

원격 점검 장치 데이터 연동 규격서

[원격 점검 장치]

Version	1.0.3
Date	'22.05.02

한국전기안전공사
원격 점검 추진 센터

Revision History

[illegible]

목 차

1.	문서의 목적	1
2.	용어의 설명	1
3.	연동 규격	4
4.	푸시 메시지	13
4.1.	Last Will	13
4.2.	주기 메시지	14
4.3.	이벤트 메시지	14
5.	제어 메시지	15
5.1.	설정 메시지	18
5.2.	조회 메시지	20
5.3.	FOTA 요청	21
5.4.	파형정보 요청	22
5.5.	재시작	23
5.6.	파일전송	24
6.	긴급제어 메시지	25
6.1.	시스템 콘솔	26
6.2.	AT Command	27
[별첨1]	이벤트 조건 설정 기본 값	28
[별첨2]	이벤트 메시지 발생 방법	29
[별첨3]	보안 규격	30
[별첨4]	참고자료 : 산출식 예제 (Octave)	34

1. 문서의 목적

일반용전기설비에 설치하는 원격점검장치가 한국전기안전공사 관제시스템과 정보전달 규칙을 표준화 하기 위해 통신 메시지에 대한 연동 규격을 정의 함

- (1) 전기안전관리법 제12조의2(관제센터의 설치.운영) 산업통상자원부장관은 원격점검의 효율적 관리를 위하여 원격점검장치와 연결하여 그 측정결과를 전산처리할 수 있는 관제센터를 설치.운영할 수 있음
- (2) 같은 법 제43조(권한의 위임.위탁) 제2항 제3의2에 따라 제12조의2에 따른 관제센터의 설치.운영을 산업통상자원부장관은 한국전기안전공사에 위탁할 수 있음

2. 용어의 설명

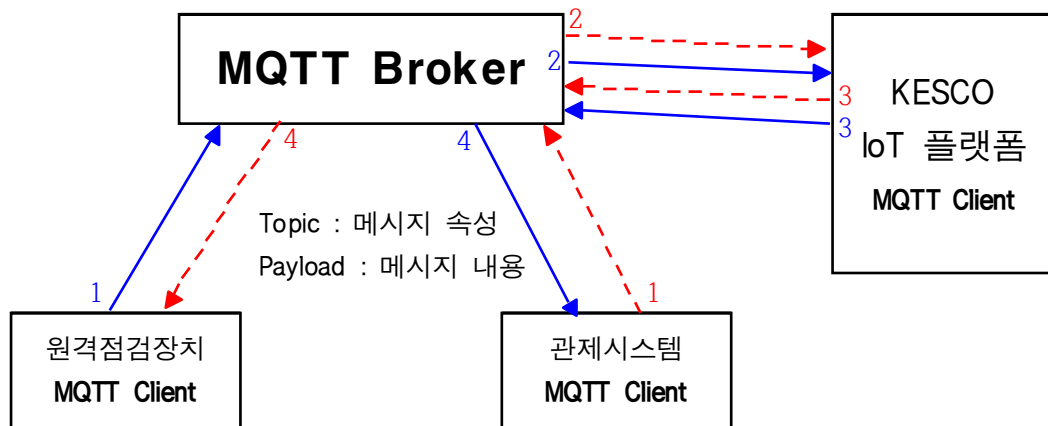
- (1) **원격점검** : 전기설비의 과전압.과전류 및 누설전류 등을 검출하여 이를 데이터로 수집, 분석 및 전송함으로써 전기설비의 안전 상태 등을 점검하는 것을 말함
- (2) **원격점검장치** : 전기안전 원격점검기능을 갖추고 측정된 정보를 관제센터로 전송하는 장치를 말함(이하 “장치” 라 함)
- (3) **관제시스템** : 원격점검의 효율적 관리를 위하여 원격점검장치와 연결하여 그 측정결과를 전산처리할 수 있는 시스템을 말함(이하 “서버” 라 한다)
- (4) **관제센터** : 원격점검장치의 정보를 수집, 저장, 분석, 알림 등 효율적인 전산처리 및 관리를 위한 운영조직을 말함
- (5) **MQTT** : 사물인터넷(IoT)을 위한 OASIS 표준 메시지 송수신 프로토콜 임. TCP/IP 위에서 동작하지만 매우 가볍고, 양방향 통신과 브로드캐스팅, QoS(서비스 품질) 수준 지정, 영구세션, TLS 암호화를 통한 클라이언트 인증을 지원하는 등 주로 코드 공간이 작게 필요하거나 네트워크 대역폭의 제한되는 통신에 사용하는 프로토콜로 사물인터넷(IoT) 통신에 이상적임

- (6) **OASIS** : OASIS(Organization for the Advancement of Structured Information Standards)는 보안, 사물인터넷, 에너지, 콘텐츠 기술, 긴급 관리 등의 기타 분야를 위한 표준 개발, 컨버전스, 채택을 담당하는 비영리 기관
- (7) **Topic** : MQTT 프로토콜에서 메시지를 발행(Publish) 시 메시지의 종류, 발행될 대상, 메시지 연동 규격 버전 등 메시지 속성을 정의 할 수 있는 메시지 제목에 해당되는 것
- (8) **Payload** : MQTT 프로토콜에서 메시지를 발행(Publish) 시 메시지 내용(Data)에 해당되는 것
- (9) **데이터 프로파일(Data Profile)** : 원격점검장치에 대한 정보를 구성하는 가상의 구조체로서 연동규격 버전 및 측정기능, 장치상태 등의 구조를 정의하고 관제센터에서 각각의 원격점검장치 설정 및 조회 등을 하기위한 경로 정보가 들어있는 구조체
- (10) **JSON** : 속성-값으로 이루어진 데이터의 객체를 전달하기 위한 개방형 데이터 표준 포맷방식으로 자료의 종류에 제한이 없으며 표현방식으로 중괄호와 따옴표를 이용해 데이터를 정리하는 방법 또는 중괄호로 묶여진 데이터 세트는 또 다시 쉼표로 구분하여 확장 할 수 있음
- (11) **인증** : 서로 통신하기 전에 물리적 객체가 접속하려는 아이디어에 해당되는 객체가 맞는지 확인하는 절차로 보안인증서를 사용함
- (12) **ADC** : 아날로그 신호를 디지털 값으로 바꾸는 장치 또는 기능을 말하며 ADC에 기준 전압과 입력신호가 입력되면 ADC 성능에 따라 출력 값이 $\text{입력신호} / \text{기준전압} \times \text{해상도}$ 로 출력됨

- (13) **MQTT Broker** : MQTT 프로토콜을 사용하기 위해 구축되어 있는 메시지 중계 프로그램으로서 모든 메시지는 MQTT Broker를 통해 목적지로 전달 됨
- (14) **FOTA** : FOTA(Firmware Over The Air)원격으로 장치 프로그램을 무선통신을 통해 변경하는 것
- (15) **KCMVP(Korea Cryptographic Module Validation Program) 검증** : 암호모듈 검증제도로써, 전자정부법 56조 및 동법 시행령 제 69조와 [암호모듈 시험 및 검증지침]에 의거, 국가 및 공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보의 보호를 위해 사용되는 암호장치의 안전성과 구현 적합성을 검증하는 제도
- (16) **보안 Suite (Cipher_suite)** : 보안 Suite는 기존 TLS, SSL 프로토콜에서 네트워크 연결 보안 설정을 협상하기 위해서 사용되는 인증, 암호화, MAC, 키 교환 알고리즘들의 조합
- (17) **X.509 인증서** : CA(Certificate Authority) 기관에서 승인과정을 통해 발행되어 PKI에서 사용하는 표준 인증서 형식이며 PKI에서 사용하는 공개키, 개인키 등의 비대칭키를 관리하는 인증서 형식

3. 연동 규격

- (1) 본 문서에서 기술하는 연동규격 프로토콜로 MQTT를 사용함
- (2) 장치 또는 관제시스템의 보안 인증을 위해 **TLS 1.2** 버전 이상의 인증서 (x.509)를 사용하며 키길이를 256비트 이상으로 제한 함 ([별첨 3] 참조)
- (3) SSL을 통해 MQTT Broker에 접속하고 송수신 데이터를 암호화할 수 있어야 하며 주기적으로 전기안전공사에게 발급 받은 인증서를 원격으로 교체하고 인증서를 메모리에 평문으로 저장하지 않아야 함
- (4) MQTT 프로토콜은 [그림1]과 같은 ACP(Access Control Policy)에 의해 MQTT Broker에서 메시지를 주고 받음



[그림1] 원격점검장치 송·수신 프로그램 MQTT 프로토콜

- (5) 메시지는 Topic과 Payload로 이루어지며, Topic은 메시지 속성을 나타내는 역할을 하고 MQTT Broker에 설정된 ACP와 접속 계정에 따라 메시지 구독(Subscribe) 권한이 설정 됨. 이 문서에서 Topic은 메시지 속성을 구분하는 역할을 하며 기능별 Topic과 Payload 규칙이 정의 되어 있음
- (6) 장치와 관제시스템이 통신하기 위해 [표 1]과 같이 장치 그룹 아이디, 장치 아이디, 접속 토큰 값을 관제시스템에 등록해야 함

[표 1] 장치 등록 정보

이름	설 명	비 고
Serviceld	장치 그룹 아이디	
deviceld (=IMEI)	장치 아이디	=mqtt user ID, client ID
devicePw	접속 토큰	=mqtt user Password

- (7) 장치에서 서버로 이동하는 메시지는 UpLink 메시지로, 반대로 서버에서 장치로 이동하는 메시지는 DownLink 메시지로 지칭함
UpLink 메시지와 DownLink 메시지는 다음과 같은 공통된 부분을 가지고 있음

```
{version}    = (연동 규격 버전)
{UpLink}     = mrm/{serviceld}/{deviceld}/up/{version}
{DownLink}   = mrm/{serviceld}/{deviceld}/down/{version}
```

- (8) 관제시스템에 장치가 하나 생성되면 다음과 같이 장치에 대한 정보를 담은 가상의 구조체가 생성됨. 이것을 데이터 프로파일(Data Profile)라고 하며 다음과 같은 JSON 형식을 갖음

```
(연동 규격 버전) = {                                     // 본 문서의 버전을 따름
  "val":{
    "data":(측정 값),                                     // 측정한 값 저장
    "hd":(고조파),
    "af":(알람코드)
  },
  "config":{                                             // (rw) 설정한 값 저장
    "event":[(이벤트 메시지 설정 값)],
    "period":(메시지 주기),
    "server":(서버정보)
  },
  "stat":(장치 상태 정보),                               // 현재 장치 상태 정보를 나타냄
  "wave":{                                              // 옵션 기능 1 : 파형정보 조회
    "trigger":(ADC 트리거 설정),                        // (rw)
    "result":(ADC 데이터)
  },
  "watt":(전력량 데이터)                                // 옵션 기능 2 : 전력량 데이터 조회
}

* // : 주석
* (rw) : 이하 경로 값 수정가능
```

