산업기반 테러시설 1, 2주차

* 산업제어 시스템

ICS(Industry Control System) : 다양한 자동화 시스템과 관련 장비에 사용되는 **포괄적인 용어**

* 정보기술(IT)와 운영기술(OT)로 나눔. / IT 영역은 일반 사무실의 네트워크와 유사
* OT는 **주요 설비 제**어와 관련된 **영역**. 즉, OT는 ICS 보안의 가장 중요한 요소 !!

Ex ) 프로그램 가능 로직 제어기(PLC), 원격단말장치(RTU) 등. PLC : 설비제어 담당 센서

* OT vs IT
* IT는 CIA 우선순위 // 별로 중요하지 않음.
* OT는 AIC 우선순위 Avaliability , integrity, confidential

전용 애플리케이션 및 비공개 전용 프로토콜 : ftp , telnet도 프로토콜로 제어를 하고 있지만, 여러가지 프로토콜을 제어할 때는 다 다르다. Modbus 및 smeise등 프로토콜 겸 어플리케이션을 사용.

OT는 가용성을 중시 : why? 공장 같은 경우는 한번이라도 멈추면 막대한 피해가 발생 ex) 병원

사고 발생시 대규모 경제적 물리적 피해가 발생 !

* 산업 제어 시스템 구조 / 각각에 대한 용어

1. **프로그래머블 로직 컨트롤 – PLC // 설비 제어 담당 센서**

: 입력채널을 통해 데이터 획득, 출력 채널을 통해 엑추에이터를 제어 // usb 및 네트워크 통신버스 수행 // 일반적으로 사용하는 프로토콜 X, **이거 꺼라 저거켜라 등에 대한 전달을 해서 서로 통신을 주고받는 역할**

