상담품질 향상 교육

MODBUS TCP Protocol 규격 및 Test Tool 사용방법

목 차

2013년 08월 09일

CFO 지원부문) 품질경영팀(고객센터P)

김지용D

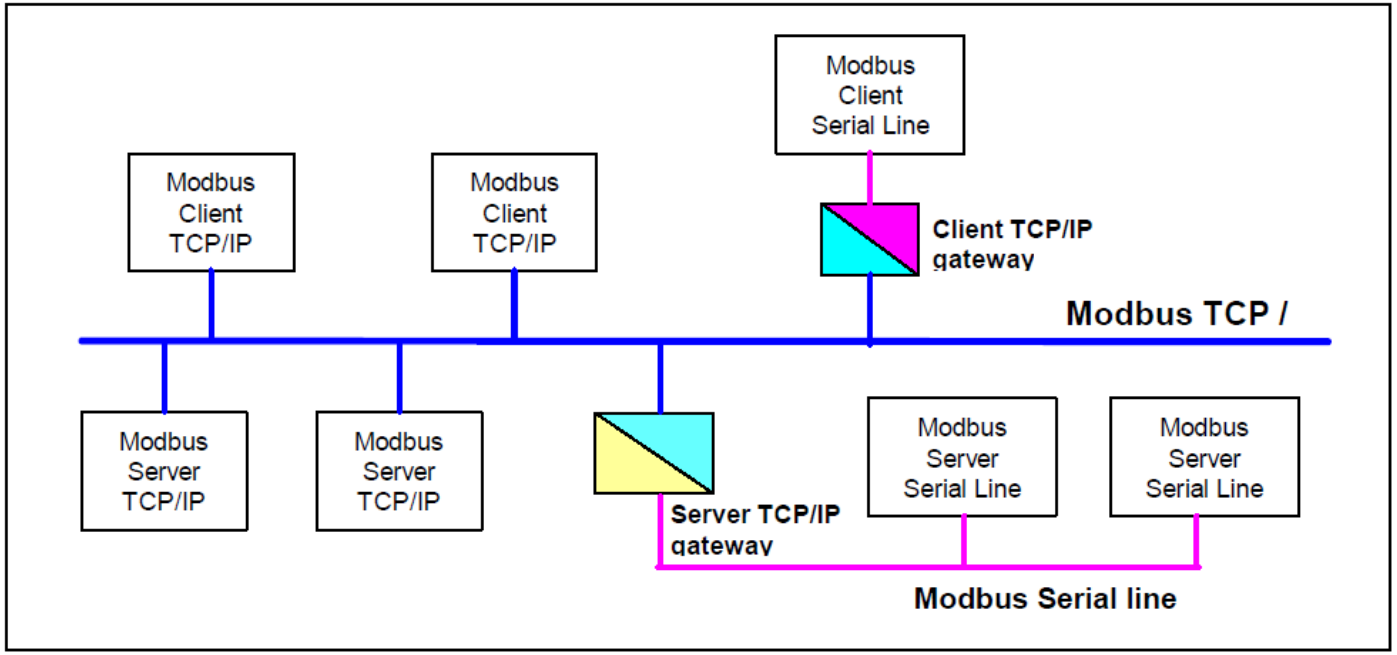
1. MODBUS Protocol 개요

개요

MODBUS 는 client/server 또는 request/reply 아키텍처 기반의 응용계층 프로토콜이다.
1979년 Modicon사에서 개발하여 산업 어플리케이션에서 많이 사용하고 있는 통신방식 중의 하나이다.

MODBUS Protocol

MODBUS 통신 프로토콜은 client/server의 아키텍처로서, client가 server에 데이터를 요청하는 구조를 가진다. 또한 client는 server에 데이터 요청 외에 다른 몇 가지 기능을 요청할 수 있다. client는 function 코드를 보냄으로 통신이 시작한다.