※ 만약 장치에 새로운 기능이 추가된다면 쉼표와 종괄호를 통해 추가 할 수 있고 추가되는 기능 중 서버에서 수행해야 하는 것이 많고 복잡하다면 데이터 프로파일에서 연동 규격 버전이 변경될 수 있음

(가) 연동 규격 버전은 문서 번호와 같으며, 다음과 같은 규칙으로 표기

[A].[B].[C] <---- 점으로 구분

- [A] : 프로파일 식별자
- [B] : 버전(Major), 같은 기능이지만 한국전기안전공사 송수신 서버 프로그램 추가/변경이 필요할 경우
- [C] : 버전(Minor)

(나) 데이터 프로파일의 상세 내용은 다음과 같음

```
(측정 값) = {  
  "v" : {  
    "c":(전압 rms 현재 값),  
    "m":(전압 rms 최대 값),  
    "n":(전압 rms 최소 값),  
    "a":(전압 rms 평균 값),  
  },  
  "c" : {  
    "c":(부하전류 rms 현재 값),  
    "m":(부하전류 rms 최대 값),  
    "n":(부하전류 rms 최소 값),  
    "a":(부하전류 rms 평균 값),  
    "x":(부하전류 rms 벡터X 현재 값),  
    "y":(부하전류 rms 벡터Y 현재 값)  
  },  
  "z" : {  
    "c":(누설전류 rms 현재 값),  
    "m":(누설전류 rms 최대 값),  
    "n":(누설전류 rms 최소 값),  
    "a":(누설전류 rms 평균 값),  
    "x":(누설전류 rms 벡터X 현재 값), //igr  
    "y":(누설전류 rms 벡터Y 현재 값) //igc  
  },  
  "g" : {                                     //추가 측정요소 선택사항  
    ...  
  },  
  "t" : {  
    "c":(기판 온도 현재 값),  
    "m":(기판 온도 최대 값),                //선택사항  
    "n":(기판 온도 최소 값),                //선택사항  
    "a":(기판 온도 평균 값),  
  }  
}
```

- * "v" 는 전압, "c" 는 부하전류, "z" 는 누설전류, "g" 추가적인 측정 값
- * 평균 값은 메시지 전송과 전송 사이 평균
- * 최대 값은 메시지 전송과 전송 사이 최대 값
- * 최소 값은 메시지 전송과 전송 사이 최소 값
- * 상기 '메시지' 에는 (측정 값)이 포함되어야 함

- * 추가적인 측정 값 예) 병렬아크 감지
 “arc” : { “ret”: 0, “stat”: (text) }
 - 추가시 안전공사와 협의 필요

구분	의미	형식	구분	의미	형식
v	전압		c	부하전류	
c	rms 현재 값	000.0	c	rms 현재 값	000.0
m	rms 최대 값	000.0	m	rms 최대 값	000.0
n	rms 최소 값	000.0	n	rms 최소 값	000.0
a	rms 평균 값	000.0	a	rms 평균 값	000.0
			x	rms 벡터X 평균 값	±000.0
			y	rms 벡터Y 평균 값	±000.0
z	누설전류		t	기판	
c	rms 현재 값	00.00	c	온도 현재 값	±000.0
m	rms 최대 값	00.00	m	온도 최대 값	±000.0
n	rms 최소 값	00.00	n	온도 최소 값	±000.0
a	rms 평균 값	00.00	a	온도 평균 값	±000.0
x	rms 벡터X 평균 값	±00.00			
y	rms 벡터Y 평균 값	±00.00			
arc	병렬아크 감지				
ret	감지 여부 (0: false, 1: true)	0			
stat	제조사 분석을 위한 추가 데이터(String)	00000000 00000000 00			

- * 현재 값 : 메시지 전송 시점에 측정된 최근 데이터 (12주기 평균)
- * 최대 값 : 메시지 전송과 전송 시점 사이 발생된 데이터 중 최대 값
- * 최소 값 : 메시지 전송과 전송 시점 사이 발생된 데이터 중 최소 값
- * 평균 값 : 메시지 전송과 전송 시점 사이 발생된 데이터 평균 값
- * rms : 실효 값
- * 벡터X : 벡터 평면 X-Y 위 전압 벡터를 기준으로 한 상대 벡터 X 값
- * 벡터Y : 벡터 평면 X-Y 위 전압 벡터를 기준으로 한 상대 벡터 Y 값

```

(고조파) = {
  "v":{
    "n":["(rms),(1차 고조파),(2차 고조파),(3차 고조파),(4차 고조파),(5차 고조파),...,(11차 고조파)"]
    "x":["(rms),(1차 고조파),(2차 고조파),(3차 고조파),(4차 고조파),(5차 고조파),...,(11차 고조파)"]
    "y":["(rms),(1차 고조파),(2차 고조파),(3차 고조파),(4차 고조파),(5차 고조파),...,(11차 고조파)"]
  },
  "c":{
    "n":["(rms),(1차 고조파),(2차 고조파),(3차 고조파),(4차 고조파),(5차 고조파),...,(11차 고조파)"]
    "x":["(rms),(1차 고조파),(2차 고조파),(3차 고조파),(4차 고조파),(5차 고조파),...,(11차 고조파)"]
    "y":["(rms),(1차 고조파),(2차 고조파),(3차 고조파),(4차 고조파),(5차 고조파),...,(11차 고조파)"]
  },
  "z":{
    "n":["(rms),(1차 고조파),(2차 고조파),(3차 고조파),(4차 고조파),(5차 고조파),...,(11차 고조파)"]
    "x":["(rms),(1차 고조파),(2차 고조파),(3차 고조파),(4차 고조파),(5차 고조파),...,(11차 고조파)"]
    "y":["(rms),(1차 고조파),(2차 고조파),(3차 고조파),(4차 고조파),(5차 고조파),...,(11차 고조파)"]
  },
  "g":{ //선택사항
    "n":["(rms),(1차 고조파),(2차 고조파),(3차 고조파),(4차 고조파),(5차 고조파),...,(11차 고조파)"]
    "x":["(rms),(1차 고조파),(2차 고조파),(3차 고조파),(4차 고조파),(5차 고조파),...,(11차 고조파)"]
    "y":["(rms),(1차 고조파),(2차 고조파),(3차 고조파),(4차 고조파),(5차 고조파),...,(11차 고조파)"]
  }
}

```

- * 모두 현재 값임(12주기 평균)
- * “v” 는 전압, “c” 는 부하전류, “z” 는 누설전류, “g” 추가적인 측정 값
- * 각 요소들은 배열로 나타내며 배열의 첫 번째는 모든 고조파 성분의 합
- * “n” 은 “x” , “y” 의 벡터 합을 나타냄

* (rms)와 (n차 고조파)의 관계

$$(rms) = \sqrt{\sum_{n=1}^{\infty} (n차 고조파)^2} \simeq \sqrt{\sum_{n=1}^{11} (n차 고조파)^2}$$

* “n” 과 “x” , “y” 의 관계

$$n = \sqrt{x^2 + y^2}$$

(알람코드)

다음과 같이 계산해서 Hex String 값으로 입력 함

만약, 이벤트 메시지 설정을 8개 이상 설정가능 할 경우엔 Hex String이 뒤로 확장되어 길이가 늘어날 수 있음

이벤트 번호	0	1	2	3	4	5	6	7	bit	HEX
0,1,2,3,4,5 이벤트발생	1	1	1	1	1	1	0	0	1111 1100	FC
정상시	0	0	0	0	0	0	0	0	0000 0000	00

확장시 이벤트 번호	0	1	2	3	4	5	6	7	...	bit	HEX
0,1,2,3,4,5 이벤트발생	1	1	1	1	1	1	0	0	0	1111 1100 0000 0000	FC00
정상시	0	0	0	0	0	0	0	0	0	0000 0000 0000 0000	0000

(이벤트 메시지 설정 값) = [

```
{
  "n":(항목이름=data/v/a),
  "h":(임계 값 상한),
  "l":(임계 값 하한),
  "t":(지속시간)
},
... 설정 항목별로 나열 됨
]
```

// 기본 값 [별첨 1] 참고

* 항목이름은 어떤 값을 참조 할 것인지 나타내며 JSON 구조에서 “val” 이하 경로를 나타냄

예) 이벤트 판단 조건으로 (측정 값) 항목들 중에서 전압의 rms 평균을 가지고 판단하려 할 경우 “data” 에서 “v”의 “a”이므로 “data/v/a”라고 설정 함

* 하한이 존재하면 “l”에 값을 입력하고, 하한이 없으면 키 값 “l” 자체를 생략

* 이벤트 메시지 설정 값은 장치 설치 시 설비 용량에 따라 변경 시킬 수 있어야 함

코드	항목	의미
n	항목이름	어떤값을 참조할 것인지 JSON 구조에서 경로 확인 예) 이벤트 판단 조건으로 (측정 값) 항목들 중에서 전압의 rms 평균을 가지고 판단하려 할 경우 data/v/a 라고 설정
h	임계 값 상한	상한을 설정할 경우 ‘h’값을 입력하고 없으면 ‘h’ 입력 생략 예) h:5
l	임계 값 하한 (알파벳 엘)	하한을 설정할 경우 ‘l’값을 입력하고 없으면 ‘l’ 입력 생략 예) l:5
t	지속시간	지속시간과 단위를 입력 함, h: 시간, m: 분, s: 초 예) t:5m

(메시지 주기) = 15m

//숫자, 단위로 표현 함, 2h15m 조합하지 않음

* 단위

- s : 초, m : 분, h : 시간

(서버정보) = {

“host“:(서버 주소),

“port“:(서버 포트),

“sid“:(장치 그룹 이름),

// ServiceId

“uid“:(장치별 접속 ID),

// mqtt user Id, deviceId, IMEI

“upw“:(장치별 접속 PW),

// mqtt user Password, devicePw

“cid“:(장치 IMEI),

// mqtt client Id, deviceId, IMEI

“cert“:(인증서 cert 파일 경로/이름),

“key“:(인증서 키 파일 경로/이름),

“ca“:(인증서 CA 파일 경로/이름)

}

코드	항목	의미	예시
host	서버주소	데이터 송신할 서버 IP주소 또는 도메인	123.456.789.123
port	서버포트	데이터 송신할 서버의 Port 정보	8883
sid	장치그룹이름	ServiceId	
uid	장치별 접속 ID	mqtt user Id에 해당 됨	
upw	장치별 접속 PW	mqtt user Password에 해당 됨	
cid	장치 IMEI	mqtt client Id에 해당 됨	
cert	인증서 cert 파일 경로	장치 내 cert 파일 저장 경로/이름	테스트시 Self-signed 인증서 활용가능
key	인증서 키 파일 경로	장치 내 키 파일 저장 경로/이름	
ca	인증서 CA 파일 경로	장치 내 ca 파일 저장 경로/이름	