1. **휴먼 머신 인터페이스 : HMI**

: 실행 중인 프로세스를 시각화해 프로세스 값의 ratk와 조작, 경보 표시와 제어 설정 값의 현황 표시

**시리얼 통신이나 이더넷 암호화 프로토콜을 통해 통신하는 터치 지원 장비** // 클릭하면 plc와 연결되서 데이터값이 들어가고 plc에서 장비에게 명령을 내리는 구조

1. **감시 제어 및 데이터 취득 : SCADA**

: **전력망, 수도 시설 등등 원격 운영 스테이션을 사용하는 ICS 유형 및 장비의 결합된 시스템**

1960년대 원격지의 시스템을 효과적으로 감시 및 제어하기 위해 사용. // 장치마다 상호 연결, 각 장치에 대한 원격 접근 및 제어 가능

1. 시스템 분산 제어 시스템 : DCS

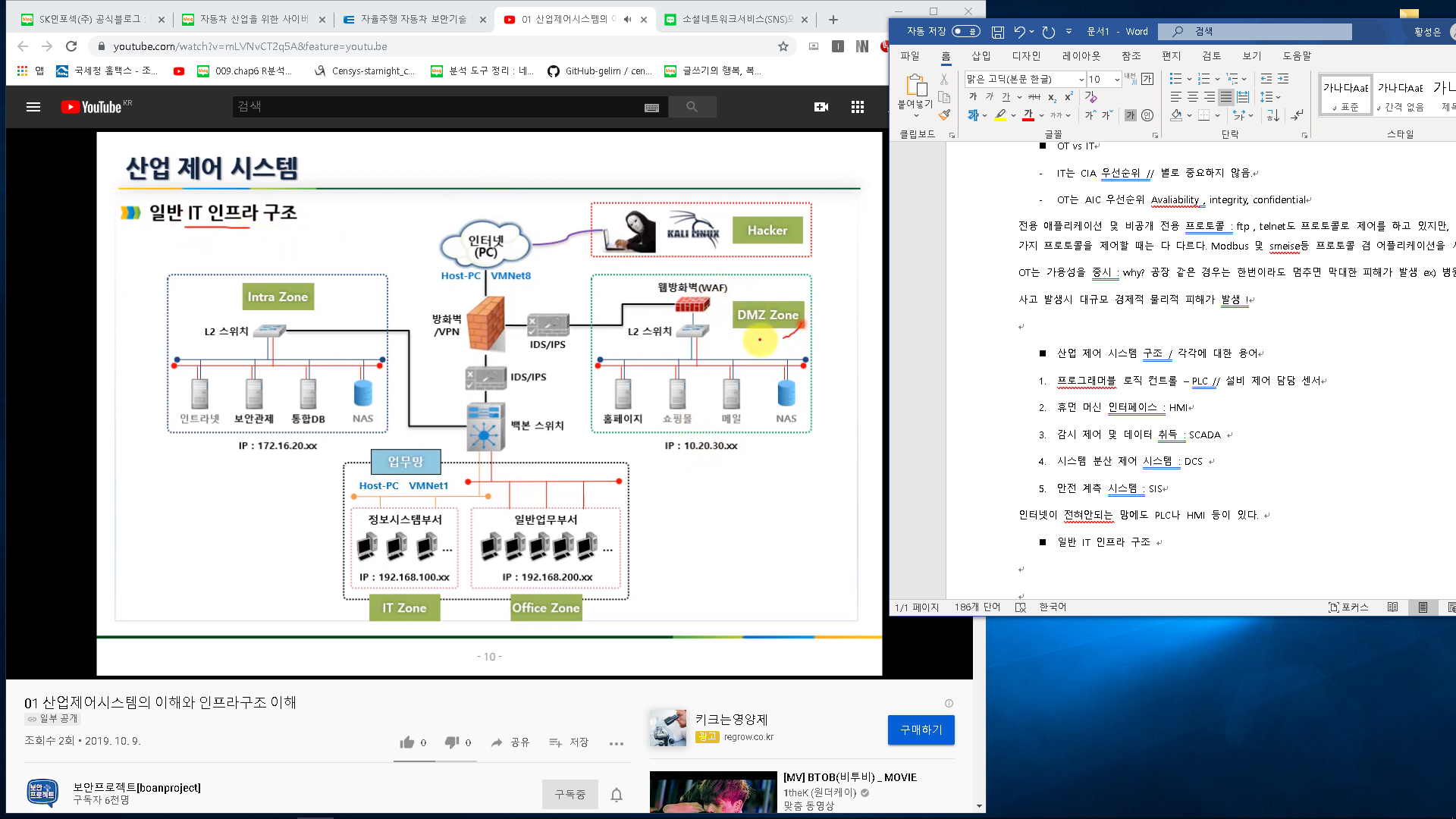
DCS는 하나의 현장에서 이뤄지는 작업을 처리하는데 사용 EX 스마트폰 / SCADA는 범위가 더 큼 EX) 아파트 등 큰지리적인 자동화의 대명사.

1. 안전 계측 시스템 : SIS

: 안전 모니터링 전용 시스템 //

인터넷이 전혀안되는 망에도 PLC나 HMI 등이 있다.

* 일반 IT 인프라 구조



DMZ 구간들이 있다. DMZ Zone 외부에서 들어올수 있는 구간.

Intra zone 함부로 들어갈 수 없는 구간

외부에서는 intra나 오피스망에 함부로 들어갈 수 없다.

* 인프라 이해

Enterprise zone 은 dmz zone과 거의 똑같음

Industrial demilitarized zone은 중계영역 // 위에존에 있는 데이터를 아래 영역으로 보내야하는데, 보안이 중요하며 이러한 것들에 대한 접근 제어를하는 기능

Industrial zone은 내부망으로써, 전체적인 부분들이 scada임. Industrial distribution이 중심이며

Plc 컨트롤러가 장비들을 하나씩 제어하는 구조

* 퍼듀 모델 ( 인프라 구조를 가지고 어떻게 적용해야 하는가?)

ISA-99의 PERA 모델에서 채택된 ICS

레벨 별로 외울필요 X, 왜 이게 이레벨에 위치해있는지만 알면됨.

