

AES 256 알고리즘을 통한 수납식 관람석 통합 제어 및 모니터링 시스템 설계에 관한 연구

정진균*, 송제호**, 박의준***, 김종직****

*전북대학교 전자공학부

**전북대학교 융합기술공학부(IT응용시스템공학), 스마트 그리드 연구센터

***전북대학교 IT응용시스템공학과

****주식회사 엔시팅

e-mail:songjh@jbnu.ac.kr

A Study on the design of retractable grandstand integrated control and monitoring system through AES 256 algorithm

Jin-Gyun Chung*, Je-Ho Song**, Eui-Jun Park***, Jong-Jik Kim****

*Dept. of Electronic Engineering, Chonbuk National University

**Dept. of Convergence Technology Engineering(IT Applied System Engineering),

Smart Grid Research Center, Chonbuk National University

***Dept. of IT Applied System Engineering, Chonbuk National University

****NATIONAL SEATING Inc.

요약

수납식 관람석은 여유 공간을 확보하여 하나의 공간을 다용도로 활용할 수 있게 하지만, 현재의 시스템 상 관람석이 구성된 상태에서 구조물에 가해지는 응력을 알 수 없고, 부주의한 조작 및 해킹으로 인해 사고의 위험성이 있다. 따라서, 본 논문에서는 AES 256 알고리즘을 통한 수납식 관람석 통합 제어 및 모니터링 시스템을 제안한다. 구조물의 취약 부위를 분석하여 보완하기 위해 구조 해석을 진행하였고, 응력 데이터 측정을 위하여 응력 센싱 보드와 소형 테스트베드를 제작하여 응력 변화 데이터를 구축하였다. 또한, 보안 알고리즘과 인증 시스템을 적용하여 지정된 사용자만이 시스템에 접근할 수 있도록 하여 보안성을 향상시켰다.

작동할 경우, 관람석 위에 사람이 있다면 인명 피해가 발생할 수도 있다.

1. 서론

수납식 관람석은 최소한의 공간에 관람석을 수납한 후에 필요한 상황에 맞추어 꺼내어 사용할 수 있는 관람석 시스템을 뜻한다. 일반적으로 넓은 공간을 기반으로 조성된 대형 행사장 및 경기장의 특성상, 여유 공간이 확보된다면 추가적인 용도로 사용될 수 있으나 일반적인 관람석을 설치하게 될 경우 이러한 여유 공간의 확보가 어렵다.[1]

기존의 관람석을 수납식 관람석 시스템으로 대체할 경우, 관람석이 필요치 않은 상황에서는 관람석을 수납시켜 여유 공간을 확보할 수 있어 하나의 공간을 다용도로 활용할 수 있게 된다. 하지만, 현재의 시스템 상 수납식 관람석이 구성된 상태에서 구성품의 하중에 의해 지지대 등에 응력이 가해지지만, 변화하는 응력을 실시간으로 확인할 수 없기 때문에 대형 사고의 위험성이 존재한다. 또한, 수납식 관람석의 제어 시 사용자의 부주의한 사용이나 해킹과 같은 상황으로 관람석이

따라서, 본 논문에서는 현재의 수납식 관람석 시스템이 가지고 있는 상기의 문제를 해결하고자 AES 256 알고리즘을 통한 수납식 관람석 통합 제어 및 모니터링 시스템의 개발을 제안한다. 수납식 관람석 통합 제어 및 모니터링 시스템은 구조물과 이용자의 하중에 따라 변화하는 응력 정보를 측정하는 IoT 기반의 안전진단 모니터링 시스템을 적용하고, 구조물의 노후화, 지진, 사용 이력, 센서의 동작 여부, 모터 진단 등 수납식 관람석과 관련된 데이터를 전송받아 사고를 미리 예방할 수 있도록 하고자 한다. 또한, AES 256 기준의 보안 알고리즘을 적용하고 보안 번호 및 인증 시스템을 적용하여 외부의 침입을 차단하고 보안성을 강화하고자 한다.

