

2022 KSC

# 운영기술 네트워크에서 자산 탐색을 위한 스캐닝 도구의 한계점

단국대학교

강해인

# INDEX

01

서론

02

관련 연구

03

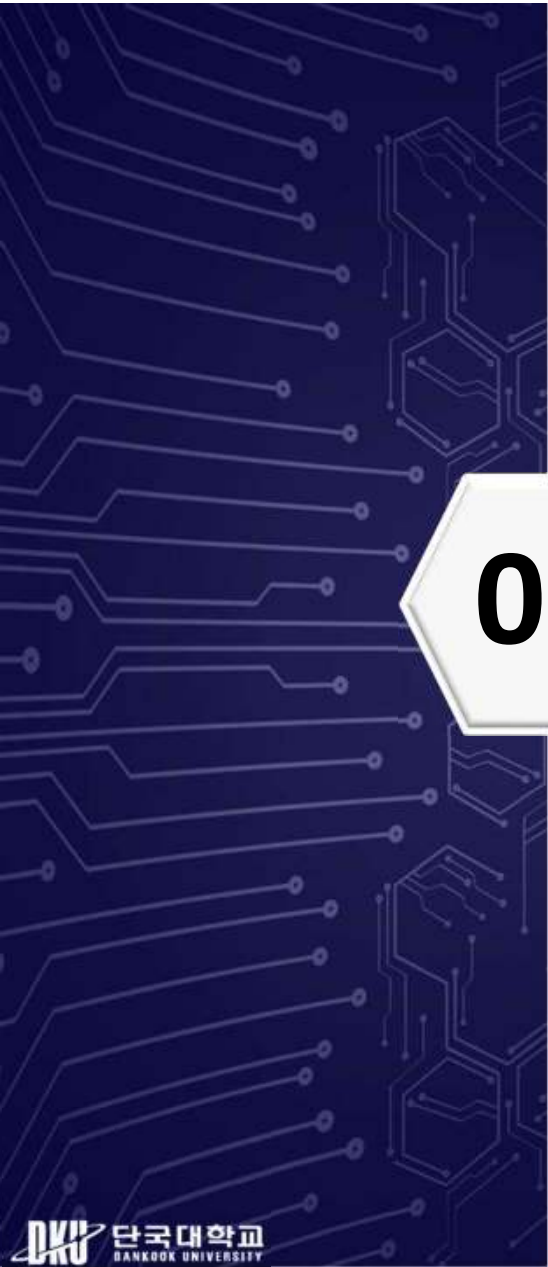
실험 환경 및 방법

04

실험 결과

05

결론 및 향후 연구



**01**

# 서론

# 서론

## ❖ OT(Operational Technology, 운영 기술)와 기술의 발전

- 하드웨어와 소프트웨어를 사용해 산업용 장비를 제어하는 방식이다.
- 실시간성(real time)이 요구되고 가용성(availability)의 보안 요소를 최우선으로 한다.
- 초기에 폐쇄적으로 운영되었지만 기술이 발전함에 따라 외부 네트워크와 연결성이 증가하였고, 동시에 공격자의 공격 표면(attack surface)도 늘어났다.
- 사이버 공격이 발생하는 경우, 인명 피해도 발생할 수 있어 공격 표면인 시스템의 자산을 식별하고 관리하여 공격에 대해 미리 예방하는 것이 중요하다.



