# 14. 고급 주제 및 최신 기술

## 14.1 PLC와 IIoT (산업용 사물인터넷) 연동

*(PLC 시스템을 산업용 사물인터넷(IIoT) 플랫폼으로 확장하는 통합 설계 전략)*

---

### ✅ 개요

**PLC와 IIoT 연동**은 이제 단순 제어를 넘어
데이터 기반 운영, 공정 최적화, 원격 모니터링, 예측정비, AI 분석 등
스마트팩토리 핵심 기술로 확장되고 있다.

IIoT는 PLC에서 수집한 데이터를 실시간으로 상위 IT 시스템, 클라우드, 분석 플랫폼으로 전달하고
상시 모니터링, 원격 제어, 고급 분석을 가능하게 한다.

---

### ✅ 1. IIoT 연동 구조 개념

```
[ 센서 / 장비 ]
    ↓ (제어 및 수집)
[ PLC 제어 시스템 ]
    ↓ (데이터 수집)
[ 게이트웨이 / OPC UA / MQTT 브로커 ]
    ↓ (데이터 전송)
[ IIoT 플랫폼 / 클라우드 / MES / AI 분석 ]
```

- **PLC는 IIoT에서 현장 실시간 데이터 수집·제어 중심 역할**
- **IIoT 플랫폼은 데이터 저장·분석·예측 중심 역할**

---

### ✅ 2. PLC-기반 IIoT 확장 방식

| 유형 | 설명 |
|---|---|
| 직접 연결형 | PLC 자체가 OPC UA, MQTT, REST API 지원 |
| 게이트웨이 중계형 | PLC는 기존제어 유지, IIoT 게이트웨이 장치 통해 상위 연결 |
| 통합 SCADA 중계형 | SCADA 시스템이 IIoT 브로커 역할 병행 |

---

### ✅ 3. 주요 표준 통신 프로토콜

| 프로토콜 | 특징 |
|---|---|
| **OPC UA** | 산업용 표준 IIoT 통신 프로토콜 (보안·실시간성 지원) |
| **MQTT** | 경량 메시지 기반 실시간 퍼블리시/서브스크라이브 |

| 프로토콜 | 특징 |
|---|---|
| **REST API** | 웹 기반 상호 통신 |
| **Modbus TCP** | 단순 이더넷 기반 저비용 연동 |
| **AMQP, CoAP** | 일부 고급 IoT 환경에서 추가 지원 |

---

## ✅ 4. 제조사별 IIoT 내장지원 여부

| 제조사 | 기본 지원 수준 |
|---|---|
| Siemens | OPC UA, MQTT, REST (S7-1500 내장) |
| Rockwell | FactoryTalk Edge Gateway, OPC UA, MQTT 지원 |
| Mitsubishi | iQ-R OPC UA 내장, MES Interface 제공 |
| LS | XGR 일부 OPC UA 확장 가능 |
| Omron | Sysmac OPC UA, MQTT 기본 지원 |
| Keyence | 최신 KV-8000 MQTT 확장 가능 |
| Delta | MQTT 일부 최신 시리즈 확장 지원 |
| Panasonic | 일부 FP7 모델 MQTT, OPC UA 지원 |

---

## ✅ 5. IIoT 연동 실전 아키텍처 예시

### 📌 (1) OPC UA 기반 통합

```
PLC → OPC UA Server → IIoT 플랫폼 (Cloud / MES / Historian)
```

### 📌 (2) MQTT 기반 경량 메시지 통합

```
PLC → MQTT Broker (Local Edge Gateway) → Cloud AI Analytics
```

- MQTT는 **저지연·저대역폭·비동기 전송에 최적화**

---

## ✅ 6. IIoT 연동시 주요 실전 활용 분야

| 활용분야 | 예시 |
|---|---|
| 원격 모니터링 | 장비 상태 실시간 가시화 |
| 생산지시 최적화 | MES 실시간 연계 |
| 품질이력 관리 | 수집데이터 장기 분석 |

| 활용분야 | 예시 |
|---|---|
| AI 이상탐지 | 센서 데이터 기반 이상조기진단 |
| 예방정비 | 센서이력 기반 Predictive Maintenance |
| 에너지 모니터링 | 공정 전력 소모량 실시간 감시 |

## ✅ 7. IIoT 연동 도입시 실전 설계 고려사항

| 항목 | 설계 기준 |
|---|---|
| 데이터 취득 주기 | 1~10초 단위 → 실시간 대응성 조정 |
| 데이터 보안 | TLS 암호화, 사용자 인증 |
| 네트워크 설계 | 제어망과 IT망 물리적 분리(VLAN, Firewall) |
| 이중화 | Edge Gateway 이중화, 메시지 큐 이중화 |
| 장애복구 | 네트워크 끊김 시 버퍼링 기능 확보 |
| 표준화 | 통신 태그명·데이터 타입 표준 설계 유지 |

## ✅ 8. IIoT 연동시 가장 자주 사용하는 게이트웨이 구조

| 구성 | 설명 |
|---|---|
| Edge Gateway | 산업용 소형 서버 장치 |
| 주요기능 | OPC UA ↔ MQTT 변환, 데이터전처리, 통합통신 중계 |
| 대표제품 | Siemens IOT2040, Kepware, Rockwell FT Edge, Moxa 등 |

## ✅ 9. 실전 적용 사례

| 산업분야 | 사례 |
|---|---|
| 반도체 | 설비이력 통합 수집 → 불량률 개선 |
| 자동차 | 라인 실시간 모니터링 → 라인변속 최적화 |
| 식음료 | 충진기 품질이력 → AI 기반 제품변동 자동보정 |
| 에너지 | 공장 전력피크 실시간 예측 → 수요예측제어 |
| 물류 | AGV 시스템 PLC ↔ IIoT 연동 → 실시간 물류 최적화 |