1. 엔터프라이즈 영역

전반적인 공장 설비의 생산 상태, 재고 및 수요를 보고하는데 사용

ICS 네트워크와의 연결을 기반으로 안쪽으로 데이터를 제공하는 역할을 하는 구간임.

레벨 5 : 기업레벨, 인터넷 정보들이 들어와야하는 부분 (공장 설비의 생산 상태 및 재고 수요 등을 보고하는 데이터를 가져오는 부분들이 Enterprise Network임.) 안쪽으로 데이터를 제공하는 역할

레벨 4 : 공장에서 생산하는 모든 프로세스를 지원 (모든 정보 기술 시스템의 본거지)

데이터들이 내부쪽으로 들어가는 데 이런 데이터들을 연결하는 시스템들이 위치함.

1. Industrial 비무장 영역

한마디로, IT와 OT 시스템간의 직접적인 통신을 방지하고 IDMZ중계서비스를 통신을 중계하여 별도의 분리 및 검사 계층이 전체 아키텍처에 추가 -> 절충한 -> 생산 // 중계역할

1. 인터스트리얼 영역

내부존이라서 레벨 3 – 사이트 운영

공장 전반의 모니터링 및 컨트롤 제어 시스템(HMI, 운영장비 등)이 위치

레벨 2 – 구역 감독 통제

PLC는 1에도 있지만 2에도 있음. 레벨 3및 레벨 1이 붙어있는 부분이 잘 동작이 되고 있는지 모니터링 하는 역할

레벨 1 – 기본통제

실제 프로세스 센서들과 연결되어있는 구간이라서 PLC PID 등 여러가지 컨트롤 들이 위치.

* 산업제서 시스템 프로토콜 이해 및 분석
* 일반 it 프로토콜 이해 // 업체마다 장비에 맞는 프로토콜을 개발 -> 표준화가 안됨.

프로세스 자동화 프로토콜 : ControlNet, Modbus // 기능이 비슷 (데이터를 받아서 시스템에 넘김.)

일반 it 프로토콜 대부분은 퍼듀 모델 레벨 3 이하에서 진행.

* 모드버스 프로토콜 // 응용 프로그램 계층 메시징 프로토콜

1979년에 도입, 사실상의 표준이며, 가장 널리 사용되는 ICS 프로토콜

OSI 모델에서는 레벨 7에 배치됨. = 다양한 유형의 통신 버스를 통해 연결된 장치간에 클라이언트 / 서버 통신을 제공

* 모드버스 프로토콜의 이해 // MODBUS-TCP는 마스터와 슬레이브의 역할이 있음.