(장치 상태 정보) = {

“gen“:{

“fw_ver“ : [(펌웨어 버전)],

// 관리해야 할 프로그램이 여러가지면 배열로 나열 함

“dev_ver“ : (하드웨어 버전),

“maker“ : (제조사),

“bat“ : (배터리 충전 상태),

// 사용 시 0 ~ 100 (%) 로 기입 / 미사용 시 생략

},

“net“:{

“comp“ : (넷사업자_망이름),

// 예) KT_EMTC, SKT_CATM1, LG_LTE 등

“ant“ : (안테나 레벨),

// 안테나 레벨 (0 ~ 5)

“band“ : (사용 밴드),

// 예) B3, B5

}

}

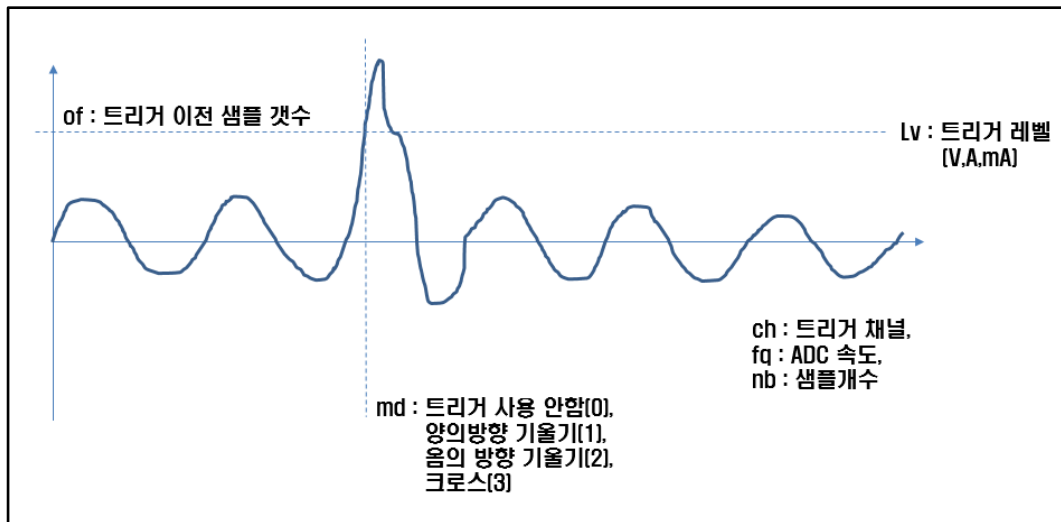
코드	항목	송신데이터(형식)
fw_ver	펌웨어 버전	통합시험때 등록된 펌웨어 일련번호 입력
dev_ver	하드웨어 버전	하드웨어 버전
maker	제조사	제조사 코드(시험시, 제조사 이름 입력)
bat	배터리 충전 상태	사용 시(%)로 기입 / 미사용 시 생략 / 정수형 (0~100)
comp	넷사업자_망이름	예) KT EMTC, SKT_CATM1, LG_LTE
ant	안테나 레벨	예) 안테나 레벨 (0~5)
band	사용 밴드	예) B3, B5

(ADC 트리거 설정) = {

```

"w":["v","c","z","g"],           // 반환 받을 데이터
"md":(트리거모드; 0/1/2/3),      // 0: "disable", 1: "Accend", 2: "Deccend", 3: "Both"
"ch":(트리거채널; 0/1/2/3/...),  // 0: "v", 1: "c", 2: "z", 3: "g"
"lv":(트리거레벨),               // % 단위로 설정, 100%면 ADC의 Vref 임
"of":(트리거오프셋),             // nb보다 작아야 함
"pd":(60Hz 주기수 0/1/2/3/...), // 0: 0.5주기, 1: 1주기, 2: 2주기, 3:...
"nb":(ADC 샘플 개수)            // 통신 메시지로 보낼 총 데이터 샘플 수 ( ~ 200)
}

```



(ADC 데이터) = {

```

"v":["...],
"c":["...],
"z":["...],
"g":["...]
}

```

* ADC 데이터는 ADC 트리거 설정이 포함된 파형 요청에 따라 응답 메시지로써 전달 됨.

코드	항목명	송신데이터(형식)
w	반환 받을 데이터	예시 [v,c,z,g] 또는 [v,c]
md	트리거모드	0(disable), 1(Accend), 2(Deccead), 3(Both)
ch	트리거채널 (트리거 조건을 적용할 신호)	반환 받을 데이터 중 첫 번째 : 0, 두 번째 : 1, ... : n(정수 입력)
lv	트리거레벨	%단위로 설정, 100이면 ADC의 Vref임 50이면 AC파형의 중간 값 임
of	트리거오프셋	nb보다 작아야 함, 트리어 시점 이전 몇 샘플을 측정할 것인지
pd	60Hz 주기 수	0(0.5주기), 1(1주기), 2(2주기), 3...
nb	ADC 샘플 개수	통신 메시지로 보낼 총 데이터 샘플 수(최대 200)
v	전압 ADC 값	ADC 전압 측정 채널 값 * (이득 보정 값)
c	전류 ADC 값	ADC 전류 측정 채널 값 * (이득 보정 값)
z	누설전류 ADC 값	ADC 누설전류 측정 채널 값 * (이득 보정 값)

```

(전력량 데이터) = { // 선택사항
    "kwh" : (적산 소비전력량),
    "kvar" : (적산 무효전력량), // 생략가능
    "kva" : (적산 피상전력량) // 생략 가능
}

```

(9) 메시지 종류는 크게 3가지로 구분함

- (가) 단순하게 장치에서 서버로 보내는 메시지인 “푸시메시지”
- (나) 서버에서 장치로 메시지를 보내고 응답을 받는 “제어메시지”
- (다) 제어메시지로 제어 불능상태에서 장치를 복구하기 위한 “긴급메시지”

4. 푸시 메시지

푸시메시지에는 Last Will, 주기적메시지, 이벤트메시지가 있고 메시지 구조는 표2와 같음

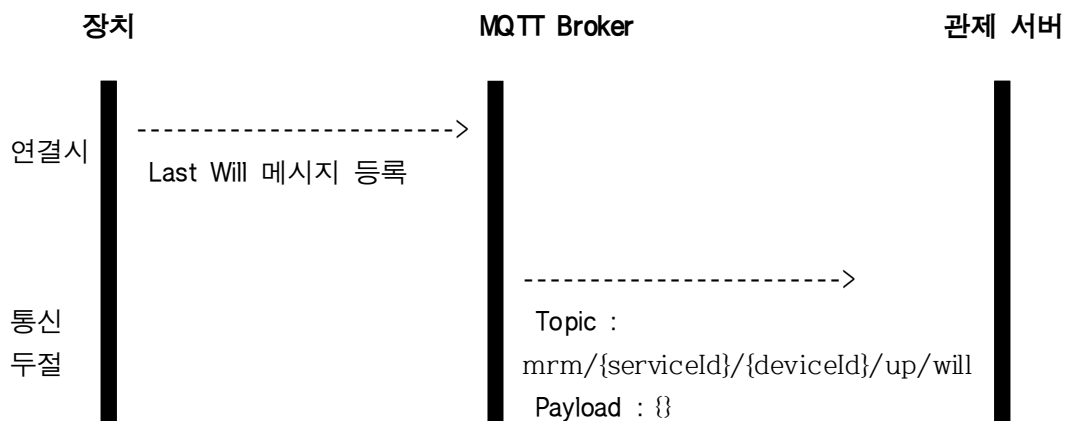
[표2] 푸시 메시지

이름	설명	메시지 구조
Last Will	예상치 못한 통신두절을 알려주는 메시지	Topic : {UpLink}/will Payload : {}
주기적 메시지	설정된 주기에 따라 주기적으로 상태를 알려주는 보고 메시지	Topic : {UpLink}/p Payload : (측정 값)
이벤트 메시지	이벤트 조건 설정에 따라 이벤트 발생시 발생하는 메시지	Topic : {UpLink}/e Payload : { "data" :(측정 값), "af" :(알람 코드)}

* {} 표시에 어떤 내용이 들어와도 상관없음

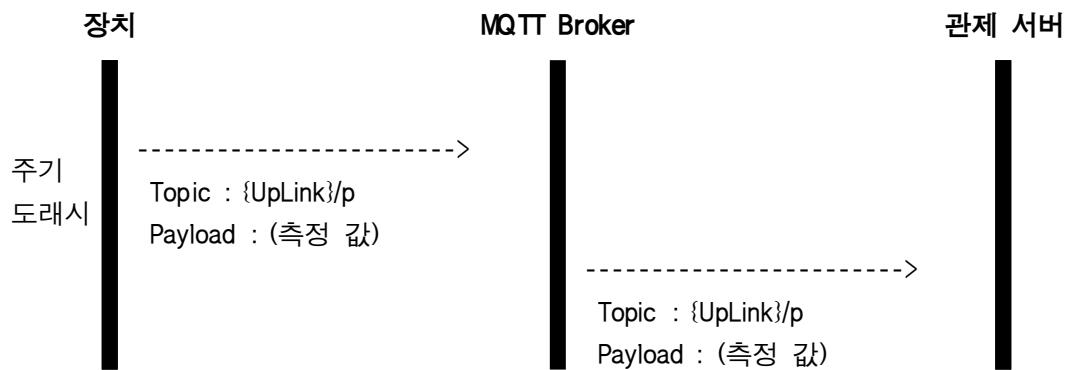
4.1. Last Will

장치가 예상치 못하게 통신두절 되는 경우 Last Will 이라는 메시지를 MQTT Broker에 접속할 때 미리 등록할 수 있으며, 예상치 못하게 통신두절 될 경우 아래와 같이 메시지를 송신함



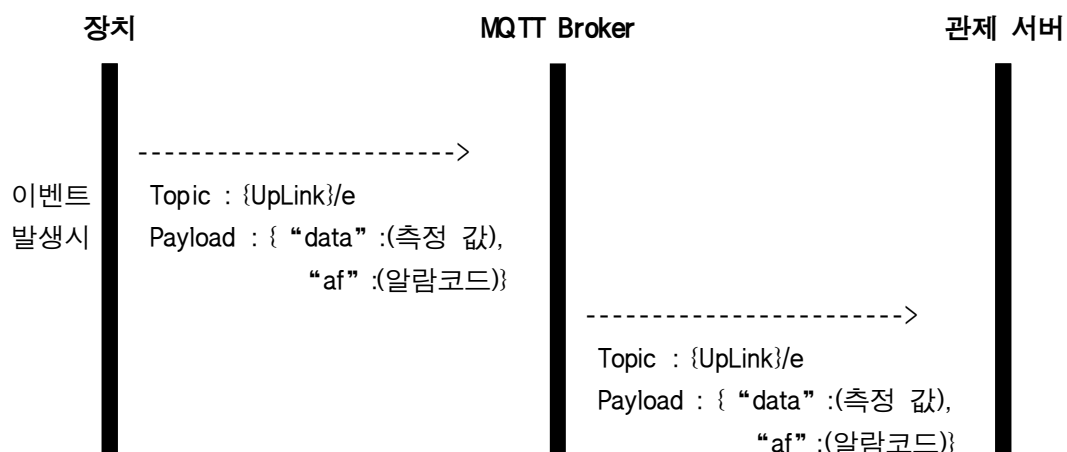
4.2. 주기 메시지

관제시스템에서 각 장치별로 상태정보 추이를 확인하기 위해 주기 메시지를 받음. 여기서 메시지 발생 주기는 장치별 설정 값을 참조



4.3. 이벤트 메시지

이벤트 발생시 즉시 관제시스템에서 알고 조치할 수 있도록 각 장치별로 설치환경에 맞게 설정된 이벤트 메시지 발생조건에 따라 이벤트 메시지를 서버로 발송함



