

# SCADA시스템 이벤트 데이터 분석을 통한 장애설비 판단모델 개발

2022.10. | 액티브 러닝!





# 1. 추진배경

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

SCADA시스템 신속한 장애설비 판단 및 복구시간 단축을 위한 모델 개발 필요

“SCADA시스템 장애 시 원인분석 및 조치에 장시간 소요”



## SCADA 설비별 운영부서 상이

- 정보보안부 : 보안장비 (방화벽)
- 전자제어부 : 주장치, 네트워크 장치, 원격소장치 (RTU)
- 설비보강부 : 정보연계장치 (SA)



## 장치별 담당자 로그 수기 분석

- 보안장비, 주장치, 네트워크 장치별 담당자가 시스템 로그\* 수기 분석  
→ 담당자 노하우로 원인파악



## 설비별 제작사 상이

- 상이한 시스템별 로그 수집체계 상이  
시스템별 로그 별도 분석

조치 지연 원인

운영부서 담당자가 해당장비 원격 접속 후 수기 원인 분석 소요 시간 평균 2~3시간 (참조 : ICT 네트워크 운영시스템내 장애관리)

신입직원 등 미숙련된 SCADA 담당자 고장판단시 조치지연 발생  
분석시간 지연으로 SCADA 고장 지속시 전력계통 운전엔 지장 초래

최대 3시간 소요

\* 시스템 로그 : ICT시스템에서 생성되는 이벤트 기록 (에러정보, 통신 및 자원상태 등)