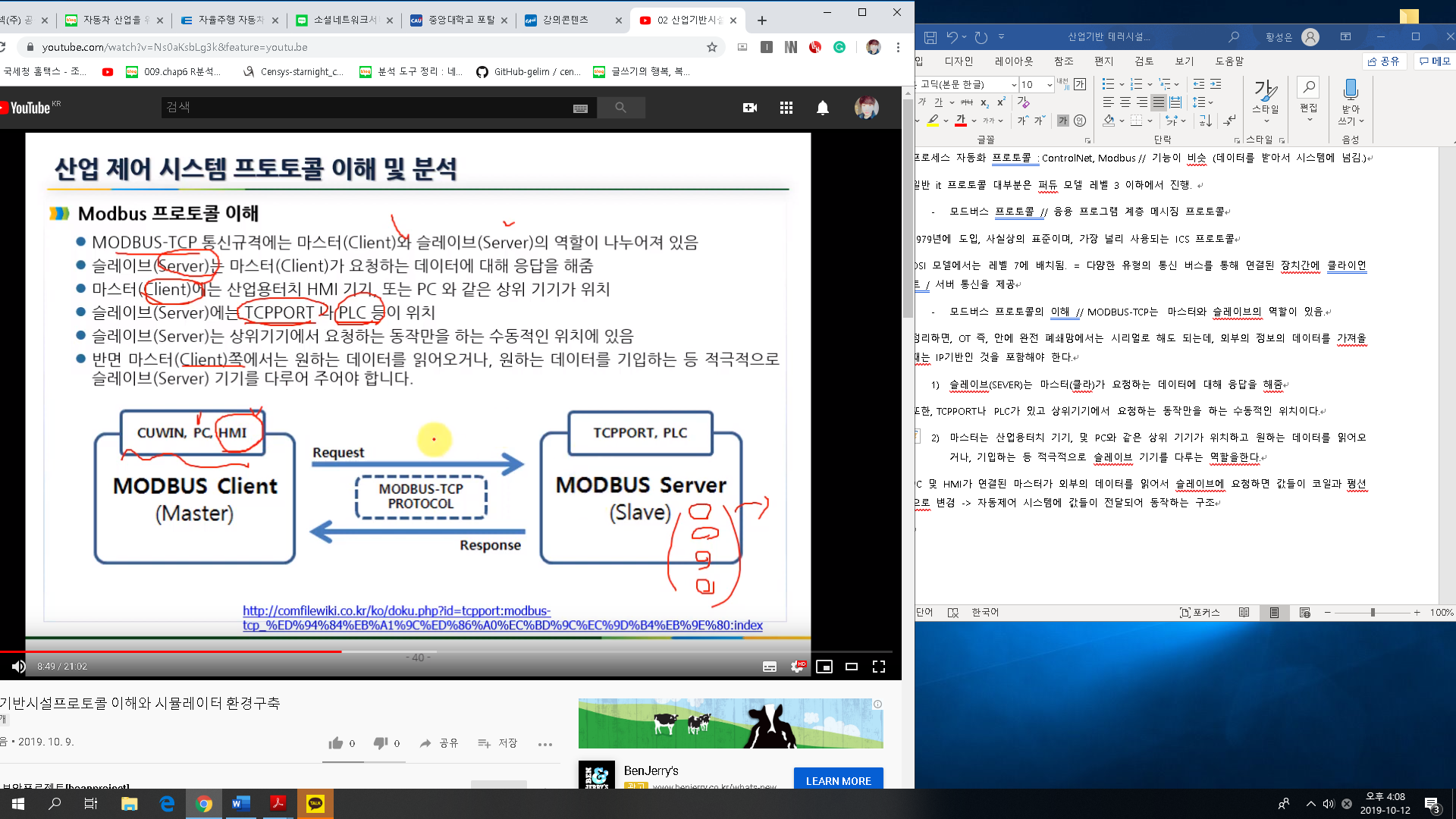
정리하면, OT 즉, 안에 완전 폐쇄망에서는 시리얼로 해도 되는데, 외부의 정보의 데이터를 가져올때는 IP기반인 것을 포함해야 한다.

1. 슬레이브(SEVER)는 마스터(클라)가 요청하는 데이터에 대해 응답을 해줌

또한, TCPPORT나 PLC가 있고 상위기기에서 요청하는 동작만을 하는 수동적인 위치이다.

1. 마스터는 산업용터치 기기, 및 PC와 같은 상위 기기가 위치하고 원하는 데이터를 읽어오거나, 기입하는 등 적극적으로 슬레이브 기기를 다루는 역할을한다.

PC 및 HMI가 연결된 마스터가 외부의 데이터를 읽어서 슬레이브에 요청하면 값들이 코일과 펑션으로 변경 -> 자동제어 시스템에 값들이 전달되어 동작하는 구조