5. 제어 메시지

관제시스템에서 장치의 상태를 조회하거나 상세한 분석을 위해 또는 알람 설정 변경/추가를 위해 제어 메시지를 송신하고 이에 따른 결과를 응답메시지를 통해 받음

본 연동 규격 버전에서 설명하는 제어 메시지는 다음 표3과 같음

[표3] 제어 메시지

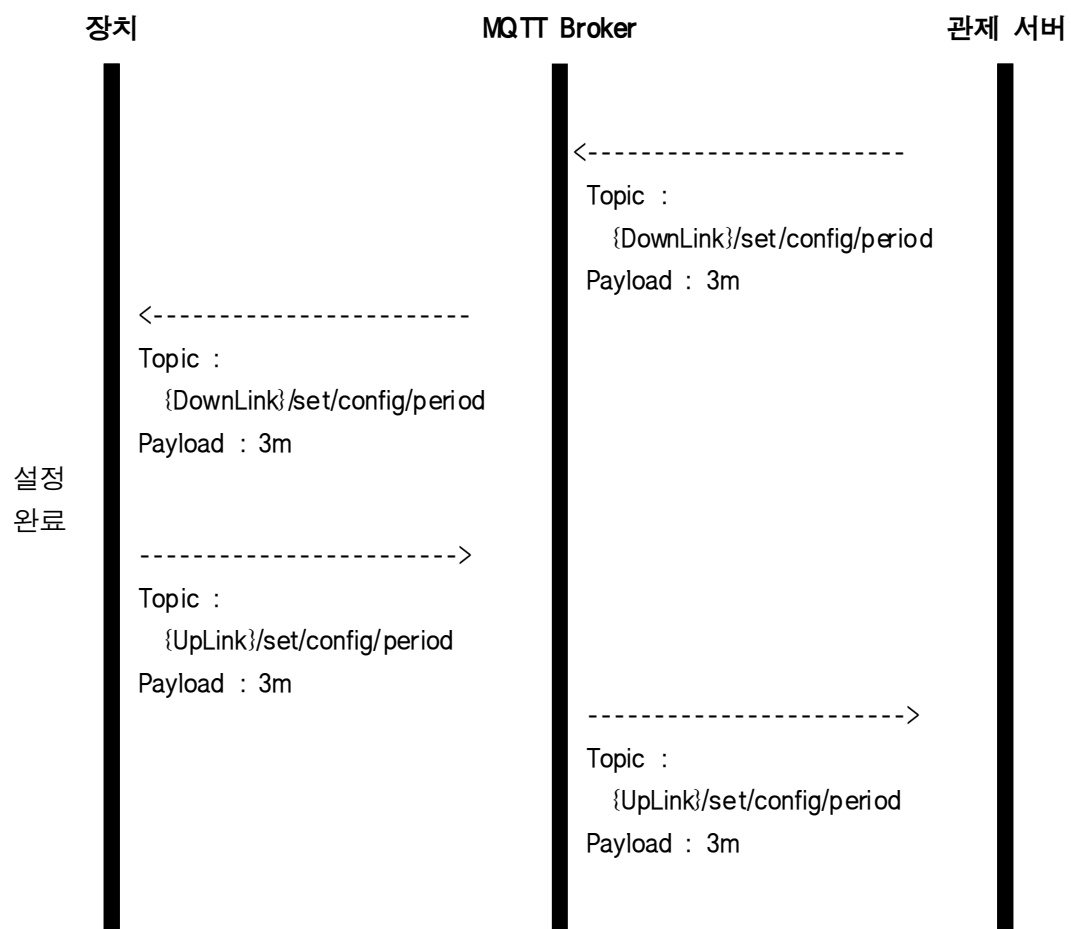
이름	설명	메시지 구조
설정 메시지	장치 설정을 변경하는 메시지	<p>[요청]</p> <p>Topic : {UpLink}/set/{JSON 경로}</p> <p>Payload : (변경 하려는 값)</p> <p>[응답]</p> <p>Topic : {UpLink}/set/{JSON 경로}</p> <p>Payload : (변경 된 값)</p>
조회 메시지	장치 설정을 조회하는 메시지	<p>[요청]</p> <p>Topic : {UpLink}/get/{JSON 경로}</p> <p>Payload : {}</p> <p>[응답]</p> <p>Topic : {UpLink}/get/{JSON 경로}</p> <p>Payload : (조회 된 값)</p>
FOTA 요청	원격으로 내부 프로그램을 변경하는 메시지	<p>[요청]</p> <p>Topic : {DownLink}/fota</p> <p>Payload : {</p> <p> "url" : (firmware url),</p> <p> "to" : (save to),</p> <p> "ver" : (version),</p> <p> "size" : (firmware file size),</p> <p> "psk" : (Pre-Shared key),</p> <p> "crc" : (CRC)</p> <p>}</p> <p>[응답]</p> <p>Topic : {UpLink}/fota</p> <p>Payload : {</p> <p> "result" : (결과; 0: success/1: fail),</p> <p> "crc" : (CRC)</p> <p>}</p> <p>// CRC = (1바이트 단위 합 계)를 256(0x100) 으로 나눈 나머지</p>

파형정보 요청	주어진 트리거 조건에 따라 파형 정보를 요청 하는 메시지	<p>[요청]</p> <p>Topic : {DownLink}/wave</p> <p>Payload : (ADC 트리거 설정)</p> <p>* ch 0: 전압, 1: 부하전류, 2: 누설전류, 3: 추가 측정 요소 // 선택사항</p> <p>* md 0: 상승, 1: 하강, 2: 상승/하강</p> <p>* fq 0~... // 숫자가 클수 록 ADC속도가 느려짐</p> <p>[응답]</p> <p>Topic : {UpLink}/get/wave</p> <p>Payload : { "v":[...], // 요청에 맞게 보낼 데이터 선정해서 보냄 "c":[...], "z":[...], "g":[...] }</p>
재시작	원격으로 장치를 재부팅 시킴	<p>[요청]</p> <p>Topic : {DownLink}/reboot</p> <p>Payload : {reboot 방법}</p> <p>*reboot 방법 "sw" : 소프트웨어 리셋 "hw" : 하드웨어 리셋</p> <p>[응답]</p> <p>Topic : {DownLink}/reboot</p> <p>Payload : {reboot 방법}</p>

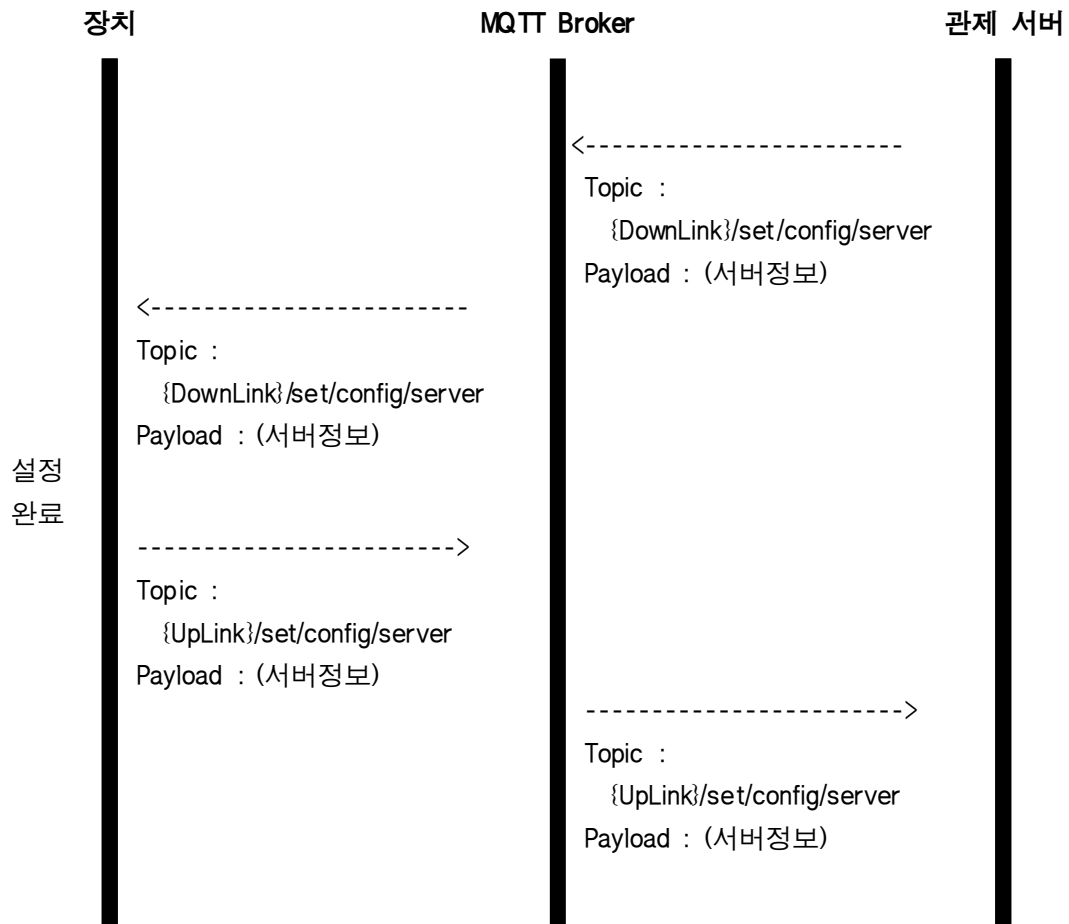
파일 전송	장치에 파일을 전송함 프로그램, 인증서 등	<p>[요청] Topic : {DownLink}/filedown Payload : { "sz":{"파일전체크기}, "nb":{"사이즈 1000으로 나눈 개수}, "crc":{"합친 파일 CRC}, "to":{"저장경로} }</p> <p>[응답] Topic : {UpLink}/filedown/0 Payload : {}</p> <p>[요청] Topic : {DownLink}/filedown/0 Payload : {Binay datas [최대길이 1000]}</p> <p>...</p> <p>[응답] Topic : {UpLink}/filedown/20 Payload : {}</p> <p>[요청] Topic : {DownLink}/filedown/20 Payload : {Binay datas [최대길이 1000]}</p> <p>다 받았으면,</p> <p>[응답] Topic : {UpLink}/filedown Payload : { "result" : 0 }</p> <p>* <i>result 0: 성공,</i> <i>1: 실패</i></p>
-------	----------------------------	--

