 취하십시오.
  a) 정전기나 그 밖의 노이즈의 영향을 받는 장소
  b) 강한 전계나 자계의 영향을 받는 장소
  c) 방사선에 노출될 위험이 있는 장소
  d) 전원선 부근
- 본 매뉴얼의 지침에 따라 올바르게 배선하십시오.
- 스위치 커버를 장착할 때는 패킹이 뒤틀리지 않았는지 확인하십시오. 또한 케이스와 패킹에 이물질이 부착되어 있지 않은지 확인하십시오.
- 유닛을 물에 계속 잠긴 상태로 사용하지 마십시오.

전원 설계

유닛/입력 전원과 출력 전원에는 항상 별개의 전원을 사용하십시오. 동일한 전원에서 전력을 공급하면 출력 기기의 부하 변동으로 인해 오동작이 발생할 수 있습니다.

AI 번역본
-For Reference Only-

EtherNet/IP 통신

운용 중에는 EtherNet/IP 통신 케이블을 분리하지 마십시오. 출력이 불안정해집니다.

통신 케이블 진단 실행

통신 케이블 진단이 실행 중인 포트에서는 통신이 중단되며, 해당 포트를 통한 모든 커넥션 (태그 데이터 링크) 및 메시지 통신이 일시적으로 정지됩니다. 통신 케이블 진단을 실행하기 전에 시스템에 악영향이 없는지 확인하십시오.

보안 대책

보안을 위해 유닛 및 프로젝트 파일에 대해 세이프티 패스워드를 설정할 것을
권장합니다. 세이프티 패스워드가 유출되지 않도록 엄중하게 관리하십시오.
특히 세이프티 패스워드 데이터를 인터넷을 통해 전송할 때는 공개키 암호화 등의 조치를 취하여
도청을 방지하십시오.

AI 번역본
-For Reference Only-

법규 및 규격

NXR-S 시리즈 세이프티 I/O 블록은 다음 규격에 대한 인증을 취득했습니다.

인증 기관	규격
TÜV Rheinland	· EN 61508 parts 1-3 · EN ISO 13849-1 · EN ISO 13849-2 · EN IEC 61131-2 · IEC 61326-3-1 · EN 60529 · EN 61131-6
UL	· NRAQ/NRAQ7 · UL 61010-1 및 UL 61010-2-201 · CSA C22.2 No. 61010-1 및 CSA C22.2 No. 61010-2-201 · FSPC (IEC 61508 parts 1-3 및 ISO 13849-1)
ODVA	· CIP Safety on EtherNet/IP · EtherNet/IP

NXR-S 시리즈 세이프티 I/O 블록을 사용하면 다음 규격을 충족하는 안전 제어 시스템을 구축할 수 있습니다.

· IEC 61508(전기/전자/프로그래머블 전자 안전 관련 시스템의 기능 안전)에서 규정하는 SIL 3(Safety Integrity Level 3) 요건

· EN ISO13849-1에서 규정하는 PLe(Performance Level e) 및 안전 카테고리 4 요건

세이프티 I/O 블록은 RCM, UKCA, KC 적합성에 대해서도 등록되어 있습니다.

EU 지침 및 규정 적합

적용 지침

· EMC Directives 2014/30/EU

· Machinery Directive 2006/42/EC

AI 번역본
-For Reference Only-

개념

● EMC Directives 2014/30/EU

EU 지침에 적합한 오므론 기기는 관련 EMC 규격에도 적합하므로 다른 기기나 전체 기계에 더 쉽게 내장할 수 있습니다. 실제 제품에 대해 EMC 규격 적합성을 확인했습니다.*1

다만 고객이 사용하는 시스템에서 제품이 해당 규격에 적합한지는 고객이 직접 확인해야 합니다. EU 지침에 적합한 오므론 기기의 EMC 관련 성능은 오므론 기기가 설치되는 설비나 제어반의 구성, 배선, 기타 조건에 따라 달라질 수 있습니다. 따라서 고객은 기기 및 전체 기계가 EMC 규격에 적합한지 최종적으로 확인해야 합니다.

*1. 적용되는 EMC(Electromagnetic Compatibility, 전자파 적합성) 규격은 다음과 같습니다: EMS(Electromagnetic Susceptibility, 전자파 내성): EN 61131-2, EMI(Electromagnetic Interference, 전자파 장해): EN 61131-2(방사 노이즈: 10 m 규제).

● Machinery Directive 2006/42/EC

Machinery Directive(기계지침)는 해당 기계의 안전을 확보하기 위해 사용되는 안전 구성 부품을 필요한 안전 수준에 따라 사용할 것을 요구합니다.
적용 규격은 EN ISO 13849-1입니다.

● EU 지침 적합

NXR-S 시리즈는 EU 지침에 적합합니다. 본 제품을 사용하는 기계나 장치가 EU 지침에 적합하도록 하려면 다음 주의사항을 준수해야 합니다.

- NXR-S 시리즈의 유닛/입력 전원 및 출력 전원으로 접속하는 DC 전원에는 SELV 전원을 사용해야 합니다.
  권장 전원으로는 오므론 S8VK-S 시리즈 전원을 사용할 것을 권장합니다. 권장 전원에 대해서는 EMC 규격 적합성을 확인했습니다.
- EU 지침에 적합한 NXR-S 시리즈 제품은 공통 방사 규격(Common Emission Standard)에도 적합합니다. 방사 노이즈 특성(10 m 규제)은 사용하는 제어반의 구성, 제어반에 접속된 다른 기기, 배선, 기타 조건에 따라 달라질 수 있습니다.
  따라서 NXR-S 시리즈 제품을 사용하는 전체 기계나 설비가 EU 지침에 적합한지 확인해야 합니다.
- NXR-S 시리즈의 유닛/입력 전원 및 출력 전원으로 접속하는 DC 전원에는 출력 유지 시간이 10 ms 이상인 전원을 사용해야 합니다.
- 본 제품은 클래스 A 제품(산업 환경용)입니다. 가정 환경에서 사용할 경우 전파 장해를 일으킬 수 있으며, 전파 장해가 발생한 경우에는 사용자가 적절한 조치를 취해야 할 수 있습니다.
- EU 지침 적합성은 케이블 길이가 30 m 이하인 전원 케이블 및 I/O 케이블을 사용하여 확인했습니다.

EN ISO 13849-1 적합

EN ISO 13849-1은 안전 제어 시스템을 구축할 때 안전 관련 소프트웨어를 작성하기 위한 프로세스 관리 체계를 갖출 것을 요구합니다. 이 프로세스 관리 체계는 소프트웨어 설계 수명 주기의 각 단계(즉, 일반 소프트웨어 설계, 안전 회로 시스템 설계, 소프트웨어 업그레이드)에서 시스템 장애를 방지하기 위해 소프트웨어를 읽고 이해하고 테스트하고 유지 관리하기 쉽도록 보장해야 합니다. 즉, 설비나 장치 등 안전 소프트웨어의 설계 및 개발에도 프로세스 관리 체계를 갖춰야 한다는 의미입니다. 모든 규격에 적합하도록 하는 것은 고객의 책임입니다.

AI 번역본
For Reference Only-

설비의 안전 성능을 검증하는 데 필요한 기계 안전에 관한 신뢰성 데이터는 다음 URL에서 다운로드할 수 있습니다:
http://www.ia.omron.com/support/sistemalibrary/index_jp.html.

UL 및 CSA 규격 적합

일부 NXR-S 시리즈 제품은 UL 및 CSA 규격에 적합합니다.

UL 또는 CSA 규격에 적합한 제품을 사용하며 해당 규격을 사용자의 기계나 장치에 적용해야 하는 경우, 제품과 함께 제공되는 지시서(Instruction Sheet)를 참조하십시오. 지시서에는 규격에 적합하기 위한 적용 조건이 기재되어 있습니다.

조선 규격 적합

본 제품은 조선 규격에 적합하지 않습니다.

KC 인증 적합

본 제품을 대한민국에서 사용할 경우 다음 주의사항을 준수하십시오.

사 용 자 안 내 문
이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

본 제품은 업무용 전자파 적합성 요건을 충족합니다. 가정에서 사용할 경우 전파 장해가 발생할 우려가 있습니다.

AI 번역본
-For Reference Only-

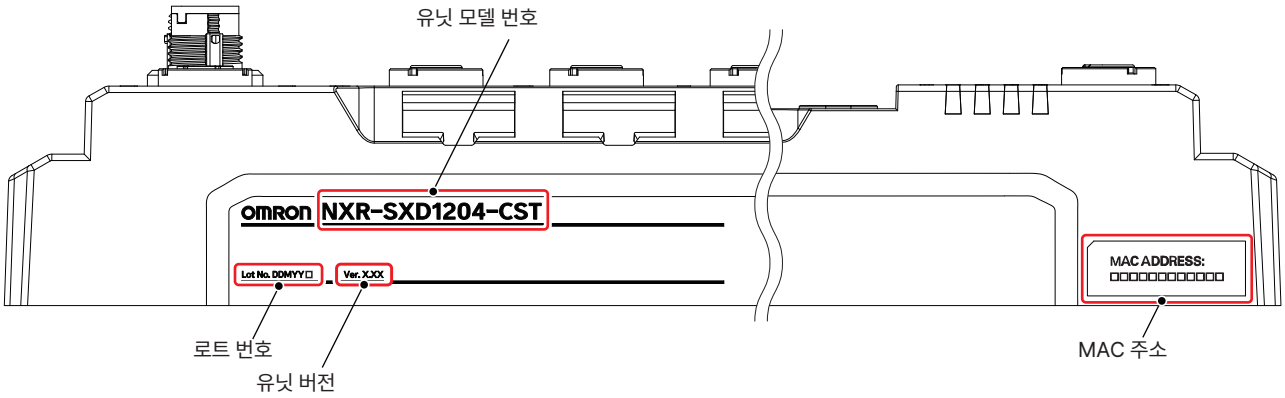
유닛 버전

유닛 버전

유닛 버전은 NXR-S 시리즈의 각 유닛에 대한 개정 번호입니다. 유닛의 모델이 동일하더라도
유닛 버전이 다르면 기능에 일부 차이가 있을 수 있습니다.

제품에서의 유닛 버전 표기

유닛 버전은 유닛 측면의 유닛 사양과 함께 표기되어 있습니다.



유닛의 유닛 사양에는 다음 정보가 표기되어 있습니다.

명칭	기능
유닛 모델 번호	유닛의 모델을 나타냅니다.
유닛 버전	유닛의 유닛 버전을 나타냅니다.
로트 번호	유닛의 로트 번호를 나타냅니다. DDMYY: 로트 번호, □: 오므론 사용. "M"은 월을 나타냅니다(1~9: 1월~9월, X: 10월, Y: 11월, Z: 12월).
MAC 주소	유닛의 EtherNet/IP 포트에 대한 MAC 주소를 나타냅니다.

AI 번역 버전
-For Reference Only-

Web UI에서의 표시

Web UI의 생산 정보 표시 기능을 사용하여 유닛 버전을 확인할 수도 있습니다. 다음은 Web UI의
"생산 정보 표시 기능"과 "생산 정보 화면"에 대한 설명입니다.

● 생산 정보 표시 기능 상세

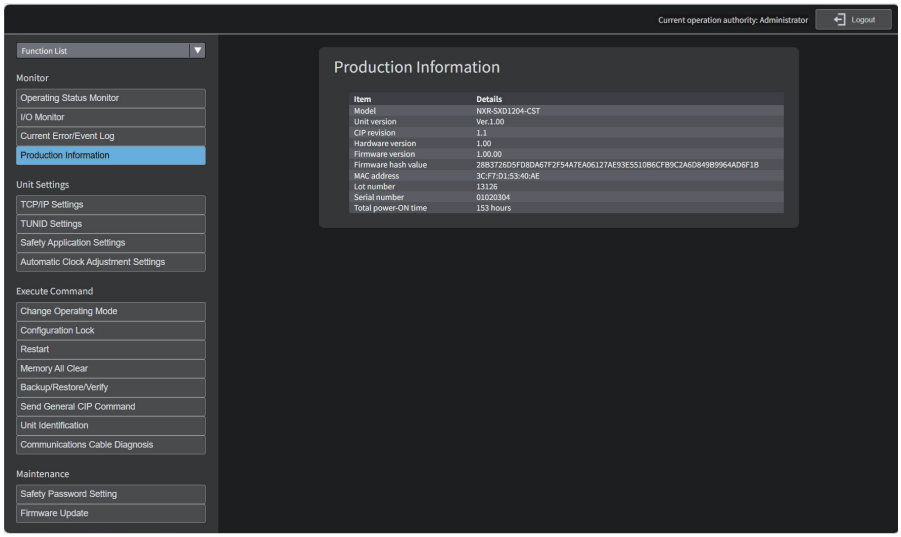
생산 정보 표시 기능은 세이프티 I/O 블록에 대해 다음 정보를 표시합니다.

- 모델
- 유닛 버전
- CIP 리비전
- 하드웨어 버전

- 펌웨어 버전
- 펌웨어 해시값
- MAC 주소
- 로트 번호
- 시리얼 번호
- 총 전원 ON 시간

● 생산 정보 화면

생산 정보 화면에는 해당 유닛의 유닛 버전 및 기타 생산 정보가 표시됩니다.



AI 번역본
-For Reference Only-

관련 매뉴얼

다음 표에 관련 매뉴얼을 나타냅니다. 이 매뉴얼들을 참조용으로 사용하십시오.

매뉴얼 이름	자료 번호	모델	용도	설명
내환경 리모트 터미널 NXR-S 시리즈 CIP Safety용 심플 로직 세이프티 I/O 블록 유저 매뉴얼 (본 매뉴얼)	W645	NXR-SXD1204-CST NXR-SXD1204B-CST	내환경 리모트 터미널 NXR-S 시리즈 CIP Safety용 심플 로직 세이프티 I/O 블록의 사용법을 학습합니다.	내환경 리모트 터미널 NXR-S 시리즈 CIP Safety용 심플 로직 세이프티 I/O 블록의 하드웨어, 설치 방법, 기능을 설명합니다.
NX 시리즈 세이프티 컨트롤 유닛/커뮤니케이션 컨트롤 유닛 유저 매뉴얼	Z395	NX-SL5□□□ NX-SI□□□□ NX-SO□□□□ NX-CSG□□□	NX 시리즈 세이프티 컨트롤 유닛 및 커뮤니케이션 컨트롤 유닛의 사용법을 학습합니다.	NX 시리즈 세이프티 컨트롤 유닛 및 커뮤니케이션 컨트롤 유닛의 하드웨어, 설치 방법, 기능을 설명합니다.
NX 시리즈 커뮤니케이션 컨트롤 유닛 내장 기능 유저 매뉴얼	Z396	NX-CSG□□□	NX 시리즈 커뮤니케이션 컨트롤 유닛의 내장 기능에 대해 학습합니다.	NX 시리즈 커뮤니케이션 컨트롤 유닛의 소프트웨어 설정 방법 및 통신 기능을 설명합니다.
NX 시리즈 세이프티 컨트롤 유닛 유저 매뉴얼	Z930	NX-SL□□□□ NX-SI□□□□ NX-SO□□□□	NX 시리즈 세이프티 컨트롤 유닛의 사용법을 학습합니다.	NX 시리즈 세이프티 컨트롤 유닛의 하드웨어, 설치 방법, 기능을 설명합니다.
NX 시리즈 세이프티 컨트롤 유닛 명령어 레퍼런스 매뉴얼	Z931	NX-SL□□□□	세이프티 CPU 유닛 명령어의 사양에 대해 학습합니다.	세이프티 CPU 유닛의 명령어를 설명합니다.
NJ/NX 시리즈 CPU 유닛 내장 EtherNet/IP™ 포트 유저 매뉴얼	W506	NX701-□□□□ NX502-□□□□ NX102-□□□□ NX1P2-□□□□ NJ501-□□□□ NJ301-□□□□ NJ101-□□□□	NJ/NX 시리즈 CPU 유닛의 내장 EtherNet/IP 포트 사용.	내장 EtherNet/IP 포트에 대한 정보를 제공합니다. 기본 설정, 태그 데이터 링크, 기타 기능에 대한 정보를 제공합니다.
NY 시리즈 IPC 머신 컨트롤러 인더스트리얼 패널 PC / 인더스트리얼 박스 PC 내장 EtherNet/IP™ 포트 유저 매뉴얼	W563	NY532-□□□□ NY512-□□□□	NY 시리즈 인더스트리얼 PC의 내장 EtherNet/IP 포트 사용.	내장 EtherNet/IP 포트에 대한 정보를 제공합니다. 기본 설정, 태그 데이터 링크, 기타 기능에 대한 정보를 제공합니다.

사본 열람
-For Reference Only-

매뉴얼 이름	자료 번호	모델	용도	설명
Sysmac Studio Version 1 오퍼레이션 매뉴얼	W504	SYSMAC -SE2□□□	Sysmac Studio의 조작 절차 및 기능에 대해 학습합니다.	Sysmac Studio의 조작 절차를 설명합니다.
팩토리 오토메이션 시스템 보안 가이드라인	P162	-	FA 시스템 전체와 관련된 보안 개념에 대해 학습합니다.	오므론의 FA 제품에 대한 보안 대책과 고객이 FA 제품을 사용할 때 실시했으면 하는 보안 조치에 대해 설명합니다.
NJ/NX 컨트롤러 보안 가이드라인	P166	NX701-□□□□ NX502-□□□□ NX102-□□□□ NX1P2-□□□□ NJ501-□□□□ NJ301-□□□□ NJ101-□□□□	NJ/NX 시리즈 CPU 유닛을 사용한 보안 대책에 대해 학습합니다.	NJ/NX 시리즈 CPU 유닛을 사용하여 실시할 수 있는 보안 대책을 설명합니다.
내환경 IP67 전원 유저 매뉴얼	T245	S8NR-S□□□24	내환경 IP67 전원의 사용법을 학습 합니다.	내환경 IP67 전원의 기능, 성능, 조작 절차를 설명합니다.

AI 번역본
-For Reference Only-

용어

용어	설명
CIP Safety 오리지네이터	CIP Safety 통신에서의 역할입니다. CIP Safety 오리지네이터는 CIP Safety 타겟에 대한 CIP Safety 커넥션을 관리합니다. CIP Safety 오리지네이터는 디바이스 유닛이 아니라 커넥션 유닛에 존재합니다.
CIP Safety 커넥션	세이프티 프로세스 데이터 통신 프로토콜이 CIP Safety인 세이프티 I/O 커넥션입니다. 통신에서의 역할에 따라 CIP Safety 오리지네이터 커넥션과 CIP Safety 타겟 커넥션이 있습니다.
CIP Safety 타겟	CIP Safety 통신에서의 역할입니다. CIP Safety 타겟은 CIP Safety 오리지네이터로부터 CIP Safety 커넥션을 열기 위한 요청을 수신합니다. CIP Safety 타겟은 디바이스 유닛이 아니라 커넥션 유닛에 존재합니다.
Device Level Ring (DLR)	EtherNet/IP 규격에서 정의하는, 단일 장애 내성을 제공하는 데이터링크 계층 프로토콜입니다.
TUNID	CIP Safety 통신을 위한 세이프티 시스템상의 모든 네트워크에서 고유하게 식별할 수 있도록 디바이스에 할당되는 ID입니다. TUNID는 6바이트의 Safety Network Number(SNN)와 4바이트의 Node ID로 구성된 총 10바이트 값입니다.
어셈블리	디바이스 내부에 보유된 데이터의 집합입니다. 외부에서 액세스할 수 있도록 데이터를 한곳에 모아 놓은 것입니다.
애드온 애플리케이션	이 유닛의 Web UI를 사용하여 로터리 스위치 번호에 로직을 할당한 세이프티 애플리케이션입니다.
세이프티 애플리케이션	세이프티 애플리케이션이란 세이프티 제어를 구현하기 위한 애플리케이션입니다. 본 매뉴얼에서는 이 유닛 내부에서 동작하는 세이프티 애플리케이션만을 "세이프티 애플리케이션"이라고 합니다. 본 매뉴얼에서는 고정 애플리케이션, 애드온 애플리케이션, 사용자 정의 애플리케이션, 리모트 I/O 모드 애플리케이션의 네 가지 유형의 세이프티 애플리케이션을 다룹니다.
심플 로직 모드	심플 로직 처리 기능을 사용하여 동작하는 모드입니다.
심플 로직 모드 애플리케이션	심플 로직 모드에서 사용되는 애플리케이션입니다. I/O 구성 설정과 로직 설정이 정의됩니다. 고정 애플리케이션, 애드온 애플리케이션, 사용자 정의 애플리케이션의 세 가지 유형이 있습니다.
고정 애플리케이션	이 유닛에 사전 설치되어 있는 세이프티 애플리케이션입니다.
커넥션	디바이스 간 통신을 수행하기 위한 논리적 통신 경로입니다.
구성	디바이스 및 네트워크에 대해 설정된 설정값입니다.
싱글 채널	이중화 없이 하나의 입력 또는 출력을 하나의 점으로 사용합니다.
스탠다드	본 매뉴얼에서 스탠다드란 세이프티 제어에 사용하기 위해 특별한 세이프티 대책이 적용된 것과 구별하기 위해, 일반 제어 용도로 사용되는 디바이스, 기능, 데이터를 가리키는 용어입니다.
스탠다드 제어	일반 제어 용도로 설계된 디바이스, 기능, 데이터를 사용하는 제어 유형입니다. 세이프티 제어와 구별하기 위해 사용하는 용어입니다.
세이프티 CPU 유닛	세이프티 제어에 사용되는 CPU 유닛입니다. NX 유닛의 한 종류입니다.
세이프티 I/O 블록	세이프티 제어에 사용되는 I/O 블록입니다.
세이프티 기능	기계의 위험에 대해 안전 상태(safe state)를 달성하기 위해 안전 제어 시스템이 실행하는 기능입니다.
세이프티 제어	특별한 세이프티 대책이 적용되어 설계된 디바이스, 기능, 데이터를 사용하는 제어 유형입니다.
세이프티 컨트롤 유닛	세이프티 제어에 사용되는 NX 유닛을 총칭하는 용어입니다.
세이프티 출력 디바이스	세이프티 제어에 사용하기 위해 특별한 세이프티 대책이 적용되어 설계된 출력 디바이스입니다. 세이프티 릴레이 등의 디바이스를 총칭하는 용어입니다.
세이프티 출력 기능	세이프티 출력 데이터 값과 세이프티 출력 단자의 출력 신호가 정상인지 이상인지를 평가하는 기능입니다. 구체적인 세이프티 평가 기능으로는 테스트 펄스 평가와 듀얼 채널 평가가 있습니다. 평가 결과가 이상으로 나타나면 세이프티 출력 단자의 출력 신호가 OFF됩니다.
안전 상태(Safe state)	인체에 대한 위험이 허용 가능한 수준으로 감소된 상태의 디바이스 또는 설비의 상태입니다.

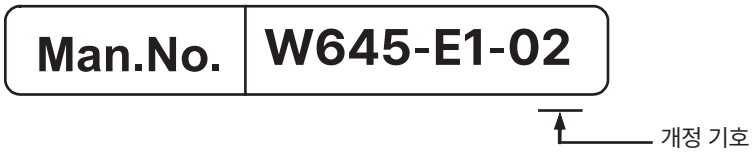
-For Reference Only-

용어	설명
세이프티 입력 디바이스	세이프티 제어에 사용하기 위해 특별한 세이프티 대책이 적용되어 설계된 입력 디바이스입니다. 비상 정지 스위치, 세이프티 도어 스위치 등의 디바이스를 총칭하는 용어입니다.
세이프티 입력 기능	세이프티 입력 단자에 입력되는 신호가 정상인지 이상인지를 평가하는 기능입니다. 구체적인 세이프티 평가 기능으로는 테스트 펄스 평가와 듀얼 채널 평가가 있습니다. 평가 결과가 이상으로 나타나면 세이프티 입력 데이터가 비활성화 (OFF)됩니다.
세이프티 네트워크 컨트롤러	NX 시리즈 커뮤니케이션 컨트롤 유닛에 세이프티 컨트롤 유닛을 장착한 빌딩 블록형 세이프티 컨트롤러를 총칭하는 용어입니다.
Safety Network Number (SNN)	CIP Safety 통신을 위해 세이프티 네트워크를 고유하게 식별할 수 있도록 세이프티 네트워크에 할당되는 번호입니다.
세이프티 프로그램	세이프티 컨트롤러용 사용자 프로그램입니다. 스탠다드 컨트롤러의 사용자 프로그램과 구별하기 위해 사용하는 용어입니다.
세이프티 반응 시간	세이프티 관련 입력(비상 정지 스위치 누름, 라이트 커튼 차광, 세이프티 도어 열림 등)이나 디바이스 고장이 발생한 후, 최악의 경우를 가정했을 때 시스템이 안전 상태(safe state)에 도달하는 데 필요한 시간입니다.
세이프티 밸리데이션	세이프티 밸리데이션 테스트에서 세이프티 제어가 세이프티 시스템의 요구 사양을 충족하는지 확인하는 검사입니다. 또한 그 확인 정보를 세이프티 애플리케이션 데이터에 추가하는 행위를 가리키는 데 사용되기도 합니다.
커뮤니케이션 컨트롤 유닛	세이프티 CPU 유닛과 EtherNet/IP상의 CIP Safety 디바이스가 네트워크에서 CIP Safety 통신을 할 수 있도록 하는 인터페이스 유닛을 총칭하는 용어입니다.
테스트 펄스 평가	접속된 외부 디바이스와의 고장이나 배선 오류를 평가하기 위해 세이프티 입력 또는 세이프티 출력에 사용되는 테스트 펄스를 출력하는 기능입니다.
듀얼 채널	이중화를 위해 두 개의 입력 또는 출력을 한 쌍의 점으로 사용합니다.
듀얼 채널 평가	세이프티 입력 또는 세이프티 출력의 상태를 평가하기 위해, 한 쌍의 세이프티 입력 또는 세이프티 출력 단자를 정합성을 확인하는 이중화 단자로 사용하는 기능입니다.
오퍼레이팅 모드	유닛 동작의 각 상태입니다. 오퍼레이팅 모드에 따라 사용 가능한 기능이 달라집니다.
Node ID	동일한 Safety Network Number (SNN)를 갖는 디바이스를 CIP Safety 통신을 위해 고유하게 식별할 수 있도록 네트워크상의 각 디바이스에 할당되는 ID입니다. 세이프티 CPU 유닛은 NX 버스상의 유일한 CIP Safety 디바이스이며, Node ID는 항상 1입니다. EtherNet/IP 네트워크상의 CIP Safety 디바이스는 IP 주소가 Node ID로 사용됩니다.
사용자 정의 애플리케이션	Type1 Safety Open의 구성(configuration)을 사용하여 유닛에 다운로드하는 로직을 갖는 세이프티 애플리케이션입 니다. 사용자 정의 애플리케이션은 사용자가 Sysmac Studio에서 작성합니다.
사용자 프로그램	사용자가 작성하는 모든 프로그램입니다. 사용자 프로그램이란 스탠다드 컨트롤러의 스탠다드 제어용 프로그램과 세이프티 CPU 유닛의 세이프티 프로그램을 가리킵니다.
리모트 I/O 모드	심플 로직 처리 기능을 사용하지 않고 간이 리모트 I/O로 동작하는 모드입니다.
리모트 I/O 모드 애플리케이션	리모트 I/O 모드에서 사용되는 애플리케이션입니다. I/O 구성 설정만 정의되며, 로직은 포함되지 않습니다. 설정은 Type1 Safety Open 또는 Web UI를 사용하여 유닛에 대해 구성합니다.
링 수퍼바이저	링 수퍼바이저는 링의 무결성을 검증하는 역할을 합니다. 장애로부터 복구하기 위해 링을 재구성하고, 링에 대한 진단 정보를 수집합니다.

AI 번역본
For Reference Only

개정 이력

매뉴얼의 앞표지와 뒤표지에 있는 자료 번호 끝에는 매뉴얼 개정 기호가 표기되어 있습니다.



개정 기호	일자	개정 내용
01	2026년 7월	최초 제작
02	2026년 7월	전원 케이블 추가에 따른 변경

AI 번역본
-For Reference Only-

1

특징 및 시스템 구성

본 장에서는 내환경 리모트 터미널 NXR-S 시리즈 CIP Safety용 심플 로직 세이프티 I/O 블록의 특징 및 시스템 구성에 대해 설명합니다.

1-1 세이프티 I/O 블록 개요 1-2

1-2 세이프티 I/O 블록의 특징 1-3

1-3 시스템 구성 1-4

1-3-1 세이프티 제어 시스템 1-4

1-3-2 네트워크 토폴로지 1-13

1-3-3 캐스케이드 접속 1-14

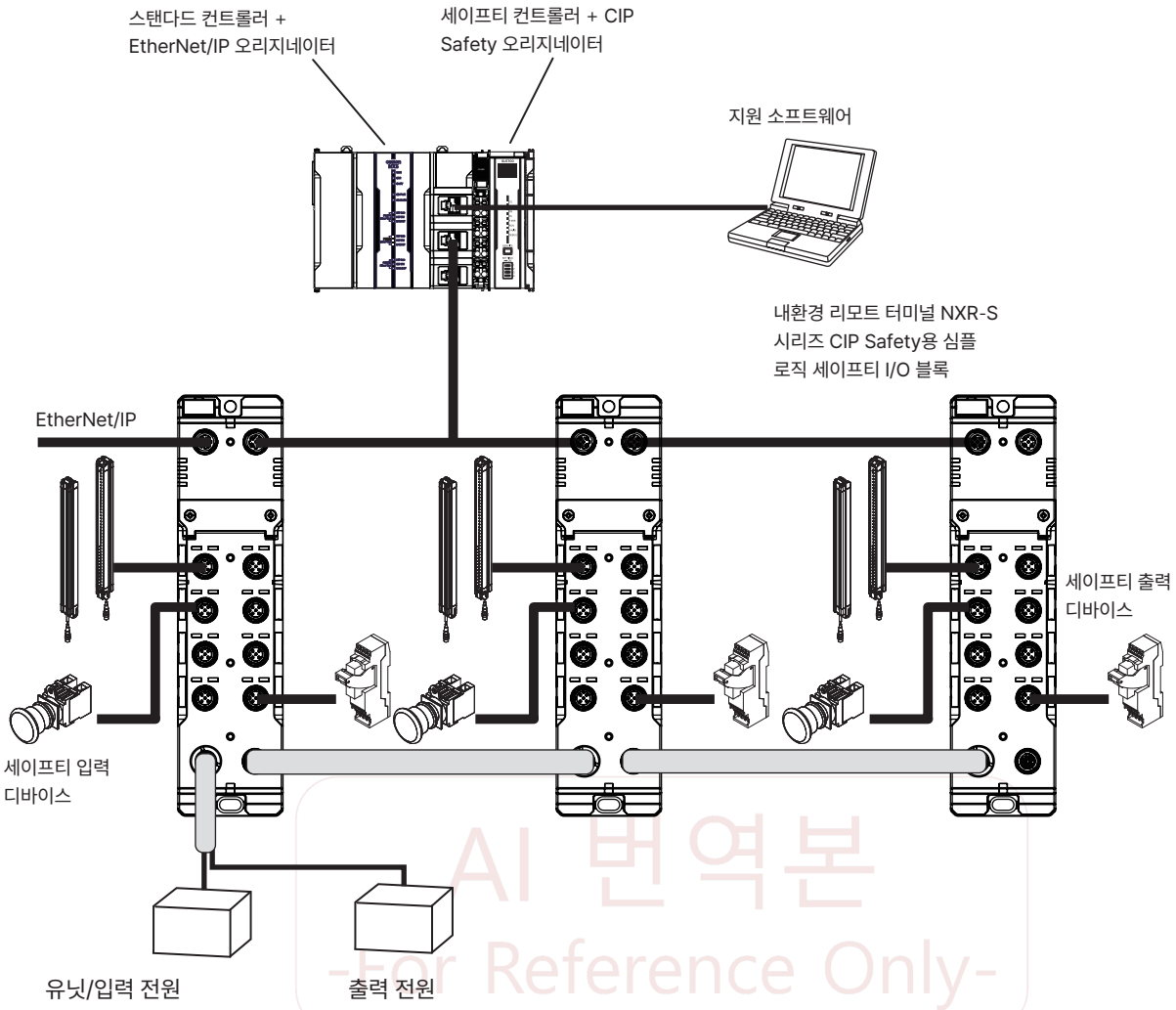
1-4 지원 소프트웨어 1-16

AI 번역본
-For Reference Only-

1-1 세이프티 I/O 블록 개요

내환경 리모트 터미널 NXR-S 시리즈 CIP Safety용 심플 로직 세이프티 I/O 블록은 IP67에 상당하는 높은 방진방수 보호등급과 CIP Safety 타겟 기능을 갖춘 세이프티 I/O 디바이스입니다. 또한 심플 로직 기능을 사용하여 세이프티 출력 디바이스를 제어할 수 있습니다.
기본 기능으로 다음 기능을 지원합니다.

- CIP Safety 타겟으로서 CIP Safety 오리지네이터와 세이프티 통신을 수행합니다.
- EtherNet/IP 타겟으로서 EtherNet/IP 오리지네이터와 데이터를 교환합니다.
- 비상 정지 스위치, 세이프티 라이트 커튼 등의 세이프티 디바이스와 I/O 처리를 수행합니다.



AI 번역본
-For Reference Only-

1-2 세이프티 I/O 블록의 특징

본 절에서는 내환경 리모트 터미널 NXR-S 시리즈 CIP Safety용 심플 로직 세이프티 I/O 블록의 특징에 대해 설명합니다.

심플 로직 기능

세이프티 I/O 블록에는 세이프티 출력 디바이스를 제어하기 위한 로직 기능이 있습니다.
따라서 프로그래밍 없이 간단한 제어가 가능하며, 세이프티 I/O 블록만으로도 고속 응답 세이프티 제어가 가능합니다.

IP67에 상당하는 방진방수 보호등급

세이프티 I/O 블록은 IP67에 상당하는 높은 방진방수 보호등급을 갖추고 있습니다. 따라서 물이나 먼지에 노출되는 환경에서도 제어반 외부에 설치할 수 있습니다.

다양한 케이블의 간편한 배선

세이프티 I/O 블록은 전원 케이블과 통신 케이블을 포함한 모든 포트가 커넥터 접속 방식이므로 단자대 접속 방식보다 배선이 쉽습니다. 또한 모든 포트에 Smartclick 커넥터가 장착되어 있어 원터치로 간편하게 접속할 수 있습니다.

간편한 유닛 교체

세이프티 I/O 블록에는 Web UI가 포함되어 있습니다.
Web UI를 사용하면 전용 지원 소프트웨어 없이도 세이프티 I/O 블록의 I/O 모니터링, 문제 해결, 복원에 필요한 백업, 복원 등의 작업을 수행할 수 있습니다.

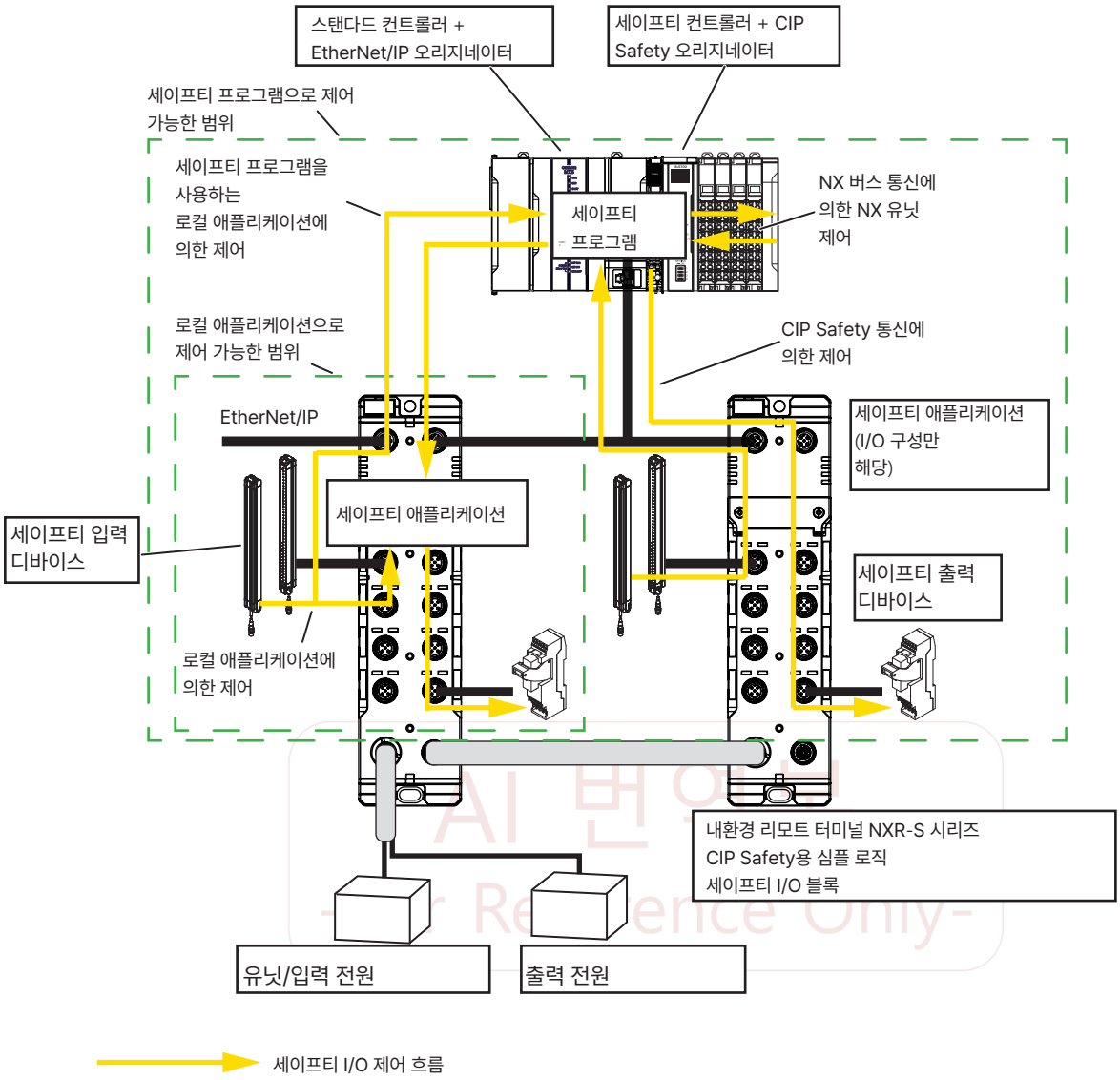
AI 번역본
-For Reference Only-

1-3 시스템 구성

세이프티 I/O 블록을 사용할 때의 시스템 구성을 세이프티 제어 시스템이라고 합니다.
본 절에서는 세이프티 제어 시스템과 세이프티 I/O 블록을 동일한 EtherNet/IP 네트워크에 접속할 때의 네트워크 토폴로지와, 세이프티 I/O 블록의 세이프티 입력 포트와 세이프티 출력 포트를 접속하는 캐스케이드 접속에 대해 설명합니다.

1-3-1 세이프티 제어 시스템

다음 그림은 세이프티 I/O 블록을 사용하는 세이프티 제어 시스템을 나타냅니다.



다음 표에서는 각 구성 디바이스에 대해 설명합니다.

구성 디바이스	설명
내환경 리모트 터미널 NXR-S 시리즈 심플 로직 CIP Safety용 세이프티 I/O 블록 NXR-SXD□□□□- CST	본 제품 CIP Safety 오리지네이터와 세이프티 데이터를 주고받는 디바이스입니다. CIP Safety 오리지네이터로부터 수신한 데이터를 세이프티 출력 디바이스로 출력하고, 세이프티 입력 디바이스로부터의 입력 신호를 CIP Safety 오리지네이터로 전송합니다. 또한 심플 로직 기능을 사용하여 세이프티 출력 디바이스를 조정 · 제어할 수도 있습니다.
스탠다드 컨트롤러 + EtherNet/IP 오리지네이터	세이프티 I/O 블록의 스탠다드 제어를 수행합니다. 또한 이 디바이스는 EtherNet/IP 통신을 수행하며, 세이프티 I/O 블록의 동작 상태를 모니터링하는 데 사용됩니다. 오므론 제품으로는 NX502 CPU 유닛과 NX102 CPU 유닛이 있습니다. 또한 오므론의 EtherNet/IP 오리지네이터로서 NX-CSG320을 사용할 수 있습니다.
세이프티 컨트롤러 + CIP Safety 오리지네이터	세이프티 I/O 블록과 CIP Safety 통신을 수행하며, 세이프티 프로그램으로 세이프티 기능을 제어합니다. 오므론 제품으로는 NX-SL5□□□가 있습니다.
세이프티 프로그램	세이프티 컨트롤러에서 실행되는 세이프티 제어용 사용자 프로그램입니다. NX 버스 통신, CIP Safety 통신, 기타 통신을 통해 세이프티 제어 시스템 전체를 제어합니다.
로컬 애플리케이션	세이프티 컨트롤러 대신 리모트 디바이스에서 실행되는 애플리케이션입니다. 본 제품에서는 이를 세이프티 애플리케이션이라고 하며, 세이프티 I/O 진단 기능과 로직 기능을 사용하여 구현됩니다. 세이프티 I/O 블록의 세이프티 애플리케이션은 I/O 구성 설정만 포함하는 애플리케이션과 로직 설정과 I/O 구성 설정을 모두 포함하는 애플리케이션의 두 가지 유형으로 분류됩니다. I/O 구성 설정만 있는 세이프티 애플리케이션은 세이프티 I/O 블록을 간이 리모트 I/O로 사용하기 위한 것으로, 세이프티 제어는 세이프티 컨트롤러의 세이프티 프로그램으로 구현됩니다. 반대로 로직 설정과 I/O 구성 설정을 모두 갖춘 세이프티 애플리케이션은 세이프티 컨트롤러를 거치지 않고 세이프티 I/O 블록 내에서 로컬 제어가 가능하므로 고속 응답이 필요한 애플리케이션에 적합합니다. 또한 세이프티 컨트롤러로부터 전송되는 세이프티 출력 데이터와 세이프티 애플리케이션의 로직 설정을 조합한 제어도 가능합니다.
유닛/입력 전원	세이프티 I/O 블록의 동작과 세이프티 입력 디바이스와의 인터페이스에 사용되는 전원입니다. 전원 커넥터(입력)에 외부 전원을 접속하여 전력을 공급합니다.
출력 전원	세이프티 출력 디바이스와의 인터페이스에 사용되는 전원입니다. 전원 커넥터(입력)에 외부 전원을 접속하여 전력을 공급합니다.
세이프티 입력 디바이스	세이프티 제어에 사용하기 위해 특별한 세이프티 대책이 적용되어 설계된 입력 디바이스입니다. 비상 정지 스위치, 세이프티 도어 스위치 등의 디바이스를 총칭하는 용어입니다.
세이프티 출력 디바이스	세이프티 제어에 사용하기 위해 특별한 세이프티 대책이 적용되어 설계된 출력 디바이스입니다. 세이프티 릴레이 등의 디바이스를 총칭하는 용어입니다.

샘플 열람본
-For Reference Only-

유형별로 분류하면 사용하는 애플리케이션과 프로그램에 따라 다음 네 가지 유형의 세이프티 제어 시스템이 있습니다. 특징에 따라 선택하십시오.

세이프티 제어 시스템 구성	세이프티 애플리케이션 사용	특징	설정 및 변경 방법 세이프티 애플리케이션	선정 기준
세이프티 컨트롤러가 제어를 수행하기 위한 구성	리모트 I/O 모드 애플리케이션	· 세이프티 컨트롤러가 네트워크를 통해 세이프티 출력 디바이스를 제어합니다. · 네트워크 통신을 사용하여 복잡하고 대규모 시스템을 구축할 수 있습니다. · 응답 시간이 길어질 수 있습니다.	· I/O 구성 설정만 있는 세이프티 애플리케이션을 설계하여 세이프티 컨트롤러에 다운로드합니다. 이 경우 세이프티 컨트롤러는 다운로드된 세이프티 애플리케이션(Type 1 Safety Open을 사용한 구성)을 바탕으로 세이프티 I/O 블록을 구성합니다. · 또는 사용자가 설계한 I/O 구성 설정만 있는 세이프티 애플리케이션을 세이프티 I/O 블록에 다운로드합니다(Web UI를 사용한 구성).	· 세이프티 I/O 블록의 로직 기능으로는 구현하기 어려운 복잡하고 대규모인 시스템을 구축하고자 하는 경우. · 세이프티 컨트롤러에서 세이프티 프로그램을 사용하는 경우.
프리셋 세이프티 애플리케이션을 사용하여 세이프티 I/O 블록이 제어를 수행하기 위한 구성	고정 애플리케이션	· 세이프티 I/O 블록이 세이프티 출력 디바이스를 제어합니다. · 심플 로직에 의한 소규모 제어 시스템입니다. · 고속 응답이 가능합니다.	· 세이프티 I/O 블록에 프리셋되어 있는 세이프티 애플리케이션(고정 애플리케이션)을 사용합니다.	· 고정 애플리케이션 중에는 그대로 사용할 수 있는 애플리케이션이 있습니다.

AI 번역본
-For Reference Only-

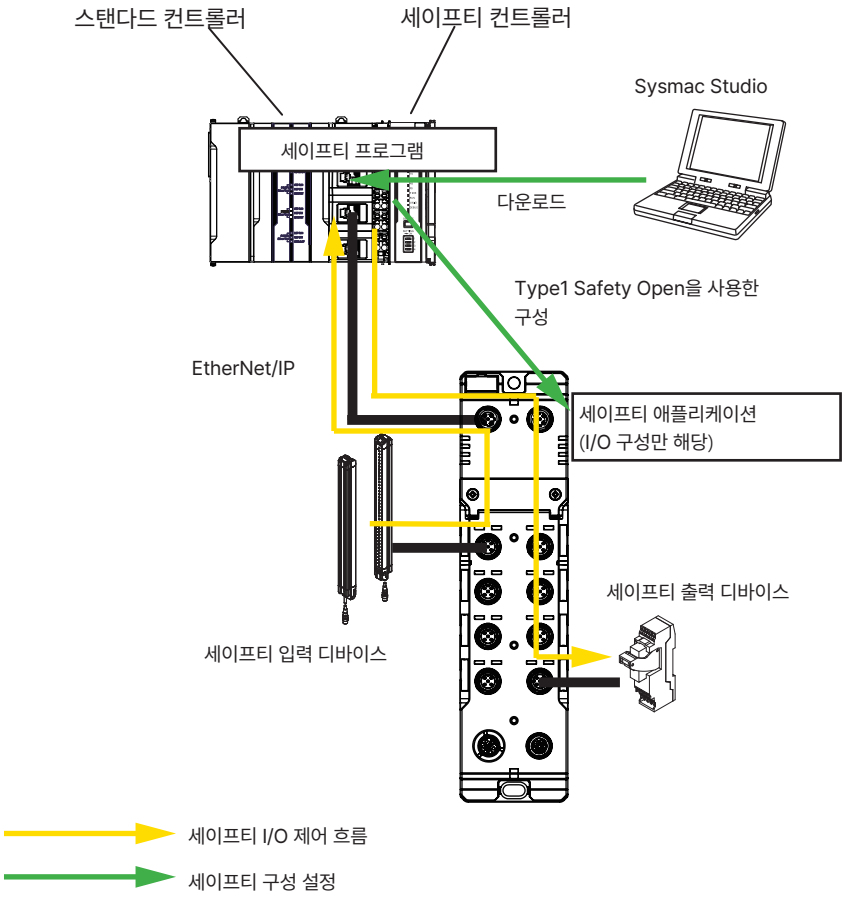
세이프티 제어 시스템 구성	세이프티 애플리케이션 사용	특징	설정 및 변경 방법 세이프티 애플리케이션	선정 기준
사용자가 설계한 세이프티 애플리케이션을 사용하여 세이프티 I/O 블록이 제어를 수행하기 위한 구성 (집중 관리형)	사용자 정의 애플리케이션	· 세이프티 I/O 블록이 세이프티 출력 디바이스를 제어합니다. · 사용자가 로직을 설계하므로 프리셋 세이프티 애플리케이션보다 유연성이 높은 제어가 가능합니다. 다음과 같은 시스템을 구축할 수 있습니다. a) 세이프티 프로그램을 사용하여 네트워크를 통해 수행하는 제어와 세이프티 애플리케이션을 사용하여 로컬에서 수행하는 고응답 제어를 조합한 제어. b) 사용자가 설계한 세이프티 애플리케이션을 사용한 로컬 제어. c) 제어점 수를 확장하기 위해 세이프티 I/O 블록을 캐스케이드 접속하여 수행하는 제어.	· 로직 설정과 I/O 구성 설정을 모두 포함하는 세이프티 애플리케이션 (사용자 정의 애플리케이션)을 설계하여 세이프티 컨트롤러에 다운로드합니다. · 세이프티 컨트롤러는 다운로드된 세이프티 애플리케이션을 바탕으로 세이프티 I/O 블록을 구성합니다(Type 1 Safety Open을 사용한 구성).	· 간단한 처리를 위해 세이프티 I/O 블록의 로직 기능으로 구현할 수 있는 애플리케이션입니다. · 고정 애플리케이션 중에는 그대로 사용할 수 있는 애플리케이션이 없습니다. · 여러 세이프티 I/O 블록 유닛에서 동일한 처리를 수행하기 위해 세이프티 컨트롤러 측에서 세이프티 애플리케이션을 관리하고자 하는 경우.
사용자가 설계한 세이프티 애플리케이션을 사용하여 세이프티 I/O 블록이 제어를 수행하기 위한 구성 (분산 관리형)	애드온 애플리케이션		· 로직 설정과 I/O 구성 설정을 포함하는 세이프티 애플리케이션 (애드온 애플리케이션)을 설계하여 세이프티 I/O 블록에 다운로드합니다 (Web UI를 사용한 구성). · 세이프티 I/O 블록에는 최대 5가지 유형의 애드온 애플리케이션을 저장할 수 있으며, 그중에서 세이프티 애플리케이션을 선택합니다.	· 간단한 처리를 위해 세이프티 I/O 블록의 로직 기능으로 구현할 수 있는 애플리케이션입니다. · 고정 애플리케이션 중에는 그대로 사용할 수 있는 애플리케이션이 없습니다. · 단일 세이프티 I/O 블록만 사용하기 위해 세이프티 I/O 블록 측에서 세이프티 애플리케이션을 관리하고자 하는 경우.

이하에 각 세이프티 제어 시스템의 구성 예와 동작 상세를 나타냅니다.

AI 번역본
-For Reference Only-

세이프티 컨트롤러가 제어를 수행하기 위한 구성(Type 1 Safety Open을 사용한 구성)

다음은 세이프티 컨트롤러가 제어를 수행하기 위한 구성(Type 1 Safety Open을 사용한 구성)의 그림입니다.

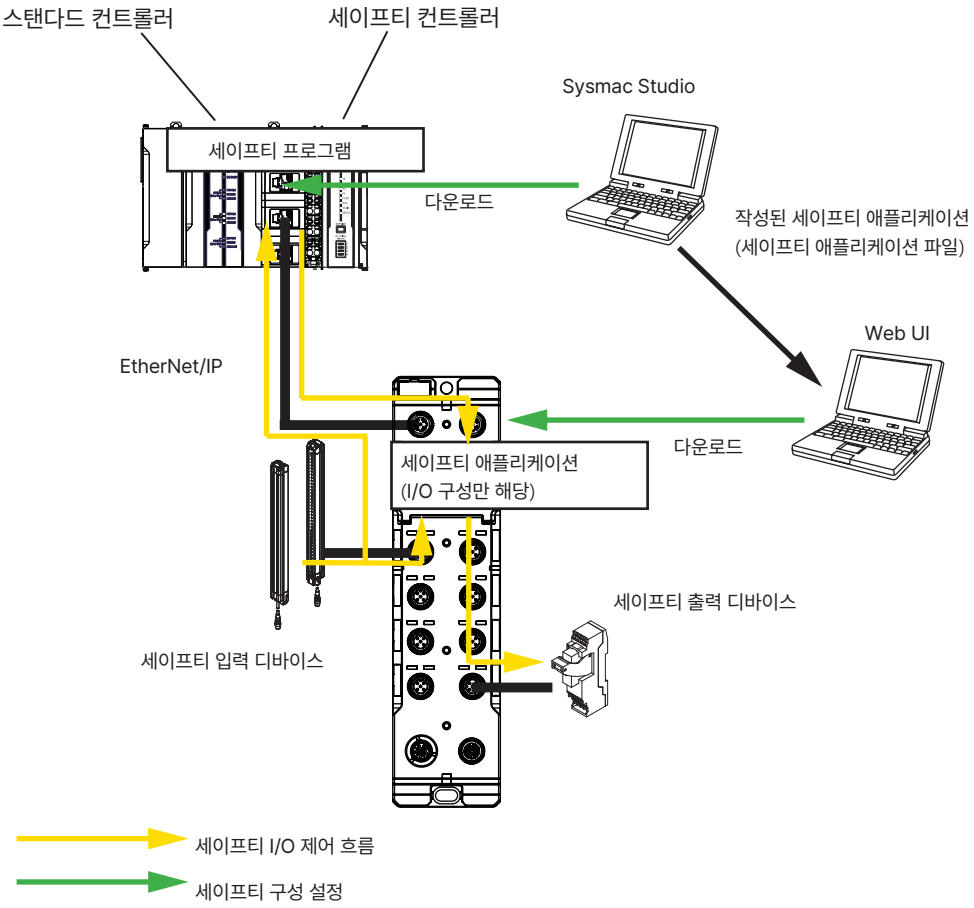


- 세이프티 컨트롤러의 세이프티 프로그램으로 제어를 수행합니다.
- 세이프티 I/O 블록에는 I/O 구성 설정만 있는 세이프티 애플리케이션을 사용합니다. 로직 기능은 사용하지 않습니다.
- 세이프티 애플리케이션은 세이프티 프로그램과 함께 세이프티 컨트롤러에 있으며, 커넥션이 열릴 때 세이프티 I/O 블록으로 전송됩니다.
- 세이프티 I/O 블록의 SETTING 로터리 스위치 SW1과 SW2를 모두 0으로 설정하십시오.

AI 번역본
-For Reference Only-

세이프티 컨트롤러가 제어를 수행하기 위한 구성(Web UI를 사용한 구성)

다음은 세이프티 컨트롤러가 제어를 수행하기 위한 구성(Web UI를 사용한 구성)의 그림입니다.

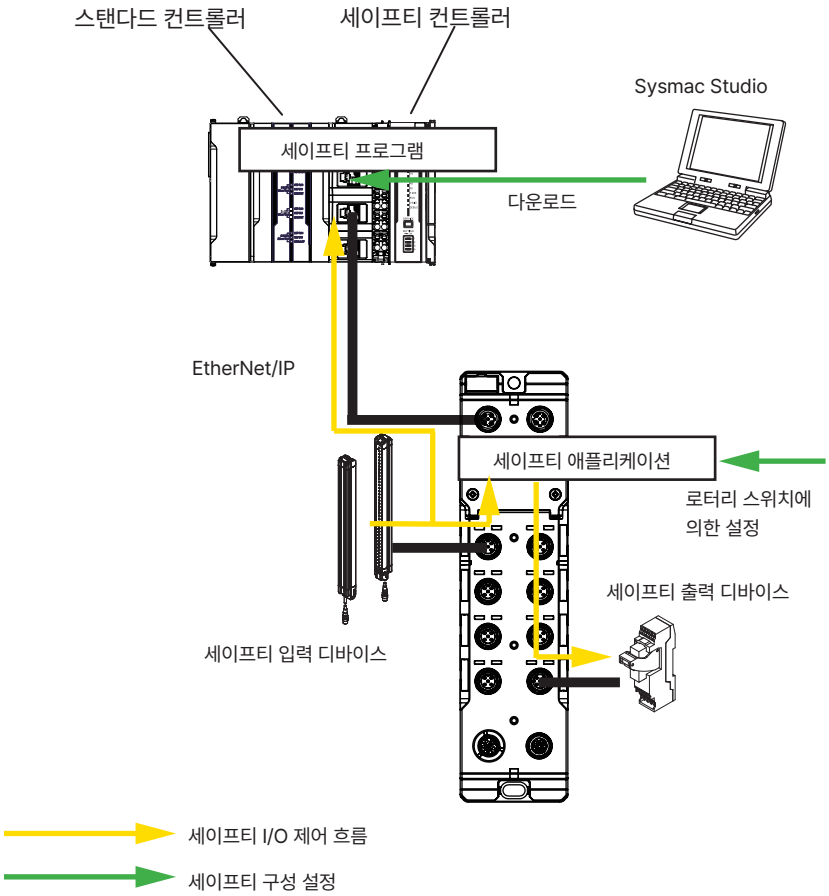


- 세이프티 컨트롤러의 세이프티 프로그램으로 제어를 수행합니다.
- 세이프티 컨트롤러가 세이프티 I/O 블록에 대해 Type 2a Safety Open 커넥션을 엽니다.
- 세이프티 I/O 블록에는 I/O 구성 설정만 있는 세이프티 애플리케이션을 사용합니다. 로직 기능은 사용하지 않습니다.
- 세이프티 프로그램은 세이프티 컨트롤러에 있습니다. 세이프티 애플리케이션은 Sysmac Studio에서 작성하며, Web UI를 사용하여 세이프티 I/O 블록에 다운로드합니다.
- 세이프티 I/O 블록의 SETTING 로터리 스위치 SW1과 SW2를 모두 0으로 설정하십시오.

AI 번역본
-For Reference Only-

프리셋 세이프티 애플리케이션을 사용하여 세이프티 I/O 블록이 제어를 수행하기 위한 구성

다음은 프리셋 세이프티 애플리케이션을 사용하여 세이프티 I/O 블록이 제어를 수행하기 위한 구성의 그림입니다.

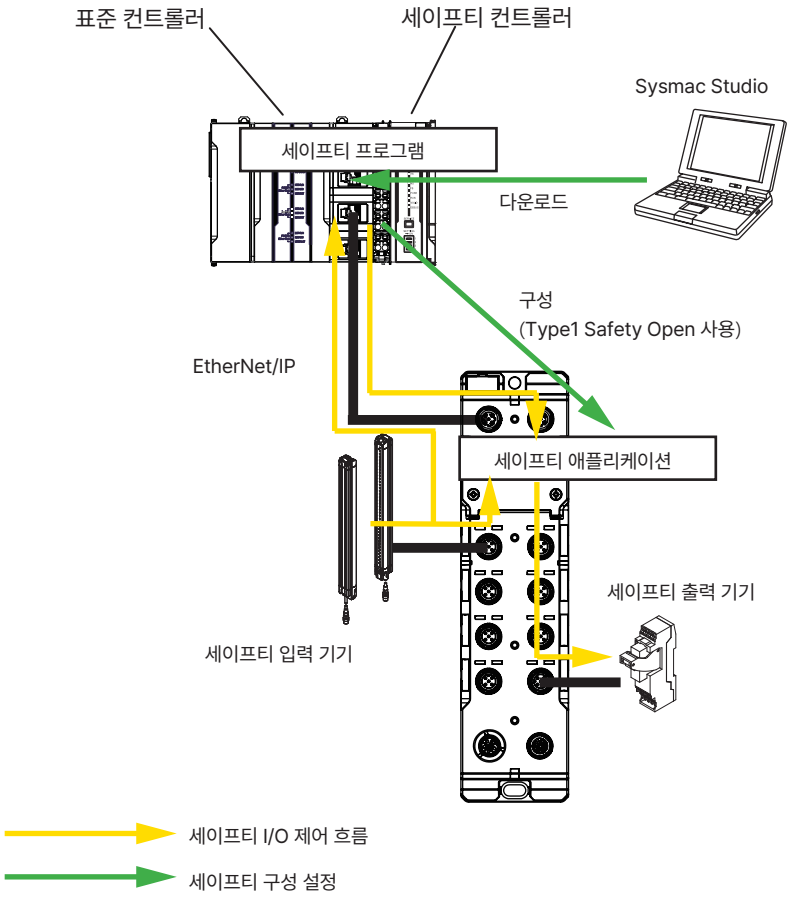


- 세이프티 I/O 블록에 프리셋된 세이프티 애플리케이션을 사용합니다. 세이프티 애플리케이션에는 로직 설정과 I/O 구성 설정이 포함됩니다.
- 세이프티 컨트롤러의 세이프티 프로그램을 사용하여 세이프티 I/O 블록의 I/O 데이터를 모니터링할 수도 있습니다.
- 세이프티 애플리케이션은 세이프티 I/O 블록에 있습니다.
- 세이프티 I/O 블록의 SETTING 로터리 스위치 SW1과 SW2를 모두 사용할 세이프티 애플리케이션(고정 애플리케이션)의 번호 1-3으로 설정하십시오.

AI 번역본
For Reference Only-

세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하기 위한 구성(집중 관리 방식)

다음 그림은 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하기 위한 구성(집중 관리 방식)을 나타냅니다.

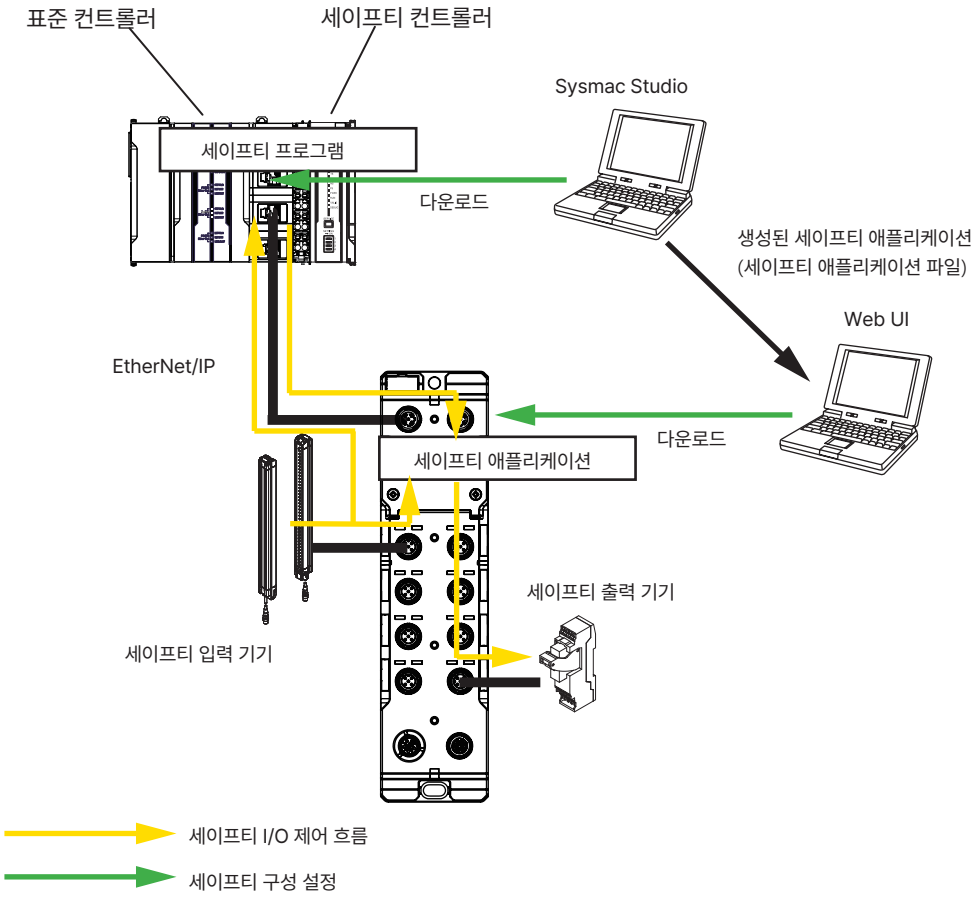


- 세이프티 I/O 블록의 세이프티 애플리케이션은 제어를 수행하는 데 사용됩니다. 세이프티 애플리케이션에는 로직 설정과 I/O 구성 설정이 포함됩니다.
- 세이프티 컨트롤러의 세이프티 프로그램과 조합하여 제어하는 것도 가능합니다.
- 세이프티 애플리케이션은 세이프티 컨트롤러 내에 세이프티 프로그램과 함께 존재하며, 접속이 열릴 때 세이프티 I/O 블록으로 전송됩니다.
- 세이프티 I/O 블록의 SETTING 로터리 스위치 SW1과 SW2를 모두 F(사용자 정의 애플리케이션)로 설정하십시오.

AI 번역본
-For Reference Only-

세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하기 위한 구성(분산 관리 방식)

다음 그림은 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하기 위한 구성(분산 관리 방식)을 나타냅니다.



- 세이프티 컨트롤러는 세이프티 I/O 블록에 대해 Type 2a Safety Open 접속을 엽니다.
- 세이프티 I/O 블록의 세이프티 애플리케이션은 제어를 수행하는 데 사용됩니다. 세이프티 애플리케이션에는 로직 설정과 I/O 구성 설정이 포함됩니다.
- 세이프티 컨트롤러의 세이프티 프로그램과 조합하여 제어하는 것도 가능합니다.
- 세이프티 프로그램은 세이프티 컨트롤러 내에 존재합니다. 세이프티 애플리케이션은 Sysmac Studio에서 작성되며, Web UI를 사용하여 세이프티 I/O 블록으로 다운로드합니다.
- 사용할 세이프티 애플리케이션(애드온 애플리케이션)의 번호 9-D로 세이프티 I/O 블록의 SETTING 로터리 스위치 SW1과 SW2를 모두 설정하십시오.

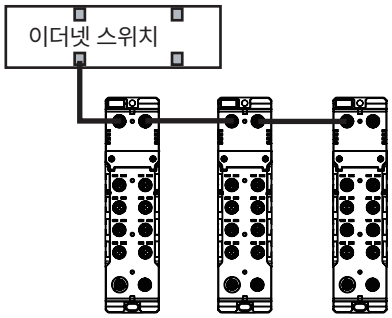
AI 번역본
-For Reference Only-

1-3-2 네트워크 토폴로지

세이프티 I/O 블록은 유닛에 통신 포트가 2개 있으므로, EtherNet/IP 네트워크의 라인, 스타, 트리, 링 토폴로지를 비롯한 다양한 토폴로지를 구성할 수 있습니다.

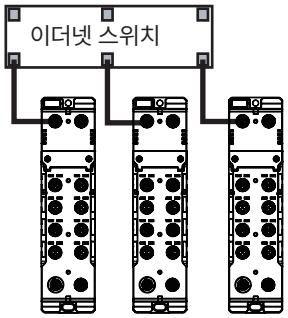
●라인

라인 토폴로지는 서로 접속된 여러 대의 세이프티 I/O 블록으로 구성됩니다.



●스타

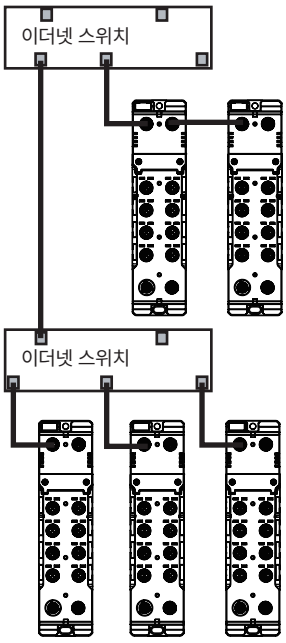
스타트 토폴로지는 이더넷 스위치에 접속된 여러 대의 세이프티 I/O 블록으로 구성됩니다.



●트리

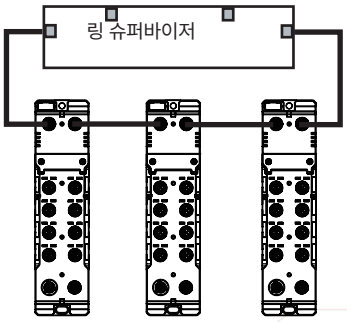
트리 토폴로지는 스타 토폴로지와 라인 토폴로지의 조합으로 구성됩니다.

AI 번역본
-For Reference Only-



● **링**

링 토폴로지는 링 슈퍼바이저와 세이프티 I/O 블록의 조합으로 구성됩니다. 링 토폴로지는 Device Level Ring(DLR) 기능을 사용하므로 한 곳에서 통신 케이블이 단선되어도 정상적인 통신을 유지할 수 있다는 특징이 있습니다. DLR 기능에 대한 자세한 내용은 8-10페이지의 8-4 Device Level Ring (DLR) 기능을 참조하십시오.



시 버 연 보
-For Reference Only-

1-3-3 캐스케이드 접속

NXR-SXD1204-CST의 경우, 여러 유닛의 세이프티 입력 포트와 세이프티 출력 포트를 캐스케이드로 접속할 수 있습니다.
이 구성에는 다음과 같은 장점이 있습니다.

・CIP Safety 통신의 통신 시간에 영향을 받지 않으므로 복잡한 로직을 구현할 수 있습니다.

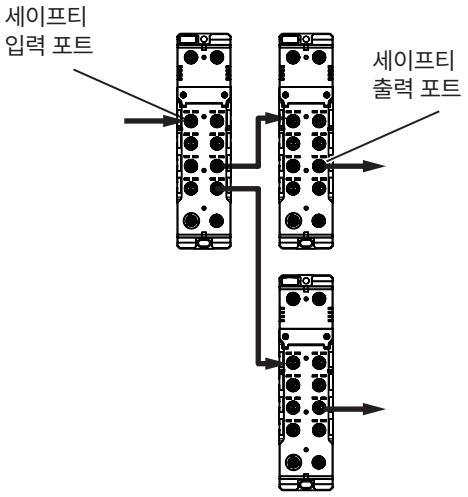
・세이프티 입력 단자와 세이프티 출력 단자의 수를 늘릴 수 있습니다.

세이프티 입력 기능과 세이프티 출력 기능의 I/O 구성 설정에는 듀얼 채널을 사용하십시오.

사용상의 주의

캐스케이드 접속을 사용할 때는 세이프티 응답 성능을 확인하십시오. 세이프티 응답 성능에 대한 자세한 내용은 9-1페이지의 섹션 9 세이프티 응답 성능을 참조하십시오.

1단 캐스케이드 접속을 지원하며, 아래 그림과 같이 최대 3대의
유닛을 접속할 수 있습니다.
캐스케이드 접속을 사용하면 CIP Safety 오리지네이터와의 CIP Safety 통신을 모든 유닛이 수행할
수 있습니다.



AI 번역본
-For Reference Only-

1-4 지원 소프트웨어

다음 표는 세이프티 I/O 블록과 함께 사용할 수 있는 지원 소프트웨어를 나타냅니다.

설정 대상	모델	지원 소프트웨어
세이프티 I/O 블록	· NXR-SXD1204-CST · NXR-SXD1204B-CST	· Sysmac Studio 버전 1.67 이상

사용상의 주의

Sysmac Studio를 사용한 설정은 NJ/NX 시리즈 CPU 유닛, NY 시리즈 인더스트리얼 패널 PC/인더스트리얼 박스 PC, 또는 통신 제어 유닛 NX-CSG320을 통해 수행합니다. 접속 방법으로는 이더넷 직접 접속 또는 이더넷 허브 접속을 사용하십시오.

AI 번역본
-For Reference Only-

2

사양 및 적용 절차

이 장에서는 세이프티 I/O 블록의 사양 및 적용 절차에 대해 설명합니다.

2-1 사양 2-2
2-1-1 일반 사양 2-2
2-1-2 통신 사양 2-3
2-1-3 세이프티 사양 2-4
2-1-4 유닛 사양 2-6
2-2 사용 절차 2-9
2-2-1 1단계. 시스템 설계 2-9
2-2-2 2단계. 소프트웨어 설계 2-9
2-2-3 3단계. 하드웨어 설계 2-10
2-2-4 4단계. 세이프티 응답 성능 계산 및 검증 2-10
2-2-5 5단계. 소프트웨어 설정 및 프로그래밍 2-11
2-2-6 6단계. 설치 및 배선 2-11
2-2-7 7단계. 동작 확인 2-12
2-2-8 8단계. 운전, 유지보수 및 점검 2-13

AI 번역본
-For Reference Only-

2-1 사양

이 절에서는 세이프티 I/O 블록의 다음 사양에 대해 설명합니다.

- 일반 사양
- 통신 사양
- 유닛 사양
- 세이프티 사양

2-1-1 일반 사양

세이프티 I/O 블록의 일반 사양은 다음과 같습니다.

항목		사양
보호 등급		IP67
동작 환경	**주위 동작 온도**	-10~55 °C
	주위 동작 습도	25%~85% (결로 없음)
	분위기	부식성 가스가 없어야 합니다.
	보관 온도	-25~65 °C
	보관 습도	25%~85% (결로 없음)
	고도	2,000 m 이하
	오염도	3 이하: IEC 61010-2-201에 준거
	노이즈 내성	IEC 61131-2 (Zone B) 및 EN 61131-2 (Zone B)에 준거 IEC 61326-3-1 및 EN 61326-3-1에 준거
	과전압 카테고리	카테고리 II: IEC 61010-2-201에 준거
	EMC 내성 레벨	Zone B
	내진동성	IEC 60068-2-6에 준거 5~8.4 Hz는 진폭 3.5 mm, 8.4~150 Hz는 10 m/s2 각 X, Y, Z 방향으로 100분간 기타 10~60 Hz는 진폭 0.35 mm, 60~150 Hz는 50 m/s2 각 X, Y, Z 방향으로 80분간
	내충격성	IEC 60068-2-27에 준거 150 m/s2, X, Y, Z축을 따라 6방향으로 각 3회
	절연내력	600 VAC (절연 회로 간)
	절연저항	20 MΩ 이상 (절연 회로 간)

한국본 -Preview Only-

항목		사양
규격 준거	TÜV Rheinland	· EN 61508 parts 1-3 · EN ISO 13849-1 · EN ISO 13849-2 · EN IEC 61131-2 · IEC 61326-3-1 · EN 60529 · EN 61131-6
	UL	· NRAQ/NRAQ7 · UL 61010-1 및 UL 61010-2-201 · CSA C22.2 No. 61010-1 및 CSA C22.2 No. 61010-2-201 · FSPC (IEC 61508 parts 1-3 및 ISO 13849-1)
	ODVA	· CIP Safety on EtherNet/IP · EtherNet/IP
	기타	· EU: EN61131-2, RCM · UKCA · KC: KC 등록 · 기계지침

주 오므론 웹사이트(www.ia.omron.com)를 참조하거나 관할 오므론 지점에 문의하여 최신 해당 규격을 확인하십시오.

2-1-2 통신 사양

세이프티 I/O 블록의 통신 사양은 다음과 같습니다.

항목		사양
물리 사양	포트	레이어2 스위치 포트
	물리 계층	10BASE-T/100BASE-TX 오토 네고시에이션 또는 고정 설정
	매체 접근 방식	CSMA/CD
	변조 방식	베이스밴드
	토폴로지	라인, 스타, 트리, 링
	전송 속도	100 Mbps (100BASE-TX)
	전송 매체	Category 5 이상의 트위스트 페어 케이블(권장 케이블: 알루미늄 테이프와 브레이드를 사용한 이중 실드 케이블)
	전송 거리	100 m 이하(노드 간 및 허브와 노드 간의 거리)
	라인당 접속 가능한 유닛 수	50
CIP Safety	CIP Safety 타겟	가능
	최대 접속 수	5 (입력 2/출력 3) 입력 접속은 멀티캐스트 통신을 사용하여 최대 8개의 CIP Safety 오리지네이터와 동일한 데이터를 공유할 수 있습니다.
	패킷 간격	5 - 500 ms
	최대 데이터 크기	입력: 9바이트 출력: 3바이트

항목		사양
EtherNet/IP 통신	**EtherNet/IP 타겟**	가능 (Exclusive Owner, Input Only, Listen Only)
	최대 접속 수	2 (입력 2/출력 0) 입력 접속은 멀티캐스트 통신을 사용하여 EtherNet/IP 오리지네이터와 동일한 데이터를 공유할 수 있습니다.
	패킷 간격	5 - 10,000 ms
	최대 데이터 크기	입력: 9바이트
	DLR	링 노드 지원
	EtherNet/IP 적합성 시험	CT21에 준거
CIP 메시지 통신	**프로토콜**	Class3/UCMM
	최대 접속 수 (Class 3)	5
	데이터 크기	504바이트
HTTPS 통신	**TLS 버전**	TLS 1.2를 지원합니다. TLS 1.0, TLS 1.1 및 SSL은 지원하지 않습니다.
	인증 방식	서버 인증(X.509) 및 세이프티 패스워드에 의한 세션 인증

다음 표는 각 외부 인터페이스별로 사용할 포트 번호, 통신 경로 암호화 기능의 사용 가능 여부, 기본값에서 활성화/비활성화 여부, 활성화와 비활성화 간 전환 가능 여부를 나타냅니다.

외부 인터페이스		포트 번호	통신 경로 암호화	활성화/비활성화 (기본값)	활성화/비활성화 전환 가능 여부
이더넷 포트	**CIP Safety**	UDP/2222	아니요	활성화	불가능
	HTTPS	TCP/443	예	활성화	불가능
	SNTP	UDP/123	아니요	비활성화	Sysmac Studio, Web UI 및 CIP 메시지로 가능
	DHCP	UDP/68	아니요	비활성화	Sysmac Studio, Web UI 및 CIP 메시지로 가능
	EtherNet/IP	UDP/2222	아니요	활성화	불가능
	CIP 메시지	TCP/44818, UDP/44818	아니요	활성화	불가능
로터리 스위치		해당 없음	해당 없음	활성화	불가능

AI 번역본 For Reference Only

2-1-3 세이프티 사양

세이프티 I/O 블록의 세이프티 사양은 다음과 같습니다:

항목	사양			
	세이프티 입력		세이프티 출력	
	듀얼 채널	싱글 채널	듀얼 채널	싱글 채널
PL	최대 PL e	최대 PL d*1	최대 PL e	최대 PL c*2
카테고리	최대 Cat.4	최대 Cat.2*1	최대 Cat.4	최대 Cat.2*2
$MTTF_D$	1428년	100년	1431년	100년
Mission Time	20년	20년	20년	20년
DCavg	98.61%	98.60%	98.60%	98.60%
SIL	최대 SIL 3	최대 SIL 2	최대 SIL 3	최대 SIL 1

항목	사양			
	세이프티 입력		세이프티 출력	
	듀얼 채널	싱글 채널	듀얼 채널	싱글 채널
PFH	4.6×10^{-10} 1/h	4.6×10^{-10} 1/h	4.6×10^{-10} 1/h	4.6×10^{-10} 1/h

***1.** 싱글 채널 세이프티 입력으로 Cat.2/PLd를 달성하려면, 세이프티 제어 시스템이 다음 요건을 충족하는 세이프티 출력 기능을 갖추도록 하십시오.

・고장이 발생했을 때 세이프티 제어 시스템이 안전 상태로 전환될 수 있어야 합니다.

・고장이 발생했을 때 세이프티 제어 시스템이 고장 원인이 해소될 때까지 안전 상태를 유지할 수 있어야 합니다.

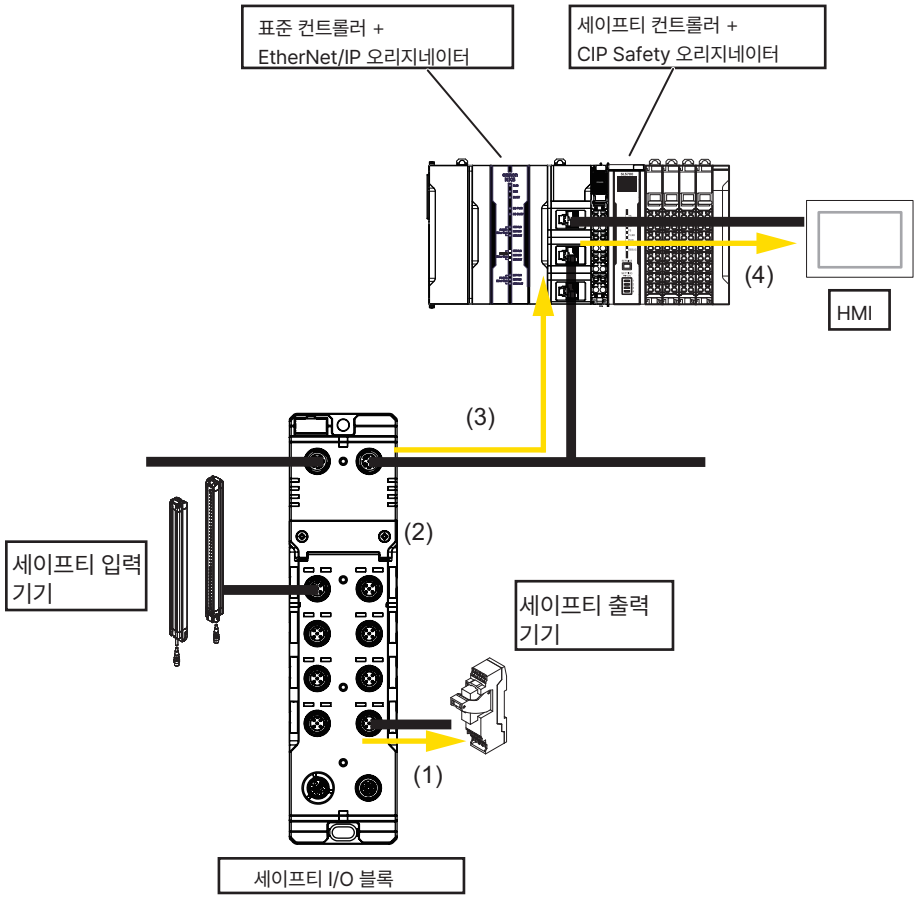
***2.** 싱글 채널 세이프티 출력으로 Cat.2/PLc를 달성하려면, CIP Safety 통신 또는 EtherNet/IP 통신을 사용하여 세이프티 I/O 블록의 출력 단자를 모니터링함으로써 세이프티 제어 시스템으로서 세이프티 출력의 고장을 검출하십시오.
세이프티 출력의 고장이 검출되면 표시등, HMI 등의 수단으로 사용자에게 에러 발생을 알리십시오.
출력 단자 상태 모니터링 대상은 입력 어셈블리의 다음 4가지 비트 유형 중 하나여야 합니다.

어셈블리	모니터링 대상 비트	비트 이름
Safety Input 1	출력 단자 상태(통합)	Combined Safety Output Status
Safety Input 2	출력 단자 상태(통합)	Combined Safety Output Status
Safety Input 3	출력 단자 상태(통합)	Combined Safety Output Status
	출력 단자 상태(개별)	Safety Output0 Status to Safety Output3 Status

세이프티 출력 단자에 에러가 발생한 후 사용자에게 에러 발생을 알리기까지의 절차는 다음과 같습니다.

1. 세이프티 출력 단자에 에러가 발생합니다.
2. 세이프티 I/O 블록이 세이프티 출력 단자의 에러를 검출하고, 에러가 발생한 세이프티 출력 단자를 Inactive로 설정합니다. 또한 대상 출력 단자 상태 비트를 FALSE로 설정합니다.
3. 세이프티 컨트롤러 또는 표준 컨트롤러가 세이프티 I/O 블록의 출력 단자 상태가 FALSE가 된 것을 검출합니다.
4. 세이프티 컨트롤러 또는 표준 컨트롤러가 표시등, HMI 등의 수단으로 사용자에게 에러 발생을 알립니다.

AI 번역본
-For Reference Only-



또한 세이프티 제어 시스템이 안전 상태로 전환될 때는 주어진 정보를 바탕으로 세이프티 I/O 블록 이외의 회로 차단기를 사용하여 세이프티 출력 기기의 전원을 차단하십시오. 세이프티 출력 기기의 전원이 차단되기까지의 시간은 (세이프티 I/O 블록이 에러 발생을 나타내기까지의 시간: 265 ms), (네트워크 반응 시간), (세이프티 I/O 블록 이외의 차단 기기의 응답 시간)의 합으로 계산해야 합니다.

모니터링 대상 비트가 출력 단자 상태(통합)인 경우, 사용자는 세이프티 I/O 블록이 제어하는 모든 세이프티 출력 기기의 전원을 차단해야 합니다. 모니터링 대상 비트가 출력 단자 상태(개별)인 경우, 사용자는 에러가 발생한 세이프티 출력 기기의 전원을 차단해야 합니다.

2-1-4 유닛 사양

세이프티 I/O 블록 유닛의 사양은 다음과 같습니다.

항목	사양	
	NXR-SXD1204-CST	NXR-SXD1204B-CST
유닛 이름	내환경 리모트 터미널 NXR-S 시리즈 CIP Safety 대응 심플 로직 세이프티 I/O 블록	
치수	60 (W) × 240 (H) × 34.2 (D) [mm] (커넥터 포함 시 60 (W) × 240 (H) × 46.65 (D) [mm])	
장착 방법	M5 나사에 의한 장착	
장착 강도	100 N	
장착 방향 및 제한 사항	장착 방향: 6방향 가능 제한 사항: 제한 없음	
사용 가능한 커넥터	· EtherNet/IP 통신 커넥터: M12 (D-coding, female) · 전원 커넥터: M12 (L-coding, female), M12 (L-coding, male) · I/O 커넥터: M12 (A-coding, female)	

항목		사양	
		NXR-SXD1204-CST	NXR-SXD1204B-CST
커넥터 강도		30 N 모든 커넥터에 적용	
나사 조임 토크		· EtherNet/IP 통신 커넥터 및 I/O 커넥터 (M12 나사): 0.5 ~0.6N · m*1 · 전원 커넥터 (M12 나사): 0.39~0.49N · m*1 · 유닛 장착 (M5 나사): 1.47~1.96 N · m · 로터리 스위치 커버 (M3 나사): 0.4~0.6 N · m	
질량		710 g	700 g
유닛/입력 전원 전압		24 VDC (19.2~28.8 VDC)	
출력 전원 전압		24 VDC (19.2~28.8 VDC)	
절연 방식		디지털 아이솔레이터 절연	
유닛 내부 절연		유닛/입력 전원과 출력 전원 사이를 절연	
절연저항		절연 회로 간 20 MΩ 이상 (100 VDC에서)	
최대 전원 전류		9 A	
소비전류		· 유닛/입력 전원: 220mA · 출력 전원: 40mA	
세이프티 I/O 단자 수	세이프티 입력 단자 수	12	
	테스트 출력 단자 수	12	
	세이프티 출력 단자 수	4	
I/O 포트 수	세이프티 입력 포트	5핀 × 6포트	5핀 × 4포트
	세이프티 출력 포트	4핀 × 2포트	0
	세이프티 I/O 포트	0	8핀 × 2포트
I/O 포트당 단자 수	세이프티 입력 포트	· 세이프티 입력: 2 · 테스트 출력: 2 · 유닛/입력 전원: 1	
	세이프티 출력 포트	· 세이프티 출력: 2 · 출력 전원: 2	-
	세이프티 I/O 포트	-	· 세이프티 입력: 2 · 테스트 출력: 2 · 세이프티 출력: 2 · 유닛/입력 전원: 1 · 출력 전원: 1
세이프티 입력 전류		4.5 mA (대표값)	
세이프티 입력 ON 전압		11 VDC 이상	
세이프티 입력 OFF 전압/OFF 전류		5 VDC 이하, 1 mA 이하	
테스트 출력 유형		소싱 출력 (PNP)	
테스트 출력 정격 전류		0.7 A/포인트	
테스트 출력 ON 잔류 전압		1.2 V 이하 (유닛/입력 전원 + 단자와 각 출력 단자 간)	
테스트 출력 누설 전류		0.1 mA 이하	
세이프티 출력 내부 I/O 공통		PNP (소싱 출력)	
세이프티 출력 최대 부하 전류		2.0 A/포인트 및 9.0 A/유닛	0.7 A/포인트 및 9.0 A/유닛

AI 번역본
-Reference Only-

항목		사양	
		NXR-SXD1204-CST	NXR-SXD1204B-CST
세이프티 출력 ON 잔류 전압		1.2 V 이하 (출력 전원 + 단자와 각 출력 단자 간)	
세이프티 출력 OFF 잔류 전압		2 V 이하 (출력 전원 - 단자와 각 출력 단자 간)	
세이프티 애플리케이션 기능	로직 없음	리모트 I/O 모드 애플리케이션	
	로직 있음	고정 애플리케이션, 사용자 정의 애플리케이션, 애드온 애플리케이션	

***1.** 이 값은 나사식 커넥터에 대한 것입니다. Smartclick 커넥터의 경우 토크 관리가 필요하지 않습니다. 커넥터를 끝까지 삽입한 후 약 1/8 회전시키십시오.

AI 번역본
-For Reference Only-

2-2 사용 절차

이 절에서는 세이프티 I/O 블록의 사용 절차에 대해 설명합니다.

2-2-1 1단계. 시스템 설계

단계	설명	참조
1-1단계 리스크 평가를 수행하여 세이프티 대책 결정	· 잠재적 위험 요인을 특정하고 리스크 평가를 수행하십시오. · 리스크를 저감하기 위한 대책을 검토하여 결정하십시오.	-
↓		
1-2단계 세이프티 기기 선정	세이프티 I/O 블록을 사용할지 여부를 결정하십시오. 또한 사용할 모델을 결정하십시오.	2-2페이지의 2-1 사양
↓		
1-3단계 네트워크 기기 선정	통신 토폴로지 및 기타 사양을 확인하고 이더넷 네트워크 구성을 결정하십시오.	1-4페이지의 1-3 시스템 구성
	세이프티 I/O 블록의 사양에 적합한 이더넷 스위치, 트위스트 페어 케이블, 통신 커넥터를 선정하십시오.	5-29페이지의 5-5 접속 기기
↓		
1-4단계 세이프티 컨트롤러와 세이프티 I/O 블록 간의 인터페이스 설계	세이프티 컨트롤러와 세이프티 I/O 블록 간의 인터페이스를 설계하십시오.	7-27페이지의 7-3 CIP Safety 통신 설정
↓		
1-5단계 표준 컨트롤러와 세이프티 I/O 블록 간의 인터페이스 설계	표준 컨트롤러와 세이프티 I/O 블록 간의 인터페이스를 설계하십시오.	7-38페이지의 7-4 EtherNet/IP 통신 설정
↓		
1-6단계 기기 보안 설계	보안 가이드라인에 따라 설비 및 기기의 보안 설정을 구성하십시오.	10-1페이지의 섹션 10 보안 가이드라인

AI 번역본
For Reference Only

2-2-2 2단계. 소프트웨어 설계

단계	설명	참조
2-1단계 I/O 기기 및 처리 설계	세이프티 I/O 블록에 대해 다음 항목을 설계하십시오. · 접속할 세이프티 I/O 기기 · 접속할 표준 I/O 기기	6-1페이지의 섹션 6 세이프티 I/O 블록의 동작
↓		

단계	설명	참조
2-2단계 프로그램 설계	**세이프티 컨트롤러가 제어를 수행하도록 구성하는 경우** 세이프티 컨트롤러용 세이프티 프로그램을 설계하십시오	NX 시리즈 세이프티 컨트롤 유닛/ 통신 컨트롤 유닛 유저 매뉴얼 (Cat. No. Z395)
	세이프티 I/O 블록이 사전 설정된 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성하는 경우 ・세이프티 애플리케이션으로 고정 애플리케이션을 사용하십시오. ・고정 애플리케이션 중에서 사용할 애플리케이션을 결정하십시오.	6-24페이지의 고정 애플리케이션
	세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성(집중 관리 방식)하는 경우 ・세이프티 애플리케이션으로 사용자 정의 애플리케이션을 사용하십시오. ・사용자 정의 애플리케이션의 로직을 설계하십시오.	6-25페이지의 사용자 정의 애플리케이션
	세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성(분산 관리 방식)하는 경우 ・세이프티 애플리케이션으로 사용자가 설계한 애드온 애플리케이션을 사용하십시오. ・애드온 애플리케이션의 로직을 설계하십시오.	6-26페이지의 애드온 애플리케이션

2-2-3 3단계. 하드웨어 설계

단계	설명	참조
3단계. 통신, 전원 공급, 외부 I/O 기기의 배선 결정	세이프티 I/O 블록에 전원을 공급하는 방법을 결정하십시오.	4-1페이지의 섹션 4 전원 공급 시스템 설계
	・세이프티 I/O 블록의 사양에 적합한 통신 케이블을 선정하십시오. ・세이프티 I/O 블록에 공급될 전원 전압과 최대 전류를 계산한 후 전원 케이블을 선정하십시오. ・세이프티 I/O 기기 간을 접속하는 I/O 케이블을 선정하십시오.	5-29페이지의 5-5 접속 기기

AI 번역본
For Reference Only

2-2-4 4단계. 세이프티 응답 성능 계산 및 검증

단계	설명	참조
4-1단계 세이프티 통신 성능 계산	1-4단계 및 1-5단계에서 결정한 CIP Safety 접속 및 태그 데이터 링크 접속을 바탕으로 세이프티 컨트롤러의 EPI, 통신 부하, 세이프티 태스크 주기를 검증하십시오.	9-1페이지의 섹션 9 세이프티 응답 성능 NX 시리즈 세이프티 컨트롤 유닛/통신 컨트롤 유닛 유저 매뉴얼의 세이프티 반응 시간 계산 (Cat. No. Z395)

단계	설명	참조
4-2단계 세이프티 반응 시간 계산	세이프티 I/O 기기 및 세이프티 I/O 블록의 I/O 응답 시간과 CIP Safety 접속의 응답 시간을 바탕으로 세이프티 반응 시간을 계산하십시오.	6-1페이지의 섹션 6 세이프티 I/O 블록의 동작 9-1페이지의 섹션 9 세이프티 응답 성능
↓		
4-3단계 세이프티 거리 계산 및 요구 사양 충족 여부 검증	세이프티 반응 시간을 사용하여 세이프티 거리를 계산하십시오. 세이프티 거리가 요구 사항을 충족하는지 확인하십시오. 요구 사항을 충족하지 않으면 시스템 설계부터 다시 설계를 재검토하십시오.	-

2-2-5 5단계. 소프트웨어 설정 및 프로그래밍

단계	설명	참조
5-1단계 세이프티 네트워크 컨트롤러 시스템 작성	세이프티 I/O 블록을 배치하십시오.	NX 시리즈 세이프티 컨트롤 유닛/통신 컨트롤 유닛 유저 매뉴얼의 CPU 랙 구성 및 설정 *(Cat. No. Z395)*
↓		
5-2단계 통신 설정, 프로그래밍, 및 세이프티 I/O 단자에 대한 접속 기기 할당	**세이프티 컨트롤러가 제어를 수행하도록 구성하는 경우** 오른쪽의 참조 항목을 참조하십시오.	7-3페이지의 7-1-1 세이프티 컨트롤러가 제어를 수행하도록 구성하는 절차 설정 (Type 1 Safety Open을 사용하는 구성)
	세이프티 I/O 블록이 사전 설정된 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성하는 경우 오른쪽의 참조 항목을 참조하십시오.	7-9페이지의 7-1-3 세이프티 I/O 블록이 사전 설정된 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성하는 절차 설정
	세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성(집중 관리 방식)하는 경우 오른쪽의 참조 항목을 참조하십시오.	7-11페이지의 7-1-4 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성 (집중 관리 방식)하는 절차 설정
	세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성(분산 관리 방식)하는 경우 오른쪽의 참조 항목을 참조하십시오.	7-14페이지의 7-1-5 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성(분산 관리 방식)하는 절차 설정

AI 번역본
For Reference Only

2-2-6 6단계. 설치 및 배선

단계	설명	참조
6-1단계 설치	장착 구멍을 사용하여 나사로 세이프티 I/O 블록을 고정하십시오.	5-2페이지의 5-1 유닛 설치

단계	설명	참조
	로터리 스위치를 사용하여 IP 주소를 설정하는 방법을 선택하십시오.	7-71페이지의 7-10 IP 주소 설정
	로터리 스위치를 사용하여 세이프티 애플리케이션을 선택하십시오.	3-10페이지의 3-3 로터리 스위치
↓		
6-2단계 전원 공급 및 I/O 배선	세이프티 I/O 블록에 전원 케이블과 I/O 케이블을 접속하십시오.	5-12페이지의 5-3 전원 배선 5-19페이지의 5-4 I/O 케이블 배선
	I/O 케이블의 배선 확인을 수행하십시오.	8-13페이지의 8-6 I/O 배선 확인 기능
↓		
6-3단계 이더넷 케이블 접속	세이프티 I/O 블록에 통신 케이블을 접속하십시오.	5-5페이지의 5-2 EtherNet/IP 네트워크 배선
	통신 케이블의 배선 확인을 수행하십시오.	8-31페이지의 8-13 통신 케이블 진단 기능

2-2-7 7단계. 동작 확인

단계	설명	참조
7단계. 동작 확인	**세이프티 컨트롤러가 제어를 수행하도록 구성하는 경우** 오른쪽의 참조 항목을 참조하십시오.	7-3페이지의 7-1-1 세이프티 컨트롤러가 제어를 수행하도록 구성하는 절차 설정 (Type 1 Safety Open을 사용하는 구성)
	세이프티 I/O 블록이 사전 설정된 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성하는 경우 오른쪽의 참조 항목을 참조하십시오.	7-9페이지의 7-1-3 세이프티 I/O 블록이 사전 설정된 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성하는 절차 설정
	세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성(집중 관리 방식)하는 경우 오른쪽의 참조 항목을 참조하십시오.	7-11페이지의 7-1-4 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성 (집중 관리 방식)하는 절차 설정
	세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성(분산 관리 방식)하는 경우 오른쪽의 참조 항목을 참조하십시오.	7-14페이지의 7-1-5 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하도록 구성(분산 관리 방식)하는 절차 설정

참고용 역본
-For Reference Only-

2-2-8 8단계. 운전, 유지보수 및 점검

단계	설명	참조
8-1단계 운전	전원 투입 시 모드를 설정하거나 동작 모드를 변경하여 동작 모드가 Executing으로 전환되는지 확인하십시오.	7-95페이지의 7-16 동작 모드 변경
↓		
8-2단계 에러 발생 시 문제 해결	에러가 발생하면 표시등 및 모니터 기능을 사용하여 에러를 확인하고 원인을 파악한 후 에러를 해소하십시오.	11-1페이지의 섹션 11 문제 해결
	세이프티 I/O 블록의 전원 모니터 기능을 실행하십시오.	8-22페이지의 8-10 전원 공급 모니터 기능
	세이프티 I/O 블록의 유닛 식별 기능을 실행하십시오.	8-16페이지의 8-8 유닛 식별 기능
	세이프티 I/O 블록의 IP 주소 표시 기능을 실행하십시오.	8-19페이지의 8-9 IP 주소 표시 기능
	세이프티 I/O 블록의 통신 케이블 진단 기능을 실행하십시오.	8-31페이지의 8-13 통신 케이블 진단 기능
↓		
8-3단계 점검 및 교체	세이프티 I/O 블록이 고장 나면 교체하십시오.	12-1페이지의 섹션 12 점검 및 유지보수
	세이프티 I/O 블록을 교체한 경우 펌웨어를 업데이트하십시오.	8-35페이지의 8-14 펌웨어 업데이트 기능

AI 번역본
-For Reference Only-

AI 번역본
-For Reference Only-

3

부품 명칭 및 기능

이 장에서는 세이프티 I/O 블록 각 부품의 명칭과 기능을 설명합니다.

3-1 부품 및 명칭 3-2

3-2 표시등 3-5

3-2-1 상태 표시등 3-5
3-2-2 I/O 표시등 3-8
3-2-3 유닛 식별 표시등 3-9

3-3 로터리 스위치 3-10

3-4 커넥터 3-11

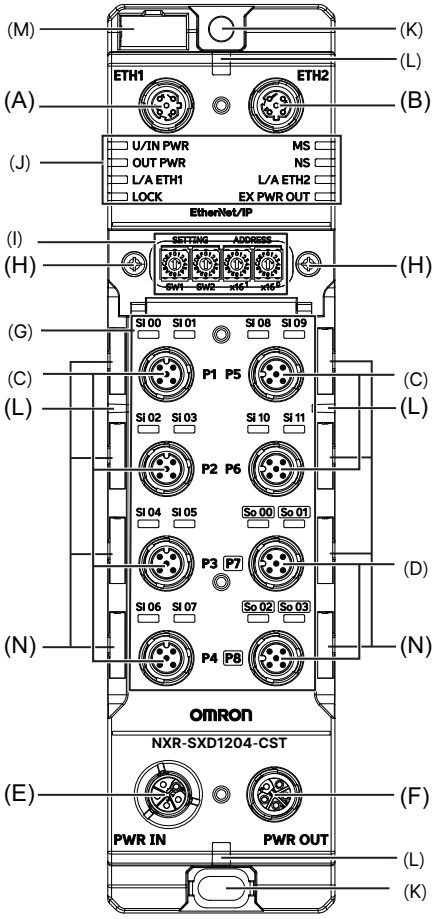
3-4-1 EtherNet/IP 통신 커넥터 3-11
3-4-2 전원 커넥터 3-11
3-4-3 I/O 커넥터 3-12

AI 번역본
-For Reference Only-

3-1 부품 및 명칭

이 절에서는 세이프티 I/O 블록의 부품 명칭을 설명합니다.

● NXR-SXD1204-CST

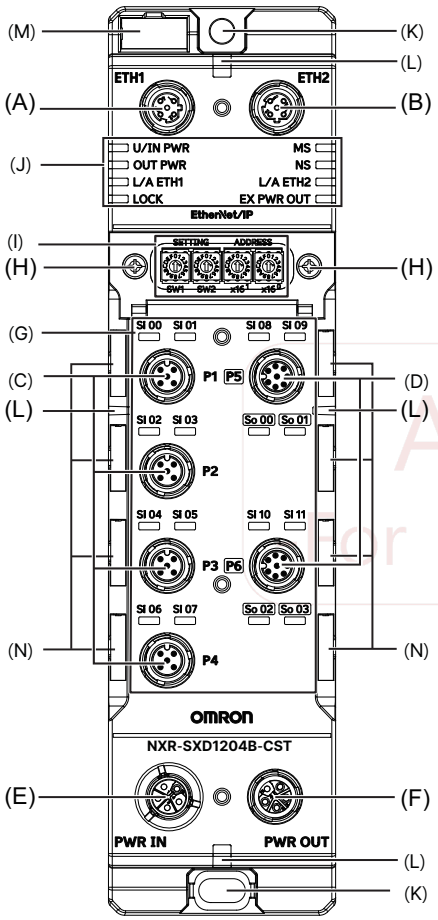


기호	명칭	기능
(A)	EtherNet/IP 통신 커넥터 1	EtherNet/IP 포트 1용 커넥터입니다. 커넥터는 M12 커넥터(D-coding, female, Smartclick 지원)입니다. 통신 케이블을 접속하십시오.
(B)	EtherNet/IP 통신 커넥터 2	EtherNet/IP 포트 2용 커넥터입니다. 커넥터는 M12 커넥터(D-coding, female, Smartclick 지원)입니다. 통신 케이블을 접속하십시오.
(C)	I/O 커넥터 (세이프티 입력 포트용)	이 커넥터는 세이프티 입력 기기를 접속하기 위한 것입니다. I/O 커넥터 측면에 탈착식 마커를 부착하십시오. 커넥터는 M12 커넥터(A-coding, female, 5핀, Smartclick 지원)입니다. I/O 케이블(5선식)을 접속하십시오.
(D)	I/O 커넥터 (세이프티 출력 포트용)	이 커넥터는 세이프티 출력 기기를 접속하기 위한 것입니다. 분리 가능한 마커를 I/O 커넥터 측면에 붙이십시오. 커넥터는 M12 커넥터(A코딩, 암형, 5핀, Smartclick 지원)입니다. I/O 케이블(5선식)을 접속하십시오.

-For Reference Only-

기호	명칭	기능
(E)	전원 공급 커넥터 (입력)	이 커넥터는 유닛/입력 전원과 출력 전원을 공급하기 위한 것입니다. 커넥터는 M12 커넥터(L코딩, 수형, Smartclick 지원)입니다. 외부 전원에 접속하기 위한 전원 공급 케이블을 접속하십시오.
(F)	전원 공급 커넥터 (출력)	이 커넥터는 로컬 노드에서 다른 노드로 유닛/입력 전원과 출력 전원을 공급하기 위한 것입니다. 전원 공급 방식이 스루 배선 전원 공급인 경우 이 커넥터를 사용하십시오. 커넥터는 M12 커넥터(L코딩, 암형, Smartclick 지원)입니다.
(G)	I/O 표시등	이 표시등은 각 포트 단자의 세이프티 입력 또는 세이프티 출력 상태를 나타냅니다.
(H)	커버 장착 구멍	이 나사 구멍은 로터리 스위치 커버를 장착하기 위한 것입니다. 이 구멍은 두 곳에 마련되어 있습니다. 위 그림은 커버를 나사로 장착한 상태의 구멍을 나타냅니다.
(I)	로터리 스위치	이 스위치는 세이프티 애플리케이션을 선택하고 IP 주소를 설정하기 위한 것입니다.
(J)	상태 표시등	이 표시등은 세이프티 I/O 블록의 현재 동작 상태를 나타냅니다.
(K)	유닛 장착 구멍	이 구멍은 유닛을 장착하기 위한 것입니다. 이 구멍은 두 곳에 마련되어 있습니다. M5 나사로 유닛을 장착하십시오.
(L)	유닛 식별 표시등	이 표시등은 유닛 식별 기능을 사용할 때 점등하여 알려줍니다.
(M)	유닛 식별 마커	이 마커는 세이프티 I/O 블록을 식별하기 위한 것입니다. 흰색입니다.
(N)	I/O 식별 마커	이 마커는 I/O 단자를 식별하기 위한 것입니다. 흰색입니다.

● NXR-SXD1204B-CST



AI 번역본
For Reference Only-

기호	명칭	기능
(A)	EtherNet/IP 통신 커넥터 1	EtherNet/IP 포트 1용 커넥터입니다. 커넥터는 M12 커넥터(D코딩, 암형, Smartclick 지원)입니다. 통신 케이블을 접속하십시오.
(B)	EtherNet/IP 통신 커넥터 2	EtherNet/IP 포트 2용 커넥터입니다. 커넥터는 M12 커넥터(D코딩, 암형, Smartclick 지원)입니다. 통신 케이블을 접속하십시오.
(C)	I/O 커넥터 (세이프티 입력 포트용)	이 커넥터는 세이프티 입력 기기를 접속하기 위한 것입니다. 분리 가능한 마커를 I/O 커넥터 측면에 붙이십시오. 커넥터는 M12 커넥터(A코딩, 암형, 5핀, Smartclick 지원)입니다. I/O 케이블(5선식)을 접속하십시오.
(D)	I/O 커넥터 (세이프티 I/O 포트용)	이 커넥터는 세이프티 입력 기기 및 세이프티 출력 기기를 접속하기 위한 것입니다. 분리 가능한 마커를 I/O 커넥터 측면에 붙이십시오. 커넥터는 M12 커넥터(A코딩, 암형, 8핀, Smartclick 지원)입니다. I/O 케이블(8선식)을 접속하십시오.
(E)	전원 공급 커넥터 (입력)	이 커넥터는 유닛/입력 전원과 출력 전원을 공급하기 위한 것입니다. 커넥터는 M12 커넥터(L코딩, 수형, Smartclick 지원)입니다. 외부 전원에 접속하기 위한 전원 공급 케이블을 접속하십시오.
(F)	전원 공급 커넥터 (출력)	이 커넥터는 로컬 노드에서 다른 노드로 유닛/입력 전원과 출력 전원을 공급하기 위한 것입니다. 전원 공급 방식이 스루 배선 전원 공급인 경우 이 커넥터를 사용하십시오. 커넥터는 M12 커넥터(L코딩, 암형, Smartclick 지원)입니다.
(G)	I/O 표시등	이 표시등은 각 포트 단자의 세이프티 입력 또는 세이프티 출력 상태를 나타냅니다.
(H)	커버 장착 구멍	이 나사 구멍은 로터리 스위치 커버를 장착하기 위한 것입니다. 이 구멍은 두 곳에 마련되어 있습니다. 위 그림은 커버를 나사로 장착한 상태의 구멍을 나타냅니다.
(I)	로터리 스위치	이 스위치는 세이프티 애플리케이션을 선택하고 IP 주소를 설정하기 위한 것입니다.
(J)	상태 표시등	이 표시등은 세이프티 I/O 블록의 현재 동작 상태를 나타냅니다.
(K)	유닛 장착 구멍	이 구멍은 유닛을 장착하기 위한 것입니다. 이 구멍은 두 곳에 마련되어 있습니다. M5 나사로 유닛을 장착하십시오.
(L)	유닛 식별 표시등	이 표시등은 유닛 식별 기능을 사용할 때 점등하여 알려줍니다.
(M)	유닛 식별 마커	이 마커는 세이프티 I/O 블록을 식별하기 위한 것입니다. 흰색입니다.
(N)	I/O 식별 마커	이 마커는 I/O 단자를 식별하기 위한 것입니다. 흰색입니다.

AI 번역본
-For Reference Only-

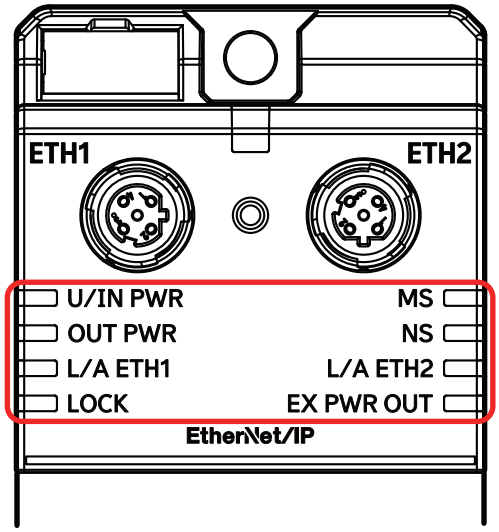
3-2 표시등

세이프티 I/O 블록에는 다음과 같은 표시등이 있습니다. 이 절에서는 이를 설명합니다.

- 상태 표시등
- I/O 표시등
- 유닛 식별 표시등

3-2-1 상태 표시등

이 표시등은 세이프티 I/O 블록의 현재 동작 상태를 나타냅니다.



U/IN PWR 표시등

이 표시등은 유닛/입력 전원의 상태를 나타냅니다.

색상	상태		설명
녹색		점등	유닛/입력 전원이 공급되고 있습니다.
–		소등	유닛/입력 전원이 공급되고 있지 않습니다.

AI 번역본
-For Reference Only-

OUT PWR 표시등

이 표시등은 출력 전원의 상태를 나타냅니다.

색상	상태		설명
녹색		점등	출력 전원이 공급되고 있습니다.
–		소등	출력 전원이 공급되고 있지 않습니다.

MS 표시등

이것은 모듈 상태 표시등입니다. 유닛의 동작 상태를 나타냅니다.

색상	상태		설명
녹색		점등	정상 동작 상태(Executing)
		점멸	정상 동작 대기 상태(Idle)
적색		점등	중대 에러 발생(Critical Fault)
		점멸	동작 정지 에러(Abort) *1
녹색/적색		점멸	초기화 중(Self-Testing), TUNID 설정 대기 상태(Waiting for TUNID), 또는 컨피그레이션 대기 상태(Configuring)
–		소등	IP 주소 표시 기능 실행 중(IP Address Display), I/O 배선 점검 기능 실행 중(I/O Wiring Checking), 또는 전원 OFF

***1.** 에러에 대한 자세한 내용은 11-6페이지의 11-2 에러 확인 및 이벤트를 이용한 문제 해결을 참조하십시오.

NS 표시등

이것은 네트워크 상태 표시등입니다. 세이프티 I/O 블록의 통신 상태를 나타냅니다.

색상	상태		설명
녹색		점등	CIP Safety, EtherNet/IP, CIP 메시지 통신 중 하나에 대해 커넥션이 확립되었습니다.
		점멸	CIP Safety, EtherNet/IP, CIP 메시지 통신 중 어느 것에 대해서도 커넥션이 확립되지 않았습니다.
적색		점등	네트워크에 영향을 미치는 중대한 폴트가 발생했습니다. 예: IP 주소가 중복되었습니다.
		점멸	CIP Safety 및 EtherNet/IP 통신의 커넥션 중 하나에서 타임아웃 에러가 발생했습니다.*1
–		소등	IP 주소가 설정되지 않았거나 전원이 OFF입니다.

***1.** 에러에 대한 자세한 내용은 11-6페이지의 11-2 에러 확인 및 이벤트를 이용한 문제 해결을 참조하십시오.

AI 번역본
-For Reference Only-

L/A ETH1 표시등

이것은 EtherNet/IP 포트 1의 Link/Activity 표시등입니다. EtherNet/IP 포트 1의 링크 상태와 통신 상태를 나타냅니다.

색상	상태		설명
녹색		점등	링크 확립됨
		점멸	링크가 확립되고 통신이 활성 상태임
–		소등	링크가 확립되지 않음

L/A ETH2 표시등

EtherNet/IP 포트 2의 Link/Activity 표시등입니다. 이 표시등은 EtherNet/IP 포트 2의 링크 상태와 통신 상태를 나타냅니다.

색상	상태		설명
녹색		점등	링크 확립됨
		점멸	링크가 확립되고 통신이 활성 상태임
–		소등	링크가 확립되지 않음

LOCK 표시등

이 표시등은 세이프티 I/O 블록의 설정 데이터에 대한 사용자 인증 상태를 나타냅니다. 애플리케이션 동작 확인 후에는 컨피그레이션을 잠금 상태로 설정하여 사용할 것을 권장합니다.

색상	상태		설명
황색		점등	컨피그레이션 잠금됨
		점멸	컨피그레이션이 잠금 해제되어 있으며 잠글 수 있음
–		소등	컨피그레이션이 잠금 해제되어 있으며 잠글 수 없음

AI 번역본
For Reference Only-

EX PWR OUT 표시등

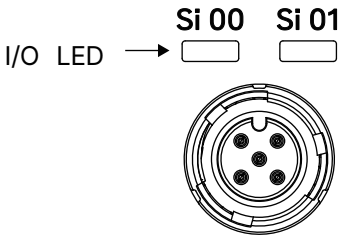
이 표시등은 스루 배선의 출력 전원 상태를 나타냅니다.

색상	상태		설명
녹색		점등	스루 배선의 출력 전원이 공급되고 있습니다.
–		소등	스루 배선의 출력 전원이 공급되고 있지 않습니다.

3-2-2 I/O 표시등

I/O 표시등은 세이프티 입력 단자와 세이프티 출력 단자의 상태를 나타냅니다.

예: 세이프티 입력 표시등



세이프티 입력 표시등

이 표시등은 세이프티 입력 단자의 상태를 나타냅니다.

색상	상태		설명
황색		점등	세이프티 입력 단자가 ON입니다(정상 동작 중).
적색		점등	다음 에러 중 하나가 검출되었습니다. ・세이프티 입력에서의 외부 테스트 신호 실패(External Test Signal Failure at Safety Input) ・세이프티 입력에서의 내부 회로 에러(Internal Circuit Error at Safety Input) ・세이프티 입력에서의 불일치 에러(Discrepancy Error at Safety Input)
		점멸	・듀얼 채널의 다른 쪽 채널의 세이프티 입력 단자에서 에러가 발생했습니다.
–		소등	세이프티 입력 단자가 OFF입니다(정상 동작 중).

세이프티 출력 표시등

이 표시등은 세이프티 출력 단자의 상태를 나타냅니다.

AI 번역본
-For Reference Only-

색상	상태		설명
황색		점등	세이프티 출력 단자가 ON입니다(정상 동작 중)
적색		점등	다음 에러 중 하나가 검출되었습니다. ・세이프티 출력에서의 단락 검출(Short Circuit Detected at Safety Output) ・세이프티 출력에서의 High 고착 검출(Stuck-at-high Detected at Safety Output) ・세이프티 출력에서의 내부 회로 에러(Internal Circuit Error at Safety Output) ・듀얼 채널 출력 간 데이터 에러(Data error between dual channel outputs)*1 ・EDM 에러(EDM error)*1
		점멸	・관련된 다른 세이프티 출력 단자에서 에러가 발생했습니다.

색상	상태		설명
–	□	소등	세이프티 출력 단자가 OFF입니다(정상 동작 중)

***1.** 세이프티 출력 단자가 Dual Channel Mode로 설정되어 있는 경우, EDM 에러 또는 듀얼 채널 출력 간 데이터 에러가 발생하면 양쪽 채널의 세이프티 출력 표시등이 적색으로 점등합니다. Single Channel Mode로 설정되어 있는 경우에는 EDM 에러 시 해당 채널의 세이프티 출력 표시등만 적색으로 점등합니다.

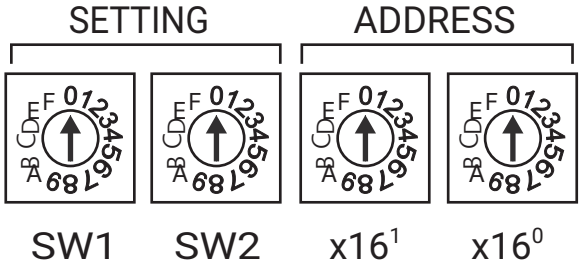
3-2-3 유닛 식별 표시등

이것은 유닛 식별 기능과 펌웨어 업데이트 기능에서 사용됩니다.
자세한 내용은 8-16페이지의 8-8 유닛 식별 기능 및 8-35페이지의 8-14 펌웨어 업데이트 기능을 참조하십시오.

AI 번역본
-For Reference Only-

3-3 로터리 스위치

로터리 스위치로 애플리케이션 설정 및 IP 주소 설정을 구성하십시오.



개요는 다음과 같습니다.

로터리 스위치명	설명
SETTING*1	세이프티 애플리케이션*2, IP 주소 표시 기능*3, I/O 배선 점검 기능*4 중에서 선택합니다. SW1과 SW2를 모두 아래 값으로 설정하십시오. · 0: 리모트 I/O 모드로 동작합니다. · 1~3: 고정 애플리케이션으로 동작합니다. · 4~7: 예약됨 · 8: IP 주소 표시 기능으로 동작합니다. · 9~D: 애드온 애플리케이션으로 동작합니다. · E: I/O 배선 점검 기능으로 동작합니다. · F: 사용자 정의 애플리케이션으로 동작합니다.
ADDRESS*1	스위치 한 쌍이 16진수 두 자리를 나타냅니다. 설정 범위는 00~FF hex이며, 초기값은 00 hex입니다. IP 주소 설정 방법에 대한 자세한 내용은 7-73페이지의 7-10-2 로터리 스위치를 이용한 IP 주소 설정 방법 선택을 참조하십시오.

***1.** 로터리 스위치로 구성한 설정을 반영하려면 전원을 재투입하거나 재시작해야 합니다. 세이프티

***2.** 애플리케이션에 대한 자세한 내용은 6-23페이지의 6-7 세이프티 애플리케이션을 참조하십시오.

***3.** IP 주소 표시 기능에 대한 자세한 내용은 8-19페이지의 8-9 IP 주소 표시 기능을 참조하십시오.

***4.** I/O 배선 점검 기능에 대한 자세한 내용은 8-13페이지의 8-6 I/O 배선 점검 기능을 참조하십시오.

AI 번역본
-For Reference Only-

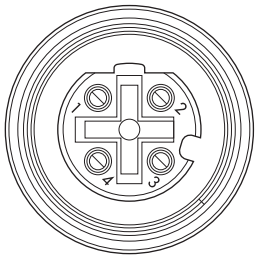
3-4 커넥터

세이프티 I/O 블록에는 다음과 같은 커넥터가 있습니다.

- EtherNet/IP 통신 커넥터
- 전원 공급 커넥터
- I/O 커넥터

3-4-1 EtherNet/IP 통신 커넥터

EtherNet/IP 통신 커넥터는 EtherNet/IP 통신에 사용됩니다. 이 매뉴얼에서는 이를 "통신 커넥터"라고 표기하는 경우도 있습니다.



전기적 특성, 커넥터 구조, 핀 배열은 다음과 같습니다.

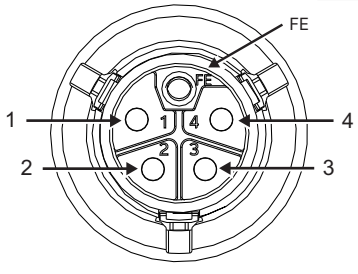
- 전기 사양
  IEEE 802.3 표준을 준수합니다.
- 커넥터 구조
  M12 커넥터(D코딩, 암형, 실드) × 2
- 핀 배열

핀 번호	신호명	설명
1	TD+	송신 데이터 +
2	RD+	수신 데이터 +
3	TD-	송신 데이터 -
4	RD-	수신 데이터 -

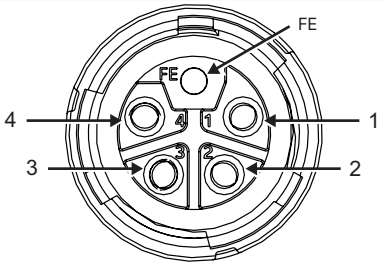
AI 번역본
-For Reference Only-

3-4-2 전원 공급 커넥터

이 커넥터는 세이프티 I/O 블록에 전원을 공급하기 위한 것입니다.



전원 공급 커넥터(입력)
(PWR IN)



전원 공급 커넥터(출력)
(PWR OUT)

● 전원 공급 커넥터(입력)

이 커넥터는 유닛/입력 전원과 출력 전원을 공급하기 위한 것입니다. 외부 전원의 전원 공급 케이블을 접속하십시오.

● 전원 공급 커넥터(출력)

이것은 로컬 노드에서 다른 노드로 출력 전원을 공급하기 위한 커넥터입니다. 스루 배선으로 전원을 공유할 때 사용하십시오.

● 커넥터 구조 및 핀 배열

커넥터 구조와 핀 배열은 다음과 같습니다.

a. 커넥터 구조

전원 공급 커넥터(입력): M12 커넥터(L코딩, 수형, Smartclick 지원)

전원 공급 커넥터(출력): M12 커넥터(L코딩, 암형, Smartclick 지원)

b. 핀 배열

전원 공급 커넥터(입력)와 전원 공급 커넥터(출력)에 공통입니다.

핀 번호	신호명	설명
1	U/IN P+	유닛/입력 전원 +
2	OUT P-	출력 전원 -
3	U/IN P-	유닛/입력 전원 -
4	OUT P+	출력 전원 +
FE (Functional Earth)	FG	프레임 접지

안전 사용을 위한 주의사항

최대 전원 공급 전류는 유닛/입력 전원 전류와 출력 전원 전류의 합계인 9 A입니다. 최대 전원 공급 전류를 초과하여 유닛을 사용하지 마십시오. 초과하면 전원 공급 케이블에 과전류가 흘러 화재가 발생할 수 있습니다.

사용상의 주의

유닛/입력 전원과 출력 전원에는 반드시 별도의 전원을 사용하십시오. 동일한 전원에서 전원을 공급하면 출력 기기의 부하 변동으로 인해 오동작이 발생할 수 있습니다.

사본 보관
For Reference Only

3-4-3 I/O 커넥터

이 커넥터는 세이프티 입력 기기 및 세이프티 출력 기기를 접속하는 데 사용됩니다. I/O 커넥터는 접속되는 기기에 따라 다음과 같이 분류됩니다.
또한 이 매뉴얼에서는 각 커넥터 단위를 "포트"라고 합니다.

- 세이프티 입력 포트
- 세이프티 출력 포트
- 세이프티 I/O 포트

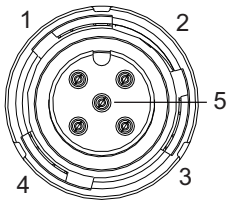
세이프티 입력 포트

세이프티 입력 단자와 테스트 출력 단자가 있는 I/O 커넥터를 세이프티 입력 포트라고 합니다. 세이프티 입력 포트의 개수와 위치는 모델에 따라 다릅니다.

· NXR-SXD1204-CST: 포트 P1~P6

· NXR-SXD1204B-CST: 포트 P1~P4

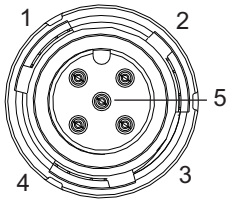
다음은 세이프티 입력 포트의 핀 배열을 나타냅니다.



핀 번호	신호명	설명	포트					
			P1	P2	P3	P4	P5	P6
1	T (n)	테스트 출력 단자 (n)	T00	T02	T04	T06	T08	T10
2	Si (n)	세이프티 입력 단자 (n)	Si00	Si02	Si04	Si06	Si08	Si10
3	U/IN P-	유닛/입력 전원 -	GND					
4	Si (n+1)	세이프티 입력 단자 (n+1)	Si01	Si03	Si05	Si07	Si09	Si11
5	T (n+1)	테스트 출력 단자 (n+1)	T01	T03	T05	T07	T09	T11

세이프티 출력 포트

세이프티 출력 단자가 있는 I/O 커넥터를 세이프티 출력 포트라고 합니다. 세이프티 출력 포트는 NXR-SXD1204-CST에만 있습니다.
세이프티 출력 포트는 포트 P7~P8입니다.
다음은 세이프티 출력 포트의 핀 배열을 나타냅니다.



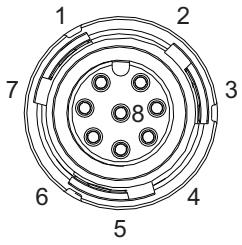
샘플 번역본
-For Reference Only-

핀 번호	신호명	설명	포트	
			P7	P8
1	NC	NC	NC	
2	So (n)	세이프티 출력 단자 (n)	So00	So02
3	OUT P-	출력 전원 -	OUT GND	
4	So (n+1)	세이프티 출력 단자 (n+1)	So01	So03
5	OUT P-	출력 전원 -	OUT GND	

세이프티 I/O 포트

세이프티 입력 단자와 세이프티 출력 단자가 있는 I/O 커넥터를 세이프티 I/O 포트라고 합니다. 세이프티 I/O 포트는 NXR-SXD1204B-CST에만 있습니다.
세이프티 I/O 포트는 포트 P5~P6입니다.

다음은 세이프티 I/O 포트의 핀 배열을 나타냅니다.



핀 번호	신호명	설명	포트	
			P5	P6
1	T (n)	테스트 출력 단자 (n)	T08	T10
2	Si (n)	세이프티 입력 단자 (n)	Si08	Si10
3	U/IN P-	유닛/입력 전원 -	GND	
4	Si (n+1)	세이프티 입력 단자 (n+1)	Si09	Si11
5	T (n+1)	테스트 출력 단자 (n+1)	T09	T11
6	So (n)	세이프티 출력 단자 (n)	So00	So02
7	So (n+1)	세이프티 출력 단자 (n+1)	So01	So03
8	OUT P-	출력 전원 -	OUT GND	

AI 번역본
-For Reference Only-

4

전원 공급 시스템 설계

이 장에서는 세이프티 I/O 블록의 전원 공급 시스템을 설계하는 방법을 설명합니다.

4-1 전원 공급 종류와 전원 공급 시스템 4-2
4-1-1 전원 공급 종류와 용도 4-2
4-1-2 전원 공급 시스템 4-2
4-2 전원 공급 시스템 설계 4-6
4-2-1 전원 공급 시스템 설계 절차 4-6
4-2-2 다이렉트 전원 공급 방식 설계 방법 4-6
4-2-3 스루 배선 방식 시스템 설계 방법 4-13
4-3 전원 공급 장치 및 보호 장치 선택 4-21
4-3-1 외부 전원 공급 장치 선택 4-21
4-3-2 보호 장치 선택 4-21

AI 번역본
-For Reference Only-

4-1 전원 공급 종류와 전원 공급 시스템

이 절에서는 세이프티 I/O 블록의 전원 공급 종류와 용도, 그리고 전원 공급 시스템에 대해 설명합니다.

4-1-1 전원 공급 종류와 용도

이 절에서는 세이프티 I/O 블록의 전원 공급 종류와 용도를 설명합니다.

전원 공급 종류

세이프티 I/O 블록에 전원을 공급하는 전원에는 다음 두 가지 종류가 있습니다.

- 유닛/입력 전원
- 출력 전원

전원 공급 용도

전원의 용도는 다음과 같습니다.

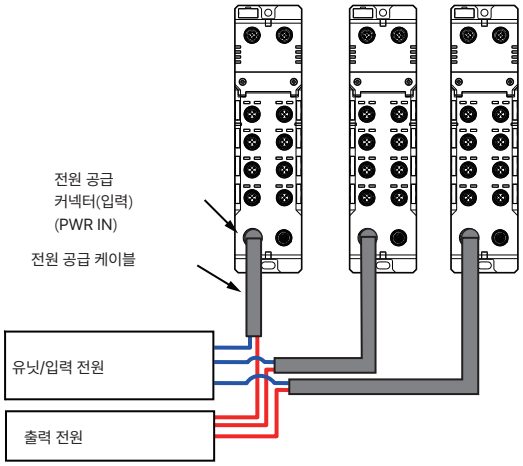
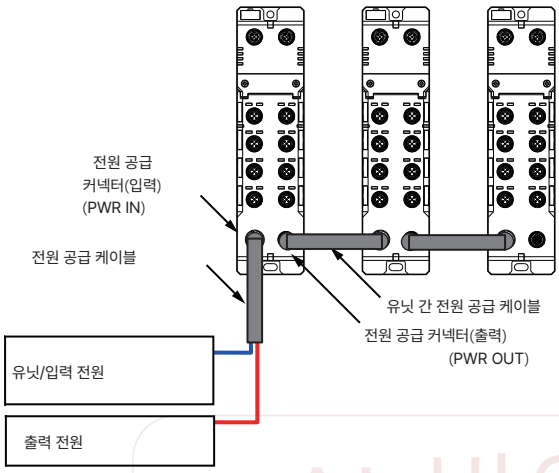
종류	용도
유닛/입력 전원	세이프티 I/O 블록의 동작과 세이프티 입력 기기와의 인터페이스에 사용되는 전원입니다. 자세한 내용은 다음과 같습니다. · 세이프티 I/O 블록 내부 회로, 세이프티 입력 회로, 테스트 출력 회로의 동작 · 기계 접점이 있는 세이프티 입력 기기로의 테스트 펄스 출력 · 반도체 출력이 있는 세이프티 입력 기기로의 전원 공급
출력 전원	세이프티 출력 기기와의 인터페이스에 사용되는 전원입니다. 자세한 내용은 다음과 같습니다. · 세이프티 I/O 블록 출력 회로의 동작 · PNP 출력을 접속할 수 있는 세이프티 출력 기기로의 부하 전류

두 전원 모두 전압 및 전류 모니터링 기능이 있으며, 과전압 및 과전류로부터 보호됩니다.

AI 번역본

4-1-2 전원 공급 시스템

세이프티 I/O 블록에 전원을 공급하는 방법에는 다음 두 가지가 있습니다.

방식	설명	특징
직접 전원 공급	각 세이프티 I/O 블록의 PWR IN 전원 공급 커넥터에 외부 전원을 접속합니다. *1 	이 방식은 스루 배선 케이블에서 전압 강하가 발생하지 않습니다.
통과 배선 전원 공급 *2	한 세이프티 I/O 블록의 PWR IN 전원 공급 커넥터에 외부 전원을 접속합니다. 그런 다음 그 유닛의 PWR OUT 전원 공급 커넥터를 다른 세이프티 I/O 블록의 PWR IN 전원 공급 커넥터에 전원 공급 케이블로 접속합니다. 이렇게 하여 후속 유닛 간에는 전원 공급 케이블로 스루 배선하여 전원을 공급합니다. *1 	스루 배선을 이용하면 시스템에서 사용하는 전원 공급 케이블의 전체 길이를 줄일 수 있습니다. 이 전원 배선 방식을 사용하는 경우 스루 배선 출력에 대해 전원 OFF 기능을 사용할 수 있습니다. 자세한 내용은 8-11페이지의 8-5 스루 배선 출력용 전원 OFF 기능을 참조하십시오.

AI 번역본
-For Reference Only-

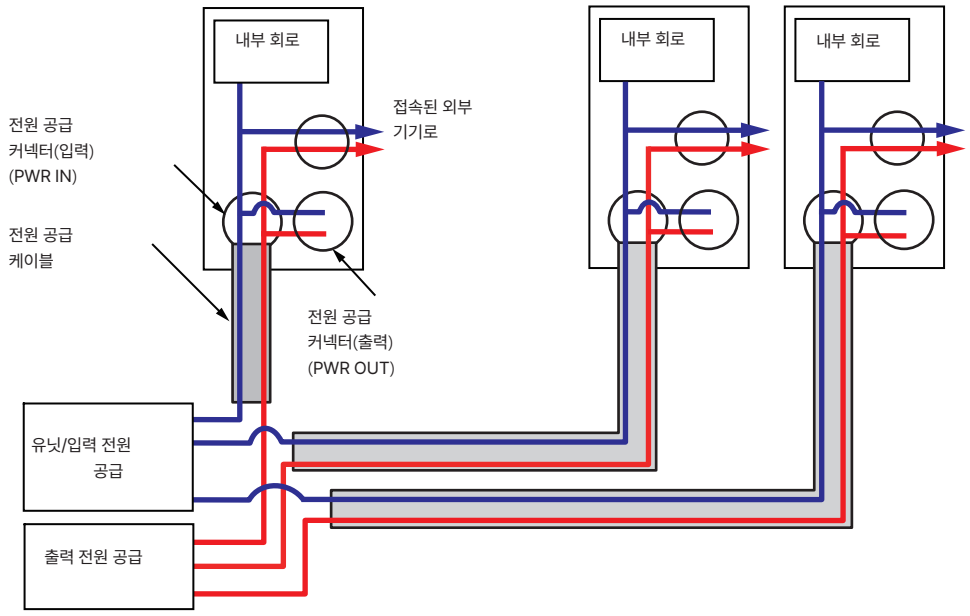
***1.** 오므론 내환경 IP67 전원 공급 장치(S8NR-S 시리즈)를 사용하는 경우, 유닛/입력 전원의 GND와 출력 전원의 GND가 전원 공급 장치 내부에서 연결됩니다. 따라서 세이프티 I/O 블록 내에서의 절연은 보장되지 않습니다. 절연이 필요한 경우 유닛/입력 전원과 출력 전원을 분리하십시오.

***2.** 출력 전원은 세이프티 I/O 블록에 유닛/입력 전원이 공급되고 있을 때만 PWR OUT에서 공급됩니다. 유닛/입력 전원이 OFF이거나 과전압 등의 이유로 유닛/입력 전원이 차단된 경우, PWR OUT의 출력 전원도 함께 차단됩니다.

시스템 구성에 대한 자세한 내용은 다음과 같습니다.

● 다이렉트 전원 공급 방식 시스템 구성

예는 다음과 같습니다. 각 세이프티 I/O 블록의 PWR IN 전원 공급 커넥터에 외부 전원을 접속하십시오.

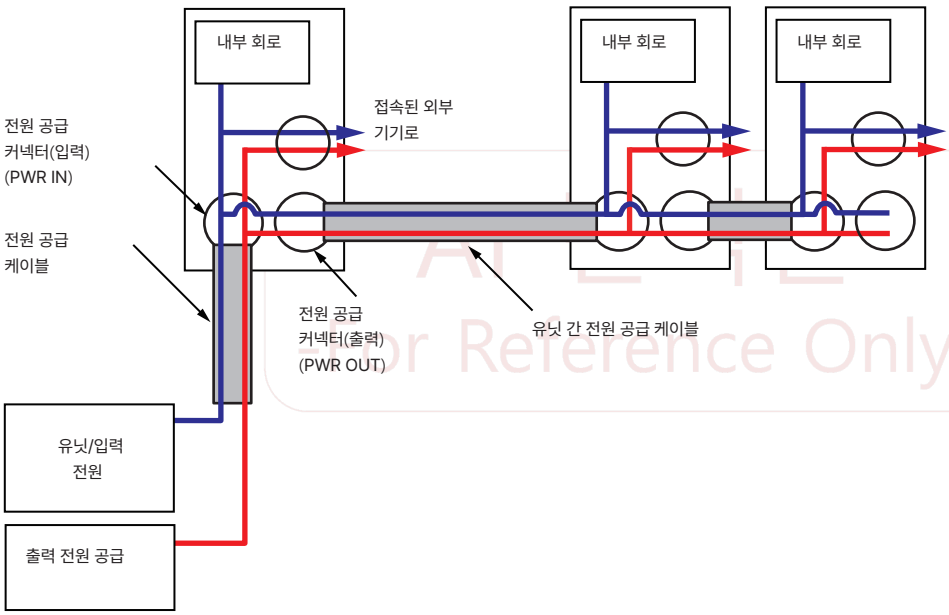


사용상의 주의

· 유닛/입력 전원과 출력 전원에는 반드시 별도의 전원을 사용하십시오. 동일한 전원에서 전원을 공급하면 출력 기기의 부하 변동으로 인해 오동작이 발생할 수 있습니다.

● 스루 배선 방식 시스템 구성

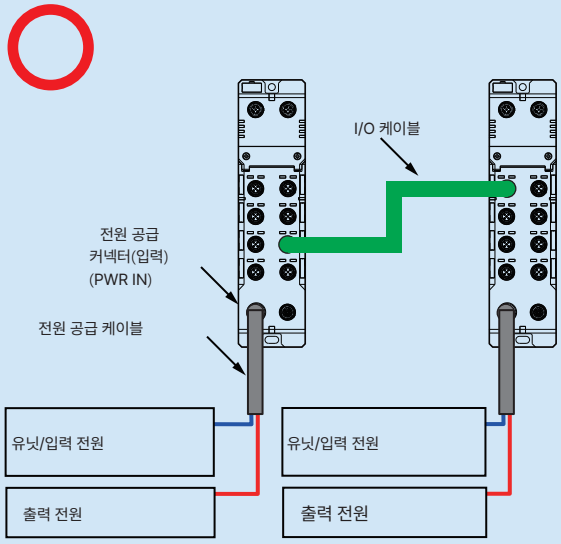
첫 번째 세이프티 I/O 블록의 PWR IN 전원 공급 커넥터에 외부 전원을 접속합니다. 그런 다음 그 유닛의 PWR OUT 전원 공급 커넥터를 다른 세이프티 I/O 블록의 PWR IN 전원 공급 커넥터에 전원 공급 케이블로 접속합니다. 이렇게 하여 후속 유닛 간에도 차례로 스루 배선으로 전원 공급 케이블을 접속합니다.

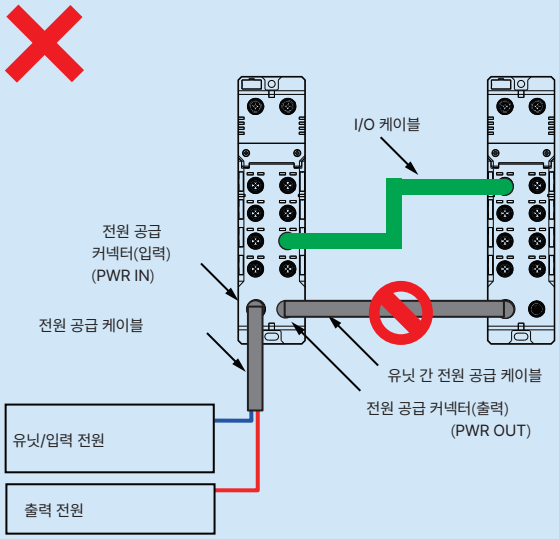


-Sample
-For Reference Only-

사용상의 주의

- 유닛/입력 전원과 출력 전원에는 반드시 별도의 전원을 사용하십시오. 동일한 전원에서 전원을 공급하면 출력 기기의 부하 변동으로 인해 오동작이 발생할 수 있습니다.
- 유닛 간 세이프티 I/O 포트를 접속하는 경우, 스루 배선으로 전원을 공급하지 마십시오. 전원 간의 GND가 I/O 케이블을 통해 연결되므로 절연되지 않습니다.





-For Reference Only-

4-2 전원 공급 시스템 설계

이 절에서는 세이프티 I/O 블록의 전원 공급 시스템 설계 방법을 설명합니다.

⚠ 경고

전원 공급 설계와 배선을 올바르게 수행하려면 이 매뉴얼의 지시 사항을 따르십시오. 규정된 범위를 벗어나는 전압이나 전류를 입력하거나 잘못 배선하면 고장이나 화재의 원인이 될 수 있습니다.

4-2-1 전원 공급 시스템 설계 절차

세이프티 I/O 블록의 전원 공급 시스템 설계에 대한 전체 절차는 다음과 같습니다.

단계	설명	참조
1. 전원 공급 방식 결정	전원 공급 방식을 결정합니다. 전원 공급 방식에는 다음 두 가지가 있습니다. ・다이렉트 전원 공급 방식 ・스루 배선 방식	4-2페이지의 4-1-2 전원 공급 시스템
↓		
2. 전원 공급 시스템 설계	전원 공급 방식에 따라 다음 설계 작업을 수행한 후 설계 조건을 충족하는지 확인합니다. ・유닛/입력 전원 설계 ・출력 전원 설계	・다이렉트 전원 공급 방식의 경우 4-6페이지의 4-2-2 직접 전원 공급 설계 방법 ・스루 배선 전원 공급의 경우 4-13페이지의 4-2-3 통과 배선 전원 공급 시스템 설계 방법
↓		
3. 외부 전원 공급 장치 및 보호 장치 선택	단계 2에서 계산한 전류 소비량을 바탕으로 전원 공급 용량을 계산하고, 이에 따라 외부 전원 공급 장치를 선택합니다. 또한 외부 회로의 단락 및 과전류로부터 보호하기 위해 보호 장치(차단기, 퓨즈 등)를 선택합니다.	4-21페이지의 4-3 전원 공급 장치 및 보호 장치 선택

참조 번역본 -Reference Only-

4-2-2 다이렉트 전원 공급 방식 설계 방법

이 절에서는 전원 공급 방식이 다이렉트 전원 공급 방식인 경우의 전원 공급 시스템 설계 방법을 설명합니다.