## ✅ 10. IIoT 도입 ROI의 핵심

- **기존 PLC 변경 최소화** → 안정적 제어 유지
- **데이터의 실시간성 확보** → 분석·예측 정확도 향상
- **유지보수 비용 절감** → 현장 점검 횟수 최소화
- **생산성·품질 향상** → AI 기반 최적화 가능성 확보

---

## ✅ 정리

- **PLC + IIoT 통합은 단순 "제어" → "데이터 중심 공장 운영"으로의 본질적 전환**
- 제조사 내장지원이 빠르게 확대되고 있으며
- 게이트웨이 방식, OPC UA 표준화, MQTT 경량화, 클라우드 연동을 종합 설계하는 것이
  **현대 PLC 설계의 필수 확장 전략**이 되었다.

# 14.2 Edge Computing과 PLC

*(PLC 시스템과 엣지 컴퓨팅 통합 구조 설계 완전 정리)*

---

## ✅ 개요

**Edge Computing**은 IIoT 확장에서 PLC 다음 단계 핵심 아키텍처다.

- PLC는 하드 실시간 제어 중심
- Edge는 데이터 수집·전처리·분석·AI 연산 중심

즉, **제어는 PLC → 데이터 분석은 Edge**로 분리 설계되면서
**"스마트 공장 실시간 지능화"** 기반이 완성된다.

---

## ✅ 1. Edge Computing의 PLC 내 역할

| 구분 | 기능 |
|---|---|
| **PLC** | 장비 제어, I/O 실시간 응답, 공정 안전 |
| **Edge** | 대용량 데이터 수집, 필터링, 이력저장, AI 연산, 예측진단, 클라우드 게이트웨이 역할 |

---

## ✅ 2. Edge Computing 연동 구조

```
[ 센서 → PLC → Edge Node → Cloud / MES / AI Analytics ]
```

- Edge 노드는 현장 제어망 가장 가까운 곳에 위치
- **네트워크 대역폭 절감 / 실시간 데이터 유지 / 클라우드 의존도 분산**

---

## ✅ 3. Edge Node 하드웨어 예시

| 제품군 | 특징 |
|---|---|
| Siemens IOT2050 / 2040 | 산업용 엣지 게이트웨이 |
| Rockwell FactoryTalk Edge Gateway | Allen-Bradley 전용 |
| Moxa Industrial Computer | 범용 Edge 서버 |
| Dell EMC Edge | 공장현장 산업용 서버 |
| Advantech EdgeLink | IIoT 전용 엣지 게이트웨이 |

- 대부분 **OPC UA ↔ MQTT ↔ SQL ↔ AI 엔진 내장**

---

## ✅ 4. 엣지 컴퓨팅의 핵심 기능

| 기능 | 설명 |
|---|---|
| 실시간 수집 | PLC 태그 실시간 수집 (ms~s 단위) |
| 데이터 정제 | 노이즈 제거, 이동평균, 스파이크 필터링 |
| 이벤트 추출 | 이상 패턴 실시간 감지 |
| 이력저장 | 로컬 Historian 구축 |
| AI 연산 | ML/AI 알고리즘 현장측 적용 |
| 클라우드 연계 | MQTT, REST API로 중앙 시스템 연동 |

---

## ✅ 5. PLC ↔ Edge 통신 연계 방식

| 방법 | 설명 |
|---|---|
| OPC UA 직접 | PLC가 OPC UA Server 제공, Edge가 Client 역할 |
| MQTT 브로커 중계 | Edge가 브로커 중계, PLC MQTT Publisher 동작 |
| Modbus 중계 | 저가 PLC에서는 Modbus TCP 통해 Edge 연결 |
| SCADA 연계형 | SCADA가 Edge 중계서버 역할 병행 가능 |

---

## ✅ 6. Edge Computing 적용 분야

| 적용영역 | 실전 활용 예시 |
|---|---|
| **Predictive Maintenance** | 모터전류 진동패턴 → AI 이상징후 조기탐지 |
| **품질 예측** | 용접·충진 공정 센서 패턴 → 실시간 품질보정 |
| **에너지 최적화** | 대용량 장비 전력소모 최적화 |
| **AI 기반 시뮬레이션** | 공정 변수 변화 예측 기반 시뮬레이션 |
| **자율보정 제어** | Edge AI 연산 → PID 세팅 자동보정 |

## ✅ 7. 엣지 컴퓨팅이 필요한 이유

| 기존 한계 | Edge의 해결 |
|---|---|
| PLC 연산 한계 | 대규모 데이터 처리 가능 |
| 클라우드 의존 | 현장 자체 연산 가능 |
| 대역폭 부담 | 데이터 사전 전처리 |
| 지연시간 문제 | 실시간 AI 연산 가능 |
| 보안 문제 | 민감데이터 현장 잔류 보호 가능 |

## ✅ 8. 실전 설계 고려 사항

| 항목 | 설계 지침 |
|---|---|
| 연산 자원 | Edge Node 스펙 → AI, 통계연산 대비 충분한 CPU/GPU |
| 신뢰성 | 산업용 장기운영 가능 하드웨어 선택 |
| 이중화 | Edge 서버 이중화 구성 고려 |
| 데이터모델 | OPC UA 기반 공통 데이터모델 통일 |
| 보안 | 현장망 내부 폐쇄형 Edge 운영 기본, 클라우드 구간만 외부 개방 |

