정 보 보 호 학 회 지
제27권 제2호, 2017. 4

# 마이크로그리드 제어시스템의 사이버 공격 위협 및 대응 방안 분석

김 성 호*, 이 건 희*

요 약

마이크로그리드는 다양한 전력공급원과 전력부하가 존재하며, 이들을 효율적으로 관리하여 안정적인 전력 공급을 하기 위해서 다양한 센서와 제어기가 존재한다. 센서를 통해서 현재 마이크로그리드의 상태를 파악하고, 제어기를 조정하여 전력망의 상태를 안정적으로 유지한다. 이러한 마이크로그리드가 사이버 공격을 받을 경우, 정전 등의 물리적 피해가 발생할 수 있으므로 사이버 위협을 미연에 방지하기 위한 사이버 보안 대책이 필요하다. 본 고에서는 유사 제어시스템 공격 사례, 관련 기기 및 제품 취약점 정보 등을 통해 식별된 마이크로그리드 내 존재 가능한 사이버 보안 위협 요소들을 활용하여 마이크로그리드 사이버 공격 시나리오들을 식별하고, 각 시나리오 별로 존재하는 보안 위협들에 대처하기 위한 방안들을 분석한다. 이를 통해 마이크로그리드의 사이버 보안성을 강화하고 운영 안정성을 확보하고자 한다.

## Ⅰ. 서 론

마이크로그리드는 지역적으로 전력의 생산, 공급, 소비 등을 할 수 있도록 구성된 전력망으로 전통적인 전력망에 연계되어 동작할 수도 있고, 전력망과 독립적으로도 운영이 가능하다. 마이크로그리드는 전력망을 통한 전력공급이 원활하지 않을 때 독립적으로 운영하여 지역에 전력을 안정적으로 공급하므로 국가 전력망의 안정성 및 신뢰성을 제고하는데 기여할 수 있다[1]. 더불어 송전망의 손실을 최소화할 수 있고, 분산전원의 활용을 최대화 할 수 있다. 이러한 장점으로 인해 최근 대학교, 빌딩, 병원, 군부대, 도서지역 등 전력의 안정성이 요구되거나 독립적으로 전력을 운영할 필요가 있는 환경에서 마이크로그리드가 도입되고 있다.

마이크로그리드는 다양한 센서를 통해서 전력망의 현재 상황을 파악하고, 파악된 상황에 따라 전원이나 부하를 조절하여 전력 공급의 균형을 맞춤으로써 효율적이고 안정적으로 전력망을 운영할 수 있다. 하지만 이 과정에 포함된 IT기술을 무력화하는 다양한 사이버 공격을 통해서 마이크로그리드의 기능을 무력화하거나 오동작을 유발할 수 있는 위협이 존재한다[1]. 2015년 우크라이나 정전사태에서 알 수 있듯이 사이버 공격으로 정전이 발생하는 것은 더 이상 영화나 소설 속의 이야기가 아니다[2].

따라서 마이크로그리드에 대한 사이버 공격의 위협을 최소화하기 위해서 마이크로그리드 사이버 위협을 분석하고, 그에 대한 대응책을 식별할 필요가 있다. 이를 위해 본 고에서는 기존 제어시스템에 대한 공격 사례 및 제어기기에 대한 취약점 등을 분석하여, 현재 국내에 설치되고 있는 다양한 마이크로그리드 시스템에 대한 공격 시나리오를 식별한다. 더불어 식별된 공격 시나리오별로 존재하는 다양한 위협요소들에 대응하기 위한 방법을 정리하여 제공한다. 이를 통해서 향후 사이버 공격으로부터 안전한 마이크로그리드를 구축하는데 도움이 되고자 한다.

## Ⅱ. 마이크로그리드 소개

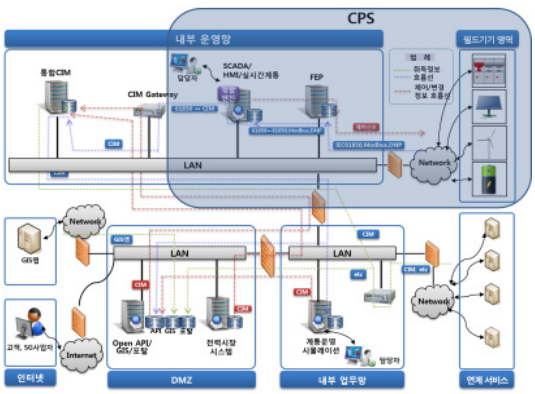
마이크로그리드에서는 분산자원이 마이크로그리드 운영시스템 또는 SCADA(Supervisory Control and Data Acquisition) 등과 연계되어 기기 상태 정보를 실시간으로 취득하고, 이를 통해서 모니터링/분석/제어 기능이 수행된다. 이를 바탕으로 마이크로그리드 시스템은 마이크로그리드의 효율적 운영을 위한 에너지 생산

본 연구는 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (No. 20141010501870)
* 국가보안기술연구소 (night12th@nsr.re.kr, icezzoco@nsr.re.kr)

관리, 부하관리, 계통분석, 설비관리 등의 기능을 수행한다. 여기서 분산자원은 전력을 생산하는 발전원과 전력을 소비하는 부하로 구성된다. 발전원의 주요 기기로는 발전기, 태양광발전(PV, PhotoVoltaic), 전기저장장치(EES, Electric Energy Storage) 등이 해당된다.