# 서론

## ❖ 네트워크 스캐닝

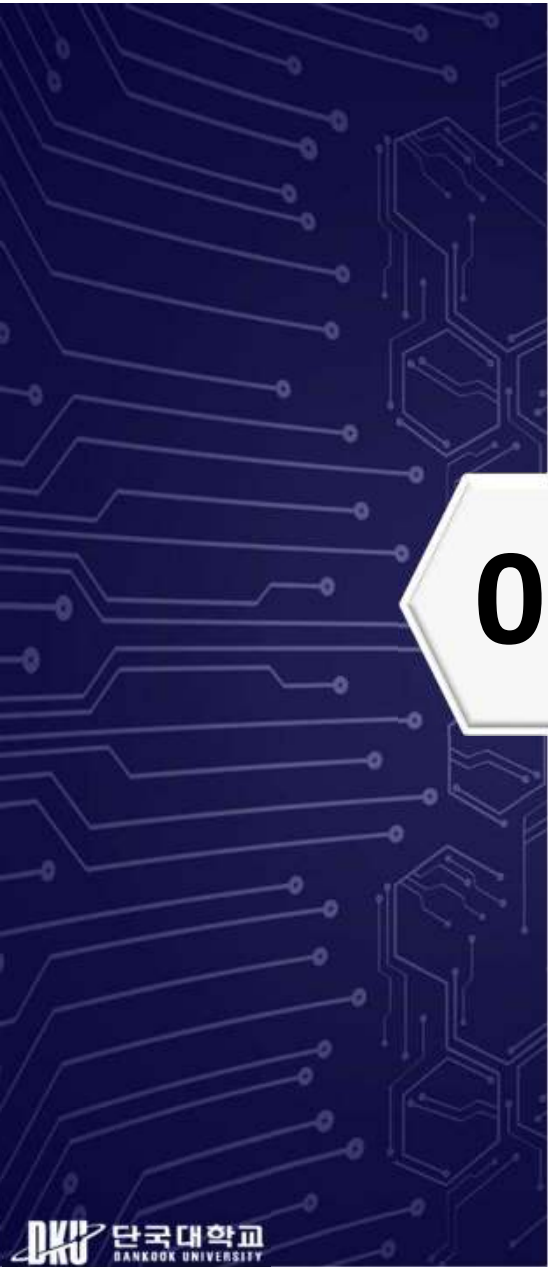
- 시스템의 네트워크 자산을 스캐닝하여 호스트, 하드웨어 정보, 운영체제 정보, 소프트웨어 정보 등을 자동으로 식별하는데 도움을 주는 기술
- 대표적인 스캐닝 도구로 Nmap, Zmap, Grassmarlin 등
- OT에 이러한 기술을 곧바로 적용하기에는 한계점 존재



# 서론

---

- 1 기존에 존재하는 네트워크 스캐닝 도구를 OT에 적용했을 때 문제점 확인
- 2 OT 실험 환경 설계한 후, 문제점 원인에 대해 분석
- 3 OT를 사용하는 환경에서 적합한 네트워크 스캐닝 방법에 대해 논의



**02**

## 관련 연구

## 관련 연구

---

### ❖ Automated asset discovery in industrial control systems-exploring the problem.

*3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015) 3. 2015.*

- 산업 제어 시스템에서 자산 자동 탐색을 위해 스캐닝 도구를 사용하고 한계점 분석
  - 능동적 스캐닝 : 네트워크 노드 또는 엔드 포인트로 패킷 전송하여 자산 탐색  
OT에 적용하면 특성으로 인하여 장치가 불안정해질 가능성 존재  
ex) Nmap, Zmap
  - 수동적 스캐닝 : 네트워크 안에서 오고 가는 패킷만을 모니터링하여 자산 탐색  
전체적인 OT 장치를 탐색하는데 어려움이 발생  
ex) Grassmarlin