5.1. 설정 메시지

장치를 관제시스템에 등록할 때 데이터 프로파일이 생성되는데 바꾸고 싶은 값이 있다면 데이터 프로파일을 참조하여 바꾸려는 값의 JSON 경로를 Topic에 표현. 예를 들어 주기메시지 주기를 3분으로 바꾸고 싶다면 아래와 같이 수행함



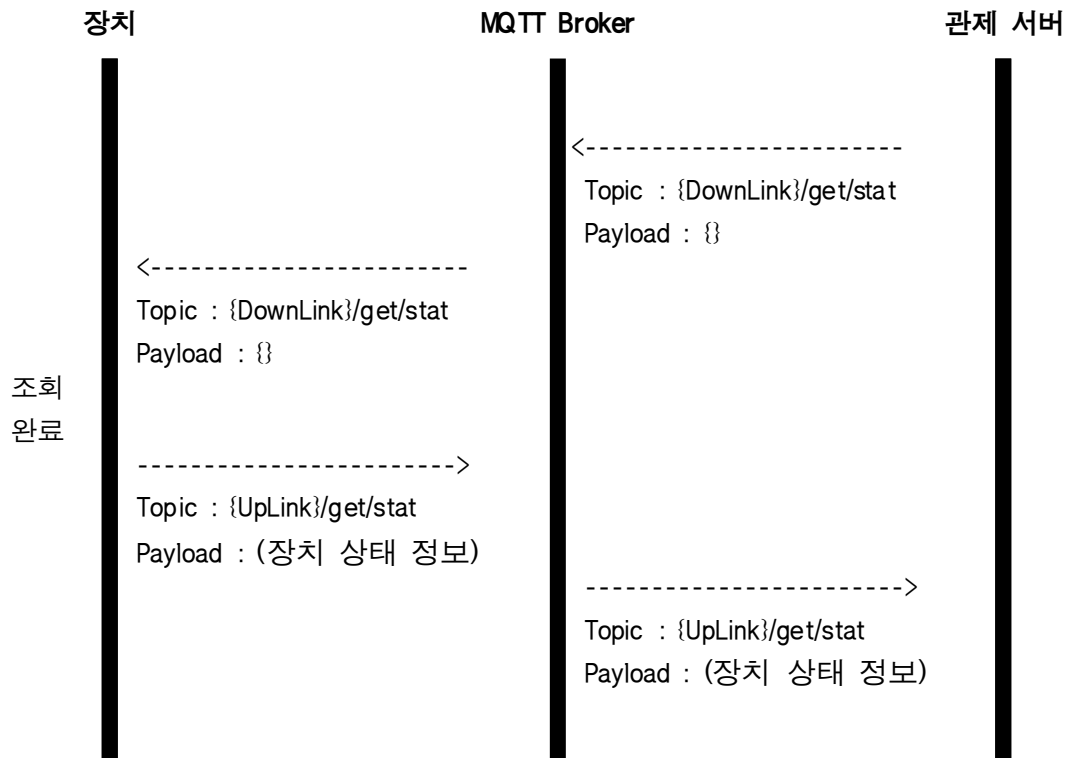
서버 정보와 같이 값들을 한꺼번에 변경하고 싶다면 아래와 같이 Payload
에 JSON 형식으로 입력함



UpLink로 전송하는 (서버정보)는 설정 완료 후 장치에 적용된 값을 나타냄

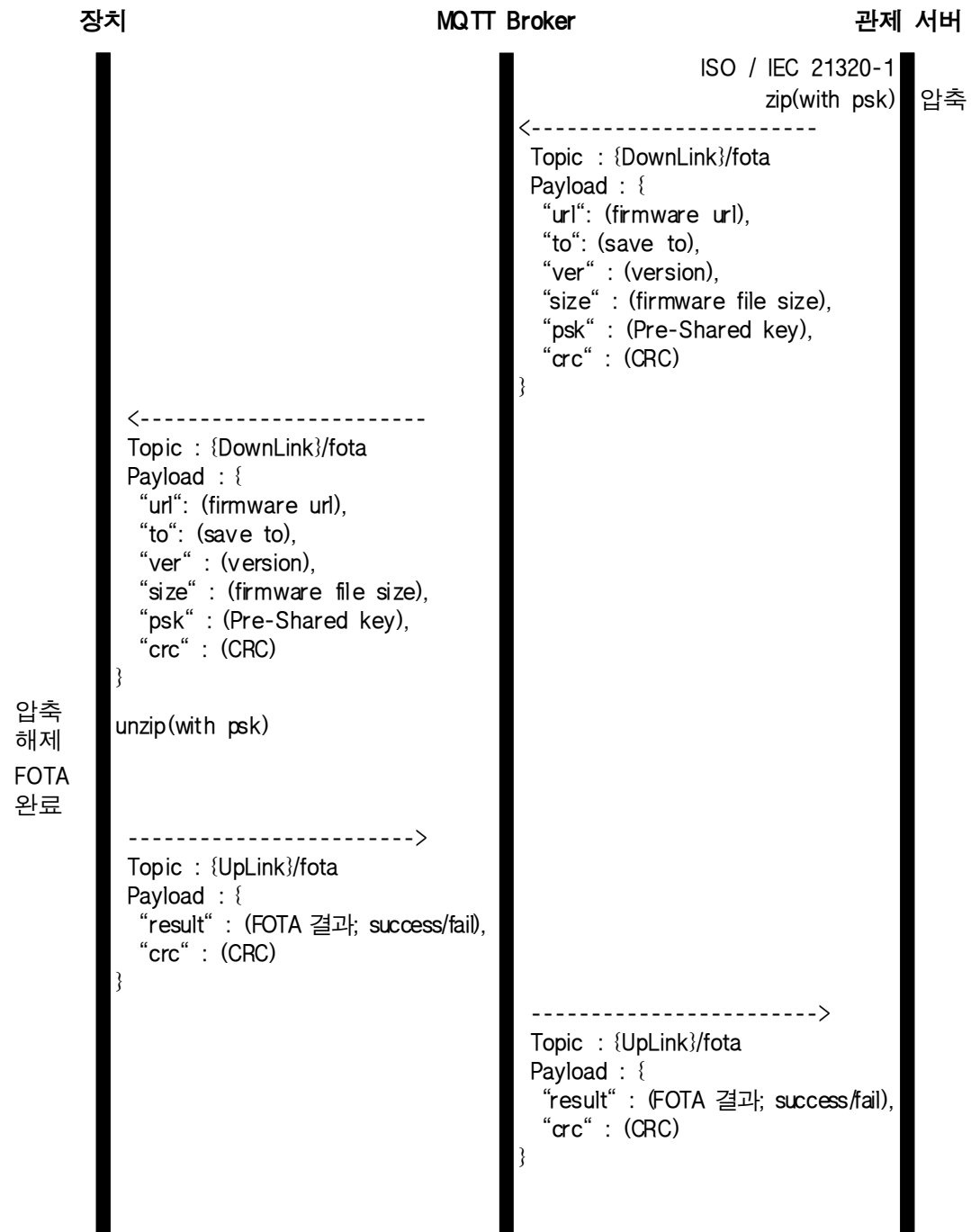
5.2. 조회 메시지

관제시스템에서 장치의 상태를 조회하기 위해서 데이터 프로파일에서 원하는 항목의 경로를 Topic에 입력하여 응답 메시지를 통해 상태 값을 받음. 예를 들어서 장치 상태정보를 알고 싶다면 다음과 같이 데이터를 송수신함



5.3. FOTA 요청

원격으로 현장에 설치된 장치의 내부 프로그램을 변경하고 싶을 때 서버에서 다음과 같은 제어 메시지를 통해 프로그램, 인증서 등 파일을 전송함



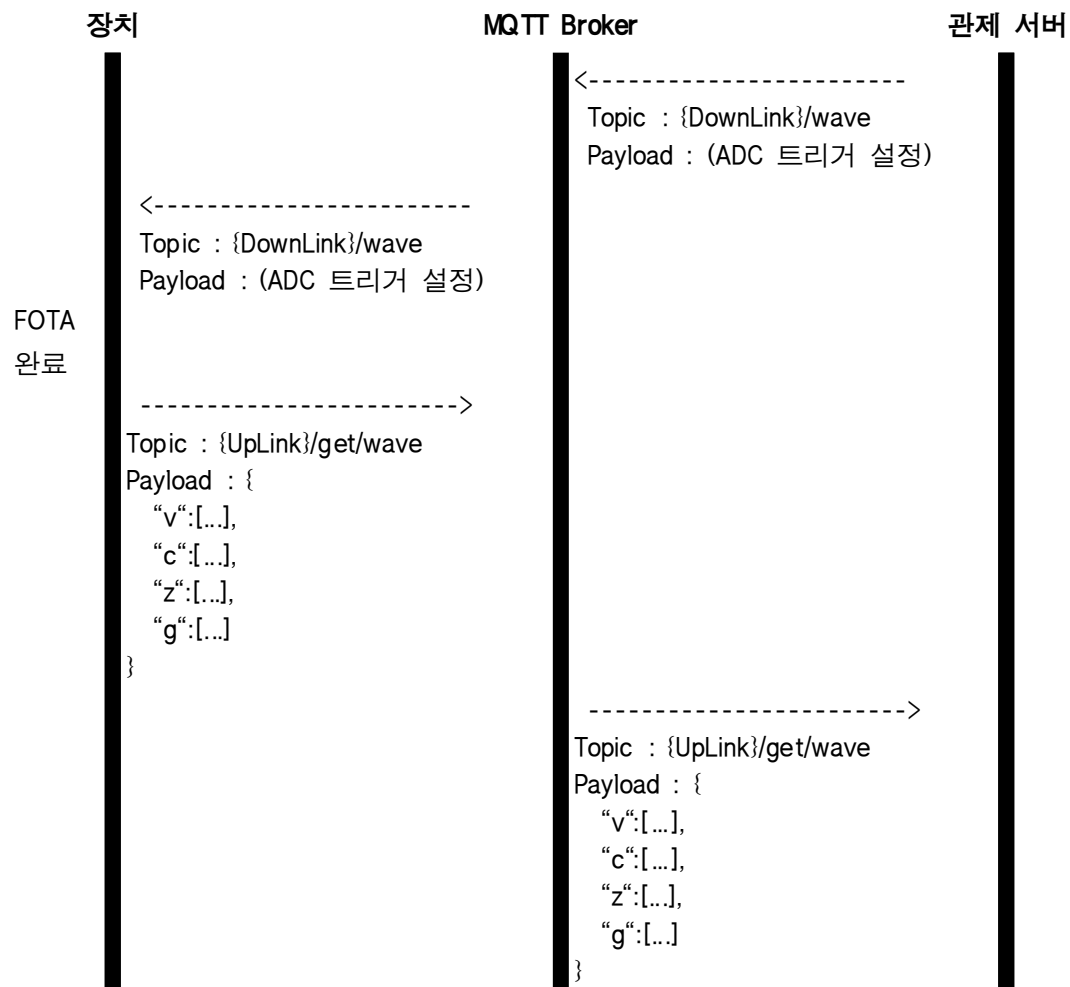
전송 받은 파일은 한국전기안전공사에서 알려 줄 암호 알고리즘과 압축 알고리즘, PSK를 통해 블록 암호화 및 압축되어있음