마이크로그리드는 제어와 정보 처리를 위한 시스템과, 표준 데이터 변화 엔진, 데이터 교환에 필요한 게이트웨이, 외부 정보 제공을 위한 웹 시스템 그리고 전력 비즈니스를 위한 시스템으로 구성된다.

이 중 마이크로그리드 중 CPS(cyber physical system)는 [그림 1]에 표시된 바와 같이 운영시스템을 통해서 분산자원의 정보를 취득하고, 상황에 따라 분산자원의 동작을 제어하는 등의 역할을 담당하는 구간으로 정의할 수 있다. 마이크로그리드에서 CPS는 마이크로그리드 내 전력공급에 중요한 역할을 하며, 오동작을 할 경우 마이크로그리드 내 전력공급에 차질을 유발할 수 있다. 따라서 마이크로그리드 CPS에 대한 사이버 공격에 대한 적절한 대응책을 마련하는 것은 마이크로그리드의 안정성 개선을 위한 중요한 요소 기술이다.




〔그림 1〕 마이크로그리드 운영 시스템 구성 및 마이크로그리드 내 사이버 물리 시스템 구성 설명

## Ⅲ. 마이크로그리드 공격 시나리오

마이크로그리드 공격에 대한 대응책을 식별하기 전에 마이크로그리드를 대상으로 한 현실적인 사이버 공격을 식별할 필요가 있다. 가능한 공격방법을 명확히 식별할 수 있을 때 정확한 대책을 세울 수 있기 때문이다.

이를 위해 본 고에서는 근래에 발생한 기반시설 대상의 사이버 공격 사례들을 기반으로 마이크로그리드에 대한 사이버 공격 시나리오를 개발하였다. 마이크로그리드 사이버 공격 시나리오 개발을 위해 우선 기반시설 사이버 공격 사례에서 분석된 보안위협, 보안취약점, 악성프로그램의 전파경로 및 공격방법 등을 식별하였다. 다음으로 식별된 정보 중 2장에서 명시한 마이크로그리드를 대상으로 실제 재현 가능한 보안위협, 보안취약점, 악성코드 전파경로 등을 식별하였다. 최종적으로 식별된 정보를 마이크로그리드 상에서 순차적으로 배열하여 사이버 공격 시나리오를 정의하였다. 정의된 사이버 공격 시나리오는 [표 1]과 같으며, 다음 절부터 각 시나리오의 세부 단계를 설명한다.

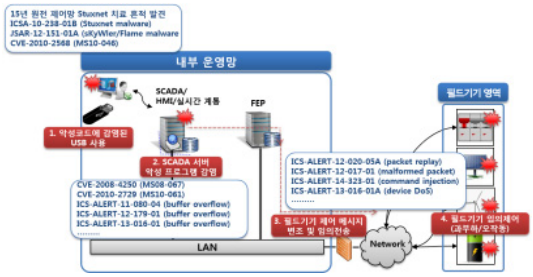
〔표 1〕 마이크로그리드 공격 시나리오

| No | 시나리오명 |
|---|---|
| 1 | 악성코드에 감염된 USB 사용 |
| 2 | 악성코드가 첨부된 이메일 열람 |
| 3 | 외부 반·출입기기에 악성코드 설치 |
| 4 | 웹사이트 악성코드 삽입 통한 악성코드 전파 |
| 5 | 인터넷 인접 기기 공격 통한 내부 침투 |
| 6 | 필드기기 물리적 접근 통한 내부 시스템 침투 |
| 7 | 필드기기 통신 취약점 이용 데이터 변조 공격 |

### 3.1. 악성코드에 감염된 USB 사용

마이크로그리드 내부자가 사용하는 저장매체를 악성코드에 감염시켜 CPS에 악성코드를 전파한 후 필드기기 불법제어 및 SCADA 시스템 장애를 유발하는 공격 시나리오다.

- ○ 1 단계 : SCADA HMI에 감염된 USB 삽입
  - 내부자가 사용하는 이동식 저장매체에 악성 코드에 감염시키고 CPS 내부망 기기 등에 삽입 시 악성코드 감염
- ○ 2 단계 : 감염된 SCADA HMI를 통한 SCADA 서버 2차 감염
  - 사전에 수집된 CPS 내부 정보 및 원격 취약점을 이용하여 내부 SCADA 서버 및 기기에 악성프로그램 원격 전파
- ○ 3 단계 : 감염된 SCADA 서버에서 조작된 기기제어 메시지 발생
  - 악성프로그램은 필드기기 제어와 관련된 비정상 행위들을 유발할 수 있도록 하는 메시지를




〔그림 2〕 악성코드에 감염된 USB를 통한 공격

발생시켜 필드기기에 무작위로 전송

○ 4 단계 : 비정상 제어 메시지 수신으로 인한 필드기기 비정상 행위 발생

- 비정상 필드기기 제어 메시지 수신에 대한 결과로 필드기기 과부하 초래 및 정상적인 SCADA 시스템 모니터링 수행 불가여기서는 소단원을 작성할 때 내용을 설명하고자 한다.