## ✅ 9. PLC + Edge 융합형 최신 확장

| 영역 | 특징 |
|---|---|
| Edge+PLC 통합장치 | 일부 제조사는 Edge 기능 내장된 PLC 제공 (Omron, Siemens 최신) |
| Edge AI 연산 내장 | AI 추론 엔진 내장된 산업용 Edge Box 등장 |

| 영역 | 특징 |
|---|---|
| Edge Historian | 장기 데이터 저비용 분산저장 기반 구축 |
| Edge Digital Twin | 현장 디지털트윈 실시간 현장측 연산 가능 |

---

## ✅ 10. 실전 적용 사례

| 분야 | 사례 |
|---|---|
| 반도체 | 공정압력 이상패턴 조기탐지 → 품질불량 20% 감소 |
| 자동차 | 용접품질 AI 분석 → 자동 오퍼셋 보정 |
| 식음료 | 충진량 초정밀 AI 예측 → 재공정률 감소 |
| 플랜트 | 대형 펌프 진동패턴 → 고장예지 후 무정지 운전 |
| 물류 | AGV 이동패턴 AI 최적화 → 충돌·지연 최소화 |

---

## ✅ 정리

- **Edge Computing은 PLC + IIoT를 넘어 '현장 실시간 AI 제어'를 가능하게 만든다**
- 초기 설계시부터 **제어 → 데이터 → 분석 → 보정**이 순환되는 구조를 설계하면
  진정한 **스마트 팩토리 고급 자동화 아키텍처**로 발전할 수 있다.

# 14.3 AI 기반 예지보전 시스템과의 연계

*(PLC 데이터를 활용한 인공지능 기반 예측정비 설계 완전 정리)*

---

## ✅ 개요

**예지보전 (Predictive Maintenance, PdM)** 은
스마트 제조 핵심 중에서도 가장 ROI가 높은 영역이다.

- PLC → 실시간 공정 데이터 수집
- Edge → 데이터 전처리 및 1차 분석
- AI → 이상징후 탐지·예측정비 모델 학습

**"PLC 제어 + Edge Computing + AI 학습"**
이 3단계가 완전히 융합될 때
**고장 발생 전 선제적 예방조치 → 생산 손실 최소화 → 유지보수 비용 최적화** 가 가능하다.

---

## ✅ 1. 예지보전 기본 흐름 구조

```
[ 센서 ] → [ PLC I/O 수집 ] → [ Edge Preprocessing ] → [ AI 분석 ] → [ 예측알람 발생 ] → [ 유지보수 조치 ]
```

- 기존 PLC가 측정하는 **일상적 센서 데이터** 자체가 예지보전의 핵심 입력이 된다.

---

## ✅ 2. 예지보전 AI 연계 핵심 데이터 요소

| 측정요소 | 활용예시 |
|---|---|
| 전류 | 모터 부하 이상 감지 |
| 진동 | 베어링 손상 조기 감지 |
| 온도 | 냉각장치 노후화 탐지 |
| 압력 | 밸브 막힘, 유량 이상 진단 |
| 유량 | 펌프 성능 저하 탐지 |
| 속도 | 서보위치 이상 조기감지 |
| 품질이력 | 제품 불량패턴과 공정 변수 연결 |

---

## ✅ 3. PLC 단에서의 데이터 수집 설계

| 구조 | 설계 방법 |
|---|---|
| 고주기 수집 | 100ms ~ 1s 단위로 태그 업데이트 |
| 이벤트 기반 트리거 | 이상신호 발생시 고속로그 |
| FIFO 버퍼링 | 네트워크 장애시 데이터 보존 |
| 장기이력 | Edge Historian 연계 장기 저장 설계 |

---

## ✅ 4. AI 예지보전 시스템 구성 요소

| 구성요소 | 설명 |
|---|---|
| **Edge Layer** | 실시간 데이터 필터링, 이상 트리거 발생 |
| **AI Layer** | 머신러닝/딥러닝 기반 고장 예측모델 운용 |
| **Visualization** | 실시간 예측상태 시각화 및 운영자 알람 |
| **Maintenance Layer** | 유지보수 스케줄 최적화, 교체주기 조정 |

---

## ✅ 5. AI 모델 유형

| 알고리즘 | 활용예시 |
|---|---|
| 시계열 예측 (LSTM, GRU) | 센서 신호 패턴 장기 추세 예측 |
| 이상탐지 (AutoEncoder, Isolation Forest) | 정상범위 벗어난 패턴 조기 탐지 |
| 분류 모델 (Random Forest, XGBoost) | 상태분류 (정상/주의/위험 등급) |
| 회귀모델 | 잔존수명(RUL: Remaining Useful Life) 예측 |
| 클러스터링 (KMeans, DBSCAN) | 고장징후 군집 탐색 |

## ✅ 6. AI 학습 데이터 구성

| 요소 | 설명 |
|---|---|
| 정상운영 이력 | 장기 정상 데이터 축적 |
| 장애 발생 이력 | 과거 고장 발생시 패턴 수집 |
| 유지보수 로그 | 교체·정비 기록 연계 |
| 환경조건 | 온습도, 생산조건 기록 포함 |

## ✅ 7. 실전 예지보전 도입 예시 흐름

```
① PLC 실시간 태그 수집
② Edge Node 실시간 Preprocessing
③ AI 서버 학습 및 실시간 추론 배포
④ 이상감지시 운영자 알림 → 정비스케줄 변경
⑤ 고장발생 전 선제적 교체
```