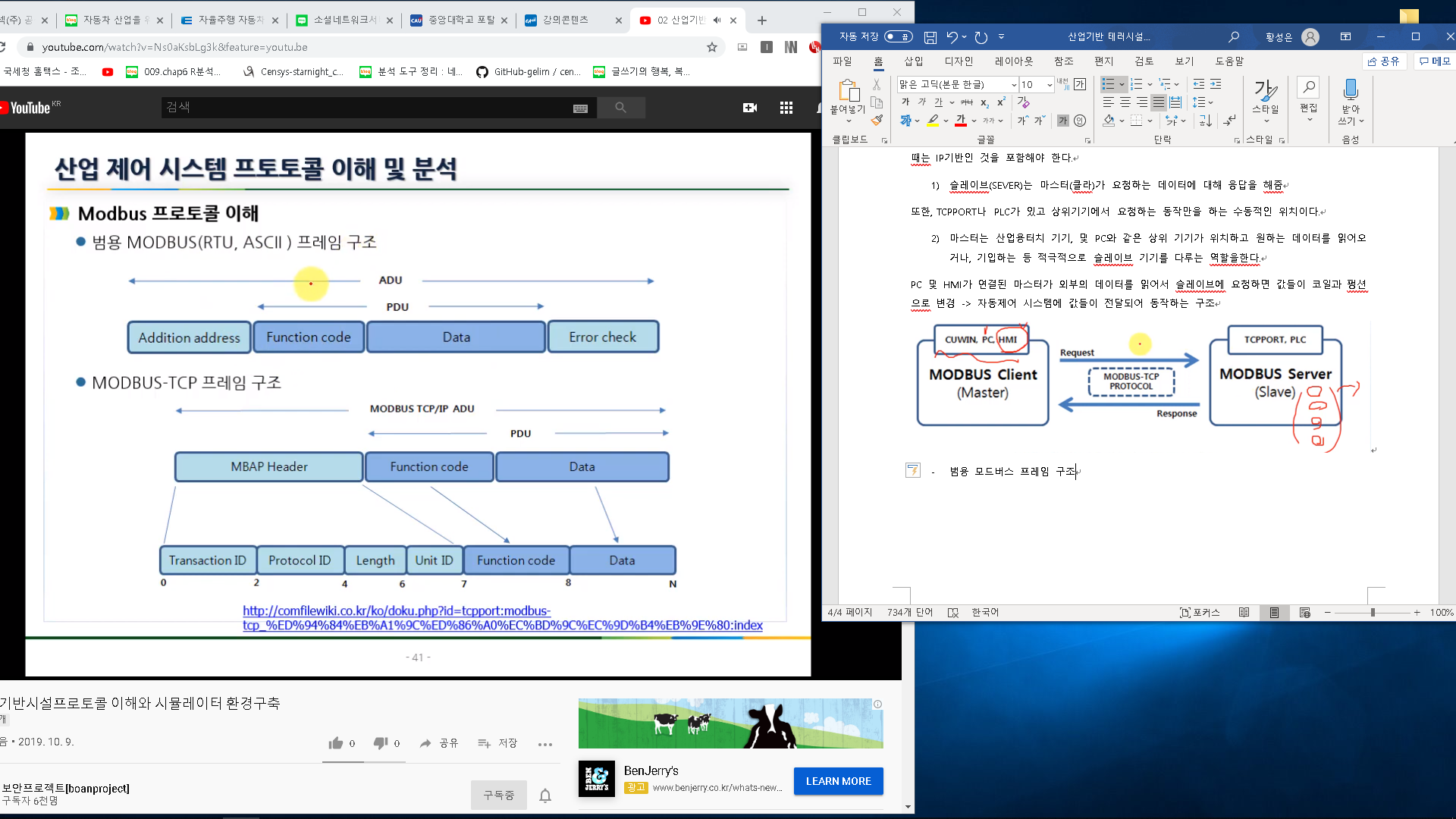
펑션 코드와 데이터가 중요함.