다이렉트 전원 공급 방식 설계 절차

전원이 다음 설계 조건 (a)~(c)를 충족하는지 확인하십시오. 확인 방법은 참조 절을 참조하십시오.

설계 조건	확인 방법 참조
(a) 유닛/입력 전원과 출력 전원의 총 전류 소비량 합계는 세이프티 I/O 블록의 최대 전원 공급 전류를 초과해서는 안 됩니다.*1	4-7페이지의 직접 전원 공급에서의 총 전류 소비량 계산
(b) 세이프티 I/O 블록의 입력 회로 사양과 접속된 외부 기기의 전압 사양은 유닛/입력 전원 전압이 강하해도 충족됩니다.*2	4-11페이지의 직접 전원 공급에서의 전압 강하 계산
(c) 세이프티 I/O 블록의 출력 회로 사양과 접속된 외부 기기의 전압 사양은 출력 전원 전압이 강하해도 충족됩니다.*3	

***1.** 최대 전원 공급 전류는 9 A입니다. 9 A를 초과하지 마십시오.
***2.** 예를 들어 세이프티 I/O 블록의 경우 유닛/입력 전원 전압이 19.2~28.8 VDC인지 확인하십시오. 예를
***3.** 들어 세이프티 I/O 블록의 경우 출력 전원 전압이 19.2~28.8 VDC인지 확인하십시오.

다이렉트 전원 공급 방식에서의 총 전류 소비량 계산

다이렉트 전원 공급 방식은 각 세이프티 I/O 블록에 전원을 공급하는 방식입니다. 따라서 각 전원별로 각 유닛의 총 전류 소비량을 계산합니다. 각 전원의 총 전류 소비량 합계가 세이프티 I/O 블록의 최대 전원 공급 전류보다 작도록 시스템을 설계하십시오.

유닛/입력 전원 및 출력 전원으로부터의 세이프티 I/O 블록 총 전류 소비량 계산 방법은 다음과 같습니다.

● 유닛/입력 전원의 총 전류 소비량

= (유닛/입력 전원의 전류 소비량)
+ (접속된 세이프티 입력 기기가 소비하는 전류) +
(테스트 출력이 소비하는 전류)

수식의 각 항목은 다음과 같습니다.

항목	설명
유닛/입력 전원의 전류 소비량	세이프티 I/O 블록이 소비하는 전류입니다. 2-6페이지의 2-1-4 유닛 사양에 있는 유닛/입력 전원 전류 소비량 값을 사용하십시오.
접속된 세이프티 입력 기기가 소비하는 전류	이 값은 다음 수식으로 계산합니다. (세이프티 입력 기기 전원의 전류 소비량) + (세이프티 입력 전류 × 사용하는 입력 수)
테스트 출력이 소비하는 전류*1	이 값은 다음 수식으로 계산합니다. (테스트 출력 부하 전류 × 사용하는 출력 수)

***1.** 반도체 출력이 있는 기기를 접속하는 경우, 테스트 출력의 출력 전류는 포인트당 0.7 A가 되어야 합니다.

참고용 번역본
-For Reference Only-

● 출력 전원의 총 전류 소비량

= (출력 전원의 전류 소비량)
+ (접속된 세이프티 출력 기기가 소비하는 전류)

수식의 각 항목은 다음과 같습니다.

항목	설명
출력 전원의 전류 소비량	세이프티 I/O 블록이 소비하는 전류입니다. 2-6페이지의 2-1-4 유닛 사양에 있는 출력 전원 전류 소비량 값을 사용하십시오.
접속된 세이프티 출력 기기가 소비하는 전류 *1	이 값은 다음 수식으로 계산합니다. (세이프티 출력 부하 전류 × 사용하는 출력 수)

*1. NXR-SXD1204-CST의 경우 세이프티 출력 최대 부하 전류 2 A/포인트를 초과하지 마십시오. NXR-SXD1204B-CST의 경우 세이프티 출력 최대 부하 전류 0.7 A/포인트를 초과하지 마십시오.

다이렉트 전원 공급 방식에서의 총 전류 소비량 계산 예

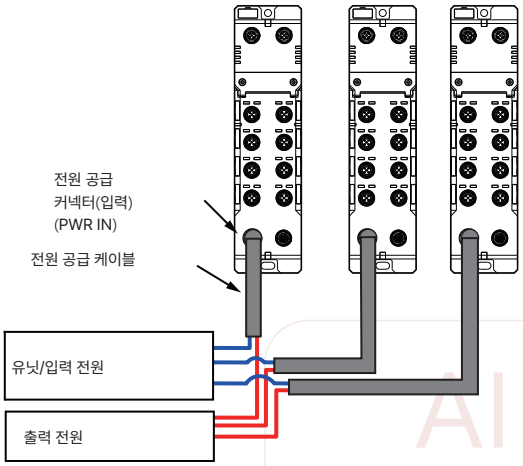
다음은 주어진 구성 및 적용 조건에 대해 유닛/입력 전원과 출력 전원으로부터의 총 전류 소비량을 계산하는 방법을 예로 나타낸 것입니다.

사용상의 주의

이것은 계산 예를 나타낸 것입니다. 고객의 설비와 환경은 각기 다르므로 실제 사용 환경에 맞게 계산을 수행하십시오.

● 구성 예

왼쪽부터 SXD1, SXD2, SXD3의 세 세이프티 I/O 블록이 있다고 가정합니다.



AI 번역본
-For Reference Only-

● 접속 외부 기기의 적용 조건

각 세이프티 I/O 블록에서 다음 조건을 사용한다고 가정합니다. SXD2와 SXD3의 조건은 동일합니다.

세이프티 I/O 블록 조건				접속 외부 기기 조건	
유닛 명칭	세이프티 I/O 포트			제품 명	사양
	포트명	신호명	단자 번호		
SXD1	세이프티 입력 포트 1	세이프티 입력	Si00 /01	세이프티 입력 기기	· 세이프티 입력 기기의 소비 전류: 50mA · 세이프티 입력 전류: 4.5 mA/포인트 · 테스트 출력 부하 전류: 200 mA/포인트
		테스트 출력	T00 /01		
	세이프티 입력 포트 2	세이프티 입력	Si02 /03	세이프티 입력 기기	· 세이프티 입력 기기의 소비 전류: 50mA · 세이프티 입력 전류: 4.5 mA/포인트 · 테스트 출력 부하 전류: 200 mA/포인트
		테스트 출력	T02 /03		
	세이프티 입력 포트 3~6	세이프티 입력	Si04~11	미사용	–
		테스트 출력	T04~11	미사용	–
	세이프티 출력 포트 1	세이프티 출력	So00 /01	세이프티 출력 기기	· 세이프티 출력 기기의 소비 전류: 50mA · 세이프티 출력 부하 전류: 500 mA/포인트
	세이프티 출력 포트 2	세이프티 출력	So02 /03	미사용	–
SXD2 및 SXD3	세이프티 입력 포트 1	세이프티 입력	Si00 /01	세이프티 입력 기기	· 세이프티 입력 기기의 소비 전류: 50mA · 세이프티 입력 전류: 4.5 mA/포인트 · 테스트 출력 부하 전류: 200 mA/포인트
		테스트 출력	T00 /01		
	세이프티 입력 포트 2~6	세이프티 입력	Si02~11	미사용	–
		테스트 출력	T02~11	미사용	–
	세이프티 출력 포트 1	세이프티 출력	So00 /01	세이프티 출력 기기	· 세이프티 출력 기기의 소비 전류: 50mA · 세이프티 출력 부하 전류: 500 mA/포인트
	세이프티 출력 포트 2	세이프티 출력	So02 /03	미사용	–

● 총 소비 전류 계산

각 세이프티 I/O 블록의 유닛/입력 전원 및 출력 전원에서 발생하는 총 소비 전류를 계산하기 위한 항목은 다음과 같습니다.

AI 번역본
-For Reference Only-

유닛 명칭	전원 공급의 종류	합계 계산 항목 소비 전류	계산 결과
SXD1	유닛/입력 전원	유닛/입력 전원으로부터의 소비 전류	세이프티 I/O 블록의 사양에 따라 220 mA.
		연결된 세이프티 입력 기기가 소비하는 전류	세이프티 입력 포트 1, 2를 대상으로 계산합니다. (세이프티 입력 기기의 전원 공급에 따른 소비 전류) + (세이프티 입력 전류 × 사용 입력 수) = (50 mA + 50 mA) + (4.5 mA × 4점) = 118 mA
		테스트 출력이 소비하는 전류	세이프티 입력 포트 1, 2를 대상으로 계산합니다. (테스트 출력 부하 전류 × 사용 출력 수) = 200 mA × 4점 = 800 mA
	출력 전원	출력 전원으로부터의 소비 전류	세이프티 I/O 블록의 사양에 따라 40 mA.
		연결된 세이프티 출력 기기가 소비하는 전류	세이프티 출력 포트 1을 대상으로 계산합니다. (세이프티 출력 부하 전류 × 사용 출력 수) = 500 mA × 2점 = 1000 mA
SXD2 및 SXD3	유닛/입력 전원	유닛/입력 전원으로부터의 소비 전류	세이프티 I/O 블록의 사양에 따라 220 mA.
		연결된 세이프티 입력 기기가 소비하는 전류	세이프티 입력 포트 1을 대상으로 계산합니다. (세이프티 입력 기기의 전원 공급에 따른 소비 전류) + (세이프티 입력 전류 × 사용 입력 수) = 50 mA + (4.5 mA × 2점) = 59 mA
		테스트 출력이 소비하는 전류	세이프티 입력 포트 1을 대상으로 계산합니다. (테스트 출력 부하 전류 × 사용 출력 수) = 200 mA × 2점 = 400 mA
	출력 전원	출력 전원으로부터의 소비 전류	세이프티 I/O 블록의 사양에 따라 40 mA.
		연결된 세이프티 출력 기기가 소비하는 전류	세이프티 출력 포트 1을 대상으로 계산합니다. (세이프티 출력 부하 전류 × 사용 출력 수) = 500 mA × 2점 = 1000 mA

AI 번역본
-For Reference Only-

위 계산 결과로부터 각 세이프티 I/O 블록의 총 소비 전류 합계를 다음과 같이 계산합니다.

a. SXD1의 총 소비 전류 합계

(SXD1의 유닛/입력 전원으로부터의 총 소비 전류) + (SXD1의 출력 전원으로부터의 총 소비 전류)

= (220 mA + 118 mA + 800 mA) + (40 mA + 1000 mA)

= (1138 mA) + (1040 mA)

≈ (1.14 A) + (1.04 A)

= 2.18 A

b. SXD2의 총 소비 전류 합계

(SXD2의 유닛/입력 전원으로부터의 총 소비 전류) + (SXD2의 출력 전원으로부터의 총 소비 전류)
= (220 mA + 59 mA + 400 mA) + (40 mA + 1000 mA)
= (679 mA) + (1040 mA)
≈ (0.68 A) + (1.04 A)
= 1.72 A

c. SXD3의 총 소비 전류 합계
계산식은 SXD2와 동일합니다.
(SXD3의 유닛/입력 전원으로부터의 총 소비 전류) + (SXD3의 출력 전원으로부터의 총 소비 전류)
≈ 1.72A

각 유닛의 총 소비 전류 합계가 세이프티 I/O 블록의 최대 전원 공급 전류인 9 A 미만이므로 이 예는 적합합니다.

다이렉트 전원 공급 방식의 전압 강하 계산

전원 케이블에서는 전압 강하가 발생합니다.
오므론 M12 L코딩 전원 케이블(XS5F-L521-□12-F, XS5W-L521- □12-F)을 사용할 때의 전압 강하는 아래 표와 같습니다.

유닛/입력 전원 또는 출력 전원으로부터의 소비 전류 (A)	전원 케이블 길이별 전압 강하 (V)			
	1 m	3 m	5 m	10 m
9	0.80	2.40	4.00	8.00
8	0.71	2.13	3.56	7.11
6	0.53	1.60	2.67	5.33
4	0.36	1.07	1.78	3.56
3	0.27	0.80	1.33	2.67
2	0.18	0.53	0.89	1.78
1	0.09	0.27	0.44	0.89

유닛/입력 전원 및 출력 전원의 전압이 강하하더라도 세이프티 I/O 블록 및 연결된 외부 기기의 전압 사양을 만족하도록 시스템을 설계하십시오.

AI 번역본

사용상의 주의

이는 계산 예시입니다. 고객의 기기 및 설비는 각기 다르므로 실제 사용 환경에 맞게 계산을 수행하십시오.

● 전압 강하 계산 예

다음 예에서는 아래 조건에서 전압 강하를 계산하는 방법을 설명합니다.

항목	조건
구성 연결된 외부 기기에 대한 적용 조건	다이렉트 전원 공급 방식의 총 소비 전류 계산 예(4-8페이지)에 명시된 조건을 사용합니다. 이 조건에 따라 각 유닛의 전원별 소비 전류는 아래와 같습니다: · SXD1: 2.18 A 유닛/입력 전원으로부터의 소비 전류: 1.14 A 출력 전원으로부터의 소비 전류: 1.04 A · SXD2: 1.72 A 유닛/입력 전원으로부터의 소비 전류: 0.68 A 출력 전원으로부터의 소비 전류: 1.04 A · SXD3: 1.72 A 유닛/입력 전원으로부터의 소비 전류: 0.68 A 출력 전원으로부터의 소비 전류: 1.04 A
전원 케이블 길이	· SXD1에 연결된 전원 케이블: 1 m · SXD2에 연결된 전원 케이블: 3 m · SXD3에 연결된 전원 케이블: 5 m
외부 전원의 전원 공급 단자 전압	· 유닛/입력 전원: 24.0 VDC · 출력 전원: 24.0 VDC

전원 케이블의 전압 강하 표에 따라 각 유닛의 전원별 전압 강하는 다음과 같이 결정됩니다.

유닛 명칭	전압 강하	
	유닛/입력 전원	출력 전원
SXD1	0.18 V (케이블 길이가 1 m이고 소비 전류가 1.14 A이므로 2 A를 사용합니다.)	0.18 V (케이블 길이가 1 m이고 소비 전류가 1.04 A이므로 2 A를 사용합니다.)
SXD2	0.27 V (케이블 길이가 3 m이고 소비 전류가 0.68 A이므로 1 A를 사용합니다.)	0.53 V (케이블 길이가 3 m이고 소비 전류가 1.04 A이므로 2 A를 사용합니다.)
SXD3	0.44 V (케이블 길이가 5 m이고 소비 전류가 0.68 A이므로 1 A를 사용합니다.)	0.89 V (케이블 길이가 5 m이고 소비 전류가 1.04 A이므로 2 A를 사용합니다.)

위 결과로부터 각 유닛에 대한 입력 전원별 전압은 다음과 같이 계산됩니다.

AI 번역본
-For Reference Only-

a. SXD1에 대한 입력 전원별 전압
유닛/입력 전원의 전압
= 24.0 V - 전원 케이블의 전압 강하
= 24.0 V - 0.18 V
= 23.82 V
출력 전원의 전압
= 24.0 V - 전원 케이블의 전압 강하 =
24.0 V - 0.18 V
= 23.89 V

b. SXD2에 대한 입력 전원별 전압 유닛/입력 전원의
전압
= 24.0 V - 전원 케이블의 전압 강하
= 24.0 V - 0.27 V

= 23.73 V
출력 전원의 전압
= 24.0 V - 전원 케이블의 전압 강하 =
24.0 V - 0.53 V
= 23.47 V

c. SXD3에 대한 입력 전원별 전압 유닛/입력
전원의 전압
= 24.0 V - 전원 케이블의 전압 강하 =
24.0 V - 0.44 V
= 23.56 V
출력 전원의 전압
= 24.0 V - 전원 케이블의 전압 강하
= 24.0 V - 0.89 V
= 23.11 V

위 전압 값은 모두 세이프티 I/O 블록의 각 전원 사양(19.2~28.8
VDC)을 만족하므로 적합합니다.
또한 연결된 세이프티 입력 기기 또는 세이프티 출력 기기의 전압 사양도 만족하는지 확인하십시오.
단, 이 예에서는 해당 확인을 생략합니다.
전압 사양을 만족하지 않는 경우에는 전원 케이블의 길이 및 연결된 외부 기기를
재검토하십시오.

4-2-3 스루 배선 방식 전원 시스템의 설계 방법

이 절에서는 전원 공급 방식이 스루 배선 방식인 경우의 전원 시스템 설계 방법에 대해 설명합니다.

스루 배선 방식 전원 시스템의 설계 절차

전원이 다음 설계 조건 (a)~(c)를 만족하는지 확인하십시오. 확인 방법은 참조 절을
참고하십시오.

설계 조건	확인 방법 참조
(a) 유닛/입력 전원 및 출력 전원으로부터의 총 소비 전류 합계는 세이프티 I/O 블록의 최대 전원 공급 전류를 초과해서는 안 됩니다.*1	스루 배선 방식의 총 소비 전류 계산 (4-14페이지)
(b) 세이프티 I/O 블록의 입력 회로 사양 및 연결된 외부 기기의 전압 사양은 유닛/입력 전원 전압이 강하하더라도 만족됩니다.*2	스루 배선 방식의 전압 강하 계산 (4-17페이지)
(c) 세이프티 I/O 블록의 출력 회로 사양 및 연결된 외부 기기의 전압 사양은 출력 전원 전압이 강하하더라도 만족됩니다.*3	

-For Reference Only-

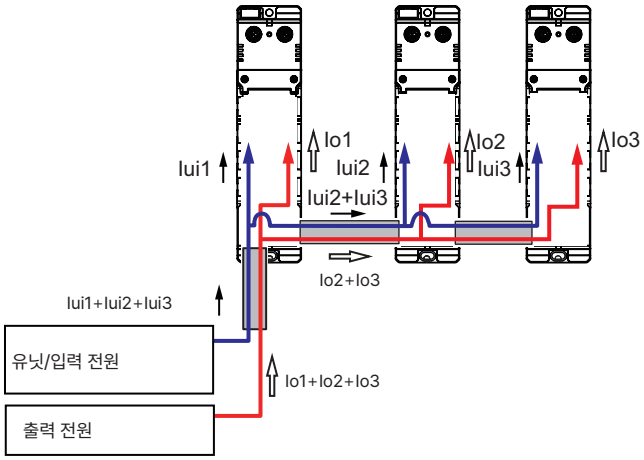
***1.** 최대 전원 공급 전류는 9 A입니다. 9 A를 초과하지 마십시오.
***2.** 예를 들어 세이프티 I/O 블록의 경우, 유닛/입력 전원 전압이 19.2~28.8 VDC인지 확인하십시오. 예를
***3.** 들어 세이프티 I/O 블록의 경우, 출력 전원 전압이 19.2~28.8 VDC인지 확인하십시오.

스루 배선 방식 전원 공급에서의 총 소비 전류 계산

전원 공급 방식이 스루 배선 방식인 경우에는 다이렉트 전원 공급 방식과 달리, 전원이 공급되는 다른 세이프티 I/O 블록이 소비할 전류가 모두 외부 전원에 연결된 세이프티 I/O 블록을 통해 흐릅니다. 즉, 각 유닛의 소비 전류 합계가 세이프티 I/O 블록의 최대 전원 공급 전류보다 작아지도록 시스템을 설계해야 합니다. 다음은

예시입니다. 이 예에서는 다음 식을 만족하는지 확인합니다.
왼쪽부터 SXD1, SXD2, SXD3의 세 개의 세이프티 I/O 블록이 있다고 가정합니다.

(Iui1 + Iui2 + Iui3 + Io1 + Io2 + Io3) < (SXD1의 최대 전원 공급 전류*1)



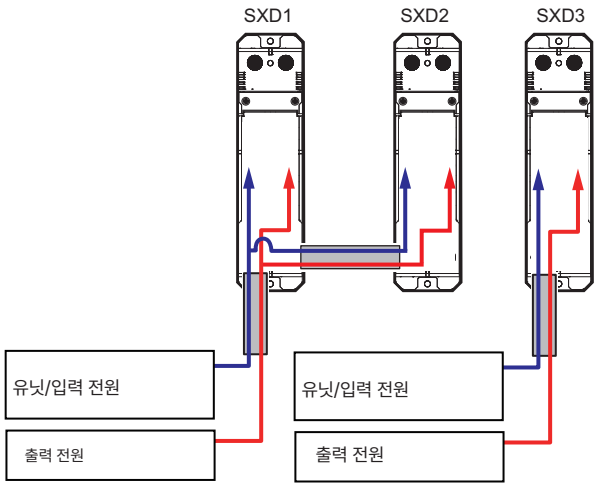
Iui1: SXD1의 유닛/입력 전원으로부터의 총 소비 전류
Iui2: SXD2의 유닛/입력 전원으로부터의 총 소비 전류
Iui3: SXD3의 유닛/입력 전원으로부터의 총 소비 전류
Io1: SXD1의 출력 전원으로부터의 총 소비 전류
Io2: SXD2의 출력 전원으로부터의 총 소비 전류
Io3: SXD3의 출력 전원으로부터의 총 소비 전류

*1. SXD1의 최대 전원 공급 전류를 초과하지 않으면 SXD2 및 SXD3의 전류도 초과하지 않습니다.

유닛/입력 전원 또는 출력 전원으로부터의 각 유닛의 총 소비 전류 계산 방법은 다이렉트 전원 공급 방식과 동일합니다. 다이렉트 전원 공급 방식의 총 소비 전류 계산(4-7페이지)을 참조하십시오.
계산 값이 지정 조건을 만족하지 않는 경우에는 조건을 만족하도록 외부 전원을 추가하십시오.

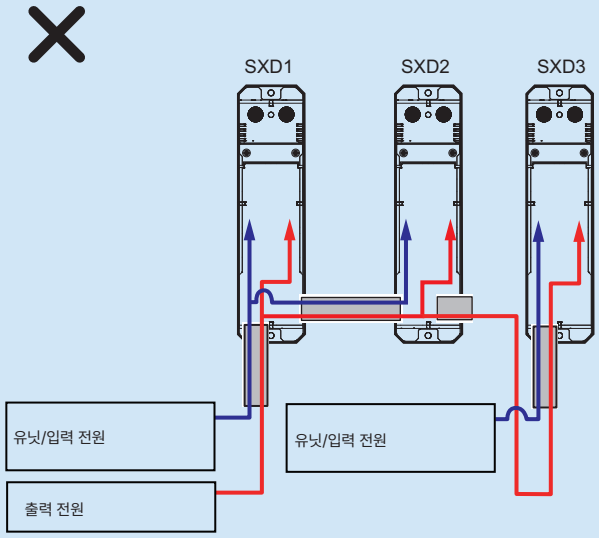
AI 번역본
-For Reference Only-

예: 외부 전원을 추가한 시스템



사용상의 주의

유닛/입력 전원과 출력 전원은 반드시 한 세트로 추가하십시오. 둘 중 하나만 추가할 수는 없습니다.



스루 배선 방식 전원 공급의 총 소비 전류 계산 예

AI 번역본
For Reference Only-

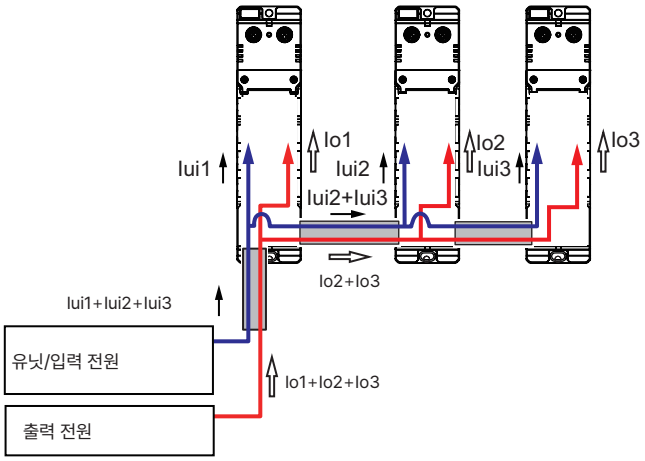
다음은 주어진 구성 및 적용 조건에서 전원 공급 방식이 스루 배선 방식인 경우의 총 소비 전류 계산 방법을 예시로 보여줍니다.

사용상의 주의

이는 계산 예시입니다. 고객의 기기 및 설비는 각기 다르므로 실제 사용 환경에 맞게 계산을 수행하십시오.

● 구성 예

왼쪽부터 SXD1, SXD2, SXD3의 세 개의 세이프티 I/O 블록이 있다고 가정합니다.



● 연결된 외부 기기에 대한 적용 조건

조건은 다이렉트 전원 공급 방식의 총 소비 전류 계산 예(4-8페이지)의 조건과 동일합니다.

● 총 소비 전류 계산

다이렉트 전원 공급 방식의 총 소비 전류 계산 예(4-8페이지)에 따라 각 유닛의 총 소비 전류는 다음과 같이 계산됩니다.

1. SXD1의 총 소비 전류 합계

(SXD1의 유닛/입력 전원으로부터의 총 소비 전류) + (SXD1의 출력 전원으로부터의 총 소비 전류)

(Iui1 + Io1)

= (220 mA + 118 mA + 800 mA) + (40 mA + 1000 mA)

= (1138 mA) + (1040 mA)

≈ (1.14 A) + (1.04 A)

= 2.18 A

2. SXD2의 총 소비 전류 합계

(SXD2의 유닛/입력 전원으로부터의 총 소비 전류) + (SXD2의 출력 전원으로부터의 총 소비 전류)

(Iui2 + Io2)

= (220 mA + 59 mA + 400 mA) + (40 mA + 1000 mA)

= (679 mA) + (1040 mA)

≈ (0.68 A) + (1.04 A)

= 1.72 A

AI 번역본
For Reference Only-

3. SXD3의 총 소비 전류 합계

계산식은 SXD2와 동일합니다.

(SXD3의 유닛/입력 전원으로부터의 총 소비 전류) + (SXD3의 출력 전원으로부터의 총 소비 전류)

(Iui3 + Io3)

≈ 1.72A

외부 전원에서 공급되는 각 유닛의 총 전류 소비량의 합은 다음과 같이 계산됩니다.
(Iui1 + Iui2 + Iui3 + Io1 + Io2 + Io3)
= (2.18 A + 1.72 A + 1.72 A)
= 5.62 A

이 계산 결과는 세이프티 I/O 블록의 전원 최대 전류인 9 A 이하이므로 허용됩니다.

전원 통과 배선 방식에서의 전압 강하 계산

전원 공급 방식이 통과 배선 방식인 경우, 다음과 같은 요인으로 인해 전압 강하가 발생합니다.
・세이프티 I/O 블록의 내부 회로
・전원 케이블

전원 공급 방식이 통과 배선 방식인 경우, 다른 유닛에서 소비되는 전류가 세이프티 I/O 블록을 통해 흐르며, 이로 인해 유닛 내부 회로에서 전압 강하가 발생합니다.
When using OMRON M12 L-coding power supply cables (XS5F-L521-□12-F, XS5W-L521-□12-F), the voltage
출력 전원의 전류 소비량에 따라 세이프티 I/O 블록 및 전원 케이블의 내부 회로에서 발생하는 전압 강하는 아래 표와 같습니다.

유닛/입력 전원으로부터의 전류 소비량 (A)	유닛 내부 회로의 전압 강하 (V)	전원 케이블 길이별 전압 강하 (V)			
		1 m	3 m	5 m	10 m
9	0.40	0.80	2.40	4.00	8.00
8	0.36	0.71	2.13	3.56	7.11
6	0.27	0.53	1.60	2.67	5.33
4	0.18	0.36	1.07	1.78	3.56
3	0.13	0.27	0.80	1.33	2.67
2	0.09	0.18	0.53	0.89	1.78
1	0.04	0.09	0.27	0.44	0.89

출력 전원으로부터의 전류 소비량 (A)	유닛 내부 회로의 전압 강하 (V)	전원 케이블 길이별 전압 강하 (V)			
		1 m	3 m	5 m	10 m
9	0.50	0.80	2.40	4.00	8.00
8	0.44	0.71	2.13	3.56	7.11
6	0.33	0.53	1.60	2.67	5.33
4	0.22	0.36	1.07	1.78	3.56
3	0.17	0.27	0.80	1.33	2.67
2	0.11	0.18	0.53	0.89	1.78
1	0.06	0.09	0.27	0.44	0.89

AT 번역본
-For Reference Only-

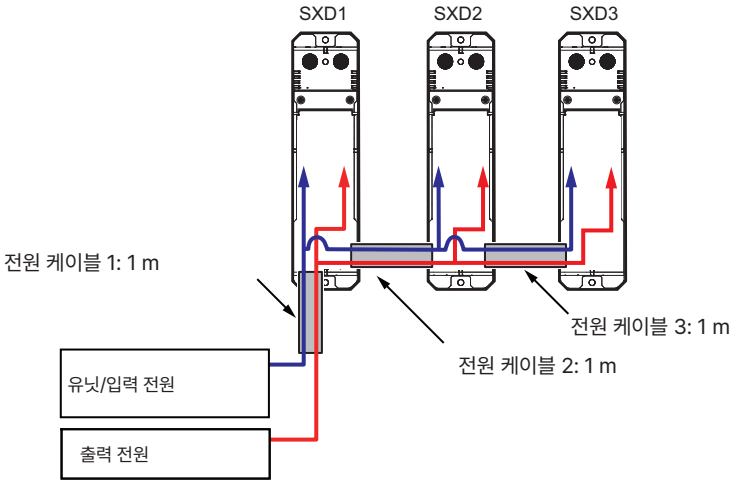
유닛/입력 전원 및 출력 전원의 전압이 저하되더라도 세이프티 I/O 블록 및 연결된 외부 기기의 전압 사양을 만족하도록 시스템을 설계하십시오.

사용상의 주의

이것은 계산 예를 나타낸 것입니다. 고객의 기기 및 설비에 따라 다르므로, 실제 사용 조건에 맞춰 계산을 수행하십시오.

● 전압 강하 계산 예

다음 예에서는 아래 조건에서 전압 강하를 계산하는 방법을 설명합니다.

항목	조건
구성 연결된 외부 기기에 대한 적용 조건	4-15페이지의 통과 배선 방식 전원 공급 시 총 전류 소비량 계산 예에 규정된 조건을 사용하십시오.
전원 공급 케이블 길이	케이블 길이는 다음과 같습니다. 
외부 전원의 전원 공급 단자 전압	· 유닛/입력 전원: 24.0 VDC · 출력 전원: 24.0 VDC

세이프티 I/O 블록의 내부 회로 및 전원 케이블의 전압 강하 표에 따라,
각 전원으로부터 각 유닛의 전압 강하는 다음과 같이 결정됩니다.

유닛 명칭	유닛 내부 회로의 전압 강하	전원 케이블의 전압 강하	비고
SXD1	–	· 전원 케이블 1의 전압 강하: 0.53 V	외부 전원으로부터의 각 유닛의 전류 소비량 합계가 5.62 A이므로, 6 A에서의 전압 강하를 사용하십시오.
SXD2	SXD1 내부 회로의 전압 강하 · 유닛/입력 전원: 0.18 V · 출력 전원: 0.22 V	· 전원 케이블 1의 전압 강하: 0.53 V · 전원 케이블 2의 전압 강하: 0.36 V	전원 케이블 1의 전압 강하에는 SXD1의 값을 사용합니다. 전원 케이블 2 및 SXD1 내부 회로의 전압 강하에는 다음과 같이 계산된 전류값을 사용합니다. (외부 전원으로부터의 각 유닛의 전류 소비량 합계) - (SXD1의 총 전류 소비 량 합계) = 5.62 A - 2.18 A = 3.44 A 따라서 4 A에서의 값을 사용합니다.

-For Reference Only-

유닛 명칭	유닛 내부 회로의 전압 강하	전원 케이블의 전압 강하	비고
SXD3	SXD1 내부 회로의 전압 강하 ・유닛/입력 전원: 0.18 V ・출력 전원: 0.22 V SXD2 내부 회로의 전압 강하 ・유닛/입력 전원: 0.09 V ・출력 전원: 0.11 V	・전원 케이블 1의 전압 강하: 0.53 V ・전원 케이블 2의 전압 강하: 0.36 V ・전원 케이블 3의 전압 강하: 0.18 V	전원 케이블 1 및 케이블 2의 전압 강하, 그리고 SXD1 내부 회로의 전압 강하에는 SXD1과 SXD2의 값을 사용합니다. 전원 케이블 3 및 SXD2 내부 회로의 전압 강하에는 다음과 같이 계산된 전류값을 사용합니다. (외부 전원으로부터의 각 유닛의 전류 소비량 합계) - (SXD1과 SXD2의 총 전류 소비량 합계) = 5.62 A - 2.18 A - 1.72 A = 1.72 A 따라서 2 A에서의 값을 사용합니다.

위 결과로부터 각 유닛의 입력 전원 전압은 다음과 같이 계산됩니다.

a. SXD1의 각 입력 전원 전압

유닛/입력 전원 전압
= 24.0 V - 전원 케이블 1의 전압 강하
= 24.0 V - 0.53 V
= 23.47 V
출력 전원 전압
= 24.0 V - 전원 케이블 1의 전압 강하 =
24.0 V - 0.53 V
= 23.47 V

b. SXD2의 각 입력 전원 전압

유닛/입력 전원 전압
= 24.0 V - (전원 케이블 1의 전압 강하 + SXD1 내부 회로의 전압 강하 + 전원 케이블 2의 전압 강하)
= 24.0 V - (0.53 V + 0.18 V + 0.36 V)
= 22.93 V
출력 전원 전압
= 24.0 V - (전원 케이블 1의 전압 강하 + SXD1 내부 회로의 전압 강하 + 전원 케이블 2의 전압 강하)
= 24.0 V - (0.53 V + 0.22 V + 0.36 V)
= 22.89 V

AI 번역본
For Reference Only-

c. SXD3의 각 입력 전원 전압

유닛/입력 전원 전압
= 24.0 V - (전원 케이블 1의 전압 강하 + SXD1 내부 회로의 전압 강하 + 전원 케이블 2의 전압 강하 + SXD2 내부 회로의 전압 강하 + 전원 케이블 3의 전압 강하)
= 24.0 V - (0.53 V + 0.18 V + 0.36 V + 0.09 V + 0.18 V)
= 22.66 V
출력 전원 전압

= 24.0 V - (전원 케이블 1의 전압 강하 + SXD1 내부 회로의 전압 강하 + 전원 케이블 2의 전압 강하 + SXD2 내부 회로의 전압 강하 + 전원 케이블 3의 전압 강하)
= 24.0 V - (0.53 V + 0.22 V + 0.36 V + 0.11 V + 0.18 V)
= 22.6 V

위 전압값은 모두 세이프티 I/O 블록의 각 전원의 전압 사양(19.2~28.8 VDC)을 만족하므로 허용됩니다.
또한 연결된 안전 입력 기기 또는 안전 출력 기기의 전압 사양을 만족하는지도 확인하십시오. 단, 이 예에서는 이 확인을 생략합니다.
전압 사양을 만족하지 않는 경우, 전원 케이블의 길이 및 연결된 외부 기기를 재검토하십시오.

AI 번역본
-For Reference Only-

4-3 전원 및 보호 장치 선택

이 절에서는 세이프티 I/O 블록의 외부 전원, 즉 유닛/입력 전원 및 출력 전원과 보호 장치를 선택하는 방법을 설명합니다.

4-3-1 외부 전원 선택

다음은 외부 전원에 권장되는 전원 및 그 전원 용량을 선택하는 방법을 설명합니다.

사용 전원

세이프티 I/O 블록의 외부 전원인 유닛/입력 전원 및 출력 전원에는, 다음 조건을 만족하는 SELV 전원 또는 오므론 내환경 IP67 전원(S8NR-S 시리즈)을 사용하십시오.

- 과전류 보호 기능이 있을 것
- 입력과 출력 사이에 이중 절연 또는 강화 절연이 되어 있을 것
- 출력 전압이 24 VDC(19.2~28.8 VDC)일 것

권장 전원: S8VK-S 시리즈(오므론), S8NR-S 시리즈(오므론)

전원 용량

유닛/입력 전원 및 출력 전원으로부터의 총 전류 소비량과 각 전원의 전원 용량을 4-6페이지의 4-2 전원 공급 시스템 설계에 기재된 계산 방법에 따라 계산하십시오.

안전 사용을 위한 주의사항

다음의 경우 유닛/입력 전원 및 출력 전원에 돌입 전류가 흐를 수 있습니다.

a. 전원을 켤 때.
b. 연결된 외부 기기에 전원 공급을 시작할 때.
c. 연결된 외부 기기를 켜거나 끌 때.

또한 I/O 케이블에 단락이 발생한 경우 보호 기능이 작동할 때까지 과전류가 흐를 수 있습니다. 이러한 전류를 고려하여 충분한 여유 용량을 가진 전원을 선택하십시오. 돌입 전류로 인해 전원이 정상적으로 동작하지 않거나 전원이 꺼질 수 있습니다.

4-3-2 보호 장치 선택

이 절에서는 외부 회로의 단락 및 과전류로부터 보호하기 위한 보호 장치(브레이커, 퓨즈 등)를 선택하는 방법을 설명합니다.

과전류란 단락 또는 기기 고장 등으로 인해 다음 정격을 초과하여 기기가 사용될 때 흐르는 전류입니다.

- 유닛/입력 전원 및 출력 전원(공통): 최대 전원 전류

・유닛/입력 전원: 테스트 출력 단자의 정격 전류
・출력 전원: 안전 출력 기기로의 최대 부하 전류

위 정격에 대해서는 2-6페이지의 2-1-4 유닛 사양을 참조하십시오.

보호 장치 선택

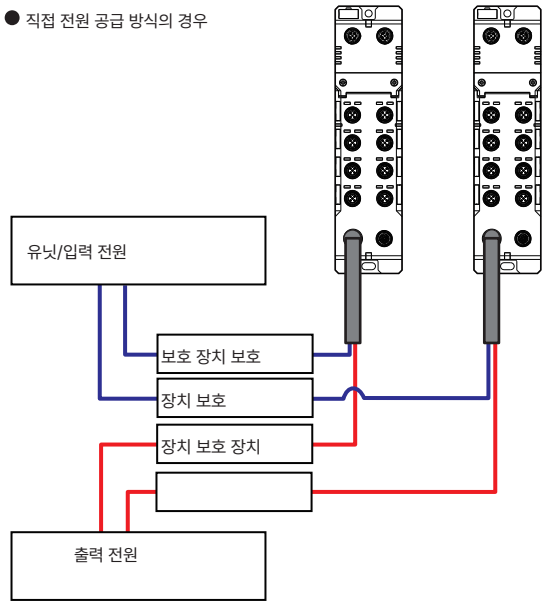
보호 장치를 선택할 때는 다음을 고려하십시오.
・보호 장치 사양(차단/용단, 검출 특성, 정상 전류값 등)
・전원을 켤 때의 돌입 전류
・연결된 외부 기기로의 전원 공급을 시작할 때의 돌입 전류
・연결된 외부 기기를 켜거나 끌 때의 돌입 전류

보호 장치 설치 위치

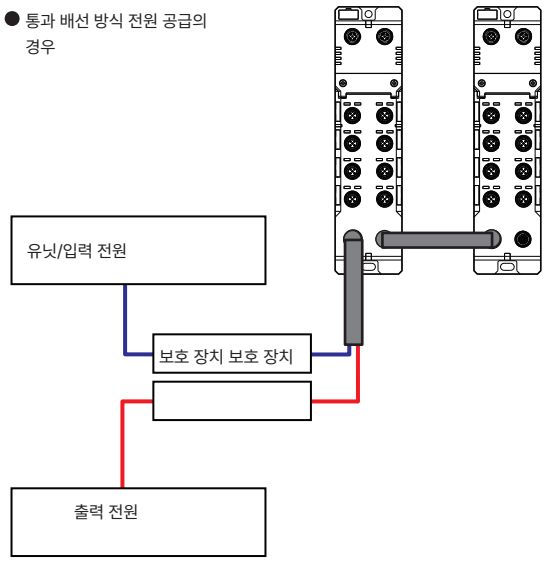
다음 그림과 같이 유닛/입력 전원 및 출력 전원 각각에
보호 장치를 설치하십시오.

AI 번역본
-For Reference Only-

● 직접 전원 공급 방식의 경우



● 통과 배선 방식 전원 공급의 경우



AI 번역본
-For Reference Only-

AI 번역본
-For Reference Only-

5

설치 및 배선

이 장에서는 세이프티 I/O 블록을 설치 및 배선하는 방법을 설명합니다.

5-1 유닛 설치 5-2
5-1-1 설치 시 주의사항 5-2
5-1-2 설치 방향 5-2
5-1-3 설치 방법 5-3

5-2 EtherNet/IP 네트워크 배선 5-5
5-2-1 설치 시 주의사항 5-5
5-2-2 통신 케이블 연결 5-6

5-3 전원 배선 5-12
5-3-1 설치 시 주의사항 5-12
5-3-2 사용할 전원 케이블, 조임 공구 및 조임 토크 5-12
5-3-3 외부 전원에 전원 케이블 연결 5-13
5-3-4 전원 케이블 연결 5-14

5-4 I/O 케이블 배선 5-19
5-4-1 설치 시 주의사항 5-19
5-4-2 I/O 케이블 연결 5-19
5-4-3 배선 예 5-24

5-5 연결 기기 5-29
5-5-1 Ethernet 케이블 5-29
5-5-2 전원 케이블 5-31
5-5-3 I/O 케이블 5-34
5-5-4 커넥터용 방수 커버 5-38

5-6 옵션 5-39
5-6-1 마커 5-39

사내 열람
-For Reference Only-

5-1 유닛 설치

이 절에서는 세이프티 I/O 블록을 설치하는 방법을 설명합니다.

5-1-1 설치 시 주의사항

세이프티 I/O 블록의 신뢰성을 높이고 기능을 충분히 활용하려면 다음 주의사항을 준수하십시오.

유닛을 다음과 같은 장소에 설치하지 마십시오.

- 직사광선이 닿는 장소
- 유닛 사양에 명시된 범위를 벗어나는 주위 온도 또는 습도에 노출되는 장소
- 급격한 온도 변화로 인해 결로가 발생하는 장소
- 부식성 가스 또는 가연성 가스가 있는 장소
- 먼지(특히 철분)나 염분이 있는 장소
- 산, 오일 또는 화학 물질에 노출되는 장소
- 충격이나 진동이 있는 장소
- 전력선 근처의 장소

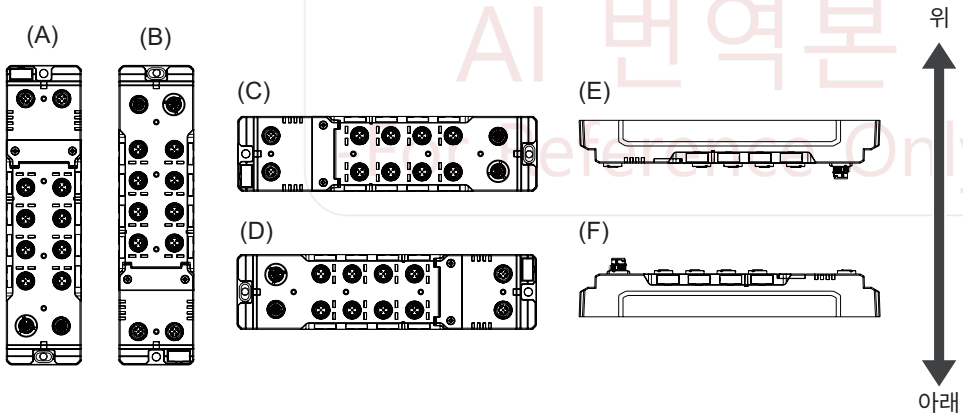
다음과 같은 장소에 설치할 때는 적절하고 충분한 대책을 마련하십시오.

- 정전기 또는 기타 형태의 노이즈가 있는 장소
- 강한 전자기장이 있는 장소
- 방사능에 노출될 가능성이 있는 장소
- 전원 공급선 근처의 장소

5-1-2 설치 방향

세이프티 I/O 블록은 다음 6가지 방향 중 어느 방향으로도 설치할 수 있습니다.

AI 번역본
-For Reference Only-



5-1-3 설치 방법

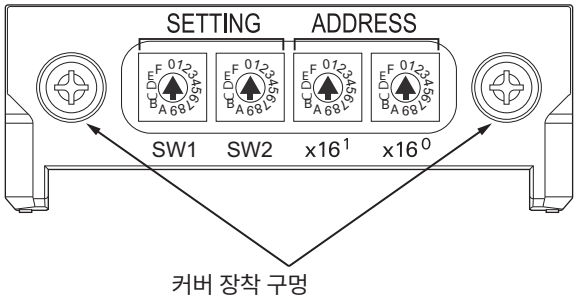
이 절에서는 세이프티 I/O 블록의 다음 항목을 설치하는 방법을 설명합니다.

・로터리 스위치 커버 설치

・유닛 설치

로터리 스위치 커버 설치

커버 장착 구멍 2개를 사용하여 로터리 스위치 커버를 나사로 고정하십시오.



M3 나사를 다음 토크로 조이십시오. 규정된 조임 토크로 나사를 조이면 IP67 보호 구조를 유지할 수 있습니다.

조임 위치	나사 크기	조임 토크
로터리 스위치 커버 장착 구멍	M3	0.4~0.6 N · m

사용상의 주의

・나사에 오일이 묻지 않도록 하십시오. 오일이 묻으면 나사가 손상될 수 있습니다.

・적절한 드라이버로 나사를 조이십시오. 부적절한 드라이버로 나사를 조이면 나사가 손상될 수 있습니다.

추가 정보

출하 시 커버가 장착되어 있습니다.

AI 번역본
For Reference Only-

유닛 설치

유닛 장착 구멍 2개를 사용하여 세이프티 I/O 블록을 나사로 고정하십시오.

유닛의 상단과 하단에 각각 장착 구멍이 있습니다. 설치 치수에 대한 자세한 내용은 A-2페이지의 A-1 치수를 참조하십시오.

M5 나사를 다음 토크로 조이십시오.

조임 위치	나사 크기	조임 토크
유닛 장착 구멍	M5	1.47~1.96N · m

사용상의 주의

- 유닛을 올바르게 설치하십시오. 올바르게 설치하지 않으면 진동의 영향을 받아 고장의 원인이 될 수 있습니다.
- 나사에 오일이 묻지 않도록 하십시오. 오일이 묻으면 나사가 손상될 수 있습니다.
- 적절한 드라이버로 나사를 조이십시오. 부적절한 드라이버로 나사를 조이면 나사가 손상될 수 있습니다.

AI 번역본
-For Reference Only-

5-2 EtherNet/IP 네트워크 배선

이 절에서는 세이프티 I/O 블록의 EtherNet/IP 네트워크를 설치하는 방법을 설명합니다.

5-2-1 설치 시 주의사항

세이프티 I/O 블록의 EtherNet/IP 네트워크 설치에 관한 기본 주의사항은 다음과 같습니다.

네트워크 설치 시 주의사항

- EtherNet/IP 네트워크를 설치할 때는 충분한 안전 대책을 강구하고 관련되는 모든 표준 및 사양에 따라 설치를 수행하십시오. 안전 대책과 표준 및 사양에 정통한 전문가에게 설치를 의뢰하십시오.
- EtherNet/IP 네트워크 기기를 노이즈 발생원 근처에 설치하지 마십시오. 노이즈가 있는 영역에 네트워크를 설치해야 하는 경우, 기기를 금속 케이스에 넣는 등 노이즈 대책을 마련하십시오.

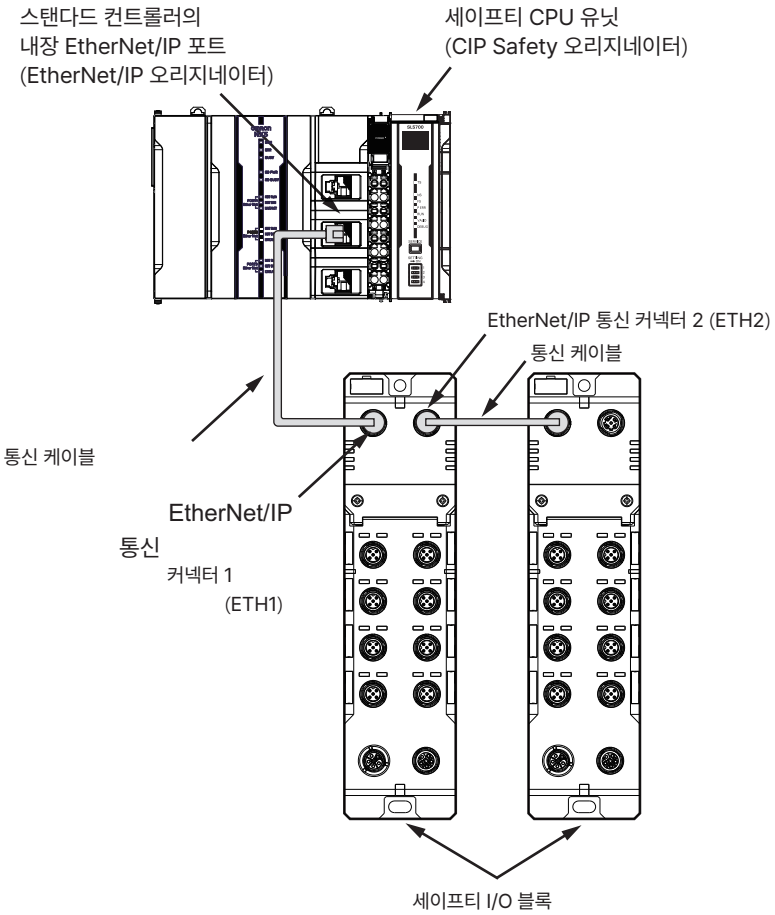
통신 케이블 설치 시 주의사항

- 세이프티 I/O 블록의 IP67 보호 구조를 유지하려면, 사용하는 통신 커넥터에 5-29페이지의 5-5-1 Ethernet 케이블에 나온 통신 케이블을 사용하십시오.
  - 세이프티 I/O 블록의 IP67 보호 구조를 유지하려면, 사용하지 않는 통신 커넥터에 5-38페이지의 5-5-4 커넥터용 방수 커버에 나온 방수 커버를 사용하십시오.
- 나사식 커넥터를 사용하는 경우, 올바른 배선 공구를 사용하여 규정된 토크로 조이십시오.
- RJ45 모듈러 커넥터가 있는 기기에 통신 케이블을 연결할 때는, 통신 케이블 커넥터를 딸깍 소리가 나며 고정될 때까지 확실하게 삽입하십시오.
- 사용하는 통신 케이블에서 다음 항목을 점검하십시오.
  단선된 부분이 있습니까?
  단락된 부분이 있습니까?
  커넥터에 문제가 있습니까?
- 통신 케이블을 고압선과 함께 배선하지 마십시오.
- 통신 케이블을 노이즈를 발생시키는 기기 근처에 배선하지 마십시오.
- 통신 케이블을 고온 또는 다습한 장소에 배선하지 마십시오.
- 먼지, 오일 미스트 또는 기타 오염 물질이 과도한 장소에서는 통신 케이블을 사용하지 마십시오.
- 통신 케이블의 굽힘 반경에는 제한이 있습니다. 굽힘 반경에 대해서는 통신 케이블의 사양을 확인하십시오.
- 케이블 실드가 양쪽 끝의 커넥터 후드에 연결되지 않은 통신 케이블을 사용하면 노이즈 내성이 저하될 수 있습니다. 통신 케이블에는 연결 기기 절에 나온 Ethernet 케이블을 사용하십시오. 이러한 통신 케이블은 케이블 실드가 양쪽 끝의 커넥터 후드에 연결되어 있습니다.

AI 번역본
For Reference Only-

5-2-2 통신 케이블 연결

EtherNet/IP 네트워크에서는 케이블을 자유롭게 연결할 수 있습니다.
다음 그림은 라인 토폴로지의 연결 예를 나타낸 것입니다.
EtherNet/IP 오리지네이터로부터의 통신 케이블을 첫 번째 세이프티 I/O 블록의 통신 커넥터에 연결합니다. 그런 다음, 첫 번째 유닛의 나머지 통신 커넥터에서 또 다른 통신 케이블을 두 번째 세이프티 I/O 블록의 통신 커넥터에 연결합니다.



통신 커넥터, 즉 ETH1과 ETH2를 구분할 필요는 없습니다. 커넥터 하나만 사용하는 스타 접속을 구성하려면 통신 케이블을 ETH1 또는 ETH2 중 어느 쪽에 연결해도 됩니다.

AI 번역본
-For Reference Only-

Smartclick 커넥터를 사용한 연결 절차

이 절에서는 Smartclick 커넥터 타입 케이블을 사용할 때의 연결 및 분리 절차를 설명합니다.

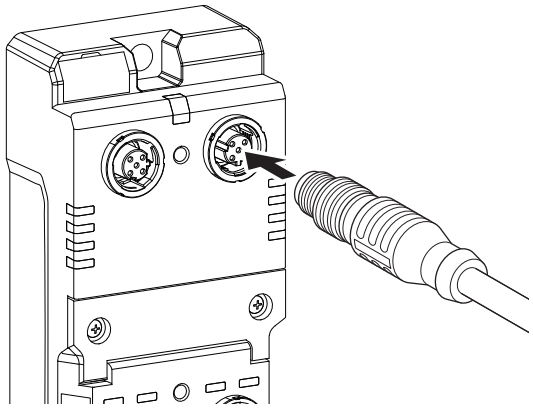
● 통신 케이블

통신 케이블에는 5-29페이지의 5-5-1 Ethernet 케이블에 나온 Ethernet 케이블을 사용하십시오.

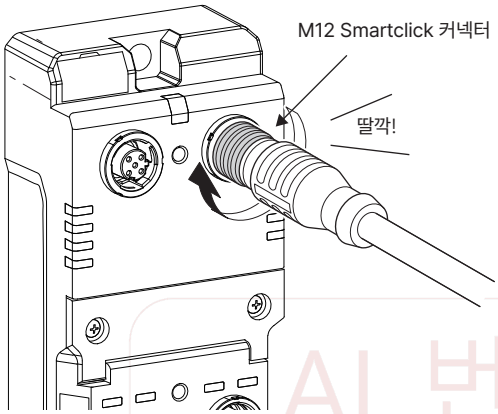
● 연결 절차(Smartclick 커넥터)

통신 케이블을 연결하는 절차는 다음과 같습니다. 통신 케이블을 연결하기 전에 세이프티 I/O 블록의 유닛/입력 전원 및 출력 전원과, 유닛과 통신할 기기의 전원을 끄십시오.

1 Ethernet 케이블의 M12 플러그(수형)를 세이프티 I/O 블록의 통신 커넥터(암형)에 통신 커넥터의 방향에 주의하면서 삽입하십시오.



2 Ethernet 케이블의 M12 Smartclick 커넥터를 끝까지 삽입한 다음 아래 그림에 표시된 방향으로 약 1/8 회전시키십시오.

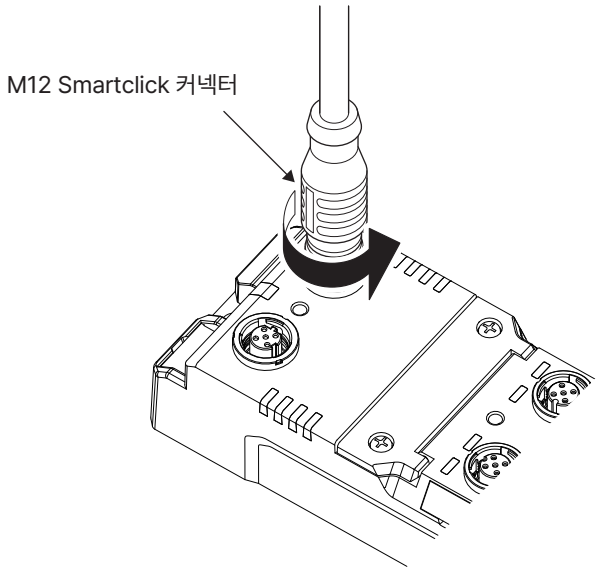


AI 번역본
For Reference Only-

● 분리 절차(Smartclick 커넥터)

통신 케이블을 분리하는 절차는 다음과 같습니다. 통신 케이블을 분리하기 전에 세이프티 I/O 블록의 유닛/입력 전원 및 출력 전원과, 유닛과 통신할 기기의 전원을 끄십시오.

1 Ethernet 케이블의 M12 Smartclick 커넥터를 아래 그림에 표시된 방향으로 약 1/8 회전시킨 다음 케이블을 분리하십시오.



나사식 커넥터를 사용한 연결 절차

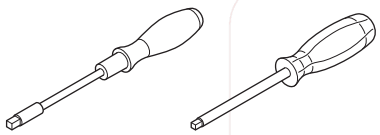
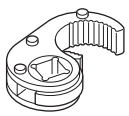
이 절에서는 나사식 커넥터 타입 케이블을 사용할 때의 연결 및 분리 절차를 설명합니다.

● 통신 케이블

통신 케이블에는 5-29페이지의 5-5-1 Ethernet 케이블에 나온 Ethernet 케이블을 사용하십시오.

● 조임 공구

Ethernet 케이블의 M12 나사식 커넥터를 규정된 토크로 조이려면 다음 공구를 사용하십시오.

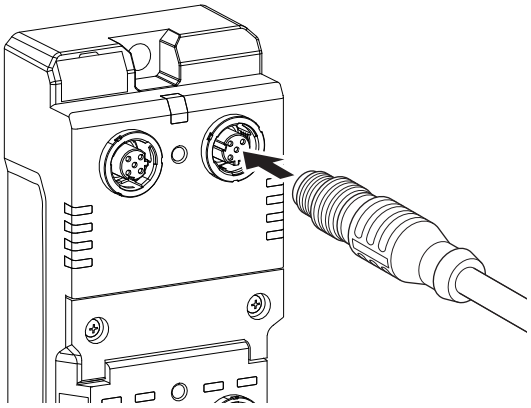
명칭 및 외관	제조사	모델
· M12 토크 핸들 제품, 토크 설정 보조구  · M12 어태치먼트 	Weidmuller	Screwty-M12-DM

AI 번역본
-For Reference Only-

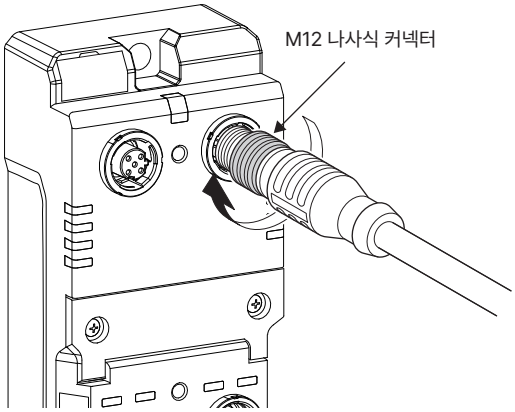
● 연결 절차(나사식 커넥터)

통신 케이블을 연결하는 절차는 다음과 같습니다. 통신 케이블을 연결하기 전에 세이프티 I/O 블록의 유닛/입력 전원 및 출력 전원과, 유닛과 통신할 기기의 전원을 끄십시오.

1 Ethernet 케이블의 M12 플러그(수형)를 세이프티 I/O 블록의 통신 커넥터(암형)에 통신 커넥터의 방향에 주의하면서 삽입하십시오.

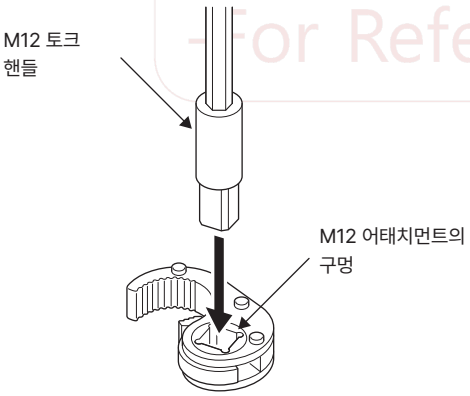


2 다음 그림에 표시된 방향으로 Ethernet 케이블의 M12 나사식 커넥터를 돌려 조이십시오. 규정된 토크로 조이기 전에 커넥터를 조이십시오.

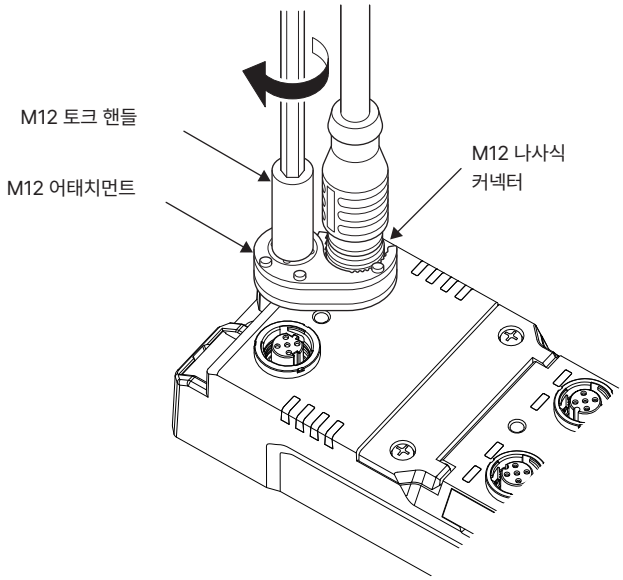


3 M12 토크 핸들을 규정된 토크로 설정하십시오. 그런 다음 토크 핸들을 M12 어태치먼트의 조임 구멍에 삽입하십시오. 커넥터를 조일 때는 다음 그림에 표시된 방향으로 M12 어태치먼트를 놓고 토크 핸들을 삽입하십시오.
규정된 토크에 대해서는 5-11페이지의 조임 토크를 참조하십시오.

사내참조용
-For Reference Only-



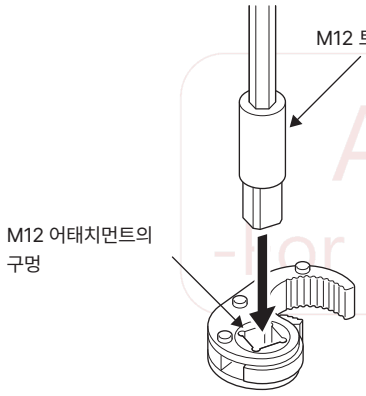
4 Ethernet 케이블의 M12 나사식 커넥터에 M12 어태치먼트를 장착하십시오. M12 어태치먼트를 장착한 후, 다음 그림에 표시된 방향으로 M12 토크 핸들을 돌려 M12 나사식 커넥터를 규정된 토크로 조이십시오.



● 분리 절차(나사식 커넥터)

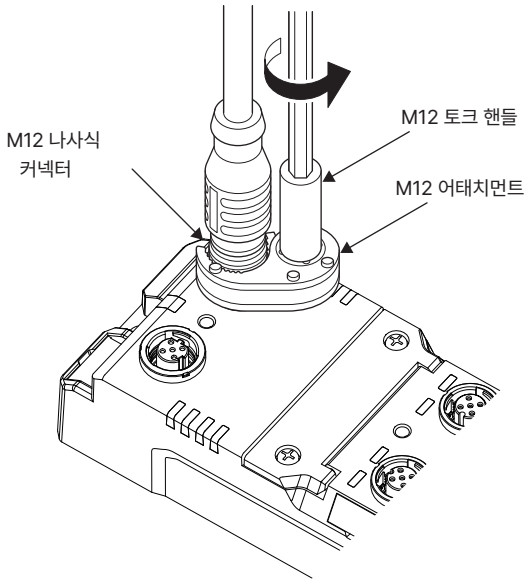
통신 케이블을 분리하는 절차는 다음과 같습니다. 통신 케이블을 분리하기 전에 세이프티 I/O 블록의 유닛/입력 전원 및 출력 전원과, 유닛과 통신할 기기의 전원을 끄십시오.

1 M12 토크 핸들을 M12 어태치먼트의 조임 구멍에 삽입하십시오. 커넥터를 분리할 때는 연결할 때와 반대 방향이 되도록 M12 어태치먼트를 거꾸로 놓으십시오.



AI 번역본
-For Reference Only-

2 Ethernet 케이블의 M12 나사식 커넥터에 M12 어태치먼트를 장착하십시오. M12 어태치먼트를 장착한 후, 다음 그림에 표시된 방향으로 M12 토크 핸들을 돌려 M12 나사식 커넥터를 풀어 주십시오.



3 Ethernet 케이블의 M12 나사식 커넥터를 연결 방향과 반대 방향으로 돌려 케이블을 분리하십시오.

조임 토크

Ethernet 케이블의 M12 나사식 커넥터를 다음 토크로 조이십시오.
나사식 커넥터를 적절한 조임 토크로 조이면 IP67 보호 구조를 유지할 수 있습니다.

조임 위치	나사 크기	조임 토크
EtherNet/IP 통신 커넥터	M12	0.5~0.6 N · m*1

***1.** Smartclick 커넥터 타입의 경우 토크 관리가 필요하지 않습니다. 커넥터를 끝까지 삽입한 다음 약 1/8 회전시키십시오.

방수 커버

사용하지 않는 EtherNet/IP 통신 커넥터에는 5-38페이지의 5-5-4 커넥터용 방수 커버에 나온 방수 커버를 장착하십시오.

AI 번역본
-For Reference Only-

5-3 전원 배선

이 절에서는 세이프티 I/O 블록에 유닛/입력 전원 및 출력 전원을 배선하는 방법을 설명합니다.

⚠ 경고

- 유닛 및 슬레이브에 입력되는 전압과 전류가 규정된 범위 내에 있는지 확인하십시오.
  규정된 범위를 벗어나는 전압 또는 전류를 입력하면 사고나 화재의 원인이 될 수 있습니다.
- 이 매뉴얼의 지시에 따라 전원 설계 및 배선을 올바르게 수행하십시오.
  규정된 범위를 벗어나는 전압 또는 전류의 입력 및 잘못된 배선은 고장이나 화재의 원인이 될 수 있습니다.



5-3-1 설치 시 주의사항

세이프티 I/O 블록에 대한 전원 설치의 기본 주의사항은 다음과 같습니다.

- 세이프티 I/O 블록의 IP67 보호 구조를 유지하려면, 전원 커넥터에 5-31페이지의 5-5-2 전원 케이블에 나온 나사식 커넥터가 달린 전원 케이블을 사용하십시오.
- 세이프티 I/O 블록의 IP67 보호 구조를 유지하려면, 사용하지 않는 전원 커넥터에 5-38페이지의 5-5-4 커넥터용 방수 커버에 나온 방수 커버를 사용하십시오.
- 통신 케이블을 고온 또는 다습한 장소에 배선하지 마십시오.
- 먼지, 오일 미스트 또는 기타 오염 물질이 과도한 장소에서는 통신 케이블을 사용하지 마십시오.
- 전원 케이블의 굽힘 반경에는 제한이 있습니다. 굽힘 반경에 대해서는 전원 케이블의 사양을 확인하십시오.

5-3-2 사용할 전원 케이블, 조임 공구 및 조임 토크

이 절에서는 세이프티 I/O 블록에 사용할 전원 케이블, 조임 공구 및 조임 토크를 설명합니다.

AI 번역본
-For Reference Only-

● 전원 케이블

전원 케이블에는 5-31페이지의 5-5-2 전원 케이블에 나온 전원 케이블을 사용하십시오.

● 조임 공구

나사식 커넥터 타입 전원 케이블의 경우, 각 제조사가 권장하는 조임 공구를 사용하십시오.
Smartclick 커넥터 타입 전원 케이블의 경우, 조임 공구가 필요하지 않습니다.

● 조임 토크

나사식 커넥터 타입 전원 케이블은 다음 토크로 조이십시오.
나사식 커넥터를 적절한 조임 토크로 조이면 IP67 보호 구조를 유지할 수 있습니다.

조임 위치	나사 크기	조임 토크
전원 커넥터	M12	0.39~0.49 N · m*1

*1. Smartclick 커넥터 타입의 경우 토크 관리가 필요하지 않습니다. 커넥터를 끝까지 삽입한 다음 약 1/8 회전시키십시오.

5-3-3 외부 전원에 전원 케이블 연결

외부 전원에는 5-31페이지의 5-5-2 전원 케이블에 나온 전원 케이블을 사용하십시오.
이 절에서는 오므론 M12 L코딩 전원 케이블(XS5F-L521-□12-F, XS5W-L521-□12-F)을 사용할 때의 연결 방법을 설명합니다.

XS5W-L521-□12-F는 양쪽 끝에 커넥터가 있는 케이블이고, XS5F-L521-□12-F는 단선 케이블입니다.

전원 케이블의 M12 소켓 쪽 끝(암형 쪽)을 세이프티 I/O 블록의 전원 커넥터(입력)에 연결하고, 반대쪽 끝은 전원 유닛에 연결하십시오.

내환경 IP67 전원(S8NR-S 시리즈)과의 연결

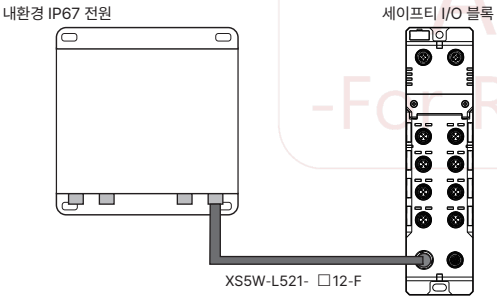
내환경 IP67 전원(S8NR-S 시리즈)을 사용하는 경우, 양쪽 끝에 커넥터가 있는 전원 케이블(XS5W-L521-□12-F)을 사용하십시오.

XS5W-L521-□12-F의 외관은 아래와 같습니다.



아래와 같이 M12 플러그 쪽 끝(수형 쪽)을 내환경 IP67 전원에 연결하십시오.

AI 번역본
-For Reference Only-



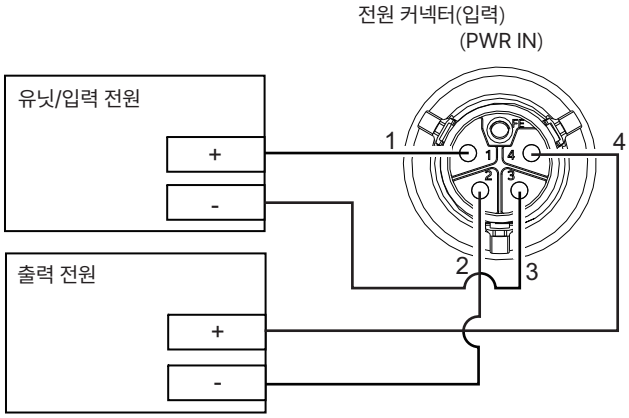
범용 전원 유닛과의 연결

범용 전원 유닛을 사용하는 경우, 단선 전원 케이블(XS5F-L521-□12-F)을 사용하십시오.

XS5F-L521-□12-F의 외관은 아래와 같습니다.



다음 배선도에 따라 전원 케이블의 단선 쪽 끝을 외부 전원에 연결하십시오.



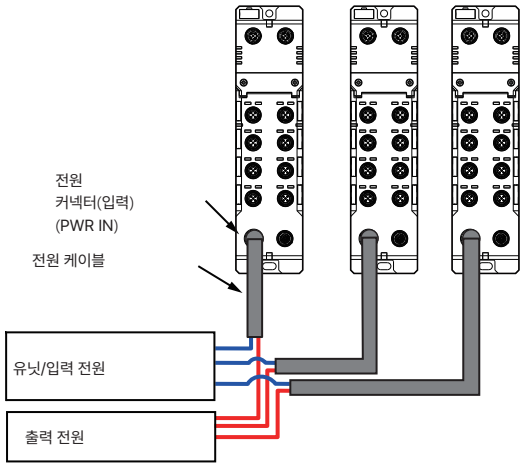
전원 커넥터(입력)의 핀 배열		외부 전원 배선	전원 케이블 단선 색상
핀 번호	신호명		
1	U/IN P+	유닛/입력 전원의 양극(+) 쪽을 연결하십시오.	갈색
2	OUT P-	출력 전원의 음극(-) 쪽을 연결하십시오.	백색
3	U/IN P-	유닛/입력 전원의 음극(-) 쪽을 연결하십시오.	청색
4	OUT P+	출력 전원의 양극(+) 쪽을 연결하십시오.	흑색
FE(기능 접지)	FG	프레임 그라운드	회색

시 버 여 보
-For Reference Only-

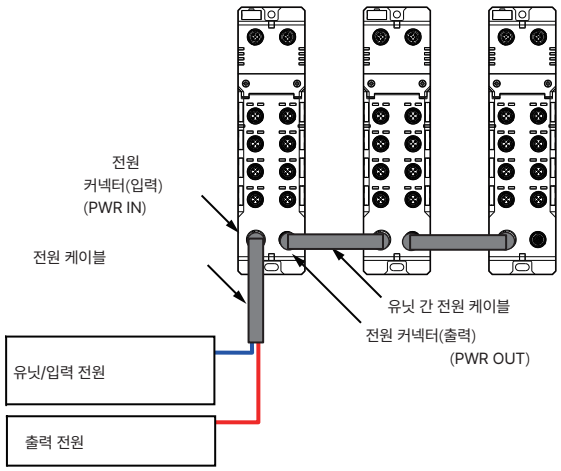
5-3-4 전원 케이블 연결

아래와 같이 세이프티 I/O 블록에 외부 전원을 공급하는 방법에는 두 가지가 있습니다.

・직접 전원 공급



· 통과 배선 방식 전원 공급



직접 전원 공급 방식에서는 각 세이프티 I/O 블록의 전원 커넥터(출력)를 사용하지 않습니다.
통과 배선 방식 전원 공급에서는 각 세이프티 I/O 블록의 전원 커넥터(출력)를 사용합니다. 단, 전원을 공급하는 마지막 유닛의 전원 커넥터(출력)는 사용하지 않습니다.

전원 공급 방식에 대한 자세한 내용은 4-2페이지의 4-1-2 전원 시스템을 참조하십시오.

안전 사용을 위한 주의사항

최대 전원 전류는 유닛/입력 전원 전류와 출력 전원 전류를 합한 9 A입니다.
유닛을 최대 전원 전류를 초과하여 사용하지 마십시오. 초과하여 사용하면 전원 케이블에 과전류가 흘러 화재의 원인이 될 수 있습니다.

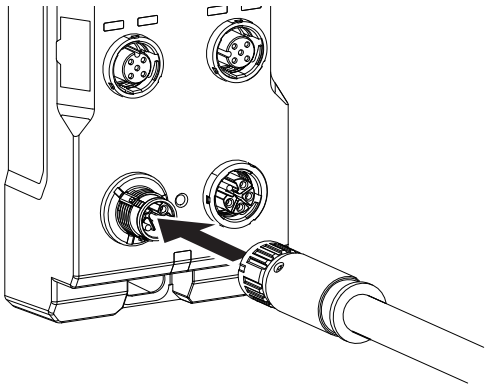
사용상의 주의

유닛/입력 전원과 출력 전원에는 항상 별도의 전원을 사용하십시오. 동일한 전원에서 전원을 공급하면 출력 기기의 부하 변동으로 인해 오작동이 발생할 수 있습니다.

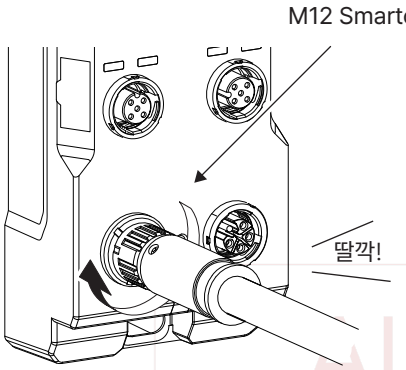
연결 절차

이 절에서는 오므론 M12 L코딩 전원 케이블을 사용할 때의 연결 절차를 설명합니다
(XS5F-L521-□12-F, XS5W-L521- □12-F).
전원 케이블을 연결하려면 다음 절차를 사용하십시오. 전원 케이블을 연결하기 전에 유닛/입력 전원
및 출력 전원을 끄십시오.

1 전원 케이블의 M12 소켓(암형)을 세이프티 I/O 블록의 전원 커넥터(입력)(수형)에
전원 커넥터의 방향에 주의하면서 삽입하십시오.

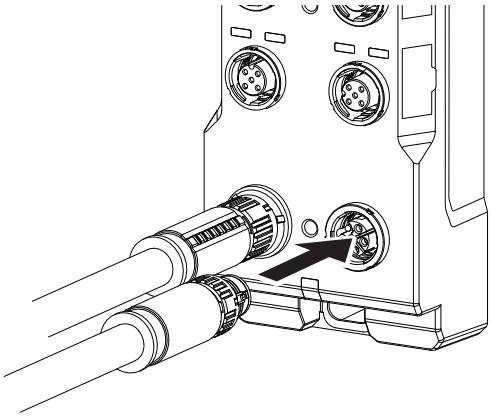


2 전원 케이블의 M12 Smartclick 커넥터를 끝까지 삽입한 다음 아래 그림에 표시된 방향으로
약 1/8 회전시키십시오.

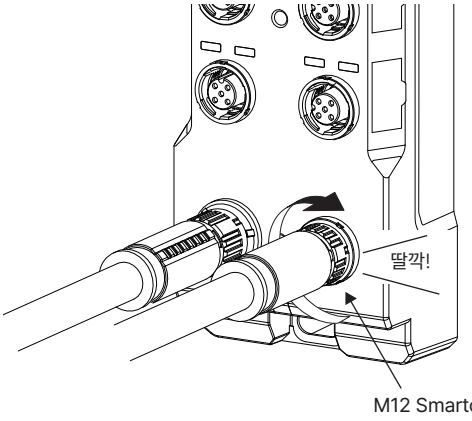


AI 번역본
-For Reference Only-

3 통과 배선 방식으로 전원을 공급하는 경우, 전원 케이블의 M12 소켓(수형)을
세이프티 I/O 블록의 전원 커넥터(출력)(암형)에 전원 커넥터의 방향에 주의하면서 삽입하십시오.



4 전원 케이블의 M12 Smartclick 커넥터를 끝까지 삽입한 다음 아래 그림에 표시된 방향으로 약 1/8 회전시키십시오.



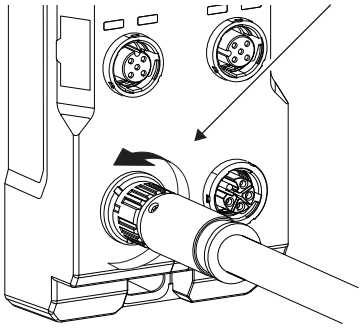
분리 절차

이 절에서는 오므론 M12 L코딩 전원 케이블을 사용할 때의 분리 절차를 설명합니다 (XS5F-L521-□12-F, XS5W-L521- □12-F).
전원 케이블을 분리하는 절차는 다음과 같습니다. 전원 케이블을 분리하기 전에 유닛/입력 전원 및 출력 전원을 끄십시오.

AI 번역본
-For Reference Only-

1 전원 케이블의 M12 Smartclick 커넥터를 아래 그림에 표시된 방향으로 약 1/8 회전시킨 다음 케이블을 분리하십시오.

M12 Smartclick 커넥터



2 통과 배선 방식으로 전원을 공급하는 경우에도 동일한 절차로 케이블을 분리하십시오.

방수 커버

사용하지 않는 전원 커넥터에는 5-38페이지의 5-5-4 커넥터용 방수 커버에
나온 방수 커버를 장착하십시오.

AI 번역본
-For Reference Only-

5-4 I/O 케이블 배선

이 절에서는 세이프티 I/O 블록에 외부 기기를 연결하기 위한 I/O 케이블 배선 방법을 설명합니다.

5-4-1 설치 시 주의사항

세이프티 I/O 블록의 I/O 케이블 설치에 관한 기본 주의사항은 다음과 같습니다.

- 세이프티 I/O 블록의 IP67 보호 구조를 유지하려면, I/O 커넥터에 5-34페이지의 Smartclick 커넥터 타입 및 5-37페이지의 나사식 커넥터에 나온 I/O 케이블을 사용하십시오.
- 세이프티 I/O 블록의 IP67 보호 구조를 유지하려면, 사용하지 않는 I/O 커넥터에 5-38페이지의 5-5-4 커넥터용 방수 커버에 나온 방수 커버를 사용하십시오.
- 나사식 커넥터를 사용하는 경우, 올바른 배선 공구를 사용하여 규정된 토크로 조이십시오.
- 통신 케이블을 고온 또는 다습한 장소에 배선하지 마십시오.
- 먼지, 오일 미스트 또는 기타 오염 물질이 과도한 장소에서는 통신 케이블을 사용하지 마십시오.
- I/O 케이블의 굽힘 반경에는 제한이 있습니다. 굽힘 반경에 대해서는 사용할 I/O 케이블의 사양을 확인하십시오.

5-4-2 I/O 케이블 연결

이 절에서는 I/O 케이블의 연결 절차, 분리 절차, 조임 토크 및 방수 커버를 설명합니다.

Smartclick 커넥터를 사용한 연결 절차

이 절에서는 Smartclick 커넥터 타입 케이블을 사용할 때 I/O 케이블의 연결 및 분리 절차를 설명합니다.

● I/O 케이블

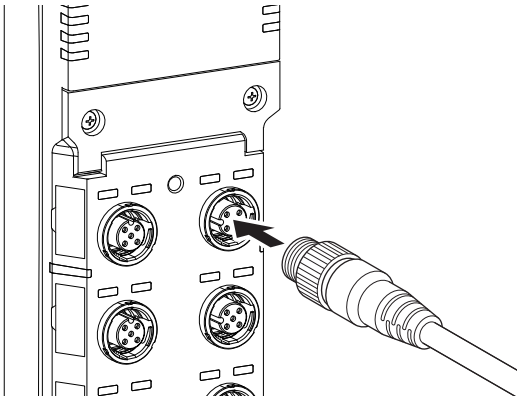
I/O 케이블에는 5-34페이지의 Smartclick 커넥터 타입에 나온 I/O 케이블을 사용하십시오.

● 연결 절차(Smartclick 커넥터)

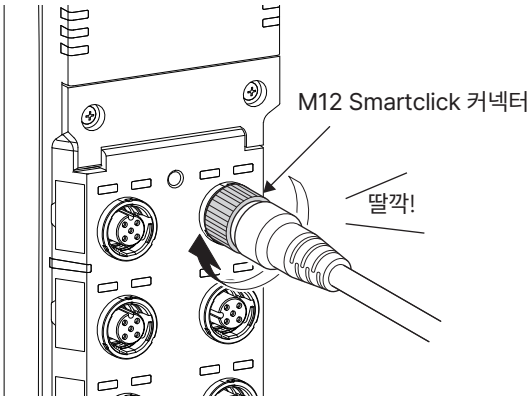
I/O 케이블을 연결하는 절차는 다음과 같습니다. I/O 케이블을 연결하기 전에 세이프티 I/O 블록의 유닛/입력 전원 및 출력 전원을 끄십시오.

AI 번역본
For Reference Only-

1 I/O 케이블의 M12 플러그(수형)를 세이프티 I/O 블록의 I/O 커넥터(암형)에 I/O 커넥터의 방향에 주의하면서 삽입하십시오.



2 I/O 케이블의 M12 Smartclick 커넥터를 끝까지 삽입한 다음 아래 그림에 표시된 방향으로 약 1/8 회전시키십시오.

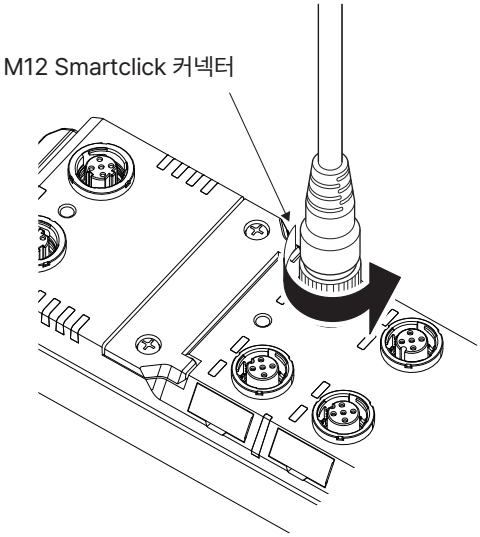


● 분리 절차(Smartclick 커넥터)

I/O 케이블을 분리하는 절차는 다음과 같습니다. I/O 케이블을 분리하기 전에 세이프티 I/O 블록의 유닛/입력 전원 및 출력 전원을 끄십시오.

1 I/O 케이블의 M12 Smartclick 커넥터를 아래 그림에 표시된 방향으로 약 1/8 회전시킨 다음 케이블을 분리하십시오.

AI 번역본
-For Reference Only-



나사식 커넥터를 사용한 연결 절차

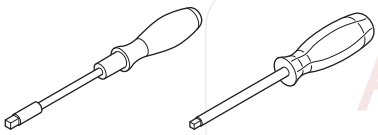
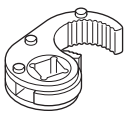
이 절에서는 나사식 커넥터 타입 케이블을 사용할 때 I/O 케이블의 연결 및 분리 절차를 설명합니다.

● I/O 케이블

I/O 케이블에는 5-37페이지의 나사식 커넥터에 나온 I/O 케이블을 사용하십시오.

● 조임 공구

I/O 케이블의 M12 나사식 커넥터를 규정된 토크로 조이려면 아래 공구를 사용하십시오.

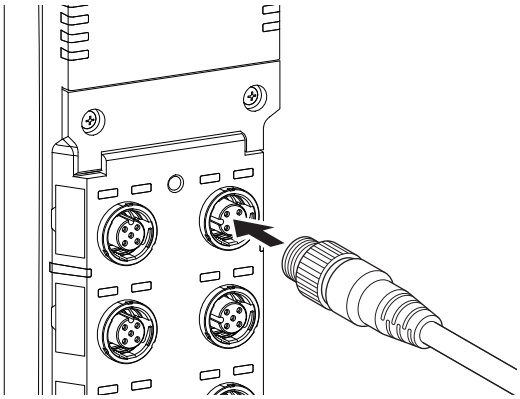
명칭 및 외관	제조사	모델
· M12 토크 핸들 제품, 토크 설정 보조구  · M12 어태치먼트 	Weidmuller	Screwty-M12-DM

AI 번역본
-For Reference Only-

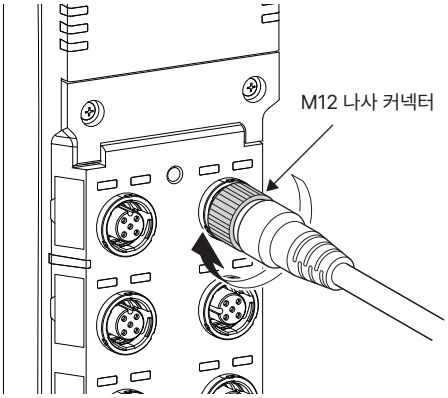
● 연결 절차(나사식 커넥터)

I/O 케이블을 연결하는 절차는 다음과 같습니다. I/O 케이블을 연결하기 전에 세이프티 I/O 블록의 유닛/입력 전원 및 출력 전원을 끄십시오.

1 I/O 케이블의 M12 플러그(수형)를 세이프티 I/O 블록의 I/O 커넥터(암형)에 I/O 커넥터의 방향에 주의하면서 삽입하십시오.

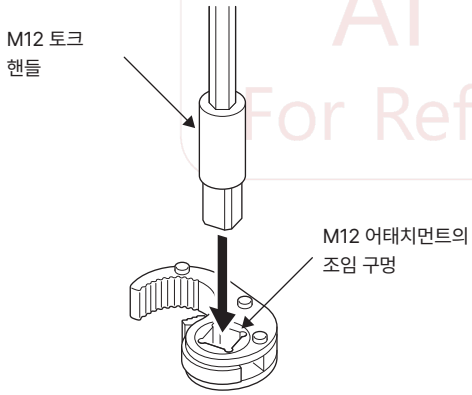


2 다음 그림에 표시된 방향으로 I/O 케이블의 M12 나사식 커넥터를 돌려 조이십시오. 규정된 토크로 조이기 전에 커넥터를 조이십시오.

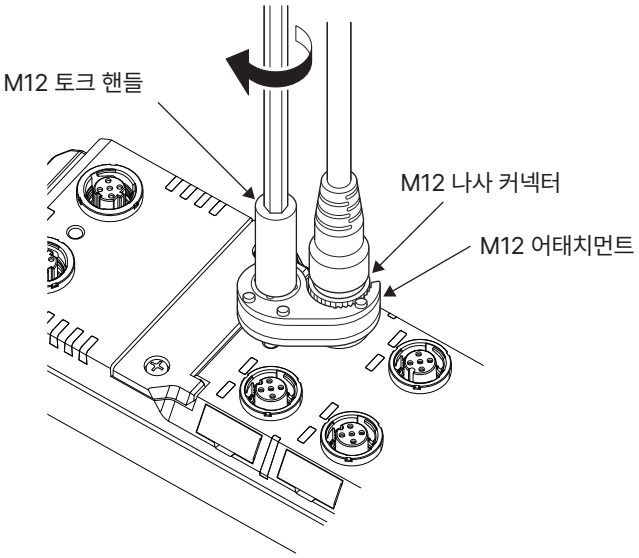


3 M12 토크 핸들을 지정된 토크로 설정하십시오. 그런 다음, 토크 핸들을 M12 어태치먼트의 조임 구멍에 삽입하십시오. 커넥터를 조일 때는 다음 그림에 표시된 방향으로 M12 어태치먼트를 배치하고 토크 핸들을 삽입하십시오.
지정된 토크에 대한 내용은 5-24페이지의 조임 토크를 참조하십시오.

AI 번역본
-For Reference Only-



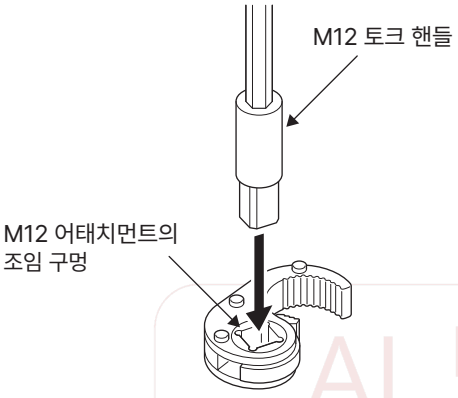
4 M12 어태치먼트를 I/O 케이블의 M12 나사 커넥터에 장착하십시오. M12 어태치먼트를 장착한 후, 다음 그림에 표시된 방향으로 M12 토크 핸들을 돌려 M12 나사 커넥터를 지정된 토크로 조이십시오.



● 분리 절차 (나사 커넥터)

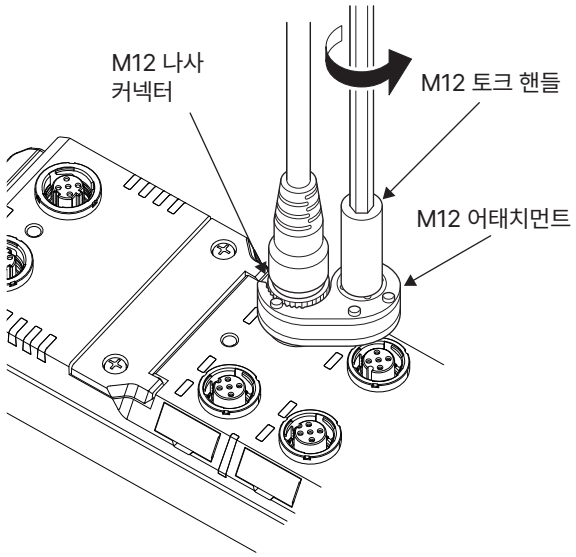
I/O 케이블을 분리하는 절차는 다음과 같습니다. I/O 케이블을 분리하기 전에 세이프티 I/O 블록의 유닛/입력 전원 및 출력 전원을 OFF로 하십시오.

1 M12 토크 핸들을 M12 어태치먼트의 조임 구멍에 삽입하십시오. 커넥터를 분리할 때는 연결할 때와 반대 방향이 되도록 M12 어태치먼트를 거꾸로 배치하십시오.



AI 번역본
For Reference Only

2 M12 어태치먼트를 I/O 케이블의 M12 나사 커넥터에 장착하십시오. M12 어태치먼트를 장착한 후, 다음 그림에 표시된 방향으로 M12 토크 핸들을 돌려 M12 나사 커넥터를 푸십시오.



3 케이블을 분리하려면 I/O 케이블의 M12 나사 커넥터를 연결 방향과 반대 방향으로 돌리십시오.

조임 토크

I/O 케이블의 M12 나사 커넥터를 다음 토크로 조이십시오.
나사 커넥터를 적절한 조임 토크로 조이면 IP67 보호 구조를 유지할 수 있습니다.

조임 위치	나사 크기	조임 토크
I/O 커넥터	M12	0.5~0.6 N · m*1

***1.** Smartclick 커넥터 타입의 경우 토크 관리가 필요하지 않습니다. 커넥터를 끝까지 삽입한 다음 약 1/8 회전만큼 돌리십시오.

방수 커버

사용하지 않는 I/O 커넥터에는 5-38페이지의 5-5-4 커넥터용 방수 커버에 표시된 방수 커버를 장착하십시오.

AI 번역본
For Reference Only

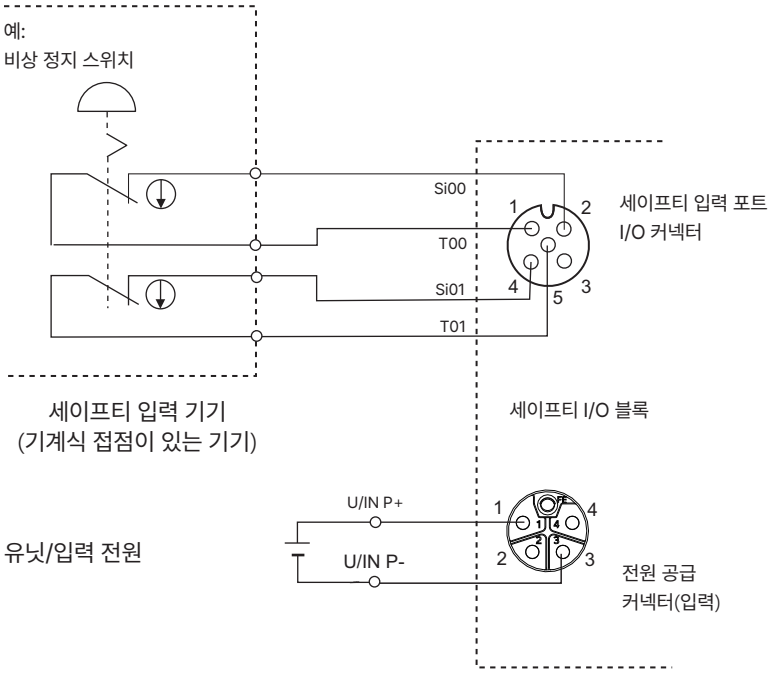
5-4-3 배선 예

세이프티 I/O 블록의 I/O 커넥터와 접속되는 외부 기기 간의 배선 예를 아래에 제공합니다.

- 세이프티 입력 기기(기계식 접점이 있는 기기)
- 세이프티 입력 기기(반도체 출력이 있는 기기)
- 세이프티 입력 기기(세이프티 라이트 커튼)
- 세이프티 출력 기기
- DC 차단 박스(S8R-BB 시리즈)
- 유닛 간 I/O 케이블 연결

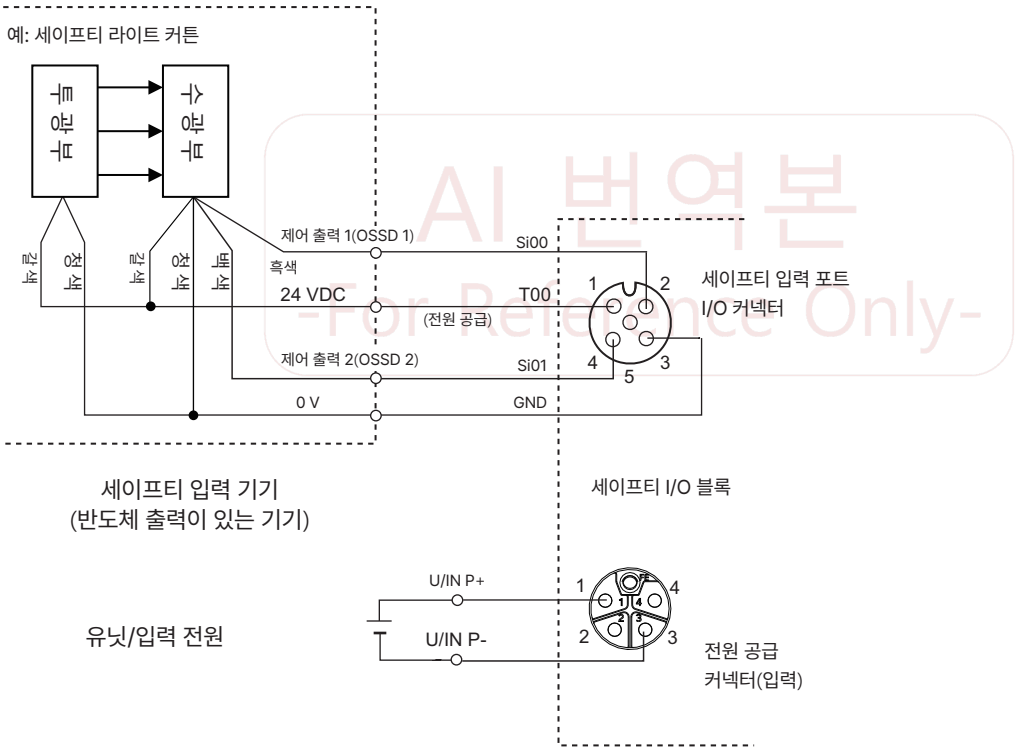
세이프티 입력 기기(기계식 접점이 있는 기기)

다음 그림은 비상 정지 스위치, 세이프티 리밋 스위치 또는 기계식 접점이 있는 기타 세이프티 입력 기기와 세이프티 I/O 블록 간의 배선 예를 나타냅니다.



세이프티 입력 기기(반도체 출력이 있는 기기)

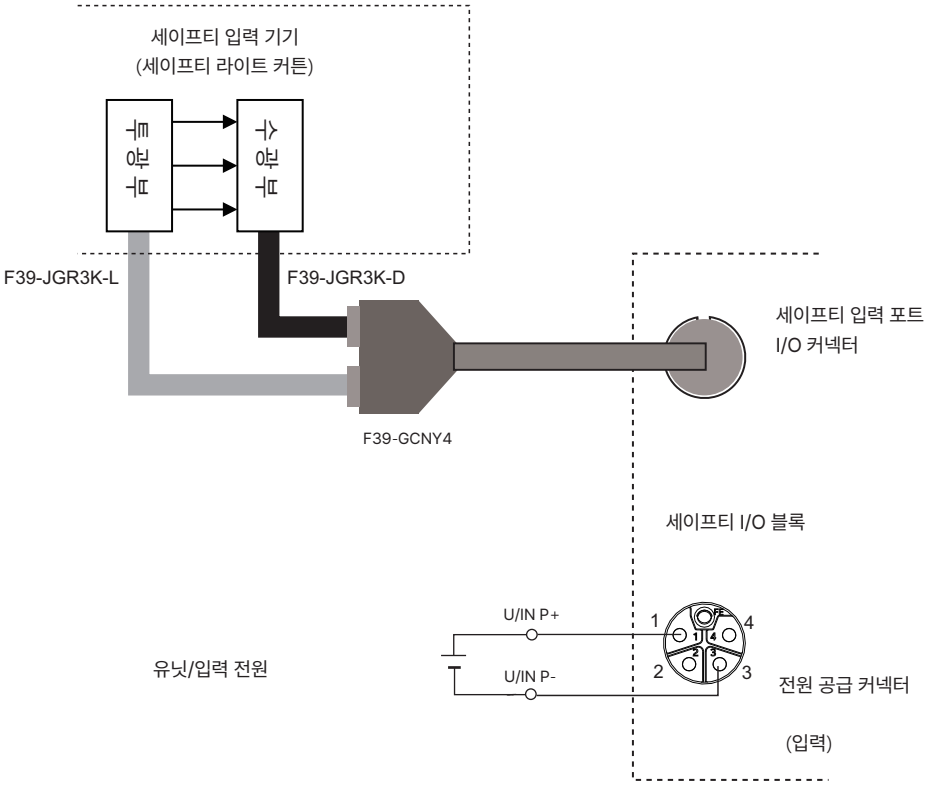
다음은 라이트 커튼 또는 반도체 출력이 있는 기타 세이프티 입력 기기와 세이프티 I/O 블록 간의 배선 예를 나타냅니다.



AI 번역본
-For Reference Only-

세이프티 입력 기기(세이프티 라이트 커튼)

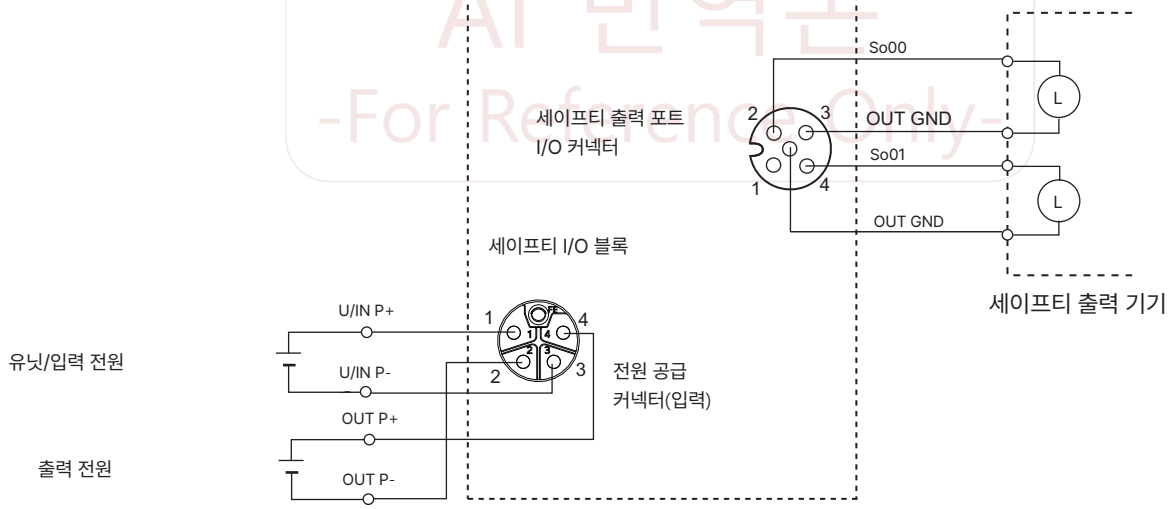
다음 그림은 F39-GCNY4를 사용하여 라이트 커튼과 연결할 때의 배선 예를 나타냅니다.



세이프티 출력 기기

다음 그림은 세이프티 릴레이 또는 기타 세이프티 출력 기기와 세이프티 I/O 블록 간의 배선 예를 나타냅니다.
출력은 PNP 출력입니다.

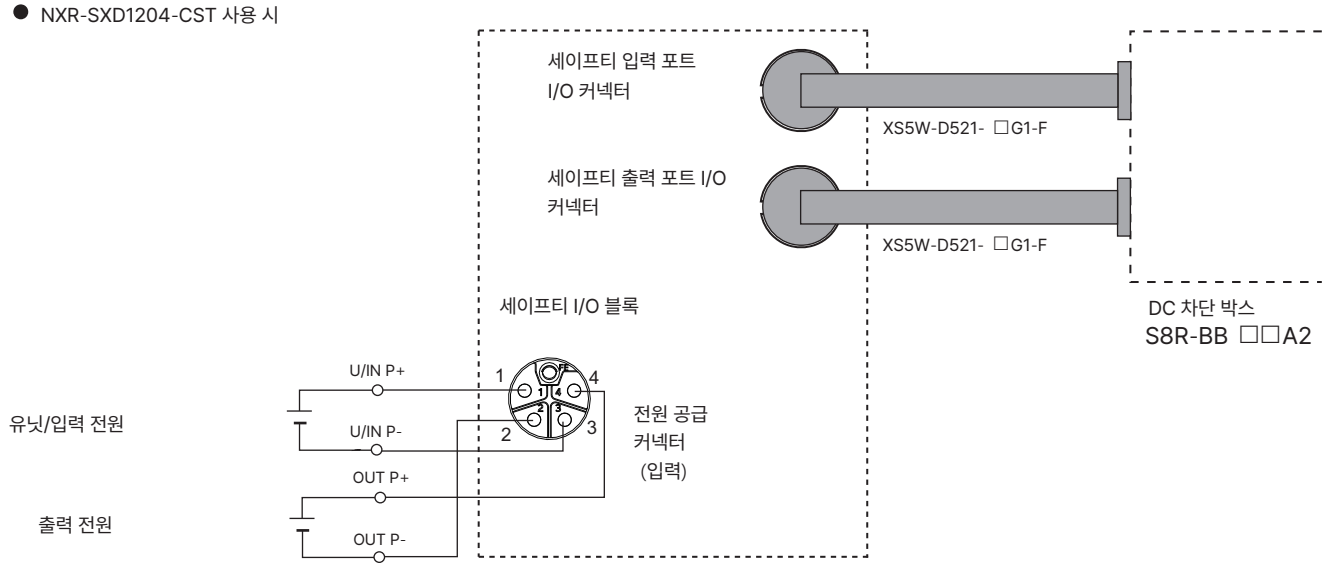
AI 번역본
-For Reference Only-



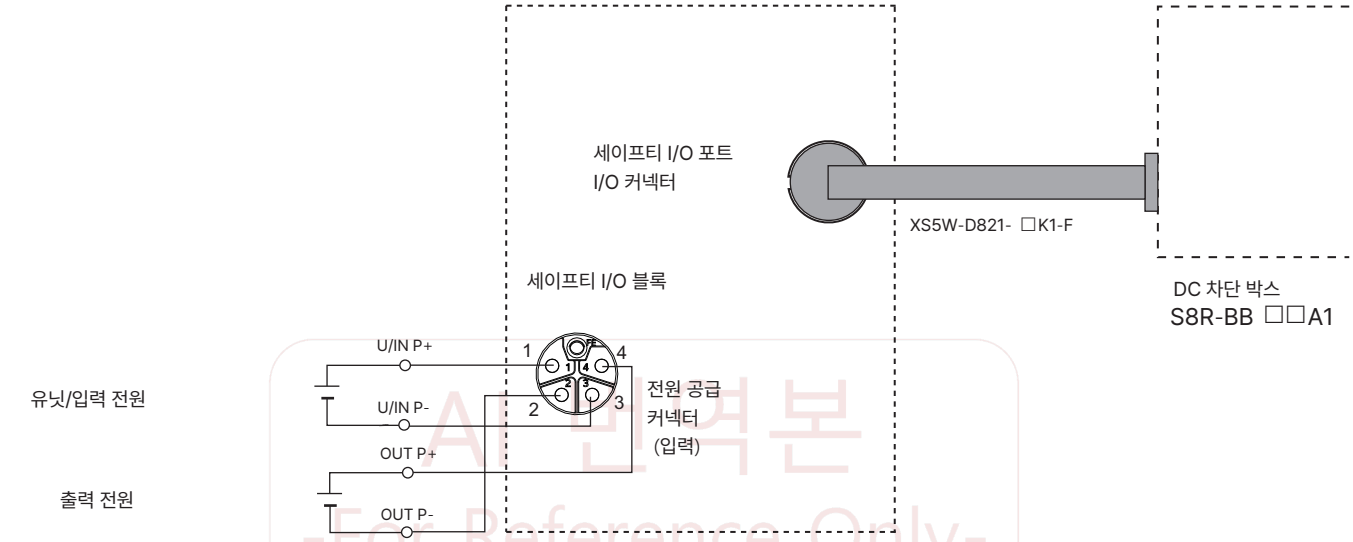
DC 차단 박스(S8R-BB 시리즈)

다음 그림은 DC 차단 박스(S8R-BB 시리즈)와 세이프티 I/O 블록 간의 배선 예를 나타냅니다. 통신 케이블을 연결하기 전에 세이프티 I/O 블록의 유닛/입력 전원 및 출력 전원과, 유닛과 통신하는 기기의 전원을 OFF로 하십시오.

● NXR-SXD1204-CST 사용 시



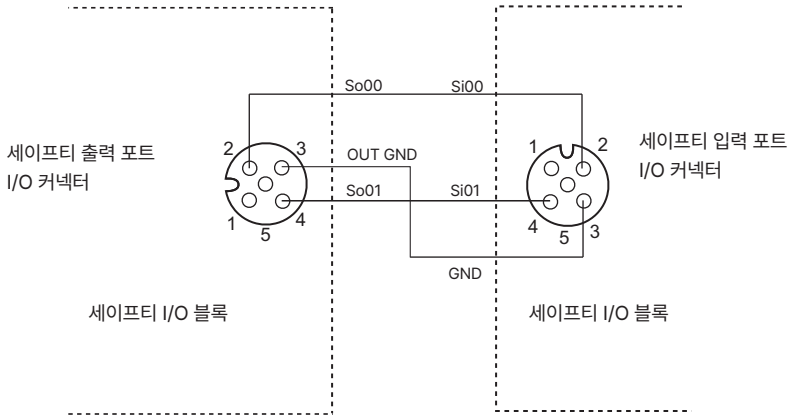
● NXR-SXD1204B-CST 사용 시



A 번역본
-For Reference Only-

유닛 간 I/O 케이블 연결

다음 그림은 유닛 간 세이프티 I/O 포트를 연결할 때의 배선 예를 나타냅니다.



사용상의 주의

- 유닛 간 I/O 케이블을 연결할 때는 5번 핀을 연결하지 마십시오. 세이프티 입력 포트의 테스트 출력과 세이프티 출력 포트의 출력 전원 - 사이에 단락이 발생하여 테스트 출력 단자에서 과전류 이상이 발생합니다.
- 유닛 간 5핀 I/O 케이블을 연결할 때는 세이프티 입력 단자 설정에서 테스트 출력 모드를 Not Used로 설정하십시오.

AI 번역본
-For Reference Only-

5-5 접속 기기

이 절에서는 세이프티 I/O 블록의 배선에 사용되는 접속 관련 기기를 소개합니다.

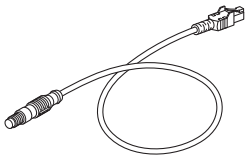
5-5-1 이더넷 케이블

이 절에서는 세이프티 I/O 블록과 함께 사용하는 이더넷 케이블을 소개합니다.
다음과 같은 커넥터가 있습니다.

- Smartclick 커넥터
- 나사 커넥터

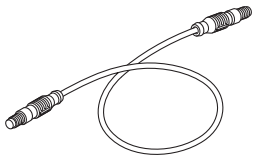
AI 번역본
-For Reference Only-

● 세이프티 I/O 블록과 EtherNet/IP 타겟 간 접속 케이블 RJ45 커넥터

명칭 및 외관	제조사	사양	케이블 도체수	사용 가능 커넥터	케이블 연결방향	케이블 길이	모델
케이블 부착형 산업용 이더넷 커넥터 	오므론 코퍼레이션	M12 플러그 (D-coding, 수형)에서 RJ45로	4	스마트 클릭 커넥터	스트레이트/ 스트레이트	0.5 m	XS5W-T421-BMC-SS
						1 m	XS5W-T421-CMC-SS
						2 m	XS5W-T421-DMC-SS
						3 m	XS5W-T421-EMC-SS
						5 m	XS5W-T421-GMC-SS
						10 m	XS5W-T421-JMC-SS
				나사 커넥터		0.5 m	XS2W-T421-BMC-SS
						1 m	XS2W-T421-CMC-SS
						2 m	XS2W-T421-DMC-SS
						3 m	XS2W-T421-EMC-SS
						5 m	XS2W-T421-GMC-SS
						10 m	XS2W-T421-JMC-SS

AI 번역본
-For Reference Only-

● 세이프티 I/O 블록 간 접속 케이블

명칭 및 외관	제조사	사양	케이블 도체수	사용 가능 커넥터	케이블 연결방향	케이블 길이	모델
산업용 이더넷 커넥터 (케이블 부착형) 	오므론 코퍼레이션	M12 플러그(D-coding, 수형)에서 M12 플러그(D-coding, 수형)로	4	스마트 클릭 커넥터	스트레이트/스트레이트	0.5 m	XS5W-T421-BM2-SS
						1 m	XS5W-T421-CM2-SS
						2 m	XS5W-T421-DM2-SS
						3 m	XS5W-T421-EM2-SS
						5 m	XS5W-T421-GM2-SS
						10 m	XS5W-T421-JM2-SS
				나사 커넥터		0.5 m	XS2W-T421-BM2-SS
						1 m	XS2W-T421-CM2-SS
						2 m	XS2W-T421-DM2-SS
						3 m	XS2W-T421-EM2-SS
						5 m	XS2W-T421-GM2-SS
						10 m	XS2W-T421-JM2-SS

AI 번역본
-For Reference Only-

5-5-2 전원 공급 케이블

이 절에서는 세이프티 I/O 블록과 함께 사용하는 전원 공급 케이블을 나타냅니다. 다음과 같은 커넥터가 있습니다.

・나사 커넥터

・Smartclick 커넥터

● 나사 커넥터

이 절에서는 나사 커넥터가 있는 전원 공급 케이블을 나타냅니다.

명칭 및 외관	제조사	사양	케이블 도체수	사용 가능 커넥터	케이블 연결방향	케이블 길이	모델
M12 L-coding 전원 공급 케이블(M12 스트레이트 암형-개별 전선)	오므론 코퍼레이션	M12 소켓(L-coding, 암형)-개별 전선	5	나사 커넥터	스트레이트	2 m	XS2FP-L521-0200
						5 m	XS2FP-L521-0500
						10 m	XS2FP-L521-1000
	Murrelektronik GmbH	M12 소켓(L-coding, 암형)-개별 전선	5	나사 커넥터	스트레이트	2 m	7000-P4221-P040200
						5 m	7000-P4221-P040500
						10 m	7000-P4221-P041000
M12 L-coding 전원 공급 케이블(M12 스트레이트 수형-M12 스트레이트 암형)	오므론 코퍼레이션	M12 플러그(L-coding, 수형)-M12 소켓(L-coding, 암형)	5	나사 커넥터	스트레이트/스트레이트	2 m	XS2WP-L521-0200
						5 m	XS2WP-L521-0500
						10 m	XS2WP-L521-1000
	Murrelektronik GmbH	M12 플러그(L-coding, 수형)-M12 소켓(L-coding, 암형)	5	나사 커넥터	스트레이트/스트레이트	2 m	7000-P4241-P040200
						5 m	7000-P4241-P040500
						10 m	7000-P4241-P041000

● Smartclick 커넥터 유형

이 절에서는 Smartclick 커넥터가 있는 전원 공급 케이블을 나타냅니다. XS5F-L521-□12-F and XS5W-L521-□12-F is IP65.

AI 번역본
-For Reference Only-

명칭 및 외관	제조사	사양	케이블 도체수	사용 가능 커넥터	케이블 연결방향	케이블 길이	모델
M12 L-coding 전원 공급 케이블(M12 스트레이트 암형-개별 전선) 	오므론 코퍼레이션	M12 소켓 (L-coding, 암형) -개별 전선	5	스마트 클릭 커넥터	스트레이트	0.5 m	XS5F-L521-B12-F
						1 m	XS5F-L521-C12-F
						2 m	XS5F-L521-D12-F
						3 m	XS5F-L521-E12-F
						5 m	XS5F-L521-G12-F
						10 m	XS5F-L521-J12-F
						15 m	XS5F-L521-K12-F
						20 m	XS5F-L521-L12-F

AI 번역본
-For Reference Only-

명칭 및 외관	제조사	사양	케이블 도체수	사용 가능 커넥터	케이블 연결방향	케이블 길이	모델
M12 L-coding 전원 공급 케이블(M12 스트레이트 수형-M12 스트레이트 암형) 	오므론 코퍼레이션	M12 플러그(L-coding, 수형)- M12 소켓 (L-coding, 암형)	5	스마트 클릭 커넥터	스트레이트/ 스트레이트	0.5 m	XS5W-L521-B12-F
						1 m	XS5W-L521-C12-F
						2 m	XS5W-L521-D12-F
						3 m	XS5W-L521-E12-F
						5 m	XS5W-L521-G12-F
						10 m	XS5W-L521-J12-F
						15 m	XS5W-L521-K12-F
						20 m	XS5W-L521-L12-F

5-5-3 I/O 케이블

이 절에서는 세이프티 I/O 블록과 함께 사용하는 I/O 케이블을 나타냅니다.

AI 번역본
-For Reference Only-

직접 연결 또는 연장 연결 케이블

이 케이블은 M12 플러그가 있는 기기에 직접 연결하는 데 사용할 수 있습니다. 또한 M12 플러그가 있는 기기 또는 외부 기기에서 연장 연결하는 데도 사용할 수 있습니다.
다음과 같은 커넥터가 있습니다.

- Smartclick 커넥터
- 나사 커넥터

● Smartclick 커넥터 유형

이 절에서는 Smartclick 커넥터가 있는 I/O 케이블을 나타냅니다.

명칭 및 외관	제조사	사양	케이블 도체수	사용 가능 커넥터	케이블 연결방향	케이블 길이	모델
XS5W 케이블 부착 커넥터 (M12 소켓/M12 플러그) 	오므론 코퍼레이션	M12 소켓 (A-coding, 암형)- M12 플러그(A-coding, 수형), DC 사용	5	스마트 클릭 커넥터	스트레이트/ 스트레이트	0.5 m	XS5W-D521-BG1-F
						1 m	XS5W-D521-CG1-F
						2 m	XS5W-D521-DG1-F
						3 m	XS5W-D521-EG1-F
						5 m	XS5W-D521-GG1-F
						10 m	XS5W-D521-JG1-F
						15 m	XS5W-D521-KG1-F
						20 m	XS5W-D521-LG1-F
XS5H 케이블 부착 커넥터 (M12 플러그/개별 전선) 	오므론 코퍼레이션	M12 플러그(A-coding, 수형), 개별 전선	5	스마트 클릭 커넥터	스트레이트	0.5 m	XS5H-D521-BG0-F
						1 m	XS5H-D521-CG0-F
						2 m	XS5H-D521-DG0-F
						3 m	XS5H-D521-EG0-F
						5 m	XS5H-D521-GG0-F

AI 번역본
-For Reference Only-

명칭 및 외관	제조사	사양	케이블 도체수	사용 가능 커넥터	케이블 연결방향	케이블 길이	모델
세이프티 라이트 커튼 Y분기 플러그/소켓, 양쪽 끝에 커넥터가 있는 케이블(세이프티 I/O 블록용) 	오므론 코퍼레이션	M12 플러그(A-coding, 수형), M12 소켓(A-coding, 암형, 5선) / M12 소켓(A-coding, 암형, 8선)	5~5/8	스마트 클릭 커넥터	스트레이트/스트레이트	0.5 m	F39-GCNY4
XS5W 케이블 부착 커넥터(M12 소켓/M12 플러그), NXR-SXD1204B-CST용 	오므론 코퍼레이션	M12 소켓(A-coding, 암형)- M12 플러그(A-coding, 수형)	8	스마트 클릭 커넥터	스트레이트/스트레이트	0.5 m	XS5W-D821-BK1-F
						1 m	XS5W-D821-CK1-F
						2 m	XS5W-D821-DK1-F
						3 m	XS5W-D821-EK1-F
						5 m	XS5W-D821-GK1-F
						10 m	XS5W-D821-JK1-F
						15 m	XS5W-D821-KK1-F
						20 m	XS5W-D821-LK1-F

AI 번역본
-For Reference Only-

명칭 및 외관	제조사	사양	케이블 도체수	사용 가능 커넥터	케이블 연결방향	케이블 길이	모델
XS5H 케이블 부착 커넥터(M12 플러그/개별 전선), NXR-SXD1204B-CST용 	오므론 코퍼레이션	M12 플러그(A-coding, 수형), 개별 전선	8	스마트 클릭 커넥터	스트레이트	0.5 m	XS5H-D821-BK0-F
						1 m	XS5H-D821-CK0-F
						2 m	XS5H-D821-DK0-F
						3 m	XS5H-D821-EK0-F
						5 m	XS5H-D821-GK0-F

● 나사 커넥터

이 절에서는 나사 커넥터가 있는 I/O 케이블을 나타냅니다.

명칭 및 외관	제조사	사양	케이블 도체수	사용 가능 커넥터	케이블 연결방향	케이블 길이	모델
XS2W 케이블 부착 커넥터 (M12 소켓/M12 플러그) 	오므론 코퍼레이션	M12 소켓(A-coding, 암형) -M12 플러그(A-coding, 수형), DC 사용	5	나사 커넥터	스트레이트/스트레이트	2 m	XS2W-D521-DG1-A
						5 m	XS2W-D521-GG1-A
			8			2 m	XS2W-D821-DH1-C
						5 m	XS2W-D821-GH1-C

AI 번역본
-For Reference Only-

명칭 및 외관	제조사	사양	케이블 도체수	사용 가능 커넥터	케이블 연결방향	케이블 길이	모델
XS2H 케이블 부착 커넥터 (M12 플러그/개별 전선) 	오므론 코퍼레이션	M12 플러그(A-coding, 수형), 개별 전선	5	나사 커넥터	스트레이트	0.3 m	XS2H-D521-AG0-A
						0.5 m	XS2H-D521-BG0-A
						1 m	XS2H-D521-CG0-A
						2 m	XS2H-D521-DG0-A
						5 m	XS2H-D521-GG0-A
			8			0.3 m	XS2H-D821-AH0-C
						1 m	XS2H-D821-CH0-C

5-5-4 커넥터용 방수 커버

이것은 사용하지 않는 M12 커넥터용 방수 커버입니다.
이 방수 커버를 사용하면 IP67 보호 구조를 유지할 수 있습니다. 다음과 같은 방수 커버가 있습니다.

명칭 및 외관	제조사	사양	사용 가능 커넥터	모델
M12 방수 커버 	OMRON Corporation	· M12 A-coding · M12 D-coding · M12 L-coding	Smartclick 커넥터	XS5Z-12

AI 번역본
-For Reference Only-

5-6 옵션

이 절에서는 세이프티 I/O 블록의 옵션에 대한 개요를 설명합니다.

5-6-1 마커

다음의 오므론 제품이 아닌 마커를 유닛 식별 마커 및 I/O 식별 마커로 사용할 수 있습니다. 마커는 프린터로도 인쇄할 수 있습니다.

명칭 및 외관	제조사	사양	모델
마커 	Phoenix Contact	백색 17.5 mm × 7.5 mm	0825495

AI 번역본
-For Reference Only-

AI 번역본
-For Reference Only-

6

세이프티 I/O 블록의 동작

이 장에서는 세이프티 I/O 블록의 다양한 동작에 대해 설명합니다.

6-1 동작 개요 6-2

6-2 CIP Safety 통신 6-4

6-3 EtherNet/IP 통신 6-6

6-3-1 태그 데이터 링크 통신 6-6

6-3-2 익스플리시트 메시지 통신 6-6

6-4 세이프티 입력 기능 6-8

6-4-1 접속 가능 기기 6-8

6-4-2 테스트 출력 기능 6-10

6-4-3 테스트 펄스 평가 기능 6-10

6-4-4 듀얼 채널 평가 6-11

6-4-5 세이프티 입력 단자의 진단 기능으로 검출 가능한 에러 6-12

6-4-6 입력 필터 기능 6-13

6-4-7 입력 에러 래치 시간 6-15

6-5 세이프티 출력 기능 6-16

6-5-1 접속 가능 기기 6-16

6-5-2 테스트 펄스 평가 기능 6-16

6-5-3 듀얼 채널 평가 6-17

6-5-4 세이프티 출력 단자의 진단 기능으로 검출 가능한 에러 6-18

6-5-5 출력 에러 래치 시간 6-18

6-5-6 EDM 피드백 6-19

6-5-7 출력 지연 6-19

6-6 로직 기능 6-20

6-6-1 논리 처리 6-20

6-7 세이프티 애플리케이션 6-23

6-7-1 세이프티 애플리케이션의 목적 6-23

6-7-2 세이프티 애플리케이션의 종류 6-23

6-7-3 고정 애플리케이션 상세 6-27

6-8 운전 모드 6-47

6-8-1 운전 모드 종류 6-47

6-8-2 각 운전 모드에서 실행 가능한 기능 6-48

6-8-3 각 운전 모드에서 실행 가능한 Web UI 기능 6-50

6-8-4 운전 모드 전환 및 전원 투입 시 모드 6-51

-For Reference Only-

6-1 동작 개요

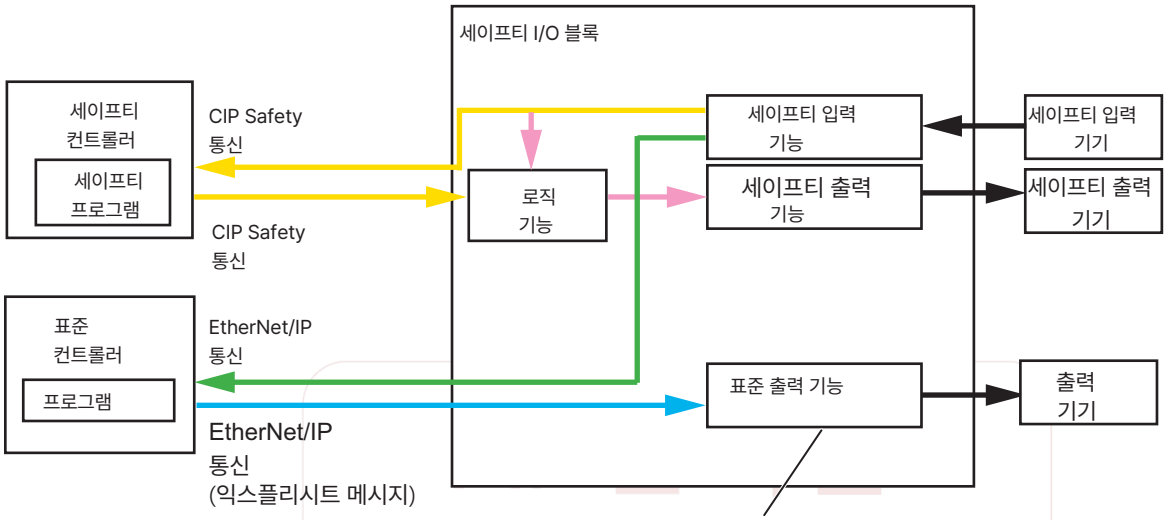
세이프티 I/O 블록의 주요 동작은 다음 기능의 조합으로 수행됩니다.

기능	설명
CIP Safety 통신	세이프티 컨트롤러(CIP Safety 오리지네이터)와 세이프티 I/O 블록(CIP Safety 타겟) 간에 수행되는 통신
EtherNet/IP 통신	표준 컨트롤러(EtherNet/IP 오리지네이터)와 세이프티 I/O 블록(EtherNet/IP 타겟) 간에 수행되는 통신
세이프티 입력 기능	세이프티 I/O 블록은 세이프티 입력 기기로부터 세이프티 입력 데이터를 취득합니다.
세이프티 출력 기능	세이프티 I/O 블록은 세이프티 출력 기기로 세이프티 출력 데이터를 출력합니다.
로직 기능	세이프티 I/O 블록 내부에서 세이프티 입력 데이터에 대해 실행되는 처리입니다. 처리 결과는 세이프티 출력 데이터로서 세이프티 출력 기능에 전달됩니다.

다음은 이들 기능과 세이프티 I/O
블록의 주변기기 간의 관계를 나타냅니다.

- 세이프티 I/O 블록 내부의 로직 기능은 세이프티 입력 기능으로부터 취득한 세이프티 입력 데이터를 로직 설정에 따라 처리한 후, 그 결과를 세이프티 출력 기능에 전달합니다.
- 또한 세이프티 컨트롤러로부터 전송되는 세이프티 출력 데이터를 로직 기능과 결합할 수도 있습니다.

- 또한 세이프티 입력 기능으로부터 취득한 세이프티 입력 데이터는 표준 컨트롤러에 의해 처리되며, 그 결과를 표준 출력 기능에 전달할 수도 있습니다.

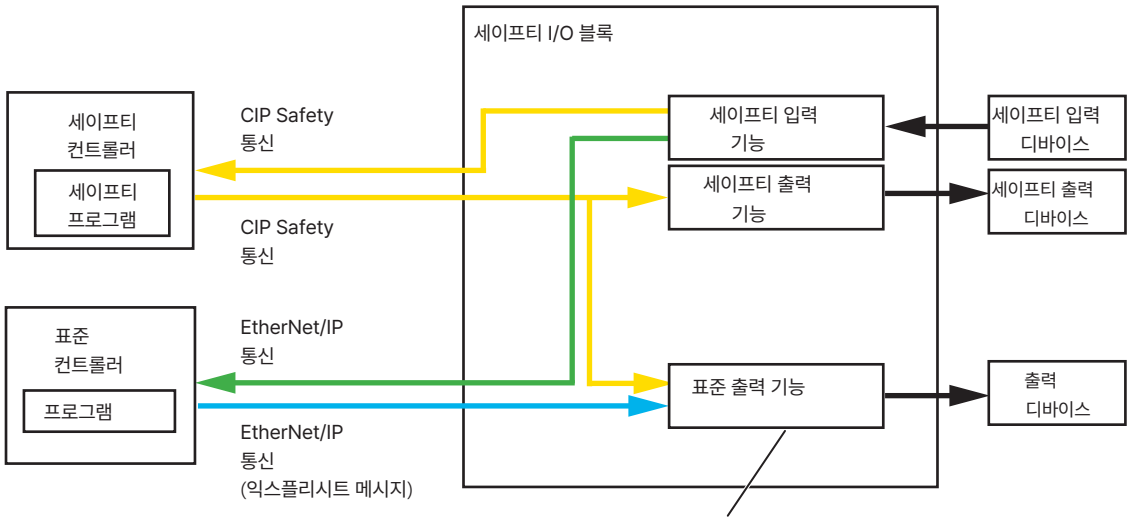


-For Reference Only-

로직 기능을 사용하지 않는 경우, 동작은 아래 그림과 같습니다.

- 세이프티 컨트롤러는 세이프티 입력 기능으로부터 취득한 데이터를 처리한 후, 그 결과를 세이프티 출력 기능에 전달합니다.
- 또한 세이프티 컨트롤러로부터 전송되는 세이프티 출력 데이터를 표준 출력 기능에 전달할 수도 있습니다.

- 또한 세이프티 입력 기능으로부터 취득한 세이프티 입력 데이터는 표준 컨트롤러에 의해 처리되며, 그 결과를 표준 출력 기능에 전달할 수도 있습니다.

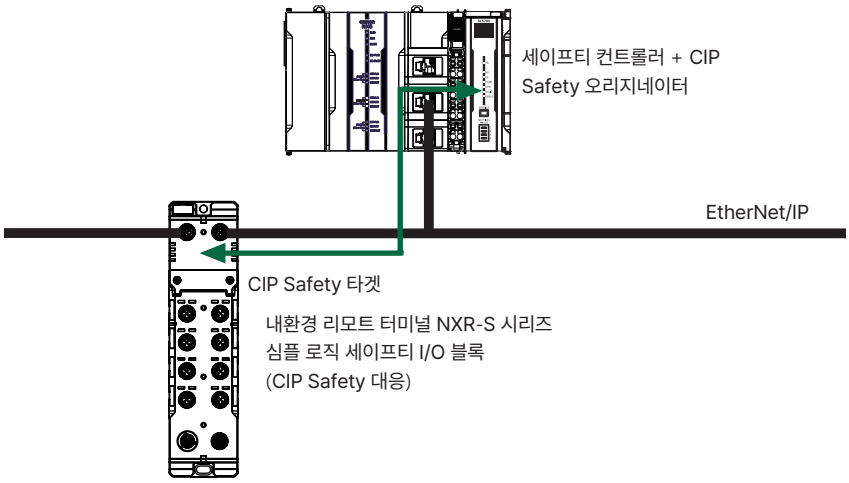


세이프티 I/O 블록의 테스트 출력 단자에 대한 테스트 출력 모드가 "Standard Output"으로 설정되어 있으면, 테스트 출력 단자를 표준 출력으로 사용할 수 있습니다.

AI 번역본
-For Reference Only-

6-2 CIP Safety 통신

CIP Safety 통신은 EtherNet/IP 네트워크상의 CIP Safety 디바이스 간에
EtherNet/IP를 통한 CIP Safety를 사용하는 통신입니다.
CIP Safety 커넥션의 확립을 요청하는 노드를 CIP Safety 오리지네이터라고 하며, 요청을 수신하는
노드를 CIP Safety 타겟이라고 합니다. 세이프티 I/O 블록은 CIP Safety 타겟 기능만
지원합니다.



CIP Safety 커넥션이 확립되면 CIP Safety 오리지네이터와 CIP Safety 타겟 간에 세이프티 I/O
데이터가 주기적으로 교환됩니다.
이를 통해 세이프티 I/O 블록의 세이프티 입력 상태를 상위 세이프티 컨트롤러로 전송하고,
세이프티 컨트롤러로부터 세이프티 출력 데이터를 수신할 수 있습니다.

CIP Safety 커넥션 설정 파라미터

CIP Safety 커넥션에는 다음 설정 파라미터가 있습니다.

● 오픈 타입

오픈 타입은 CIP Safety 커넥션의 오픈 요청 방식을 나타내는 설정입니다.
이 오픈 타입은 CIP Safety 오리지네이터가 세이프티 I/O 블록에 CIP Safety 커넥션의
오픈을 요청할 때 지정할 수 있습니다.
사용 가능한 오픈 타입은 다음과 같습니다.

사내 배포용
-For Reference Only-

오픈 타입	설명
Configure Target Device (Type 1)	커넥션 확립 시 세이프티 I/O 블록을 구성합니다.
Check Safety Signature (Type 2a)	세이프티 시그니처를 사용하여 커넥션을 확립할 때 세이프티 I/O 블록이 올바르게 구성되어 있는지 확인합니다. 세이프티 시그니처는 Safety Configuration CRC와 Safety Configuration Time Stamp로 구성됩니다.
Open Only (Type 2b)	커넥션을 확립할 때 세이프티 I/O 블록의 구성 확인이 수행되지 않습니다.

⚠ 경고

오픈 타입을 Open Only로 설정한 경우, 사용하기 전에 오리지네이터와 타겟이 올바르게 구성되어 있는지 반드시 확인하십시오.
필요한 세이프티 기능의 상실로 인해 중상을 입을 수 있습니다.

● 커넥션 타입

CIP Safety 커넥션 설정에서는 커넥션 타입으로 멀티캐스트 커넥션 또는 싱글캐스트(포인트 투 포인트) 커넥션을 선택할 수 있습니다.
멀티캐스트 커넥션을 사용하면 하나의 입력 어셈블리를 하나의 패킷으로 여러 오리지네이터 디바이스에 전송할 수 있습니다. 이에 비해 싱글캐스트 커넥션을 사용하면 하나의 입력 어셈블리를 각 오리지네이터 디바이스에 개별적으로 전송할 수 있습니다.
따라서 하나의 입력 어셈블리를 여러 오리지네이터 디바이스에 전송할 때는 멀티캐스트 커넥션을 사용하여 통신 부하를 줄일 수 있습니다.
단, 멀티캐스트 커넥션을 사용하여 하나의 입력 어셈블리를 하나의 패킷으로 여러 오리지네이터 디바이스에 전송하는 경우는, 이를 수신하는 각 커넥션의 커넥션 타입이 모두 멀티캐스트 커넥션이고, 커넥션 I/O 타입, 예상 패킷 간격(EPI), 타임아웃 값이 모두 동일한 경우에만 허용됩니다.

사용상의 주의

단, 멀티캐스트 커넥션을 사용하는 경우, 네트워크 내의 모든 노드가 패킷을 수신하는 경우가 아니라면 멀티캐스트 필터링 기능이 있는 이더넷 스위치를 사용하십시오.
멀티캐스트 필터링 기능이 없는 이더넷 스위치를 사용하면 멀티캐스트 패킷이 전체 네트워크에 브로드캐스트되어, 수신이 필요하지 않은 노드에도 패킷이 전송되므로 해당 노드의 통신 부하가 증가하게 됩니다.

● 예상 패킷 간격(EPI)

예상 패킷 간격(EPI)이란 CIP Safety 통신에서 이더넷 회선상의 I/O 데이터 갱신 주기입니다. EtherNet/IP에서는 노드 수와 관계없이 각 커넥션에 설정된 EPI로 통신 회선상에서 데이터가 교환됩니다.
내장 EtherNet/IP 포트를 사용하면 커넥션별로 EPI를 설정할 수 있습니다.

사용상의 주의

통신 기기의 성능은 각 제품 사양의 한계로 인해 어느 정도 제한됩니다.
따라서 예상 패킷 간격(EPI)을 무제한으로 설정할 수 없습니다.
자세한 내용은 NX-시리즈 세이프티 컨트롤 유닛/커뮤니케이션 컨트롤 유닛 유저 매뉴얼(자료 번호 Z395)을 참조한 후, 적절한 예상 패킷 간격(EPI)을 설정하십시오.

● I/O 어셈블리

I/O 어셈블리는 오리지네이터와 타겟 간에 주기적으로 교환되는 I/O 데이터의 단위입니다.
세이프티 I/O 블록에는 여러 I/O 어셈블리가 정의되어 제공됩니다. 정의된 I/O 어셈블리 중에서 선택하여 커넥션당 하나의 I/O 어셈블리를 설정합니다.
세이프티 I/O 블록과 CIP Safety 오리지네이터 간에 설정 가능한 I/O 어셈블리는 다음과 같습니다.

- 입력 커넥션: 25C hex(2바이트), 3C0 hex(5바이트), 3C1 hex(9바이트)
- 출력 커넥션: 없음

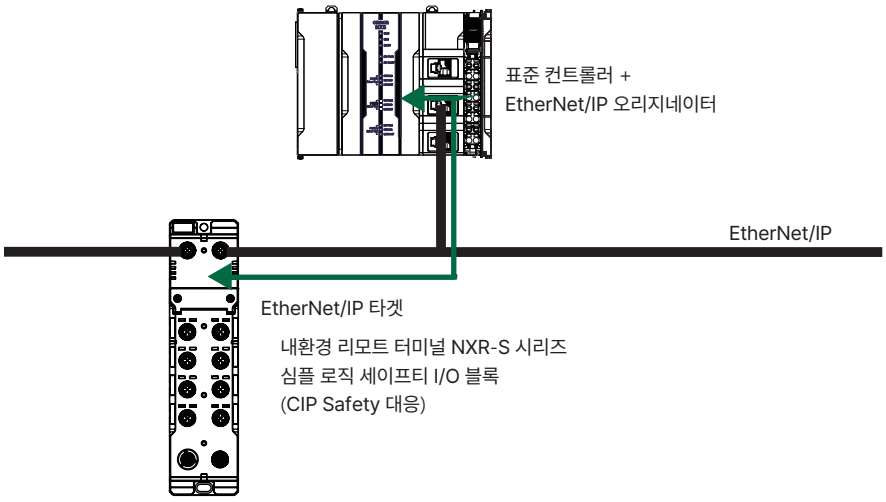
I/O 어셈블리 데이터에 대한 자세한 내용은 A-4페이지의 A-2 세이프티 I/O 어셈블리 데이터를 참조하십시오.

6-3 EtherNet/IP 통신

EtherNet/IP 통신은 EtherNet/IP 네트워크상의 디바이스 간에 데이터를 교환하기 위한 것입니다. 통신 방식으로는 태그 데이터 링크 통신과 익스플리시트 메시지 통신을 사용할 수 있습니다.

6-3-1 태그 데이터 링크 통신

태그 데이터 링크 통신이란 EtherNet/IP 네트워크상의 디바이스 간에 I/O 데이터를 주기적으로 교환하는 통신입니다.
태그 데이터 링크 통신에서는 한 노드가 다른 노드와 I/O 데이터를 교환하기 위해 통신 회선의 커넥션(오픈)을 요청합니다.
태그 데이터 링크 통신 커넥션의 확립을 요청하는 노드를 EtherNet/IP 오리지네이터라고 하며, 요청을 수신하는 노드를 EtherNet/IP 타겟이라고 합니다. 세이프티 I/O 블록은 EtherNet/IP 타겟 기능만 지원합니다.



I/O 데이터 교환의 대상이 되는 단위를 태그라고 하며, 데이터는 오리지네이터와 타겟 간에 주기적으로 교환됩니다.
세이프티 I/O 블록에는 여러 I/O 어셈블리가 정의되어 제공됩니다.
I/O 어셈블리 데이터 설정을 포함하여 태그 데이터 링크 통신을 설정하는 방법은 7-38페이지의 「 태그 데이터 링크 통신 설정 순서 」를 참조하십시오.