## ✅ 8. PLC 제조사별 예지보전 연계 지원

| 제조사 | 지원 현황 |
|---|---|
| Siemens | Industrial Edge, MindSphere, AI Runtime |
| Rockwell | FactoryTalk Analytics, Logix AI Module |
| Mitsubishi | iQ Works AI 연동 패키지 |
| Omron | Sysmac AI Controller 내장형 AI 추론 |
| LS산전 | EdgeBox, OPC UA 연계 기반 AI 시스템 가능 |
| Keyence | KV-8000 실시간 고속 진동분석 지원 |

| 제조사 | 지원 현황 |
|---|---|
| Delta | IIoT Edge 기반 AI 연계 가능 (일부 모델) |

## ✅ 9. 실전 적용 분야 사례

| 분야 | 사례 |
|---|---|
| 모터 구동계 | 전류·진동·소음 → 베어링 파손 조기 감지 |
| 펌프·압축기 | 유량·압력 → 캐비테이션 초기 징후 탐지 |
| 공정용 히터 | PID 보정패턴 → 열효율 저하 진단 |
| 로봇 서보축 | 위치오차·속도패턴 → 감속기 마모 조기 감지 |
| 반도체 장비 | 압력·온도·유량 조합 → 공정불량 사전 경고 |

## ✅ 10. 예지보전 ROI 실전 수치 예시

| 개선항목 | 성과 |
|---|---|
| 갑작스러운 정지시간 | 50~80% 감소 |
| 유지보수 비용 | 20~40% 절감 |
| 부품 교체주기 최적화 | 불필요한 조기교체 감소 |
| 생산품질 안정성 | 불량률 10~30% 저감 |
| 유지보수팀 업무부하 | 단순점검 → 문제부위 집중화 |

## ✅ 11. 초기 설계 핵심 전략

| 단계 | 설계포인트 |
|---|---|
| ① 센서 확장 | PLC에 필요한 진동, 전류 등 신규 센서 증설 |
| ② Edge 수집 안정화 | 네트워크 이중화, 실시간 수집 완전성 확보 |
| ③ AI PoC (파일럿) | 초기 제한영역 AI 모델 실증시험 |
| ④ 시스템 표준화 | 데이터모델, 태그명 표준화 |
| ⑤ 유지보수 프로세스 통합 | AI 결과를 유지보수 스케줄 자동반영 |

## ✅ 정리

- **PLC 예지보전은 센서 기반 데이터 중심 정비로의 패러다임 전환 핵심**
- Edge → AI → PLC의 순환구조 구축이
  장기적 스마트공장 고장감소·비용절감·품질향상 핵심이다.

# 14.4 PLC와 클라우드 데이터 연동

*(PLC 데이터를 클라우드로 안전하고 실시간으로 연계하는 통합 설계 전략 정리)*

---

## ✅ 개요

**PLC + 클라우드 연동**은 이제 현대 스마트팩토리에서
가장 필수적이면서도 전략적인 설계 영역이다.

- 현장 제어는 PLC 중심 유지
- 데이터 분석·장기 이력·AI 학습·MES 통합·전사 가시화 → 클라우드로 이동

**현장 Edge → 클라우드 중앙분석 → 피드백 최적화 제어**
이 흐름이 PLC 기반 제조라인의 미래형 아키텍처가 된다.

---

## ✅ 1. 전체 통합 아키텍처

```
[ 센서 / 장비 ]
    ↓
[ PLC 실시간 제어 ]
    ↓
[ Edge Gateway (실시간 수집·전처리) ]
    ↓
[ 클라우드 데이터 플랫폼 (AWS / Azure / GCP / Private Cloud) ]
    ↓
[ AI, BI, MES, ERP, 중앙 가시화 ]
```

- **현장 실시간성은 PLC 유지, 장기분석은 클라우드에서 처리**

---

## ✅ 2. 클라우드 연동의 주요 필요성

| 목적 | 설명 |
|---|---|
| 이력저장 | 장기 데이터 축적 (수년 단위 가능) |
| 고급 분석 | AI, BI 기반 품질·생산성 최적화 |
| MES/ERP 통합 | 생산·경영 전사 통합 |
| 현장간 통합 | 다공장, 해외공장 중앙 집중 가시화 |
| 협업 플랫폼 | R&D, 품질, 경영팀간 협업데이터 공유 |

## ✅ 3. 주요 통신 연동 방식

| 방식 | 설명 |
|---|---|
| **OPC UA → Cloud** | 표준 OPC UA 서버 → 클라우드 게이트웨이 연계 |
| **MQTT Broker → Cloud** | 현장 Edge Broker → Cloud MQTT Broker 연계 |
| **REST API → Cloud** | SCADA ↔ RESTful API로 중앙 시스템 직접 연계 |
| **Message Bus** | Kafka / AMQP 기반 메시징 연동 |
| **Cloud Connector** | 제조사 전용 클라우드 게이트웨이 솔루션 활용 |

## ✅ 4. 제조사별 클라우드 연동 플랫폼 예시

| 제조사 | 클라우드 연계 솔루션 |
|---|---|
| **Siemens** | MindSphere, Industrial Edge |
| **Rockwell** | FactoryTalk Edge, Plex Cloud MES |
| **Mitsubishi** | iQ Edgecross, MELSEC Edge Gateway |
| **Omron** | Sysmac AI Cloud Connect |
| **LS산전** | EdgeBox → OPC UA → MES/ERP 연동 |
| **Keyence** | OPC UA, MQTT 확장 연결 |
| **Delta** | DIACloud 플랫폼 제공 |

## ✅ 5. 클라우드 플랫폼 일반 구조

| 계층 | 기능 |
|---|---|
| **Device Layer** | PLC, 센서, 장비 |
| **Edge Layer** | 실시간 수집, 필터링, 버퍼링 |
| **Ingestion Layer** | Cloud Gateway (OPC UA/MQTT 수신) |
| **Storage Layer** | Data Lake, SQL, NoSQL |
| **Analytics Layer** | AI/ML, BI, 시계열 예측 |
| **Application Layer** | MES, ERP, Dashboard, API 서비스 |