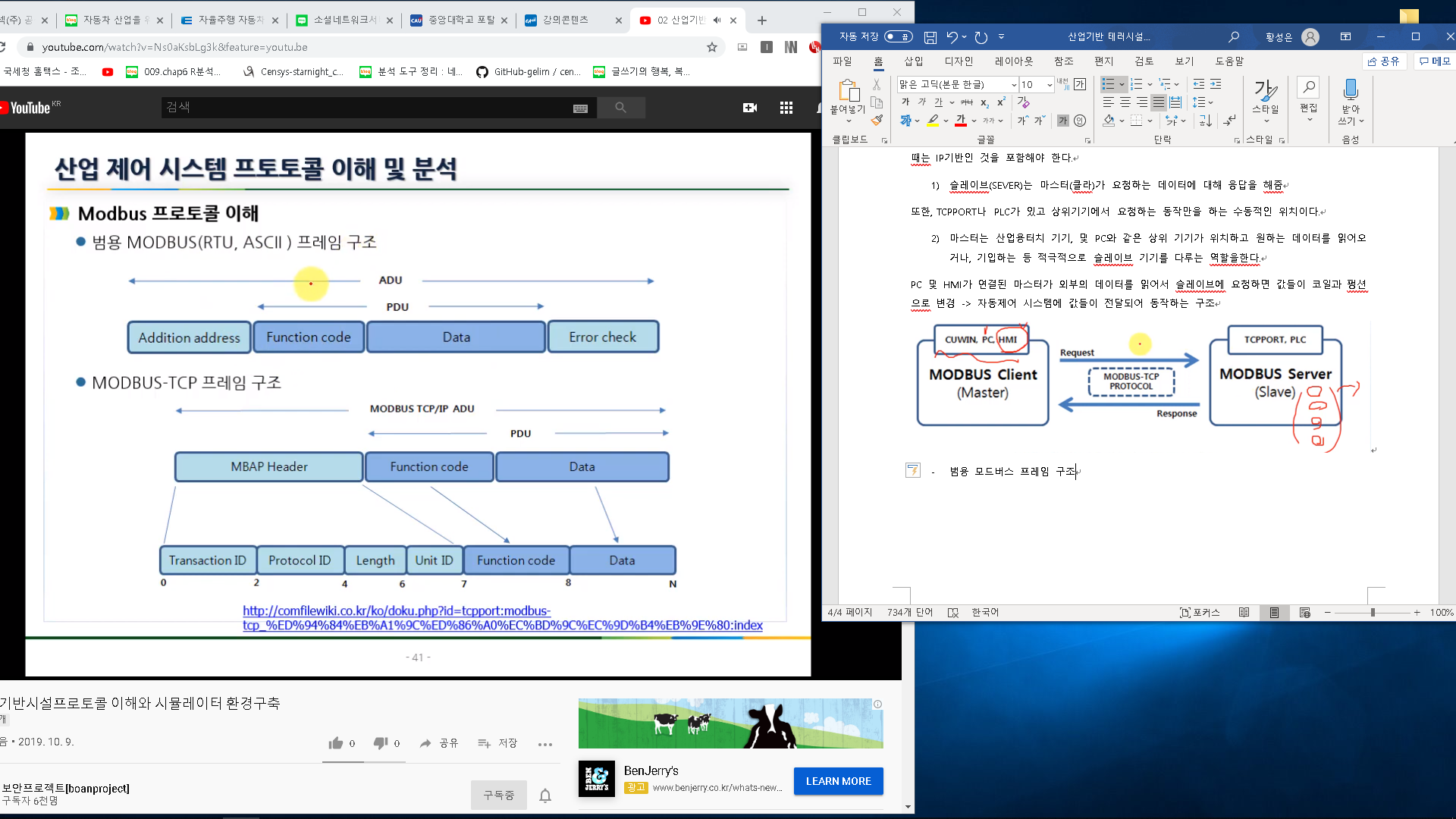
펑션코드는 명령어. 뭐를 할거냐 등의 지시

실질적으로 명령어를 내리기 위한 컴퓨터가 알아먹을 수 있도록 하는 것이 DATA

즉, 펑션코드 = 데이터

Java -jar modbusPal.jar





* MBAP Header 부분

모드버스 어플리케이션 프로토콜의 약자, 우리가 nmap을 통해 스캔을 하면 헤더 정보들이 나옴 -> 아 모드 버스 프로토콜을 사용하고있구나

칼리리눅스에 파일을 복사 어캐함? 걍 옮기면 됨.