# 1. 추진배경

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

추진 목표

**“SCADA시스템 이벤트 분석을 통한 장애구간 및 고장설비 판단 모델 개발”**SCADA 시스템  
로그데이터 수집고장설비  
판단모델 개발고장발생  
예측모델 개발

향 후



변전소 (RTU) 장치 로그 수집

네트워크 장치 로그 수집

급전분소 장치 로그 수집



장애시 발생 데이터 변환

로그 데이터 전처리

로그 분석 및 고장설비 판단



로그 자동수집기능 추가

트래픽 증감 및 이상징후 탐지

장애 발생 징후 포착 및 알림



## 2. 팀 구성

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

### “SCADA시스템 이벤트 분석을 위한 최적 전문가로 팀구성 ”





### 3. 과제 개요

추진배경

팀 구성

과제개요

개발과정

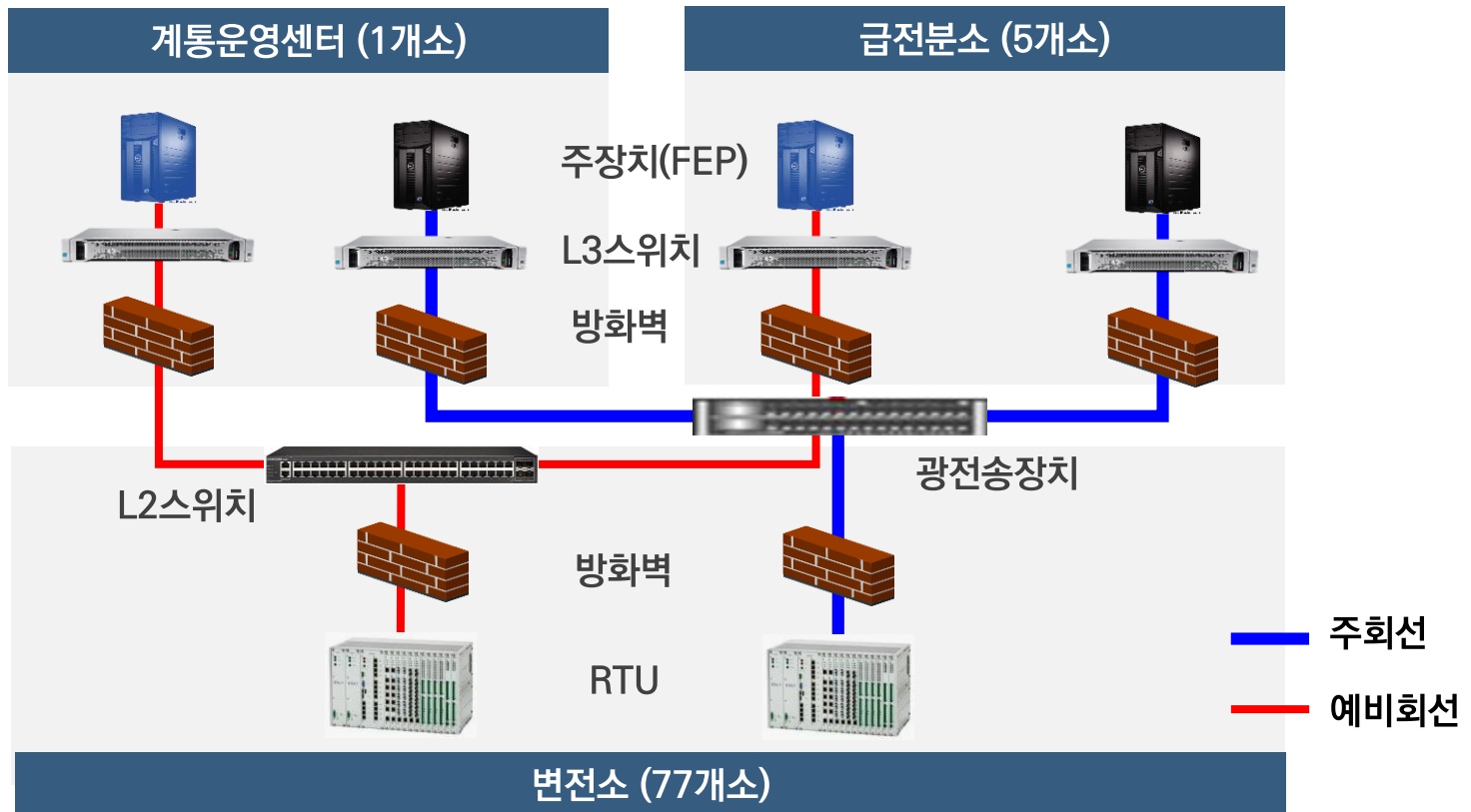
기대효과

향후계획

#### 목 표

SCADA 시스템 이벤트 분석을 통한 장애설비 판단 모델 개발

#### 구성도





### 3. 과제 개요

추진배경

팀 구성

과제개요

개발과정

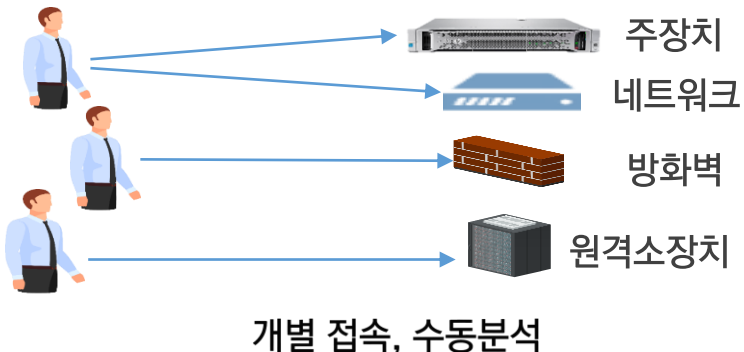
기대효과

향후계획

#### 내 용

- SCADA시스템 로그 데이터 수집
    - 변전소(RTU), 방화벽, 네트워크 장치(L3, L2 및 광전송장치), 주장치(계통운영센터, 급전분소)
  - 장비별 시스템 로그 수기 분석 → 수집된 로그 상관관계 분석을 통한 장애설비 조기 판단
- ※ 기존) 설비별 장애로그 개별 분석, 개선) 장애로그 종합분석/판단

#### AS-IS



#### TO-BE



✓ 신속 정확한 고장 판단 모델 적용으로 전력계통 안정적 운영에 기여





### 3. 과제 개요

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

#### 추진 방안

##### 분석도구

- Python, PyQt5, Excel
- 분석환경 : 노트북

##### 적용알고리즘

- 모델명 : 고장분석 판단 알고리즘
- 판정기준 : 고장시 분석결과 확인 (정확도 : 95%)
- 테스트 : 신일변전소 현장 검증

#### 단계별 추진내용

1단계

데이터수집



2단계

데이터 전처리



3단계

탐색적 분석



4단계

모델링



## 4. 개발과정

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

### 개발과정 1단계 - 데이터 수집

#### 내 용

- 급전분소 ~ 변전소 원격소장치(RTU) 간 모든 ICT설비 로그 데이터 수집

설비	수집 항목 (이벤트 내용)	데이터 기간
주장치(FEP)	주장치(계통운영센터, 급전분소)-RTU간 통신 패킷 세부내용 (일시, 출발지/목적지 IP, 서비스포트, 정보* 등)	'22.8.28~'22.9.28
스위치 (L3)	일시, 인터페이스 Up/Down 및 상태 변화 내역	'22.8.28~'22.9.28
스위치(L2)	일시, 변전소명, 인터페이스 Up/Down 내역	'22.8.28~'22.9.28
광전송장치	일시, 변전소명, 인터페이스 Up/Down 내역	'22.8.28~'22.9.28
FW(방화벽)	일시, 출발지/목적지 IP, 데이터 길이, 정보, 통신포트 등	'22.8.28~'22.9.28
RTU	일시, 변전소명, 모듈 상태 변동 내역	'22.8.28~'22.9.28