## ✅ 6. 데이터 수집 주기 실전 설계

| 구분 | 수집주기 |
|---|---|
| 알람 이벤트 | 즉시 이벤트 |
| 일반 생산이력 | 1~10초 |
| 품질변수 | 1초 이하 가능 |
| 고속 진동 | 100ms 이하 (Edge 전처리 필요) |

---

## ✅ 7. 데이터보안 설계

| 위험요소 | 대응 설계 |
|---|---|
| 제어망 노출 | 현장망 ↔ IT망 분리 (DMZ 이중 네트워크 설계) |
| 데이터암호화 | TLS 기반 전송 암호화 |
| 인증관리 | Device 인증서 기반 접속 관리 |
| 로그감사 | 이력조회 이중 기록체계 유지 |
| Fail-safe | 네트워크 중단시 Edge 버퍼 기능 확보 |

---

## ✅ 8. 실전 연동 흐름 예시

### 📌 예: Siemens S7-1500 → MindSphere 연동

```
S7-1500 PLC → OPC UA Server 활성화
   ↓
Edge Gateway (Industrial Edge) → MindSphere Cloud Ingestion
   ↓
Data Lake → AI Analytics → MES / ERP → Dashboard
```

### 📌 예: LS XGK → MES Cloud 연동

```
LS PLC → OPC UA Gateway → EdgeBox → Private Cloud MES
   ↓
생산계획 ↔ 실시간 생산량 ↔ 품질피드백 실시간 연계
```

---

## ✅ 9. 실전 적용 사례

| 산업 | 활용 사례 |
|---|---|
| 반도체 | 설비이력 전사 클라우드 집계 → 품질분석 |

| 산업 | 활용 사례 |
|---|---|
| 자동차 | 글로벌 공장 MES 통합 → 생산진도 실시간 통합 |
| 식음료 | 공장간 에너지소비 실시간 비교 |
| 제약 | 생산이력 eBR 전사 디지털로그 관리 |
| 전력 | 발전소 설비 Health Monitoring 글로벌 통합감시 |

---

## ✅ 10. 초기 도입시 실전 전략

| 단계 | 전략 |
|---|---|
| ① 파일럿 선정 | 단일 장비·라인부터 시작 |
| ② Tag Mapping | PLC ↔ 클라우드 태그명 일관성 유지 |
| ③ Edge 안정화 | 현장 데이터완전성 확보 (결측 최소화) |
| ④ AI/BI 활용 확장 | 예지보전·에너지관리부터 적용 |
| ⑤ 중앙통합 확장 | MES/ERP 통합으로 발전 |

---

## ✅ 정리

- **PLC의 클라우드 연동은 스마트제조 '제어 → 경영 최적화' 통합 핵심**
- 초기에 안정적 수집 아키텍처와 데이터 표준모델을 잡아두면
  장기적으로 AI, BI, MES, ERP 확장이 손쉽게 이루어진다.

# 14.5 사이버 보안 (PLC 해킹 대응)

## ✅ 개요

**PLC 해킹**은 과거엔 이론적 위협이었지만,
**실제 산업제어시스템(ICS) 공격** 사례가 급증하고 있다.

- Stuxnet (이란 핵시설 PLC 파괴)
- Triton (석유플랜트 Safety PLC 해킹)
- Industroyer, BlackEnergy (발전소·전력망 공격)

스마트팩토리로 PLC가 네트워크화되고 IIoT·클라우드 연계가 확산되면서
**PLC 보안은 이제 필수 시스템 설계 요소**가 되었다.

---

## ✅ 1. PLC 보안의 취약 포인트

| 영역 | 주요 취약점 |
|---|---|
| **물리 접근** | 유지보수 PC 통한 비인가 접근 |
| **네트워크 취약점** | PLC ↔ SCADA ↔ MES 연계망 해킹 |
| **펌웨어 공격** | 펌웨어 변조, 악성코드 삽입 |
| **프로그램 조작** | 래더 프로그램 비인가 수정 |
| **통신스니핑** | 실시간 I/O 제어 신호 탈취 |
| **이중화 우회** | Fail-Safe 시스템 무력화 시도 |

---

## ✅ 2. ICS 해킹 시나리오 예시

| 단계 | 공격방법 |
|---|---|
| 초기 침입 | 유지보수 노트북 → 현장망 침입 |
| lateral 이동 | SCADA, PLC 네트워크 확산 |
| 제어권 장악 | PLC 프로그램 직접 변경 |
| 파괴적 실행 | 모터 과속, 압력초과, Safety 무력화 등 파괴지령 |

---

## ✅ 3. PLC 보안 설계의 핵심 계층

| 보안층 | 내용 |
|---|---|
| 물리보안 | 제어실 출입통제, 유지보수 장비 관리 |
| 네트워크분리 | OT망 ↔ IT망 논리적·물리적 분리 |
| 인증·권한 | 접근자 인증, 권한별 계정 분리 |
| 프로그램보호 | 소스 무결성 검증, 서명기반 펌웨어 |
| 실시간 탐지 | 이상제어명령, 비인가 접속 감시 |
| 이력·감사 | 모든 접속·변경 이력 무결성 저장 |

---

## ✅ 4. PLC 보안 아키텍처 기본 설계

```
[ 생산 제어망 (PLC 제어망) ]
 ↕ (Firewall / DMZ)
[ Edge Gateway ]
 ↕ (암호화된 Secure Tunnel)
[ IT망 / MES / Cloud ]
```