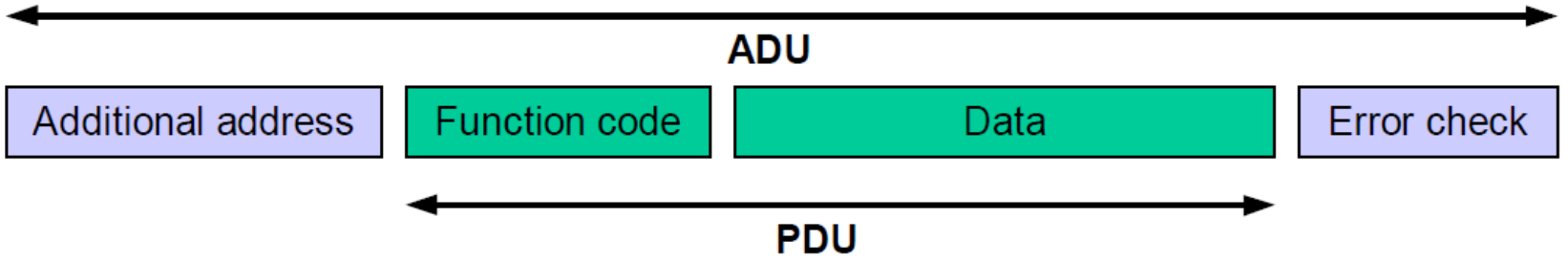


<MODBUS TCP/IP communication architecture>

2. MODBUS RTU/TCP Frame

MODBUS Frame

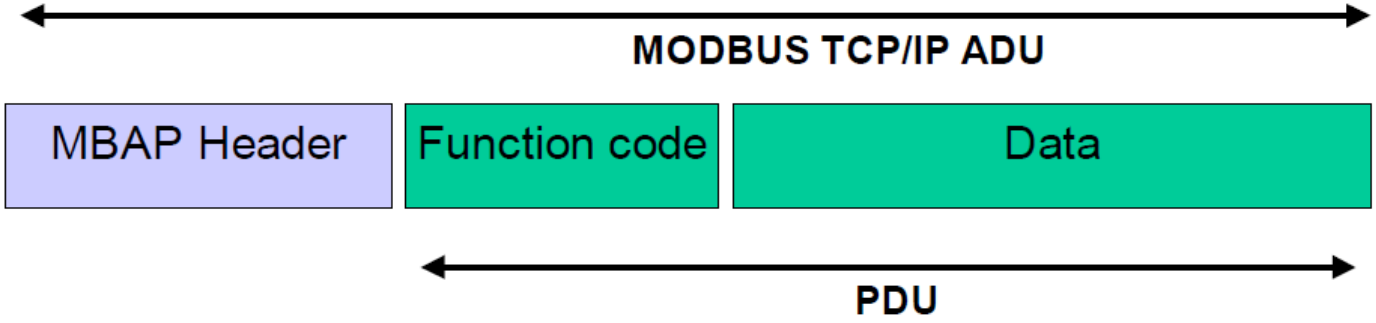
Client와 Server 사이의 주고 받는 메시지를 프레임이라 하며,
PDU(Protocol Data Unit)과 ADU(Application Data Unit)의 두 가지 타입의 MODBUS 프레임이 있다.
PDU 프레임은 Function 코드와 데이터를 포함한다.



<General MODBUS frame>

MODBUS TCP Frame

MBAP Header(MODBUS Application Protocol Header)와 PDU(Protocol Data Unit)로 구성되어 있다.

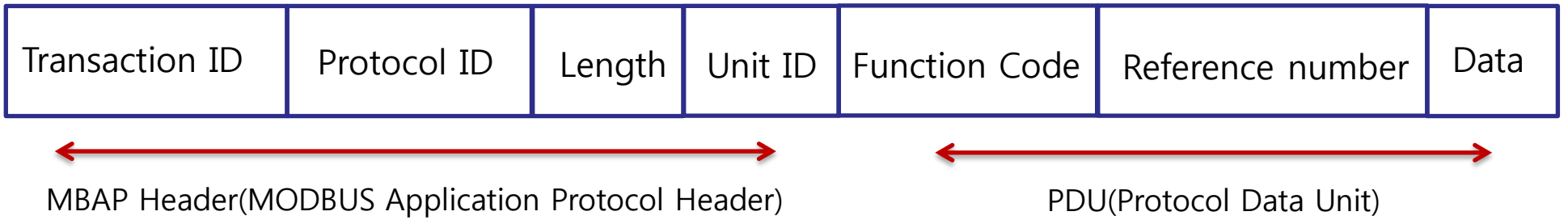


<MODBUS request/response over TCP/IP>

3. MODBUS TCP Frame

1. MODBUS TCP Frame 구성

MODBUS TCP Frame은 MBAP Header 7 bytes, PUD 5 bytes이상 구성되어 있음.



MODBUS Application Protocol Header

구역	길이	설명
Transaction Identifier	2 Bytes	고유의 전송 번호로 Client에서 Server로 Data Frame을 보낼 때 마다 1씩 증가한다.
Protocol Identifier	2 Bytes	프로토콜의 ID를 나타내며 0x0000 으로 고정되어 있다.
Length	2 Bytes	Modbus의 Data Frame길이로 MBAP Header에서 Unit Identifier 부터의 Byte단위의 길이를 나타냅니다.
Unit Identifier	1 Bytes	Modbus TCP와 Modbus RTU가 Gate를 통해 연결되어 있을 경우 Slave번호가 적혀 있게 된다. Modbus TCP만 사용할 경우에 0xFF로 고정된다.

Function Code

MODBUS TCP는 Client와 Server로 나누어 지며, Client는 명령을 내리는 입장이며 Server는 명령에 대한 응답을 하는 입장이다. 일반적으로 Client는 PLC, HMI, PC이며, Server는 인버터를 말한다.

1) Read Holding Registers

인버터(Server)에 있는 Data를 읽을 때 사용하는 함수이다.