AI 번역본
For Reference Only

6-3-2 익스플리시트 메시지 통신

익스플리시트 메시지 통신은 EtherNet/IP 네트워크상에서 요청/응답 형식으로 기기의 설정 및 상태를 교환하는 CIP 통신입니다.
통신은 익스플리시트 메시지 서버가 익스플리시트 메시지 클라이언트로부터의 요청에 응답을 보냄으로써 이루어집니다.
세이프티 I/O 블록은 익스플리시트 메시지 서버 기능만 지원합니다.

익스플리시트 메시지 서버 기능

익스플리시트 메시지 서버 기능을 사용하여 익스플리시트 메시지 클라이언트로부터의
익스플리시트 메시지로 세이프티 I/O 블록의 CIP 오브젝트에 액세스하면 다음 작업을 수행할 수 있습니다.

・이벤트 로그 읽기, 이벤트 로그 지우기 등을 통한 세이프티 I/O 블록의 문제 해결

・세이프티 I/O 블록의 디바이스 파라미터 설정, IP 주소 및 기타 통신 파라미터 설정

또한 익스플리시트 메시지 클라이언트 기능을 갖춘 디바이스가 태그 데이터 링크(즉, 임플리시트
메시지) 통신을 지원하지 않는 경우, 세이프티 I/O 블록의 I/O를 제어하는 대체 수단으로
익스플리시트 메시지를 사용할 수 있습니다.
세이프티 I/O 블록이 지원하는 CIP 오브젝트에 대한 자세한 내용은 A-16페이지의 A-4 지원 CIP 오브젝트를
참조하십시오.
익스플리시트 메시지를 통해 세이프티 I/O 블록의 CIP 오브젝트에 액세스하는 방법은 사용 중인 컨트롤러의 매뉴얼을
참조하십시오.

AI 번역본
-For Reference Only-

6-4 세이프티 입력 기능

이 절에서는 세이프티 I/O 블록의 세이프티 입력 기능에 대해 설명합니다.

6-4-1 접속 가능한 디바이스

세이프티 I/O 블록은 세이프티 입력 단자를 통해 접속된 외부 디바이스를 진단합니다.
세이프티 입력 단자에 접속할 수 있는 세이프티 입력 디바이스 및 표준 입력 디바이스는 다음 표에 나와 있습니다.

입력 디바이스 타입	채널 모드			테스트 출력 단자
	듀얼 채널 (등가 입력)	듀얼 채널 (상보 입력)	싱글 채널	테스트 출력 모드
세이프티 입력 디바이스 (기계식 접점을 갖는 디바이스)	· 비상 정지 스위치 (2NC 접점) · 세이프티 도어 스위치 (2NC 접점) · 세이프티 리밋 스위치 (2NC 접점) · 세이프티 키 셀렉터 스위치 (2NC 접점) · 인에이블 스위치 (2NC 접점) · 듀얼 채널 등가 입력용 기계식 접점 (2NC 접점)	· 세이프티 도어 스위치 (1NC/1NO 접점) · 세이프티 리밋 스위치 (1NC/1NO 접점) · 양수 스위치 (1NO/1NC 접점) · 세이프티 키 셀렉터 스위치 (1NC/1NO 접점) · 듀얼 채널 상보 입력용 기계식 접점 (1NC/1NO 접점)	· 비상 정지 스위치 (1NC 접점) · 세이프티 도어 스위치 (1NC 접점) · 세이프티 리밋 스위치 (1NC 접점) · 세이프티 키 셀렉터 스위치 (1NC 접점) · EDM 피드백 (1NC 접점) · 싱글 채널용 기계식 접점 (1NC 접점)	테스트 출력
세이프티 입력 디바이스 (반도체 출력을 갖는 디바이스)	· 세이프티 라이트 커튼 · 세이프티 레이저 스캐너 · 하이코드 도어 스위치 · 하이코드 도어 스위치 (게이트용) · 하이코드 도어 스위치 (가드 록 타입) · 듀얼 채널 등가 입력용 반도체 출력	· 듀얼 채널 상보 입력용 반도체 출력	· 싱글 채널용 반도체 출력	· 전원 공급 · 표준 출력 · 사용 안 함
표준 입력 디바이스	해당 없음	해당 없음	· 테스트 펄스가 있는 리셋 스위치 (1NO 접점)	테스트 출력
	해당 없음	해당 없음	· 테스트 펄스가 없는 리셋 스위치 (1NO 접점)	전원 공급

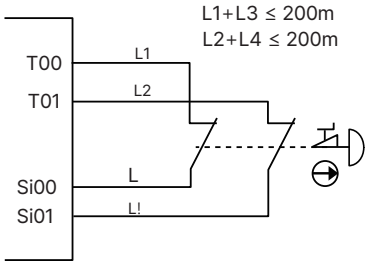
AI 번역본
-For Reference Only-

세이프티 입력 디바이스는 크게 두 가지 타입으로 분류할 수 있습니다.
하나는 기계식 접점을 갖는 디바이스이고, 다른 하나는 반도체 출력을 갖는 디바이스입니다.

● 기계식 접점을 갖는 디바이스

비상 정지 스위치나 세이프티 리밋 스위치와 같은 접점 출력을 갖는 디바이스를 세이프티 입력에 접속합니다.
세이프티 입력(Si)과 테스트 출력(T)을 조합하여 사용합니다.

다음은 듀얼 채널 입력을 사용하는 경우의 접속 예입니다.



세이프티 입력과 테스트 출력의 조합에는 동일한 번호만 사용할 수 있습니다. 위 예에서는 "Si00"과 "T00", "Si01"과 "T01"의 조합을 보여줍니다.
이 경우 "T00"과 "T01"의 테스트 출력 모드 설정은 Test Output이 됩니다.

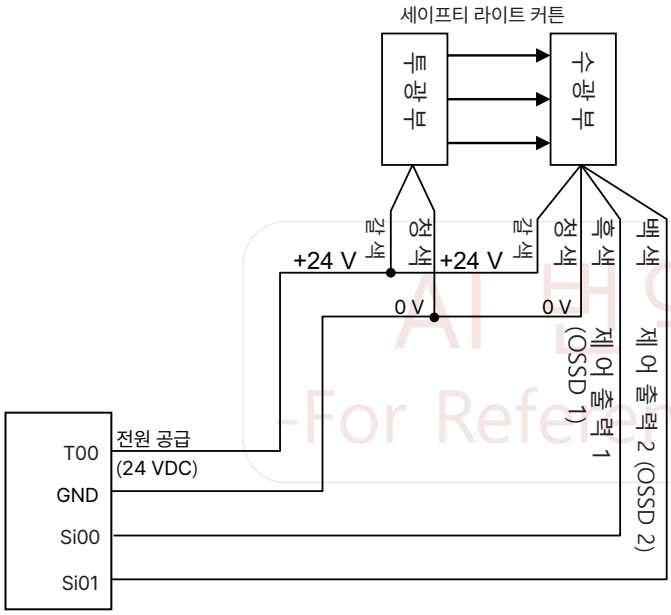
사용상의 주의

하나의 테스트 출력에 접속하는 케이블의 총 길이는 200m 이하여야 합니다.

● 반도체 출력을 갖는 디바이스

라이트 커튼과 같은 반도체 출력을 갖는 디바이스를 세이프티 입력 단자(Si)에 접속합니다. 다음은

듀얼 채널 입력을 사용하는 경우의 접속 예입니다.



AI 번역본
-For Reference Only-

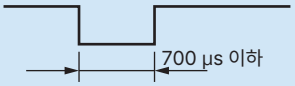
라이트 커튼의 출력을 세이프티 입력의 "Si00"과 "Si01"에 접속하고, "T00" 테스트 출력을 라이트 커튼의 전원 공급으로 사용합니다.
이 경우 "T00"의 테스트 출력 모드 설정은 Power Supply가 됩니다.

사용상의 주의

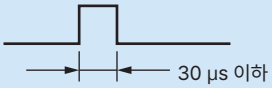
· 라이트 커튼의 전원은 테스트 출력 단자에서 공급됩니다. 테스트 출력에서 공급 가능한 출력 전류는 0.7A/점 이하입니다.

· 세이프티 라이트 커튼과 같은 일부 반도체 출력 디바이스는 배선 오류를 검출하기 위해 펄스를 출력합니다. 반도체 출력을 갖는 디바이스를 세이프티 입력 단자에 접속할 때는 다음 사항을 준수하십시오.

a) 반도체 출력이 ON일 때의 OFF 펄스 폭은 700 µs 이하여야 합니다.



b) 반도체 출력이 OFF일 때의 ON 펄스 폭은 30 µs 이하여야 합니다.



6-4-2 테스트 출력 기능

테스트 출력 단자는 테스트 펄스 평가 시의 테스트 출력(기계식 접점을 갖는 디바이스)이나 반도체 출력을 갖는 디바이스에 대한 전원 공급과 같이 세이프티 입력의 보조 기능으로 동작합니다. 테스트 출력 기능(테스트 출력 단자의 기능)은 다음과 같습니다.

테스트 펄스 유무	테스트 출력 모드	설명
테스트 펄스 있음 (기계식 접점을 갖는 디바이스)	**Test Output**	테스트 출력 단자에서 특정 주기의 테스트 펄스가 있는 24 VDC를 출력합니다. 테스트 펄스 평가에 대한 자세한 내용은 6-10페이지의 6-4-3 테스트 펄스 평가 기능을 참조하십시오.
테스트 펄스 없음 (기계식 접점을 갖는 디바이스)	**Power Supply**	테스트 출력 단자에서 24 VDC를 출력합니다.
테스트 펄스 없음 (반도체 출력을 갖는 디바이스)	**Power Supply**	테스트 출력 단자에서 24 VDC를 출력합니다. 반도체 출력을 갖는 디바이스의 전원 공급으로 사용합니다.
	Standard Output	테스트 출력 단자를 사용하여 컨트롤러로부터의 표준 출력이 가능합니다. *1 비세이프티 디지털 신호 출력 단자로 사용합니다. 예를 들어 표시등이나 PLC의 입력에 접속하여 모니터 출력으로 사용할 수 있습니다. 설정 순서는 7-47페이지의 7-5-2 표준 출력 기능 설정 순서를 참조하십시오.

AI 번역본
-For Reference Only-

***1.** 컨트롤러로부터의 표준 출력 기능은 세이프티 기능이 아닙니다.

테스트 출력 단자에는 과전류를 검출하는 기능도 있습니다. 과전류가 검출되면 이벤트 로그에 기록됩니다. 자세한 내용은 11-12페이지의 11-2-4 이벤트 상세 및 문제 해결을 참조하십시오.

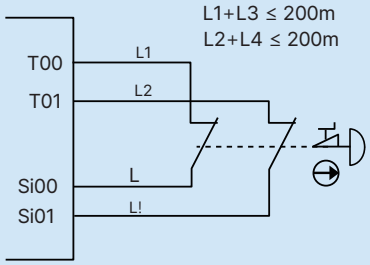
6-4-3 테스트 펄스 평가 기능

테스트 펄스가 있는 경우(기계식 접점을 갖는 디바이스), 외부에 접속된 디바이스의 배선 오류 및 고장을 검출하기 위해 테스트 출력 단자에서 특정 주기의 테스트 펄스가 있는 24 VDC를 출력할 수 있습니다.

테스트 펄스 유무	테스트 출력 모드	설명
테스트 펄스 있음 (기계식 접점을 갖는 디바이스)	**Test Output**	테스트 출력 신호(테스트 펄스)가 기계식 접점을 통해 세이프티 입력 단자에 입력됩니다. 입력 신호선과 전원선(양극 측)의 접촉 및 다른 입력 신호선과의 단락을 검출할 수 있습니다.

사용상의 주의

세이프티 입력 단자와 테스트 출력 단자의 조합에는 동일한 번호만 사용할 수 있습니다. 다음 예는 "Si00"과 "T00", "Si01"과 "T01"의 조합을 보여줍니다.



6-4-4 듀얼 채널 평가

세이프티 입력 단자는 듀얼 채널(이중화)로 사용할 수 있습니다. 듀얼 채널 평가는 두 입력 간 데이터의 불일치 시간을 평가합니다.
불일치 시간이란 한쪽 입력값이 변화한 시점부터 다른 쪽이 변화할 때까지의 시간입니다.
Discrepancy Time에 설정된 시간을 초과했는데도 다른 쪽 입력에 변화가 없으면 에러가 **발생한 것으로 판정됩니다.**

듀얼 채널 평가 기능 설정

입력 디바이스에 대해 듀얼 채널 모드의 디바이스를 선택하고 Discrepancy time을 설정합니다.

다음 표는 설정 내용을 보여줍니다.

설정 데이터명	설명	설정 범위
채널 모드	입력 디바이스에 대해 듀얼 채널 모드의 디바이스를 선택합니다.	다음 중에서 선택합니다. ・듀얼 채널 등가 입력 ・듀얼 채널 상보 입력 채널 모드 및 디바이스에 대한 자세한 내용은 6-8페이지의 6-4-1 접속 가능한 디바이스를 참조하십시오.
Discrepancy time	불일치 시간 *1 인 두 입력 간 데이터를 모니터링합니다. 이 불일치가 이 값을 초과하면 에러가 발생합니다.	10~64,000(ms) 범위의 값을 설정합니다. 5(ms) 단위로 설정합니다. 공장 출하 시 기본값은 500(ms)입니다.

***1.** 불일치 시간이란 한쪽 입력값이 변화한 시점부터 다른 쪽이 변화할 때까지의 시간입니다.

설정 순서는 7-44페이지의 7-5-1 세이프티 입력 기능 설정 순서를 참조하십시오.

-For Reference Only-

세이프티 입력 단자의 입력 신호와 세이프티 입력 데이터의 관계

세이프티 입력 신호와 세이프티 입력 데이터의 관계는 다음과 같습니다.

채널 모드	세이프티 입력 단자의 입력 신호		세이프티 입력 데이터		상태의 의미
	Si (n)	Si (n+1)	Si (n)	Si (n+1)	
듀얼 채널 등가 입력	0	0	0	0*1	비활성(OFF)
	0	1	0	0*1	두 입력 간 데이터 불일치
	1	0	0	0*1	두 입력 간 데이터 불일치
	1	1	1	0*1	활성(ON)
듀얼 채널 상보 입력	0	0	0	0*1	두 입력 간 데이터 불일치
	0	1	0	0*1	비활성(OFF)
	1	0	1	0*1	활성(ON)
	1	1	0	0*1	두 입력 간 데이터 불일치

***1.** 단자가 Dual Channel Mode로 설정된 경우, 짝수 번호 단자의 세이프티 입력 데이터가 세이프티 컨트롤러의 세이프티 프로그램에서 사용됩니다.

6-4-5 세이프티 입력 단자의 진단 기능으로 검출 가능한 에러

세이프티 입력 단자에서 검출 가능한 에러는 파라미터 설정에 따라 결정됩니다.
다음 표는 각 파라미터 설정에서 검출되는 에러를 보여줍니다.

파라미터 설정		에러 검출			
채널 모드	테스트 펄스	전원선과의 접속 (양극 측)	지락 고장*1	단선	입력 배선의 단락
싱글 채널	테스트 펄스 없음 (반도체 출력을 갖는 디바이스)	검출 불가	검출 불가	검출 불가	–
	테스트 펄스 있음 (기계식 접점을 갖는 디바이스)	검출 가능	검출 가능 (입력이 ON될 때)	검출 불가	–
듀얼 채널 (등가 입력)	테스트 펄스 없음 (반도체 출력을 갖는 디바이스)	검출 불가*2	검출 가능 (입력이 ON될 때)	검출 불가*3	검출 불가*2
	테스트 펄스 있음 (기계식 접점을 갖는 디바이스)	검출 가능	검출 가능 (입력이 ON될 때)	검출 불가*3	검출 가능

-For Reference Only-

파라미터 설정		에러 검출			
채널 모드	테스트 펄스	전원선과의 접속 (양극 측)	지락 고장*1	단선	입력 배선의 단락
듀얼 채널 (상보 입력)	테스트 펄스 없음 (반도체 출력을 갖는 디바이스)	검출 가능 (ON→OFF 또는 OFF→ON으로 전환될 때)	검출 가능 (ON→OFF 또는 OFF→ON으로 전환될 때)	검출 가능 (ON→OFF 또는 OFF→ON으로 전환될 때)	검출 가능
	테스트 펄스 있음 (기계식 접점을 갖는 디바이스)	검출 가능	검출 가능 (ON→OFF 또는 OFF→ON으로 전환될 때)	검출 가능 (ON→OFF 또는 OFF→ON으로 전환될 때)	검출 가능

***1.** 지락 고장을 검출하려면 외부 전원의 0V 라인을 접지해야 합니다.
***2.** 라이트 커튼 또는 레이저 스캐너의 OSSD 진단 기능으로 검출할 수 있습니다. 입력이
***3.** ON될 때 신호선 중 하나가 단선된 경우에만 검출할 수 있습니다.

6-4-6 입력 필터 기능

입력 필터 기능은 세이프티 입력 단자에 접속된 외부 디바이스의 채터링이나 노이즈로 인한 오동작을 방지합니다.
외부 디바이스의 채터링이나 노이즈를 걸러내려면 ON->OFF Delay time 또는 OFF->ON Delay time을 설정합니다.

다음 표는 설정 내용을 보여줍니다.

설정 데이터명	설명	설정 범위
ON->OFF Delay time	입력 데이터가 ON에서 OFF로 전환되는 지연 시간입니다.	0~1,600(ms) 범위의 값을 설정합니다. 5(ms) 단위로 설정합니다. 공장 출하 시 기본값은 0(ms)입니다.
OFF->ON Delay time	입력 데이터가 OFF에서 ON으로 전환되는 지연 시간입니다.	0~1,600(ms) 범위의 값을 설정합니다. 5(ms) 단위로 설정합니다. 공장 출하 시 기본값은 0(ms)입니다.

설정 순서는 7-44페이지의 7-5-1 세이프티 입력 기능 설정 순서를 참조하십시오.

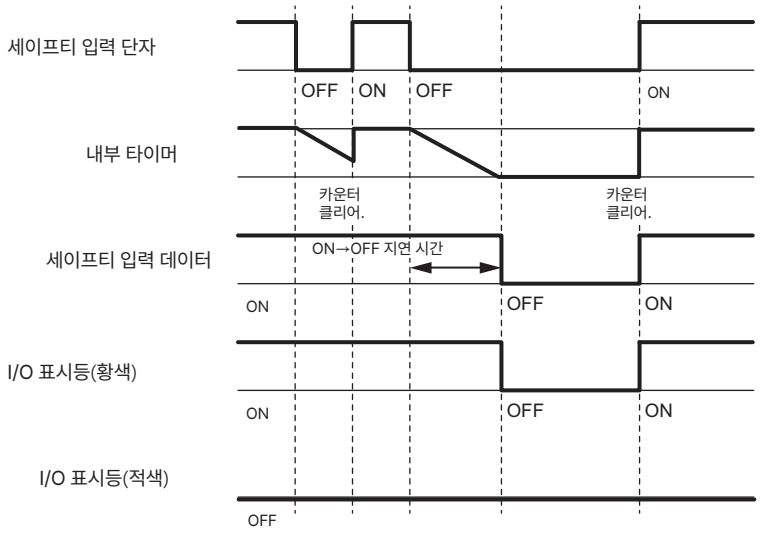
AI 번역본
For Reference Only

사용상의 주의

지연 시간을 길게 설정하면 채터링 및 노이즈에 대한 내성이 높아지지만, 입력 신호에 대한 응답은 느려집니다.

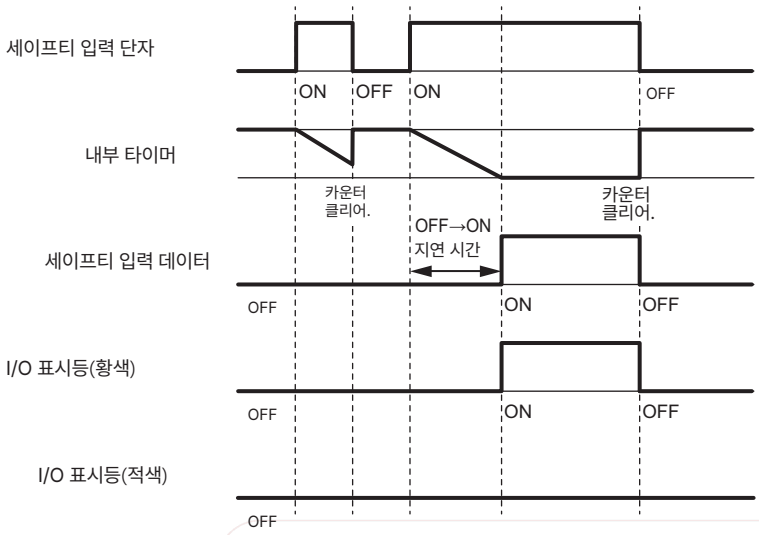
OFF Delay Time을 설정한 경우의 동작

ON->OFF Delay time에 설정된 시간보다 짧은 OFF 펄스를 걸러낼 수 있습니다.



ON Delay Time을 설정한 경우의 동작

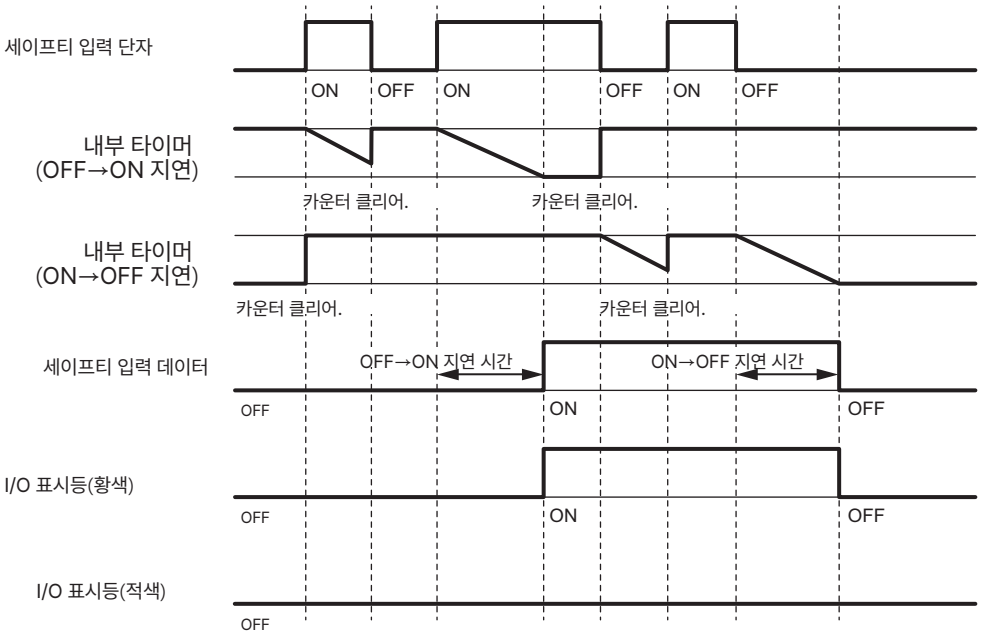
OFF->ON Delay time에 설정된 시간보다 짧은 ON 펄스를 걸러낼 수 있습니다.



AI 번역본
For Reference Only

ON Delay Time과 OFF Delay Time을 모두 설정한 경우의 동작

OFF->ON Delay time에 설정된 시간보다 짧은 ON 펄스와, ON->OFF Delay time에 설정된 시간보다 짧은 OFF 펄스를 걸러낼 수 있습니다.



6-4-7 입력 에러 래치 시간

입력 에러 래치 시간은 모든 입력 단자에 적용되는 파라미터입니다.
입력 단자에서 에러가 발생했을 때 에러 상태를 래치하는 시간을 설정합니다.
세이프티 I/O 블록이 간헐적으로 발생하는 에러를 검출할 수 있도록 최소 래치 시간을 설정합니다.
에러 래치 시간에는 세이프티 I/O 블록과 오리지네이터 디바이스 간의 네트워크 응답 시간을 고려하여 에러를 검출할 수 있는 최적의 값을 설정하십시오.

다음 표는 설정 내용을 보여줍니다.

설정 데이터명	설명	설정 범위
입력 에러 래치 시간	에러 발생 시부터 리셋까지의 최소 시간을 설정합니다.*1	0~65530(ms) 범위의 값을 설정합니다. 10(ms) 단위로 설정합니다. 0(ms)인 경우 에러 래치가 없습니다. 공장 출하 시 기본값은 1000(ms)입니다.

***1.** 에러의 원인이 제거되고 해당 세이프티 입력이 비활성(OFF)이 되면 에러가 리셋됩니다.

AI 번역본
-For Reference Only-

6-5 세이프티 출력 기능

이 절에서는 세이프티 I/O 블록의 세이프티 출력 기능에 대해 설명합니다.

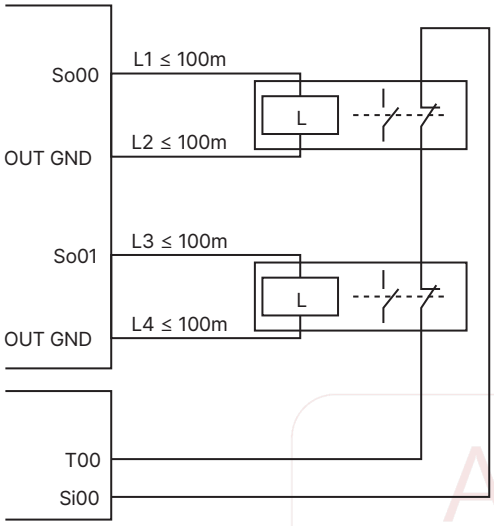
6-5-1 접속 가능한 디바이스

세이프티 I/O 블록은 세이프티 출력 단자를 통해 접속된 외부 디바이스를 진단합니다.
세이프티 출력 단자에 접속할 수 있는 세이프티 출력 디바이스는 다음 표에 나와 있습니다.

채널 모드		출력 단자 설정
듀얼 채널	싱글 채널	테스트 펄스
· 세이프티 릴레이(듀얼 채널) · 듀얼 채널 등가 출력(테스트 펄스 있음)	· 세이프티 릴레이(싱글 채널) · 싱글 채널(테스트 펄스 있음)	테스트 펄스 있음
· 듀얼 채널 등가 출력(테스트 펄스 없음)	· 싱글 채널(테스트 펄스 없음)	테스트 펄스 없음

세이프티 출력 디바이스에 세이프티 릴레이, 컨택터, 솔레노이드 밸브 등의 디바이스를 접속합니다. PNP 출력입니다.

다음은 세이프티 릴레이 또는 컨택터를 사용하는 경우의 접속 예입니다.



AI 번역본
-For Reference Only-

사용상의 주의

세이프티 출력 단자에서 세이프티 출력 디바이스까지의 배선 길이(L1, L2, L3, L4)는 각 배선당 100m 이하입니다.

6-5-2 테스트 펄스 평가 기능

이 기능은 출력 단자의 배선 오류를 검출하기 위해 세이프티 출력 단자에서 특정 주기로 테스트 펄스를 출력합니다.
다음 표는 설정 내용을 보여줍니다.

설정 데이터명	설명	설정 범위
테스트 펄스	세이프티 출력 디바이스에 테스트 펄스가 있는 디바이스를 선택합니다.	다음 중에서 선택합니다. ・세이프티 릴레이(듀얼 채널) ・듀얼 채널 등가 출력(테스트 펄스 있음) ・세이프티 릴레이(싱글 채널) ・싱글 채널(테스트 펄스 있음)

사용상의 주의

테스트 펄스 평가 기능을 사용하면 출력 회로를 진단하기 위해 세이프티 출력이 ON인 동안 펄스 폭 500 μs의 OFF 펄스 신호가 출력됩니다.
이러한 OFF 펄스로 인해 오동작하지 않도록 접속된 제어 기기의 입력 응답 시간을 확인하십시오.

추가 정보

세이프티 릴레이는 듀얼 채널과 싱글 채널 모두에서 테스트 펄스가 있는 디바이스입니다.

6-5-3 듀얼 채널 평가

세이프티 출력 단자는 듀얼 채널(이중화)로 사용할 수 있습니다. 듀얼 채널 평가는 두 출력 간 신호를 평가하여 불일치를 확인합니다.
두 출력 단자 중 하나에서 에러가 검출되면 두 출력이 모두 OFF됩니다.

듀얼 채널 평가 기능 설정

출력 디바이스에 대해 듀얼 채널 모드의 디바이스를 선택하여 듀얼 채널 평가 기능을 설정합니다.

다음 표는 설정 내용을 보여줍니다.

설정 데이터명	설명	설정 범위
채널 모드	출력 디바이스에 대해 듀얼 채널 모드의 디바이스를 선택합니다.	다음 중에서 선택합니다. ・세이프티 릴레이(듀얼 채널) ・듀얼 채널 등가 출력(테스트 펄스 있음) ・듀얼 채널 등가 출력(테스트 펄스 없음) 채널 모드 및 디바이스에 대한 자세한 내용은 6-16페이지의 6-5-1 접속 가능한 디바이스를 참조하십시오.

AI 번역본
-For Reference Only-

설정 순서는 7-50페이지의 7-6-1 세이프티 출력 기능 설정 순서를 참조하십시오.

세이프티 출력 데이터와 세이프티 출력 단자에서 출력되는 신호의 관계

듀얼 채널 모드의 디바이스에서 세이프티 출력 데이터와 세이프티 출력 신호의 관계는 다음과 같습니다.

채널 모드	세이프티 출력 데이터		세이프티 출력 단자의 출력 신호		상태의 의미
	So (n)	So (n+1)	So (n)	So (n+1)	
· 세이프티 릴레이 (듀얼 채널) · 듀얼 채널 등가 출력 (테스트 펄스 있음) · 듀얼 채널 등가 출력 (테스트 펄스 없음)	0	0	0 (OFF)	0 (OFF)	비활성(OFF)
	0	1	0 (OFF)	0 (OFF)	비활성(OFF)*1
	1	0	0 (OFF)	0 (OFF)	비활성(OFF)*1
	1	1	1 (ON)	1 (ON)	활성(ON)

***1.** 듀얼 채널 출력 간에 데이터 에러가 발생하여 비활성이 됩니다.

6-5-4 세이프티 출력 단자의 진단 기능으로 검출 가능한 에러

세이프티 출력 단자에서 검출 가능한 에러는 파라미터 설정에 따라 결정됩니다.
다음 표는 검출되는 에러를 보여줍니다.

파라미터 설정		에러 검출						
		전원선과의 접속 (양극측)		지락 고장*1		출력 배선의 단락*2		
출력 단자 설정	설명	출력 ON	출력 OFF	출력 ON	출력 OFF	단락 (두 출력이 모두 ON일 때)	단락 (두 출력이 모두 OFF일 때)	단락 (한쪽 출력이 ON이고 다른 쪽이 OFF 일 때)
테스트 펄스 없음	출력이 ON일 때 테스트 펄스가 출력되지 않습니다.	검출 불가	검출 가능	검출 가능	검출 불가	검출 불가	검출 불가	검출 가능
테스트 펄스 사용	출력이 ON일 때 테스트 펄스가 출력됩니다.	검출 가능	검출 가능	검출 가능	검출 불가능	검출 가능	검출 불가능	검출 가능

AI 번역본
-For Reference Only-

***1.** 지락 고장을 검출하려면 외부 전원의 0V 라인을 접지해야 합니다.
***2.** 출력 배선의 단락 검출은 듀얼 채널 모드에서만 유효합니다.

6-5-5 출력 에러 래치 시간

출력 에러 래치 시간은 모든 출력 단자에 적용되는 파라미터입니다.
출력 단자에서 에러가 발생했을 때 에러 상태를 래치하는 시간을 설정합니다.
간헐적으로 발생하는 에러를 세이프티 I/O 블록이 검출할 수 있도록 최소 래치 시간을 설정합니다.
에러 래치 시간에는 세이프티 I/O 블록과 오리지네이터 기기 간의
네트워크 응답 시간을 고려하여 에러를 검출할 수 있는 최적의 값을 설정합니다.

다음 표는 설정 내용을 나타냅니다.

설정 데이터명	설명	설정 범위
출력 에러 래치 시간	에러 발생부터 리셋까지의 최소 시간을 설정합니다.*1	0~65530(ms) 범위의 값을 설정합니다. 10(ms) 단위로 설정합니다. 0(ms)인 경우 에러 래치는 없습니다. 공장 출하 시 초기 설정값은 1000(ms)입니다.

***1.** 에러의 원인이 제거되고 해당 세이프티 출력이 비활성(OFF)이 되면 에러가 리셋됩니다.

6-5-6 EDM 피드백

세이프티 애플리케이션이 사용자 정의 애플리케이션인 경우, EDM 피드백 설정이 표시됩니다.

다음 표는 설정 내용을 나타냅니다.

설정 데이터명	설명	설정 범위
EDM 피드백	세이프티 입력 기기에 EDM 피드백이 등록된 단자 중에서 선택합니다.	다음 중에서 선택합니다. ・0: 미사용 ・1: Si00 ~ 12: Si11 공장 출하 시 초기 설정값은 0(미사용)입니다.

6-5-7 출력 지연

세이프티 애플리케이션이 사용자 정의 애플리케이션인 경우, 세이프티 출력 단자에 접속된 외부 기기로의 출력에 지연 시간을 설정할 수 있습니다. 이 기능은 모터, 로봇 암 등 외부 기기가 완전히 정지할 때까지의 시간을 고려하여 출력을 지연시킴으로써 급정지로 인한 기계 손상을 방지하거나, 외부 기기가 복귀한 후 동작이 안정된 다음 세이프티 출력을 ON으로 전환하는 등의 애플리케이션에 사용됩니다.

다음 표는 설정 내용을 나타냅니다.

설정 데이터명	설명	설정 범위
ON->OFF 지연 시간	출력 데이터가 ON에서 OFF로 전환되는 지연 시간입니다. 모터, 로봇 암 등 외부 기기가 완전히 정지할 때까지의 시간을 고려하여 출력을 지연시킴으로써 급정지로 인한 기계 손상을 방지하는 데 사용됩니다.	출력은 설정값 × 100(ms)의 값만큼 지연됩니다. 0~1500 범위의 값을 설정합니다. 공장 출하 시 초기 설정값은 0(ms)입니다.
OFF->ON 지연 시간	출력 데이터가 OFF에서 ON으로 전환되는 지연 시간입니다. 외부 기기가 복귀한 후 동작이 안정된 다음 세이프티 출력을 ON으로 전환하는 데 사용됩니다.	

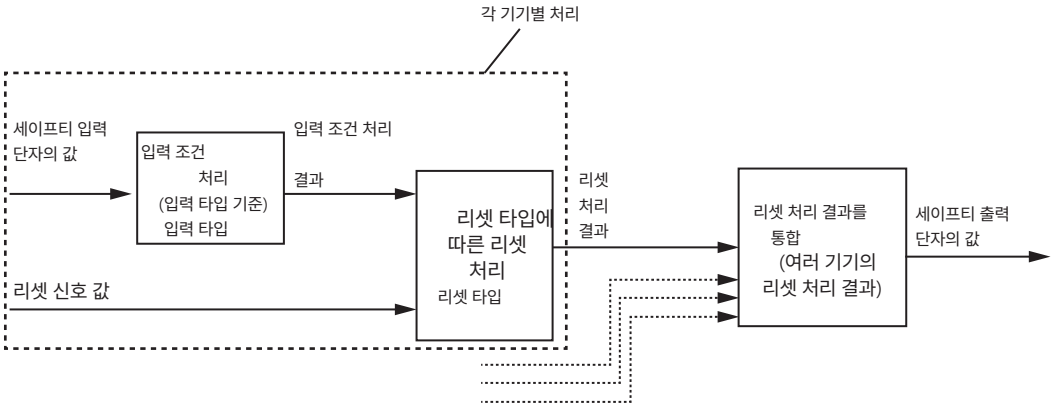
참고 번역본 -For Reference Only-

6-6 로직 기능

로직 기능은 세이프티 I/O 블록 내부에서 세이프티 입력 데이터에 대해 실행되는 처리입니다. 처리 결과는 세이프티 출력 데이터로서 세이프티 출력에 전달됩니다.
이 절에서는 로직 처리의 구조에 대해 설명합니다.

6-6-1 로직 처리

로직 설정에서는 입력 타입, 리셋 타입, 세이프티 출력 단자 So00~So03에 대한 출력값이라는 세 종류의 파라미터를 설정해야 합니다.
로직 처리는 먼저 각 기기의 세이프티 입력 단자 SiXX 값에 대해 입력 타입에 따른 입력 조건 처리와 리셋 타입에 따른 리셋 처리를 실행합니다. 그 후 여러 기기의 리셋 처리 결과를 통합하고, 마지막으로 세이프티 출력 단자 SoXX의 값을 결정합니다. 로직 설정을 구성할 때는 이러한 처리의 상세 내용을 유의해야 합니다.



입력 타입에 따른 입력 조건 처리

입력 조건 처리에서는 입력 타입 설정에 따라 두 종류 기기의 입력값을 통합하여 입력 조건 처리 결과를 얻을 수 있습니다. 이를 통해 예를 들어 두 쌍의 세이프티 라이트 커튼이 모두 차단되었을 때만 기기를 정지시키는 등의 처리가 가능합니다.
입력 타입 설정에는 2 Input (OR), 2 Input (AND), 미설정의 세 가지 설정 옵션이 있습니다. 각 설정과 입력 조건 처리 결과의 관계는 아래와 같습니다.

사 번역본
-For Reference Only-

입력 타입	입력 조건 처리 결과
2 Input (OR)	두 종류 기기의 입력값에 대한 OR 처리 결과
2 Input (AND)	두 종류 기기의 입력값에 대한 AND 처리 결과
미설정	두 종류 기기의 입력값을 통합하지 않습니다. 한쪽 기기의 입력값이 그대로 입력 조건 처리 결과가 됩니다.

리셋 타입에 따른 리셋 처리

각 기기의 출력값이 FALSE가 되면 리셋을 실행할 때까지 TRUE로 돌아가지 않습니다. 리셋 타입은 각 기기의 출력값을 리셋하는 방법이며, Manual(SiXX)과 Auto의 두 종류가 있습니다. 각 설정과 리셋 조건의 관계는 아래와 같습니다.

리셋 타입	리셋 조건
Manual (SiXX)	세이프티 입력 단자 SiXX의 값을 리셋 신호로 사용합니다. 리셋이 실행되면 해당 기기의 출력값이 리셋됩니다.
Auto	리셋 신호를 사용하지 않습니다. 해당 기기의 입력 조건 처리 결과가 TRUE가 되는 시점에 출력값이 리셋됩니다.

표의 리셋 신호는 해당 기기의 출력을 리셋하기 위한 Low-High-Low 펄스 신호입니다.
리셋 신호는 자동으로 등록할 수 있으며, 등록 후에는 설정을 변경할 수 있습니다. 각 절차는 7-7-1 로직 설정 절차(7-53페이지)를 참조하십시오.

리셋 처리는 입력 조건 처리 결과와 리셋 조건 충족 여부를 기준으로 각 기기별로 실행됩니다. 입력 조건 처리 결과, 리셋 조건 충족 여부, 리셋 처리 결과의 관계는 아래와 같습니다.

입력 조건 처리 결과	리셋 조건	리셋 조건 처리 결과
TRUE	조건 충족	TRUE
	조건 미충족	현재 값을 유지합니다.
FALSE	조건 충족	FALSE
	조건 미충족	FALSE

사용상의 주의

리셋 타입을 Auto로 설정하여 사용하는 경우, 재기동이나 리셋으로 인해 예기치 않은 기동이나 위험한 기계 동작이 발생하여 인체에 상해를 입힐 위험이 없는지 확인하십시오. 확인할 수 없는 경우에는 리셋 타입 Auto를 사용하지 마십시오.

세이프티 출력 단자 So00~So03에 출력하는 값 설정

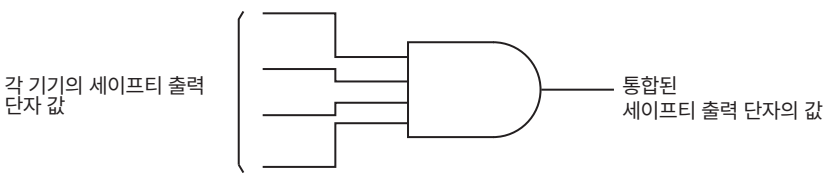
세이프티 출력 단자 So00~So03에 대한 출력값 설정은 각 기기의 리셋 처리 결과를 세이프티 출력 단자에 할당합니다. So00~So03의 각 세이프티 출력 단자에 각 기기별로 설정값 0 또는 1을 할당합니다. 각 설정값의 의미는 다음과 같습니다.

설정값	의미
0	리셋 처리 결과가 해당 세이프티 출력 단자에 반영됩니다.
1	리셋 처리 결과가 해당 세이프티 출력 단자에 반영되지 않습니다.

AI 번역본
-For Reference Only-

여러 기기의 출력 처리 결과 통합

여러 기기가 접속되어 있는 경우, 세이프티 출력 단자의 값은 각 기기의 세이프티 출력 단자 값에 대해 AND 연산을 수행하여 통합된 값이 됩니다. 즉, 여러 기기 중 하나라도 세이프티 출력 단자 값이 FALSE이면 세이프티 출력 단자 값은 FALSE가 됩니다.



설정 예

다음 표는 로직 설정의 설정 예를 나타냅니다.

입력	기기	입력 타입	리셋 타입	So00	So02
Si00	비상 정지 스위치(듀얼 채널 등가 입력)	-	Manual (Si10)	0	0
Si02	세이프티 라이트 커튼	2 Input (OR)	Manual (Si11)	1	0
Si04	세이프티 라이트 커튼				
Si06	세이프티 도어 스위치(듀얼 채널 등가 입력)	-	Auto	0	1
Ro1-01	리모트 출력 1-01	2 Input (OR)	Manual (Si10)	0	0
Ro2-01	리모트 출력 2-01				

이러한 설정에서는 다음 조건 중 하나라도 발생하면 So00의 값이 FALSE가 됩니다.

- 비상 정지 스위치가 눌립니다.
- 세이프티 도어 스위치가 설치된 도어가 열립니다.
- 리모트 출력 1-01과 리모트 출력 2-01의 값이 모두 FALSE가 됩니다.

또한 다음 조건 중 하나라도 발생하면 So02의 값이 FALSE가 됩니다.

- 비상 정지 스위치가 눌립니다.
- 두 쌍의 세이프티 라이트 커튼이 모두 차단됩니다.
- 리모트 출력 1-01과 리모트 출력 2-01의 값이 모두 FALSE가 됩니다.

So00 또는 So02의 값이 FALSE가 된 상태에서 다음 조건이 충족되면 리셋이 실행되어 값이 TRUE로 돌아갑니다.

So00 또는 So02의 값이 FALSE가 된 이유	So00 또는 So02의 값을 리셋하는 조건
비상 정지 스위치가 눌립니다.	Si10의 리셋 조건이 충족됩니다.
두 쌍의 세이프티 라이트 커튼이 모두 차단됩니다.	Si11의 리셋 조건이 충족됩니다.
세이프티 도어 스위치가 설치된 도어가 열립니다.	세이프티 도어 스위치가 설치된 도어가 닫힙니다.
리모트 출력 1-01과 리모트 출력 2-01의 값이 모두 FALSE가 되었습니다.	Si10의 리셋 조건이 충족됩니다.

AI 번역본
-For Reference Only-

6-7 세이프티 애플리케이션

이 절에서는 세이프티 애플리케이션의 목적과 종류, 그리고 세이프티 I/O 블록에 미리 설정된 고정 애플리케이션의 상세 내용에 대해 설명합니다.

6-7-1 세이프티 애플리케이션의 목적

세이프티 애플리케이션의 로직 기능을 사용하면 세이프티 컨트롤러를 거치지 않고 로컬에서 제어를 수행하여 고속 응답을 실현할 수 있습니다.
또한 세이프티 애플리케이션은 세이프티 컨트롤러로부터 전송되는 세이프티 출력 데이터를 필요에 따라 내부 로직과 결합함으로써 제어의 유연성을 높일 수 있습니다.

6-7-2 세이프티 애플리케이션의 종류

세이프티 애플리케이션에는 리모트 I/O 모드 애플리케이션, 고정 애플리케이션, 사용자 정의 애플리케이션, 애드온 애플리케이션의 네 가지 종류가 있습니다.
각각에 대한 개요, 애플리케이션 상세 내용, 선택 기준, 해당하는 세이프티 제어 시스템을 아래에 나타냅니다.

세이프티 애플리케이션	설명	선택 기준	세이프티 제어 시스템
리모트 I/O 모드 애플리케이션	I/O 단자 설정만 있고 로직 기능을 사용하지 않는 세이프티 애플리케이션입니다. 로직 기능을 사용하지 않으므로 세이프티 컨트롤러가 제어를 수행합니다.	· 세이프티 I/O 블록의 로직 기능으로는 구현하기 어려운 복잡하고 대규모인 시스템을 구축하고자 하는 경우.	세이프티 컨트롤러가 제어를 수행하는 구성 (Type 1 Safety Open을 사용한 구성)(1-8페이지) 세이프티 컨트롤러가 제어를 수행하는 구성 (Web UI를 사용한 구성)(1-9페이지)
고정 애플리케이션	로직 기능과 I/O 구성 설정이 있는 세이프티 애플리케이션입니다. 세이프티 I/O 블록에 미리 설정되어 있으며, 사양을 변경할 수 없습니다. 세이프티 I/O 블록이 제어를 수행합니다.	· 고정 애플리케이션 중에 그대로 사용할 수 있는 애플리케이션이 있는 경우.	미리 설정된 세이프티 애플리케이션을 사용하여 세이프티 I/O 블록이 제어를 수행하는 구성(1-10페이지)

AI 번역본
-For Reference Only-

세이프티 애플리케이션	설명	선택 기준	세이프티 제어 시스템
사용자 정의 애플리케이션	로직 기능과 I/O 구성 설정이 있는 세이프티 애플리케이션입니다. 사용자가 각 설정을 커스터마이즈할 수 있습니다. 세이프티 I/O 블록이 제어를 수행합니다.	· 세이프티 I/O 블록의 로직 기능으로 간단한 처리를 구현할 수 있는 애플리케이션인 경우. · 고정 애플리케이션 중에 그대로 사용할 수 있는 애플리케이션이 없는 경우. · 여러 세이프티 I/O 블록 유닛에서 동일한 처리를 수행하기 위해 세이프티 컨트롤러 측에서 세이프티 애플리케이션을 관리하고자 하는 경우.	사용자가 설계한 세이프티 애플리케이션을 사용하여 세이프티 I/O 블록이 제어를 수행하는 구성 (중앙 집중 관리 방식) (1-11페이지)
애드온 애플리케이션		· 세이프티 I/O 블록의 로직 기능으로 간단한 처리를 구현할 수 있는 애플리케이션인 경우. · 고정 애플리케이션 중에 그대로 사용할 수 있는 애플리케이션이 없는 경우. · 하나의 세이프티 I/O 블록만 단독으로 사용하기 위해 세이프티 I/O 블록 측에서 세이프티 애플리케이션을 관리하고자 하는 경우.	사용자가 설계한 세이프티 애플리케이션을 사용하여 세이프티 I/O 블록이 제어를 수행하는 구성 (분산 관리 방식) (1-12페이지)

리모트 I/O 모드 애플리케이션

리모트 I/O 모드 애플리케이션은 사용자가 Sysmac Studio를 사용하여 I/O 구성 설정만 정의하는 애플리케이션입니다. 로직 설정은 구성하지 않습니다. 세이프티 컨트롤러의 세이프티 프로그램과 조합하여 사용합니다. 이 애플리케이션은 세이프티 I/O 블록의 로직 기능으로는 구현하기 어려운 복잡하고 대규모인 시스템을 구축하는 데 적합합니다.

세이프티 I/O 블록에 리모트 I/O 모드 애플리케이션을 구성하는 방법은 다음 두 가지입니다.

· 세이프티 컨트롤러에서 Type 1 Safety Open을 사용하는 방법

· Web UI를 통한 구성을 사용하는 방법

AI 번역본
- For Reference Only -

고정 애플리케이션

고정 애플리케이션은 세이프티 I/O 블록에 미리 설치되어 있는 세이프티 애플리케이션입니다. 사양을 변경할 수 없습니다.

고정 애플리케이션에는 다음 세 종류가 있습니다. 모두 비상 정지 스위치나 세이프티 라이트 커튼 등의 기기를 사용하여 위험한 상황이 발생하기 전에 구동 유닛이나 로봇을 정지시키는 애플리케이션입니다. 구현하고자 하는 애플리케이션과 일치하는 것이 있으면 사용하십시오.

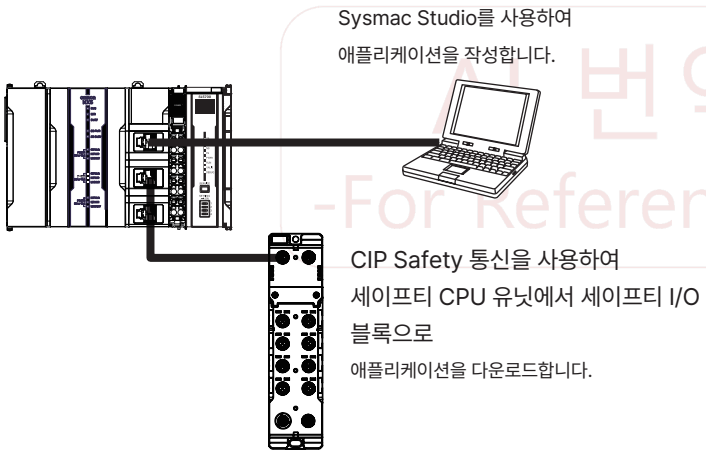
각 애플리케이션의 상세 내용은 아래 표에 나열된 참조 항목을 확인하십시오.

SETTING SW1, SW2 로터리 스위치 번호	이름	애플리케이션	참조
1	부분 정지 + 전체 정지 애플리케이션	세이프티 라이트 커튼으로 부분 정지를 수행하고 비상 정지 스위치로 전체 정지를 수행하는 애플리케이션입니다. 외부 기기 모니터링(EDM)은 없습니다.	No. 1 부분 정지 + 전체 정지 애플리케이션 6-27 페이지 참조
2	부분 정지 + 전체 정지 애플리케이션(EDM 포함)	세이프티 라이트 커튼으로 부분 정지를 수행하고 비상 정지 스위치로 전체 정지를 수행하는 애플리케이션입니다. 외부 기기 모니터링(EDM)이 있습니다.	No. 2 부분 정지 + 전체 정지 애플리케이션(EDM 포함) 6-34페이지 참조
3	작업자 · 로봇 자동 전환 애플리케이션	작업자와 로봇의 자동 전환을 수행하고 비상 정지 스위치와 가드로 전체 정지를 수행하는 애플리케이션입니다.	No. 3 작업자 · 로봇 자동 전환 애플리케이션 (6-38페이지 참조)

고정 애플리케이션은 로터리 스위치 번호에 미리 할당되어 있습니다. 로터리 스위치를 설정하면 원하는 고정 애플리케이션을 시작할 수 있습니다.

사용자 정의 애플리케이션

사용자 정의 애플리케이션은 사용자가 Sysmac Studio를 사용하여 직접 작성할 수 있는 애플리케이션입니다. CIP Safety 통신을 사용하여 세이프티 CPU 유닛에서 세이프티 I/O 블록으로 애플리케이션을 다운로드하여 사용합니다. 사용자 정의 애플리케이션은 CIP Safety 통신을 사용하여 오픈 타입 Type1 Safety Open 커넥션을 설정함으로써 세이프티 I/O 블록에 구성됩니다.

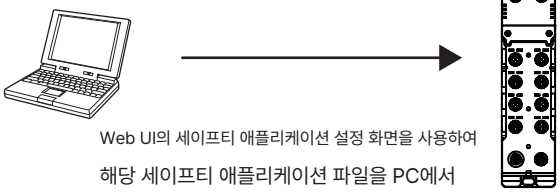


샘플 번역본
-For Reference Only-

애드온 애플리케이션

애드온 애플리케이션은 세이프티 I/O 블록에 미리 설치되어 있지 않고,
필요에 따라 세이프티 애플리케이션 파일을 세이프티 I/O 블록에 다운로드하여 사용하는 세이프티 애플리케이션입니다.
Sysmac Studio를 사용하여 사용자만의 커스텀 로직 설정 및 I/O 구성 설정을 구성하고
세이프티 애플리케이션 파일을 작성합니다.
Web UI의 세이프티 애플리케이션 설정 화면을 사용하여 해당 세이프티 애플리케이션 파일을 세이프티 I/O 블록에
다운로드합니다.

Sysmac Studio를 사용하여
세이프티 애플리케이션 파일을 작성합니다.



Web UI의 세이프티 애플리케이션 설정 화면을 사용하여
해당 세이프티 애플리케이션 파일을 PC에서
세이프티 I/O 블록으로
다운로드합니다.

AI 번역본
-For Reference Only-

6-7-3 고정 애플리케이션 상세

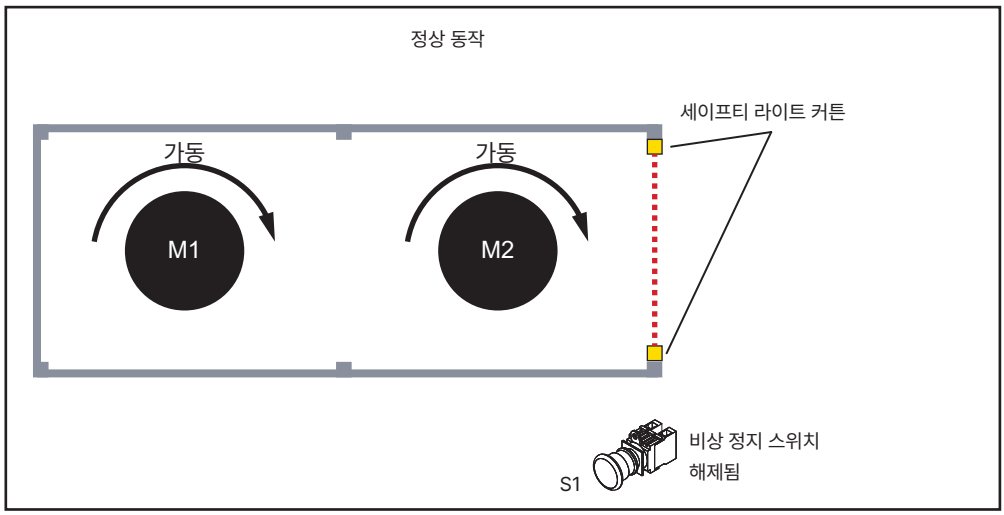
이 절에서는 각 고정 애플리케이션의 로직 및 I/O 구성 설정에 대해 설명합니다.

No. 1 부분 정지 + 전체 정지 애플리케이션

부분 정지 + 전체 정지 애플리케이션은 세이프티 라이트 커튼으로 부분 정지를 수행하고 비상 정지 스위치로 전체 정지를 수행하는 애플리케이션입니다. 외부 기기 모니터링(EDM)은 사용하지 않습니다. 두 구동 장치를 모두 전체 정지시키는 경우와 그중 하나만 부분 정지시키는 경우를 구분하여 사용합니다.

● 애플리케이션 개요

생산 현장에서 두 대의 구동 장치 M1, M2가 가동되고 있습니다.
구동 장치가 설치된 공간은 삼면이 벽으로 둘러싸여 있지만, 한 방향은 작업자가 작업할 수 있도록 개방되어 있으며 세이프티 라이트 커튼이 설치되어 있습니다.
이상 발생 시 작업자가 비상 정지 스위치를 누르면 두 구동 장치가 모두 정지합니다.
세이프티 라이트 커튼이 차단되면 세이프티 라이트 커튼에 가장 가까운 구동 장치 M2만 정지하고, 구동 장치 M1은 계속 동작합니다.



세이프티 카테고리/PL/SIL	사양
세이프티 카테고리	Cat.3까지*1
PL	PLe까지
SIL	SIL3까지

AI 번역본
-For Reference Only-

***1.** 접속할 것으로 예상되는 세이프티 서보 드라이브의 세이프티 카테고리가 Cat.3이므로, 이 애플리케이션의 세이프티 카테고리도 Cat.3입니다.

● 동작

각 기기의 입력 신호를 사용한 동작 사양은 다음과 같습니다.

비상 정지 스위치 S1을 눌렀을 때

・비상 정지 스위치 S1을 누르면 구동 장치 M1, M2로의 전원 공급이 즉시 차단됩니다.

・구동 장치 M1, M2로의 전원 공급은 비상 정지 스위치 S1이 해제되고 리셋 스위치 S2를 누를 때까지 차단 상태로 유지됩니다.

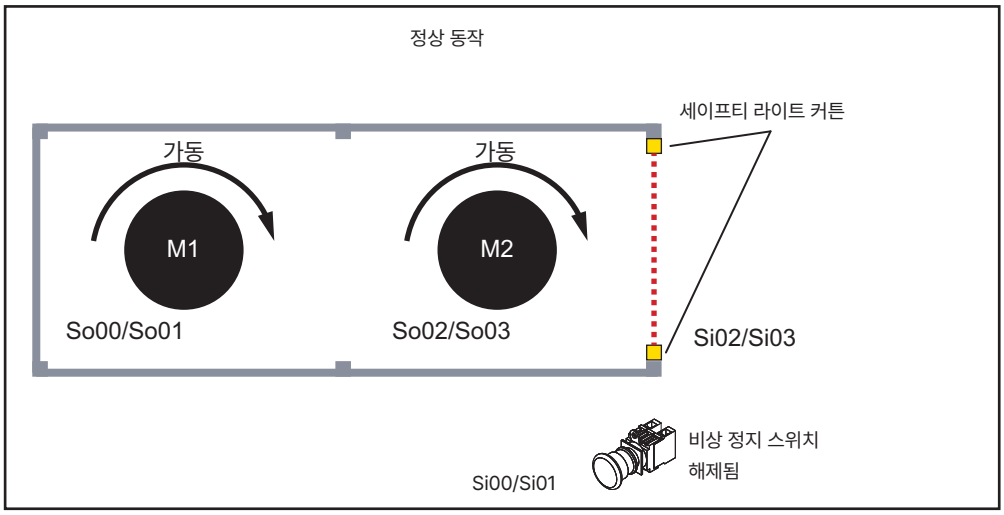
세이프티 라이트 커튼이 차단되었을 때(비상 정지 스위치 S1을 누르지 않은 경우)

・세이프티 라이트 커튼이 차단되면 구동 장치 M2로의 전원 공급이 즉시 차단됩니다. 구동 장치 M1에는 계속 전원이 공급됩니다.

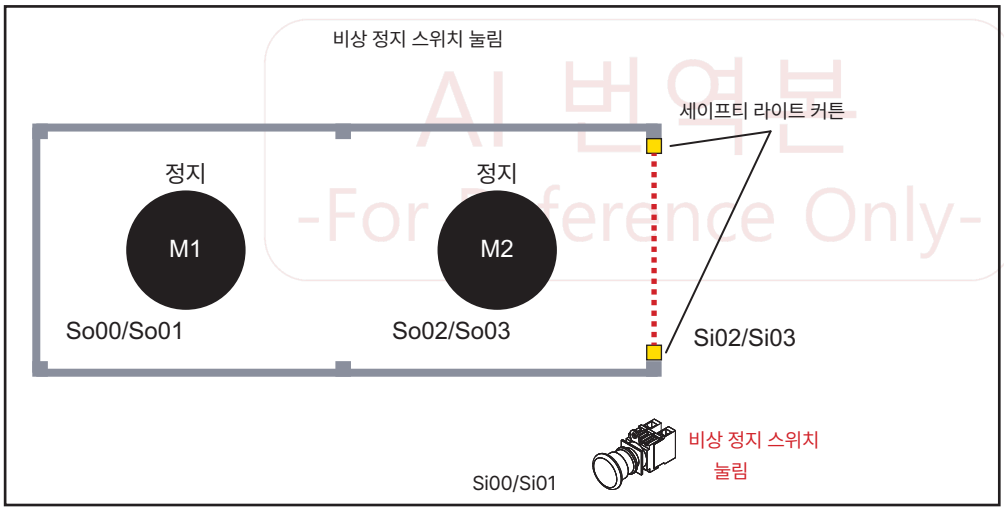
・구동 장치 M2로의 전원 공급은 리셋 스위치 S2를 누를 때까지 차단 상태로 유지됩니다.

각 상황에서의 동작은 그림에 나타나 있습니다.

정상 동작 시 두 대의 구동 장치 M1, M2가 가동되고 있습니다.

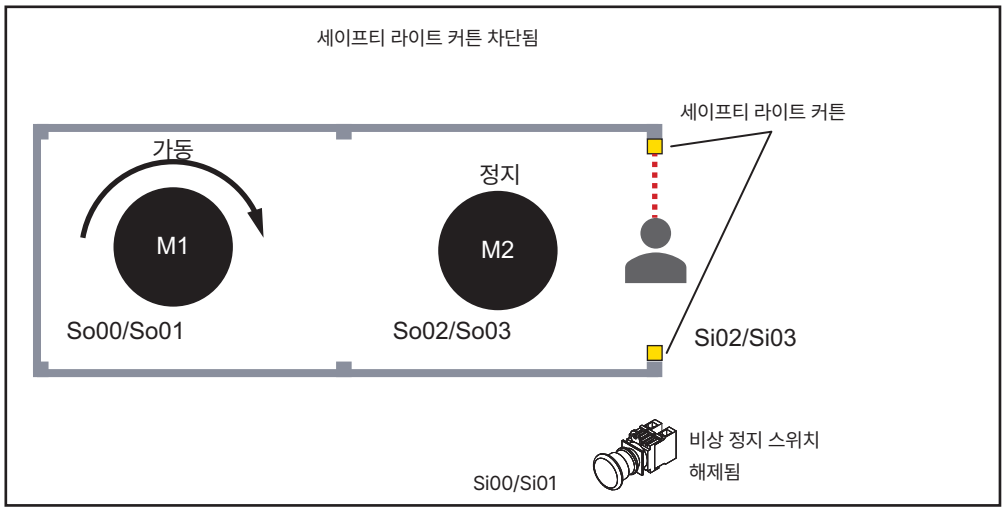


비상 정지 스위치 S1을 누르면 구동 장치 M1, M2가 모두 정지합니다.



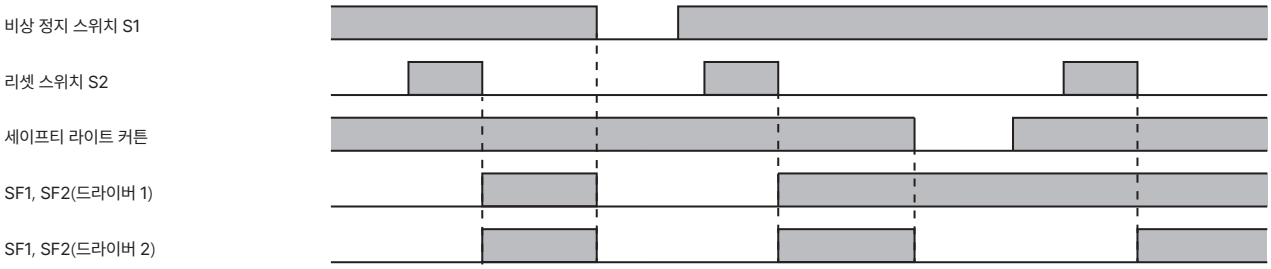
AI 번역본
-For Reference Only-

세이프티 라이트 커튼이 차단되면 구동 장치 M2만 정지합니다.



● 타이밍 차트

타이밍 차트는 아래와 같습니다.



AI 번역본
-For Reference Only-

● I/O 구성 설정

I/O 구성 설정의 상세 내용은 다음과 같습니다.

입력

입력	기기	테스트 출력 모드	ON->OFF 지연 시간	OFF->ON 지연 시간	불일치 시간
Si00/T00	비상 정지 스위치(듀얼 채널 등가 입력)	테스트 출력	0 ms	0 ms	500 ms
Si01/T01		테스트 출력	0 ms	0 ms	
Si02/T02	세이프티 라이트 커튼	전원 공급	0 ms	0 ms	500 ms
Si03/T03		표준 출력	0 ms	0 ms	
Si04/T04	-	미사용	-	-	-
Si05/T05	-	미사용	-	-	-
Si06/T06	리셋 스위치	테스트 출력	0 ms	0 ms	-
Si07/T07	-	표준 출력	-	-	-
Si08/T08	-	미사용	-	-	-
Si09/T09	-	미사용	-	-	-
Si10/T10	-	미사용	-	-	-
Si11/T11	-	미사용	-	-	-

입력 에러 래치 신호: 1,000 ms

출력

출력	기기	EDM 피드백 설정	ON->OFF 지연 시간	OFF->ON 지연 시간
So00/So01	듀얼 채널 등가 출력(테스트 펄스 포함)	미사용	0 × 100 ms	0 × 100 ms
So02/So03	듀얼 채널 등가 출력(테스트 펄스 포함)	미사용	0 × 100 ms	0 × 100 ms

출력 에러 래치 신호: 1,000 ms

로직

입력	기기	입력 타입	리셋 타입	So00/So01	So02/So03
Si00/Si01	비상 정지 스위치(듀얼 채널 등가 입력)	-	Manual (Si06)	0	0
Si02/Si03	세이프티 라이트 커튼	-	Manual (Si06)	1	0

리셋 신호	최소 ON 펄스 폭 [ms]	최대 ON 펄스 폭 [ms]
Si06	350	2,000

AI 번역본
-For Reference Only-

전원 투입 모드: 실행 중

서명

세이프티 구성 CRC(SCCRC): 519F5023

세이프티 구성 타임스탬프(SCTS): 4D0C00000000

● 결선도

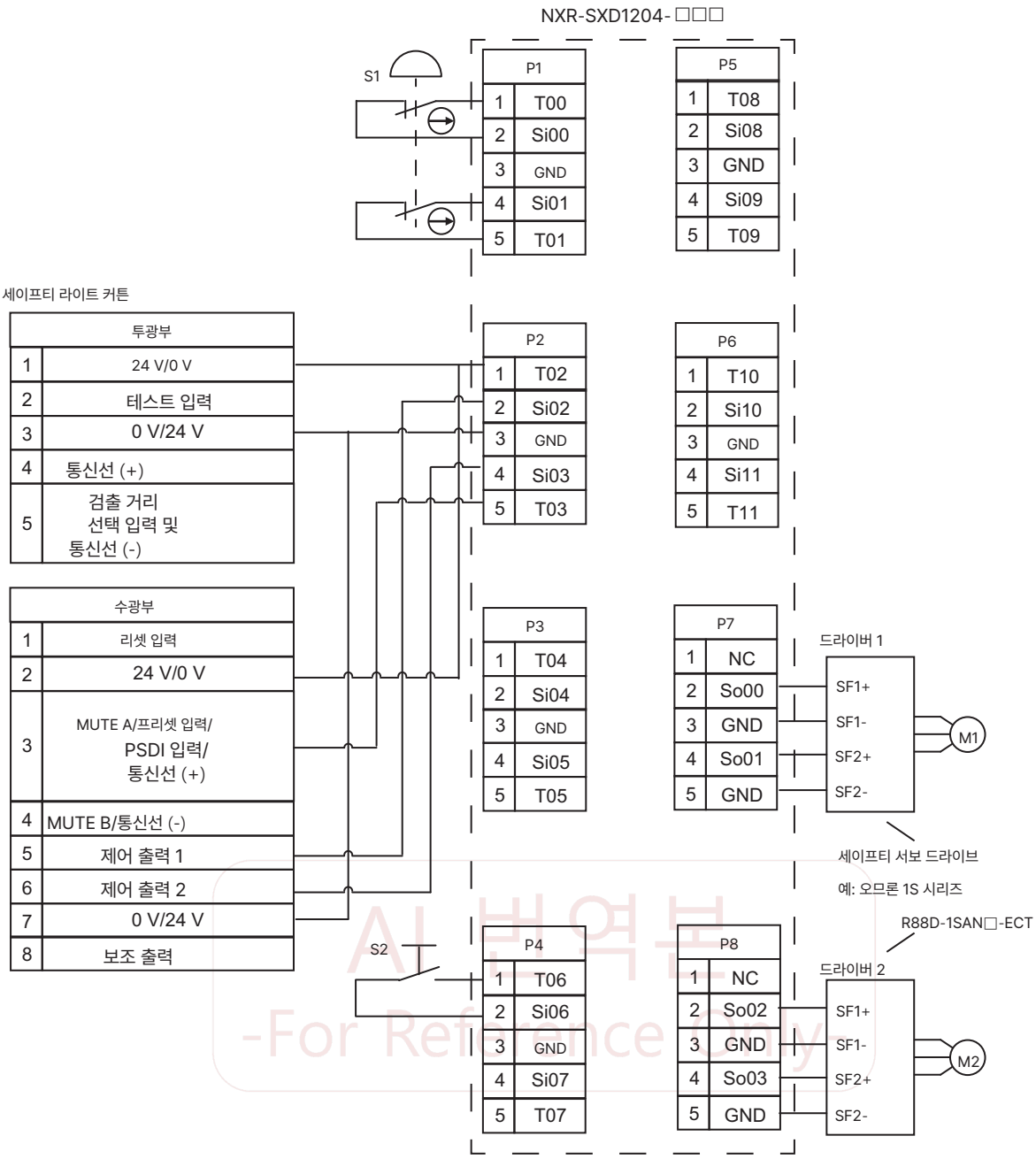
NXR-SXD1204-□□□의 결선도는 아래와 같습니다.

S1: 비상 정지 스위치

S2: 리셋 스위치

SF1, SF2: 세이프티 서보 드라이브 STO 기능의 세이프티 입력 M1,

M2: 구동 장치



AI 번역본
-For Reference Only-

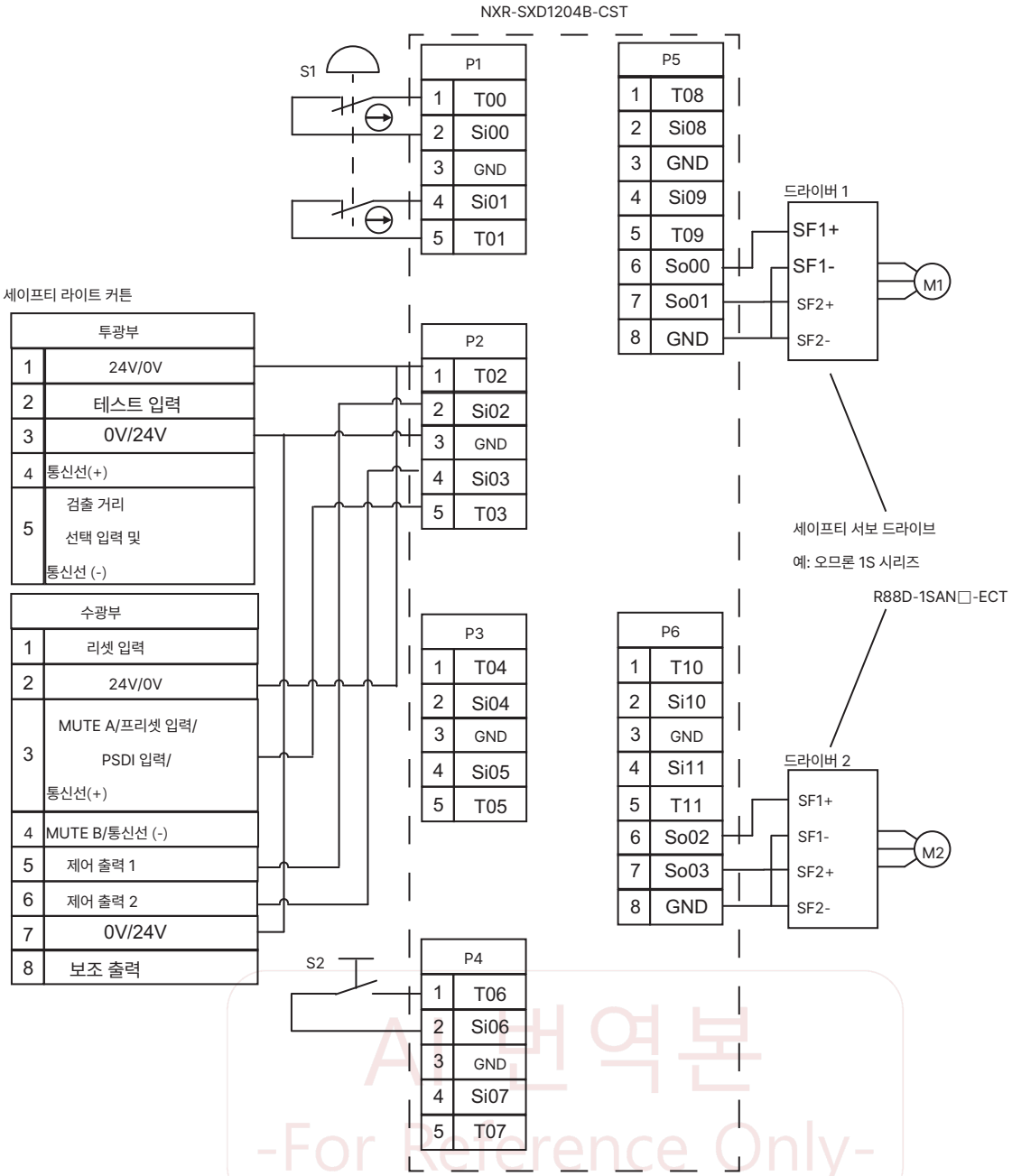
NXR-SXD1204B-CST의 결선도는 아래와 같습니다.

S1: 비상 정지 스위치

S2: 리셋 스위치

SF1, SF2: 세이프티 서보 드라이브 STO 기능의 세이프티 입력 M1,

M2: 구동 장치



사본 역본
-For Reference Only-

● 주의 사항

사용상의 주의

· 시스템의 세이프티 요구 수준에 맞는 세이프티 라이트 커튼 및 비상 정지 스위치를 선택하십시오.

· 세이프티 서보 드라이브는 EDM을 사용하지 않고도 시스템의 세이프티 요구 수준을 달성할 수 있는 기기를 선택하십시오.

· 서보 드라이브의 세이프티 입력 회로에서 고장을 검출하기 위해 6개월마다 기능을 테스트하십시오.

· 시스템 전체의 규격 적합성을 확보하는 것은 고객의 책임입니다.

· 전기적 및 기계적 고장을 검출하려면 이중화된 반도체 출력 접점과 이중화된 기계식 출력 기기를 조합하여 사용하십시오.

AI 번역본
-For Reference Only-

No. 2 부분 정지 + 전체 정지 애플리케이션(EDM 포함)

부분 정지 + 전체 정지 애플리케이션(EDM 포함)은 세이프티 라이트 커튼으로 부분 정지를 수행하고 비상 정지 스위치로 전체 정지를 수행하는 애플리케이션입니다. 부분 정지 + 전체 정지 애플리케이션에 외부 기기 모니터링(EDM)을 추가한 애플리케이션입니다.

● 애플리케이션 개요

애플리케이션의 상세 내용은 부분 정지 + 전체 정지 애플리케이션과 동일합니다.

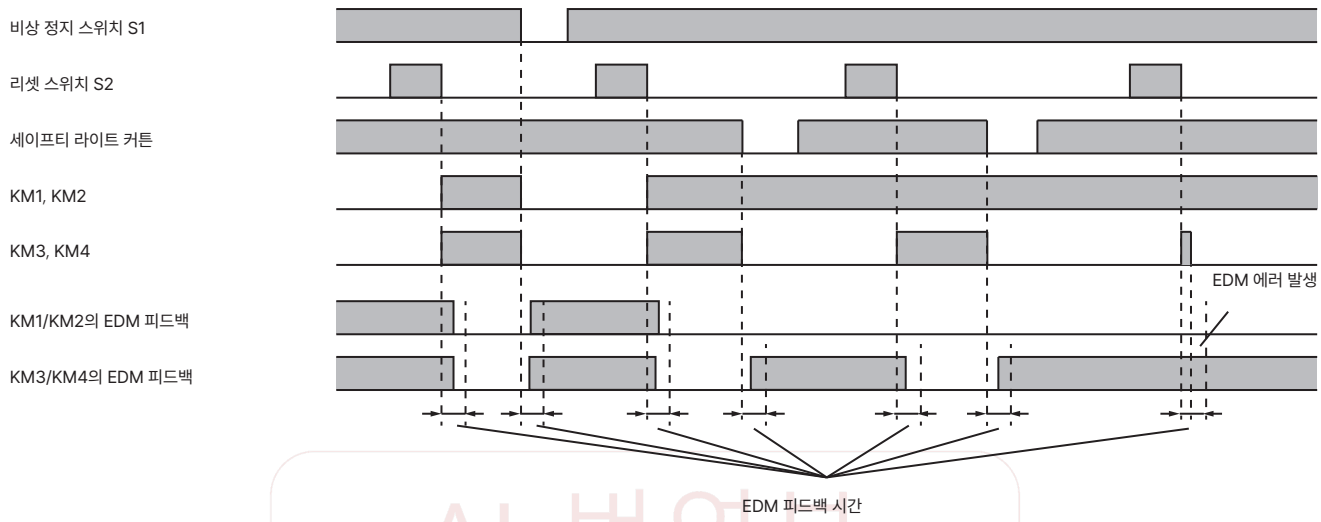
세이프티 카테고리/PL/SIL	사양
세이프티 카테고리	Cat.4까지
PL	PLe까지
SIL	SIL3까지

● 동작

동작은 부분 정지 + 전체 정지 애플리케이션과 동일합니다.

● 타이밍 차트

타이밍 차트는 아래와 같습니다.



AI 번역본
-For Reference Only-

● I/O 구성 설정

I/O 구성 설정의 상세 내용은 다음과 같습니다.

입력

입력	기기	테스트 출력 모드	ON->OFF 지연 시간	OFF->ON 지연 시간	불일치 시간
Si00/T00	비상 정지 스위치 (듀얼 채널 등가 입력)	테스트 출력	0 ms	0 ms	500 ms
Si01/T01		테스트 출력	0 ms	0 ms	
Si02/T02	세이프티 라이트 커튼	전원 공급	0 ms	0 ms	500 ms
Si03/T03		표준 출력	0 ms	0 ms	
Si04/T04	-	미사용	-	-	-
Si05/T05	-	미사용	-	-	-
Si06/T06	리셋 스위치	테스트 출력	0 ms	0 ms	-
Si07/T07	-	미사용	-	-	-
Si08/T08	EDM 피드백	테스트 출력	0 ms	0 ms	-
Si09/T09	-	미사용	-	-	-
Si10/T10	EDM 피드백	테스트 출력	0 ms	0 ms	-
Si11/T11	-	미사용	-	-	-

입력 에러 래치 신호: 1,000 ms

출력

출력	기기	EDM 피드백 설정	ON->OFF 지연 시간	OFF->ON 지연 시간
So00/So01	듀얼 채널 등가 출력 (테스트 펄스 포함)	Si08	0 × 100 ms	0 × 100 ms
So02/So03	듀얼 채널 등가 출력 (테스트 펄스 포함)	Si10	0 × 100 ms	0 × 100 ms

출력 에러 래치 신호: 1,000 ms

로직

입력	기기	입력 유형	리셋 유형	So00/So01	So02/So03
Si00/Si01	비상 정지 스위치 (듀얼 채널 등가 입력)	-	수동 (Si06)	0	0
Si02/Si03	세이프티 라이트 커튼	-	수동 (Si06)	1	0

리셋 신호	최소 ON 펄스 폭 [ms]	최대 ON 펄스 폭 [ms]
Si06	350	2,000

AI 번역본
-For Reference Only-

전원 투입 모드: 실행 중

서명

세이프티 컨피규레이션 CRC (SCCRC): C54E34C8

세이프티 컨피규레이션 타임 스탬프 (SCTS): 4D0C00000000

● 접속선도

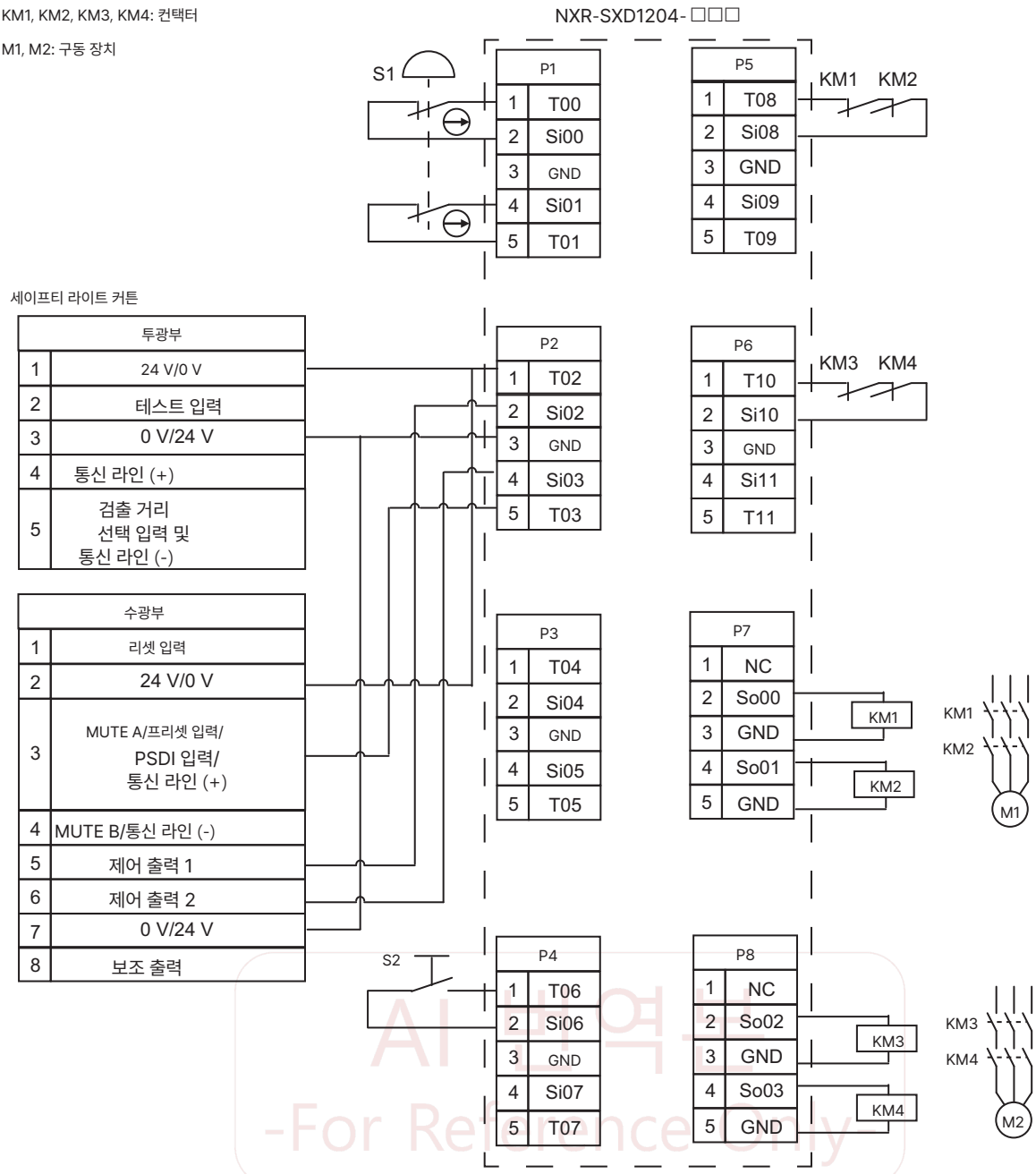
NXR-SXD1204-□□□의 접속선도는 아래와 같습니다.

S1: 비상 정지 스위치

S2: 리셋 스위치

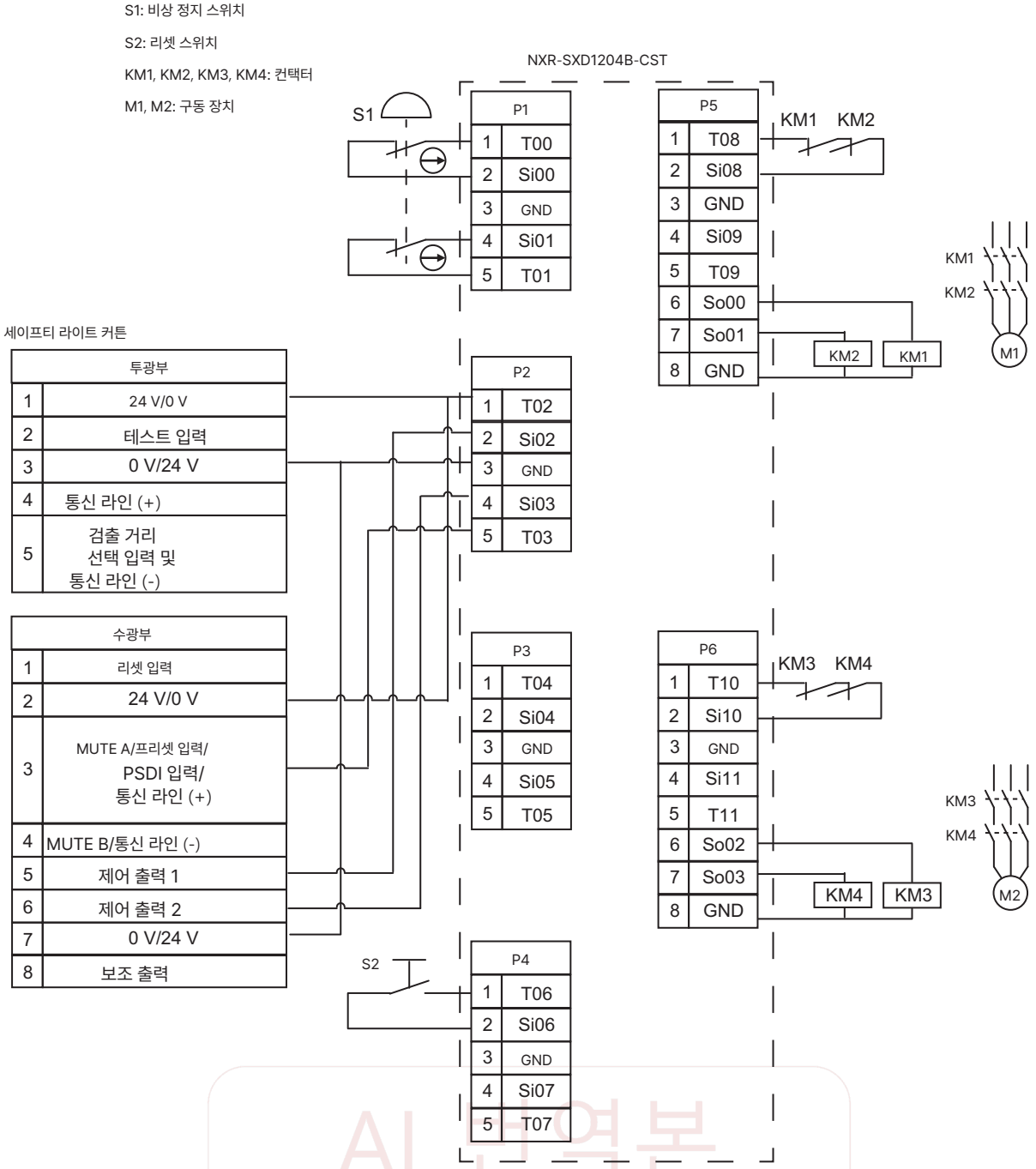
KM1, KM2, KM3, KM4: 컨택터

M1, M2: 구동 장치



AI 번역 본
-For Reference Only

NXR-SXD1204B-CST의 접속선도는 아래와 같습니다.



AI 번역본
-For Reference Only-

● 주의 사항

사용상의 주의

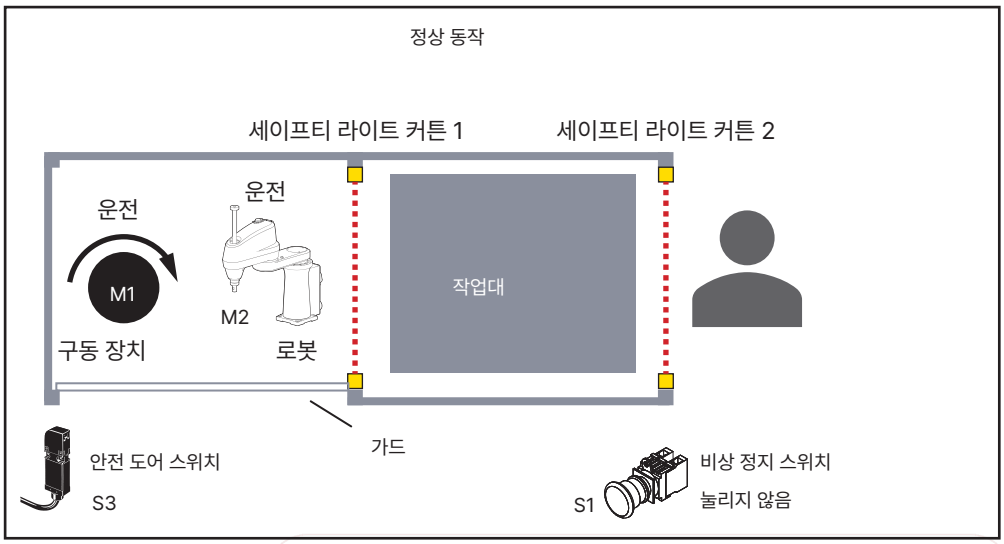
- 시스템의 안전 요구 수준에 맞게 세이프티 라이트 커튼과 비상 정지 스위치를 선택하십시오.
- 컨택터 접점의 융착을 검출하기 위해 매월 기능을 테스트하십시오.
- 전체 시스템이 규격에 적합하도록 하는 것은 고객의 책임입니다.
- 전기적 및 기계적 고장을 검출하려면 이중화된 반도체 출력 접점과 이중화된 기계식 출력 기기를 조합하여 사용하십시오.

No. 3 작업자와 로봇 자동 전환 애플리케이션

작업자와 로봇 자동 전환 애플리케이션은 작업자와 로봇을 자동으로 전환하고 비상 정지 스위치와 가드를 사용하여 전체 정지를 수행하는 애플리케이션입니다. 작업자와 로봇의 접촉을 방지하기 위해 필요에 따라 로봇을 정지시킵니다.

● 애플리케이션 개요

생산 현장에는 구동 장치 1대와 로봇 1대가 운전되고 있습니다.
로봇 옆에는 작업대가 있습니다. 로봇이 작업대에 제품을 놓으면 작업자가 반대쪽에서 그 워크피스를 집습니다.
작업대 양쪽에는 세이프티 라이트 커튼이 설치되어 있습니다. 로봇과 작업자가 동시에 작업대에 접근하면 위험하므로, 두 쌍의 세이프티 라이트 커튼이 모두 차광되면 로봇이 정지합니다. 이때 로봇 뒤쪽의 구동 장치는 정지하지 않습니다.
구동 장치와 로봇이 설치된 공간에는 보수 점검용 가드가 있으며, 안전 도어 스위치가 설치되어 있습니다. 작업자가 도어를 열면 구동 장치와 로봇이 모두 전체 정지합니다.
이상이 발생한 경우 작업자는 비상 정지 스위치를 누릅니다. 이 경우에도 구동 장치와 로봇이 모두 전체 정지합니다.



안전 카테고리/PL/SIL	사양
안전 카테고리	Cat.3까지
PL	PLe까지
SIL	SIL3까지

AI 번역본
For Reference Only-

● 동작

각 기기의 입력 신호를 사용하는 동작 사양은 다음과 같습니다.

비상 정지 스위치 S1을 눌렀을 때

・비상 정지 스위치 S1을 누르면 구동 장치 M1과 로봇 M2에 대한 전원 공급이 즉시 차단됩니다.

・로봇 M2에 대한 전원 공급은 가드가 닫히고, 세이프티 라이트 커튼 1 또는 세이프티 라이트 커튼 2의 광축이 들어오고, 비상 정지 스위치 S1이 해제되고, 리셋 스위치 S2를 누를 때까지 차단 상태로 유지됩니다.

・구동 장치 M1에 대한 전원 공급은 가드가 닫히고, 비상 정지 스위치 S1이 해제되고, 리셋 스위치 S2를 누를 때까지 차단 상태로 유지됩니다.

가드를 열었을 때 (비상 정지 스위치 S1을 누르지 않은 경우)

・가드가 열린 것을 안전 도어 스위치 S3이 검출하여 구동 장치 M1과 로봇 M2에 대한 전원 공급이 즉시 차단됩니다.

・로봇 M2에 대한 전원 공급은 가드가 닫히고, 세이프티 라이트 커튼 1 또는 세이프티 라이트 커튼 2의 광축이 들어오고, 리셋 스위치 S2를 누를 때까지 차단 상태로 유지됩니다.

・구동 장치 M1에 대한 전원 공급은 가드가 닫히고 리셋 스위치 S2를 누를 때까지 차단 상태로 유지됩니다.

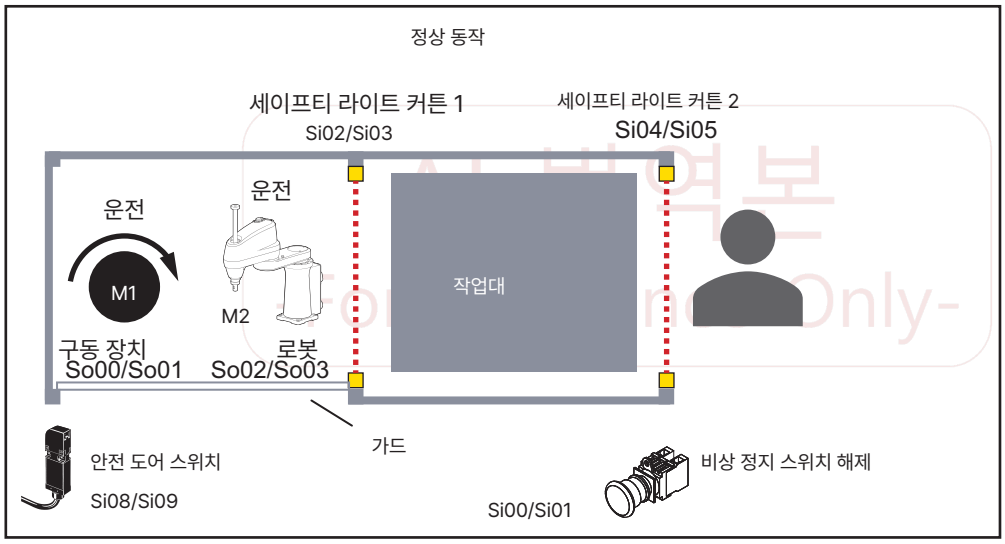
세이프티 라이트 커튼이 차광되었을 때 (비상 정지 스위치 S1을 누르지 않고 가드가 닫혀 있는 경우)

・세이프티 라이트 커튼 1과 세이프티 라이트 커튼 2가 모두 차광되면 로봇 M2에 대한 전원 공급이 즉시 차단됩니다. 구동 장치 M1에는 전원이 계속 공급됩니다.

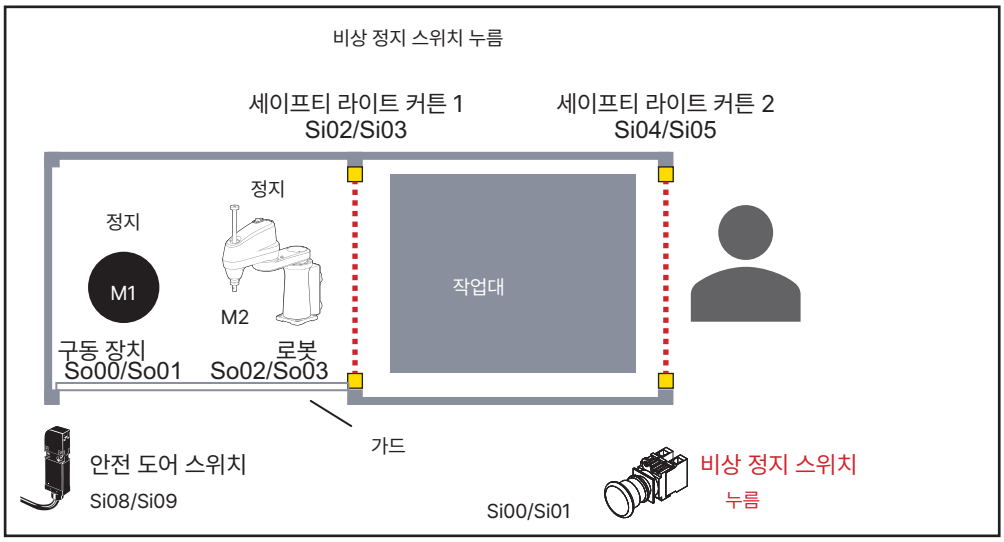
・로봇 M2에 대한 전원 공급은 세이프티 라이트 커튼 1 또는 세이프티 라이트 커튼 2의 광축이 들어올 때까지 차단 상태로 유지됩니다.

각 상황에서의 동작은 그림에 나타나 있습니다.

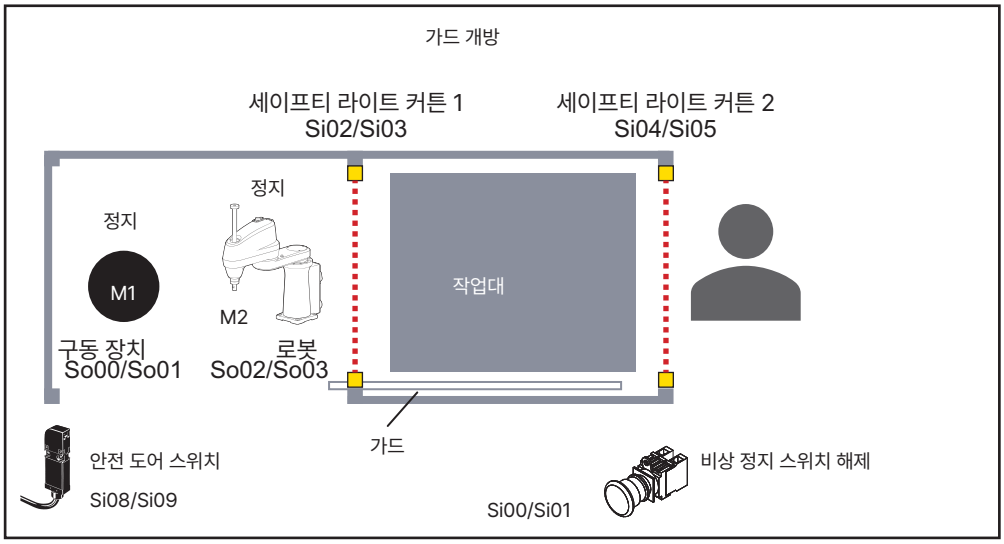
정상 동작 시에는 구동 장치 M1 1대와 로봇 M2 1대가 운전 중입니다.



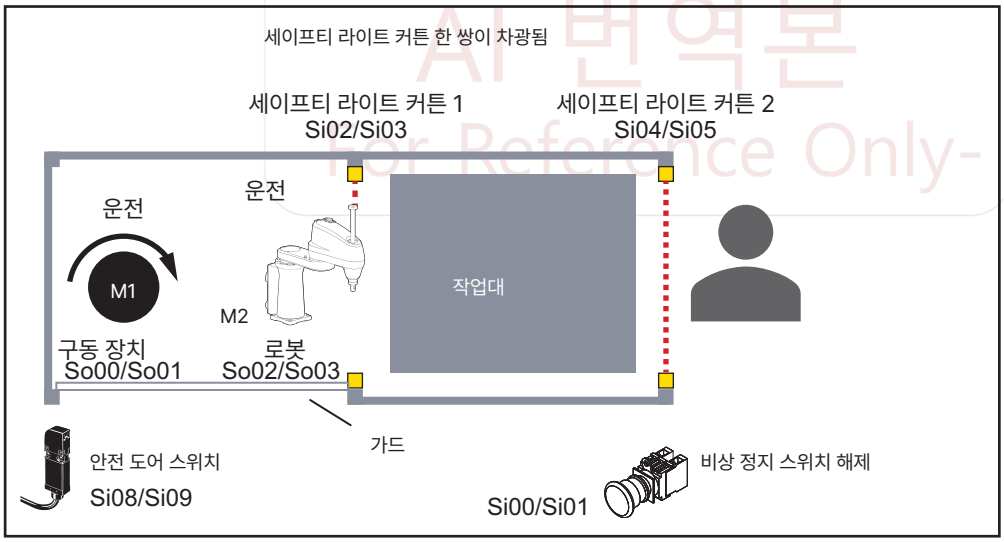
비상 정지 스위치 S1을 누르면 구동 장치 M1과 로봇 M2가 모두 정지합니다.



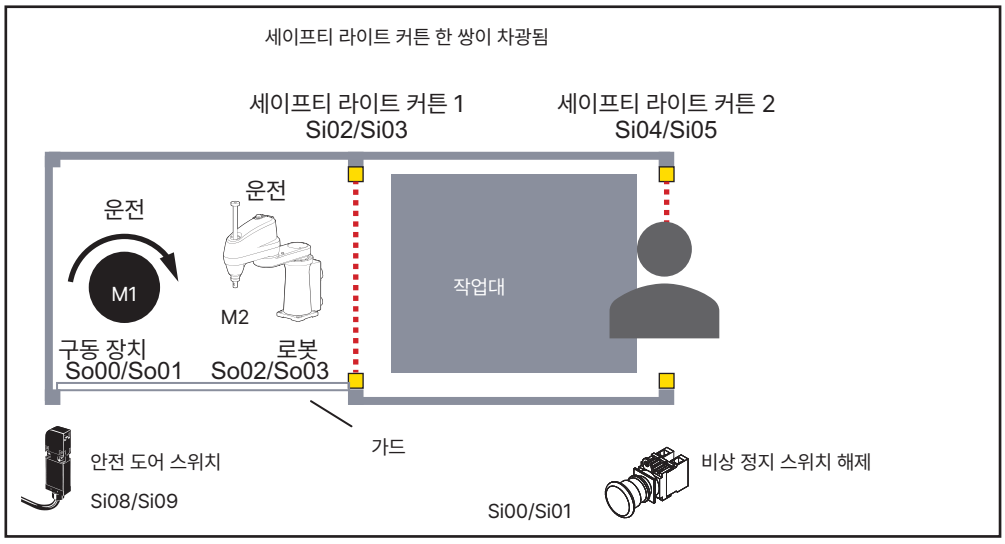
가드를 열면 구동 장치 M1과 로봇 M2가 모두 정지합니다.



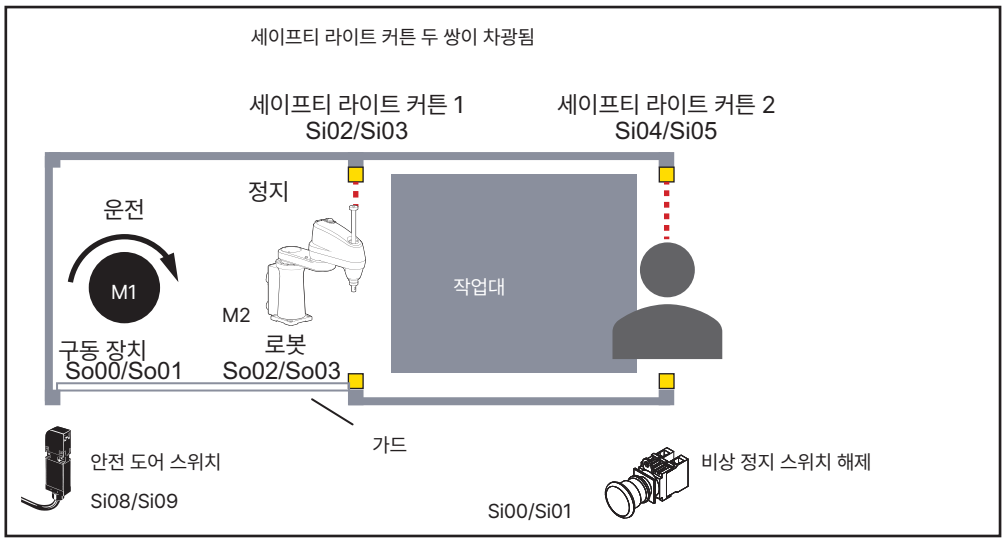
세이프티 라이트 커튼 두 쌍 중 한 쌍이 차광되어도 구동 장치 M1과 로봇 M2는 모두 계속 운전됩니다.



AI 번역본
For Reference Only-



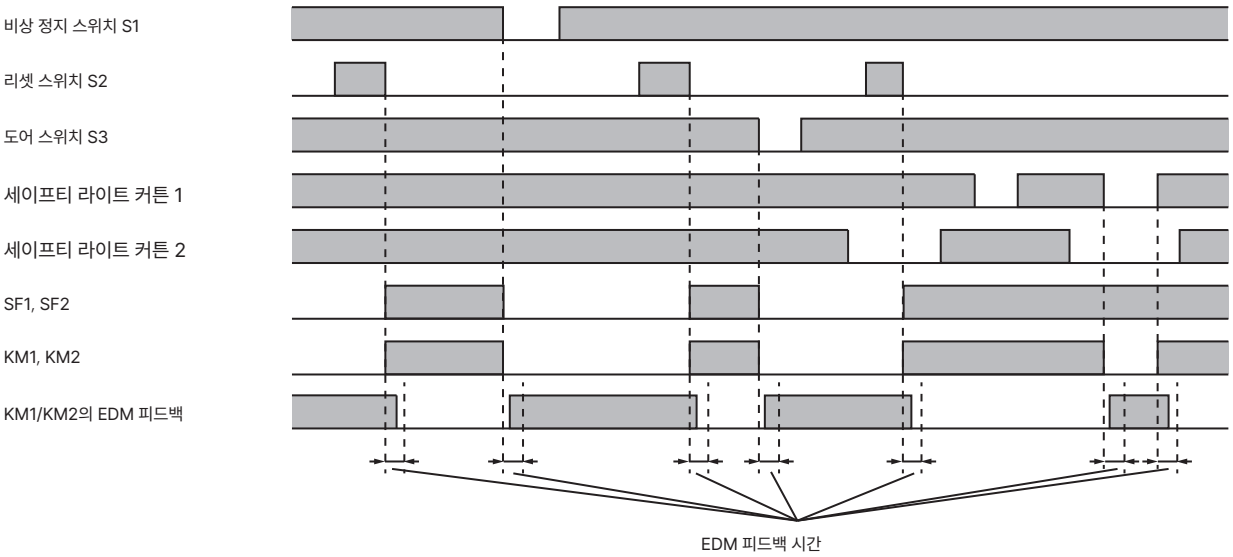
세이프티 라이트 커튼 두 쌍이 모두 차광되면 작업자와 로봇 M2가 접촉할 위험이 있으므로 로봇 M2가 정지합니다. 구동 장치 M1은 계속 운전됩니다.



AI 번역본
-For Reference Only-

● 타이밍 차트

타이밍 차트는 아래와 같습니다.



● I/O 구성 설정

I/O 구성 설정의 상세 내용은 다음과 같습니다.

입력

입력	기기	테스트 출력 모드	ON->OFF 지연 시간	OFF->ON 지연 시간	불일치 시간
Si00/T00	비상 정지 스위치 (듀얼 채널 등가 입력)	테스트 출력	0 ms	0 ms	500 ms
Si01/T01		테스트 출력	0 ms	0 ms	
Si02/T02	세이프티 라이트 커튼	전원 공급	0 ms	0 ms	500 ms
Si03/T03		표준 출력	0 ms	0 ms	
Si04/T04	세이프티 라이트 커튼	전원 공급	0 ms	0 ms	500 ms
Si05/T05		표준 출력	0 ms	0 ms	
Si06/T06	리셋 스위치	테스트 출력	0 ms	0 ms	-
Si07/T07	-	표준 출력	-	-	-
Si08/T08	안전 도어 스위치 (듀얼 채널 등가 입력)	테스트 출력	0 ms	0 ms	500 ms
Si09/T09		테스트 출력	0 ms	0 ms	
Si10/T10	EDM 피드백	테스트 출력	0 ms	0 ms	-
Si11/T11	-	미사용	-	-	-

입력 에러 래치 신호: 1,000 ms

AI 번역본
-For Reference Only-

출력

출력	기기	EDM 피드백 설정	ON->OFF 지연 시간	OFF->ON 지연 시간
So00/So01	듀얼 채널 등가 출력 (테스트 펄스 포함)	미사용	0 × 100 ms	0 × 100 ms
So02/So03	듀얼 채널 등가 출력 (테스트 펄스 포함)	Si10	0 × 100 ms	0 × 100 ms

출력 에러 래치 신호: 1,000 ms

로직

입력	기기	입력 유형	리셋 유형	So00/So01	So02/So03
Si00/Si01	비상 정지 스위치 (듀얼 채널 등가 입력)	-	수동 (Si06)	0	0
Si08/Si09	안전 도어 스위치 (듀얼 채널 등가 입력)	-	수동 (Si06)	0	0
Si02/Si03	세이프티 라이트 커튼	2 입력 (OR)	자동	1	0
Si04/Si05	세이프티 라이트 커튼				

리셋 신호	최소 ON 펄스 폭 [ms]	최대 ON 펄스 폭 [ms]
Si06	350	2,000

전원 투입 모드: 실행 중

서명

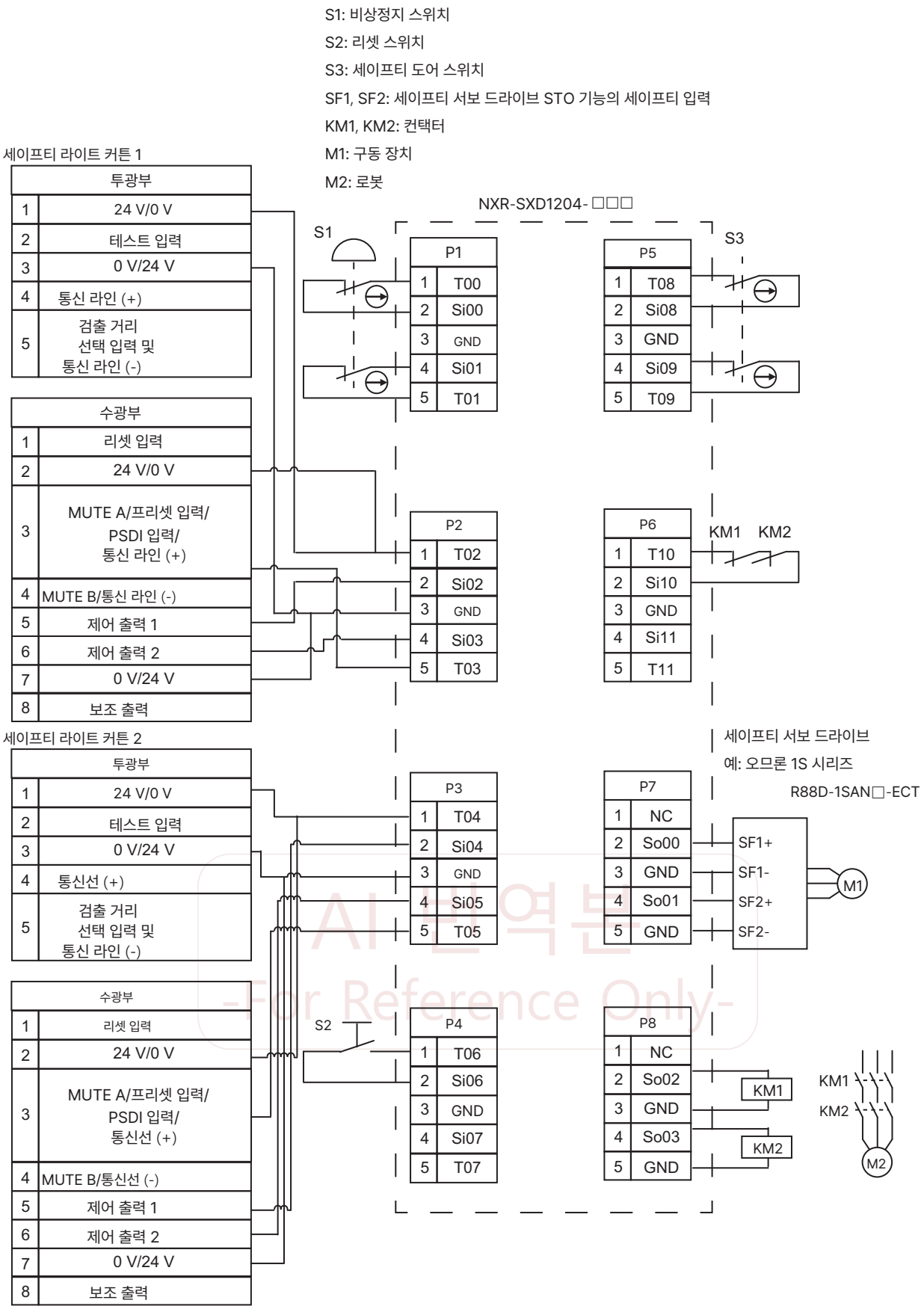
세이프티 컨피규레이션 CRC (SCCRC): F63EF4B6

세이프티 컨피규레이션 타임 스탬프 (SCTS): 4D0C00000000

AI 번역본
-For Reference Only-

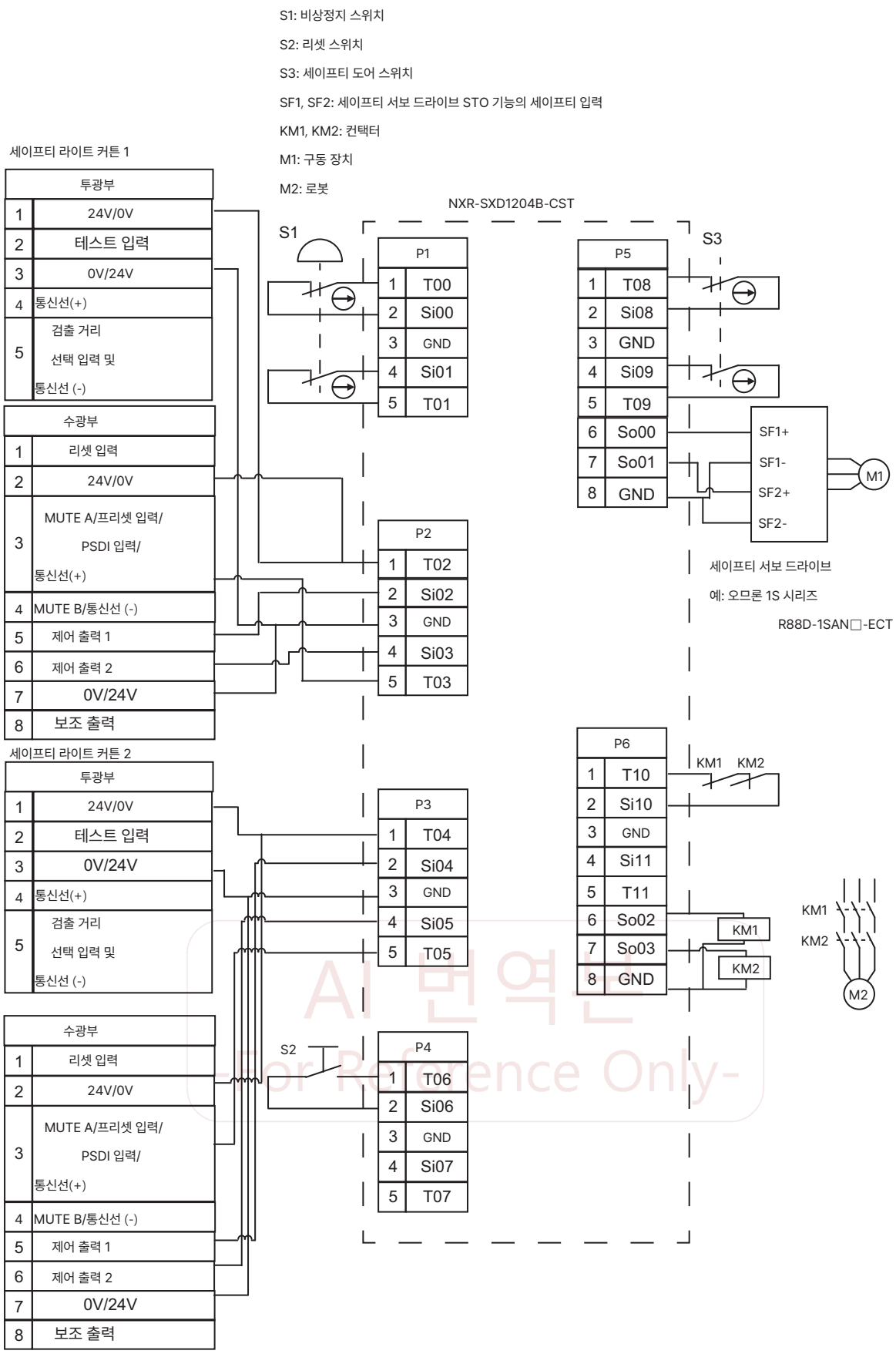
● 접속선도

NXR-SXD1204-□□□의 접속선도는 아래와 같습니다.



AI 번역본
-For Reference Only-

NXR-SXD1204B-CST의 결선도는 다음과 같습니다.



AI 번역본
-For Reference Only-

● 주의사항

사용상의 주의

- 시스템의 안전 요구 수준에 따라 접속할 기기를 선택하십시오.
- 세이프티 서보 드라이브의 경우, EDM을 사용하지 않고도 시스템의 안전 요구 수준을 달성할 수 있는 기기를 선택하십시오.
- 컨택터 접점의 용착을 검출하기 위해 매달 기능을 테스트하십시오.
- 서보 드라이브의 세이프티 입력 회로 고장을 검출하기 위해 6개월마다 기능을 테스트하십시오.
- 전체 시스템의 규격 적합성을 확보하는 것은 고객의 책임입니다.
- 전기적 및 기계적 고장을 검출하려면, 이중화된 반도체 출력 접점과 이중화된 기계식 출력 장치를 조합하여 사용하십시오.
- 가드와 관련된 인터록 장치가 무효화될 가능성을 최소화하기 위한 추가 조치는 ISO 14119:2013을 참조하십시오.

AI 번역본
-For Reference Only-

6-8 운전 모드

이 절에서는 세이프티 I/O 블록의 운전 모드에 대해 설명합니다.

6-8-1 운전 모드 종류

세이프티 I/O 블록에는 다음과 같은 운전 모드가 있습니다.
운전 모드는 Web UI의 MS 표시등 또는 운전 상태 모니터에서 확인할 수 있습니다.

운전 모드	표시 Web UI 내	MS 표시등 상태	리모트 I/O 모드에서의 동작	심플 로직 모드에서의 동작
운전 상태 (Executing)	Executing	점등 녹색	세이프티 I/O 블록이 운전 중일 때의 상태 모든 기능이 운전 중이며, 정상적인 운전이 수행되고 있습니다. 이 상태에서 주요 세이프티 기능의 상태는 다음과 같습니다. ・로직 기능: 무효 ・CIP Safety 통신: 접속 확립됨 ・세이프티 입력: 유효 ・세이프티 출력: 유효 운전 대기 상태(idle)에서 CIP Safety 접속이 개설되면 상태가 이 상태로 전환됩니다.	세이프티 I/O 블록이 운전 중일 때의 상태 모든 기능이 운전 중이며, 정상적인 운전이 수행되고 있습니다. 이 상태에서 주요 세이프티 기능의 상태는 다음과 같습니다. ・로직 기능: 실행 중 ・CIP Safety 통신: 통신 가능 ・세이프티 입력: 유효 ・세이프티 출력: 유효 운전 대기 상태(idle)에서 운전 모드 전환 기능에 의해 운전 상태로 전환하도록 지시되면, 이 상태로 전환됩니다.
운전 대기 상태 (Idle)	Idle	점멸 녹색	세이프티 구성이 완료되어 운전 상태(executing)로 전환하기를 대기하는 상태입니다. 이 상태에서 주요 세이프티 기능의 상태는 다음과 같습니다. ・로직 기능: 무효 ・CIP Safety 통신: 접속 확립 대기 중 ・세이프티 입력: 유효 ・세이프티 출력: 클리어 운전 상태(executing)에서 CIP Safety 접속이 모두 끊어지면, 상태가 이 상태로 전환됩니다.	세이프티 구성이 완료되어 운전 상태(executing)로 전환하기를 대기하는 상태입니다. 이 상태에서 주요 세이프티 기능의 상태는 다음과 같습니다. ・로직 기능: 정지 ・CIP Safety 통신: 통신 가능 ・세이프티 입력: 유효 ・세이프티 출력: 클리어 운전 상태(executing)에서 운전 모드 전환 기능에 의해 운전 대기 상태로 전환하도록 지시되면, 이 상태로 전환됩니다.
TUNID 설정 대기 상태 (Waiting for TUNID)	Waiting for TUNID	점멸 녹색 적색	TUNID가 설정되지 않은 상태입니다. 이 상태에서 IP 주소의 소프트웨어 설정을 구성할 수 있습니다.	
구성 대기 상태 (Configuring)	Configur-ing	점멸 녹색 적색	TUNID 설정이 완료되었으며, 세이프티 구성이 설정되지 않은 상태입니다.	
운전 중단 오류 (Abort)	Abort	점멸 적색	비치명적 오류가 발생 중입니다.	

AI 번역본
-For Reference Only-

운전 모드	표시 Web UI 내	MS 표시등 상태	리모트 I/O 모드에서의 동작	심플 로직 모드에서의 동작
치명적 결함 (Critical Fault)	Critical Fault	점등: 적색	치명적 결함이 발생 중입니다. 모든 기능이 정지하고 안전한 상태로 전환됩니다.	
초기화 (Self-Testing)	Self-Testing	점멸 녹색 적색	세이프티 기능을 보증하기 위해 필요한 자가진단을 실행 중인 상태입니다.	-
IP 주소 표시 (IP Address Display)	Web UI 액세스가 불가능 합니다	소등	IP 주소 표시 기능을 실행 중인 상태입니다.	-
I/O 배선 점검 (I/O Wiring Checking)	판독 불가능 합니다. Web UI 액세스 불가능 합니다.	소등	I/O 배선 점검 기능을 실행 중인 상태입니다.	-

6-8-2 각 운전 모드에서 실행 가능한 기능

각 운전 모드에서 각 기능을 실행할 수 있는지 여부는 다음과 같습니다.

기능	일반 운전 모드							특수 모드	
	초기화 (Self-Testing)	TUNID 설정 대기 상태(Waiting for TUNID)	구성 대기 상태(Configuring)	운전 대기 상태(Idle)	운전 상태 (Executing)	운전 중단 오류 (Abort)	치명적 결함 (Critical Fault)	IP 주소 표시 (IP Address Display)	I/O 배선 점검(I/O Wiring Checking)
CIP Safety 통신	불가능	불가능	불가능	가능	가능	불가능	불가능	불가능	불가능
EtherNet/IP 통신	불가능	불가능	불가능	가능	가능	불가능	불가능	불가능	불가능
CIP 메시지 통신	불가능	가능	가능	가능	가능	가능	불가능	불가능	불가능
Web UI에서의 액세스	불가능	가능	가능	가능	가능	가능	불가능	불가능	불가능
세이프티 입력 기능	불가능	불가능	불가능	가능	가능	가능	불가능	불가능	가능*1
테스트 출력 기능	불가능	불가능	불가능	가능	가능	가능	불가능	불가능	가능*1

AI 번역본
For Reference Only

기능	일반 운전 모드							특수 모드	
	초기화 (Self-Testing)	TUNID 설정 대기 상태 (Waiting for TUNID)	구성 대기 상태 (Configuring)	운전 대기 상태 (Idle)	운전 상태 (Executing)	운전 중단 오류 (Abort)	치명적 결함 (Critical Fault)	IP 주소 표시 (IP Address Display)	I/O 배선 점검 (I/O Wiring Checking)
세이프티 출력 기능	불가능	불가능	불가능	불가능	가능	가능	불가능	불가능	가능*1
IP 주소 설정 기능	불가능	가능	불가능	불가능	불가능	불가능	불가능	불가능	불가능
스루 배선 출력용 전원 OFF 기능	불가능	가능	가능	가능	가능	가능	불가능	불가능	불가능
심플 로직 기능	불가능	불가능	불가능	불가능	가능*2	불가능	불가능	불가능	가능*1
I/O 배선 점검 기능	불가능	불가능	불가능	불가능	불가능	불가능	불가능	불가능	가능
IP 주소 표시 기능	불가능	불가능	불가능	불가능	불가능	불가능	불가능	가능	불가능
백업 기능의 백업	불가능	불가능	불가능	가능	가능	불가능	불가능	불가능	불가능
백업 기능의 검증	불가능	가능	가능	가능	가능	가능	불가능	불가능	불가능
백업 기능의 복원	불가능	가능	가능	가능*3	가능*3	가능	불가능	불가능	불가능
펌웨어 업데이트 기능	불가능	가능	가능	가능*3	가능*3	가능	불가능	불가능	불가능
세이프티 비밀번호 변경	불가능	가능	가능	가능	가능	가능	불가능	불가능	불가능
운전 모드 전환 기능	불가능	불가능	불가능	가능	가능	불가능	불가능	불가능	불가능
구성 잠금 기능	불가능	불가능	불가능	가능	가능	가능*4	불가능	불가능	불가능
재시작 기능	불가능	가능	가능	가능*3	가능*3	가능	불가능	불가능	불가능

AI 번역본
-For Reference Only-

기능	일반 운전 모드							특수 모드	
	초기화 중 (Self-Testing)	TUNID 설정 대기 상태 (Waiting for TUNID)	구성 대기 상태 (Configuring)	운전 대기 상태 (Idle)	운전 상태 (Executing)	운전 중단 에러 (Abort)	치명적 폴트 (Critical Fault)	IP 주소 표시 (IP Address Display)	I/O 배선 점검 (I/O Wiring Checking)
전체 메모리 클리어 기능	불가능	가능	가능	가능*3	가능*3	가능	불가능	불가능	불가능

***1.** I/O 배선 점검 전용 설정으로 동작합니다.
***2.** 리모트 I/O 모드에서는 심플 로직 처리 기능이 동작하지 않습니다. CIP
***3.** Safety 통신 접속이 확립되어 있는 동안에는 불가능합니다.
***4.** 구성의 잠금 해제만 가능합니다.

6-8-3 각 운전 모드에서 실행 가능한 Web UI 기능

각 운전 모드에서 각 Web UI 기능의 실행 가능 여부는 다음과 같습니다.

화면	기능	운전 모드				
		TUNID 설정 대기 상태 (Waiting for TUNID)	구성 대기 상태 (Configuring)	운전 대기 상태 (Idle)	운전 상태 (Executing)	운전 중단 에러 (Abort)
운전 상태 모니터 화면	운전 상태 모니터	가능	가능	가능	가능	가능
I/O 모니터 화면	I/O 모니터	가능	가능	가능	가능	가능
현재 에러/이벤트 로그 화면	현재 에러 표시	가능	가능	가능	가능	가능
	이벤트 로그 표시 및 파일 출력	가능	가능	가능	가능	가능
	이벤트 로그 클리어	가능	가능	가능	가능	가능
생산 정보 화면	생산 정보 표시	가능	가능	가능	가능	가능
TCP/IP 설정 화면	TCP/IP 설정 쓰기	가능	불가능	불가능	불가능	불가능
	TCP/IP 설정 읽기	가능	가능	가능	가능	가능
TUNID 설정 화면	TUNID 쓰기	가능	불가능	불가능	불가능	불가능
	TUNID 읽기	가능	가능	가능	가능	가능
세이프티 애플리케이션 설정 화면	세이프티 애플리케이션 설정 표시	가능	가능	가능	가능	가능
	세이프티 애플리케이션 설정 쓰기 및 삭제	가능	가능	가능	가능	가능
자동 시계 조정 설정 화면	자동 시계 조정 설정 쓰기	가능	가능	가능	가능	가능
	자동 시계 조정 설정 읽기	가능	가능	가능	가능	가능

AI 번역본 -For Reference Only

화면	기능	운전 모드				
		TUNID 설정 대기 상태 (Waiting for TUNID)	구성 대기 상태 (Configuring)	운전 대기 상태 (Idle)	운전 상태 (Executing)	운전 중단 에러 (Abort)
운전 모드 변경 화면	운전 모드 변경	불가능	불가능	가능	가능	불가능
컨피규레이션 잠금 화면	컨피규레이션 잠금	불가능	불가능	가능	가능	불가능
	구성 잠금 해제	불가능	불가능	가능	가능	가능
재시작 화면	재시작	가능	가능	가능*1	가능*1	가능
전체 메모리 클리어 화면	전체 메모리 클리어	가능	가능	가능*1	가능*1	가능
백업	백업	불가능	불가능	가능	가능	불가능
	검증	가능	가능	가능	가능	가능
	복원	가능	가능	가능*1	가능*1	가능
일반 CIP 명령 전송 화면	일반 CIP 명령 전송	가능	가능	가능	가능	가능
유닛 식별 화면	유닛 식별	가능	가능	가능	가능	가능
통신 케이블 진단 화면	통신 케이블 진단	가능	가능	가능	가능	가능
세이프티 패스워드 설정 화면	세이프티 패스워드 설정	가능	가능	가능	가능	가능
펌웨어 업데이트 화면	펌웨어 업데이트	가능	가능	가능*1	가능*1	가능

***1.** CIP Safety 통신 접속이 확립되어 있는 동안에는 불가능합니다.

6-8-4 운전 모드 전환 및 전원 투입 시 모드

사용할 세이프티 애플리케이션이 고정 애플리케이션, 사용자 정의 애플리케이션, 또는 애드온 애플리케이션인 경우에는, 로직 기능의 실행과 정지를 전환하려면 운전 모드를 변경해야 합니다.
운전 모드를 변경하는 절차는 Sysmac Studio 또는 Web UI를 사용하는 방법으로 7-95페이지의 7-16 운전 모드 변경을 참조하십시오.
또한 세이프티 애플리케이션의 설정에서 전원 투입 시의 운전 모드를 지정할 수 있습니다.
전원 투입 모드에 따른 동작의 차이는 다음과 같습니다.

전원 투입 모드	동작
Executing	· 전원 투입 시 운전 상태가 되며, 로직 기능이 자동으로 실행됩니다. · 고정 애플리케이션의 전원 투입 모드는 Executing으로 설정되어 있으므로, TUNID가 설정된 상태에서 전원을 다시 투입하면 운전 상태로 기동합니다. · 사용자 정의 애플리케이션에서 Type1 Safety Open을 사용하여 구성을 완료하면 즉시 운전 상태로 전환됩니다.

-For Reference Only-

전원 투입 모드	동작
Idle	· 전원 투입 시 운전 대기 상태가 되며, 로직 기능이 정지된 상태로 기동합니다.

AI 번역본
-For Reference Only-

7

세이프티 I/O 블록 설정

이 장에서는 세이프티 I/O 블록의 다양한 설정에 대해 설명합니다.

7-1 설정 절차 7-3
7-1-1 세이프티 컨트롤러가 제어를 수행하기 위한 구성의 설정 절차 (Type 1 Safety Open을 사용하는 구성) 7-3
7-1-2 세이프티 컨트롤러가 제어를 수행하기 위한 구성의 설정 절차 (Web UI를 사용하는 구성) 7-6
7-1-3 세이프티 I/O 블록이 제어를 수행하기 위한 구성의 설정 절차 (사전 설정된 세이프티 애플리케이션 사용) 7-9
7-1-4 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하기 위한 구성(집중 관리형)의 설정 절차 7-11
7-1-5 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하기 위한 구성(분산 관리형)의 설정 절차 7-14

7-2 Web UI 개요 7-17
7-2-1 Web UI의 각종 사양 7-17
7-2-2 Web UI의 조작 권한 7-17
7-2-3 Web UI의 화면 구성 7-17
7-2-4 메인 메뉴 목록 7-18
7-2-5 Web UI 시작 절차 7-21
7-2-6 로그인 7-22
7-2-7 로그아웃 7-24
7-2-8 최초 로그인 시 주의사항 7-24

7-3 CIP Safety 통신 설정 7-27
7-3-1 CIP Safety 통신을 위한 접속 설정 7-27
7-3-2 세이프티 I/O 블록 설정의 익스포트 및 임포트 7-36

7-4 EtherNet/IP 통신 설정 7-38
7-4-1 태그 데이터 링크 통신 설정 7-38
7-4-2 LLDP 기능 7-42

7-5 세이프티 입력 기능 설정 7-44
7-5-1 세이프티 입력 기능의 설정 절차 7-44
7-5-2 표준 출력 기능의 설정 절차 7-47

7-6 세이프티 출력 기능 설정 7-50
7-6-1 세이프티 출력 기능 설정 절차 7-50

7-7 로직 기능 설정 7-53
7-7-1 로직 설정 절차 7-53
7-7-2 파라미터 목록 표시 7-58

A 배포본 -For Reference Only-

7-7-3 고려해야 할 입력 기기의 이상 동작 예 7-59

7-8 세이프티 시그니처 설정 7-63

7-9 세이프티 애플리케이션 파일 작성 7-65
7-9-1 세이프티 I/O 블록 등록 7-65
7-9-2 세이프티 애플리케이션 설정 7-66
7-9-3 세이프티 I/O 기능 설정 7-68
7-9-4 로직 기능 설정 7-68
7-9-5 세이프티 애플리케이션 파일 익스포트 7-68

7-10 IP 주소 설정 7-71
7-10-1 IP 주소 구성 7-71
7-10-2 로터리 스위치를 사용한 IP 주소 설정 방법 선택 7-73
7-10-3 Sysmac Studio에 의한 설정 7-74
7-10-4 Web UI에 의한 설정 7-76

7-11 TUNID 설정 7-78
7-11-1 TUNID의 목적 7-78
7-11-2 TUNID 설정 절차 7-78

7-12 세이프티 애플리케이션 선택 7-83

7-13 재시작 7-84
7-13-1 재시작의 목적 7-84
7-13-2 재시작 사용 절차 7-84

7-14 구성 7-87
7-14-1 세이프티 컨트롤러 구성 7-87
7-14-2 세이프티 I/O 블록의 구성 7-87

7-15 자동 시계 조정 설정 7-91
7-15-1 자동 시계 조정의 목적 7-91
7-15-2 자동 시계 조정 사용 절차 7-91
7-15-3 자동 시계 조정 상세 7-94

7-16 동작 모드 변경 7-95
7-16-1 동작 모드 변경 사용 절차 7-95

7-17 컨피규레이션 잠금 7-99
7-17-1 컨피규레이션 잠금의 목적 7-99
7-17-2 컨피규레이션 잠금 사용 절차 7-99
7-17-3 컨피규레이션 잠금 상세 7-103

7-18 세이프티 비밀번호 설정 7-104
7-18-1 세이프티 비밀번호의 목적 7-104
7-18-2 세이프티 비밀번호 설정 사용 절차 7-104
7-18-3 세이프티 비밀번호 상세 7-106

7-19 백업 7-108
7-19-1 백업의 목적 7-108
7-19-2 백업 사용 절차 7-108
7-19-3 백업 상세 7-111

AI 번역본
-For Reference Only-

7-1 설정 절차

세이프티 I/O 블록의 설정 절차는 세이프티 제어 시스템에 따라 다릅니다.
세이프티 제어 시스템 구성에 대한 자세한 내용은 1-4페이지의 1-3-1 세이프티 제어 시스템을 참조하십시오.

사용상의 주의

Sysmac Studio에서 세이프티 I/O 블록의 설정을 변경한 경우, 동기화 전송을 실행하여 Sysmac Studio의 설정 정보를 세이프티 I/O 블록에 적용하십시오. Sysmac Studio의 동기화 전송에 대한 자세한 내용은 Sysmac Studio Version 1 Operation Manual (Cat. No. W504)을 참조하십시오.

7-1-1 세이프티 컨트롤러가 제어를 수행하기 위한 구성의 설정 절차 (Type 1 Safety Open을 사용하는 구성)

다음은 세이프티 컨트롤러가 제어를 수행하기 위한 구성(Type 1 Safety Open을 사용하는 구성)의 설정 절차를 보여줍니다.

설치 및 배선 전의 절차는 다음과 같습니다.

단계	설정 항목	사용 지원 소프트웨어 사용	설명	참조
1	세이프티 컨트롤러 및 세이프티 I/O 블록 간의 CIP Safety 통신을 설정	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 컨트롤러와 세이프티 I/O 블록 간의 CIP Safety 통신 설정을 구성합니다. **오픈 타입으로 Configure Target Device (Type1)를** 선택합니다.	7-3 CIP Safety 통신 설정 (7-27 페이지)
2	EtherNet/IP 통신을 설정	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 표준 컨트롤러와 세이프티 I/O 블록 간의 EtherNet/IP 통신 설정을 구성합니다.	7-4 EtherNet/IP 통신 설정 (7-38 페이지)
3	세이프티 애플리케이션을 설정	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 애플리케이션 설정을 구성합니다. 00: Remote I/O mode를 선택합니다.	7-9-2 세이프티 애플리케이션 설정 (7-66페이지)
4	세이프티 I/O 기능을 설정	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 I/O 블록의 I/O 구성 설정을 구성합니다.	7-5 세이프티 입력 기능 설정 (7-44 페이지) 7-6 세이프티 출력 기능 설정 (7-50페이지)

설치 및 배선 후의 절차는 다음과 같습니다.

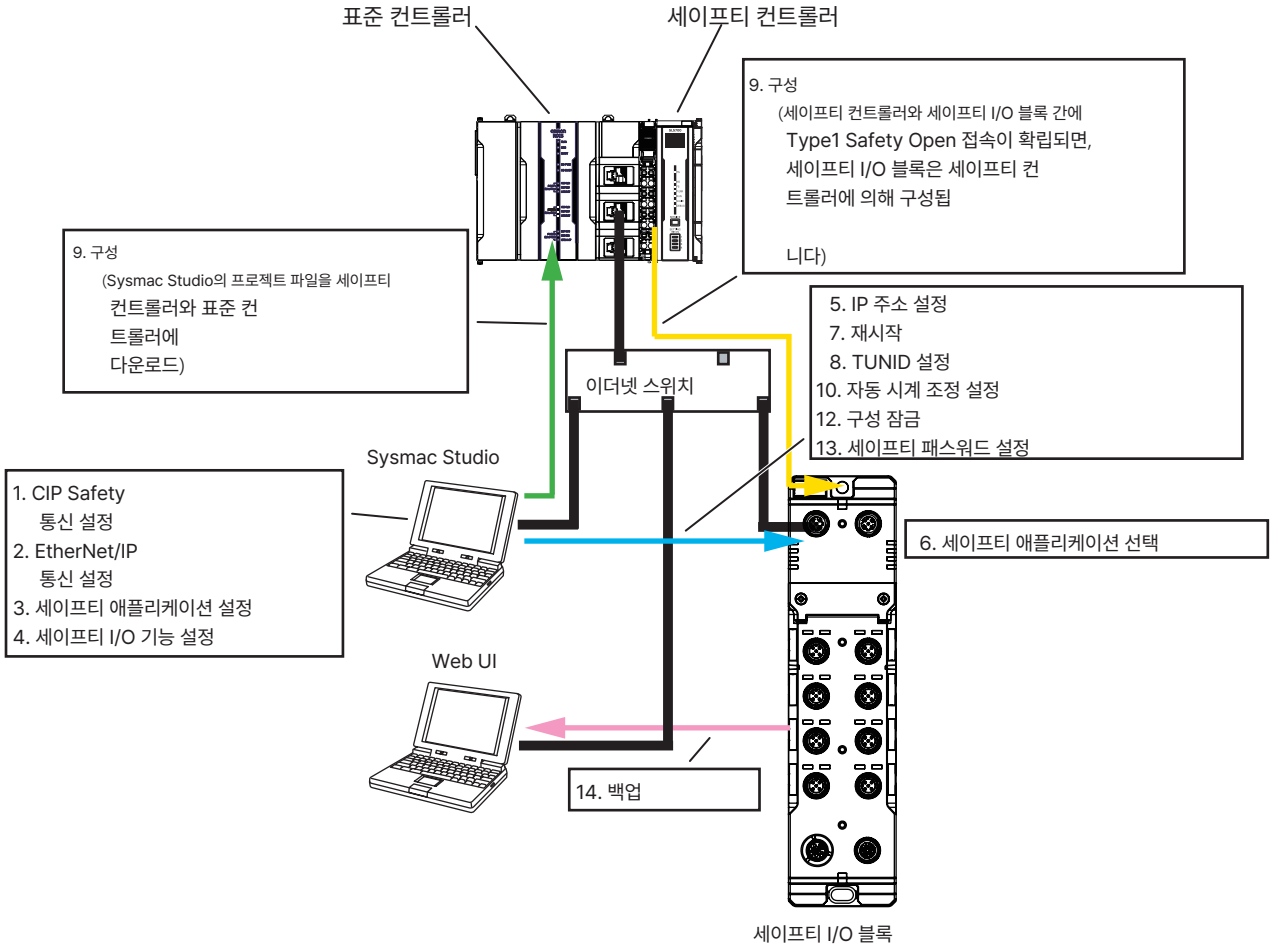
단계	설정 항목	사용 지원 소프트웨어 사용	설명	참조
5	IP 주소를 설정	Sysmac Studio*1	세이프티 I/O 블록의 IP 주소 설정을 구성합니다.	7-10 IP 주소 설정 (7-71페이지)
6	세이프티 애플리케이션을 선택	-	세이프티 I/O 블록의 SETTING 로터리 스위치 SW1과 SW2를 모두 0으로 설정합니다.	7-12 세이프티 애플리케이션 선택 (7-83 페이지)
7	재시작	Sysmac Studio*1	세이프티 I/O 블록을 재시작합니다.	7-13 재시작 (7-84 페이지)
8	TUNID를 설정	Sysmac Studio*1	세이프티 I/O 블록의 TUNID 설정을 구성합니다.	7-11 TUNID 설정 (7-78페이지)

AI 번역본
-For Reference Only-

단계	설정 항목	사용 지원 소프트웨어 사용	설명	참조
9	구성	Sysmac Studio	Sysmac Studio의 프로젝트 파일을 다운로드하여 세이프티 컨트롤러와 표준 컨트롤러를 구성합니다. 세이프티 컨트롤러와 세이프티 I/O 블록 간에 Type1 Safety Open 접속이 확립되면 세이프티 컨트롤러가 세이프티 I/O 블록을 구성합니다.	7-14 구성 (7-87페이지)
10	자동 시계 조정을 설정	Sysmac Studio*1	세이프티 I/O 블록의 자동 시계 조정 설정을 구성합니다.	7-15 자동 시계 조정 설정 (7-91페이지)
11	동작을 확인	-	모든 I/O 배선과 프로그램의 동작을 확인하여 세이프티 I/O 블록이 의도한 대로 동작하는지 확인합니다.	-
12	구성을 잠금	Sysmac Studio*1	세이프티 제어 시스템의 세이프티 밸리데이션을 실행하여 설정값이 올바른지 확인합니다. 확인 후 구성 잠금을 실행합니다. 구성 잠금을 실행한 후에는 잠금이 해제될 때까지 세이프티 I/O 블록의 설정값을 변경할 수 없습니다.	7-17 컨피규레이션 잠금 (7-99페이지)
13	세이프티 비밀번호를 설정	Sysmac Studio*1	세이프티 I/O 블록의 세이프티 패스워드 설정을 구성합니다.	7-18 세이프티 비밀번호 설정 (7-104페이지)
14	백업	Web UI	세이프티 I/O 블록의 백업 파일을 작성합니다.	7-19 백업 (7-108페이지)

***1.** 이 설정은 Web UI를 사용하여 구성할 수도 있습니다.

AI 번역본
-For Reference Only-



AI 번역본
-For Reference Only-

7-1-2 세이프티 컨트롤러가 제어를 수행하기 위한 구성의 설정 절차 (Web UI를 사용하는 구성)

다음은 세이프티 컨트롤러가 제어를 수행하기 위한 구성(Web UI를 사용하는 구성)의 설정 절차를 보여줍니다.
설치 및 배선 전의 절차는 다음과 같습니다.