칼리 리눅스 – 공격자 // 칼리 리눅스 자체에 모드버스 시뮬을 올리고 칼리리눅스에서 공격을해서 조작이 되는지 보는 것.

* Function Code 부분

코일과 레지스터가 중요함. 펑션 코드에서 1~127사이 값

그러나 tcpport에서 1 2 4 5 6 15 16 why? -> 실질적으로 사용하는 서비스기 때문

Modbuspal은 슬레브 // 모드버스의 기본 프로토콜은 502이다.

모드버스 슬레브는 하나의 데이터베이스 역할로 보면됨. 슬레이브를 추가할 수 있음.

스카다 – 전체 개념 / 슬레이브 하나는 장치하나로 생각 (a영역의 장비를 제어하는 장비나 그냥 장비)

코일의 Value는 1과 0밖에 안된다. 이런 것들을 코일에 넣어서 관리를 해주면 됨.

레지스트리는 65535까지 가능 – 뭔가 더 확장해서 사용가능

PC로 치면, 슬레이브 메모리에서 레지스트리 정보를 통해서 cpu 정보를 넣고 메모리를 넣어서 연산 진행해서 진행하는 그런 구조임.

IFCONFIG 해서 네트워크 따고

Nmap 192.. -p 를 하던가 -p 502를 하면 됨.

이제 외부에서 접근을 해봐야겠죠? 다음시간에 ~

// 포트가 열려있는 것 까지 확인을 했다.

* 클라이언트 쪽에서 모드버스라는 프로토콜을 이용해서 plc에서 scada를 제어한다는 흐름.