## 4. 개발과정

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

### 개발과정 2단계 – 데이터 전처리 (변환)

#### 내 용

- 시간별 설비별 장애시 발생 데이터 추출

설비	추출 항목 (이벤트 내용)
주장치(FEP)	주장치(FEP)-RTU 통신 로그내에 TCP Retransmission 발생 여부
스위치 (L3)	인터페이스 Down 발생 여부
스위치(L2)	인터페이스 Down 발생 여부
광전송장치	인터페이스 Down 발생 여부
FW(방화벽)	방화벽 전원 및 인터페이스 고장 발생
RTU	RTU 통신 고장 발생 여부



## 4. 개발과정

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

### 개발과정 2단계 – 데이터 전처리 (병합)

#### 내 용

- 로그 병합을 위해 전처리 수행
  - ✓ 시간형식 통일(1초 단위)
  - ✓ 불필요한 column 삭제
  - ✓ 중복데이터 삭제

TIME	SS_NAME	FW_IP	SCADA_IP_C	SS_CAT	PRI_ALT	RCC_RET	RCC_L3	SCC_RET	SCC_L3	SS_L2	SS_SONG	RCC_FW_PW	SCC_FW_PW	SS_FW_PW	RCC_FW_PT	SCC_FW_PT	SS_FW_PT	RTU
2022-09-21 15:26:00	가수원변전소	0.51.05.131	0.51.05	RTU	주	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:26:00	가수원변전소	11.58.51.14	0.51.5	RTU	예비	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:26:00	대화변전소	11.58.52.16	0.52.7	RTU	예비	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:26:00	서세종변전소	11.58.52.24	0.52.15	RTU	예비	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:26:00	신서산변전소	11.58.54.23	0.54.14	RTU	예비	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:26:00	신일변전소	11.58.52.14	0.52.5	RTU	예비	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:26:00	온양변전소	0.53.04.131	0.53.04	RTU	주	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:26:00	인주변전소	11.58.53.11	0.53.2	RTU	예비	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:26:00	인주변전소	11.58.53.11	0.53.63	SA	예비	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:26:00	한샘변전소	0.53.122.131	0.53.122	RTU	주	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:26:00	함덕변전소	11.58.54.56	0.54.56	SA	예비	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:27:00	대화변전소	11.58.52.16	0.52.7	RTU	예비	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:27:00	신일변전소	11.58.52.14	0.52.5	RTU	예비	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:27:00	온양변전소	0.53.04.131	0.53.04	RTU	주	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:27:00	인주변전소	11.58.53.11	0.53.2	RTU	예비	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
2022-09-21 15:27:00	인주변전소	11.58.53.11	0.53.63	SA	예비	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE



## 4. 개발과정

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

### 개발과정 3단계 -탐색적 분석

#### 내용

수집데이터  
상관관계 분석

- 특정 시간대 조건문 활용한 시간로그 매칭
  - ✓ 조건문 : 재전송, 포트 다운, 전원 OFF 등 데이터 이력 유무

#### 계통운영센터 FEP 장애로그 분석

시간	변전소	계통센터 FEP 장애
2022-09-21 15:25	신일변전소	[TCP Retransmission]

#### 변전소 방화벽 장애로그 분석

시간	변전소	변전소 방화벽 장애
2022-09-21 15:25	신일변전소	ErrorCode : 실패

#### RTU 로그 분석

#### 장애발생 통합DB생성

시간	변전소	계통센터 FEP 장애	계통센터 방화벽 장애	계통센터 L3 장애	분소 FEP 장애	분소 방화벽 장애	분소 L3 장애	변전소 L2 장애	변전소 송광치 장애	변전소 방화벽 장애	RTU 장애
2022-09-21 15:25	신일변전소	[TCP Retransmission]								ErrorCode : 실패	