### 3.2. 악성코드가 첨부된 이메일 열람

마이크로그리드 내부 사용자에게 악성코드가 첨부된 이메일을 전송하고, 내부 사용자가 이메일을 열람하는 경우 악성코드가 전이되어 SCADA 서버 및 SCADA HMI에서 MBR 삭제 등을 수행하는 시나리오다.

○ 1 단계 : 이메일 첨부파일을 통해 악성코드가 삽입된 문서파일 전송

- 공격자는 제어망 관계자가 첨부 파일을 읽도록 유도하는 내용으로 메일을 작성하고, 악성코드가 삽입된 문서파일 첨부시킴

○ 2 단계 : 감염된 문서파일 사용으로 인한 악성코드 감염

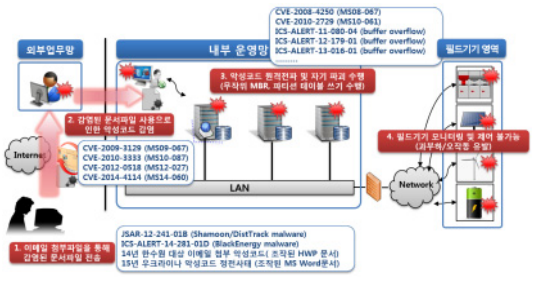
- 저장매체를 등을 이용하여 악성코드가 삽입된 문서파일이 CPS 내부로 이동된 후 내부 기기에서 문서 열람 시 악성코드 내부 감염

○ 3 단계 : 악성코드 원격전파 및 자기파괴 수행

- 원격 취약점을 이용하여 CPS 기기에 악성코드가 전파되고, 무작위 파일 쓰기 등의 자기파괴 행위가 수행되어 정상기능 방해 및 장애 유발

○ 4 단계 : SCADA 시스템 장애 발생으로 인한 필드 기기 모니터링 및 제어 불가

- 필드기기 계측 및 상태 값 처리 불능으로 인한 정상적인 시스템 모니터링 및 원격제어 기능 불가로 필드기기 과부하 및 오작동 초래




〔그림 3〕 악성코드에 감염된 이메일 열람을 통한 공격

### 3.3. 외부 반·출입기기에 악성코드 설치

마이크로그리드 내부 기기가 반출되어 협력사 내부망에 연결될 때 악성코드를 감염시키고, 마이크로그리드 기기 재반입 시 악성코드가 내부로 전파되게 하여 SCADA 서버 및 SCADA HMI에서 MBR 삭제 등 공격 행위를 수행하는 시나리오다.

○ 1 단계 : 협력사 내부망에서 외부 반출기기 악성코드 설치

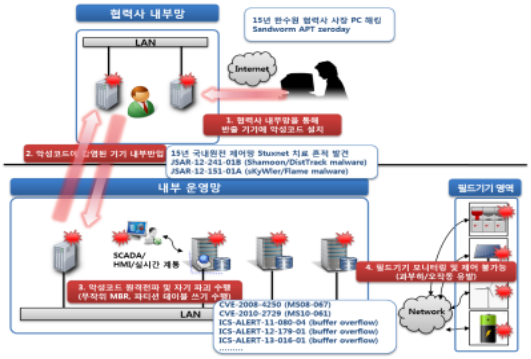
- 유지보수를 위해 외부로 반출된 CPS 기기를 원격 취약점 등을 통해 악성코드에 감염시킴

○ 2 단계 : 악성코드에 감염된 기기 내부반입

- 반출기기 내부 반입 시 보안점검 수행 없이 CPS 내부 영역에 설치

○ 3 단계 : 악성코드 원격전파 및 자기파괴 수행

- 원격 취약점을 이용하여 CPS 기기에 악성코드가 전파되고, 무작위 파일 쓰기 등의 자기파괴 행위가 수행되어 정상기능 방해 및 장애 유발




〔그림 4〕 외부 반출입 기기에 악성코드 삽입하여 마이크로그리드 침투

○ 4 단계 : SCADA 시스템 장애 발생으로 인한 필드 기기 모니터링 및 제어 불가
- 필드기기 계측 및 상태 값 처리 불능으로 인한 정상적인 시스템 모니터링 및 원격제어 기능 불가로 필드기기 과부하 및 오작동 초래

### 3.4. 웹사이트 악성코드 삽입 통한 악성코드 전파

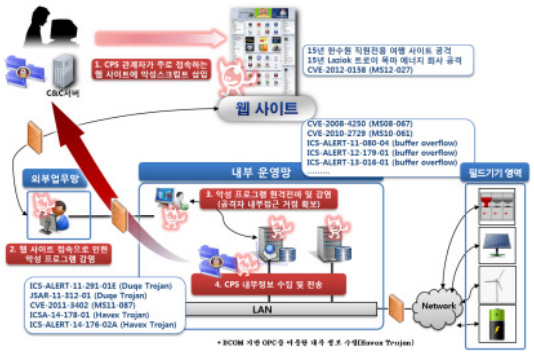
마이크로그리드 운영자가 주로 이용하는 웹사이트에 악성프로그램 설치를 유도하는 코드를 삽입하여 마이크로그리드 내부망까지 악성 프로그램 설치 및 전파 후 마이크로그리드 내부 정보수집 및 유출하는 시나리오다.