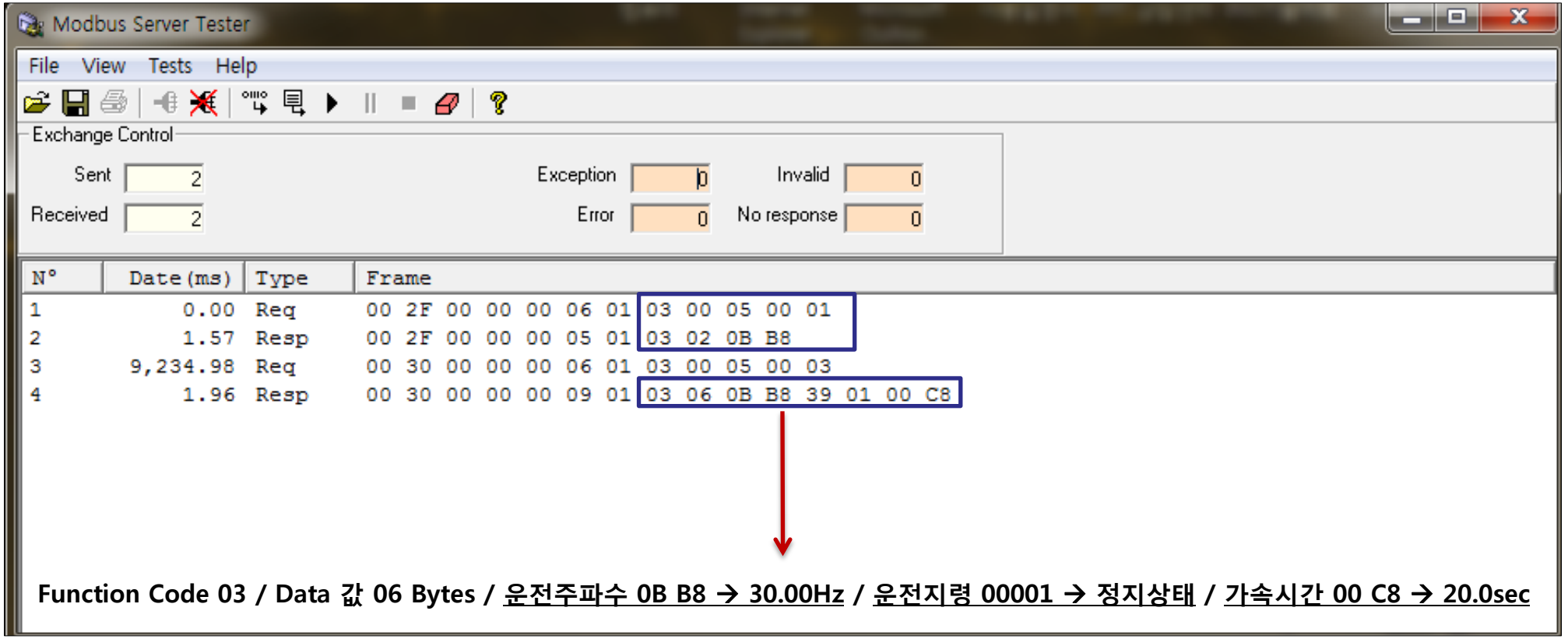
<Client에서 Server로 요구하는 Frame 구성>

요구 Frame	길이	값
Function Code	1 Bytes	0x03
통신주소	2 Bytes	0x0000 ~ 0xFFFF
Data 요구 개수	2 Bytes	1~16 (LS산전 인버터 기준)

Data 요구 개수는 최대 8개까지 가능
설계팀으로 사용설명서 수정필요!