2. 본론

2.1 기술의 개요

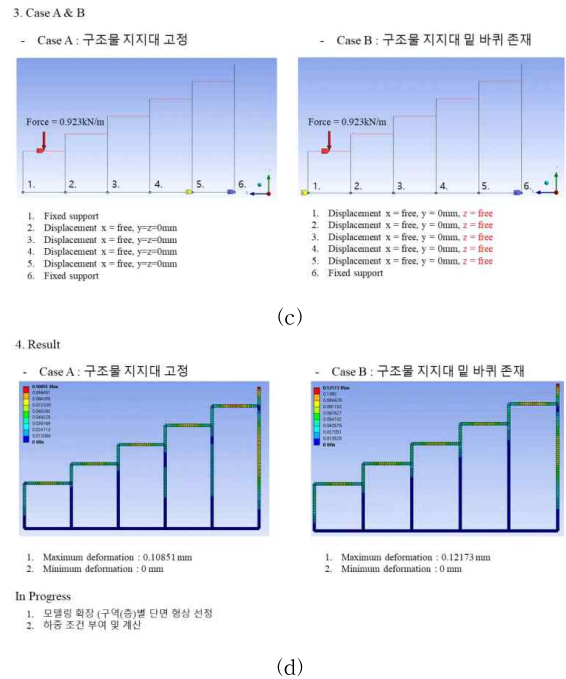
AES 256 알고리즘을 통한 수납식 관람석 통합 제어 및 모

네터링 시스템은 관람석 구조물의 응력 측정 기술을 확보하여 관람석에 관람객들이 올라간 상태에서 응력 변화 정보를 받아 관람석이 현재 안전한 상태인지 확인이 가능하게 하며, 아울러 지진계 센서, 모터 전류, 모터 온도, 적외선, 전방 센서 등의 센서 모듈을 통해 구조물의 하중과 떨림 등을 확인하여 예방 진단할 수 있도록 하여 구조물 또는 모터에 이상이 발생할 경우 동작을 중지하고 알람을 보내도록 하여 안전사고를 예방하고자 하였다.[2,3]

또한 AES 256 알고리즘을 통한 수납식 관람석 통합 제어 및 모니터링 시스템은 인터넷에 접근 가능한 환경이라면 어플리케이션을 통해 관람석 설치 장소에 있지 않더라도 원격으로 관람석의 제어가 가능하도록 하였다. 시스템에 원격으로 접속이 가능하기 때문에 수납식 관람석 제어기와 서버, 스마트폰 간에 AES 256 알고리즘을 적용하여 외부로부터의 침입을 방지하고 SMS 서버를 구축하여 보안 번호와 인증 시스템을 적용하여 보안성을 더욱 높이고자 하였다.

2.2 관람석 철골 구조물 응력 변화 데이터 구축 및 응력 변화 센싱 시스템

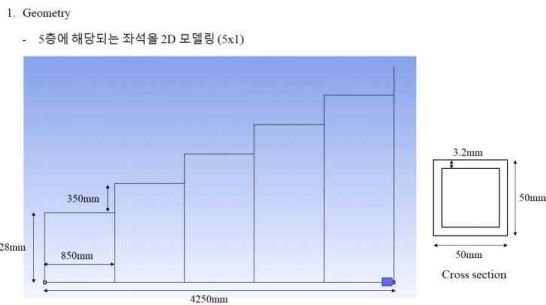
응력 변화 측정용 센싱 시스템의 개발을 위하여 관람석 구조물의 철골 구조 해석을 통해 취약 부위를 분석한 후에 이를 보완하여 안정성을 높이고, 응력 변화 측정용 센싱 보드와 소형 테스트베드를 제작하여 구조물의 동적, 정적 하중과 관람객의 몰림 정도에 따른 응력 변화 데이터를 구축하고자 하였다. 철골 구조 해석 과정과 응력 센싱 보드, 소형 테스트베드의 모습을 그림 1~3에 나타내었다.



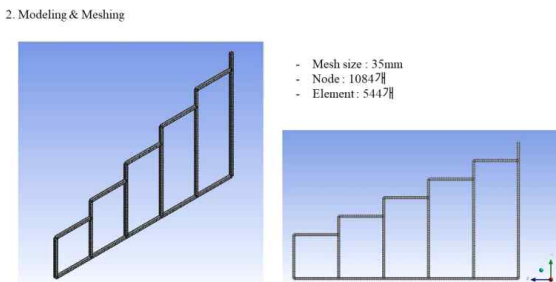
[그림 1] 철골 구조 해석 과정



[그림 2] 응력 센싱 보드



(a)



(b)



(a)

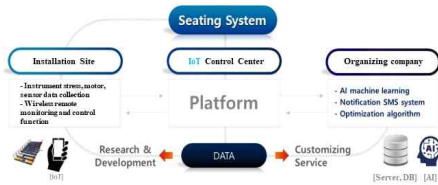


(b)

[그림 3] 소형 테스트베드

2.3 IoT 제어기 개발 및 통합 모니터링 프로그램 개발

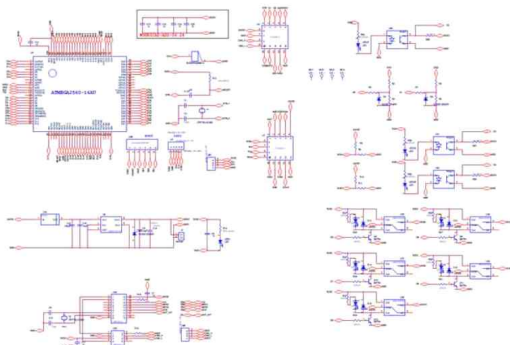
다음 그림은 IoT 통합 관제 시스템의 구성도를 나타낸 것이다.