○ 1 단계 : CPS 내부 관계자가 주로 접속하는 웹 사이트에 악성스크립트 삽입
- 공격자는 CPS 내부 관계자 빈번하게 접속하는 사이트들을 조사한 후 해당 사이트 중 보안이 취약한 사이트에 악성 코드를 삽입시킴

○ 2 단계 : 웹사이트 접속으로 인한 악성 코드 감염
- 웹사이트 접속 단말들 중 일부 외부 업무망 단말에서 악성코드가 실행되고 이로 인해 트로이 목마 등과 같은 악성 프로그램에 감염

○ 3 단계 : 악성 프로그램 내부망 원격전이 및 감염
- 외부업무망의 악성 프로그램은 원격 취약점 등을 이용하여 CPS 내부 시스템에 존재하는 단말들에 악성 프로그램을 전이시킴

○ 4 단계 : CPS 내부정보 수집 및 외부전송
- 악성 프로그램은 마이크로그리드 CPS 운영상 중요 정보 및 내부 운영망에서 사용되는 장비 및 소프트웨어 정보 등을 외부로 유출




〔그림 5〕 운영자가 자주 방문하는 웹사이트에 악성코드를 삽입하여 내부로 악성코드를 전파

### 3.5. 인터넷 인접 기기 공격 통한 내부 침투

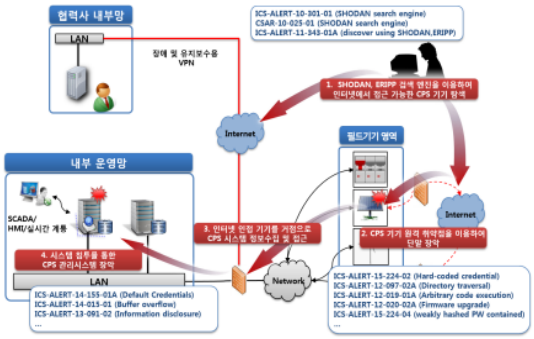
마이크로그리드 기기 중 인터넷 인접 기기들을 대상으로 접근을 시도하여 마이크로그리드 내부망까지의 접근 경로 확보 후 내부 관리 시스템 침투하는 시나리오다.

○ 1 단계 : 인터넷에 인접한 CPS 기기 탐색
- Shodan 등 특수 목적의 검색 엔진을 활용하여 대상 시스템에서 인터넷에 노출된 기기 탐색

○ 2 단계 : 원격 취약점을 이용한 기기 장악
- 인터넷 인접 기기에 원격 취약점 공격을 수행하여 단말을 장악하고, 해당 단말을 내부 침투를 위한 거점으로 활용

○ 3 단계 : CPS 시스템 영역 침투를 위한 정보 수집
- 장악된 단말에서 내부 시스템 정보들을 지속적으로 수집하여 공격 및 익스플로잇 도구 제작 등에 사용

○ 4 단계 : 침투를 통한 CPS 관리시스템 장악
- SCADA 서버 HMI 등의 원격 취약점을 이용하여 장악 후 필드기기 불법 제어를 통한 과부하, 오작동 등을 유발

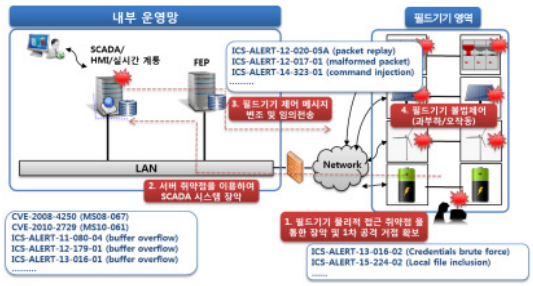



〔그림 6〕 인터넷에 연계된 기기 침투를 통한 마이크로그리드 내부 침투

### 3.6. 필드기기 물리적 접근 통한 내부 시스템 침투

필드기기에 물리적으로 접근하여 취약점 공격 수행 후 필드기기 장악을 통해 공격거점을 확보하고 이를 통해 마이크로그리드 내부 관리 시스템으로 침투하는 시나리오다.

○ 1 단계 : 필드기기 취약점을 이용하여 필드기기




〔그림 7〕 외부에 노출된 필드기기에 무단 접근하여 마이크로그리드 내부 시스템으로 침투

장악 및 공격 거점 확보

- 디버그 및 유지 보수 목적으로 존재하는 외부 인터페이스 및 로컬 취약점 정보 등 필드기기 정보를 이용하여 취약점 공격 수행

○ 2 단계 : 필드기기를 통해 SCADA 서버 접근 및 서버취약점을 이용한 시스템 장악

- 장악된 필드기기를 거점으로 활용하여 알려진 취약점 정보 및 SCADA 시스템에 대한 직접적인 취약점 분석 정보를 활용하여 관리 시스템 장악

○ 3 단계 : 감염된 SCADA 서버에서 의도치 않은 기기제어 메시지 전송

- 장악된 관리 시스템 기기에서 필드기기 제어와 관련된 비정상 행위를 유발할 수 있는 기기 제어 메시지를 필드기기들에 무작위로 전송

○ 4 단계 : 비정상 제어 메시지 수신으로 인한 필드기기 비정상 행위 발생

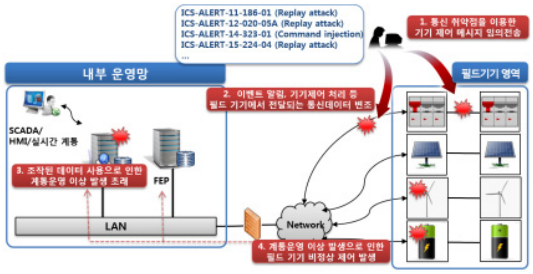
- 비정상 필드기기 제어 메시지 수신에 대한 결과로 필드기기 과부하 초래 및 정상적인 SCADA 시스템 모니터링 수행 불가

### 3.7. 필드기기 통신 취약점 이용 데이터 변조 공격

필드기기들에서 전송되는 통신 및 네트워크 데이터들을 분석하여 기기 제어 메시지를 임의로 전송하거나 필드기기 상태 정보를 변조하여 계통운영 모니터링 및 제어를 방해하는 시나리오다.