단계	설정 항목		사용 지원 소프트웨어 사용	설명	참조
1	리모트 I/O 모드 세이프티 애플리케이션*1	세이프티 애플리케이션 파일 작성	Sysmac Studio	세이프티 애플리케이션 파일을 익스포트하기 위한 프로젝트 파일을 작성합니다. 이 프로젝트 파일로 세이프티 애플리케이션 파일의 익스포트를 실행합니다. 이 세이프티 애플리케이션 파일에는 I/O 구성 설정만 정의합니다.	7-9 세이프티 애플리케이션 파일 작성 (7-65페이지)
2	세이프티 컨트롤러의 세이프티 프로그램을 위한 프로젝트 파일을 작성*1	CIP Safety 통신을 설정	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 컨트롤러와 세이프티 I/O 블록 간의 CIP Safety 통신 설정을 구성합니다. 오픈 타입으로 Check Safety **Signature (Type2a)를 선택합니다.**	7-3 CIP Safety 통신 설정 (7-27페이지)
3		표준 컨트롤러와 EtherNet/IP 통신을 설정	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 표준 컨트롤러와 세이프티 I/O 블록 간의 EtherNet/IP 통신 설정을 구성합니다.	7-4 EtherNet/IP 통신 설정 (7-38페이지)
4		세이프티 애플리케이션을 설정	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 애플리케이션 설정을 구성합니다. 00: Remote I/O mode를 선택합니다.	7-9-2 세이프티 애플리케이션 설정 (7-66페이지)
5		세이프티 시그니처를 설정	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 시그니처 설정을 구성합니다. 7-9-5 세이프티 애플리케이션 파일 익스포트 (7-68페이지)에 기록된 SCCRC와 SCTS를 입력합니다.	7-8 세이프티 시그니처 설정 (7-63페이지)

***1.** 세이프티 애플리케이션 파일 익스포트용 프로젝트 파일과 세이프티 컨트롤러의 세이프티 프로그램용 프로젝트 파일은 별도로 작성하십시오.

설치 및 배선 후의 절차는 다음과 같습니다.
세이프티 컨트롤러를 설정하려면 세이프티 프로그램용 프로젝트 파일을 사용하십시오.

AI 번역본

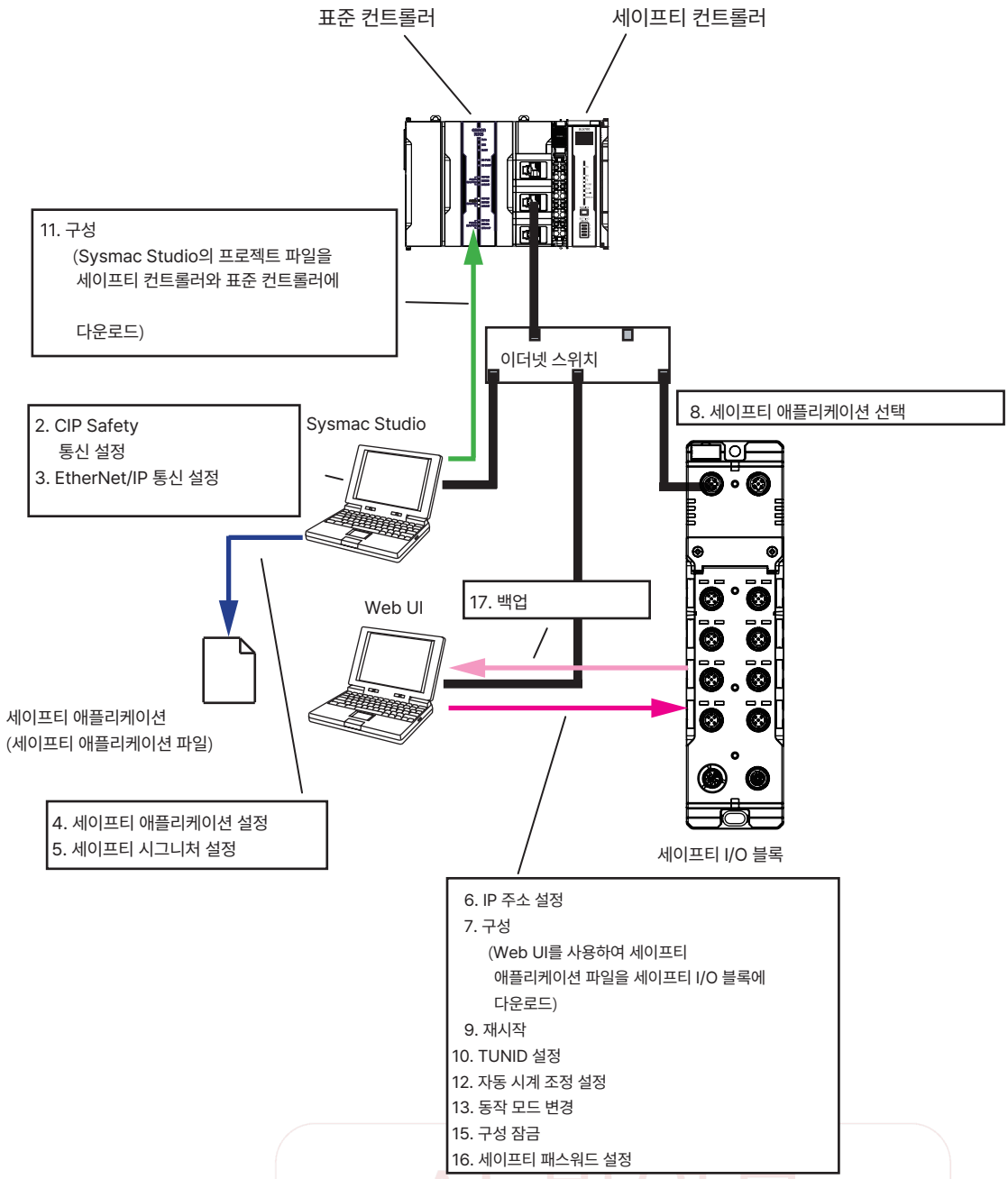
단계	설정 항목	사용 지원 소프트웨어 사용	설명	참조
6	IP 주소를 설정	Web UI*1	세이프티 I/O 블록의 IP 주소 설정을 구성합니다.	7-10 IP 주소 설정 (7-71 페이지)
7	구성 (세이프티 I/O 블록 측)	Web UI	Web UI를 사용하여 세이프티 애플리케이션 파일을 세이프티 I/O 블록에 다운로드함으로써 세이프티 I/O 블록을 구성합니다. Remote I/O mode용 세이프티 애플리케이션 파일을 사용하십시오. 애드온 애플리케이션용 세이프티 애플리케이션 파일은 사용할 수 없습니다.	7-14-2 세이프티 I/O 블록의 구성 (7-87페이지)
8	세이프티 애플리케이션을 선택	-	세이프티 I/O 블록의 SETTING 로터리 스위치 SW1과 SW2를 모두 0으로 설정합니다.	7-12 세이프티 애플리케이션 선택 (7-83페이지)

단계	설정 항목	사용 지원 소프트웨어 사용	설명	참조
9	재시작	Web UI*1	세이프티 I/O 블록을 재시작합니다.	7-13 재시작 (7-84페이지)
10	TUNID를 설정	Web UI*1	세이프티 I/O 블록의 TUNID 설정을 구성합니다.	7-11 TUNID 설정 (7-78페이지)
11	구성 (세이프티 컨트롤러 및 표준 컨트롤러 측)	Sysmac Studio	Sysmac Studio의 프로젝트 파일을 다운로드하여 세이프티 컨트롤러와 표준 컨트롤러를 구성합니다.	7-14-1 세이프티 컨트롤러 구성 (7-87페이지)
12	자동 시계 조정을 설정	Web UI*1	세이프티 I/O 블록의 자동 시계 조정 설정을 구성합니다.	7-15 자동 시계 조정 설정 (7-91페이지)
13	동작 모드 변경 *2	Web UI*1	세이프티 I/O 블록의 동작 모드를 Executing으로 변경합니다.	7-16 동작 모드 변경 (7-95 페이지)
14	동작을 확인	-	모든 I/O 배선과 프로그램의 동작을 확인하여 세이프티 I/O 블록이 의도한 대로 동작하는지 확인합니다.	-
15	구성 잠금	Web UI*1	세이프티 제어 시스템의 세이프티 밸리데이션을 실행하여 설정값이 올바른지 확인합니다. 확인 후 구성 잠금을 실행합니다. 구성 잠금을 실행한 후에는 세이프티 I/O 블록의 설정값이 잠금 해제 전까지 변경되지 않습니다.	7-17 구성 잠금 (7-99페이지)
16	세이프티 패스워드 설정	Web UI*1	세이프티 I/O 블록의 세이프티 패스워드 설정을 구성합니다.	7-18 세이프티 비밀번호 설정 (7-104 페이지)
17	백업	Web UI	세이프티 I/O 블록의 백업 파일을 작성합니다.	7-19 백업 (7-108페이지)

***1.** 이 설정은 Sysmac Studio를 사용하여 구성할 수도 있습니다.

***2.** 이 설정은 4단계 로직 기능 설정에서 파워온 모드를 Idle로 설정한 경우에만 필요합니다. 파워온 모드를 Executing으로 설정한 경우에는 필요하지 않습니다.

AI 번역본
-For Reference Only-



AI 번역본
-For Reference Only-

7-1-3 세이프티 I/O 블록이 제어를 수행하기 위한 구성의 설정 절차 (사전 설정된 세이프티 애플리케이션 사용)

다음은 세이프티 I/O 블록이 사전 설정된 세이프티 애플리케이션을 사용하여 제어를 수행하기 위한 구성의 설정 절차를 보여줍니다.
설치 및 배선 전의 절차는 다음과 같습니다.

단계	설정 항목	사용 지원 소프트웨어 사용	설명	참조
1	CIP Safety를 설정 통신*1	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 컨트롤러와 세이프티 I/O 블록 간의 CIP Safety 통신 설정을 구성합니다. 오픈 타입으로 Check Safety Signature **(Type2a)를 선택합니다.**	7-3 CIP Safety 통신 설정 (7-27 페이지)
2	표준 컨트롤러와 EtherNet/IP 통신을 설정*2	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 표준 컨트롤러와 세이프티 I/O 블록 간의 EtherNet/IP 통신 설정을 구성합니다.	7-4 EtherNet/IP 통신 설정 (7-38 페이지)
3	세이프티 애플리케이션을 설정*1	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 애플리케이션 설정을 구성합니다. 사용할 고정 애플리케이션을 선택합니다.	7-9-2 세이프티 애플리케이션 설정 (7-66페이지)

***1.** 세이프티 컨트롤러를 사용하지 않는 경우, 이 설정은 필요하지 않습니다.
***2.** 표준 컨트롤러를 사용하지 않는 경우, 이 설정은 필요하지 않습니다.

설치 및 배선 후의 절차는 다음과 같습니다.

단계	설정 항목	사용 지원 소프트웨어 사용	설명	참조
4	IP 주소를 설정*1	Web UI*2	세이프티 I/O 블록의 IP 주소 설정을 구성합니다.	7-10 IP 주소 설정 (7-71페이지)
5	TUNID를 설정	Web UI*2	세이프티 I/O 블록의 TUNID 설정을 구성합니다.	7-11 TUNID 설정 (7-78페이지)
6	세이프티 애플리케이션을 선택	-	세이프티 I/O 블록의 SETTING 로터리 스위치 SW1과 SW2를 사용할 세이프티 애플리케이션(고정 애플리케이션)의 번호 1-3 중 하나로 설정합니다.	7-12 세이프티 애플리케이션 선택 (7-83 페이지)
7	재시작	Web UI*2	세이프티 I/O 블록을 재시작합니다.	7-13 재시작 (7-84 페이지)
8	구성*3	Sysmac Studio	Sysmac Studio의 프로젝트 파일을 다운로드하여 세이프티 컨트롤러와 표준 컨트롤러를 구성합니다. 세이프티 I/O 블록의 구성은 필요하지 않습니다.	7-14-1 세이프티 컨트롤러 구성 (7-87페이지)
9	자동 시계 조정을 설정	Web UI*2	세이프티 I/O 블록의 자동 시계 조정 설정을 구성합니다.	7-15 자동 시계 조정 설정 (7-91페이지)
10	동작을 확인	-	모든 I/O 배선과 프로그램의 동작을 확인하여 세이프티 I/O 블록이 의도한 대로 동작하는지 확인합니다.	-
11	구성을 잠금	Web UI*2	세이프티 제어 시스템의 세이프티 밸리데이션을 실행하여 설정값이 올바른지 확인합니다. 확인 후 구성 잠금을 실행합니다. 구성 잠금을 실행한 후에는 잠금이 해제될 때까지 세이프티 I/O 블록의 설정값을 변경할 수 없습니다.	7-17 컨피규레이션 잠금 (7-99페이지)

AI 번역본
-For Reference Only-

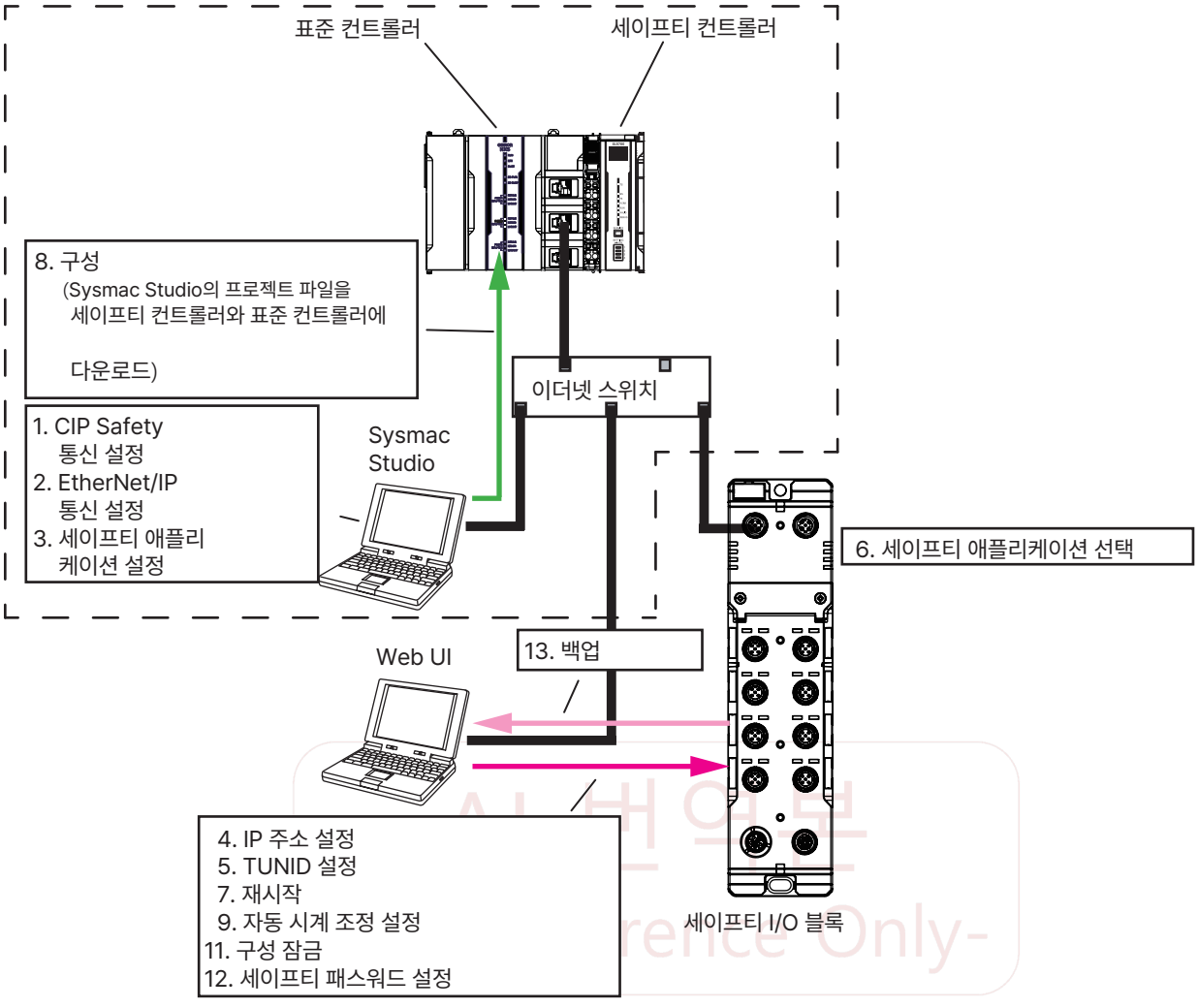
단계	설정 항목	사용 지원 소프트웨어 사용	설명	참조
12	세이프티 비밀번호를 설정	Web UI*2	세이프티 I/O 블록의 세이프티 패스워드 설정을 구성합니다.	7-18 세이프티 비밀번호 설정 (7-104페이지)
13	백업	Web UI	세이프티 I/O 블록의 백업 파일을 작성합니다.	7-19 백업 (7-108페이지)

***1.** 세이프티 컨트롤러와 표준 컨트롤러를 모두 사용하지 않는 경우, 이 설정은 필요하지 않습니다. 이 경우 세이프티 I/O 블록은 기본 IP 주소로 동작합니다.

***2.** 이 설정은 Sysmac Studio를 사용하여 구성할 수도 있습니다.

***3.** 세이프티 컨트롤러와 표준 컨트롤러를 모두 사용하지 않는 경우, 이 설정은 필요하지 않습니다.

세이프티 컨트롤러와 표준 컨트롤러를 모두 사용하지 않는 경우, 점선 안쪽은 필요하지 않습니다.



7-1-4 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하기 위한 구성(집중 관리형)의 설정 절차

다음은 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하기 위한 구성(집중 관리형)의 설정 절차를 보여줍니다.
설치 및 배선 전의 절차는 다음과 같습니다.

단계	설정 항목	사용 지원 소프트웨어 사용	설명	참조
1	CIP Safety 통신을 설정	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 컨트롤러와 세이프티 I/O 블록 간의 CIP Safety 통신 설정을 구성합니다. 오픈 타입으로 Configure Target Device **(Type1)를 선택합니다.**	7-3 CIP Safety 통신 설정 (7-27 페이지)
2	표준 컨트롤러와 EtherNet/IP 통신을 설정*1	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 표준 컨트롤러와 세이프티 I/O 블록 간의 EtherNet/IP 통신 설정을 구성합니다.	7-4 EtherNet/IP 통신 설정 (7-38 페이지)
3	세이프티 애플리케이션을 설정	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 애플리케이션 설정을 구성합니다. 15: User defined를 선택합니다.	7-9-2 세이프티 애플리케이션 설정 (7-66페이지)
4	세이프티 I/O 기능을 설정	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 I/O 블록의 I/O 구성 설정을 구성합니다.	7-5 세이프티 입력 기능 설정 (7-44 페이지) 7-6 세이프티 출력 기능 설정 (7-50페이지)
5	로직 기능을 설정	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 I/O 블록의 로직 및 파워온 모드 설정을 구성합니다.	7-7 로직 기능 설정 (7-53페이지)

***1.** 표준 컨트롤러를 사용하지 않는 경우, 이 설정은 필요하지 않습니다.

설치 및 배선 후의 절차는 다음과 같습니다.

단계	설정 항목	사용 지원 소프트웨어 사용	설명	참조
6	IP 주소를 설정	Sysmac Studio*1	세이프티 I/O 블록의 IP 주소 설정을 구성합니다.	7-10 IP 주소 설정 (7-71페이지)
7	TUNID를 설정	Sysmac Studio*1	세이프티 I/O 블록의 TUNID 설정을 구성합니다.	7-11 TUNID 설정 (7-78페이지)
8	세이프티 애플리케이션을 선택	-	세이프티 I/O 블록의 SETTING 로터리 스위치 SW1과 SW2를 모두 F로 설정합니다.	7-12 세이프티 애플리케이션 선택 (7-83 페이지)
9	재시작	Sysmac Studio*1	세이프티 I/O 블록을 재시작합니다.	7-13 재시작 (7-84 페이지)
10	구성	Sysmac Studio	Sysmac Studio의 프로젝트 파일을 다운로드하여 세이프티 컨트롤러와 표준 컨트롤러를 구성합니다. 세이프티 컨트롤러와 세이프티 I/O 블록 간에 Type1 Safety Open 접속이 확립되면 세이프티 컨트롤러가 세이프티 I/O 블록을 구성합니다.	7-14-1 세이프티 컨트롤러 구성 (7-87페이지)

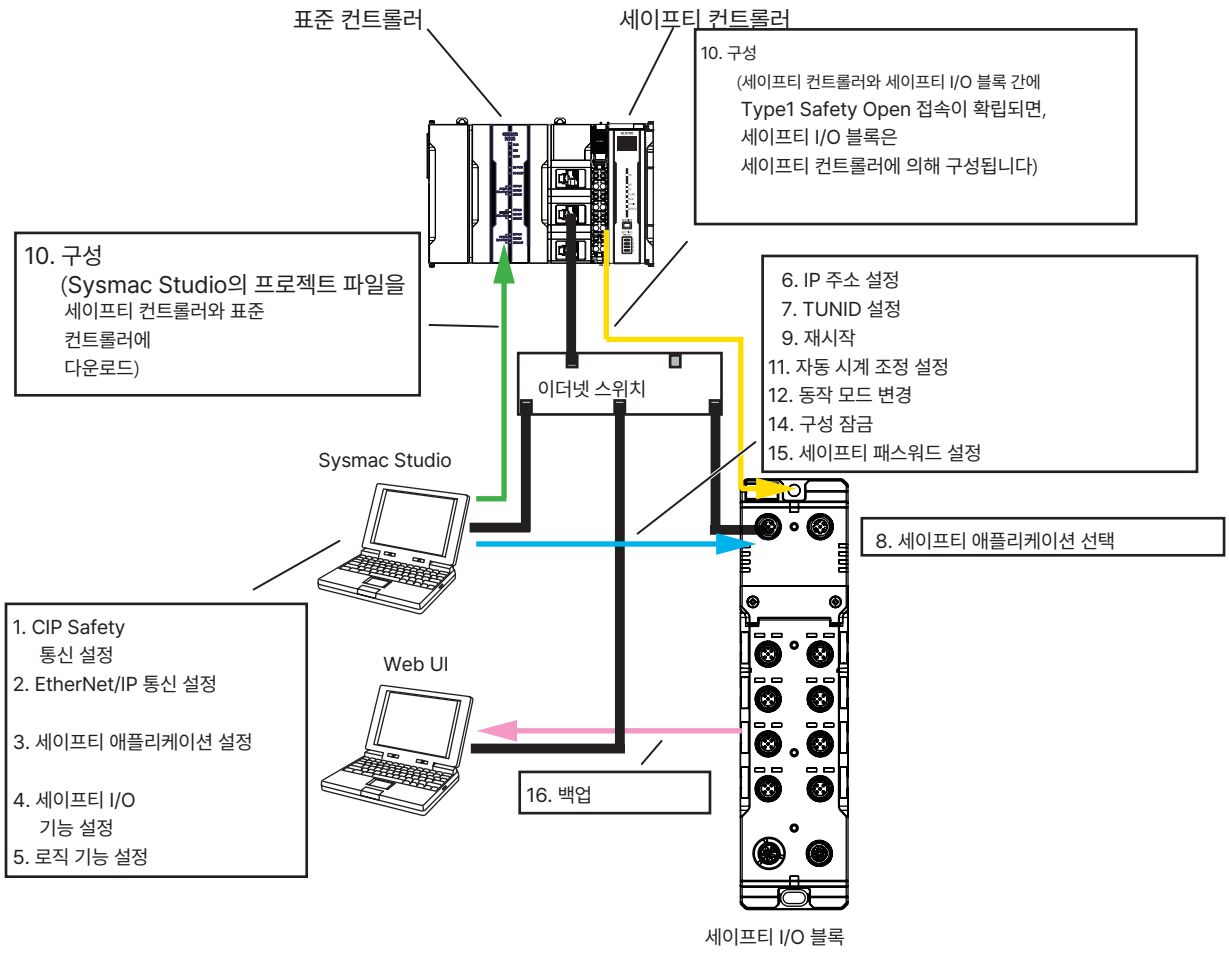
AI 번역본 For Reference Only

단계	설정 항목	사용 지원 소프트웨어 사용	설명	참조
11	자동 시계 조정을 설정	Sysmac Studio*1	세이프티 I/O 블록의 자동 시계 조정 설정을 구성합니다.	7-15 자동 시계 조정 설정 (7-91페이지)
12	동작 모드를 변경*2	Sysmac Studio*1	세이프티 I/O 블록의 동작 모드를 Executing으로 변경합니다.	7-16 동작 모드 변경 (7-95 페이지)
13	동작을 확인	-	모든 I/O 배선과 프로그램의 동작을 확인하여 세이프티 I/O 블록이 의도한 대로 동작하는지 확인합니다.	-
14	구성을 잠금	Sysmac Studio*1	세이프티 제어 시스템의 세이프티 밸리데이션을 실행하여 설정값이 올바른지 확인합니다. 확인 후 구성 잠금을 실행합니다. 구성 잠금을 실행한 후에는 잠금이 해제될 때까지 세이프티 I/O 블록의 설정값을 변경할 수 없습니다.	7-17 컨피규레이션 잠금 (7-99페이지)
15	세이프티 비밀번호를 설정	Sysmac Studio*1	세이프티 I/O 블록의 세이프티 패스워드 설정을 구성합니다.	7-18 세이프티 비밀번호 설정 (7-104페이지)
16	백업	Web UI	세이프티 I/O 블록의 백업 파일을 작성합니다.	7-19 백업 (7-108페이지)

***1.** 이 설정은 Web UI를 사용하여 구성할 수도 있습니다.

***2.** 이 설정은 4단계 로직 기능 설정에서 파워온 모드를 Idle로 설정한 경우에만 필요합니다. 파워온 모드를 Executing으로 설정한 경우에는 필요하지 않습니다.

AI 번역본
-For Reference Only-



AI 번역본
-For Reference Only-

7-1-5 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하기 위한 구성(분산 관리형)의 설정 절차

다음은 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 수행하기 위한 구성(분산 관리형)의 설정 절차를 보여줍니다.
설치 및 배선 전의 절차는 다음과 같습니다.

단계	설정 항목		사용 지원 소프트웨어 사용	설명	참조
1	애드온 애플리케이션 용 세이프티 애플리케이션 파일 작성*1	세이프티 애플리케이션 파일 익스포트	Sysmac Studio	세이프티 애플리케이션 파일을 익스포트하기 위한 프로젝트 파일을 작성합니다. 이 프로젝트 파일로 세이프티 애플리케이션을 익스포트합니다. 이 세이프티 애플리케이션 파일에는 로직 설정과 I/O 구성 설정을 정의합니다.	7-9 세이프티 애플리케이션 파일 작성 (7-65페이지)
2	세이프티 컨트롤러의 세이프티 프로그램을 위한 프로젝트 파일을 작성*1	CIP Safety 통신을 설정*2	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 컨트롤러와 세이프티 I/O 블록 간의 CIP Safety 통신 설정을 구성합니다. 오픈 타입으로 Check Safety **Signature (Type2a)를 선택합니다.**	7-3 CIP Safety 통신 설정 (7-27페이지)
3		표준 컨트롤러와 EtherNet/IP 통신을 설정*3	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 표준 컨트롤러와 세이프티 I/O 블록 간의 EtherNet/IP 통신 설정을 구성합니다.	7-4 EtherNet/IP 통신 설정 (7-38페이지)
4		세이프티를 설정 애플리케이션*2	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 애플리케이션 설정을 구성합니다. 사용할 애드온 애플리케이션을 선택합니다.	7-9-2 세이프티 애플리케이션 설정 (7-66페이지)
5		세이프티를 설정 시그니처*2	Sysmac Studio	Sysmac Studio의 프로젝트 파일에서 세이프티 시그니처 설정을 구성합니다. "세이프티 애플리케이션 파일 익스포트"에 기록된 SCCRC와 SCTS를 입력합니다.	7-8 세이프티 시그니처 설정 (7-63페이지)

***1.** 세이프티 애플리케이션 파일 익스포트용 프로젝트 파일과 세이프티 컨트롤러의 세이프티 프로그램용 프로젝트 파일은 별도로 작성하십시오.
***2.** 세이프티 컨트롤러를 사용하지 않는 경우, 이 설정은 필요하지 않습니다.
***3.** 표준 컨트롤러를 사용하지 않는 경우, 이 설정은 필요하지 않습니다.

AI 번역본
-For Reference Only-

설치 및 배선 후의 절차는 다음과 같습니다.
세이프티 컨트롤러를 설정하려면 세이프티 프로그램용 프로젝트 파일을 사용하십시오.

단계	설정 항목	사용 지원 소프트웨어 사용	설명	참조
6	IP 주소를 설정*1	Web UI*2	세이프티 I/O 블록의 IP 주소 설정을 구성합니다.	7-10 IP 주소 설정 (7-71 페이지)
7	TUNID를 설정	Web UI*2	세이프티 I/O 블록의 TUNID 설정을 구성합니다.	7-11 TUNID 설정 (7-78페이지)

단계	설정 항목	사용 지원 소프트웨어 사용	설명	참조
8	구성 (세이프티 I/O 블록 측)	Web UI	Web UI를 사용하여 세이프티 애플리케이션 파일을 세이프티 I/O 블록에 다운로드함으로써 세이프티 I/O 블록을 구성합니다. 애드온 애플리케이션용 세이프티 애플리케이션 파일을 사용하십시오. Remote I/O mode용 세이프티 애플리케이션 파일은 사용할 수 없습니다.	7-14-2 세이프티 I/O 블록의 구성 (7-87페이지)
9	세이프티 애플리케이션을 선택	-	세이프티 I/O 블록의 SETTING 로터리 스위치 SW1과 SW2를 모두 사용할 세이프티 애플리케이션(애드온 애플리케이션)의 번호 9-D 중 하나로 설정합니다.	7-12 세이프티 애플리케이션 선택 (7-83페이지)
10	재시작	Web UI*2	세이프티 I/O 블록을 재시작합니다.	7-13 재시작 (7-84페이지)
11	구성 (세이프티 컨트롤러 및 표준 컨트롤러 측)*3	Sysmac Studio	Sysmac Studio의 프로젝트 파일을 다운로드하여 세이프티 컨트롤러와 표준 컨트롤러를 구성합니다.	7-14-1 세이프티 컨트롤러 구성 (7-87페이지)
12	자동 시계 조정을 설정	Web UI*2	세이프티 I/O 블록의 자동 시계 조정 설정을 구성합니다.	7-15 자동 시계 조정 설정 (7-91페이지)
13	동작 모드 변경 *4	Web UI*2	세이프티 I/O 블록의 동작 모드를 Executing으로 변경합니다.	7-16 동작 모드 변경 (7-95 페이지)
14	동작을 확인	-	모든 I/O 배선과 프로그램의 동작을 확인하여 세이프티 I/O 블록이 의도한 대로 동작하는지 확인합니다.	-
15	구성 잠금	Web UI*2	세이프티 제어 시스템의 세이프티 밸리데이션을 실행하여 설정값이 올바른지 확인합니다. 확인 후 구성 잠금을 실행합니다. 구성 잠금을 실행한 후에는 세이프티 I/O 블록의 설정값이 잠금 해제 전까지 변경되지 않습니다.	7-17 구성 잠금 (7-99페이지)
16	세이프티 패스워드 설정	Web UI*2	세이프티 I/O 블록의 세이프티 패스워드 설정을 구성합니다.	7-18 세이프티 비밀번호 설정 (7-104 페이지)
17	백업	Web UI	세이프티 I/O 블록의 백업 파일을 작성합니다.	7-19 백업 (7-108페이지)

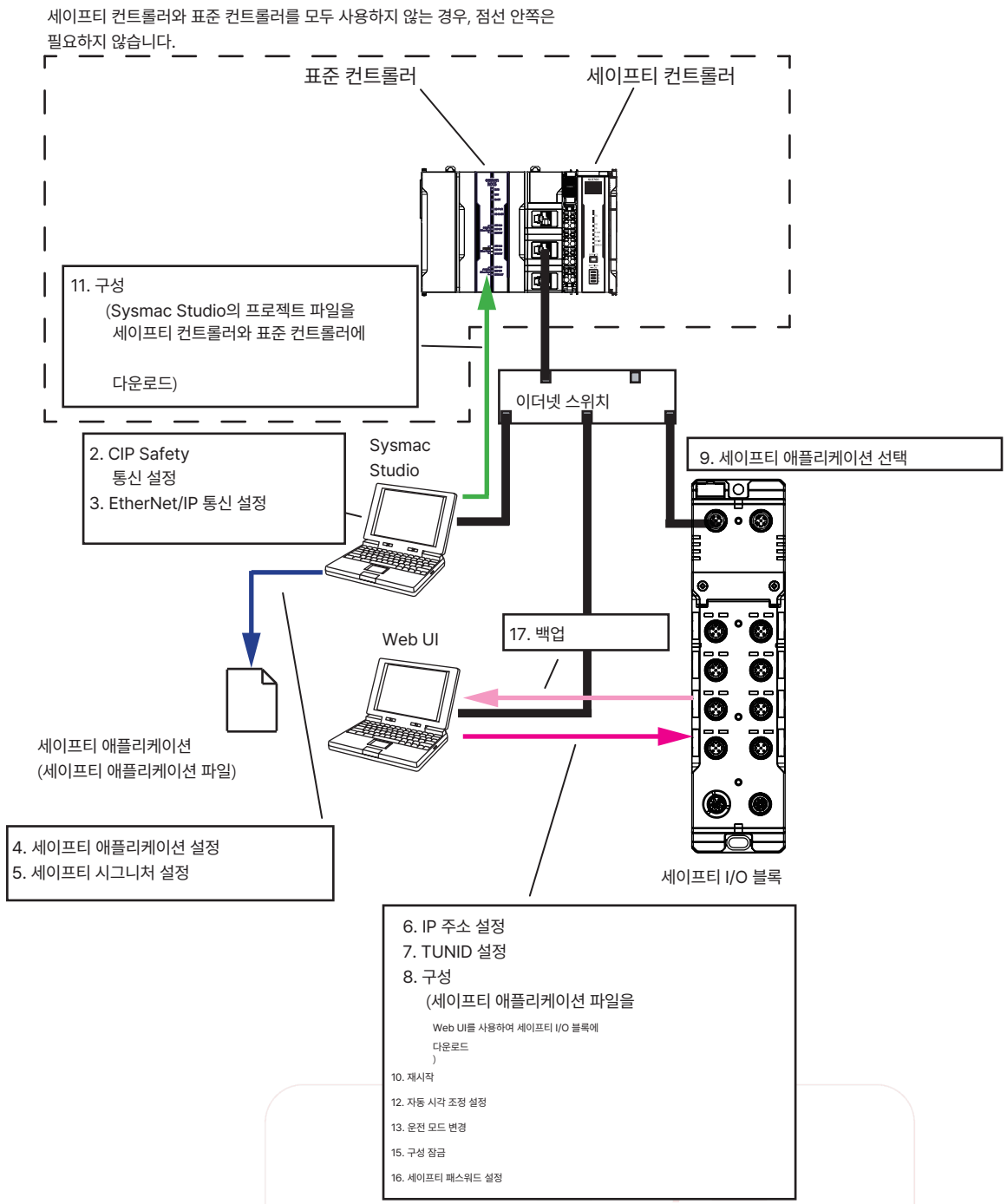
AI 번역본
-For Reference Only-

***1.** 세이프티 컨트롤러와 표준 컨트롤러를 모두 사용하지 않는 경우, 이 설정은 필요하지 않습니다. 이 경우 세이프티 I/O 블록은 기본 IP 주소로 동작합니다.

***2.** 이 설정은 Sysmac Studio를 사용하여 구성할 수도 있습니다.

***3.** 세이프티 컨트롤러와 표준 컨트롤러를 모두 사용하지 않는 경우, 이 설정은 필요하지 않습니다.

***4.** 이 설정은 4단계 로직 기능 설정에서 파워온 모드를 Idle로 설정한 경우에만 필요합니다. 파워온 모드를 Executing으로 설정한 경우에는 필요하지 않습니다.



-For Reference Only-

7-2 Web UI 개요

이 절에서는 설정에 사용하는 Web UI의 전체적인 내용과 각 화면에 공통되는 내용에 대해 설명합니다.

7-2-1 Web UI의 각종 사양

다음 표에 Web UI의 각종 사양을 나타냅니다.

항목	사양
동시 로그인 가능 사용자 수	옵저버와 관리자를 합쳐 1명
로컬 포트 번호	443
지원 언어	일본어(ja) 및 영어(en-US)
지원 문자 코드	UTF-8
권한	관리자 및 옵저버
지원 프로토콜	HTTPS
지원 브라우저	Edge(PC용) 및 Chrome(PC용)
세션 타임아웃 시간	10분간 액세스 없음
TLS 버전	TLS 1.2를 지원합니다. TLS 1.0, TLS 1.1, SSL은 지원하지 않습니다.

7-2-2 Web UI의 조작 권한

Web UI에는 관리자와 옵저버 두 가지 조작 권한이 있습니다.
다음 표에 관리자와 옵저버 각각이 할 수 있는 작업과 세이프티 패스워드 인증이 필요한지 여부를 나타냅니다. 세이프티 패스워드는 세이프티 I/O 블록의 안전에 관련된 설정을 구성할 때 필요합니다. 세이프티 패스워드는 Web UI를 사용하여 설정할 수도 있습니다.

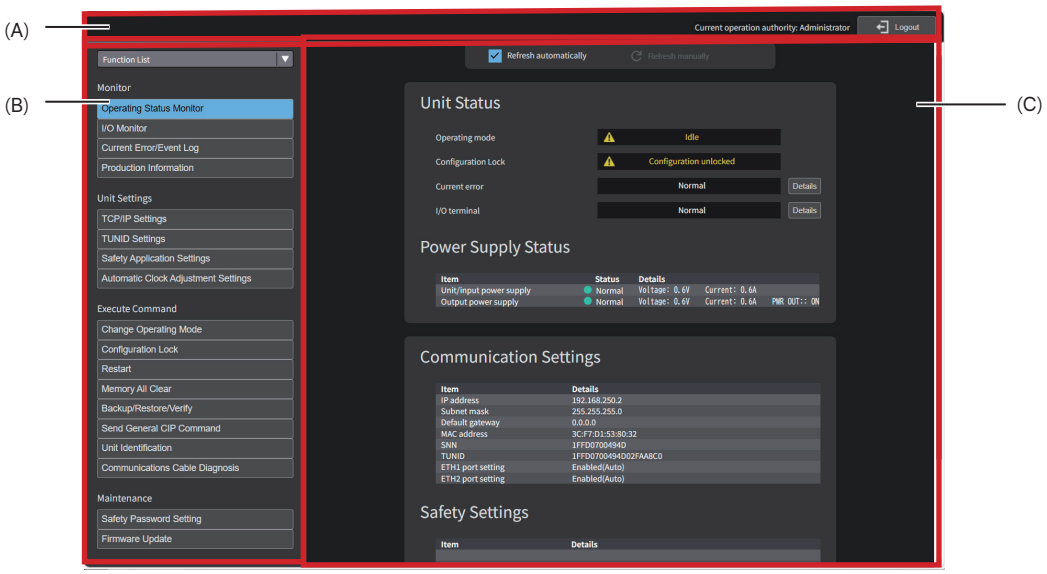
조작 권한	할 수 있는 작업	세이프티 패스워드 인증
관리자	각종 정보 읽기, 설정 및 변경과 각종 명령 실행	필요
옵저버	각종 정보 읽기	불필요

Web UI의 각 화면과 옵저버 또는 관리자로 사용 가능한지 여부의 관계는 7-18페이지의 7-2-4 메인 메뉴 목록을 참조하십시오.
조작 권한을 변경하려면 Web UI에서 로그아웃한 후 새로운 조작 권한으로 다시 로그인하십시오.

AI 번역본
-For Reference Only-

7-2-3 Web UI의 화면 구성

다음은 Web UI의 화면 구성입니다.



기호	명칭	설명
(A)	공통 메뉴	선택한 조작 메뉴와 관계없이 모든 메인 메뉴에 공통으로 구성되는 메뉴 Current operation authority 필드에는 로그인한 조작자의 권한이 표시됩니다. Logout 버튼을 클릭하면 Logout 화면이 표시되어 로그아웃할 수 있습니다.
(B)	조작 메뉴	메인 메뉴를 선택하는 메뉴
(C)	메인 메뉴	선택한 조작 메뉴의 세부 설정을 하는 메뉴

메인 메뉴 상단에는 Refresh automatically 확인란과 Refresh manually 버튼이 있는 화면이 있습니다.
이 컨트롤을 사용하여 화면을 새로 고치는 타이밍을 설정할 수 있습니다. 각각의 의미는 다음과 같습니다.

항목	설명
Refresh automatically	이 확인란을 선택하면 화면이 1초 간격으로 자동으로 새로 고쳐집니다. 기본값: 선택됨
Refresh manually	이 버튼을 클릭하면 화면이 새로 고쳐집니다. 이 버튼은 Refresh automatically 확인란이 선택되어 있지 않을 때만 사용할 수 있습니다.

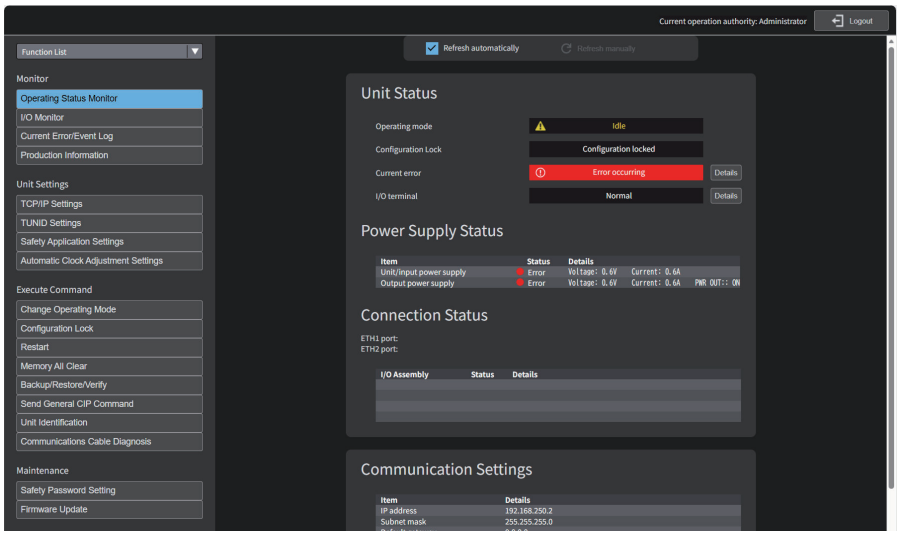
7-2-4 메인 메뉴 목록

메인 메뉴에는 아래와 같이 Function List와 Replace Unit이 있습니다.
조작 메뉴 맨 위쪽의 풀다운 메뉴에서 Function List와 Replace Unit을 전환합니다.

메뉴 명령	설명
Function List	세이프티 I/O 블록의 각종 설정 및 모니터링에 사용합니다.
Replace Unit	유닛을 교체할 때 사용합니다. Function List의 기능 중 유닛 교체에 필요한 기능만 모아 놓은 것입니다.

AI 번역본
For Reference Only

기능 목록



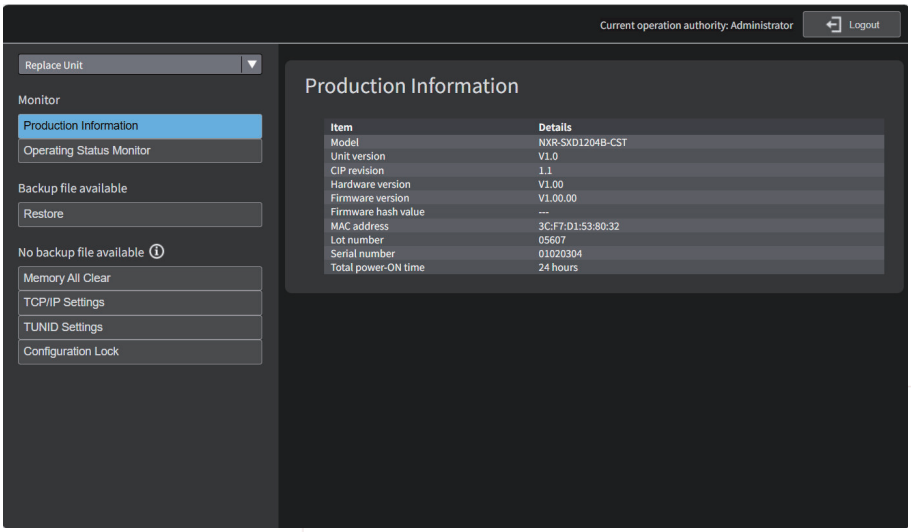
Function List에는 다음 항목이 있습니다. 다음 표에 각 항목의 개요, 옵저버로 사용 가능한지 여부, 참조처를 나타냅니다.

메인 메뉴 그룹	메인 메뉴의 화면 이름	설명	사용 가능한지 여부 (옵저버)	참조처
Monitor	Operating Status Monitor	해당 유닛의 유닛 상태, 전원 공급 상태 등 다양한 상태를 표시합니다.	가능	11-3페이지의 11-1-3 운전 상태 모니터 기능
	I/O Monitor	해당 유닛의 각 I/O 단자 값을 표시합니다.	가능	8-27페이지의 8-11 I/O Monitor 기능
	Current Error/ Event Log	해당 유닛의 현재 에러 및 이벤트 로그를 표시합니다. 또한 이벤트 로그의 저장 및 삭제를 가능하게 합니다.	가능	11-6페이지의 11-2 이벤트를 사용한 에러 확인 및 문제 해결
	Production information	해당 유닛의 유닛 버전 등 생산 정보를 표시합니다.	가능	*Production Information Screen* 33페이지
Unit Settings	TCP/IP Settings	해당 유닛의 IP 주소, 서브넷 마스크, 디폴트 게이트웨이, LINK 설정을 구성합니다.	불가능	7-71페이지의 7-10 IP 주소 설정
	TUNID Settings	해당 유닛의 TUNID를 설정합니다.	불가능	7-78페이지의 7-11 TUNID 설정
	Safety Application Settings	해당 유닛에서 실행되는 세이프티 애플리케이션을 로터리 스위치 번호에 할당하거나 로터리 스위치 번호에서 제거합니다.	불가능	7-87페이지의 7-14 구성 설정
	Automatic Clock Adjustment Settings	해당 유닛의 시각을 조정합니다.	불가능	7-91페이지의 7-15 자동 시각 조정 설정
Execute Command	Change Operating Mode	운전 모드를 Idle 또는 Executing으로 설정합니다.	불가능	7-95페이지의 7-16 운전 모드 변경
	Configuration Lock	구성의 잠금 및 잠금 해제를 실행합니다.	불가능	7-99페이지의 7-17 구성 잠금
	Restart	해당 유닛을 재시작합니다.	불가능	7-84페이지의 7-13 Restart

AI 번역본 For Reference Only

메인 메뉴 그룹	메인 메뉴의 화면 이름	설명	사용 가능한지 여부 (옵저버)	참조처
	Memory All Clear	해당 유닛의 모든 설정 데이터를 공장 출하 시 기본값으로 되돌립니다.	불가능	8-4페이지의 8-2 Clear All Memory 기능
	Backup/Restore/ Verify	해당 유닛의 설정 데이터를 백업, 복원, 검증합니다.	불가능	7-108페이지의 7-19 백업
	Send General CIP Command	전용 도구를 사용하지 않고 해당 유닛에 CIP 메시지 명령을 발행하고 실행 결과를 표시합니다.	불가능	8-15페이지의 8-7 Send General CIP Command 기능
	Unit Identification	해당 유닛의 유닛 식별 표시등을 점등합니다.	불가능	8-16페이지의 8-8 Unit Identification 기능
	Communications Cable Diagnosis	통신 케이블이 단선되었는지 또는 단락되었는지 확인합니다.	불가능	8-31페이지의 8-13 Communications Cable Diagnosis 기능
Maintenance	Safety Password Setting	해당 유닛의 Web UI에 대한 세이프티 패스워드를 설정합니다.	불가능	7-104페이지의 7-18 세이프티 패스워드 설정
	Update Firmware	해당 유닛의 펌웨어를 업데이트합니다.	불가능	8-35페이지의 8-14 펌웨어 업데이트 기능

유닛 교체



For Reference Only

Replace Unit에는 다음 항목이 있습니다. 각 항목의 개요, 옵저버로 사용 가능한지 여부, 참조처는 Function List와 동일합니다.

메인 메뉴 그룹	메인 메뉴의 화면 이름	참조처
Monitor	Production Information	33페이지의 Production Information Screen
	Operating Status Monitor	11-3페이지의 11-1-3 운전 상태 모니터 기능
백업 파일이 있는 경우	Restore*1	7-108페이지의 7-19 백업
백업 파일이 없는 경우	Memory All Clear	8-4페이지의 8-2 Clear All Memory 기능
	TCP/IP Settings	7-71페이지의 7-10 IP 주소 설정
	TUNID Settings	7-78페이지의 7-11 TUNID 설정
	Configuration Lock	7-99페이지의 7-17 컨피규레이션 잠금

*1. Function List의 Backup/Restore/Verify 화면에서 복원 기능만 발췌한 것입니다.

7-2-5 Web UI 시작 절차

Web UI를 시작하는 방법에는 두 가지가 있습니다.

- PC의 Web 브라우저에 세이프티 I/O 블록의 IP 주소를 입력하는 방법
- 세이프티 I/O 블록의 IP 주소가 할당된 도메인 이름을 PC의 Web 브라우저에 입력하는 방법

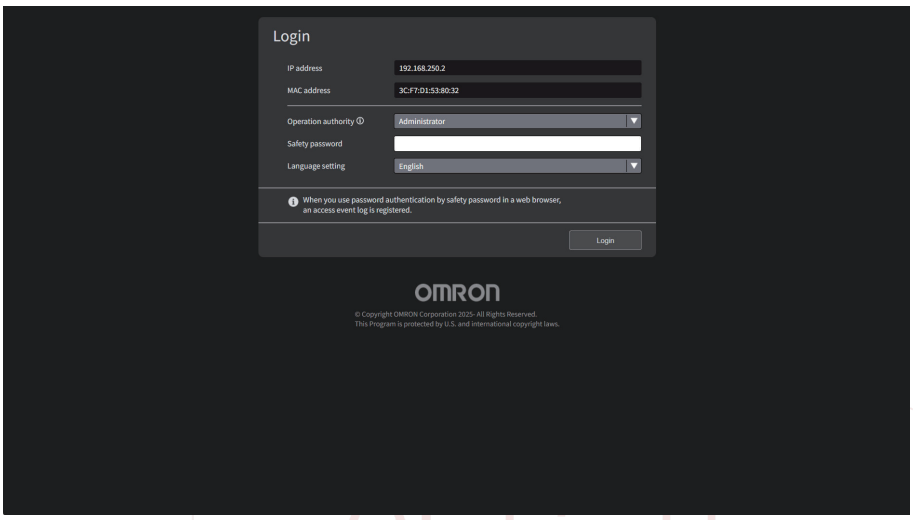
IP 주소를 입력하는 방법

이 절에서는 PC의 Web 브라우저에 세이프티 I/O 블록의 IP 주소를 입력하는 방법의 절차에 대해 설명합니다.

1 이더넷 케이블을 사용하여 세이프티 I/O 블록의 EtherNet/IP 포트와 PC의 이더넷 포트를 연결합니다.

2 PC의 Web 브라우저를 시작합니다.

3 Web 브라우저에 세이프티 I/O 블록의 IP 주소를 입력합니다. 예를 들어 세이프티 I/O 블록의 IP 주소가 192.168.250.1인 경우 https://192.168.250.1/를 입력합니다. Web UI가 시작되고 Web 브라우저에 다음 Login 화면이 표시됩니다.



-For Reference Only-

사용상의 주의

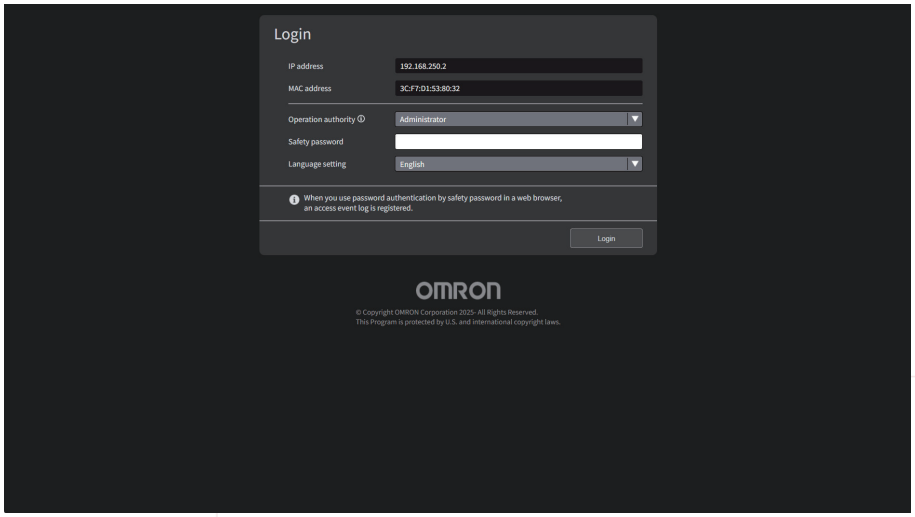
PC의 Web 브라우저에 세이프티 I/O 블록의 IP 주소를 입력하는 방법을 사용할 때는 다음과 같은 보안 위험이 있습니다. 네트워크상에서 PC와 세이프티 I/O 블록 사이에 부정한 기기가 개입하면 세이프티 패스워드 등의 정보가 그 부정한 기기에 의해 유출될 수 있습니다. 따라서 다음과 같은 보안 대책을 취하십시오.

- 생산 영역 외부에서 세이프티 I/O 블록에 액세스하지 못하도록 방화벽 등의 조치를 사용하십시오.
- 출입 관리 등을 통해 부정한 제3자가 생산 영역에 들어오지 못하도록 방지하십시오.
- PC와 세이프티 I/O 블록을 직접 연결하는 등의 방법으로 부정한 기기가 PC와 세이프티 I/O 블록 간의 통신을 가로채지 못하도록 방지하십시오.

도메인 이름을 입력하는 방법

이 절에서는 PC의 Web 브라우저에 세이프티 I/O 블록의 IP 주소가 할당된 도메인 이름을 입력하는 방법의 절차에 대해 설명합니다. 통신 데이터의 암호화 및 서버 증명서에 의한 인증이 수행되므로, 이 방법의 보안 위험은 IP 주소를 입력하는 방법보다 낮습니다.
도메인 이름을 입력하는 방법을 사용하려면 미리 PC에서 HTTPS 통신 기능을 사용하기 위한 설정을 구성해야 합니다. HTTPS 통신 기능에 대한 자세한 내용은 8-8페이지의 8-3 HTTPS 통신 기능을 참조하십시오. HTTPS 통신 기능을 사용하기 위한 설정은 각 PC에서 한 번만 구성하면 됩니다. 이 절에서는 HTTPS 통신 기능을 사용하기 위한 설정이 이미 구성된 PC를 사용하여 Web UI를 시작하는 절차에 대해 설명합니다.

1. 이더넷 케이블을 사용하여 세이프티 I/O 블록의 EtherNet/IP 포트와 PC의 이더넷 포트를 연결합니다.
2. PC의 Web 브라우저를 시작합니다.
3. Web 브라우저에 세이프티 I/O 블록의 IP 주소에 할당된 도메인 이름을 입력합니다. 예를 들어 도메인 이름이 device1.NXR-SXD.local인 경우 다음과 같이 입력합니다. https://device1.NXR-*SXD.local*
   Web UI가 시작되고 Web 브라우저에 다음 Login 화면이 표시됩니다.



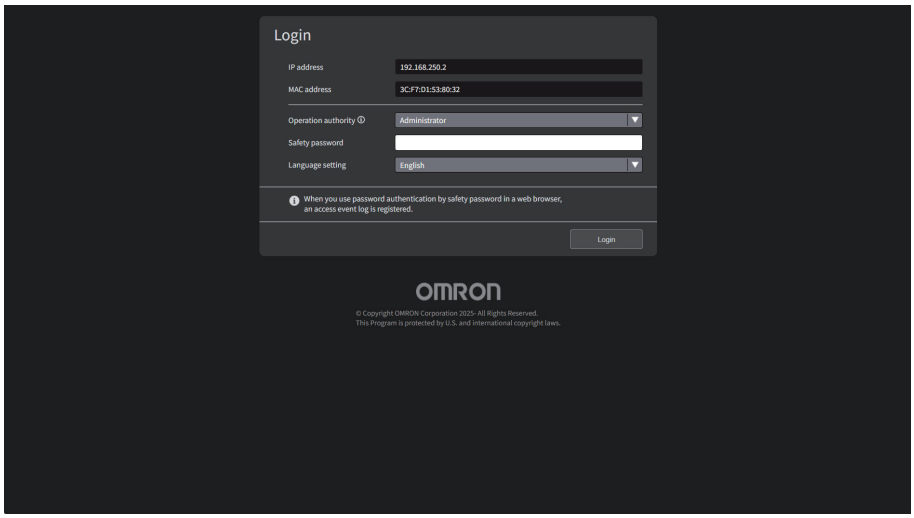
-For Reference Only-

사용상의 주의

PC의 Web 브라우저에 세이프티 I/O 블록의 IP 주소가 할당된 도메인 이름을 입력하는 방법을 사용할 때는 다음 사항에 유의하십시오. 도메인 이름 서버의 설정을 변경하지 않고 세이프티 I/O 블록의 IP 주소를 변경하면, 할당된 IP 주소로 도메인 이름을 입력했을 때 의도하지 않은 기기에 액세스하게 될 수 있습니다.
세이프티 I/O 블록의 IP 주소를 변경할 때는 도메인 이름 서버의 설정도 함께 변경하십시오. 또한 Web UI의 Login 화면에 표시되는 MAC 주소가 의도한 세이프티 I/O 블록의 MAC 주소와 일치하는지 확인하십시오.

7-2-6 로그인

세이프티 패스워드를 입력하여 권한 인증을 수행하고 Web UI에 로그인합니다.



세이프티 패스워드는 공장 출하 시 설정되어 있지 않습니다.

세이프티 패스워드를 5회 잘못 입력하면 10분간 로그인할 수 없습니다. 세이프티 패스워드를 잘못 입력한 횟수는 로그인 성공, 전원 재투입, 또는 10분 경과 중 어느 하나에 의해 재설정됩니다.

로그인 후 10분 이상 조작이 없으면 관리자 권한이 없는 제3자에 의한 부정 사용을 방지하기 위해 세이프티 패스워드를 다시 입력해야 합니다.

로그인 후 로그아웃하지 않고 Web 브라우저를 종료하면 로그인 상태가 10분간 유지됩니다. 따라서 동일한 사용자가 동일한 PC에서 Web 브라우저를 시작하면 로그인 조작을 수행하지 않고도 Web UI를 사용할 수 있습니다. 그동안에는 다른 사용자가 로그인할 수 없습니다.

로그인 후 로그아웃하지 않고 세이프티 I/O 블록의 전원을 OFF하면 로그인 상태가 파기됩니다. 따라서 동일한 사용자가 동일한 PC에서 Web 브라우저를 시작하더라도 다시 Web UI에 로그인해야 합니다.

Safety password 필드에서는 세이프티 패스워드의 표시와 숨김을 전환할 수 있습니다.

사용상의 주의

- 사용하기 전에 Login 화면에 표시되는 MAC 주소가 의도한 유닛의 MAC 주소인지 확인하십시오. 유닛의 MAC 주소는 유닛 측면에 기재되어 있습니다.
- 제3자에 의한 부정 사용을 방지하기 위해, Web UI를 통한 조작을 중단하고 컴퓨터를 떠나기 전에 세이프티 I/O 블록에서 로그아웃하십시오. Web UI에서 Operating Status Monitor 화면, I/O Monitor 화면, Current Error 화면, Event log 화면에서 Refresh automatically를 선택하면 10분 이상 조작이 없어도 세이프티 패스워드를 다시 입력할 필요가 없습니다.

로그인 사용 절차

로그인 사용 절차는 다음과 같습니다.

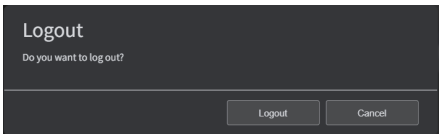
1. IP address 필드에 해당 유닛의 IP 주소가 표시되고, MAC address 필드에 해당 유닛의 MAC 주소가 표시되는지 확인합니다.
2. **Operation authority에서 Administrator 또는 Observer를 선택합니다.**

3 **Language settings에서 English 또는 Japanese를 선택합니다.**
Web UI에 표시되는 언어가 결정됩니다.

4 관리자인 경우 세이프티 패스워드를 입력하고 Login 버튼을 클릭합니다. 옵저버인 경우에는 세이프티 패스워드를 입력할 필요가 없습니다.
관리자로서 해당 유닛에 처음 로그인하는 경우, 로그인 후 Change Initial Safety Password 화면이 표시됩니다. 그렇지 않은 경우에는 로그인 후 Operating Status Monitor 화면이 표시됩니다.

7-2-7 로그아웃

Web UI에서 로그아웃합니다.
공통 메뉴에서 Logout 버튼을 클릭하면 Logout 화면이 표시됩니다.



로그아웃 사용 절차

Logout 화면에서 Web UI로부터 로그아웃합니다. 설정 절차는 다음과 같습니다.

1 Logout 버튼을 클릭합니다.
로그아웃이 수행되고 Login 화면이 표시됩니다.

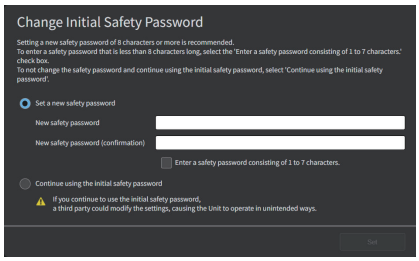
7-2-8 초기 로그인 시 주의 사항

초기 로그인 시 Change Initial Safety Password 화면이 표시됩니다. 보안을 강화하기 위해 반드시 세이프티 패스워드를 변경하십시오.

Change Initial Safety Password

Change Initial Safety Password 화면은 초기 로그인 시 초기 세이프티 패스워드를 변경하는 데 사용합니다. 이 화면은 초기 로그인 시 Login 화면 직후에 표시됩니다. 새로운 세이프티 패스워드를 설정하거나 Continue using the initial safety password 옵션을 선택하면, 다음 로그인부터는 이 화면이 표시되지 않습니다.
세이프티 패스워드 인증 기능에 대한 자세한 내용은 7-104페이지의 7-18 세이프티 패스워드 설정을 참조하십시오.

AI 번역본
-For Reference Only-



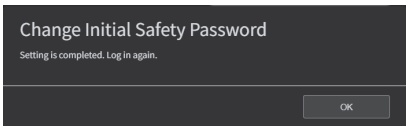
● Change Initial Safety Password 사용 절차

Change Initial Safety Password 화면은 초기 세이프티 패스워드로부터 세이프티 패스워드를 변경하는 데 사용합니다. 사용 절차는 다음과 같습니다.

1 **Set a new safety password 또는 Continue using the initial safety password 옵션 중** 하나를 선택합니다.
Continue using the initial safety password 옵션을 선택하면 세이프티 패스워드를 변경할 수 없습니다. 다만 보안을 향상시키기 위해 세이프티 패스워드를 변경할 것을 권장합니다.

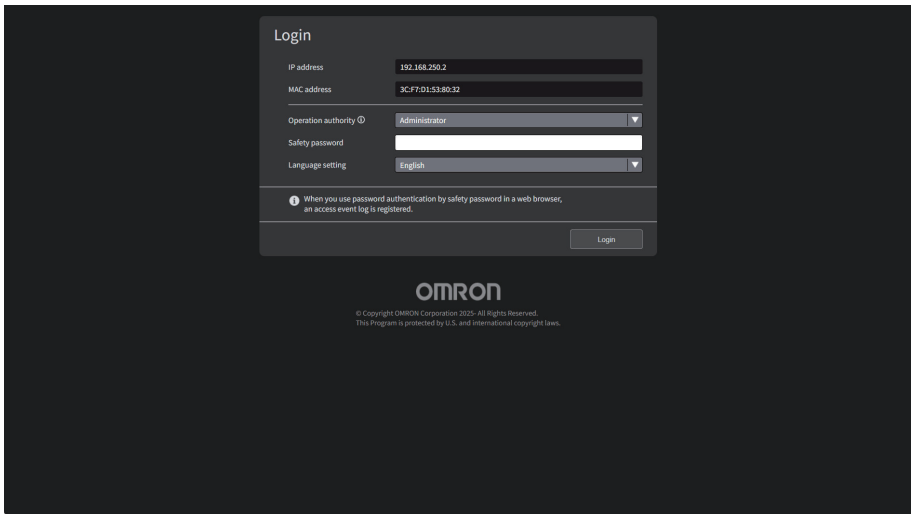
2 Set a new safety password 옵션을 선택한 경우, New safety password와 New safety **password (confirmation)에 새로운 세이프티 패스워드를 입력합니다.**
보안을 강화하려면 8자 이상의 세이프티 패스워드를 입력하십시오.
단, 다른 기기와 동일한 패스워드를 사용하고 싶은 경우 등 특별한 사정이 있는 경우에는 Enter a safety password consisting of 1 to 7 characters. 확인란을 선택하면 1~7자의 **세이프티 패스워드를 설정할 수 있습니다.**

3 Set 버튼을 클릭합니다.
세이프티 패스워드가 설정되고 다음 메시지가 표시됩니다.



4 OK 버튼을 클릭합니다.
Login 화면이 표시됩니다.

AI 번역본
-For Reference Only-



5 새로운 세이프티 패스워드를 입력하고 Login 버튼을 클릭합니다.
Operating Status Monitor 화면이 표시됩니다.

AI 번역본
-For Reference Only-

7-3 CIP Safety 통신 설정

이 절에서는 CIP Safety 오리지네이터와 CIP Safety 타겟의 세이프티 I/O 블록을 사용한 CIP Safety 통신용 커넥션 설정 방법에 대해 설명합니다.

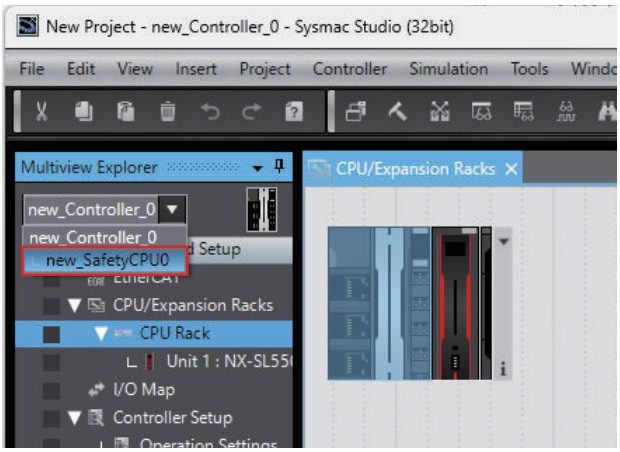
7-3-1 CIP Safety 통신 커넥션 설정

이 절에서는 세이프티 I/O 블록의 CIP Safety 커넥션 설정을 구성하는 방법에 대해 설명합니다.

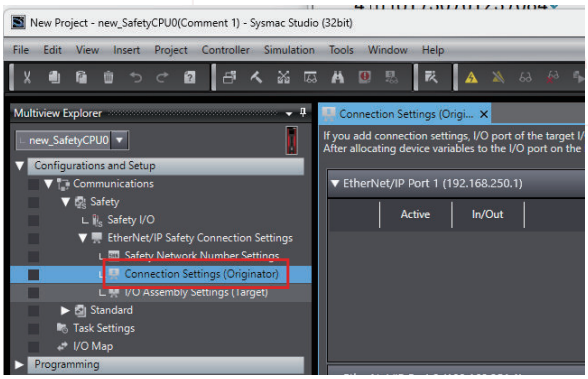
커넥션 등록 절차

이 절에서는 CIP Safety 오리지네이터의 예시로 세이프티 네트워크 컨트롤러를 사용하여 Sysmac Studio에서 세이프티 I/O 블록의 CIP Safety 커넥션을 등록하는 절차에 대해 설명합니다.

1 멀티뷰 익스플로러에서 Controller Selection Box의 대상 세이프티 CPU 유닛을 선택합니다.



2 **멀티뷰 익스플로러에서 Configurations and Setup - Communications - Safety - EtherNet/IP Safety Connection Settings로 이동하여 Connection Settings (Originator)를 더블 클릭하거나,** 마우스 오른쪽 버튼을 클릭하고 Edit를 선택합니다.
Edit Pane에 Connection Settings (Originator) Edit Pane이 표시됩니다.

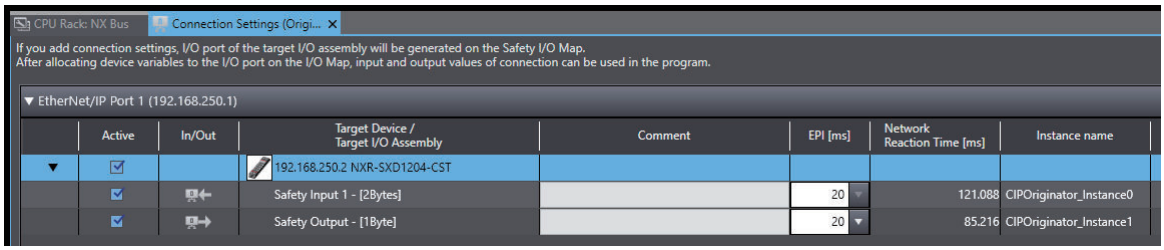


3 **Toolbox에서 Safety I/O and Logic Device를 선택하고, NXR-SXD1204-CST 또는 NXR-SXD1204B-CST를 선택합니다.**

사 본 예 본
-Reference Only-



4 Toolbox에서 선택한 세이프티 I/O 블록을 드래그하여 Connection Settings (Originator) Edit Pane에 드롭하거나, 선택한 세이프티 I/O 블록을 더블 클릭합니다.



5 필요에 따라 세이프티 I/O 블록의 IP 주소를 설정합니다.
추가된 커넥션의 IP 주소는 세이프티 네트워크 컨트롤러에 설정된 EtherNet/IP 포트의 IP 주소를 기준으로 자동으로 할당됩니다. 네트워크 구성에 맞게 IP 주소를 편집하십시오.
IP 주소 편집 방법에 대한 자세한 내용은 7-28페이지의 커넥션 IP 주소 설정 절차를 참조하십시오.

6 필요에 따라 I/O 어셈블리를 변경합니다.
초기 상태에서는 NXR-SXD1204-CST에 Safety Input 1과 Safety Output이 등록되어 있습니다.
NXR-SXD1204B-CST도 마찬가지입니다.
I/O 어셈블리 변경 방법에 대한 자세한 내용은 7-29페이지의 추가 커넥션 등록 절차를 참조하십시오.

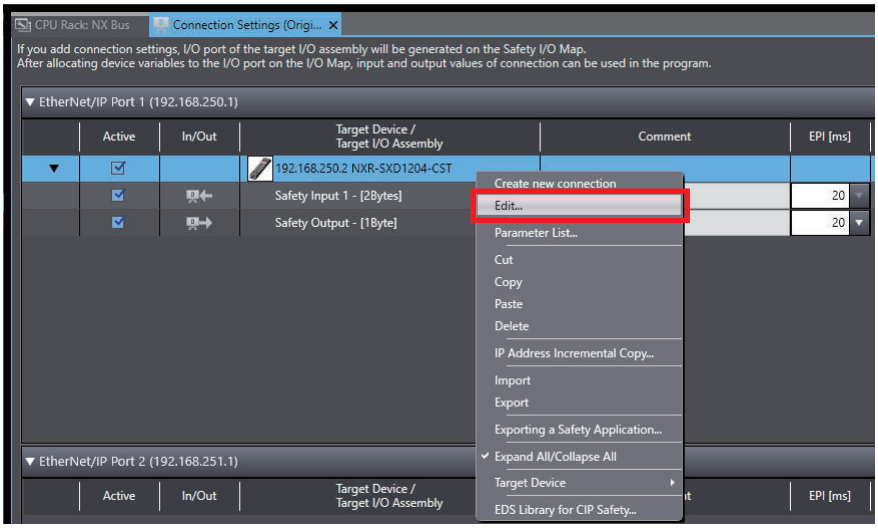
샘플 번역본
-For Reference Only-

7 등록된 커넥션의 파라미터를 편집합니다.
커넥션의 파라미터 편집 방법에 대한 자세한 내용은 7-32페이지의 커넥션 파라미터 편집 절차를 참조하십시오.

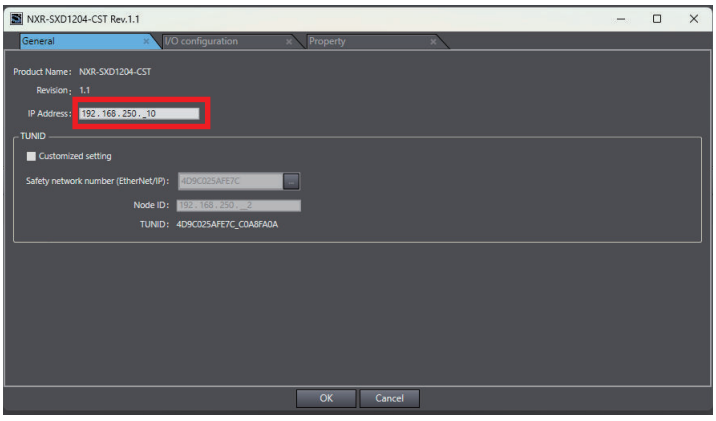
커넥션 IP 주소 설정 절차

이 절에서는 세이프티 I/O 블록의 IP 주소를 커넥션 설정의 IP 주소로 설정하는 절차에 대해 설명합니다.

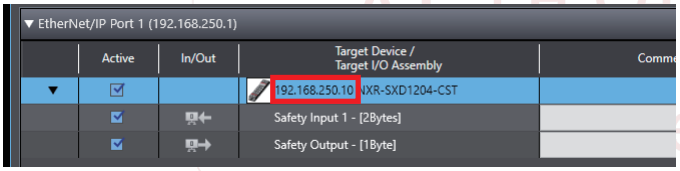
1 Connection Settings (Originator) Edit Pane에서 Safety I/O Block을 선택한 후 마우스 오른쪽 버튼을 클릭하고 메뉴에서 Edit를 선택합니다.



2 IP address 필드에 IP 주소를 입력하고 OK 버튼을 클릭합니다.



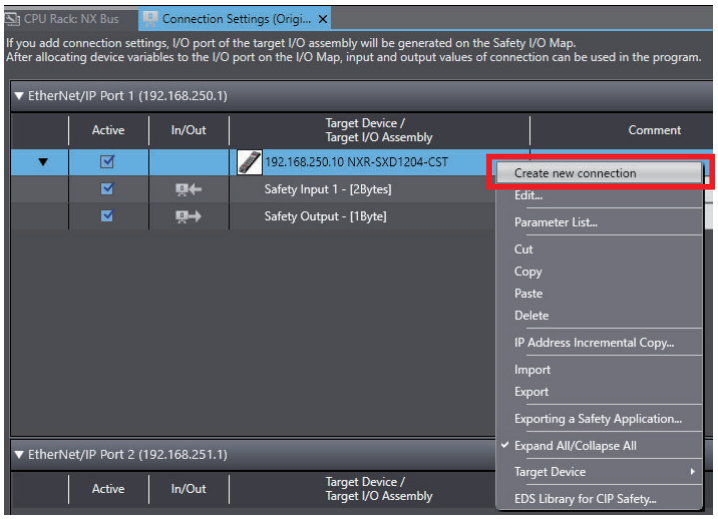
입력한 IP 주소가 Connection Settings (Originator) Edit Pane에 반영됩니다.



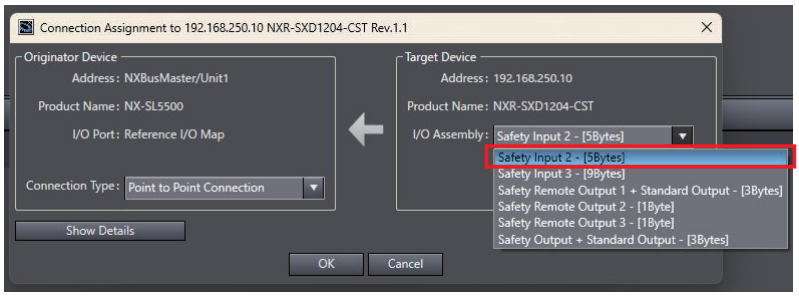
추가 커넥션 등록 절차

세이프티 I/O 블록에 추가 커넥션을 등록하는 절차는 다음과 같습니다.

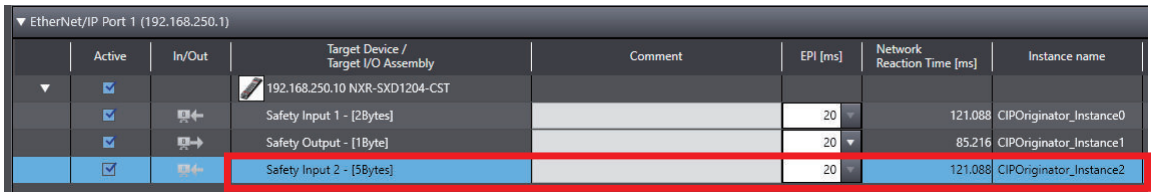
1 Connection Settings (Originator) Edit Pane에서 Safety I/O Block을 선택한 후 마우스 **오른쪽 버튼을 클릭하고 Create new connection을 선택합니다.**



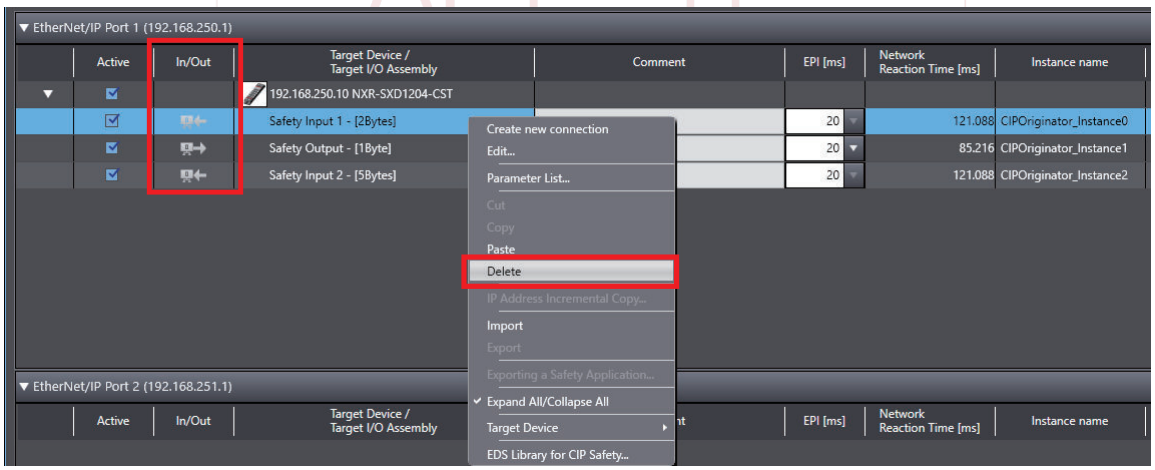
2 I/O Assembly 풀다운 목록에서 추가할 항목을 선택한 후 OK 버튼을 클릭합니다.



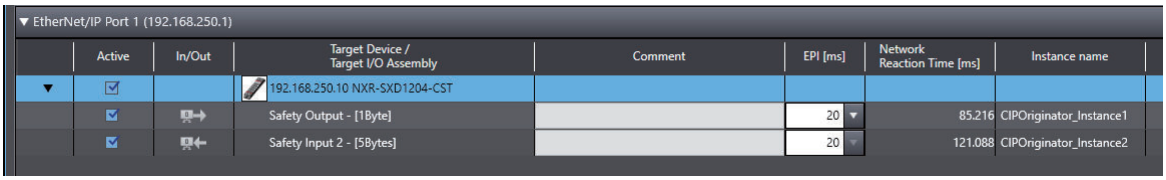
추가된 I/O 어셈블리가 Connection Settings (Originator) Edit Pane에 표시됩니다.



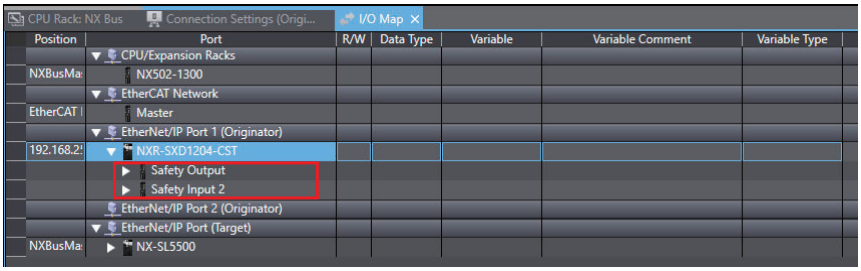
3 사용하지 않을 I/O 어셈블리를 선택한 후 마우스 오른쪽 버튼을 클릭하고 Delete를 선택합니다.



AI 번역본



설정한 I/O 어셈블리는 I/O 맵에도 자동으로 반영됩니다.



● I/O 어셈블리의 종류 및 제한 사항

세이프티 I/O 블록에 등록 가능한 입력 어셈블리와 출력 어셈블리의 종류 및 제한 사항은 다음과 같습니다.

・입력 어셈블리

입력 어셈블리는 세이프티 I/O 블록에서 세이프티 컨트롤러 방향으로 전송되는 데이터입니다.

어셈블리	데이터 크기	비고
세이프티 입력 1	2byte	세이프티 입력 단자값 + 세이프티 입력 단자의 상태 정보(집약) + 세이프티 출력 단자의 상태 정보(집약) + 출력 전원 공급 에러 플래그 + 커넥션 상태 정보
세이프티 입력 2	5byte	세이프티 입력 단자값 + 세이프티 입력 단자의 상태 정보 + 세이프티 입력 단자의 상태 정보(집약) + 세이프티 출력 단자의 상태 정보(집약) + 출력 전원 공급 에러 플래그 + 커넥션 상태 정보 + 세이프티 애플리케이션 번호
세이프티 입력 3	9byte	세이프티 입력 단자값 + 세이프티 입력 단자의 상태 정보 + 세이프티 출력 단자의 상태 정보 + 세이프티 출력 단자로 실제 출력된 값 + 테스트 출력 단자의 상태 정보 + 테스트 출력 단자값 + 세이프티 입력 단자의 상태 정보(집약) + 세이프티 출력 단자의 상태 정보(집약) + 출력 전원 공급 에러 플래그 + 커넥션 상태 정보 + 세이프티 애플리케이션 번호

・출력 어셈블리

출력 어셈블리는 세이프티 컨트롤러에서 세이프티 I/O 블록 방향으로 전송되는 데이터입니다.

Assembly	데이터 크기	비고
Safety Output	1byte	세이프티 출력 단자로의 ON/OFF
Safety Output + Standard Output	3byte	세이프티 출력 단자로의 ON/OFF + 테스트 출력 단자로의 대기 출력 ON/OFF
Safety Remote Output 1 + Standard Output	3byte	리모트 출력 Ro 1의 ON/OFF + 테스트 출력 단자로의 대기 출력 ON/OFF
Safety Remote Output 2	1byte	리모트 출력 Ro 2의 ON/OFF
Safety Remote Output 3	1byte	리모트 출력 Ro 3의 ON/OFF

-For Reference Only-

설정 가능한 출력 어셈블리는 세이프티 애플리케이션에 사용되는 설정에 따라 다릅니다. 출력 어셈블리의 조합은 다음과 같습니다.

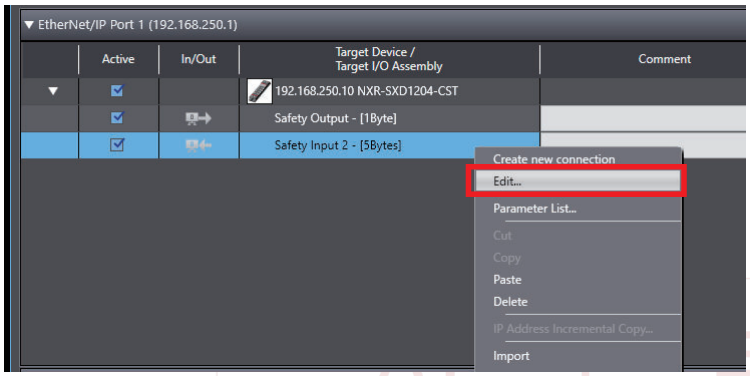
세이프티 애플리케이션의 Sysmac Studio 설정값 및 로터리 스위치 설정	출력 어셈블리의 조합
세이프티 애플리케이션 미사용 (애플리케이션의 설정값이 "00: Remote I/O mode"이고 로터리 스위치 SW1 = SW2 = 0인 경우)	다음 두 종류의 어셈블리를 사용할 수 있습니다. · Safety Output · Safety Output + Standard Output 단, 두 어셈블리에 대한 커넥션을 동시에 확립할 수는 없습니다.
세이프티 애플리케이션 사용 (애플리케이션의 설정값이 "00: Remote I/O mode" 이외이고 로터리 스위치 SW1 = SW2가 1~3, 9~13, 또는 15인 경우)	다음 세 종류의 어셈블리를 사용할 수 있습니다. · Safety Remote Output 1 + Standard Output · Safety Remote Output 2 · Safety Remote Output 3

I/O 어셈블리에 대한 자세한 내용은 A-14페이지의 A-3 I/O 어셈블리 포트 및 대응하는 세이프티 I/O 어셈블리 데이터 요소를 참조하십시오.

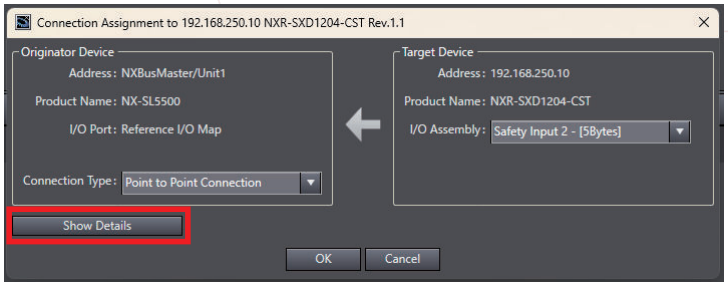
커넥션 파라미터 편집 절차

다음 절차를 사용하여 CIP Safety 커넥션의 파라미터를 편집합니다.

1 Connection Settings (Originator) Edit Pane에서 세이프티 I/O 블록의 커넥션을 선택한 후 마우스 오른쪽 버튼을 클릭하고 Edit를 선택합니다.

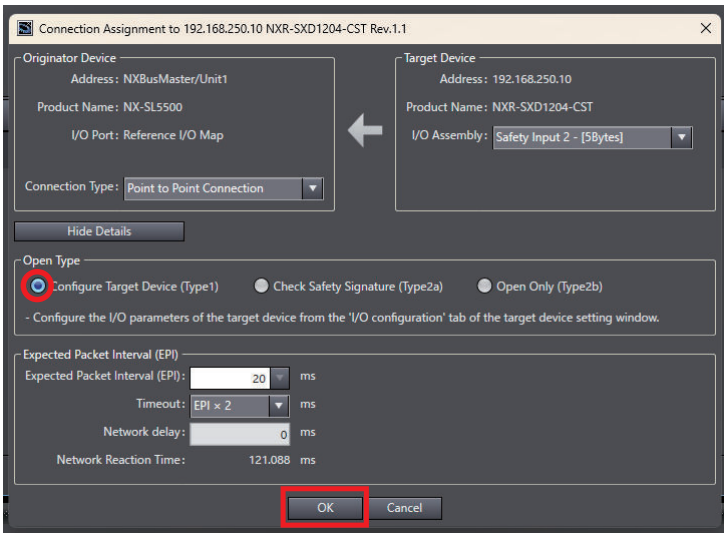


2 **Detailed Display를 선택합니다.**



3 Open Type 설정에서 Configure Target Device를 선택하고 OK 버튼을 클릭합니다.

AI 번역본
-For Reference Only-



항목	설명
I/O 어셈블리	I/O 어셈블리는 CIP Safety 오리지네이터와 CIP Safety 타겟 간에 주기적으로 교환되는 I/O 데이터의 단위입니다. 세이프티 I/O 블록에는 여러 I/O 어셈블리가 정의되어 제공됩니다. 정의된 I/O 어셈블리 중에서 선택하여 CIP Safety 커넥션당 하나의 I/O 어셈블리를 등록합니다. CIP Safety 커넥션을 열 수 있는 타겟 기기의 I/O 어셈블리가 나열됩니다.
Connection Type	입력 커넥션(타겟 기기로부터 수신)의 경우, Point to Point Connection 또는 **Multicast Connection 중 하나를 선택합니다.** **기본 설정은 Point to Point Connection입니다.**
Open Type	커넥션을 여는 방식의 유형을 선택합니다. ・Configure Target Device (Type1) 커넥션이 확립된 후 타겟 기기를 구성합니다. ・Check Safety Signature (Type2a) 세이프티 시그니처를 사용하여 커넥션을 확립할 때 타겟 기기가 올바르게 구성되어 있는지 확인합니다. 세이프티 시그니처는 Safety Configuration CRC와 Safety Configuration Time Stamp로 구성됩니다. ・Open Only (Type2b) 커넥션을 확립할 때 타겟 기기의 구성 확인을 수행하지 않습니다. **기본 설정은 Configure Target Device (Type1)입니다.**
Expected Packet Interval (EPI)	오리지네이터와 타겟 간 세이프티 프로세스 데이터의 통신 간격을 설정합니다. 기본 설정은 20(ms)입니다. 설정 범위에 대한 자세한 내용은 2-3페이지의 2-1-2 통신 사양을 참조하십시오.
Timeout	통신 에러를 판정하기 위한 타임아웃 기간을 EPI의 배수로 지정합니다. 기본 설정은 EPI x 2(ms)입니다(타임아웃은 1회만 허용). 배수의 설정 범위는 1~4입니다.
Network Delay	네트워크상의 전송 지연 시간을 설정합니다. 기본 설정은 0(ms)입니다.
Network Reaction Time	커넥션 응답 성능값이 ms 단위로 표시됩니다. 이 값은 세이프티 반응 시간을 계산하는 데 사용됩니다.

- For Reference Only -

⚠ 경고

Open Type을 Open Only로 설정한 경우, 사용하기 전에 오리지네이터와 타겟이 올바르게 구성되어 있는지 반드시 확인하십시오.
필요한 세이프티 기능이 상실되어 중대한 상해가 발생할 수 있습니다.

추가 정보

다음은 등록된 커넥션 수에 대한 EPI 최솟값의 지침입니다. 입력의 커넥션 유형이 멀티캐스트인 경우, 8개의 오리지네이터가 연결되어 있는 것으로 간주합니다.

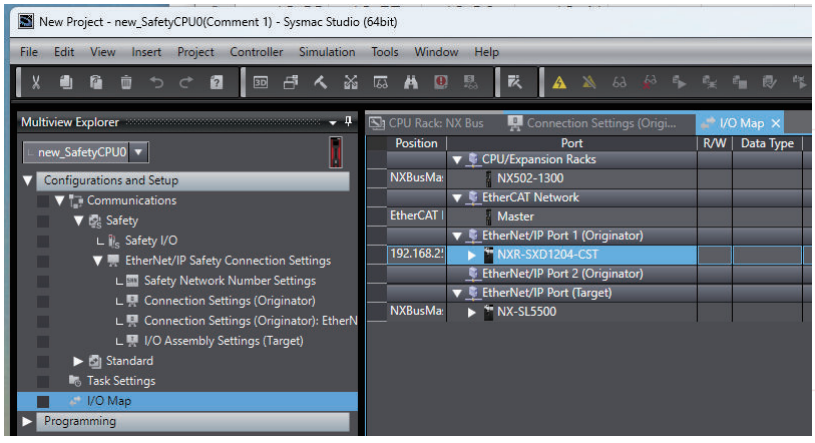
커넥션 수	EPI 최솟값
1(입력 1개 또는 출력 1개)	5 ms
5(입력 2개 및 출력 3개)	20 ms

4 설정이 완료되면 OK 버튼을 클릭합니다.

디바이스 변수 등록 절차

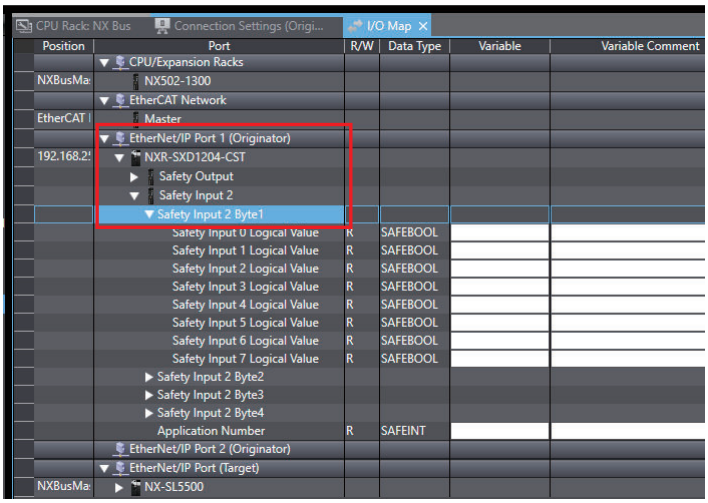
디바이스 변수는 기기(슬레이브, 유닛, 세이프티 I/O 블록)의 데이터에 액세스하는 데 사용됩니다.
세이프티 CPU 유닛은 "I/O 포트"라고 하는 논리 인터페이스를 통해 외부 기기와 신호를 교환합니다.
다음은 세이프티 CPU 유닛의 세이프티 프로그램에서 기기의 I/O 값을 사용할 수 있도록, 기기의 I/O 포트에 디바이스 변수를 등록하는 절차입니다.
이는 NXR-SXD1204-CST 세이프티 I/O 블록을 사용한 예시입니다.

1 멀티뷰 익스플로러에서 Configurations and Setup - I/O Map을 선택합니다.

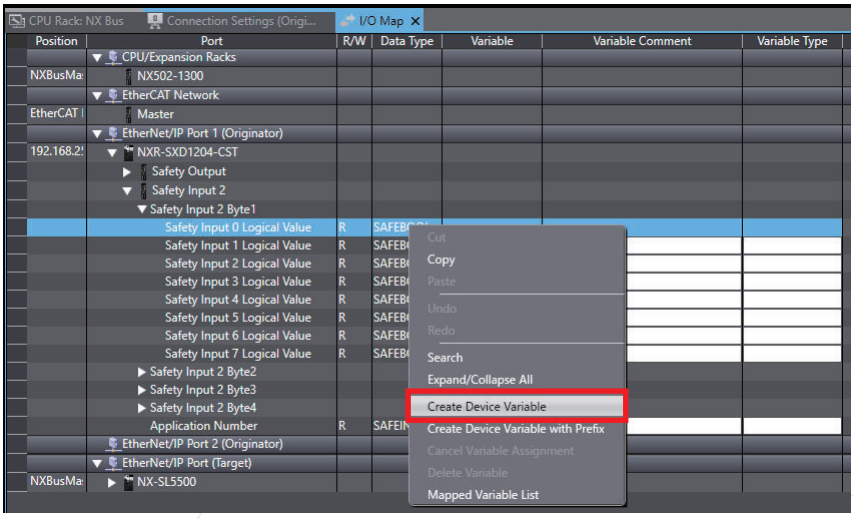


Edit Pane에 I/O Map Edit Pane이 표시됩니다.

2 **I/O Map Edit Pane에서 EtherNet/IP Port 1 (Originator) - NXR-SXD1204-CST–Safety Input 2–Safety Input 2 Byte1을 엽니다.**

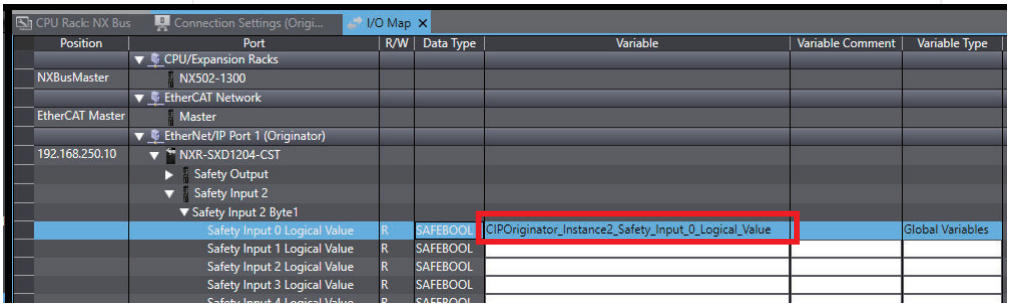


3 I/O 포트를 선택하고 Variable 열에 변수를 직접 입력합니다. 또는 세이프티 I/O 블록 이름이나 I/O 포트(복수 선택 가능)를 선택한 후 마우스 오른쪽 버튼을 클릭하고 Create Device Variable을 선택합니다. Create Device Variable을 선택하면 디바이스 변수의 이름이 기기 이름과 포트 이름으로 자동으로 지정됩니다.



AI 번역본

디바이스 변수가 등록됩니다.



입력하거나 자동으로 생성한 디바이스 변수는 글로벌 변수 테이블에 등록됩니다.

추가 정보

변수를 미리 등록해 둔 경우, 풀다운 목록에서 I/O 포트에 할당할 변수를 선택합니다.

7-3-2 세이프티 I/O 블록 설정의 익스포트 및 임포트

세이프티 I/O 블록의 설정을 하나의 파일(확장자 .tds)로 익스포트 및 임포트하여 재사용할 수 있습니다. 다음

데이터가 처리됩니다.

- CPU 유닛 및 커넥션 설정
- Sysmac Studio에서 설정한 세이프티 I/O 블록의 IP 주소
- 세이프티 I/O 블록의 I/O 기능 설정

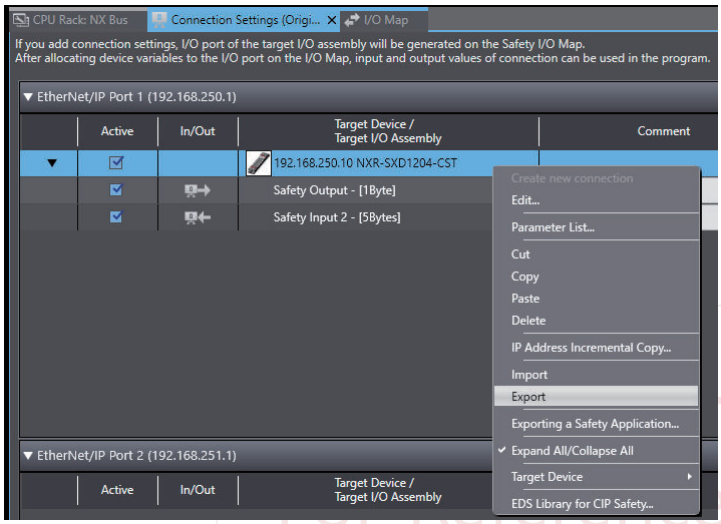
추가 정보

Web UI를 사용한 백업, 검증, 복원에 대한 자세한 내용은 7-108페이지의 7-19 백업을 참조하십시오.

설정 익스포트 방법

세이프티 I/O 블록의 설정을 익스포트하는 절차는 다음과 같습니다.

1 Connection Settings (Originator) Edit Pane에서 Safety I/O Block을 선택한 후 마우스 오른쪽 버튼을 클릭하고 메뉴에서 Export를 선택합니다.



Export 대화 상자가 표시됩니다.

2 저장 위치를 선택하고 파일 이름을 입력한 후 Save 버튼을 클릭합니다.

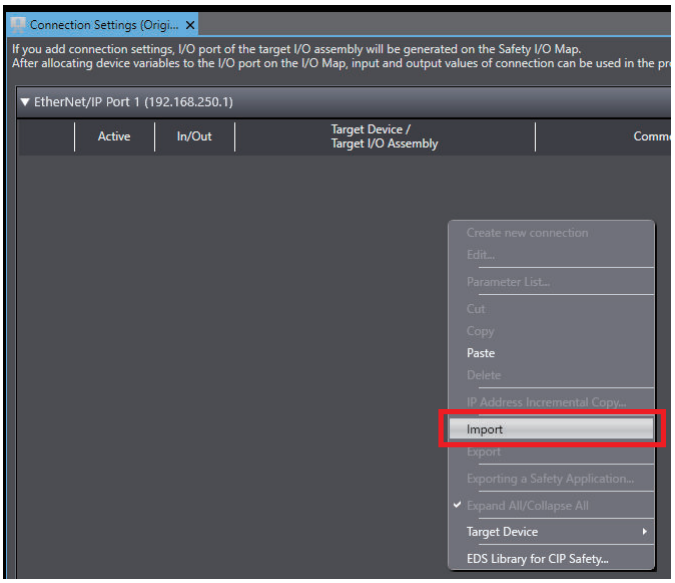
세이프티 I/O 블록의 구성 파일이 지정한 저장 위치에 .tds 확장자로 저장됩니다.
기본 파일 이름은 IP 주소_타겟 기기 이름.tds입니다.

For Reference Only-

설정 임포트 절차

세이프티 I/O 블록의 설정을 임포트하는 절차는 다음과 같습니다.

1 Connection Settings (Originator) Edit Pane에서 Safety I/O Block을 선택한 후 마우스 오른쪽 버튼을 클릭하고 메뉴에서 Import를 선택합니다.



Import 대화 상자가 표시됩니다.

2 확장자가 .tds인 원하는 세이프티 I/O 블록 구성 파일을 선택하고 Open 버튼을 클릭합니다.

사용상의 주의

타겟 기기 구성 파일의 데이터 무결성은 임포트 시 CRC로 확인되지 않습니다.
임포트 후 설정이 올바른지 확인하고, 실제 운전으로 전환하기 전에 동작을 충분히 확인하는 것은 사용자의 책임입니다.

AI 번역본
-For Reference Only-

7-4 EtherNet/IP 통신 설정

이 절에서는 EtherNet/IP 오리지네이터와 EtherNet/IP 타겟의 세이프티 I/O 블록을 사용한 태그 데이터 링크 통신용 커넥션 설정 방법 및 LLDP 기능 설정 방법에 대해 설명합니다.

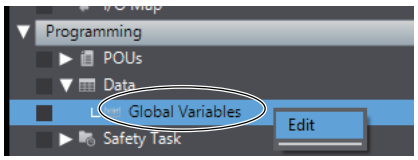
7-4-1 태그 데이터 링크 통신 설정

세이프티 I/O 블록과 오리지네이터 간의 태그 데이터 링크 통신용 커넥션을 설정합니다.

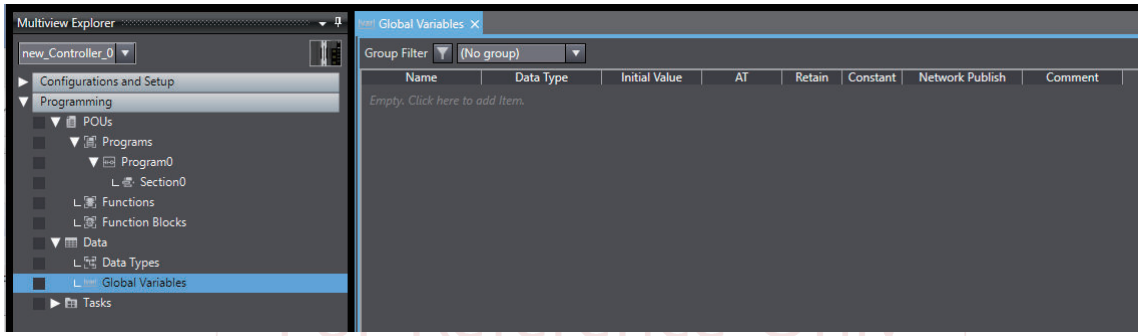
태그 데이터 링크 통신 설정 절차

이 절에서는 Sysmac Studio를 사용하여 세이프티 I/O 블록의 태그 데이터 링크 통신을 설정하는 절차에 대해 설명합니다.
다음 절차는 표준 컨트롤러에 내장된 EtherNet/IP 포트를 오리지네이터로 사용하여, 태그 데이터 링크의 I/O 어셈블리 데이터에서 입력 데이터(Assembly 960~3C0 hex)와 크기: 5바이트를 설정하는 예시입니다.

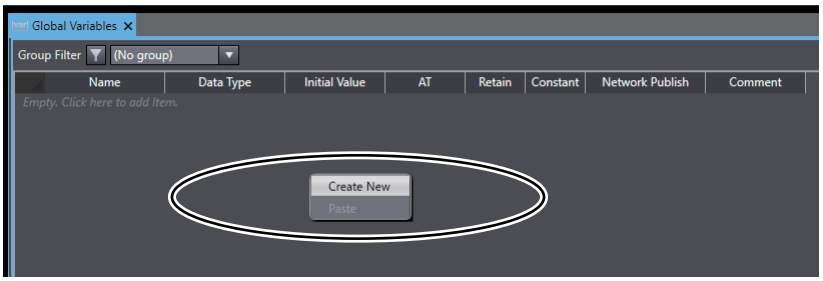
1 멀티뷰 익스플로러에서 Programming - Data 아래의 Global Variables를 더블 클릭합니다.
또는 Programming - Data 아래의 Global Variables를 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 Edit를 선택합니다.



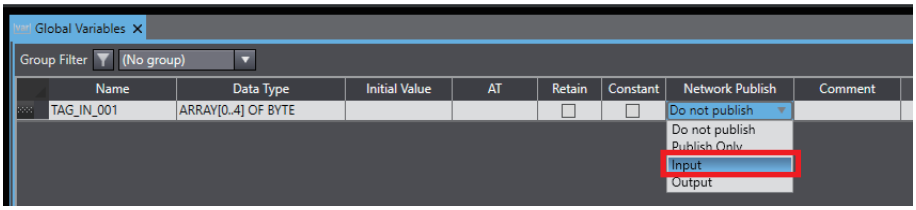
글로벌 변수 등록 테이블이 표시됩니다.



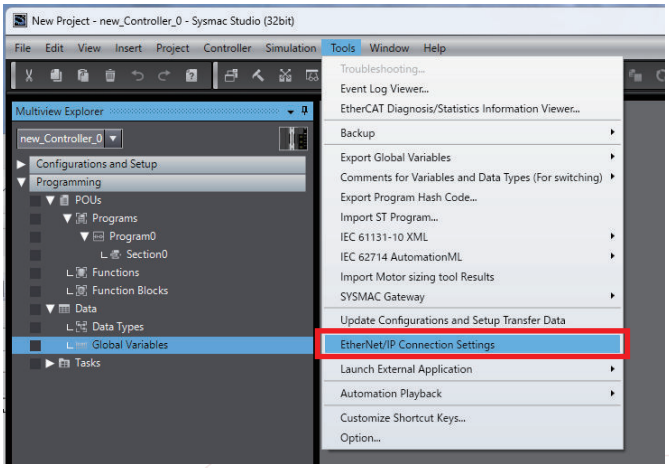
2 글로벌 변수 테이블에서 Insert 키를 누르거나, 글로벌 변수 테이블을 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 Create New를 선택합니다.



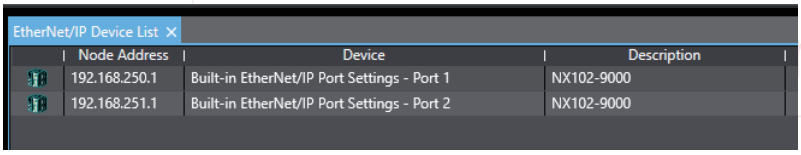
3 글로벌 변수에 5바이트 변수를 등록하고 Network Publish를 Input으로 설정합니다.



4 멀티뷰 익스플로러에서 Standard PLC(초기 표시 new_Controller_0)를 선택하고, 화면 상단의 메뉴 바에 있는 Tools 메뉴에서 EtherNet/IP Connection Settings를 선택합니다.

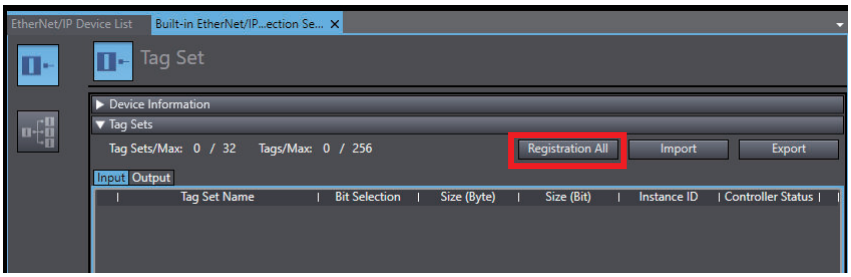


5 태그 데이터 링크를 설정할 네트워크를 더블 클릭하거나, 마우스 오른쪽 버튼을 클릭하고 Edit를 선택합니다.

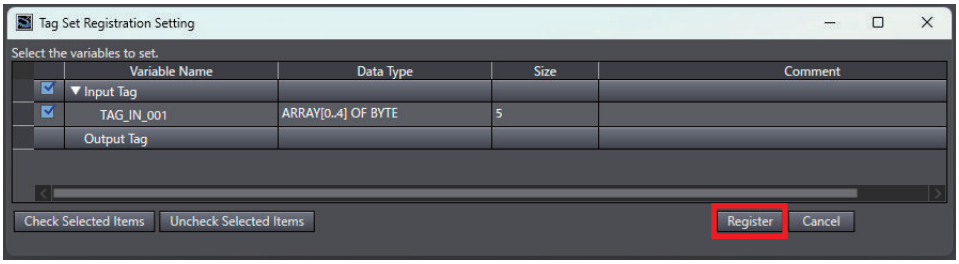


6 Input 탭이 선택되어 있는지 확인한 후 Registration All을 클릭합니다.

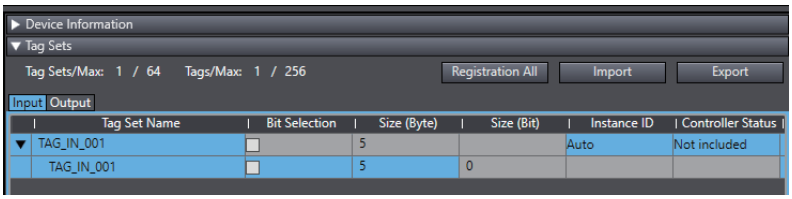
AI 번역본



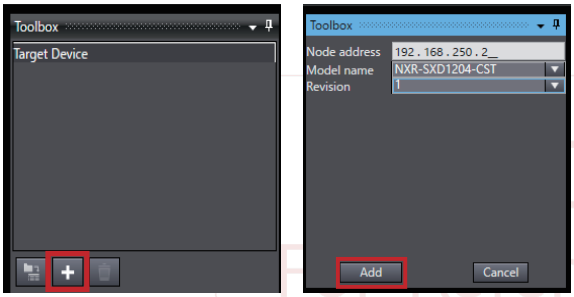
7 3단계에서 등록한 변수가 표시되는지 확인한 후 Register를 클릭합니다.



태그 세트가 등록됩니다.



8 Target Device 필드의 + 버튼을 클릭하고, 타겟의 IP 주소, 모델명, 리비전을 입력한 후 Add 버튼을 클릭합니다.

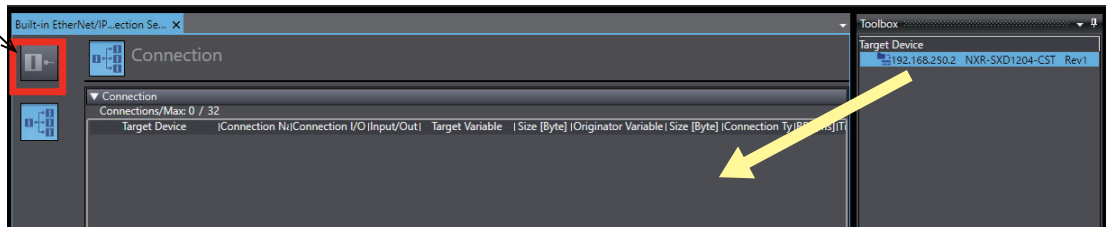


검토용 견본
Reference Only

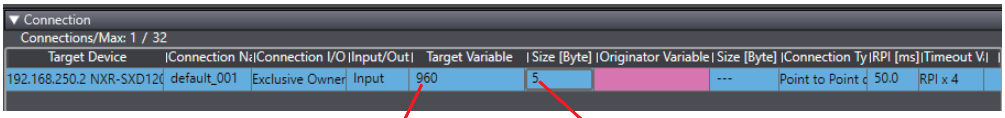
모델명이 풀다운 목록에 없는 경우, 해당 모델의 EDS 파일을 설치하십시오. EDS 파일의 설치 절차는 아래의 추가 정보에 있는 EDS 파일 설치 절차를 참조하십시오.

9 Connection 버튼을 클릭하여 Connection Settings 화면을 엽니다. 방금 추가한 타겟의 정보가 Target Device 필드에 표시됩니다. 이를 Connection 창으로 드래그 앤 드롭합니다.

Connection
버튼



10 타겟 기기가 Connection 창에 추가됩니다. 타겟 변수를 입력합니다.



Input Data (Assembly 960 to 3C0 Hex), Size 5 Bytes

Byte	Bit							
	7	6	5	4	3	2	1	0
0	Safety Input 7	Safety Input 6	Safety Input 5	Safety Input 4	Safety Input 3	Safety Input 2	Safety Input 1	Safety Input 0
1	Safety Input 3 Status	Safety Input 2 Status	Safety Input 1 Status	Safety Input 0 Status	Safety Input 11	Safety Input 10	Safety Input 9	Safety Input 8
2	Safety Input 11 Status	Safety Input 10 Status	Safety Input 9 Status	Safety Input 8 Status	Safety Input 7 Status	Safety Input 6 Status	Safety Input 5 Status	Safety Input 4 Status
3	Safety Input Status	Safety Output Status	Output Power Supply Error Flag	Cnxn Status	Reserved	Reserved	Reserved	Reserved
4	Application Number							

타겟 변수 및 크기에는 A-4페이지의 A-2 세이프티 I/O 어셈블리 데이터 표에 나와 있는 Assembly 및 Size 값을 입력합니다.

필요에 따라 Connection I/O Type, Connection Type, RPI, Timeout Value를 설정합니다.

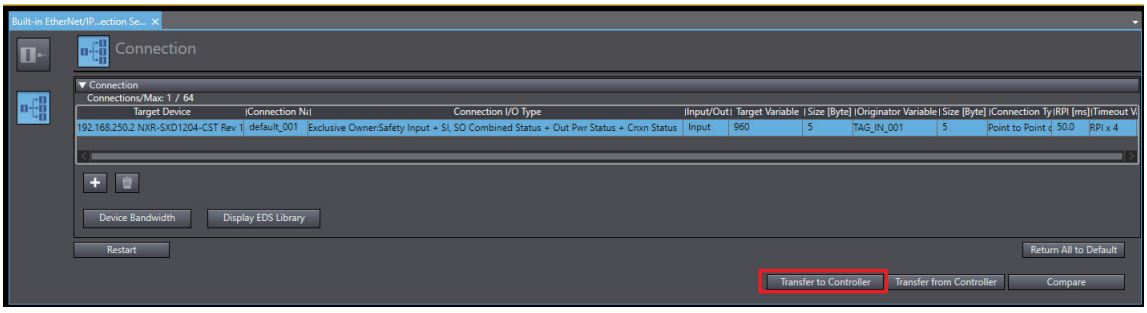
11 오리지네이터 변수도 동일한 방법으로 입력합니다.

오리지네이터 변수의 경우, 풀다운 목록에서 7단계에서 설정한 태그 세트 이름을 선택합니다.

12 온라인 상태로 전환하고 태그 세트 및 커넥션 설정을 기기에 씁니다.●

태그 데이터 링크 설정만 전송하는 경우

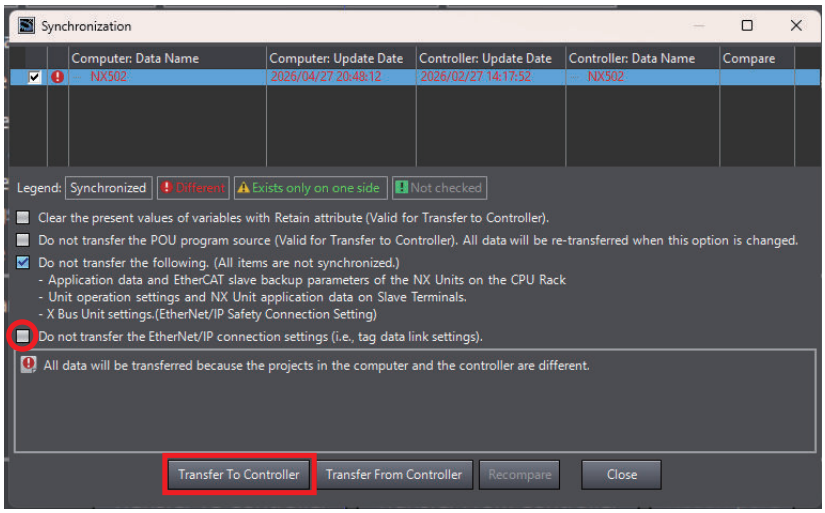
커넥션 설정 화면에서 Transfer to Controller를 클릭합니다.



● 프로그램을 포함한 모든 데이터를 동기화하는 경우

AI 번역본
For Reference Only

Controller 메뉴에서 Synchronization을 선택하여 Synchronization 창을 표시합니다.
Do not transfer the EtherNet/IP connection settings (i.e., the tag data link settings) 확인란의 선택을 해제하고 Transfer to Controller를 클릭합니다.



7-4-2 LLDP 기능

Link Layer Discovery Protocol(LLDP) 기능은 세이프티 I/O 블록과 네트워크상에서 물리적으로 통신 가능한 범위 내에 연결된 다른 네트워크 기기 간에 정보를 교환하는 데 사용됩니다.

LLDP 기능의 목적

LLDP 기능의 목적은 인접한 네트워크 기기의 정보를 수집하여 신속한 네트워크 구성 변경 및 에러 원인 파악을 가능하게 하는 것입니다.
예를 들어, 이 기능을 사용하면 어떤 기기가 네트워크에 연결되어 있는지, 해당 기기에서 현재 어떤 기능이 활성화되어 있는지를 검출할 수 있습니다. 이를 통해 통신 에러의 원인이 네트워크 기기 구성 실수임을 파악할 수 있는 등의 이점이 있습니다.

LLDP 기능 사용 절차

LLDP 기능의 활성화/비활성화 설정은 익스플리시트 메시지 통신을 사용하여 구성합니다.
LLDP 기능과 관련된 CIP 오브젝트는 LLDP Management 오브젝트와 LLDP Data Table 오브젝트입니다.
각각에 대한 자세한 내용은 A-51페이지의 A-4-12 LLDP Management Object(Class ID: 109 Hex)와 A-53페이지의 A-4-13 LLDP Data Table Object(Class ID: 10A Hex)를 참조하십시오.
익스플리시트 메시지를 통해 CIP 오브젝트에 액세스하는 방법에 대한 자세한 내용은 6-7페이지의 익스플리시트 메시지 서버 기능을 참조하십시오.

AI 번역본
-For Reference Only-

LLDP 기능 상세

LLDP 기능을 사용하여 취득할 수 있는 네트워크 기기 정보는 다음과 같습니다.

- MAC 주소
- 인터페이스 라벨

- 취득한 정보의 유효 시간
- 지원 기능
- 관리 주소
- CIP Identity
- Ethernet Preemption 기능 상태
- 정보가 마지막으로 갱신된 시각 정보

AI 번역본
-For Reference Only-

7-5 세이프티 입력 기능 설정

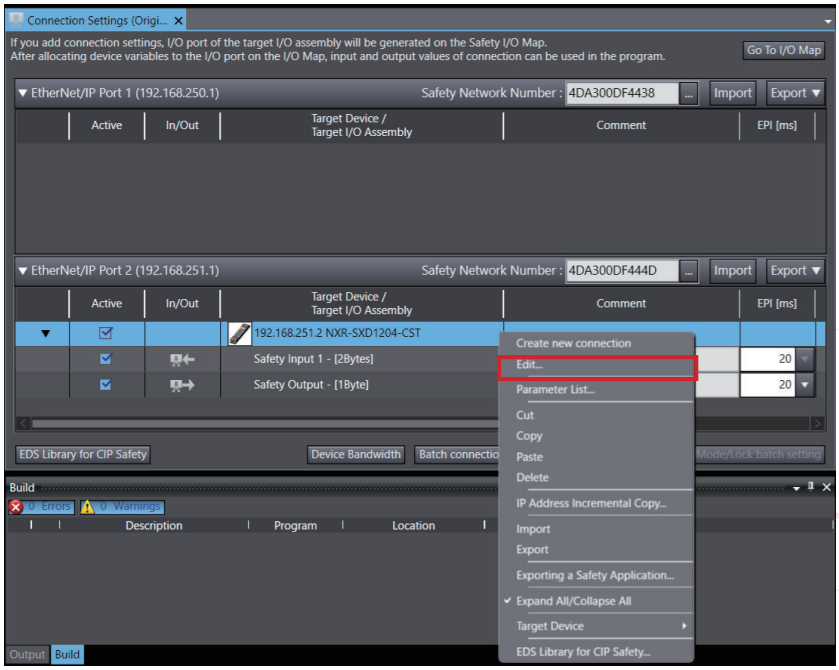
세이프티 입력 기능의 설정을 구성하려면 연결된 기기에 맞게 파라미터를 설정해야 합니다.

이 절에서는 Sysmac Studio를 사용한 절차를 예시로 설명합니다.

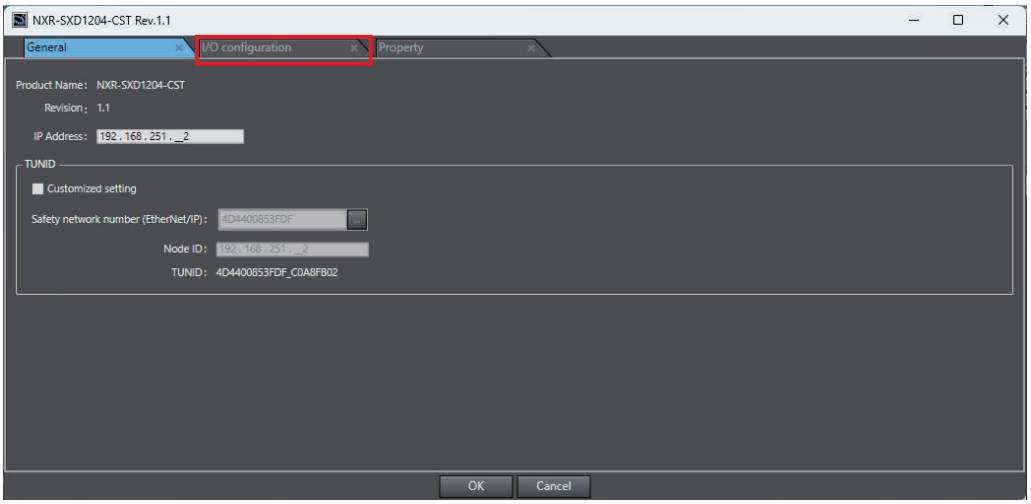
7-5-1 세이프티 입력 기능 설정 절차

입력 기기를 세이프티 I/O 블록에 할당하여 세이프티 I/O 블록의 세이프티 입력 기능을 설정합니다.
또한 연결된 입력 기기로부터의 신호를 취입하려면, 세이프티 I/O 블록의 각 입력
단자에 대한 I/O 구성 설정을 구성해야 합니다.
Sysmac Studio에서는 이러한 설정이 Connection Settings (Originator) Edit Pane에 있으므로,
그 페인부터 설명을 시작합니다.
CIP Safety 커넥션 설정에 대한 자세한 내용은 7-27페이지의 7-3-1 CIP Safety 통신 커넥션
설정을 참조하십시오.
세이프티 입력 기능에 대한 자세한 내용은 6-8페이지의 6-4 세이프티 입력 기능도 참조하십시오.
다음은 Connection Settings (Originator) Edit Pane에 등록된 기기에 대해 I/O 구성
설정을 구성하는 절차입니다.

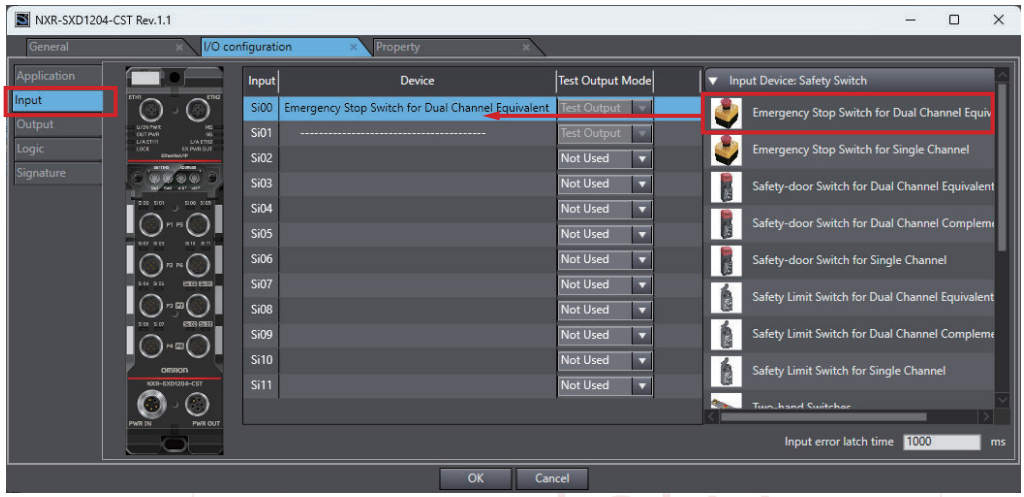
1 Connection Settings (Originator) Edit Pane에서 Safety I/O Block을 선택하고 더블 클릭하거나, 마우스 오른쪽 버튼을 클릭하고 메뉴에서 Edit를 선택합니다.



2 **I/O configuration 탭을 선택합니다.**

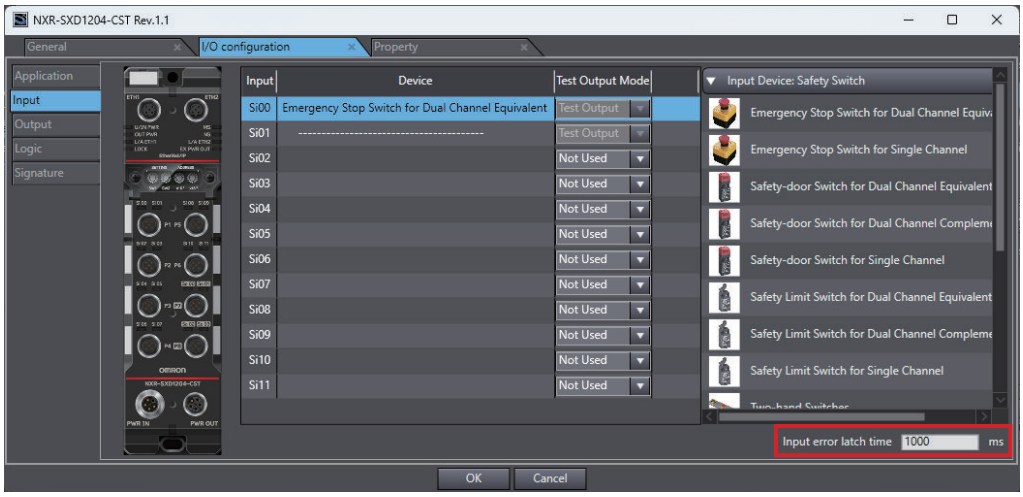


3 I/O Configuration Pane에서 입력 기기를 등록합니다. 다음 등록은 세이프티 애플리케이션이 remote I/O mode 또는 사용자 정의 애플리케이션인 경우에만 가능합니다.
왼쪽의 Input 탭을 선택하면 입력 기기 등록 화면이 표시됩니다. 오른쪽의 툴박스를 확장하고 원하는 기기를 지정된 단자로 드래그 앤 드롭하여 입력 기기를 등록합니다.

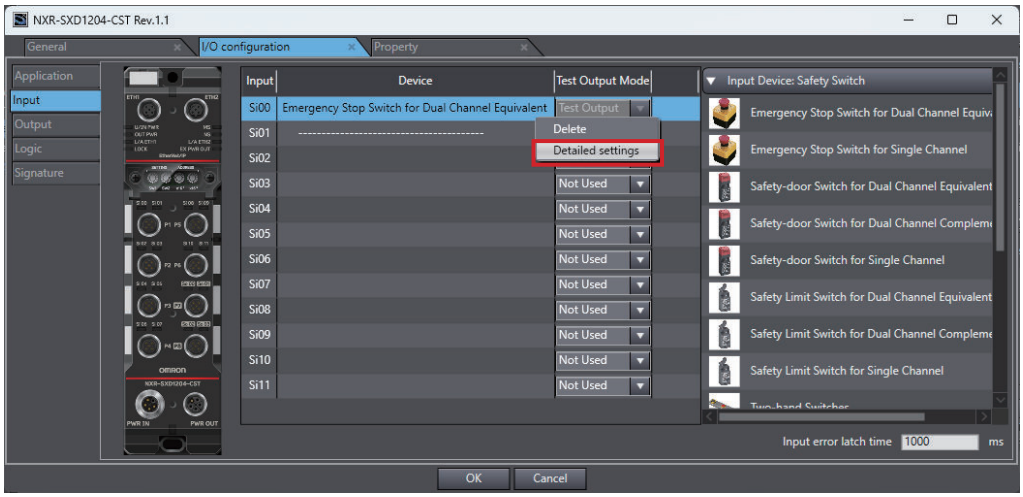


4 필요에 따라 화면 오른쪽 하단의 Input error latch time을 설정합니다.

AI 번역본
-For Reference Only-



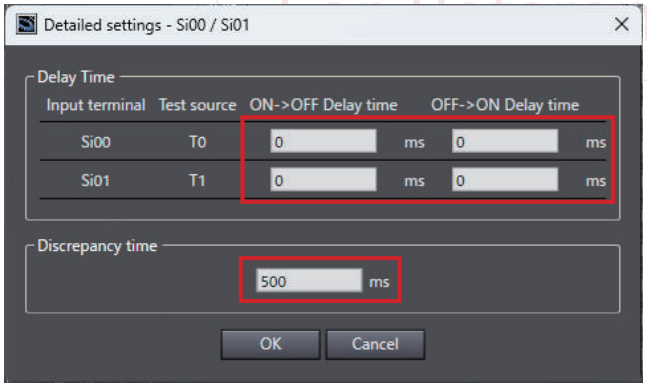
5 등록된 입력 기기를 선택하고 더블 클릭하거나, 등록된 입력 기기의 컨텍스트 메뉴에서 Detailed settings를 선택하여 Detailed settings 화면을 표시합니다.



6 필요에 따라 다음 항목을 설정합니다.

- **ON->OFF Delay time**
- **OFF->ON Delay time**
- Discrepancy Time(듀얼 채널 입력 기기 전용)

AI 번역본
For Reference Only-



7 설정이 완료되면 OK 버튼을 클릭합니다.

7-5-2 표준 출력 기능 설정 절차

세이프티 입력 기기가 반도체 출력을 갖는 기기인 경우, 테스트 출력 단자의 Test Output Mode 설정에서 Standard Output을 선택할 수도 있습니다.
테스트 출력 단자를 사용하여 컨트롤러로부터의 표준 출력이 가능합니다.
비세이프티 디지털 신호 출력 단자로 사용하십시오. 예를 들어 표시등이나 PLC의 입력에 연결하여 모니터 출력용으로 사용할 수 있습니다.
표준 출력 기능에는 Sysmac Studio를 사용하는 방법과 익스플리시트 메시지 통신을 사용하는 방법이 있습니다.

추가 정보

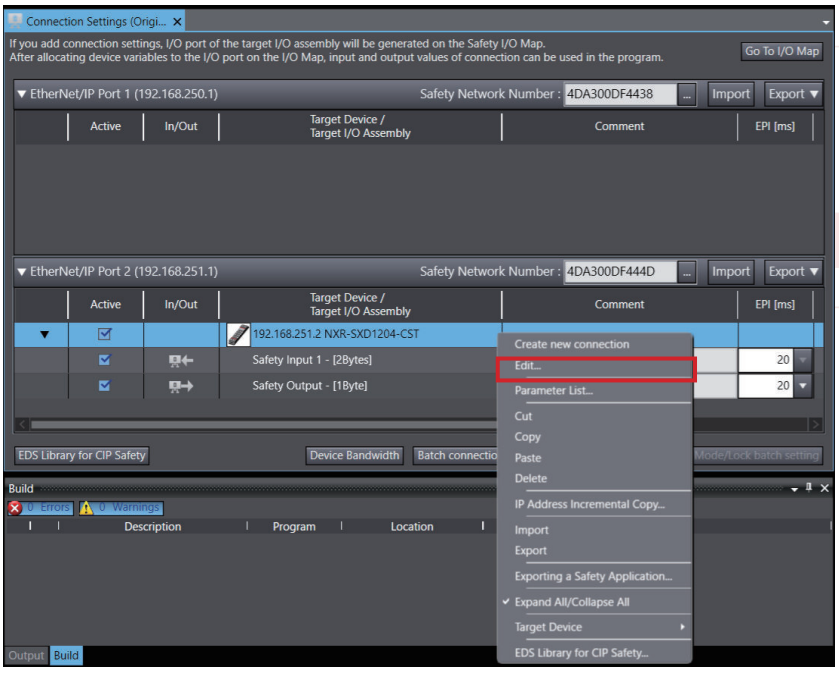
이 기능은 세이프티 기능이 아닙니다.

Sysmac Studio를 사용한 설정 절차

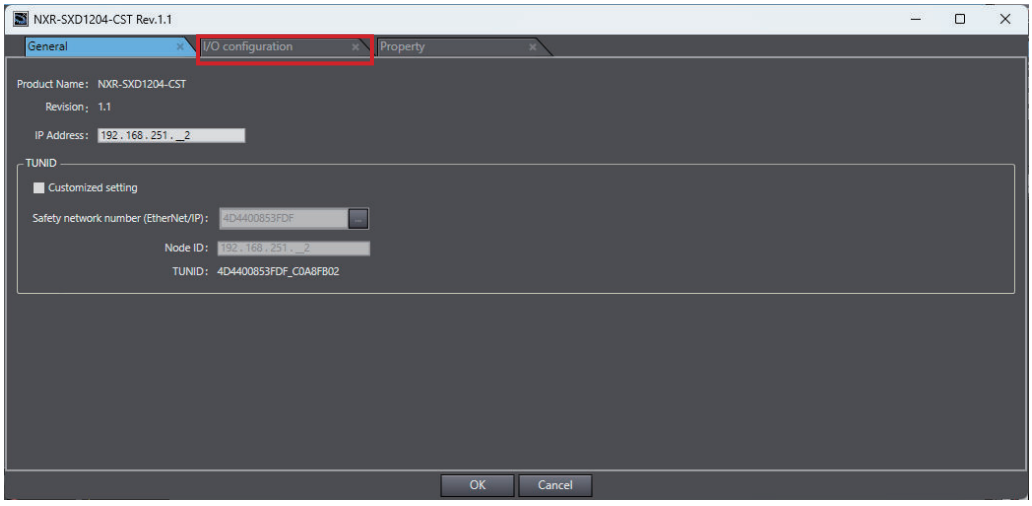
Sysmac Studio를 사용한 절차는 다음과 같습니다.
Sysmac Studio에서는 이러한 설정이 Connection Settings (Originator) Edit Pane에 있으므로, 그 페인부터 설명을 시작합니다.
CIP Safety 커넥션 설정에 대한 자세한 내용은 7-27페이지의 7-3-1 CIP Safety 통신 커넥션 설정을 참조하십시오.

세이프티 입력 기능에 대한 자세한 내용은 6-8페이지의 6-4 세이프티 입력 기능도 참조하십시오.
다음은 Connection Settings (Originator) Edit Pane에 등록된 기기에 대해 I/O 구성 설정을 구성하는 절차입니다.

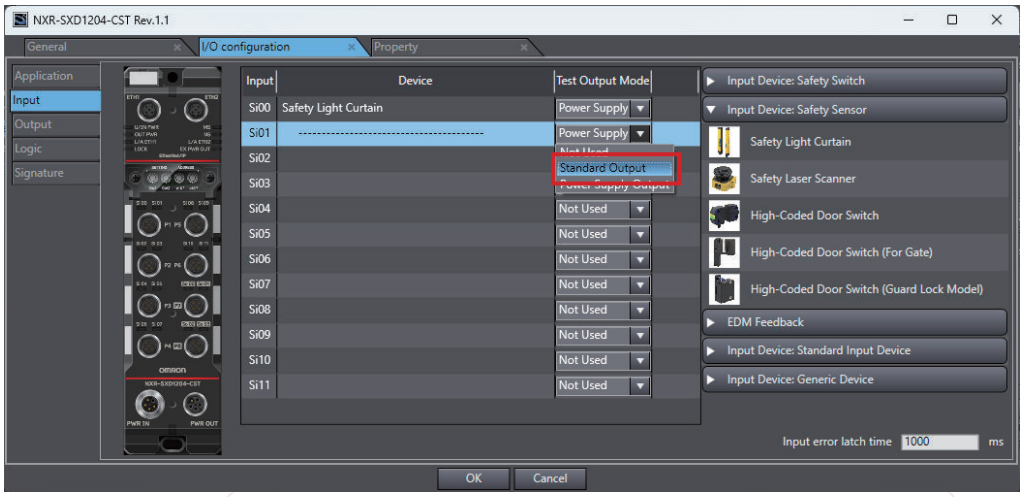
1 Connection Settings (Originator) Edit Pane에서 Safety I/O Block을 선택하고 더블 클릭하거나, 마우스 오른쪽 버튼을 클릭하고 메뉴에서 Edit를 선택합니다.