#### 통합 DB 결과분석

#### 데이터 케이스별 장애내용 분류

시간	변전소	계통센터 FEP 장애	계통센터 방화벽 장애	계통센터 L3 장애	분소 FEP 장애	분소 방화벽 장애	분소 L3 장애	변전소 L2 장애	변전소 송광치 장애	변전소 방화벽 장애	RTU 장애
2022-09-21 15:25:23	신일변전소	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE

#### 장애내용 추출





## 4. 개발과정

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

### 개발과정 4단계 – 결과 모델링

#### 내용

#### 모델링 알고리즘 현장 테스트 결과 (신일변전소)

- 장해 설비 판단을 위한 프로그램 적용

#### 장애 설비 판단 프로그램

시작시간	2022-09-21 15:26:00	종료 완료
종료시간	2022-09-21 15:50:00	
장소	가수원변전소	
장애 분류		
세션끊김	전원 OFF	포트 다운

2022-09-21 15:27:00 신일변전소 예비에서 방화벽 전원 off 발생

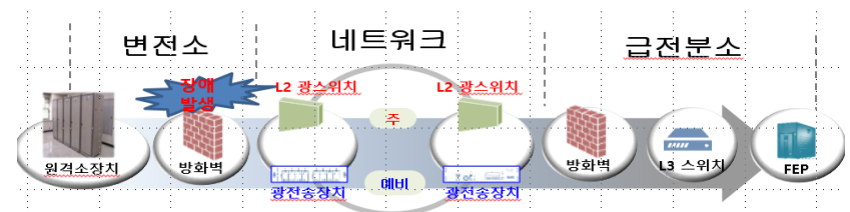


신일변전소 예비에서 방화벽 전원 off 발생

구성도



#### SCADA 설비 장애시 화면





## 5. 기대 효과

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

01

### SCADA 시스템 이벤트 분석 및 대응시간 단축으로 담당자 업무부담 경감

#### ■ 정량적 효과 : 연간 인건비 약 6억원 절감

– 전사 적용시 설비담당자 대응시간 단축으로 인한 인력 감축 효과

(산식) 연간 설비 장애건수 × 장애판단 단축시간 × 4직급 시간단가

= 8,080건(년) × 2.8시간(단축시간) × 26.8천원(4직급 시간단가) = 606,323천원

※ 전사 설비 장애 건수 : 변전소 및 급전분소(계통운영센터) 총 808개소 × 10건 = 8,080건(년)

장애판단 단축시간 : 기존 판단시간 - 개선 판단시간 = 약 3시간 - 15분 = 2.8시간

02

### SCADA 시스템 장애시 신속한 복구로 안정적인 전력계통 운전지원



## 6. 향후 계획

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

### 01 완료

- SCADA이벤트 데이터 분석으로 장애구간 판단모델 개발



### 02 ~' 23.6

- SCADA이벤트 자동 통합수집 로그 시스템기반 개발



### 03 ~' 23.12

- 차세대 DAS시스템 장애구간 판단모델로 적용 확대





# 프로토타입 시연

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

✓ 프로토타입 시연 동영상



# 감사합니다

I T H A N K Y O U I



# 붙임 1. DATA SET

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

## DATA SET 상세설명

설비	컬럼명	데이터 값 설명
주장치 (FEP)	rcc_server_ tcp_fault	(0 / 1) : 계통운영센터 FEP-RTU간 세션끊김 (발생 / 미발생)
	scc_server_tcp_fault	(0 / 1) : 급전분소 FEP-RTU간 세션끊김 (발생 / 미발생)
스위치 (L3)	rcc_l3_PortDown	(0 / 1) 계통운영센터 L3 스위치 인터페이스 포트 Down (발생 / 미발생)
	scc_l3_PortDown	(0 / 1) 급전분소 L3 스위치 인터페이스 포트 Down (발생 / 미발생)
	rcc_l3_PortDownNumber	0 ~ 34 : 계통운영센터 L3 스위치 인터페이스 Down 발생포트 번호
스위치 (L2)	scc_l3_PortDownNumber	0 ~ 34 : 급전분소 L3 스위치 인터페이스 Down 발생포트 번호
	ss_l2_PortDown	(0 / 1) : 변전소 L2 스위치 인터페이스 포트 Down (발생 / 미발생)
광전송장치	ss_l2_PortDownNumber	0 ~ 34 : 변전소 L2 스위치 인터페이스 Down 발생포트 번호
	ss_song_PortDown	(0 / 1) : 변전소 송광치 인터페이스 포트 Down (발생 / 미발생)
FW (방화벽)	rcc_fw_PowerDown	(0 / 1) : 계통운영센터 방화벽 전원off (발생 / 미발생)
	scc_fw_PowerDown	(0 / 1) : 급전분소 방화벽 전원off (발생 / 미발생)
	ss_fw_PowerDown	(0 / 1) : 변전소 방화벽 전원off (발생 / 미발생)
	rcc_fw_PortDown	(0 / 1) : 계통운영센터 방화벽 인터페이스 포트 Down (발생 / 미발생)
	scc_fw_PortDown	(0 / 1) : 급전분소 방화벽 인터페이스 포트 Down (발생 / 미발생)
RTU	ss_fw_PortDown	(0 / 1) : 변전소 방화벽 인터페이스 포트 Down (발생 / 미발생)
	ss_rtu_PortDown	(0 / 1) : 변전소 RTU 인터페이스 포트 Down (발생 / 미발생)



