



# 화재수신기 Network과 통신Network 접속시 데이터 전송에 관한 연구

백 동현 · 류 근호\* · 신 승철\*\*

가천대학교 환경·디자인대학원 소방방재공학과, 한국화재보험협회

## A Study of Connection Data transmission to the Firereciver Network and Telecommunication Network

Dong Hyun Baek · Keun Ho Ryu· Seung-Chul Shin\*\*

Gachon Univeristy Graduate school of Environment&Design

Dept of Fire&Disaster Protection Engineering\*, Korean Fire Protection Association\*\*

### 요 약

신호처리원과 그 방식은 네트워크 구성시 매우 중요하다. 따라서 대단위단지에서 많이 적용되고 있는 자동화재탐지설비의 화재수신기 네트워크와 통신네트워크에 접속시와 수신기에서 발생하는 통신 데이터를 일반 통신네트워크에 접속하여 발생하는 데이터전송시 문제점에 대하여 고찰한 것이다. 경보설비의 구성에서 중계기와 수신기간의 통신 형태를 측정하여 보편화된 통신방식을 사용하였다는 것을 알 수 있었으며 수신기에서 통신네트워크간의 연결은 수신기의 Ethernet 통신모듈을 통한 프로토콜 형태를 확인하였다.

### 1. 서 론

경보설비에는 감지기로 시작하여 중계기, 연동반, R형 또는 P형 수신반으로 연결되고 중앙의 주 장비로 연결되는 네트워크를 구성한다. 각 감지기, 수신반등의 통신연결은 중계기, 수신반 등이 정해져 연결되어 있고 수신기 네트워크와 통신 네트워크간의 접속장치를 통하여 특정 통신 규약에 의한 연결이 가능하다. 그러나 경보설비의 네트워크와 통신 네트워크 간의 접속에 따른 데이터전송의 경우 각각의 통신방식과 원천 리소스의 개방 불가로 서로간의 접속이 어렵다. 따라서 임의의 다른 접속장치를 설치하여 이를 통한 각종 데이터 값을 모니터링 하는 수준에서 마무리되는 것이 현재의 단계이다.

그러므로 경보설비네트워크의 기본 연결고리가 되는 수신기와 통신네트워크 간의 접속에 대하여 각각의 통신방식과 연결의 가능성과 수신기의 입·출력 데이터 전송 상태를 확인하고 이 데이터가 통신네트워크에 접속되어 전달되는지를 알고자 한다. 아울러 수신기에서 발생하는 통신 데이터를 일반 통신네트워크에 접속하여 발생하는 데이터전송의 문제점에 대하여 고찰하고자 한다.

### 2. 통신방식과 Network

#### 2.1 수신기통신방식

(1) 데이터 다중통신

다중화 통신의 한 방식으로 서로 떨어져 있는 다수의 컴퓨터를 하나의 고속 펄스 전송회선으로 접속하고 각 장소에 있는 변복조기(變復調器)는 펄스가 시분할된 일정 시간을 택하여 각 맥 어드레스를 펄스 부호화 즉, 디지털 부호로 변환하여 데이터와 함께 송출하며, 자기 쪽으로 오는 데이터만을 수신인 부호를 해독하여 수취하는 방식이 실현되고 있으며, 정보설비분야의 P형 또는 R형 수신기의 통신방식에 적용된다.

(2) 수신기 통신방식의 특성수신지는 각 제품 및 제조사별 방식에 따라 다르다. 그러나 기본적인 방식은 동일하므로 네트워크 구성에 문제가 없다. Table 1은 제조사별 수신기의 통신방식이다.

Table 1. Fire Receiver Signal Transmission Form in Manufacturer's

SYSTEM 항목	Z사	T 사	K사
1. 최대 회로 수	최대 34,545회로	최대입력260,096 출력260,096	최대입력260,096 출력260,096
2. 최대 LOOP	최대272LOOP	최대32LOOP*64대	최대16LOOP*32대
3. LOOP별 회로 수	LOOP당 127개 이하	LOOP당 127개 이하	LOOP당 127개 이하
4. 신호전송방식	Polling Addressing	N- NET	N-MAST Polling Addressing
5. 형식승인 및 인증	KFI	KFI	KFI / FILK

2.2 수신기Network과 통신Network의 접속

(1) 수신기와 통신Network 접속

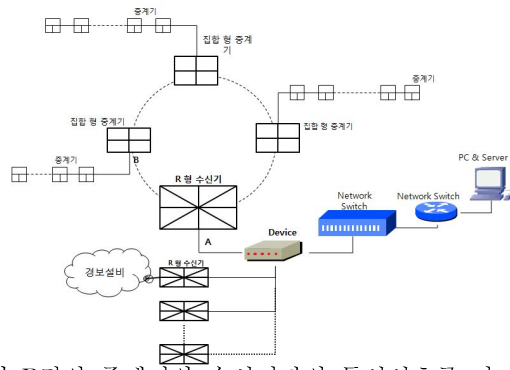
Figure 1은 수신기 네트워크와 통신네트워크간의 접속에 대한 것으로 여기에 통신네트워크의 연결 접속장치를 부착하여 수신기에서 발생하는 통신규약을 전달받아 이를 TCP/IP로 변환하여 통신네트워크에 연결된다.