따라서 원격점검 장치에서 압축해제 후 복호화 해서 (save to) 경로에 저장하고 CRC 검증 결과를 응답 메시지로 서버에 전송해야 함

{{설정된 주기메시지 주기} + 60} 초 안에 서버로 FOTA 응답 메시지가 오지 않을 경우 Fail로 간주함

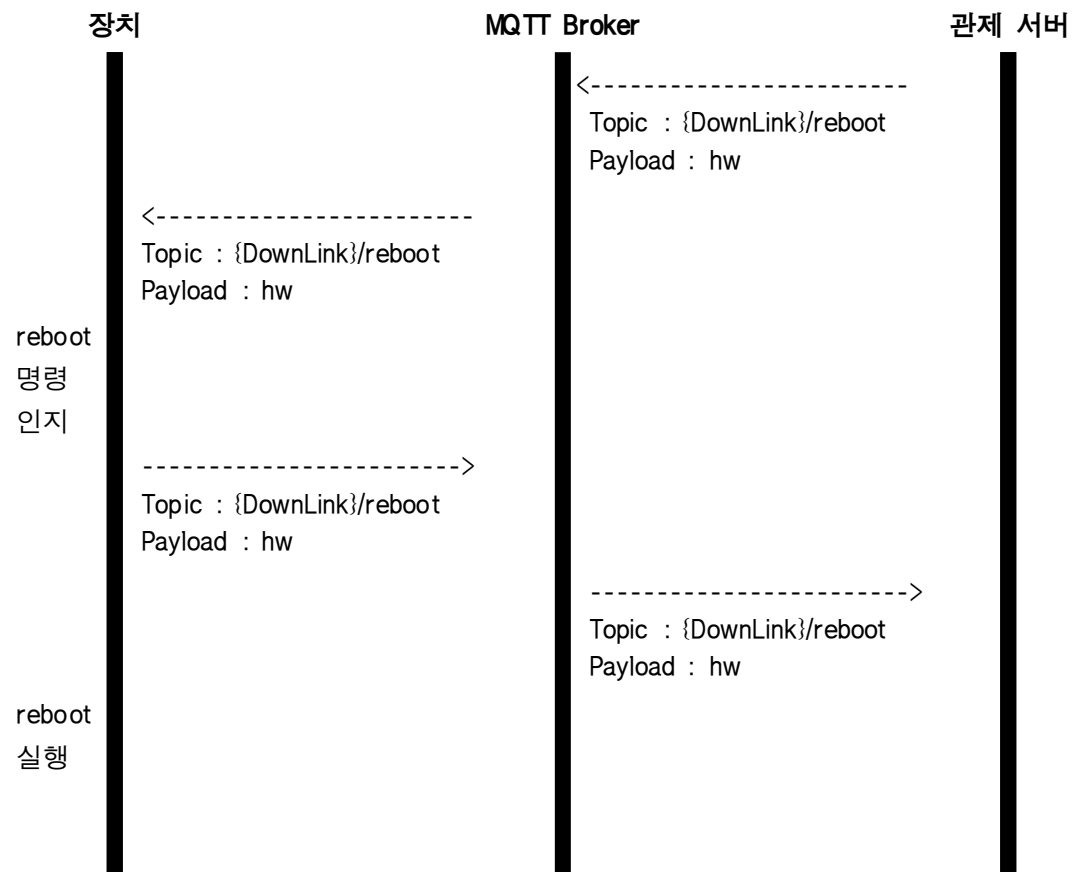
5.4. 파형정보 요청

관제시스템에서 사용자가 특정설비의 상태를 분석하기 위해 파형정보를 요청할 수 있음. 이때 트리거 조건을 설정하여 특정 채널의 파형만을 얻을 수도 있고, ADC 속도를 빠르게 조정하여 더 상세한 파형을 취득하거나 느리게 조정하여 전체적인 파형 추이를 볼 수 있음



5.5. 재시작

관제시스템에서 원격으로 장치를 재시작 할 수 있어야 함
요청 메시지에 따라 하드웨어 리셋 또는 소프트웨어 리셋이 수행 됨



5.6. 파일전송

관제시스템에서 장치로 인증서, 프로그램파일을 전송할 수 있어야 함
장치에 파일시스템이 없는 경우 저장경로는 파일종류를 구분하기 위해 사용할 수 있음

장치	MQTT Broker	관제 서버
<pre> <----- Topic : {DownLink}/filedown Payload : { "sz":{"파일전체크기}, "nb":{"사이즈 1000으로 나눈 개 수}, "crc":{"합친 파일 CRC}, "to":{"저장경로} } -----> Topic : {UpLink}/filedown/0 Payload : {} <----- Topic : {DownLink}/filedown/0 Payload : {Binay datas [최대길이 1000]} ... -----> Topic : {UpLink}/filedown/20 Payload : {} <----- Topic : {DownLink}/filedown/20 Payload : {Binay datas [최대길이 1000]} -----> Topic : {UpLink}/filedown Payload : { "result" : 0 } </pre>	<pre> <----- Topic : {DownLink}/filedown Payload : { "sz":{"파일전체크기}, "nb":{"사이즈 1000으로 나눈 개 수}, "crc":{"합친 파일 CRC}, "to":{"저장경로} } -----> Topic : {UpLink}/filedown/0 Payload : {} <----- Topic : {DownLink}/filedown/0 Payload : {Binay datas [최대길이 1000]} ... -----> Topic : {UpLink}/filedown/20 Payload : {} <----- Topic : {DownLink}/filedown/20 Payload : {Binay datas [최대길이 1000]} -----> Topic : {UpLink}/filedown Payload : { "result" : 0 } </pre>	<p>순차적 전송</p> <p>파일 전송 완료</p>

6. 긴급제어 메시지

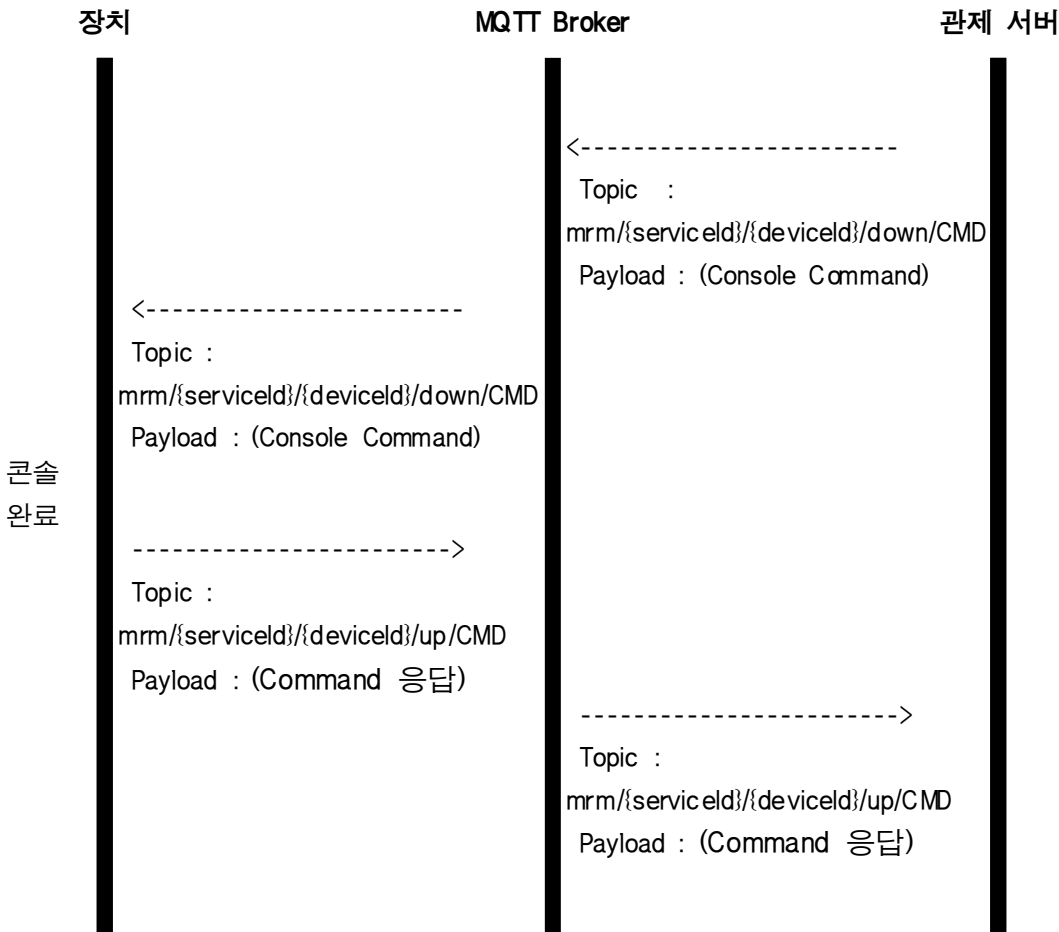
장치에서 메시지가 오지 않거나 제어메시지를 보내도 응답이 없는 상황일 경우 긴급제어 메시지를 통해 상태를 복구 할 수 있음. 긴급제어 메시지에 는 시스템 콘솔과 AT Command가 있음

[표4] 긴급 메시지

이름	설명	메시지 구조
시스템 콘솔	내부 시스템 콘솔	<p>[요청] Topic : mrm/{serviceld}/{deviceld}/down/CMD Payload : (Console Command)</p> <p>[응답] Topic : mrm/{serviceld}/{deviceld}/up/CMD Payload : (Command 응답)</p>
AT Command	통신모듈 직접 제어명령	<p>[요청] Topic : mrm/{serviceld}/{deviceld}/down/AT Payload : (AT Command)</p> <p>[응답] Topic : mrm/{serviceld}/{deviceld}/up/AT Payload : (AT Command 응답)</p>