- **제어망은 절대 인터넷 직접 연결 금지**
- **현장 유지보수용 임시접속도 무조건 감시·기록**

---

## ✅ 5. 통신계층 보안 강화

| 계층 | 방어전략 |
|---|---|
| PLC ↔ SCADA | OPC UA 암호화 통신 (TLS 기반) |
| PLC ↔ MES | Secure MQTT, HTTPS, 인증서 기반 |
| Remote Maintenance | VPN + 다중인증 기반 제한적 허용 |
| 프로그램 다운로드 | Secure Boot / Code Signing 필수 적용 |

---

## ✅ 6. 제조사별 보안 기능 현황

| 제조사 | 주요 내장 보안 |
|---|---|
| Siemens | Secure Communication, Certificate-based Access (S7-1500), TIA Security |
| Rockwell | FactoryTalk Security, CIP Security, Signed Firmware |
| Mitsubishi | iQ-R Secure Key, Access Control, Firmware Signature |
| LS산전 | XGR 이중화 Secure Key, Secure Remote Access |
| Omron | Sysmac Secure Key, Safety Lock, Signed Project |
| Keyence | 일부 모델 암호화 통신 지원 |
| Delta | 일부 고급 모델 Secure Firmware 적용 |

---

## ✅ 7. 실전 유지보수 보안 설계

| 관리항목 | 권고방안 |
|---|---|
| 유지보수 장비 | 현장용 노트북 전용, 외부망 분리 |
| USB 접근 | 이동식 미디어 사용금지 또는 이중검사 |

| 관리항목 | 권고방안 |
|---|---|
| 원격진단 | VPN 전용계정, 시간제한 접속, MFA |
| 유지보수 기록 | 모든 다운로드 이력, 계정이력 로그화 |

---

## ✅ 8. 이상제어 탐지 시스템 (ICS IDS)

| 기능 | 설명 |
|---|---|
| 실시간 명령분석 | 비정상 제어명령 발생시 즉시 경고 |
| 패턴이상 탐지 | 정상 제어패턴 벗어남 감지 |
| I/O 비정상감시 | 센서값과 제어명령 불일치 감지 |
| ICS 전용 IDS 솔루션 | Claroty, Nozomi, Dragos, Fortinet 등 적용 가능 |

---

## ✅ 9. 실전 해킹 사고 분석 사례

| 사례 | 특징 |
|---|---|
| **Stuxnet** | 원심분리기 과속 제어 (PLC 래더변조) |
| **Triton** | Safety PLC Disable (SIS 이중화 무력화 시도) |
| **Industroyer** | 변전소 제어망 장악 (Modbus, OPC 우회 공격) |
| **BlackEnergy** | 발전소 SCADA 무력화 (원격조작 파괴명령) |

---

## ✅ 10. 스마트팩토리 PLC 보안 도입 원칙

| 단계 | 목표 |
|---|---|
| 제어망 폐쇄 기본 | 외부망 직접노출 차단 |
| 통신계층 암호화 | TLS 기반 모든 통신 보안 |
| 계정권한 분리 | 관리자/유지보수/모니터 분리 |
| 이력무결성 확보 | 모든 변경이력 불변성 기록 |
| 비인가 소프트웨어 금지 | 승인된 엔지니어링 소프트웨어만 사용 |
| 정기 보안교육 | 현장운영자 보안 교육 필수화 |

---

## ✅ 정리

- **PLC 보안은 이제 제어 설계의 필수 내장 요소**
- 초기 설계에서 폐쇄성·감시성·인증성·무결성 체계를 구조적으로 확보해야 장기적 산업보안 체계가 된다.

**스마트팩토리는 항상 '제어+보안'을 동시에 설계해야 한다.**

# 14.6 Safety PLC (Fail-safe, SIL 인증)

## ✅ 개요

**Safety PLC**는 산업자동화에서 **"생명·장비·시설 보호"**를 목적으로 하는 Fail-safe 전용 제어 시스템이다.

- 기존 일반 PLC와 논리구조는 유사하지만
- 안전회로에 요구되는 **이중진단·무결성·SIL/PL 인증 기준**을 만족한다.

특히 대형 제조설비, 중공업, 플랜트, 발전, 반도체, 제약, 로봇라인 등에서는 **Safety PLC 통합설계**가 거의 필수화되고 있다.

---

## ✅ 1. 일반 PLC와 Safety PLC의 핵심 차이

| 구분 | 일반 PLC | Safety PLC |
|---|---|---|
| 목적 | 생산제어 | 안전제어 |
| 고장 대응 | Stop or 계속 운전 | 반드시 안전상태로 Fail-safe |
| 내부진단 | 일반 연산오류 검사 | 이중CRC, 이중메모리, 진단회로 |
| 프로그래밍 | 표준 LD 등 | 전용 Safety 블록 사용 |
| 인증 | 필요없음 | SIL / PL 등 국제안전인증 필요 |
| 이중화 | 선택사항 | 내부 이중구조 내장 필수 |

---

## ✅ 2. Safety PLC가 보호하는 주요 대상

| 보호대상 | 예시 |
|---|---|
| 인명안전 | 작업자 협착, 로봇 충돌, 감전, 낙하물 |
| 장비보호 | 과부하, 이상동작, 모터 손상 |
| 공정안정 | 연쇄사고 확산 방지 |
| 시설보전 | 폭발위험, 과압파괴, 과열손상 |

---

## ✅ 3. 국제 안전 인증 체계

| 인증명 | 의미 | 적용범위 |
|---|---|---|
| **SIL (IEC 61508, 62061)** | Safety Integrity Level | 일반 산업안전 |
| **PL (ISO 13849)** | Performance Level | 기계안전, 로봇제어 |
| **TÜV 인증** | 독립 인증기관 인증 | 각종 Safety 모듈 기준 |