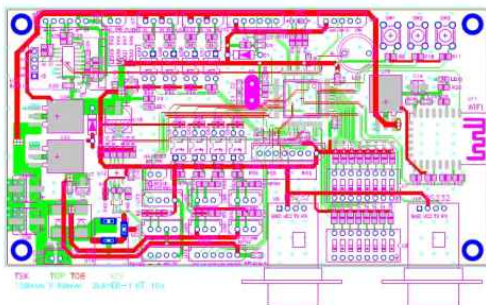
[그림 4] IoT 통합 관제 시스템 구성도

IoT 제어기는 양방향 데이터 송-수신 환경의 개발과 안정적인 통신환경 구축, 통신 프로토콜 개발을 통해 IoT 시스템을 구축하고자 하였다. 또한 응력 측정 모듈 데이터를 취득할 수 있고, 센서 회로의 입력, 처리, 디스플레이 출력 제어 기능을 갖는 전자식 컨트롤 박스 개발로 구현하고자 하였다.

WiFi(ESP-8266) 모듈을 통한 IoT 제어 보드를 개발하였고 제어기와 프로그램 간의 패킷정확도 99% 이상의 프로토콜 및 통신환경을 구현하였다. 모터 정보, 구조물의 응력 데이터, 각종 센서, AC모터 제어 기능의 펌웨어를 개발하였으며 이를 그림 5~7에 나타내었다.



[그림 5] IoT 제어기 회로 설계



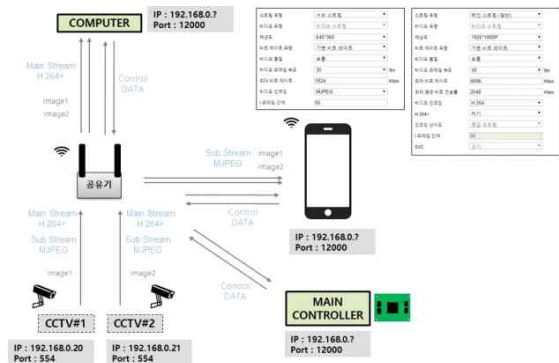
[그림 6] IoT 제어기 PCB 설계



[그림 7] IoT 제어기 PCB 제작

2.4 AES 256 알고리즘을 통한 보안 강화 통신 프로토콜 개발

수납식 관람식 시스템의 보안성을 향상시키기 위해 SMS 서버를 구축한 후에 보안 번호 및 인증 시스템을 적용하여 허가된 사용자만이 본인 인증 과정을 거쳐 시스템에 접근할 수 있도록 하였으며, 관람식 제어기와 서버, 스마트폰 간에 AES 256 보안 알고리즘을 적용하여 외부의 침입을 차단하고자 하였다. 시스템 보안 블록도와 알고리즘 일부를 그림 8과 그림 9에 나타내었다.[4,5]



[그림 8] 수납식 관람식 시스템 보안 블록도

```
Serial.println("-----<< SHA256 Setting>>-----");
//SHA256 Encrypt//
uint8_t *hash;
Sha256.init();
Sha256.print(USERID);
hash = Sha256.result();

for (int i=0; i<32; i++) {
    sha_result += "0123456789abcdef"[hash[i]>>4];
    sha_result += "0123456789abcdef"[hash[i]&0xf];
}

Serial.println(USERID);
Serial.println(sha_result);
Serial.println("SHA256 setting success...");
Serial.println("----->>>");
```

[그림 9] 알고리즘 적용

3. 결론

수납식 관람식이란 사용하지 않을 때는 관람석을 수납하였

다 필요 시에 인출하여 관람석으로 사용할 수 있는 시스템을 뜻한다. 따라서 하나의 장소에 여유 공간을 확보하여 다용도로 사용할 수 있는 장점이 존재한다.

하지만, 현재 시스템의 문제는 관람석이 구성된 상태일 때 구조물에 가해지는 응력의 변화를 알 수 없고, 수납식 관람석 제어 시 부주의한 사용이나, 해킹과 같은 침입에 의하여 의도치 않은 조작이 발생할 경우 대형 사고의 위험이 있다.

따라서, 본 논문에서는 철골 구조 해석을 통해 취약한 부위를 보완하고 수납식 관람석에 가해지는 응력 변화 데이터를 측정하여 응력 측정 센싱 보드와 소형 테스트베드를 제작하여 시험을 진행하였다.

또한 IoT 제어기의 회로와 PCB 설계와 제작을 통해 전체 IoT 통합 관제 시스템을 구현하고 보안 번호 및 인증 시스템, 제어기와 서버 간에 AES 256 보안 알고리즘을 적용하여 외부로부터의 침입을 방지하여 보안성을 높이고자 하였다.

참고문헌

- [1] 서준, “수납식관람석용 원격 인출시스템 개발에 관한 연구”, 한국정밀공학회, 2012
- [2] Norman S. Nise, “제어시스템공학”, 홍릉과학출판사, 2015
- [3] 김상진, 송병근, 오세준, “최신 자동제어”, 북스힐, 2012
- [4] 강민석, “AES 암호 알고리즘 기반 디지털 영상 보안 시스템의 설계”, 보안공학연구논문지, pp. 277-288, 2011
- [5] 오영택, 조인준, “인공지능기술의 IoT 통합보안관제를 위한 데이터모델링”, 한국콘텐츠학회논문지, pp. 57-65, 2021

본 연구는 2020년도 중소벤처기업부의 중소기업기술혁신개발사업(시장대응형) 지원에 의한 연구수행 결과물임을 밝힙니다. [과제번호 : S2983003]