2 **I/O configuration 탭을 선택합니다.**



3 반도체 출력을 갖는 기기인 입력 기기 단자의 Test Output Mode 설정에서 Standard Output을 선택합니다.
설정은 세이프티 애플리케이션이 remote I/O mode 또는 사용자 정의
애플리케이션인 경우에만 가능합니다.



4 설정이 완료되면 OK 버튼을 클릭합니다.

AI 번역본
For Reference Only

익스플리시트 메시지 통신을 사용한 설정 절차

테스트 출력 모드의 사용 방법을 Standard Output으로 설정합니다. 또한 테스트 출력 단자의 출력값을 설정합니다.
전송할 명령은 다음과 같습니다.

구현 세부 사항	전송 명령 항목	전송 명령값
테스트 출력 단자의 출력값 설정*1	Service code	10 hex (Set_Attribute_Single)
	Class ID	09 hex (Discrete Output Point (DOP) 오브젝트)
	Instance ID	01 hex~0C hex(각 테스트 출력 단자의 인스턴스를 지정합니다.)
	Attribute ID	3 (Value)
	Service data	TRUE: 테스트 출력 단자 ON FALSE: 테스트 출력 단자 OFF

***1.** Test Output Mode가 Standard Output인 경우에만 값을 쓸 수 있습니다. 그 외의 경우에는 테스트 출력 단자의 출력값이 TRUE로 고정됩니다.

익스플리시트 메시지를 통해 CIP 오브젝트에 액세스하는 방법에 대한 자세한 내용은 6-7페이지의 익스플리시트 메시지 서버 기능을 참조하십시오.

AI 번역본
-For Reference Only-

7-6 세이프티 출력 기능 설정

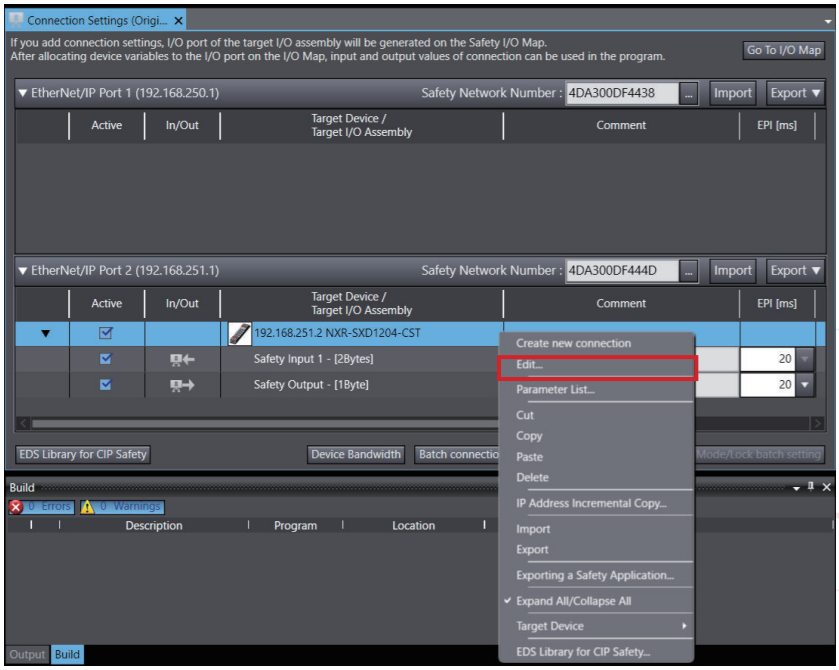
세이프티 출력 기능의 설정을 구성하려면 연결된 기기에 맞게 파라미터를 설정해야 합니다.

이 절에서는 Sysmac Studio를 사용한 절차를 예시로 설명합니다.

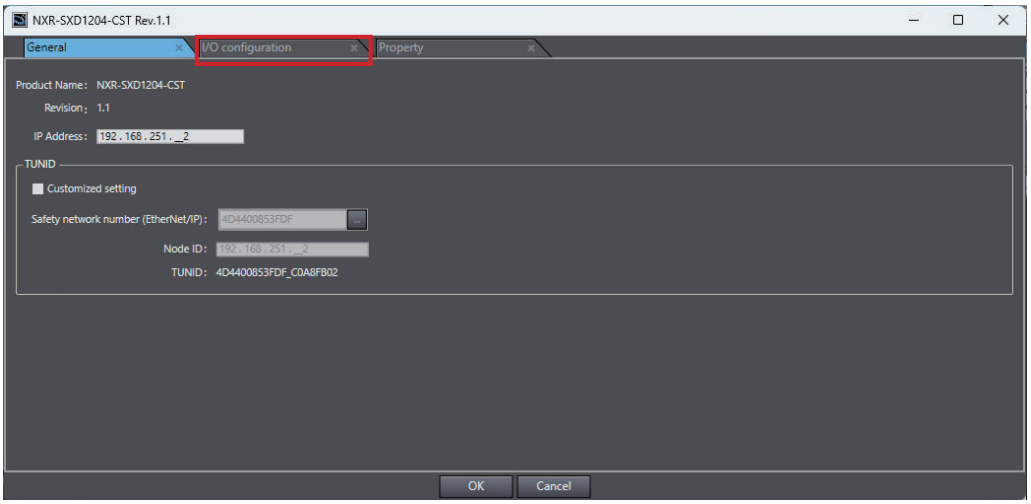
7-6-1 세이프티 출력 기능 설정 절차

출력 기기를 세이프티 I/O 블록에 할당하여 세이프티 I/O 블록의 세이프티 출력 기능을 설정합니다.
또한 연결된 출력 기기로 신호를 출력하려면, 세이프티 I/O 블록의 각 출력 단자에 대한
I/O 구성 설정을 구성해야 합니다.
Sysmac Studio에서는 이러한 설정이 Connection Settings (Originator) Edit Pane에 있으므로,
그 페인부터 설명을 시작합니다.
CIP Safety 커넥션 설정에 대한 자세한 내용은 7-27페이지의 7-3-1 CIP Safety 통신 커넥션
설정을 참조하십시오.
세이프티 출력 기능에 대한 자세한 내용은 6-16페이지의 6-5 세이프티 출력 기능도 참조하십시오.
다음은 Connection Settings (Originator) Edit Pane에 등록된 기기에 대해 I/O 구성
설정을 구성하는 절차입니다.

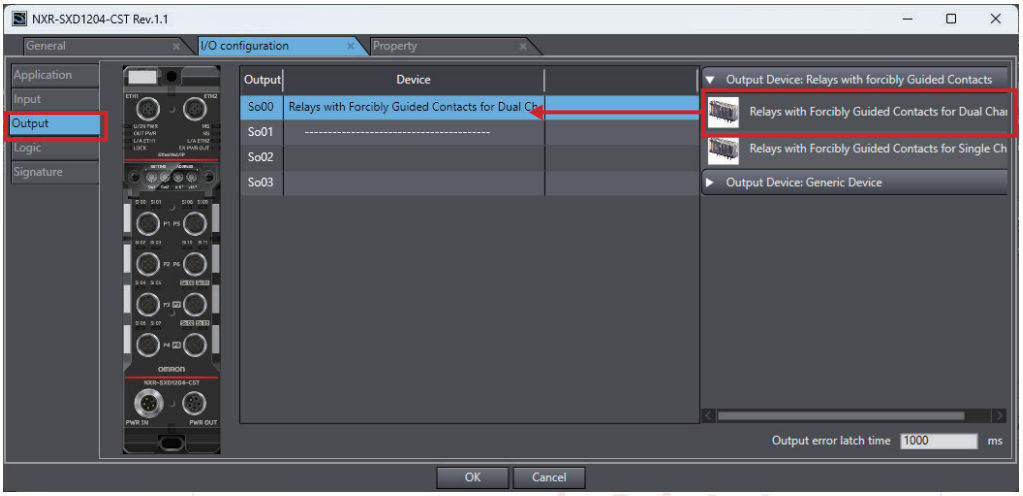
1 Connection Settings (Originator) Edit Pane에서 Safety I/O Block을 선택하고 더블 클릭하거나, 마우스 오른쪽 버튼을 클릭하고 메뉴에서 Edit를 선택합니다.



2 **I/O configuration 탭을 선택합니다.**



3 I/O 설정 화면에서 출력 기기를 등록합니다. 다음 등록은 세이프티 애플리케이션이 리모트 I/O 모드 또는 사용자 정의 애플리케이션인 경우에만 가능합니다.
왼쪽의 Output 탭을 선택하여 출력 기기 등록 화면을 표시합니다. 오른쪽의 툴박스를 확장하고 원하는 기기를 지정된 단자로 드래그 앤드 드롭하여 출력 기기를 등록합니다.



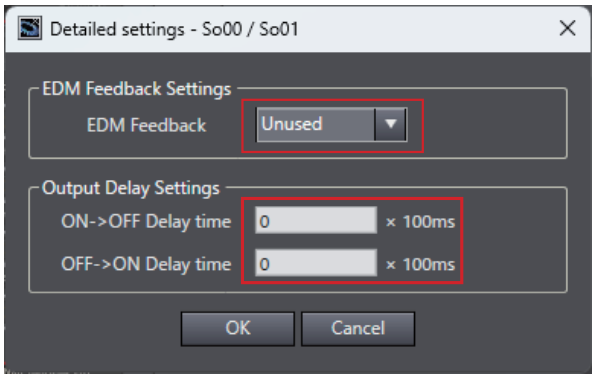
4 보안 애플리케이션이 사용자 정의 애플리케이션인 경우, 드래그 앤드 드롭하면 상세 설정 화면이 표시되며, 여기서 다음 항목을 설정할 수 있습니다.

・EDM 피드백(세이프티 입력 기기에 EDM 피드백이 등록된 단자에서만 표시됨)

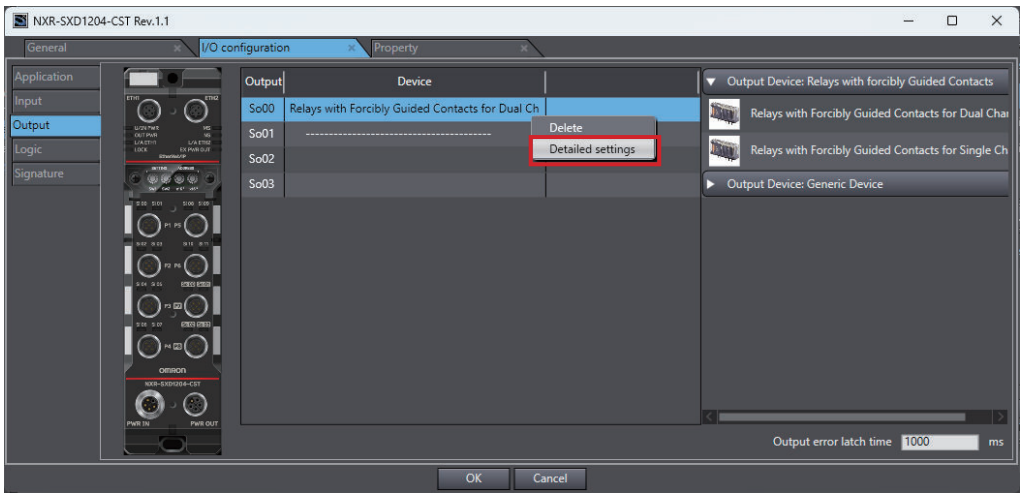
・ON->OFF 지연 시간

・OFF->ON 지연 시간

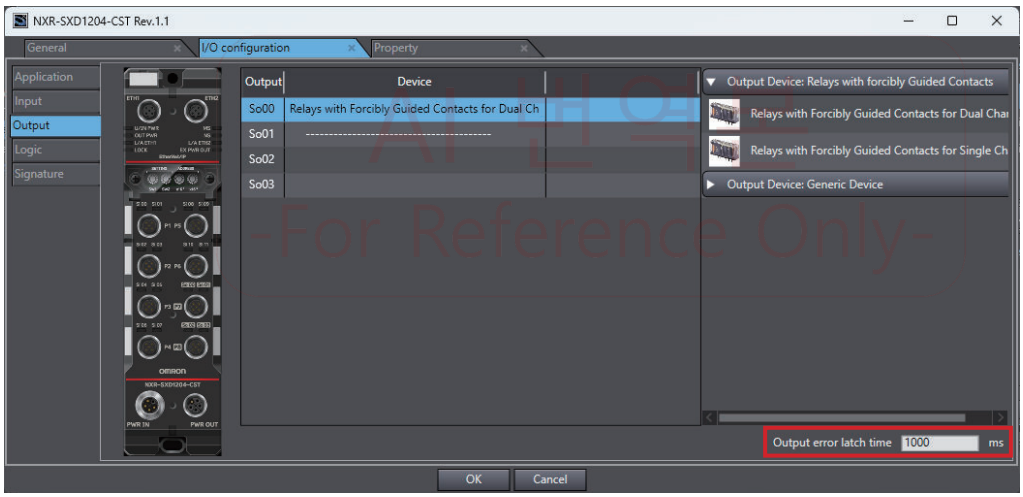
AI 번역본
-For Reference Only-



5 세이프티 애플리케이션이 사용자 정의 애플리케이션인 경우, 등록된 출력 기기를 선택하고 더블 클릭하거나, 등록된 출력 기기의 컨텍스트 메뉴에서 Detailed settings를 선택하여 상세 설정 화면을 표시할 수도 있습니다.



6 필요에 따라 화면 오른쪽 하단에서 Output error latch time을 설정합니다.



7 설정이 완료되면 OK 버튼을 클릭합니다.

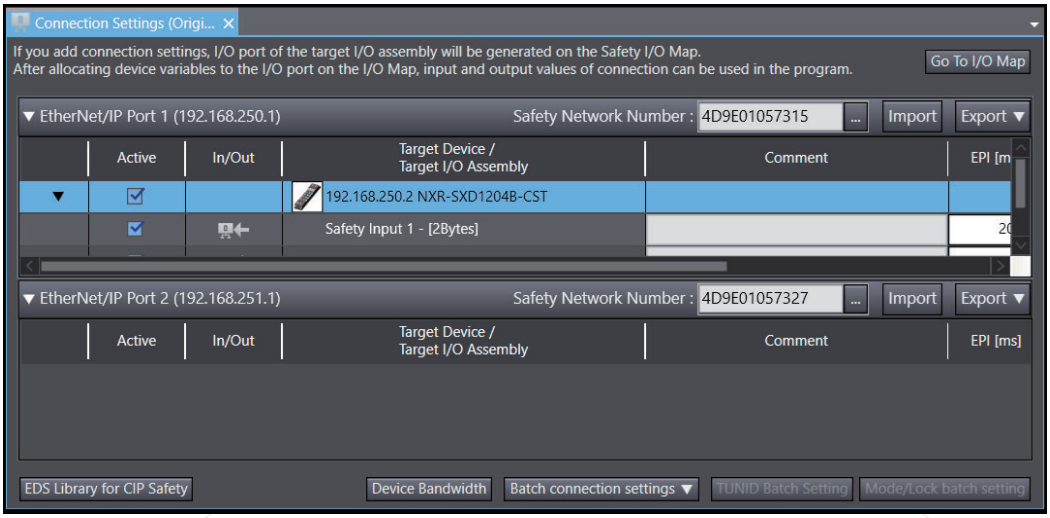
7-7 로직 기능 설정

사용자 정의 애플리케이션 및 애드온 애플리케이션에서는 직접 커스텀 로직을 설계할 수 있습니다. 로직을 구성하려면 Sysmac Studio를 사용하십시오.

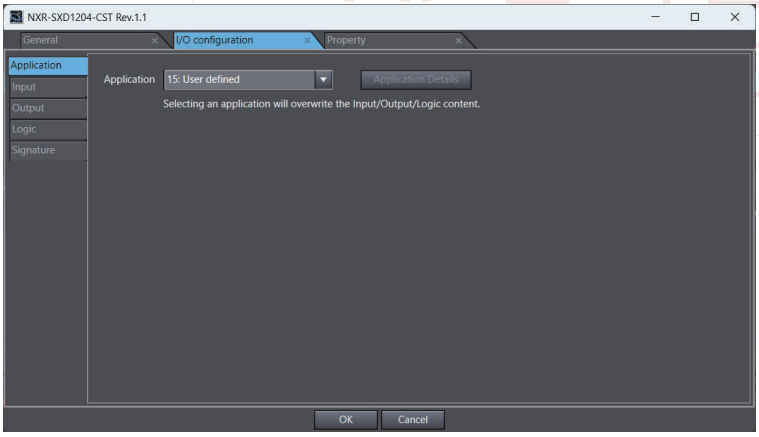
7-7-1 로직 설정 절차

세이프티 I/O 블록에 연결할 각 타겟 디바이스 및 타겟 I/O 어셈블리의 EtherNet/IP 세이프티 접속 설정을 구성한 후 로직 설정을 구성합니다. 여기서는 세이프티 입력 기기 설정이 이미 완료된 것으로 가정하고 설명합니다.
세이프티 입력 기기 설정 절차에 대한 자세한 내용은 7-5-1 세이프티 입력 기능 설정 절차(7-44페이지)를 참조하십시오.
로직 설정 절차는 다음과 같습니다.

1 **Sysmac Studio에서 Configurations and Setup - Communications - Safety - EtherNet/IP Safety Connection Settings of the Safety CPU Unit로 이동하여 Connection Settings (Originator)를 선택합니다.**
Connection Settings (Originator) 탭 페이지가 표시됩니다.



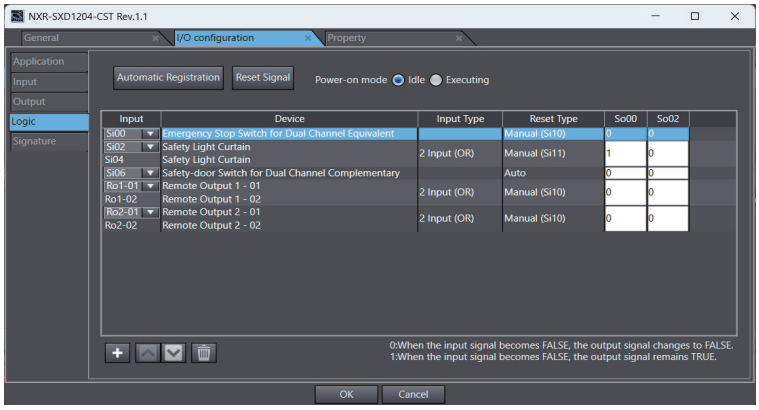
2 I/O configuration 탭의 Application 탭을 선택하고 애플리케이션을 15: User defined로 설정합니다.



3 **I/O configuration 탭의 Logic 탭을 선택합니다.**

AI 번역본 -Only-

다음과 같은 로직 설정 화면이 표시됩니다.



4 **Automatic Registration 버튼을 클릭합니다.**

디바이스 행이 추가됩니다. 또한 각 행에 리셋 타입, 입력 타입, 입력 신호 설정이 자동으로 등록됩니다. 자동 등록 규칙은 다음과 같습니다.

항목	자동 등록 규칙
Device	Input 탭에서 설정된 기기 중 리셋 스위치도 EDM 피드백도 아닌 기기가 추가됩니다.
Reset type	Input 탭에 리셋 스위치가 설정된 경우: 리셋 스위치가 설정된 최소 입력 단자 번호의 수동 리셋 Input 탭에 리셋 스위치가 설정되지 않은 경우: Auto
Input type	모두 미설정
So00~So03	Output 탭의 설정에 따라 로직 설정 화면에 열이 생성됩니다. 값은 모두 0입니다.

또한 Input 탭에서 설정된 리셋 스위치의 입력 단자 번호가 리셋 신호에 자동으로 등록됩니다.

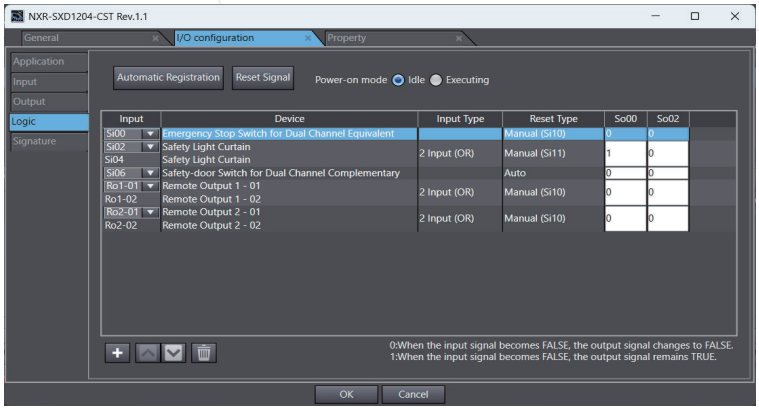
5 다음으로 리셋 신호 설정을 변경하고, 로직 설정을 변경하고, 리모트 출력 설정을 구성합니다.

리셋 신호 설정 변경

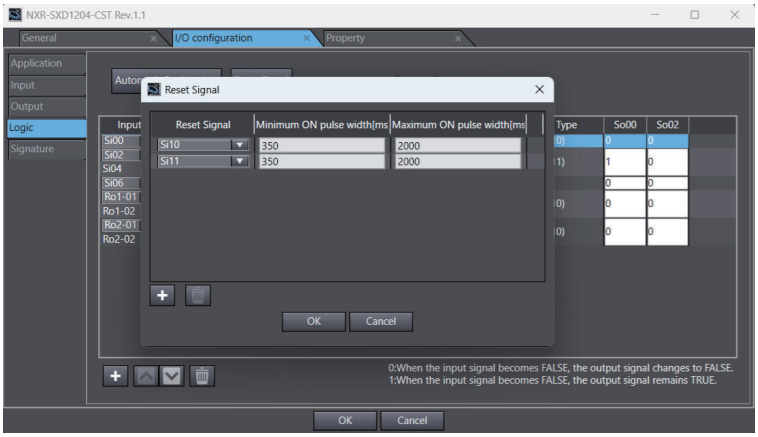
필요에 따라 자동으로 등록된 리셋 신호 설정을 변경합니다.

AI 번역본
For Reference Only-

1 **I/O configuration 탭과 Logic 탭에서 Reset signal 버튼을 클릭합니다.**



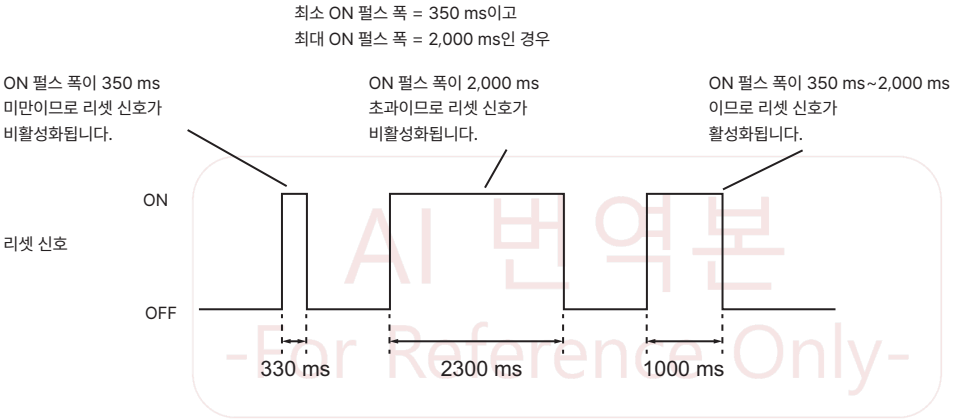
Reset signal 화면이 표시됩니다.



2 세이프티 입력 단자 Si00~Si11 중 하나 또는 리모트 출력 Ro1-01, Ro1-02, Ro2-01, Ro2-02, Ro3-01, Ro3-02 중 하나를 리셋 신호로 설정합니다.

3 리셋 신호의 최소 ON 펄스 폭 및 최대 ON 펄스 폭을 설정합니다.
리셋 신호가 ON인 시간이 최소 ON 펄스 폭 이상이고 최대 ON 펄스 폭 이하이면 로직이 리셋됩니다. 각 설정 항목의 초기값 및 설정 가능 범위는 다음과 같습니다.

설정 항목	초기값 [ms]	설정 가능 범위 [ms]
Minimum ON pulse width	350	100~1,000 50 ms 단위
Maximum ON pulse width	2,000	1,000~30,000 50 ms 단위

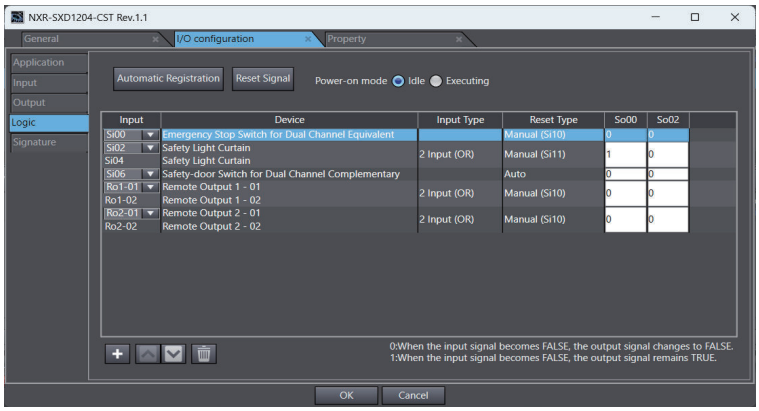


AI 번역본
-For Reference Only-

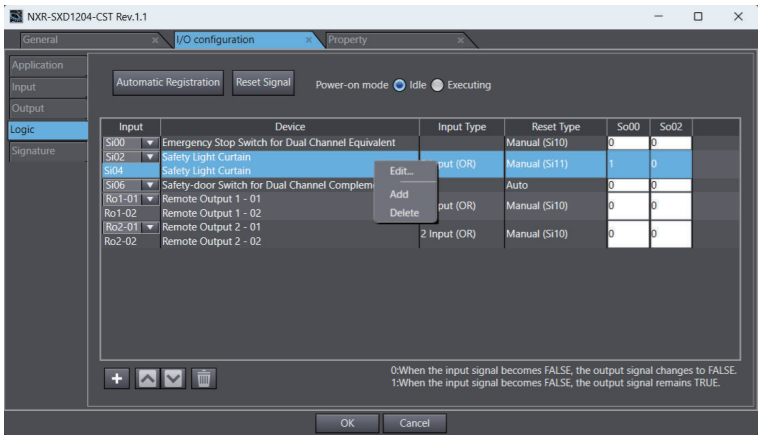
로직 설정 변경

필요에 따라 각 기기의 로직 설정을 변경합니다.

1 I/O configuration 탭과 Logic 탭을 선택하고, 설정을 변경하려는 기기의 행으로 커서를 이동한 후 마우스 오른쪽 버튼을 클릭합니다.

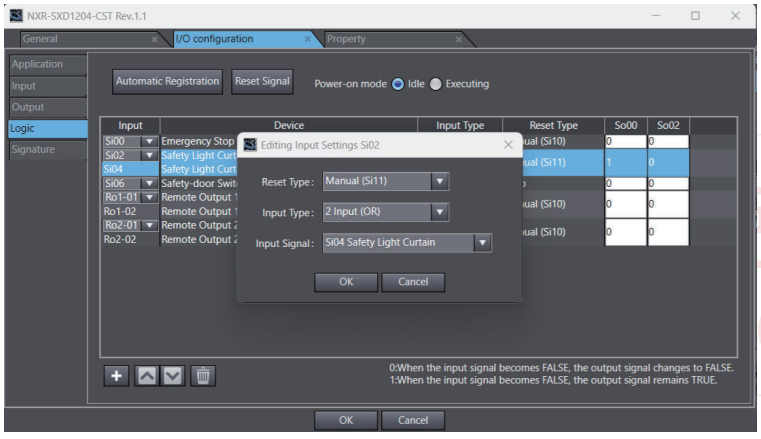


다음과 같은 서브메뉴가 표시됩니다.



2 Edit를 선택합니다.

다음과 같은 편집 화면이 표시됩니다.



3 **Reset type, Input type, Input signal을 설정합니다.**

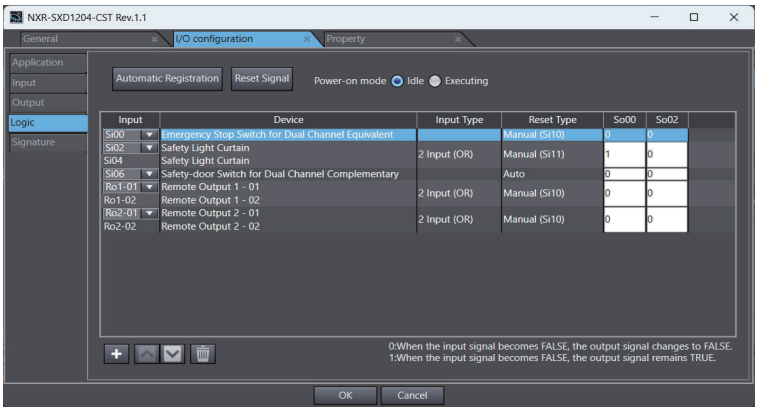
4 세이프티 출력 단자 So00~So03의 필드에 0 또는 1을 직접 입력합니다.

5 행을 추가하려면 서브메뉴에서 Add를 선택합니다. 행을 삭제하려면 Remove를 선택합니다.

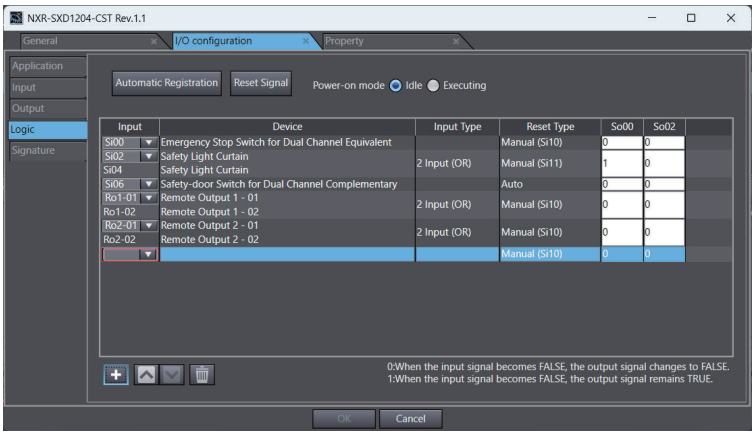
리모트 출력 설정

필요에 따라 리모트 출력을 추가하고 구성합니다.

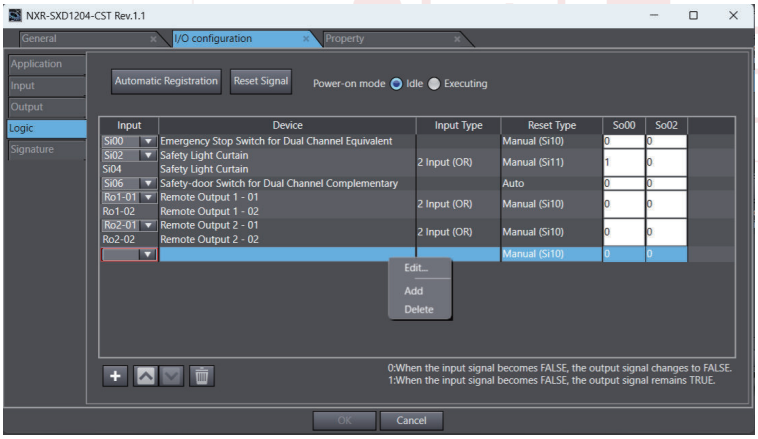
1 I/O configuration 탭과 Logic 탭에서 + 버튼을 클릭합니다.



새 행이 추가됩니다.

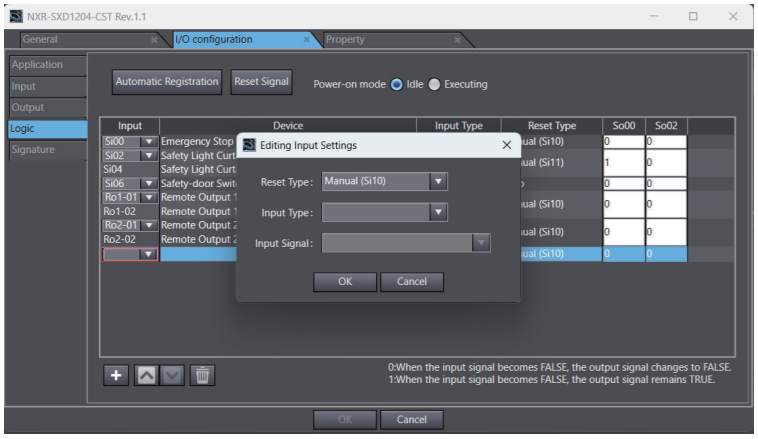


2 추가된 행으로 커서를 이동한 후 마우스 오른쪽 버튼을 클릭합니다.
다음과 같은 서브메뉴가 표시됩니다.



3 Edit를 선택합니다.

다음과 같은 편집 화면이 표시됩니다.

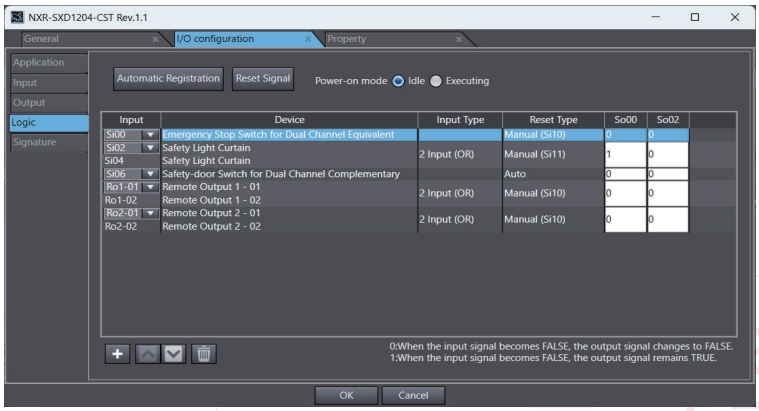


4 **Reset Type, Input Type, Input Signal을 설정합니다. Input Signal에는 Ro1-01, Ro1-02, Ro2-01, Ro2-02, Ro3-01, Ro3-02 중 하나를 설정합니다.**

Power-on Mode 설정

전원을 ON했을 때 진입할 동작 모드를 설정합니다. 전원을 ON했을 때의 동작 모드가 Executing이면 전원을 ON한 직후 세이프티 애플리케이션이 실행됩니다.

1 **I/O configuration 탭과 Logic 탭에서 Power-on mode를 Idle 또는 Executing으로 설정합니다.**



-For Reference Only-

2 OK 버튼을 클릭합니다.

사용상의 주의

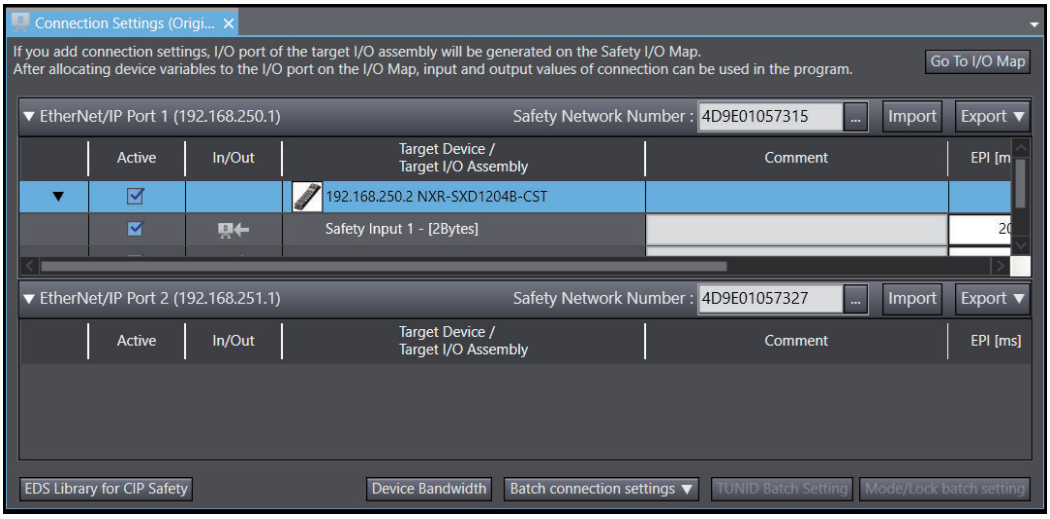
전원을 ON했을 때의 동작 모드가 Idle이면 전원을 ON해도 세이프티 애플리케이션이 실행되지 않으므로 세이프티 출력이 OFF됩니다. 세이프티 애플리케이션을 실행하려면 세이프티 I/O 블록의 동작 모드를 변경하십시오. Executing으로 설정하십시오.

7-7-2 파라미터 목록 표시

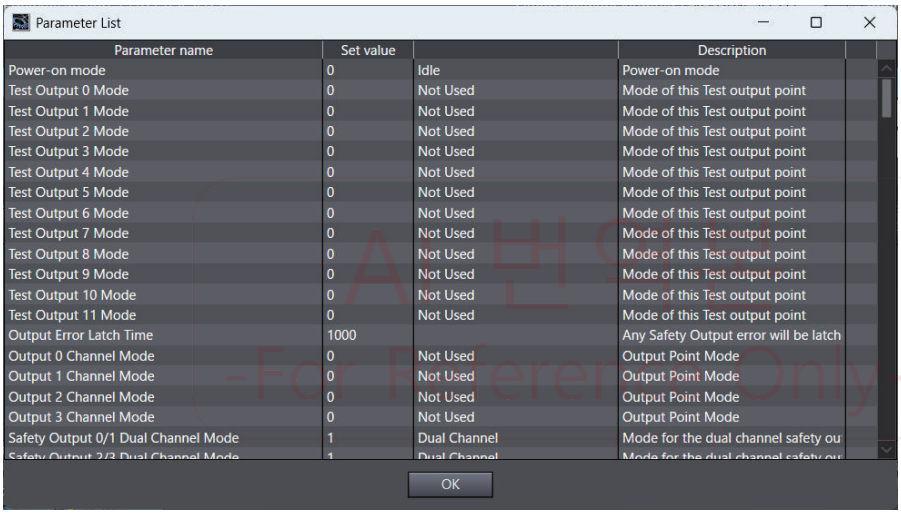
설정된 파라미터의 목록이 표시됩니다. 각 파라미터가 의도한 대로 설정되었는지 확인하십시오. 표시되는 항목은 다음과 같습니다.

항목	설명
Parameter name	설정 파라미터명
Setting value	설정값
Setting value (enum value)	설정값의 의미
Description	파라미터명의 의미

1 **Sysmac Studio에서 Configurations and Setup - Communications - Safety - EtherNet/IP Safety Connection Settings of the Safety CPU Unit로 이동하여 Connection Settings (Originator)를 선택합니다.**
Connection Settings (Originator) 탭 페이지가 표시됩니다.



2 Safety I/O Block을 더블 클릭하거나 마우스 오른쪽 버튼으로 클릭하고 Parameter List를 선택합니다.
파라미터 목록이 표시됩니다.

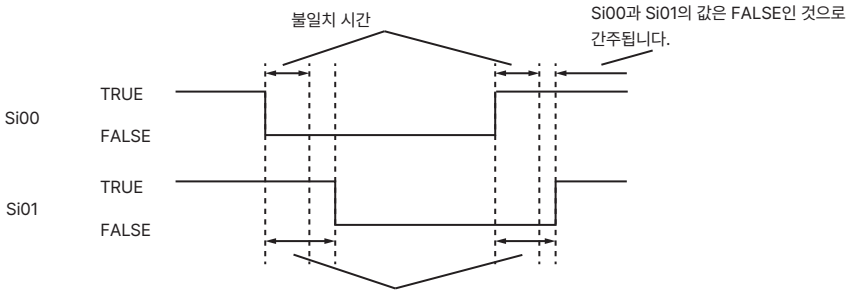


7-7-3 고려해야 할 입력 기기의 이상 동작 예시

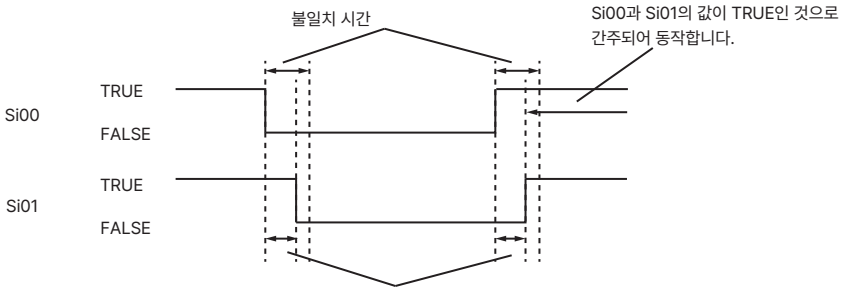
로직 기능을 구성할 때는 설비가 항상 안전하게 동작하도록 입력 기기가 예기치 않게 이상 동작할 가능성을 고려해야 합니다. 이 절에서는 입력 기기의 이상 동작 예시를 설명합니다.

세이프티 입력 불일치 에러

듀얼 채널 입력 기기의 두 입력 중 한쪽 값이 변화한 시점부터 다른 쪽 값이 변화한 시점까지의 시간이 사전 설정된 불일치 시간을 초과하면 입력값의 변화를 정상적으로 검출할 수 없으므로 세이프티 입력 불일치 에러(65230000 hex) 이벤트가 발생합니다. 세이프티 입력 불일치 에러 (65230000 hex) 이벤트가 발생하면 세이프티 입력 데이터 값이 FALSE인 것으로 간주하여 동작합니다.
불일치 시간에 대한 자세한 내용은 6-4-4 듀얼 채널 평가(6-11페이지)를 참조하십시오.
이벤트에 대한 자세한 내용은 11-2-4 이벤트 상세 및 문제 해결(11-12페이지)를 참조하십시오.



Si00이 변화한 시점부터 Si01이 변화한 시점까지의 시간이 불일치 시간을 초과하므로, Si00과 Si01의 값이 TRUE가 된 후에도 Si00과 Si01의 값은 FALSE인 것으로 간주되어 동작합니다.

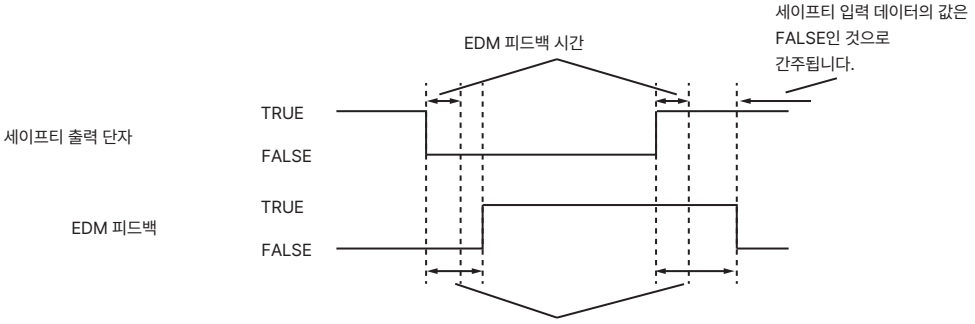


Si00이 변화한 시점부터 Si01이 변화한 시점까지의 시간이 불일치 시간 이내이므로, Si00과 Si01의 값에 따라 동작합니다.

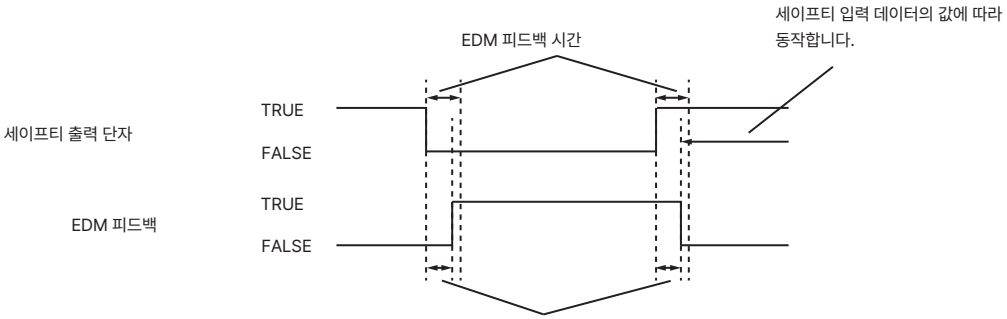
EDM 에러

EDM 피드백이 설정된 상태에서 세이프티 출력 단자의 값이 변화한 시점부터 EDM 피드백의 값이 변화한 시점까지의 시간이 EDM 피드백 시간을 초과하면 EDM 에러(652B0000 hex) 이벤트가 발생합니다. EDM 에러(652B0000 hex) 이벤트가 발생하면 세이프티 입력 데이터의 값이 FALSE인 것으로 간주하여 동작합니다.
EDM 피드백에 대한 자세한 내용은 6-5 세이프티 출력 기능(6-16페이지)를 참조하십시오. 또한, 이벤트에 대한 자세한 내용은 11-2-4 이벤트 상세 및 문제 해결(11-12페이지)를 참조하십시오.

AI 번역본
For Reference Only-



세이프티 출력 단자의 값이 변화한 시점부터 EDM 피드백의
값이 변화한 시점까지의 시간이 EDM 피드백 시간을 초과하므로,
세이프티 입력 데이터의 값이 FALSE인 것으로 간주되어 동작합니다.



세이프티 출력 단자의 값이 변화한 시점부터 EDM 피드백의
값이 변화한 시점까지의 시간이 EDM 피드백 시간 이내이므로,
세이프티 입력 데이터의 값에 따라 동작합니다.

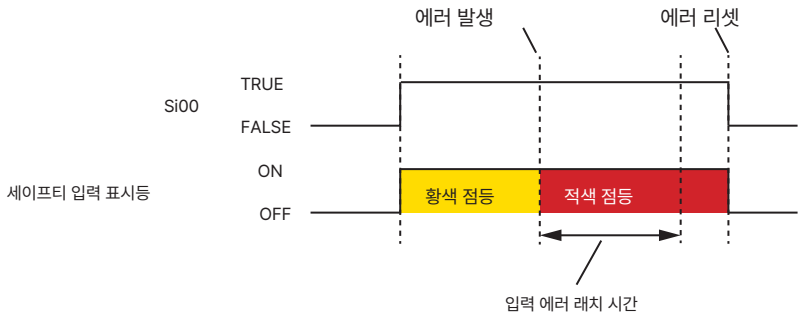
세이프티 입력 외부 테스트 신호 이상

테스트 펄스 평가 사용 시 입력 신호선이 전원선(플러스 측)과 접촉하거나, 입력 신호선이
단락되거나, 연결된 외부 기기에 고장이 발생하는 등의 문제가 발생하면 세이프티 입력 외부 테스트
신호 이상(65220000 hex) 이벤트가 발생합니다. 세이프티 입력 외부 테스트 신호
이상(65220000 hex) 이벤트가 발생하면 세이프티 입력 데이터의 값이 FALSE인 것으로 간주하여 동작합니다.
테스트 펄스 평가에 대한 자세한 내용은 6-4-3 테스트 펄스 평가 기능(6-10페이지)를 참조하십시오.
이벤트에 대한 자세한 내용은 11-2-4 이벤트 상세 및 문제 해결(11-12페이지)를 참조하십시오.

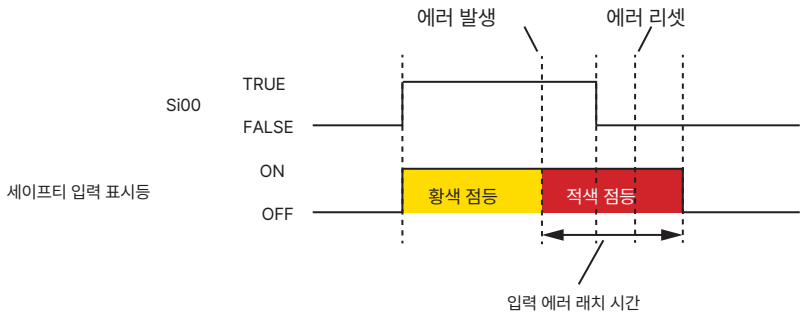
AI 번역본
For Reference Only

연속 시간이 입력 에러 래치 시간보다 짧은 경우의 에러

입력 에러 래치 시간이 설정된 경우, 에러 발생부터 에러 리셋까지의 시간이 입력 에러
래치 시간보다 짧더라도 입력 에러 래치 시간 동안 에러 처리가 계속됩니다.
예를 들어, 에러가 리셋되었더라도 세이프티 입력 표시등은 입력 에러 래치 시간이 종료될 때까지
적색으로 점등된 상태를 유지합니다.
입력 에러 래치 시간에 대한 자세한 내용은 6-4-7 입력 에러 래치 시간(6-15페이지)를 참조하십시오.



에러 발생부터 에러 리셋까지의 시간이 입력 에러 래치 시간을 초과하므로
에러 리셋 직후 세이프티 입력 표시등이 꺼집니다.



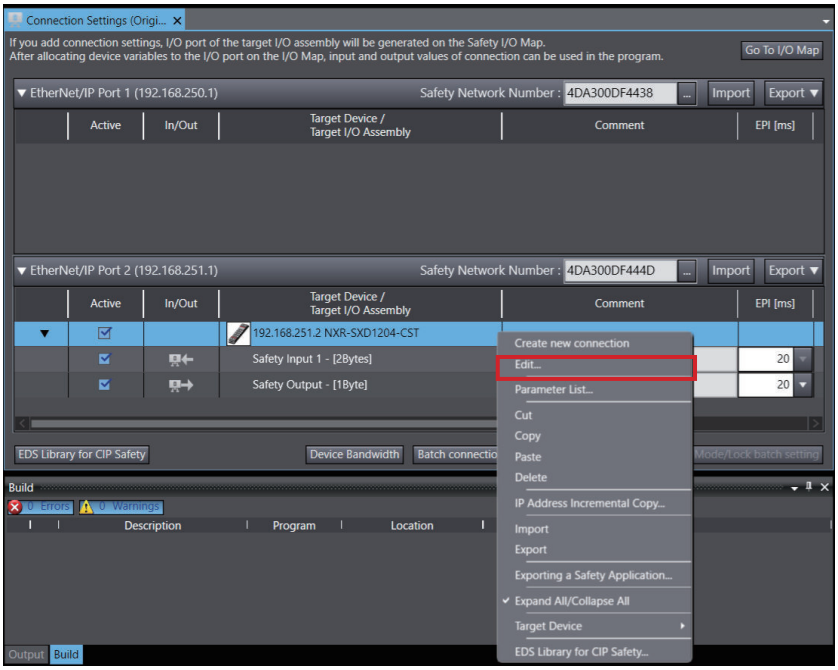
에러가 리셋되더라도 입력 에러 래치 시간이 종료될 때까지
세이프티 입력 표시등은 적색으로 점등된 상태를 유지합니다.

AI 번역본
-For Reference Only-

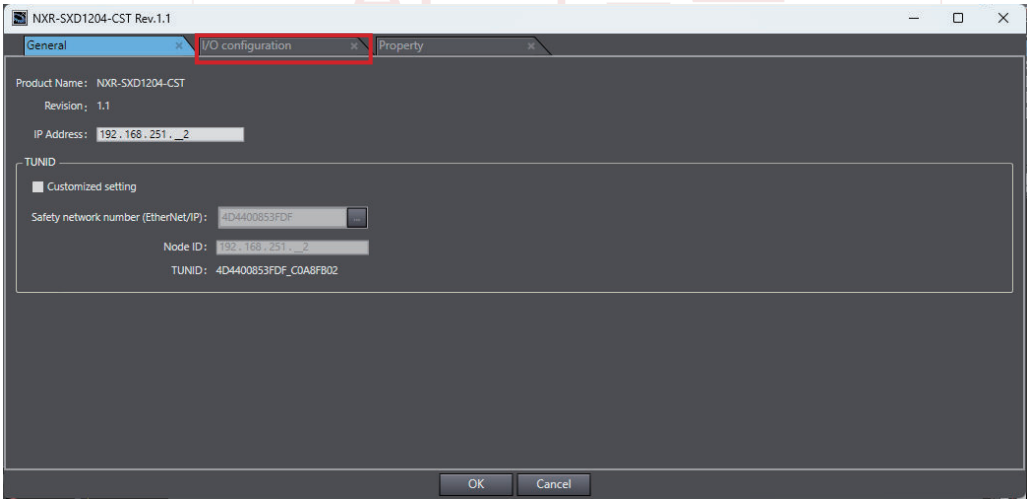
7-8 세이프티 시그니처 설정

세이프티 I/O 블록의 세이프티 시그니처 설정을 구성합니다.
Sysmac Studio에서 이 설정은 Connection Settings (Originator) Edit Pane에 있으므로, 그 화면부터 설명을 시작합니다.
CIP Safety 접속 설정에 대한 자세한 내용은 7-3-1 CIP Safety 통신 접속 설정(7-27페이지)를 참조하십시오.
다음은 Connection Settings (Originator) Edit Pane에 등록된 기기에 사용할 세이프티 애플리케이션 설정을 구성하는 절차를 설명합니다.

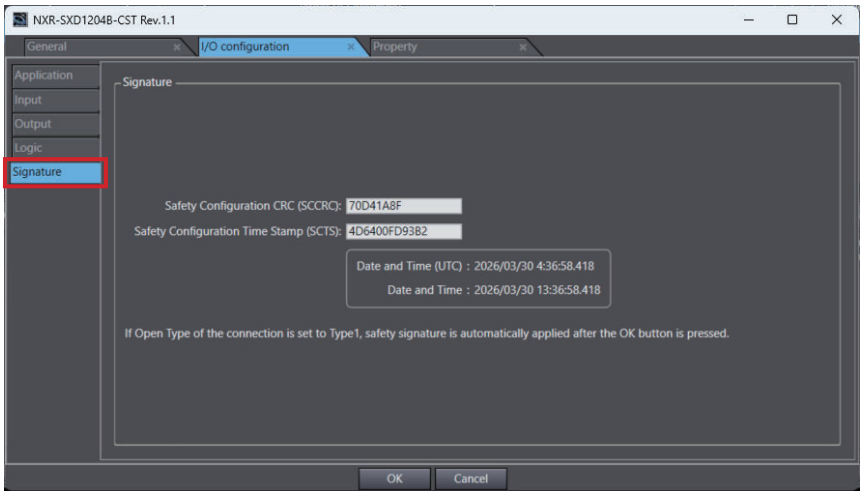
1 Connection Settings (Originator) Edit Pane에서 Safety I/O Block을 선택하고 더블 클릭하거나, 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 Edit를 선택합니다.



2 **I/O configuration 탭을 선택합니다.**



3 Signatures 탭을 선택합니다.



4 Safety Configuration CRC(SCCRC) 및 Safety Configuration Time Stamp(SCTS)를 설정하고 OK 버튼을 클릭합니다.

AI 번역본
-For Reference Only-

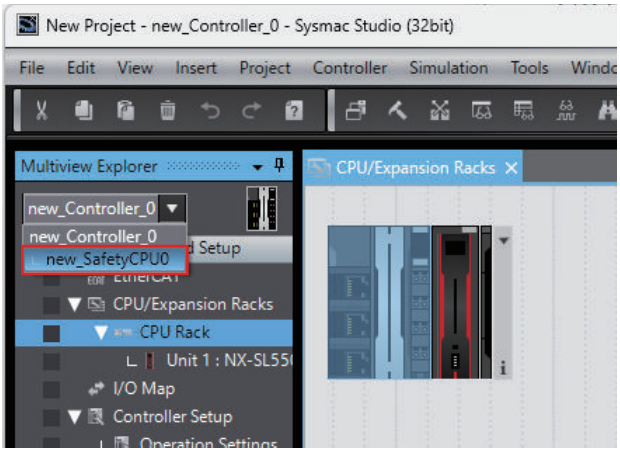
7-9 세이프티 애플리케이션 파일 생성

이 절에서는 세이프티 애플리케이션 파일을 생성하고 익스포트하는 절차를 설명합니다.
세이프티 제어 시스템이 세이프티 컨트롤러가 제어를 수행하는 구성(Web UI를 이용한 구성)인 경우, 리모트 I/O 모드용 세이프티 애플리케이션 파일을 생성하여 익스포트하십시오. 이 세이프티 애플리케이션 파일은 I/O 설정만 정의합니다.
세이프티 제어 시스템이 사용자가 설계한 세이프티 애플리케이션을 이용하여 세이프티 I/O 블록이 제어를 수행하는 구성(분산 관리형)인 경우, 애드온 애플리케이션용 세이프티 애플리케이션 파일을 생성하여 익스포트하십시오.
이 세이프티 애플리케이션 파일은 로직 설정 및 I/O 설정을 정의합니다.

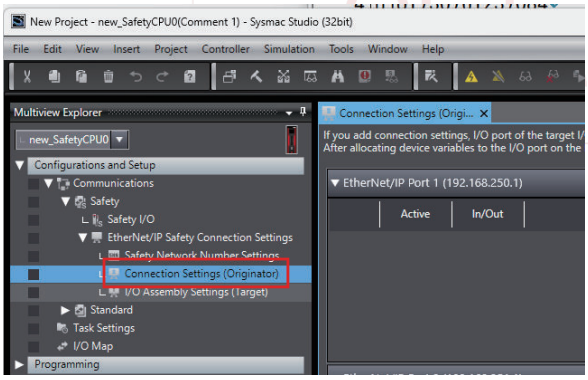
7-9-1 세이프티 I/O 블록 등록

세이프티 애플리케이션 파일을 익스포트하려면 세이프티 I/O 블록을 등록하십시오.

1 Multiview Explorer에서 Controller Selection Box의 대상 Safety CPU Unit을 선택합니다.



2 **Multiview Explorer에서 Configurations and Setup - Communications - Safety - EtherNet/IP Safety Connection Settings로 이동하여 Connection Settings (Originator)를 더블 클릭하거나, 마우스** 오른쪽 버튼으로 클릭하고 Edit를 선택합니다.
Connection Settings (Originator) Edit Pane이 Edit Pane에 표시됩니다.

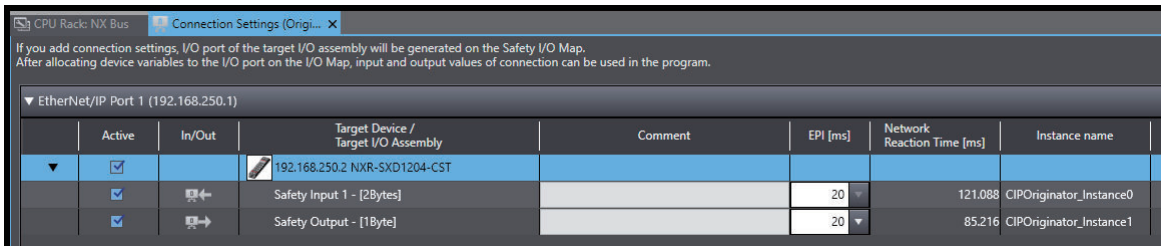


3 **Toolbox에서 Safety I/O and Logic Device를 선택하고, NXR-SXD1204-CST 또는 NXR-SXD1204B-CST를 선택합니다.**

AI 번역본
-Reference Only-



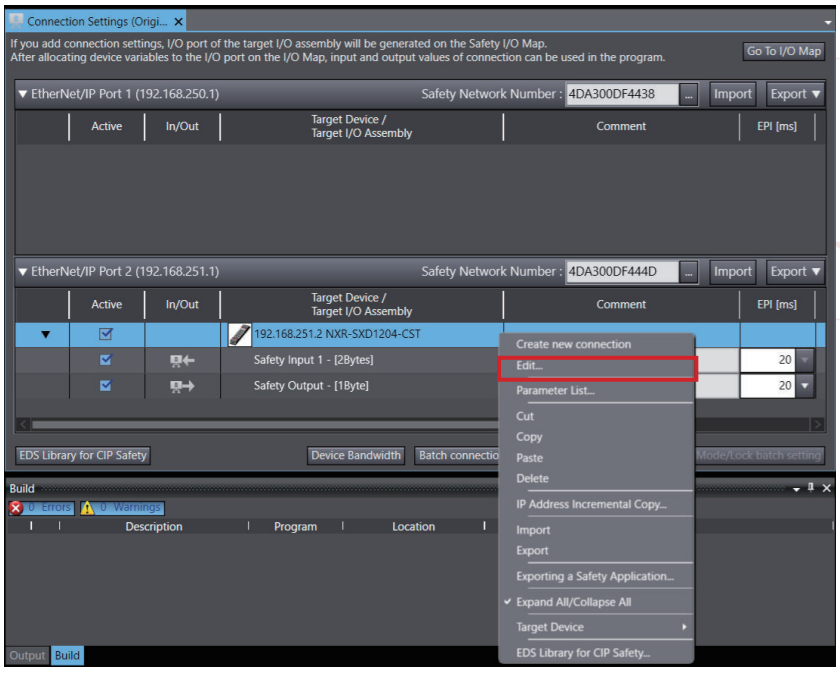
4 Toolbox에서 선택한 Safety I/O Block을 드래그합니다.



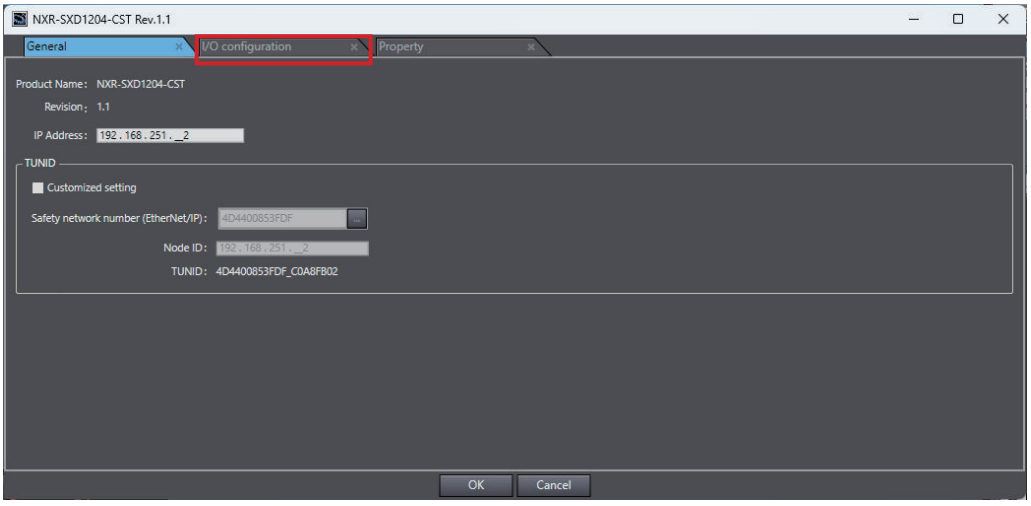
7-9-2 세이프티 애플리케이션 설정

세이프티 I/O 블록에서 사용할 세이프티 애플리케이션의 설정을 구성합니다.

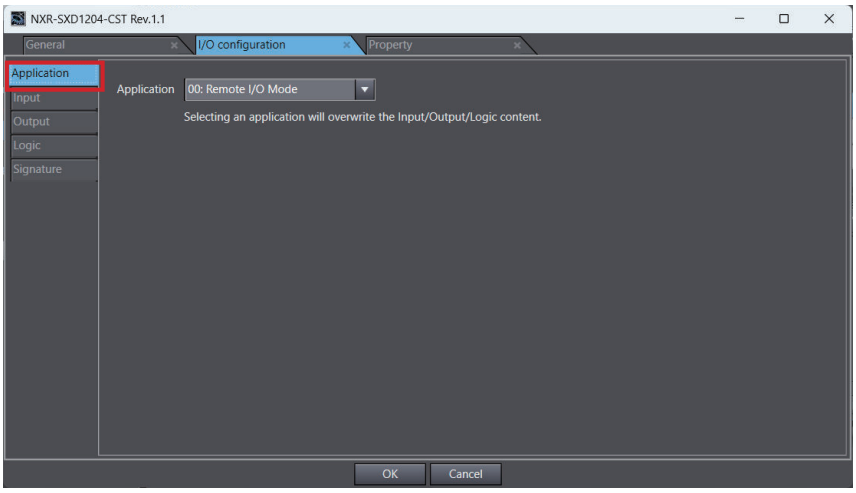
1 Connection Settings (Originator) Edit Pane에서 Safety I/O Block을 선택하고 더블 클릭하거나, 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 Edit를 선택합니다.



2 **I/O configuration 탭을 선택합니다.**



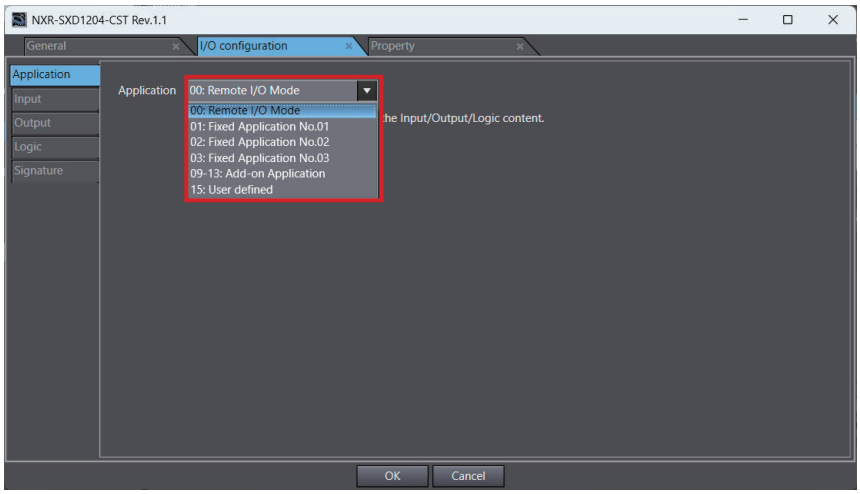
3 Application 탭을 선택합니다.



4 사용할 세이프티 애플리케이션을 선택합니다.
세이프티 제어 시스템과 세이프티 애플리케이션의 대응 관계는 다음과 같습니다.

세이프티 제어 시스템	세이프티 애플리케이션
세이프티 컨트롤러가 제어를 수행하는 구성(Type 1 Safety Open을 이용한 구성)(1-8페이지) 세이프티 컨트롤러가 제어를 수행하는 구성(Web UI를 이용한 구성)(1-9페이지)	00: Remote I/O Mode
사전 설정된 세이프티 애플리케이션을 이용하여 세이프티 I/O 블록이 제어를 수행하는 구성(1-10페이지)	01: Fixed Application No.01 02: Fixed Application No.02 03: Fixed Application No.03
사용자가 설계한 세이프티 애플리케이션을 이용하여 세이프티 I/O 블록이 제어를 수행하는 구성(집중 관리형)(1-11페이지)	15: User defined
사용자가 설계한 세이프티 애플리케이션을 이용하여 세이프티 I/O 블록이 제어를 수행하는 구성(분산 관리형)(1-12페이지)	09-13: Add-on Application

-For Reference Only-



5 설정이 완료되면 OK 버튼을 클릭합니다.

7-9-3 세이프티 I/O 기능 설정

Sysmac Studio의 프로젝트 파일에서 세이프티 I/O 블록의 I/O 설정을 구성합니다. 자세한 내용은 7-5 세이프티 입력 기능 설정(7-44페이지) 및 7-6 세이프티 출력 기능 설정(7-50페이지)를 참조하십시오.

7-9-4 로직 기능 설정

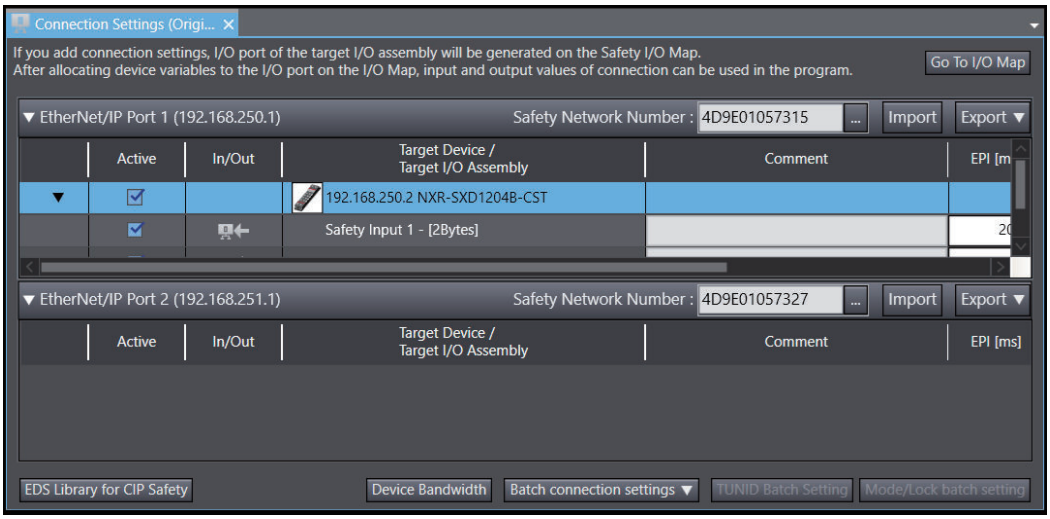
Sysmac Studio의 프로젝트 파일에서 세이프티 I/O 블록의 로직 및 Power-on mode 설정을 구성합니다. 이 단계는 세이프티 제어 시스템이 사용자가 설계한 세이프티 애플리케이션을 이용하여 세이프티 I/O 블록이 제어를 수행하는 구성(분산 관리형)인 경우에만 필요합니다. 자세한 내용은 7-7 로직 기능 설정(7-53페이지)을 참조하십시오.

7-9-5 세이프티 애플리케이션 파일 익스포트

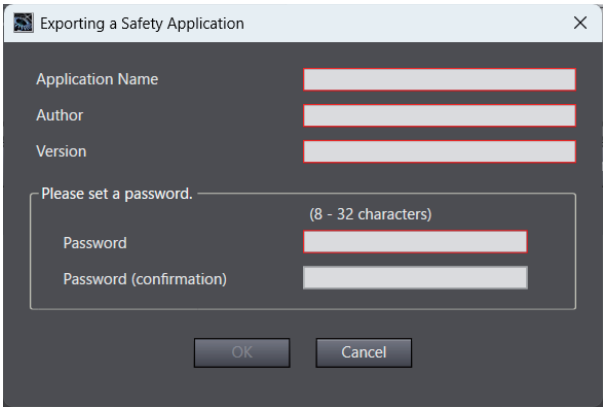
세이프티 애플리케이션 파일을 익스포트하는 절차는 다음과 같습니다.

1 **Sysmac Studio에서 Configurations and Setup - Communications - Safety - EtherNet/IP Safety Connection Settings of the Safety CPU Unit로 이동하여 Connection Settings (Originator)를 선택합니다.**
Connection Settings (Originator) 탭 페이지가 표시됩니다.

AI 번역본
-For Reference Only-



2 Safety I/O Block을 마우스 오른쪽 버튼으로 클릭하고 Exporting a Safety Application을 선택합니다.
세이프티 I/O 블록의 Exporting a Safety Application 화면이 표시됩니다.



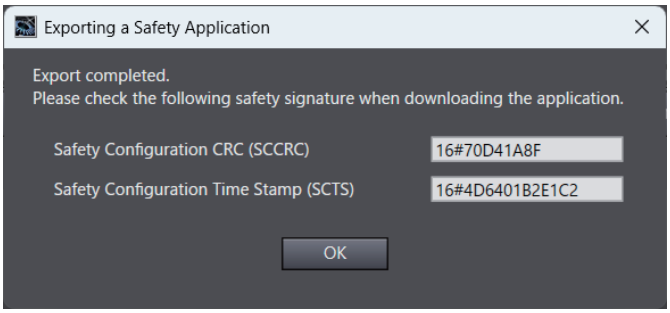
3 애플리케이션명, 작성자, 버전, 세이프티 애플리케이션 파일 비밀번호, 세이프티 애플리케이션 파일 비밀번호(확인용)를 입력하고 OK 버튼을 클릭합니다.
각 설정 항목의 문자 수 제한은 다음과 같습니다.

설정 항목	문자 수 제한
Application name	반각 영숫자 32자 이내
Creator	반각 영숫자 32자 이내
Version	반각 영숫자 32자 이내
Safety application file password	반각 영숫자 8~32자
Safety application file password (for confirmation)	

세이프티 애플리케이션 파일 비밀번호는 세이프티 애플리케이션을 사용하기 위해 세이프티 애플리케이션 파일마다 설정하는 비밀번호입니다. 세이프티 패스워드와는 다릅니다.

4 익스포트할 파일의 저장 위치를 지정하고 파일을 저장합니다.
익스포트 완료 화면이 표시됩니다.

-For Reference Only-



5 세이프티 시그니처를 확인하고 OK 버튼을 클릭합니다.
익스포트가 실행되며 세이프티 애플리케이션 파일이 저장됩니다.

사용상의 주의

입력한 애플리케이션명, 작성자, 버전, 세이프티 애플리케이션 파일 비밀번호, 세이프티 시그니처(SCCRC 및 SCTS)를 기록해 두십시오. 이 정보는 세이프티 애플리케이션 파일에서 세이프티 애플리케이션을 설정할 때 사용됩니다.

세이프티 애플리케이션 파일 비밀번호 사양

세이프티 애플리케이션 파일 비밀번호에 사용할 수 있는 문자열의 조건은 다음과 같습니다.

항목	설명
문자 수	8~32
사용 가능 문자	A~Z, a~z, 0~9, ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ 반각 스페이스

사용상의 주의

- 보안 위험을 줄이기 위해 설정하는 세이프티 애플리케이션 파일 비밀번호에는 알파벳, 기호, 숫자를 조합하여 사용하십시오.
- 세이프티 애플리케이션 파일 비밀번호는 표시할 수도 초기화할 수도 없습니다. 비밀번호를 잊어버릴 경우에 대비하여 세이프티 애플리케이션 파일 비밀번호를 관리하십시오.

AI 번역본
-For Reference Only-

속성 정보 사양

다음 표는 사용자가 생성한 애드온 애플리케이션의 속성 정보를 나타냅니다.

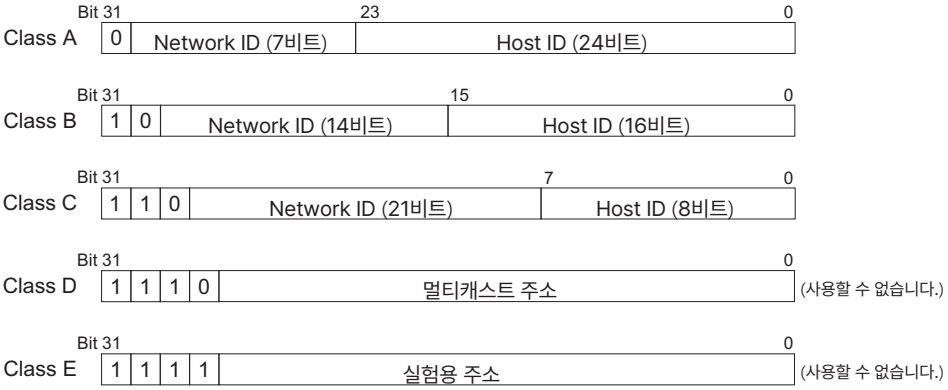
항목	사용 가능 문자	문자 수
Application name	반각 영숫자	1~32
Creator	반각 영숫자	1~32
Version	반각 영숫자	1~32

7-10 IP 주소 설정

이 절에서는 IP 주소 구성 및 IP 주소 설정 방법에 대해 설명합니다.

7-10-1 IP 주소 구성

IP 주소는 네트워크 번호(net ID)와 호스트 번호(host ID)를 지정하는 32비트의 바이너리 데이터로 구성됩니다.
net ID는 이더넷 네트워크를 식별하는 데 사용되는 주소입니다. host ID는 호스트(노드)를 식별하는 데 사용되는 주소입니다.
IP 주소는 네트워크 규모에 따라 주소 체계를 선택할 수 있도록 클래스 A, B, C의 3가지로 구분됩니다. 클래스 D 및 E는 사용되지 않습니다.



각 클래스의 네트워크 수 및 네트워크에서 가능한 호스트 수는 클래스에 따라 다릅니다.

클래스	네트워크 수	호스트 수
Class A	소규모	224-2 최대 (최대 16,777,214)
Class B	중규모	216-2 최대 (최대 65,534)
Class C	대규모	28-2 최대 (최대 254)

IP 주소의 32비트 바이너리 데이터는 각각 8비트씩 4개 구간으로 나뉩니다. IP 주소는 32비트 주소의 4개 옥텟 각각을 10진수로 변환하여 마침표로 구분하여 나타냅니다. 예를 들어, 바이너리 주소 10000010 00111010 00010001 00100000은 130.58.17.32로 나타냅니다.

샘플 번역본
-For Reference Only-

IP 주소 할당

IP 주소는 네트워크 내에서 또는 여러 네트워크에 걸쳐 중복되지 않도록 노드에 할당해야 합니다.

CIDR 기능

CIDR은 Classless Inter-Domain Routing의 약자로, 클래스를 사용하지 않고 IP 주소를 할당하는 기능입니다.

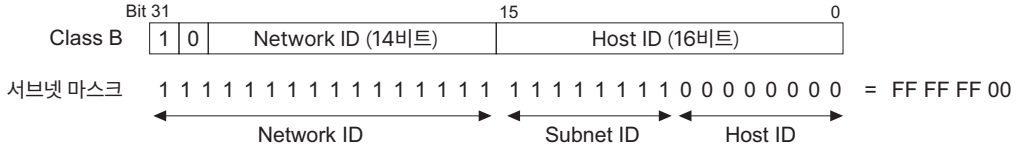
클래스 기반 IP 주소는 network ID 부분과 host ID 부분이 미리 정해진 블록 단위로 구분되므로 IP 주소 공간(호스트 수)을 효율적으로 할당하지 못한다는 단점이 있습니다. CIDR은 클래스를 사용하지 않으므로 network ID 부분과 host ID 부분을 임의의 IP 주소 공간으로 구분할 수 있어 IP 주소 공간(호스트 수)을 효율적으로 사용할 수 있습니다. 예를 들어 Class C(192.168....)를 사용하더라도 CIDR로 넷마스크를 설정하면 254개 노드를 초과하는 수평 분산 네트워크를 구축할 수 있습니다.

서브넷 마스크 범위
192.0.0.0~255.255.255.252

서브넷 마스크

하나의 네트워크에 많은 노드가 연결되면 네트워크 운용 및 관리가 어려워집니다. 이러한 경우 하나의 네트워크를 여러 서브네트워크로 분할하여 시스템을 구축하는 것이 편리합니다.
이 시스템은 내부적으로는 여러 네트워크로 동작하지만 외부에서는 하나의 네트워크로 보입니다.
이러한 동작을 구현하려면 IP 주소의 host ID 부분을 서브넷 ID 부분과 host ID 부분의 두 부분으로 나눕니다. 이 서브넷 ID 부분을 식별하기 위한 정보가 서브넷 마스크입니다.
서브넷 마스크는 network ID 부분과 서브넷 ID 부분을 "1"로, host ID 부분을 "0"으로 설정한 비트 마스크입니다.

(예) 서브넷 ID에 8비트를 사용하는 Class B IP 주소의 경우, 서브넷 마스크는 다음과 같습니다:



서브네트워크의 모든 노드에 동일한 서브넷 마스크를 설정하십시오. 내장 EtherNet/IP 포트는 CIDR (Classless Inter-Domain Routing)을 지원합니다. 이를 통해 서브넷 마스크를 192.0.0.0~255.255.255.252로 설정할 수 있습니다.

추가 정보

서브네트워크를 사용하지 않는 경우, IP 주소의 host ID 부분 전체를 "0"으로 마스크하십시오.
IP 주소의 클래스(Class A~Class C)에 따라 아래의 해당 서브넷 마스크 값을 설정하십시오.

클래스	서브넷 마스크 값
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

네트워크 주소

서브넷 마스크를 이용하여 각 네트워크를 식별하기 위한 정보에는 네트워크 주소가 있습니다.
네트워크 주소는 특정 여러 노드가 동일한 네트워크에 속하는지를 나타냅니다.
네트워크 주소는 노드의 IP 주소와 서브넷 마스크의 논리 AND 연산으로 계산됩니다.

다음은 네트워크 주소 계산 예를 나타냅니다.

노드 1의 IP 주소가 "192.168.250.20"으로, 노드 2의 IP 주소가 "192.168.245.30"으로, 서브넷 마스크가 "255.255.240.0"으로 설정된 경우, 각 노드의 네트워크 주소는 다음 표와 같이 계산됩니다.

・노드 1의 네트워크 주소 계산은 다음과 같습니다.

항목	10진 표기	2진 표기
IP address	192.168.250.20	11000000.10101000.11111010.00010100
Subnet mask	255.255.240.0	11111111.11111111.11110000.00000000
Network address	192.168.240.0	11000000.10101000.11110000.00000000

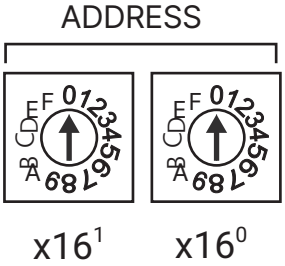
・노드 2의 네트워크 주소 계산은 다음과 같습니다.

항목	10진 표기	2진 표기
IP address	192.168.245.30	11000000.10101000.11110101.00011110
Subnet mask	255.255.240.0	11111111.11111111.11110000.00000000
Network address	192.168.240.0	11000000.10101000.11110000.00000000

위 결과로부터 노드 1과 노드 2는 네트워크 주소가 동일하므로 동일한 네트워크에 속함을 알 수 있습니다.

7-10-2 로터리 스위치를 이용한 IP 주소 설정 방법 선택

세이프티 I/O 블록의 로터리 스위치를 이용하여 IP 주소를 설정하는 방법을 선택한 후 IP 주소 자체를 설정할 수 있습니다.
ADDRESS 로터리 스위치를 사용하십시오.



다음과 같이 로터리 스위치의 설정값을 구성하여 소프트웨어 설정 또는 하드웨어 설정 중 하나를 선택하십시오. 선택한 방법을 사용하여 IP 주소를 설정합니다.

설정명	설정값 (hex)	IP 주소 설정 방법
소프트웨어 설정	00	Sysmac Studio 또는 Web UI에서 다음 방법 중 하나를 선택하여 설정을 구성합니다. ・고정 IP 주소 설정 ・DHCP 서버로부터 취득 출하 시 초기값은 192.168.250.1입니다. Sysmac Studio를 이용하여 설정을 구성하는 방법에 대한 자세한 내용은 7-10-3 Sysmac Studio를 이용한 설정(7-74페이지)를 참조하십시오. Web UI를 이용하여 설정을 구성하는 방법에 대한 자세한 내용은 7-10-4 Web UI를 이용한 설정(7-76페이지)를 참조하십시오.
하드웨어 설정*2	01~FE	192.168.250.□*1
	FF	DHCP 서버로부터 IP 주소를 취득합니다.

***1.** "□"는 로터리 스위치의 설정값입니다.

*2. 로터리 스위치를 설정한 후 재시작을 수행하면 설정이 적용됩니다.

사용상의 주의

DHCP 서버로부터 IP 주소를 취득하는 경우, 취득에 성공하더라도 전원을 OFF하거나 유닛을 재시작하면 취득한 IP 주소가 삭제됩니다. 따라서 이후 운용을 위해서는 DHCP 서버가 필요합니다.

추가 정보

권장 DHCP 서버는 DHCP Server 3.06 이상입니다.

7-10-3 Sysmac Studio를 이용한 설정

Sysmac Studio의 TCP/IP Settings 화면을 사용하여 해당 유닛의 IP 주소 설정 및 LINK 설정을 구성합니다.

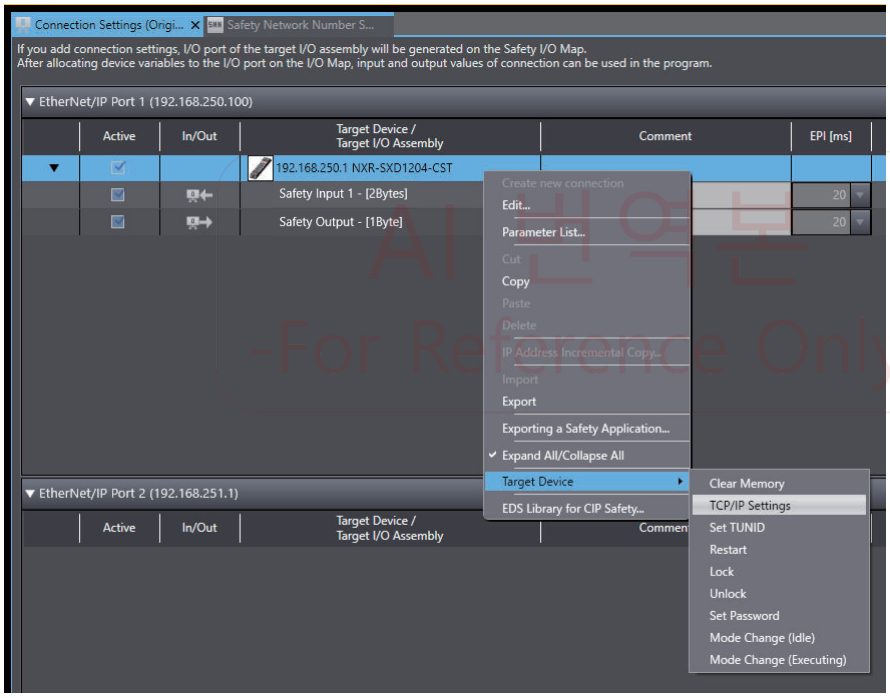
사용상의 주의

세이프티 I/O 블록은 이 TCP/IP 설정에서 다음 기능을 지원하지 않습니다.

- **IP Adress에서 Obtain from BOOTP Server 선택**
- DNS

1 ADDRESS 로터리 스위치의 설정값을 "00"으로 설정한 후 유닛을 시작합니다.
최초 시작 시 값은 192.168.250.1입니다.

2 접속 설정(오리지네이터)의 설정 화면에서 Safety I/O Block을 마우스 오른쪽 버튼으로 클릭하고, 표시된 메뉴에서 Target Device - TCP/IP Settings를 클릭합니다.

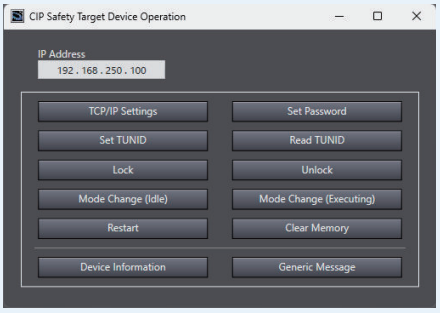


AI 번역 본
-For Reference Only-

추가 정보

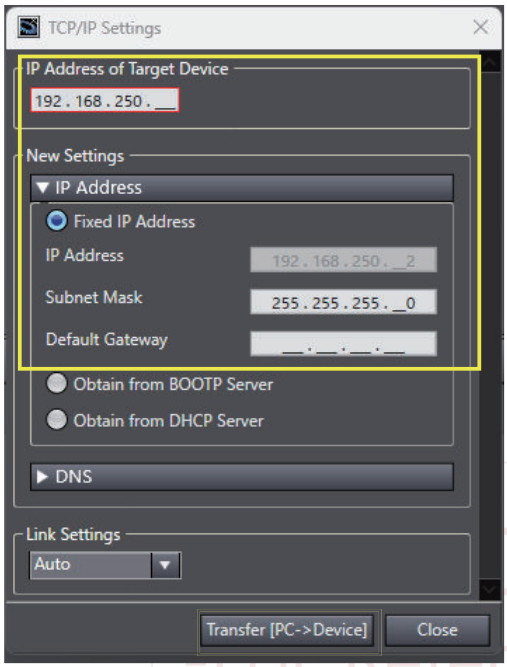
CIP Safety Target Device Operation 창에서 실행할 수도 있습니다.

1) Multiview Explorer에서 Safety PLC(초기 표시 new_SafetyCPU_0)를 선택하고, 화면 상단의 메뉴 바에서 Tools 메뉴의 CIP Safety Target Device Operation을 선택합니다.
2) Safety I/O Block의 IP Address에 현재 설정된 IP 주소를 입력하고 TCP/IP Settings 버튼을 **클릭합니다.**



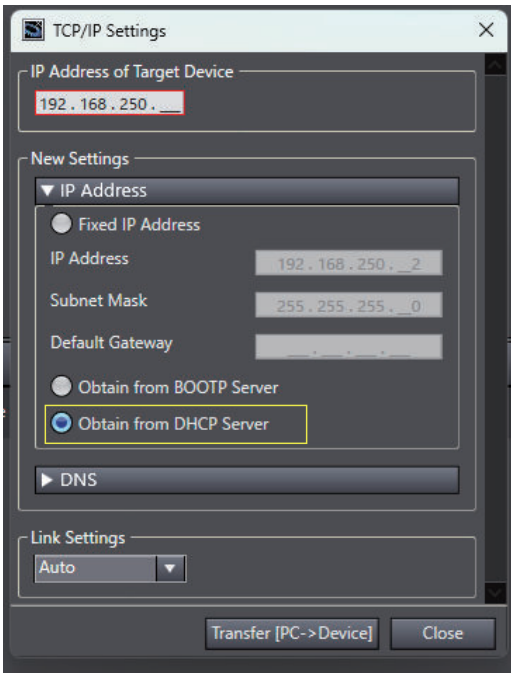
3 고정 IP 주소를 사용하거나 DHCP 서버로부터 IP 주소를 취득하여 IP 주소를 설정합니다.

a) 고정 IP 주소를 사용하는 경우, Static IP address settings 옵션을 선택하고 IP 주소 설정을 입력합니다.



-For Reference Only-

b) DHCP 서버로부터 IP 주소를 취득하는 경우, Obtain from DHCP server 옵션을 선택합니다.



4 **LINK settings를 설정합니다.**

선택 옵션은 다음과 같습니다.

- Auto
- 10 Mbps Half Duplex
- 10 Mbps Full Duplex
- 100 Mbps Half Duplex
- 100 Mbps Full Duplex

5 **Transfer [PC->Device] 버튼을 클릭합니다.**

설정값이 세이프티 I/O 블록으로 전송됩니다.

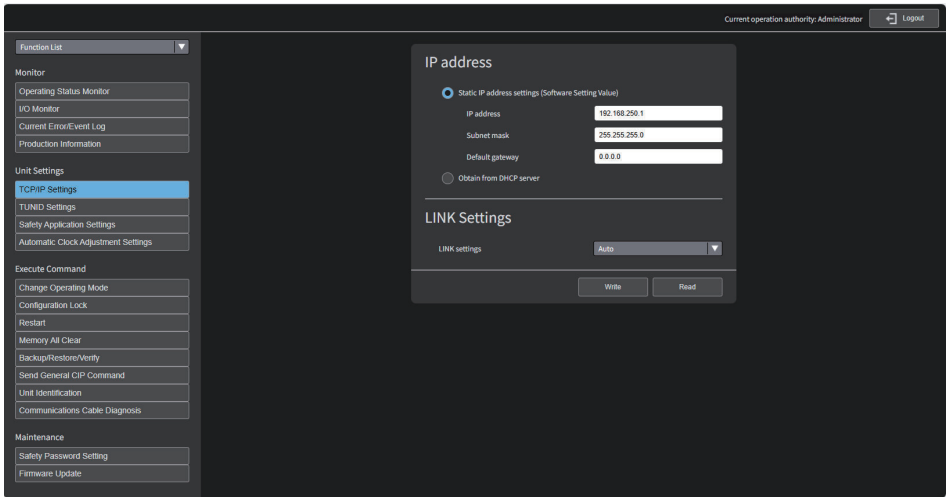
6 전송된 설정값을 적용하려면 전원을 재투입하거나 재시작을 수행하십시오.

사 내 배 포 부
-For Reference Only-

7-10-4 Web UI를 이용한 설정

Web UI의 TCP/IP Settings 화면을 사용하여 해당 유닛의 IP 주소 설정 및 LINK 설정을 구성합니다.

이 화면의 설정은 관리자 권한을 가진 사용자만 구성할 수 있습니다.



설정 절차는 다음과 같습니다.

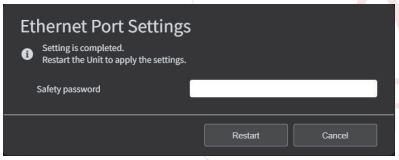
1 Static IP address settings와 Obtain from DHCP server 중에서 IP 주소를 결정하는 **방법을 선택합니다.**

2 **Static IP address settings를 선택한 경우, IP address, Subnet mask, Default gateway에 값을 입력합니다.**
Read 버튼을 클릭하면 현재 IP 주소, 서브넷 마스크, 기본 게이트웨이를 확인할 수 있습니다.

3 **LINK settings를 설정합니다.**
선택 옵션은 다음과 같습니다.
- Auto
- 100 Mbps Half Duplex
- 100 Mbps Full Duplex

Read 버튼을 클릭하면 현재 LINK 설정을 확인할 수 있습니다.

4 Write 버튼을 클릭합니다.
구성한 설정이 해당 유닛으로 전송됩니다. 전송에 성공하면 다음 메시지가 표시됩니다.



AI 번역본
-Reference Only-

5 ADDRESS 로터리 스위치의 설정값을 00"00"으로 설정합니다.

6 세이프티 패스워드를 입력하고 Restart 버튼을 클릭합니다.
세이프티 I/O 블록이 재시작되며 IP 주소 설정 및 LINK 설정이 반영됩니다.

7-11 TUNID 설정

이 절에서는 세이프티 I/O 블록의 TUNID 설정 절차에 대해 설명합니다.

7-11-1 TUNID의 목적

TUNID는 CIP Safety 통신에서 특정 세이프티 커넥션을 식별하는 데 사용됩니다.
TUNID는 6바이트의 Safety Network Number(SNN)와 4바이트의 Node ID로 구성된 총 10바이트 값입니다.

세이프티 네트워크 번호는 여러 세이프티 네트워크를 식별하는 번호이며, 노드 ID는 EtherNet/IP 네트워크에서 각 기기를 식별하는 번호입니다.

7-11-2 TUNID 설정 절차

TUNID 설정에는 Sysmac Studio를 이용하는 방법과 Web UI를 이용하는 방법이 있습니다.

Sysmac Studio를 이용한 설정

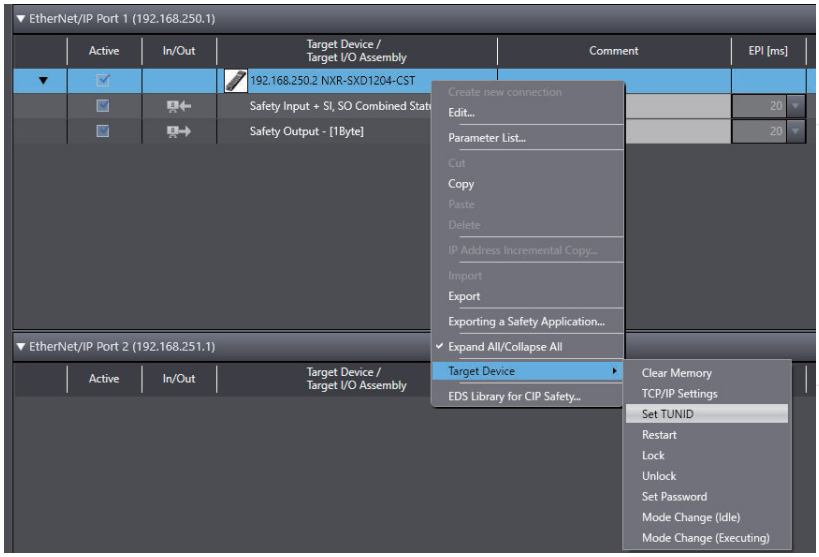
유닛의 TUNID를 설정하는 방법에는 개별 설정과 일괄 설정 두 가지가 있습니다.

● TUNID 설정(개별)

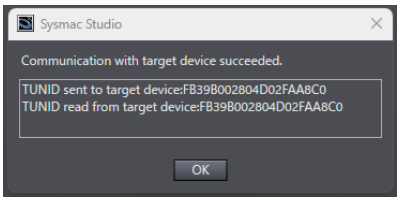
1 Safety CPU Unit과 온라인으로 접속합니다.

2 Connection Settings (Originator) Edit Pane에서 Safety I/O Block을 선택한 후 마우스 오른쪽 **버튼으로 클릭하고**

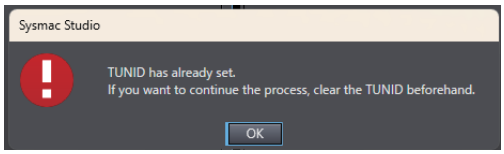
Target Device - Set TUNID를 선택합니다.



3 TUNID 설정에 성공하면 OK 버튼을 클릭합니다.



TUNID가 이미 설정되어 있는 경우, 다음 화면이 표시됩니다.



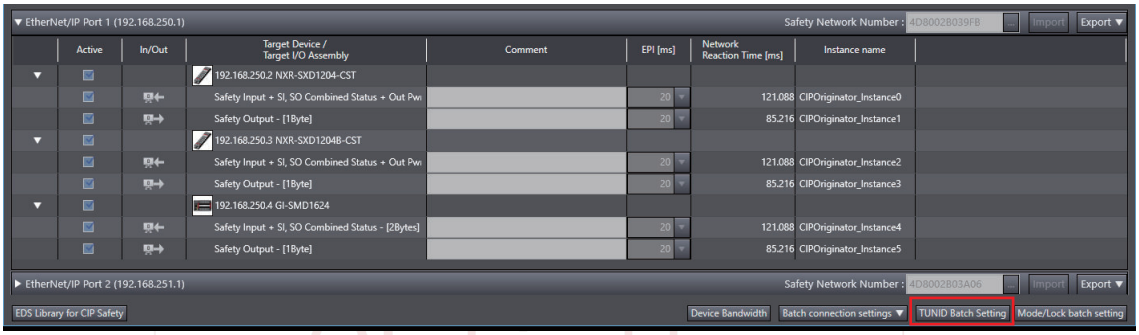
새 TUNID를 설정하려면 clear all memory 기능을 사용하여 세이프티 I/O 블록에서 TUNID를 삭제하십시오. clear all memory 기능에 대한 자세한 내용은 8-2 Clear All Memory 기능(8-4페이지)를 참조하십시오.

● TUNID 설정(일괄 설정)

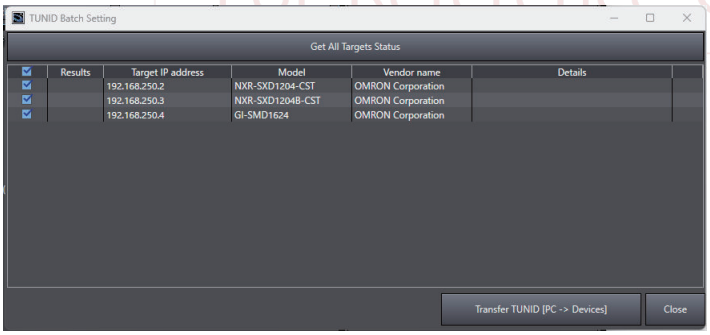
Connection Settings (Originator) Edit Pane에 등록된 모든 타겟의 TUNID 설정을 한 번에 구성할 수 있습니다.

1 Safety CPU Unit과 온라인으로 접속합니다.

2 Connection Settings (Originator) Edit Pane 오른쪽 하단의 TUNID Batch Setting 버튼을
클릭합니다.



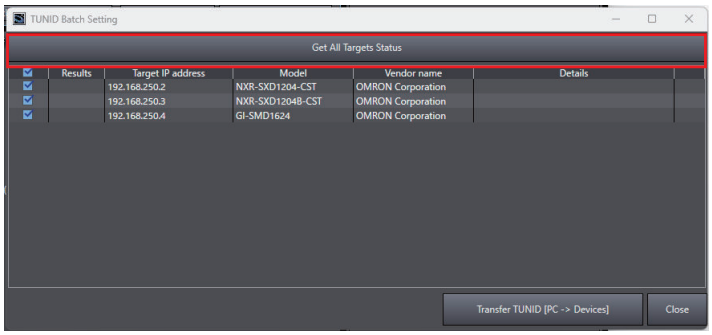
TUNID Batch Setting 창이 표시됩니다.



3 **Get All Targets Status 버튼을 클릭합니다.**

-For Reference Only-

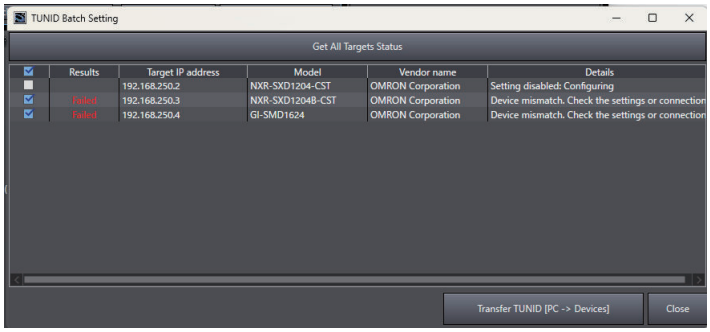
유닛이 목록에 표시된 타겟으로부터 상태를 취득하여 타겟이 현재 TUNID를 설정할 수 있는 상태인지 판별합니다.



추가 정보

체크박스를 해제하면 해당 타겟을 상태 취득 대상에서 제외할 수 있습니다.

4 취득한 상태를 확인합니다.
TUNID를 설정할 수 없는 상태인 경우, 체크박스가 해제됩니다.



또한 Details 열에는 아래와 같이 상태 취득 결과가 표시됩니다.

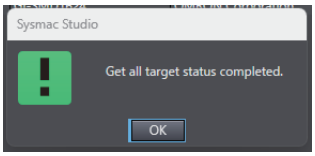
- TUNID를 설정할 수 있는 경우
  Setting enabled: Waiting for TUNID
- TUNID를 설정할 수 없는 경우
  Setting disabled: 해당 기기의 상태가 표시됩니다.
  상태 정보는 CIP Safety 사양에 정의되어 있습니다.
- 기기와 통신할 수 없었던 경우
  Communicate with target failed.

AI 번역본
For Reference Only-

Communicate with target failed.가 표시되면 통신 케이블의 연결 상태, 타겟의 IP 주소 설정 등을 확인하십시오.

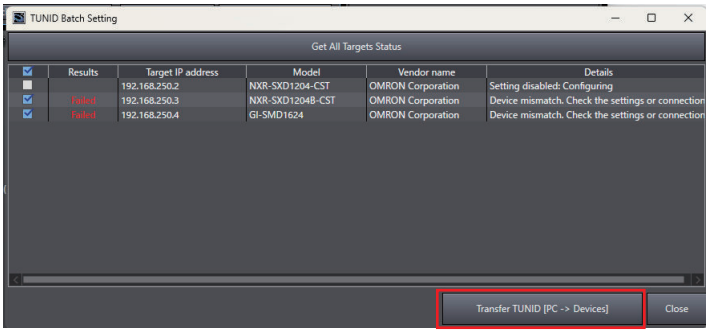
또한 Setting disabled가 표시되면 clear all memory 기능을 사용하여 상황에 따라 타겟의 상태를 변경하십시오.

상태 취득이 완료되면 다음과 같이 표시됩니다.



5 **Transfer TUNID [PC -> Devices] 버튼을 클릭합니다.**

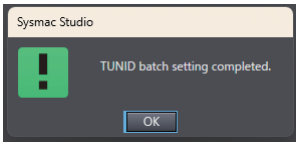
TUNID 일괄 설정이 시작됩니다.



추가 정보

이때 체크박스의 선택 상태도 편집할 수 있습니다.

6 TUNID 일괄 설정 결과를 확인합니다.



TUNID 설정 결과는 Result 열에 표시됩니다.

Result 열	설명
Successful	TUNID 설정이 올바르게 실행되었습니다.
Failed	TUNID 설정이 올바르게 실행되지 않았습니다.

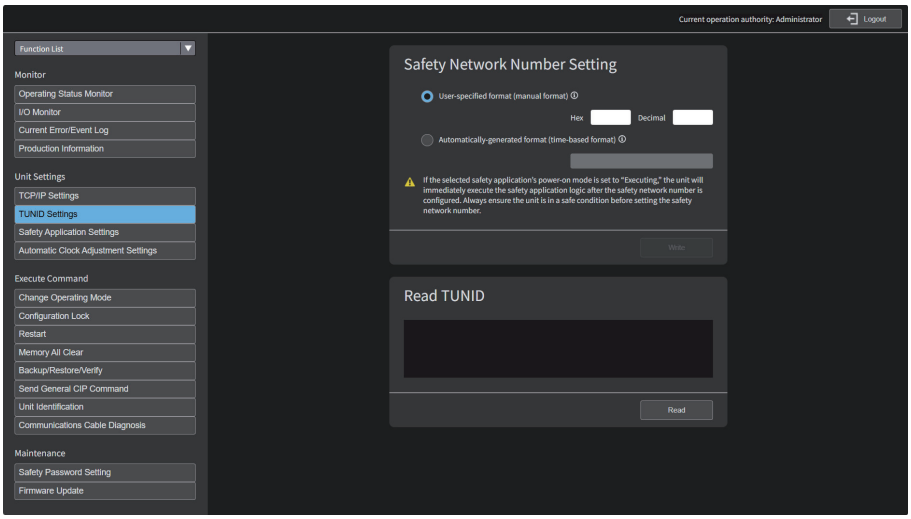
통신 환경을 재검토하거나, TUNID가 이미 설정되어 있는 경우 clear all memory 기능으로 TUNID를 삭제한 후 TUNID를 다시 설정하십시오.

AI 학습용
-For Reference Only-

Web UI를 이용한 설정

Web UI의 TUNID Settings 화면에서 세이프티 네트워크 번호를 확인하여 해당 유닛의 TUNID를 설정합니다.

이 화면의 설정은 관리자 권한을 가진 사용자만 구성할 수 있습니다.



설정 절차는 다음과 같습니다.

1 User-specified format (manual format)과 Automatically-generated format (time-based format) 중에서 **세이프티 네트워크 번호의 결정 방법을 선택합니다.**
각 결정 방법의 의미와 사양은 다음과 같습니다. 이들 방법 중 하나를 사용하여 세이프티 I/O 블록이 연결된 네트워크의 세이프티 네트워크 번호를 설정합니다.

세이프티 네트워크 번호 결정 방법	의미	사양
User-specified format (manual format)	사용자가 다른 시스템과 중복되지 않는 세이프티 네트워크 번호를 결정하여 입력합니다.	**Hex** 자릿수는 4자리이며, 입력 가능한 문자는 0~9 및 A~F입니다. **Decimal** 자릿수는 4자리이며, 입력 가능한 문자는 0~9입니다.
Automatically-generated format (time-based format)	사용자가 CIP Safety 오리지네이터의 세이프티 네트워크 구성 도구가 자동으로 생성한 세이프티 네트워크 번호를 미리 입력합니다.	자릿수는 4자리이며, 입력 가능한 문자는 0~9 및 A~F입니다.

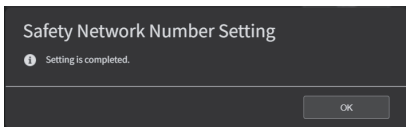
2 선택한 세이프티 네트워크 번호 결정 방법에 따라 세이프티 네트워크

번호를
입력합니다.

Read 버튼을 클릭하면 현재 TUNID, 세이프티 네트워크 번호, 노드 ID를 확인할 수 있습니다.

AI 번역본
-For Reference Only-

3 Write 버튼을 클릭합니다.
구성한 설정이 해당 유닛으로 전송됩니다. 전송에 성공하면 다음 메시지가 표시됩니다.



4 OK 버튼을 클릭합니다.

7-12 세이프티 애플리케이션 선택

세이프티 애플리케이션은 SETTING 로터리 스위치 SW1 및 SW2로 선택합니다.

세이프티 애플리케이션 종류	SETTING 로터리 스위치 SW1 및 SW2
Remote I/O mode application	둘 다 0으로 설정합니다.
Fixed application	사용할 고정 애플리케이션의 번호 1~3으로 둘 다 설정합니다.
User-defined application	둘 다 F로 설정합니다.
Add-on application	사용할 고정 애플리케이션의 번호 9~D로 둘 다 설정합니다.

AI 번역본
-For Reference Only-

7-13 재시작

세이프티 I/O 블록을 재시작합니다.

7-13-1 재시작의 목적

재시작의 목적은 IP 주소 및 기타 설정 정보의 설정이나 변경 사항을 적용하기 위함입니다.

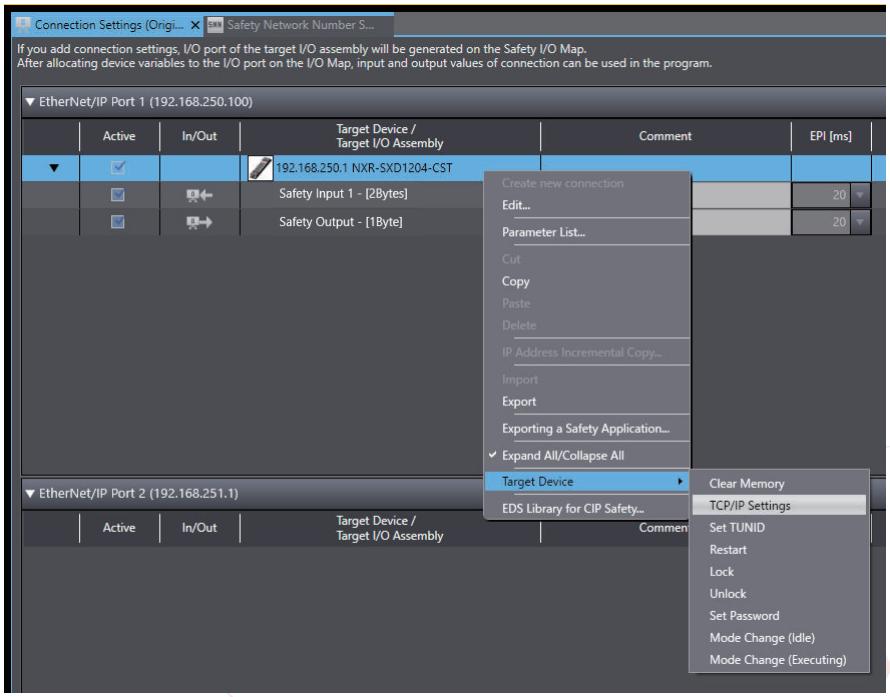
7-13-2 재시작 사용 절차

재시작에는 Sysmac Studio를 이용하는 방법과 Web UI를 이용하는 방법이 있습니다.

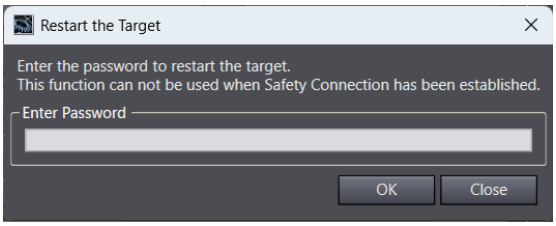
Sysmac Studio를 이용한 절차

Sysmac Studio를 이용한 절차는 다음과 같습니다.

1 접속 설정(오리지네이터)의 설정 화면에서 Safety I/O Block을 마우스 오른쪽 버튼으로 클릭하고, 표시된 메뉴에서 Target Device를 클릭합니다.



2 **Restart를 클릭합니다.**
다음 화면이 표시됩니다.

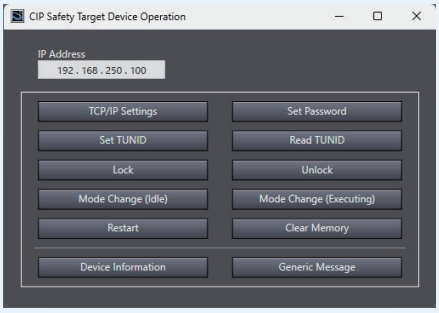


3 세이프티 패스워드를 입력하고 OK 버튼을 클릭합니다.
재시작이 수행됩니다.

추가 정보

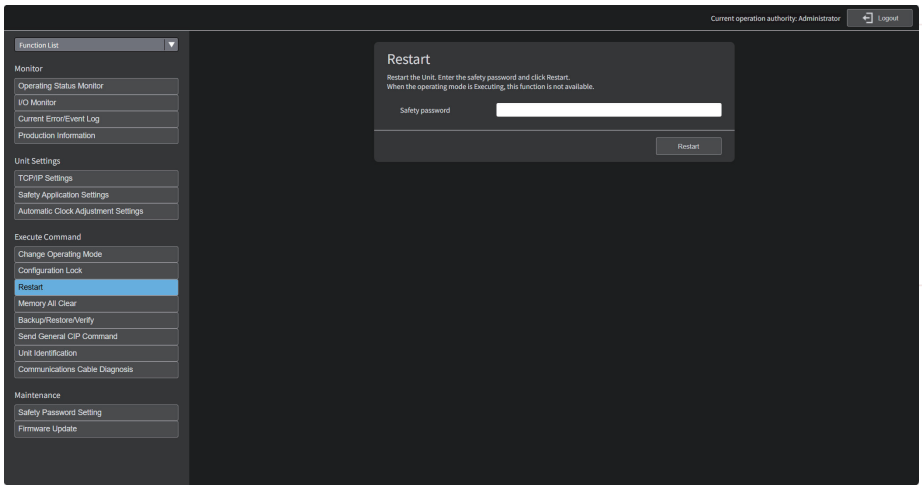
CIP Safety Target Device Operation 창에서 실행할 수도 있습니다.

1) Multiview Explorer에서 Safety PLC(초기 표시 new_SafetyCPU_0)를 선택하고, 화면 상단의 메뉴 바에서 Tools 메뉴의 CIP Safety Target Device Operation을 선택합니다.
2) Safety I/O Block의 IP Address에 설정되어 있는 IP 주소를 입력합니다.



Web UI를 이용한 절차

Web UI의 Restart 화면에서 세이프티 I/O 블록을 재시작하십시오.
이 화면의 설정은 관리자 권한을 가진 사용자만 구성할 수 있습니다.



설정 순서는 다음과 같습니다.

1 세이프티 패스워드를 입력하고 Restart 버튼을 클릭하십시오.
재시작이 실행되고 다음 화면이 표시됩니다.



2 OK 버튼을 클릭하십시오.
Web UI에서 로그아웃이 실행되고 Login 화면이 표시됩니다.

AI 번역본
-For Reference Only-

7-14 구성

이 절에서는 세이프티 컨트롤러와 세이프티 I/O 블록을 구성하는 절차를 설명합니다.
세이프티 컨트롤러의 구성에 대한 자세한 내용은 NX 시리즈 세이프티 컨트롤 유닛/커뮤니케이션 컨트롤 유닛 유저 매뉴얼(자료 번호 Z395)을 참조하십시오.
세이프티 I/O 블록에는 세이프티 애플리케이션 파일을 사용하고, Web UI의 Safety Application Settings 화면에서 설정을 구성하십시오.

7-14-1 세이프티 컨트롤러 구성

세이프티 컨트롤러를 구성하십시오.

1 Sysmac Studio에서 작성한 리모트 I/O 모드 애플리케이션을 세이프티 컨트롤러로 전송하십시오.
세이프티 I/O 블록의 오픈 타입이 Type1 Safety Open인 경우, 세이프티 컨트롤러와 세이프티 I/O 블록 사이에 Type1 Safety Open 커넥션이 확립되면 세이프티 컨트롤러에 의해 세이프티 I/O 블록이 구성됩니다.

7-14-2 세이프티 I/O 블록의 구성

이 절에서는 세이프티 애플리케이션 파일을 사용하여 세이프티 애플리케이션을 설정하는 절차를 설명합니다. 세이프티 애플리케이션은 로터리 스위치 번호를 할당하여 사용합니다. 실수로 세이프티 애플리케이션 파일을 다운로드한 경우, 로터리 스위치 번호에서 해당 세이프티 애플리케이션(Safety I/O 블록)을 제거하십시오.

로터리 스위치로 선택한 세이프티 애플리케이션 구성

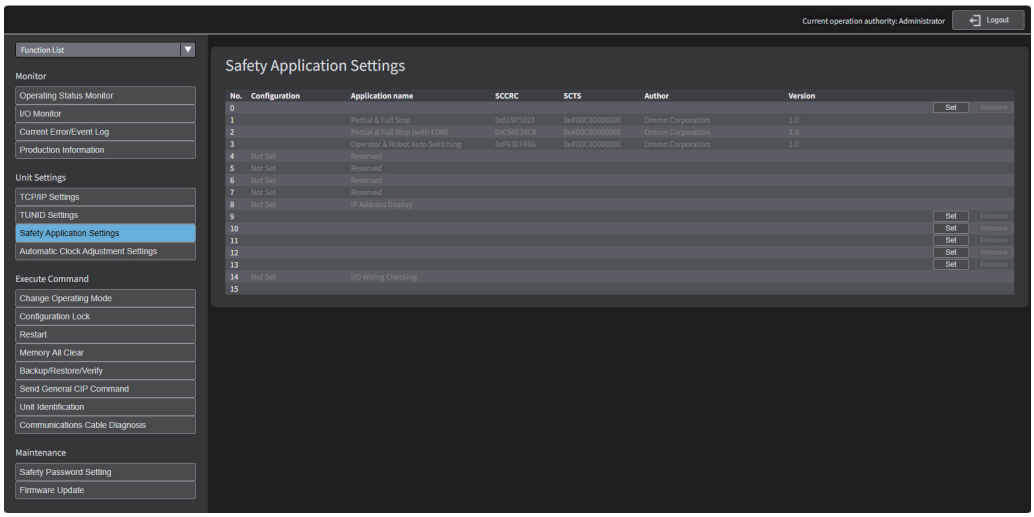
로터리 스위치로 선택한 세이프티 애플리케이션을 구성하는 절차는 다음과 같습니다.

1 Sysmac Studio에서 작성한 세이프티 애플리케이션 파일을 준비하십시오.

2 PC를 세이프티 I/O 블록의 EtherNet/IP 포트에 연결하고 Web UI에 로그인하십시오.

3 Web UI의 Safety Application Settings 화면을 표시하십시오. 이 화면의 설정은 관리자 권한을 가진 사용자만 구성할 수 있습니다.

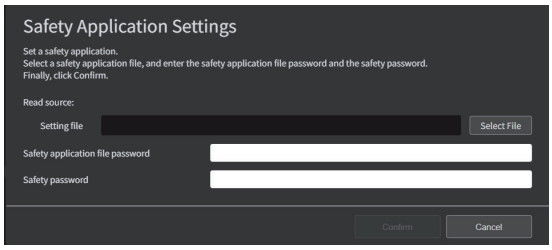
AI 번역본
-For Reference Only-



사용상의 주의

리모트 I/O 모드 애플리케이션용 세이프티 애플리케이션 파일은 애드온 애플리케이션으로 구성할 수 없습니다. 또한 애드온 애플리케이션용 세이프티 애플리케이션 파일은 리모트 I/O 모드 애플리케이션으로 구성할 수 없습니다.

4 애드온 애플리케이션을 할당할 로터리 스위치 번호의 Set 버튼을 클릭하십시오.
다음 메시지가 표시됩니다.

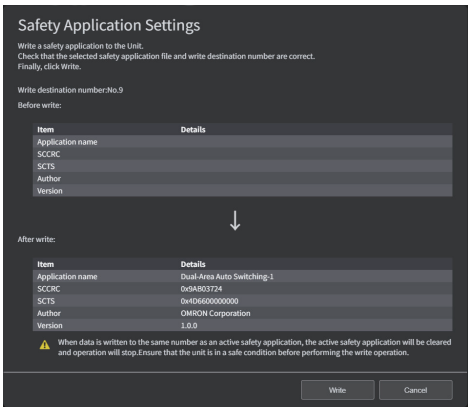


5 Select File 버튼을 클릭하고 PC에서 세이프티 애플리케이션 파일을 선택하십시오.
선택한 세이프티 애플리케이션 파일이 Setting file 필드에 표시됩니다.

6 세이프티 애플리케이션 파일 비밀번호와 세이프티 패스워드를 입력하십시오.

7 Confirm 버튼을 클릭하십시오.
다음 메시지가 표시됩니다.

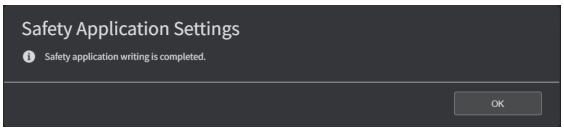
AI 번역본
-For Reference Only-



사용상의 주의

Safety Application Settings 화면에 표시된 SCCRC와 SCTS가 의도한 대로인지 확인하십시오.

8 읽기 소스와 쓰기 대상에 표시된 정보를 확인하고 Write 버튼을 클릭하십시오.
설정이 세이프티 I/O 블록에 반영되고 다음 메시지가 표시됩니다.



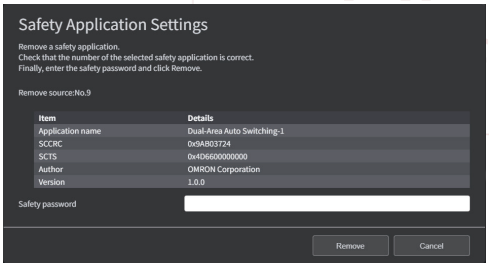
9 애드온 애플리케이션을 동작시키려면 전원 공급을 OFF하고 로터리 스위치를 설정한 후 전원 공급을 ON하십시오.

로터리 스위치 번호에서 애드온 애플리케이션 제거

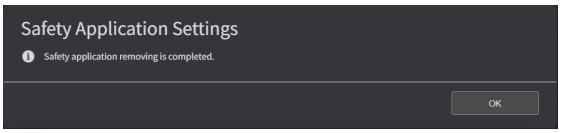
로터리 스위치 번호에서 애드온 애플리케이션을 제거하는 절차는 다음과 같습니다.

1 Web UI의 Safety Application Settings 화면에서 애드온 애플리케이션을 제거할 로터리 스위치 번호의 Remove 버튼을 클릭하십시오.
다음 메시지가 표시됩니다.

AI 번역본
-For Reference Only-



2 삭제 소스에 표시된 정보를 확인하고 세이프티 패스워드를 입력한 후
Remove 버튼을 클릭하십시오.
애드온 애플리케이션이 로터리 스위치 번호에서 제거되고 다음 메시지가 표시됩니다.



AI 번역본
-For Reference Only-

7-15 자동 시계 조정 설정

자동 시계 조정은 해당 유닛의 시각을 조정하기 위한 것입니다.

7-15-1 자동 시계 조정의 목적

자동 시계 조정의 목적은 이벤트 로그에 정확한 날짜와 시각이 기록되도록 하는 것입니다.
이 기능은 세이프티 I/O 블록의 시계 정보를 자동으로 조정합니다.
정확한 시각을 기록하면 에러 발생의 정확한 타이밍을 파악할 수 있어 신속한 대응과
원인 분석에 도움이 됩니다.

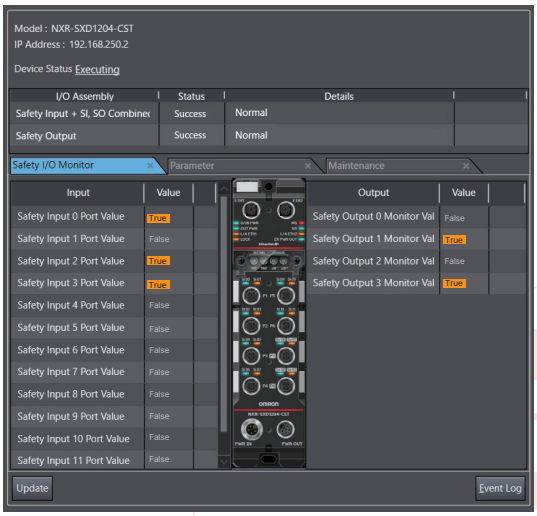
7-15-2 자동 시계 조정 사용 절차

자동 시계 조정에는 Sysmac Studio를 사용하는 방법, Web UI를 사용하는 방법, 익스플리시트 메시지
통신을 사용하는 방법이 있습니다.

Sysmac Studio를 사용하는 절차

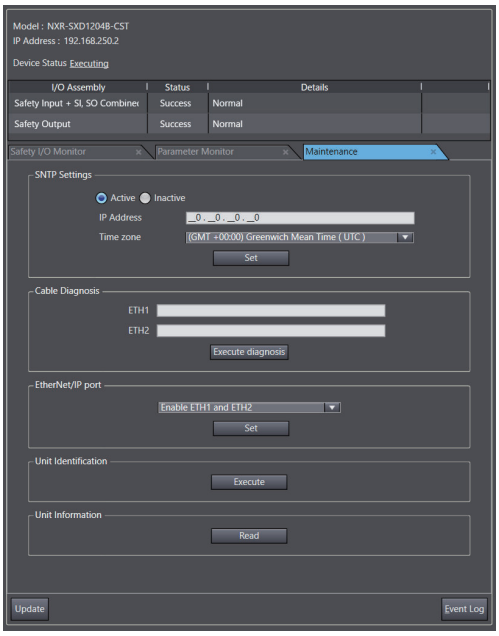
Sysmac Studio를 사용하는 절차는 다음과 같습니다.

1 Sysmac Studio의 CIP Safety Monitor 화면에서 Safety I/O Block을 선택하십시오.
다음 화면이 표시됩니다.



2 Maintenance 탭을 선택하십시오.
다음 화면이 표시됩니다.

번역본
-Reference Only-



3 SNTP Settings의 Active 라디오 버튼을 선택하십시오.

4 SNTP Settings의 IP Address에 NTP 서버 또는 SNTP 서버의 IP 주소를 설정하십시오.

5 Time zone에 설정할 시간대를 선택하십시오.

6 Set을 클릭하십시오.

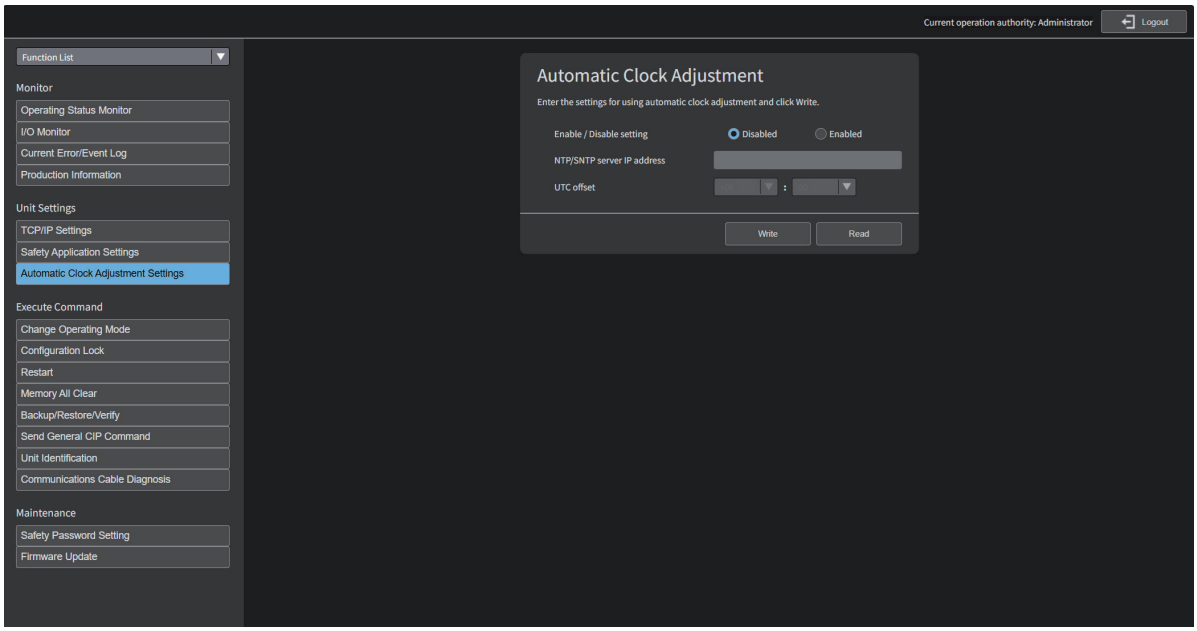
7 유닛을 재시작하십시오.
NTP 서버 또는 SNTP 서버에서 취득한 날짜와 시각이 유닛에 내장된 시계에 설정됩니다.

Web UI를 사용하는 절차

Web UI의 Automatic Clock Adjustment Settings 화면은 세이프티 I/O 블록의 시각을 조정하는 데 사용됩니다.

이 화면의 설정은 관리자 권한을 가진 사용자만 구성할 수 있습니다.

AI 번역본
-For Reference Only-

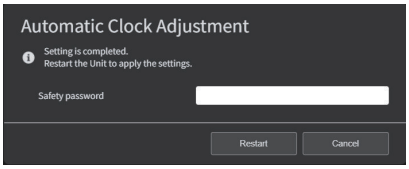


설정 순서는 다음과 같습니다.

1 **Enable/Disable setting을 Enabled로 설정하십시오.**

2 NTP/SNTP server IP address에 NTP/SNTP 서버의 IP 주소를 입력하십시오. UTC offset에 협정 세계시(UTC)와의 시간차를 설정하십시오.

3 Write 버튼을 클릭하십시오.
구성한 설정이 해당 유닛으로 전송됩니다. 전송이 성공하면 다음 메시지가 표시됩니다.



4 세이프티 패스워드를 입력하고 Restart 버튼을 클릭하십시오.
세이프티 I/O 블록이 재시작되고 시각 설정이 반영됩니다.

AI 번역 본
-For Reference Only-

익스플리시트 메시지 통신을 사용하는 절차

NTP/SNTP 서버의 IP 주소 설정 및 시간대 설정에 대한 송신 커맨드는 다음과 같습니다.

구현 세부 사항	송신 커맨드 항목	송신 커맨드 값
SNTP 서버의 IP 주소 설정	서비스 코드	10 hex (Set_Attribute_Single)
	Class ID	380 hex (Unit Manager object)
	Instance ID	01 hex (인스턴스 지정)
	Attribute ID	12 (SNTP Server IP Address)
	Service data	SNTP 서버의 IP 주소

구현 세부 사항	송신 커맨드 항목	송신 커맨드 값
현재 시각 보정을 위한 오프셋(분)	서비스 코드	10 hex (Set_Attribute_Single)
	Class ID	380 hex (Unit Manager object)
	Instance ID	01 hex (인스턴스 지정)
	Attribute ID	102 (Time Zone Offset - Minutes)
	Service data	-720~840

익스플리시트 메시지를 통해 CIP 객체에 액세스하는 방법은 6-7페이지의 익스플리시트 메시지 서버 기능을 참조하십시오.

7-15-3 자동 시계 조정 상세

유닛의 시각 정보는 전원 차단 시 클리어됩니다.
시계 정보의 자동 조정은 주기적으로 실행되지만, 조정 타이밍을 임의로 설정할 수는 없습니다.

일광 절약 시간제(서머타임)는 지원되지 않습니다.

NTP 서버 또는 SNTP 서버와의 연결에 실패하면 NTP Server Connection Error(84040000 hex) 이벤트가 발생합니다. 자세한 내용은 11-12페이지의 11-2-4 이벤트 상세 및 트러블슈팅을 참조하십시오.

사용상의 주의

- 자동 시계 조정을 사용하지 않는 경우, 전원을 투입하면 유닛의 내부 시계가 1972년 1월 1일 00:00:00으로 설정되고 그 시점부터 시각 계측이 진행됩니다.
- 보안 위험을 줄이려면 항상 자동 시계 조정을 실행하십시오.

AI 번역본
-For Reference Only-

7-16 운전 모드 변경

세이프티 I/O 블록의 운전 모드를 Idle 또는 Executing으로 변경하십시오.
운전 모드에 대한 자세한 내용은 6-47페이지의 6-8 운전 모드를 참조하십시오.

7-16-1 Change Operating Mode 사용 절차

운전 모드 변경에는 Sysmac Studio를 사용하는 방법과 Web UI를 사용하는 방법이 있습니다.

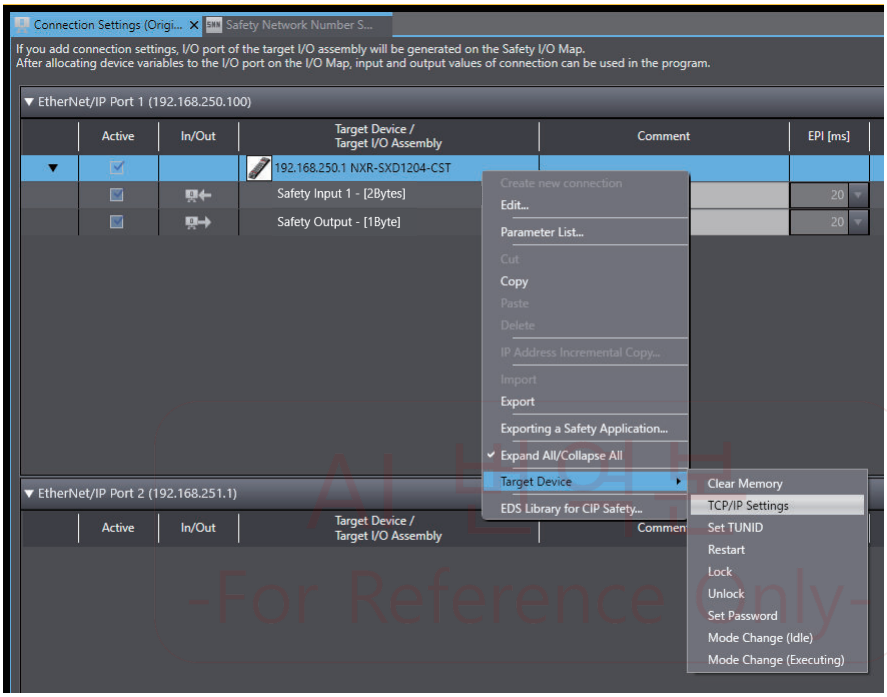
Sysmac Studio를 사용하는 절차

Sysmac Studio에는 유닛별로 개별적으로 운전 모드를 변경하는 방법과, CIP Safety Connection Setting 화면에 등록된 여러 유닛의 운전 모드를 한 번에 변경하는 방법이 있습니다.

● 유닛별 개별 모드 변경

유닛별로 개별적으로 모드를 변경하는 절차는 다음과 같습니다.

1 커넥션 설정(오리지네이터)의 설정 화면에서 세이프티 I/O 블록을 마우스 오른쪽 버튼으로 클릭한 후, 표시된 메뉴에서 Target Device를 클릭하십시오.



2 **Mode Change (Idle) 또는 Mode Change (Executing)을 클릭하십시오.**

3 세이프티 패스워드 입력 창이 표시됩니다. 세이프티 패스워드를 입력하십시오.

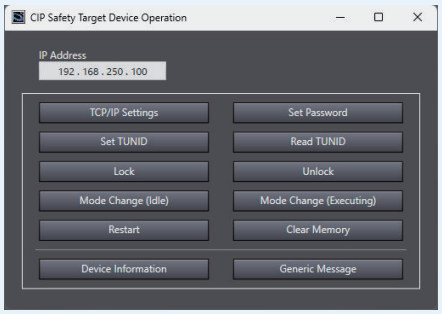


4 OK 버튼을 클릭하십시오.
운전 모드가 변경됩니다.

추가 정보

CIP Safety Target Device Operation 창에서 실행할 수도 있습니다.

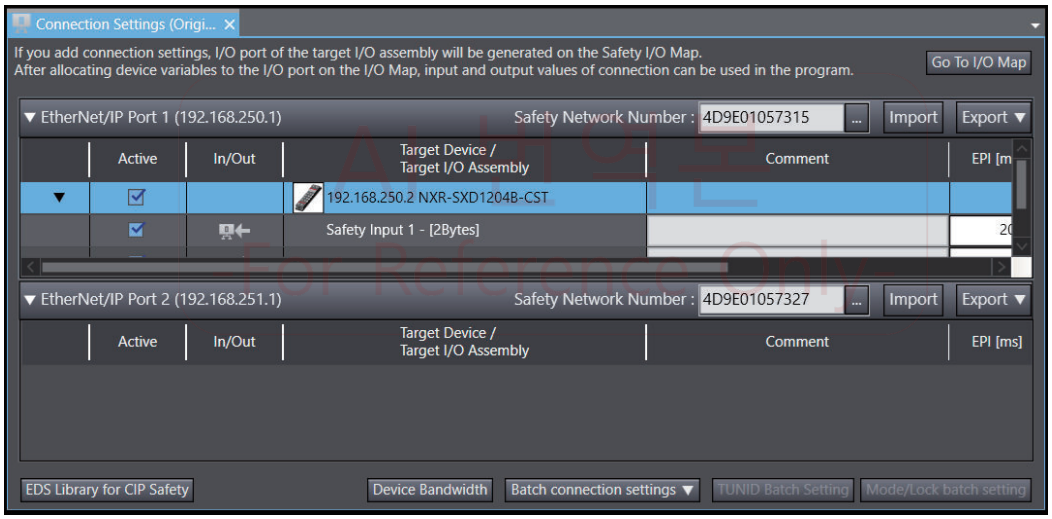
1) Multiview Explorer에서 Safety PLC(초기 표시 new_SafetyCPU_0)를 선택하고, 화면 상단의 메뉴 바에서 Tools 메뉴의 CIP Safety Target Device Operation을 선택하십시오.
2) 세이프티 I/O 블록의 IP Address에 설정된 IP 주소를 입력하십시오.



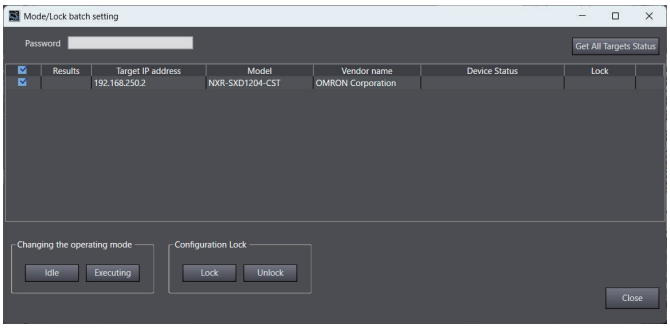
● 여러 유닛의 운전 모드 일괄 변경

여러 유닛의 운전 모드를 일괄 변경하는 절차는 다음과 같습니다.

1 Sysmac Studio에서 커넥션 설정(오리지네이터)의 설정 화면을 표시하십시오.

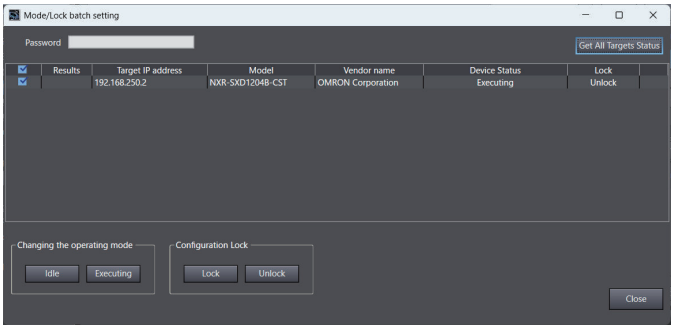


2 **Mode/Lock batch setting 버튼을 클릭하십시오.**
다음 화면이 표시됩니다.



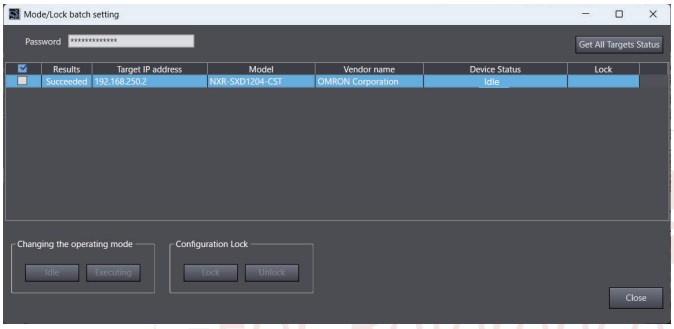
3 **Get All Targets Status 버튼을 클릭하십시오.**

각 타겟의 디바이스 상태가 아래와 같이 Device status 열에 표시됩니다. 디바이스 상태는 운전 모드와 같은 의미입니다.



4 세이프티 패스워드를 입력하고 Changing the operating mode에서 Idle 버튼 또는 **Executing 버튼을 클릭하십시오.**

여러 유닛의 운전 모드가 변경됩니다. 각 타겟의 운전 모드 변경 성공 또는 실패 여부가 아래와 같이 Results 열에 표시됩니다.

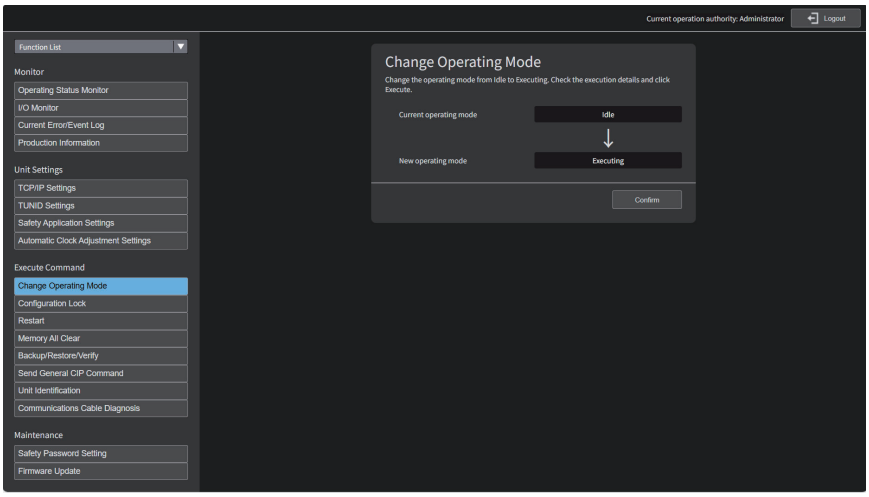


-For Reference Only-

Web UI를 사용하는 절차

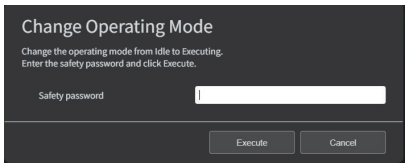
Web UI의 Change Operating Mode 화면은 세이프티 I/O 블록의 운전 모드를 변경하는 데 사용됩니다.

