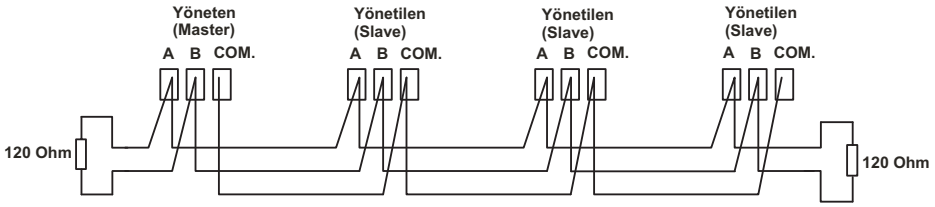
ENDA
MODBUS PROTOKOLÜ

1. GİRİŞ

Modbus protokolü istemci/sunucu mimarisine dayalı bir endüstriyel iletişim protokolüdür. İlk kez Modicon firması tarafından geliştirilmiş bir standart olup sahadaki cihazlar ile RS485 standardını kullanarak veri alınıp gönderilmesi işlevini görür. Ayrıntılı bilgi için Modicon Modbus Protokolü Referans Rehberine bakılabilir (PI-MBUS-300 Rev .J) .

Enda firmasınının Modbus Protokolünü destekleyen cihazları için desteklenen iletişim özellikleri aşağıdaki tabloda verilmiştir .

Arabirim Standardı	RS-485
İletişim Sistemi	Yarı Çift
Senkronizasyon Sistemi	Start Stop Senkronizasyonu
Veri Uzunluğu	8 Bit
Parite	NONE
Hata Kontrol Sistemi	CRC
Baud Rate	1200,2400,4800,9600,19200 bps
Bağlanabilecek Maksimum Cihaz Adedi	128
Maksimum hat uzunluğu	1200 m



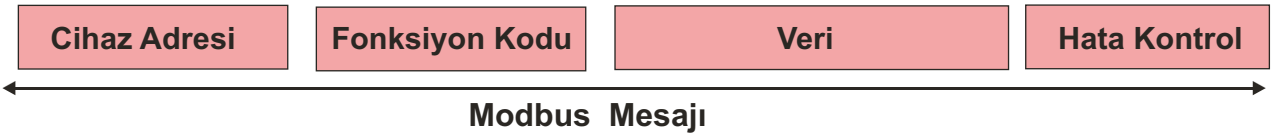
Bağlantı şekli olarak yukarıdaki konfigürasyon kullanılmalıdır. Yıldız ya da ağaç şeklindeki bağlantılar veri kayıplarına sebep olabileceği için tavsiye edilmez. Maksimum kablo uzunluğu haberleşme hızına (baud rate), kablo özelliğine (kapasite, karakteristik empedans vb.) ve hattaki cihaz sayısına göre değişir. Örneğin 9600 baud rate ve AWG26 kablo kullanıldığında maksimum uzunluk 1000 m olmalıdır.

Hattın başında ve sonunda 120 Ohm sonlandırma direnci kullanılmalıdır.