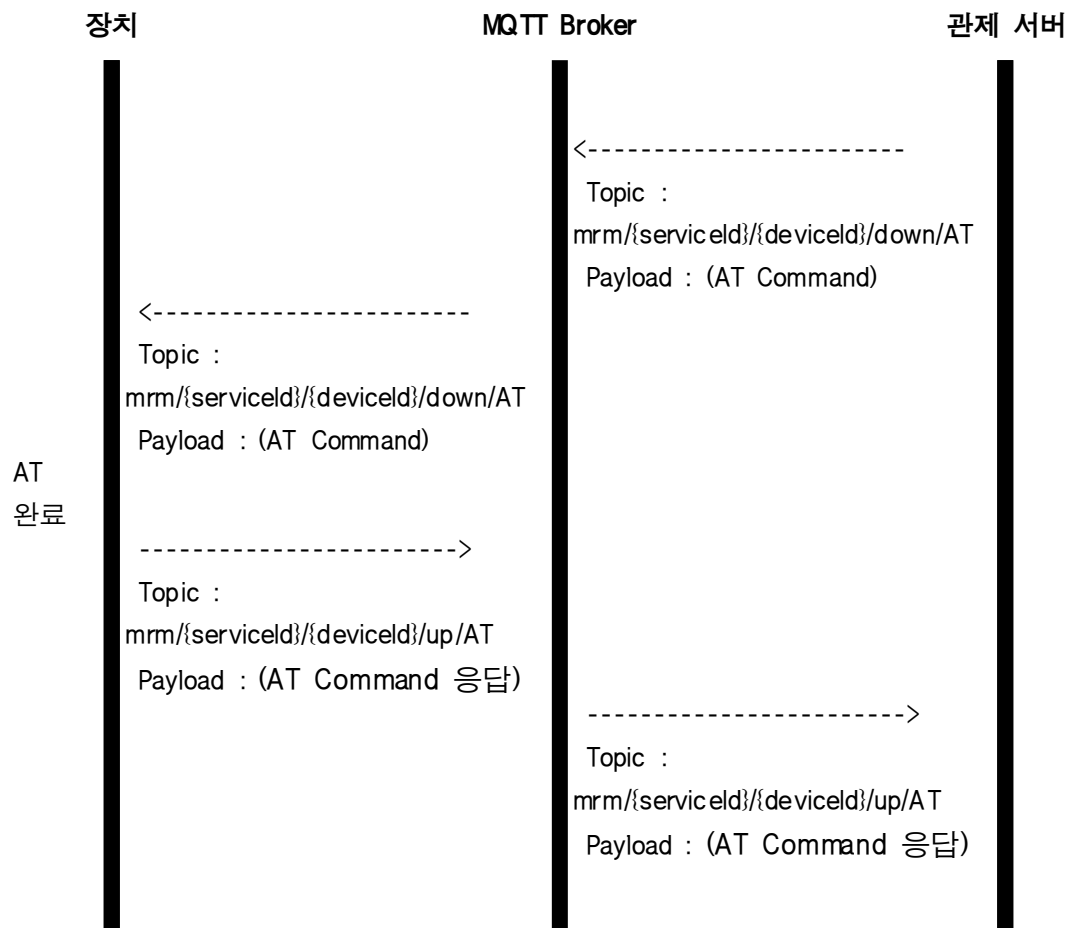
6.1. 시스템 콘솔

장치 내부 OS에 접근하여 기초적인 명령을 내릴 수 있는 시스템 콘솔에 접근하여 관제서버에서 메시지를 보내고 이에 대한 응답을 받을 수 있음



6.2. AT Command

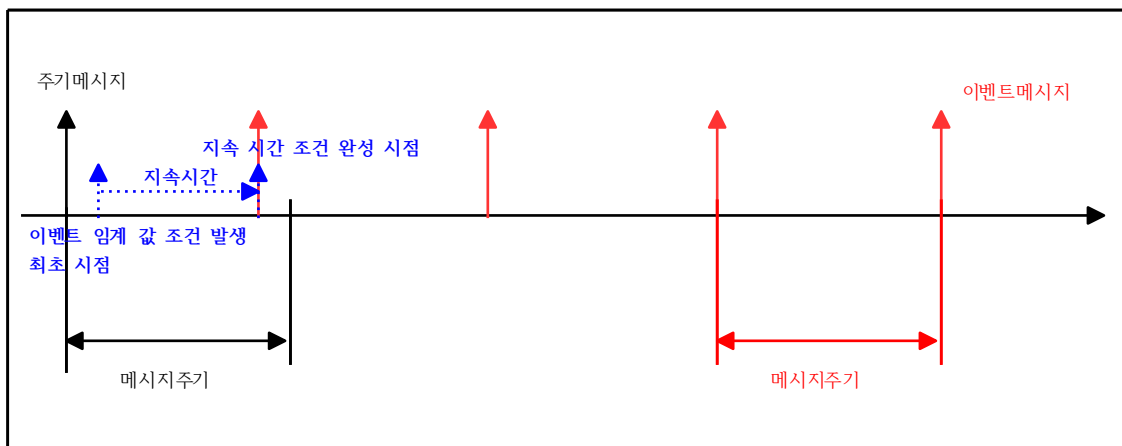
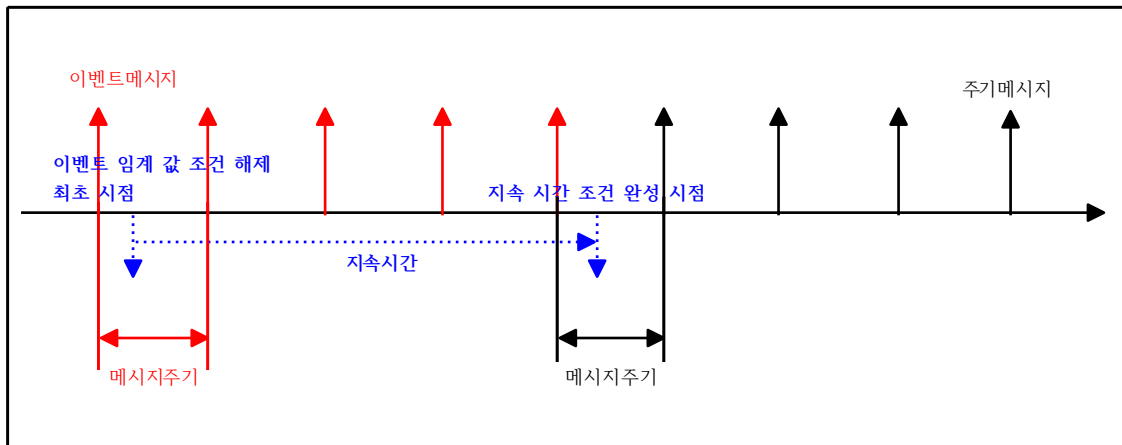
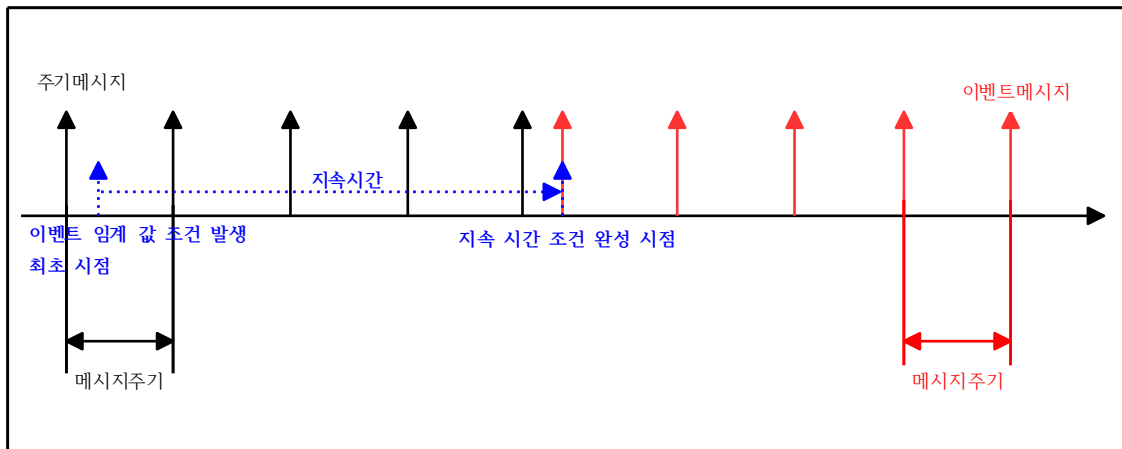
장치에서 사용하는 통신모듈이 AT Command를 지원한다면 이 메시지 형식을 갖추어서 AT Command를 실행하고 이에 대한 응답을 받을 수 있음



[별첨 1] 이벤트 조건 설정 기본 값

```
(이벤트 메시지 설정 값) = [  
  {  
    "n" : "data/v/c" ,  
    "l" : 207,  
    "t" : "5m"  
  },  
  {  
    "n" : "data/v/c" ,  
    "h" : 233,  
    "t" : "5m"  
  },  
  {  
    "n" : "data/v/c" ,  
    "h" : 190,  
    "t" : "5s"  
  },  
  {  
    "n" : "data/c/c" ,  
    "h" : 43,  
    "t" : "1h"  
  },  
  {  
    "n" : "data/z/x" ,  
    "h" : 10,  
    "t" : "5m"  
  },  
  {  
    "n" : "data/z/c" ,  
    "h" : 20,  
    "t" : "5m"  
  },  
  {  
    "n" : "data/t/c" ,  
    "h" : 80,  
    "t" : "5s"  
  }  
]
```

[별첨 2] 이벤트 메시지 발생 방법



* 지속시간 : 이벤트 임계 값 조건이 연속적으로 발생한 시간을 말 함

[별첨 3] 보안 규격

(a) 적용범위

- ① 보안 규격의 범위는 SSL로 보호되는 통신장비의 SSL library에 대한 운영모드와 사용방법을 지정하는데 있음
- ② SSL 클라이언트와 서버는 사용하고 있는 보안 모듈과 관계없이 본 규격서에서 제시한 암호 알고리즘을 통해 연동되어야 함
- ③ 원격점검장치와 전기안전공사 서버 간 통신에서 인터넷 또는 무선 통신을 이용할 경우 반드시 이 규격을 적용해야 함
- ④ Point-to-point 방식 모뎀을 사용하는 유선 폐쇄망에서는 이 규격을 적용하지 않음
- ⑤ 타시스템과 연계 또는 확장되는 형태로 원격점검장치가 타시스템을 경유하여 통신하는 경우에도 이 규격을 적용해야 함
- ⑥ 같은 장비 안에서 근거리 유선통신시에는 선택적으로 이 규격을 준용할 수 있음

(b) 운영기준

- ① 원격점검장치와 전기안전공사 서버 간 정보시스템을 신설 또는 개선하는 모든 공사에서는 이 보안 규격을 적용한 후 CC인증을 득한 통신 장비를 사용해야 하며, 보안적합성심사를 받아야 함
- ② 이 보안 규격에 따라 제조된 장비는 설치 또는 운영 전에 전문기관으로부터 이 규격에 따른 보안장비 호환성 검사를 받아야 함

(c) 요구사항

- ① 인증, 기밀성과 무결성 보호, 접근제어, 종단 보안 제어, 침입탐지가 되어야 함
- ② SSL 터널이 형성된 후 터널로 송/수신되는 데이터는 TLS 프로토콜의 보안에 의존하며, 이를 위해 SSL 서버, 클라이언트는 SSL 세션동안 사용할 보안 설정을 협상함
- ③ TLS는 1.2버전 이상이어야 하며, 서버와 클라이언트 사이에 암호화방법, 인증방법과 같은 보안설정을 협상할 수 있어야 함
- ④ 원격점검장치의 사용 IP 제한 등 방화벽 정책을 적용할 수 있어야 함