<Server에서 Master로 요구하는 Frame 구성>

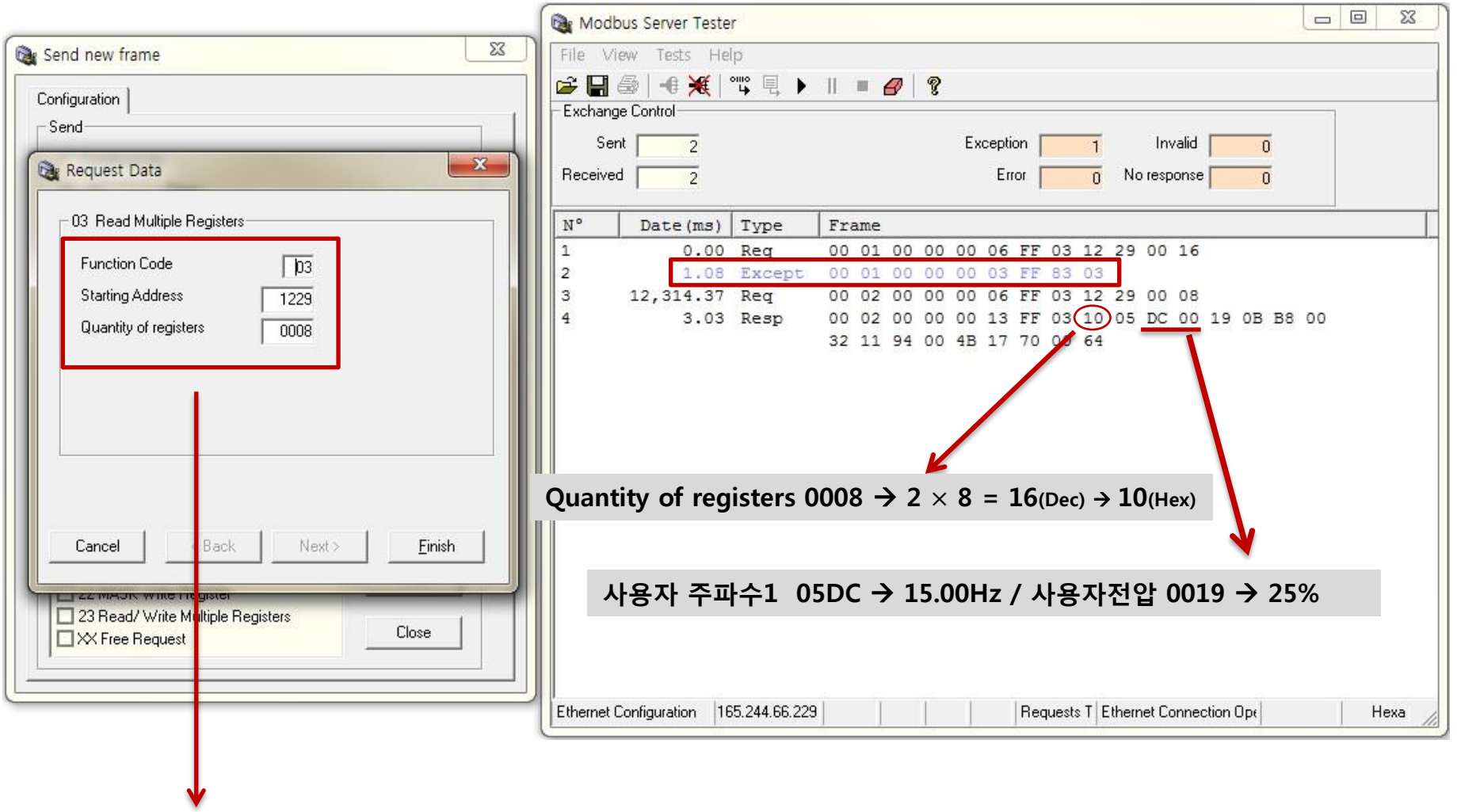
요구 Frame	길이	값
Function Code	1 Bytes	0x03
통신주소	1 Bytes	2 x Data 요구 개수
Data 요구 개수	Data 요구 개수 x 2 Bytes	통신 주소로부터 개수 만큼의 Data 값



Function Code 03 / Data 값 06 Bytes / 운전주파수 0B B8 → 30.00Hz / 운전지령 00001 → 정지상태 / 가속시간 00 C8 → 20.0sec

4. MODBUS TCP Function Code

- Read Holding Registers 2



Function Code 03 / Starting Address 0x1229 / Quantity of registers 0008 → 0x1229 ~ 0x1230(사용자주파수1~사용자전압4)

2) Write Single Registers

인버터(Server)에 있는 Data를 1개 수정할 때 사용하는 함수이다.

<Client에서 Server로 요구하는 Frame 구성>

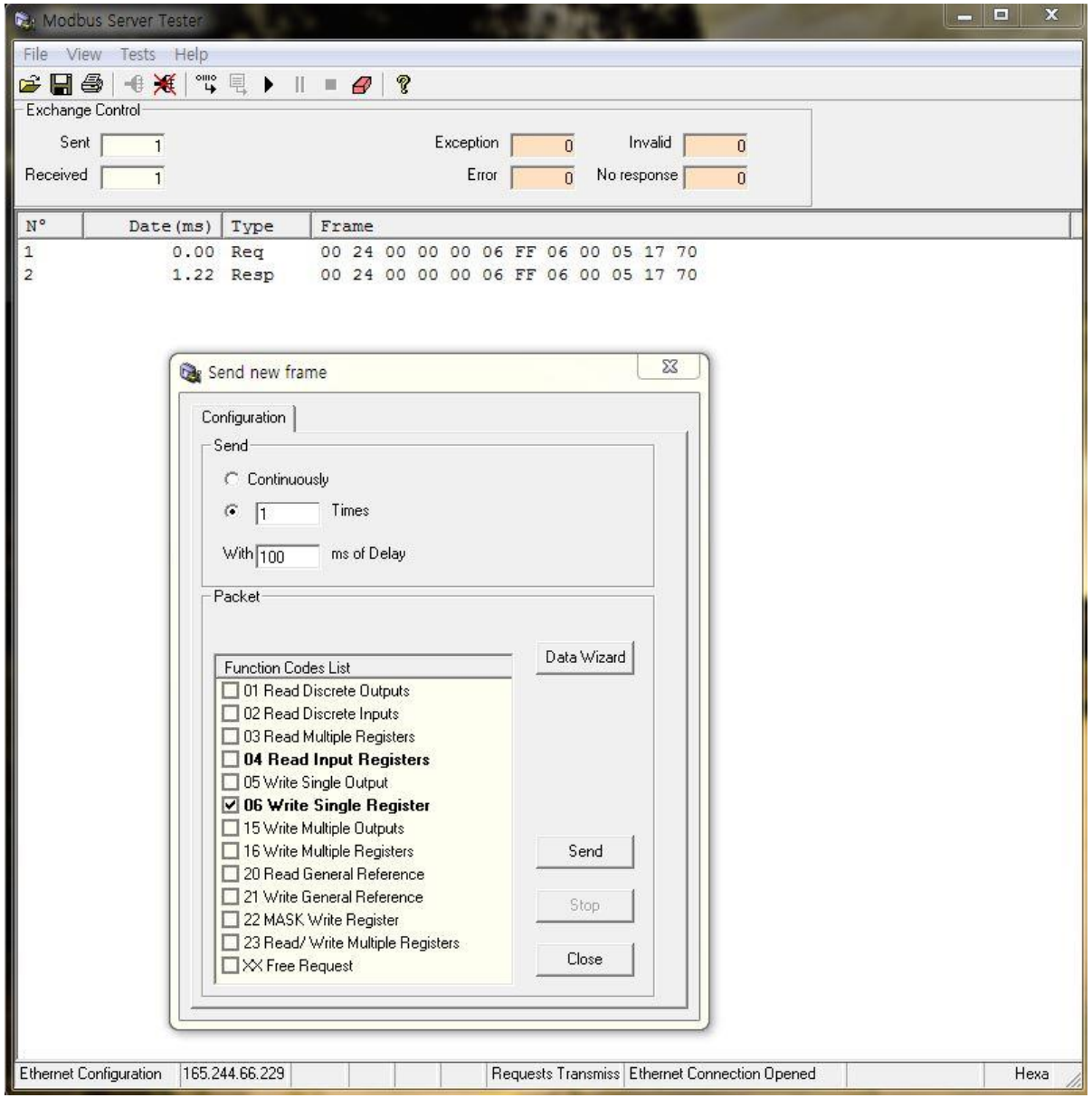
요구 Frame	길이	값
Function Code	1 Bytes	0x06
통신주소	2 Bytes	0x0000 ~ 0xFFFF
Data 값	2 Bytes	0x0000 ~ 0xFFFF