2. MODBUS PROTOKOLÜ

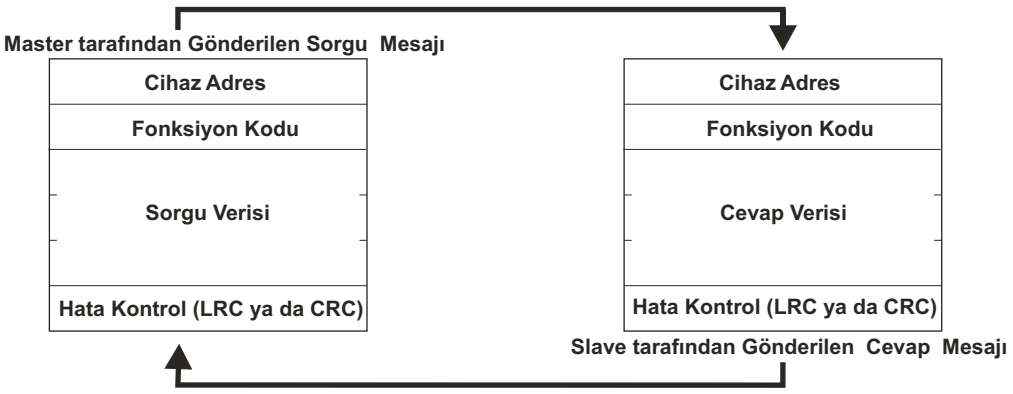
2.1 Genel Tanımlama

Modbus protokolü bilgi gönderip alırken Yöneten (Master) / Yönetilen (Slave) yöntemini kullanır. Bir Modbus ağında 1 Yöneten (Master) cihaz ve maksimum 247 Yönetilen (Slave) cihaz bulunabilmektedir. Yönetilen sürekli Yönetenden gelen mesajları dinlemede kalmalıdır. Sürekli gelen mesajları dinler ve gönderilen adres bilgisini kontrol eder. Eğer adres kendisinin adresi ise gelen mesaja cevap gönderir. Bir mesaj için kullanılan çerçeve aşağıdaki gibi 4 bloğun peşpeşe gönderilmesiyle oluşturulmaktadır.



Modbus Mesajı

İlk olarak adres bilgisi ile, mesajın hangi Yönetilen'e gönderildiği belirtilir. Daha sonra hangi fonksiyonun uygulanacağı belirtilir. Ardından veri gönderilir. En son olarak da verinin doğru gönderilip gönderilmediğini kontrol etmek için CRC veya LRC kodu gönderilir. Cevap veren Yönetilen ise yine aynı formatta cevap verir.



2.2 Modbus Mesaj Çerçevelemesi

ASCII Çerçevelemesi

Ascii çerçevelemesinde mesajlar iki nokta (:) karakteriyle başlar ve (CR-LF) Ascii karakterleriyle bitirilir(Hex karşılıkları 0x0D ve 0x0A)

BAŞLANGIÇ	ADRES	FONKSİYON	VERİ	LRC KONTROL	SON
1 KARAKTER	2 KARAKTER	2 KARAKTER	N KARAKTER	2 KARAKTER	2 KARAKTER (CRLF)

RTU Çerçevelemesi

RTU çerçevelemesinde mesajlar en az 3.5 karakter süresi kadar boşluk gönderilerek başlatılır. Daha sonra sırasıyla Adres, Fonksiyon, Veri ve CRC kontrol ile bitirilir. Çoğunlukla daha hızlı olduğu için RTU çerçevelemesi kullanılmaktadır. Veri gönderimi aşağıdaki şekilde görüldüğü gibi yapılmaktadır.

BAŞLANGIÇ	ADRES	FONKSİYON	VERİ	CRC KONTROL	SON
T1-T2-T3-T4	8 BİT	8 BİT	N * 8 BİT	16 BİT	T1-T2-T3-T4

Adres Bölümü : Bu kısımda veriyi alacak olan slave'in adresi belirtilir. Geçerli slave adres numaraları 1-247 arasındadır. Yöneten (Master) sahadaki hangi Yönetilen'e (Slave'e) bilgi gönderecekse onun adresini yazar. Cevap veren Yönetilen (Slave) ise aynı bölüme kendi adresini tekrar yazarak cevap verir. Bu sayede Yöneten (Master) doğru adresten bilgi geldiğini anlar.

Fonksiyon Bölümü : Geçerli fonksiyon kodları 1-255 arasındadır. Yönetenden (Masterdan) Yönetilene (Slave'e) bir mesaj gönderildiğinde Fonksiyon koduna göre o cihazın hangi çeşit işlem yapacağı belirtilir.

Yönetilen cevap verdiğinde fonksiyon kodu bölümüne bakarak Yönetilen'in (slave in) uygun cevap verip vermediği anlaşılır. Yönetilen (Slave) eğer herhangi bir uygunsuzluk sebebiyle hata kodu gönderecek ise Fonksiyon kodunun en değerlikli bitini lojik 1 yaparak geri gönderir. Bu durumda Yöneten (Master) hangi çeşit hatanın oluştuğunu anlar. Hata kodlarından ileride ayrıntılı olarak bahsedilecektir.

Veri Bölümü : Veri bölümündeki bilgi fonksiyon kodu ile tanımlanan fonksiyona göre hangi verinin kullanılması gerektiğini belirtir. Veri bölümünün uzunluğu 1-244 byte arasında olabilmektedir.