수신기 Ethernet개념의 연결단자로 구성된 수신기 연결단자와 통신네트워크 접속장치에 입출력 단자를 연결한 후 상호간의 통신개통을 수행하여 연결한다. 통신네트워크에 연결하는 접속장치는 경우 256개의 중계기 연결이 가능하다. 수신기에서 발생하는 통신 패킷을 통신네트워크 연결 접속장치의 입력으로 수신하여 변환을 거쳐 TCP/IP로 전송도로를 통하여 통신 네트워크망에 전송된다. Figure 1은 수신기 네트워크와 통신네트워크간의 접속에 대한 구성을 나타낸다.

(2) 수신기 Data전달

Figure 1.은 감지기를 통하여 화재신호를 중계기에서 수신하고 이 신호를 중계기반에서 종합하여 수신기에 발신한다. 중계기반과 수신기간의 통신을 수행하고 수신에서는 중계기의 RS422 통신을 수신하여 다시 수신기의 Ethernet출력을 통하여 통신네트워크에 신호를 전달하는 수신기 네트워크와 통신네트워크 간의 연결 형태를 나타낸다.

Figure 1. Connection Datatransmission to the FireReceiver Network and Telecommunication Network Configuration.



이 때 Figure 1 에서 B점의 중계기와 수신기간의 통신신호를 나타낸 것이 Figure 2.이며, 상위 그래프는 측정된 그래프의 시간이 짧아 아래의 확대 그래프로 표현한 것이다. 그래프의 모양은 구형파를 형성하고 이를 신호로 발송하게 된다. 중계기의 신호를 받아 수신기에서 다시 Ethernet 개념의 통신을 발송하며 수신기의 Ethernet 연결단자와 통신네트워크 연결용 접속장치 입력단자를 접속하여 수신기의 신호를 TCP/IP로 변환하여 A점에서 통신네트워크에 Figure 3의 형태로 데이터를 전달한다. Figure 3은 시간에 따른 발신주소와 도착 주소간의 통신연결을 나타낸 것으로, 각각의 맥 어드레스를 지정하고 이를 통한 수신기와 통신네트워크 연결 접속장치간의 통신연결을 보여준다. Figure 2.에서 신호의 크기는 2V/DIV, 2ns/DIV, 전압폭은 5~8V, 통신속도는 19200BPS이며, YOKOGAWA(DL1720)를 사용하여 측정하였다.

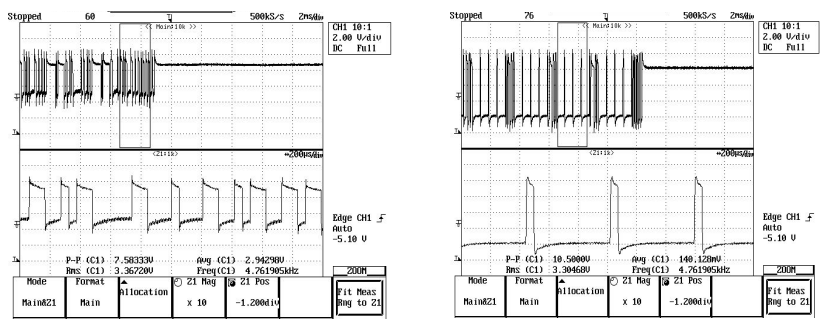


Figure 2. Connection Datatransmission to the FireReciver and FireRepeater(RX,TX)

Figure 1에서 Device는 Figure 3의 프로토콜 형태로 수신기와 통신을 하여 각각의 주소를 가지는 수신기의 데이터를 TCP/IP를 이용하여 네트워크 스위치의 라우팅 과정을 거쳐 각 필요한 서버 및 데이터베이스 장비에 저장된다. 이 저장된 데이터를 일정한 규칙과 값으로 정리하고 수치화하여 그래프 및 각종 신호, 이상 현상에 대한 표시 값으로 나타낸다. 이를 일정한 형상화된 프로그램으로 표시되어 각각의 주소별 모니터링을 하는 것이다. 이러한 과정으로 통신네트워크에서 수많은 건물, 장거리 지역의 경보설비를 모니터링하고 관리운영이 가능하다. Figure 3.은 수신기와 통신네트워크 연결용 접속장치간의 통신 프로토콜 형태를 나타낸다.