## 붙임 2. SCADA 설비현황

추진배경

팀 구성

과제개요

개발과정

기대효과

향후계획

### □ 전체 설비 운영현황

(단위 : 식, '22.8.31 기준)

구분	중앙SCADA	계통운영센터	급전분소	원격소장치	비 고
수량(식)	1	14	52	742	

### □ 사업소별 운영현황

사업소	계통운영센터	후비 계통운영센터	급전분소	원격소장치	비 고
서울본부	1	1	3	46	
남서울본부	1	1	4	55	
인천본부	1	1	4	53	
경기북부본부	1	1	3	41	
경기본부	1	1	5	88	
강원본부	1	1	3	38	
충북본부	1	1	2	35	
대전세종충남본부	1	1	5	64	
전북본부	1	1	3	35	
광주전남본부	1	1	4	59	
대구본부	1	1	4	71	
경북본부	1	1	2	24	
부산울산본부	1	1	5	67	
경남본부	1	1	4	53	
제주본부		1	1	13	급전분소
합 계	14	15	52	742	



# 붙임 3. SCADA 구성도

추진배경

팀 구성

과제개요

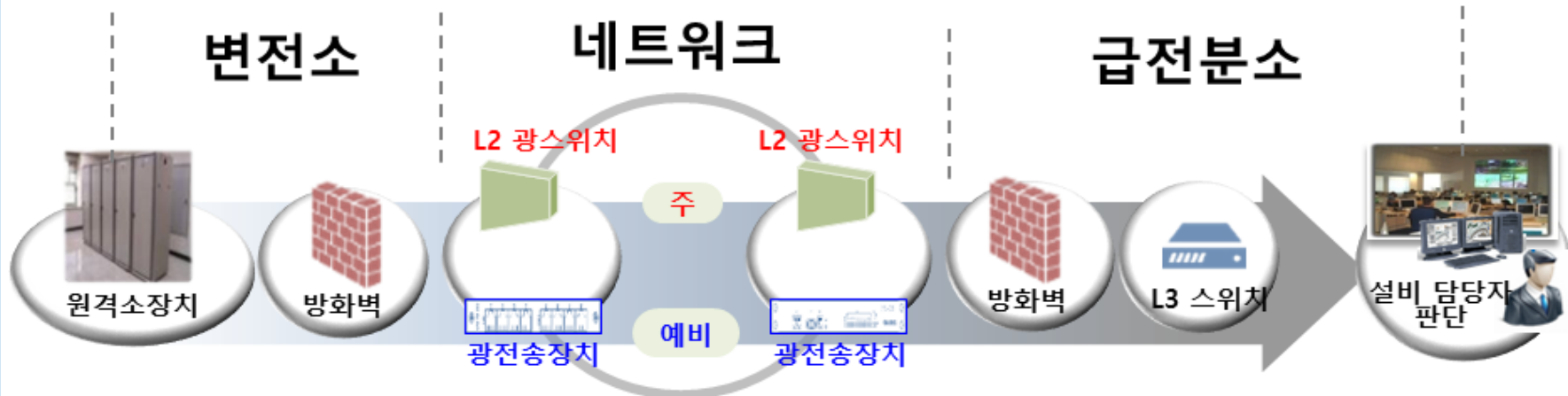
개발과정

기대효과

향후계획

## SCADA 시스템 구성도

급전분소장치	네트워크장치	원격소장치/SA	방화벽	계
5개소 63대	166대	64대/13대	193대	499대



- 장애 설비
- 발생 시간
- 통신 상태
- 자원 상태
- 에러 로그



이벤트 데이터 분석  
장애구간 예측모델 개발