Hata Kontrol Bölümü : ASCII ve RTU çerçevelemelerinde iki değişik hata kontrol yöntemi kullanılmaktadır. RTU çerçevelemesinde CRC yöntemi kullanılmaktadır. ASCII çerçevelemesinde ise LRC yöntemi kullanılmaktadır.Ancak Enda cihazlarında sadece Modbus RTU protokolü uygulandığı için burada sadece CRC kontrolü yönteminden bahsedilecektir.

CRC Kontrolü

RTU modunda gönderilen ve alınan her mesajın içerisinde CRC kodu bulunmalıdır. Bunun amacı gelen bilginin hat üzerinde bütünlüğünün bozulmadan geldiğini anlayabilmektir. Çerçevedeki tüm veriler kullanılarak CRC-16 algoritmasına göre 2 Byte uzunluğunda CRC kodu oluşturulur. Algoritmanın detaylarına burada girilmeyecektir.

2.3 Modbus Veri Modeli

MODBUS veri modeli dört guruba ayrılır.Değişik fonksiyonlar için değişik veri grupları tahsis edilmiştir.

Veri Tipi	Nesne Tipi	Erişim Şekli	Adres Aralığı
Discretes Input	1 bit	Sadece Okunabilir	0 FFFFh
Coils	1 bit	Okunabilir ve Yazılabilir	0 FFFFh
Input Registers	16-bit word	Sadece Okunabilir	0 FFFFh
Holding Registers	16-bit word	Okunabilir ve Yazılabilir	0 FFFFh

Görüldüğü gibi Modbus ağına bağlı her cihazda verilerin okunup yazılması için belli bellek bölgeleri tahsis edilmesi gerekmektedir. Veri tipine göre değişik 4 ayrı bellek bölgesi tahsis edilmelidir. Modbus protokolünde 4 değişik veri formatı kullanılmaktadır. Adres aralıkları aynı fakat fiziksel olarak bellek bölgeleri farklıdır. Her fonksiyon kendisi ile ilgili bellek bölgesine veri yazar yada okur.

Coils

Coiller 1 bit ile temsil edilebilen sistem değişkenlerinin değiştirilebilmesini yada gözlemlenmesini sağlar. Örneğin bir rölenin açık yada kapalı oluşu ,bir fonksiyonun aktif olup olmayışı gibi. 0-FFFFh adres bölgesinde adreslenebilmektedir.

Discretes Input

Dijital girişlerin ON / OFF olma konumlarını okumak için kullanılır. Bu bellek bölgesinden sadece okuma yapılabilmektedir. Örneğin bir PLC de dijital girişlerin hangi konumda bulunduğunu okumak için kullanılabilmektedir. Adres bölgesi 0-FFFFh aralığındadır.

Input Registers

Bu bellek bölgesi cihazlardan analog girişleri okumak için yada cihazlardan bilgi toplamak için kullanılabilir. Bu registerlar 16 bit uzunluğunda olup sadece verileri okuma amacıyla kullanılmaktadır. Adres bölgesi 0-FFFFh aralığındadır.

Holding Registers

Bu bellek bölgesi sahadaki cihazdan eğer varsa analog çıkışların değerlerini yada cihazlara herhangi bir bilgi yollamak amacıyla kullanılabilmektedir. Adres bölgesi 0-FFFFh aralığındadır.

EUC442 UNIVERSAL CONTROLLER için maksimum veri sayıları:

Fonksiyon Kodu	Anlamı	Bir Mesaj İçindeki Maksimum Veri Sayısı	Mesajın Maksimum Uzunluğu(Byte)
$(01)_h$	Coilleri oku	16 bit	8 Byte
$(02)_h$	Discrete inputları oku	16 bit	8 Byte
$(03)_h$	Holding Registerları Oku	33 Word	72 Byte
$(04)_h$	Input Registerları Oku	1 Word	8 Byte
$(06)_h$	Tek Holding Registerı Oku	1 Word	8 Byte
$(0F)_h$	Coillere Yaz	16 bit	8 Byte
$(10)_h$	Holding Registerlara Yaz	33 Word	72 Byte

2.4 Modbus Fonksiyon Kodları ve Tanımlamaları

2.4.1 Read Coil Status (01h)

Bu fonksiyon kodu (0000 FFFFh) adresleri arasında bit düzeyindeki verileri okumak için kullanılmaktadır. Eğer 8 bitin katlarından az ise geriye kalan bitler için 0 koyulur.