<Server에서 Master로 요구하는 Frame 구성>

요구 Frame	길이	값
Function Code	1 Bytes	0x06
통신주소	2 Bytes	0x0000 ~ 0xFFFF
Data 값	2 Bytes	0x0000 ~ 0xFFFF

4. MODBUS TCP Function Code

- Write Single Registers



Function Code → 0x06

통신주소 → 0x0005

Data → 0x1770

PDU(Protocol Data Unit)

Frame

Req 00 24 00 00 00 06 FF 06 00 05 17 70

Resp 00 24 00 00 00 06 FF 06 00 05 17 17

MBAP Header(MODBUS Application Protocol Header)

3) Write Multiple Registers

인버터(Server)에 Data를 1개에서 16개까지 연속적인 Data에 한하여 수정할 때 사용하는 함수이다.

<Client에서 Server로 요구하는 Frame 구성>

요구 Frame	길이	값
Function Code	1 Bytes	0x10
통신주소	2 Bytes	0x0000 ~ 0xFFFF
수정하는 Data 개수	2 Bytes	1~16 (LS산전 인버터 기준)
Byte Count	1Bytes	2 x Data 개수
수정할 Data 값	Data 개수 x 2 Bytes	수정할 Data

<Server에서 Master로 요구하는 Frame 구성>

요구 Frame	길이	값
Function Code	1 Bytes	0x10
통신주소	2 Bytes	0x0000 ~ 0xFFFF
Data 값	2 Bytes	1~16 (LS산전 인버터 기준)

4) Except Frame

Except Frame은 Client에서 Server로 요구하는 Frame을 보냈을 때 요구 Frame을 수행 하면서 Error 가 발생하였을 경우 Server에서 응답하는 Frame이다.