○ 1 단계 : 필드기기 통신 취약점을 이용한 필드기기 임의 제어

- 필드기기 대상 통신 취약점 노출로 인해 기기 제어가 임의로 가능하여 공격자는 이를 악용해




〔그림 8〕 필드기기의 통신모듈 및 프로토콜 취약점을 이용한 데이터 변조 공격을 통한 모니터링 및 제어 방해

임의의 기기제어 메시지 전송

○ 2 단계 : 필드기기에서 관리 시스템으로 전달되는 통신 데이터 변조

- 기기에서 주기적으로 전달되는 데이터 값을 공격자가 임의로 전송하여 비정상 데이터들이 계통운영 정보로 활용되게 유도함

○ 3 단계 : 변조 데이터로 인한 마이크로그리드 운영 이상 발생

- 필드기기의 비정상 데이터들의 사용 누적으로 비정상적인 마이크로그리드 운영이 발생할 가능성이 높아짐

○ 4 단계 : 계통운영 이상 발생으로 인한 필드기기 비정상 제어 발생

- 비정상 계통운용의 영향으로 필드 기기에 실제와 다른 제어 메시지가 전달되어 필드 기기 비정상 동작 발생

## Ⅳ. 마이크로그리드 사이버 공격 대응 대책

마이크로그리드 공격 시나리오들은 각각의 시나리오 개발 시 고려된 보안 위협요소들이 모두 발생 가능할 경우를 고려하여 작성되었다. 즉, 개별 공격 시나리오에서 고려된 보안 위협요소들 중 일부가 보안대책 적용으로 인해 제거될 경우 전체 시나리오의 전개는 진행되지 않을 수 있다.

그러나 개별 보안 위협요소 존재 자체가 마이크로그리드의 보안성에 영향을 미칠 수 있고, 본 고에서 다루지 않은 다른 공격으로 전개될 가능성도 있으므로 각공격 시나리오들에서 언급된 모든 보안 위협 요소들의 발생 가능성을 확인하고, 이에 대한 대응 조치를 취해야 한다.

본 고에서 정의된 마이크로그리드 CPS 사이버 공격 시나리오 상의 보안 위협요소별 보안 대책(SC, Security Countermeasure)은 [표 2]와 같으며, 각각에 대해서 다음 절에서 상세히 설명한다.

### 4.1. 시나리오1에 대한 보안대책

○ SC1 : 감염된 이동식 저장매체 사용에 관한 대책
대응목표 : 이동식 저장매체를 통해 악성코드가 내부 운영망으로 전파되는 것에 대한 차단 및 관리
- 이동식 저장매체 사용 관리
- 이동식 저장매체 사용단말 관리

○ SC2 : SCADA서버 S/W 취약점 내포에 대한 대책
대응목표 : SCADA 운영과 관련된 S/W에서 발생 가능한 보안위협을 사전 차단하거나 사후조치 시행
- 운영체제 최신 보안패치 유지
- SCADA 솔루션 취약점 진단 및 관리
  • SCADA 솔루션 도입 전 시큐어 코딩(Secure Coding) 점검 도구를 이용한 점검하며, 점검 항목은 행안부 시큐어 코딩 항목 43개, 행안부 Java 시큐어 코딩 가이드, 행안부 C 시큐어 코딩 가이드, 행안부 Android-Java 시큐어 코딩 가이드, OWASP(Open web Application Security Project) 시큐어 코딩 가이드라인 등에서 제시된 항목을 활용
  • 상용 취약점 점검 도구 및 스캐너 등을 활용하여 SCADA 솔루션을 대상으로 취약점 점검을 정기적으로 수행

○ SC3 : 필드기기 제어 메시지 변조 및 임의전송에 대한 보안대책
대응목표 : 제어메시지 구조, 데이터 노출 방지 및 출처가 불분명한 송수신 제어메시지 처리 방지
- 필드기기 제어메시지 송수신 보안 강화
  • 필드기기 제어메시지가 평문 등으로 전송되어 기밀성이 보장되지 못할 경우, 암호화 통신 등을 통해 제어메시지를 전송하여 메시지 구조가 노출되는 것을 방지
  • 암호화 채널을 통한 제어메시지 송수신이 용이하지 않을 경우, 제어메시지 페이로드(Payload) 자체를 암호화하여 송수신이 가능한 필드기기를 사용
  • 제어메시지 트래픽이 수집되어 재사용되지 못하도록 프로토콜을 구현