이 화면의 설정은 관리자 권한을 가진 사용자만 구성할 수 있습니다.

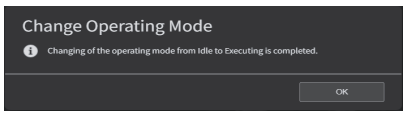


설정 순서는 다음과 같습니다.

1 Current operating mode 필드에는 현재 운전 모드가 표시되고, New operating mode 필드에는 새 운전 모드가 표시됩니다. Confirm 버튼을 클릭하십시오.
다음 메시지가 표시됩니다.



2 세이프티 패스워드를 입력하고 Execute 버튼을 클릭하십시오.
운전 모드가 변경되고 다음 메시지가 표시됩니다.



3 OK 버튼을 클릭하십시오.

AI 번역본
-For Reference Only-

7-17 컨피규레이션 잠금

구성 잠금은 세이프티 I/O 블록의 구성을 잠그거나 해제하는 데 사용됩니다.
CIP Safety Connection Settings 화면에 등록된 여러 세이프티 I/O 블록의 구성 잠금을 동시에 실행할 수도 있습니다.

7-17-1 컨피규레이션 잠금의 목적

구성 잠금의 목적은 세이프티 I/O 블록의 세이프티와 관련된 설정 데이터 및 실행 중인 세이프티 애플리케이션이 의도치 않게 변경되는 것을 방지하는 것입니다. 구성 잠금을 실행하면 세이프티 비밀번호를 입력하지 않는 한 모든 설정 데이터를 변경할 수 없게 됩니다.

7-17-2 컨피규레이션 잠금 사용 절차

구성 잠금에는 Sysmac Studio를 사용하는 방법과 Web UI를 사용하는 방법이 있습니다.

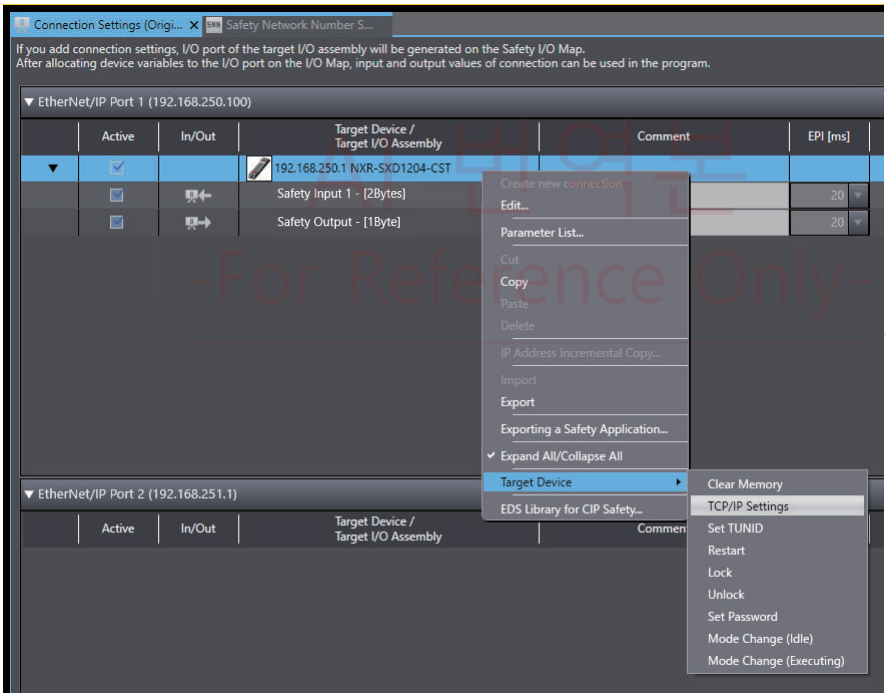
Sysmac Studio를 사용하는 절차

Sysmac Studio에는 유닛별로 개별적으로 구성의 잠금 및 잠금 해제를 실행하는 방법과, CIP Safety Connection Setting 화면에 등록된 여러 유닛의 구성 잠금 및 잠금 해제를 한 번에 실행하는 방법이 있습니다.

● 유닛별 개별 컨피규레이션 잠금 설정

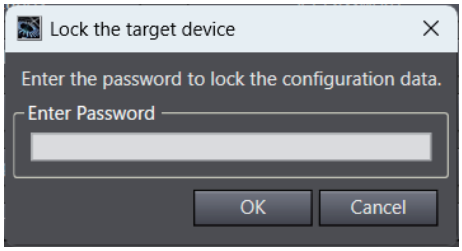
유닛별로 개별적으로 구성을 잠그거나 잠금 해제하는 절차는 다음과 같습니다.

1 커넥션 설정(오리지네이터)의 설정 화면에서 세이프티 I/O 블록을 마우스 오른쪽 버튼으로 클릭한 후, 표시된 메뉴에서 Target Device를 클릭하십시오.



2 **Lock 또는 Unlock을 클릭하십시오.**

3 세이프티 패스워드 입력 창이 표시됩니다. 세이프티 패스워드를 입력하십시오.

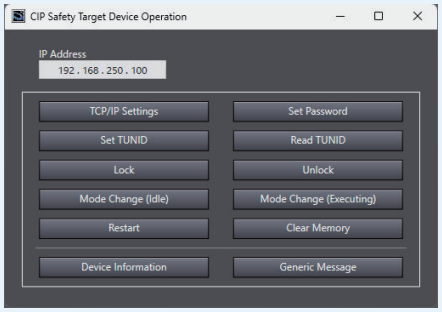


4 OK를 클릭하십시오.
구성의 잠금 또는 잠금 해제가 실행됩니다.

추가 정보

CIP Safety Target Device Operation 창에서 실행할 수도 있습니다.

1) Multiview Explorer에서 Safety PLC(초기 표시 new_SafetyCPU_0)를 선택하고, 화면 상단의 메뉴 바에서 Tools 메뉴의 CIP Safety Target Device Operation을 선택하십시오.
2) 세이프티 I/O 블록의 IP Address에 설정된 IP 주소를 입력하십시오.

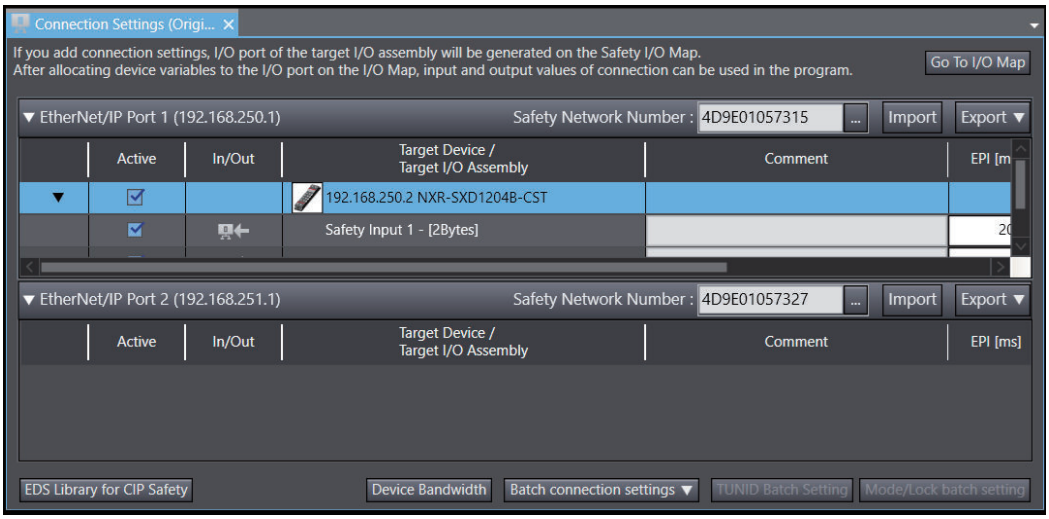


● 여러 유닛 일괄 구성

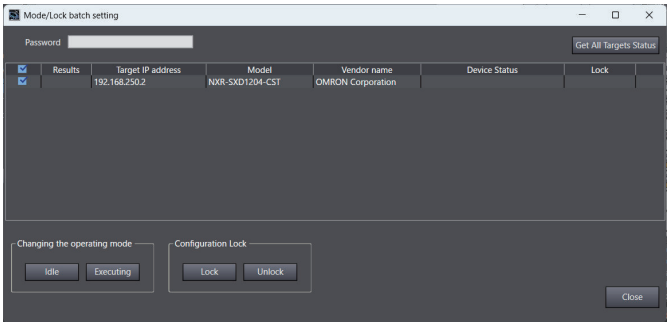
여러 유닛을 일괄 구성하는 절차는 다음과 같습니다.

1 Sysmac Studio에서 커넥션 설정(오리지네이터)의 설정 화면을 표시하십시오.

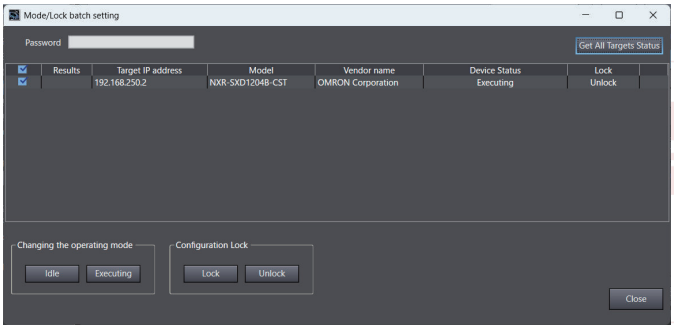
AI 번역본
-For Reference Only-



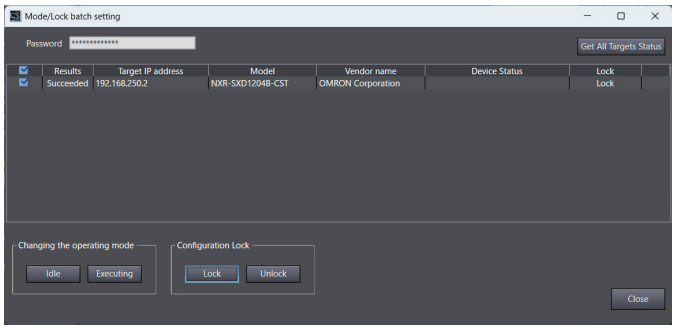
2 **Mode/Lock 일괄 설정 버튼을 클릭합니다.** 다음 화면이 표시됩니다.



3 **Get All Targets Status 버튼을 클릭합니다.**
아래와 같이 각 타겟의 컨피규레이션 잠금 상태가 Lock 열에 표시됩니다.

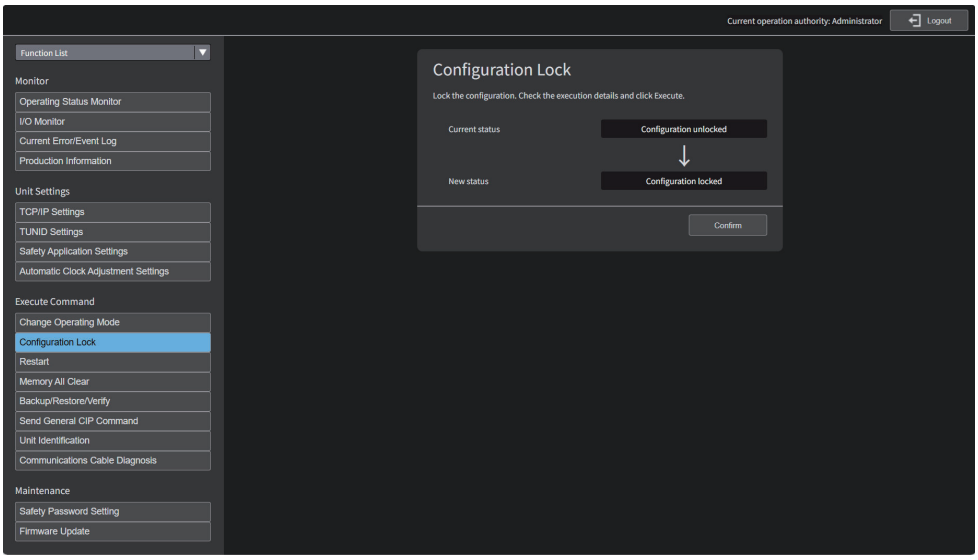


4 세이프티 패스워드를 입력하고 Configuration lock의 Lock 버튼 또는 Unlock 버튼을 클릭합니다.
컨피규레이션의 잠금 또는 잠금 해제는 여러 유닛에 대해 한 번에 실행됩니다. 컨피규레이션의 잠금 또는 잠금 해제가 성공했는지 실패했는지는 아래와 같이 Results 열에 표시됩니다.



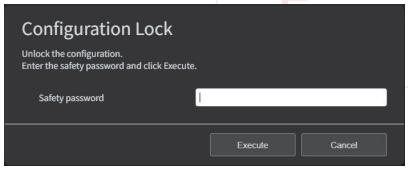
Web UI를 사용하는 절차

Web UI의 Configuration Lock 화면을 사용하여 세이프티 I/O 블록의 컨피규레이션을 잠그거나 잠금 해제합니다.
이 화면의 설정은 관리자 권한이 있는 사용자만 설정할 수 있습니다.



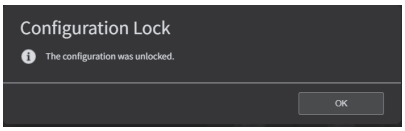
설정 절차는 다음과 같습니다.

1 Current status 필드에 현재 컨피규레이션 잠금 상태가 표시되고, New status 필드에 새로운 컨피규레이션 잠금 상태가 표시됩니다. Confirm 버튼을 클릭합니다.
다음 메시지가 표시됩니다.



AI 번역본
-For Reference Only-

2 세이프티 패스워드를 입력하고 Execute 버튼을 클릭합니다.
컨피규레이션이 잠기거나 잠금 해제되고, 다음 메시지가 표시됩니다.



3 OK 버튼을 클릭합니다.

7-17-3 컨피규레이션 잠금 상세

유닛 표시기의 LOCK 표시기로 컨피규레이션이 잠겨 있는지 확인할 수 있습니다. LOCK 표시기는 컨피규레이션이 잠겨 있을 때 점등하고, 잠금 해제되어 있을 때는 점멸하거나 소등합니다. LOCK 표시기에 대한 자세한 내용은 3-7페이지의 LOCK 표시기를 참조하십시오.

컨피규레이션 잠금의 대상 데이터

컨피규레이션 잠금의 대상 데이터는 다음과 같습니다. 잠금 상태에서는 이 데이터를 변경할 수 없습니다.

항목	설명
CIP Safety 통신 설정	TUNID를 포함한 CIP Safety 통신 기본 설정
세이프티 애플리케이션 설정	애드온 애플리케이션 및 사용자 정의 애플리케이션의 설정과 리모트 I/O 모드 애플리케이션의 I/O 컨피규레이션 설정 고정 애플리케이션의 설정은 잠금 상태와 관계없이 변경할 수 없습니다.
비세이프티 기능의 설정 데이터	EtherNet/IP 통신 설정, TCP/IP 설정, LINK 설정, Ethernet 포트 사용/미사용 설정, LLDP 기능 설정, 스루 배선 출력용 전원 차단 기능의 사용/미사용 설정, SNTP 설정

컨피규레이션 잠금이 실행된 후 로터리 스위치가 다른 값으로 변경된 상태에서 전원을 켜면 Rotary switch settings changed after configuration was locked 이벤트가 발생하고 해당 유닛의 동작이 정지합니다.

컨피규레이션 잠금의 대상 기능

컨피규레이션 잠금의 대상 기능은 다음과 같습니다. 잠금 상태에서는 이 기능을 실행할 수 없습니다.

- I/O 배선 점검 기능
- 백업 복원 기능
- 전체 메모리 삭제 기능

반대로 다음 기능이 실행 중일 때는 컨피규레이션을 잠글 수 없습니다.

- I/O 배선 점검 기능

AI 번역본
-For Reference Only-

7-18 안전 비밀번호 설정

세이프티 패스워드는 세이프티 I/O 블록 유닛에 대한 무단 액세스를 방지하고 세이프티 I/O 블록 유닛에 저장된 자산을 보호하기 위한 것입니다.

7-18-1 안전 비밀번호의 목적

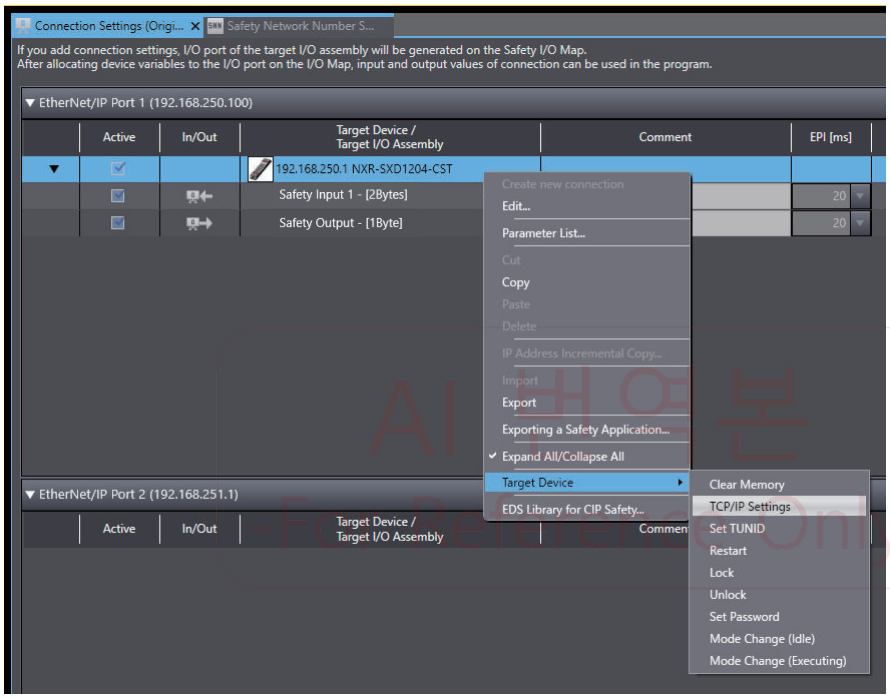
세이프티 패스워드의 목적은 사용자의 권한에 해당하는 조작만 사용할 수 있도록 함으로써 세이프티 I/O 블록의 자산이 변조되거나 유출되는 것을 방지하는 것입니다.
따라서 세이프티 패스워드를 포함한 사용자의 계정 정보는 적절히 관리해야 합니다.

7-18-2 안전 비밀번호 설정 사용 절차

세이프티 패스워드 설정에는 Web UI를 사용하는 방법이 있습니다.
또한 Sysmac Studio에서도 세이프티 패스워드를 변경할 수 있습니다.

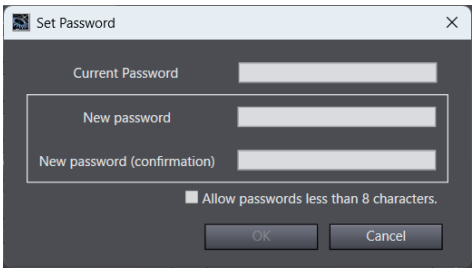
Sysmac Studio에서 안전 비밀번호 변경 절차

1 커넥션 설정(오리지네이터)의 설정 화면에서 세이프티 I/O 블록을 마우스 오른쪽 버튼으로 클릭하고, 표시된 메뉴에서 Target Device를 클릭합니다.



2 **Set Password를 클릭합니다.**

3 비밀번호 설정 창이 표시됩니다. 현재 세이프티 패스워드와 새 세이프티 패스워드를 입력합니다.

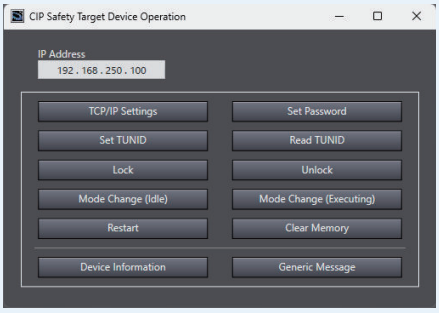


4 OK를 클릭합니다.
새 세이프티 패스워드가 설정됩니다.

추가 정보

CIP Safety Target Device Operation 창에서도 실행할 수 있습니다.

1) Multiview Explorer에서 Safety PLC(초기 표시 new_SafetyCPU_0)를 선택하고, 화면 상단의 메뉴 바에서 Tools 메뉴의 CIP Safety Target Device Operation을 선택합니다.
2) 세이프티 I/O 블록의 IP Address에 설정되어 있는 IP 주소를 입력합니다.



Web UI를 사용하는 절차

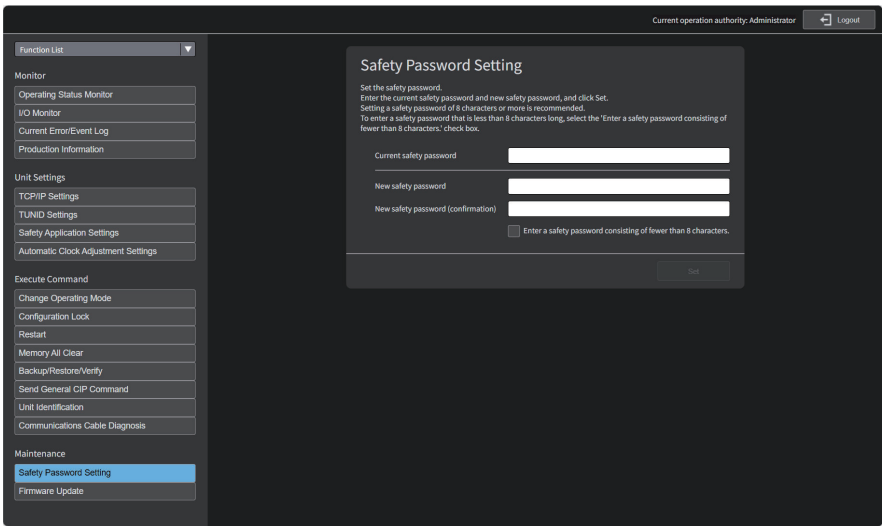
Web UI의 세이프티 패스워드 관련 사용 절차는 다음 표를 참조하십시오.

기능	참조처
세이프티 패스워드 인증	7-22페이지의 7-2-6 Login
세이프티 패스워드 설정	7-105페이지의 Web UI를 사용하는 세이프티 패스워드 설정 절차
초기 안전 비밀번호 변경	7-24페이지의 초기 안전 비밀번호 변경

샘플 번역본
-For Reference Only-

Web UI를 사용하는 안전 비밀번호 설정 절차

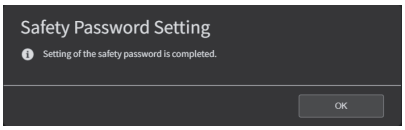
Web UI의 Safety Password Setting 화면에서 세이프티 패스워드를 설정합니다.
이 화면의 설정은 관리자 권한이 있는 사용자만 설정할 수 있습니다.



설정 절차는 다음과 같습니다.

1 Current safety password에 현재 세이프티 패스워드를 입력합니다. New **safety password 및 New safety password(confirmation)에 새 세이프티 패스워드를 입력합니다.**
보안을 강화하려면 8자 이상의 세이프티 패스워드를 입력하십시오.
단, 다른 기기와 동일한 비밀번호를 사용하고 싶은 경우 등 특별한 사정이 있을 때는 Enter a safety password less than 8 characters long 체크박스를 선택하면 8자 미만의 세이프티 패스워드를 설정할 **수 있습니다.**

2 Set 버튼을 클릭합니다.
세이프티 패스워드가 설정되고, 다음 메시지가 표시됩니다.



3 OK 버튼을 클릭합니다.
Web UI에서 로그아웃되고 Login 화면이 표시됩니다.

AI 번역본
For Reference Only-

7-18-3 안전 비밀번호 상세

이 절에서는 세이프티 패스워드의 다양한 사양에 대해 설명합니다.

안전 비밀번호 입력이 필요한 조작

Sysmac Studio에서는 다음 조작을 실행할 때 세이프티 패스워드 입력이 필요합니다. 안전 비밀번호를 입력하지 않으면 이 조작은 실행되지 않습니다.

- 세이프티 패스워드 변경
- 컨피규레이션 잠금/잠금 해제
- 재시작
- 운전 모드 변경

・전체 메모리 삭제

Web UI는 사용자 권한을 Web UI가 화면에 표시하는 다양한 정보를 볼 수 있는 옵서버와,
Web UI가 제공하는 다양한 설정을 설정할 수 있는 관리자로 구분합니다.
Web UI의 각 화면과 옵서버 또는 관리자로서 사용할 수 있는지 여부의 관계는 7-18페이지의
7-2-4 Main Menu List를 참조하십시오.

안전 비밀번호 사양

세이프티 패스워드에 사용할 수 있는 문자열의 조건은 다음과 같습니다.

항목	설명
문자 수	8~32
사용 가능 문자	A~Z, a~z, 0~9, ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ 반각 스페이스

공장 출하 시에는 세이프티 패스워드가 설정되어 있지 않습니다.

사용상의 주의

보안 위험을 줄이기 위해 반드시 세이프티 패스워드를 설정하십시오. 설정하는 세이프티 패스워드에는 영문자, 기호, 숫자를 사용하여 복잡하게 만드십시오.

기타 사양

Web UI에 로그인한 후 10분 이상 조작이 없으면 편집 권한이 없는 제3자에 의한 부정 사용을 방지하기 위해 세이프티 패스워드를 다시 입력해야 합니다.

무차별 대입 공격에 대한 대책으로, Web UI에서 세이프티 패스워드를 5회 잘못 입력하면
10분 동안 로그인할 수 없습니다. 세이프티 패스워드 오입력 횟수는 로그인 성공, 전원 재투입, 10분 경과
중 어느 하나로 초기화됩니다.

사용상의 주의

・세이프티 패스워드는 표시할 수 없습니다. 또한 전체 메모리 삭제로 세이프티 패스워드가 초기화된 경우에는 세이프티 패스워드를 입력해야 합니다.
・제3자의 부정 사용을 방지하기 위해 Web UI를 통한 조작을 중단하고 컴퓨터에서 자리를 뜨기 전에 세이프티 I/O 블록에서 로그아웃하십시오. Web UI에서 Operating Status Monitor 화면, I/O Monitor 화면, Current Error 화면, Event log 화면의 Refresh automatically를 선택하면 10분 이상 조작이 없어도 세이프티 패스워드를 다시 입력할 필요가 없습니다.

7-19 백업

백업에는 백업, 복원, 검증의 세 가지 기능이 있습니다.

- **백업**

  해당 유닛의 모든 설정 데이터를 백업 파일로 PC에 일괄 저장합니다. 보안 대책으로 백업 파일에 백업 파일 비밀번호를 설정합니다.

- **복원**

  PC의 백업 파일 내용을 해당 유닛에 반영합니다.

- **검증**

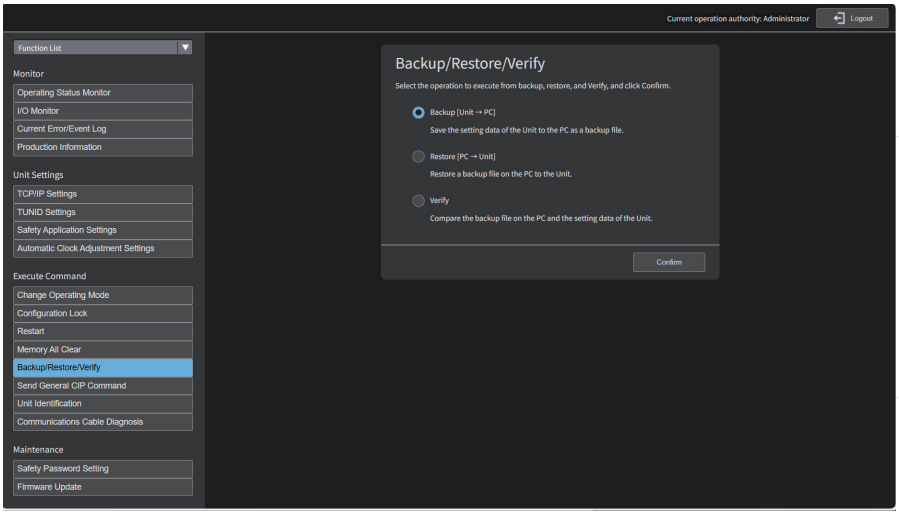
  해당 유닛의 설정 데이터와 PC의 백업 파일을 대조하여 내용이 동일한지 검증합니다.

7-19-1 백업의 목적

백업의 목적은 세이프티 I/O 블록의 모든 설정 데이터를 한 번에 백업, 복원, 검증함으로써 세이프티 I/O 블록 교체 시 파라미터 설정 시간을 줄이는 것입니다.
세이프티 I/O 블록의 설정이 항상 백업 파일의 설정과 일치하도록 정기적으로, 그리고 설정을 변경했을 때 백업을 수행하십시오.

7-19-2 백업 사용 절차

Web UI의 Backup/Restore/Verify 화면을 사용하여 백업, 복원, 검증을 수행합니다. 이 화면의 설정은 관리자 권한이 있는 사용자만 설정할 수 있습니다.



이 절에서는 각 절차에 대해 설명합니다.

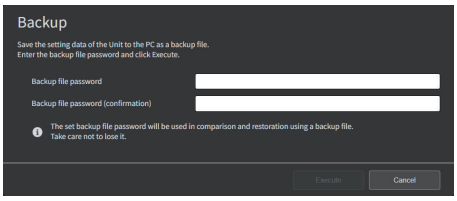
사용상의 주의

백업을 실행하려면 컨피규레이션 잠금 기능을 사용하여 세이프티 I/O 블록을 잠금 상태로 설정해야 합니다.
또한 복원을 실행하려면 세이프티 I/O 블록을 잠금 해제 상태로 설정해야 합니다. 컨피규레이션 잠금 기능에 대한 자세한 내용은 7-99페이지의 7-17 컨피규레이션 잠금을 참조하십시오.

백업

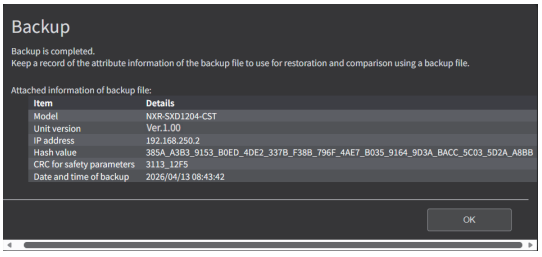
백업 절차는 다음과 같습니다.

1 Backup [Unit → PC]를 선택하고 Confirm 버튼을 클릭합니다.
다음 화면이 표시됩니다.



2 **Backup file password 및 Backup file password(confirmation)에 백업 파일 비밀번호를 입력합니다.** 백업 파일 비밀번호는 백업 파일을 작성, 복원, 검증하기 위한 것입니다. 안전 비밀번호와는 다릅니다.

3 Execute 버튼을 클릭합니다.
백업 파일이 PC의 Downloads 폴더에 저장됩니다. 파일 이름은 Unit Model_IP Address_Date.dat입니다.
다음 메시지가 표시됩니다.



표시된 백업 파일 속성 정보는 복원에 필요합니다. 메모해 두십시오.

4 OK 버튼을 클릭합니다.

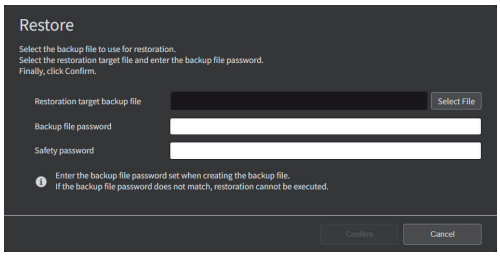
AI 번역본
-For Reference Only-

복원

복원 절차는 다음과 같습니다.

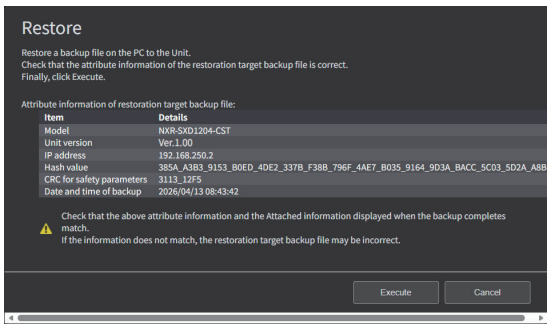
1 복원 대상 세이프티 I/O 블록을 공장 출하 시 상태 또는 전체 메모리 삭제 상태로 준비하고,
백업 파일 및 백업 파일 작성 시 기록해 둔 백업 파일의 속성 정보를
준비합니다.

2 Web UI의 Backup/Restore/Verify 화면에서 Restore [PC → Unit]를 선택하고 Confirm 버튼을 클릭합니다.
다음 화면이 표시됩니다.



3 Select 버튼을 클릭하고 PC에서 복원 대상 백업 파일을 선택합니다.
선택한 백업 파일이 Restoration target backup file 필드에 표시됩니다.

4 백업 파일 비밀번호와 세이프티 패스워드를 입력하고 Confirm 버튼을 클릭합니다. 다음 메시지가 표시됩니다.

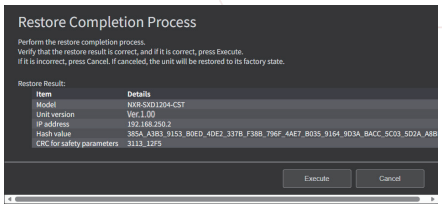


5 Attribute information of restoration target backup file 필드에 표시된 속성 정보가 백업 파일 작성 시 표시된 속성 정보와 일치하는지 확인하고 Execute 버튼을 클릭합니다. 일치하지 않는 경우에는 지정한 백업 파일이 손상되었을 수 있으므로 Cancel 버튼을 클릭하십시오.
Execute 버튼을 클릭하면 복원이 실행되고 다음 메시지가 표시됩니다.



AI 번역본
- For Reference Only -

6 세이프티 패스워드를 입력하고 Restart 버튼을 클릭합니다.
세이프티 I/O 블록이 재시작되고 복원된 내용이 반영됩니다. 다음 메시지가 표시됩니다.



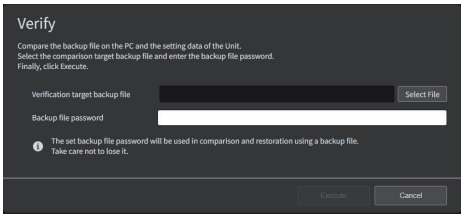
7 Restore Result 필드에 표시된 속성 정보가 백업 파일 작성 시 표시된 속성 정보와 일치하는지 확인하고 Execute 버튼을 클릭합니다. 일치하지 않는 경우에는 복원이 실패했을 수 있으므로 Cancel 버튼을 클릭하십시오.

8 전원을 재투입하거나 Web UI의 Restart 화면을 사용하여 세이프티 I/O 블록을 재시작합니다.
복원이 완료되고 세이프티 I/O 블록이 재시작됩니다. 7단계에서 Cancel 버튼을 클릭한 경우에는 전체 메모리가 자동으로 삭제됩니다.
재시작 후 운전 모드는 복원된 백업 데이터의 전원 투입 시 모드 설정에 따릅니다. 컨피규레이션 잠금은 잠긴 상태가 됩니다.

데이터 검증

검증 절차는 다음과 같습니다.

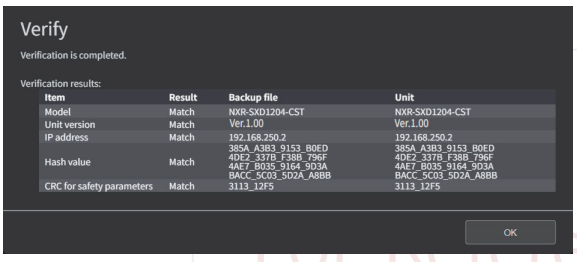
1 Verify를 선택하고 Confirm 버튼을 클릭합니다. 다음 화면이 표시됩니다.



2 Select File 버튼을 클릭하고 PC에서 검증 대상 백업 파일을 선택합니다.
선택한 백업 파일이 Verification target backup file 필드에 표시됩니다.

3 Backup file password에 백업 파일 작성 시 설정한 백업 파일 비밀번호를 입력합니다.
백업 파일 비밀번호는 백업 파일을 작성, 복원, 검증하기 위한 것입니다. 안전 비밀번호와는 다릅니다.

4 Execute 버튼을 클릭합니다.
백업 파일 비밀번호가 일치하면 검증이 실행되고 검증 결과가 표시됩니다.



역본
-For Reference Only-

5 OK 버튼을 클릭합니다.

7-19-3 백업 상세

이 절에서는 백업의 다양한 사양에 대해 설명합니다.

백업 대상 데이터

백업, 복원, 검증 대상 데이터는 다음과 같습니다.

항목	설명
CIP Safety 통신 설정	SNN 및 TUNID를 포함한 CIP Safety 통신 기본 설정
세이프티 애플리케이션 설정	애드온 애플리케이션 및 사용자 정의 애플리케이션의 설정과 리모트 I/O 모드 애플리케이션의 I/O 컨피규레이션 설정 고정 애플리케이션의 설정은 포함되지 않습니다.
컨피규레이션 잠금 상태	컨피규레이션이 잠겨 있음을 나타내는 정보와 컨피규레이션이 잠겼을 때 저장된 각종 설정값
생산 정보	유닛 모델, 유닛 버전
비세이프티 기능의 설정 데이터	EtherNet/IP 통신 설정, TCP/IP 설정 *1, LINK 설정, Ethernet 포트 사용/미사용 설정, LLDP 기능 설정, 스루 배선 출력용 전원 차단 기능의 사용/미사용 설정, SNTP 설정

***1.** IP 주소를 DHCP로 설정하는 경우 DHCP 서버로부터 취득한 IP 주소는 백업, 복원, 검증 대상에서 제외됩니다.

백업 파일 이름

백업 파일의 기본 파일 이름은 Unit Model_IP Address_Date.dat입니다. 파일 이름은 자유롭게 변경할 수 있습니다.

백업 파일 비밀번호 사양

백업 파일 비밀번호에 사용할 수 있는 문자열의 조건은 다음과 같습니다.

항목	설명
문자 수	8~32
사용 가능 문자	A~Z, a~z, 0~9, ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ 반각 스페이스

사용상의 주의

- 보안 위험을 줄이기 위해 백업 파일 비밀번호에는 영문자, 기호, 숫자를 조합하여 사용하십시오.
- 백업 파일 비밀번호는 표시하거나 초기화할 수 없습니다. 잊어버릴 경우를 대비하여 백업 파일 비밀번호를 관리하십시오.

-For Reference Only-

8

세이프티 I/O 블록의 기능

이 장에서는 세이프티 I/O 블록의 다양한 기능에 대해 설명합니다.

8-1 기능 일람 8-3

8-2 전체 메모리 삭제 기능 8-4
8-2-1 전체 메모리 삭제 기능의 목적 8-4
8-2-2 전체 메모리 삭제 기능 사용 절차 8-4
8-2-3 전체 메모리 삭제 기능 상세 8-7

8-3 HTTPS 통신 기능 8-8
8-3-1 HTTPS 통신 기능의 목적 8-8
8-3-2 HTTPS 통신 기능 사용 절차 8-8
8-3-3 HTTPS 통신 기능 상세 8-9

8-4 디바이스 레벨 링(DLR) 기능 8-10
8-4-1 DLR 기능의 목적 8-10
8-4-2 DLR 기능 사용 절차 8-10
8-4-3 DLR 기능 상세 8-10

8-5 스루 배선 출력 전원 OFF 기능 8-11
8-5-1 스루 배선 출력 전원 OFF 기능의 목적 8-11
8-5-2 스루 배선 출력 전원 OFF 기능 사용 절차 8-11

8-6 I/O 배선 점검 기능 8-13
8-6-1 I/O 배선 점검 기능의 목적 8-13
8-6-2 I/O 배선 점검 기능의 동작 8-13
8-6-3 I/O 배선 점검 기능의 I/O 컨피규레이션 설정 8-13
8-6-4 I/O 배선 점검 기능 사용 절차 8-14

8-7 범용 CIP 커맨드 송신 기능 8-15
8-7-1 범용 CIP 커맨드 송신 기능의 목적 8-15
8-7-2 범용 CIP 커맨드 송신 기능 사용 절차 8-15

8-8 유닛 식별 기능 8-16
8-8-1 유닛 식별 기능의 목적 8-16
8-8-2 유닛 식별 기능 사용 절차 8-16
8-8-3 유닛 식별 기능 상세 8-18

8-9 IP 주소 표시 기능 8-19
8-9-1 IP 주소 표시 기능의 목적 8-19
8-9-2 IP 주소 표시 기능 사용 절차 8-19
8-9-3 IP 주소 표시 기능 상세 8-19

8-10 전원 감시 기능 8-22
8-10-1 전원 감시 기능의 목적 8-22
8-10-2 전원 감시 기능 사용 절차 8-22

사용 설명서
For Reference Only

8-10-3 전원 감시 기능 상세 8-24

8-11 I/O 감시 기능 8-27
8-11-1 I/O 감시 기능의 목적 8-27
8-11-2 I/O 감시 기능 사용 절차 8-27

8-12 접점 동작 횟수 감시 기능 8-29
8-12-1 접점 동작 횟수 감시 기능의 목적 8-29
8-12-2 세이프티 입력 단자 사용 절차 8-29
8-12-3 세이프티 출력 단자 사용 절차 8-29

8-13 통신 케이블 진단 기능 8-31
8-13-1 통신 케이블 진단 기능의 목적 8-31
8-13-2 통신 케이블 진단 기능 사용 절차 8-31
8-13-3 통신 케이블 진단 기능 상세 8-33

8-14 펌웨어 업데이트 기능 8-35
8-14-1 펌웨어 업데이트 기능의 목적 8-35
8-14-2 펌웨어 업데이트 기능 사용 절차 8-35
8-14-3 펌웨어 업데이트 기능 상세 8-36

AI 번역본
-For Reference Only-

8-1 기능 일람

세이프티 I/O 블록의 다양한 기능은 다음과 같습니다.

기능명	목적	설명	참조처
전체 메모리 삭제 기능	해당 유닛의 설정 데이터 정보가 유출되는 것을 방지합니다.	해당 유닛의 모든 설정 데이터를 공장 출하 시 설정으로 되돌립니다.	8-4페이지의 8-2 전체 메모리 삭제 기능
HTTPS 통신 기능	통신 데이터 정보가 유출되는 것을 방지합니다.	Web UI 사용 시 PC와 해당 유닛 간에 암호화된 통신을 수행합니다.	8-8페이지의 8-3 HTTPS 통신 기능
디바이스 레벨 링 (DLR) 기능	통신 케이블이 한 곳에서 끊어져도 정상적인 통신을 유지할 수 있도록 합니다.	통신 케이블을 링 토폴로지로 접속합니다.	8-10페이지의 8-4 디바이스 레벨 링 (DLR) 기능
스루 배선 출력 전원 OFF 기능	사용하는 전력량을 절감합니다.	출력 전원을 스루 배선으로 여러 유닛에 접속했을 때, 해당 유닛보다 뒤쪽에 있는 유닛으로의 출력 전원 공급을 차단합니다.	8-11페이지의 8-5 스루 배선 출력 전원 OFF 기능
I/O 배선 점검 기능	세이프티 I/O 단자로의 배선을 확실하고 쉽게 점검할 수 있도록 합니다.	세이프티 I/O 단자로의 배선이 올바르게 이루어졌는지 확인합니다.	8-13페이지의 8-6 I/O 배선 점검 기능
범용 CIP 커맨드 송신 기능	전용 툴이나 SNCT 없이 해당 유닛이 보유한 CIP 오브젝트의 기능을 실행합니다.	CIP 메시지 커맨드를 발행합니다.	8-15페이지의 8-7 범용 CIP 커맨드 송신 기능
유닛 식별 기능	동작 중인 유닛을 식별할 수 있도록 합니다.	해당 유닛의 유닛 식별 표시기를 점등합니다.	8-16페이지의 8-8 유닛 식별 기능
IP 주소 표시 기능	설치 위치는 알지만 IP 주소를 잊어버린 유닛의 IP 주소를 확인합니다.	I/O 표시기를 사용하여 IP 주소 값을 표시합니다.	8-19페이지의 8-9 IP 주소 표시 기능
전원 감시 기능	전원 전압 또는 전원 전류 값이 정상 범위를 벗어났을 때 적절한 조치를 취할 수 있도록 합니다.	전원 전압 및 전원 전류 값을 확인합니다.	8-22페이지의 8-10 전원 감시 기능
I/O 감시 기능	해당 유닛의 동작을 확인하고 에러 원인을 파악하는 데 걸리는 시간을 단축합니다.	해당 유닛의 각 I/O 단자 값을 표시합니다.	8-27페이지의 8-11 I/O 감시 기능
접점 동작 횟수 감시 기능	해당 유닛의 유지보수 시기를 확인합니다.	해당 유닛의 세이프티 입력 단자 및 세이프티 출력 단자의 ON/OFF 횟수를 감시합니다.	8-29페이지의 8-12 접점 동작 횟수 감시 기능
통신 케이블 진단 기능	통신 에러의 원인을 파악하는 효율을 높입니다.	통신 케이블의 단선 또는 단락 여부를 확인합니다.	8-31페이지의 8-13 통신 케이블 진단 기능
펌웨어 업데이트 기능	해당 유닛에서 발견된 보안 취약점을 수정합니다.	해당 유닛의 펌웨어를 업데이트합니다.	8-35페이지의 8-14 펌웨어 업데이트 기능

AI 번역본
-For Reference Only-

8-2 전체 메모리 삭제 기능

전체 메모리 삭제 기능은 세이프티 I/O 블록의 모든 설정 데이터를 공장 출하 시 설정으로 되돌리는 데 사용합니다.

단, 다음 정보는 전체 메모리 삭제 대상에서 제외할 수 있습니다.

- IP 주소
- TUNID
- 세이프티 패스워드
- 이벤트 로그
- 로터리 스위치 설정 No.9~D의 애드온 애플리케이션

사용상의 주의

세이프티 I/O 블록을 폐기할 때는 정보 유출을 방지하기 위해 반드시 Web UI에서 전체 메모리 삭제 기능을 실행하십시오. Sysmac Studio를 사용한 전체 메모리 삭제에서는 이벤트 로그와 로터리 스위치 설정 No. 9~D의 애드온 애플리케이션을 삭제할 수 없습니다. 고장 등의 이유로 전체 메모리 삭제 기능을 실행할 수 없는 경우에는 오므론 담당자에게 문의하십시오.

8-2-1 전체 메모리 삭제 기능의 목적

전체 메모리 삭제 기능의 목적은 세이프티 I/O 블록의 설정 변경 시 설정을 공장 출하 시 상태로 복원하거나, 세이프티 I/O 블록을 폐기할 때 모든 설정 데이터를 삭제하는 것입니다.

8-2-2 전체 메모리 삭제 기능 사용 절차

전체 메모리 삭제 기능에는 Sysmac Studio를 사용하는 방법과 Web UI를 사용하는 방법이 있습니다.

사용상의 주의

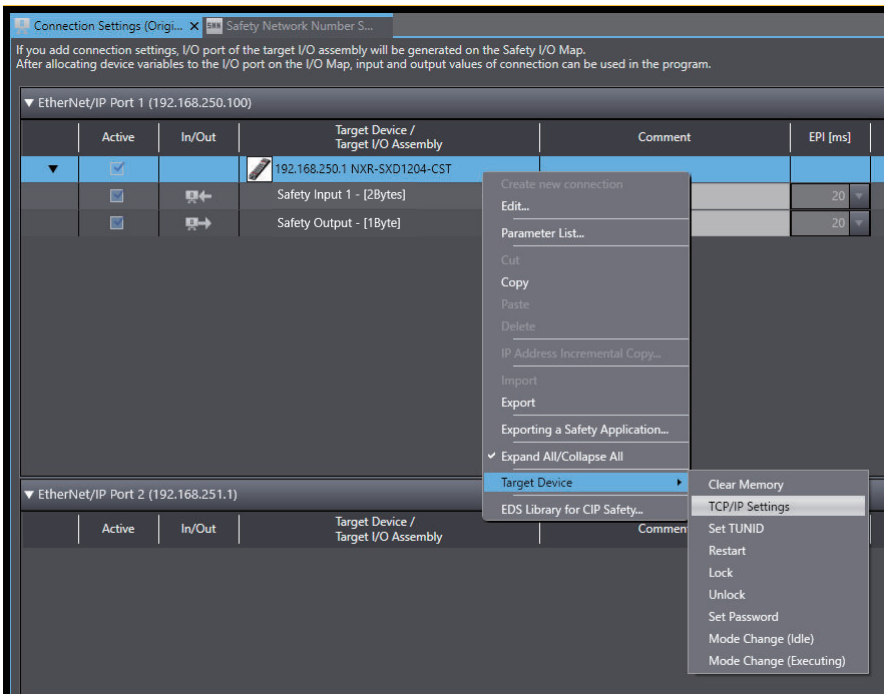
전체 메모리 삭제 기능을 실행하려면 컨피규레이션 잠금 기능을 사용하여 세이프티 I/O 블록을 잠금 해제 상태로 설정해야 합니다. 컨피규레이션 잠금 기능에 대한 자세한 내용은 7-99페이지의 7-17 컨피규레이션 잠금을 참조하십시오.

AI 번역본
-For Reference Only-

Sysmac Studio를 사용하는 절차

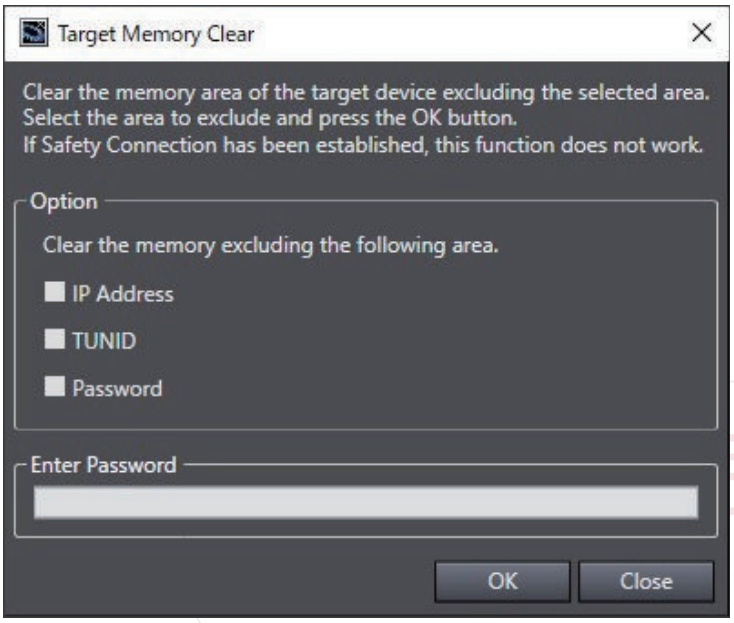
Sysmac Studio를 사용하는 절차는 다음과 같습니다.

1 커넥션 설정(오리지네이터)의 설정 화면에서 세이프티 I/O 블록을 마우스 오른쪽 버튼으로 클릭하고, 표시된 메뉴에서 Target Device를 클릭합니다.



2 **Clear Memory를 클릭합니다.**

다음 Target Memory Clear 창이 표시됩니다.



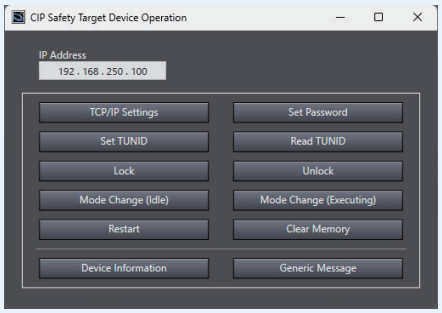
3 IP Address, TUNID, Password 중 삭제하지 않을 항목의 체크박스를 선택하고, Enter Password 상자에 세이프티 패스워드를 입력한 후 OK 버튼을 클릭합니다.

전체 메모리 삭제 기능이 실행됩니다.

추가 정보

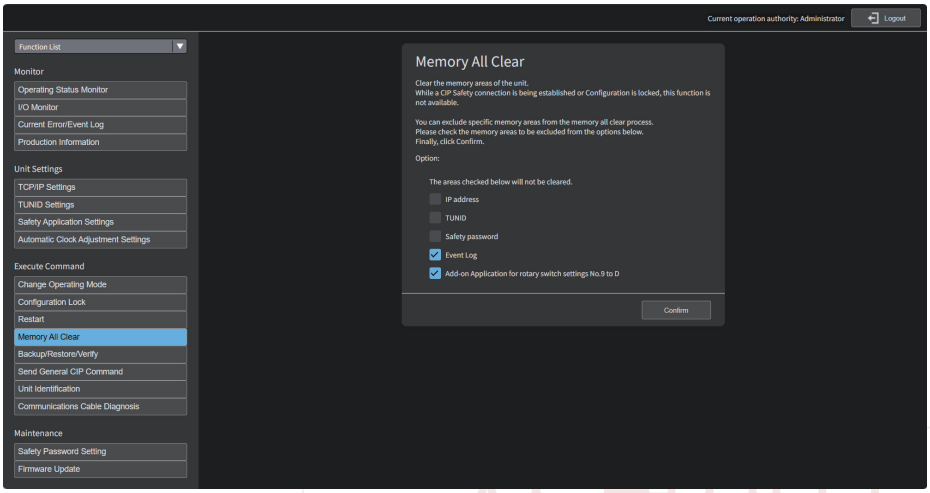
CIP Safety Target Device Operation 창에서도 실행할 수 있습니다.

1) Multiview Explorer에서 Safety PLC(초기 표시 new_SafetyCPU_0)를 선택하고, 화면 상단의 메뉴 바에서 Tools 메뉴의 CIP Safety Target Device Operation을 선택합니다.
2) 세이프티 I/O 블록의 IP Address에 설정되어 있는 IP 주소를 입력합니다.



Web UI를 사용하는 절차

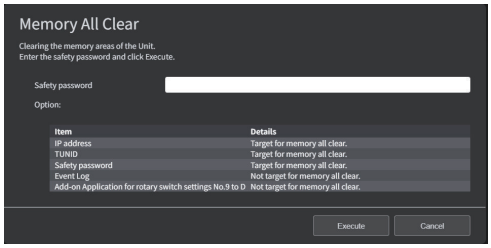
Web UI의 Memory All Clear 화면에서 세이프티 I/O 블록의 모든 설정을 삭제합니다.
이 화면의 설정은 관리자 권한이 있는 사용자만 설정할 수 있습니다.



AI 번역본
For Reference Only

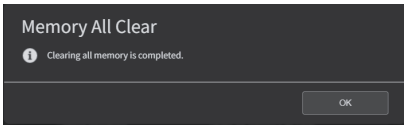
설정 절차는 다음과 같습니다.

1 메모리에서 삭제하지 않을 항목의 체크박스를 선택하고 Confirm 버튼을 클릭합니다. 다음 메시지가 표시됩니다.



2 세이프티 패스워드를 입력하고 Execute 버튼을 클릭합니다.

전체 메모리가 삭제되고 다음 화면이 표시됩니다.



3 OK 버튼을 클릭합니다.
Web UI에서 로그아웃합니다.

8-2-3 전체 메모리 삭제 기능 상세

전체 메모리 삭제 기능의 대상 데이터는 다음과 같습니다.
대상 데이터는 전체 메모리 삭제 기능을 Sysmac Studio에서 실행하는지 Web UI에서 실행하는지에 따라 다릅니다.

카테고리	설명	Sysmac Studio에서 실행	Web UI에서 실행
CIP Safety 통신 설정	IP 주소	대상(선택 가능)	대상(선택 가능)
	TUNID	대상(선택 가능)	대상(선택 가능)
	IP 주소 및 TUNID를 제외한 CIP Safety 통신 기본 설정	대상	대상
세이프티 애플리케이션 설정	사용자 정의 애플리케이션의 설정과 리모트 I/O 모드 애플리케이션의 I/O 컨피규레이션 설정	대상	대상
	애드온 애플리케이션의 설정	대상 아님	대상(선택 가능)
비세이프티 기능의 설정 데이터	EtherNet/IP 통신 설정, TCP/IP 설정, LINK 설정, Ethernet 포트 사용/미사용 설정, LLDP 기능 설정, 스루 배선 출력용 전원 차단 기능의 사용/미사용 설정, SNTP 설정	대상	대상
세이프티 패스워드	세이프티 패스워드	대상(선택 가능)	대상(선택 가능)
이벤트 로그	시스템 이벤트 로그 및 액세스 이벤트 로그	대상 아님	대상(선택 가능)

AI 번역본
-For Reference Only-

8-3 HTTPS 통신 기능

HTTPS 통신 기능은 Web UI 사용 시 PC와 세이프티 I/O 블록 간의 통신을 암호화합니다.
HTTPS 통신 기능을 사용하려면 사용 중인 PC의 웹 브라우저에 세이프티 I/O 블록의 Web 서버 인증서에 대한 CA 인증서를 설치해야 합니다. CA 인증서는 오므론 웹 사이트에서 다운로드하십시오.
한 번 설치하면 해당 PC에서 계속 HTTPS 통신 기능을 사용할 수 있습니다.

사용상의 주의

Web UI를 사용하는 방법에는 IP 주소를 입력하는 방법과 도메인 이름을 입력하는 방법이 있습니다. 도메인 이름을 입력하는 방법이 보안성이 가장 높습니다. 여기서 설명하는 내용은 도메인 이름을 입력하는 방법을 사용하기 위해 필요합니다. IP 주소를 입력하는 방법과 도메인 이름을 입력하는 방법에 대한 자세한 내용은 각각 7-21페이지의 Method to Enter an IP Address 및 7-22페이지의 Method to Enter Domain Name을 참조하십시오.

8-3-1 HTTPS 통신 기능의 목적

HTTPS 통신 기능의 목적은 PC와 세이프티 I/O 블록 간 통신 경로의 도청으로 인한 정보 유출을 방지하는 것입니다.

8-3-2 HTTPS 통신 기능 사용 절차

HTTPS 통신 기능을 사용하여 Web UI를 사용하는 절차는 다음과 같습니다.

1. 오므론 웹 사이트에서 CA 인증서를 다운로드합니다.
2. PC의 웹 브라우저에 CA 인증서를 설치합니다.
3. 생산 영역에 도메인 네임 서버를 설치하여 도메인 네임 서버로 이름 확인을 수행합니다. 이렇게 하면 사용자가 정의한 도메인 이름이 세이프티 I/O 블록의 IP 주소에 할당됩니다.

   도메인 이름은 *.NXR-SXD.local로 설정합니다.
   *에는 임의의 문자열을 입력하십시오. 단, 세이프티 I/O 블록의 IP 주소마다 다른 문자열을 설정하십시오. 다음 표는 도메인 이름의 예를 나타냅니다.

IP 주소	도메인 이름
192.168.250.1	device1.NXR-SXD.local
192.168.250.2	device2.NXR-SXD.local

4. 이더넷 케이블을 사용하여 세이프티 I/O 블록의 EtherNet/IP 포트와 PC의 이더넷 포트를 접속합니다.
5. PC의 웹 브라우저를 시작합니다.
6. 웹 브라우저에 3단계에서 할당한 도메인 이름을 입력합니다. 예를 들어 다음과 같은 도메인 이름을 입력합니다.
   https://device1.NXR-SXD.local
   Web UI가 시작됩니다.

AI 번역본
-For Reference Only-

1~3단계는 각 PC에서 한 번만 수행하면 됩니다. 이후에는
4단계부터의 절차만 수행하면 Web UI를 시작할 수 있습니다.

8-3-3 HTTPS 통신 기능 상세

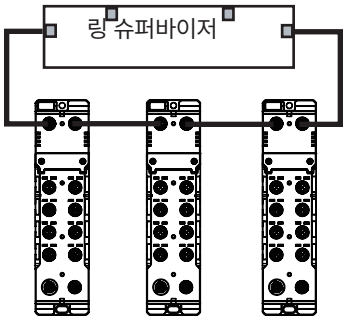
CA 인증서에는 유효기간이 있습니다. 유효기간이 만료되면 최신 CA 인증서를 다시 설치해야 합니다. CA 인증서의 다운로드처와 유효기간은 오므론 웹 사이트에서 확인하십시오.

세이프티 I/O 블록의 Web 서버 인증서에도 유효기간이 있습니다. 유효기간이 만료된 상태에서 웹 브라우저로 세이프티 I/O 블록에 액세스하면 NET::ERR_CERT_DATE_INVALID 에러 메시지가 표시됩니다.
서버 인증서는 펌웨어 업데이트 기능을 실행하여 업데이트할 수 있습니다. 펌웨어 업데이트 기능에 대한 자세한 내용은 8-35페이지의 8-14 펌웨어 업데이트 기능을 참조하십시오.

AI 번역본
-For Reference Only-

8-4 디바이스 레벨 링(DLR) 기능

디바이스 레벨 링(DLR) 기능은 다음과 같이 통신 케이블을 링 토폴로지로 접속하는 데 사용합니다.



8-4-1 DLR 기능의 목적

EtherNet/IP 네트워크의 통신 케이블이 끊어지면 일반적으로 끊어진 지점 이후의 유닛과의 통신을 수행할 수 없게 됩니다. DLR 기능의 목적은 통신 케이블이 한 곳에서 끊어져도 정상적인 통신을 유지할 수 있도록 하는 것입니다.
DLR 기능을 사용하려면 링 슈퍼바이저를 통해 통신 케이블을 링 토폴로지로 접속하십시오. 이렇게 하면 통신 케이블이 한 곳에서 끊어져도 반대 방향의 경로를 사용하여 통신을 유지할 수 있습니다.

8-4-2 DLR 기능 사용 절차

DLR 기능을 사용하는 데 특별한 설정은 필요하지 않습니다. 링 슈퍼바이저를 통해 통신 케이블을 링 토폴로지로 접속하기만 하면 DLR 기능을 사용할 수 있습니다.

8-4-3 DLR 기능 상세

DLR 기능을 사용하려면 비컨 기반 링 노드를 지원하는 링 슈퍼바이저가 필요합니다. 다음 표는 권장 링 슈퍼바이저 제품을 나타냅니다.

기기 종류	제조사	모델
매니지드 스위치	Rockwell Automation	Stratix 5400 switches
EtherNet/IP 탭	Rockwell Automation	1756-EN2TR

수출용 역본
-For Reference Only-

사용상의 주의

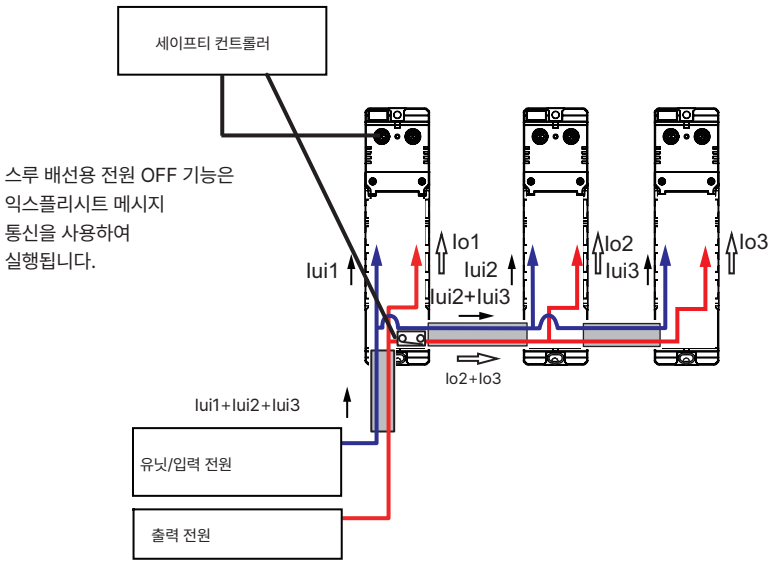
세이프티 I/O 블록을 링 노드로 사용할 때는 링 토폴로지의 링 노드 수가 128개 이하가 되도록 하십시오.

8-5 스루 배선 출력 전원 OFF 기능

스루 배선 출력 전원 OFF 기능은 출력 전원이 스루 배선으로 여러 유닛에 접속되어 있을 때, 해당 유닛보다 뒤쪽에 있는 유닛으로의 출력 전원 공급을 차단하는 데 사용합니다.

8-5-1 스루 배선 출력 전원 OFF 기능의 목적

스루 배선 출력 전원 OFF 기능의 목적은 사용 전력량을 절감하는 것입니다. 일반적으로 스루 배선으로 접속된 각 유닛으로의 출력 전원 공급은 세이프티 출력 단자의 출력이 ON인지 OFF인지에 관계없이 계속됩니다. 스루 배선 출력 전원 OFF 기능을 사용하면 해당 유닛보다 뒤쪽에 있는 유닛으로의 출력 전원 공급이 차단됩니다.



사용상의 주의

스루 배선 출력 전원 OFF 기능은 사용 전력량을 절감하기 위한 것이며, 세이프티 기능이 아닙니다. 설비의 안전은 다른 수단으로 확보하십시오.

8-5-2 스루 배선 출력 전원 OFF 기능 사용 절차

스루 배선용 전원 OFF 기능은 익스플리시트 메시지 통신을 사용하여 실행됩니다. 스루 배선용 전원 OFF 기능을 실행하기 위한 송신 커맨드는 다음과 같습니다.

구현 상세	송신 커맨드 항목	송신 커맨드 값
스루 배선 출력 전원	서비스 코드	10 hex (Set_Attribute_Single)
	Class ID	380 hex (Unit Manager object)
	Instance ID	01Hex
	Attribute ID	28 (Cross-Wiring Output Power Shut-off Control)
	Service data	TRUE: 스루 배선 출력 전원이 공급됩니다(기본값). FALSE: 스루 배선 출력 전원이 공급되지 않습니다.
	업데이트 타이밍	즉시
	재시작 시 동작	스루 배선 출력 전원이 공급됩니다.
스루 배선 출력용 전원 차단 기능을 사용/미사용으로 설정	Service code	10 hex (Set_Attribute_Single)
	Class ID	380 hex (Unit Manager object)
	Assembly Instance ID	01Hex
	Attribute ID	29 (Cross-Wiring Output Power Shut-off Enable)
	Service data	TRUE: 스루 배선 출력용 전원 차단 기능을 사용합니다(기본값). FALSE: 스루 배선 출력용 전원 차단 기능을 사용하지 않습니다.
	업데이트 타이밍	즉시
	재시작 시 동작	재시작 전 설정이 그대로 계속 사용됩니다.

익스플리시트 메시지를 통해 CIP 오브젝트에 액세스하는 방법에 대한 자세한 내용은 6-7페이지의 Explicit Message Server Function을 참조하십시오.

AI 번역본
-For Reference Only-

8-6 I/O 배선 점검 기능

I/O 배선 점검 기능은 세이프티 I/O 블록의 세이프티 I/O 단자로의 배선이 올바르게 이루어졌는지를 확인합니다.

8-6-1 I/O 배선 점검 기능의 목적

세이프티 I/O 블록의 세이프티 I/O 단자로의 배선을 잘못하면 중대한 사고로 이어질 수 있습니다. 그러나 일부 애플리케이션에서는 배선이 복잡해져 배선 점검이 쉽지 않은 경우가 있습니다.
I/O 배선 점검 기능의 목적은 세이프티 I/O 단자로의 배선을 확실하고 쉽게 점검할 수 있도록 하는 것입니다.

8-6-2 I/O 배선 점검 기능의 동작

I/O 배선 점검 기능의 세이프티 출력 단자 동작은 다음과 같습니다.
I/O 배선 점검 기능은 세이프티 입력 단자 Si00~Si03 및 세이프티 출력 단자 So00~So03의 동작을 확인할 수 있습니다. 세이프티 입력 단자 Si04~Si11의 동작은 세이프티 입력 표시기를 육안으로 확인하여 점검하십시오.

세이프티 출력 단자	동작
So00	Si00이 TRUE이고 인에이블 스위치가 눌려 있는 동안 TRUE입니다. 그 외에는 FALSE입니다.
So01	Si01이 TRUE이고 인에이블 스위치가 눌려 있는 동안 TRUE입니다. 그 외에는 FALSE입니다.
So02	Si02가 TRUE이고 인에이블 스위치가 눌려 있는 동안 TRUE입니다. 그 외에는 FALSE입니다.
So03	Si03이 TRUE이고 인에이블 스위치가 눌려 있는 동안 TRUE입니다. 그 외에는 FALSE입니다.

8-6-3 I/O 배선 점검 기능의 I/O 컨피규레이션 설정

I/O 배선 점검 기능은 세이프티 입력 단자 Si06 및 Si07에 접속된 인에이블 스위치를 눌러 I/O 배선 점검을 수행하는 것을 전제로 합니다. I/O 컨피규레이션 설정은 다음과 같습니다.

입력

입력	기기	Test Output Mode
Si00/T00	User-specified (single)	Power Supply Output
Si01/T01	User-specified (single)	Power Supply Output
Si02/T02	User-specified (single)	Power Supply Output
Si03/T03	User-specified (single)	Power Supply Output
Si04/T04	User-specified (single)	Power Supply Output
Si05/T05	User-specified (single)	Power Supply Output
Si06/T06	Enable switch (dual-channel equivalent input)	Test Output
Si07/T07	Enable switch (dual-channel equivalent input)	Test Output
Si08/T08	User-specified (single)	Power Supply Output
Si09/T09	User-specified (single)	Power Supply Output
Si10/T10	User-specified (single)	Power Supply Output
Si11/T11	User-specified (single)	Power Supply Output

AI 내용 For Reference Only-

출력

출력	기기
So00	Single channel (without test pulse)
So01	Single channel (without test pulse)
So02	Single channel (without test pulse)
So03	Single channel (without test pulse)

8-6-4 I/O 배선 점검 기능 사용 절차

I/O 배선 점검 기능 사용 절차는 다음과 같습니다.

1. 원하는 대로 세이프티 I/O 블록의 세이프티 I/O 단자에 배선을 접속합니다.
2. 세이프티 I/O 블록의 SETTING SW1 및 SW2 로터리 스위치를 모두 E로 설정한 후 전원을 켭니다.
3. 세이프티 I/O 블록의 세이프티 입력 단자에 임의로 입력합니다. 해당 세이프티 출력 단자에서 적절한 출력이 이루어지는지 확인합니다. 또한 I/O 표시기가 적절히 점등하는지도 확인합니다.

AI 번역본
-For Reference Only-

8-7 범용 CIP 커맨드 송신 기능

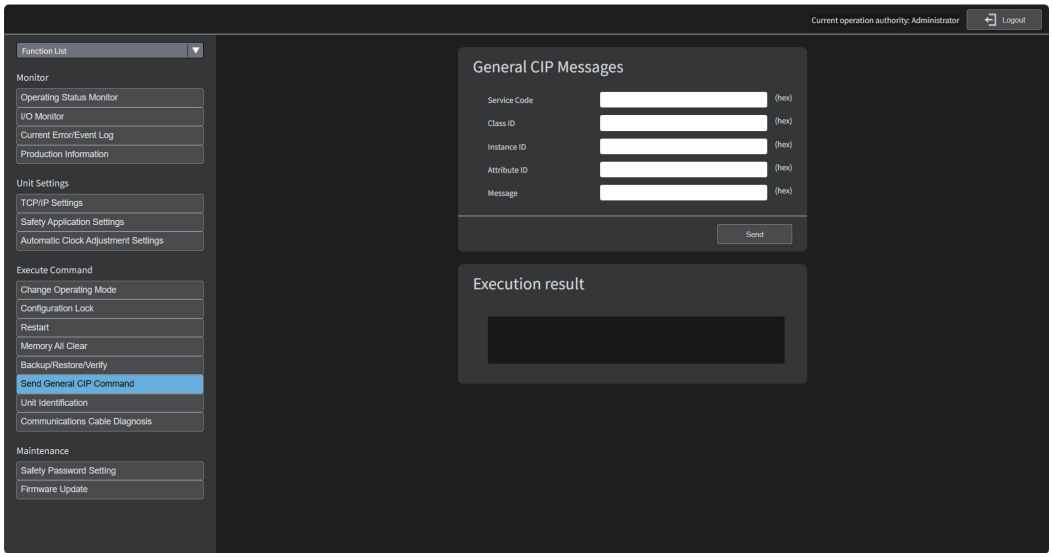
범용 CIP 커맨드 송신 기능은 세이프티 I/O 블록이 제공하는 CIP 오브젝트에 임의의 CIP 메시지 커맨드를 발행하는 데 사용합니다.

8-7-1 범용 CIP 커맨드 송신 기능의 목적

범용 CIP 커맨드 송신 기능의 목적은 전용 툴이나 Safety Network Configuration Tool(SNCT) 없이 세이프티 I/O 블록이 제공하는 CIP 오브젝트의 기능을 실행하는 것입니다.

8-7-2 범용 CIP 커맨드 송신 기능 사용 절차

Web UI의 Send General CIP Command 화면에서 CIP 메시지 커맨드를 발행합니다.
이 화면의 설정은 관리자 권한이 있는 사용자만 설정할 수 있습니다. CIP
오브젝트 사양에 대한 자세한 내용은 A-16페이지의 A-4 Supported CIP Objects를 참조하십시오.



설정 절차는 다음과 같습니다.

1 **Service Code, Class ID, Instance ID, Attribute ID, Message에 각 항목을 입력한 후 Send** 버튼을 클릭합니다.
해당 유닛으로 범용 CIP 커맨드가 송신됩니다.

2 **Execution result 필드를 확인합니다.**

AI 번역본
-For Reference Only-

8-8 유닛 식별 기능

유닛 식별 기능은 해당 유닛의 유닛 식별 표시기를 점멸시킵니다.

8-8-1 유닛 식별 기능의 목적

유닛 식별 기능의 목적은 여러 대의 세이프티 I/O 블록을 사용할 때 유닛 식별 표시기를 점멸시켜 현재 동작 중인 유닛을 식별할 수 있도록 하는 것입니다.

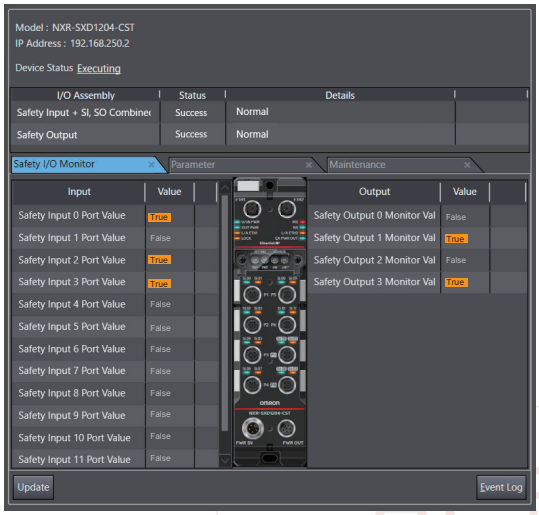
8-8-2 유닛 식별 기능 사용 절차

유닛 식별 기능에는 Sysmac Studio를 사용하는 방법과 Web UI를 사용하는 방법이 있습니다.

Sysmac Studio를 사용하는 절차

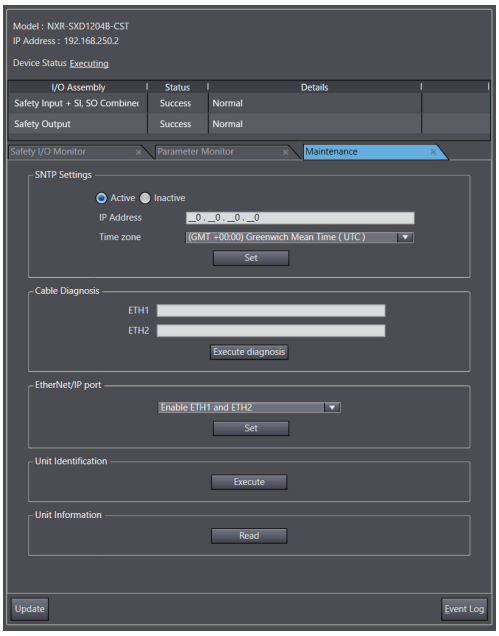
Sysmac Studio를 사용하는 절차는 다음과 같습니다.

1 Sysmac Studio의 CIP Safety Monitor 화면에서 세이프티 I/O 블록을 선택합니다.
다음 화면이 표시됩니다.



2 Maintenance 탭을 선택합니다.
다음 화면이 표시됩니다.

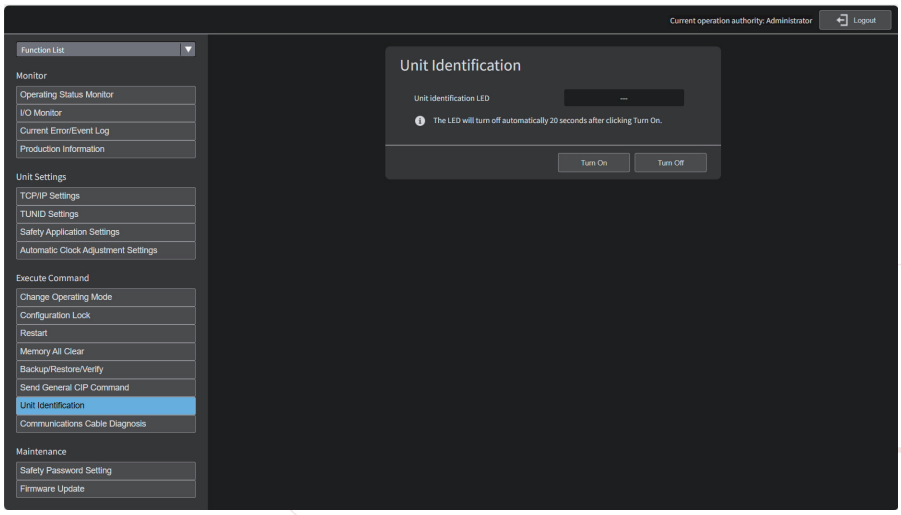
AI 번역본
For Reference Only-



3 **Unit Identification의 Execute 버튼을 클릭합니다.**
지정한 유닛의 유닛 식별 표시기가 점멸합니다.

Web UI를 사용하는 절차

Web UI의 Unit Identification 화면은 동작 중인 유닛의 유닛 식별 표시기를 점멸시키는 데 사용합니다.



설정 절차는 다음과 같습니다.

1 Turn On 버튼을 클릭합니다.
해당 유닛에서 유닛 식별 기능이 실행되고 유닛 식별 표시기가 점멸합니다. Unit identification LED 필드에 Lit가 표시됩니다.

2 Turn Off 버튼을 클릭합니다.
유닛 식별 기능이 정지하고 유닛 식별 표시기가 꺼집니다. Unit identification LED **필드에 Not lit가 표시됩니다.**

Turn Off 버튼을 클릭하지 않아도 Turn On 버튼을 클릭한 후 60초가 지나면 유닛 식별 표시기가 자동으로 꺼집니다.

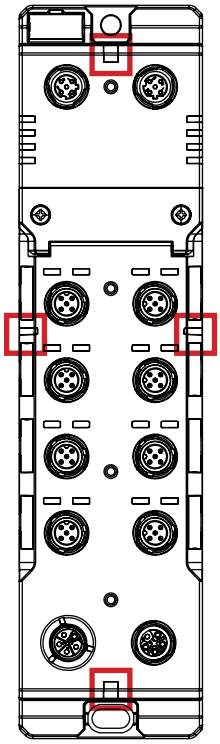
8-8-3 유닛 식별 기능 상세

유닛 식별 기능이 실행되면 다음 그림의 네 곳에 있는 유닛 식별 표시기가 점멸합니다.

・각 표시기가 시계 방향으로 100ms씩 순차적으로 점등하며, 이 동작이 4회 반복됩니다.

・그 후 네 곳의 표시기가 모두 500ms 동안 꺼집니다.

・위 동작이 60초 동안 반복됩니다.



AI 번역본
-For Reference Only-

8-9 IP 주소 표시 기능

IP 주소 표시 기능은 유닛의 I/O 표시등으로 Sysmac Studio 또는 Web UI에서 설정한 세이프티 I/O 블록의 IP 주소를 표시하는 데 사용합니다.

8-9-1 IP 주소 표시 기능의 목적

IP 주소 표시 기능의 목적은 Support Software와 같은 특수한 도구를 사용하지 않고도 Sysmac Studio 또는 Web UI에서 설정한 세이프티 I/O 블록의 IP 주소를 확인할 수 있도록 하는 것입니다.

8-9-2 IP 주소 표시 기능 사용 절차

이 절에서는 IP 주소 표시 기능을 사용하는 절차에 대해 설명합니다.

1 해당 유닛을 네트워크에서 분리합니다.

2 SETTING 로터리 스위치 SW1과 SW2를 모두 8로 설정합니다.

3 유닛을 재시작합니다.
IP 주소를 표시하기 위해 I/O 표시등이 점등하기 시작합니다.

8-9-3 IP 주소 표시 기능 상세

IP 주소는 첫 번째 옥텟, 두 번째 옥텟, 세 번째 옥텟, 네 번째 옥텟의 순서로 표시됩니다. 각 옥텟을 나타내는 I/O 표시등은 다음과 같습니다. 먼저 첫 번째 옥텟의 I/O 표시등이 9.5초 동안 점등합니다.
같은 과정이 두 번째 옥텟, 세 번째 옥텟, 네 번째 옥텟의 I/O 표시등에 대해 순서대로 실행됩니다.

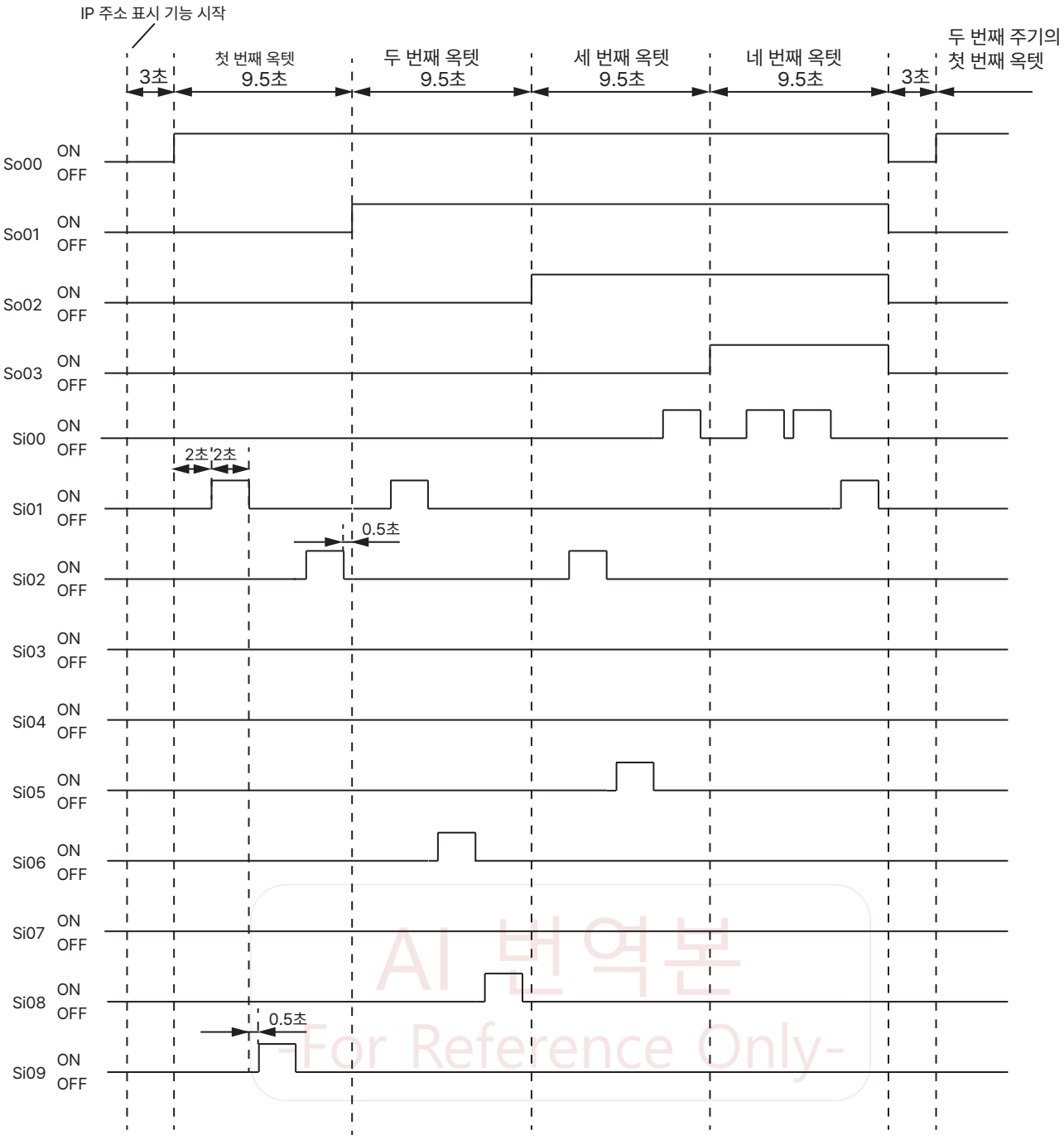
옥텟	I/O 표시등
첫 번째 옥텟	So00
두 번째 옥텟	So00 ~ So01
세 번째 옥텟	So00 ~ So02
네 번째 옥텟	So00 ~ So03

각 옥텟의 세 자리 숫자는 각 자리를 순서대로 2초씩 점등하여 표시합니다. 각 표시등 점등 사이에는 0.5초 동안 표시등이 꺼집니다. 각 숫자를 나타내는 I/O 표시등은 다음과 같습니다.

숫자	I/O 표시등
0	Si00
1	Si01
2	Si02
3	Si03
4	Si04
5	Si05
6	Si06
7	Si07
8	Si08
9	Si09

AI 번역본
-For Reference Only-

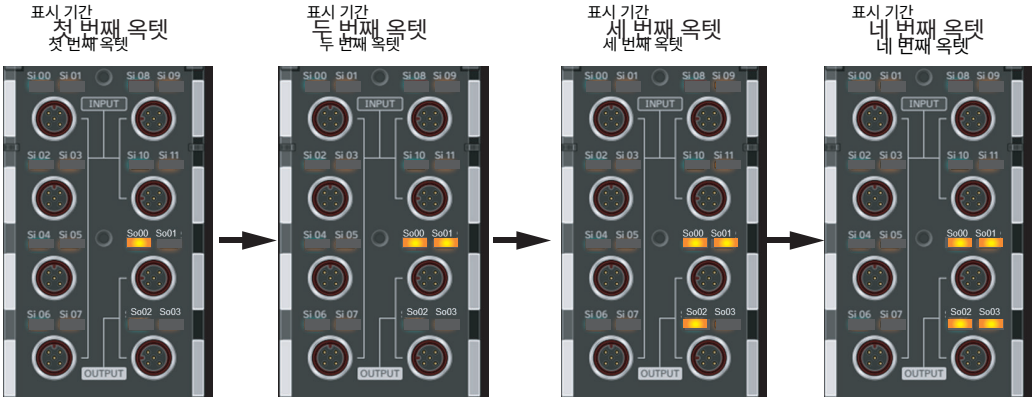
IP 주소 표시 기능이 시작된 후 3초 뒤에 첫 번째 옥텟의 점등이 시작됩니다. 또한 첫 번째 옥텟의 점등이 시작된 후 2초 뒤에 첫 번째 옥텟의 첫째 자리의 점등이 시작됩니다.
예를 들어 다음은 IP 주소 192.168.250.001을 표시할 때의 I/O 표시등 타이밍 차트를 나타냅니다.



로터리 스위치 값이 변경될 때까지 같은 과정이 반복됩니다.

첫 번째 옥텟부터 네 번째 옥텟까지를 표시하는 I/O 표시등의 실제 상태는 다음과 같습니다. 이 그림은 NXR-SXD1204-CST의 경우를 나타냅니다.

AI 번역본
-For Reference Only-



AI 번역본
-For Reference Only-

8-10 전원 공급 모니터 기능

전원 공급 모니터 기능은 세이프티 I/O 블록의 전원 전압값과 전원 전류값을 확인하는 데 사용합니다.

8-10-1 전원 공급 모니터 기능의 목적

세이프티 I/O 블록이 정상적으로 동작하려면 전원 전압값과 전원 전류값이 모두 정상 범위 내에 있어야 합니다. 전원 공급 모니터 기능의 목적은 전원 전압값과 전원 전류값이 정상 범위 내에 있는지 확인하여, 정상 범위를 벗어났을 때 적절한 조치를 취할 수 있도록 하는 것입니다.

8-10-2 전원 공급 모니터 기능 사용 절차

전원 공급 모니터 기능으로 다음 값을 확인할 수 있습니다.

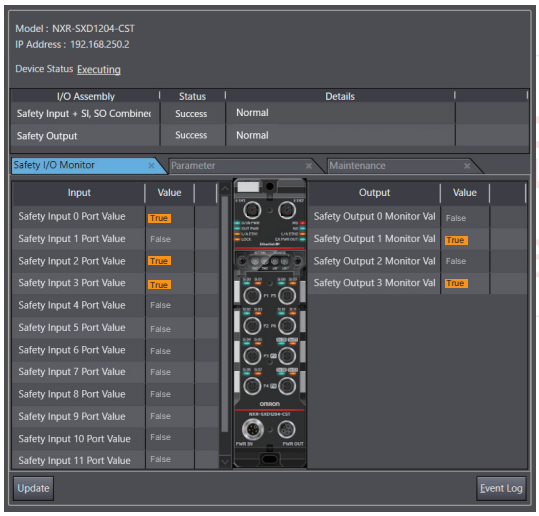
- 유닛/입력 전원 전압
- 출력 전원 전압
- 유닛/입력 전원 전류
- 출력 전원 전류

전원 공급 모니터 기능에는 Sysmac Studio를 사용하는 방법과 Web UI를 사용하는 방법이 있습니다.

Sysmac Studio를 사용하는 절차

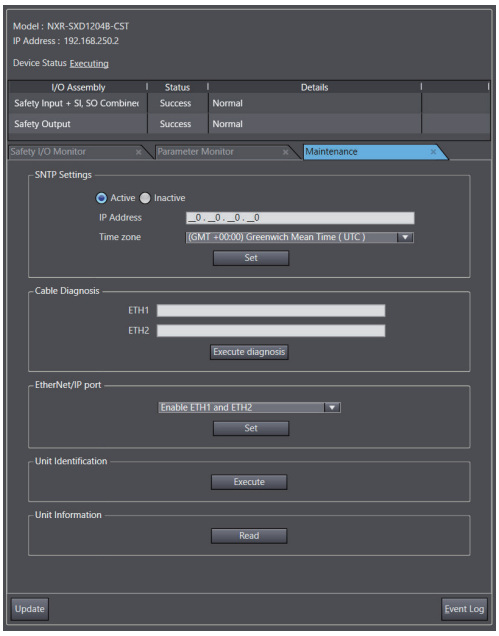
Sysmac Studio를 사용하는 절차는 다음과 같습니다.

1 Sysmac Studio의 CIP Safety Monitor 화면에서 세이프티 I/O 블록을 선택합니다.
다음 화면이 표시됩니다.

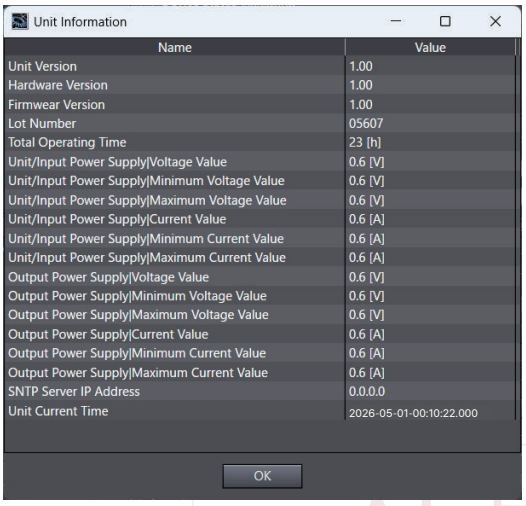


번 역본
erence Only-

2 Maintenance 탭을 선택합니다.
다음 화면이 표시됩니다.



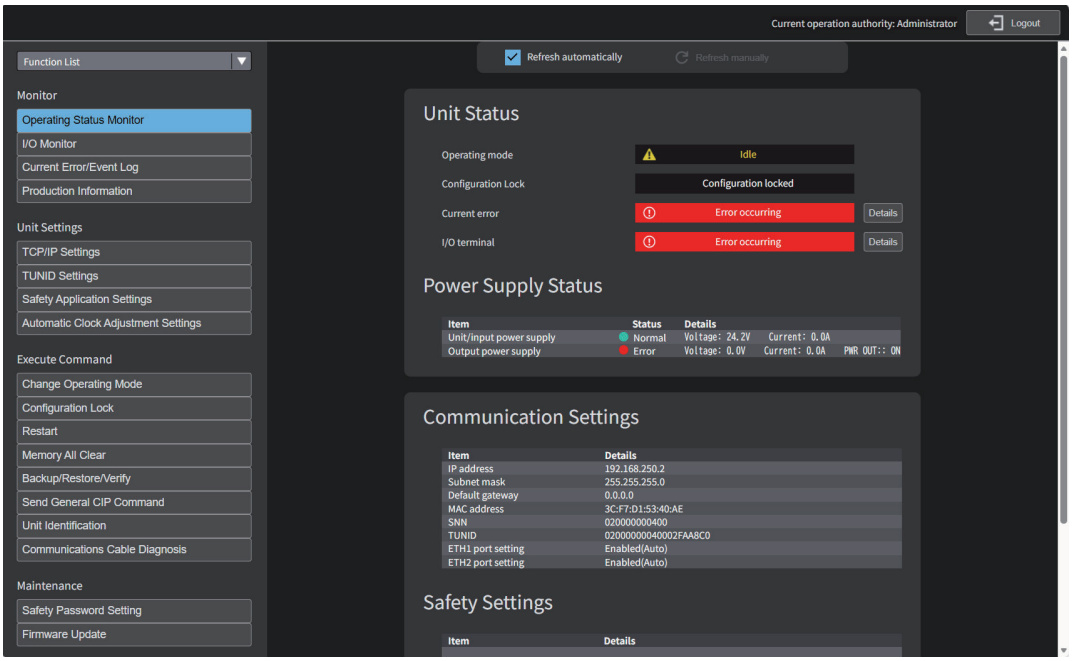
3 **Unit Information의 Read 버튼을 클릭합니다.**
다음 화면이 표시됩니다.



AI 번역본
For Reference Only-

Web UI를 사용하는 절차

Web UI의 Operating Status Monitor 화면에서 해당 유닛의 유닛 상태와 전원 공급 상태를 확인합니다.



8-10-3 전원 공급 모니터 기능 상세

전원 공급 모니터 기능에는 전원 전압 모니터와 전원 전류 모니터가 있습니다.

전원 전압 모니터링

전원 전압을 모니터링합니다. 유닛/입력 전원 전압과 출력 전원
전압의 상태는 U/IN PWR 표시등과 OUT PWR 표시등으로 확인할 수 있습니다. 전압 이상이 발생하면 이벤트가 발생합니다.
전원 전압이 허용 범위를 초과하면 전원 입력이 자동으로 차단됩니다.

● 유닛/입력 전원 전압

다음 표는 유닛/입력 전원 전압값과 표시등 상태, 모니터링 가능한 값,
이벤트 발생 여부, 복구 방법의 관계를 나타냅니다.

전압값 [V]	상태	U/IN PWR 표시등	모니터링 가능한 값	이벤트	복구 방법
0에서 저전압 검출 임계값까지	저전압 검출에 의한 전원 차단 *1	소등	모니터링할 수 없음.	이벤트가 발생하지 않습니다.	적절한 값으로 전원을 공급하십시오.
저전압 검출 임계값에서 19.2까지	사양 범위를 벗어난 전압	점등	전압값	유닛/입력 전원 사양 범위를 벗어난 전압 검출	적절한 값으로 전원을 공급하십시오.
19.2 ~ 28.8	정상 전압	점등	전압값	이벤트가 발생하지 않습니다.	복구가 필요하지 않습니다.

전압값 [V]	상태	U/IN PWR 표시 등	모니터링 가능한 값	이벤트	복구 방법
28.8에서 과전압 검출 임계값까지	사양 범위를 벗어난 전압	점등	전압값	유닛/입력 전원 사양 범위를 벗어난 전압 검출	적절한 값으로 전원을 공급하십시오.
과전압 검출 임계값을 초과하는 전압	과전압 검출에 의한 전원 차단 *2	소등	모니터링할 수 없음.	이벤트가 발생하지 않습니다.	적절한 값으로 전원을 공급한 후 재시작하십시오.

***1.** 유닛 내부 회로의 전원이 차단됩니다. 전원 공급 커넥터(출력)로부터의 유닛/입력 전원 공급은 차단되지 않습니다. 전원 공급 커넥터(출력)로부터의 출력 전원 공급은 차단됩니다.

***2.** 유닛 내부 회로의 전원이 차단됩니다. 전원 공급 커넥터(출력)로부터의 유닛/입력 전원 공급은 검출 전압에 따라 차단되거나 유지될 수 있습니다. 전원 공급 커넥터(출력)로부터의 출력 전원 공급은 차단됩니다.

● 출력 전원 전압

다음 표는 출력 전원 전압값과 표시등 상태, 모니터링 가능한 값, 이벤트 발생 여부, 복구 방법의 관계를 나타냅니다.

전압값 [V]	상태	OUT PWR 표시 등	모니터링 가능한 값	이벤트	복구 방법
0에서 저전압 검출 임계값까지	저전압 검출에 의한 전원 차단 *1 모든 세이프티 출력이 OFF	소등	전압 값	출력 전원 공급 에러	적절한 값으로 전원을 공급하십시오.
저전압 검출 임계값에서 19.2까지	사양 범위를 벗어난 전압	점등	전압 값	출력 전원 공급 사양 범위를 벗어난 전압 검출	적절한 값으로 전원을 공급하십시오.
19.2 ~ 28.8	정상 전압	점등	전압 값	이벤트가 발생하지 않습니다.	복구가 필요하지 않습니다.
28.8에서 과전압 검출 임계값까지	사양 범위를 벗어난 전압	점등	전압 값	출력 전원 공급 사양 범위를 벗어난 전압 검출	적절한 값으로 전원을 공급하십시오.
과전압 검출 임계값을 초과하는 전압	과전압 검출에 의한 전원 차단 *2 모든 세이프티 출력이 OFF	소등	전압 값	출력 전원 공급 에러	적절한 값으로 전원을 공급한 후 재시작하십시오.

***1.** 유닛 내부 회로의 전원이 차단됩니다. 전원 공급 커넥터(출력)로부터의 출력 전원 공급은 차단되지 않습니다.

***2.** 유닛 내부 회로의 전원이 차단됩니다. 전원 공급 커넥터(출력)로부터의 출력 전원 공급은 검출 전압에 따라 차단되거나 유지될 수 있습니다.

AI 번역본
For Reference Only

전원 전류 모니터링

전원 전류를 모니터링합니다. 전원이 차단되는 과전류 이상이 발생하면 이벤트가 발생합니다. 전원 전류가 허용값을 초과하면 전원 입력이 자동으로 차단됩니다.

● 유닛/입력 전원 전류

다음 표는 유닛/입력 전원 전류값과 모니터링 가능한 값, 이벤트 발생 여부, 복구 방법의 관계를 나타냅니다.

전류값 [A]	상태	모니터링 가능한 값	이벤트	복구 방법
0 ~ 9	정상 전류	전류값	이벤트가 발생하지 않습니다	복구가 필요하지 않습니다.
9에서 과전류 검출 임계값까지	사양 범위를 벗어난 전류	전류값	유닛/입력 전원 공급 사양 범위를 벗어난 전류 검출	적절한 값으로 전원을 공급하십시오.
과전류 검출 임계값을 초과하는 전류	과전류 검출에 의한 전원 차단 *1	모니터링할 수 없습니다.	이벤트가 발생하지 않습니다.	적절한 값으로 전원을 공급한 후 재시작하십시오.

***1.** 유닛 내부 회로의 전원이 차단됩니다. 전원 공급 커넥터(출력)로부터의 유닛/입력 전원 공급과 출력 전원 공급이 차단됩니다.

● 출력 전원 전류

다음 표는 출력 전원 전류값과 모니터링 가능한 값, 이벤트 발생 여부, 복구 방법의 관계를 나타냅니다.

전류값 [A]	상태	모니터링 가능한 값	이벤트	복구 방법
0 ~ 9	정상 전류	전류값	이벤트가 발생하지 않습니다.	복구가 필요하지 않습니다.
9에서 과전류 검출 임계값까지	사양 범위를 벗어난 전류	전류값	출력 전원 공급 사양 범위를 벗어난 전류 검출	적절한 값으로 전원을 공급하십시오.
과전류 검출 임계값을 초과하는 전류	과전류 검출에 의한 전원 차단 *1 모든 세이프티 출력이 OFF	전류값	출력 전원 공급 에러	적절한 값으로 전원을 공급한 후 재시작하십시오.

***1.** 유닛 내부 회로의 전원이 차단됩니다. 전원 공급 커넥터(출력)로부터의 출력 전원 공급이 차단됩니다.

AI 번역본 For Reference Only

8-11 I/O 모니터 기능

I/O 모니터 기능은 I/O 단자의 값을 표시합니다.

8-11-1 I/O 모니터 기능의 목적

세이프티 I/O 블록의 동작을 확인하거나 에러의 원인을 파악할 때, 세이프티 I/O 데이터의 상태를 확인하는 것이 유용합니다. I/O 모니터 기능의 목적은 세이프티 I/O 데이터를 확인하여 세이프티 I/O 블록의 동작을 확인하고 에러의 원인을 파악하는 데 걸리는 시간을 단축하는 것입니다.

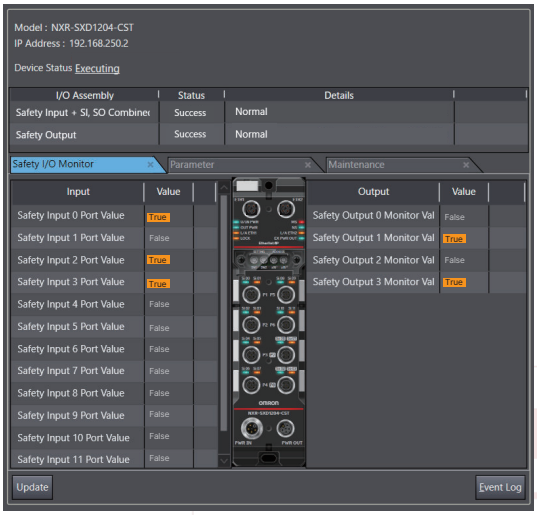
8-11-2 I/O 모니터 기능 사용 절차

I/O 모니터 기능에는 Sysmac Studio를 사용하는 방법과 Web UI를 사용하는 방법이 있습니다.

Sysmac Studio를 사용하는 절차

Sysmac Studio를 사용하는 절차는 다음과 같습니다.

1 Sysmac Studio의 CIP Safety Monitor 화면에서 세이프티 I/O 블록을 선택합니다.
다음 화면이 표시됩니다.

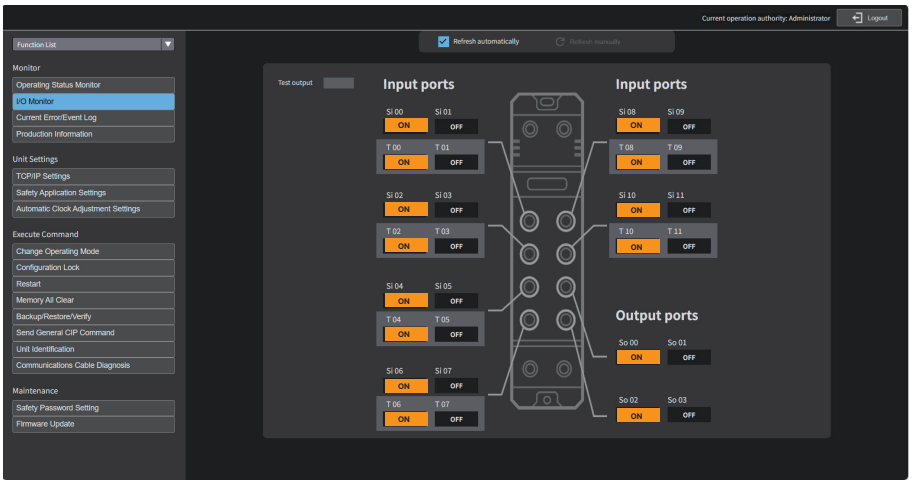


검토용 역본
-For Reference Only-

2 **Safety I/O Monitor 탭을 선택합니다.**
세이프티 I/O 출력 데이터의 값이 표시됩니다.

Web UI를 사용하는 절차

Web UI의 I/O Monitor 화면에서 I/O 단자의 값을 확인합니다.



AI 번역본
-For Reference Only-

8-12 접점 동작 횟수 모니터 기능

접점 동작 횟수 모니터 기능은 접점 동작 횟수(단위: 회)를 확인하는 데 사용합니다.
이 기능은 세이프티 입력 단자와 세이프티 출력 단자가 ON/OFF로 전환되는 횟수를 카운트하고,
그 결과를 현재 카운트값으로 유지합니다.
이 값은 CIP 메시지 통신(익스플리시트 메시지 통신)을 통해 현재 카운트값으로
취득됩니다.
또한 현재 카운트값을 클리어할 수도 있습니다.

8-12-1 접점 동작 횟수 모니터 기능의 목적

접점 동작 횟수 모니터 기능의 목적은 접점 동작 횟수를 모니터링하여
유지보수 시기를 확인하는 것입니다.

추가 정보

임계값에 도달하거나 임계값을 초과했을 때 알리는 기능은 아닙니다.

8-12-2 세이프티 입력 단자에서 사용하는 절차

CIP 메시지 통신(익스플리시트 메시지 통신)을 사용하여 세이프티 입력 단자에 대한 접점 동작
횟수 모니터 기능을 실행합니다.
전송할 명령은 다음과 같습니다.

구현 내용	전송 명령 항목	전송 명령값
세이프티 입력 단자의 현재 카운트값 취득	서비스 코드	0E hex (Get_Attribute_Single)
	클래스 ID	3D hex (Safety Discrete Input Point (SDIP) 오브젝트)
	인스턴스 ID	01 hex ~ 0C hex (각 세이프티 입력 단자의 인스턴스를 지정합니다.)
	어트리뷰트 ID	102 (Maintenance Counter)
세이프티 입력 단자의 현재 카운트값 클리어	서비스 코드	10 hex (Set_Attribute_Single)
	클래스 ID	3D hex (Safety Discrete Input Point (SDIP) 오브젝트)
	인스턴스 ID	01 hex ~ 0C hex (각 세이프티 입력 단자의 인스턴스를 지정합니다.)
	어트리뷰트 ID	102 (Maintenance Counter)
	서비스 데이터	00000000 hex (값을 클리어하려면 0을 씁니다.)

AI 번역본
-For Reference Only-

CIP 메시지 통신(익스플리시트 메시지 통신) 사용 절차는 6-7페이지의 익스플리시트 메시지 서버 기능을
참조하십시오.

8-12-3 세이프티 출력 단자에서 사용하는 절차

CIP 메시지 통신(익스플리시트 메시지 통신)을 사용하여 세이프티 출력 단자에 대한 접점 동작
횟수 모니터 기능을 실행합니다.
전송할 명령은 다음과 같습니다.

구현 내용	전송 명령 항목	전송 명령값
세이프티 출력 단자의 현재 카운트값 취득	서비스 코드	0E hex (Get_Attribute_Single)
	클래스 ID	3B hex (Safety Discrete Output Point (SDOP) 오브젝트)
	인스턴스 ID	01 hex ~ 04 hex (각 세이프티 출력 단자의 인스턴스를 지정합니다.)
	어트리뷰트 ID	102 (Maintenance Counter)
세이프티 출력 단자의 현재 카운트값 클리어	서비스 코드	10 hex (Set_Attribute_Single)
	클래스 ID	3B hex (Safety Discrete Output Point (SDOP) 오브젝트)
	인스턴스 ID	01 hex ~ 04 hex (각 세이프티 출력 단자의 인스턴스를 지정합니다.)
	어트리뷰트 ID	102 (Maintenance Counter)
	서비스 데이터	00000000 hex (값을 클리어하려면 0을 씁니다.)

CIP 메시지 통신(익스플리시트 메시지 통신) 사용 절차는 6-7페이지의 익스플리시트 메시지 서버 기능을 참조하십시오.

AI 번역본
-For Reference Only-

8-13 통신 케이블 진단 기능

통신 케이블 진단 기능은 통신 에러가 발생했을 때 그 원인이 통신 케이블의 단선인지 단락인지 확인하는 데 사용합니다. 또한 단선 또는 단락이 발생한 위치의 추정값도 확인할 수 있습니다.

8-13-1 통신 케이블 진단 기능의 목적

EtherNet/IP 포트 1과 포트 2를 사용하는 통신에서 통신 에러가 발생하는 원인은 여러 가지가 있을 수 있습니다. 통신 케이블 진단 기능의 목적은 통신 에러의 원인을 확인하는 것입니다.

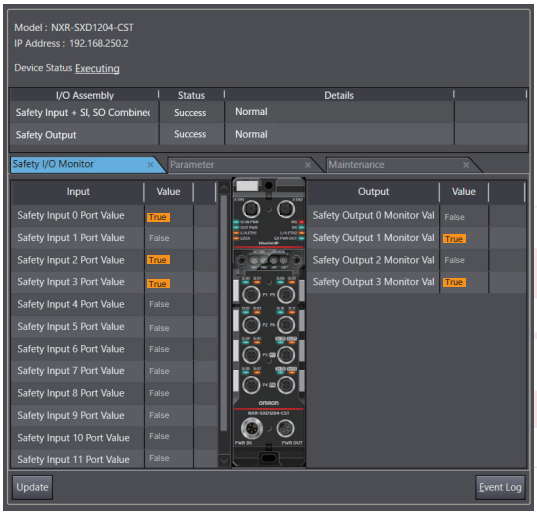
8-13-2 통신 케이블 진단 기능 사용 절차

통신 케이블 진단 기능에는 Sysmac Studio를 사용하는 방법, Web UI를 사용하는 방법, 익스플리시트 메시지 통신을 사용하는 방법이 있습니다.

Sysmac Studio를 사용하는 절차

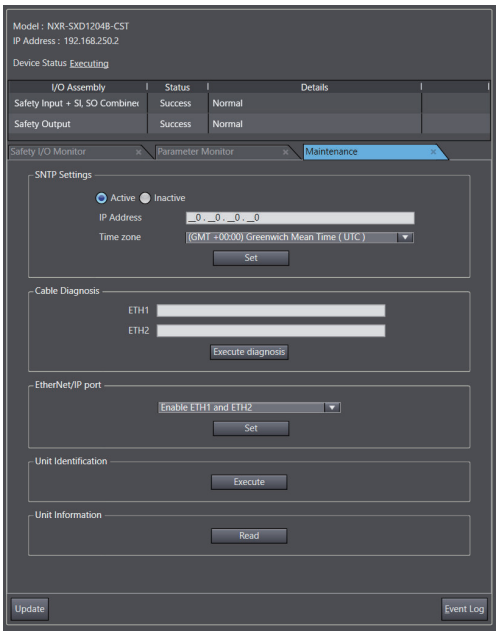
Sysmac Studio를 사용하는 절차는 다음과 같습니다.

1 Sysmac Studio의 CIP Safety Monitor 화면에서 세이프티 I/O 블록을 선택합니다.
다음 화면이 표시됩니다.



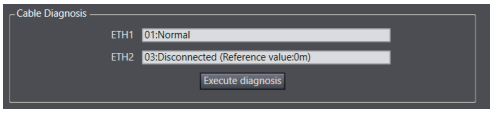
2 Maintenance 탭을 선택합니다.
다음 화면이 표시됩니다.

번 역본
rence Only-



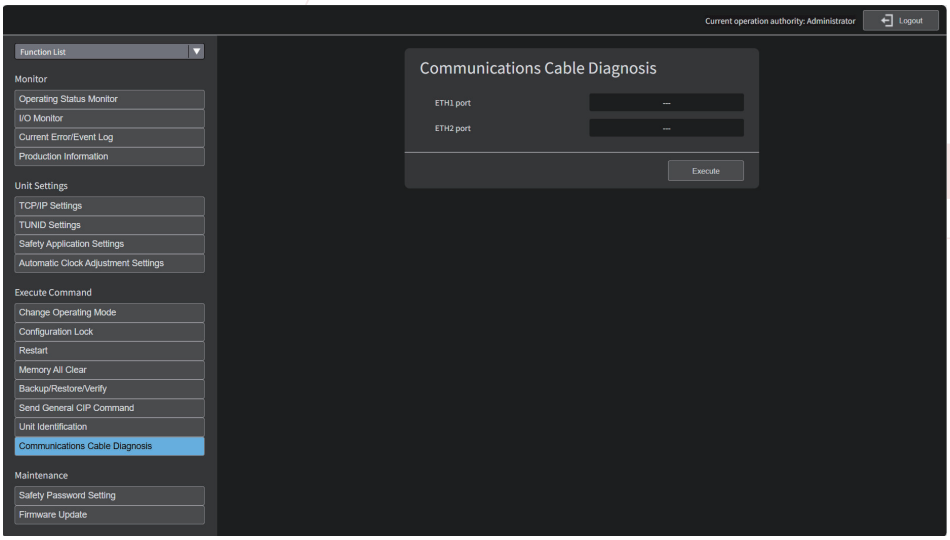
3 **Cable Diagnosis의 Execute diagnosis 버튼을 클릭합니다.**

포트 1과 포트 2에 대해 케이블이 정상인지 단선인지가 표시됩니다. 케이블이 단선된 경우 유닛에서 통신 케이블이 단선된 위치까지의 거리에 대한 참고값도 표시됩니다.



Web UI를 사용하는 절차

Web UI의 Communications Cable Diagnosis 화면은 EtherNet/IP 통신 케이블이 단선되었는지 단락되었는지 확인하는 데 사용합니다.



Execute 버튼을 클릭하면 EtherNet/IP 포트 1의 진단 결과가 ETH1 port 필드에 표시되고,
EtherNet/IP 포트 2의 진단 결과가 ETH2 port 필드에 표시됩니다.
다음 결과 중 하나가 표시됩니다.

- 01: Normal
- 02: Short-circuit (참고값: □m) □는 수치입니다.
- 03: Disconnection (참고값: □m) □는 수치입니다.
- 04: Port disabled
- F1: Diagnosing
- F2: Failed to read
- F3: Other diagnosis error

익스플리시트 메시지 통신을 사용하는 절차

통신 케이블 진단 실행 및 진단 결과 취득을 위해 전송할 명령은 다음과 같습니다.

구현 내용	전송 명령 항목	전송 명령값
통신 케이블 진단 실행	서비스 코드	3A hex (Exec_Cable_Diagnosis)
	클래스 ID	F6 hex (Ethernet Link 오브젝트)
	인스턴스 ID	01 hex: Port1 02 hex: Port2
통신 케이블 진단 결과	서비스 코드	0E hex (Get_Attribute_Single)
	클래스 ID	F6 hex (Ethernet Link 오브젝트)
	인스턴스 ID	01 hex: Port1 02 hex: Port2
	어트리뷰트 ID	100 (Communication Cable Diagnosis)
	응답 데이터	A-50페이지의 Values of Communication Cable Diagnosis를 참조하십시오.

익스플리시트 메시지 통신 사용 절차는 6-7페이지의 익스플리시트 메시지 서버 기능을
참조하십시오.

8-13-3 통신 케이블 진단 기능 상세

통신 케이블 진단 기능에는 다음과 같은 제한 사항이 있습니다.

- 링크가 확립된 포트의 진단 결과는 항상 정상입니다.
- 통신 케이블의 송신선과 수신선이 단락된 경우 단선을 검출할 수 없습니다. 진단 결과는 정상입니다.
- 접속 타임아웃이 발생하거나 접속을 확립할 수 없는 경우, 그 원인이 통신 케이블의 전송 특성에 의한 것이면 진단 결과가 정상으로 표시될 수 있습니다.

-For Reference Only-

통신 케이블 진단 기능을 실행하기 위한 네트워크 토폴로지와 PC의 접속 구성은 다음과 같은
관계가 있습니다. 네트워크 토폴로지에 대한 자세한 내용은 1-13페이지의
1-3-2 네트워크 토폴로지를 참조하십시오.

네트워크 토폴로지	PC의 접속 구성
라인 또는 링	Ethernet 스위치에 접속

네트워크 토폴로지	PC의 접속 구성
스타 또는 트리	미사용 세이프티 I/O 블록의 Ethernet 포트에 접속

AI 번역본
-For Reference Only-

8-14 펌웨어 업데이트 기능

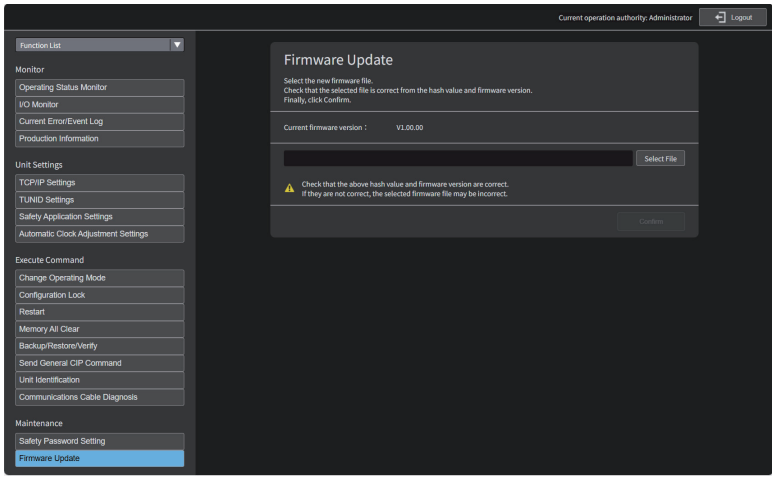
펌웨어 업데이트 기능은 세이프티 I/O 블록의 통신 기능 및 세이프티 기능과 관련된 펌웨어를 업데이트합니다.
최신 펌웨어 파일 취득 방법에 대한 자세한 내용은 OMRON 웹사이트를 확인하십시오.

8-14-1 펌웨어 업데이트 기능의 목적

펌웨어 업데이트 기능의 목적은 세이프티 I/O 블록의 보안 취약점을 수정하는 것입니다.

8-14-2 펌웨어 업데이트 기능 사용 절차

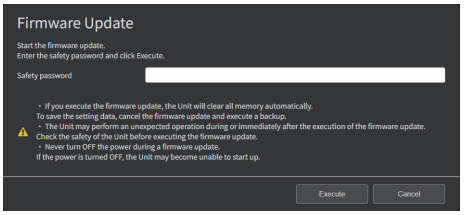
펌웨어 업데이트 기능은 Web UI의 Firmware Update 화면을 사용하여 실행합니다.
이 화면의 설정은 관리자 권한이 있는 사용자만 구성할 수 있습니다.



설정 절차는 다음과 같습니다.

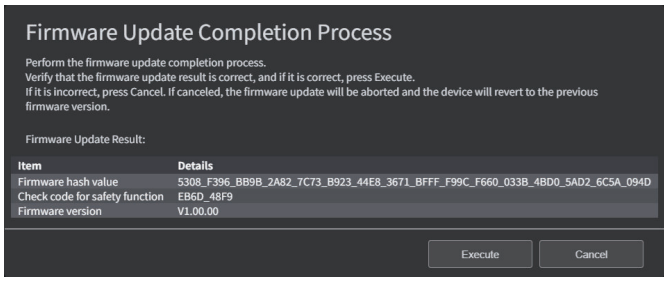
1 Select File 버튼을 클릭하고, PC에서 펌웨어 파일을 선택합니다.
선택한 파일이 표시됩니다. 또한 선택한 펌웨어의 해시값, 세이프티 기능 체크 코드, 펌웨어 버전이 표시됩니다.

2 펌웨어의 해시값, 세이프티 기능 체크 코드, 펌웨어 버전에 문제가 없는지 확인한 후 Confirm 버튼을 클릭합니다.
다음 메시지가 표시됩니다.

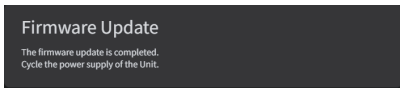


3 세이프티 패스워드를 입력하고 Execute 버튼을 클릭합니다.
다음 메시지가 표시됩니다.

AI 번역본
-For Reference Only-



4 펌웨어의 해시값, 세이프티 기능 체크 코드, 펌웨어 버전에 문제가 없는지 확인한 후 Execute 버튼을 클릭합니다.
펌웨어 업데이트 완료 처리가 실행됩니다. 다음 메시지가 표시됩니다.



5 세이프티 I/O 블록의 전원을 재투입합니다.

6 Web UI의 Production Information 화면에서 펌웨어 버전이 변경되었는지 확인합니다.

8-14-3 펌웨어 업데이트 기능 상세

펌웨어 업데이트 기능을 실행하면 MS 표시등과 유닛 식별 표시등으로 세이프티 I/O 블록의 상태를 확인할 수 있습니다. 다음 표는 세이프티 I/O 블록의 상태와 MS 표시등, 유닛 식별 표시등의 상태의 관계를 나타냅니다.

세이프티 I/O 블록의 상태	MS 표시등	유닛 식별 표시등
펌웨어 업데이트 준비 중	소등	모두 점등
펌웨어 업데이트 중	0.5초 ON, 0.5초 OFF로 녹색 점멸	모두 점등
펌웨어 업데이트 성공	녹색 점등	모두 점등
펌웨어 업데이트 실패	적색 점등	모두 점등

펌웨어 업데이트 기능에는 펌웨어 버전 제약이 없습니다. 버전 업그레이드뿐만 아니라 버전 다운그레이드도 가능합니다.

AI 번역본

사용상의 주의

- 펌웨어 업데이트 기능 실행 중에는 전원을 OFF하지 마십시오. 재시작이 불가능해질 수 있습니다.

9

세이프티 응답 성능

이 장에서는 세이프티 I/O 블록의 세이프티 응답 성능(세이프티 반응 시간)을 산출하는 방법에 대해 설명합니다.

9-1 세이프티 I/O 블록의 세이프티 응답 성능 9-2
9-1-1 세이프티 응답 성능 산출 9-2
9-1-2 세이프티 응답 성능 검증 9-5

AI 번역본
-For Reference Only-

9-1 세이프티 I/O 블록의 세이프티 응답 성능

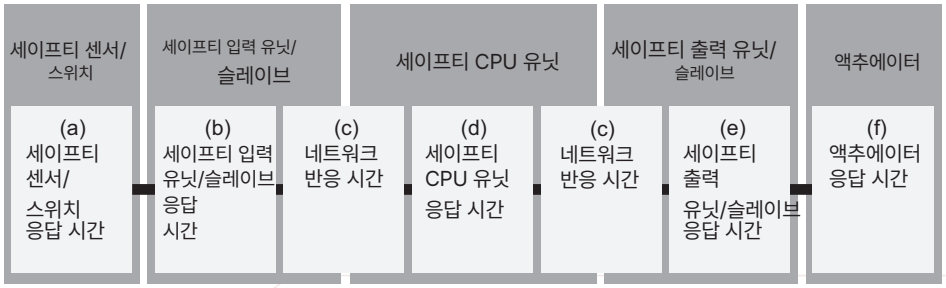
세이프티 응답 성능(세이프티 반응 시간)은 출력을 OFF하는 데 필요한 최대 시간입니다
세이프티 체인*1의 고장 및 파손을 고려했을 때를 말합니다.
세이프티 시스템 설계에서는 세이프티 응답 성능으로부터 세이프티 거리를 산출합니다.
모든 세이프티 체인에 대해, 세이프티 입력이 작동한 시점부터 운전 중인 기기를 정지시키는 데 걸리는 가장 긴 시간이 요구 사양을 만족해야 합니다.
이 절에서는 세이프티 I/O 블록의 세이프티 응답 성능에 대해 설명합니다.

*1. 세이프티 체인은 세이프티 입력 기기에서 세이프티 I/O 블록 또는 세이프티 제어 유닛을 거쳐 세이프티 출력에 이르는, 세이프티 기능을 달성하기 위한 논리적 연결입니다.

9-1-1 세이프티 응답 성능 산출

이 절에서는 CIP Safety 통신을 사용할 때와 사용하지 않을 때로 구분하여 세이프티 응답 성능의 산출 방법에 대해 설명합니다.

a. CIP Safety 통신을 사용하는 세이프티 컨트롤러로 세이프티 제어를 수행하는 경우
아래 그림과 같이, 세이프티 응답 성능은 (a) 세이프티 센서/스위치 응답 시간, (b) 세이프티 입력 유닛/슬레이브 응답 시간, (c) 네트워크 반응 시간, (d) 세이프티 컨트롤러 응답 시간, (e) 세이프티 출력 유닛/슬레이브 응답 시간, (f) 액추에이터 응답 시간의 합으로 결정됩니다.
요소의 수와 시간의 길이는 세이프티 체인의 경로에 따라 달라집니다.



기호	시간 요소	값
(a)	세이프티 센서/ 스위치 응답 시간	이는 라이트 커튼과 같은 세이프티 센서 또는 스위치가 OFF하는 데 필요한 응답 시간입니다. 이 값은 각 센서 또는 스위치마다 정의됩니다.

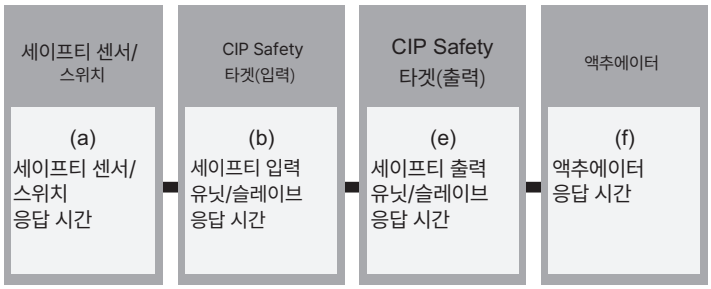
-For Reference Only-

Let-터	시간 요소	값
(b)	세이프티 입력 유닛/슬레이브 응답 시간	이것은 CIP Safety 타겟의 입력 응답 시간입니다. 입력 단자의 채널 모드와 세이프티 요구 수준에 따라 다음 세 가지 시간이 있습니다. ・듀얼 채널을 사용하는 경우 10 ms ・싱글 채널을 사용하고 세이프티 입력의 위험한 고장을 고려하지 않는 경우 (세이프티 요구 수준이 Cat.2/PLc/SIL1) 10 ms ・싱글 채널을 사용하고 세이프티 입력의 위험한 고장을 고려하는 경우 (세이프티 요구 수준이 Cat.2/PLd/SIL2) 260 ms 세이프티 I/O 블록의 입력 응답 시간에 대해서는, 위 시간에 입력 단자의 ON->OFF 지연 시간을 더하십시오.
(c)	네트워크 반응 시간	이것은 CIP Safety 커넥션의 응답 시간입니다. NJ/NX/NY 시리즈의 경우, Sysmac Studio에서 계산되어 표시됩니다. *1 네트워크 반응 시간 확인 방법에 대한 자세한 내용은 7-32페이지의 커넥션 파라미터 편집 순서를 참조하십시오.
(d)	세이프티 컨트롤러 응답 시간	이것은 세이프티 컨트롤러의 응답 시간입니다. 세이프티 CPU 유닛에 대해서는 NX 시리즈 세이프티 컨트롤 유닛/커뮤니케이션 컨트롤 유닛 사용자 매뉴얼(자료 번호 Z395)을 참조하십시오. *1
(e)	세이프티 출력 유닛/슬레이브 응답 시간	이것은 CIP Safety 타겟의 출력 응답 시간입니다. 출력 단자의 채널 모드와 세이프티 요구 수준에 따라 다음 두 가지 시간이 있습니다. ・듀얼 채널을 사용하는 경우 5 ms ・싱글 채널을 사용하는 경우 5 ms(싱글 채널은 Cat.2까지이므로 고장이 없다는 가정하의 응답 시간) 세이프티 I/O 블록의 출력 응답 시간에 대해서는, 위 시간에 출력 단자의 ON->OFF 지연 시간을 더하십시오. 세이프티 I/O 블록의 로직 기능을 사용하는 경우, 로직 실행 시간도 이 시간에 포함됩니다.
(f)	액추에이터 응답 시간	이것은 세이프티 릴레이 등의 액추에이터가 OFF되는 데 필요한 응답 시간입니다. 이 값은 액추에이터마다 정의되어 있습니다.

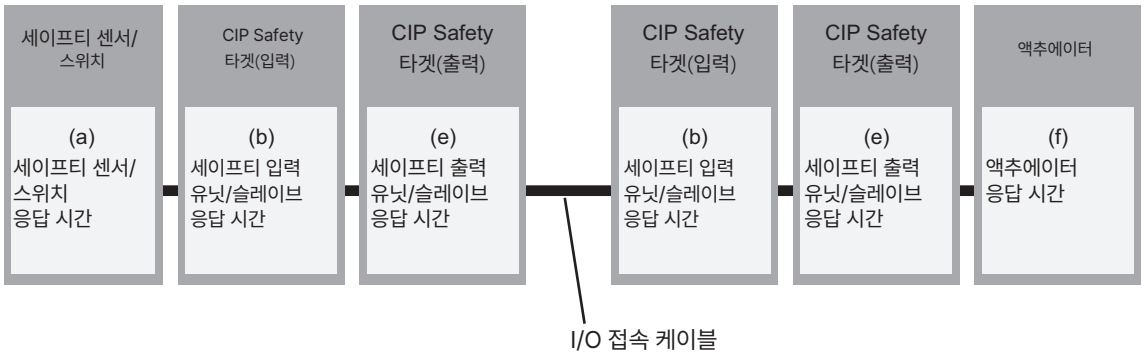
***1.** 다른 회사의 컨트롤러에 유닛을 접속하는 경우, 접속할 컨트롤러의 지원 소프트웨어에 대한 취급 설명서를 확인하십시오.

b. CIP Safety 통신을 사용하지 않는 세이프티 애플리케이션으로 세이프티 제어를 수행하는 경우
세이프티 응답 성능에 대해서는, 입출력 처리가 세이프티 I/O 블록에서 수행되므로 a.의 (c)와 (d)의 시간은 제외됩니다.
・개별 세이프티 I/O 블록에 대한 컨피규레이션

사본 여부
-For Reference Only-



・I/O 접속 케이블로 세이프티 I/O 블록 유닛 2대를 접속하는 컨피규레이션
세이프티 응답 성능에 대해서는, 접속된 세이프티 I/O 블록 유닛 수만큼 (b)와 (e)의 합계 시간을 더하십시오.



사용상의 주의

・세이프티 응답 성능 계산 시에는 "입력 단자의 ON->OFF 지연 시간"과 "출력 단자의 ON->OFF 지연 시간"의 영향을 더하십시오.

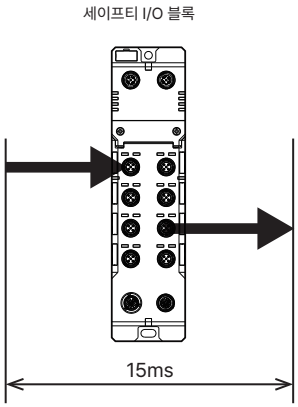
개별 세이프티 I/O 블록 컨피규레이션을 사용하는 경우

개별 세이프티 I/O 블록의 슬레이브 응답 시간(I/O 응답 시간)은 세이프티 입력 및 세이프티 출력 설정의 조합에 따라 다음과 같습니다.

세이프티 입력	세이프티 출력	세이프티 요구 수준	슬레이브 응답 시간
듀얼 채널	듀얼 채널	Cat.4/PLe/SIL3	15 ms (= 10 ms + 5 ms)
듀얼 채널	싱글 채널	Cat.2/PLc/SIL1	15 ms (= 10 ms + 5 ms)*1
싱글 채널	듀얼 채널	Cat.2/PLd/SIL2	265 ms (= 260 ms + 5 ms)
싱글 채널	싱글 채널	Cat.2/PLc/SIL1	15 ms (= 10 ms + 5 ms)*1

-For Reference Only-

*1. 세이프티 요구 수준은 Cat.2/PLc/SIL1이며, 이 응답 시간은 고장이 발생하지 않았다고 가정한 것입니다. 세이프티 출력을 싱글 채널 모드로 사용하는 경우, 고장 검출 시간은 265 ms + 네트워크 응답 시간입니다. 자세한 내용은 2-4페이지의 2-1-3 세이프티 사양을 참조하십시오.



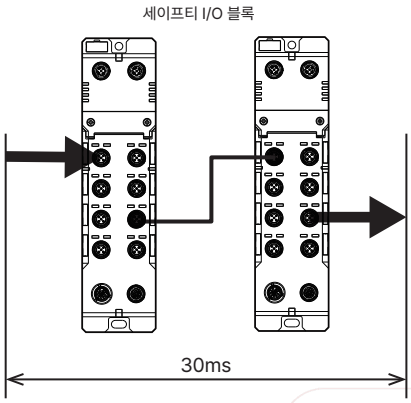
I/O 케이블 접속 컨피규레이션인 경우

다음 조건에서 I/O 케이블로 세이프티 I/O 블록 유닛 2대를 접속하여 세이프티 애플리케이션을 사용할 때의 I/O 응답 성능은 30 ms입니다.

・CIP Safety 통신을 사용하지 않습니다.

・세이프티 입력 단자와 세이프티 출력 단자가 모두 듀얼 채널로 설정되어 있습니다.

・"입력 단자의 ON->OFF 지연 시간"과 "출력 단자의 ON->OFF 지연 시간"은 더하지 않습니다.



시 버 여 보
-For Reference Only-

9-1-2 세이프티 응답 성능 검증

모든 세이프티 체인에 대해 계산된 세이프티 응답 성능이 요구 사양을 충족하는지 확인하십시오. 계산된 세이프티 응답 성능이 요구 사양을 충족하지 않는 경우, 다음 조치 중 하나를 검토하여 소프트웨어 또는 하드웨어 설계를 수정하십시오.

・CIP Safety 커넥션의 데이터 패킷 간격(EPI) 값을 줄이십시오.
데이터 패킷 간격(EPI)에 대해서는 7-32페이지의 커넥션 파라미터 편집 순서를 참조하십시오.

AI 번역본
-For Reference Only-

10

보안 가이드라인

본 장에서는 세이프티 I/O 블록을 사용할 때의 보안 가이드라인에 대해 설명합니다.
FA 시스템 전체의 보안 대책에 대해서는 Security Guideline for Factory Automation System(자료 번호 P162)을 참조하십시오. 또한 NJ/NX 시리즈 CPU 유닛을 사용하여 구현할 수 있는 보안 대책에 대해서는 Security Guideline for NJ/NX Controller (자료 번호 P166)를 참조하십시오.

10-1 세이프티 I/O 블록에 의한 다층 방어 10-2
10-1-1 세이프티 I/O 블록의 운용 환경..... 10-2
10-1-2 세이프티 I/O 블록을 사용한 기술 계층의 보안 대책 10-3

10-2 자산을 보호하기 위한 세이프티 I/O 블록의 보안 기능 10-5
10-2-1 통신 회선상의 데이터 보호..... 10-5
10-2-2 세이프티 I/O 블록에 대한 외부 공격 차단..... 10-7
10-2-3 세이프티 I/O 블록에 대한 부정 조작 방지 10-9
10-2-4 세이프티 I/O 블록 자산의 변조 방지..... 10-10
10-2-5 세이프티 애플리케이션 파일 및 백업 파일 보호 10-11
10-2-6 부인 방지..... 10-12

10-3 보안 패치 적용..... 10-13
10-3-1 세이프티 I/O 블록 업데이트 10-13
10-3-2 Sysmac Studio 업데이트..... 10-13
10-3-3 PC의 OS 업데이트..... 10-13

10-4 기기의 안전한 폐기 10-14
10-4-1 세이프티 I/O 블록의 자산 삭제..... 10-14

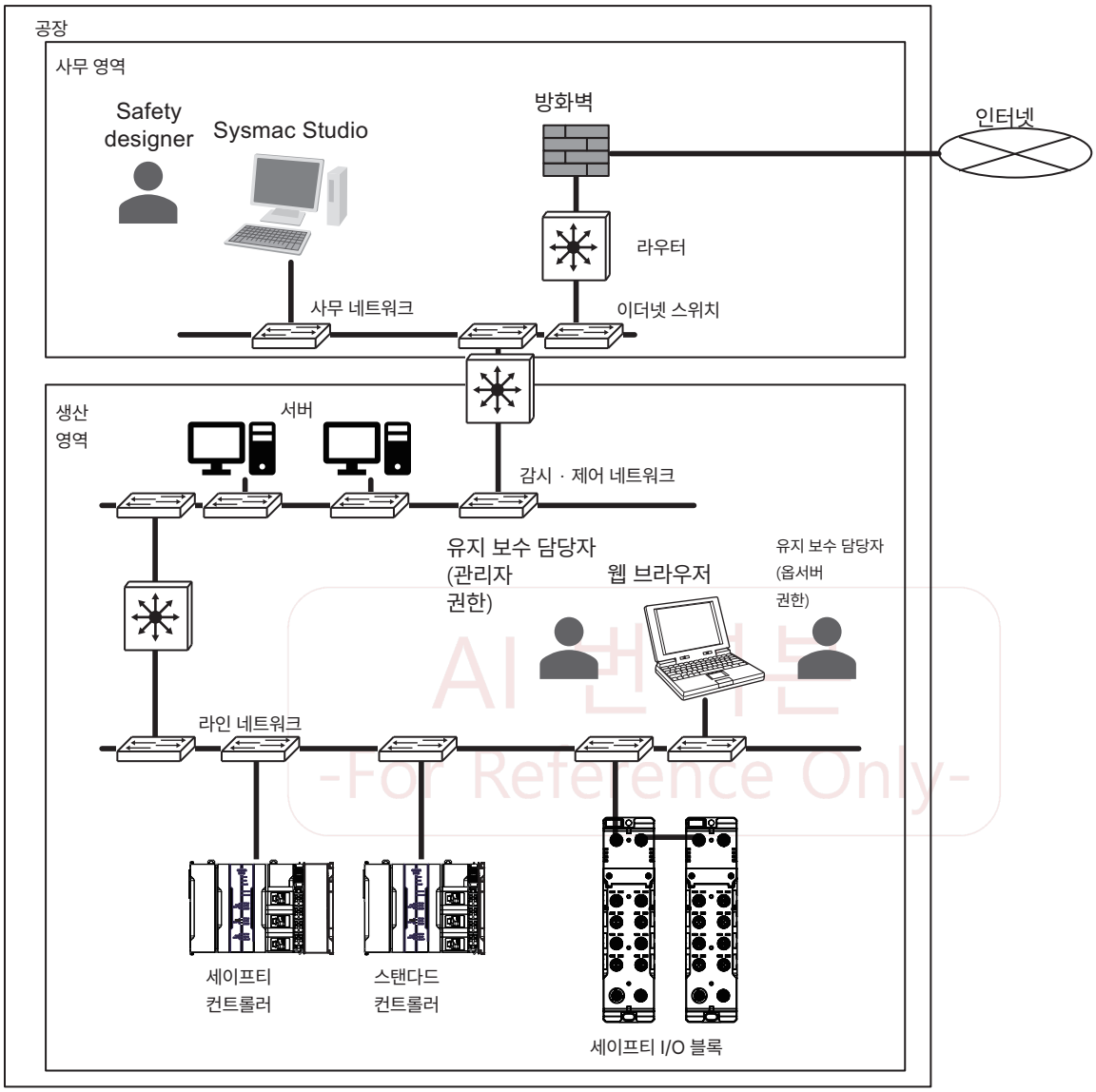
AI 번역본
-For Reference Only-

10-1 세이프티 I/O 블록에 의한 다층 방어

세이프티 I/O 블록은 다층 방어를 실현하기 위해 여러 보안 기능을 제공합니다.
본 절에서는 세이프티 I/O 블록의 보안 기능으로 실현되는 다층 방어에 대해 설명합니다.

10-1-1 세이프티 I/O 블록의 운용 환경

세이프티 I/O 블록은 자사의 보안 기능을 효과적으로 활용하여 설비의 운용 및 자산, 그리고 세이프티 I/O 블록 자체를 보호합니다.
아래 그림과 같이 생산 영역과 사무 영역을 분리하는 등 네트워크를 세그먼트화하면 외부로부터 공격을 받았을 때 그 영향 범위를 최소화하는 데 효과적입니다. 또한 세이프티 I/O 블록의 주변 기기에도 보안 대책을 적용하십시오. 구체적인 절차는 주변
기기의 매뉴얼을 참조하십시오.