<Exception Frame 구성>

Error Frame	길이	값
Error Code	1 Bytes	0x10
Exception Code	1 Bytes	0x0000 ~ 0xFFFF

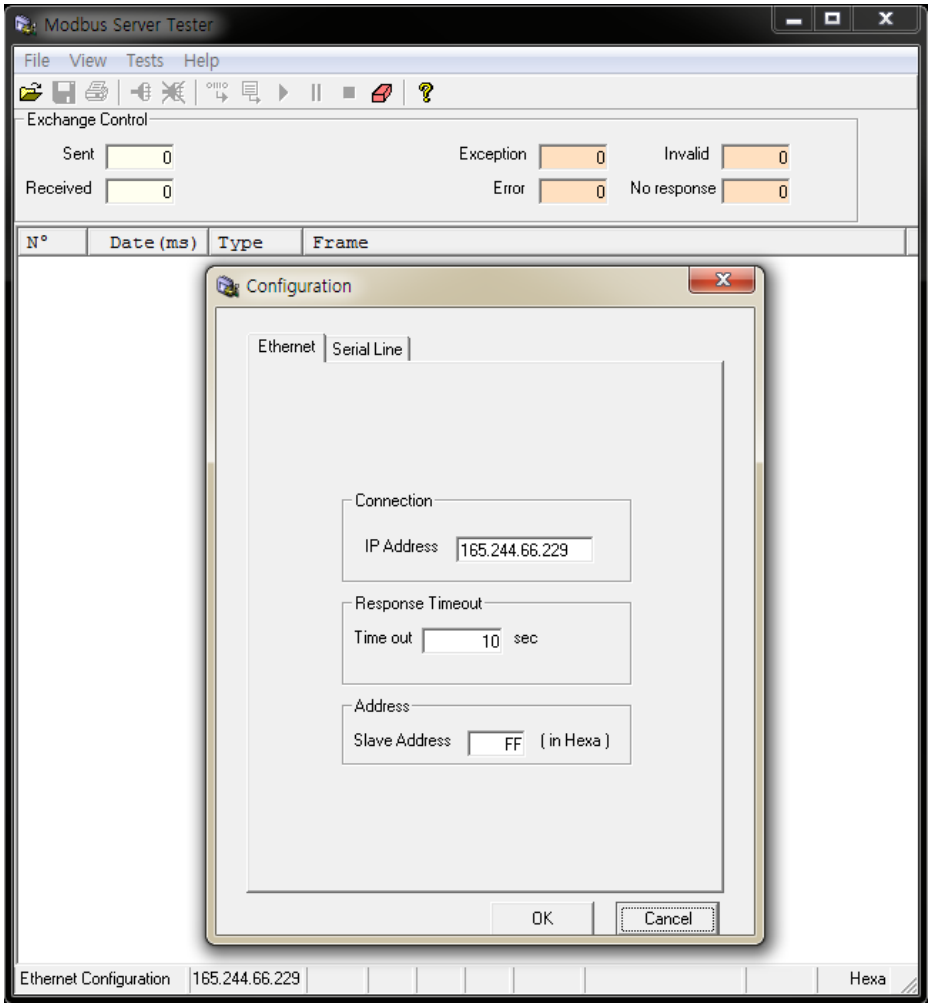
<Exception Code 종류>

종류	Code	설명
ILLEGAL FUNCTION	0x01	지원하지 않는 Function에 대해서 요구가 있을 경우
ILLEGAL DATA ADDRESS	0x02	사용하지 않는 어드레스의 Data를 요구하거나 수정하려는 경우
ILLEGAL DATA VALUE	0x03	Data 수정을 할 때 Data 허용 범위를 밖에 값으로 수정하려는 경우
SEAVE DEVICE FAILURE	0x04	Server에 오류가 있을 경우 (인버터와의 DATA통신 실패, CAN 통신/옵션 초기화 ERROR 발생할 경우)
SLAVE DEVICE BUSY	0x06	Server가 다른 처리 중이라서 응답을 할 수 없을 때 (인버터 파라미터 초기화, 옵션의 초기 설정 중일 경우)
WRITE PERMITION ERROR	0x20	LS 인버터에만 존재하는 Code로 수정 금지 파라미터에 값을 수정하려고 할 때

5. MODBUS Protocol Test Tool

- Inverter IP Address 등록

MODBUS Server Test Tool 실행하면 Configuration 화면이 생성되며 인버터의 IP Address 설정 후 통신을 시도한다.



<Inverter IP Address>

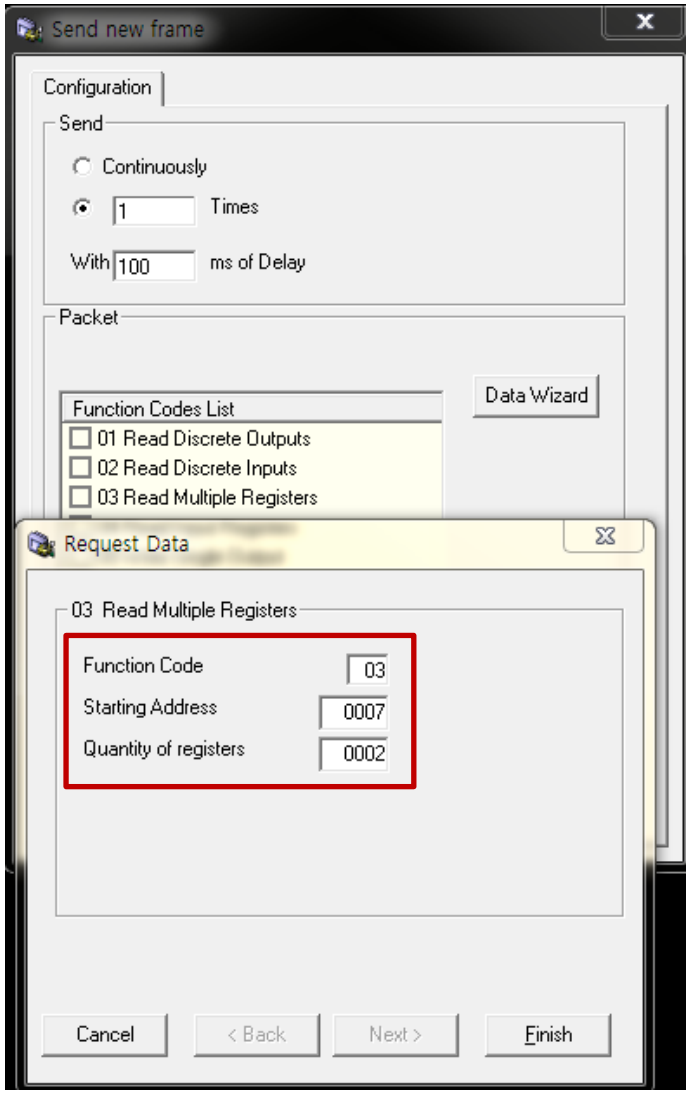
IP Address: 165.244.66.229 → A5.F4.42.E5

