2019. 09. 09 2주차

산업제어 시스템 프로토콜 이해 및 분석

* 일반 IT 프로토콜 이해

시리얼 통신로 통신 / TCP , IP로 통신을 하는 것 - 차이가 있음

P32.

일반 IT 프로토콜은 장비마다 프로토콜이 있음.

Modbus - 제일 많이 사용하는 프로토콜.

Profinet, Ehernet/ip, Devicenet, Modbus (4가지)가 많이 사용하는 프로토콜.

P33.

* 모드버스 프로토콜의 이해

P34.

Modbus – 100% 표준은 X / 많이 사용함.

응용 프로그램 계층 메시지 프로토콜

OSI 모델 7레벨

버스 및 통신 매체를 통해 연결된 장치간의 클라이언트 / 서버 통신 제공

P35.

1. 시리얼을 통한 모드버스 통신 - 마지막 라인과 직접 연결
2. 이더넷을 통한 통신에 동일한 응용 프로그램 계층 프로토콜 사용

P36.

모드버스 TCP : 마스터 / 슬레이브 역할 (2가지)

서버 (server) - 마스터(client0가 요청하는 데이터에 대해 응답 // tcpport 및 PLC 등 위치

마스터 (client) - PC 등의 상위기기 //

Cmd 킴

Cd c:\Temp

Java –jar Modbuspal.jar (-<-서버)

Add – slave – 1- add (이 슬렝ㅣ브 안에 코일, 레짓ㅡ트리가 들어감<- 이를 외부에서 조작할 수 있는 지가 고려해야할 보안 부분) - 눈알 클릭 - Holding registers – add – from 1 to 10 – add – value를 65535까지 변경가능 (65536(2의 16승)개 까지 만들수 있다.)

Coils – add – from 1 to 10 – add (coil는 밸류값을 0,1로 밖에 못바꿈)

Functions

Run -> 502포트가 열림(원격에서 502포트로 연결하여 이용가능)

Modbus는 502포트가 표준 (http 80 / https 443)

Qmodmaster(클라이언트) 압축 제한 파일로 ㅡㄹ어가서 exe 파일 누름

랜선모양의 모드버스 tcp - 무선 랜 어댑터 와이파이 ipv4 주소) - connect 버튼 클릭

Modbus protocol 에서 중요한 것은 functions code 랑

모드버스 프로토콜 ㅇㅣ해 - function code 부분 (이 슬라이드 절대 외우지 x)

메모리 - 저장공간 (코일+레지스트리로 구성)

코일 : 0 or 1, 장비 동작 상태의 정보(동작하는지 안하느지), 작은 용량 ex 전원, 스위치

레지스트리 : 여러 가지 숫자 표현, 동작할 때의 정보, 큰 용량

Write 방식 - ( start address --> write로 )

Coil – 0 / start address – 1 / Unit ID – 1 / --> RUN

Read 방식 - 코일 값을 1로 몇개 바꿔 놓고 리드하면 리드 됨.

P41. 시험문제 x

TCPPORT 설명 - COILS 메모리는 펑션 코드에 의해 구성됨.