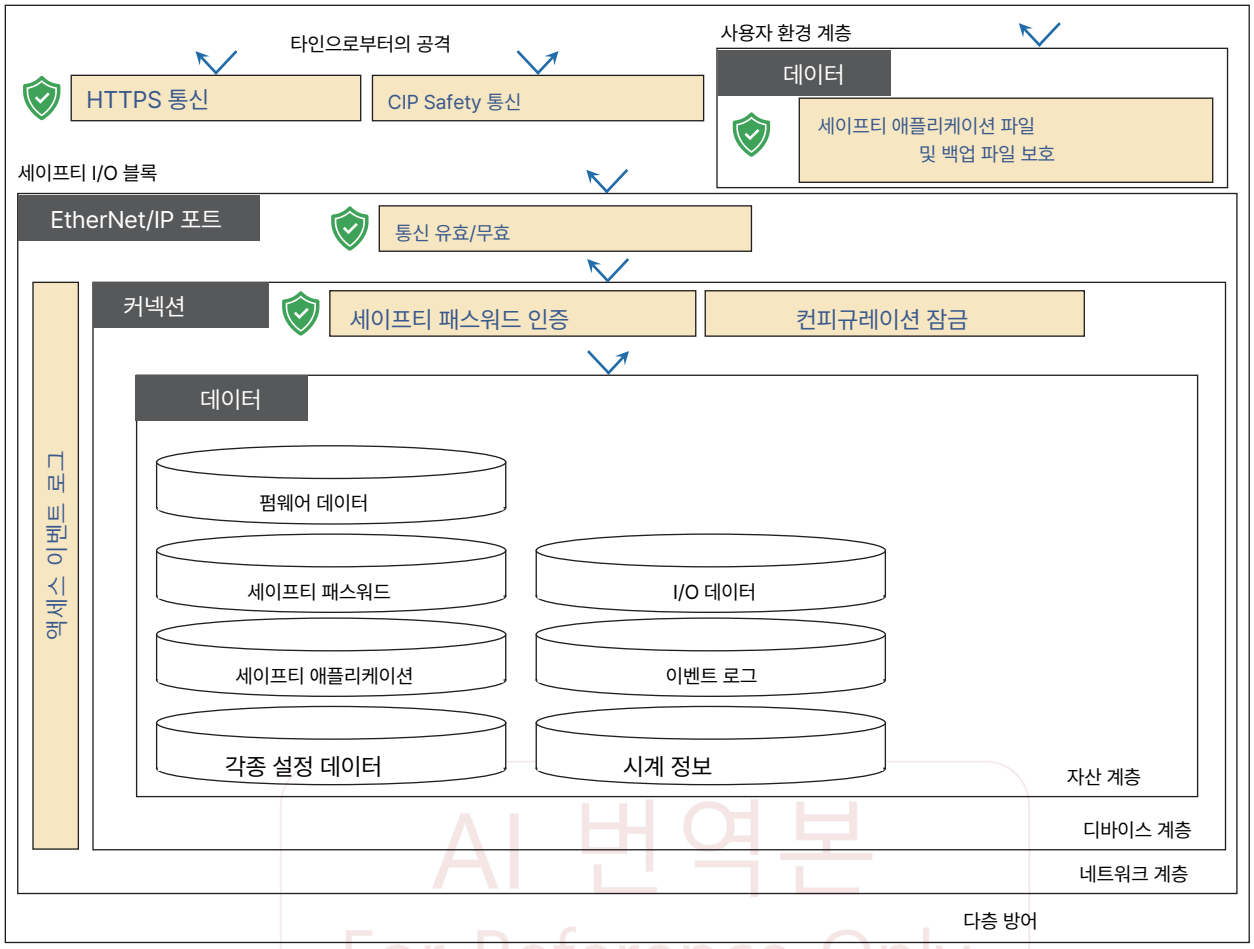


AI 번역본
-For Reference Only-

10-1-2 세이프티 I/O 블록을 사용한 기술 계층의 보안 대책

세이프티 I/O 블록은 다층 방어를 통해 자산을 보호할 수 있는 보안 기능을 제공합니다. 공격자가 한 계층을 뚫더라도, 자산에 가장 가까운 계층의 보안 기능이 그 자산을 보호할 수 있습니다.
목적과 위협의 종류에 따라 Security Guideline for Factory Automation System(자료 번호 P162)에 기재된 대책과 본 절에 기재된 여러 보안 기능을 조합하여 다층 방어를 적용하십시오.

본 절에서는 보안 기능을 사용하여 특히 수행해야 할 사항을 설명합니다. 본 절을 함께 읽고 필요한 조치를 취하십시오.
또한 각 보안 기능이 의도한 대로 동작하고 있는지 반드시 스스로 확인하십시오.



AI 번역본
-For Reference Only-

아래 표는 각 계층에서 제공되는 기능을 나타냅니다.

보호 대상 자산 계층	목적	세이프티 I/O 블록이 제공하는 기능	참조
네트워크 계층	통신 회선상의 데이터 보호	HTTPS 통신 기능 (Web UI)	10-5페이지의 HTTPS 통신 기능 (Web UI)
		CIP Safety 통신 기능	CIP Safety 통신 기능 10-5페이지
	세이프티 I/O 블록에 대한 외부 공격 차단	통신 유효/무효 설정 기능	10-7페이지의 통신 유효/무효 설정
디바이스 계층	세이프티 I/O 블록에 대한 부정 조작 방지	세이프티 패스워드 인증 기능	10-9페이지의 세이프티 패스워드 인증 기능

보호 대상 자산 계층	목적	세이프티 I/O 블록이 제공하는 기능	참조
	세이프티 I/O 블록 자산의 변조 방지	컨피규레이션 잠금 기능	10-10페이지의 컨피규레이션 잠금 기능
사용자 환경 계층	세이프티 애플리케이션 파일 및 백업 파일 보호	세이프티 애플리케이션 파일 및 백업 파일 보호	10-11페이지의 세이프티 애플리케이션 파일 및 백업 파일 보호
전 계층 공통	부인 방지	액세스 이벤트 로그 기능	10-12페이지의 액세스 이벤트 로그 기능

AI 번역본
-For Reference Only-

10-2 자산을 보호하기 위한 세이프티 I/O 블록의 보안 기능

본 절에서는 세이프티 I/O 블록이 제공하는 보안 기능에 대해 설명합니다.

10-2-1 통신 회선상의 데이터 보호

네트워크에 접속된 설비는 네트워크를 통한 사이버 공격의 위험에 노출됩니다. 통신 회선상을 흐르는 데이터로부터의 정보 유출, 변조, 서비스 거부를 방지하려면 다음 기능을 사용하십시오.

HTTPS 통신 기능(Web UI)

HTTPS 통신 기능은 웹 브라우저와 세이프티 I/O 블록 간 통신의 보안을 향상시키기 위한 것입니다.

송수신 전에 통신 데이터를 암호화한 후 해시값을 부여하므로, 제3자에 의한 도청 및 변조를 방지하는 데 유용합니다.
HTTPS 통신 기능에 대한 자세한 내용은 7-17페이지의 7-2 Web UI 개요를 참조하십시오.

● 대응 가능한 위협

S: 스푸핑	T: 변조	R: 부인	I: 정보 유출	D: 서비스 거부	E: 권한 상승
○	○		○	○	

● 사용자가 해야 할 사항

- 보안을 강화하려면 최신 버전의 웹 브라우저로 Web UI를 사용하십시오.
- 제어 시스템 및 설비의 네트워크를 IT 네트워크로부터 분리하기 위해 방화벽(사용하지 않는 통신 포트 차단 및 통신 호스트 제한)을 설치하고, Web UI에서 세이프티 제어 시스템으로의 접속이 방화벽 내부에서 이루어지도록 하십시오.
- Web UI를 통해 제어 시스템 및 설비에 원격으로 액세스할 때는 가상 사설망(VPN)을 사용하십시오.
- HTTPS 통신 기능을 사용하려면 CA 인증서가 필요합니다. 오므론 웹사이트에서 CA 인증서를 다운로드한 후 웹 브라우저에 설치하십시오. CA 인증서가 설치되지 않은 상태에서 세이프티 I/O 블록에 액세스를 시도하면 웹 브라우저에 에러가 발생합니다. 자세한 내용은 8-8페이지의 8-3 HTTPS 통신 기능을 참조하십시오.
- Web UI를 시작하려면 IP 주소를 입력하는 방법과 도메인 이름을 입력하는 방법이 있습니다. IP 주소를 입력하는 방법을 사용하는 경우, 부정한 디바이스가 PC와 세이프티 I/O 블록 간의 통신을 가로채지 않도록 조치를 취하십시오. 조치에 대한 자세한 내용은 7-21페이지의 7-2-5 Web UI 시작 순서를 참조하십시오.

-For Reference Only-

CIP Safety 통신 기능

CIP Safety 통신 기능은 CIP Safety 오리지네이터(세이프티 컨트롤러)와 CIP Safety 타겟(세이프티 I/O 블록) 간에 데이터를 주기적으로 교환하기 위한 세이프티 기능입니다. 통신의 신뢰성은 TUNID, SCCRC, SCTS 등의 메커니즘으로 보장됩니다.

CIP Safety 통신 기능에 대한 자세한 내용은 6-4페이지의 6-2 CIP Safety 통신을 참조하십시오.

● 대응 가능한 위협

S: 스푸핑	T: 변조	R: 부인	I: 정보 유출	D: 서비스 거부	E: 권한 상승
○	○			○	

AI 번역본
-For Reference Only-

10-2-2 세이프티 I/O 블록에 대한 외부 공격 차단

인터넷에 접속된 설비는 네트워크를 통한 사이버 공격의 위험에 노출됩니다. 생산 설비의 오동작과 사고를 방지하기 위해 외부 공격을 차단하십시오.

통신 유효/무효 설정

통신 유효/무효 설정 기능을 사용하면 세이프티 I/O 블록의 각 통신 기능을 유효 또는 무효로 설정할 수 있습니다. 사용하지 않는 통신 기능을 무효로 하여 외부로부터 세이프티 I/O 블록에 대한 액세스 경로 수를 줄이면 정보 유출 및 공격을 방지할 수 있습니다.
통신 유효/무효 설정 기능은 다음 대상에 대해 구성할 수 있습니다.

대상	설명
EtherNet/IP 포트	EtherNet/IP 포트 1과 2의 이더넷 통신 기능을 포트별로 유효 또는 무효로 설정할 수 있습니다. 두 포트 모두 기본값은 유효입니다.
DHCP(IP 주소 설정)	DHCP 서버로부터 IP 주소를 취득하는 기능을 유효 또는 무효로 설정할 수 있습니다. 기본값은 무효입니다.
SNTP(시계 자동 조정)	SNTP 서버로부터 시계 정보를 취득하는 기능을 유효 또는 무효로 설정할 수 있습니다. 기본값은 무효입니다.

● EtherNet/IP 포트 통신 유효/무효 설정

익스플리시트 메시지 통신을 사용하여 EtherNet/IP 포트의 통신 유효/무효를 설정하십시오.

전송할 명령은 다음과 같습니다.

구현 상세	전송 명령 항목	전송 명령값
EtherNet/IP 포트 통신 유효/무효 설정	서비스 코드	10 hex (Set_Attribute_Single)
	클래스 ID	F6 hex (Ethernet Link object)
	인스턴스 ID	01 hex: Port1 02 hex: Port2
	속성 ID	101 (Communication Port Enable)
	서비스 데이터	TRUE: 유효 FALSE: 무효

익스플리시트 메시지를 통해 CIP 오브젝트에 액세스하는 방법에 대한 자세한 내용은 6-7페이지의 익스플리시트 메시지 서버 기능을 참조하십시오.

AI 번역본
-For Reference Only-

● DHCP 통신 유효/무효 설정

Sysmac Studio를 사용하여 DHCP 통신 유효/무효를 설정하려면, IP 주소 설정 화면에서 Obtain from DHCP server를 다음과 같이 설정하십시오.
Web UI를 사용하여 DHCP 통신 유효/무효를 설정하려면, Web UI의 TCP/IP 설정 화면에서 IP 주소에 대한 Obtain from DHCP server를 다음과 같이 설정하십시오.

DHCP 통신	Obtain from DHCP server
유효	체크박스를 선택합니다.
무효	체크박스를 선택 해제합니다.

Sysmac Studio로 IP 주소를 설정하는 순서에 대한 자세한 내용은 7-74페이지의 7-10-3 Sysmac Studio에 의한 설정을 참조하십시오.
Web UI의 TCP/IP 설정 화면에 대한 자세한 내용은 7-76페이지의 7-10-4 Web UI에 의한 설정을 참조하십시오.

● SNTP 통신 유효/무효 설정

Sysmac Studio를 사용하여 SNTP 통신 유효/무효를 설정하려면, 시계 자동 조정 설정 화면에서 SNTP Settings를 다음과 같이 설정하십시오.
Web UI를 사용하여 SNTP 통신 유효/무효를 설정하려면, Web UI의 시계 자동 조정 설정 화면에서 NTP/SNTP server IP address를 다음과 같이 설정하십시오.

SNTP 통신	설정
Active	IP 주소를 설정합니다.
Inactive	IP 주소를 설정하지 않습니다.

Sysmac Studio에서 시계 자동 조정을 구성하는 순서에 대한 자세한 내용은 7-91페이지의 Sysmac Studio를 사용한 순서를 참조하십시오.
Web UI의 시계 자동 조정 설정 화면에 대한 자세한 내용은 7-92페이지의 Web UI를 사용한 순서를 참조하십시오.

● 대응 가능한 위협

S: 스푸핑	T: 변조	R: 부인	I: 정보 유출	D: 서비스 거부	E: 권한 상승
○	○		○	○	

● 사용자가 해야 할 사항

- DHCP 및 SNTP 프로토콜에는 보안 대책이 적용되어 있지 않습니다. DHCP 및 SNTP 프로토콜을 사용할 때는 애플리케이션 측에서 보안을 확보하십시오.
- 세이프티 I/O 블록에 부정한 패킷이 도달하지 않도록 방화벽을 설치하는 등, 다른 대책과 조합하여 이 기능을 사용하십시오.

AI 번역본
-For Reference Only-

10-2-3 세이프티 I/O 블록에 대한 부정 조작 방지

귀사의 중요한 지적 재산인 세이프티 애플리케이션과 설비를 도난, 부정 이용,
생산 설비의 오동작,
사고로부터 보호하기 위해 세이프티 I/O 블록에 대한 부정 조작을 방지하십시오.

세이프티 패스워드 인증 기능

세이프티 I/O 블록의 설정 데이터 및 조작을 변경하면 인명 상해나 재산 피해를 초래할 위험이 있습니다.
조작자의 권한에 따라 조작자가 조작할 수 있는 기능을 제한하여 권한이 없는
조작자에 의한 조작을 방지하십시오. 세이프티 I/O 블록의 세이프티 패스워드 인증 기능은
다음과 같습니다.

기능	설명
기능 안전에 영향을 미치는 조작의 제한	전체 메모리 클리어, 재시작, 컨피규레이션 잠금 및 잠금 해제, 운전 모드 변경, 세이프티 패스워드 기능을 실행할 때는 세이프티 패스워드에 의한 인증이 필요합니다.
Web UI 조작의 제한	Web UI에는 관리자와 옵서버의 조작 권한이 있습니다. 설정 데이터를 변경할 수 있는 것은 관리자뿐입니다. 관리자로서 Web UI를 사용하려면 세이프티 패스워드에 의한 인증이 필요합니다.

기능 안전에 영향을 미치는 조작의 제한에 대한 자세한 내용은 각 기능의 페이지를 참조하십시오. 자세한 내용은
7-17페이지의 7-2-2 Web UI의 조작 권한을 참조하십시오. 세이프티
패스워드 설정에 대한 자세한 내용은 7-104페이지의 7-18 세이프티 패스워드 설정을 참조하십시오.

● 대응 가능한 위협

S: 스푸핑	T: 변조	R: 부인	I: 정보 유출	D: 서비스 거부	E: 권한 상승
○	○	○	○	○	○

● 사용자가 해야 할 사항

- 세이프티 I/O 블록에는 반드시 세이프티 패스워드를 설정하십시오.
- 세이프티 패스워드는 정기적으로 직접 변경하십시오.
- 제3자에 의한 부정 사용을 방지할 수 있도록 세이프티 패스워드를 적절하게 설정 및 관리하십시오.
- 무차별 대입 공격에 의한 비밀번호 분석을 방지할 수 있도록 복잡한 패스워드(여러 종류의 문자를 포함하여 8자 이상)를 설정하십시오.
- 세이프티 패스워드의 기밀성을 높이기 위해 다른 기기와 동일한 패스워드를 설정하지 마십시오.
- 본 제품이 준수하는 CIP Safety는 공장 등 산업 환경의 FA 애플리케이션에서 기기 안전을 실현하기 위한 세이프티 통신 메커니즘입니다. 본 제품의 부정 조작 등 보안 리스크를 경감하려면 본 제품의 기능뿐 아니라, 생산 영역에 대한 액세스 제어 및 네트워크에 대한 액세스 제한을 포함하여 시스템 전체에 걸쳐 적절한 대책을 시행하십시오.

AI 번역본
For Reference Only

10-2-4 세이프티 I/O 블록 자산의 변조 방지

귀사의 중요한 지적 재산인 설정 데이터의 변조, 그리고 의도하지 않은 세이프티 애플리케이션의 부정 실행을 방지하십시오.

컨피규레이션 잠금 기능

컨피규레이션 잠금 기능은 세이프티 I/O 블록의 세이프티에 관련된 설정 데이터와 실행 중인 세이프티 애플리케이션이 의도치 않게 변경되는 것을 방지합니다. 컨피규레이션이 잠겨 있는 동안에는 세이프티 I/O 블록의 설정 데이터를 변경할 수 없습니다. 또한 선택된 세이프티 애플리케이션을 다른 세이프티 애플리케이션으로 변경할 수 없습니다.
컨피규레이션 잠금에 대한 자세한 내용은 7-99페이지의 7-17 컨피규레이션 잠금을 참조하십시오.

● 대응 가능한 위협

S: 스푸핑	T: 변조	R: 부인	I: 정보 유출	D: 서비스 거부	E: 권한 상승
	○				

● 사용자가 해야 할 사항

・세이프티 I/O 블록을 전체 운전하기 전에 반드시 컨피규레이션을 잠그십시오.

AI 번역본
-For Reference Only-

10-2-5 세이프티 애플리케이션 파일 및 백업 파일 보호

귀사의 중요한 지적 재산인 설계 자산의 부정 사용을 방지하십시오.

세이프티 애플리케이션 파일 및 백업 파일 보호

세이프티 애플리케이션 파일 및 백업 파일은 파일에 대한 부정 액세스를 방지하기 위해 패스워드로 보호됩니다. 파일을 보호하는 패스워드는 각각 세이프티 애플리케이션 파일 패스워드와 백업 파일 패스워드입니다.
세이프티 애플리케이션 파일 패스워드에 대한 자세한 내용은 7-68페이지의 7-9-5 세이프티 애플리케이션 파일 익스포트를 참조하십시오. 백업 파일 패스워드에 대한 자세한 내용은 7-108페이지의 7-19 백업을 참조하십시오.

● 대응 가능한 위협

S: 스푸핑	T: 변조	R: 부인	I: 정보 유출	D: 서비스 거부	E: 권한 상승
	○				

● 사용자가 해야 할 사항

- 제3자에 의한 부정 사용을 방지할 수 있도록 세이프티 애플리케이션 파일 패스워드와 백업 파일 패스워드를 적절하게 설정 및 관리하십시오.
- 무차별 대입 공격에 의한 비밀번호 분석을 방지할 수 있도록 복잡한 패스워드(여러 종류의 문자를 포함하여 8자 이상)를 설정하십시오.

AI 번역본
-For Reference Only-

10-2-6 부인 방지

귀사의 자산을 보호하려면 그 자산이 부정 조작을 받았다는 사실을 파악하는 것도 중요합니다. 또한 보안 사고가 발생했을 때는 사고의 원인과 경위를 파악해야 합니다. 보안 침해와 사이버 공격을 기록해 두면 언제 누가 무엇을 했는지 확인할 수 있으며, 문제 발생 시 부인 방지 대책으로 활용할 수 있습니다.

액세스 이벤트 로그 기능

세이프티 I/O 블록은 Sysmac Studio 또는 Web UI를 사용하여 사용자가 세이프티 I/O 블록에 대해 수행한 조작을 액세스 이벤트 로그로 기록합니다. 액세스 이벤트 로그는 Sysmac Studio 또는 Web UI를 사용하여 읽거나 지울 수 있습니다.
액세스 이벤트 로그 기능에 대한 자세한 내용은 11-6페이지의 11-2-1 이벤트 로그 기능을 참조하십시오.

● 대응 가능한 위협

S: 스푸핑	T: 변조	R: 부인	I: 정보 유출	D: 서비스 거부	E: 권한 상승
		○			

● 사용자가 해야 할 사항

・액세스 이벤트 로그를 지우면 부인을 방지할 수 없게 됩니다. 이벤트 수가 허용된 기록 수를 초과하면, 세이프티 I/O 블록은 액세스 이벤트 로그를 오래된 정보부터 덮어씁니다.
로그를 정기적으로 백업하여 일정 기간 보관할 것을 권장합니다.

AI 번역본
-For Reference Only-

10-3 보안 패치 적용

나날이 진화하는 사이버 공격으로부터 귀사의 자산과 생산을 보호하려면, 기기를 항상 최신 상태로 유지하여 보안 강도를 높이는 것이 효과적입니다.
본 절에서는 업데이트를 위해 세이프티 I/O 블록이 제공하는 기능에 대해 설명합니다.

10-3-1 세이프티 I/O 블록 업데이트

기능 추가, 조작성 향상, 보안 강화를 위해 세이프티 I/O 블록을 항상 최신 버전으로 업데이트하여 사용하십시오.

펌웨어 업데이트 기능

펌웨어 업데이트 기능은 세이프티 I/O 블록이 사용하는 펌웨어를 최신 버전으로 업데이트하기 위한 것입니다. 펌웨어 업데이트 기능에 대한 자세한 내용은 8-35페이지의 8-14 펌웨어 업데이트 기능을 참조하십시오.
펌웨어를 업데이트하면 이벤트 로그에 이벤트가 기록됩니다. 변경 이력을 확인할 때는 11-6페이지의 11-2-1 이벤트 로그 기능에 설명된 대로 이벤트를 확인하십시오.
최신 펌웨어 파일을 입수하는 방법에 대한 자세한 내용은 오므론 웹사이트를 확인하십시오.

● 사용자가 해야 할 사항

- 세이프티 I/O 블록의 펌웨어가 최신 버전인지 정기적으로 확인하십시오.
- 펌웨어 업데이트 기능을 실행한 후 백업 파일을 복원하는 경우, 보안을 강화하기 위해 세이프티 패스워드를 설정하십시오.

10-3-2 Sysmac Studio 업데이트

기능 추가, 조작성 향상, 보안 강화를 위해 Sysmac Studio를 항상 최신 버전으로 업데이트하여 사용하십시오.
Sysmac Studio의 자동 업데이트에 대한 자세한 내용은 Sysmac Studio Version 1 Operation Manual(자료 번호 W504)을 참조하십시오.

샘플 복사본
For Reference Only

10-3-3 PC의 OS 업데이트

OS의 취약점으로 인한 보안 리스크를 피하려면, Sysmac Studio, Web UI, 그 지원 소프트웨어가 실행되는 PC의 OS를 항상 최신 상태로 유지하십시오.

10-4 기기의 안전한 폐기

본 절에서는 폐기를 위해 세이프티 I/O 블록이 제공하는 기능에 대해 설명합니다.

10-4-1 세이프티 I/O 블록의 자산 삭제

세이프티 I/O 블록을 폐기 또는 양도하면 제3자가 세이프티 I/O 블록에 저장된 설정 데이터 등의 정보를 열람할 수 있게 되어 정보 유출의 위험이 있습니다.
폐기 또는 양도하기 전에 자신의 책임하에 설정 데이터를 삭제하십시오.

전체 메모리 클리어 기능

전체 메모리 클리어 기능은 세이프티 I/O 블록의 설정 데이터를 완전히 지우기 위한 것입니다. 완전히 지우려면, Web UI에서 전체 메모리 클리어 기능을 선택하여 Web UI에서 설정된 이벤트 로그와 세이프티 애플리케이션도 함께 지우십시오. Sysmac Studio의 전체 메모리 클리어 기능을 실행해도, Web UI에서 설정된 이벤트 로그와 세이프티 애플리케이션은 지워지지 않으므로 주의하십시오.
전체 메모리 클리어 기능에 대한 자세한 내용은 8-4페이지의 8-2 전체 메모리 클리어 기능을 참조하십시오.
전체 메모리 클리어 기능이 실패하는 경우, 세이프티 I/O 블록이 고장일 수 있습니다. 가까운 오므론 지점 또는 영업소로 문의하십시오.

AI 번역본
-For Reference Only-

11

문제 해결

본 장에서는 세이프티 I/O 블록에서 에러가 발생하고 있는지 확인하는 방법과, 에러가 발생했을 때 문제 해결을 수행하는 방법에 대해 설명합니다.

11-1 에러 확인 11-2
11-1-1 에러 알림 방법 및 확인해야 할 정보.....11-2
11-1-2 에러 확인 방법.....11-2
11-1-3 운전 상태 모니터 기능.....11-3

11-2 이벤트를 통한 에러 확인 및 문제 해결..... 11-6
11-2-1 이벤트 로그 기능 11-6
11-2-2 Sysmac Studio를 사용한 이벤트 확인 11-6
11-2-3 Web UI를 사용한 이벤트 확인 11-9
11-2-4 이벤트 상세 및 문제 해결..... 11-12

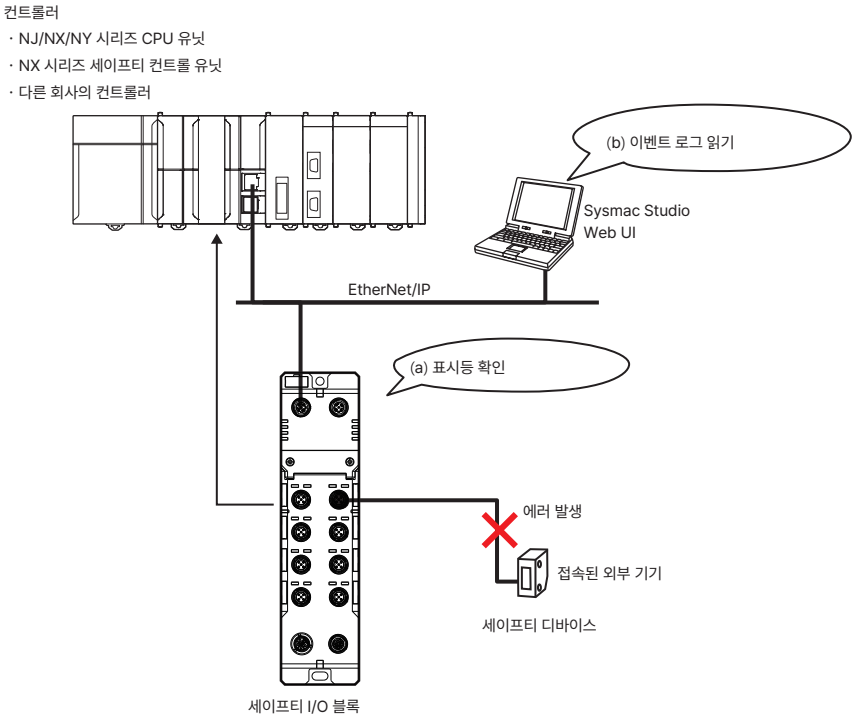
AI 번역본
-For Reference Only-

11-1 에러 확인

본 절에서는 에러 알림 및 확인 방법, 그리고 에러 확인을 위한 기본 순서에 대해 설명합니다.

11-1-1 에러 알림 방법 및 확인해야 할 정보

세이프티 I/O 블록이 에러를 검출하면 다음과 같은 방법으로 알림을 받습니다.
에러 알림을 받으면 유닛의 상태를 확인하고 시정 조치를 취하십시오.



기호	알림 방법	확인 방법	참조
(a)	표시등에 의한 세이프티 I/O 블록의 에러 알림	세이프티 I/O 블록의 각 표시등의 상태를 눈으로 확인합니다.	3-5페이지의 3-2-1 상태 표시등 3-8페이지의 3-2-2 I/O 표시등
(b)	이벤트에 의한 세이프티 I/O 블록의 에러 발생 및 그에 관한 정보 알림	Sysmac Studio의 CIP Safety Monitor 화면 또는 Web UI의 운전 상태 모니터 화면에서 세이프티 I/O 블록의 이벤트를 읽어 확인합니다.	11-6페이지의 11-2 이벤트를 통한 에러 확인 및 문제 해결

AI 번역본
-For Reference Only-

11-1-2 에러 확인 방법

다음 표는 에러 확인을 위한 기본 순서를 나타냅니다.

단계	항목	설명	참조
1	에러 발생 확인	표시등의 점등 상태를 사용하여 에러가 발생했는지 확인합니다.	3-5페이지의 3-2-1 상태 표시등 3-8페이지의 3-2-2 I/O 표시등

단계	항목	설명	참조
		↓	
2	에러 원인 특정	에러가 있는 경우, 원인을 특정하기 위해 다음 확인을 수행합니다.	-
		세이프티 I/O 블록의 각 상태 정보를 확인합니다.	11-3페이지의 11-1-3 운전 상태 모니터 기능
		세이프티 I/O 블록의 이벤트 로그를 확인합니다.	11-6페이지의 11-2 이벤트를 통한 에러 확인 및 문제 해결
		↓	
3	에러 원인에 대한 대처	에러 원인을 특정한 후, 이를 해소하기 위한 적절한 조치를 취합니다.	-

11-1-3 운전 상태 모니터 기능

운전 상태 모니터 기능은 세이프티 I/O 블록의 각 상태 정보를 표시합니다.

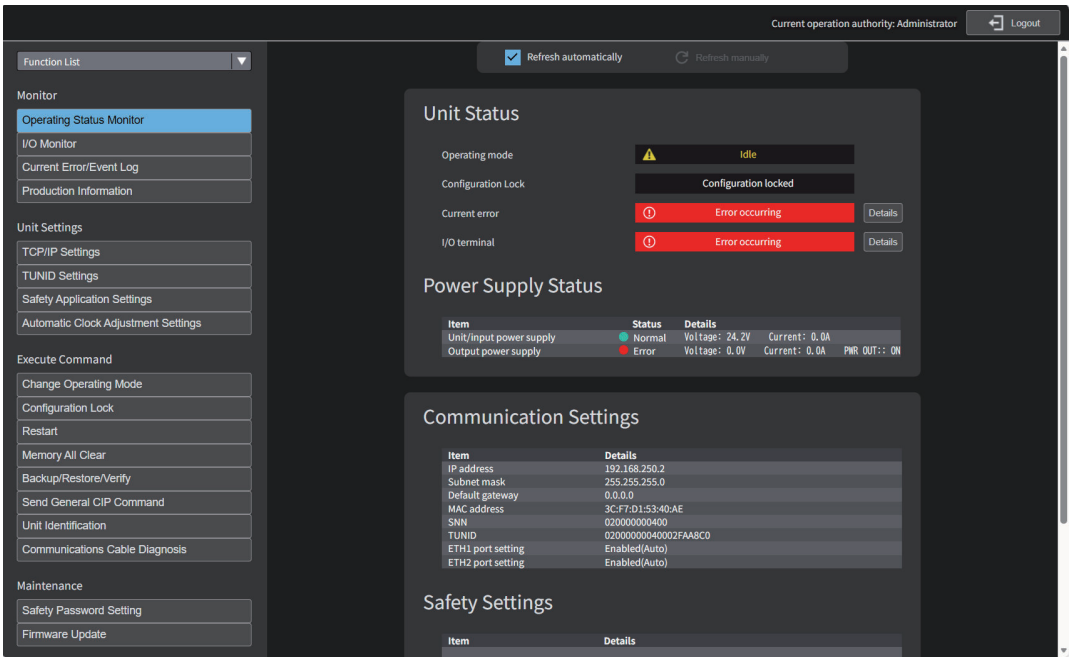
운전 상태 모니터 기능의 목적

운전 상태 모니터 기능의 목적은 각 상태 정보를 통해 세이프티 I/O 블록의 현재 상태를 파악하는 것입니다.

운전 상태 모니터 기능 사용 순서

Web UI의 운전 상태 모니터 화면에서 해당 유닛의 운전 상태를 확인하십시오.

AI 번역본
-For Reference Only-



운전 상태 모니터 기능 상세

운전 상태 모니터 기능을 사용하면 유닛 상태, 전원 공급 상태, 커넥션 상태, 통신 설정, 세이프티 **설정을 확인할 수 있습니다.**

● 유닛 상태

유닛 상태에는 운전 모드, 컨피규레이션 잠금, 현재 에러, I/O 단자가 표시됩니다.

a. 운전 모드

현재 운전 모드가 표시됩니다. 운전 모드에 대한 자세한 내용은 6-47페이지의 6-8 운전 모드를 참조하십시오.

b. 현재 에러

현재 에러로 표시되는 정보는 다음과 같습니다.

표시	설명
Normal	유닛이 정상 상태입니다
Error occurring	유닛에서 에러가 발생하고 있습니다

Error occurring이 표시된 상태에서 Details 버튼을 클릭하면 현재 에러/이벤트 로그 화면으로 전환됩니다.

AI 번역본
For Reference Only

c. 컨피규레이션 잠금

컨피규레이션 잠금으로 표시되는 정보는 다음과 같습니다.

표시	설명
Configuration locked	컨피규레이션이 잠겨 있습니다.
Configuration unlocked	컨피규레이션이 잠금 해제되어 있습니다.

컨피규레이션 잠금에 대한 자세한 내용은 7-99페이지의 7-17 컨피규레이션 잠금을 참조하십시오.

d. I/O 단자

I/O 단자로 표시되는 정보는 다음과 같습니다.

표시	설명
Normal	세이프티 I/O 단자가 정상입니다.
Error occurring	세이프티 I/O 단자에서 에러가 발생했습니다.

Error occurring이 표시된 상태에서 Details 버튼을 클릭하면 I/O 모니터 화면으로 전환됩니다.

● 전원 공급 상태

전원 공급 상태에는 각 전원 단자의 상태와 값이 표시됩니다. 다음 정보가 표시됩니다.

항목	설명
Status	정상 또는 에러*1
Details	전압값 및 전류값

***1.** 출력 전원(PWR 출력 포트)을 사용하지 않는 경우, 출력 전원(PWR 출력 포트)의 Status 필드에 OFF가 표시됩니다.

● 통신 설정

통신 설정에는 각종 통신 설정 정보가 표시됩니다. 다음 정보가 표시됩니다.

- IP 주소
- 서브넷 마스크
- 디폴트 게이트웨이
- MAC 주소
- SNN(Safety Network Number)
- TUNID(Target Unit Network Identifier)
- ETH1 포트의 유효/무효 여부, 통신 속도, 통신 모드
- ETH2 포트의 유효/무효 여부, 통신 속도, 통신 모드

● 세이프티 설정

세이프티 설정에는 각종 세이프티 설정 정보가 표시됩니다. 다음 정보가 표시됩니다.

항목	설명
Configuration	구성됨 또는 구성되지 않음
Rotary switch (SETTING)	SETTING의 로터리 스위치 값
CFUNID	configuration unique identification(CFUNID)의 값
Application name	설정된 세이프티 애플리케이션의 이름
Creator name	설정된 세이프티 애플리케이션 작성자의 이름
Comment	임의의 코멘트
SCCRC	safety configuration CRC(SCCRC)의 값
SCTS	safety configuration time stamp(SCTS)의 값

사본 역본
-For Reference Only-

또한 모든 컨피규레이션 어셈블리 데이터의 값이 파라미터 리스트로 표시됩니다. 자세한 내용은 A-7페이지의 A-2-3 컨피규레이션 어셈블리 데이터를 참조하십시오.

11-2 이벤트를 통한 에러 확인 및 문제 해결

본 절에서는 현재 에러 이벤트 및 이벤트 로그로 에러를 확인하고 문제를 해결하는 방법에 대해 설명합니다.

이벤트 확인에는 Sysmac Studio 또는 Web UI를 사용하십시오.

11-2-1 이벤트 로그 기능

이벤트 로그 기능은 다음 범주로 분류되는 이벤트를 기록합니다.

a. 시스템 이벤트 로그

이 로그는 세이프티 I/O 블록 내부에서 발생한 상태 변화, 세이프티 정지의 원인, 통신 에러 등의 이벤트를 기록합니다.

이는 세이프티 기능이 올바르게 동작하는지 확인하고, 에러 및 정지의 원인을 파악하며, 세이프티를 유지하기 위해 사용하도록 되어 있습니다.

b. 액세스 이벤트 로그

이 로그는 사용자 또는 다른 기기가 세이프티 I/O 블록에 대해 구성한 설정과 실행한 명령을 기록합니다.

이는 데이터 변조나 정보 유출 등 보안 문제가 발생했을 때 그 조작을 수행한 사람을 파악하고, 본인이 그 행위를 부인하지 못하도록 하는 데 사용하도록 되어 있습니다.

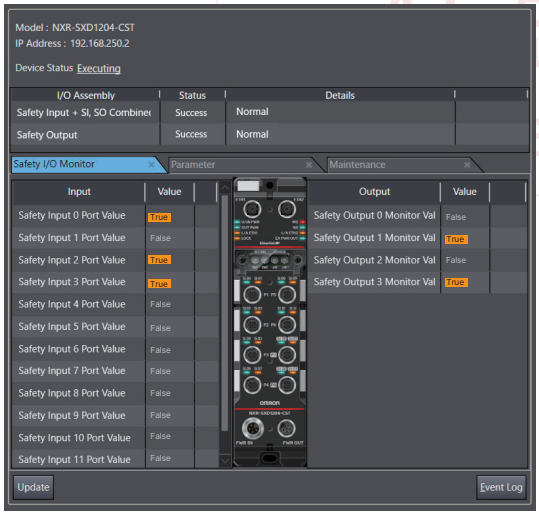
11-2-2 Sysmac Studio를 사용한 이벤트 확인

현재 에러 화면과 이벤트 로그 화면에서 이벤트를 확인할 수 있습니다.

현재 에러 화면 및 이벤트 로그 화면 표시 방법

본 절에서는 Sysmac Studio로 현재 에러 및 이벤트 로그를 표시하는 방법에 대해 설명합니다.

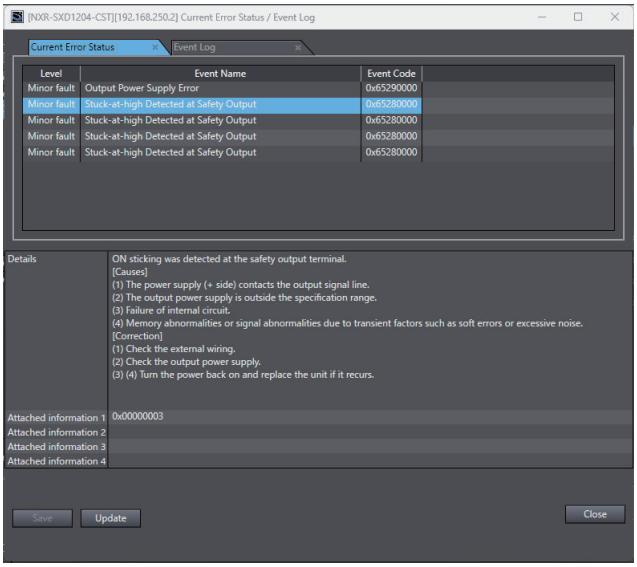
1 Tools - CIP Safety Monitor를 클릭하여 CIP Safety Monitor 화면을 엽니다.



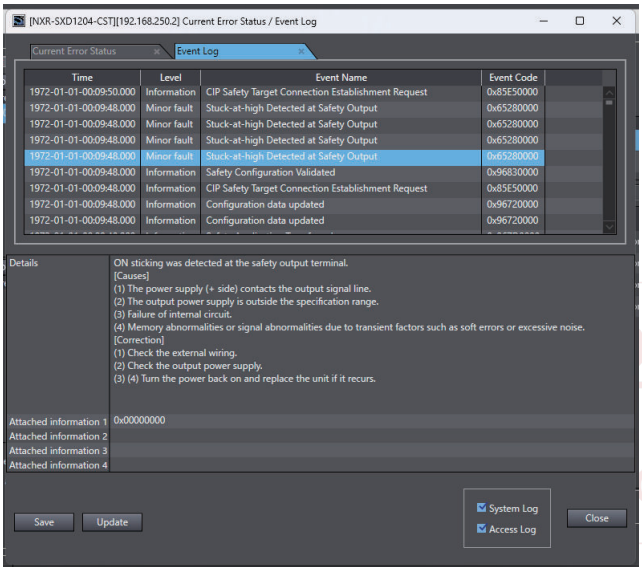
AI 번역본
-Reference Only-

2 CIP Safety Target List에서 세이프티 I/O 블록을 선택합니다.
세이프티 I/O 블록의 디바이스 상태와 현재 I/O 어셈블리 에러가 표시됩니다.

3 오른쪽 아래의 Event Log 버튼을 클릭합니다.
현재 에러가 표시됩니다.



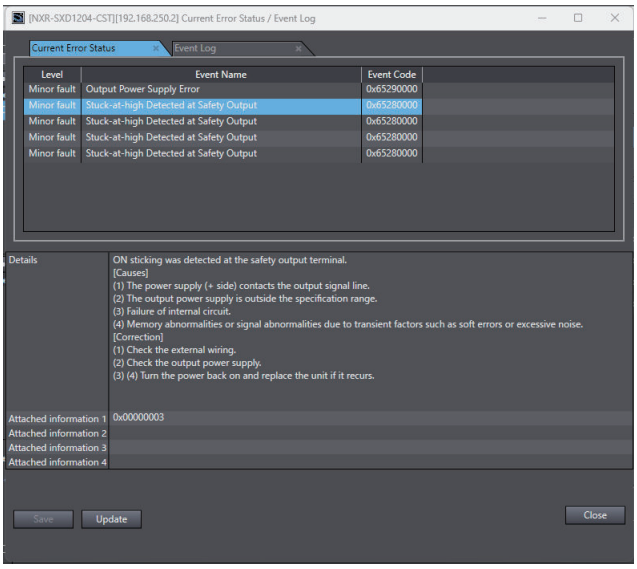
4 Event Log 탭을 클릭합니다.
이벤트 로그가 표시됩니다.



-견본
-ce Only-

현재 에러 화면

본 절에서는 현재 에러 화면의 표시 항목 및 조작 버튼의 기능에 대해 설명합니다.



· 표시 항목

항목	설명
Level	에러(이벤트)가 제어에 미치는 영향의 수준을 나타냅니다.
Event name	발생한 이벤트의 이름을 표시합니다.
Event code	세이프티 I/O 블록에서 발생한 에러(이벤트)의 코드입니다.
Details	선택한 이벤트의 원인, 대책, 첨부 정보를 표시합니다.
Attached information 1 to 4	

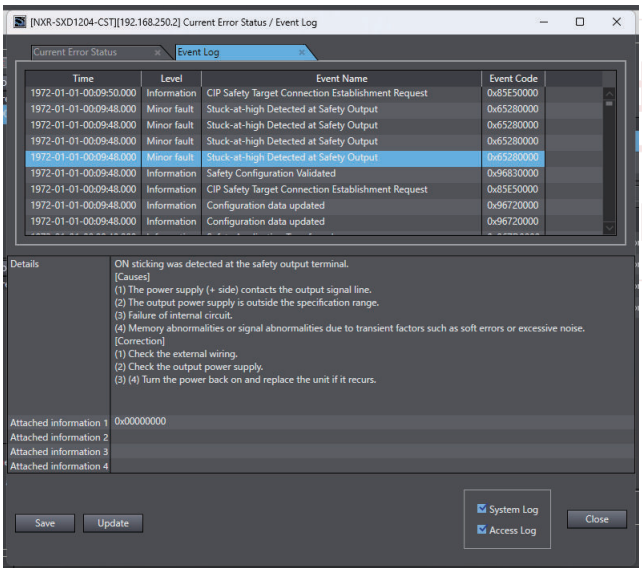
· 조작 버튼

a) Update

현재 에러 정보를 최신 정보로 업데이트합니다.

이벤트 로그 화면

이벤트 로그 화면의 표시 항목과 상세는 다음과 같습니다.



· 표시 항목

항목	설명
Date/Time	이벤트가 발생한 날짜와 시간을 표시합니다. *1
Level	에러(이벤트)가 제어에 미치는 영향의 수준을 나타냅니다.
Event name	발생한 이벤트의 이름을 표시합니다. 이 유닛은 최근 100건의 이벤트를 표시할 수 있습니다.
이벤트 코드	세이프티 I/O 블록에서 발생한 에러(이벤트)의 코드입니다.
상세	선택한 이벤트의 원인, 대책 및 첨부 정보를 표시합니다.
첨부 정보 1~4	

***1.** 이 유닛에 시간 정보가 없는 경우 "-----"가 표시됩니다.

・조작 버튼

a) Update

이벤트 로그의 데이터를 최신 데이터로 업데이트합니다.

b) Save

이벤트 로그를 저장합니다.

c) Clear

이벤트 로그를 지웁니다. 지우려면 세이프티 패스워드가 필요합니다.

d) "System log" 및 "Access log" 확인란

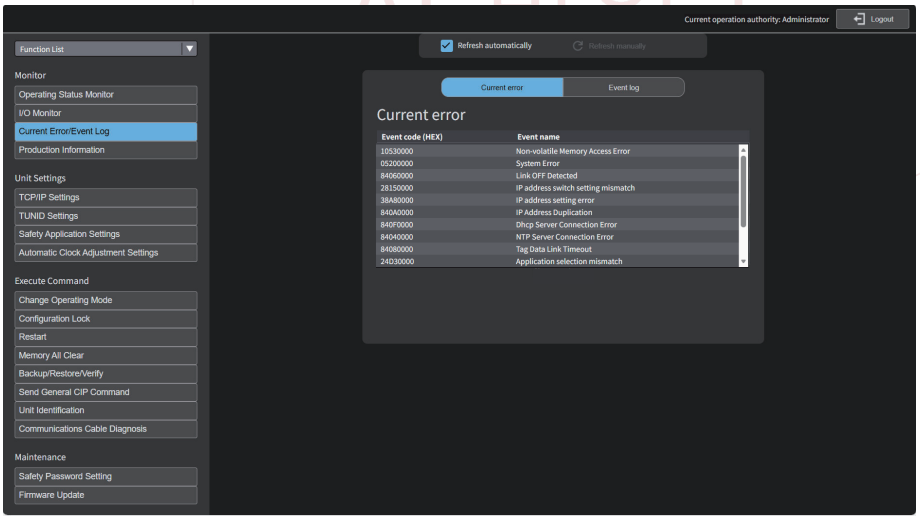
선택한 로그를 표시합니다. 두 확인란은 기본적으로 모두 선택되어 있습니다.

11-2-3 Web UI를 이용한 이벤트 확인

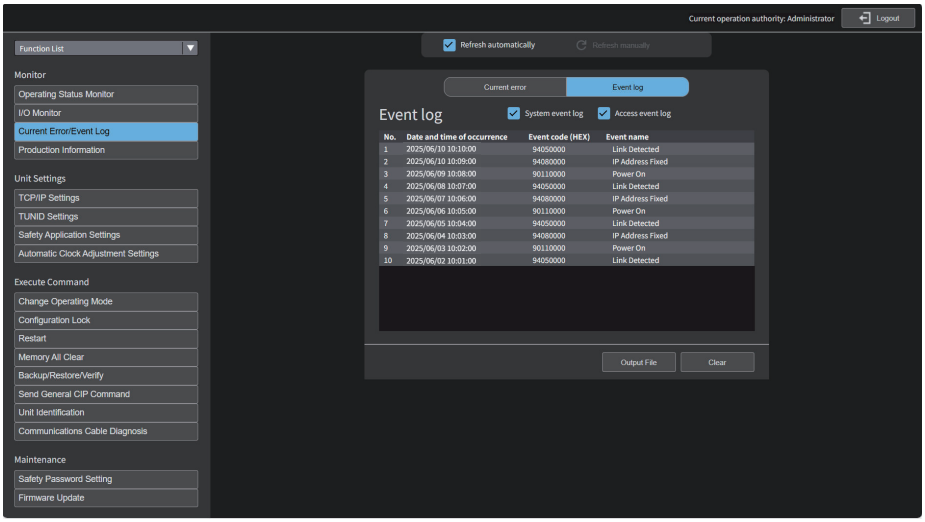
Web UI의 Current Error/Event Log 화면에서 이벤트를 확인합니다.
Current Error/Event Log 화면에는 해당 유닛의 현재 에러 및 이벤트 로그가 표시됩니다.
이벤트 로그는 CSV 형식으로 PC에 저장할 수 있습니다. 또한 이벤트 로그는 세이프티 I/O 블록의 내부 메모리에서 지울 수 있습니다.

Current Error 화면 및 Event Log 화면 표시 방법

1 왼쪽 메뉴에서 Current Error/Event Log를 클릭합니다.
다음과 같은 Current error 화면이 표시됩니다.

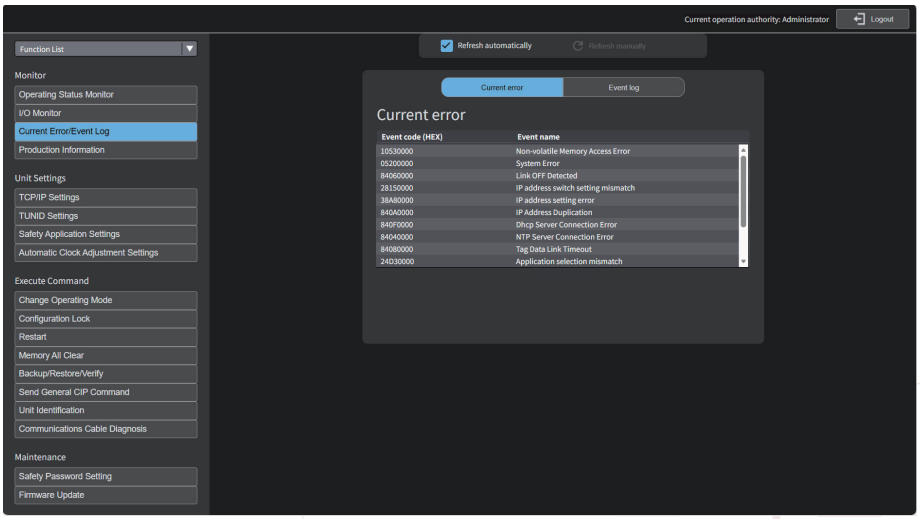


2 Event log 버튼을 클릭합니다.
다음과 같은 Event log 화면이 표시됩니다.



Current Error 화면

Current error 화면에는 현재 에러에 대한 다음 정보가 표시됩니다.

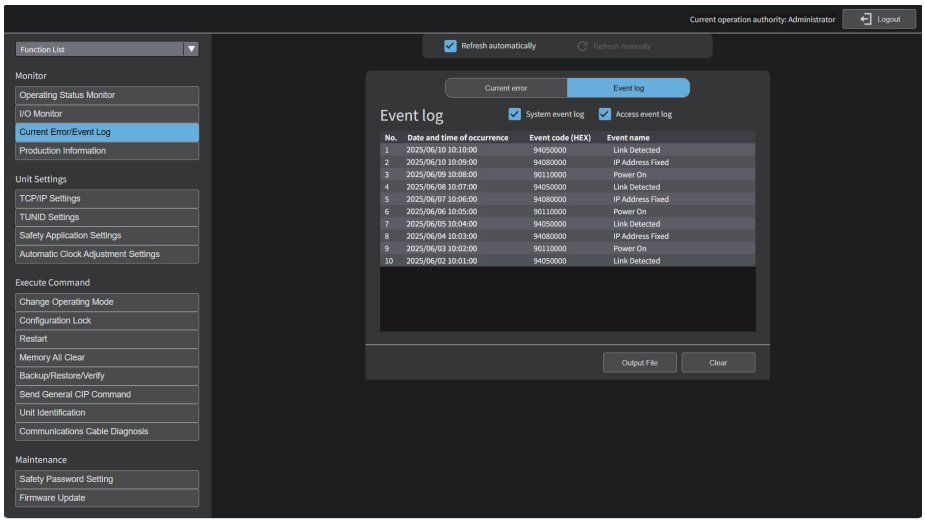


For Reference Only-

항목	설명
이벤트 코드 (Hex)	발생한 에러의 이벤트 코드
이벤트 이름	발생한 에러의 이벤트 이름
첨부 정보	발생한 이벤트의 첨부 정보

Event Log 화면

Event log 화면에는 지금까지 발생한 이벤트 로그에 대한 다음 정보가 표시됩니다.



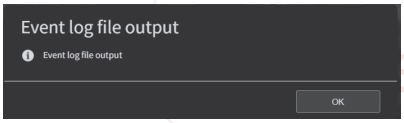
항목	설명
발생 일시	이벤트가 발생한 시간 및 날짜
레벨	발생한 이벤트의 레벨
이벤트 이름	발생한 이벤트의 이벤트 이름
이벤트 코드 (Hex)	발생한 이벤트의 이벤트 코드
첨부 정보	발생한 이벤트의 첨부 정보

System event log 확인란을 선택하면 시스템 이벤트 로그가 표시됩니다. Access event log 확인란을 선택하면 액세스 이벤트 로그가 표시됩니다. 둘 다 동시에 표시할 수 있습니다.

● 이벤트 로그 저장

이벤트 로그를 저장할 때는 System event log 및 Access event log 확인란의 선택 여부와 관계없이 두 이벤트 로그가 모두 저장됩니다.

1 Event Log 화면에서 Output File 버튼을 클릭합니다.
이벤트 로그가 포함된 파일이 CSV 형식으로 PC의 Downloads 폴더에 저장됩니다. 이 파일에는 시스템 이벤트 및 액세스 이벤트 로그뿐 아니라 펌웨어 버전, 제품 시리얼 번호, IP 주소도 포함됩니다.
다음 메시지가 표시됩니다.



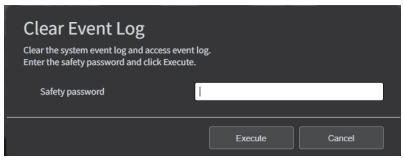
AI 번역본
-For Reference Only-

2 OK 버튼을 클릭합니다.

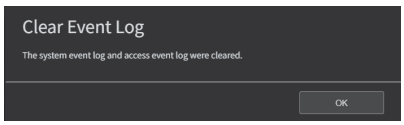
● 이벤트 로그 지우기

이벤트 로그를 지울 때는 System event log 및 Access event log 확인란이 선택된 이벤트 로그가 지워집니다.

1 Event Log 탭 페이지에서 Clear 버튼을 클릭합니다.
다음 메시지가 표시됩니다.



2 세이프티 패스워드를 입력하고 Execute 버튼을 클릭합니다.
이벤트 로그가 지워지고 다음 메시지가 표시됩니다.



3 OK 버튼을 클릭합니다.

11-2-4 이벤트 상세 및 문제 해결

이 절에서는 이벤트를 확인하고 문제를 해결하는 방법을 설명합니다.
현재 이벤트는 리셋하지 않는 한 유지됩니다.
이벤트를 리셋하려면 현재 에러의 원인을 제거해야 합니다. 에러의 원인을 제거하지 않고 이벤트를 리셋하면 동일한 이벤트가 다시 발생합니다.

이벤트 리스트

이 절에서는 발생할 수 있는 이벤트(에러)를 나열합니다.
NJ/NX 시리즈 컨트롤러의 전체 이벤트 코드에 대해서는 NJ/NX 시리즈 트러블슈팅 매뉴얼(자료 번호 W503)을 참조하십시오.
NY 시리즈 컨트롤러의 전체 이벤트 코드에 대해서는 NY 시리즈 트러블슈팅 매뉴얼(자료 번호 W564)을 참조하십시오. NY 시리즈 컨트롤러입니다.

● 이벤트 리스트 보는 법

이벤트 리스트의 내용은 아래에 설명되어 있습니다.

항목	설명
이벤트 코드	세이프티 I/O 블록에서 발생한 에러(이벤트)의 코드입니다. 16진수 8자리로 표시됩니다.
이벤트 이름	에러(이벤트)의 이름입니다.
설명	에러(이벤트)에 대한 설명입니다.
원인 (추정 원인)	에러(이벤트)의 추정 원인입니다.

-For Reference Only-

항목	설명
레벨	에러(이벤트)가 제어에 미치는 영향의 정도를 나타냅니다. 약어의 의미는 다음과 같습니다. Maj: 주요 폴트 레벨 Prt: 부분 폴트 레벨 Min: 경미한 폴트 레벨 Obs: 관찰 Info: 정보 기호의 의미는 다음과 같습니다. ○: 시스템에서 정의하는 이벤트 레벨 ⊙: 사용자가 변경할 수 있는 이벤트 레벨*1
참조	에러(이벤트)에 대한 상세 내용이 있는 페이지입니다.

***1.** 이 기호는 사용자가 이벤트 레벨을 변경할 수 있는 이벤트에만 표시됩니다.

● 이벤트 리스트

이벤트 코드	이벤트 이름	설명	추정 원인	레벨				참조
				Prt	Min	Obs	Info	
05200000 hex	시스템 에러	하드웨어의 자체 진단 중에 하드웨어 에러가 검출되었습니다.	· 소프트웨어 에러나 과도한 노이즈 등의 일시적 요인으로 인해 메모리 에러가 발생했습니다 · 하드웨어 고장		○			페이지 11-23
05210000 hex	세이프티 입력 내부 회로 에러	세이프티 입력 단자의 내부 회로에서 폴트가 검출되었습니다.	· 세이프티 입력 단자의 내부 회로에 결함이 있습니다. · 소프트웨어 에러나 과도한 노이즈 등의 일시적 요인으로 인한 메모리 이상 또는 신호 이상		○			페이지 11-23
05220000 hex	테스트 출력 내부 회로 에러	테스트 출력 단자의 내부 회로에서 폴트가 검출되었습니다.	· 테스트 출력 단자의 내부 회로에 결함이 있습니다. · 소프트웨어 에러나 과도한 노이즈 등의 일시적 요인으로 인한 메모리 이상 또는 신호 이상		○			페이지 11-24
05230000 hex	세이프티 출력 내부 회로 에러	세이프티 출력 단자의 내부 회로에서 폴트가 검출되었습니다.	· 세이프티 출력 단자의 내부 회로에 결함이 있습니다. · 소프트웨어 에러나 과도한 노이즈 등의 일시적 요인으로 인한 메모리 이상 또는 신호 이상		○			페이지 11-24
155E0000 hex	비휘발성 메모리 액세스 에러	비휘발성 메모리에서의 읽기 또는 쓰기에 실패했습니다.	· 잘못된 설정 데이터 · 설정 데이터 쓰기 중 정전 · 비휘발성 메모리 고장		○			페이지 11-25

AI 번역본
-For Reference Only-

이벤트 코드	이벤트 이름	설명	추정 원인	레벨				참조
				Prt	Min	Obs	Info	
24D30000 hex	세이프티 애플리케이션의 로터리 스위치 설정 무효	세이프티 애플리케이션의 로터리 스위치 설정이 무효합니다.	세이프티 애플리케이션의 로터리 스위치 설정이 무효합니다.		○			페이지 11-26
28150000 hex	컨피규레이션 잠금 후 로터리 스위치 설정 변경 됨	컨피규레이션이 잠긴 시점의 로터리 스위치 설정과 현재 설정이 일치하지 않습니다.	컨피규레이션이 잠긴 후 로터리 스위치가 변경된 상태로 유닛이 시작되었습니다.		○			페이지 11-27
359E0000 hex	로터리 스위치 설정이 세이프티 애플리케이션에 대해 무효한지 확인	IP 주소를 설정할 수 없는 상태에서 IP 주소가 변경되었습니다.	· IP 주소를 설정할 수 없는 상태에서 IP 주소용 로터리 스위치가 변경된 후 유닛이 시작되었습니다. · IP 주소를 설정할 수 없는 상태에서 DHCP 서버 설정이 변경되어 다른 IP 주소가 할당되었습니다.		○			페이지 11-28
38A80000 hex	IP 주소 설정 에러	IP 주소 설정에서 에러가 검출되었습니다.	· 잘못된 설정 데이터 · TCP/IP 설정 쓰기 중 정전 · DHCP 서버에서 얻은 IP 주소가 무효합니다. · 비휘발성 메모리 액세스 에러		○			페이지 11-29
38A90000 hex	TUNID 설정 후 IP 주소 변경	TUNID 설정 에러가 검출되었습니다.	· TUNID 설정 후 IP 주소용 로터리 스위치가 변경되어 유닛이 시작되었습니다. · TUNID 설정 후 DHCP 서버 설정이 변경되어 TUNID 설정 시와 다른 IP 주소가 할당 되었습니다.		○			페이지 11-30
55030000 hex	듀얼 채널 출력 간 데이터 에러	잘못된 세이프티 출력 데이터가 기록되었습니다.	듀얼 채널에 대해 설정된 세이프티 출력에 서로 다른 값이 기록되었습니다.		○			페이지 11-31
65210000 hex	출력 전원 차단 회로 에러	출력 전원 차단 테스트에서 에러가 검출되었습니다.	배선 에러 또는 하드웨어 고장입니다.		○			페이지 11-31

AI 번역본
-For Reference Only-

이벤트 코드	이벤트 이름	설명	추정 원인	레벨				참조
				Port	Min	Obs	Info	
65220000 hex	세이프티 입력 외부 테스트 신호 실패	세이프티 입력 단자의 테스트 펄스 평가에서 에러가 검출되었습니다.	· 입력 신호선에 양(+) 전원 배선이 접촉되어 있습니다. · 입력 신호선이 단락되었습니다. · 접속된 외부 기기의 고장 · 해당 세이프티 입력 단자와 조합하여 사용하는 테스트 출력 단자에서 에러가 발생하고 있습니다.		○			페이지 11-32
65230000 hex	세이프티 입력 불일치 에러	세이프티 입력 단자의 불일치 평가에서 에러가 검출되었습니다.	· 입력 신호선에 지락 또는 단선이 있습니다. · 접속된 기기에 결함이 있습니다. · 불일치 시간 설정이 잘못되었습니다. · 세이프티 도어 등의 외부 입력 기기로부터의 입력 신호에 채터링이 발생했습니다. · 해당 세이프티 입력 단자와 조합하여 사용하는 테스트 출력 단자에서 에러가 발생하고 있습니다.		○			페이지 11-33
65240000 hex	테스트 출력 과부하 검출	테스트 출력 단자에서 과전류가 검출되었습니다.	· 출력 신호선에 지락이 있습니다. · 접속된 외부 기기의 고장		○			페이지 11-33
65250000 hex	테스트 출력 ON 고착 검출	ON으로 고착된 테스트 출력 단자가 검출되었습니다.	· 출력 신호선에 양(+) 전원 배선이 접촉되어 있습니다. · 내부 회로에 결함이 있습니다. · 소프트웨어 에러나 과도한 노이즈 등의 일시적 요인으로 인한 메모리 이상 또는 신호 이상 · 해당 세이프티 입력 단자와 조합하여 사용하는 테스트 출력 단자에서 에러가 발생하고 있습니다.		○			페이지 11-34

AI 번역본
-For Reference Only-

이벤트 코드	이벤트 이름	설명	추정 원인	레벨				참조
				Prt	Min	Obs	Info	
65270000 hex	세이프티 출력 단락 검출	세이프티 출력 단자에서 지락이 검출되었습니다.	출력 신호선에 지락이 있습니다.		○			페이지 11-34
65280000 hex	세이프티 출력 ON 고착 검출	ON으로 고착된 세이프티 출력 단자가 검출되었습니다.	· 출력 신호선에 양(+) 전원 배선이 접촉되어 있습니다. · 출력 전원이 규격을 벗어났습니다. · 내부 회로에 결함이 있습니다. · 소프트웨어 에러나 과도한 노이즈 등의 일시적 요인으로 인한 메모리 이상 또는 신호 이상		○			페이지 11-35
65290000 hex	출력 전원 공급 에러	잘못된 출력 전원이 검출되었습니다.	· 출력 전원이 연결되어 있지 않습니다. · 출력 전원의 전압이 검출 임계값보다 낮아져 출력 전원이 차단되었습니다. · 출력 전원의 전압이 검출 임계값보다 높아져 출력 전원이 차단되었습니다. · 출력 전원의 전류가 검출 임계값보다 높아져 출력 전원이 차단되었습니다.		○			페이지 11-36
652B0000 hex	EDM 에러	EDM에서 에러가 검출되었습니다.	· 출력 신호선이 단선되었습니다. · 출력 신호선에 지락이 있습니다. · 출력 신호선이 전원 배선과 접촉되어 있지 않습니까? · 외부 배선 기기인 컨택터 및 릴레이 접점의 용착 · 외부 배선 기기의 단선 또는 지락		○			페이지 11-37
84040000 hex	NTP 서버 접속 에러	NTP 서버와의 접속에 실패했습니다.	· 잘못된 설정 데이터 · 서버가 다운되었습니다. · 통신 경로에서 에러가 발생했습니다.		○			페이지 11-38

AI 번역본
-For Reference Only-

이벤트 코드	이벤트 이름	설명	추정 원인	레벨				참조
				Prt	Min	Obs	Info	
840F0000 hex	DHCP 서버 접속 에러	DHCP 서버와의 접속에 실패했습니다.	· 서버 설정 에러 · 서버가 다운되었습니다. · 통신 경로에서 에러가 발생했습니다.		○			페이지 11-39
85E20000 hex	IP 주소 중복 에러	IP 주소가 중복되었습니다.	IP 주소가 다른 노드의 IP 주소와 중복되었습니다.		○			페이지 11-40
85E30000 hex	태그 데이터 링크 타임아웃	태그 데이터 링크에서 타임아웃이 발생했습니다.	· 오리지네이터 노드의 전원이 OFF입니다. · 오리지네이터 노드의 통신이 정지되어 있습니다. · EtherNet/IP용 Ethernet 케이블이 접속 해제되어 있습니다. · EtherNet/IP용 Ethernet 케이블이 단선되어 있습니다. · EtherNet/IP 포트로의 링크가 OFF입니다. · 네트워크 통신 부하로 인해 경로에서 패킷 손실이 발생했습니다. · 노이즈		○			페이지 11-41

AI 번역본
-For Reference Only-

이벤트 코드	이벤트 이름	설명	추정 원인	레벨				참조
				Prt	Min	Obs	Info	
85E40000 hex	CIP Safety 타겟 커넥션 타임 아웃	CIP Safety 타겟 커넥션에서 타임아웃이 발생했습니다.	· 케이블이 단선되었습니다. · 오리지네이터 기기가 커넥션을 수락할 수 없는 상태가 되었습니다. · 통신 설정의 타임아웃 값이 너무 짧습니다. · EtherNet/IP 포트 설정의 Packet Filter(Simple) 또는 Packet Filter 기능이나 통신 경로상의 기기에서 오리지네이터 노드로부터의 CIP Safety 패킷이 허용되지 않습니다. • **오리지네이터 노드의 CIP** message server가 Do not **use로 설정되어 있습니다.** · 오리지네이터 노드의 Packet Filter 기능이 활성화된 경우, 타겟 노드로부터의 CIP Safety 패킷이 허용되지 않습니다. · 노이즈 • **EtherNet/IP 포트 설정에서 CIP Safety 통신이 Do not use로** 설정되어 있습니다.		○			페이지 11-42
652F0000 hex	유닛/입력 전원 전압 규격 벗어남 검출	유닛/입력 전원의 전압이 규격 범위를 벗어난 것으로 검출되었습니다.	유닛/입력 전원의 전압이 규격 범위를 벗어난 것으로 검출되었습니다.			○		페이지 11-43
65300000 hex	유닛/입력 전원 전류 규격 벗어남 검출	유닛/입력 전원의 전류가 규격 범위를 벗어난 것으로 검출되었습니다.	유닛/입력 전원의 전류가 규격 범위를 벗어난 것으로 검출되었습니다.			○		페이지 11-43
65310000 hex	출력 전원 전압 규격 벗어남 검출 됨	출력 전원의 전압이 규격 범위를 벗어난 것으로 검출되었습니다.	출력 전원의 전압이 규격 범위를 벗어난 것으로 검출되었습니다.			○		페이지 11-44

AI 번역본 -For Reference Only-

이벤트 코드	이벤트 이름	설명	추정 원인	레벨				참조
				Port	Min	Obs	Info	
65320000 hex	출력 전원 전류 규격 벗어남 검출 됨	출력 전원의 전류가 규격 범위를 벗어난 것으로 검출되었습니다.	출력 전원의 전류가 규격 범위를 벗어난 것으로 검출되었습니다.			○		페이지 11-44
85E10000 hex	링크 OFF 검출	Ethernet 링크 OFF가 검출되었습니다.	· Ethernet 케이블이 단선, 접속 해제 또는 헐거워짐 · Ethernet 스위치의 전원이 OFF되어 있습니다. · 통신 속도 불일치 · 노이즈 · 재시작을 실행하거나 메모리 전체 클리어를 실행하십시오.			○		페이지 11-45
85E50000 hex	CIP Safety 타겟 커넥션 오픈 요청	CIP Safety 오리지네이터로부터 커넥션 오픈 요청이 있었습니다.	CIP Safety 오리지네이터로부터 커넥션 오픈 요청이 있었습니다.				○	페이지 11-45
90110000 hex	전원 ON	전원이 ON되었습니다.	전원이 ON되었습니다.				○	페이지 11-46
94080000 hex	IP 주소 확정	올바른 IP 주소가 결정되어 Ethernet 통신을 시작할 수 있습니다.	올바른 IP 주소가 결정되어 Ethernet 통신을 시작할 수 있습니다.				○	페이지 11-46
966C0000 hex	컨피규레이션 잠금	컨피규레이션 잠금이 실행되었습니다.	컨피규레이션 잠금 실행				○	페이지 11-46
966D0000 hex	컨피규레이션 잠금 해제	컨피규레이션 잠금 해제가 실행되었습니다.	컨피규레이션 잠금 해제 실행				○	페이지 11-47
96710000 hex	출력 전원 (PWR OUT) OFF 전환	PWR OUT 전원 커넥터에서 공급되는 출력 전원이 OFF 되었습니다.	스루 배선 출력 전원 차단 명령에 의해 스루 배선 출력 전원의 차단이 지시되었습니다.				○	페이지 11-47
96720000 hex	설정 데이터 변경	설정 데이터가 변경되었습니다.	설정 데이터가 변경되었습니다.				○	페이지 11-48
96730000 hex	로그인	로그인함. (Web UI)	Web UI를 사용하여 로그인했습니다.				○	페이지 11-49
96750000 hex	세이프티 애플리케이션 삭제	세이프티 애플리케이션 데이터가 유닛에서 삭제되었습니다.	Web UI로부터 삭제가 접수되었습니다.				○	페이지 11-49

사내 번역본
-For Reference Only-

이벤트 코드	이벤트 이름	설명	추정 원인	레벨				참조
				Prt	Min	Obs	Info	
96760000 hex	세이프티 비밀번호 불일치	세이프티 비밀번호가 필요한 서비스를 실행할 때 비밀번호 불일치가 검출되었습니다.	세이프티 패스워드가 필요한 서비스를 실행할 때 비밀번호 불일치가 검출되었습니다.				○	페이지 11-49
96770000 hex	출력 전원 (PWR OUT) ON 전환	PWR OUT 전원 커넥터에서 공급되는 출력 전원이 ON 되었습니다.	스루 배선 출력 전원 복구 명령에 의해 스루 배선 출력 전원의 복구가 지시되었습니다.				○	페이지 11-50
96780000 hex	펌웨어 업데이트 실행	펌웨어 업데이트가 실행되었습니다.	펌웨어 업데이트가 실행되었습니다.				○	페이지 11-50
96790000 hex	메모리 전체 클리어	메모리 전체 클리어가 실행되었습니다.	메모리 전체 클리어가 실행되었습니다.				○	페이지 11-51
967A0000 hex	링크 검출	Ethernet 링크의 확립이 검출되었습니다.	Ethernet 링크의 확립이 검출되었습니다.				○	페이지 11-51
967B0000 hex	운전 모드 변경	운전 모드 변경이 실행되었습니다.	운전 모드 변경이 실행되었습니다.				○	페이지 11-52
967C0000 hex	세이프티 비밀번호 변경	세이프티 비밀번호가 변경되었습니다.	세이프티 패스워드가 변경되었습니다.				○	페이지 11-52
967D0000 hex	세이프티 애플리케이션 데이터 전송	세이프티 애플리케이션 데이터가 유닛으로 전송되었습니다.	· Web UI를 통한 전송이 접수되었습니다. · 세이프티 컨트롤러로부터 Type 1 Safety Open 요청이 접수되었습니다.				○	페이지 11-53
967E0000 hex	이벤트 로그 지움	이벤트 로그가 지워졌습니다.	이벤트 로그가 지워졌습니다.				○	페이지 11-53
967F0000 hex	백업 실행	백업이 실행되었습니다.	백업이 실행되었습니다.				○	페이지 11-54
96800000 hex	복원 실행	복원이 실행되었습니다.	복원이 실행되었습니다.				○	페이지 11-54
96810000 hex	오므론 보수 점검 실행	오므론 보수 점검 담당자에 의해 점검이 실행되었습니다.	오므론 보수 점검 담당자에 의해 점검이 실행되었습니다.				○	페이지 11-54
96820000 hex	재시작됨	재시작이 실행되었습니다.	재시작이 실행되었습니다.				○	페이지 11-55
96830000 hex	세이프티 컨피규레이션 검증	세이프티 컨피규레이션이 검증되었습니다.	세이프티 컨피규레이션이 검증되었습니다.				○	페이지 11-55

AI 번역본 -For Reference Only-

이벤트 코드	이벤트 이름	설명	추정 원인	레벨				참조
				Part	Min	Obs	Info	
96840000 hex	IP 주소 표시 기능 실행	IP 주소 표시 기능이 실행되었습니다.	SW1 = SW2 = 8로 시작됨 (IP 주소 표시 기능).				○	페이지 11-56
96850000 hex	I/O 배선 체크 기능 실행	I/O 배선 체크 기능이 실행되었습니다.	SW1 = SW2 = E로 시작됨 (I/O 배선 체크 기능).				○	페이지 11-56

이벤트 상세

이 절에서는 각 이벤트에 대한 상세를 설명합니다.

● 이벤트 상세 보는 법

개별 에러(이벤트)를 설명하는 데 사용되는 항목은 다음 에러 테이블 사본에서 설명합니다.

AI 번역본
-For Reference Only-

<table>
<tr><td>이벤트 이름</td><td colspan="2">에러의 이름을 나타냅니다.</td><td>이벤트 코드</td><td colspan="2">에러의 코드를 나타냅니다.</td></tr>
<tr><td>설명</td><td colspan="5">에러에 대한 간단한 설명을 나타냅니다.</td></tr>
<tr><td>발생원</td><td colspan="2">에러의 발생원을 나타냅니다.</td><td>발생원 상세</td><td>에러의 발생원에 대한 상세를 나타냅니다.</td><td>검출 타이밍</td><td>에러가 검출되는 시점을 나타냅니다.</td></tr>
<tr><td>에러 속성</td><td>레벨</td><td>제어에 미치는 영향의 정도를 나타냅니다. *1</td><td>복구 방법</td><td>복구 방법을 나타냅니다. *2</td><td>로그 카테고리</td><td>에러가 어느 로그에 저장되는지를 나타냅니다. *3</td></tr>
<tr><td>영향</td><td>사용자 프로그램</td><td>사용자 프로그램의 실행에 어떤 일이 일어나는지를 나타냅니다. *4</td><td>동작</td><td colspan="3">에러로 인해 발생하는 동작에 대한 특별한 정보를 제공합니다.</td></tr>
<tr><td>원인 및 대책</td><td colspan="2">추정 원인</td><td colspan="2">대책</td><td>예방</td></tr>
<tr><td></td><td colspan="5">에러에 대해 가능한 원인, 대책 및 예방 조치를 나열합니다.</td></tr>
<tr><td>부가 정보</td><td colspan="5">이것은 Sysmac Studio/HMI에 표시되는 부가 정보입니다. *5</td></tr>
<tr><td>주의사항/ 비고</td><td colspan="5">주의사항, 제한 사항 및 보충 정보를 제공합니다. 사용자가 이벤트 레벨을 설정할 수 있는 경우, 설정 가능한 이벤트 레벨, 복구 방법, 동작 정보 및 기타 정보도 함께 제공됩니다.</td></tr>
</table>

***1.** 다음 중 하나입니다.
- Major fault: 주요 폴트 레벨
- Partial fault: 부분 폴트 레벨
- Minor fault: 경미한 폴트 레벨
- Observation
- Information

***2.** 대책 후 컨트롤러의 에러 상태를 리셋하는 방법으로, 다음 중 하나입니다.
- 자동 복구: 에러 원인이 제거되면 정상 상태로 자동 복귀됩니다.
- 에러 리셋: 에러 원인이 제거된 후 에러를 리셋하면 정상 상태로 복귀됩니다.
- 전원 재투입: 에러 원인이 제거된 후 컨트롤러의 전원을 OFF했다가 다시 ON하면 정상 상태로 복귀됩니다.
- 컨트롤러 리셋: 에러 원인이 제거된 후 컨트롤러를 리셋하면 정상 상태로 복귀됩니다.
- 원인에 따라 다름: 복구 방법은 에러의 원인에 따라 다릅니다.

***3.** 다음 중 하나입니다.
- System: 시스템 이벤트 로그
- Access: 액세스 이벤트 로그

***4.** 다음 중 하나입니다.
- Continues: 사용자 프로그램의 실행이 계속됩니다.
- Stops: 사용자 프로그램의 실행이 정지됩니다.
- Starts: 사용자 프로그램의 실행이 시작됩니다.

***5.** HMI 트러블슈터의 적용 범위에 대한 자세한 내용은 NJ/NX 시리즈 트러블슈팅 매뉴얼(자료 번호 W503) 또는 NY 시리즈 트러블슈팅 매뉴얼(자료 번호 W564)을 참조하십시오.

AI 번역본
-For Reference Only-

● 이벤트 설명

이벤트 이름	시스템 에러			**이벤트 코드**	05200000 hex	
설명	하드웨어의 자체 진단 중에 하드웨어 에러가 검출되었습니다.					
발생원	-		**발생원 상세**	-	**검출 타이밍**	상시
에러 속성	**레벨**	경미한 폴트	**복구 방법**	전원을 재투입	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	해당 유닛의 동작이 정지되고 I/O 데이터가 안전 상태로 바뀝니다.		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	· 소프트웨어 에러나 과도한 노이즈 등의 일시적 요인으로 인한 메모리 에러가 발생했습니다 · 하드웨어 고장		전원을 재투입하십시오. 에러가 다시 발생하면 유닛을 교체하십시오.		전원을 재투입하여 정상 동작으로 복구되는 경우, 유닛 근처에 과도한 노이즈가 있을 수 있습니다. 노이즈 대책을 실시하십시오.	
부가 정보	부가 정보 1: 시스템 정보 부가 정보 2: 시스템 정보 부가 정보 3: 시스템 정보 부가 정보 4: 시스템 정보					
주의사항/ 비고	없음					

이벤트 이름	세이프티 입력 내부 회로 에러			**이벤트 코드**	05210000 hex	
설명	세이프티 입력 단자의 내부 회로에서 폴트가 검출되었습니다.					
발생원	-		**발생원 상세**	-	**검출 타이밍**	· 대기 중 · 실행 중일 때
에러 속성	**레벨**	경미한 폴트	**복구 방법**	· 전원을 재투입 · 재시작을 실행	**로그 카테고리**	시스템
영향	사용자 프로그램	계속	동작	전원이 재투입될 때까지 해당 세이프티 입력 단자는 안전 상태로 유지됩니다.		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	세이프티 입력 단자의 내부 회로에 결함이 있습니다.		전원을 재투입하십시오. 에러가 다시 발생하면 유닛을 교체하십시오.		전원을 재투입하여 정상 동작으로 복구되는 경우, 유닛 근처에 과도한 노이즈가 있을 수 있습니다. 노이즈 대책을 실시하십시오.	
	소프트웨어 에러나 과도한 노이즈 등의 일시적 요인으로 인한 메모리 이상 또는 신호 이상					
부가 정보	부가 정보 1: 단자 번호					
주의사항/ 비고	없음					

Advance
For Reference Only

이벤트 이름	테스트 출력 내부 회로 에러			이벤트 코드		05220000 hex
설명	테스트 출력 단자의 내부 회로에서 폴트가 검출되었습니다.					
발생원	-		발생원 상세	-	검출 타이밍	· 대기 중 · 실행 중일 때
에러 속성	레벨	경미한 폴트	복구 방법	· 전원을 재투입 · 재시작을 실행	로그 카테고리	시스템
영향	사용자 프로그램	계속	동작	해당 테스트 출력 단자는 전원이 재투입될 때까지 안전 상태로 유지됩니다. 또한, 해당 테스트 출력 단자를 테스트 소스로 사용하는 세이프티 입력 단자에서 세이프티 입력에서의 외부 테스트 신호 실패 이벤트(65220000 hex)가 발생합니다.		

원인 및 대책	추정 원인	대책	예방
	테스트 출력 단자의 내부 회로에 결함이 있습니다.	전원을 재투입하십시오. 에러가 다시 발생하면 유닛을 교체하십시오.	전원을 재투입하여 정상 동작으로 복구되는 경우, 유닛 근처에 과도한 노이즈가 있을 수 있습니다. 노이즈 대책을 실시하십시오.
	소프트웨어 에러나 과도한 노이즈 등의 일시적 요인으로 인한 메모리 이상 또는 신호 이상		
부가 정보	부가 정보 1: 단자 번호		
주의사항/ 비고	없음		

이벤트 이름	세이프티 출력 내부 회로 에러			이벤트 코드		05230000 hex
설명	세이프티 출력 단자의 내부 회로에서 폴트가 검출되었습니다.					
발생원	-		발생원 상세	-	검출 타이밍	· 대기 중 · 실행 중일 때
에러 속성	레벨	경미한 폴트	복구 방법	· 전원을 재투입 · 재시작을 실행	로그 카테고리	시스템
영향	사용자 프로그램	계속	동작	전원이 재투입될 때까지 해당 세이프티 출력 단자는 안전 상태로 유지됩니다.		

원인 및 대책	추정 원인	대책	예방
	세이프티 출력 단자의 내부 회로에 결함이 있습니다.	전원을 재투입하십시오. 에러가 다시 발생하면 유닛을 교체하십시오.	전원을 재투입하여 정상 동작으로 복구되는 경우, 유닛 근처에 과도한 노이즈가 있을 수 있습니다. 노이즈 대책을 실시하십시오.
	소프트웨어 에러나 과도한 노이즈 등의 일시적 요인으로 인한 메모리 이상 또는 신호 이상		
부가 정보	부가 정보 1: 단자 번호		
주의사항/ 비고	없음		

이벤트 이름	비휘발성 메모리 액세스 에러			**이벤트 코드**	155E0000 hex	
설명	비휘발성 메모리에서의 읽기 또는 쓰기에 실패했습니다.					
발생원	-		**발생원 상세**	-	**검출 타이밍**	상시
에러 속성	**레벨**	경미한 폴트	**복구 방법**	· 전원을 재투입 · 재시작을 실행 · 설정을 다운로드한 후 자동 복구	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	해당 유닛의 동작이 정지되고 I/O 데이터가 안전 상태로 바뀝니다.		

원인 및 대책	**추정 원인**	**대책**	**예방**
	잘못된 설정 데이터	부가 정보에서 에러의 원인을 확인하십시오. · 부가 정보 1이 01 hex인 경우 전원을 재투입하십시오. · 부가 정보 1이 02 hex인 경우 부가 정보 2의 값에 따라 다음을 실시하십시오. 02xx ~ 05xx hex: 해당 설정을 다시 구성하십시오. 20xx hex: - -CST 모델의 경우, 전체 메모리 클리어를 실행한 후 설정을 다시 구성하십시오. - -EIT 모델의 경우, 로터리 스위치를 SW1 = SW2 = 0으로 맞춘 후, 전체 메모리 클리어를 실행하고 세이프티 애플리케이션 설정을 다시 구성하십시오. 21xx hex: 세이프티 애플리케이션을 다시 구성하십시오. FExx hex: 펌웨어를 업데이트하십시오. 위 조치로도 복구되지 않으면 유닛을 교체하십시오.	없음
	설정 데이터 쓰기 중 정전		설정 데이터를 쓰는 동안에는 해당 유닛의 전원을 OFF하지 마십시오.
	비휘발성 메모리 고장		없음

AI 번역본
-For Reference Only-

부가 정보	부가 정보 1: 원인 01 hex: 비휘발성 메모리 액세스 실패 02 hex: 데이터 손상 부가 정보 2: 검출 대상 02xx hex: 링크 설정 03xx hex: Ethernet 포트 사용/사용 안 함 설정 04xx hex: SNTP 설정 05xx hex: 스루 배선 출력 전원 차단 기능 사용/사용 안 함 설정 20xx hex: 기타 세이프티 관련 데이터 21xx hex: 세이프티 애플리케이션 데이터 80xx hex: QoS 설정 81xx hex: LLDP 기능 설정 FExx hex: 펌웨어 데이터 그 외: 기타 시스템 데이터
주의사항/ 비고	없음

이벤트 이름	세이프티 애플리케이션의 로터리 스위치 설정 무효			**이벤트 코드**	24D30000 hex	
설명	세이프티 애플리케이션의 로터리 스위치 설정이 무효합니다.					
발생원	-		**발생원 상세**	-	**검출 타이밍**	· 전원 투입 시 · 재시작 실행 시
에러 속성	**레벨**	경미한 폴트	**복구 방법**	· 전원을 재투입 · 재시작을 실행	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	해당 유닛의 동작이 정지되고 I/O 데이터가 안전 상태로 바뀝니다.		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	세이프티 애플리케이션의 로터리 스위치 설정이 무효합니다.		세이프티 애플리케이션의 로터리 스위치 설정이 무효한지 확인하십시오.		없음	
부가 정보	부가 정보 1: 현재 세이프티 애플리케이션의 로터리 스위치 설정값 표시 형식은 [SW1, SW2]입니다. 예: SW1 = 1, SW2 = E인 경우 → 1E					
주의사항/ 비고	없음					

AI 번역본
-For Reference Only-

<table>
<tr><td>이벤트 이름</td><td colspan="2">구성이 잠긴 후 로터리 스위치
설정이 변경됨</td><td>이벤트 코드</td><td colspan="2">28150000 hex</td></tr>
<tr><td>설명</td><td colspan="5">구성이 잠겼을 때의 로터리 스위치 설정과 현재 설정이 일치하지 않습니다.</td></tr>
<tr><td>발생원</td><td colspan="2">-</td><td>발생원 상세</td><td>검출 타이밍</td><td>・전원 투입 시
・재시작 실행 시</td></tr>
<tr><td>에러 속성</td><td>레벨</td><td>경미한 폴트</td><td>복구 방법</td><td>・전원을 재투입
・재시작을 실행</td><td>로그 카테고리</td><td>시스템</td></tr>
<tr><td>영향</td><td>사용자 프로그램</td><td>계속</td><td>동작</td><td colspan="3">해당 유닛의 동작이 정지되고
I/O 데이터가 안전 상태로 바뀝니다.</td></tr>
<tr><td>원인 및 대책</td><td colspan="2">추정 원인
구성이 잠긴 후
로터리 스위치가 변경된
상태로 유닛이
시작되었습니다.</td><td colspan="2">대책
・로터리 스위치의 설정값을
구성이 잠겼을 때의
설정값으로
되돌리십시오.
・구성 잠금을 해제한 후 전체 메모리
클리어를 실행하고
설정을 다시 구성하십시오.

위 대책을 실시한 후에는
전원을 재투입하거나 재시작을
실행하십시오.</td><td>예방
구성이 잠긴 후에는
로터리 스위치의 설정값을
변경하지 마십시오.</td></tr>
<tr><td>부가 정보</td><td colspan="5">부가 정보 1: 로터리 스위치의 현재 설정값
표시 형식은 [SW1, SW2, x161, x160]입니다.
예: SW1=F, SW2=F, x161=0, x160=1인 경우
→ FF01 hex
부가 정보 2: 구성이 잠겼을 때의 로터리 스위치 설정값 표시 형식은
[SW1, SW2, x161, x160]입니다.
예: SW1=3, SW2=3, x161=0, x160=1인 경우
→ 3301 hex</td></tr>
<tr><td>주의사항/ 비고</td><td colspan="5">없음</td></tr>
</table>

AI 번역본
-For Reference Only-

<table>
<tr><td>이벤트 이름</td><td colspan="2">세이프티 애플리케이션의 로터리 스위치 설정이 무효한지 확인</td><td>이벤트 코드</td><td colspan="2">359E0000 hex</td></tr>
<tr><td>설명</td><td colspan="5">IP 주소를 설정할 수 없는 상태에서 IP 주소가 변경되었습니다.</td></tr>
<tr><td>발생원</td><td colspan="2">-</td><td>발생원 상세</td><td>검출 타이밍</td><td>· 전원 투입 시
· 재시작 실행 시</td></tr>
<tr><td>에러 속성</td><td>레벨</td><td>경미한 폴트</td><td>복구 방법</td><td>· 전원을 재투입
· 재시작을 실행</td><td>로그 카테고리</td><td>시스템</td></tr>
<tr><td>영향</td><td>사용자 프로그램</td><td>계속</td><td>동작</td><td colspan="3">해당 유닛의 동작이 정지되고 I/O 데이터가 안전 상태로 바뀝니다.</td></tr>
<tr><td>원인 및 대책</td><td colspan="2">추정 원인</td><td colspan="2">대책</td><td>예방</td></tr>
<tr><td></td><td colspan="2">· IP 주소를 설정할 수 없는 상태에서 IP 주소용 로터리 스위치가 변경된 후 유닛이 시작되었습니다.
· IP 주소를 설정할 수 없는 상태에서 DHCP 서버 설정이 변경되어 다른 IP 주소가 할당되었습니다.</td><td colspan="2">· IP 주소용 로터리 스위치를 원래 값으로 되돌리십시오.
· DHCP 서버 설정을 원래 값으로 되돌리십시오.
· 전체 메모리 클리어를 실행한 후 IP 주소를 다시 설정하십시오.
위 조치로도 복구되지 않으면 유닛을 교체하십시오.</td><td>IP 주소를 설정할 수 없는 상태에서 IP 주소용 로터리 스위치를 조작하거나 DHCP 서버 설정을 변경하지 마십시오.</td></tr>
<tr><td>부가 정보</td><td colspan="5">부가 정보 1: 현재 IP 주소
예: IP 주소가 192.168.250.100인 경우 C0A8FA64 hex.
부가 정보 2: 설정 가능한 상태에서 설정된 IP 주소
예: IP 주소가 192.168.250.100인 경우 C0A8FA64 hex.</td></tr>
<tr><td>주의사항/ 비고</td><td colspan="5">없음</td></tr>
</table>

AI 번역본
-For Reference Only-

<table>
<tr><td>이벤트 이름</td><td colspan="2">IP 주소 설정 에러</td><td>이벤트 코드</td><td colspan="2">38A80000 hex</td></tr>
<tr><td>설명</td><td colspan="5">IP 주소 설정에서 에러가 검출되었습니다.</td></tr>
<tr><td>발생원</td><td colspan="2">-</td><td>발생원 상세</td><td>검출 타이밍</td><td>・전원 투입 시
・재시작 실행 시</td></tr>
<tr><td>에러 속성</td><td>레벨</td><td>경미한 폴트</td><td>복구 방법</td><td>・전원을 재투입
・재시작을 실행</td><td>로그 카테고리</td><td>시스템</td></tr>
<tr><td>영향</td><td>사용자 프로그램</td><td>계속</td><td>동작</td><td colspan="3">EtherNet/IP 통신이 동작하지 않습니다.
CIP Safety 통신이 동작하지 않습니다.</td></tr>
<tr><td rowspan="4">원인 및 대책</td><td colspan="2">추정 원인</td><td colspan="2">대책</td><td>예방</td></tr>
<tr><td colspan="2">잘못된 설정 데이터</td><td colspan="2" rowspan="3">IP 주소는 기본값인 192.168.250.1이 됩니다.
다음 중 하나를 실시하십시오.
・부가 정보에서 에러의 원인을 확인한 후 올바른 값을 다시 설정하십시오.
・전체 메모리 클리어를 실행하거나 설정을 다시 쓰십시오.
・DHCP 서버가 제공하는 IP 주소 설정이 해당 유닛에 지정된 범위 내에 들도록 수정 하십시오.
위 대책을 실시한 후에는 전원을 재투입하거나 재시작을 실행하십시오.
위 조치로도 복구되지 않으면 유닛을 교체하십시오.</td><td>없음</td></tr>
<tr><td colspan="2">TCP/IP 설정 쓰기 중 정전</td><td>TCP/IP 설정을 쓰는 동안에는 해당 유닛의 전원을 OFF하지 마십시오.</td></tr>
<tr><td colspan="2">DHCP 서버에서 취득한 IP 주소가 무효합니다.</td><td>DHCP 서버가 제공하는 IP 주소 설정이 해당 유닛에 지정된 범위 내에 들도록 수정하십시오.</td></tr>
<tr><td colspan="2">비휘발성 메모리 액세스 에러</td><td colspan="2">없음</td></tr>
<tr><td>부가 정보</td><td colspan="5">부가 정보 1: 에러 종류
01 hex: 비휘발성 메모리 액세스 에러
02 hex: 설정 불일치
부가 정보 2: 에러 상세(부가 정보 1이 02 hex인 경우)
11 hex: IP 주소 무효
12 hex: 서브넷 마스크 무효
13 hex: 기본 게이트웨이 무효</td></tr>
<tr><td>주의사항/ 비고</td><td colspan="5">없음</td></tr>
</table>

AI 번역본
-For Reference Only-

<table>
<tr><td>이벤트 이름</td><td colspan="2">TUNID 설정 후 IP 주소 변경</td><td>이벤트 코드</td><td colspan="2">38A90000 hex</td></tr>
<tr><td>설명</td><td colspan="5">TUNID 설정 에러가 검출되었습니다.</td></tr>
<tr><td>발생원</td><td colspan="2">-</td><td>발생원 상세</td><td>검출 타이밍</td><td>· 전원 투입 시
· 재시작 실행 시</td></tr>
<tr><td>에러 속성</td><td>레벨</td><td>경미한 폴트</td><td>복구 방법</td><td>· 전원을 재투입
· 재시작을 실행</td><td>로그 카테고리</td><td>시스템</td></tr>
<tr><td>영향</td><td>사용자 프로그램</td><td>계속</td><td>동작</td><td colspan="3">해당 유닛의 동작이 정지되고
I/O 데이터가 안전 상태로 바뀝니다.</td></tr>
<tr><td rowspan="4">원인 및 대책</td><td colspan="2">추정 원인</td><td colspan="2">대책</td><td>예방</td></tr>
<tr><td colspan="2">TUNID를 설정한 후 IP 주소용 로터리 스위치가 변경된 상태로 유닛이 시작되었습니다.</td><td colspan="2">IP 주소용 로터리 스위치를 TUNID를 설정했을 때의 값으로 되돌리십시오.</td><td rowspan="3">TUNID를 설정한 후에는 IP 주소용 로터리 스위치를 조작하거나 DHCP 서버 설정을 변경하지 마십시오.</td></tr>
<tr><td colspan="2">TUNID를 설정한 후 DHCP 서버 설정이 변경되어 TUNID를 설정했을 때와 다른 IP 주소가 할당되었습니다.</td><td colspan="2">DHCP 서버 설정을 TUNID를 설정했을 때의 값으로 되돌리십시오.</td></tr>
<tr><td colspan="2"></td><td colspan="2">또는 전체 메모리 클리어를 실행한 후 TUNID를 다시 설정하십시오.

위 조치로도 복구되지 않으면 유닛을 교체하십시오.</td></tr>
<tr><td>부가 정보</td><td colspan="5">부가 정보 1: 현재 IP 주소
예: IP 주소가 192.168.250.1인 경우 C0A8FA01 hex.
부가 정보 2: TUNID를 설정했을 때의 IP 주소(TUNID의 IP 주소 부분)
예: IP 주소가 192.168.250.100인 경우 C0A8FA64 hex.</td></tr>
<tr><td>주의사항/ 비고</td><td colspan="5">없음</td></tr>
</table>

AI 번역본
-For Reference Only-

이벤트 이름	듀얼 채널 출력 간 데이터 에러			**이벤트 코드**	55030000 hex	
설명	잘못된 세이프티 출력 데이터가 쓰여졌습니다.					
발생원	—		**발생원 상세**	-	**검출 타이밍**	· 대기 중 · 실행 중일 때
에러 속성	**레벨**	경미한 폴트	**복구 방법**	세이프티 출력 단자를 비활성화하여 복구	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	>해당 세이프티 출력 단자는 에러가 해제될 때까지 안전 상태로 유지됩니다.		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	듀얼 채널로 설정된 세이프티 출력에 서로 다른 값이 쓰여졌습니다.		세이프티 프로그램을 확인하고, 듀얼 채널로 설정된 세이프티 출력에 동일한 값을 쓰십시오.		왼쪽에 제시된 대책을 고려하여 세이프티 프로그램을 설계하십시오.	
부가 정보	부가 정보 1: 단자 번호					
주의사항/ 비고	없음					

이벤트 이름	출력 전원 차단 회로 에러			**이벤트 코드**	65210000 hex	
설명	출력 전원 차단 테스트에서 에러가 검출되었습니다.					
발생원	-		**발생원 상세**	-	**검출 타이밍**	· 전원 투입 시 · 재시작 실행 시
에러 속성	**레벨**	경미한 폴트	**복구 방법**	· 전원을 재투입 · 재시작을 실행	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	해당 유닛은 계속 동작하지만, I/O 데이터는 안전 상태로 유지됩니다.		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	배선 에러 또는 하드웨어 고장입니다.		다음을 확인한 후 정격 전원을 공급하십시오. · 전원 전압이 사양 범위 내에 있습니까? · 배선에 에러나 단선이 없습니까? · 세이프티 출력 단자에 24 VDC가 인가되어 있고, 세이프티 출력 단자가 전원 플러스 배선과 접촉하지 않았습니까? 측정한 전압이 올바른 경우, 유닛이 고장났을 수 있습니다. 이 경우 유닛을 교체하십시오.		왼쪽에 제시된 대책을 고려하여 시스템을 설계하십시오.	
부가 정보	없음					
주의사항/ 비고	없음					

AI 번역본
-For Reference Only-

<table>
<tr><td>이벤트 이름</td><td colspan="2">세이프티 입력에서의 외부 테스트 신호 실패</td><td>이벤트 코드</td><td colspan="2">65220000 hex</td></tr>
<tr><td>설명</td><td colspan="5">세이프티 입력 단자의 테스트 펄스 평가에서 에러가 검출되었습니다.</td></tr>
<tr><td>발생원</td><td colspan="2">-</td><td>발생원 상세</td><td>검출 타이밍</td><td>· 대기 중
· 실행 중일 때</td></tr>
<tr><td>에러 속성</td><td>레벨</td><td>경미한 폴트</td><td>복구 방법</td><td>로그 카테고리</td><td>시스템</td></tr>
<tr><td>영향</td><td>사용자 프로그램</td><td>계속</td><td>동작</td><td colspan="2">해당 세이프티 입력 단자는 에러가 해제될 때까지 안전 상태로 유지됩니다.</td></tr>
<tr><td rowspan="5">원인 및 대책</td><td colspan="2">추정 원인</td><td colspan="2">대책</td><td>예방</td></tr>
<tr><td colspan="2">전원 플러스 배선이 입력 신호 라인과 접촉하고 있습니다.</td><td colspan="2" rowspan="2">외부 배선을 확인하십시오.</td><td rowspan="3">왼쪽에 제시된 대책을 고려하여 파라미터를 설정하고 배선하십시오.</td></tr>
<tr><td colspan="2">입력 신호 라인이 단락되었습니다.</td></tr>
<tr><td colspan="2">접속된 외부 기기의 고장</td><td colspan="2">접속된 외부 기기를 교체하십시오.</td></tr>
<tr><td colspan="2">해당 세이프티 입력 단자와 함께 사용되는 테스트 출력 단자에서 에러가 발생하고 있습니다.</td><td colspan="2">테스트 출력 단자에서 발생한 에러를 확인하고 대책에 제시된 해결 방법을 시도하십시오.</td><td>테스트 출력 단자에서 발생한 에러에 대해 예방에 제시된 해결 방법을 시도하십시오.</td></tr>
<tr><td>부가 정보</td><td colspan="5">부가 정보 1: 단자 번호</td></tr>
<tr><td>주의사항/ 비고</td><td colspan="5">없음</td></tr>
</table>

AI 번역본
-For Reference Only-

이벤트 이름	세이프티 입력의 불일치 에러			**이벤트 코드**	65230000 hex	
설명	세이프티 입력 단자의 불일치 평가에서 에러가 검출되었습니다.					
발생원	-		**발생원 상세**	-	**검출 타이밍**	· Idle 중 · Executing 중
에러 속성	**레벨**	경미한 폴트	**복구 방법**	해당 세이프티 입력 단자를 비활성화하여 복구	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	에러가 해제될 때까지 해당 세이프티 입력 단자는 안전 상태로 유지됩니다.		
원인 및 대책	**추정 원인**		**대책**		**예방책**	
	입력 신호선에 지락 또는 단선이 있습니다.		외부 배선을 확인하십시오.		왼쪽에 제시된 대책을 고려하여 파라미터를 설정하고 시스템을 배선하십시오.	
	접속된 기기가 고장입니다.		접속된 외부 기기를 교체하십시오.			
	불일치 시간의 설정이 잘못되었습니다.		불일치 평가 시간을 수정하십시오. 이것으로 문제가 해결되지 않으면 입력 필터를 사용하여 ON 딜레이 또는 OFF 딜레이를 설정하십시오.			
	세이프티 도어 등 외부 입력 기기로부터의 입력 신호에 채터링이 발생했습니다.					
	해당 세이프티 입력 단자와 조합하여 사용하는 테스트 출력 단자에서 에러가 발생하고 있습니다.		테스트 출력 단자에서 발생한 에러를 확인하고 대책에 명시된 해결 방법을 시도하십시오.		테스트 출력 단자에서 발생하는 에러에 대해 예방책에 명시된 해결 방법을 시도하십시오.	
부가 정보	부가 정보 1: 단자 번호					
주의사항/ 비고	없음					

이벤트 이름	테스트 출력에서 과부하 검출			**이벤트 코드**	65240000 hex	
설명	테스트 출력 단자에서 과전류가 검출되었습니다.					
발생원	-		**발생원 상세**	-	**검출 타이밍**	· Idle 중 · Executing 중
에러 속성	**레벨**	경미한 폴트	**복구 방법**	자동 복구	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	해당 테스트 출력 단자를 테스트 소스로 사용하는 세이프티 입력 단자는 에러가 해제될 때까지 안전 상태로 유지됩니다.		
원인 및 대책	**추정 원인**		**대책**		**예방책**	
	출력 신호선에 지락이 있습니다.		외부 배선을 확인하십시오.		왼쪽에 제시된 대책을 고려하여 파라미터를 설정하고 시스템을 배선하십시오.	
	접속된 외부 기기의 고장		접속된 외부 기기를 교체하십시오.			
부가 정보	부가 정보 1: 단자 번호					
주의사항/ 비고	없음					

이벤트 이름	테스트 출력에서 하이 고착 검출			이벤트 코드		65250000 hex
설명	ON 상태로 고착된 테스트 출력 단자가 검출되었습니다.					
발생원	-		발생원 상세	-	검출 타이밍	· Idle 중 · Executing 중
에러 속성	레벨	경미한 폴트	복구 방법	자동 복구	로그 카테고리	시스템
영향	사용자 프로그램	계속	동작	해당 테스트 출력 단자를 테스트 소스로 사용하는 세이프티 입력 단자는 에러가 해제될 때까지 안전 상태로 유지됩니다.		
원인 및 대책	추정 원인		대책		예방책	
	양극 전원선이 출력 신호선과 접촉되어 있습니다.		외부 배선을 확인하십시오.		왼쪽에 제시된 대책을 고려하여 파라미터를 설정하고 시스템을 배선하십시오.	
	내부 회로가 고장입니다. 소프트웨어 에러나 과도한 노이즈와 같은 일시적 요인으로 인한 메모리 이상 또는 신호 이상		전원을 재투입하십시오. 에러가 다시 발생하면 유닛을 교체하십시오.		전원을 재투입하여 정상 동작으로 복원되면 유닛 주변에 과도한 노이즈가 있을 수 있습니다. 노이즈 대책을 실시하십시오.	
부가 정보	부가 정보 1: 단자 번호					
주의사항/ 비고	없음					

이벤트 이름	세이프티 출력에서 단락 검출			이벤트 코드		65270000 hex
설명	세이프티 출력 단자에서 지락이 검출되었습니다.					
발생원	-		발생원 상세	-	검출 타이밍	· Idle 중 · Executing 중
에러 속성	레벨	경미한 폴트	복구 방법	해당 세이프티 출력 단자를 비활성화하여 복구	로그 카테고리	시스템
영향	사용자 프로그램	계속	동작	에러가 해제될 때까지 해당 세이프티 출력 단자는 안전 상태로 유지됩니다.		
원인 및 대책	추정 원인		대책		예방책	
	출력 신호선에 지락이 있습니다.		외부 배선을 확인하십시오.		왼쪽에 제시된 대책을 고려하여 파라미터를 설정하고 시스템을 배선하십시오.	
부가 정보	부가 정보 1: 단자 번호					
주의사항/ 비고	출력 전원에 이상이 발생하면 세이프티 출력 단자에 지락이 없는 경우에도 이 에러가 등록될 수 있습니다.					

AI 번역본
For Reference Only

<table>
<tr><td>이벤트 이름</td><td colspan="2">세이프티 출력에서 하이 고착 검출</td><td>이벤트 코드</td><td colspan="2">65280000 hex</td></tr>
<tr><td>설명</td><td colspan="5">ON 상태로 고착된 세이프티 출력 단자가 검출되었습니다.</td></tr>
<tr><td>발생원</td><td colspan="2">-</td><td>발생원 상세</td><td>-</td><td>검출 타이밍</td><td>· Idle 중
· Executing 중</td></tr>
<tr><td>에러 속성</td><td>레벨</td><td>경미한 폴트</td><td>복구 방법</td><td>해당 세이프티 출력 단자를 비활성화하여 복구</td><td>로그 카테고리</td><td>시스템</td></tr>
<tr><td>영향</td><td>사용자 프로그램</td><td>계속</td><td>동작</td><td colspan="3">에러가 해제될 때까지 해당 세이프티 출력 단자는 안전 상태로 유지됩니다.</td></tr>
<tr><td rowspan="5">원인 및 대책</td><td colspan="2">추정 원인</td><td colspan="2">대책</td><td colspan="2">예방책</td></tr>
<tr><td colspan="2">양극 전원선이 출력 신호선과 접촉되어 있습니다.</td><td colspan="2">외부 배선을 확인하십시오.</td><td colspan="2" rowspan="2">왼쪽에 제시된 대책을 고려하여 파라미터를 설정하고 시스템을 배선하십시오.</td></tr>
<tr><td colspan="2">출력 전원이 사양 범위를 벗어났습니다.</td><td colspan="2">출력 전원을 확인하십시오.</td></tr>
<tr><td colspan="2">내부 회로가 고장입니다.</td><td colspan="2" rowspan="2">전원을 재투입하십시오.
에러가 다시 발생하면 유닛을 교체하십시오.</td><td colspan="2" rowspan="2">전원을 재투입하여 정상 동작으로 복원되면 유닛 주변에 과도한 노이즈가 있을 수 있습니다. 노이즈 대책을 실시하십시오.</td></tr>
<tr><td colspan="2">소프트웨어 에러나 과도한 노이즈와 같은 일시적 요인으로 인한 메모리 이상 또는 신호 이상</td></tr>
<tr><td>부가 정보</td><td colspan="5">부가 정보 1: 단자 번호</td></tr>
<tr><td>주의사항/ 비고</td><td colspan="5">출력 전원에 이상이 발생하면 세이프티 출력 단자가 ON 상태로 고착되지 않은 경우에도 이 에러가 등록될 수 있습니다.</td></tr>
</table>

AI 번역본
-For Reference Only-

이벤트 이름	출력 전원 에러			**이벤트 코드**	65290000 hex	
설명	출력 전원이 올바르지 않은 것이 검출되었습니다.					
발생원	-		**발생원 상세**	-	**검출 타이밍**	상시
에러 속성	**레벨**	경미한 폴트	**복구 방법**	자동 복구. 단, 출력 전원의 전류가 검출 임계값을 초과하여 출력 전원이 차단된 경우에는 출력 전원의 전원을 재투입한 후 복구됩니다.	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	해당 유닛은 계속 동작하지만 출력 데이터에 대해서는 안전 상태가 유지됩니다.		

원인 및 대책	**추정 원인**	**대책**	**예방책**
	· 출력 전원이 접속되어 있지 않습니다. · 출력 전원의 전압이 검출 임계값 아래로 떨어져 출력 전원이 차단되었습니다. · 출력 전원의 전압이 검출 임계값을 초과하여 상승해 출력 전원이 차단되었습니다. · 출력 전원의 전류가 검출 임계값을 초과하여 상승해 출력 전원이 차단되었습니다.	다음을 확인한 후 정격 전원을 공급하십시오. · 전원 전압이 사양 범위 내에 있습니까? · 배선 오류나 단선이 없습니까? · 전원 배선의 단락으로 인한 과전류가 발생하지 않습니까? 측정된 전압이 정상이면 유닛이 고장일 수 있습니다. 이 경우 유닛을 교체하십시오.	왼쪽에 제시된 대책을 고려하여 시스템을 설계하십시오.
부가 정보	없음		
주의사항/ 비고	없음		

AI 번역본
-For Reference Only-

이벤트 이름	EDM 에러			**이벤트 코드**	652B0000 hex	
설명	EDM에서 에러가 검출되었습니다.					
발생원	-		**발생원 상세**	-	**검출 타이밍**	Executing 중
에러 속성	**레벨**	경미한 폴트	**복구 방법**	FB의 출력과 피드백 입력의 관계를 비활성화하여 복구	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	에러가 해제될 때까지 해당 세이프티 출력 단자는 안전 상태로 유지됩니다.		

원인 및 대책	**추정 원인**	**대책**	**예방책**
	다음 항목을 확인하십시오. ・출력 신호선이 단선되었습니다. ・출력 신호선에 지락이 있습니다. 　・출력 신호선이 전원과 접촉되어 있습니까? ・외부 배선 기기인 컨택터 및 릴레이 접점의 용착 ・외부 배선 기기의 단선 또는 지락	외부 배선을 확인하십시오.	왼쪽에 제시된 대책을 고려하여 파라미터를 설정하고 시스템을 배선하십시오.

부가 정보	부가 정보 1: 에러가 발생한 EDM의 출력 단자 번호 0: So00 ~ 3: So03
주의사항/ 비고	없음

AI 번역본
-For Reference Only-

<table>
<tr><td>이벤트 이름</td><td colspan="2">NTP 서버 접속 에러</td><td>이벤트 코드</td><td colspan="2">84040000 hex</td></tr>
<tr><td>설명</td><td colspan="5">NTP 서버와의 접속에 실패했습니다.</td></tr>
<tr><td>발생원</td><td colspan="2">-</td><td>발생원 상세</td><td>검출 타이밍</td><td>NTP 동작 중</td></tr>
<tr><td>에러 속성</td><td>레벨</td><td>경미한 폴트</td><td>복구 방법</td><td>로그 카테고리</td><td>시스템</td></tr>
<tr><td></td><td></td><td></td><td>자동 복구.
서버 사양을

수정하고
다시 다운로드한

후에는
전원을
재투입하거나
재시작을 실행하십시오.</td><td></td><td></td></tr>
<tr><td>영향</td><td>사용자 프로그램</td><td>계속</td><td>동작</td><td colspan="2">NTP를 통해 시각을 취득할 수 없습니다.</td></tr>
<tr><td>원인 및 대책</td><td colspan="2">추정 원인</td><td colspan="2">대책</td><td>예방책</td></tr>
<tr><td></td><td colspan="2">잘못된 설정 데이터</td><td colspan="2">접속 대상 서버의 사양에
오류가 있는 경우 서버
사양을 수정한 후 설정 데이터를
다시
다운로드하십시오.</td><td>접속 대상 서버 설정이 올바른지
확인하십시오.</td></tr>
<tr><td></td><td colspan="2">서버가 다운되었습니다.</td><td colspan="2">접속 대상 서버가 정상적으로
동작하고 있는지 확인하고,
그렇지 않은 경우 정상적으로
동작하도록
설정하십시오.</td><td>접속 대상 서버가 정상적으로 동작하고
있는지 확인하십시오.</td></tr>
<tr><td></td><td colspan="2">통신 경로에서 에러가
발생했습니다.</td><td colspan="2">서버까지의 통신 경로를
확인하고 문제가 있으면
시정 조치를 취하십시오.</td><td>없음</td></tr>
<tr><td>부가 정보</td><td colspan="5">없음</td></tr>
<tr><td>주의사항/ 비고</td><td colspan="5">수정 후 이벤트 로그에 TCP Server Run이 기록되면 CPU 유닛이 DNS 서버에 올바르게
접속된 것입니다.</td></tr>
</table>

AI 번역본
-For Reference Only-

이벤트 이름	DHCP 서버 접속 에러			**이벤트 코드**	840F0000 hex	
설명	DHCP 서버와의 접속에 실패했습니다.					
발생원	-		**발생원 상세**	-	**검출 타이밍**	DHCP 동작 중
에러 속성	**레벨**	경미한 폴트	**복구 방법**	자동 복구	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	EtherNet/IP 통신이 동작하지 않습니다. DHCP 서버로부터 응답이 있을 때까지 DHCP 서버에 대한 요청이 계속됩니다.		
원인 및 대책	**추정 원인**		**대책**		**예방책**	
	서버 설정 오류		서버가 다운되었습니다.		접속 대상 서버 설정이 올바른지 확인하십시오.	
	서버가 다운되었습니다.		접속 대상 서버가 정상적으로 동작하고 있는지 확인하고, 그렇지 않은 경우 정상적으로 동작하도록 설정하십시오.		접속 대상 서버가 정상적으로 동작하고 있는지 확인하십시오.	
	통신 경로에서 에러가 발생했습니다.		서버까지의 통신 경로를 확인하고 문제가 있으면 시정 조치를 취하십시오.		없음	
부가 정보	없음					
주의사항/ 비고	없음					

AI 번역본
-For Reference Only-

<table>
<tr><td>이벤트 이름</td><td colspan="2">IP 주소 중복 에러</td><td>이벤트 코드</td><td colspan="2">85E20000 hex</td></tr>
<tr><td>설명</td><td colspan="5">IP 주소가 중복되었습니다.</td></tr>
<tr><td>발생원</td><td colspan="2">-</td><td>발생원 상세</td><td>검출 타이밍</td><td>IP 주소가 확정될 때</td></tr>
<tr><td>에러 속성</td><td>레벨</td><td>경미한 폴트</td><td>복구 방법</td><td>・전원을 재투입
・재시작을 실행</td><td>로그 카테고리</td><td>시스템</td></tr>
<tr><td>영향</td><td>사용자 프로그램</td><td>계속</td><td>동작</td><td colspan="3">EtherNet/IP 통신이 동작하지 않습니다
CIP Safety 통신이 동작하지 않습니다</td></tr>
<tr><td rowspan="2">원인 및 대책</td><td colspan="2">추정 원인</td><td colspan="2">대책</td><td>예방책</td></tr>
<tr><td colspan="2">이 IP 주소가 다른 노드의 IP 주소와 중복됩니다.</td><td colspan="2">다음 대책 중 하나를 실시하십시오.
・다른 노드의 IP 주소를 확인하고 동일한 주소가 둘 이상의 노드에서 사용되지 않도록 IP 주소 설정을 수정하십시오.
・중복된 IP 주소를 가진 다른 노드를 네트워크에서 제거하십시오.
대책을 실시한 후에도 전원을 재투입하거나 재시작을 실행하십시오.</td><td>네트워크 내의 각 노드에 서로 중복되지 않도록 IP 주소를 할당하십시오.</td></tr>
<tr><td>부가 정보</td><td colspan="5">부가 정보 1: 중복된 IP 주소
예: IP 주소가 192.168.250.1인 경우 C0A8FA01 hex.</td></tr>
<tr><td>주의사항/ 비고</td><td colspan="5">설정된 IP 주소로 ARP를 전송했을 때 ARP 응답이 있으면 중복 주소 에러가 발생합니다.</td></tr>
</table>

AI 번역본
-For Reference Only-

<table>
<tr><td>이벤트 이름</td><td colspan="3">태그 데이터 링크 타임아웃</td><td>이벤트 코드</td><td colspan="2">85E30000 hex</td></tr>
<tr><td>설명</td><td colspan="6">태그 데이터 링크에서 타임아웃이 발생했습니다.</td></tr>
<tr><td>발생원</td><td colspan="2">-</td><td>발생원 상세</td><td>-</td><td>검출 타이밍</td><td>상시</td></tr>
<tr><td>에러 속성</td><td>레벨</td><td>경미한 폴트</td><td>복구 방법</td><td>자동 복구</td><td>로그 카테고리</td><td>시스템</td></tr>
<tr><td>영향</td><td>사용자 프로그램</td><td>계속</td><td>동작</td><td colspan="3">해당 유닛은 계속 동작합니다.</td></tr>
<tr><td rowspan="8">원인 및 대책</td><td colspan="2">추정 원인</td><td colspan="2">대책</td><td colspan="2">예방책</td></tr>
<tr><td colspan="2">오리지네이터 노드의 전원이 OFF입니다.</td><td colspan="2" rowspan="2">오리지네이터 노드의 상태를 확인하고 정상적으로 시작하십시오.</td><td colspan="2" rowspan="2">오리지네이터 노드가 정상적으로 동작하고 있는지 확인한 후 태그 데이터 링크를 사용하십시오.</td></tr>
<tr><td colspan="2">오리지네이터 노드의 통신이 정지되어 있습니다.</td></tr>
<tr><td colspan="2">EtherNet/IP용 이더넷 케이블이 분리되어 있습니다.</td><td colspan="2">커넥터를 다시 접속하고 올바르게 결합되었는지 확인하십시오.</td><td colspan="2">커넥터를 확실히 접속하십시오.</td></tr>
<tr><td colspan="2">EtherNet/IP용 이더넷 케이블이 단선되어 있습니다.</td><td colspan="2">이더넷 케이블을 교체하십시오.</td><td colspan="2">없음</td></tr>
<tr><td colspan="2">EtherNet/IP 포트로의 링크가 OFF입니다.</td><td colspan="2">링크 OFF의 추정 원인 및 기타 정보는 링크 OFF 검출 에러 (85E10000 hex)를 참조하십시오. 오리지네이터 노드 및 통신 경로상의 기기에서 CIP 통신을 허용하고, Firewall 및 Packet Filter 기능을 확인하십시오.</td><td colspan="2">링크 OFF의 추정 원인 및 기타 정보는 링크 OFF 검출 에러 (85E10000 hex)를 참조하십시오. 오리지네이터 노드 및 통신 경로상의 기기에서 CIP 통신을 허용하고, Firewall 및 Packet Filter 기능을 확인하십시오.</td></tr>
<tr><td colspan="2">네트워크 통신 부하로 인해 경로에서 패킷 손실이 발생했습니다.</td><td colspan="2">접속 타임아웃 값 또는 RPI를 늘리십시오. 또는 네트워크 환경 및 네트워크 기기를 재검토하십시오.</td><td colspan="2">네트워크가 과부하 상태가 되지 않도록 설계하십시오.</td></tr>
<tr><td colspan="2">노이즈</td><td colspan="2">과도한 노이즈가 있는 경우 노이즈 대책을 실시하십시오.</td><td colspan="2">과도한 노이즈가 있는 경우 노이즈 대책을 실시하십시오.</td></tr>
<tr><td>부가 정보</td><td colspan="6">부가 정보 1: 오리지네이터 IP 주소
예: IP 주소가 192.168.250.1인 경우 C0A8FA01 hex.
부가 정보 2: Assembly Instance No
025C hex: Input Assembly 1
03C0 hex: Input Assembly 2
03C1 hex: Input Assembly 3</td></tr>
<tr><td>주의사항/ 비고</td><td colspan="6">동일한 노드에서 여러 접속 에러가 발생하고 있는 경우, 발생한 에러 중 하나만 이벤트 로그에 기록됩니다.</td></tr>
</table>

AI 번역본
-For Reference Only-

<table>
<tr><td>이벤트 이름</td><td colspan="2">CIP Safety 타겟 접속 타임아웃</td><td>이벤트 코드</td><td colspan="2">85E40000 hex</td></tr>
<tr><td>설명</td><td colspan="5">CIP Safety 타겟 접속에서 타임아웃이 발생했습니다.</td></tr>
<tr><td>발생원</td><td colspan="2">-</td><td>발생원 상세</td><td>검출 타이밍</td><td>Executing 중</td></tr>
<tr><td>에러 속성</td><td>레벨</td><td>경미한 폴트</td><td>복구 방법</td><td>로그 카테고리</td><td>시스템</td></tr>
<tr><td>영향</td><td>사용자 프로그램</td><td>계속</td><td>동작</td><td colspan="2">해당 유닛은 계속 동작하지만
에러가 검출된 세이프티 커넥션의 I/O 데이터는 안전 상태로 유지됩니다.</td></tr>
<tr><td>원인 및 대책</td><td colspan="2">추정 원인</td><td colspan="2">대책</td><td>예방책</td></tr>
<tr><td></td><td colspan="2">케이블이 단선되었습니다.</td><td colspan="2">케이블이 단선되었는지 확인하십시오.</td><td rowspan="9">왼쪽에 제시된 대책을 고려하여 시스템을 구축하십시오.</td></tr>
<tr><td></td><td colspan="2">오리지네이터 기기가 접속을 수신할 수 없는 상태로 전환되었습니다.</td><td colspan="2">오리지네이터 기기가 접속을 수신할 수 있는 상태인지 확인하십시오.</td></tr>
<tr><td></td><td colspan="2">통신 설정의 타임아웃 값이 너무 짧습니다.</td><td colspan="2">통신 설정의 타임아웃 값이 적절한지 확인하십시오.</td></tr>
<tr><td></td><td colspan="2">오리지네이터 노드로부터의 CIP Safety 패킷이 EtherNet/IP 포트 설정의 Packet Filter (Simple) 또는 Packet Filter 기능, 또는 통신 경로상의 기기에 의해 허용되지 않고 있습니다.</td><td colspan="2">오리지네이터 노드로부터의 CIP Safety 패킷이 EtherNet/IP 포트 설정의 Packet Filter (Simple) 또는 Packet Filter 기능, 또는 통신 경로상의 기기에 의해 허용되는지 확인하십시오.</td></tr>
<tr><td></td><td colspan="2">오리지네이터 노드의 CIP 메시지 서버가 Do not use로 설정되어 있습니다.</td><td colspan="2">오리지네이터 노드의 CIP 메시지 서버가 Use로 설정되어 있는지 확인하십시오.</td></tr>
<tr><td></td><td colspan="2">오리지네이터 노드의 Packet Filter 기능이 유효한 경우, 타겟 노드로부터의 CIP Safety 패킷이 허용되지 않습니다.</td><td colspan="2">오리지네이터 노드의 Packet Filter 설정에서 타겟 노드로부터의 CIP Safety 패킷이 허용되는지 확인하십시오.</td></tr>
<tr><td></td><td colspan="2">노이즈</td><td colspan="2">통신이 노이즈의 영향을 받는지 확인하십시오.</td></tr>
<tr><td></td><td colspan="2">EtherNet/IP 포트 설정에서 CIP Safety 통신이 Do not use로 설정되어 있습니다.</td><td colspan="2">EtherNet/IP 포트 설정에서 CIP Safety 통신이 Use로 설정되어 있는지 확인하십시오.</td></tr>
<tr><td>부가 정보</td><td colspan="5">부가 정보 1: Assembly Instance No</td></tr>
<tr><td>주의사항/ 비고</td><td colspan="5">없음</td></tr>
</table>

AI 번역본
-For Reference Only-

이벤트 이름	유닛/입력 전원 전압 사양 범위 초과 검출			**이벤트 코드**	652F0000 hex	
설명	유닛/입력 전원의 전압이 사양 범위를 벗어난 것이 검출되었습니다.					
발생원	-		**발생원 상세**	-	**검출 타이밍**	상시
에러 속성	**레벨**	관찰	**복구 방법**	자동 복구	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	영향 없음		
원인 및 대책	**추정 원인**		**대책**		**예방책**	
	유닛/입력 전원의 전압이 사양 범위를 벗어난 것이 검출되었습니다.		유닛/입력 전원의 전압을 사양 범위 내의 정상적인 값으로 조정하십시오.		없음	
부가 정보	부가 정보 1: 유닛/입력 전원의 전압 모니터값 100 mV 단위					
주의사항/ 비고	없음					

이벤트 이름	유닛/입력 전원 전류 사양 범위 초과 검출			**이벤트 코드**	65300000 hex	
설명	유닛/입력 전원의 전류가 사양 범위를 벗어난 것이 검출되었습니다.					
발생원	-		**발생원 상세**	-	**검출 타이밍**	상시
에러 속성	**레벨**	관찰	**복구 방법**	자동 복구	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	영향 없음		
원인 및 대책	**추정 원인**		**대책**		**예방책**	
	유닛/입력 전원의 전류가 사양 범위를 벗어난 것이 검출되었습니다.		유닛/입력 전원의 전류를 사양 범위 내의 정상적인 값으로 조정하십시오.		없음	
부가 정보	부가 정보 1: 유닛/입력 전원의 전류 모니터값 100 mA 단위					
주의사항/ 비고	없음					

AI 번역본
-For Reference Only-

이벤트 이름	출력 전원 전압 사양 범위 초과 검출		이벤트 코드	65310000 hex	
설명	출력 전원의 전압이 사양 범위를 벗어난 것이 검출되었습니다.				
발생원	-		발생원 상세	-	검출 타이밍	상시
에러 속성	레벨	관찰	복구 방법	자동 복구	로그 카테고리	시스템
영향	사용자 프로그램	계속	동작	영향 없음		
원인 및 대책	추정 원인		대책		예방책	
	출력 전원의 전압이 사양 범위를 벗어난 것이 검출되었습니다.		출력 전원의 전압을 사양 범위 내의 정상적인 값으로 조정하십시오.		없음	
부가 정보	부가 정보 1: 출력 전원의 전압 모니터값 100 mV 단위					
주의사항/ 비고	없음					

이벤트 이름	출력 전원 전류 사양 범위 초과 검출		이벤트 코드	65320000 hex	
설명	출력 전원의 전류가 사양 범위를 벗어난 것이 검출되었습니다.				
발생원	-		발생원 상세	-	검출 타이밍	상시
에러 속성	레벨	관찰	복구 방법	자동 복구	로그 카테고리	시스템
영향	사용자 프로그램	계속	동작	영향 없음		
원인 및 대책	추정 원인		대책		예방책	
	출력 전원의 전류가 사양 범위를 벗어난 것이 검출되었습니다.		출력 전원의 전류를 사양 범위 내의 정상적인 값으로 조정하십시오.		없음	
부가 정보	부가 정보 1: 출력 전원의 전류 모니터값 100 mA 단위					
주의사항/ 비고	없음					

AI 번역본
-For Reference Only-

이벤트 이름	링크 OFF 검출			이벤트 코드	85E10000 hex	
설명	이더넷 링크 OFF가 검출되었습니다.					
발생원	-		발생원 상세	-	검출 타이밍	상시
에러 속성	레벨	관찰	복구 방법	자동 복구	로그 카테고리	시스템
영향	사용자 프로그램	계속	동작	EtherNet/IP 통신이 동작하지 않습니다.		
원인 및 대책	추정 원인		대책		예방책	
	이더넷 케이블이 단선, 분리 또는 헐거워졌습니다.		이더넷 케이블을 확실히 접속하십시오. 케이블이 단선된 경우 교체하십시오.		이더넷 케이블을 확실히 접속하십시오. 케이블이 단선되지 않았는지 확인하십시오.	
	이더넷 스위치의 전원이 OFF입니다.		이더넷 스위치의 전원을 ON하십시오. 이더넷 스위치가 고장난 경우 교체하십시오.		이더넷 스위치의 전원을 OFF하지 마십시오.	
	보드레이트 불일치.		리모트 통신 노드와 동일한 보드레이트가 사용되도록 설정을 수정하십시오.		리모트 통신 노드와 동일한 보드레이트를 설정하십시오.	
	노이즈		과도한 노이즈가 있는 경우 노이즈 대책을 실시하십시오.		노이즈 대책을 실시하십시오.	
	재시작을 실행하거나 메모리 올 클리어를 실행하십시오.		없음. 이 이벤트는 왼쪽의 조작이 실행되었을 때 발생합니다.		없음. 이 이벤트는 왼쪽의 조작이 실행되었을 때 발생합니다.	
부가 정보	부가 정보 1: 링크 OFF가 검출된 EtherNet/IP 통신 커넥터 1: EtherNet/IP 통신 커넥터 1 (ETH1) 2: EtherNet/IP 통신 커넥터 2 (ETH2)					
주의사항/ 비고	없음					

이벤트 이름	CIP Safety 타겟 접속 오픈 요청			이벤트 코드	85E50000 hex	
설명	CIP Safety 오리지네이터로부터 접속 오픈 요청이 있었습니다.					
발생원	-		발생원 상세	-	검출 타이밍	· Idle 중 · Executing 중
에러 속성	레벨	정보	복구 방법	-	로그 카테고리	액세스
영향	사용자 프로그램	계속	동작	영향 없음		
원인 및 대책	추정 원인		대책		예방책	
	CIP Safety 오리지네이터로부터 접속 오픈 요청이 있었습니다.		—		—	
부가 정보	부가 정보 1: 예약 부가 정보 2: Assembly Instance No 부가 정보 3: CIP 사양에 정의된 General Status 부가 정보 4: CIP 사양에 정의된 Extended Status					
주의사항/ 비고	없음					

AI 내용 For Reference Only-

이벤트 이름	전원 ON			이벤트 코드	90110000 hex	
설명	전원이 ON되었습니다.					
발생원	-		발생원 상세	-	검출 타이밍	전원이 ON될 때.
에러 속성	레벨	정보	복구 방법	-	로그 카테고리	시스템
영향	사용자 프로그램	계속	동작	동작이 시작됩니다.		
원인 및 대책	추정 원인		대책		예방책	
	전원이 ON되었습니다.		없음		없음	
부가 정보	없음					
주의사항/ 비고	없음					

이벤트 이름	IP 주소 확정			이벤트 코드	94080000 hex	
설명	올바른 IP 주소가 확정되어 이더넷 통신을 시작할 수 있습니다.					
발생원	-		발생원 상세	-	검출 타이밍	・전원이 ON될 때. ・재시작을 실행할 때
에러 속성	레벨	정보	복구 방법	-	로그 카테고리	시스템
영향	사용자 프로그램	계속	동작	영향 없음.		
원인 및 대책	추정 원인		대책		예방책	
	올바른 IP 주소가 확정되어 이더넷 통신을 시작할 수 있습니다.		없음		없음	
부가 정보	부가 정보 1: IP 주소 예: IP 주소가 192.168.250.1인 경우 C0A8FA01 hex.					
주의사항/ 비고	없음					

이벤트 이름	컨피규레이션 잠금			이벤트 코드	966C0000 hex	
설명	컨피규레이션 잠금이 실행되었습니다.					
발생원	-		발생원 상세	-	검출 타이밍	컨피규레이션 잠금이 실행될 때
에러 속성	레벨	정보	복구 방법	-	로그 카테고리	액세스
영향	사용자 프로그램	계속	동작	영향 없음		
원인 및 대책	추정 원인		대책		예방책	
	컨피규레이션 잠금 실행		없음		없음	
부가 정보	부가 정보 1: 예약 부가 정보 2: SCCRC 부가 정보 3: 컨피규레이션 잠금 시 로터리 스위치 설정값 표시 형식은 [SW1, SW2, x161, x160]입니다. 예: SW1=3, SW2=3, x161=0, x160=1인 경우					
주의사항/ 비고	없음					

AI 내부본 For Reference Only

이벤트 이름	컨피규레이션 잠금 해제			**이벤트 코드**	966D0000 hex	
설명	컨피규레이션 잠금 해제가 실행되었습니다.					
발생원	-		**발생원 상세**	-	**검출 타이밍**	컨피규레이션 잠금 해제가 실행될 때
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	액세스
영향	**사용자 프로그램**	계속	**동작**	영향 없음		
원인 및 대책	**추정 원인**		**대책**		**예방책**	
	컨피규레이션 잠금 해제 실행		없음		없음	
첨부 정보	첨부 정보 1: 예약					
주의 사항/ 비고	없음					

이벤트 이름	출력 전원 공급(PWR OUT) 꺼짐			**이벤트 코드**	96710000 hex	
설명	PWR OUT 전원 공급 커넥터에서 공급되는 출력 전원 공급이 꺼졌습니다.					
소스	-		**소스 상세**	-	**검출 시점**	출력 전원 공급 (PWR OUT)을 끌 때
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	액세스
영향	**사용자 프로그램**	계속	**동작**	PWR OUT 전원 공급 커넥터에서 공급되는 출력 전원 공급이 꺼집니다.		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	스루 배선 출력 전원 공급의 차단이 스루 배선 출력 전원 공급 차단 명령에 의해 지시되었습니다.		없음		없음	
첨부 정보	없음					
주의 사항/ 비고	없음					

AI 번역본
-For Reference Only-

<table>
<tr><td>이벤트 이름</td><td colspan="2">설정 데이터 변경됨</td><td>이벤트 코드</td><td colspan="2">96720000 hex</td></tr>
<tr><td>설명</td><td colspan="5">설정 데이터가 변경되었습니다.</td></tr>
<tr><td>소스</td><td colspan="2">-</td><td>소스 상세</td><td>검출 시점</td><td>설정이 변경되었을 때</td></tr>
<tr><td>에러 속성</td><td>레벨</td><td>정보</td><td>복구 방법</td><td>로그 카테고리</td><td>액세스</td></tr>
<tr><td>영향</td><td>사용자 프로그램</td><td>계속</td><td>동작</td><td colspan="2">영향 없음.</td></tr>
<tr><td>원인 및 대책</td><td colspan="2">추정 원인</td><td colspan="2">대책</td><td>예방</td></tr>
<tr><td></td><td colspan="2">설정 데이터가 변경되었습니다.</td><td colspan="2">없음</td><td>없음</td></tr>
<tr><td>첨부 정보</td><td colspan="5">첨부 정보 1: 예약
첨부 정보 2: 변경 대상
0100 hex: TCP/IP 설정(IP 결정 방법)
0101 hex: TCP/IP 설정(IP 주소)
0102 hex: TCP/IP 설정(Encapsulation Inactivity Timeout)
0200 hex: LINK 설정
0300 hex: 통신 포트 사용/사용 안 함 기능 설정
0400 hex: 자동 시계 조정 설정(NTP/SNTP 서버 IP 주소)
0401 hex: 자동 시계 조정 설정(시간대)
0500 hex: 스루 배선 출력용 전원 차단 기능 설정
2000 hex: 세이프티 패스워드
2006 hex: 컨피규레이션 잠금 상태
2008 hex: 복원 활성 플래그
2001 hex: TUNID
2002 hex: Alarm Enable
2003 hex: Warning Enable
2004 hex: Output Connection Owner
2005 hex: CFUNID
21*1 hex: 컨피규레이션 데이터
21*2 hex: SCID
21*5 hex: 애플리케이션 이름
21*6 hex: 버전
21*7 hex: 작성자
(*는 애플리케이션 번호를 나타내는 0~F의 값입니다)
8000 hex: QoS 설정(DSCP Urgent)
8001 hex: QoS 설정(DSCP Scheduled)
8002 hex: QoS 설정(DSCP High)
8003 hex: QoS 설정(DSCP Low)
8004 hex: QoS 설정(DSCP Explicit)
8100 hex: LLDP 설정(LLDP Enable)
8101 hex: LLDP 설정(LLDP Tx Interval)
8102 hex: LLDP 설정(LLDP Tx Hold)</td></tr>
<tr><td>주의 사항/ 비고</td><td colspan="5">없음</td></tr>
</table>

참조번 역본
-For Reference Only-

이벤트 이름	로그인			**이벤트 코드**	96730000 hex	
설명	로그인했습니다. (Web UI)					
소스	-		**소스 상세**	-	**검출 시점**	사용자(Web UI)가 조작했을 때
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	액세스
영향	**사용자 프로그램**	계속	**동작**	영향 없음.		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	Web UI를 사용하여 로그인했습니다.		없음		없음	
첨부 정보	첨부 정보 1: 접속원 IP 주소 예: IP 주소가 192.168.250.100인 경우 C0A8FA64 hex입니다. 첨부 정보 2: 로그인 권한 종류 0: 관리자 권한으로 로그인 1: 옵서버 권한으로 로그인					
주의 사항/ 비고	없음					

이벤트 이름	세이프티 애플리케이션 삭제됨			**이벤트 코드**	96750000 hex	
설명	유닛에서 세이프티 애플리케이션 데이터가 삭제되었습니다.					
소스	-		**소스 상세**	-	**검출 시점**	사용자로부터 명령(삭제)이 있었을 때
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	액세스
영향	**사용자 프로그램**	계속	**동작**	영향 없음		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	Web UI에서 삭제가 접수되었습니다.		없음		없음	
첨부 정보	첨부 정보 1: 예약 첨부 정보 2: 애플리케이션 번호					
주의 사항/ 비고	없음					

이벤트 이름	세이프티 패스워드 불일치			**이벤트 코드**	96760000 hex	
설명	세이프티 패스워드가 필요한 서비스를 실행할 때 패스워드 불일치가 검출되었습니다.					
소스	-		**소스 상세**	-	**검출 시점**	패스워드가 필요한 서비스를 실행할 때
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	액세스
영향	**사용자 프로그램**	계속	**동작**	해당 유닛은 계속 동작합니다.		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	세이프티 패스워드가 필요한 서비스를 실행할 때 패스워드 불일치가 검출되었습니다.		올바른 세이프티 패스워드를 입력한 후 서비스를 다시 실행하십시오.		없음	
첨부 정보	첨부 정보 1: 예약					
주의 사항/ 비고	없음					

AI 번역본
-For Reference Only

이벤트 이름	출력 전원 공급(PWR OUT) 켜짐		이벤트 코드		96770000 hex	
설명	PWR OUT 전원 공급 커넥터에서 공급되는 출력 전원 공급이 켜졌습니다.					
소스	-		소스 상세	-	검출 시점	출력 전원 공급 (PWR OUT)을 켤 때
에러 속성	레벨	정보	복구 방법	-	로그 카테고리	액세스
영향	사용자 프로그램	계속	동작	PWR OUT 전원 공급 커넥터에서 공급되는 출력 전원 공급이 켜집니다.		
원인 및 대책	추정 원인		대책		예방	
	스루 배선 출력 전원 공급의 복구가 스루 배선 출력 전원 공급 복구 명령에 의해 지시되었습니다.		없음		없음	
첨부 정보	없음					
주의 사항/ 비고	없음					

이벤트 이름	펌웨어 업데이트 실행됨		이벤트 코드		96780000 hex	
설명	펌웨어 업데이트가 실행되었습니다.					
소스	-		소스 상세	-	검출 시점	펌웨어가 업데이트되었을 때
에러 속성	레벨	정보	복구 방법	-	로그 카테고리	액세스
영향	사용자 프로그램	계속	동작	영향 없음.		
원인 및 대책	추정 원인		대책		예방	
	펌웨어 업데이트가 실행되었습니다.		없음		없음	
첨부 정보	첨부 정보 1: 접속원 IP 주소 예: IP 주소가 192.168.250.100인 경우 C0A8FA64 hex입니다. 첨부 정보 2: 실행 결과 0000 hex: 성공 0001 hex: 실패 첨부 정보 3: 기입된 펌웨어의 버전(BCD) 예: Ver. 1.10.01인 경우 01100100 hex가 됩니다.					
주의 사항/ 비고	없음					

AI 번역본
-For Reference Only-

이벤트 이름	메모리 전체 클리어			**이벤트 코드**	96790000 hex	
설명	메모리 전체 클리어가 실행되었습니다.					
소스	-		**소스 상세**	-	**검출 시점**	메모리 전체 클리어가 실행되었을 때
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	액세스
영향	**사용자 프로그램**	계속	**동작**	리셋 실행 후 동작이 시작됩니다.		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	메모리 전체 클리어가 실행되었습니다.		없음		없음	
첨부 정보	첨부 정보 1: 예약 첨부 정보 2: 리셋 종류 1: 메모리 전체 클리어(첨부 정보 3의 전체 데이터가 클리어됨) 2: 메모리 전체 클리어(첨부 정보 3의 일부 데이터가 클리어됨) 첨부 정보 3: 미초기화 데이터(해당 비트 값이 1인 데이터는 초기화되지 않음)*1 Bit 0: IP Address Bit 2: TUNID Bit 3: Password Bit 4: CFUNID Bit 5: Output Connection Owner						
주의 사항/ 비고	없음					

***1.** 이것은 첨부 정보 2가 2인 경우에만 유효합니다.

이벤트 이름	링크 검출됨			**이벤트 코드**	967A0000 hex	
설명	이더넷 링크의 확립이 검출되었습니다.					
소스	-		**소스 상세**	-	**검출 시점**	링크가 확립되었을 때
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	영향 없음.		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	이더넷 링크의 확립이 검출되었습니다.		없음		없음	
첨부 정보	첨부 정보 1: 링크 ON이 검출된 EtherNet/IP 통신 커넥터 1: EtherNet/IP 통신 커넥터 1(ETH1) 2: EtherNet/IP 통신 커넥터 2(ETH2)					
주의 사항/ 비고	없음					

참고용 번역본
-For Reference Only-

이벤트 이름	운전 모드 변경됨			이벤트 코드	967B0000 hex	
설명	운전 모드 변경이 실행되었습니다.					
소스	-		소스 상세	-	검출 시점	운전 모드 변경이 실행되었을 때
에러 속성	레벨	정보	복구 방법	-	로그 카테고리	액세스
영향	사용자 프로그램	계속	동작	영향 없음		
원인 및 대책	추정 원인		대책		예방	
	운전 모드 변경이 실행되었습니다.		없음		없음	
첨부 정보	첨부 정보 1: 예약 첨부 정보 2: 새 운전 모드 2: Idle 3: Executing					
주의 사항/ 비고	없음					

이벤트 이름	세이프티 패스워드 변경됨			이벤트 코드	967C0000 hex	
설명	세이프티 패스워드가 변경되었습니다.					
소스	-		소스 상세	-	검출 시점	사용자로부터 명령(전송)이 있었을 때
에러 속성	레벨	정보	복구 방법	-	로그 카테고리	액세스
영향	사용자 프로그램	계속	동작	영향 없음.		
원인 및 대책	추정 원인		대책		예방	
	세이프티 패스워드가 변경되었습니다.		없음		없음	
첨부 정보	첨부 정보 1: 예약					
주의 사항/ 비고	없음					

AI 번역본
-For Reference Only-

이벤트 이름	세이프티 애플리케이션 전송됨			**이벤트 코드**	967D0000 hex	
설명	세이프티 애플리케이션 데이터가 유닛으로 전송되었습니다.					
소스	-		**소스 상세**	-	**검출 시점**	· 사용자로부터 명령(전송)이 있었을 때 · Type1 Safety Open이 접수되었을 때
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	액세스
영향	**사용자 프로그램**	계속	**동작**	영향 없음		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	· Web UI를 이용한 전송이 접수되었습니다. · 세이프티 컨트롤러로부터 Type 1 Safety Open 요청이 접수되었습니다.		없음		없음	
첨부 정보	첨부 정보 1: 예약 첨부 정보 2: 애플리케이션 번호 첨부 정보 3: SCCRC 첨부 정보 4: 설정 방법 1: Type1 Safety Open 2: Web UI 기능에 의한 설정					
주의 사항/ 비고	없음					

이벤트 이름	이벤트 로그 클리어됨			**이벤트 코드**	967E0000 hex	
설명	이벤트 로그가 클리어되었습니다.					
소스	-		**소스 상세**	-	**검출 시점**	항상
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	액세스
영향	**사용자 프로그램**	계속	**동작**	영향 없음.		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	이벤트 로그가 클리어되었습니다.		없음		없음	
첨부 정보	첨부 정보 1: 접속원 IP 주소 예: IP 주소가 192.168.250.1인 경우 C0A8FA01 hex입니다. 첨부 정보 2: 클리어된 이벤트 0: 전체 카테고리의 로그가 클리어되었습니다. 1: 시스템 이벤트 로그가 클리어되었습니다. 2: 액세스 이벤트 로그가 클리어되었습니다.					
주의 사항/ 비고	없음					

AI 번역본
For Reference Only

이벤트 이름	백업 실행됨			**이벤트 코드**	967F0000 hex	
설명	백업이 실행되었습니다.					
소스	-		**소스 상세**	-	**검출 시점**	백업이 실행되었을 때
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	액세스
영향	**사용자 프로그램**	계속	**동작**	영향 없음		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	백업이 실행되었습니다.		없음		없음	
첨부 정보	첨부 정보 1: 접속원 IP 주소 예: IP 주소가 192.168.250.100인 경우 C0A8FA64 hex입니다. 첨부 정보 2: 실행 결과 0000 hex: 성공 0001 hex: 실패					
주의 사항/ 비고	없음					

이벤트 이름	복원 실행됨			**이벤트 코드**	96800000 hex	
설명	복원이 실행되었습니다.					
소스	-		**소스 상세**	-	**검출 시점**	복원이 실행되었을 때
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	액세스
영향	**사용자 프로그램**	계속	**동작**	영향 없음		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	복원이 실행되었습니다.		없음		없음	
첨부 정보	첨부 정보 1: 접속원 IP 주소 예: IP 주소가 192.168.250.100인 경우 C0A8FA64 hex입니다. 첨부 정보 2: 실행 결과 0000 hex: 성공 0001 hex: 실패					
주의 사항/ 비고	없음					

이벤트 이름	오므론 유지보수 실행됨			**이벤트 코드**	96810000 hex	
설명	오므론 유지보수 담당자에 의한 유지보수가 실행되었습니다.					
소스	-		**소스 상세**	-	**검출 시점**	오므론 유지보수가 실행되었을 때
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	액세스
영향	**사용자 프로그램**	계속	**동작**	영향 없음		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	오므론 유지보수 담당자에 의한 유지보수가 실행되었습니다.		없음		없음	
첨부 정보	첨부 정보 1: 접속원 IP 주소 예: IP 주소가 192.168.250.100인 경우 C0A8FA64 hex입니다.					
주의 사항/ 비고	없음					

AI 번역 본
-For Reference Only

이벤트 이름	재시작됨			**이벤트 코드**	96820000 hex	
설명	재시작이 실행되었습니다.					
소스	-		**소스 상세**	-	**검출 시점**	재시작을 실행했을 때
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	액세스
영향	**사용자 프로그램**	계속	**동작**	영향 없음		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	재시작이 실행되었습니다.		없음		없음	
첨부 정보	첨부 정보 1: 예약					
주의 사항/ 비고	없음					

이벤트 이름	세이프티 컨피규레이션 검증됨			**이벤트 코드**	96830000 hex	
설명	세이프티 컨피규레이션이 검증되었습니다.					
소스	-		**소스 상세**	-	**검출 시점**	· 전원을 ON했을 때 · 재시작을 실행했을 때
에러 속성	**레벨**	정보	**복구 방법**	-	**로그 카테고리**	시스템
영향	**사용자 프로그램**	계속	**동작**	영향 없음		
원인 및 대책	**추정 원인**		**대책**		**예방**	
	세이프티 컨피규레이션이 검증되었습니다.		없음		없음	
첨부 정보	첨부 정보 1: 애플리케이션 번호 첨부 정보 2: SCCRC 첨부 정보 3: 컨피규레이션 잠금 상태 0: 잠금 해제 1: 잠금 첨부 정보 4: 시작 모드 0: Idle 1: Executing					
주의 사항/ 비고	없음					

AI 번역본
-For Reference Only-

이벤트 이름	IP 주소 표시 기능 실행됨			이벤트 코드	96840000 hex	
설명	IP 주소 표시 기능이 실행되었습니다.					
소스	-		소스 상세	-	검출 시점	· 전원을 ON했을 때 · 재시작을 실행했을 때
에러 속성	레벨	정보	복구 방법	-	로그 카테고리	시스템
영향	사용자 프로그램	계속	동작	영향 없음		
원인 및 대책	추정 원인		대책		예방	
	SW1 = SW2 = 8로 시작함 (IP 주소 표시 기능).		없음		없음	
첨부 정보	없음					
주의 사항/ 비고	없음					

이벤트 이름	I/O 배선 확인 기능 실행됨			이벤트 코드	96850000 hex	
설명	I/O 배선 확인 기능이 실행되었습니다.					
소스	-		소스 상세	-	검출 시점	· 전원을 ON했을 때 · 재시작을 실행했을 때
에러 속성	레벨	정보	복구 방법	-	로그 카테고리	시스템
영향	사용자 프로그램	계속	동작	영향 없음		
원인 및 대책	추정 원인		대책		예방	
	SW1 = SW2 = E로 시작함 (I/O 배선 확인 기능).		없음		없음	
첨부 정보	없음					
주의 사항/ 비고	없음					

AI 번역본
-For Reference Only-

12

점검 및 유지보수

이 장에서는 세이프티 I/O 블록의 점검 및 유지보수에 대해 설명합니다.