Fonksiyon Kodu	Bir mesajda okunabilecek maksimum bit sayısı	Modbus Adres Aralığı
(01)h	2000 (07D0h)	0 - FFFFh

2.4.2 Read Discrete Inputs (02h)

Bu fonksiyon kodu (0000 FFFFh) adresleri arasında bit düzeyindeki kontrol çıkışlarını okumak için kullanılmaktadır. Mesajın yapısı Read Coil Status fonksiyonundaki gibidir.

Fonksiyon Kodu	Bir mesajda okunabilecek maksimum bit sayısı	Modbus Adres Aralığı
(02)h	2000 (07D0h)	0 - FFFFh

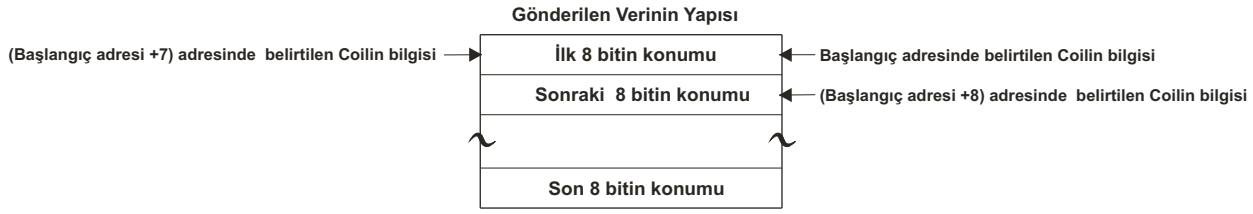
Mesajın Yapısı :

Komut Mesajının Yapısı (Byte Formatında)

Cihaz Adres	
Fonksiyon Kodu	
Okunacak Coillerin Başlangıç Adresi	MSB
	LSB
Okunacak Coil Sayısı(N)	MSB
	LSB
CRC DATA	LSB
	MSB

Cevap Mesajının Yapısı (Byte Formatında)

Cihaz Adres	
Fonksiyon Kodu	
Toplam Byte Sayısı (INTEGER{(N+7)/8})	
İlk 8 bitin konumu	
Sonraki 8 bitin konumu	
∿	∿
Son 8 bitin konumu	
CRC DATA	LSB
	MSB



Mesaj Örneği :

Burada (00000) adresinde bulunan Coilin bilgisi istenmektedir.

Komut Mesajının Yapısı (Byte Formatında)

Cihaz Adres		(01)h
Fonksiyon Kodu		(01)h
Okunacak Coillerin Başlangıç Adresi	MSB	(00)h
	LSB	(00)h
Okunacak Coil Sayısı(N)	MSB	(00)h
	LSB	(01)h
CRC DATA	LSB	(FD)h
	MSB	(CA)h

Cevap Mesajının Yapısı (Byte Formatında)

Cihaz Adres		(01)h
Fonksiyon Kodu		(01)h
Byte Sayısı		(01)h
İlk 8 bitin konumu		(00)h
CRC DATA	LSB	(51)h
	MSB	(88)h

Alınan verinin anlamı:

(0)	(0)	(0)	(0)	(0)	(0)	(0)	(0)

1 no lu Coil'in Değeri =0

2.4.3 Read Holding Registers (03h)

Başlangıç adresi ve miktar belirterek Holding Registerların peş peşe okunmasını sağlar. Gelen veriler önce en ağırlıklı byte(MSB) sonra düşük değerlikli byte(LSB) olarak gelir.