### 📌 SIL 수준 예시

| SIL 등급 | 평균 고장발생 간격 (MTTFd) |
|---|---|
| SIL 1 | ≥ $10^4$ 시간 |
| SIL 2 | ≥ $10^5$ 시간 |
| SIL 3 | ≥ $10^6$ 시간 |
| SIL 4 | ≥ $10^7$ 시간 (특수분야만 해당) |

---

## ✅ 4. Safety PLC 내부 진단 구조

| 진단영역 | 설명 |
|---|---|
| 이중 CPU 연산 | 병렬 이중처리 → 상호검증 |
| 이중 RAM / ROM | CRC 이중무결성 검사 |
| Watchdog | 사이클 이상 감시 |
| 통신진단 | Safety Protocol 이중화 (CRC 기반) |
| 출력회로 자기검사 | 릴레이접점, 솔리드스테이트 출력 자기진단 내장 |

---

## ✅ 5. Fail-safe 제어 구조 흐름

```
[ 입력 (이중센서, 안전스위치) ]
  ↓
[ Safety PLC 이중진단 ]
  ↓
[ 안전 출력 (접촉기, 밸브 차단, 로봇정지) ]
  ↓
[ 안전 상태 유지 → 비상복구 승인 후 정상복귀 ]
```

---

## ✅ 6. 제조사별 Safety PLC 제공 체계

| 제조사 | 안전제어 시스템 |
|---|---|
| **Siemens** | S7-1500F, S7-1200F (F-CPU), Fail-safe IO |
| **Rockwell** | GuardLogix (ControlLogix 통합), Safety IO |
| **Mitsubishi** | iQ-R Safety CPU, Safe Motion 내장 |
| **LS산전** | XGR Safety 이중화 (국내 공급 확대 중) |
| **Omron** | NX-S Safety Controller, Safety Task 분리 |
| **Keyence** | Safety PLC KV-S Series |
| **Pilz, Sick, ABB, Schmersal** | 전용 독립 Safety PLC 전문회사 존재 |

---

## ✅ 7. Safety PLC 프로그램 구조 예시

### 📌 Siemens S7-1500F 기준

- Safety Program (F-Program) 이 일반 OB와 별도 존재
- Safety 기능 블록 예시:

| 블록명 | 기능 |
|---|---|
| F-ESTOP | 비상정지 회로 |
| F-Mode | 운전/보호모드 전환 |
| F-Door | 보호문 스위치 감시 |
| F-Light Curtain | 광커튼 감시 |
| F-Monitoring | 속도·위치 이상 감시 |

---

## ✅ 8. Safety Protocol (통신 이중화 안전프로토콜)

| 프로토콜 | 특징 |
|---|---|
| **PROFIsafe (Siemens)** | PROFINET 기반 이중 CRC |
| **CIP Safety (Rockwell)** | EtherNet/IP 기반 확장 |
| **CC-Link Safety (Mitsubishi)** | CC-Link Field 기반 |
| **Fail-safe over EtherCAT (FSoE)** | EtherCAT 확장 안전층 |
| **Safety over OPC UA (IEC 62541)** | 차세대 Safety Layer 연구중 |

---

## ✅ 9. 실전 현장 Safety PLC 적용 사례

| 산업 | 적용사례 |
|---|---|
| 로봇라인 | 작업자 협착방지, 로봇속도제어 |
| 프레스공정 | 이중비상정지, 광커튼 인터록 |
| 용접라인 | 가스차단, 냉각수 이상시 자동정지 |
| 물류자동화 | AGV 충돌방지, 스태커크레인 안전구간 |
| 발전소 | 증기배관 과압, 터빈 속도이상 차단 |

---

## ✅ 10. 도입시 초기설계 전략

| 단계 | 핵심 |
|---|---|
| 위험도 평가 | 위험요소 리스트 정량화 (Risk Graph 기반) |
| SIL/PL 목표 수립 | 공정별 인증목표 등급 정의 |
| 이중센서 설계 | 단일센서 오류 대비 이중화 |
| Fail-safe 회로화 | 모든 비정상 → 안전정지 경로 확보 |
| 비인가변경 차단 | 프로그램 인증키·서명 관리 |
| 유지보수 교육 | 비상정지 복귀 절차 체계화 |

---

## ✅ 정리

- **Safety PLC는 "사고 전 반드시 안전상태로 넘어가는 보장 시스템" 설계의 핵심**
- 단순 제어가 아니라 **무조건 안전 우선 보호 설계 철학이 핵심**
- 초기부터 전체 설비 안전설계가 통합되면,
  장기운영시 **작업자 안전, 장비수명, 품질 안정성**이 모두 극적으로 향상된다.

# 14.7 모델 기반 자동화 설계 (MBSE)

*(PLC 기반 제어 시스템에서의 모델 기반 시스템 엔지니어링(MBSE) 완전 정리)*

---

## ✅ 개요

**MBSE (Model-Based Systems Engineering)**는
전통적 문서중심 설계에서 → **"디지털 모델 중심 시스템 설계"** 로 전환하는 핵심 개념이다.

PLC 시스템 설계에서도 MBSE 개념을 적용하면:

- 공정 분석 → 제어 논리 → 안전시나리오 → 통신 연계 → 시뮬레이션 → 테스트 → 문서화
  **전 과정을 일관된 모델로 관리**할 수 있게 된다.