Subnet Mast: 255.255.255.192 → FF.FF.FF.C0

Gateway Address: 165.244.66.193 → A5.F4.42.C1

Code	기능표시	설정값	설명
COM-10	Opt Parameter1	0xA5E5	IP Address를 설정한다.
COM-11	Opt Parameter2	0x42FC	
COM-12	Opt Parameter3	0xFFFF	Subnet Mast를 설정한다.
COM-13	Opt Parameter4	0xFFC0	
COM-14	Opt Parameter5	0xA5F4	Gateway Address를 설정한다.
COM-15	Opt Parameter6	0x42C1	
COM-94	Comm Updata	NO → Yes	통신 관련 파라미터를 저장한다.

가감속 시간을 Read Multiple Registers 명령을 이용해서 통신으로 읽어본다.



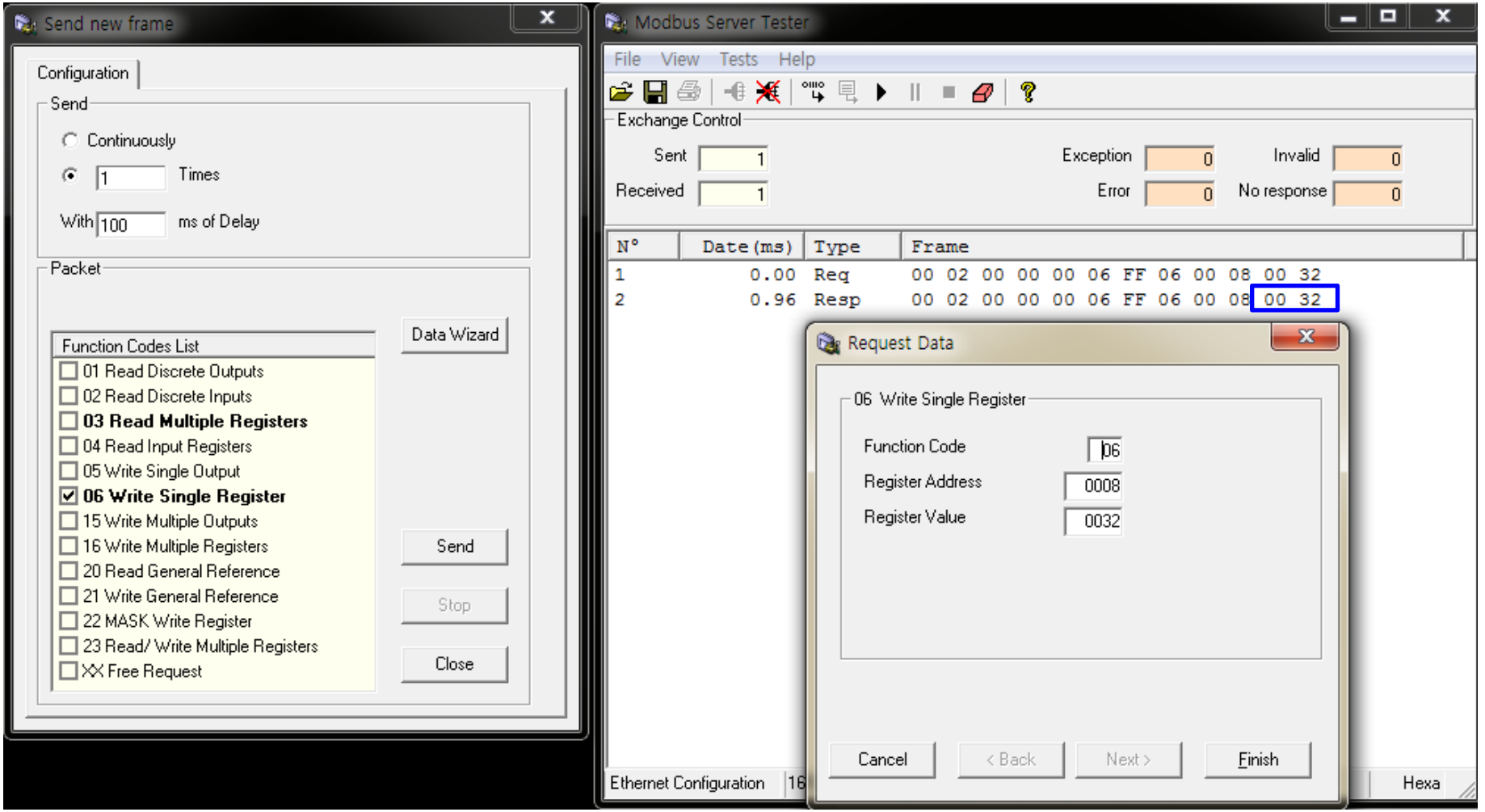
통신으로 가속 시간과 감속 시간이 올바른지 확인한다.

```
Req  17 5D 00 00 00 06 FF 03 00 07 00 02
Resp 17 5D 00 00 00 07 FF 03 04 00 37 00 64
```