### 4.2. 시나리오2에 대한 보안대책

○ SC4 : 이메일 악성코드 첨부파일 열람을 통한 악성코드 감염 보안대책
대응목표 : 이메일 수신에 사용되는 단말에 대한 악성코드 감염 방지 및 관리
- 이메일 첨부파일 열람단말 보안관리
  • 이메일 첨부파일 열람단말에 백신 프로그램 설치 및 최신 버전상태 유지
  • 이메일 수신업무 등 업무 이외의 개인용 프로그램 설치 및 사용 금지
- 이메일 수신단말 통신 트래픽 관리
  • 이메일 수신단말에서 송수신되는 네트워크 트래픽에 대한 모니터링을 수행하여 악성코드 시그니처 등의 패턴 발생 시 해당 이메일 수신단말의 네트워크 트래픽을 차단하고, 해당 단말에 대한 보안검사 수행
- 이메일 사용자 보안의식 및 교육 강화

○ SC5 : 망간 자료 및 데이터 이동에 대한 보안대책
대응목표 : 망간 자료 이동으로 인한 악성코드가 내부 운영망으로 전파에 대한 차단 및 방지
- 안전한 망간 자료 및 데이터 전달
  • 망간 문서 및 자료 이동 시 트래픽 분석을 통해 악성코드 탐지 시 차단할 수 있는 망간 자료교환 시스템 구축

○ SC6 : 악성코드 원격전파에 대한 보안대책
대응목표 : SCADA 운영과 관련된 S/W에서 발생 가능한 원격 보안위협을 사전 차단하고, 공격 분석을 통한 사후조치 시행
- 불필요한 운영체제 데몬 및 서비스 비활성화
  • 운영체제 구동 시 기본으로 동작되는 서비스 및 데몬들 중 원격 포트를 개방하고 있는 서비스 및 데몬들을 식별하고, SCADA 운영에 필요하지 않는 서비스 비활성화

○ SC7 : 악성 코드로 인한 장애 발생에 대한 대책
대응목표 : 사이버 공격으로 인한 장애 대비 및

발생 시 피해 최소화
- 서버 이중화 및 중요자료 백업 시스템 구축
  • 서버 이중화 구성을 통해 서버 장애 발생 시 대체 장비를 통해 필드기기 모니터링 및 제어 기능의 연속성 유지
  • 서버 데이터의 정기적 백업을 수행하여 장애 발생 시 대체 장비에서 관련 데이터를 적재 후 즉시 사용할 수 있도록 구성
- 서버 복구 절차 및 훈련 수행
  • 사이버 보안사고 발생 시에 대한 장애복구 매뉴얼을 개발하고, 정기적 장애복구 모의훈련 수행

### 4.3. 시나리오3에 대한 보안대책

○ SC8 : 외부 협력사를 통한 악성코드 감염 대책
대응목표 : 외부 협력사 반출기기를 통해 악성코드가 내부 운영망으로 전파되는 것에 대한 차단 및 관리
- 외부 협력사 보안 관리
  • 외부 협력사 개발환경 보안실태 정기 점검 및 개발인력 보안교육 실시
- 내부기기 반입 및 반출 보안 관리
  • CPS 내부기기 반출 전 설치된 소프트웨어 및 라이브러리를 식별하고, 반입 시 해당 소프트웨어 및 라이브러리에 대한 변조 여부 확인
  • CPS 내부기기 반입 시 최신 업데이트 상태를 유지하고 있는 백신 프로그램을 사용하여 악성코드 감염여부 조사

○ 악성코드 원격전파에 대한 보안 대책(SC6) 적용
○ 악성 코드로 인한 장애 발생 대책(SC7) 적용

### 4.4. 시나리오4에 대한 보안대책

○ SC9 : 내부 사용자 대상의 취약한 웹사이트 접근 보안 대책
대응목표 : 내부 사용자의 인터넷 사용 단말에 대한 악성코드 감염 방지 및 관리
- 인터넷 사용 단말 보안 관리 강화
  • 웹 브라우저의 안전한 보안설정 기준을 세우고, 수립된 웹 브라우저 보안설정 기준을 적용할 수 있는 도구 등을 배포하여 웹 브라우저 사용 보안 강화
  • 인터넷 사용 단말을 업무망 및 제어망과 별로로 분리된 네트워크로 구성하는 등 망분리 상태로 운영
- 인터넷 사용단말 통신 트래픽 관리
  • 자료 조사 등의 업무와 연관성이 없는 인터넷 접근으로 인해 발생되는 네트워크 트래픽 차단
  • 인터넷 사용단말에서 송수신되는 네트워크 트래픽에 대한 모니터링을 수행하여 악성코드 패턴 발생 시 해당 인터넷 사용단말의 네트워크 트래픽 차단 및 해당 단말 보안검사 수행
- 인터넷 단말 사용자 보안의식 강화

○ SC10 : 내부정보 외부 유출에 대한 보안대책
대응목표 : 정보의 외부유출 차단 및 탐지환경 구축
- 망분리 및 네트워크 장비 설정을 통한 외부 유출 차단
  • 네트워크 장비에서 사전에 정의된 네트워크 흐름 이외의 트래픽은 차단하도록 설정하고, 정기적으로 네트워크 장비 점검을 수행하여 해당 설정 변동여부 확인
  • 내부 단말에서 테더링(Tethering)을 통한 인터넷 연결이 발생되지 않도록 단말에서 임의의 USB, WiFi, 블루투스 연결을 감지하고 차단
- 네트워크 트래픽 분석을 통한 데이터 유출 탐지
  • 내부에서 외부망으로의 연결 구간에서 사전 정의 되지 않은 데이터 및 트래픽(예, reverse shell) 등을 차단할 수 있도록 정보보호시스템 구축