Fonksiyon Kodu	Bir mesajda okunabilecek maksimum word sayısı	Modbus Adres Aralığı
(03)h	125 (7D0h) Word	0 - FFFFh

Mesajın Yapısı :

Komut Mesajının Yapısı (Byte Formatında)

Cihaz Adres	
Fonksiyon Kodu	
Okunacak Registerların Başlangıç Adresi	MSB
	LSB
Okunacak Register Sayısı(N)	MSB
	LSB
CRC DATA	LSB
	MSB

1 ~ 125

Cevap Mesajının Yapısı (Byte Formatında)

Cihaz Adres	
Fonksiyon Kodu	
Toplam Okunacak Byte Sayısı	
İstenen ilk verinin içeriği (16 Bit)	MSB
	LSB
İstenen ikinci verinin içeriği (16 Bit)	MSB
	LSB
~	~
İstenen son verinin içeriği (16 Bit)	MSB
	LSB
CRC DATA	LSB
	MSB

Mesaj Örneği :

Aşağıdaki mesaj örneğinde (02)h adresine sahip olan cihazdan (0015)h göreli adresinden başlayarak 2 adet Holding Register okunmaktadır. Bu adreslerden sıcaklık set değerinin maksimum ve minimum değerleri okunmaktadır.

Komut Mesajının Yapısı (Byte Formatında)

Cihaz Adres		(02)h
Fonksiyon Kodu		(03)h
Okunacak Registerların Başlangıç Adresi	MSB	(00)h
	LSB	(18)h
Okunacak Register Sayısı	MSB	(00)h
	LSB	(02)h
CRC DATA	LSB	(XX)h
	MSB	(XX)h

Cevap Mesajının Yapısı (Byte Formatında)

Cihaz Adres		(02)h
Fonksiyon Kodu		(03)h
Byte Sayısı		(04)h
Okunacak ilk Holding Register'ın içeriği	MSB	(02)h
	LSB	(58)h
Okunacak ikinci Holding Register'ın içeriği	MSB	(0)h
	LSB	(0)h
CRC DATA	LSB	(49)h
	MSB	(58)h

Alınan verinin anlamı:

Sıcaklık set değerinin maksimum değeri : (0258)h = (600)

Sıcaklık set değerinin minimum değeri : (0000)h = (0)

2.4.4 Read Input Registers (04h)

Başlangıç adresi ve miktar belirterek Input Registerların peş peşe okunmasını sağlar. Gelen veriler önce en ağırlıklı byte(MSB) sonra düşük değerlikli byte(LSB) olarak gelir.

Fonksiyon Kodu	Bir mesajda okunabilecek maksimum word sayısı	Modbus Adres Aralığı
(04)h	125 (7D0h) Word	0 - FFFFh

Mesaj Yapısı :

Komut Mesajının Yapısı (Byte Formatında)

Cihaz Adres	
Fonksiyon Kodu	
Okunacak Registerların Başlangıç Adresi	MSB
	LSB
Okunacak Register Sayısı(N)	MSB
	LSB
CRC DATA	LSB
	MSB

1 ~ 125

Cevap Mesajının Yapısı (Byte Formatında)

Cihaz Adres	
Fonksiyon Kodu	
Toplam Okunacak Byte Sayısı	
İstenen ilk verinin içeriği (16 Bit)	MSB
	LSB
İstenen ikinci verinin içeriği (16 Bit)	MSB
	LSB
~	~
İstenen son verinin içeriği (16 Bit)	MSB
	LSB
CRC DATA	LSB
	MSB

Mesaj Örneği :

Aşağıdaki mesaj örneğinde sahada bulunan (05)h adresine sahip olan cihazdan (0000)h adresinden başlayarak 1 adet Input Register okunmaktadır. Adres tablosuna bakıldığında bu adreste ölçülen sıcaklık değerinin olduğu görülebilir.

Komut Mesajının Yapısı (Byte Formatında)

Cihaz Adres		(05)h
Fonksiyon Kodu		(04)h
Okunacak Registerların Başlangıç Adresi	MSB	(00)h
	LSB	(00)h
Okunacak Register Sayısı	MSB	(00)h
	LSB	(01)h
CRC DATA	LSB	(XX)h
	MSB	(XX)h

Cevap Mesajının Yapısı (Byte Formatında)

Cihaz Adres		(05)h
Fonksiyon Kodu		(04)h
Byte Sayısı		(02)h
Okunacak ilk Input Register'ın içeriği	MSB	(00)h
	LSB	(55)h
CRC DATA	LSB	(88)h
	MSB	(CF)h

Alınan verinin anlamı:

Ölçülen Sıcaklık Değeri : (0055)h = (85)

2.4.5 Write Single Register (06h)

Tek bir Holding Register ın adres belirterek okunmasını sağlar. Gelen veriler önce en ağırlıklı byte (MSB) sonra düşük değerlikli byte (LSB) olarak gelir.