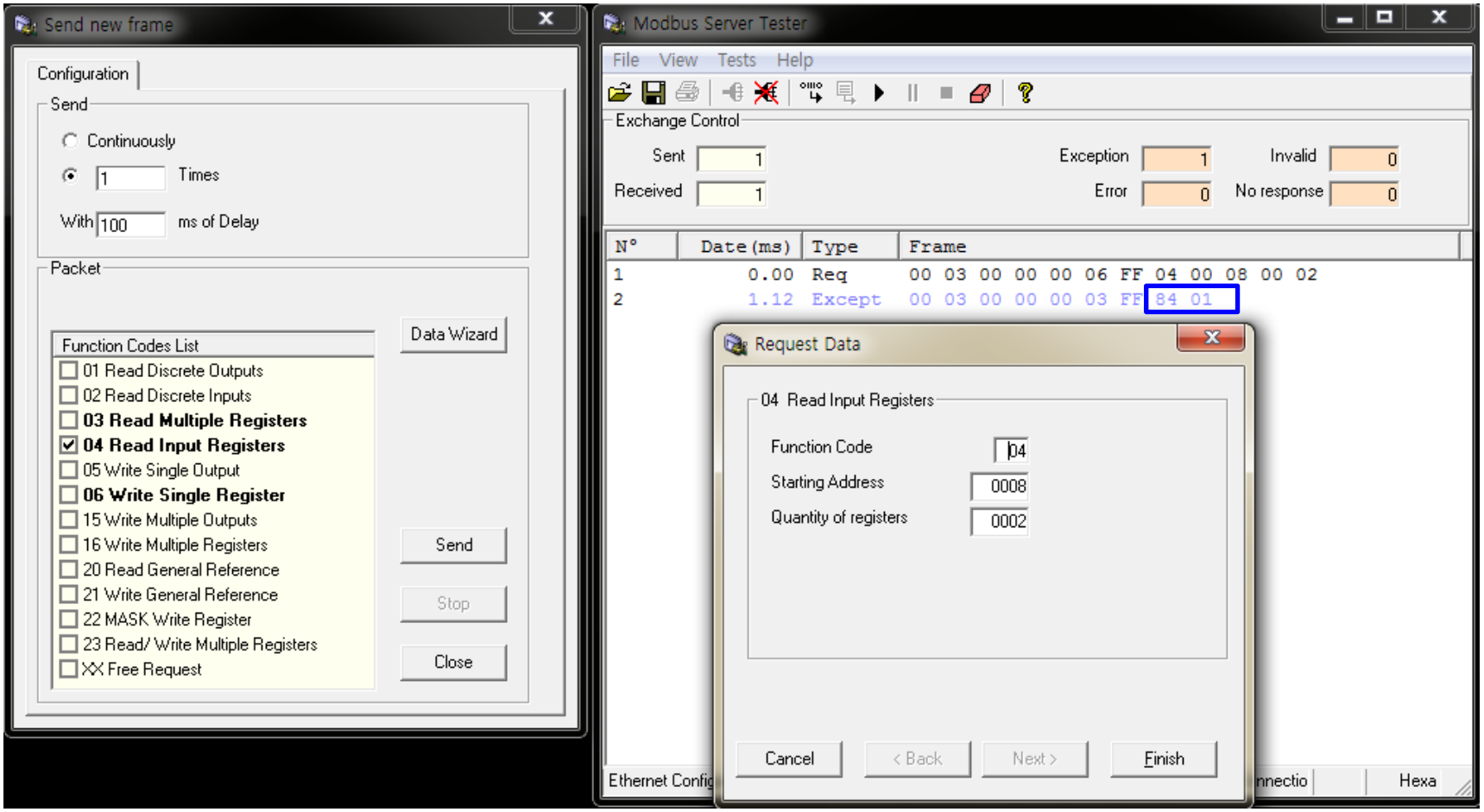
<설정 Parameter>

Code	기능표시	설정값
DRV-03	Acc Time	5.5 sec
DRV-04	Dec Time	10.0 sec

감속 시간을 Write Single Register 명령을 이용해서 5.0sec 로 Write한다.
송수신 Frame 확인 했을 때 0x0008 감속시간이 0032(hex) → 50(dec)→ 5.0sec 변경을 확인 할 수 있다.



MODBUS TCP가 제공하지 않는 Function을 입력 시 Error응답을 잘 하는지 확인한다.
아래 설정은 MODBUS TCP가 제공하지 않는 0x04 Function Code를 사용한 경우이다.



→ Error Code 1bytes 0x80 + Client가 요구한 Function Code
→ Exception Code 1bytes 0x001 → 지원하지 않는 Function에 대해서 요구가 있을 경우