No.	Time	Source	Destination	Protocol	Length	Info
4457	597.934678	192.168.10.108	192.168.10.255	NBNS	92	Name query NB SU2.AHNLAB.COM<00>
4458	598.028727	192.168.10.108	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xd95e241c
4459	598.684367	192.168.10.108	192.168.10.255	NBNS	92	Name query NB SU2.AHNLAB.COM<00>
4460	599.079110	00:fa:01:a2:23:14	Broadcast	ARP	60	who has 192.168.10.42? Tell 192.168.10.41
4461	599.494359	192.168.10.108	192.168.10.255	NBNS	92	Name query NB SU2.AHNLAB.COM<00>
4462	599.729800	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4463	599.842822	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4464	599.959628	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4465	599.998829	00:fa:01:a2:23:14	00:db:11:11:26:04	ARP	60	who has 192.168.10.40? Tell 192.168.10.41
4466	600.069623	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4467	600.078805	00:fa:01:a2:23:14	Broadcast	ARP	60	who has 192.168.10.42? Tell 192.168.10.41
4468	600.180813	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4469	600.187653	De11_c9:f1:e3	Broadcast	ARP	42	who has 192.168.10.17? Tell 192.168.10.108
4470	600.289582	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4471	600.399573	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4472	600.509542	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4473	600.619646	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4474	600.729671	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4475	600.842562	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4476	600.998707	00:fa:01:a2:23:14	00:db:11:11:26:04	ARP	60	who has 192.168.10.40? Tell 192.168.10.41
4477	601.078699	00:fa:01:a2:23:14	Broadcast	ARP	60	who has 192.168.10.42? Tell 192.168.10.41
4478	601.998507	00:fa:01:a2:23:14	00:db:11:11:26:04	ARP	60	who has 192.168.10.40? Tell 192.168.10.41
4479	602.162333	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4480	602.279196	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4481	602.399169	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4482	602.509127	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4483	602.619236	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4484	602.729204	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4485	602.842182	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4486	602.959047	192.168.10.41	192.168.10.40	UDP	1092	Source port: 5000 Destination port: 5000
4487	603.078521	00:fa:01:a2:23:14	Broadcast	ARP	60	who has 192.168.10.40? Tell 192.168.10.41
4488	603.408459	00:fa:01:a2:23:14	Broadcast	ARP	60	who has 192.168.10.42? Tell 192.168.10.41
4489	604.078170	00:fa:01:a2:23:14	Broadcast	ARP	60	who has 192.168.10.40? Tell 192.168.10.41
4490	604.184174	De11_c9:f1:e3	Broadcast	ARP	42	who has 192.168.10.17? Tell 192.168.10.108
4491	604.408097	00:fa:01:a2:23:14	Broadcast	ARP	60	who has 192.168.10.42? Tell 192.168.10.41

# Frame 4479: 1092 bytes on wire (8736 bits), 1092 bytes captured (8736 bits) on interface 0  
 # Ethernet II, Src: 00:fa:01:a2:23:14 (00:fa:01:a2:23:14), Dst: 00:db:11:11:26:04 (00:db:11:11:26:04)  
 # Internet Protocol Version 4, Src: 192.168.10.41 (192.168.10.41), Dst: 192.168.10.40 (192.168.10.40)  
 # User Datagram Protocol, Src Port: 5000 (5000), Dst Port: 5000 (5000)  
 # Data (1092 bytes)

Figure 3. Datatransmission to the FireReciver Network and Device Protocol

### 3. 결론

수신기 네트워크와 통신네트워크간의 연결은 경보설비의 작동과 통신네트워크간의 데이터 전송이 이루어지고 있으나 현재는 문화재에만 적용된 자동화재 속도설비의 통신규정이외엔 자동화재탐지설비 및 그 외의 소화설비관련의 통신에 대해서는 정해진 통신규약이 없다. 본 연구결과와 같이 수신반의 통신은 일반화된 기준을 준수하고 있어 데이터 전송의 문제가 없는 곳으로 사료된다. 수신기의 네트워크와 통신네트워크간의 연결은 대형 인텔리전트 빌딩 또는 대단위 단지에서의 간편한 네트워크 구성과 장거리에서의 원격 모니터링이 가능하다고 할 수 있다. 앞으로 수신기 네트워크와 통신네트워크간의 접속에 따른 이상 현상에 의한 비화재보에 관련한 연구와 경보설비 네트워크 통신규약의 표준화가 필요하다.

### 참고문헌

1. 백동현, “화재신호처리공학”, 가천대학교, 미출간.(2001)
2. 오남열, “소방방재 통합시스템 구축에 관한 연구”, 경기대학교 산업정보대학원 학위논문, (2005)
3. 김은수, “수신기간 네트워크 효용성 분석에 대한 연구”, 경원대학교 대학원 석사학위논문,(2010)
4. 백동현, 강원선, “통합소방방재 시스템 구축을 위한 통합망 구현에 관한 연구”, 한국화재소방학회 춘계학술논문,(2005)
5. NFPA 101, LIFE SAFETY CODE(인명안전코드),(2007)
6. NFPA 72, NATIONAL FIRE ALARM CODE(화재경보코드),(2007)
7. PI-MBUS-300 Rev.J, Modicon Modbus Protocol Reference Guide,(1996)