### ❖ Active Scanning in the Industrial Control Systems.

*2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC). IEEE 2021.*

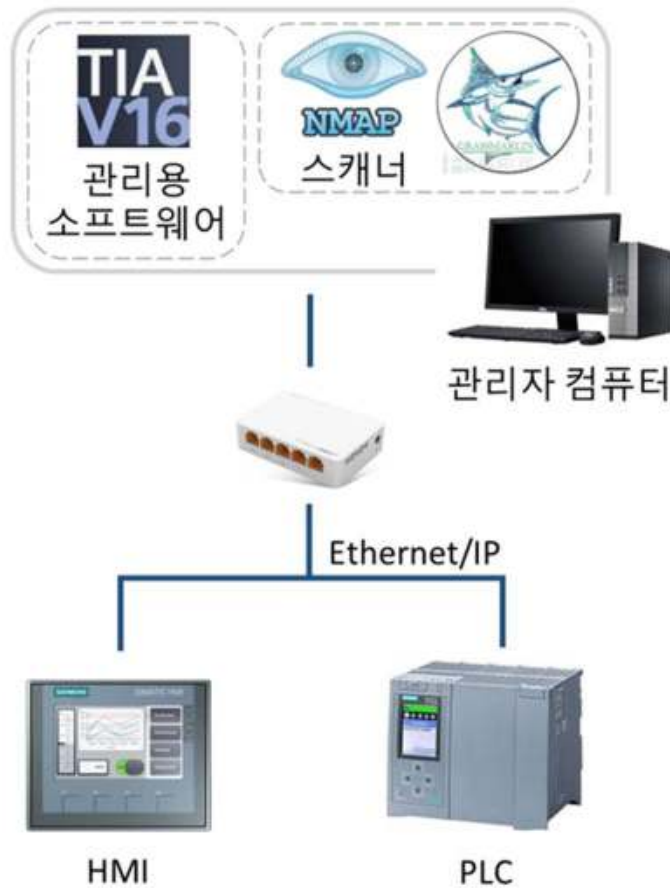
- OT 네트워크와 유사한 자동화 시스템 환경을 만들고 Nmap, Zmap 네트워크 스캐닝 도구 사용했을 때, 발생할 수 있는 영향을 확인
- Ping 응답 시간의 지연과 PLC 동작이 멈추는 이벤트 관찰

# 03

## 실험 환경 및 방법

# 실험 환경 및 방법

## ❖ 실험 환경



[실험 환경 장치 정보]

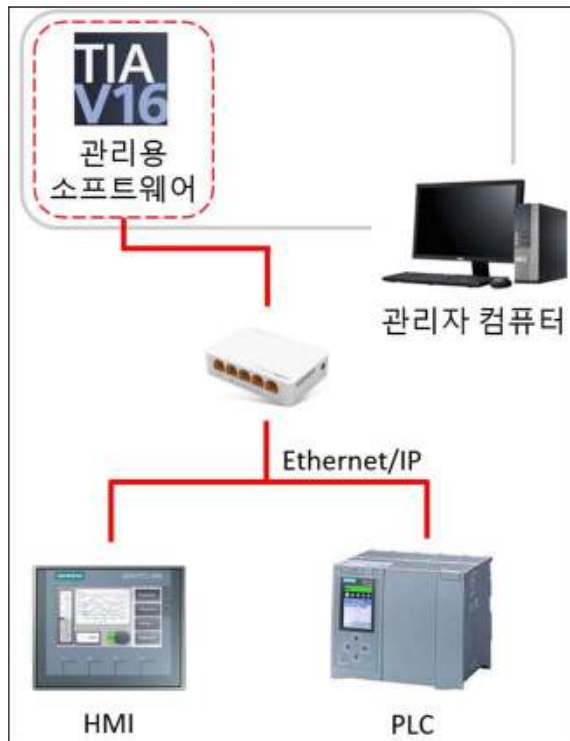
| 장치                                    | 세부 정보                           |
|---------------------------------------|---------------------------------|
| 관리자 컴퓨터                               | 윈도우 운영체제                        |
| 관리용 소프트웨어                             | TIA Portal V16                  |
| 스캐너                                   | Nmap, Grassmarlin               |
| 허브                                    | iptime H6005                    |
| HMI                                   | SIMATIC KTP 700 Basic           |
| PLC (Programmable Logical Controller) | SIMATIC S7 1500, CPU 1511C-1 PN |