Fonksiyon Kodu	Bir mesajda yazılabilecek maksimum word sayısı	Modbus Adres Aralığı
(06)h	1Word	0 - FFFFh

Mesajın Yapısı :

Komut Mesajının Yapısı (Byte Formatında)

Cihaz Adres	
Fonksiyon Kodu	
Yazılacak Register ın Başlangıç Adresi	MSB
	LSB
Yazılacak verinin içeriği (16 Bit)	MSB
	LSB
CRC DATA	LSB
	MSB

Cevap Mesajının Yapısı (Byte Formatında)

Cihaz Adres	
Fonksiyon Kodu	
Yazılan Registerın Başlangıç Adresi	MSB
	LSB
Yazılacak verinin içeriği (16 Bit)	MSB
	LSB
CRC DATA	LSB
	MSB

Mesaj Örneği :

Aşağıdaki mesaj örneğinde sahada bulunan (06)h adresine sahip olan cihazdan (0002)h adresinden başlayarak 1 adet Holding Registere veri yazılmaktadır. Adres tablosuna bakıldığında bu adreste Alarm 2 histeresiz parametresinin bulunduğu görülebilir.

Komut Mesajının Yapısı (Byte Formatında)

Cihaz Adres		(06)h
Fonksiyon Kodu		(06)h
Yazılacak Registerın Başlangıç Adresi	MSB	(00)h
	LSB	(02)h
Yazılacak verinin içeriği (16 Bit)	MSB	(00)h
	LSB	(11)h
CRC DATA	LSB	(E9)h
	MSB	(B1)h

Cevap Mesajının Yapısı (Byte Formatında)

Cihaz Adres		(06)h
Fonksiyon Kodu		(06)h
Yazılan Registerın Başlangıç Adresi	MSB	(00)h
	LSB	(02)h
Yazılacak verinin içeriği (16 Bit)	MSB	(00)h
	LSB	(11)h
CRC DATA	LSB	(E9)h
	MSB	(B1)h

Gönderilen verinin anlamı: Alarm2 histeresiz parametresini (11)h = 17 yap

2.4.6 Write Multiple Coils (0Fh)

Başlangıç adresi ve miktar belirterek Coillerin On yada Off yapılmasını sağlar. Eğer set edilecek coillerin sayısı 8'in katlarından az ise geri kalan bitler için Off yani '0' gönderilir.

Fonksiyon Kodu	Bir mesajda yazılabilecek maksimum coil sayısı	Modbus Adres Aralığı
(0F)h	7B0h bit	0 - FFFFh

Mesajın Yapısı :

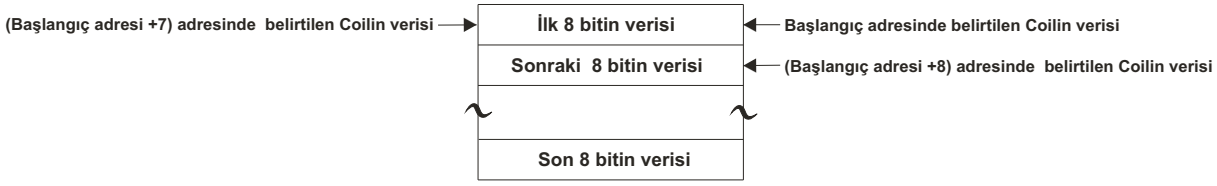
Komut Mesajının Yapısı (Byte Formatında)

Cihaz Adres	
Fonksiyon Kodu	
Yazılacak Coillerin Başlangıç Adresi	MSB
	LSB
Yazılacak Coil Sayısı(N)	MSB
	LSB
Toplam Byte Sayısı (INTEGER{(N+7)/8})	
İlk 8 bitin bilgisi	
Sonraki 8 bitin bilgisi	
~	~
Son 8 bitin bilgisi	
CRC DATA	LSB
	MSB

Cevap Mesajının Yapısı (Byte Formatında)

Cihaz Adres	
Fonksiyon Kodu	
Yazılacak Coillerin Başlangıç Adresi	MSB
	LSB
Yazılacak Coil Sayısı(N)	MSB
	LSB
CRC DATA	LSB
	MSB