○ 악성코드 원격전파에 대한 보안대책(SC6) 적용

### 4.5. 시나리오5에 대한 보안대책

○ SC11 : 검색 엔진을 통한 인터넷 접근 노출 탐색에 대한 보안대책
대응목표 : 인터넷 인접기기의 원격 취약점 발

생으로 인해 내부 침투 경로로 악용되는 것을 방지

- 인터넷 인접 기기의 외부노출 차단
  - Shodan,ERIPP 등의 검색 엔진을 통한 정기적 검색을 통해 CPS 인터넷 인접기기 노출 여부를 확인
- 인터넷 인접기기 원격접근에 대한 보안 강화
  - 인터넷 인접기기에서 구동 중인 데몬 및 서비스들 중 원격에서 접근 가능한 대상들 및 이를 구현하기 위해 사용된 라이브러리 등을 사전에 식별하고 관련 보안정보를 정기적으로 수집
  - 인터넷 인접기기에 대한 원격 접근 시 접근제어가 올바로 수행되는지 확인하며, 접근제어에 사용되는 중요 정보들에 대한 관리를 강화

○ 악성코드 원격전파에 대한 보안대책(SC6) 적용

### 4.6. 시나리오6에 대한 보안대책

○ SC12 : 필드기기 물리적 접근 취약점에 대한 보안대책

대응목표 : 필드기기에 대한 임의의 물리적 접근 차단 및 관리

- 필드기기에 대한 물리적 보안 및 접근관리 강화
  - 영상보안관제 시스템을 활용하여 넓은 지역에서 운용되고 있는 필드기기에 대한 접근감시 강화
  - 적외선, 레이저, 진동, 장력 센서, 모션 디텍터 등의 기기를 이용한 알림 모니터링 시스템을 활용하여 넓은 지역에서 운용되고 있는 필드기기에 대한 접근감시 강화
  - 필드기기의 물리적 인터페이스(디버그용 시리얼 포트, 디버그용 이더넷 포트)에 임의로 연결하지 못하도록 보호

○ 악성코드 원격전파에 대한 보안대책(SC6) 적용

○ 필드기기 제어 메시지 변조 및 임의전송에 대한 보안대책(SC3) 적용

### 4.7. 시나리오7에 대한 보안대책

○ SC13 : 필드기기 네트워크 접근 취약점에 대한 보안대책

대응목표 : 필드기기에서 사용되고 있는 네트워크에 대한 임의의 참여 차단 및 통신보안 강화

- 필드기기에서 사용되는 네트워크 프로토콜 보안 강화
  - 필드기기에서 사용되고 있는 유무선 통신 프로토콜(Zigbee, 시리얼, WiFi, 이더넷) 등을 사전에 식별하고 관련 보안취약점 정보를 정기적으로 수집
  - 운용되고 있는 필드기기에서 수집된 보안취약점이 존재하는지 정기적 보안점검 수행
  - 필드기기의 네트워크에 임의로 네트워크에 참여하지 못하도록 구성하고, 임의로 네트워크 참여 시도 시 알림 등을 발생할 수 있는 시스템 구축

○ 필드기기 제어 메시지 변조 및 임의전송에 대한 보안대책(SC3) 적용

## Ⅴ. 결 론

마이크로그리드 대상 사이버 보안사고 발생 시 이에 효과적으로 대응하고 피해를 최소화하기 위해 본 고에서는 이를 위해 마이크로그리드 관련 보안사고 및 보안 취약점 등을 분석하여 이에 기반을 둔 공격 시나리오를 개발하였으며, 이에 대응하기 위한 방안을 제시하였다.

최근 다양한 제어시스템을 대상으로 한 악성코드가 발견되고 있고, 실제 피해사례도 발생하고 있으므로 마이크로그리드 구축 및 운영 시 이를 고려하여 관련 보안 위협요소 및 취약점 등을 제거하여 이에 대응할 수 있어야 할 것이다.