(d) 인증서 관리

- ① 원격점검장치와 서버간 상호인증을 위한 인증서는 신뢰할 수 있는 별도의 인증기관에서 발급된 인증서를 사용할 수 있어야 함. 따라서 인증서 주입 절차가 필요함
- ② 테스트나 인증서 업데이트를 위해 별도의 인증서를 주입할 수 있어야 함
- ③ 원격점검장치 내부에 저장된 개인키(Private Key)에 정보보안상 허용되지 않은 제 3자가 접근할 수 없도록 함

(e) 암호알고리즘

[표 6-1]와 같이 암호알고리즘을 사용 할 수 있어야 하고 [표 6-2]와 같은 Cipher Suite를 갖출 것

[표 6-1] 사용 암호알고리즘 목록

구분	형 식	설 명	관 련 표 준
블록 암호	ARIA	Data Channel 암호화 방식	KS X 1213-1 128비트 블록 암호 알고리즘 ARIA-제1부 : 일반 (2009) KS X 1213-1 128비트 블록 암호 알고리즘 ARIA-제2부 : 운영모드 (2014) IETF RFC 5794, A Description of the ARIA Encryption Algorithm (2010)
	LEA	Data Channel 암호화 방식	TTAK.KO-12.0223 128비트 블록 암호 알고리즘 LEA (2013) TTAK.KO-12.0246 128비트 블록 암호 LEA 운영모드 (2014)
암호 키 길이	256 bit	암호화키 길이	
운영 모드	CBC	기밀성(블록암호)	KS X 1213-2 128비트 블록암호 알고리즘 ARIA-제2부:운영모드 (2014) TTAS.KO-12.0025 블록암호알고리즘 SEED의 운영모드 (2003) TTAK.KO-12.0246 128비트 블록 암호 LEA 운영모드 (2014)
	GCM	기밀성/인증(블록암호)	TTAS.KO-12,0131 기밀성과 메시지 인증을 제공하는 128비트 블록암호알고리즘 운영모드 (2010)
해시 함수	SHA384	무결성 보장	ISO/IEC 10118-3 Information technology - Security techniques - Hash-functions
키 교환	ECDH	NIST-P256 또는 P224 curve	ANSI X9.63
전자 서명	ECDSA	NIST-P256 또는 P224 curve	ISO/IEC 14888-3 Information technology - Security techniques - Digital signatures with appendix, Part 3 : Discrete algorithm based mechanisms (2006) TTAS.KO-12.0001/R1 부가형 전자서명 방식 표준, 제2부 : 인증서 기반 전자서명 알고리즘 (2000) TTAS.KO-12.0015 부가형 전자서명 방식 표준, 제3부 : 타원곡선을 이용한 인증서 기반 전자서명 알고리즘 (2001) NIST FIPS 186-3 Digital Signature Standard (DSS)

[표 6-2] Cipher Suites

순번	Cipher Suite 이름
1	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384
2	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384
3	TLS_ECDH_ECDSA_WITH_LEA_256_CBC_SHA384
4	TLS_ECDH_ECDSA_WITH_LEA_256_GCM_SHA384
5	TLS_RSA_WITH_ARIA_256_CBC_SHA384
6	TLS_RSA_WITH_ARIA_256_GCM_SHA384
7	TLS_RSA_WITH_LEA_256_CBC_SHA384
8	TLS_RSA_WITH_LEA_256_GCM_SHA384

* TLS_키교환(Kx)_전자서명(Au)_WITH_블록암호(Enc)_해시함수(Mac)

[별첨 4] 참고자료 : 산출식 예제 (Octave)

main.m

```
close all;
clear all;
clc;
adc_samples = 200; # 1주기당 ADC 샘플개수
n = 1:1:200;
f = 60; # 60Hz
# 검증용 실험 조건 1
R_ins = 10^6; # 절연저항 1 Mohm
C_ins = 0; # 정전용량 0 F
# 검증용 실험 데이터 생성
adc_V = 220*sqrt(2)*sin(2*pi/adc_samples * n); # 220V 일 때 전압 ADC 측정 값 *
이득 값
dVdt = 220*sqrt(2)*2*pi*f/adc_samples*cos(2*pi/adc_samples * n); # 전압 미분 값
adc_Z = adc_V/R_ins + dVdt * C_ins;
figure(1);
subplot(3,1,1);
plot(adc_V);
subplot(3,1,2);
plot(dVdt);
subplot(3,1,3);
plot(adc_Z);
# 기본파 산출방법
[Vx, Vy] = separateFreq(1, adc_V, adc_samples); # 전압 벡터
[Zx, Zy] = separateFreq(1, adc_Z, adc_samples); # 누설전류 벡터
# Vx가 220이 나왔는지 확인
# Zx가 0.00022가 나왔는지 확인
# 검증용 실험 조건 2
R_ins = 500*10^3; # 절연저항 500 kohm
C_ins = 10*10^-9; # 정전용량 10 nF
# 검증용 실험 데이터 생성
adc_V = 220*sqrt(2)*sin(2*pi/adc_samples * (n + 80)); # 220V 일 때 전압 ADC 측
정 값 * 이득 값
dVdt = 220*sqrt(2)*2*pi*f/adc_samples*cos(2*pi/adc_samples * (n + 80)); # 전압
미분 값
adc_Z = adc_V/R_ins + dVdt * C_ins;
figure(2);
subplot(3,1,1);
plot(adc_V);
subplot(3,1,2);
plot(dVdt);
subplot(3,1,3);
plot(adc_Z);
# n 고조파 산출방법
```

```

Vx_hd0 = 1:11;
Vy_hd0 = 1:11;
Zx_hd0 = 1:11;
Zy_hd0 = 1:11;
for i=1:1:11
    [Vx_hd0(i), Vy_hd0(i)] = separateFreq(i, adc_V, adc_samples); # 계산한 전압 벡터
    [Zx_hd0(i), Zy_hd0(i)] = separateFreq(i, adc_Z, adc_samples); # 계산한 전압 벡터
end
# 전압 벡터(기본파)가 기준이 되도록(X 좌표 축으로 이동되도록) 좌표 변환하기
Vx_hd1 = 1:11;
Vy_hd1 = 1:11;
Zx_hd1 = 1:11;
Zy_hd1 = 1:11;
Xref = Vx_hd0(1);
Yref = Vy_hd0(1);
for i=1:1:11
    [Vx_hd1(i), Vy_hd1(i)] = transformationVector(Vx_hd0(i),Vy_hd0(i),Xref,Yref); #
    [Zx_hd1(i), Zy_hd1(i)] = transformationVector(Zx_hd0(i),Zy_hd0(i),Xref,Yref); #
end

```

separateFreq.m

```

function [A,B] = separateFreq(nth,data,oneCycleLen)
    A = 0;
    B = 0;
    for i=1:1:oneCycleLen
        A = A + data(i)*sin(2*pi/oneCycleLen*nth*i);
        B = B + data(i)*cos(2*pi/oneCycleLen*nth*i);
    endfor
    A = A * sqrt(2)/oneCycleLen;
    B = B * sqrt(2)/oneCycleLen;
endfunction

```

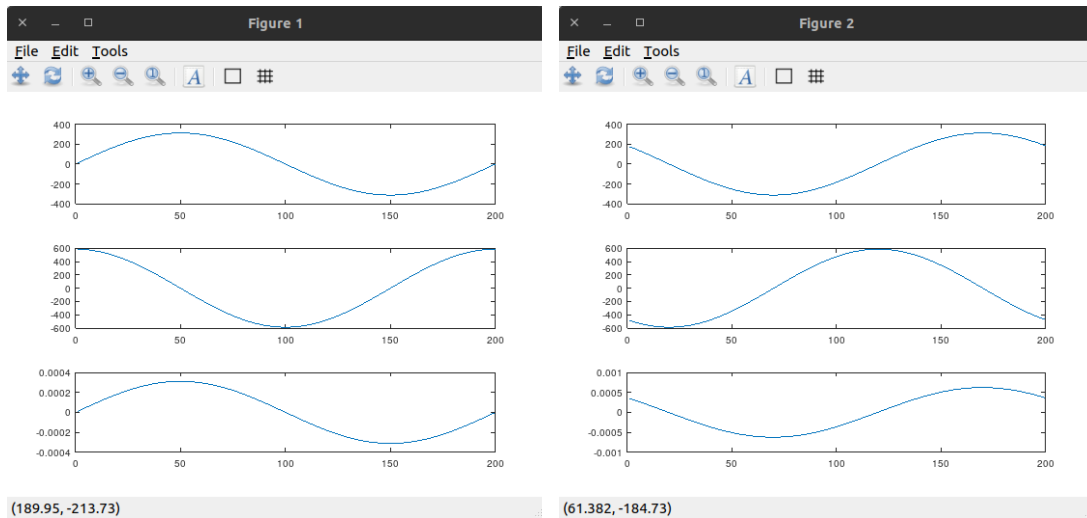
transformationVector.m

```

function [Xr,Yr] = transformationVector(X0,Y0,Xref,Yref)
    Vref = sqrt(Xref^2 + Yref^2);
    Xr = (X0*Xref + Y0*Yref)/Vref;
    Yr = (Y0*Xref - X0*Yref)/Vref;
endfunction

```

* 실행결과



Name	Class	Dimension	Value
C_ins	double	1x1	1.0000e-08
R_ins	double	1x1	500000
Vx	double	1x1	220.00
Vx_hd0	double	1x11	[-177.98, -2.1687e-14, -8.3610e-15, -1.1896e-14, 1.5063...
Vx_hd1	double	1x11	[220.28885e-14, 1.2907e-14, 1.2459e-14, -2.8724e-15, ...
Vy	double	1x1	-3.7925e-14
Vy_hd0	double	1x11	[129.31, 1.9293e-14, 1.0451e-14, 4.8233e-15, -2.8136e-...
Vy_hd1	double	1x11	[0, -2.8614e-15, -3.5402e-15, 3.0904e-15, 1.3909e-15, -...
Xref	double	1x1	-177.98
Yref	double	1x1	129.31
Zx	double	1x1	2.2000e-04
Zx_hd0	double	1x11	[-3.5840e-04, -2.6903e-20, 3.6169e-20, -2.0600e-20, -4....
Zx_hd1	double	1x11	[4.4000e-04, 4.8126e-20, -1.6869e-20, 2.5002e-20, -2.4...
Zy	double	1x1	-1.6493e-20
Zy_hd0	double	1x11	[2.5527e-04, 4.4849e-20, 2.1083e-20, 1.4183e-20, -6.89...
Zy_hd1	double	1x11	[4.1469e-06, -2.0470e-20, -3.8316e-20, 6.3408e-22, 8.3...
adc_V	double	1x200	[174.88, 166.71, 158.38, 149.89, 141.25, 132.47, 123.56...
adc_Z	double	1x200	[3.4491e-04, 3.2847e-04, 3.1171e-04, 2.9463e-04, 2.77...
adc_samples	double	1x1	200
dVdt	double	1x200	[-485.05, -495.17, -504.79, -513.92, -522.54, -530.65, -53...
f	double	1x1	60
i	double	1x1	11
n	double	1x200	1:200