Gönderilen Verinin Yapısı



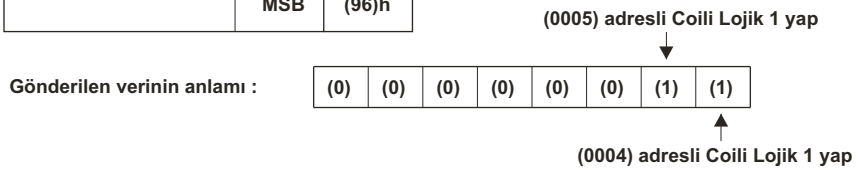
Mesaj Örneği :

Komut Mesajının Yapısı (Byte Formatında)

Cihaz Adres		(01)h
Fonksiyon Kodu		(0F)h
Yazılacak Coillerin Başlangıç Adresi	MSB	(00)h
	LSB	(04)h
Yazılacak Coil Sayısı(N)	MSB	(00)h
	LSB	(02)h
Toplam Byte Sayısı		(01)h
İlk 8 bitin bilgisi		(03)h
CRC DATA	LSB	(AE)h
	MSB	(96)h

Cevap Mesajının Yapısı (Byte Formatında)

Cihaz Adres		(01)h
Fonksiyon Kodu		(0F)h
Yazılacak Coillerin Başlangıç Adresi	MSB	(00)h
	LSB	(04)h
Yazılacak Coil Sayısı(N)	MSB	(00)h
	LSB	(02)h
CRC DATA	LSB	(95)h
	MSB	(CB)h



2.4.7 Write Multiple Holding Registers (10h)

Başlangıç adresi ve miktar belirterek Holding Registerlara peş peşe veri yazmak için kullanılır. Gönderilen veriler önce en ağırlıklı byte(MSB) sonra düşük değerlikli byte(LSB) olarak gönderilmelidir.

Fonksiyon Kodu	Bir mesajda yazılabilecek maksimum word sayısı	Modbus Adres Aralığı
(10)h	123 (7Bh) word	0 - FFFFh

Mesajın Yapısı :

Komut Mesajının Yapısı (Byte Formatında)

Cihaz Adres		
Fonksiyon Kodu		
Yazılacak Registerların Başlangıç Adresi	MSB	
	LSB	
Yazılacak Register Sayısı(N)	MSB	1 ~ 123
	LSB	
Byte Sayısı		N * 2
Yazılacak ilk verinin içeriği (16 Bit)	MSB	
	LSB	
Yazılacak ikinci verinin içeriği (16 Bit)	MSB	
	LSB	
~		
Yazılacak son verinin içeriği (16 Bit)	MSB	
	LSB	
CRC DATA	LSB	
	MSB	

Cevap Mesajının Yapısı (Byte Formatında)

Cihaz Adres	
Fonksiyon Kodu	
Yazılacak Registerların Başlangıç Adresi	MSB
	LSB
Yazılacak Register Sayısı(N)	MSB
	LSB
CRC DATA	LSB
	MSB

Mesaj Örneği :

Komut Mesajının Yapısı (Byte Formatında)

Cihaz Adres		(02)h
Fonksiyon Kodu		(10)h
Yazılacak Registerların Başlangıç Adresi	MSB	(00)h
	LSB	(16)h
Yazılacak Register Sayısı	MSB	(00)h
	LSB	(02)h
Byte Sayısı		(04)h
Yazılacak ilk verinin içeriği (16 Bit)	MSB	(00)h
	LSB	(7E)h
Yazılacak ikinci verinin içeriği (16 Bit)	MSB	(01)h
	LSB	(26)h
CRC DATA	LSB	(XX)h
	MSB	(XX)h

Cevap Mesajının Yapısı (Byte Formatında)

Cihaz Adres		(02)h
Fonksiyon Kodu		(10)h
Yazılacak Registerların Başlangıç Adresi	MSB	(00)h
	LSB	(16)h
Yazılacak Register Sayısı	MSB	(00)h
	LSB	(02)h
CRC DATA	LSB	(XX)h
	MSB	(XX)h

Gönderilen verinin anlamı:

(0016)h adresinde bulunan Ti_set paramatresi = (0x7E) = 12.6 dakika yap
(0017)h adresinde bulunan Td_set parametresi = (0x126) = 2.94 dakika yap