〔표 2〕 마이크로그리드 공격 시나리오별 보안 위협요소와 각 보안위협 요소별 대응되는 대책

| No | 시나리오 | 보안 위협요소 | 대책 번호 | 대책 |
|---|---|---|---|---|
| 1 | 감염된 USB를 통한 악성코드 전파 | 감염된 이동식 저장매체 사용 | SC1 | 이동식 저장매체 사용 관리 |
| | | | | 이동식 저장매체 사용단말 관리 |
| | | SCADA서버 S/W 취약점 내포 | SC2 | 운영체제 최신 보안패치 유지 관리 |
| | | | | SCADA 솔루션 취약점 진단 및 관리 |
| | | 제어메시지 변조 및 임의 전송 가능 | SC3 | 필드기기 제어메시지 송수신 보안 강화 |
| 2 | 악성코드가 첨부된 이메일 수신을 통한 악성코드 전파 | 이메일에 첨부된 악성파일 열람 | SC4 | 이메일 첨부파일 열람단말 보안 관리 |
| | | | | 이메일 열람단말 통신 트래픽 관리 |
| | | | | 이메일 사용자 보안의식 및 교육 강화 |
| | | 임의의 망간자료 이동 | SC5 | 안전한 망간 자료 및 데이터 전달 체계 수립 |
| | | SCADA서버 S/W 원격 취약점 내포 | SC6 | 악성코드 분석을 통한 추가전파 차단 |
| | | | | 불필요한 데몬 및 서비스 비활성화 |
| | | | | 운영체제 최신 보안패치 유지 관리 |
| | | | | SCADA 솔루션 취약점 진단 및 관리 |
| | | 악성코드로 인한 장애 발생 시 대책 부재 | SC7 | 서버 이중화 및 자료 백업 시스템 구축 |
| | | | | 서버복구 절차 수립 및 복구훈련 수행 |
| 3 | 외부 반·출입 기기에 설치된 악성코드를 통한 전파 | 협력사 보안 관리 부재 | SC8 | 외부 협력사 보안실태 관리 |
| | | | | 내부기기 반입 및 반출 보안 관리 |
| | | SCADA서버 S/W 원격 취약점 내포 | SC6 | 악성코드 분석을 통한 추가전파 차단 |
| | | | | 불필요한 데몬 및 서비스 비활성화 |
| | | | | 운영체제 최신 보안패치 유지 관리 |
| | | | | SCADA 솔루션 취약점 진단 및 관리 |
| | | 악성코드로 인한 장애 발생 시 대책 부재 | SC7 | 서버 이중화 및 자료 백업 시스템 구축 |
| | | | | 서버복구 절차 수립 및 복구훈련 수행 |
| 4 | 내부자 관련 웹사이트에 악성코드 삽입을 통한 전파 | 인터넷 사용단말 취약 | SC9 | 인터넷 사용 단말 보안관리 강화 |
| | | | | 인터넷 사용단말 통신 트래픽 관리 |
| | | | | 인터넷 단말 사용자 보안의식 강화 |
| | | SCADA서버 S/W 원격 취약점 내포 | SC6 | 악성코드 분석을 통한 추가전파 차단 |
| | | | | 불필요한 데몬 및 서비스 비활성화 |
| | | | | 운영체제 최신 보안패치 유지 관리 |
| | | | | SCADA 솔루션 취약점 진단 및 관리 |
| | | 트래픽 관리 부재 | SC10 | 망분리 구성 및 네트워크 장비 설정을 통한 외부 연결 및 데이터 유출 차단 |
| | | | | 트래픽 분석을 통한 데이터 감시 강화 |
| 5 | 인터넷 인접 기기 공격을 통한 내부 침투 | 인터넷 인접 기기 인터넷 노출 무방비 | SC11 | 인터넷 인접기기의 외부노출 차단 |
| | | | | 인터넷 인접기기 원격접근에 대한 보안 강화 |
| | | SCADA서버 S/W 원격 취약점 내포 | SC6 | 악성코드 분석을 통한 추가전파 차단 |
| | | | | 불필요한 데몬 및 서비스 비활성화 |
| | | | | 운영체제 최신 보안패치 유지 관리 |
| | | | | SCADA 솔루션 취약점 진단 및 관리 |
| 6 | 필드기기 물리적 접근을 통한 내부 시스템 침투 | 필드기기 물리 접근 취약점 존재 | SC12 | 필드기기에 대한 물리적 보안 및 접근관리 강화 |
| | | SCADA서버 S/W 원격 취약점 내포 | SC6 | 악성코드 분석을 통한 추가전파 차단 |
| | | | | 불필요한 데몬 및 서비스 비활성화 |
| | | | | 운영체제 최신 보안패치 유지 관리 |
| | | | | SCADA 솔루션 취약점 진단 및 관리 |
| | | 제어메시지 변조 및 임의 전송 가능 | SC3 | 필드기기 제어메시지 송수신 보안 강화 |
| 7 | 필드기기 통신 취약점을 이용한 데이터 변조 | 필드기기 네트워크 임의 접근 및 참여 가능 | SC13 | 필드기기에서 사용되는 네트워크 프로토콜 보안 강화 |
| | | 제어메시지 변조 및 임의 전송 가능 | SC3 | 필드기기 제어메시지 송수신 보안 강화 |

## 참 고 문 헌

[1] JongBo Ahn, “Microgrid operational technology and domestic research trends”, The Korean Institue of Power Electronics, pp. 25-29. Apr. 2010

[2] Rebert M. Lee, Michael J. Assante and Tim Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid”, E-ISAC, Mar. 2016

## 〈저 자 소 개〉

사 진

**김 성 호 (Sungho Kim)**
정회원

2009년 2월 : 인하대학교 컴퓨터공학 졸업
2012년 2월 : 인하대학교 컴퓨터공학 석사
2012년 9월 ~ 현재 : 국가보안기술연구소 연구원

관심분야 : 취약점 분석, 트래픽 분석, 스마트그리드

사 진

**이 건 희 (Gunhee Lee)**
정회원

2001년 2월 : 아주대학교 정보 및 컴퓨터공학부 졸업
2003년 2월 : 아주대학교 정보통신전문대학원 석사
2009년 2월 : 아주대학교 정보통신전문대학원 박사
2009년 3월~현재 : 국가보안기술연구소 선임연구원

관심분야 : 인증 프로토콜, 접근제어, 스마트그리드