# 실험 환경 및 방법

## ❖ 실험 방법

- 총 3가지 상황에서 발생하는 패킷들을 관리자 컴퓨터에서 수집

① 일반적인 상황 → ② Nmap 실행 → ③ Grassmarlin 실행



## 04

## 실험 결과

- 시스템 가용성 영향의 원인
- 식별 자산 정보 부족의 원인

## 04

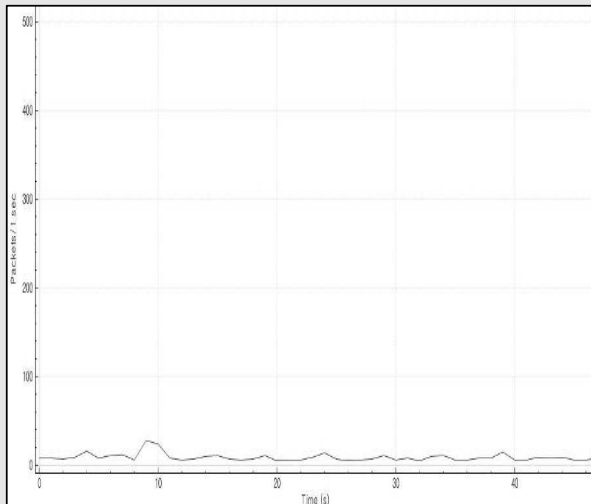
## 실험 결과

- 시스템 가용성 영향의 원인
- 식별 자산 정보 부족의 원인

## 실험 결과 ➤ 시스템 가용성 영향의 원인

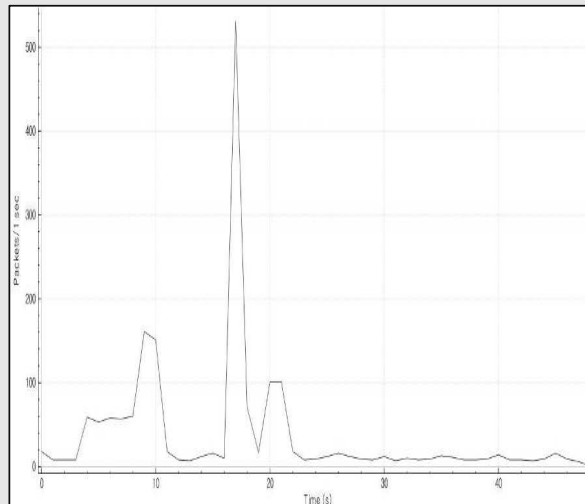
### ① 일반적인 상황

- 일정 시간마다 PN-PTCP 프로토콜 패킷을 연결된 다른 장치로 전송하며 시간 동기화
- 초당 30개 미만의 패킷 이동



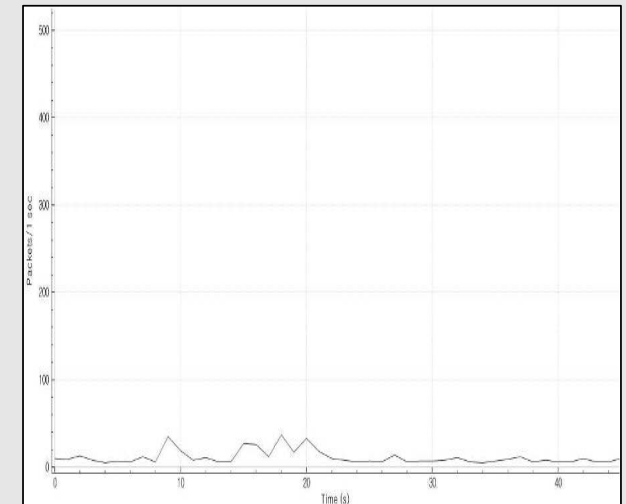
### ② Nmap 실행

- 전반적인 트래픽 양 증가
- 피크 시점의 패킷은 531개로 17배 차이 발생
- 지멘스 장치 이상 작동은 감지하지 못했으나 패킷 수 증가가 ABB 장치 이상 작동을 관찰한 관련 연구 존재



### ③ Grassmarlin 실행

- 패킷 수 차이 발생하지 않음
- 패킷을 생성하지 않았다는 것
- 이러한 방식은 OT 작동에 영향을 주지 않는다는 것을 의미



## 04

## 실험 결과

- 시스템 가용성 영향의 원인
- 식별 자산 정보 부족의 원인

## 실험 결과 ➤ 식별 자산 정보 부족의 원인

❖ Nmap, Grassmarlin의 OT 네트워크 자산 식별 정보 결과

| 식별 정보       | Nmap |     | Grassmarlin |     |
|-------------|------|-----|-------------|-----|
|             | PLC  | HMI | PLC         | HMI |
| IP          | ●    | ●   | ○           | ○   |
| MAC주소       | ●    | ●   | ○           | ○   |
| 제조업체        | ●    | ●   | ○           | ○   |
| 포트 넘버       | ●    | ●   | X           | X   |
| 제공 서비스      | ●    | ●   | X           | X   |
| 하드웨어 정보     | ●    | X   | X           | X   |
| 하드웨어 버전     | ●    | X   | X           | X   |
| 하드웨어 시리얼 넘버 | ●    | X   | X           | X   |
| 운영체제 정보     | Δ    | Δ   | X           | X   |
| 운영체제 버전     | Δ    | Δ   | X           | X   |
| 소프트웨어 정보    | X    | X   | X           | X   |
| 소프트웨어 버전    | X    | X   | X           | X   |