12-1 청소 및 점검 12-2
12-1-1 청소 12-2
12-1-2 점검 순서 12-2
12-2 유닛 교체 12-4
12-2-1 유닛 교체 시 주의 사항 12-4
12-2-2 백업 기능을 사용한 유닛 교체 12-4
12-2-3 백업 기능을 사용하지 않는 유닛 교체 12-5

AI 번역본
-For Reference Only-

12-1 청소 및 점검

이 절에서는 청소, 점검 등 기기의 일상적인 유지보수에 대해 설명합니다.
세이프티 I/O 블록을 최적의 동작 상태로 유지하기 위해 매일 또는 정기적으로 점검하십시오.

12-1-1 청소

기기를 최적의 동작 상태로 유지하기 위해 아래와 같이 정기적으로 청소하십시오.

- 일상 청소 시에는 부드럽고 마른 천으로 기기를 닦으십시오.
- 부드럽고 마른 천으로 닦은 후에도 오염이 남아 있으면 충분히 희석한 세제(2%)에 적셔 물기를 짠 천으로 닦으십시오.
- 껌, 비닐, 테이프 등을 장시간 붙여 두면 기기에 얼룩이 남을 수 있습니다. 정기 청소 시 이러한 물질을 제거하십시오.

사용상의 주의

페인트 시너, 벤젠, 화학 걸레 등 휘발성 용제는 절대 사용하지 마십시오. 제품의 각인면이나 인쇄면이 변질될 수 있습니다.

12-1-2 점검 순서

유닛을 최적의 동작 상태로 유지하기 위해 반드시 정기 점검을 실시하십시오.
점검은 6~12개월에 1회 실시하십시오(세이프티 검증 시험은 매월 1회).
온도와 습도가 매우 높거나 먼지가 많은 장소에서 기기를 사용하는 경우에는 더 자주 점검하십시오.
아래 표의 조건 중 하나라도 충족하지 못하면 즉시 조치를 취해 상황을 바로잡으십시오. 조건에 대한 자세한 내용은 12-3페이지의 점검 항목을 참조하십시오.

- 유닛이 사양 범위 내에서 사용되고 있는지 확인하십시오.
- 유닛이 올바르게 장착 및 배선되어 있는지 확인하십시오.
- 세이프티 기능의 동작 신뢰성을 일정한 수준으로 유지하기 위해 세이프티 기능을 진단하십시오.
- 진단 처리의 일부는 통상 처리의 유휴 시간 동안 나뉘어 실행되므로 모든 진단을 완료하려면 본 제품을 최소 8시간 이상 연속으로 동작시키십시오.

AI 번역본
-For Reference Only-

점검에 필요한 공구

● 항상 필요한 공구

- 십자 드라이버
- 토크 핸들
- 전압 테스터 또는 디지털 전압계
- 공업용 알코올 및 순면 천

● 경우에 따라 필요한 공구

- 오실로스코프

· 온도계 및 습도계

점검 항목

아래 항목을 점검하여 결과가 기준을 충족하는지 확인하십시오.
결과가 기준을 충족하지 않으면 환경을 개선하거나 기기를 조정하여 점검 결과가 기준을 충족하도록 하십시오.

점검 항목	점검 내용	기준	점검 수단
환경	주위 온도 및 패널 내부 온도 확인	-10~55 °C	온도계
	주위 습도 및 패널 내부 습도 확인	25%~85%(결로 없음)	습도계
	먼지 누적 확인	먼지 누적 없음	육안 검사
설치 상태	유닛이 단단히 고정되어 있는지 확인	느슨함 없음	십자 드라이버
	케이블의 방수 커버가 유닛의 커넥터에 적절한 토크로 조여져 있는지 확인	커버가 규정된 토크로 조여져 있음	토크 핸들
	로터리 스위치 커버가 단단히 조여져 있음	느슨함 없음	십자 드라이버
	접속 케이블의 손상 확인	육안상 손상 없음	육안 검사
세이프티 검증 시험(사용자 시험)	모든 세이프티 기능이 올바르게 동작하는지 확인	모든 기능이 의도대로 동작해야 함	세이프티 기능을 동작시키는 조작을 실시합니다.

AI 번역본
-For Reference Only-

12-2 유닛 교체

이 절에서는 고장 또는 유지보수 등의 이유로 가동 중인 세이프티 I/O 블록을 교체하는 방법에 대해 설명합니다.
유닛 교체 방법에는 다음 두 가지가 있습니다.
백업 기능을 사용한 유닛 교체에서는 고객이 설정한 모든 세이프티 애플리케이션 및 비세이프티 기능의 설정 데이터를 동시에 설정할 수 있습니다.
백업 기능을 사용하지 않는 경우에는 필요한 설정을 개별적으로 설정하십시오.

- 백업 기능을 사용한 유닛 교체
- 백업 기능을 사용하지 않는 유닛 교체

12-2-1 유닛 교체 시 주의 사항

점검 중 결함을 발견하여 기기를 교체할 때는 다음 사항에 유의하십시오.

- 교체 작업은 세이프티 제어에 대한 지식을 가진 담당자만 실시해야 합니다.
- 모든 작업자의 안전을 확보하기 위해 모든 위험원(즉, 액추에이터 등)의 전원 공급을 OFF하십시오.
- 세이프티 I/O 블록은 네트워크 구성 부품입니다. 유닛의 고장이 네트워크 전체에 영향을 줄 수 있으므로 유의하십시오. 유닛이 고장 나면 즉시 수리하십시오. 네트워크 기능을 최대한 빨리 복구 하려면 예비품을 준비해 두는 것이 좋습니다.
- 교체 후 새 기기에 문제가 없는지 확인하십시오.
- 고장 난 기기를 수리를 위해 반송할 때는 문제를 가능한 한 자세히 기재한 메모와 함께 오므론 담당자에게 기기를 보내십시오.
- 접촉 불량이 있는 경우 깨끗한 면 천에 공업용 알코올을 적셔 접점을 조심스럽게 닦으십시오.

12-2-2 백업 기능을 사용한 유닛 교체

이 절에서는 백업 기능을 사용하여 세이프티 I/O 블록 유닛을 교체하는 방법에 대해 설명합니다.
백업 기능을 사용하여 미리 백업 파일을 작성해 두면 설정 데이터를 쉽게 복구할 수 있습니다. 이렇게 하면 복구에 필요한 작업량이 줄어듭니다. 컨피규레이션을 잠글 때 백업을 실시하는 것을 권장합니다. 백업 기능에 대한 자세한 내용은 7-108페이지의 7-19 백업을, 복원 순서에 대한 자세한 내용은 7-109페이지의 복원을 참조하십시오.

샘플 역본
-For Reference Only-

교체 순서는 아래와 같습니다.

단계	항목	설명	사용 툴
1	백업 실행*1	백업을 실행합니다. 교체 작업을 실시하기 전에 미리 이 순서를 실시하십시오. 기기를 시작할 때 이 순서를 실시하는 것을 권장합니다.	Web UI
2	설치 및 배선	교체 대상 세이프티 I/O 블록을 분리하고 세이프티 I/O 블록을 설치합니다. 로터리 스위치 설정을 이전 유닛과 동일하게 설정하십시오. 이더넷, 전원 공급, I/O 케이블을 접속하십시오. PC를 세이프티 I/O 블록에 접속하십시오.	불필요
3	세이프티 패스워드 설정*1	세이프티 I/O 블록의 세이프티 패스워드를 설정합니다.	Web UI

단계	항목	설명	사용 툴
4	복원 실행*1	세이프티 I/O 블록에 대한 복원을 실행합니다.	Web UI
5	전원 공급 재투입	세이프티 I/O 블록의 전원 공급을 재투입하거나 재시작을 실시합니다.	불필요
6	EtherNet/IP 커넥션 및 CIP Safety 커넥션 확립	CIP Safety 오리지네이터 및 EtherNet/IP 오리지네이터가 세이프티 I/O 블록과 커넥션을 확립합니다.	불필요

***1.** 이 작업에는 세이프티 패스워드가 필요합니다.

12-2-3 백업 기능을 사용하지 않는 유닛 교체

이 절에서는 백업 기능을 사용하지 않고 세이프티 I/O 블록 유닛을 교체하는 방법에 대해 설명합니다.

・세이프티 컨트롤러가 제어를 실시하기 위한 컨피규레이션인 경우(Type 1 Safety Open을 사용한 컨피규레이션)
7-3페이지의 7-1-1 세이프티 컨트롤러가 제어를 실시하기 위한 컨피규레이션 설정 순서 (Type 1 Safety Open을 사용한 컨피규레이션)의 세이프티 I/O 블록 설정만 구성하십시오.
세이프티 컨트롤러와 세이프티 I/O 블록 사이에 Type1 Safety Open 커넥션이 확립되면 원격 I/O 세이프티 애플리케이션이 세이프티 컨트롤러에 의해 설정됩니다.

・세이프티 컨트롤러가 제어를 실시하기 위한 컨피규레이션인 경우(Web UI를 사용한 컨피규레이션)
7-6페이지의 7-1-2 세이프티 컨트롤러가 제어를 실시하기 위한 컨피규레이션 설정 순서 (Web UI를 사용한 컨피규레이션)의 세이프티 I/O 블록 설정만 구성하십시오.
Web UI를 사용하여 세이프티 애플리케이션 파일을 세이프티 I/O 블록에 다운로드함으로써 원격 I/O 세이프티 애플리케이션이 설정됩니다.

・세이프티 I/O 블록이 사전 설정된 세이프티 애플리케이션을 사용하여 제어를 실시하기 위한 컨피규레이션인 경우
7-9페이지의 7-1-3 세이프티 I/O 블록이 사전 설정된 세이프티 애플리케이션을 사용하여 제어를 실시하기 위한 컨피규레이션 설정 순서의 세이프티 I/O 블록 설정만 구성하십시오.
세이프티 I/O 블록의 고정 애플리케이션은 SETTING 로터리 스위치 SW1 및 SW2로 설정할 수 있습니다.

・세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 실시하기 위한 컨피규레이션인 경우(중앙 집중 관리형)
7-11페이지의 7-1-4 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 실시하기 위한 컨피규레이션 설정 순서(중앙 집중 관리형)의 세이프티 I/O 블록 설정만 구성하십시오.
세이프티 컨트롤러와 세이프티 I/O 블록 사이에 Type1 Safety Open 커넥션이 확립되면 사용자 정의 애플리케이션이 세이프티 컨트롤러에 의해 설정됩니다.

AI 번역본
-For Reference Only-

・세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 실시하기 위한 컨피규레이션인 경우(분산 관리형)
7-14페이지의 7-1-5 세이프티 I/O 블록이 사용자가 설계한 세이프티 애플리케이션을 사용하여 제어를 실시하기 위한 컨피규레이션 설정 순서(분산 관리형)의 세이프티 I/O 블록 설정만 구성하십시오.
Web UI를 사용하여 세이프티 애플리케이션 파일을 세이프티 I/O 블록에 다운로드함으로써 애드온 애플리케이션이 설정됩니다.

AI 번역본
-For Reference Only-

A

부록

부록에서는 세이프티 I/O 블록의 치수, 세이프티 I/O 어셈블리 데이터 및 기타 보충 정보를 제공합니다.

A-1 치수 A-2

A-2 세이프티 I/O 어셈블리 데이터 A-4

A-2-1 세이프티 입력 어셈블리 데이터 A-4
A-2-2 세이프티 출력 어셈블리 데이터 A-6
A-2-3 컨피규레이션 어셈블리 데이터 A-7

A-3 I/O 어셈블리 포트 및 대응하는 세이프티 I/O 어셈블리 데이터 요소 A-14

A-4 지원 CIP 객체 A-16

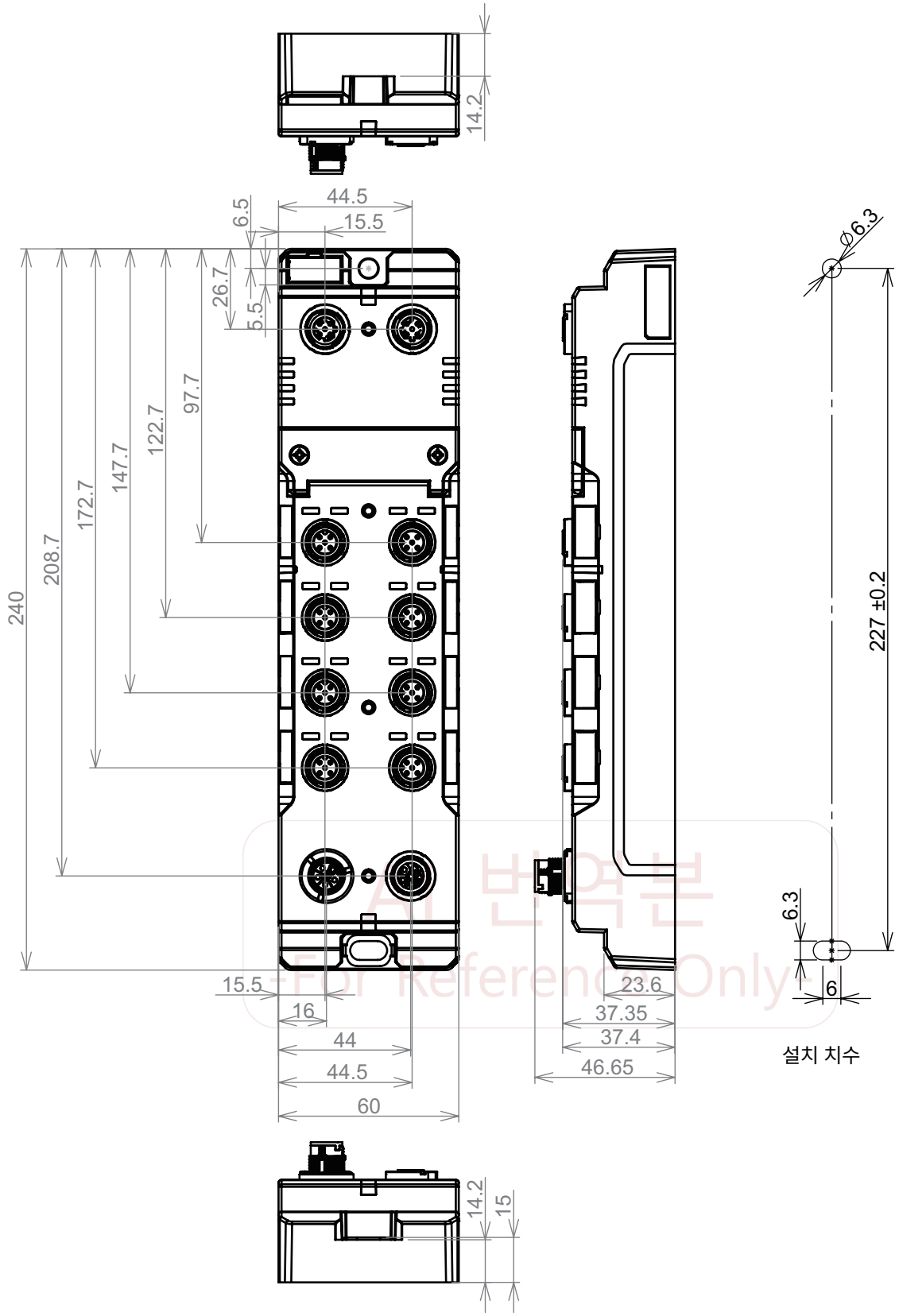
A-4-1 Identity Object (Class ID: 01 Hex) A-17
A-4-2 Assembly Object (Class ID: 04 Hex) A-19
A-4-3 Unit Manager Object (Class ID: 380 Hex) A-22
A-4-4 Event History Log Object (Class ID: 34B Hex) A-27
A-4-5 Error Event Object (Class ID: 34C Hex) A-30
A-4-6 Safety Discrete Input Point (SDIP) Object (Class ID: 3D Hex) A-33
A-4-7 Safety Discrete Output Point (SDOP) Object (Class ID: 3B Hex) A-35
A-4-8 Device Level Ring (DLR) Object (Class ID: 47 Hex) A-37
A-4-9 QoS Object (Class ID: 48 Hex) A-39
A-4-10 TCP/IP Interface Object (Class ID: F5 Hex) A-41
A-4-11 Ethernet Link Object (Class ID: F6 Hex) A-45
A-4-12 LLDP Management Object (Class ID: 109 Hex) A-51
A-4-13 LLDP Data Table Object (Class ID: 10A Hex) A-53
A-4-14 Logic Process Object (Class ID: 309 Hex) A-58

A-5 적합성 선언 A-60

Advanced
-For Reference Only-

A-1 치수

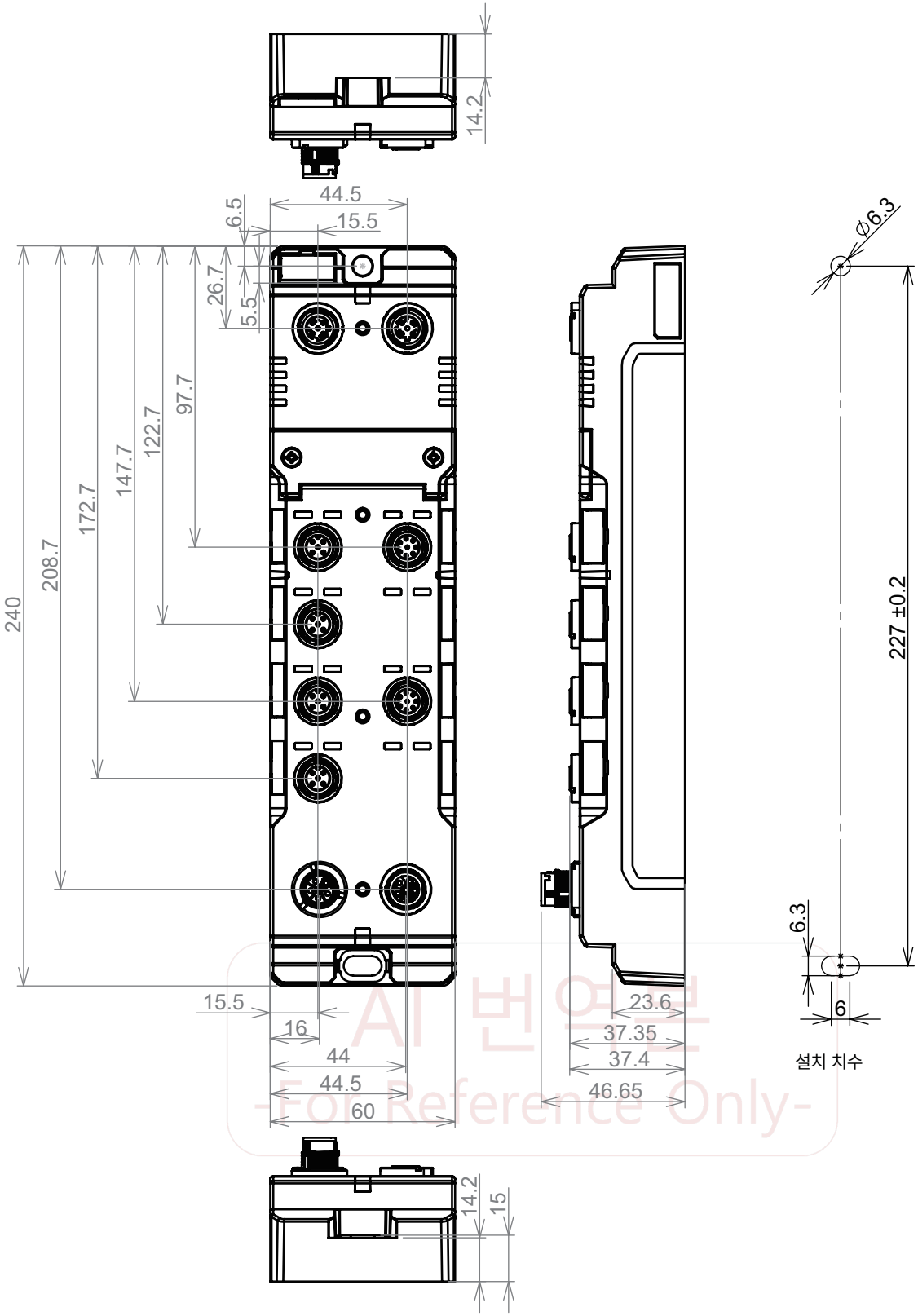
NXR-SXD1204-CST



설치 치수

AI 번역본
For Reference Only!

NXR-SXD1204B-CST



AI 번역본
-For Reference Only-

A-2 세이프티 I/O 어셈블리 데이터

세이프티 I/O 블록의 I/O 어셈블리 데이터는 다음과 같이 구성됩니다.

A-2-1 세이프티 입력 어셈블리 데이터

이 절에서는 세이프티 입력 어셈블리 데이터를 보여줍니다.
데이터의 각 요소의 의미는 다음과 같습니다.

요소	의미	어트리뷰트
Safety Input N	세이프티 입력 단자 Si N의 값 0: 세이프티 입력 단자가 OFF이거나 에러가 발생 중 1: 세이프티 입력 단자가 ON	Safety
Safety Input N Status	세이프티 입력 단자 Si N의 상태 정보 0: 에러 발생 중 1: 정상(에러 없음)	Safety
세이프티 입력 상태	세이프티 입력 단자의 상태 정보(통합) 0: 세이프티 입력 단자 중 하나에 에러가 있음 1: 모든 세이프티 입력 단자가 정상임	세이프티
테스트 출력 N 모니터	테스트 출력 단자 T N의 값 0: 테스트 출력 단자가 OFF이거나 에러가 발생 중임 1: 테스트 출력 단자가 ON임	비세이프티
테스트 출력 N 상태	테스트 출력 단자 T N의 상태 정보 0: 에러 발생 중 1: 정상(에러 없음)	비세이프티
세이프티 출력 N 모니터	세이프티 출력 단자 So N에 실제로 출력되는 값 0: 세이프티 출력 단자가 OFF임 1: 세이프티 출력 단자가 ON임	비세이프티
세이프티 출력 N 상태	세이프티 출력 단자 So N의 상태 정보 0: 에러 발생 중 1: 정상(에러 없음)	세이프티
세이프티 출력 상태	세이프티 출력 단자의 상태 정보(통합) 0: 세이프티 출력 단자 중 하나에 에러가 있음 1: 모든 세이프티 출력 단자가 정상임	세이프티
출력 전원 공급 에러 플래그	출력 전원 공급 에러 플래그 0: 출력 전원 공급이 정상임 1: 출력 전원 공급이 비정상이거나 전원이 OFF임	비세이프티
애플리케이션 번호	세이프티 애플리케이션 번호	비세이프티
커넥션 상태	커넥션 상태 정보 0: 커넥션이 확립되어 있지 않습니다. 1: 커넥션이 확립되어 있습니다.	비세이프티

오너 엽보
-For Reference Only-

입력 데이터(어셈블리 604~25C Hex), 크기 2바이트

바이트	비트							
	7	6	5	4	3	2	1	0
0	세이프티 입력 7	세이프티 입력 6	세이프티 입력 5	세이프티 입력 4	세이프티 입력 3	세이프티 입력 2	세이프티 입력 1	세이프티 입력 0

바이트	비트							
	7	6	5	4	3	2	1	0
1	세이프티 입력 상태	세이프티 출력 상태	출력 전원 공급 에러 플래그	커넥션 상태	세이프티 입력 11	세이프티 입력 10	세이프티 입력 9	세이프티 입력 8

입력 데이터(어셈블리 960~3C0 Hex), 크기 5바이트

바이트	비트							
	7	6	5	4	3	2	1	0
0	세이프티 입력 7	세이프티 입력 6	세이프티 입력 5	세이프티 입력 4	세이프티 입력 3	세이프티 입력 2	세이프티 입력 1	세이프티 입력 0
1	세이프티 입력 3 상태	세이프티 입력 2 상태	세이프티 입력 1 상태	세이프티 입력 0 상태	세이프티 입력 11	세이프티 입력 10	세이프티 입력 9	세이프티 입력 8
2	세이프티 입력 11 상태	세이프티 입력 10 상태	세이프티 입력 9 상태	세이프티 입력 8 상태	세이프티 입력 7 상태	세이프티 입력 6 상태	세이프티 입력 5 상태	세이프티 입력 4 상태
3	세이프티 입력 상태	세이프티 출력 상태	출력 전원 공급 에러 플래그	커넥션 상태	예약	예약	예약	예약
4	애플리케이션 번호							

입력 데이터(어셈블리 961~3C1 Hex), 크기 9바이트

바이트	비트							
	7	6	5	4	3	2	1	0
0	세이프티 입력 7	세이프티 입력 6	세이프티 입력 5	세이프티 입력 4	세이프티 입력 3	세이프티 입력 2	세이프티 입력 1	세이프티 입력 0
1	세이프티 입력 3 상태	세이프티 입력 2 상태	세이프티 입력 1 상태	세이프티 입력 0 상태	세이프티 입력 11	세이프티 입력 10	세이프티 입력 9	세이프티 입력 8
2	세이프티 입력 11 상태	세이프티 입력 10 상태	세이프티 입력 9 상태	세이프티 입력 8 상태	세이프티 입력 7 상태	세이프티 입력 6 상태	세이프티 입력 5 상태	세이프티 입력 4 상태
3	세이프티 출력 3 모니터	세이프티 출력 2 모니터	세이프티 출력 1 모니터	세이프티 출력 0 모니터	세이프티 출력 3 상태	세이프티 출력 2 상태	세이프티 출력 1 상태	세이프티 출력 0 상태
4	테스트 출력 7 상태	테스트 출력 6 상태	테스트 출력 5 상태	테스트 출력 4 상태	테스트 출력 3 상태	테스트 출력 2 상태	테스트 출력 1 상태	테스트 출력 0 상태
5	테스트 출력 3 모니터	테스트 출력 2 모니터	테스트 출력 1 모니터	테스트 출력 0 모니터	테스트 출력 11 상태	테스트 출력 10 상태	테스트 출력 9 상태	테스트 출력 8 상태
6	테스트 출력 11 모니터	테스트 출력 10 모니터	테스트 출력 9 모니터	테스트 출력 8 모니터	테스트 출력 7 모니터	테스트 출력 6 모니터	테스트 출력 5 모니터	테스트 출력 4 모니터
7	세이프티 입력 상태	세이프티 출력 상태	출력 전원 공급 에러 플래그	커넥션 상태	예약	예약	예약	예약
8	애플리케이션 번호							

AI 번역본 -For Reference Only-

A-2-2 세이프티 출력 어셈블리 데이터

이 절에서는 세이프티 출력 어셈블리 데이터를 보여줍니다.
데이터의 각 요소가 의미하는 바는 다음과 같습니다.

요소	의미	속성
세이프티 출력 N	세이프티 출력 단자 So N으로의 ON/OFF 0: 세이프티 출력 OFF 1: 세이프티 출력 ON	세이프티
스탠다드 출력 N	테스트 출력 단자 T N으로의 대기 출력 ON/OFF 0: 스탠다드 출력 OFF 1: 스탠다드 출력 ON	비세이프티
리모트 N 출력 M	리모트 출력 Ro N - M의 ON/OFF 0: 리모트 출력 OFF 1: 리모트 출력 ON	세이프티

출력 데이터(어셈블리 563~233 Hex), 크기 1바이트

바이트	비트							
	7	6	5	4	3	2	1	0
0	예약	예약	예약	예약	세이프티 출력 3	세이프티 출력 2	세이프티 출력 1	세이프티 출력 0

출력 데이터(어셈블리 881~371 Hex), 크기 3바이트

바이트	비트							
	7	6	5	4	3	2	1	0
0	예약	예약	예약	예약	예약	예약	리모트1 출력 1	리모트1 출력 0
1	스탠다드 출력 7	스탠다드 출력 6	스탠다드 출력 5	스탠다드 출력 4	스탠다드 출력 3	스탠다드 출력 2	스탠다드 출력 1	스탠다드 출력 0
2	예약	예약	예약	예약	스탠다드 출력 11	스탠다드 출력 10	스탠다드 출력 9	스탠다드 출력 8

AI 번역본

출력 데이터(어셈블리 882~372 Hex), 크기 1바이트

바이트	비트							
	7	6	5	4	3	2	1	0
0	예약	예약	예약	예약	예약	예약	리모트2 출력 1	리모트2 출력 0

출력 데이터(어셈블리 883~373 Hex), 크기 1바이트

바이트	비트							
	7	6	5	4	3	2	1	0
0	예약	예약	예약	예약	예약	예약	리모트3 출력 1	리모트3 출력 0

출력 데이터(어셈블리 896~380 Hex), 크기 3바이트

바이트	비트							
	7	6	5	4	3	2	1	0
0	예약	예약	예약	예약	세이프티 출력 3	세이프티 출력 2	세이프티 출력 1	세이프티 출력 0
1	스탠다드 출력 7	스탠다드 출력 6	스탠다드 출력 5	스탠다드 출력 4	스탠다드 출력 3	스탠다드 출력 2	스탠다드 출력 1	스탠다드 출력 0
2	예약	예약	예약	예약	스탠다드 출력 11	스탠다드 출력 10	스탠다드 출력 9	스탠다드 출력 8

A-2-3 컨피규레이션 어셈블리 데이터

이 절에서는 컨피규레이션 어셈블리 데이터를 보여줍니다.
데이터의 각 요소가 의미하는 바는 다음과 같습니다.

요소	의미
전원 투입 모드	시작 모드 0: 정지(idle) 1: Executing
테스트 출력 N 모드	테스트 출력 단자 T N에 사용하는 모드 0: 미사용 1: 스탠다드 출력 2: 테스트 출력 3: 전원 공급 출력
세이프티 출력 에러 래치 시간	세이프티 출력 단자의 출력 에러 래치 시간
세이프티 출력 N 채널 모드	세이프티 출력 단자 So N에 사용하는 모드 0: 미사용 1: 테스트 펄스 없이 사용 2: 테스트 펄스와 함께 사용
세이프티 출력 N/N+1 듀얼 채널 모드	세이프티 출력 단자 So N 및 So N+1에 사용하는 모드 0: 싱글 채널 1: 듀얼 채널
세이프티 입력 에러 래치 시간	세이프티 입력 단자의 입력 에러 래치 시간
세이프티 입력 N Off_On_Delay	세이프티 입력 단자 Si N의 OFF→ON 지연 시간
세이프티 입력 N On_Off_Delay	세이프티 입력 단자 Si N의 ON→OFF 지연 시간
세이프티 입력 N 채널 모드	세이프티 입력 단자 Si N에 사용하는 모드 0: 미사용 1: 테스트 출력 단자와 함께 사용 2: 반도체 입력 기기로서 테스트 펄스 없이 사용 3: 스탠다드 입력으로서 테스트 펄스 없이 사용
세이프티 입력 N 테스트 소스	세이프티 입력 단자 Si N에 연결하여 사용할 테스트 출력 단자 번호
세이프티 입력 N/N+1 듀얼 채널 모드	세이프티 입력 단자 Si N 및 Si N+1에 사용하는 모드 0: 싱글 채널 1: 듀얼 채널 등가 입력 2: 듀얼 채널 상보 입력
세이프티 입력 N/N+1 불일치 시간	불일치 시간
출력 로직 N Off_On_Delay	세이프티 출력 단자 So N의 OFF→ON 지연 시간
출력 로직 N On_Off_Delay	세이프티 출력 단자 So N의 ON→OFF 지연 시간
출력 로직 N 출력 조건	세이프티 출력 단자 So N에 대한 로직의 출력값 조건

사용금지
-For Evaluate Only-

요소	의미
출력 로직 N EDM 피드백	세이프티 출력 단자 So N에 EDM 피드백 값을 입력하는 데 사용할 세이프티 입력 단자 번호
입력 로직 N 입력 조건1	세이프티 입력 단자 Si N 및 리모트 출력의 로직 입력 조건 연산의 조건
입력 로직 N 리셋 조건	세이프티 입력 단자 Si N 및 리모트 출력의 로직 리셋 연산의 조건
입력 로직 N 리셋 최소 ON 펄스 폭	세이프티 입력 단자 Si N 및 리모트 출력에 대한 리셋 신호의 최소 ON 펄스 폭
입력 로직 N 리셋 최대 ON 펄스 폭	세이프티 입력 단자 Si N 및 리모트 출력에 대한 리셋 신호의 최대 ON 펄스 폭

컨피규레이션(어셈블리 864~360 Hex), 크기 340바이트

데이터	크기(바이트)	오프셋(바이트)
전원 투입 모드	1	0
패딩	1	1
테스트 출력 0 모드	1	2
테스트 출력 1 모드	1	3
테스트 출력 2 모드	1	4
테스트 출력 3 모드	1	5
테스트 출력 4 모드	1	6
테스트 출력 5 모드	1	7
테스트 출력 6 모드	1	8
테스트 출력 7 모드	1	9
테스트 출력 8 모드	1	10
테스트 출력 9 모드	1	11
테스트 출력 10 모드	1	12
테스트 출력 11 모드	1	13
세이프티 출력 에러 래치 시간	2	14
세이프티 출력 0 채널 모드	1	16
세이프티 출력 1 채널 모드	1	17
세이프티 출력 2 채널 모드	1	18
세이프티 출력 3 채널 모드	1	19
세이프티 출력 0/1 듀얼 채널 모드	1	20
세이프티 출력 2/3 듀얼 채널 모드	1	21
세이프티 입력 에러 래치 시간	2	22
세이프티 입력 0 Off_On_Delay	2	24
세이프티 입력 0 On_Off_Delay	2	26
세이프티 입력 0 채널 모드	1	28
세이프티 입력 0 테스트 소스	1	29
세이프티 입력 1 Off_On_Delay	2	30
세이프티 입력 1 On_Off_Delay	2	32
세이프티 입력 1 채널 모드	1	34
세이프티 입력 1 테스트 소스	1	35
세이프티 입력 2 Off_On_Delay	2	36
세이프티 입력 2 On_Off_Delay	2	38
세이프티 입력 2 채널 모드	1	40

AI 번역본
-For Reference Only-

데이터	크기(바이트)	오프셋(바이트)
세이프티 입력 2 테스트 소스	1	41
세이프티 입력 3 Off_On_Delay	2	42
세이프티 입력 3 On_Off_Delay	2	44
세이프티 입력 3 채널 모드	1	46
세이프티 입력 3 테스트 소스	1	47
세이프티 입력 4 Off_On_Delay	2	48
세이프티 입력 4 On_Off_Delay	2	50
세이프티 입력 4 채널 모드	1	52
세이프티 입력 4 테스트 소스	1	53
세이프티 입력 5 Off_On_Delay	2	54
세이프티 입력 5 On_Off_Delay	2	56
세이프티 입력 5 채널 모드	1	58
세이프티 입력 5 테스트 소스	1	59
세이프티 입력 6 Off_On_Delay	2	60
세이프티 입력 6 On_Off_Delay	2	62
세이프티 입력 6 채널 모드	1	64
세이프티 입력 6 테스트 소스	1	65
세이프티 입력 7 Off_On_Delay	2	66
세이프티 입력 7 On_Off_Delay	2	68
세이프티 입력 7 채널 모드	1	70
세이프티 입력 7 테스트 소스	1	71
세이프티 입력 8 Off_On_Delay	2	72
세이프티 입력 8 On_Off_Delay	2	74
세이프티 입력 8 채널 모드	1	76
세이프티 입력 8 테스트 소스	1	77
세이프티 입력 9 Off_On_Delay	2	78
세이프티 입력 9 On_Off_Delay	2	80
세이프티 입력 9 채널 모드	1	82
세이프티 입력 9 테스트 소스	1	83
세이프티 입력 10 Off_On_Delay	2	84
세이프티 입력 10 On_Off_Delay	2	86
세이프티 입력 10 채널 모드	1	88
세이프티 입력 10 테스트 소스	1	89
세이프티 입력 11 Off_On_Delay	2	90
세이프티 입력 11 On_Off_Delay	2	92
세이프티 입력 11 채널 모드	1	94
세이프티 입력 11 테스트 소스	1	95
세이프티 입력 0/1 듀얼 채널 모드	1	96
패딩	1	97
세이프티 입력 0/1 불일치 시간	2	98
세이프티 입력 2/3 듀얼 채널 모드	1	100
패딩	1	101
세이프티 입력 2/3 불일치 시간	2	102
세이프티 입력 4/5 듀얼 채널 모드	1	104
패딩	1	105
세이프티 입력 4/5 불일치 시간	2	106
세이프티 입력 6/7 듀얼 채널 모드	1	108

AI 번역본
-For Reference Only-

데이터	크기(바이트)	오프셋(바이트)
패딩	1	109
세이프티 입력 6/7 불일치 시간	2	110
세이프티 입력 8/9 듀얼 채널 모드	1	112
패딩	1	113
세이프티 입력 8/9 불일치 시간	2	114
세이프티 입력 10/11 듀얼 채널 모드	1	116
패딩	1	117
세이프티 입력 10/11 불일치 시간	2	118
출력 로직 0 Off_On_Delay	2	120
출력 로직 0 On_Off_Delay	2	122
출력 로직 0 출력 조건	4	124
출력 로직 0 EDM 피드백	1	128
패딩	1	129
출력 로직 1 Off_On_Delay	2	130
출력 로직 1 On_Off_Delay	2	132
출력 로직 1 출력 조건	4	134
출력 로직 1 EDM 피드백	1	138
패딩	1	139
출력 로직 2 Off_On_Delay	2	140
출력 로직 2 On_Off_Delay	2	142
출력 로직 2 출력 조건	4	144
출력 로직 2 EDM 피드백	1	148
패딩	1	149
출력 로직 3 Off_On_Delay	2	150
출력 로직 3 On_Off_Delay	2	152
출력 로직 3 출력 조건	4	154
출력 로직 3 EDM 피드백	1	158
패딩	1	159
입력 로직 0 입력 조건	4	160
입력 로직 0 리셋 조건	1	164
패딩	1	165
입력 로직 0 리셋 최소 ON 펄스 폭	2	166
입력 로직 0 리셋 최대 ON 펄스 폭	2	168
입력 로직 1 입력 조건	4	170
입력 로직 1 리셋 조건	1	174
패딩	1	175
입력 로직 1 리셋 최소 ON 펄스 폭	2	176
입력 로직 1 리셋 최대 ON 펄스 폭	2	178
입력 로직 2 입력 조건	4	180
입력 로직 2 리셋 조건	1	184
패딩	1	185
입력 로직 2 리셋 최소 ON 펄스 폭	2	186

AI 번역본
-For Reference Only-

데이터	크기(바이트)	오프셋(바이트)
입력 로직 2 리셋 최대 ON 펄스 폭	2	188
입력 로직 3 입력 조건	4	190
입력 로직 3 리셋 조건	1	194
패딩	1	195
입력 로직 3 리셋 최소 ON 펄스 폭	2	196
입력 로직 3 리셋 최대 ON 펄스 폭	2	198
입력 로직 4 입력 조건	4	200
입력 로직 4 리셋 조건	1	204
패딩	1	205
입력 로직 4 리셋 최소 ON 펄스 폭	2	206
입력 로직 4 리셋 최대 ON 펄스 폭	2	208
입력 로직 5 입력 조건	4	210
입력 로직 5 리셋 조건	1	214
패딩	1	215
입력 로직 5 리셋 최소 ON 펄스 폭	2	216
입력 로직 5 리셋 최대 ON 펄스 폭	2	218
입력 로직 6 입력 조건	4	220
입력 로직 6 리셋 조건	1	224
패딩	1	225
입력 로직 6 리셋 최소 ON 펄스 폭	2	226
입력 로직 6 리셋 최대 ON 펄스 폭	2	228
입력 로직 7 입력 조건	4	230
입력 로직 7 리셋 조건	1	234
패딩	1	235
입력 로직 7 리셋 최소 ON 펄스 폭	2	236
입력 로직 7 리셋 최대 ON 펄스 폭	2	238
입력 로직 8 입력 조건	4	240
입력 로직 8 리셋 조건	1	244
패딩	1	245
입력 로직 8 리셋 최소 ON 펄스 폭	2	246
입력 로직 8 리셋 최대 ON 펄스 폭	2	248
입력 로직 9 입력 조건	4	250
입력 로직 9 리셋 조건	1	254
패딩	1	255
입력 로직 9 리셋 최소 ON 펄스 폭	2	256

AI 번역본
-For Reference Only-

데이터	크기(바이트)	오프셋(바이트)
입력 로직 9 리셋 최대 ON 펄스 폭	2	258
입력 로직 10 입력 조건	4	260
입력 로직 10 리셋 조건	1	264
패딩	1	265
입력 로직 10 리셋 최소 ON 펄스 폭	2	266
입력 로직 10 리셋 최대 ON 펄스 폭	2	268
입력 로직 11 입력 조건	4	270
입력 로직 11 리셋 조건	1	274
패딩	1	275
입력 로직 11 리셋 최소 ON 펄스 폭	2	276
입력 로직 11 리셋 최대 ON 펄스 폭	2	278
입력 로직 12 입력 조건	4	280
입력 로직 12 리셋 조건	1	284
패딩	1	285
입력 로직 12 리셋 최소 ON 펄스 폭	2	286
입력 로직 12 리셋 최대 ON 펄스 폭	2	288
입력 로직 13 입력 조건	4	290
입력 로직 13 리셋 조건	1	294
패딩	1	295
입력 로직 13 리셋 최소 ON 펄스 폭	2	296
입력 로직 13 리셋 최대 ON 펄스 폭	2	298
입력 로직 14 입력 조건	4	300
입력 로직 14 리셋 조건	1	304
패딩	1	305
입력 로직 14 리셋 최소 ON 펄스 폭	2	306
입력 로직 14 리셋 최대 ON 펄스 폭	2	308
입력 로직 15 입력 조건	4	310
입력 로직 15 리셋 조건	1	314
패딩	1	315
입력 로직 15 리셋 최소 ON 펄스 폭	2	316
입력 로직 15 리셋 최대 ON 펄스 폭	2	318
입력 로직 16 입력 조건	4	320
입력 로직 16 리셋 조건	1	324
패딩	1	325
입력 로직 16 리셋 최소 ON 펄스 폭	2	326

AI 번역본
-For Reference Only-

데이터	크기(바이트)	오프셋(바이트)
입력 로직 16 리셋 최대 ON 펄스 폭	2	328
입력 로직 17 입력 조건	4	330
입력 로직 17 리셋 조건	1	334
패딩	1	335
입력 로직 17 리셋 최소 ON 펄스 폭	2	336
입력 로직 17 리셋 최대 ON 펄스 폭	2	338

AI 번역본
-For Reference Only-

A-3 I/O 어셈블리 포트와 대응하는 세이프티 I/O 어셈블리 데이터 요소

다음은 세이프티 I/O 블록의 I/O 어셈블리와, I/O 어셈블리를 I/O 맵에서
확장했을 때의 포트 이름을 보여줍니다.
각 포트는 세이프티 I/O 어셈블리 데이터의 요소와 1대1로 대응합니다.
세이프티 I/O 어셈블리 데이터 요소의 의미는 A-4페이지의 A-2 세이프티 I/O 어셈블리 데이터를 참조하십시오.

I/O 어셈블리	포트	데이터 유형	R/W	크기 (비트)	대응하는 세이프티 I/O 어셈블리 데이터의 요소
세이프티 입력 1	세이프티 입력 0-11 논리 값	SAFEBOOL	R	12	세이프티 입력 N
	세이프티 커넥션 상태	SAFEBOOL	R	1	커넥션 상태
	출력 전원 상태	SAFEBOOL	R	1	출력 전원 공급 에러 플래그
	통합 세이프티 출력 상태	SAFEBOOL	R	1	세이프티 출력 상태
	통합 세이프티 입력 상태	SAFEBOOL	R	1	세이프티 입력 상태
세이프티 입력 2	세이프티 입력 0-11 논리 값	SAFEBOOL	R	12	세이프티 입력 N
	세이프티 입력 0-11 상태	SAFEBOOL	R	12	세이프티 입력 N 상태
	세이프티 커넥션 상태	SAFEBOOL	R	1	커넥션 상태
	출력 전원 상태	SAFEBOOL	R	1	출력 전원 공급 에러 플래그
	통합 세이프티 출력 상태	SAFEBOOL	R	1	세이프티 출력 상태
	통합 세이프티 입력 상태	SAFEBOOL	R	1	세이프티 입력 상태
	애플리케이션 번호	SAFEINT	R	8	애플리케이션 번호
세이프티 입력 3	세이프티 입력 0-11 논리 값	SAFEBOOL	R	12	세이프티 입력 N
	세이프티 입력 0-11 상태	SAFEBOOL	R	12	세이프티 입력 N 상태
	세이프티 출력 0-3 상태	SAFEBOOL	R	4	세이프티 출력 N 상태
	세이프티 출력 0-3 모니터 값	SAFEBOOL	R	4	세이프티 출력 N 모니터
	테스트 출력 0-11 상태	SAFEBOOL	R	12	테스트 출력 N 상태
	테스트 출력 0-11 값	SAFEBOOL	R	12	테스트 출력 N 모니터
	세이프티 커넥션 상태	SAFEBOOL	R	1	커넥션 상태
	출력 전원 상태	SAFEBOOL	R	1	출력 전원 공급 에러 플래그
	통합 세이프티 출력 상태	SAFEBOOL	R	1	세이프티 출력 상태
	통합 세이프티 입력 상태	SAFEBOOL	R	1	세이프티 입력 상태
	애플리케이션 번호	SAFEINT	R	8	애플리케이션 번호
세이프티 출력	세이프티 출력 0-3 값	SAFEBOOL	W	4	세이프티 출력 N

샘플 번역본 For Reference Only

I/O 어셈블리	포트	데이터 유형	R/W	크기 (비트)	대응하는 세이프티 I/O 어셈블리 데이터의 요소
세이프티 리모트 출력 1 + 스탠다드 출력	리모트 1 출력 0-1	SAFEBOOL	W	2	리모트 N 출력 M
	테스트 출력 0-11 값	SAFEBOOL	W	12	스탠다드 출력 N
세이프티 리모트 출력 2	리모트 2 출력 0-1	SAFEBOOL	W	2	리모트 N 출력 M
세이프티 리모트 출력 3	리모트 3 출력 0-1	SAFEBOOL	W	2	리모트 N 출력 M
세이프티 출력 + 스탠다드 출력	세이프티 출력 0-3 값	SAFEBOOL	W	4	세이프티 출력 N
	테스트 출력 0-11 값	SAFEBOOL	W	12	스탠다드 출력 N

AI 번역본
-For Reference Only-

A-4 지원 CIP 오브젝트

지원되는 CIP 오브젝트는 아래와 같습니다.
세이프티 I/O 블록의 CIP 오브젝트에 액세스하려면 익스플리시트 메시지를 사용하십시오. 익스플리시트 메시지를 통해 CIP 오브젝트에 액세스하는 방법에 대한 자세한 내용은 6-7페이지의 익스플리시트 메시지 서버 기능을 참조하십시오.

오브젝트명	기능	참조
Identity 오브젝트	세이프티 I/O 블록의 제품 정보를 읽습니다.	A-17페이지의 A-4-1 Identity 오브젝트 (Class ID: 01 Hex)
어셈블리 오브젝트	세이프티 I/O 블록에 연결된 외부 기기의 I/O 데이터를 바인딩합니다.	A-19페이지의 A-4-2 어셈블리 오브젝트 (Class ID: 04 Hex)
Unit Manager 오브젝트	세이프티 I/O 블록의 유닛 정보를 집계합니다.	A-22페이지의 A-4-3 Unit Manager 오브젝트 (Class ID: 380 Hex)
Event History Log 오브젝트	이벤트 로그를 관리합니다.	A-27페이지의 A-4-4 Event History Log 오브젝트(Class ID: 34B Hex)
Error Event 오브젝트	현재 발생 중인 에러 이벤트를 관리합니다.	A-30페이지의 A-4-5 Error Event 오브젝트 (Class ID: 34C Hex)
Safety Discrete Input Point(SDIP) 오브젝트	세이프티 입력 단자를 한 번에 한 단자씩 개별 관리합니다.	A-33페이지의 A-4-6 Safety Discrete Input Point (SDIP) 오브젝트(Class ID: 3D Hex)
Safety Discrete Output Point(SDOP) 오브젝트	세이프티 출력 단자를 한 번에 한 단자씩 개별 관리합니다.	A-35페이지의 A-4-7 Safety Discrete Output Point (SDOP) 오브젝트(Class ID: 3B Hex)
Device Level Ring (DLR) 오브젝트	DLR 네트워크의 상태를 나타냅니다.	A-37페이지의 A-4-8 Device Level Ring (DLR) 오브젝트 (Class ID: 47 Hex)
QoS 오브젝트	이더넷 프레임 우선순위 제어에서 IPv4 DiffServ Code Point(DSCP)의 값을 설정합니다.	A-39페이지의 A-4-9 QoS 오브젝트 (Class ID: 48 Hex)
TCP/IP Interface 오브젝트	TCP/IP 인터페이스 설정을 구성합니다.	A-41페이지의 A-4-10 TCP/IP Interface 오브젝트(Class ID: F5 Hex)
Ethernet Link 오브젝트	이더넷 링크에 대한 다양한 정보를 가져옵니다.	A-45페이지의 A-4-11 Ethernet Link 오브젝트 (Class ID: F6 Hex)
LLDP Management 오브젝트	LLDP 기능을 관리합니다.	A-51페이지의 A-4-12 LLDP Management 오브젝트(Class ID: 109 Hex)
LLDP Data Table 오브젝트	LLDP 기능의 데이터를 관리합니다.	A-53페이지의 A-4-13 LLDP Data Table 오브젝트(Class ID: 10A Hex)
Logic Process 오브젝트	동작 중인 애플리케이션의 번호를 읽습니다.	A-58페이지의 A-4-14 Logic Process 오브젝트 (Class ID: 309 Hex)

AI 번역
-For Reference Only-

사용상의 주의

위 CIP 오브젝트의 경우, 파라미터 데이터의 데이터 유형이 INT, UINT, UDINT, ULINT, WORD 또는 DWORD이면 기록할 데이터를 리틀 엔디안 형식으로 저장하십시오.
읽은 데이터도 리틀 엔디안 형식으로 저장됩니다. 이 매뉴얼의 표기법은 상위 자릿수를 왼쪽에, 하위 자릿수를 오른쪽에 두는 표준 16진수 형식을 따른다는 점에 유의하십시오.

A-4-1 Identity 오브젝트(Class ID: 01 Hex)

Identity 오브젝트는 세이프티 I/O 블록에서 제품 정보를 읽는 데 사용됩니다.

Class ID 및 Instance ID

class ID 및 instance ID는 다음 표에 나와 있습니다.

ID 유형	값(hex)	설명
Class ID	01	-
Instance ID	00	클래스 자체를 지정합니다.
	01	인스턴스를 지정합니다.

Attribute ID

attribute ID는 읽을 정보를 지정합니다.

● Class Attribute ID

class attribute ID는 오브젝트 전체의 속성을 지정합니다.

Attribute ID	파라미터명	설명	어트리뷰트	데이터	
				데이터 타입	값(16진수)
1	리비전	오브젝트의 리비전	읽기	UINT	0002

● 인스턴스 Attribute ID

인스턴스 Attribute ID는 인스턴스의 Attribute ID를 지정합니다.

Attribute ID	파라미터명	설명	어트리뷰트	데이터	
				데이터 타입	값
1	Vendor ID	Vendor ID	읽기	UINT	002F hex
2	기기 유형	기기 유형	읽기	UINT	0308 hex (Safety IO and Logic Device)
3	제품 코드	제품 코드	읽기	UINT	NXR-SXD1204-CST: 0BF9 hex NXR-SXD1204B-CST: 0BFA hex
4	리비전	기기 CIP 리비전	읽기	STRUCT	–
	메이저 리비전	메이저 리비전		USINT	01 hex
	마이너 리비전	마이너 리비전		USINT	01 hex
5	상태	세이프티 I/O 블록의 상태	읽기	WORD	아래 A-18페이지의 상태 값을 참조하십시오.
6	시리얼 번호	시리얼 번호	읽기	UDINT	각 제품 유닛의 고유 번호
7	제품명	제품명	읽기	SHORT STRING	아래 A-18페이지의 제품명 값을 참조하십시오.

AI 번역본
-For Reference Only-

● 상태 값

비트	이름	설명
0	Owned	세이프티 I/O 블록이 타겟으로서 커넥션을 오픈했음을 나타냅니다. · TRUE: 오픈됨 · FALSE: 오픈되지 않음
1	예약	항상 FALSE
2	Configured	세이프티 I/O 블록이 구성되어 있음을 나타냅니다. · TRUE: 구성됨 · FALSE: 구성되지 않음
3	예약	항상 FALSE
4~7	확장 기기 상태	*1
8	예약	항상 FALSE
9	예약	항상 FALSE
10	Major Recoverable Fault	· TRUE: MS 표시등이 적색으로 점멸하는 에러가 발생하고 있습니다. · FALSE: MS 표시등이 적색으로 점멸하는 에러가 발생하고 있지 않습니다.
11	Major Unrecoverable Fault	· TRUE: MS 표시등이 적색으로 점등하는 에러가 발생하고 있습니다. · FALSE: MS 표시등이 적색으로 점등하는 에러가 발생하고 있지 않습니다.
12~15	예약	항상 FALSE

***1.** Extended Status 값의 의미는 다음과 같습니다.

- 0~1: 예약
- 2: 클래스 1 통신(태그 데이터 링크) 커넥션에서 1개 이상의 타임아웃이 발생하고 있습니다.
- 3: 클래스 1 통신(태그 데이터 링크) 커넥션이 확립되어 있지 않습니다.
- 4-5 : 예약
- 6: 1개 이상의 클래스 1 통신(태그 데이터 링크) 커넥션이 RUN 모드에서 정상적으로 통신하고 있습니다.
- 7: 1개 이상의 클래스 1 통신(태그 데이터 링크) 커넥션이 확립되어 있고, 모두 Idle 모드입니다.
- 8~15: 예약

● 제품명 값

모델	값(16진수)
NXR-SXD1204-CST	0F 4E 58 52 2D 53 58 44 31 32 30 34 2D 43 53 54
NXR-SXD1204B-CST	10 4E 58 52 2D 53 58 44 31 32 30 34 42 2D 43 53 54

AI 번역본
-For Reference Only-

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

서비스 코드(16진수)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
01	Get_Attribute_All	모든 어트리뷰트의 값을 읽습니다.	불가	가능
0E	Get_Attribute_Single	지정된 어트리뷰트의 값을 읽습니다.	가능	가능

A-4-2 어셈블리 오브젝트 (Class ID: 04 Hex)

어셈블리 오브젝트는 세이프티 I/O 블록에 접속된 외부 기기의 I/O 데이터를 결합하는 데 사용됩니다.

Class ID 및 Instance ID

Class ID 및 Instance ID는 다음 표에 나와 있습니다.

ID 타입	값(16진수)	설명
Class ID	04	–
Instance ID	00	클래스 자체를 지정합니다.
	25C, 3C0, 3C1	세이프티 입력 어셈블리 데이터
	233, 371, 372, 373, 380	세이프티 출력 어셈블리 데이터
	360	컨피규레이션 어셈블리 데이터

Attribute ID

Attribute ID는 읽어들일 정보를 지정합니다.

● 클래스 Attribute ID

클래스 Attribute ID는 오브젝트 전체의 어트리뷰트를 지정합니다.

Attribute ID	파라미터명	설명	어트리뷰트	데이터	
				데이터 타입	값(16진수)
1	리비전	오브젝트의 리비전	읽기	UINT	0003

● 인스턴스 Attribute ID

인스턴스 Attribute ID는 인스턴스의 Attribute ID를 지정합니다.
할당된 인스턴스가 스탠다드 출력뿐인 경우 쓰기가 가능합니다.

Instance ID 25C hex에 대한 Attribute ID

Attribute ID	파라미터명	설명	어트리뷰트	데이터	
				데이터 타입	값
03	데이터	입출력 데이터	읽기	ARRAY OF BYTE	A-4페이지의 입력 데이터(어셈블리 604 ~25C Hex), 크기 2바이트를 참조하십시오.

AI 번역본
-For Reference Only-

Instance ID 3C0 hex에 대한 Attribute ID

Attribute ID	파라미터명	설명	어트리뷰트	데이터	
				데이터 타입	값
03	데이터	입출력 데이터	읽기	ARRAY OF BYTE	A-5페이지의 입력 데이터(어셈블리 960 ~3C0 Hex), 크기 5바이트를 참조하십시오.

Instance ID 3C1 hex에 대한 Attribute ID

Attribute ID	파라미터명	설명	어트리뷰트	데이터	
				데이터 타입	값
03	데이터	입출력 데이터	읽기	ARRAY OF BYTE	A-5페이지의 출력 데이터(어셈블리 961~3C1 Hex), 크기 9바이트를 참조하십시오.

Instance ID 233 hex에 대한 Attribute ID

Attribute ID	파라미터명	설명	어트리뷰트	데이터	
				데이터 타입	값
03	데이터	입출력 데이터	읽기	ARRAY OF BYTE	A-6페이지의 출력 데이터(어셈블리 563~233 Hex), 크기 1바이트를 참조하십시오.

Instance ID 371 hex에 대한 Attribute ID

Attribute ID	파라미터명	설명	어트리뷰트	데이터	
				데이터 타입	값
03	데이터	입출력 데이터	읽기	ARRAY OF BYTE	A-6페이지의 출력 데이터(어셈블리 881~371 Hex), 크기 3바이트를 참조하십시오.

Instance ID 372 hex에 대한 Attribute ID

Attribute ID	파라미터명	설명	어트리뷰트	데이터	
				데이터 타입	값
03	데이터	입출력 데이터	읽기	ARRAY OF BYTE	A-6페이지의 출력 데이터(어셈블리 882~372 Hex), 크기 1바이트를 참조하십시오.

Instance ID 373 hex에 대한 Attribute ID

Attribute ID	파라미터명	설명	어트리뷰트	데이터	
				데이터 타입	값
03	데이터	입출력 데이터	읽기	ARRAY OF BYTE	A-6페이지의 출력 데이터(어셈블리 883~373 Hex), 크기 1바이트를 참조하십시오.

AI 번역본

Instance ID 380 hex에 대한 Attribute ID

Attribute ID	파라미터명	설명	어트리뷰트	데이터	
				데이터 타입	값
03	데이터	입출력 데이터	읽기	ARRAY OF BYTE	A-7페이지의 출력 데이터(어셈블리 896~380 Hex), 크기 3바이트를 참조하십시오.

Instance ID 360 hex에 대한 Attribute ID

Attribute ID	파라미터명	설명	어트리뷰트	데이터	
				데이터 타입	값
03	데이터	입출력 데이터	읽기	ARRAY OF BYTE	컨피규레이션(어셈블리 864~360 Hex), 크기 340바이트, A-8 페이지

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

서비스 코드(16진수)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
0E	Get_Attribute_Single	지정한 어트리뷰트의 값을 읽습니다.	가능	가능

AI 번역본
-For Reference Only-

A-4-3 유닛 매니저 오브젝트 (클래스 ID: 380 Hex)

유닛 매니저 오브젝트는 세이프티 I/O 블록의 유닛 정보를 집약합니다.

클래스 ID 및 인스턴스 ID

클래스 ID 및 인스턴스 ID는 다음 표와 같습니다.

ID 유형	값(16진수)	설명
클래스 ID	380	
인스턴스 ID	00	클래스 자체를 지정합니다.
	01	인스턴스를 지정합니다.

어트리뷰트 ID

어트리뷰트 ID는 읽을 정보를 지정합니다.

● 클래스 어트리뷰트 ID

클래스 어트리뷰트 ID는 오브젝트 전체의 어트리뷰트를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값(16진수)
1	Revision	오브젝트의 리비전	읽기	UINT	0001

● 인스턴스 어트리뷰트 ID

인스턴스 어트리뷰트 ID는 인스턴스의 어트리뷰트 ID를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
1	Unit Version	유닛 버전	읽기	DWORD	아래 A-25쪽의 Unit Version 및 Hardware Version 값을 참조하십시오.
2	Hardware Version	하드웨어 버전	읽기	DWORD	아래 A-25쪽의 Unit Version 및 Hardware Version 값을 참조하십시오.
3	Firmware Version	펌웨어 버전	읽기	DWORD	아래 A-25쪽의 Firmware Version 값을 참조하십시오.
5	Unit/Input Power Voltage	유닛/입력 전원 공급 전압	읽기	UINT	유닛/입력 전원 공급 전압의 현재값 *1 값의 단위는 100 mV입니다. 예를 들어 24.1 V인 경우 값은 241입니다.
6	Max Unit/Input Power Voltage	최대 유닛/입력 전원 공급 전압	읽기	UINT	유닛/입력 전원 공급 전압의 최댓값 *1 값의 단위는 100 mV입니다.

AI 번역본 -For Reference Only-

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
7	Min Unit/ Input Power Voltage	최소 유닛/ 입력 전원 공급 전압	읽기	UINT	유닛/입력 전원 공급 전압의 최솟값 *1 값의 단위는 100 mV입니다.
8	Output Power Voltage	출력 전원 공급 전압	읽기	UINT	출력 전원 공급 전압의 현재값 *1 값의 단위는 100 mV입니다.
9	Max Output Power Voltage	최대 출력 전원 공급 전압	읽기	UINT	출력 전원 공급 전압의 최댓값 *1 값의 단위는 100 mV입니다.
10	Min Output Power Supply Voltage	최소 출력 전원 공급 전압	읽기	UINT	출력 전원 공급 전압의 최솟값 *1 값의 단위는 100 mV입니다.
11	Operate Hours	유닛 총 동작 시간	읽기	UDINT	유닛의 총 동작 시간 (단위: h)
12	SNTP server IP address	SNTP 서버의 IP 주소	읽기/쓰기	UDINT	"0": 자동 시각 조정 비활성화 "0" 이외: SNTP 서버의 IP 주소 이 설정은 유닛을 재시작한 후 유효합니다. 다음 값은 설정할 수 없습니다. · 0, 127, 255로 시작하는 IP 주소 · 클래스 D IP 주소 (224.0.0.0~ 239.255.255.255) · 클래스 E IP 주소 (240.0.0.0~ 255.255.255.255) · 링크 로컬 주소 (169.254.0.0~ 169.254.255.255)
20	Unit/Input Power Current	유닛/입력 전원 공급 전류	읽기	UINT	유닛/입력 전원 공급 전류의 현재값 *1 값의 단위는 100 mA입니다. 예를 들어 5.1 A인 경우 값은 51입니다.
21	Max Unit/ Input Power Current	최대 유닛/입력 전원 공급 전류	읽기	UINT	유닛/입력 전원 공급 전류의 최댓값 *1 값의 단위는 100 mA입니다.
22	Min Unit/ Input Power Current	최소 유닛/ 입력 전원 공급 전류	읽기	UINT	유닛/입력 전원 공급 전류의 최솟값 *1 값의 단위는 100 mA입니다.
23	Output Power Current	출력 전원 공급 전류	읽기	UINT	출력 전원 공급 전류의 현재값 *1 값의 단위는 100 mA입니다.

AI 번역
For Reference Only

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
24	Max Output Power Current	최대 출력 전원 공급 전류	읽기	UINT	출력 전원 공급 전류의 최댓값 *1 값의 단위는 100 mA입니다.
25	Min Output Power Current	최소 출력 전원 공급 전류	읽기	UINT	출력 전원 공급 전류의 최솟값 *1 값의 단위는 100 mA입니다.
26	Unit/Input Power Supply Error Flag	유닛/입력 전원 공급 에러 플래그	읽기	BOOL	TRUE: 전압값이 정상 범위를 벗어남 FALSE: 전압값이 정상 범위 이내
27	Output Power Supply Error Flag	출력 전원 공급 에러 플래그	읽기	BOOL	TRUE: 전압값이 정상 범위를 벗어남 FALSE: 전압값이 정상 범위 이내
28	Cross-Wiring Output Power Shut-off Control	스루 배선 출력 전원 공급	읽기/쓰기	BOOL	TRUE: 스루 배선 출력 전원이 공급됨 (초기값). FALSE: 스루 배선 출력 전원이 공급되지 않음. 단, 이는 Cross-Wiring Output Shut-off Enable의 값이 TRUE일 때만 유효합니다.
29	Cross-Wiring Output Power Shut-off Enable	스루 배선 출력의 전원 차단 기능 사용 여부	읽기/쓰기	BOOL	TRUE: 스루 배선 출력의 전원 차단 기능을 사용함(초기값). FALSE: 스루 배선 출력의 전원 차단 기능을 사용하지 않음. 새 설정은 즉시 적용됩니다.
30	Communication Port Enable	통신 사용/사용 안 함 설정	읽기/쓰기	USINT	0: 포트 1과 포트 2가 모두 사용됨(초기값) 1: 포트 1은 사용되고 포트 2는 사용되지 않음 2: 포트 1은 사용되지 않고 포트 2는 사용됨 이 설정은 재시작 후 유효합니다.
100	Time	현재 시각	읽기	DATE_AND_TIME	시간대에 따른 현지 시각입니다. 시각 정보를 자동 시각 조정(SNTP)으로 취득한 경우 SNTP로 보정된 시각이 됩니다. SNTP를 사용하지 않는 경우 1972년 1월 1일 00:00:00부터 카운트한 시각이 됩니다. 초기값은 DT#1972-01-01-00:00:00.000입니다.
102	Time Zone Offset - Minutes	협정 세계시 (UTC)와 Time 사이의 차이 (분)	읽기/쓰기	INT	-720~840 협정 세계시(UTC)와 Time 사이의 차이를 분 단위로 나타냅니다. 예를 들어 UTC가 0:00 AM이고 Time이 2:30 AM인 경우 Time Zone Offset - Minutes의 값은 150이 됩니다. 초기값은 0입니다. 이 설정은 유닛을 재시작한 후 유효합니다.

AI 번역본
-For Reference Only-

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
104	Firmware Hash Value	펌웨어 해시 값	읽기	ARRAY OF USINT	펌웨어 해시값 32바이트

*1. 유닛을 재시작하면 값이 리셋됩니다.

● Unit Version 및 Hardware Version 값

비트	이름	설명
0~15	예약	항상 FALSE
16~23	마이너 버전 번호 필드	마이너 버전은 BCD로 표시됩니다. 0~99
24~31	메이저 버전 번호 필드	메이저 버전은 BCD로 표시됩니다. 0~9

예를 들어 유닛 버전이 1.01인 경우 유닛 버전 값은 01010000 hex입니다.
유닛 버전이 7.12인 경우 유닛 버전 값은 07120000 hex입니다.

● Firmware Version 값

비트	이름	설명
0~7	예약	항상 FALSE
8~15	리비전 번호 필드	리비전 번호는 BCD로 표시됩니다. 0~99
16~23	마이너 버전 번호 필드	마이너 버전은 BCD로 표시됩니다. 0~99
24~31	메이저 버전 번호 필드	메이저 버전은 BCD로 표시됩니다. 0~9

예를 들어 펌웨어 버전이 1.01.02인 경우 펌웨어 버전 값은 01010200 hex입니다.
펌웨어 버전이 7.00.10인 경우 펌웨어 버전 값은 07001000 hex입니다.

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

AI 번역본

서비스 코드(16진수)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
0E	Get_Attribute_Single	지정한 어트리뷰트의 값을 읽습니다.	가능	가능
10	Set_Attribute_Single	지정한 어트리뷰트의 값을 씁니다.	불가능	가능
4B	Execute_WhereAmI	유닛 식별 기능을 실행합니다.	불가능	가능

Execute_WhereAmI (서비스 코드: 4B Hex)

유닛 식별 기능을 실행합니다. 요청 형식은 다음과 같습니다.

● 요청 형식

파라미터 명	설명	데이터형	값
Service	서비스 코드	USINT	4B hex
Request Path Size	요청 경로의 크기	USINT	03
Request Path	요청 경로	Padded EPATH	210080032401 hex
Blink Dura-tion	유닛 식별 기능 실행 시간	UINT	0: 유닛 식별 기능을 정지합니다. 5~1,800: 지정한 시간 동안만 유닛 식별 기능을 실행합니다. 단위는 초입니다. 유닛 식별 표시등은 Blink Duration에서 지정한 시간 동안 아래와 같이 점등과 소등을 반복합니다. · 표시등은 시계 방향으로 각각 100 ms씩 점등하며, 이를 4회 반복합니다. · 표시등은 모두 500 ms 동안 소등됩니다.

AI 번역본
-For Reference Only-

A-4-4 이벤트 히스토리 로그 오브젝트 (클래스 ID: 34B Hex)

이벤트 히스토리 로그 오브젝트는 이벤트 로그를 관리하는 데 사용됩니다.

클래스 ID 및 인스턴스 ID

클래스 ID 및 인스턴스 ID는 다음 표와 같습니다.

ID 유형	값(16진수)	설명
클래스 ID	34B	
인스턴스 ID	01~02	인스턴스를 지정합니다. 01: 시스템 이벤트 로그(전체 MPU 공용) 02: 액세스 이벤트 로그(전체 MPU 공용)

어트리뷰트 ID

어트리뷰트 ID는 읽을 정보를 지정합니다.

● 클래스 어트리뷰트 ID

클래스 어트리뷰트 ID는 오브젝트 전체의 어트리뷰트를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값(16진수)
1	Revision	오브젝트의 리비전	읽기	UINT	0001
2	Max Instance	최대 인스턴스 번호	읽기	UINT	0005
3	Number of Instance	인스턴스 수	읽기	UINT	0005

● 인스턴스 어트리뷰트 ID

인스턴스 어트리뷰트 ID는 인스턴스의 어트리뷰트 ID를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
1	Max Number of Record	등록 가능한 레코드 수	읽기	UINT	인스턴스 ID 값에 따라 개수가 다음과 같이 달라집니다. 01 hex: 100 레코드 02 hex: 100 레코드
2	Number of Record	등록된 레코드 수	읽기	UINT	0~Max Number of Record
3	Undate Counter	카운터	읽기	UINT	1~65,535
4	Size of Record	읽을 레코드의 바이트 크기	읽기	UINT	40

AI 번역본 -For Reference Only-

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

서비스 코드(16진수)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
01	Get_Attribute_All	모든 어트리뷰트의 값을 읽습니다.	가능	가능

서비스 코드(16진수)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
0E	Get_Attribute_Single	지정한 어트리뷰트의 값을 읽습니다.	가능	가능
34	Get Event Log	지정한 이벤트 로그의 내용을 읽습니다.	불가능	가능

Get_Event_Log (서비스 코드: 34 Hex)

지정한 이벤트 로그의 내용을 읽습니다. 요청 형식 및 응답 형식은 다음과 같습니다.

● 요청 형식

파라미터명	설명	데이터형	값
Service	서비스 코드	USINT	34 hex
Request Path Size	요청 경로의 크기	USINT	03
Request Path	요청 경로	Padded EPATH	21004B032401~ 21004B032402 hex
Start Number of Read	읽기를 시작할 레코드 번호 첫 번째 번호는 0입니다.	UINT	
Number of Read	읽을 레코드 수*1	UINT	
Update Counter	어트리뷰트 ID 3(Update Counter)의 값(대상 인스턴스를 사전에 읽음)*2 0: 레코드 갱신 검출 비활성화 0 이외: 레코드 갱신 검출 활성화	UINT	

*1. 지정한 레코드 수가 존재하지 않는 경우, 실제로 읽은 레코드 수는 응답의 Actual Number of Read에 저장됩니다.

*2. 값이 현재 Update Counter의 값과 다른 경우 Object state conflict(0C hex)가 반환됩니다.

● 응답 형식

파라미터명	설명	데이터형	값
Reply Service	Get Event Log 서비스에 대한 응답	USINT	B4 hex
Reserved	예약	octet	00
General Status	정상을 나타내는 코드	USINT	00
Size of Additional Status	Additional status의 크기	USINT	00
Start Number of Read	실제로 읽은 첫 번째 레코드 번호	UINT	
Actual Number of Read	실제로 읽은 레코드 수	UINT	
Update Counter	카운터	UINT	
Number of Record	등록된 레코드 수	UINT	
Record	이벤트 로그 레코드	ARRAY OF STRUCT OF*1	

AI 번역본 -For Reference Only-

파라미터명	설명	데이터형	값
Index	레코드의 인덱스*2	UDINT	0~4,294,967,295 레코드마다 값이 증가하며, 최댓값에 도달하면 0으로 돌아갑니다.
Time	이벤트가 발생한 시각	DATE_AND_TIME	
Product Code	제품 코드	DWORD	
Event Code	이벤트 코드*3	DWORD	
Event Priority	이벤트 레벨	WORD	3: 경미한 폴트 4: 관찰 5: 정보
Additional Info Data Type1	이벤트 추가 정보 1의 데이터형	BYTE	
Additional Info Data Type2	이벤트 추가 정보 2의 데이터형	BYTE	
Additional Info Data Type3	이벤트 추가 정보 3의 데이터형	BYTE	
Additional Info Data Type4	이벤트 추가 정보 4의 데이터형	BYTE	
Additional Info1	추가 정보 1 이벤트*3	Additional Info Data Type1에 지정된 데이터형(4옥텟)	
Additional Info2	추가 정보 2 이벤트*3	Additional Info Data Type2에 지정된 데이터형(4옥텟)	
Additional Info3	추가 정보 3 이벤트*3	Additional Info Data Type3에 지정된 데이터형(4옥텟)	
Additional Info4	추가 정보 4 이벤트*3	Additional Info Data Type4에 지정된 데이터형(4옥텟)	

***1.** 구조체의 크기는 40바이트입니다.

***2.** 번호는 인스턴스 ID = 01 hex(시스템 이벤트 로그) 및 인스턴스 ID = 02 hex(액세스 이벤트 로그)를 통해 할당됩니다.

***3.** 설명에 대한 자세한 내용은 11-12쪽의 11-2-4 이벤트 상세 및 문제 해결을 참조하십시오.

AI 번역본
-For Reference Only-

A-4-5 에러 이벤트 오브젝트 (클래스 ID: 34C Hex)

에러 이벤트 오브젝트는 현재 발생 중인 에러 이벤트를 관리하는 데 사용됩니다.

클래스 ID 및 인스턴스 ID

클래스 ID 및 인스턴스 ID는 다음 표와 같습니다.

ID 유형	값(16진수)	설명
클래스 ID	34C	
인스턴스 ID	00	클래스 자체를 지정합니다.
	01	인스턴스를 지정합니다.

어트리뷰트 ID

어트리뷰트 ID는 읽을 정보를 지정합니다.

● 클래스 어트리뷰트 ID

클래스 어트리뷰트 ID는 오브젝트 전체의 어트리뷰트를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값(16진수)
1	Revision	오브젝트의 리비전	읽기	UINT	0001
2	Max Instance	최대 인스턴스 번호	읽기	UINT	0001
3	Number of Instance	인스턴스 수	읽기	UINT	0001

● 인스턴스 어트리뷰트 ID

인스턴스 어트리뷰트 ID는 인스턴스의 어트리뷰트 ID를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
1	Max Number of Record	등록 가능한 레코드 수	읽기	UINT	
2	Number of Record	등록된 레코드 수	읽기	UINT	0~Max Number of Record
3	Undate Counter	카운터	읽기	UINT	1~65,535
4	Size of Record	읽을 레코드의 바이트 크기	읽기	UINT	34

AI 번역본
-For Reference Only-

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

서비스 코드(16진수)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
01	Get_Attribute_All	모든 어트리뷰트의 값을 읽습니다.	가능	가능
0E	Get_Attribute_Single	지정한 어트리뷰트의 값을 읽습니다.	가능	가능
34	Get Error Event	현재 발생 중인 에러 이벤트를 가져옵니다.	불가능	가능

Get_Error_Event (서비스 코드: 34 Hex)

현재 발생 중인 에러 이벤트를 가져옵니다. 요청 형식 및 응답 형식은 다음과 같습니다.

● 요청 형식

파라미터명	설명	데이터형	값
Service	서비스 코드	USINT	34 hex
Request Path Size	요청 경로의 크기	USINT	03
Request Path	요청 경로	Padded EPATH	21004C032401 hex
Start Number of Read	읽기를 시작할 레코드 번호 첫 번째 번호는 0입니다.	UINT	
Number of Read	읽을 레코드 수*1	UINT	
Update Counter	어트리뷰트 ID 3(Update Counter)의 값(사전에 읽은 인스턴스용)*2 0: 레코드 갱신 검출 비활성화 0 이외: 레코드 갱신 검출 활성화	UINT	

***1.** 지정한 레코드 수가 존재하지 않는 경우, 실제로 읽은 레코드 수는 응답의 Actual Number of Read에 저장됩니다.

***2.** 값이 현재 Update Counter의 값과 다른 경우 Object state conflict(0C hex)가 반환됩니다.

● 응답 형식

파라미터명	설명	데이터형	값
Reply Service	Get Error Event 서비스에 대한 응답	USINT	B4 hex
Reserved	예약	octet	00
General Status	정상을 나타내는 코드	USINT	00
Size of Additional Status	Additional status의 크기	USINT	00
Start Number of Read	실제로 읽은 첫 번째 레코드 번호	UINT	
Actual Number of Read	실제로 읽은 레코드 수	UINT	
Update Counter	카운터	UINT	
Number of Record	등록된 레코드 수	UINT	
Record	에러 이벤트 레코드	ARRAY OF STRUCT OF*1	

AI 번역본
-For Reference Only-

파라미터명	설명	데이터형	값
Index	레코드의 인덱스*2	UDINT	0~4,294,967,295 레코드마다 값이 증가하며, 최댓값에 도달하면 0으로 돌아갑니다.
Product Code	제품 코드	DWORD	
Event Code	이벤트 코드*3	DWORD	
Event Priority	이벤트 레벨	WORD	3: 경미한 폴트
Additional Info Data Type1	이벤트 추가 정보 1의 데이터형	BYTE	
Additional Info Data Type2	이벤트 추가 정보 2의 데이터형	BYTE	
Additional Info Data Type3	이벤트 추가 정보 3의 데이터형	BYTE	
Additional Info Data Type4	이벤트 추가 정보 4의 데이터형	BYTE	
Additional Info1	이벤트의 추가 정보 1*3	Additional Info Data Type1에 지정된 데이터형 (4옥텟)	
Additional Info2	이벤트의 추가 정보 2*3	Additional Info Data Type2에 지정된 데이터형 (4옥텟)	
Additional Info3	이벤트의 추가 정보 3*3	Additional Info Data Type3에 지정된 데이터형 (4옥텟)	
Additional Info4	이벤트의 추가 정보 4*3	Additional Info Data Type4에 지정된 데이터형 (4옥텟)	

***1.** 구조체의 크기는 34바이트입니다.

***2.** 이 오브젝트는 현재 발생 중인 에러 이벤트를 대상으로 합니다. Index는 에러 이벤트가 발생한 시점에 할당되므로, 이후 복구된 에러 이벤트가 있으면 값이 불연속적으로 됩니다.

***3.** 설명에 대한 자세한 내용은 11-12쪽의 11-2-4 이벤트 상세 및 문제 해결을 참조하십시오.

AI 번역본
-For Reference Only-

A-4-6 세이프티 디스크리트 입력 포인트(SDIP) 오브젝트 (클래스 ID: 3D Hex)

세이프티 디스크리트 입력 포인트(SDIP) 오브젝트는 세이프티 입력 단자를 한 번에 하나씩 개별적으로 관리하는 데 사용됩니다.

클래스 ID 및 인스턴스 ID

클래스 ID 및 인스턴스 ID는 다음 표와 같습니다.

ID 유형	값(16진수)	설명
클래스 ID	3D	
인스턴스 ID	00	클래스 자체를 지정합니다.
	01-0C	세이프티 입력 단자별 인스턴스를 지정합니다. 01: 세이프티 입력 단자 Si00 02: 세이프티 입력 단자 Si01 03: 세이프티 입력 단자 Si02 04: 세이프티 입력 단자 Si03 05: 세이프티 입력 단자 Si04 06: 세이프티 입력 단자 Si05 07: 세이프티 입력 단자 Si06 08: 세이프티 입력 단자 Si07 09: 세이프티 입력 단자 Si08 0A: 세이프티 입력 단자 Si09 0B: 세이프티 입력 단자 Si10 0C: 세이프티 입력 단자 Si11

어트리뷰트 ID

어트리뷰트 ID는 읽을 정보를 지정합니다.

● 클래스 어트리뷰트 ID

클래스 어트리뷰트 ID는 오브젝트 전체의 어트리뷰트를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값(16진수)
1	Revision	오브젝트의 리비전	읽기	UINT	0001
2	Max Instance	최대 인스턴스 번호	읽기	UINT	000C
3	Number of Instance	인스턴스 수	읽기	UINT	000C
8	Latch Input Error Time	Instance Attribute의 Safety Status에서 Alarm 상태에 대한 래치 시간	읽기 *1	UINT	0~65,530 초기값은 1000(DEC)입니다. 단위는 ms입니다. 10 ms 단위로 설정 가능합니다.

산업 억분 For Reference Only

*1. 컨피규레이션이 잠금 해제된 상태에서 쓸 수 있습니다.

● 인스턴스 어트리뷰트 ID

인스턴스 어트리뷰트 ID는 인스턴스의 어트리뷰트 ID를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
102	Maintenance Counter	Maintenance Counter의 현재값	읽기/ 쓰기	UDINT	Maintenance Counter의 현재값 세이프티 입력 단자의 접점 동작 횟수를 나타냅니다. (단위: 회). 값을 지우려면 0을 쓰십시오.

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

서비스 코드(16진수)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
0E	Get_Attribute_Single	지정한 어트리뷰트의 값을 읽습니다.	가능	가능
10	Set_Attribute_Single	지정한 어트리뷰트의 값을 씁니다.	불가능	가능

AI 번역본
-For Reference Only-

A-4-7 세이프티 디스크리트 출력 포인트(SDOP) 오브젝트 (클래스 ID: 3B Hex)

세이프티 디스크리트 출력 포인트(SDOP) 오브젝트는 세이프티 출력 단자를 한 번에 하나씩 개별적으로 관리하는 데 사용됩니다.

클래스 ID 및 인스턴스 ID

클래스 ID 및 인스턴스 ID는 다음 표와 같습니다.

ID 유형	값(16진수)	설명
클래스 ID	3B	
인스턴스 ID	00	클래스 자체를 지정합니다.
	01~04	세이프티 출력 단자별 인스턴스를 지정합니다.

어트리뷰트 ID

어트리뷰트 ID는 읽을 정보를 지정합니다.

● 클래스 어트리뷰트 ID

클래스 어트리뷰트 ID는 오브젝트 전체의 어트리뷰트를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값(16진수)
1	Revision	오브젝트의 리비전	읽기	UINT	0001
2	Max Instance	최대 인스턴스 번호	읽기	UINT	0004
3	Number of Instance	인스턴스 수	읽기	UINT	0004
8	Latch Output Error Time	Instance attribute의 Safety Status에 대한 Alarm 상태의 래치 시간	읽기	UINT	0~65,530 초기값은 1000(DEC)입니다. 단위는 ms입니다. 10 ms 단위로 설정 가능합니다.

● 인스턴스 어트리뷰트 ID

Instance Attribute ID는 인스턴스의 Attribute ID를 지정합니다.

속성 ID	파라미터명	설명	속성	데이터	
				데이터형	값
102 Maintenance Counter Maintenance Counter의 현재값			읽기/쓰기	UDINT	Maintenance Counter의 현재값입니다. 세이프티 출력 단자의 접점 동작 횟수를 나타냅니다 (단위: 회). 값을 지우려면 0을 씁니다.

사 내 참 고 부
-For Reference Only

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

서비스 코드(16진수)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
0E	Get_Attribute_Single	지정된 속성의 값을 읽습니다.	가능	가능
10	Set_Attribute_Single	지정된 속성의 값을 씁니다.	불가능	가능

AI 번역본
-For Reference Only-

A-4-8 Device Level Ring (DLR) Object (Class ID: 47 Hex)

Device Level Ring (DLR) 오브젝트는 DLR 네트워크의 상태를 나타냅니다.

Class ID 및 Instance ID

Class ID 및 Instance ID는 다음 표와 같습니다.

ID 유형	값(16진수)	설명
Class ID	47	
Instance ID	00	클래스 자체를 지정합니다.
	01	인스턴스를 지정합니다.

Attribute ID

Attribute ID는 읽을 정보를 지정합니다.

● Class Attribute ID

Class Attribute ID는 오브젝트 전체의 속성을 지정합니다.

Attribute ID	파라미터명	설명	속성	데이터	
				데이터형	값(16진수)
1	Revision	오브젝트의 리비전	읽기	UINT	0003
2	Max Instance	최대 인스턴스 수	읽기	UINT	0001
3	Number of Instance	인스턴스 수	읽기	UINT	0001

● Instance Attribute ID

Instance Attribute ID는 인스턴스의 Attribute ID를 지정합니다.

Attrib-ute ID	파라미터 명	설명	Attrib-ute	데이터	
				데이터형	값
1	Network Topolo-gy	현재 네트워크 토폴로지의 모드	읽기	USINT	0: 선형 1: 링 네트워크에 링 슈퍼바이저가 있으면 항상 1: 링을 나타냅니다. 네트워크에 링 슈퍼바이저가 없거나 설정된 링 파라미터가 현재 동작 중인 링 슈퍼바이저에서 지원되지 않으면 0: 선형이 되며, 이후 네트워크 상태에 따라 링과 선형 사이를 전환합니다.
2	Network Status	기기에서 본 네트워크의 현재 상태	읽기	USINT	아래 A-38페이지의 Network Status 값을 참조하십시오.
3-9	예약됨 41옥텟				

AI 번역본
-For Reference Only-

Attribute ID	파라미터 명	설명	Attribute	데이터	
				데이터형	값
10	Active Supervisor Address	액티브 링 슈퍼바이저의 IP 주소 및 MAC 주소	읽기	STRUCT	
	Supervisor IP Address	액티브 링 슈퍼바이저의 IP 주소		UDINT	액티브 링 슈퍼바이저의 IP 주소 기기의*1
	Supervisor MAC Address	액티브 링 슈퍼바이저의 MAC 주소		ARRAY OF 6 USINTs	기기의 액티브 링 슈퍼바이저 MAC 주소*1
12	Capability Flags	기기가 보유한 DLR 관련 기능	읽기	DWORD	00000082 hex로 고정 이는 링 기능이 비컨 프레임 방식이며 Flush_Table 프레임을 지원함을 의미합니다.

***1.** 기본값은 All0입니다. 액티브 링 슈퍼바이저가 결정되면 값이 해당 값으로 갱신됩니다.

● Network Status 값

값	이름	설명
0	정상	정상 상태
1	링 폴트	링 폴트가 감지되었습니다. 이는 네트워크 토폴로지가 링일 때만 유효합니다.
2	예기치 않은 루프 감지	네트워크에서 루프가 감지되었습니다. 이는 네트워크 토폴로지가 선형일 때만 유효합니다.

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

서비스 코드(16진수)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
01	Get_Attribute_All	모든 속성의 값을 읽습니다.	불가능	가능
0E	Get_Attribute_Single	지정된 속성의 값을 읽습니다.	가능	가능

AI 번역본
-For Reference Only-

A-4-9 QoS Object (Class ID: 48 Hex)

QoS 오브젝트는 이더넷 프레임 우선순위 제어에서 IPv4 DiffServ Code Point(DSCP) 값을 설정합니다.

Class ID 및 Instance ID

Class ID 및 Instance ID는 다음 표와 같습니다.

ID 유형	값(16진수)	설명
Class ID	48	
Instance ID	00	클래스 자체를 지정합니다.
	01	인스턴스를 지정합니다.

Attribute ID

Attribute ID는 읽을 정보를 지정합니다.

● Class Attribute ID

Class Attribute ID는 오브젝트 전체의 속성을 지정합니다.

Attribute ID	파라미터명	설명	속성	데이터	
				데이터형	값(16진수)
1	Revision	오브젝트의 리비전	읽기	UINT	0001
2	Max Instance	최대 인스턴스 수	읽기	UINT	0001
3	Number of Instance	인스턴스 수	읽기	UINT	0001

● Instance Attribute ID

Instance Attribute ID는 인스턴스의 Attribute ID를 지정합니다.

Attribute ID	파라미터명	설명	속성	데이터	
				데이터형	값
4	DSCP Urgent	CIP Transport Class 0/1 메시지의 우선순위가 Urgent로 설정된 경우의 DSCP 값	읽기/쓰기*1	USINT	CIP Transport Class 0/1 메시지의 우선순위가 Urgent로 설정된 경우의 DSCP 값입니다. 기본값은 55('110111')입니다.
5	DSCP Scheduled	CIP Transport Class 0/1 메시지의 우선순위가 Scheduled로 설정된 경우의 DSCP 값	읽기/쓰기*1	USINT	CIP Transport Class 0/1 메시지의 우선순위가 Scheduled로 설정된 경우의 DSCP 값입니다. 기본값은 47('101111')입니다.
6	DSCP High	CIP Transport Class 0/1 메시지의 우선순위가 High로 설정된 경우의 DSCP 값	읽기/쓰기*1	USINT	CIP Transport Class 0/1 메시지의 우선순위가 High로 설정된 경우의 DSCP 값입니다. 기본값은 43('101011')입니다.
7	DSCP Low	CIP Transport Class 0/1 메시지의 우선순위가 Low로 설정된 경우의 DSCP 값	읽기/쓰기*1	USINT	CIP Transport Class 0/1 메시지의 우선순위가 Low로 설정된 경우의 DSCP 값입니다. 기본값은 31('011111')입니다.

AI 번역본 -For Reference Only-

At-trib-ute ID	파라미터명	설명	속성	데이터	
				데이터형	값
8	DSCP Explicit	CIP Transport Class 0/1 메시지의 우선순위가 Explicit로 설정된 경우의 DSCP 값	읽기/ 쓰기*1	USINT	CIP Transport Class 0/1 메시지의 우선순위가 Explicit로 설정된 경우의 DSCP 값입니다. 기본값은 27('011011')입니다.

***1.** 이 설정은 재시작 후 유효합니다.

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

서비스 코드(16진수)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
0E	Get_Attribute_Single	지정된 속성의 값을 읽습니다.	가능	가능
10	Set_Attribute_Single	지정된 속성의 값을 씁니다.	불가능	가능

AI 번역본
-For Reference Only-

A-4-10 TCP/IP Interface Object (Class ID: F5 Hex)

TCP/IP Interface 오브젝트는 TCP/IP 인터페이스 설정을 구성하는 데 사용됩니다.

Class ID 및 Instance ID

Class ID 및 Instance ID는 다음 표와 같습니다.

ID 유형	값(16진수)	설명
Class ID	F5	
Instance ID	00	클래스 자체를 지정합니다.
	01	인스턴스를 지정합니다.

Attribute ID

Attribute ID는 읽을 정보를 지정합니다.

● Class Attribute ID

Class Attribute ID는 오브젝트 전체의 속성을 지정합니다.

Attribute ID	파라미터명	설명	속성	데이터	
				데이터형	값(16진수)
1	Revision	TCP/IP Interface 오브젝트가 지원하는 리비전	읽기	UINT	0004
2	Max Instance	최대 인스턴스 수	읽기	UINT	0001
3	Number of Instance	인스턴스 수	읽기	UINT	0001

● Instance Attribute ID

Instance Attribute ID는 인스턴스의 Attribute ID를 지정합니다.

Attribute ID	파라미터 명	설명	속성	데이터	
				데이터형	값
1	Status	TCP/IP 인터페이스의 상태	읽기	DWORD	아래 A-43페이지의 Status 값을 참조하십시오.
2	Configuration Capability	TCP/IP 인터페이스가 지원하는 다양한 기능의 비트맵	읽기	DWORD	아래 A-43페이지의 Configuration Capability 값을 참조하십시오.
3	Configuration Control	TCP/IP 인터페이스의 설정 결정 방법	읽기/쓰기	DWORD	아래 A-44페이지의 Configuration Control 값을 참조하십시오.

AI 번역 문 - For Reference Only -

Attribute ID	파라미터 명	설명	속성	데이터	
				데이터형	값
4	Physical Link Object	물리 계층 링크 오브젝트로의 경로	읽기	STRUCT	
	Path size	워드 단위 경로 크기		UINT	0000
	Path	물리 계층 링크 오브젝트로의 고정 경로		Padded EPATH	All0 hex
5	Interface Configuration*1	인터페이스 설정	읽기/쓰기	STRUCT	
	IP Address	IP 주소		UDINT	IP 주소 기본값은 192.168.250.1입니다. 다음 값은 설정할 수 없습니다. ・호스트 ID가 모두 0이거나 모두 1인 IP 주소 ・0, 127, 255로 시작하는 IP 주소 ・Class-D IP 주소(224.0.0.0~239.255.255.255) ・Class-E IP 주소(240.0.0.0~255.255.255.255) ・링크 로컬 주소(169.254.0.0~169.254.255.255)
	Network Mask	네트워크 마스크		UDINT	네트워크 마스크 기본값은 255.255.255.0입니다. 유효 조건은 다음과 같습니다. ・비트는 앞에서부터 연속되어야 합니다. ・192.0.0.0~255.255.255.252 범위 내여야 합니다.
	Gateway Address	기본 게이트웨이		UDINT	게이트웨이 주소 기본값은 0.0.0.0입니다(게이트웨이가 없음을 나타냄). 다음 값은 설정할 수 없습니다. ・IP Address의 설정 조건을 충족하지 않는 값 ・IP Address에 지정된 네트워크 주소와 다른 세그먼트의 IP 주소
	Name Server	DNS 서버의 1차 네임 서버		UDINT	항상 0.0.0.0입니다.
	Name Server 2	DNS 서버의 2차 네임 서버		UDINT	항상 0.0.0.0입니다.
	Domain Name	도메인 이름		STRING	도메인 이름 기본값은 ""(NULL)입니다.

AI 번역본
-For Reference Only-

At-trib-ute ID	파라미터 명	설명	속성	데이터	
				데이터형	값
6	Host Name	호스트 이름	읽기/ 쓰기	STRING	기기의 호스트 이름을 64자 이하의 ASCII 문자로 설정합니다. 64자 미만인 경우 나머지 문자 수만큼 패딩이 사용됩니다.
7	Safety Network Number	Safety Net-work Number (SNN)	읽기	6옥텟	Safety Network Number
13	Encapsulation In-activity Timeout	인캡슐레이션 비활성 타임아웃 시간	읽기/ 쓰기	UINT	0~3,600 Encapsulation Inactivity Timeout에 설정된 시간 동안 EtherNet/IP를 통한 통신이 없으면 TCP 연결이 닫힙니다. Encapsulation Inactivity Timeout = 0이면 TCP 연결이 닫히지 않습니다. 단위는 초입니다. 기본값은 120입니다.

***1.** IP 주소 설정 방법이 로터리 스위치에 의한 직접 설정인 경우, 이 속성에는 쓸 수 없습니다.

● Status 값

비트	이름	설명
0 to 3	Interface Con-figuration Sta-tus	Instance Attribute ID 05 hex(Interface Configuration)의 설정 상태 0: 미설정 또는 초기화 중 1: 하드웨어 스위치로 IP 주소를 직접 설정하는 방법 외의 방법으로 이미 설정됨 2: 하드웨어 스위치로 직접 설정하여 이미 설정됨 3~15: 예약됨
4	예약됨	항상 FALSE
5	Interface Con-figuration Pending	TRUE: Instance Attribute ID 05 hex(Interface Configuration)의 설정이 변경되었습니다. 변경 사항을 적용하려면 세이프티 I/O 블록을 재시작해야 합니다. FALSE: Instance Attribute ID 05 hex(Interface Configuration)의 설정이 변경되지 않았습니다.
6	AcdStatus	TRUE: IP 주소 중복이 감지되었습니다. 다만 이 IP 주소로 CIP 통신을 계속할 수 있습니다. FALSE: IP 주소 중복이 감지되지 않았습니다.
7	AcdFault	TRUE: 이 IP 주소로는 CIP 통신을 계속할 수 없습니다. FALSE: IP 주소 중복이 감지되지 않았습니다. 또는 IP 주소 중복이 감지되었더라도 이 IP 주소로 CIP 통신을 계속할 수 있습니다.
8~ 31	예약됨	항상 FALSE

● Configuration Capability 값

비트	이름	설명
0	BOOTP Client	항상 FALSE BOOTP 클라이언트 기능을 사용할 수 없습니다
1	DNS Client	항상 FALSE DNS 클라이언트 기능을 사용할 수 없습니다

참고용 번역본 -For Reference Only-

비트	이름	설명
2	DHCP Client	항상 TRUE DHCP 클라이언트 기능을 사용할 수 있습니다
3	DHCP-DNS Update	항상 FALSE DHCP-DNS Update 기능을 사용할 수 없습니다
4	Configuration Settable	항상 TRUE 인터페이스 설정 속성을 설정할 수 있습니다
5	Hardware Configuration	항상 TRUE 하드웨어에서 IP 주소를 설정할 수 있습니다
6	Interface Configuration Change Requires Reset	항상 TRUE 이 속성의 변경 사항을 적용하려면 기기를 재시작해야 합니다.
7	AcdCapable	항상 FALSE IP 주소 중복 감지 기능을 사용할 수 없습니다
8 to 31	예약됨	항상 FALSE

● Configuration Control 값

비트	이름	설명
0~3	Configuration Method	세이프티 I/O 블록의 IP 주소 설정 방법 0: 불휘발성 메모리에 저장된 설정을 사용합니다(기본값). 1: BOOTP 서버에 의해 IP 주소를 설정합니다. 2: DHCP 서버에 의해 IP 주소를 설정합니다. 3~15: 예약됨
4	DNS Enable	항상 FALSE DNS 클라이언트 기능을 사용할 수 없습니다
5 to 31	예약됨	항상 FALSE

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

서비스 코드(16진수)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
0E	Get_Attribute_Single	지정된 속성의 값을 읽습니다.	가능	가능
10	Set_Attribute_Single	지정된 속성의 값을 씁니다.	불가능	가능

AI 번역본
-For Reference Only-

A-4-11 Ethernet Link Object (Class ID: F6 Hex)

Ethernet Link 오브젝트는 이더넷 링크의 다양한 정보를 얻는 데 사용됩니다.

Class ID 및 Instance ID

Class ID 및 Instance ID는 다음 표와 같습니다.

ID 유형	값(16진수)	설명
Class ID	F6	
Instance ID	00	클래스 자체를 지정합니다.
	01~02	인스턴스를 지정합니다.

Attribute ID

Attribute ID는 읽을 정보를 지정합니다.

● Class Attribute ID

Class Attribute ID는 오브젝트 전체의 속성을 지정합니다.

Attribute ID	파라미터명	설명	속성	데이터	
				데이터형	값(16진수)
1	Revision	Ethernet Link 오브젝트가 지원하는 리비전	읽기	UINT	0004
2	Max Instance	최대 인스턴스 수	읽기	UINT	0002
3	Number of Instance	인스턴스 수	읽기	UINT	0002

● Instance Attribute ID

Instance Attribute ID는 인스턴스의 Attribute ID를 지정합니다.

Attribute ID	파라미터명	설명	속성	데이터	
				데이터형	값
1	Interface Speed	인터페이스 통신 속도	읽기	UDINT	000A hex: 10 Mbps 0064 hex: 100 Mbps
2	Interface Flags	인터페이스 상태	읽기	DWORD	아래 A-49페이지의 Interface Flags 값을 참조하십시오.
3	Physical Address	인터페이스 MAC 주소	읽기	ARRAY OF USINT*1	인터페이스 MAC 주소

AI 번역본 -For Reference Only-

Attribute ID	파라미터명	설명	속성	데이터	
				데이터형	값
4	Interface Counters	인터페이스 통신 통계 정보	읽기	STRUCT	
	In Octets	수신 데이터의 바이트 수		UDINT	수신 데이터의 바이트 수
	In Ucast Packets	수신된 유니캐스트 패킷 수		UDINT	수신된 유니캐스트 패킷 수
	In NUcast Packets	수신된 비유니캐스트 패킷 수		UDINT	수신된 비유니캐스트 패킷 수
	In Discards	폐기된 수신 패킷 수		UDINT	폐기된 수신 패킷 수
	In Errors	수신된 에러 패킷 수		UDINT	수신된 에러 패킷 수입니다. 단, In Discards에 해당하는 것은 제외합니다.
	In Unknown Protos	수신된 미지원 프로토콜 패킷 수		UDINT	수신된 미지원 프로토콜 패킷 수
	Out Octets	송신 데이터의 바이트 수		UDINT	송신 데이터의 바이트 수
	Out Ucast Packets	송신된 유니캐스트 패킷 수		UDINT	송신된 유니캐스트 패킷 수
	Out NUcast Packets	송신된 비유니 캐스트 패킷 수		UDINT	송신된 비유니 캐스트 패킷 수
	Out Discards	폐기된 송신 패킷 수		UDINT	폐기된 송신 패킷 수
	Out Errors	송신된 에러 패킷 수		UDINT	송신된 에러 패킷 수

AI 번역본
-For Reference Only-

Attribute ID	파라미터명	설명	속성	데이터	
				데이터형	값
5	Media Counters	인터페이스 미디어 통계 정보	읽기	STRUCT	
	Alignment Errors	수신된 얼라인먼트 에러 프레임 수		UDINT	수신된 얼라인먼트 에러 프레임 수
	FCS Errors	FCS 에러를 수신한 횟수		UDINT	FCS 에러를 수신한 횟수
	Single Collisions	충돌이 감지된 상태에서 정상적으로 송신에 성공한 프레임 수		UDINT	충돌이 감지된 상태에서 정상적으로 송신에 성공한 프레임 수
	Multiple Collisions	두 번 이상의 충돌이 감지된 상태에서 정상적으로 송신에 성공한 프레임 수		UDINT	두 번 이상의 충돌이 감지된 상태에서 정상적으로 송신에 성공한 프레임 수
	SQE Test Errors	SQE 테스트 에러 발생 횟수		UDINT	SQE 테스트 에러 발생 횟수
	Deferred Transmissions	송신이 지연된 프레임 수		UDINT	송신이 지연된 프레임 수
	Late Collisions	패킷 송신 후 512비트 시간 내에 충돌이 감지된 횟수		UDINT	패킷 송신 후 512비트 시간 내에 충돌이 감지된 횟수
	Excessive Collisions	과도한 충돌로 인해 송신에 실패한 프레임 수		UDINT	과도한 충돌로 인해 송신에 실패한 프레임 수
	MAC Transmit Errors	MAC 계층 송신 에러로 인해 송신에 실패한 프레임 수		UDINT	MAC 계층 송신 에러로 인해 송신에 실패한 프레임 수
	Carrier Sense Errors	캐리어 센서 에러가 감지된 횟수		UDINT	캐리어 센서 에러가 감지된 횟수
	Frame Too Long	최대 프레임 크기를 초과한 프레임 수		UDINT	최대 프레임 크기를 초과한 프레임 수
	MAC Receive Errors	MAC 계층 수신 에러로 인해 수신에 실패한 프레임 수		UDINT	MAC 계층 수신 에러로 인해 수신에 실패한 프레임 수
6	Interface Control	인터페이스 설정	읽기/쓰기*2	STRUCT	
	Control Bits	통신 속도를 결정하는 방법		WORD	아래 A-49페이지의 Control Bits 값을 참조하십시오. 기본값은 0001 hex입니다.
	Forced Interface Speed	Auto-Negotiation이 비활성화된 경우의 통신 속도		UINT	0064 hex: 100 Mbps 기본값은 0000 hex입니다. ***3*4**
7	Interface Type	이 인스턴스의 물리 인터페이스 유형	읽기	USINT	02 hex: Twisted Pair로 고정

AI 번역본
-For Reference Only-

Attribute ID	파라미터명	설명	속성	데이터	
				데이터형	값
8	Interface State	인터페이스 상태	읽기	USINT	00 hex: 상태 불명 01 hex: 송수신 준비 완료 02 hex: 비활성화 03 hex: 테스트 중 04~FF hex: 예약됨
10	Interface Label	인터페이스 식별 텍스트 문자열	읽기	SHORT STRING	Instance 1: "Ethernet Port 1"로 고정 Instance 2: "Ethernet Port 2"로 고정
11	Interface Capability	인터페이스 통신 성능	읽기	STRUCT	-
	Capability Bits	통신 성능 설정		DWORD	아래 A-49페이지의 Capability Bits 값을 참조하십시오.
	Speed/Duplex Options	인터페이스가 허용하는 통신 속도와 듀플렉스 모드의 조합		STRUCT	
	Speed/Duplex Array Count	통신 속도/양방향 배열 크기		USINT	항상 2
	Speed/Duplex Array	통신 속도/양방향 배열		ARRAY OF STRUCT	
	Interface Speed	인터페이스 통신 속도		UINT	0064 hex: 100 Mbps
	Interface Duplex Mode	인터페이스 양방향 모드		USINT	00 hex: Half Duplex
	Speed/Duplex Array	통신 속도/양방향 배열		ARRAY OF STRUCT	
	Interface Speed	인터페이스 통신 속도		UINT	0064 hex: 100 Mbps
	Interface Duplex Mode	인터페이스 양방향 모드		USINT	01 hex: Full Duplex
14	Ethernet Errors	인터페이스 카운터, 미디어 카운터, HC 미디어 카운터의 합계	읽기	UDINT	인터페이스 카운터, 미디어 카운터, HC 미디어 카운터의 합계입니다. 기본값은 0입니다.
15	Link Down Counter	이더넷 포트가 링크 업 상태에서 링크 다운 상태로 전환된 횟수	읽기	UDINT	이더넷 포트가 링크 업 상태에서 링크 다운 상태로 전환된 횟수입니다. 기본값은 0입니다.
100	Communication Cable Diagnosis	통신 케이블 진단 결과	읽기	UINT	아래 A-50페이지의 Communication Cable Diagnosis 값을 참조하십시오.

AI 번역본
-For Reference Only-

***1.** 배열 크기는 6입니다.

***2.** 이 설정은 재시작 후 유효합니다.

***3.** 다음의 경우 09 hex(Invalid Attribute Value) 에러가 발생합니다.
- Control Bits의 비트 2~15(예약 비트) 중 하나라도 TRUE인 경우.
- Control Bits의 비트 0(Auto-negotiate)이 FALSE이고 비트 1(Forced Duplex Mode)이 TRUE인 상태에서 Forced Interface Speed의 설정 범위를 벗어난 값을 설정하려고 한 경우.

***4.** 다음의 경우 0C hex(Object State Conflict) 에러가 발생합니다.
- Control Bits의 비트 0(Auto-negotiate)이 TRUE이고 비트 1(Forced Duplex Mode)이 FALSE인 상태에서 Forced Interface Speed에 어떤 값을 설정하려고 한 경우.

● Interface Flags 값

비트	이름	설명
0	Link Status	TRUE: 이더넷 링크가 확립되어 있습니다. FALSE: 이더넷 링크가 확립되어 있지 않습니다.
1	Half/Full Duplex*1	TRUE: Full Duplex FALSE: Half Duplex
2~4	Negotiation Status	0: Auto-negotiation 실행 중입니다. 1: Auto-negotiation에 실패했습니다. 통신 속도 10 Mbps에서 Half Duplex로 동작합니다. 2: Auto-negotiation에 실패했습니다. 설정된 통신 속도에서 Half Duplex로 동작합니다. 3: Auto-negotiation에 성공했습니다. 4: Auto-negotiation이 비활성화되어 있습니다.
5	Manual Setting Requires Reset	TRUE: Interface Control Attribute가 변경된 후 기기 재설정이 필요합니다. FALSE: Interface Control Attribute가 변경된 후 기기 재설정이 필요하지 않습니다.
6	Local Hardware Fault	TRUE: 하드웨어 폴트 FALSE: 하드웨어 폴트 없음
7 to 31	예약됨	항상 FALSE

***1.** Link Status = 0인 경우에는 의미가 없습니다.

● Control Bits 값

비트	이름	설명
0	Auto-negotiate	TRUE: Auto-negotiate가 활성화되어 있습니다. FALSE: Auto-negotiate가 비활성화되어 있습니다. Forced Duplex Mode 및 Forced Interface Speed의 설정에 따라 동작합니다.
1	Forced Duplex Mode	TRUE: Full Duplex FALSE: Half Duplex 이 비트는 Auto-negotiate가 FALSE일 때 사용됩니다. Auto-negotiate가 TRUE일 때 이 비트를 설정하면 에러 코드 0C hex(Object State Conflict)가 반환됩니다.
2-15	예약됨	항상 FALSE

AI 번역부
-For Reference Only-

● Capability Bits 값

비트	이름	설명
0	Manual Setting Requires Reset	항상 TRUE: Interface Control Attribute가 변경된 후 기기 재설정이 필요함을 나타냅니다.
1	Auto-negotiate	항상 TRUE: Auto-negotiation을 지원합니다.
2	Auto-MDIX	항상 TRUE: Auto-MDIX를 지원합니다.
3	Manual Speed/Duplex	항상 TRUE: 수동 속도/듀플렉스 설정을 지원합니다.
4 to 31	예약됨	항상 FALSE

● Communication Cable Diagnosis 값

비트	설명
0~7	포트로부터의 에러 발생 위치 단위: m 진단 결과 에러인 경우 0
8~15	00 hex: 미실행 01 hex: 정상 02 hex: 단락 03 hex: 단선 04 hex: 포트 비활성화 F1 hex: 진단 중 F2 hex: 진단 결과 에러 F3 hex: PHY 읽기 에러

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

서비스 코드 (hex)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
0E	Get_Attribute_Single	지정한 어트리뷰트의 값을 읽습니다.	가능	가능
10	Set_Attribute_Single	지정한 어트리뷰트의 값을 씁니다.	불가능	가능
3A	Exec_Cable_Diagnosis	통신 케이블 진단을 실행합니다.*1	불가능	가능
4C	Get_and_Clear	지정한 어트리뷰트 값을 읽은 후 지 **웁니다.*2*3**	불가능	가능

***1.** 이 서비스가 이미 링크가 확립되어 있는 통신 포트의 인스턴스에서 실행되면 통신 케이블 진단은 실행되지 않으며 항상 이상 없음으로 처리됩니다. 또한 이 서비스가 통신 케이블 진단이 진행 중인 통신 포트의 인스턴스에서 실행되면 0C hex(Object State Conflict) 에러가 발생합니다.

***2.** 이 서비스는 다음 인스턴스 어트리뷰트에서 지원됩니다.

- Interface Counters (04)
- Media Counters (05)
- Link_Down Counter (15)

위 이외의 어트리뷰트가 지정된 경우, 응답 코드로 09 hex(잘못된 어트리뷰트 값)가 반환됩니다.

***3.** 다음 조합에서는 그중 하나에 대해 이 서비스를 실행하면 그중 하나에 대해서만 값이 읽히고, 둘 다 리셋됩니다.

- Interface Counters (04 hex) and HC Interface Counters (12 hex)
- Media Counters (05 hex) and HC Media Counters (13 hex)

AI 번역 버전
For Reference Only-

A-4-12 LLDP 매니지먼트 오브젝트 (Class ID: 109 Hex)

LLDP 매니지먼트 오브젝트는 LLDP 기능을 관리하는 데 사용됩니다.

클래스 ID 및 인스턴스 ID

클래스 ID 및 인스턴스 ID는 다음 표와 같습니다.

ID 종류	값 (hex)	설명
클래스 ID	109	
인스턴스 ID	00	클래스 자체를 지정합니다.
	01	인스턴스를 지정합니다.

어트리뷰트 ID

어트리뷰트 ID는 읽을 정보를 지정합니다.

● 클래스 어트리뷰트 ID

클래스 어트리뷰트 ID는 오브젝트 전체의 어트리뷰트를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값 (hex)
1	Revision	오브젝트의 리비전	읽기	UINT	0001
2	Max Instance	최대 인스턴스 번호	읽기	UINT	0001
3	Number of Instance	인스턴스 수	읽기	UINT	0001

● 인스턴스 어트리뷰트 ID

인스턴스 어트리뷰트 ID는 인스턴스의 어트리뷰트 ID를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
1	LLDP Enable	LLDP 활성화	읽기/쓰기	STRUCT	
	LLDP Enable Array 길이	LLDP Enable Array에 설정할 포트 수		UINT	LLDP 기능 전체의 설정도 포함하므로 이 값은 EthernetLink 오브젝트 인스턴스 + 1이 됩니다. 항상 3
	LLDP Enable Array	LLDP 기능 전체 또는 각 포트의 LLDP 활성화/비활성화 설정		ARRAY OF BYTE	아래 A-52페이지의 LLDP Enable Array의 값을 참조하십시오.
2	msgTxInterval	LLDP 프레임의 송신 간격	읽기/쓰기	UINT	LLDP 프레임의 송신 간격 1~3,600 단위는 초입니다. 기본값은 30입니다.

AI 번역본
-For Reference Only

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
3	msgTxHold	LLDP 프레임 TTL 값을 결정하기 위한 배수	읽기/쓰기	USINT	1~100 TTL 값은 msgTxInterval × msgTxHold로 구해집니다. 기본값은 4입니다. 따라서 TTL 값의 기본값은 30 × 4 = 120초 입니다. msgTxInterval × msgTxHold의 결과가 65,535를 초과하면 TTL 값은 65,535초가 됩니다.
4	LLDP Datastore	LLDP 데이터베이스를 취득하는 방법	읽기	WORD	1로 고정: SNMP로 취득
5	Last Change	로컬 LLDP 데이터베이스의 어떤 항목이 마지막으로 변경되었을 때 취득되는 sysUpTime의 값	읽기	UDINT	로컬 LLDP 데이터베이스의 항목이 마지막으로 변경되었을 때 취득된 sysUpTime 값 sysUpTime은 시스템의 네트워크 관리 부분이 마지막으로 초기화된 이후 경과 시간을 나타냅니다. 단위는 0.01초입니다.

● LLDP Enable Array의 값

비트	이름	설명
0	Global Enable	TRUE: LLDP 송수신이 활성화됩니다(기본값). FALSE: LLDP 송수신이 비활성화됩니다. 값을 TRUE에서 FALSE로 변경하면 기존 테이블 항목이 모두 삭제됩니다.
1	Port 1 Enable	TRUE: 포트 1에서 LLDP 송신이 활성화됩니다(기본값). FALSE: 포트 1에서 LLDP 송신이 비활성화됩니다.
2	Port 2 Enable	TRUE: 포트 2에서 LLDP 송신이 활성화됩니다(기본값). FALSE: 포트 2에서 LLDP 송신이 비활성화됩니다.
3~7	Reserved	항상 FALSE

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

서비스 코드 (hex)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
0E	Get_Attribute_Single	지정한 어트리뷰트의 값을 읽습니다.	가능	가능
10	Set_Attribute_Single	지정한 어트리뷰트의 값을 씁니다.	불가능	가능

AI 번역본

A-4-13 LLDP 데이터 테이블 오브젝트 (Class ID: 10A Hex)

LLDP 데이터 테이블 오브젝트는 LLDP 기능의 데이터를 관리하는 데 사용됩니다.

클래스 ID 및 인스턴스 ID

클래스 ID 및 인스턴스 ID는 다음 표와 같습니다.

ID 종류	값 (hex)	설명
클래스 ID	10A	
인스턴스 ID	00	클래스 자체를 지정합니다.
	01-30	인스턴스를 지정합니다.

어트리뷰트 ID

어트리뷰트 ID는 읽을 정보를 지정합니다.

● 클래스 어트리뷰트 ID

클래스 어트리뷰트 ID는 오브젝트 전체의 어트리뷰트를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값 (hex)
1	Revision	오브젝트의 리비전	읽기	UINT	0001
2	Max Instance	현재 생성되어 있는 인스턴스 ID의 최댓값	읽기	UINT	0000-0030
3	Number of Instance	현재 생성되어 있는 인스턴스 수	읽기	UINT	0000-0030

● 인스턴스 어트리뷰트 ID

인스턴스 어트리뷰트 ID는 인스턴스의 어트리뷰트 ID를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
1	Ethernet Link Instance Number	LLDP 프레임을 수신한 이더넷 포트와 링크되는 Ethernet Link 오브젝트(F6 hex)의 인스턴스 번호	읽기	UINT	LLDP 프레임을 수신한 이더넷 포트와 링크되는 Ethernet Link 오브젝트(F6 hex)의 인스턴스 번호 알 수 없는 경우 0입니다.

사본 역본
-For Reference Only-

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
2	MAC Address	수신한 LLDP 프레임을 송신한 인접 기기의 MAC 주소	읽기	ETH_MAC_ADDR	저장되는 값은 다음 우선순위에 따라 결정됩니다. Priority 1: TLV Type = 127, Subtype = 2인 경우, CIP MAC 주소 Priority 2: TLV Type = 1, Subtype = 4인 경우, Chassis ID Priority 3: TLV Type = 2, Subtype = 3인 경우, Port ID Priority 4: 모두 0
3	Interface Label	수신한 LLDP 프레임을 송신한 인접 기기의 인터페이스 레이블	읽기	SHORT STRING	저장되는 값은 다음 우선순위에 따라 결정됩니다. Priority 1: TLV Type = 127, Subtype = 3인 경우, CIP Interface Label Priority 2: TLV Type = 1, Subtype = 6인 경우, Chassis ID Priority 3: TLV Type = 2, Subtype = 5인 경우, Port ID Priority 4: Null
4	Time to Live	인접 기기의 정보가 유효한 시간	읽기	UINT	인접 기기의 정보가 유효한 시간입니다. 단위는 초입니다. Time to Live = 0인 경우, 이 인스턴스를 삭제해야 함을 의미합니다.
5	System Capabilities TLV	인접 기기가 지원하는 기능	읽기	STRUCT	
	System Capabilities	인접 기기가 지원할 수 있는 기능		WORD	아래 A-56페이지의 System Capabilities and Enabled Capabilities의 값을 참조하십시오.
	Enabled Capabilities	인접 기기에서 현재 활성화된 기능		WORD	아래 A-56페이지의 System Capabilities and Enabled Capabilities의 값을 참조하십시오.

AI 번역본
-For Reference Only-

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
6	IPv4 Management Addresses	인접 기기의 매니지먼트 주소	읽기	STRUCT	
	Management Address Count	저장할 매니지먼트 주소 수		USINT	저장할 매니지먼트 주소 수 최대 255
	Management Address	매니지먼트 주소의 값		ARRAY OF UDINT	매니지먼트 주소의 값 Class A, B, C인 경우 유효합니다. 이 값은 모두 0이거나 루프백 주소인 경우에는 저장되지 않습니다.
7	CIP Identification	인접 기기의 CIP Identity	읽기	STRUCT	
	Vendor ID	벤더 ID		UINT	벤더 ID 수신한 LLDP 프레임에 해당하는 TLV가 포함되어 있지 않으면 값은 0입니다.
	Device Type	기기 타입		UINT	기기 타입 수신한 LLDP 프레임에 해당하는 TLV가 포함되어 있지 않으면 값은 0입니다.
	Product Code	제품 코드		UINT	제품 코드 수신한 LLDP 프레임에 해당하는 TLV가 포함되어 있지 않으면 값은 0입니다.
	Major Revision	메이저 리비전		BYTE	메이저 리비전 수신한 LLDP 프레임에 해당하는 TLV가 포함되어 있지 않으면 값은 0입니다.
	Minor Revision	마이너 리비전		USINT	마이너 리비전 수신한 LLDP 프레임에 해당하는 TLV가 포함되어 있지 않으면 값은 0입니다.
	CIP Serial Number	CIP 시리얼 번호		UDINT	CIP 시리얼 번호 수신한 LLDP 프레임에 해당하는 TLV가 포함되어 있지 않으면 값은 0입니다.

AI 번역본
-For Reference Only-

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
8	Additional Ethernet Capabilities	이더넷 프리엠션 기능 상태	읽기	STRUCT	
	Preemption Support	인접 노드의 Preemption (TSN 기능) 지원 상태		BOOL	TRUE: 지원 FALSE: 미지원
	Preemption Status	인접 노드의 Preemption (TSN 기능) 활성화/ 비활성화		BOOL	TRUE: 활성화 FALSE: 비활성화
	Preemption Active	인접 노드의 Preemption (TSN function)이 활성 상태인지 여부		BOOL	TRUE: 활성 FALSE: 비활성
	Additional Fragment Size	인접 노드의 Preemption (TSN 기능)이 발생하기 전에 하나의 프레임에서 송신해야 하는 옥텟 수		USINT	0: 64옥텟 1: 128옥텟 2: 192옥텟 3: 256옥텟 4~255: Reserved
9	Last Change	이 인스턴스가 마지막으로 변경되었을 때 취득된 sysUpTime 값	읽기	UDINT	이 인스턴스가 마지막으로 변경되었을 때 취득된 sysUpTime 값 sysUpTime은 시스템의 네트워크 관리 부분이 마지막으로 초기화된 이후 경과 시간을 나타냅니다. 단위는 0.01초입니다.

● System Capabilities and Enabled Capabilities의 값

비트	설명
0	Other
1	Repeater
2	Bridge
3	Access Point
4	Router
5	Telephone
6	DOCSIS Cable Device
7	End Station
8	C-VLAN component
9	S-VLAN component
10	Two-port MAC Relay Component
11~15	Reserved

AI 번역본
-For Reference Only-

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

서비스 코드 (hex)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
0E	Get_Attribute_Single	지정한 어트리뷰트의 값을 읽습니다.	가능	가능
11	Find_Next_Object_Instance	다음 오브젝트를 검색합니다.	가능	가능

Find_Next_Object_Instance (Service Code: 11 Hex)

다음 오브젝트를 검색합니다. 요청 형식 및 응답 형식은 다음과 같습니다.

● 요청 형식

파라미터명	설명	데이터형	값
Service	서비스 코드	USINT	11 hex
Maximum Returned Values	Instance ID List 내 인스턴스 ID 멤버의 최대 수	USINT	

● 응답 형식

파라미터명	설명	데이터형	값
Reply Service	Find_Next_Object_Instance 서비스에 대한 응답	USINT	91 hex
Number Of List Members	멤버 수	USINT	
Instance ID List	인스턴스 ID 목록	ARRAY OF UINT	

AI 번역본
-For Reference Only-

A-4-14 로직 프로세스 오브젝트 (Class ID: 309 Hex)

로직 프로세스 오브젝트는 동작 중인 애플리케이션의 번호를 읽는 데 사용됩니다.

클래스 ID 및 인스턴스 ID

클래스 ID 및 인스턴스 ID는 다음 표와 같습니다.

ID 종류	값 (hex)	설명
클래스 ID	309	
인스턴스 ID	00	클래스 자체를 지정합니다.
	01	인스턴스를 지정합니다.

어트리뷰트 ID

어트리뷰트 ID는 읽을 정보를 지정합니다.

● 클래스 어트리뷰트 ID

클래스 어트리뷰트 ID는 오브젝트 전체의 어트리뷰트를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값 (hex)
1	Revision	오브젝트의 리비전	읽기	UINT	0001

● 인스턴스 어트리뷰트 ID

인스턴스 어트리뷰트 ID는 인스턴스의 어트리뷰트 ID를 지정합니다.

어트리뷰트 ID	파라미터명	설명	어트리뷰트	데이터	
				데이터형	값
101	Application Number	애플리케이션 번호	읽기	USINT	아래 A-58페이지의 Application Number의 값을 참조하십시오.

● Application Number의 값

값	설명
0	리모트 I/O 모드 애플리케이션
1	고정 애플리케이션 1 부분 정지 + 전체 정지 애플리케이션
2	고정 애플리케이션 2 부분 정지 + 전체 정지 애플리케이션 (EDM 포함)
3	고정 애플리케이션 3 작업자 및 로봇 자동 전환 애플리케이션
4~7	Reserved
8	Reserved
9~13	애드온 애플리케이션 1~5
14	Reserved
15	사용자 정의 애플리케이션

로터리 스위치의 값이 유효하지 않거나 읽기에 실패한 경우, 잠금 상태이면 잠겼을 때의 값이 반환됩니다.
잠금 해제 상태이면 FF hex가 반환됩니다.

AI 번역본
-For Reference Only-

서비스 코드

서비스 코드는 실행할 서비스를 지정합니다.

서비스 코드 (hex)	파라미터명	설명	지원 서비스 범위	
			클래스	인스턴스
0E	Get_Attribute_Single	지정한 어트리뷰트의 값을 읽습니다.	가능	가능
10	Set_Attribute_Single	지정한 어트리뷰트의 값을 씁니다.	불가능	가능

AI 번역본
-For Reference Only-

A-5 적합성 선언

No. EUSP0001A

Original

OMRON

EU DECLARATION OF CONFORMITY

1. **Product Models/Products:**
   NXR-S series
2. **Name and address of the manufacturer:**
   OMRON Corporation
   Shiokoji Horikawa, Shimogyo-Ku, Kyoto, 600-8530 Japan
3. **This declaration of conformity is issued under the sole responsibility of the manufacturer.**
4. **Objects of the declaration:**
   NXR-S series, Remote Terminal
5. **The objects of the declaration described above are in conformity with the relevant Union harmonisation legislation:**
   2014/30/EU EMC Directive
   2006/42/EC Machinery Directive
   2011/65/EU RoHS Directive
6. **References to the relevant harmonised standards used or references to the other technical specifications in relation to which conformity is declared:**
   EMC Directive: EN 61131-2: 2007
   Machinery Directive: EN ISO 13849-1:2023
   RoHS Directive: EN IEC 63000: 2018
7. **Name, address, and identification number of Notified Body, Number of EC Type Examination**
   Notified body: TÜV Rheinland Industrie Service GmbH
   Address: Am Grauen Stein, 51105 Köln / Germany
   Notified Body identification No.: 0035
   Certificate for EU Type Examination: 01/205/6092.00/26

AI 번역본
-For Reference Only-

Signed and on behalf of: OMRON Corporation
Place and date of issue: Kyoto, Japan 13th Jul, 2026

Signature:
Name: Kozo Kando
Function: Senior General Manager, Controller Division, Industrial Automation Company

1/3
GQ-151845A1

No. EUSP0001A

Name and address of contact in EU

OMRON Europe B.V.
Quality & Environment Department
Attn: J.J.P.W. Vogelaar, European Quality & Environment Manager
Zilverenberg 2, 5234 GM, 's-Hertogenbosch, The Netherlands

AI 번역본
-For Reference Only-

2/3
GQ-151845A1

No. EUSP0001A

Additional information

Models List

Model	Type	EMI	EMS	RoHS	Rev
		EN61131-2	EN61131-2	EN IEC 63000	
NXR-SXD1204-CST	Safety I/O Block	2007	2007 zone B	2018	<A>
NXR-SXD1204B-CST	Safety I/O Block	2007	2007 zone B	2018	<A>
NXR-SXD1204-EIT	Safety I/O Block	2007	2007 zone B	2018	<A>

Model name may be followed by additional letter (s) and /or number (s) for sale purposes.

AI 번역본
-For Reference Only-

3/3
GQ-151845A1

I

색인

AI 번역본
-For Reference Only-

색인

A

자동 시각 조정.....7-91

B

백업.....7-108

C

다이렉트 전원 공급의 총 소비전류 계산.....4-7
스루 배선을 사용하는 전원 공급의 총 강하 계산.....4-14
다이렉트 전원 공급의 전압 강하 계산.....4-11
스루 배선을 사용하는 전원 공급의 전압 넥터).....4-17
초기 세이프티 패스워드 변경.....7-24
운전 모드 변경.....7-95
전체 메모리 클리어 기능.....8-4
통신 케이블 연결 절차 (나사식 커 커넥터).....5-8
통신 케이블 연결 절차 (Smartclick 터).....5-7
통신 케이블 진단 기능.....8-31
통신 케이블 분리 절차 (나사식 커넥 터).....5-10
통신 케이블 분리 절차 (Smartclick 커넥 넥터).....5-7
통신 커넥터.....3-11
컨피규레이션 잠금.....7-99
접점 동작 횟수 모니터 기능.....8-29
커버 장착 구멍.....3-3, 3-4
사이클릭 통신.....6-6

D

Device Level Ring (DLR) 기능.....8-10
다이렉트 전원 공급.....4-3

E

EtherNet/IP 통신 커넥터 1.....3-2, 3-4
EtherNet/IP 통신 커넥터 2.....3-2, 3-4
이벤트.....11-2
이벤트 로그 기능.....11-6
EX PWR OUT 표시등.....3-7
Expected Packet Interval (EPI).....7-33
익스포트.....7-36

F

펌웨어 업데이트 기능.....8-35

H

HTTPS 통신 기능.....8-8

I

I/O 케이블 연결 절차 (나사식 커넥터).....5-21
I/O 케이블 연결 절차 (Smartclick 커넥터).....5-19
I/O 케이블 분리 절차 (나사식 커넥터).....5-23
I/O 케이블 분리 절차 (Smartclick 커넥터).....5-20
I/O 커넥터.....3-2, 3-4
I/O 식별 마커.....3-3, 3-4
I/O 표시등.....3-3, 3-4
I/O 모니터 기능.....8-27
I/O 배선 체크 기능.....8-13
임플리시트 통신.....6-6
임포트.....7-37
점검 항목.....12-3
로터리 스위치 커버 설치.....5-3
유닛 설치.....5-3
IP 주소 표시 기능.....8-19

L

L/A ETH1 표시등.....3-6
L/A ETH2 표시등.....3-7
라인.....1-13
LLDP 기능.....7-42
Lock 표시등.....3-7
로그인.....7-22
로그아웃.....7-24
로트 번호.....32

M

M12 부착.....5-8, 5-21
M12 토크 핸들.....5-8, 5-21
MAC 주소 MS.....32
표시등.....3-6

N

NS 표시등.....3-6

O

오픈 타입.....6-4
운전 상태 모니터 기능.....11-3
OUT PWR 표시등.....3-5
출력 전원 공급.....4-2

P

핀 배열.....3-11, 3-12
포트.....3-12
스루 배선 출력 전원 OFF 기능.....8-11
전원 공급 케이블 연결 절차.....5-16
전원 공급 케이블 분리 절차.....5-17
전원 공급 용량.....4-21
전원 공급 커넥터(입력).....3-3, 3-4

AI 번역본
-For Reference Only-

전원 공급 커넥터(입력)..... 3-12
전원 공급 커넥터(출력)..... 3-3, 3-4
전원 공급 커넥터(출력)..... 3-12
전원 공급 모니터 기능..... 8-22
사용 전원 공급..... 4-21
스루 배선을 사용하는 전원 공급..... 4-3
Production Information 화면 33

R

재기동..... 7-84
링..... 1-14
로터리 스위치..... 3-3, 3-4

S

세이프티 I/O 포트..... 3-13
세이프티 입력 표시등..... 3-8
세이프티 입력 포트..... 3-12
세이프티 출력 표시등..... 3-8
세이프티 출력 포트..... 3-13
세이프티 패스워드.....7-104
세이프티 반응 시간.....9-2
세이프티 응답 성능.....9-2
제너럴 CIP 커맨드 전송 기능..... 8-15
태그 데이터 링크 통신 설정 절차.....7-38
스타.....1-13
상태 표시등..... 3-3, 3-4

T

태그 데이터 링크..... 6-6
조임 공구.....5-8, 5-12, 5-21
조임 토크.....5-11, 5-12, 5-24
점검에 필요한 공구..... 12-2
출력 전원 공급으로부터의 총 소비전류.....4-7
유닛/입력 전원 공급으로부터의 총 소비전류..... 4-7
트리.....1-13

U

U/IN PWR 표시등..... 3-5
유닛 식별 기능.....8-16
유닛 식별 표시등.....3-3, 3-4
유닛 식별 마커..... 3-3, 3-4
유닛 장착 구멍..... 3-3, 3-4
백업 기능을 사용한 유닛 교체..... 12-4
백업 기능을 사용하지 않는 유닛 교체..... 12-5
유닛/입력 전원 공급..... 4-2

AI 번역본
-For Reference Only-

AI 번역본
-For Reference Only-

AI 번역본
-For Reference Only-

⚠ 안내 (For Reference Only)

본 문서는 AI 번역으로 작성된 참고용 국문자료 입니다.
일부 표현은 원문과 다소 다를 수 있으며,
중요한 내용은 원문과 함께 참고해 주시기 바랍니다.

한국오므론제어기기주식회사 https://www.ia.omron.co.kr/

서울특별시 서초구 강남대로 465, B동 18층(서초동, 교보타워)
TEL: 1522-8994 FAX: 02-3483-7788

Authorized Distributor:

©OMRON Corporation 2026 All Rights Reserved.
In the interest of product improvement,
specifications are subject to change without notice.

Cat. No. W645-E1-02 0726