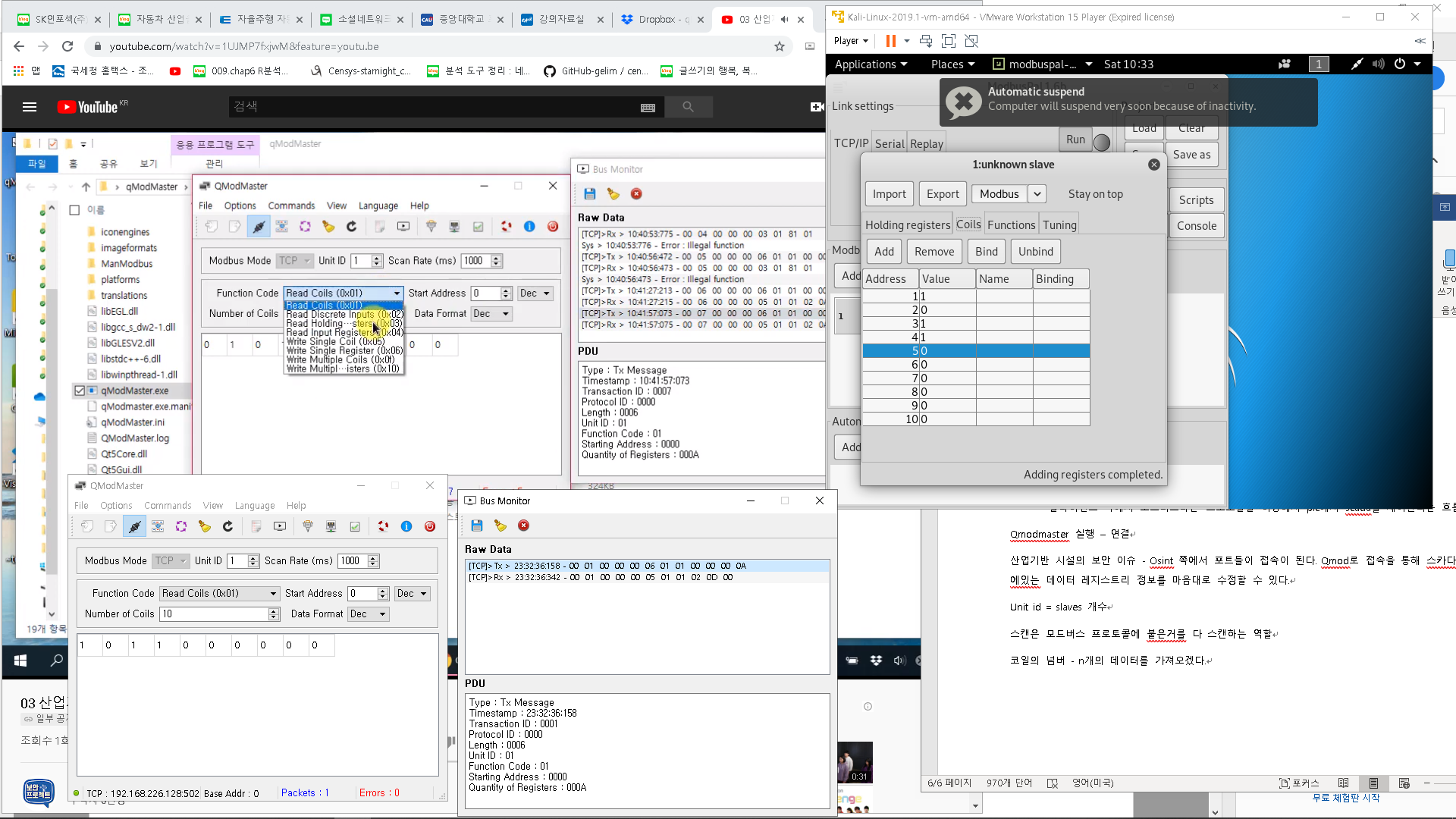
Qmodmaster 실행 – 연결

산업기반 시설의 보안 이슈 - Osint 쪽에서 포트들이 접속이 된다. Qmod로 접속을 통해 스카다쪽에있는 데이터 레지스트리 정보를 마음대로 수정할 수 있다.

Unit id = slaves 개수

스캔은 모드버스 프로토콜에 붙은거를 다 스캔하는 역할

코일의 넘버 - n개의 데이터를 가져오겠다.



write해서 돌리면 칼리상의 모드 버스 값이 달라짐.

이렇게 서버/클라이언트에 접속할수 있는 것을 살펴봄

즉, 모드버스가 열려있고 502포트가 열려있다면 이 데이터에 접속할 수 있다 !!

* 모의해킹 과정 – 산업제어시스템 프로토콜 패킷 분석

Gem install modbus-cil

Modbus 치면 헬프창 나옴 사용방법

Loopback을 더블클릭하던가 / 캡쳐 – 옵션가서 loopback을 클릭

modbus read 192.168.226.128 1 8 // 모드버스를 돌린 상태에서 각 코일을 읽음 1부터 8까지

modbus write 192~ 8 1 // 모드버스 8번째 코일 데이터 값을 1로 바꾼다.

이러면 와이어 샤크에 분석이 나타남.

필터에 modbus 검색 // 와이어샤크에 대해서 모드버스 해석이 가능하다

Modbus/TCP 를 검색해서 첫번재 보면, modbus/tcp는 연결을 위한 구간

Modbus는 데이터 영역

마스터쪽 -> 슬래브 // 55886 -> 502 요청한거임

슬레브 – 마스터쪽 502 -> 55886 반응

마스터쪽 – 슬래브 응답 55886 – 502 연결이 되었다. / 3hand shake

마스터쪽에서 – 슬래브 // Query : Trans

Modbus/tcp는 identifier정보와 unit 정보가 한번에 날라간다.

헥사 값을 찍으면 서로 바뀐다 탭이 / 즉, 와이어샤크는 이 규격화된 규칙들을 보면서 해석해나간다. 00 06 이라는 것은 length 위치정보이고 등등 ..

Read coils 이라는 것이 1으로 저장 / 레퍼 0000 으로 저장 /

response값은 데이터들이 날라오면서 모드버스 데이터가 0번부터 x번까지 리드하라고 한게 나옴.

그다음 쿼리 : 트랜스가 2개가 나오는데 하나는 리드부분/ 하나는 write부분임

레퍼런스 값이 7 =0~7R지 data 1번을 수정