● : 식별함  
 ○ : 특정 경우 식별함  
 Δ : 식별 내용 다름  
 X : 식별하지 못함

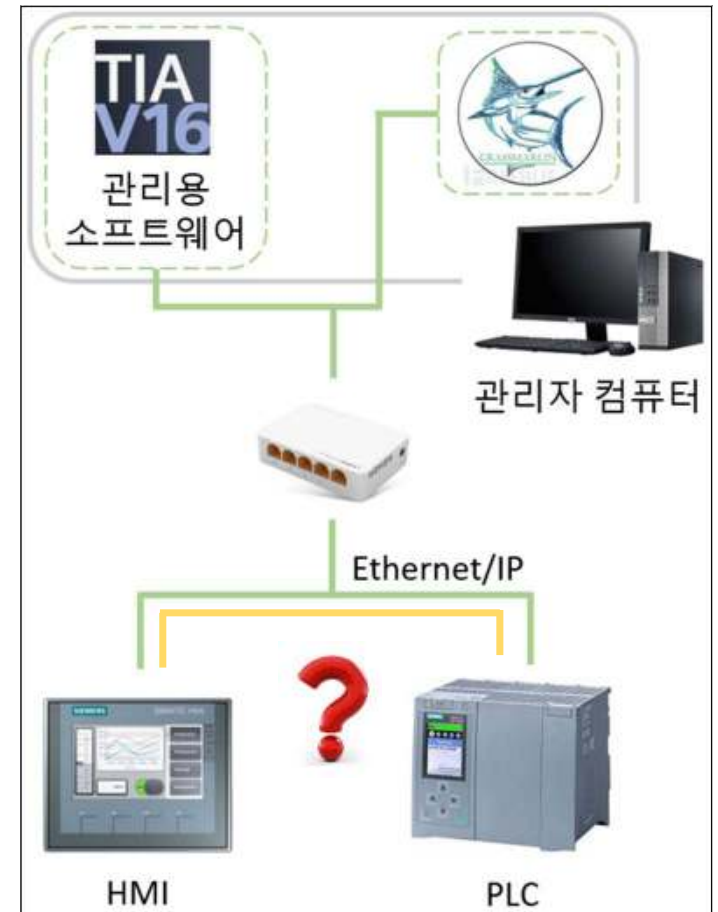
## 실험 결과 ➤ 식별 자산 정보 부족의 원인

- ❖ Nmap은 하드웨어 정보와 운영체제 정보를 식별하지 못함.
  - OT 장치에 대한 사전 정보가 부족함.
  - IT 시스템의 하드웨어 시그니처, 운영체제 시그니처는 보유하고 있지만 OT 장치는 그러지 못함.
  - OT 장치 특성 상 무수히 많은 장치들이 존재하고 독자적인 운영체제를 사용하기 때문에 다양한 시그니처를 모아두는데 한계가 있을 것으로 보임.



## 실험 결과 ➤ 식별 자산 정보 부족의 원인

- ❖ Grassmarlin은 특정 경우 장치만 식별하고 있음.
  - 관리자 컴퓨터에서 모니터링할 수 있는 패킷만으로 장치를 탐색함.
  - 패킷이 스캐너에 도달하지 못하면 장치를 감지할 수 없는 현상 발생함.
  - 즉, 스캐너가 존재하는 장치와 OT 장치가 통신을 수행하는 경우에만 식별이 가능함.
  - 더욱이 포트 넘버, 하드웨어 정보, 운영체제 정보 등의 내용은 모니터링한 패킷만으로 식별하기 어려운 정보이므로 얻어지는 자산의 정보가 한정적임.



# 05

## 결론 및 향후 연구

## 결론 및 향후 연구

---

1

기존에 존재하는 네트워크 스캐닝 도구를 OT에 적용했을 때 문제점 확인

- 시스템의 가용성에 악영향을 줄 수 있다.
- 얻어지는 정보량이 자산을 관리하고 보호하기에 부족하다.

