[MODBUS : 모드버스 통신]

홍지우

1. 개요

MODBUS - RTU.

PLC와 장비 통신을 위한 맞춤 프로토콜.

보통 시리얼 통신은 장비에 맞추어 프로그램 설계 된다. 장비에 어떤 입출력이 있고 무엇을 제어해야 하는지와 구해야 할 정보에 따라서 프로토콜을 설계한다. 즉, 장비와 프로젝트에 따라서 프로토콜이 바뀌고 그때마다 프로그램을 수정하거나 새로 작성한다.

그러나 MODBUS는 장비가 바뀌어도 프로토콜은 바뀌지 않는다. 생소한 제품도 MODBUS를 지원한다면 프로토콜 수정 없이 통신이 가능한데, 이유는 사전에 정의되어있는 MODBUS Memory Map 때문이다.

2. MODBUS Memory Map Table

코일/레지스터	용도	함수	읽기 주소
1~9999	읽기/쓰기 코일	1, 5, 15	0x0000~0x270E
10001-19999	읽기만 코일	2	0x0000~0x270E
30001-39999	읽기 전용 레지스터	4	0x0000~0x270E
40001-49999	읽기/쓰기 레지스터	3,6,16	0x0000~0x270E

장비가 MODBUS를 지원한다면 반드시 위와 같은 형식의 메모리 맵을 갖추어야 한다.

이전까지의 시리얼 통신은 장비와 직접 통신하는 느낌이라면 MODBUS 통신은 장비 사이에 메모리 맵이 가로막고 있다. 장비는 자기 상태가 바뀌면 메모리 맵에 미리 지정된 주소의 값을 변경한다. 외부 프로그램은 장비의 메모리 맵을 읽어서 상태를 확인하고 제어하고 싶다면 기능에 해당하는 주소의 값을 변경한다. 장비는 계속해서 그 주소 값을 확인해서 시스템에 반영한다.

Register	Address	Name	Format
40001	0	Slot #1 DI/DO	F001
40002	1	Slot #2 DI/DO	F001
40003	2	Slot #3 DI/DO	F001
40004	3	Slot #4 DI/DO	F001
40005	4	Slot #5 DI/DO	F001
40006	5	SW #1	F002
40007	6	SW #2	F002
40008	7	SW #3	F002
40009	8	SW #4	F002
40010	9	PPA Voltage	F010
40012	11	PPB Voltage	F010
40014	13	PPC Voltage	F010

MODBUS 통신을 지원하는 장비는 외부에 위와 같은 모드버스 메모리 맵 테이블을 제공한다.
예를들어, Slot #1번 입력 값이 필요하다면 40001번 레지스터 값을 읽으면 된다. 스위치 SW #1이 켜진 것을 알고 싶다면 40006번 레지스터를 읽고 Off하고 싶다면 같은 40006번 레지스터에 제어 값을 쓰기 하면 된다.
이와 같이 장비의 기능에 따라서 메모리 맵을 구성 한다. MODBUS 프로토콜은 단지 장비의 메모리 맵에서 특정 주소의 값을 읽거나 쓰기를 하는 것뿐이다. **이런 이유로 장비에 따라서 메모리 맵 구성이 다를 뿐 MODBUS 프로토콜은 바뀌지 않는다.**

3. 용도에 따른 코일과 레지스터 영역

MODBUS 메모리 맵을 다시 보면 번호 구역에 따라 코일과 레지스터로 나뉘어 있는데, 이는 MODBUS가 PLC를 대상으로 만들어졌기 때문이다. 코일은 1 bit의 값과 같고 레지스터는 2byte의 word 값으로 생각할 수 있다. **즉, 코일은 On/Off하는 스위치를, 레지스터는 16bit의 입출력 값입니다.**

코일과 레지스터에는 각각 읽기·쓰기가 가능한 영역과 읽을 수만있는 영역으로 나뉘며 해당 영역의 코일과 레지스터에 접근하려면 지정된 함수 코드를 사용해야 한다.

4. MODBUS 프로토콜 기본 구성

국번	함수	주소		길이		CRC	
		high	low	high	low	low	high
01	04	00	0A	00	01	11	C8

MODBUS 프로토콜의 기본 구성은 어떤 슬레이브와 통신하는지 정하는 국번, 함수 번호, 레지스터의 주소, 필요한 데이터로 구성되어 있다.
위의 패킷은 아래와 같이 요구한다.
01: 슬레이브 1번에게
04 : 4번 함수를 이용하여 30001~39999사이에 있는 레지스터 중
00 0A : 10번 주소부터
00 01 : 1개 레지스터(즉, 10번 주소 레지스터 값만) 값을 요구

국번	함수	길이	데이터		CRC	
			high	low	low	high
01	04	02	12	34	B4	47

위는 마스터의 요구에 따라 아래와 같이 응답한다.
01: 국번 1번 슬레이브 에게
04: 4번 함수에 대한 응답
02: 전송할 데이터 길이는 2 byte(1개의 레지스터 값을 요구했으므로)
12 34 : 데이터 값

MODBUS 통신은 장비에 따라 프로토콜이 바뀌는 것이 아니라 MODBUS 메모리 맵이 장비에 따라 구성되는 것이다. 그러므로 MODBUS 장비에 대해 몰라도 메모리 맵을 알고 있다면 MODBUS 통신으로 제어할 수 있고 상태 값을 구할 수 있다.

Register	Address	Name	Format
30001	0	Voltage	F006
30003	2	Current	F006
30005	4	Power	F006
30007	6	Humid	F006
30009	8	Temp	F006
30011	10	Error code	F001
30012	11	Alarm code	F001

Register	Address	Name	Format
40001	0	Slot #1 DI/DO	F001
40002	1	Slot #2 DI/DO	F001
40003	2	Slot #3 DI/DO	F001
40004	3	Slot #4 DI/DO	F001
40005	4	Slot #5 DI/DO	F001
40006	5	SW #1	F002
40007	6	SW #2	F002
40008	7	SW #3	F002

5. MODBUS 프로토콜 메모리 맵과 함수 정리

타입	블록	번호	접근	용도	함수
Bit	Coils	1~9999	Read/Write	Read Coil	1
				Write Single Coil	5
				Write Multiple Coils	15
	Discrete Input	10001~19999	Read Only	Read Discrete Inputs	2
Word (16Bit)	Input Registers	30001-39999	Read Only	Read Input Register	4
	Holding Registers	40001-49999	Read/Write	Read Holding Register	3
				Write Single Register	6
				Write Multiple Register	16