---

## ✅ 1. PLC 설계에서 MBSE가 필요한 이유

| 기존 문제 | MBSE 해결 |
|---|---|
| 사양서-회로-소프트 분리 | 통합 모델로 자동 일관성 유지 |
| 프로그램-하드웨어 불일치 | 모델기반 하드+소프트 동시 설계 |
| 변경·추적 어려움 | 변경 이력 자동화 |
| 시뮬레이션 부족 | 가상 시뮬레이션 모델 동시검증 |
| 협업 한계 | 공통 표준모델 통한 다부서 협업 지원 |

---

## ✅ 2. PLC 시스템 MBSE 적용 흐름

```
요구분석 → SysML 기반 시스템 모델 생성
  ↓
동작 논리 모델링 (시퀀스, 상태기계)
  ↓
제어 블록 설계 (Function Block 설계)
  ↓
I/O 모델링, 통신 매핑
  ↓
안전 논리 모델링 (Safety Logic 설계 포함)
  ↓
시뮬레이션 및 검증
  ↓
PLC 코드 자동생성 → 다운로드 → 운영
```

---

## ✅ 3. MBSE 표준 모델링 언어

| 언어 | 설명 |
|---|---|
| **SysML** | 시스템 전체기능 요구분석 모델링 |
| **UML** | 시퀀스, 상태전이, 클래스 다이어그램 |
| **IEC 61131-3 표준** | PLC Function Block 구조 직접 연계 |
| **SCD (System Control Diagram)** | 공정 중심 상태기계 설계 |
| **Statechart** | 시퀀스 기반 상태전이 설계 |

---

## ✅ 4. MBSE가 적용되는 PLC 설계 상세영역

| 설계영역 | 모델 적용 |
|---|---|
| I/O 설계 | 입출력 매트릭스 모델 |
| 시퀀스 제어 | 상태기계 기반 모델링 |
| 에러처리 | 인터록·에러상태 상태도 모델 |
| Safety 설계 | ISO13849 / SIL 통합 위험도 모델 |
| 통신설계 | 통신 링크 매핑 다이어그램 |
| 공정동작 흐름 | 전체 시스템 시퀀스 모델 |

---

## ✅ 5. MBSE 도구 환경 예시

| 도구 | 설명 |
|---|---|
| Siemens PLM | TIA Portal + Polarion MBSE |
| Rockwell Emulate 3D | PLC 시뮬레이션 연계 3D MBSE |
| IBM Rhapsody | SysML/UML 통합 시스템 모델링 |
| Enterprise Architect | 일반 MBSE 통합 도구 |
| Simulink / Simscape | 제어 모델 기반 시뮬레이션 연계 |
| TwinCAT 3 | PLC 모델 기반 자동코드생성 지원 |
| Codesys UML | PLC 소프트웨어 직접 UML 연동 가능 |

---

## ✅ 6. MBSE 기반 PLC 프로젝트 실전 가치

| 효과 | 설명 |
|---|---|
| 요구정의 명확화 | 현장 요구 → 제어 모델 바로 매핑 |
| 시뮬레이션 사전검증 | 실제 하드설비 없이 가상 검증 가능 |
| 코드 일관성 | 모델 → 코드 자동생성 가능 |
| 변경추적성 | 모델 변경이력 자동 기록 |
| 협업성 | 공정, 기계, 전기, 제어 부서간 공통모델 공유 가능 |
| 문서자동화 | 유지보수 문서 자동생성 가능 |

---

## ✅ 7. MBSE와 디지털 트윈의 연결

| 구분 | 역할 |
|---|---|
| MBSE | 시스템 "설계 초기단계" 전체 모델링 |
| 디지털트윈 | "운영중 현장설비" 실시간 가상연동 |

👉 **MBSE 모델을 기반으로 디지털트윈 플랫폼 구축 가능**

---

## ✅ 8. MBSE 적용 시 필수 개념

| 항목 | 설명 |
|---|---|
| 요구명세 추적성 (Requirement Traceability) | 사양 요구 → 모델 요소 연결 |
| 상태기계(State Machine) | 시퀀스 논리의 핵심 표현 |
| 블록다이어그램 | 전체 기능 블록 흐름 정의 |
| 인터페이스 명확화 | 각 모듈간 신호·데이터 흐름 일관성 확보 |
| Safety Logic 통합 | Fail-safe 조건 완전 모델화 |

---

## ✅ 9. 실전 PLC MBSE 적용 사례

| 산업 | 적용 사례 |
|---|---|
| 자동차 | 용접·조립라인 통합 시퀀스 자동생성 |
| 반도체 | 장비 자동이력 생성, Safety 상태기계 모델 자동검증 |
| 식음료 | 공정모듈화 라이브러리 기반 재사용 |
| 물류 | AGV 제어 시뮬레이션 검증 포함 전체 모델링 |
| 발전 | 전체 발전제어시퀀스 통합 모델로 안정성 검증 |

---

## ✅ 10. 초기 MBSE 도입 전략

| 단계 | 실전 전략 |
|---|---|
| ① 파일럿 선택 | 단일설비 시퀀스부터 시작 |
| ② 표준블록 정의 | 재사용가능 FB, 시퀀스블록 설계 |
| ③ Safety 모델화 | Fail-safe 시나리오부터 통합 |
| ④ 시뮬레이션 통합 | 물리장치 없이 가상테스트 환경 구축 |

| 단계 | 실전 전략 |
| --- | --- |
| ⑤ 조직협업 체계화 | 다부서간 공통모델 언어 표준화 추진 |

---

## ✅ 정리

- **PLC 기반 자동화는 이제 단순 "코드 작성"이 아니라**
  **"시스템 모델링 기반 설계" 시대로 확장되고 있다.**
- MBSE를 적용하면 **요구분석 → 설계 → 시뮬레이션 → 자동코드생성 → 운영유지보수**까지
  모든 과정을 **일관된 논리로 통합관리**할 수 있다.