2

OT 실험 환경 설계한 후, 문제점 원인에 대해 분석

- 급격하게 패킷이 증가했다.
- OT 장치에 대한 사전 정보 부족했다.
- 스캐너에 도달하지 못하는 패킷의 존재했다.

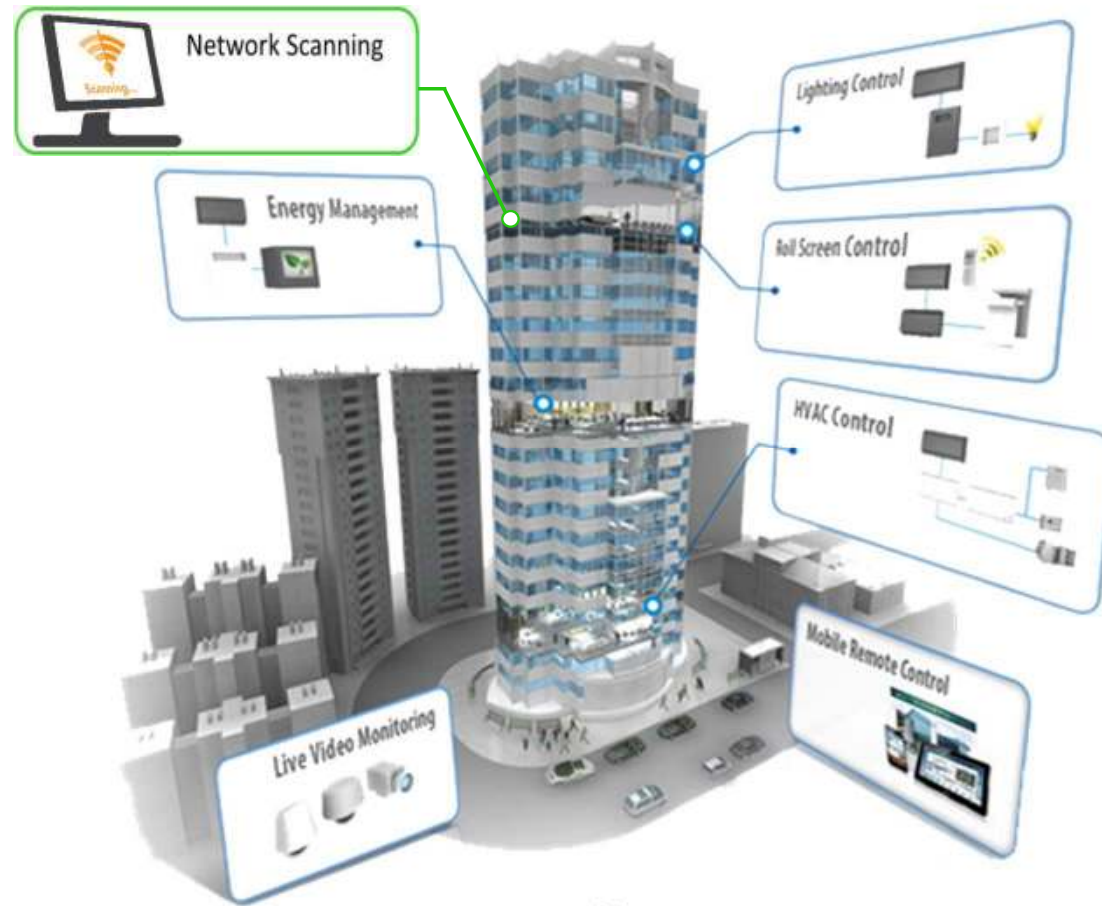
3

OT를 사용하는 환경에서 적합한 네트워크 스캐닝 방법에 대해 논의

- 시스템의 가용성에 악영향을 미치지 않아야한다.
- 자산의 하드웨어 정보, 운영체제 정보, 소프트웨어 정보를 탐지할 수 있어야한다.

## 결론 및 향후 연구

OT 설비 제어가 존재하는  
스마트 빌딩에 적합한 네트워크 스캐닝 방법에 대한 연구 계획 중



---

# Q&A

---